

中国电信集团公司文件

中国电信〔2008〕1521号

关于印发中国电信 IP 城域网设备 技术规范（V3.0）的通知

集团公司各省级分公司，股份公司并转各省级分公司，各专业公司，各研究院；中国通信服务股份有限公司：

为了逐步提升中国电信 IP 城域网的技术水平，更好地服务于全业务经营，集团公司技术部组织广州研究院对《中国电信 IP 城域网设备技术规范（V2.0）》（中国电信〔2007〕145号）进行了升级，形成了《中国电信 IP 城域网设备技术规范（V3.0）》，现随文印发，请各地在 IP 网络建设和改造工作中参照执行。



中国电信集团公司技术标准

Q/CT 2076-2008

中国电信 IP 城域网设备技术规范 (核心路由器)

(V3.0)

2008-12-31 发布

2009-1-1 实施

中国电信集团公司 发布

目 录

目 录.....	i
1 编制说明.....	1
1.1 范围.....	1
1.2 引用标准.....	1
1.3 定义、术语和缩写.....	9
1.3.1 定义.....	9
1.3.2 术语和缩写.....	9
2 概述.....	13
2.1 核心路由器的定位.....	13
2.2 核心路由器的功能组成.....	13
2.3 设备要求说明.....	14
2.4 设备分类.....	14
3 接口要求.....	15
3.1 常规.....	15
3.2 以太网接口.....	15
3.2.1 接口类型及特性.....	15
3.2.2 功能要求.....	16
3.3 POS 接口.....	16
3.3.1 接口类型及特性.....	16
3.3.2 链路层及功能要求.....	17
3.4 ATM 接口.....	18
3.4.1 接口类型及特性.....	18
3.4.2 ATM 层要求.....	18
3.5 其它接口.....	18
4 路由功能.....	19
4.1 常规要求.....	19
4.1.1 协议和地址.....	19
4.1.2 路由.....	19
4.2 OSPF 路由协议功能要求.....	20
4.3 ISIS 路由协议功能要求.....	21
4.4 RIPv1/v2 路由协议功能要求.....	23
4.5 BGP-4 路由协议功能要求.....	23
5 QoS.....	25
5.1 QoS 机制.....	25
5.2 QoS 能力.....	27
6 MPLS 功能.....	27
6.1 MPLS 基本功能.....	28
6.2 MPLS 流量工程 (TE).....	29
7 组播.....	29
8 IPv6.....	30
9 设备管理功能.....	31

9.1	基本管理功能	31
9.2	SNMP MIB	32
9.3	故障管理	34
9.4	配置管理	34
9.5	性能管理	35
9.6	安全管理	35
10	安全	35
10.1	访问控制和流量控制	35
10.2	路由协议安全	36
10.3	抗攻击能力	36
10.4	网络地址/端口翻译	37
10.5	冗余	37
11	性能	38
11.1	设备容量要求	38
11.1.1	设备整机处理能力	38
11.1.2	设备互通兼容能力	38
11.2	路由性能	38
11.3	组播性能	40
12	设备其它要求	40
12.1	机箱要求	40
12.2	线缆管理	40
12.3	设备可用性	40
12.4	定时与同步要求	41
12.5	网络时间同步	42
12.6	设备硬件要求	42
12.7	设备软件要求	42
12.8	环境要求	42
12.9	设备绿色要求	43
12.9.1	设备管理要求	43
12.9.2	设备环保与包装要求	43
12.9.3	能耗分级标准	44

1 编制说明

1.1 范围

本技术规范以 RFC 文档、IEEE 标准以及国内相关行业标准为依据，根据中国电信实际情况和具体要求，对 IP 城域网中核心路由器的定义、网络定位、路由功能、接口、用户管理、认证、计费、流量控制、拥塞管理、服务级别、组播应用、网络管理、网络安全等进行了规定。

本技术规范适用于中国电信集团宽带网络核心路由器的选型。

在本规范中：

必须：表示该条目是本规范必须，违反这样的要求是原则性错误。

必须实现：表示该要求必须实现，但不要求缺省使能。

不允许（不可以）：表示该条目绝对禁止。

应当（建议）：表示在某些特定条件下存在忽视该条目的理由，但是忽视或违反该条目时必须仔细衡量。

应当（建议）实现：与应当（建议）类似，实现时不必要缺省使能。

不应当（不建议）：表示在某些特定条件下存在所描述行为可接受或有效的理由，但实现该行为时必须仔细衡量。

可以：表示该条目确实可选。

1.2 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。

GB/T17625.1-2003	《电磁兼容 限值 谐波电流发射限值(设备每相输入电流≤16A)》
GB17625.2-1999	《电磁兼容 限值 对额定电流不大于 16A 的设备在低压供电系统中产生电压波动和闪烁的限制》
YD/T 1051-2000	《通信局站电源系统总技术要求》
SPECpower_ssJ2008	标准效能公司能耗测试标准
能源之星 4.0	主要针对消费性电子产品的能源节约计划。
COC on Energy Consumption of Broadband	宽带设备能源消耗管理

Equipment	
GB/T 2423 系列	电工电子产品的基本环境试验规程
GB/T 4798.3-1990	电工电子产品应用环境条件 有气候防护场所固定使用
GB/T 4798.1-2005	电工电子产品应用环境条件 贮存
GB/T 4798.9-1997	电工电子产品应用环境条件 产品内部的微气候
YDN 052-1998	B-ISDN ATM 层技术规范
YDN 053.4-1998	B-ISDN ATM 适配层（AAL）类型 5 技术规范
YDN 099-1998	光同步传送网技术体制（暂行规定）
YDN 104-1999	ATM 网络业务量控制和拥塞控制功能
YDN 120-1999	光波分复用系统总体技术要求（暂行规定）
YD/T 877-1996	同步数字体系(SDH)利用设备和系统的电接口技术要求
YD/T 973-1998	SDH 155Mb/s 和 622Mb/s 光发送模块和光接收模块技术条件
YD/T 976-1998	B-ISDN 用户网络接口(UNI)物理层规范
YD/T 1097-2001	路由器设备技术规范-高端路由器
YDN 1109-2001	ATM 交换机设备技术规范
YD/T 1111.1-2001	SDH 光发送/光接收模块技术要求-2.488320Gb/s 光接收模块
YD/T 1111.2-2001	SDH 光发送/光接收模块技术要求-2.488320Gb/s 光发送模块
YD/T 1162.1-2005	多协议标签交换（MPLS）技术要求
YD/T 1162.2-2001	在 ATM 上实现 MPLS 的技术要求
YD/T 1190-2002	基于网络的虚拟 IP 专用网（IP-VPN）框架
YD/T 1199.1-2002	SDH 光发送/光接收模块技术要求-SDH 10Gb/s 光接收模块
YD/T 1199.2-2002	SDH 光发送/光接收模块技术要求-SDH 10Gb/s 光发送模块
YD/T 1267-2003	基于 SDH 传送网的同步网技术要求
YD/T 1345-2005	基于 SDH 的多业务传送节点（MSTP）技术要求-内嵌弹性分组环（RPR）功能部分
YD/T 1359-2005	路由器设备安全技术要求一高端路由器（基于 IPv4）
YD/T 1471-2006	基于 IP 的二层虚拟专用网（VPN）业务技术要求

YD/T 1474-2006	基于 SDH 的多业务传送节点（MSTP）技术要求-内嵌多协议标签交换（MPLS）功能部分
YD/T 1476-2006	基于边界网关协议/多协议标签交换的虚拟专用网（BGP/MPLS VPN）技术要求
YD/T 1477-2006	基于边界网关协议/多协议标签交换的虚拟专用网（BGP/MPLS VPN）组网要求
RFC 768	UDP 协议
RFC 791	IP 协议
RFC 792	ICMP 协议
RFC 793	TCP 协议
RFC 826	以太网 ARP 协议
RFC 854	TELNET 协议规范
RFC 862	Echo 协议
RFC 863	丢弃协议
RFC 894	在以太网上传输 IP 数据报的标准
RFC 896	IP/TCP 互联网拥塞控制
RFC 922	IP 广播
RFC 950	IP 相关子网
RFC 959	FTP
RFC 1042	在 IEEE802 网络上的 IP 数据报传输标准
RFC 1122	互联网主机要求一通信层
RFC 1144	低速串行链路上的 TCP/IP 头的压缩算法
RFC 1155	基于 TCP/IP 的互联网管理信息的结构和标识
RFC 1157	简单网络管理协议
RFC 1166	互联网号码
RFC 1195	用于在 TCP/IP 和 OSI 双重环境中 IS-IS 路由
RFC 1212	简明 MIB 定义
RFC 1213	基于 TCP/IP 的互联网的网络管理信息库：MIB-II
RFC 1256	ICMP 路由器发现消息

RFC 1321	MD5 算法
RFC 1332	IPCP 协议
RFC 1334	PAP 协议
RFC 1519	CIDR：一种地址分配和聚合的策略
RFC 1631	IP 网络地址转换(NAT)
RFC 1661	PPP 协议
RFC 1662	在类 HDLC 帧中的 PPP 协议
RFC 1772	互联网中 BGP 的应用
RFC 1812	IPv4 路由器要求
RFC 1918	私网地址分配
RFC 1990	PPP 多链协议
RFC 1994	CHAP 协议
RFC 1997	BGP 团体属性
RFC 1998	多归属路由中 BGP 团体属性的应用
RFC 2080	IPv6 的 RIPng
RFC 2082	RIP v2 MD5 认证
RFC 2153	PPP 厂商扩展
RFC 2205	RSVP 功能技术规范
RFC 2209	RSVPv1 消息处理规则
RFC 2210	IETF 综合业务的 RSVP 使用
RFC 2228	FTP 安全扩展
RFC 2236	互联网组管理协议 IGMPv2
RFC 2328	OSPF v2 协议
RFC 2362	协议无关组播—稀疏模式
RFC 2364	AAL5 上的 PPP
RFC 2385	通过 TCP MD5 签名选项对 BGP 会话的保护
RFC 2370	OSPF Opaque LSA 选项
RFC 2401	互联网协议安全体系

RFC 2439	BGP4 路由振荡抑制
RFC 2453	RIPv2 协议
RFC 2460	互联网协议—第六版（IPv6）规范
RFC 2461	IPv6 的邻居发现
RFC 2464	在以太网上传送 IPv6 报文
RFC 2465	IPv6 MIB 的文本规定和总体组
RFC 2466	IPv6 MIB: ICMP 组
RFC 2474	IPv4 和 IPv6 报头中 DS 字段的定义
RFC 2475	Diff-Serv 体系结构
RFC 2484	PPP LCP 国际配置选项
RFC 2515	ATM 管理目标定义
RFC 2516	传输 PPPoE 之方法
RFC 2529	在 IPv4 域中不使用显式隧道传输 IPv6
RFC 2545	用于 IPv6 域间路由的 BGP-4 多协议扩展
RFC 2597	AF PHB 组
RFC 2615	SONET/SDH 上 PPP 协议
RFC 2661	L2TP 协议
RFC 2684	AAL5 上的多协议封装
RFC 2697	单一速率三色标记
RFC 2698	两个速率三色标记
RFC 2702	MPLS 上 TE 要求
RFC 2750	用于策略控制的 RSVP 扩展
RFC 2763	IS-IS 动态主机名交换机制
RFC 2773	使用 KEA 和 SKIPJACK 的加密技术
RFC 2858	BGP-4 多协议扩展
RFC 2865	RADIUS 协议—认证
RFC 2866	RADIUS 协议—计费
RFC 2867	RADIUS 协议—隧道协议的计费
RFC 2868	RADIUS 协议—隧道协议的认证

RFC 2869	RADIUS 协议扩展
RFC 2918	BGP-4 路由刷新能力
RFC 2966	两层 ISIS 域范围的前缀分发
RFC 3022	传统的 IP 网络地址翻译
RFC 3031	MPLS 体系架构
RFC 3032	MPLS 标签堆栈编码
RFC 3035	使用 LDP 和 ATM VC 交换的 MPLS
RFC 3036	LDP 技术规范
RFC 3037	LDP 适用性
RFC 3063	MPLS 环回检测机制
RFC 3065	BGP 自治系统联盟
RFC 3101	OSPF NSSA 选项
RFC 3168	IP 显式拥塞通知(ECN)的增加
RFC 3170	IP 组播应用: 挑战和解决方案
RFC 3181	预占通知的优先级策略要素
RFC 3209	RSVP-TE: LSP 隧道的 RSVP 扩展
RFC 3241	PPP 上强健性头压缩
RFC 3246	快速 (EF) PHB
RFC 3260	Diffserv.新增术语和澄清
RFC 3272	互联网流量工程概述和原则
RFC 3277	IS-IS 瞬时黑洞避免
RFC 3346	MPLS 流量工程适用性说明
RFC 3373	IS-IS 点对点邻接的三次握手
RFC 3376	互联网组管理协议—第三版 (IGMPv3)
RFC 3392	BGP-4 能力发布
RFC 3443	MPLS 网络中 TTL 处理
RFC 3478	LDP 平滑重启机制
RFC 3564	支持差分服务感知的 MPLS 流量工程要求

RFC 3576	RADIUS 动态认证扩展
RFC 3618	组播源发现协议
RFC 3623	OSPF 平滑重启
RFC 3630	OSPFv2 的流量工程扩展
RFC 3635	以太网接口类型的管理目标定义
RFC 3784	IS-IS 的流量工程扩展
RFC 3768	虚拟路由器冗余协议 (VRRP)
RFC 3847	IS-IS 的重启信令
RFC 3936	修改 RSVP 过程
RFC 4022	TCP 的 MIB
RFC 4087	IP 隧道 MIB
RFC 4090	用于 LSP 隧道的 RSVP-TE 快速重路由
RFC 4113	UDP 的 MIB
RFC 4182	删除 MPLS 显式为 NULL 的限制
RFC 4203	支持 GMPLS 的 OSPF 扩展
RFC 4205	支持 GMPLS 的 IS-IS 扩展
RFC 4271	边界网关协议—第 4 版 (BGP-4)
RFC 4273	BGP-4 管理目标定义
RFC 4292	IP 转发表 MIB
RFC 4293	IP 的 MIB
RFC 4302	IP 认证头
RFC 4303	IP 安全载荷封装
RFC 4305	安全载荷封装 (ESP) 和认证头 (AH) 加密算法实现要求
RFC 4364	BGP/MPLS IP 虚拟专用网
RFC 4379	MPLS 数据平面故障检测
RFC 4420	使用 RSVP 流量工程建立 MPLS LSP 的属性编码
RFC 4456	BGP 路由反射
RFC 4486	BGP 中止通知消息子编码
RFC 4495	减少一个流的预留带宽的 RSVP 扩展

RFC 4560	远程 Ping, Traceroute, 和 Lookup 操作的管理目标定义
RFC 4576	BGP/MPLS IP VPN 中使用 LSA 选项比特阻止环回
RFC 4577	BGP/MPLS IP VPN 中运营商/客户之间使用 OSPF 协议
RFC 4724	BGP 的平滑重启功能
RFC 4915	OSPF 多拓扑路由功能
RFC 5304	IS-IS 加密认证
RFC 5308	Routing IPv6 with IS-IS
RFC 5120	ISIS 多拓扑路由功能
RFC 5309	链路状态路由协议 LAN 上的点到点操作要求
RFC 5340	OSPF for Ipv6
IEEE 802.1ad	运营商桥接
IEEE 802.1p	服务等级和优先级标准
IEEE 802.1Q	虚拟局域网
IEEE 802.3	CSMA/CD 访问方法和物理层技术规范
IEEE 802.3ac	VLAN 标记扩展
IEEE 802.3ae	10Gb/s 以太网物理层接口规范
IEEE 802.3ab	1000Base-T 以太网物理层接口规范
IEEE 802.3ad	链路聚合
IEEE 802.3u	100Base-T 以太网接口物理层规范
IEEE 802.3x	以太网接口流量控制
IEEE 802.3z	千兆以太网接口物理层规范
IEEE 802.17	RPR 物理层规范
ITU-T G.707	SDH 网络节点接口
ITU-T I.610	B-ISDN 操作和维护原则功能
ITU-T I.731	ATM 设备类型和通用特征
ITU-T I.732	ATM 设备功能特征
ATM Forum af-uni-0010.002	ATM 用户-网络接口规范 V3.1

ATM Forum af-tm-0121.000	业务量管理规范 V4.1
ATM Forum af-tm-0149.000	业务量管理规范 V4.1-补遗：差分 UBR 业务
ATM Forum af-tm-0150.000	业务量管理规范 V4.1-补遗：UBR 最小接入信元速率的可选指示
draft-ietf-bfd-base-08	双向转发检测
draft-ietf-bfd-v4v6-1hop-08	IPv4/v6 双向转发检测（单跳）
draft-ietf-bfd-multihop-06	多跳路径的双向转发检测
draft-ietf-bfd-mpls-07	MPLS LSP 中的双向转发检测
draft-martini-l2 circuit-trans-mpls-19	Martini 二层 MPLS VPNs
draft-ietf-isis-wg- multi-topology-11	IS-IS 的多拓扑路由
draft-ietf-isis-igp-p2p-over-lan-06	链路状态路由协议 LAN 上的点到点操作
draft-ietf-ospf-mt-06	OSPF 的多拓扑路由

1.3 定义、术语和缩写

1.3.1 定义

核心路由器（Core Router，简称 CR）位于城域网的核心层，负责进行业务接入控制点设备汇接，并提供城域网到骨干网的出口。

1.3.2 术语和缩写

AAL	ATM Adaptation Layer（ATM 适配层）
ACL	Access Control List（访问控制列表）
ADSL	Asymmetric Digital Subscriber Line（非对称数字用户线）
AF	Assured Forward（确保转发）
AIS	Alarm Indication Signal（告警指示信号）
APS	Auto-Protection Switching（自动保护倒换）
ATM	Asynchronous Transfer Mode（异步转移模式）
BGP	Border Gateway Protocol（边界网关协议）

BF	Besteffort Forwarding (尽力转发)
BITS	Building Integrated Timing Source (通信楼综合定时供给系统)
BRAS	Broadband Remote Access Service (宽带远程接入服务)
CAR	Committed Access Rate (提交的接入速率)
CBS	Committed Burst Size (提交的突发长度)
CBWFQ	Class-Based Weighted Fair Queueing (基于类的加权公平排队)
CPE	Customer Presidial Equipment (用户驻地设备)
CIR	Committed Information Rate (提交信息速率)
CQ	Custom Queuing (自定义排队)
CR	Core Router (核心路由器)
DHCP	Dynamic Host Configuration Protocol (动态主机配置协议)
DiffServ	Differentiate Service (差分服务)
DSCP	Diff-Serv Code Point (差分服务码点)
DSLAM	Digital Subscriber Line Access Multiplexer (数字用户接入线复用器)
EBS	Exceed Burst Size (超过的突发长度)
E-LSP	EXP-Inferred-PSC LSPs (PSC 使用 exp 字段的 LSP)
ECMP	Equal Cost Multi-Path (等值多路径)
FRR	Fast ReRoute (快速重路由)
GBIC	GigaBit Interface Converter (吉比特接口转换器)
GE	Gigabits Ethernet (千兆以太网)
GRE	Generic Routing Encapsulation (通用路由协议封装)
ICP	Internet Content Provider (互联网内容提供商)
IGMP	Internet Group Management Protocol (互联网组管理协议)
IPsec	IP Security Protocol (IP 网络安全协议)
IPTV	IP Television (IP 电视)
IS-IS	Intermediate System to Intermediate System (中间系统到中间系统)
ISP	Internet Service Provider (互联网服务提供商)
L2TP	Layer 2 Tunneling Protocol (第二层隧道协议)

LAC	L2TP Access Concentrator (L2TP 接入集中器)
LAN	Local Area Networks (局域网)
LDP	Label Distribution Protocol (标签分发协议)
LLC	Logical Link Control (逻辑链路控制)
LLQ	Low Latency Queue (低延迟队列)
L-LSP	Label-Only-Inferred-PSC LSP
LNS	L2TP Network Server (L2TP 网络服务器)
LSP	Label Switch Path (标签交换路径)
MAC	Media Access Control (介质访问控制)
MDCR	Minimum Desired Cell Rate (最小希望信元速率)
MBGP	Multi-Protocol BGP (多协议 BGP)
MPLS	Multi-Protocol Label Switching (多协议标签交换)
MPLS EXP	MPLS experimental Field (MPLS 试验字段)
MSDP	Multicast Source Discover Protocol (组播源发现协议)
MSTP	Multi-Service Transport Platform (多业务传送平台)
MTBF	Mean Time Between Failures (平均无故障间隔时间)
OAM	Operation And Maintenance (操作和维护)
OSI	Open System Interconnection (开放的系统互联)
OSPF	Open Shortest Path First Protocol (开放式最短路径优先协议)
OUT	Optical Transport Unit (光传送单元)
PE	Provider Edge (运营商边缘)
PHB	Per-Hop Behavior (每跳行为)
PoS	Packet over SDH (SDH 上承载分组)
PPP	Point To Point Protocol (点到点协议)
PPPOA	PPP Over AAL5 (AAL5 上承载 PPP)
PPPOE	PPP Over Ethernet (以太网上承载 PPP)
PPS	Packets Per Second (每秒分组数)
PSC	PHB Scheduling Class (PHB 预定类别)
PVC	Permanent Virtual Circuit (永久虚连接)

PQ	Priority Queuing （优先级排队）
QoS	Quality of Service （服务质量保证）
RADIUS	Remote Authorization Dial In User Service （远程认证拨号用户服务）
RDI	Remote Defect Indication （远端故障指示）
RED	Random Early Detection （随机早期检测）
RIP	Routing Information Protocol （路由信息协议）
RPR	Resilient Packet Ring （弹性分组环）
SDH	Synchronous Digital Hierarchy （同步数字序列）
SDN	Switched Data Network （交换数据网）
SNAP	Service Network Access Point （业务网络接入点）
SNMP	Simple Network Management Protocol （简单网络管理协议）
CR	Service Router （业务路由器）
TE	Traffic Engineering 流量工程
TOS	Type Of Service 业务类型
uRPF	unicast Reverse Path Forwarding （单播反向路径转发）
VLAN	Virtual LAN （虚拟局域网）
VC	Virtual Channel （虚通道）
VP	Virtual Path （虚通路）
VPDN	Virtual Private Dial_up Network （虚拟拨号专网）
VPLS	Virtual Private LAN Service （虚拟专用以太网服务）
VPN	Virtual Private Network （虚拟专用网）
VR	Virtual Router （虚拟路由器）
VRF	Virtual Route Forwarding Table （VPN 路由转发表）
WRED	Weighted Random Early Detection （加权随机早期检测）
WRR	Weighted Round-Robin （加权循环队列调度）

2 概述

2.1 核心路由器的定位

IP 城域网的网络结构分为城域网骨干网和宽带接入网两个层面，城域网骨干网是业务接入控制点（包括 BRAS 和业务路由器）及控制点以上的城域网核心路由器组成的三层路由网络，划分为核心层和业务接入控制层两层。

核心路由器为核心层唯一组成设备，负责进行业务接入控制点设备汇接并提供 IP 城域网到骨干网的出口。核心路由器可级联为两级。其中，出口路由器双挂 ChinaNet 和 CN2，提供 IP 城域网到骨干网的出口；其它核心路由器上联出口路由器，完成业务接入控制点的分片汇接。

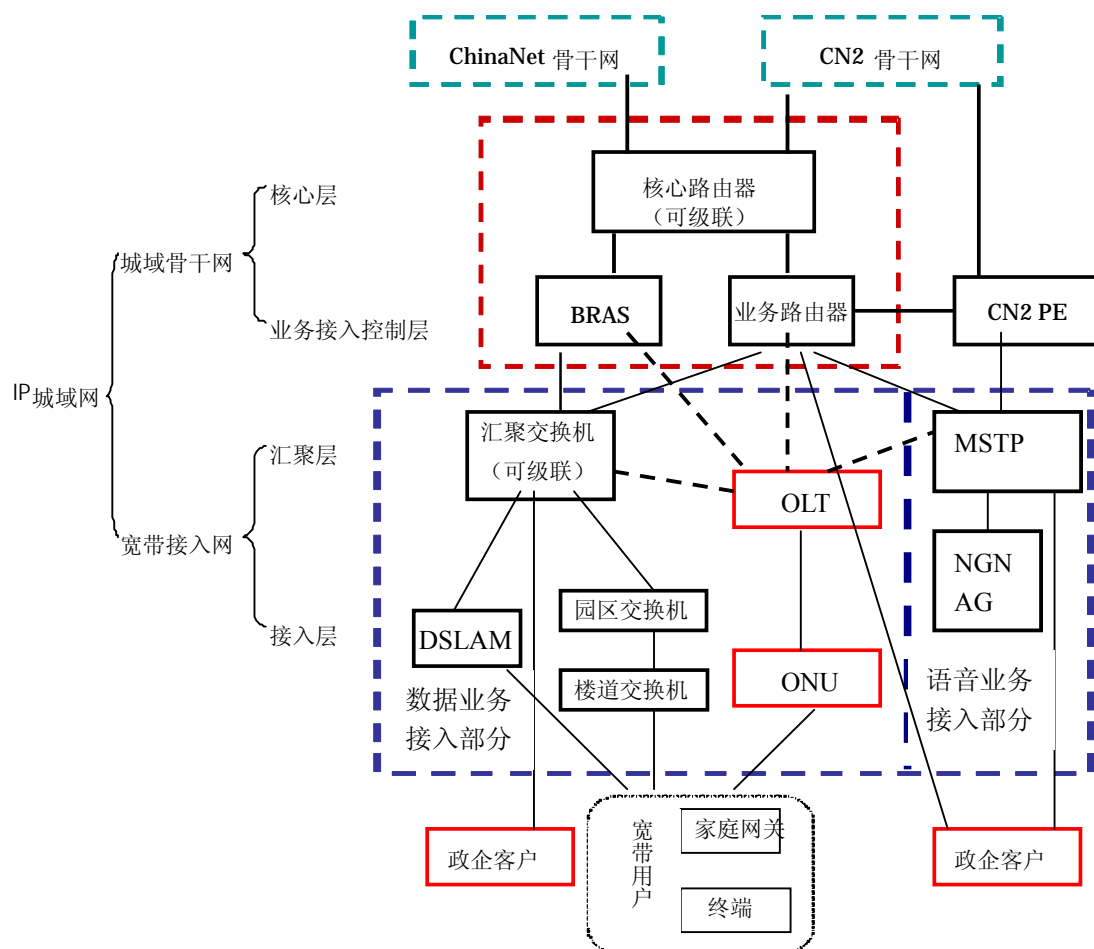


图 2-1 中国电信IP城域网网络拓扑图

2.2 核心路由器的功能组成

CR 作为路由器设备，应能提供符合 YD/T 1097-2001《路由器设备技术规范—高端路由器》4.2 节中的高端路由器功能要求。

CR 主要完成城域网与长途骨干网设备的出口对接, 完成对城域网内部对 SR/BRAS 的汇接, 及在城域网开展 MPLS VPN 后充当城域网的 P 设备。核心路由器的功能组成包括: 路由功能 (包括路由策略控制)、QoS 功能、MPLS 功能、组播功能、设备管理和安全功能。

2.3 设备要求说明

根据集团对 IP 城域网优化指导意见, 在特大型、大型和部分业务量大的中兴 IP 城域网, 可设置两级级联的核心路由器 (通常称为汇接路由器和出口路由器), 其余城域网只设置单级核心路由器。

除非有特殊说明, 以下章节中出口路由器与汇接路由器所必需具备的功能与性能都归纳为核心路由器所应具备。

2.4 设备分类

根据城域网的规模 and 用户业务开展情况, 将中国电信城域网核心路由器分为两类如下:

表 2-1 中国电信IP城域网核心路由器分类表

	A 类	B 类	C 类	D 类
单槽交换及可配置容量	不少于 40G (单向)	不少于 40G (单向)	不小于 40G (单向)	不小于 10G (单向)
整机端口线速配置容量	不小于 2.56T (单向)	不小于 1.28T (单向)	不小于 640G (单向)	不小于 320G (单向)
交换矩阵与背板容量	不少于 5.12T (单向)	不小于 2.56T (单向)	不小于 1.28T (单向)	不小于 640G (单向)
部署位置	大型城域网	大型城域网	中型城域网	中小型城域网
接口要求	必须支持 40GPoS、10GPOS、10GE、2.5GPOS、GE 接口	必须支持 40GPoS、10GPOS、10GE、2.5GPOS、GE 接口	必须支持 10GPOS、10GE、2.5GPOS、GE 接口, 支持升级到 40G 端口能力	必须支持 10GPOS、10GE、2.5GPOS、GE 接口
架构要求	支持集群形式	支持集群形式	可扩展至集群形式	

3 接口要求

3.1 常规

CR 必须具备通过 RS-232C VT-100 类型终端访问的控制接口。

CR 应该具备冗余得 BITS 外部时钟输入接口。

CR 必须能够从通道化接口取得时钟。

CR 必须支持在所有 SONET/SDH/TDM 端口的物理端口 loopback。

CR 必须支持 100BASE/GE/2.5G POS 接口, 必须支持 10GE、10G POS 接口, 建议支持 40G PoS 接口和 STM-1/STM-4 的 ATM 接口。

3.2 以太网接口

CR 必须支持由“IEEE Std 802.3, 2005 Edition, Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications”所定义的 10/100Mbps 和 1000Mbps 双绞线及光纤要求。

建议 CR 支持“IEEE802.3ae, 2002 Edition, Media Access Control (MAC) Parameters, Physical Layers, and Management Parameters for 10Gb/s Operation”。

要求以下各种类型接口的 MTU 可配置, 支持 L3 MTU 值必须不小于 1500; 接口的 MTU 应不小于 9178。GE 和 10GE 接口必须支持超长帧 (Jumbo Ethernet frame)。

3.2.1 接口类型及特性

3.2.1.1 10Mbit/s 和 100M bit/s 以太网接口

10Mbit/s 以太网接口应符合 IEEE802.3。

100Mbit/s 以太网接口应符合 IEEE802.3u。100Base-T 技术中可采用三类传输介质: 100Base-T4、100Base-TX 和 100Base-FX。

CR 必须支持 10/100Base-T 自适应接口。

3.2.1.2 1000Mbit/s 以太网接口

CR 必须支持千兆以太网 (1000Mbit/s) 接口。1000Mb/s 以太网物理接口可以支持 1000Base-Sx、1000Base-LX 以及 1000Base-T。其中, 1000Base-SX 和 1000Base-LX 接口特性应符合 YD/T1097-2001 的 5.2.2 节的要求。1000Base-T 接口应符合 IEEE802.3ab。

千兆以太网光接口必须支持 GBIC(GigaBit Interface Converter)或 SFP(Small Form-factor Pluggable) 模块。

3.2.1.3 10Gbit/s 以太网接口

CR 必须支持 10Gbit/s 以太网接口，必须支持 10GBASE-R，应支持 10GBASE-W。所支持的 10Gbit/s 以太网接口特性应符合 IEEE802.3ae。

3.2.2 功能要求

必须支持 IEEE802.1Q VLAN，和 IEEE 802.1p 的优先级设定功能。

CR 必须支持符合 IEEE802.1ad 的 VLAN 堆叠 (Stack VLAN)。

在最高速接口上应支持长达 15 分钟的比特计数而不溢出。

支持流控功能。

CR 应该支持在物理端口上的 IEEE 802.3ad 链路汇聚/负载分担功能。

3.3 POS 接口

3.3.1 接口类型及特性

POS 接口的 SDH 帧封装应符合标准 ITU-T G.707 (1996)；接口性能应符合标准 ITU-T G.957 (1995)；误码率应符合标准 ITU-T G.826 (1996)；抖动与漂移应符合标准 ITU-T G.825 (1993)。

接口类型必须支持 OC-3、OC-12、OC-48、OC-192 接口,其中 OC-3 和 OC-12 接口必须符合 YD/T973-1998 规定的 SDH 155 Mb/s、622Mb/s 光发送和接收模块的技术条件要求；OC-48 接口必须符合 YD/T 1111.1-2001 和 YD/T 1111.2-2001 规定的 SDH 2.488320Gb/s 光接收模块和光发送模块技术要求；OC-192 接口则必须符合 YD/T 1199.1-2002 和 YD/T 1199.2-2002 规定的 SDH 10Gb/s 光接收模块和光发送模块技术要求。

建议支持 OC-768 白光口和彩光口。

设备的 POS 接口必须支持 1+1 自动保护倒换，所有的光接口必须支持单模和多模。

必须支持长距、中距、短距三种接口模块，长距要求至少达到 70 公里 (1550nm)，中距要求至少达到 15 公里 (1310nm)、40 公里 (1550nm)、短距要求达到 2 公里 (1310nm)。

3.3.2 链路层及功能要求

POS 端口链路层协议要求支持 HDLC 和 PPP over SONET/SDH (RFC 1662、RFC2615)。

POS 端口应该具备内置时钟和从线路提取时钟的能力。接口板上的时钟应具有保持工作模式，即当外部定时源中断时，时钟能在 24 小时内仍能维持相对于外定时中断瞬间时钟频率不劣于 0.37×10^{-6} (20℃ 至 30℃ 范围内) 的时钟准确度。

POS 端口应该具备如下故障检测和将告警发送到对端的能力：

- Alarm Indication Signal (AIS-L, AIS-P)
- Bit Error Rate Signal Degrade (BERR-SD), Bit Error Rate Signal Fail (BERR-SF)
- Bit Interleaved Parity Errors B1, B2, B3 (CV-S, CV-L, CV-P)
- Errored Seconds (ES-S, ES-L, ES-P), Far-end Bit Errors REI-L, REI-P (CV-LFE, CV-PFE),
- Far-end Errored Seconds (ES-LFE, ES-PFE), Far-end Severely Errored Seconds
- (SES-LFE, SES-PFE), Far-end Unavailable Seconds (UAS-LFE, UAS-PFE)
- Loss of Frame (LoF), Loss of Pointer (LoP-P), Loss of Signal (LoS)
- Payload Mismatch (PLM-P), Payload Unequipped (UNEQ-P)
- Remote Defect Indication (RDI-L, RDI-P)
- Severely Errored Framing (SEF), Severely Errored Framing Seconds (SEFS-S)
- Severely Errored Seconds (SES-S, SES-L, SES-P), Unavailable Seconds (UAS-L, UAS-P)

PPP 协议由标准 RFC 1661 描述。IP 数据包也可以遵循 YD/T 1061-2000 同步数字体系 (SDH) 上传送 IP 的 LAPS 技术要求，先转换成 LAPS 帧结构，再映射到 SDH 虚容器 VC 中。IPv6 数据包遵循 RFC 5172。

能通过调度排队算法提供 QoS (或 CoS)。

必须支持基于 IP 的拥塞管理。

建议支持 POS 上的 MPLS。

3.4 ATM 接口

3.4.1 接口类型及特性

路由器的 ATM 接口必须支持 OC-3 接口标准、OC-12 接口标准。

ATM 接口应支持光接口和电接口两种类型，电接口适用于局内、干扰信号弱的情况；光接口必须符合 YD/T 976-1998 中的相关要求；物理层采用两种速率接口：155520Kbit/s 和 622080Kbit/s。

必须支持 APS 1+1 保护。

应支持光接口和电接口两种类型，电接口适用于局内、干扰信号弱的情况。

3.4.2 ATM 层要求

ATM 层应该符合 YDN 052-1997 的规定；ATM 适配层必须符合 YDN 053.4-1997 中的规定；ATM 接口必须按照 RFC2684 规定将 IP 包封装到 AAL5 的帧格式中；

必须支持 LLC/SNAP 和 IP 复用 PVC（路由协议的 LLC 封装）；

CR 应该支持 ATM 论坛用户-网络互联接口（UNI）规范，版本 3.1；

CR 必须支持 ATM 论坛流量管理规范 4.1 所定义的 ATM CBR 服务等级、UBR 业务等级、ATM nrt-VBR 服务等级和 ATM rt-VBR 服务等级；应该支持 ATM 流量管理规范 4.1 补遗所定义的带有 MDCR 参数的 ATM UBR 服务等级；

CR 应该支持 I.610 所规定的 ATM OAM VC 管理；

CR 必须在所有 ATM 端口上支持 ITU-T I.610 所规定的 ATM F4 和 F5 OAM；

CR 必须支持 PVC，建议支持 SVC；

输出队列必须支持对每条 VC 分段和业务整形功能。

3.5 其它接口

建议支持信道化 DS3/E3、OC-3、OC-12。

信道化的 POS 接口可以灵活而高密度地提供多种低速接口，包括 E1、E3 等。

建议支持速率为 155Mbit/s、622Mbit/s、2.5Gbit/s 的 RPR 接口。

4 路由功能

本节中的路由功能规定为基于 IPv4 的路由功能，Ipv6 的相应功能应当可以通过软件升级来支持。

4.1 常规要求

4.1.1 协议和地址

CR 必须支持下列链路层协议：ARP/RARP、PPP、ATM、POS；

CR 必须支持下列互联网层协议：IP、ICMP、IGMP；

CR 必须支持下列应用层协议：FTP、Telnet、SNMP 等；

IP 地址必须支持下列规定：

- 必须支持 A、B、C、D、E 类地址的配置及使用规定；
- 必须支持与地址分配和汇总策略相关的无类别域内路由 CIDR；
- 必须支持私网地址使用的规定；

CR 必须支持在主端口上配置 primary/secondary IP 地址；

CR 必须支持使用 unnumbered IP 端口；

CR 应当支持静态及动态 NAT 功能（可选，放置在有 NAT 业务需求的城域网的 CR 需支持）。

4.1.2 路由

CR 必须支持静态路由配置和动态路由协议。

CR 必须支持基于 IPv4 的域内动态路由协议（RIPv1/v2、OSPFv2、ISIS）和域间路由协议（BGP4）。

CR 必须支持为静态路由配置如下参数：TOS、子网掩码（或前缀长度）、路径权值；在配置某静态路由时，必须允许静态路由定义成任何路由协议使用的路径权值；必须允许用户规定一组静态路由是否通过某路由协议扩散；CR 必须支持基于用户定义的策略，提供静态配置的策略路由能力。

CR 必须支持多条缺省路由和静态路由的 ECMP；必须支持允许配置路由是否公告的时间间隔。

CR 必须支持根据逻辑或物理端口过滤进出路由信息；必须支持路由汇总；必须支持路由协议的重分发功能。

CR 应能够实现重设 TOS/DSCP 域、指定下一跳、指定输出端口、指定 IP

到 MPLS 等功能。

CR 必须支持禁止直接域广播。

CR 必须支持 BFD 功能，包括 BFD for 静态路由、BFD for Vlan、BFD for OSPF、BFD for ISIS、BFD for BGP、BFD for LDP。基本功能应符合 draft-ietf-bfd-base-08 规定的各项要求，包括 BFD 检测的承载协议及使用的端口号，BFD 的包类型、包格式，检测模式、发送周期及检测时间、参数修改过程、会话初始化和建立等内容；应支持 draft-ietf-bfd-v4v6-1hop-08 和 draft-ietf-bfd-multihop-06 的相关规定。

必须支持 OSPF/ISIS/BGP/LDP 路由协议的 NSR 功能，当设备在当前激活的主路由引擎或软件突然失效而进行主备切换时，能够保持路由协议的稳定性和数据包持续的转发。

建议 CR 支持 IP FRR 功能，能够将备份路由表下发到转发表中。

必须支持 PBR 策略路由能力；能基于源地址、源地址+目的地址、源地址+目的地址+TCP/UDP 端口、IPP 值进行路由重定向。

必须支持策略路由至少 8 条、建议 16 条负载分担，分担误差在 10%以内。

设备在启用策略路由业务后，必须能保证业务流无丢包、乱序、时延明显增大等异常现象；并且设备主 CPU 和线卡 CPU 保持稳定。

必须支持对策略路由的可靠保护，即当策略路由失效后，能自动将路由方式切换到按目的地址路由。

必须支持主、备用策略下一跳功能。

建议支持对策略路由失效的日志及告警功能。

4.2 OSPF 路由协议功能要求

CR 必须支持 RFC 2328 OSPFv2 路由协议的全部功能和要求，其中包括：链路状态数据库、自治系统内对区的分割、域内路由功能、自治系统外部路由的处理、路由协议包格式、基本功能实现要求（定时器、IP 组播包接收和发送、可变长子网掩码支持、IP 超网支持、低层协议支持、非广播低层协议支持、操作原语列表、激活其它过程的任务支持）、协议数据结构、区数据结构、邻居路由器状态维护、收发协议包的处理、接口数据结构、邻居数据结构、路由表结构、LSA 包数据结构及处理、虚链路要求、路由表计算等。

CR 必须支持如下 OSPF LSA：

- type1: router-LSA;

- type2: Network-LSA;
- type3: Network Summary-LSA;
- type4: ASBR Summary-LSA;
- type5: AS-External-LSA;
- type6: Group Membership LSA;
- type7: NSSA External LSA;
- type8: External Attributes LSA;
- type9: Opaque LSA (link-local scope);
- type10: Opaque LSA (area-local scope);
- type11: Opaque LSA (AS scope)。

CR 在满足作为 stub 路由器的条件下, 必须能发布 OSPF Stub Route。

CR 必须能够实现作为 ABR 和 ASBR 的功能。

CR 建议支持规定 OSPF 平滑重启功能。当路由控制平面重新启动时, 网络拓扑未发生变化, 则必须启动 OSPF 平滑重启过程; 若检测到网络发生了变化, 则必须能转换到正常到 OSPF 重启过程。路由器必须能够实现平滑重启的发起者功能, 也必须能够在作为平滑重启发起者的邻居时, 运行在平滑重启助手模式下。无论作为平滑重启的发起者还是作为助手, 路由器必须提供 OSPF 平滑重启的后向兼容能力, 能够感知在邻居无法作为助手时, 进入正常的 OSPF 重启状态。整个平滑重启过程必须符合 RFC3623 的规定。

在启动了 OSPF 的邻居之间必须支持协议消息的保密认证功能, 符合 RFC 2328 的规定。

必须支持 OSPF 多路径负载分担, 最大负载分担链路条数不小于 16 条, 其分担误差要求在 10%之内。

必须支持对路由协议优先级/管理距离的调整。

必须支持 OSPF 多进程。

可选支持 OSPF 多拓扑路由功能,符合 RFC4915 的规定。

4.3 ISIS 路由协议功能要求

CR 必须遵守 RFC1195 中的规定, 包括: 与子网无关的功能, 与子网相关的功能, PDU 的结构和编码, 路由信息的类型和编码, 序列号分组编码及路由算法; 对路由信息的 QoS 设置必须符合 RFC2474 中的规定; CR 必须支持 RFC1195 中的 IS-IS 路由信息的简单认证功能和 RFC5304 中的加密认证功能, 支持 ISIS Hello 和 LSP Interface 级、Area 级和 Domain 级的 MD5 加密, 以保证路由信息的安全。

在点到点链路之间建立 ISIS 链路时，必须通过 3 次握手机制实现，实现方式应符合 RFC3373 中的规定。

必须支持 RFC2763 规定的动态主机名 TLV (类型 137)，以便于运维管理。

必须支持 RFC 2966 规定的两层 ISIS 域范围的前缀分发功能；必须支持 Level2 到 Level1 的路由泄漏特性。

必须支持 RFC3277 ISIS 瞬时黑洞避免功能，即在重启时，给建立了邻接关系的路由器快速发出带有 Overload bit 置位的 LSP 消息，在该路由器同步路由数据库完成后，再次发布 LSP 消息时，应清除 Overload bit 原置位。

必须支持 ISIS 多路径负载分担及其管理，最大负载分担链路条数不小于 16 条，分担误差在 10%之内。

必须支持 RFC 3847 中规定 ISIS 的重启信令，即增加相关的定时器 T1/T2/T3，及 Restart TLV (类型 211)，在重启（或启动）的路由器及其邻居在重启（启动）过程中的操作（如邻居的获得、多层间操作、数据库同步等），要符合该 RFC 文档的规定。

必须支持 ISIS 协议的快速路由收敛机制，相关参数可配置：

- ✓ 必须支持 ISIS PRC（部分路由计算）和 I-SPF（增量 SPF）。
- ✓ ISIS 可配置的时间参数应包括 hello 间隔时间、LSP 发送间隔时间、SPF 初始时间、SPF 间隔时间。
- ✓ 必须支持 POS 对 SDH Section、Line 和 Path 故障信号的检测，并根据这些信号触发 IP 接口状态，触发机制和相关时间参数可以配置。
- ✓ 必须支持 10GE、GE 接口 keepalive 发送间隔可配置为不大于 1 秒，要求具备物理端口故障快速检测能力（不大于 100ms）。
- ✓ 必须支持设备根据传输误码率判断链路状态的能力。
- ✓ 必须支持物理端口的 damping 功能，打开该功能不影响端口状态变化 TRAP 的发送。

建议支持在 RFC3784 和 RFC4205 中规定扩展 TLV 及其 sub-TLV，其中(1)一(3)为 IS-IS 用于 TE 的扩展；(4)则为 ISIS 用于 GMPLS 的扩展：

(1)extended IS Reachability TLV (类型 22)及其 sub-TLV(子类型 3,4,6,8-11,18, 20, 21)；

(2)extended IP Reachability TLV(类型 135)；

(3)The TE Router ID TLV (类型 134)；

(4)shared Risk Link Group (类型 138)。

可选支持 ISIS 的多拓扑路由功能，符合 **RFC5120** 的要求。

可选支持链路状态路由协议 LAN 上的点到点操作，符合 **RFC5309** 的要求。

4.4 RIPv1/v2 路由协议功能要求

CR 必须支持 RFC 2453 RIP Version 2 规定的各项功能要求、各项协议消息封装格式、协议算法。

CR 必须支持 RFC 2091，以保证 RIPv2 在与邻接设备通过面向连接的电路连接时的可用性。

CR 必须支持只向客户 CPE 发送 RIP 更新，但不接收由 CPE 传来的更新。

CR 必须支持 RIPv2 的加密认证功能；在启用 RIPv2 版本时，必须支持与 RIPv1 版本的后向兼容。

4.5 BGP-4 路由协议功能要求

CR 必须符合 RFC 4271-BGP4 协议中规定的全部功能和要求，包括：

(1) 路由发布和存储规定。

(2) BGP 各类消息包（OPEN、UPDATE、KEEPALIVE、NOTIFICATION 和 ROUTE- REFRESH 消息类型）格式规定，并支持 BGP 各类消息包所包含的内容。

■ 对于 OPEN 消息，必须支持 RFC 4271 第 4.2 节的规定，同时必须支持 RFC3392 中规定的能力选项格式；

■ 对于 UPDATE 消息，必须支持下列 Path Attribute（通道属性）类型：

- Type Code 1: ORIGIN;
- Type Code 2: AS_PATH;
- Type Code 3: NEXT_HOP;
- Type Code 4: MULTI_EXIT_DISC;
- Type Code 5: LOCAL_PREF;
- Type Code 6: ATOMIC_AGGREGATE;
- Type Code 7: AGGREGATION;
- Type Code 8: COMMUNITY;
- Type Code 9: ORIGINATOR_ID;
- Type Code 10: CLUSTER_LIST;
- Type Code 14: MP_REACH_NLRI;
- Type Code 15: MP_UNREACH_NLRI。

其中，TypeCode 1~7 必须符合 RFC4271 中第 4.3 节和第 5 章的相关规定；对 TypeCode8 团体属性值的范围、操作、聚合和使用，必须符合 RFC 1997 的规定，属性值应可配置；TypeCode9、10 是路由反射功能实现时，避免出现路由信息环路使用的，其格式和使用，必须符合 RFC4456 的规定；TypeCode 14、15 则用于 BGP-4 的多协议扩展，其功能实现在 RFC 2858 中规定。

- 对于 KEEPALIVE 消息，必须支持 RFC4271 第 4.4 节的规定
- 对于 NOTIFICATION 消息，必须支持 RFC4271 中第 4.5 节中对错误码和错误子码的规定和第 6 章对各类 NOTIFICATION 消息的处理，必须支持 RFC4486 的“终止通知”的 8 个子编码（subcode）的定义和处理。
- 对于 ROUTE-REFRESH 消息，消息格式和操作过程必须符合 RFC2918 中的规定。

(3) BGP 版本协商的规定。

(4) BGP 中有限状态机规定。

(5) BGP 内所有定时器相关规定。

CR 除了支持基于 AS 配置 BGP，还必须支持能够实现基于团体配置 BGP，相关措施应该符合 RFC 1998 的规定。

CR 必须支持 BGP 路由振荡抑制，符合 RFC 2439 的规定。提供限制发布路由的相关定时器；支持实现稳定发布路由的方法；所有的定时器参数及动作均应可配置。

CR 必须支持 BGP-4 多协议扩展，必须支持多协议可达 NLRI 属性（类型码为 14）和多协议不可达 NLRI 属性（类型码为 15），对这两个属性的编码格式、后续地址族标识（单播、多播、组播）、发布和处理，以及错误码的处理均要符合 RFC2858 的规定；网络层协议为 IPv6 的 BGP 多协议扩展则必须支持 RFC 2545。

CR 必须支持自治系统联盟的功能，支持 RFC3065 中规定的 AS_PATH 新增段类型，即 AS_CONFED_SEQUENCE（value=3）和 AS_CONFED_SET（value=4），相关的操作、管理、兼容性、部署等均要符合 RFC3065 中的规定。

建议支持 4 字节长度的 AS 号。

CR 必须支持 RFC2385 定义的，新增 TCP 选项携带 MD5 摘要，通过 TCP 的这项扩展功能增强 BGP 的安全性，MD5 加密涵盖的内容、相关语法、发送/接收操作，以及有关面向无连接复位的处理、性能、TCP 头的长度、MD5 算法、密钥的设置等，必须要符合 RFC2385 中的规定。

CR 必须支持 IBGP 路由反射功能，其路由反射的操作、路由反射器的备份、路由信息环路的避免等过程，均必须符合 RFC4456 的规定。

CR 必须支持在 BGP-4 消息中携带 MPLS 标签的功能，有关标签携带和功能实现方式均必须符合 RFC 3107 的规定。

CR 必须支持 IBGP/EBGP 多路径负载分担，最大负载分担链路条数不少于 8 条，建议支持 16 条及以上，分担误差在 10%之内。

CR 建议支持 IBGP/EBGP 的路由收敛优先级区分功能，能够保证高优先级业务路由在故障时优先收敛。

必须支持 BGP 的日常配置和维护操作功能；必须支持灵活丰富的路由控制和过滤功能。

必须支持基于 BGP 进行流量控制。具体为：实现基于 BGP 的 ACL、或者 QOS 的 classification，必须支持 extended community。支持根据客户类型、业务类型等在网络之间等地方进行控制。

建议 CR 支持 BGP 的平滑重启功能，其能力消息格式、发起者和接收者的操作过程、状态转换等应符合 RFC4724 的规定。

5 QoS

5.1 QoS 机制

设备必须实现 DiffServ QoS 机制，包括分类、标记、速率限制、带宽保证、流量整形、策略和测量等，符合 RFC 2475 的规定；设备必须支持 RFC 2597 定义的 AF 转发功能；必须支持 RFC3246 定义 EF 转发功能,并保证对此类业务流对转发时延低于 30ms;必须支持 RFC2474 定义的 BF 转发功能;必须支持 RFC3662 中规定的为属于 BF 的某服务进一步降低服务的功能;必须支持 RFC2697 和 RFC 2698 中规定的单速率和双速率的业务合同参数，以及不同情况下的漏桶算法规定。

(1)分类

设备必须支持基于多种方式对数据流进行分类功能，包括：

- IPv4 及 IPv6 的 DSCP
- 用户会话接入的物理/逻辑端口
- 源 IP 地址
- 目的 IP 地址
- IP 协议字段

- 源 TCP/UDP 端口号
- 目的 TCP/UDP 端口号

(2) 标记和映射

基于上述的分类字段，设备必须支持根据配置的策略控制，提供对 IP 包的 DSCP 字段、MPLS 的 EXP 字段进行标记的功能，并能够实现这两层之间各 COS 字段的相互映射。设备必须支持在 MPLS 网络里，可以将不同等级的数据流量加上 MPLS-EXP 的 QOS 定义，建议可以对第二层的 MPLS VPN 线路做 MPLS-EXP 的 QOS 定义。

(3) 速率限制和带宽保证

设备必须具备在任意端口、会话和应用流上加载控制策略的能力，支持对物理端口、子端口的流量进行限速，支持对基于 IP 地址的流量限速。要求 10/100 Mbit/s 接口颗粒度最少 64kbit/s; 1000Mbit/s 接口速率限制颗粒度最小为 1Mbit/s, 误差小于 5%。

设备必须支持基于物理端口/子端口、PVC 和 IP 地址的可配置最小吞吐量以保证不会出现完全无法得到带宽的情况。

必须支持利用 BGP 属性传递 QOS 信息的能力。

必须支持组播业务的服务等级分类和 QoS 队列调度。

(4) 流量整形

设备必须支持基于流分类加载流量整形的控制功能，并根据配置实现流量整形功能；设备必须实现对每个队列的整形能力；设备必须实现对 L2TP 隧道的流量整形功能。设备中的分级调度器必须能够基于网络拓扑模型对下行流量进行整形以保证下行的二层端口无拥塞。

(5) 统计功能，设备具备对实施分类后的数据包进行统计的手段。

(6) 动态调整 QoS 策略

设备应该能够提供对外部策略服务器的接口，利用公共协议（如 COPS、RADIUS 或 DIAMETER 协议），支持向外部策略服务平台通知状态（如申请/释放 QoS 资源的结果、用户掉线异步通知等），并接受外部策略控制平台的控制，动态改变在 ATM 层、IP 层的策略及整形参数，而无需重建会话。

(7) 队列和拥塞控制

设备必须支持队列技术，如 PQ/CQ/LLQ/WRR/CBWFQ 等队列技术，并为每个队列提供不同的控制策略；设备必须支持速率限制、WRR、WRED、尾丢弃（TAILDROP）等拥塞控制技术。

(8) 层次化 QoS 要求，CR 建议支持层次化 QoS 功能，实现分级调度，分级

调度必须能有效利用资源，任何流量必须可以使用分配给其它流量等级的未使用带宽。

5.2 QoS 能力

要求队列数量大于 8 个/物理端口，ACL 大于 3000 个/物理端口，数据缓冲内存大于 128MB/OC-48 端口，最大延时小于 100us、最大抖动小于 30us，要求每队列带宽保证误差小于 5%。

与外部的策略服务器直连且无阻塞时，设备必须支持并应用每秒至少 50 条策略的改变；策略规则由策略条件和策略动作构成，设备必须支持对每个用户加载 10 个策略规则或者整机支持至少 10,000 个策略规则的应用。

设备必须能够在每个端口(任意的物理或逻辑端口)应用至少 2 个策略(进和出方向，每个策略包含至少 10 个规则)，而不影响设备的性能。

设备的性能在流量整形开启时必须不受任何影响；设备必须支持基于 IP 优先级、DSCP 的 WRED 或尾丢弃，必须支持能根据 IP 优先级、DSCP 值执行相应的拥塞处理能力。

对于层次化 QoS 要求 SR 必须支持三层 QoS 控制，各层次调度器的数目视系统规格而定，并实现基于类（或队列）的每级限速，即实现对每类（或队列）的最高速率限制；对每层均实现拥塞控制，支持拥塞处理和拥塞避免等 QoS 功能；对每个层次都能够进行流量监管或整形。

6 MPLS 功能

CR 的体系结构必须支持 MPLS，支持 MPLS LER 和 LSR 功能，支持 MPLS 显式路由。CR 必须支持标准的 LDP 和 RSVP-TE 信令协议，不应使用厂商私有的协议。

CR 必须能配置备份 LSP；支持多路径 LSP 的负荷分担；支持标签堆栈；支持基于约束的路径计算，能够基于源/目的 IP 地址、协议、源/目的端口号、TOS/优先级、TCP 标志、路由表的下一跳等参数将数据包路由至输出 LSP。

CR 必须支持 MPLS 协议的基本功能。

CR 必须支持 MPLS 流量工程。

CR 必须支持 MPLS 虚拟专网。

CR 必须支持实现 MPLS IP VPN 的 P 路由器功能。

CR 必须能够根据所配置的策略，把输入的业务量自动分配到不同的 TE LSP 中；建议采用硬件来完成该功能，在完成该功能时，仍然能以线速转发 MPLS 数据包。

必须支持基于策略（如路由前缀）控制标签的分配。

必须支持 LSP 跨 IS-IS 的不同 Level、OSPF 不同 AREA 建立。

必须支持一层标签的负载分担，建议支持 Native IP（包括源 IP 和目的 IP）、及多层标签的负载分担，误差都必须在 10%之内，负载分担路径条数必须不少于 8 条。

必须支持匹配 MPLS 标签中的 S 位(栈底标志)。

6.1 MPLS 基本功能

MPLS 帧的封装格式必须符合 RFC 3032 的规定，能够确定网络层协议类型、能够产生打标签的 ICMP 包、能够正确处理超大 IP 报文、能够在 PPP 链路上传递打标签的 IP 包；标签值的使用必须符合 RFC 3032 和 RFC 4182 的规定；MPLS 帧格式的 TTL 字段的处理必须符合 RFC 3032 和 RFC3443 的规定；CR 的 MPLS 标签堆栈应该支持至少 3 层标签；必须支持符合 RFC 3035 的使用 LDP 或 ATM VC 交换的 MPLS。

CR 必须支持 LDP 协议，LDP 协议的实现必须符合 RFC 3036 的规定：

- 能够作为 LDP Peer 实现 LDP 消息（发现、会话、通告和通知消息）的交换；
- 能够实现 LDP 协议的各项操作，包括：FEC 的确定；标签空间、LDP 标识符；LDP 发现；LDP 会话的维护和建立；非直连 LSR 之间 LDP 会话的实现；和 LDP 传送的实现；非直连的 LSR 之间 LDP 会话的实现；LDP 的传送；标签的分发和管理；LDP 环回检测；LDP 消息的真实性和完整性验证；显式路由 LSP 的标签分发等；
- 协议规范：包括 LDP PDU 格式；LDP 过程；TLV 编码；LDP 消息的构成等。

CR 建议支持 RFC3478 规定的 LDP 的平滑重启机制。

CR 必须具备 LSP 环回检测和防止功能，必须支持 RFC 3063 规定的 MPLS 环回检测机制提供的 Thread 功能；SR 必须支持 RFC4379 规定的 MPLS 数据平面故障检测功能，并应能与 draft-ietf-bfd-mpls-07 中规定的 BFD 在 MPLS LSP 中的应用相结合,实现对 MPLS LSP 的故障检测功能。

标签保持模式必须使用自由(liberal) 标签保持模式，参见 RFC 3031 的 3.8 节。

CR 必须支持 LDP 过滤。

CR 应支持基于标签对数据包的转发，并可通过手动配置或标签分配协议（LDP）建立 LSP。

CR 建议支持 RFC 3270 定义的 L-LSPs 的各项功能操作。

建议在支持 IP FRR 的基础上，支持 LDP FRR 功能。

6.2 MPLS 流量工程（TE）

必须支持基本的 MPLS TE 标准，必须支持 RSVP-TE 信令协议。必须支持差分服务感知 TE 功能，为每类业务级别保证带宽。必须支持 E-LSP，在 E-LSP 中，一条 LSP 承载多个 CoS 类别的数据包，使用 EXP 比特来区别不同的 CoS 数据。

CR 必须支持实现符合 RFC 2702 的 MPLS 上 TE 需求；必须 RFC3181 规定的抢占通知的优先级策略要素；必须符合 RFC3272 互联网流量工程的概述和原则；必须符合 RFC3346 使用 MPLS 实现链路工程的适用性描述；必须支持 MPLS 流量工程的差分服务感知要求。

CR 必须支持 RSVP 协议，必须实现 RFC 2205 中 RSVPv1 功能的规定，RSVPv1 的消息处理必须符合 RFC 2209 的规定。

CR 必须支持 RSVP-TE 功能，该功能实现必须符合 RFC 3209 规定的支持 LSP 隧道的 RSVP 扩展、RFC 3396 规定的修改 RFVP 的过程。

必须支持 RFC 3784 规定的 IS-IS 流量工程扩展功能。

CR 必须支持 LSP 的 RSVP-TE 的快速重路由功能，符合 RFC 4090 的规定，当链路或节点发生故障时，从故障链路或节点切换到备份链路的时间小于或等于 50ms；必须支持 RFC 4561，以实现 TE LSP 的跨域倒换，必须支持 MPLS-TE FRR 中 Facility 和 Detour 两种方式，支持 1:N 和 1:1 的备份，必须支持手工配置保护通道，建议支持通过自动计算实现。

CR 必须支持根据所配置策略，将输入的业务量自动分配到不同的 TE LSP 中。建议采用硬件来完成该功能，在使用该功能时，CR 必须能以线速转发。

7 组播

设备必须实现 RFC 1112-Host extensions for IP multicasting，必须实现 RFC 2236 规定的 IGMPv2，必须实现 RFC 3376 规定的 IGMPv3。

设备必须支持 RFC2362，PIM-SM 模式；必须支持 PIM-SM 中的集合点（RP）自动发现。设备必须支持 PIM-DM、MSDP（RFC 3618 组播源发现协议）等组播协议；设备必须支持 IP 定源组播（SSM）。

设备必须支持通过 MBGP 和 MSDP 协议实现跨域组播功能，并实现 RP 功能。

设备所支持的三层功能必须同样适用于组播，例如速率限制和过滤等。

设备须具有灵活的组播业务控制机制，设备必须对静默丢弃所有上行用户组播流量功能可配置。

建议设备支持 PIM-SM 隧道；建议设备应支持在 MPLS 环境实现组播业务，并实现 RFC 4364 中描述的组播 VPN 业务。

设备支持由 RPT 模式切换到 SPT 过程中不丢包。支持包转发依赖硬件完成，不影响主控板的 CPU 性能。必须支持对组播流量的 QoS 功能而不影响性能。

必须支持 MSDP Peer 间使用 MD5 认证，并能与其他厂家设备互通。

必须支持丰富的组播过滤策略，例如根据(S,G)对组播流进行过滤，设置 PIM 边界等。

单域组播和跨域组播都必须支持组播源+组播组的负载分担。

为支持 IPTV 业务，CR 设备还需具备以下功能：

设备必须支持对上送到控制层处理的 IGMP、PIM 和组播数据流进行限速，防止产生组播攻击。

设备必须提供动态组播 QoS 功能，提供对每组播组流量的限速。

8 IPv6

设备必须支持 IPv6 协议，主要包括 IPv6 数据包线速转发，IPv6 动态路由协议，过渡机制等。

必须支持 IPv6 基本协议，符合 RFC 2460-互联网协议（版本六）。

必须支持 IPv6 地址结构的规定，符合 RFC 4291—IP v6 地址体系结构。

必须支持基于 IPv6 的邻居发现机制，包括路由器和前缀发现，地址解析和邻居不可达检测，重定向等功能要求，符合 RFC 2461 和 RFC3122 中邻居发现等相关等规定。支持在同一链路上使用邻居发现协议来获知其它节点等存在，从而确定彼此的链路层地址，并发现路由器以及维护通向活动邻居的可达性信息。

必须支持 RFC 4443 规定的 ICMPv6。

CR 必须支持 IPv6 静态路由，到特定目的地的静态路由由网络前缀定义。支持 IPv6 静态路由中附加信息，包括：前缀长度、对给定路由协议引入静态路由的特定度量。

CR 必须支持 IPv6 动态路由，路由器应支持 IS-ISv6 协议，符合 RFC5308 中

的规定。支持为适应 IPv6 协议增加的两个 TLV，即 IPv6 可达性 TLV 和 IPv6 接口地址 TLV，支持增加的 IPv6 协议标志符。

CR 必须实现在 RFC5340 中规定的 OSPFv3。支持 IPv6 OSPF 包格式，并直接运行在 IPv6 上。支持路由器 LSA 选项字段中增加的两个选项比特：R 比特和 V6 比特。支持 LSA 的格式变化。在 LSA 头和路由器 LSA、网络 LSA 中删去所有地址语义，这两个 LSA 以网络协议无关的方式描述路由域的拓扑。支持新增的用于分布 IPv6 地址信息的新 LSA，以及进行下一跳解析所需要的数据。

CR 必须支持 BGP4+，符合 RFC2545 的规定。BGP4 用作传达 IPv6 可达性信息时下一跳属性可能需要包含全局地址以及本链路地址。用作构造 MP_REACH_NLRI 属性中下一跳域网络地址需要遵守 IPv6 特定的规则。满足在下一跳域 IPv6 地址中向对等实体传送下一跳全局 IPv6 地址，并且后接下一跳本链路 IPv6 地址。如果下一跳地址字段包含本链路地址，则地址长度值等于 32。

路由器必须支持 RIPng，并符合 RFC2080 的规定。

路由器必须支持 IPv6 端口的 CoS/QoS 分类，并实施 QoS 策略控制和队列调度。

路由器必须支持在 IPv4 的 L2TP 隧道中传递 IPv6 包，并支持 IPv6 的 L2TP 的 LNS 功能。

路由器必须支持 IPv4 到 IPv6 的过渡机制，主要包括双栈方式、隧道方式及 6to4 隧道方式。

必须支持 IPV6 的各种安全特性，支持 IPV6 的 uRPF 功能，应线速支持 IPv6 DDOS 攻击限制和过滤功能。

必须支持 IPV6 的策略路由。

建议支持 IPv6 上的协议 PIM-SM，MLD，IPv6 based LDP for MPLS 等。

设备必须硬件支持 IPv6 数据包转发，端口转发达到线速。

9 设备管理功能

9.1 基本管理功能

设备必须提供配套网元管理系统：系统能自动发现设备，可以管理多台设备。

必须支持中国电信的城域网网管。

网管系统必须具有配置管理、故障管理、性能管理、计费管理和安全管理功能：管理系统可以通过图形化管理界面实现完全的配置操作，建议系统支持 web

方式进行配置；能够收集、显示、设置告警阈值、编排、过滤、处理和清除等告警管理；能够收集、统计、显示所有的性能参数；系统能提供认证、授权、控制、审计等安全管理功能；系统必须提供北向接口如 CORBA/COPS/LDAP，可以无缝地集成在第三方网管平台上。

设备要求具备可管理性，设备必须支持通过 Console Port 或 Telnet 的模式实现配置管理。

设备必须支持 SNMPv1，符合 RFC 1155 和 RFC 1157 的规定。

设备必须支持 SNMPv2，符合 RFC 2578、RFC2579、RFC 2580、RFC 3416 及 RFC 3417 的规定。

设备必须支持 SNMPv3，符合 RFC 3410 的规定。

设备必须支持带外网管，可以将管理流量与用户流量从物理或逻辑上分开，带外网管与带内网管具有同等的功能。

设备必须支持 NTP，必须支持在本地存放多个版本的软件和配置文件。

必须对一些重要的操作提供操作撤消功能。

必须支持 QoS 管理功能，包括 QoS 参数集中分发、参数的配置方法、QoS 运行参数的采集，相关的通信协议和管理信息库。

必须支持通过 SNMP 进行 QOS 参数配置机制和运行状态统计。

建议具备 QoS 流量、故障、安全、配置等关键统计信息的本地存储功能，并以 XML 的形式表达、通过 FTP 方式传送到指定的 FTP 服务器。

建议支持基于 XML 的 Network Configuration (NETCONF) 网管协议。

必须支持流量采样，在 40G POS 接口、10G POS、10GE 和 2.5G POS 接口开启 1:1000，对 300 万数量的流，进行 xFlow 采样的情况下仍保持线速转发，只开启此项功能时 CPU 利用率不超过 30%，采样精度大于 90%，建议支持针对子端口的 xFlow 采样。应当支持 2 个 xFlow 的发送目标。

9.2 SNMP MIB

设备必须支持分布式管理 MIB，即对 Remote Ping，Traceroute 和 Loopback 操作的管理目标定义，符合 RFC 4560 的规定。

设备必须支持以太网 MIB，符合 RFC3635 中的规定。必须支持 IEEE 802.1ag & ITU-T Y.1731 和 IEEE 802.3ah 定义的以太网 OAM 要求。

设备必须支持接口组 MIB，符合 RFC 2863 的接口组 MIB 的规定。

设备必须支持 IP MIB, 包括 RFC 1213 基于 TCP/IP 的互联网网络管理 MIB (MIB-II)、RFC 2011 使用 SMIV2 的 IP SNMPv2 MIB、RFC 2012 使用 SMIV2 的 TCP SNMPv2 MIB、RFC 2013 使用 SMIV2 的 UDP SNMPv2 MIB、RFC 4292 IP 转发表 MIB、RFC4087 IP 隧道 MIB。

设备必须支持组播 MIB, 包括: RFC2932 中 IPv4 组播路由 MIB、RFC2933 中 IGMP MIB、RFC 2934 中 IPv4 PIM MIB 的规定。

设备必须支持 PPP MIB, 包括: RFC 1471 的 PPP LCP 的管理目标定义; RFC 1472 的 PPP 的安全协议管理目标定义; RFC 1473 的 PPP IPCP 管理目标定义。

设备必须支持 RIP MIB, 符合 RFC 1724 的规定。

设备必须支持 OSPF MIB, 符合 RFC 1850 的 OSPFv2 MIB 的规定, 符合 OSPFv3 MIB draft-ietf-ospf-ospfv3-mib-11 的规定。

设备必须支持 ISIS MIB, 符合 RFC 4444 的规定。

设备必须支持 BGP-4 MIB, 符合 RFC 4273 的规定。

设备提供商必须提供所有相关 QoS 相关的 MIB, 若含定义 MIB, 则必须符合下述要求。

设备必须支持 MPLS MIB, 包括: RFC3814 MPLS FEC 到 NHLFE MIB; RFC 3815 的 LDP 管理目标定义; RFC 3813 MPLS LSR MIB; RFC 3812 MPLS TE MIB; RFC 4220 TE LINK MIB; RFC 4368 MPLS 受控标签 ATM 和帧中继管理接口定义; RFC 4687 对 MPLS 及其相关内容的管理必须符合 RFC 4377 MPLS 网络的 OAM 需求、RFC 4378 的 MPLS OAM 框架及点到多点 MPLS 网络 OAM 需求和 RFC4379 的 MPLS 数据平面失效检测。建议支持 MPLS 快速重路由 MIB, 符合 draft-ietf-mpls-fastreroute-mib-10.txt 的规定。

设备必须支持 BFD MIB, 符合 draft-ietf-bfd-mib-06 草案的规定。

设备必须必须支持 VRRP MIB, 符合 RFC 2787 规定的 VRRP 管理目标定义。

设备必须支持事件 MIB, 符合 RFC 2981 的规定。

设备必须支持通告 MIB, 符合 RFC 3014 的规定。

设备必须支持统计 MIB, 符合 RFC 2513 对面向连接对网络计费信息收集和存储的控制的管理目标定义。

设备必须支持 SNMP MIB, 符合 RFC 3418 SNMP MIB 的规定。

设备必须支持 SNMPv3 MIB, 符合 RFC 3411 规定的 SNMP 管理框架的体系架构; 符合 RFC 3412 规定的 SNMP 消息处理和分发; 符合 RFC 3413 SNMP 应用规定; RFC 3414 SNMPv3 的基于用户安全模型 (USM); RFC 3415 SNMP 基

于视图接入控制模型（VACM）。

设备提供商自定义的 MIB 必须符合 RFC 1155 B 标准，并符合 RFC 1212 资源的描述和命名机制；必须能有效地支持特定对象的状态显示、统计、配置和控制，可通告一定途径获取其自定义 MIB 信息，并能对设备进行写操作。

9.3 故障管理

设备必须能够向网元管理系统发送告警信息；在告警信息中提供足够的信息以协助排障，例如日期时间戳、严重程度、部件标识、软件/硬件/固件版本等。

设备的故障告警必须至少要有以下几个严重级别的分类：紧急（critical），主要（major）；次要（minor）和通知（informational），并可以定制。

设备对以下情况必须发送告警：当 Radius 服务器不可用时；当设备的组成部件、逻辑端口或服务控制不可用时；设备必须支持对系统资源（例如 CPU 利用率）检测，在资源利用达到配置对阈值时。

故障事件的发生与事件的告警报告时间相差要小于 5 秒钟；当故障被修正时，设备将自动清除该故障的当前告警，并将改故障转存至历史告警信息中。

设备必须具备预先维护监测功能，例如事件审计、内存使用情况的监控、进程“丢失”或软件故障的监察等，并能采取适当的故障恢复措施。

设备必须允许通过用户名、IP、MAC 等进行会话的查找；设备必须支持 ping、traceroute 等工具辅助故障的处理；设备必须支持回退能力，如将操作系统软件/配置退回到先前的版本。

设备必须在网元管理系统无法工作时提供远程访问的手段；必须提供自检测或者故障诊断手段/工具，可完成连通性测试、性能测试、业务测试、硬件故障的检测及定位等；设备必须支持用户定位。

9.4 配置管理

网管系统必须实现对设备系统、端口和业务数据的配置、查询和修改；必须支持远程系统软件升级，建议设备支持在升级过程中不中断业务；设备必须提供软件备份、配置文件备份功能并能恢复；设备必须支持从 FTP 或 TFTP 服务器下载软件/配置文件。

网管系统必须支持 QoS 管理，支持对 IEEE 802.1p 的 COS 字段、LSP EXP 字段、IP Precedence 字段等的配置，支持这些字段之间相互映射关系的配置，支持层次化 QoS 的配置，支持 VPN QoS 的配置，支持 QoS 队列、拥塞策略的配置。

9.5 性能管理

设备必须能够对系统内部对资源进行统计，如 CPU 及内存利用率等；设备必须支持对 QoS 策略的实施进行统计；设备必须支持与业务相关对统计功能。

设备必须支持可设定一个端口每秒钟处理数据包个数的基本阈值，当超过时必须提供告警信息。

设备必须提供流量镜像功能；必须支持对基于单个用户流的监控和统计功能，包括应用层端口、会话连接数等。

9.6 安全管理

设备必须支持管理的安全功能，必须支持能够通过用户名和口令实现对设备对管理和控制；必须支持远程 telnet 访问功能；必须支持采用加密的方式进行安全的远程访问，如 SSH。对于远程访问必须提供访问超时控制，同时远程访问连接数限制，远程登录尝试次数限制，远程访问的相关信息记录（如访问终端的地址，端口，用户名和密码）等。

对于通过 console 端口的访问，也应提供访问超时、访问连接数、登录尝试次数等安全控制。

设备必须支持分级分权管理。

设备必须支持 RADIUS 进行网管登录密码认证，对密码进行集中管理。

设备应提供对登录口令长度的控制要求，建议至少不少于 8 个字符。

设备必须具有良好的访问控制，对设备所有网管操作都可配置为需要经过认证和授权方可进行，设备还必须支持 SNMP 对访问级别，必须支持网管日志功能，对超越权限或者失败的关键操作进行登记并作为安全告警；失败必须提供安全性审计的功能，并提供一种方法来记录配置的改变及操作人员改变配置的时间。

设备不允许存在未记载于文档的访问后门或通用密码。厂商必须确保这种用于调试或开发的途径在产品分销到客户手中之前已删除。

10 安全

10.1 访问控制和流量控制

设备必须支持源地址校验功能，支持单播反向路径转发/查找 uRPF 功能。

设备必须支持标准的五元组（源/目的 IP 地址、IP 协议字段、源/目的端口）

的访问控制列表功能，还必须提供基于 MAC 地址（包括源和目的地址）的访问控制策略手段。访问控制列表必须可定制为在设备全局生效还是在端口生效。

设备必须提供流量监管功能。

10.2 路由协议安全

设备必须路由协议安全功能，支持 OSPF、ISIS、BGP 等路由协议的 MD5 认证，保证路由信息的可信度。

对于 MPLS LSP 对标签分配，使用 LDP/CR-LDP 的标签交换使用 UDP 协议承载，对于基本 hello 消息，设备应只接受与可信 LSR 直接相连的接口上的基本 hello 消息，忽略地址不是到该子网组播组的所有路由器的基本 hello 消息的地址；对于扩展 hello 消息，可利用 ACL 只接受允许的源发送来的扩展 hello 消息。LDP 会话过程使用的消息由 TCP 协议承载，应通过 TCP MD5 签名选项对会话消息进行真实性和完整性验证；使用 RSVP-TE 时，则应通过加密散列函数支持邻居验证，应支持 HMAC-MD5 算法，建议实现 HMAC-SHA1 算法。

10.3 抗攻击能力

设备必须支持抵抗大流量攻击的能力，包括过路流量和对设备本身对攻击。对于第一种攻击，路由器应能采取限速策略；对于第二种攻击，路由器必须丢弃攻击流，并生成告警日志。在此情况下，路由器必须完成正常对路由协议和管理报文对正常发送和接收处理。

设备必须支持抵抗畸形包的能力，能够检测超短/超长报文，并采取丢弃策略，同时对这种报文进行统计；能够检测到链路层错误并采取丢弃策略，同时进行日志记录和统计；能够检测网络层报文 并采取丢弃策略，同时进行错误报文统计；设备不能犹豫错误报文/畸形报文而崩溃；设备本身必须不能发出错误报文/畸形报文。

设备必须支持对定向广播报文攻击的防范，禁止该类报文转发或者以广播形势转发，对于分布式 DOS 攻击，设备必须提供简单策略阻止这种分布式 DOS 攻击向设备扩散。

设备必须支持对 IP 地址哄骗的防范，必须支持单播逆向路径转发（URPF）功能限制这类报文在网络中出现。

设备必须支持至少一种针对去往/来自用户的流量，基于包类型（如 TCP SYN、ICMP 等）的机制（如可配置的速率限制），以防护来自被黑的/恶意的用户主机的 flooding 拒绝服务攻击。

设备必须支持对 IP spoofing 的诊断和阻断；必须支持对 IP 源路由选项攻击对诊断和阻断；必须支持对 IP Address sweep 攻击的诊断和阻断；必须支持对端口扫描的诊断和阻断。

10.4 网络地址/端口翻译

设备必须支持网络地址翻译和网络地址/端口翻译；必须支持混合编址方式，对于来自私网的非私网地址的报文直接进行转发；支持黑名单功能，对黑名单中的地址不进行地址转换和报文转发；支持对不同级别用户并发连接数的限制。

设备必须支持 NAT 日志的输出。

10.5 冗余

设备必须支持冗余服务器的故障切换机制，包括：Radius 服务器、LDAP 服务器（如果支持 LDAP）和 COPS 服务器(如果支持 COPS)。

设备必须支持 VRRP 功能。

所有元件必须支持热插拔；对于关键部件必须提供冗余备份功能，如主控卡、路由控制卡等；必须支持从故障板卡到冗余板卡到自动切换，手工切换应该作为选项支持；设备中的所有元件必须能够提供 1:1、N:1 或分布式设备冗余能力，这些元件的倒换应是自动的，并且不能影响业务（除第 8 项），设备元件包括：

- (1) 交换单元
- (2) 包转发引擎
- (3) 控制和路由处理器
- (4) 管理系统/管理接口
- (5) 馈电接口
- (6) 电源转换模块/供电单元
- (7) 风扇
- (8) 物理接口模块包括 APS（如 SONET GR253）的冗余能力。所有各种速率（up to OC-48）的 ATM、POS 和通道化接口模块必须支持 N:1 冗余

11 性能

11.1 设备容量要求

11.1.1 设备整机处理能力

要求整机满配置下无阻塞交换，交换容量与端口容量之比大于 2，背板容量大于交换容量（端口容量指可配置的最大数量端口的总带宽；交换容量指交换矩阵最大交换能力；背板容量指背板单位时间内可传输的最大数据量）。

路由器吞吐量在系统满负荷时，（1）所有端口必须能够以线速处理混合字节的 IP 包，必须使用硬件来支持 IP/MPLS 包转发和所有相关业务、控制和安全功能；（2）系统应能够无阻塞地以线速处理所有接口的交换（其中 20% 的流量为组播业务）；（3）同时开启组播、QoS、网络管理、MPLS 等功能时，设备性能应该不低于正常时的 70%。

丢包率：（1）轻载条件下（端口吞吐量 10%），设备的 IP 包丢包率为 0；（2）重载条件下（端口吞吐量 80%），设备的 IP 包丢包率小于 0.1%。

当设备和链路负载小于 90% 的情况下，1518Byte 长度及以下包转发时延均应小于 200us，抖动小于 20us。同时在部署 QoS 后，在低等级的业务造成网络拥塞时，保证高等级业务流量的延时和抖动不受影响。

流量整形能力，接口板上应可以支持 2048 个队列，当支持 2048 个队列时仍能做到线速转发，应支持 8 个等级的丢弃优先级。

11.1.2 设备互通兼容能力

设备应具备与其它厂家设备良好的互联、互通程度和能力；

各种设备接口必须与其它设备的同类型接口具备互通能力（统一标准下）；

设备支持的各种协议与其它设备具备互通能力（统一标准下）。

11.2 路由性能

设备应该支持至少 50,000 条 RIB 表目，平均每个目的地址至少提供 2 条路径；设备必须支持同时维持至少 1000 个 BGP 对等体；至少 100 个 IGP 邻居关系。

当设备容纳 10,000 条 IGP 路由时，建议路由更新收敛时间不大于 500ms。

OSPF 协议路由性能要求：

- (1) 至少应支持 200 个邻居/ospfinstance;
- (2) 至少支持每个 OSPF 区里有 5000 条路由;
- (3) 每台设备至少支持 16 个 OSPF 进程数;
- (4) 支持 ospf instance 的数应不少于支持的 VR 数。

IS-IS 协议路由性能要求:

- (1) 至少应支持 200 个邻居;
- (2) 至少支持每个 ISIS 区里有 5000 条路由;
- (3) ISIS 单 Level 必须支持 1500 条 LSP, 1 万条路由表处理能力

RIP 协议路由性能要求:

- (1) RIB 至少可以支持 50,000 条, 建立至少支持 250,000 条;
- (2) FIB 至少可以支持 50,000 条, 建立至少支持 250,000 条。

BGP 协议路由性能要求:

- (1) A、B、C 类路由器 BGP 会话数量必须不小于 200 个、路由转发表容量不小于 100 万条、path 容量不小于 400 万, 各类板卡能够支持的转发表容量都不小于 100 万条。D 类路由器 BGP 会话数量必须不小于 100 个、路由转发表容量不小于 60 万条, path 容量不小于 240 万, 各类板卡能够支持的转发表容量都不小于 60 万条。;
- (2) BGP/MP-BGP 路由波动对内存占用不能超过 50%, 对 CPU 使用影响不超过 10%。

MPLS 相关性能要求:

- (1) 设备必须支持至少 2000 个 LSP, 整机单向标签表容量大于 300,000 条;
- (2) 在 25 个 LDP 邻居的情况下, 要求至少 2000 个标签/秒的更新能力, 单台设备故障切换造成包转发中断施加不小于 500ms;
- (3) 建立和拆除 LSP 的速度, 要求大于 2000LSP/秒;
- (4) 设备必须支持快速重路由功能, 当链路或节点发生故障时, 在建立 4000 条 LSP 的情况下, 从故障链路或节点切换到备份链路的时间小于或等于 50ms;
- (5) 当设备作为 MPLS 网络 LSR 路由器时, 必须支持 ≥ 32000 条 LSP; 当设备作为 MPLS 边缘路由器 LER 时, 必须支持至少 16000 条 LSP。当

设备在支持最多的 LSP 数量时，应仍然能以限速转发 MPLS 数据包。

11.3 组播性能

要求设备在由 RPT 模式切换到 SPT 过程不能丢包。

单播路由切换后，组播路由切换的时间小于 1 秒。

要求设备必须至少 2000 个组播组；至少支持 10,000 条组播路由；在承载 600 个组，每组 4Mbps 流量的业务时，能稳定运行，要求包转发依赖硬件完成，不影响主控板 CPU 的性能；在启动了组播流量的 QoS 功能后，不能影响业务路由器的性能。

12 设备其它要求

12.1 机箱要求

任何接口模块必须可以被不受限制地插入任何非保留给控制/交换模块地槽位中。

冷却系统必须是冗余和可热插拔的，当一个风扇故障时，剩余的风扇必须能够维持对满载系统的冷却。

必须使用温度传感器监测系统的温度，当系统温度超过预设的阈值时，必须产生一个告警指示，并发送给适当的告警/故障管理系统；必须提供视觉指示（LED）用于显示设备的冷却系统或温度情况（如风扇工作/故障，温度正常/过热等）。

设备应该提供多种机箱以应用于小型、中型及大型接入节点。本规范的要求适用于大型节点的部署，本规范中的功能要求（规模要求除外）适用于任何规模的设备。

12.2 线缆管理

设备应该在机箱的背部提供适当的线缆管理，使用户可以方便地对线缆进行操作。

12.3 设备可用性

集群系统或单台设备必须有高的可靠性，可用率不小于 99.99%，无故障连续工作时间：MTBF 大于 69000 小时。同时要求单端口故障恢复时间小于 10 分钟，单卡板故障恢复时间小于 20 分钟，单机或集群系统故障恢复时间小于 30

分钟。

必须允许对运行系统进行所有适当的配置更改和软件升级而不影响在线用户。建议支持在线软件版本升级 ISSU 能力，小版本升级不影响业务，大版本升级时的业务中断时间少于 1 分钟。

所有元件必须支持热插拔；必须支持关键部件冗余，及从故障板卡到备份板卡的自动切换，详细内容可参见 12.5 节；建议支持不同业务转发板的端口备份；从主用电源到备用电源的切换必须是自动的，不能引起业务的中断；设备应该支持以太网冗余，可以在 800ms 内恢复点对点的千兆以太网连接；在切换到冗余控制板卡时，建议设备能维护 VC、PPP 或 RFC 1483/2684 会话的状态，并保持与之相关的所有功能或协议；满配的设备冷启动后应该在 10 分钟内完全正常运行；在有冗余配置的情况下，从机箱中抽走控制板卡时及重新插入控制板卡时，设备必须能够继续转发流量。

12.4 定时与同步要求

设备必须支持采用主从同步方式。

设备应设置外定时源输入接口，从通信楼定时供给设备（BITS）获得定时。同步接口可以为 2048kbit/s 或 2048kHz，优选 2048kbit/s 接口。

设备应具有从线路信号中恢复定时，并用于同步功能。当不能使用外定时方式时，采用线路定时。可从 STM-N 线路信号中获得，帧结构应符合 ITU-T 建议 G.707 的要求。

设备内部时钟应采用二或三级时钟。时钟单元可采用有保持功能的高稳晶体时钟。二级时钟的自由运行频率准确度优于： $\pm 4 \times 10^{-7}$ ；三级时钟的自由运行频率准确度优于： $\pm 4.6 \times 10^{-6}$ 。

设备在失去全部输入频率基准时钟信号时，内部时钟应能自动进入保持工作方式。时钟能在 24 小时内仍能维持相对于外定时中断瞬间时钟频率不劣于 $\pm 1 \times 10^{-8}$ 的时钟准确度。

设备的定时信号可从下列信号中提取：

- （1）从外同步接口获取；
- （2）从线路信号中获取；
- （3）设备内部时钟产生的可用定时信号中获取。

定时信号的提取顺序为：先（1）后（2）再（3）提取定时信号。

12.5 网络时间同步

设备必须支持网络时间同步协议 NTP，支持 NTP 认证和 NTP 服务器/客户端。

12.6 设备硬件要求

设备必须具备冗余的 Stratum3（或更佳）内部振荡器用于内部时钟，需满足或高于 Issue1 revision 2, of Telcordia GR-1110-Core 第 4.6 节中指定的同步要求。

设备必须为无阻塞的，例如转发容量的内部实现（交换单元，转发平面等）必须等于或超过所有安装的输入端口的容量。

设备必须不存在线头阻塞问题。

12.7 设备软件要求

操作系统的软件升级必须不影响在线用户。必须支持在本地存放多个版本的软件和配置文件。必须支持回退能力，如将操作系统软件/配置退回到先前的版本。

软件的升级版本必须可以在线获取。设备必须支持从 FTP 或 TFTP 服务器下载软件/配置文件。

软件应采用模块化结构，模块之间的通信应按规定的接口进行。

企业必须通过 CMM Level 3 认证，满足对软件开发和质量保证过程的要求。企业必须通过 ISO 9001 认证，满足对软件开发和质量保证过程的要求。设备的工程和制造过程必须通过 TL-9000 认证。

12.8 环境要求

室内型设备必须能够在以下环境条件下正常运行：环境温度：5℃～45℃，每小时变化<10℃；相对湿度：10%～90%（非凝露、非结霜）。

在以下灰尘环境下，设备应能正常工作：直径大于 5 μm 的灰尘浓度≤3×10⁴ 粒/m³；灰尘粒子是非导电、导磁和腐蚀性的。

设备的电磁兼容性应符合国标 GB 9254-1998《信息技术设备无线电骚扰限值和测试方法》和 GB/T 17618-1998《信息技术设备抗扰度限值和测试方法》。设备产生的电磁辐射建议符合 FCC Class A、EN55022/CISPR-22 Class A、VCCI Class A 等标准。

抗震措施：按 8 级烈度进行计算。

机械振动：4.9 牛顿/平方米（50 赫兹至 200 赫兹）。

应提供双电源备份和负载分担功能，必须支持—48V 直流电源，直流电压及其波动范围要求：直流电压及其波动范围要求：额定电压-48V，允许变动范围为-40V~-57V；建议支持-220V 交流电源，交流电压及其波动范围要求：单相 220V±10%，频率 50Hz±5%，线电压波形畸变率小于 3%。

12.9 设备绿色要求

12.9.1 设备管理要求

（1）基本要求

1. 对于机框插槽式设备，设备应有高温报警功能。
2. 对于机框插槽式设备，应具备能源监控及管理功能。在设备管理员需要时，可检测到设备当前能耗状态。
3. 对于机框插槽式设备，应支持根据实际情况中断未用板卡供电或进入微电状态。
4. 设备电源反灌杂音应满足通信电源 YD/T 1051-2000《通信局站电源系统总技术要求》的要求。

（2）扩展要求

1. 对于机框插槽式设备，能通过查询方式监控到目前工作状态下能耗，以及设备各个组件，如各板卡、机框、风扇，所消耗的能耗比例。
2. 对于机框插槽式设备，设备可通过命令行或网管工具远程关闭设备部分模块或功能以减少其工作能耗。
3. 对于机框插槽式设备，可根据实际情况动态调整风扇转速。
4. 对于机框插槽式设备和服务器设备，宜具有可根据用户需求和不同应用场合配置交流或直流供电的选择。

12.9.2 设备环保与包装要求

（1）设备环保要求

设备设计阶段，设备的主要部分（如电路板、机箱、电缆等）应尽量减少铅、镉、汞、六价铬、溴化耐燃剂等有害物质，并严格按 ROHS 规范进行产品生产与设计。

（2）设备包装要求

实行包装减量化（Reduce）。绿色包装在满足保护、方便、销售等功能的条件下，应是用量最少的适度包装。

包装应易于重复利用（Reuse）或易于回收再生（Recycle）。

包装废弃物可以降解腐化（Degradable）。为了不形成永久的垃圾，不可回收利用的包装废弃物要能分解腐化，进而达到改善土壤的目的。

包装材料对人体和生物应无毒无害，包装材料中不应含有有毒物质或有毒物质的含量应控制在有关标准以下。

包装材料应尽量减少木材的使用。

在包装产品的整个生命周期中，均不应对环境产生污染或造成公害。

（3）其它要求

设备内部应有合理的气流组织，应采用前进后出或垂直通风方式，不宜从侧面进出通风。

同时，机框式数据设备内风扇应具有自动调节速率的功能，机架内采用防热风回流等技术，降低对机房环境的局部制冷要求。

机架门开孔率：考虑到通风和散热的需求，在保证门的强度和刚度要求前提下，机架正面门和背面门开孔率至少不得低于 30%，以获得良好的排吸风效果。

12.9.3 能耗分级标准

设备能耗等级应达到最新版本的中国电信《绿色数据设备技术规范》所定义的标准。

中国电信集团公司技术标准

Q/CT 2077-2008

中国电信 IP 城域网设备技术规范 (业务路由器)

(V3.0)

2008-12-31 发布

2009-1-1 实施

中国电信集团公司 发布

目 录

1	编制说明	1
1.1	范围	1
1.2	引用标准	1
1.3	定义、术语和缩写	8
1.3.1	定义	8
1.3.2	术语和缩写	8
2	概述	11
2.1	SR 的定位	11
2.2	SR 的功能组成	12
2.3	SR 能够提供的业务	13
2.3.1	互联网业务的实现思路	14
2.3.2	VPN 业务等实现思路	14
2.3.3	组播业务的实现思路	14
2.4	设备分类	14
3	接口要求	15
3.1	常规	15
3.2	以太网接口	15
3.2.1	接口类型及特性	15
3.2.1.1	10Mbit/s 和 100M bit/s 以太网接口	15
3.2.1.2	1000Mbit/s 以太网接口	15
3.2.1.3	10Gbit/s 以太网接口	16
3.2.2	功能要求	16
3.3	PoS 接口	16
3.3.1	接口类型及特性	16
3.3.2	链路层及功能要求	17
3.4	ATM 接口	17
3.4.1	接口类型及特性	17
3.4.2	ATM 层要求	17
3.5	其它接口	18
4	用户管理	18
4.1	用户认证方式	18
4.2	IPOE 认证方式	19
4.3	授权	21
4.4	计费	21
4.5	地址管理与分配	22
4.6	RADIUS	23
5	策略控制	23
6	路由功能	26
6.1	常规要求	26
6.1.1	协议和地址	26
6.1.2	路由	27
6.2	OSPF 路由协议功能要求	28

6.3	ISIS 路由协议功能要求.....	29
6.4	RIPv1/v2 路由协议功能要求	30
6.5	BGP-4 路由协议功能要求.....	30
7	QoS.....	33
7.1	QoS 机制	33
7.2	QoS 能力	35
7.3	DPI 功能.....	35
8	MPLS 功能.....	36
8.1	MPLS 基本功能.....	36
8.2	MPLS 流量工程.....	37
9	VPN	38
9.1	L2 VPN.....	38
9.1.1	L2TP.....	38
9.1.1.1	L2TP 基本要求.....	38
9.1.1.2	LAC 和 LNS.....	39
9.1.2	基于 IP/MPLS 二层的 VPN.....	40
9.2	L3 VPN.....	41
9.2.1	MPLS VPN	41
9.2.2	IPSec	42
9.2.3	GRE.....	42
10	组播.....	43
11	IPv6.....	44
12	设备管理功能	46
12.1	基本管理功能	46
12.2	SNMP MIB.....	47
12.3	故障管理	48
12.4	配置管理	49
12.5	计费管理.....	49
12.6	性能管理	49
12.7	安全管理	49
13	安全	50
13.1	访问控制和流量控制	50
13.2	路由协议安全	50
13.3	抗攻击能力	51
13.4	网络地址/端口翻译.....	51
13.5	MPLS VPN.....	51
13.6	冗余	52
14	性能	53
14.1	设备容量要求	53
14.2	路由性能.....	53
14.3	VPN 性能	54
14.4	组播性能.....	55
14.5	整机业务叠加性能.....	55
15	设备其它要求	55

15.1	机箱要求	55
15.2	线缆管理	56
15.3	设备可用性	56
15.4	定时与同步要求	56
15.5	网络时间同步	57
15.6	OAM 要求	57
15.7	设备硬件要求	57
15.8	设备软件要求	58
15.9	环境要求	58
15.10	绿色要求	59
15.10.1	设备管理要求	59
15.10.2	设备环保与包装要求	60
15.10.3	能耗分级标准	60
附 录 A	CE 设备技术要求	61
A1	CE 的定位	61
A2	CE 设备的技术要求	61
A2.1	设备分类及接口要求	61
A2.2	基本功能要求	61
A2.2.1	链路聚合	61
A2.2.2	生成树协议	61
A2.2.3	VALN/SVLAN	62
A2.2.4	VRRP 功能	62
A2.3	路由功能要求	63
A2.4	QoS 要求	63
A2.5	VPN 要求	63
A2.6	组播要求	63
A2.7	IPv6 要求	63
A2.8	设备管理功能要求	63
A2.9	安全要求	63
A2.10	BFD 功能要求	63
A2.11	OAM 要求	64
A2.12	定时与同步要求	64
A2.13	性能要求	64

1 编制说明

1.1 范围

本技术规范以 RFC 文档、IEEE 标准以及国内相关行业标准为依据，根据中国电信实际情况和具体要求，对 IP 城域网中业务路由器的定义、网络定位、业务功能、接口、用户管理、认证、计费、IP 地址分配、流量控制、拥塞管理、服务级别、组播应用、网络管理、网络安全等进行了规定。

本技术规范适用于中国电信集团宽带网络业务路由器的选型。

在本规范中：

必须：表示该条目是本规范必须，违反这样的要求是原则性错误。

必须实现：表示该要求必须实现，但不要求缺省使能。

不允许(不可以)：表示该条目绝对禁止。

应当(建议)：表示在某些特定条件下存在忽视该条目的理由，但是忽视或违反该条目时必须仔细衡量。

应当(建议)实现：与应当(建议)类似，实现时不必要缺省使能。

不应当(不建议)：表示在某些特定条件下存在所描述行为可接受或有效的理由，但实现该行为时必须仔细衡量。

可以：表示该条目确实可选。

1.2 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。

GB/T17625.1-2003	《电磁兼容 限值 谐波电流发射限值(设备每相输入电流 $\leq 16\text{A}$)》
GB17625.2-1999	《电磁兼容 限值 对额定电流不大于 16A 的设备在低压供电系统中产生电压波动和闪烁的限制》
YD/T 1051-2000	《通信局站电源系统总技术要求》
SPECpower_ssj2008	标准效能公司能耗测试标准
能源之星 4.0	主要针对消费性电子产品的能源节约计划。
COC on Energy Consumption of Broadband	宽带设备能源消耗管理

Equipment	
GB/T 2423 系列	电工电子产品的基本环境试验规程
GB/T 4798.3-1990	电工电子产品应用环境条件 有气候防护场所固定使用
GB/T 4798.1-2005	电工电子产品应用环境条件 贮存
GB/T 4798.9-1997	电工电子产品应用环境条件 产品内部的微气候
YDN 052-1998	B-ISDN ATM 层技术规范
YDN 053.4-1998	B-ISDN ATM 适配层 (AAL) 类型 5 技术规范
YDN 099-1998	光同步传送网技术体制 (暂行规定)
YDN 104-1999	ATM 网络业务量控制和拥塞控制功能
YDN 120-1999	光波分复用系统总体技术要求 (暂行规定)
YD/T 877-1996	同步数字体系 (SDH) 利用设备和系统的电接口技术要求
YD/T 973-1998	SDH 155Mb/s 和 622Mb/s 光发送模块和光接收模块技术条件
YD/T 976-1998	B-ISDN 用户网络接口 (UNI) 物理层规范
YD/T 1097-2001	路由器设备技术规范-高端路由器
YDN 1109-2001	ATM 交换机设备技术规范
YD/T 1111.1-2001	SDH 光发送/光接收模块技术要求-2.488320Gb/s 光接收模块
YD/T 1111.2-2001	SDH 光发送/光接收模块技术要求-2.488320Gb/s 光发送模块
YD/T 1162.1-2005	多协议标签交换 (MPLS) 技术要求
YD/T 1162.2-2001	在 ATM 上实现 MPLS 的技术要求
YD/T 1190-2002	基于网络的虚拟 IP 专用网 (IP-VPN) 框架
YD/T 1199.1-2002	SDH 光发送/光接收模块技术要求-SDH 10Gb/s 光接收模块
YD/T 1199.2-2002	SDH 光发送/光接收模块技术要求-SDH 10Gb/s 光发送模块
YD/T 1267-2003	基于 SDH 传送网的同步网技术要求
YD/T 1345-2005	基于 SDH 的多业务传送节点 (MSTP) 技术要求-内嵌弹性分组环 (RPR) 功能部分
YD/T 1359-2005	路由器设备安全技术要求—高端路由器 (基于 IPv4)
YD/T 1471-2006	基于 IP 的二层虚拟专用网 (VPN) 业务技术要求
YD/T 1474-2006	基于 SDH 的多业务传送节点 (MSTP) 技术要求-内嵌多协议标签交换 (MPLS) 功能部分
YD/T 1476-2006	基于边界网关协议/多协议标签交换的虚拟专用网 (BGP/MPLS VPN) 技术要求
YD/T 1477-2006	基于边界网关协议/多协议标签交换的虚拟专用网 (BGP/MPLS VPN) 组网要求
RFC768	UDP 协议
RFC791	IP 协议
RFC792	ICMP 协议

RFC793	TCP 协议
RFC826	以太网 ARP 协议
RFC854	TELNET 协议规范
RFC862	Echo 协议
RFC863	丢弃协议
RFC894	在以太网上传输 IP 数据报的标准
RFC896	IP/TCP 互联网拥塞控制
RFC922	IP 广播
RFC950	IP 相关子网
RFC959	FTP
RFC1042	在 IEEE802 网络上的 IP 数据报传输标准
RFC1122	互联网主机要求—通信层
RFC1144	低速串行链路上的 TCP/IP 头的压缩算法
RFC1155	基于 TCP/IP 的互联网管理信息的结构和标识
RFC1157	简单网络管理协议
RFC1166	互联网号码
RFC1195	用于在 TCP/IP 和 OSI 双重环境中 IS-IS 路由
RFC1212	简明 MIB 定义
RFC1213	基于 TCP/IP 的互联网的网络管理信息库：MIB-II
RFC1256	ICMP 路由器发现消息
RFC1321	MD5 算法
RFC1332	IPCP 协议
RFC1334	PAP 协议
RFC1519	CIDR：一种地址分配和聚合的策略
RFC1631	IP 网络地址转换 (NAT)
RFC1661	PPP 协议
RFC1662	在类 HDLC 帧中的 PPP 协议
RFC1772	互联网中 BGP 的应用
RFC1812	IPv4 路由器要求
RFC1918	私网地址分配
RFC1990	PPP 多链协议
RFC1994	CHAP 协议
RFC1997	BGP 团体属性
RFC1998	多归属路由中 BGP 团体属性的应用
RFC2080	IPv6 的 RIPng
RFC2082	RIP v2 MD5 认证

RFC2153	PPP 厂商扩展
RFC2205	RSVP 功能技术规范.
RFC2209	RSVPv1 消息处理规则
RFC2210	IETF 综合业务的 RSVP 使用
RFC2228	FTP 安全扩展
RFC2236	互联网组管理协议 IGMPv2
RFC2328	OSPF v2 协议
RFC2362	协议无关组播一稀疏模式
RFC2364	AAL5 上的 PPP
RFC2385	通过 TCP MD5 签名选项对 BGP 会话的保护
RFC2370	OSPF Opaque LSA 选项
RFC2401	互联网协议安全体系
RFC2439	BGP4 路由振荡抑制
RFC2453	RIPv2 协议
RFC2460	互联网协议一第六版 (IPv6) 规范
RFC2461	IPv6 的邻居发现
RFC2464	在以太网上传送 IPv6 报文
RFC2465	IPv6 MIB 的文本规定和总体组
RFC2466	IPv6 MIB: ICMP 组
RFC2474	IPv4 和 IPv6 报头中 DS 字段的定义
RFC2475	Diff-Serv 体系结构
RFC2484	PPP LCP 国际配置选项
RFC2515	ATM 管理目标定义
RFC2516	传输 PPPoE 之方法
RFC2529	在 IPv4 域中不使用显式隧道传输 IPv6
RFC2545	用于 IPv6 域间路由的 BGP-4 多协议扩展
RFC2597	AF PHB 组
RFC2615	SONET/SDH 上 PPP 协议
RFC2661	L2TP 协议
RFC2684	AAL5 上的多协议封装
RFC2697	单一速率三色标记
RFC2698	两个速率三色标记
RFC2702	MPLS 上 TE 要求
RFC2750	用于策略控制的 RSVP 扩展
RFC2763	IS-IS 动态主机名交换机制
RFC2773	使用 KEA 和 SKIPJACK 的加密技术

RFC2858	BGP-4 多协议扩展
RFC2865	RADIUS 协议—认证
RFC2866	RADIUS 协议—计费
RFC2867	RADIUS 协议—隧道协议的计费
RFC2868	RADIUS 协议—隧道协议的认证
RFC2869	RADIUS 协议扩展
RFC2918	BGP-4 路由刷新能力
RFC2966	两层 ISIS 域范围的前缀分发
RFC3022	传统的 IP 网络地址翻译
RFC3031	MPLS 体系架构
RFC3032	MPLS 标签堆栈编码
RFC3035	使用 LDP 和 ATM VC 交换的 MPLS
RFC3036	LDP 技术规范
RFC3037	LDP 适用性
RFC3063	MPLS 环回检测机制
RFC3065	BGP 自治系统联盟
RFC3101	OSPF NSSA 选项
RFC3168	IP 显式拥塞通知 (ECN) 的增加
RFC3181	抢占通知的优先级策略要素
RFC3209	RSVP-TE: LSP 隧道的 RSVP 扩展
RFC3241	PPP 上强健性头压缩
RFC3246	快速转发 (EF) PHB
RFC3260	Diffserv.新增术语和澄清
RFC3272	互联网流量工程概述和原则
RFC3277	IS-IS 瞬时黑洞避免
RFC3346	MPLS 流量工程适用性说明
RFC3373	IS-IS 点对点邻接的三次握手
RFC3376	互联网组管理协议—第三版 (IGMPv3)
RFC3392	BGP-4 能力发布
RFC3443	MPLS 网络中 TTL 处理
RFC3478	LDP 平滑重启机制
RFC3564	支持差分服务感知的 MPLS 流量工程要求
RFC3567	IS-IS 加密认证
RFC3576	RADIUS 动态认证扩展
RFC3618	组播源发现协议
RFC3623	OSPF 平滑重启

RFC3630	OSPFv2 的流量工程扩展
RFC3635	以太网接口类型的管理目标定义
RFC3784	IS-IS 的流量工程扩展
RFC3768	虚拟路由器冗余协议 (VRRP)
RFC3847	IS-IS 的重启信令
RFC3936	修改 RSVP 过程
RFC4022	TCP 的 MIB
RFC4087	IP 隧道 MIB
RFC4090	用于 LSP 隧道的 RSVP-TE 快速重路由
RFC4113	UDP 的 MIB
RFC4182	删除 MPLS 显式为 NULL 的限制
RFC4203	支持 GMPLS 的 OSPF 扩展
RFC4205	支持 GMPLS 的 IS-IS 扩展
RFC4271	边界网关协议—第 4 版 (BGP-4)
RFC4273	BGP-4 管理目标定义
RFC4292	IP 转发表 MIB
RFC4293	IP 的 MIB
RFC4302	IP 认证头
RFC4303	IP 安全载荷封装
RFC4305	安全载荷封装 (ESP) 和认证头 (AH) 加密算法实现要求
RFC4364	BGP/MPLS IP 虚拟专用网
RFC4379	MPLS 数据平面故障检测
RFC4420	使用 RSVP 流量工程建立 MPLS LSP 的属性编码
RFC4456	BGP 路由反射
RFC4486	BGP 中止通知消息子编码
RFC4495	减少一个流的预留带宽的 RSVP 扩展
RFC4560	远程 Ping, Traceroute, 和 Lookup 操作的管理目标定义
RFC4576	BGP/MPLS IP VPN 中使用 LSA 选项比特阻止环回
RFC4577	BGP/MPLS IP VPN 中运营商/客户之间使用 OSPF 协议
RFC4750	OSPFv2 MIB
RFC4124	支持差分服务感知流量工程的协议扩展
RFC4125	最大分配带宽约束模型
RFC4126	基于带宽预留的最大分配带宽约束模型
RFC4127	俄罗斯套娃带宽约束模型
RFC3630	OSPFv2 流量工程扩展
RFC 4905	MPLS 网络上二层帧传送的封装方法

RFC 4906	MPLS 上二层帧的传送
RFC 4762	使用 LDP 信令的 VPLS
RFC 4761	使用 BGP 自动发现和信令的 VPLS
IEEE 802.1ad	运营商桥接
IEEE 802.1p	服务等级和优先级标准
IEEE 802.1Q	虚拟局域网
IEEE 802.3	CSMA/CD 访问方法和物理层技术规范
IEEE 802.3ac	VLAN 标记扩展
IEEE 802.3ae	10Gb/s 以太网物理层接口规范
IEEE 802.3ab	1000Base-T 以太网物理层接口规范
IEEE 802.3ad	链路聚合
IEEE 802.3u	100Base-T 以太网接口物理层规范
IEEE 802.3x	以太网接口流量控制
IEEE 802.3z	千兆以太网接口物理层规范
IEEE 802.17	RPR 物理层规范
ITU-T G.707	SDH 网络节点接口
ITU-T I.610	B-ISDN 操作和维护原则功能
ITU-T I.731	ATM 设备类型和通用特征
ITU-T I.732	ATM 设备功能特征
af-uni-0010.002	ATM 用户-网络接口规范 V3.1
af-tm-0121.000	业务量管理规范 V4.1
af-tm-0149.000	业务量管理规范 V4.1-补遗：差分 UBR 业务
af-tm-0150.000	业务量管理规范 V4.1-补遗：UBR 最小接入信元速率的可选指示
draft-ietf-bfd-base-08	双向转发检测
draft-ietf-bfd-v4v6-1hop-08	IPv4/v6 双向转发检测（单跳）
draft-ietf-bfd-multihop-06	多跳路径的双向转发检测
draft-ietf-bfd-mpls-07	MPLS LSP 中的双向转发检测
RFC4724	BGP 平滑重启机制
RFC 5120	IS-IS 的多拓扑路由
RFC 4915	OSPF 的多拓扑路由

1.3 定义、术语和缩写

1.3.1 定义

业务路由器(Service Router, 简称 SR)是面向宽带网络应用的新型接入网关,是城域网的业务接入控制点,位于 IP 城域网的骨干网内的业务接入控制层。

1.3.2 术语和缩写

AAL	ATM Adaptation Layer (ATM 适配层)
ACL	Access Control List (访问控制列表)
ADSL	Asymmetric Digital Subscriber Line (非对称数字用户线)
AF	Assured Forward (确保转发)
AIS	Alarm Indication Signal (告警指示信号)
APS	Auto-Protection Switching (自动保护倒换)
AS	Autonomous system (自治系统)
ATM	Asynchronous Transfer Mode (异步转移模式)
BGP	Border Gateway Protocol (边界网关协议)
BF	Besteffort Forwarding (尽力转发)
BFD	Bidirectional Forwarding Detection (双向转发检测)
BITS	Building Integrated Timing Source (通信楼综合定时供给系统)
BRAS	Broadband Remote Access Service (宽带远程接入服务)
CAR	Committed Access Rate (提交的接入速率)
CBS	Committed Burst Size (提交的突发长度)
CBWFQ	Class-Based Weighted Fair Queueing (基于类的加权公平排队)
CE	Customer edge (客户边缘)
CPE	Customer Presidial Equipment (用户驻地设备)
CQ	Custom Queuing (自定义排队)
CIR	Committed Information Rate (提交信息速率)
CSPF	基于约束的最短路径优先
CT	Class-Type (级别类型)
DHCP	Dynamic Host Configuration Protocol (动态主机配置协议)
DiffServ	Differentiate Service (差分服务)
DPI	Deep Packet Inspection (深度包检测)
DSCP	Diff-Serv Code Point (差分服务码点)
DSLAM	Digital Subscriber Line Access Multiplexer (数字用户接入线复用器)
EBS	Exceed Burst Size (超过的突发长度)

E-LSP	EXP-Inferred-PSC LSPs (PSC 使用 exp 字段的 LSP)
ECMP	Equal Cost Multi-Path (等值多路径)
EF	Expressed Forward (加快转发)
FRR	Fast ReRoute (快速重路由)
GBIC	GigaBit Interface Converter (吉比特接口转换器)
GE	Gigabits Ethernet (千兆以太网)
GRE	Generic Routing Encapsulation (通用路由协议封装)
ICP	Internet Content Provider (互联网内容提供商)
IGMP	Internet Group Management Protocol (互联网组管理协议)
IPsec	IP Security Protocol (IP 网络安全协议)
IPTV	IP Television (IP 电视)
IPoE	IP Over Ethernet (以太网上承载 IP 报文)
IS-IS	Intermediate System to Intermediate System (中间系统到中间系统)
ISP	Internet Service Provider (互联网服务提供商)
ISPF	Increment SPF (增量 SPF 算法)
L2	Layer 2 (本文特指以太帧层)
L2TP	Layer 2 Tunneling Protocol (第二层隧道协议)
L3	Layer 3 (本文特指 IP 层)
LAC	L2TP Access Concentrator (L2TP 接入集中器)
LAN	Local Area Networks (局域网)
LDP	Label Distribution Protocol (标签分发协议)
LLC	Logical Link Control (逻辑链路控制)
LLQ	Low Latency Queue (低延迟队列)
L-LSP	Label-Only-Inferred-PSC LSP
LNS	L2TP Network Server (L2TP 网络服务器)
LSP	Label Switch Path (标签交换路径)
MAC	Media Access Control (介质访问控制)
MDCR	Minimum Desired Cell Rate (最小希望信元速率)
MBGP	Multi-Protocol BGP (多协议 BGP)
MPLS	Multi-Protocol Label Switching (多协议标签交换)
MPLS EXP	MPLS experimental Field (MPLS 试验字段)
MSTP	Multi-Service Transport Platform (多业务传送平台)
MTBF	Mean Time Between Failures (平均无故障间隔时间)
MAM	Maximum Allocation Model (最大分配带宽约束模型)
MAR	Maximum Allocation with Reservation (基于带宽预留的最大分配带宽约

	束模型)
OAM	Operation And Maintenance (操作和维护)
OLT	Optical Line Terminal (光线路终端)
ONU	ONU Optical Network Unit (光网络单元)
OSI	Open System Interconnection (开放的系统互联)
OSPF	Open Shortest Path First Protocol (开放式最短路径优先协议)
OTU	Optical Transport Unit (光传送单元)
PE	Provider Edge (运营商边缘)
PHB	Per-Hop Behavior (每跳行为)
PoS	Packet over SDH (SDH 上承载分组)
PPP	Point To Point Protocol (点到点协议)
PPPOA	PPP Over AAL5 (AAL5 上承载 PPP)
PPPOE	PPP Over Ethernet (以太网上承载 PPP)
PPS	Packets Per Second (每秒分组数)
PRC	Partial Route Calculation (部分路由计算)
PSC	PHB Scheduling Class (PHB 预定类别)
PVC	Permanent Virtual Circuit (永久虚连接)
PQ	Priority Queuing (优先级排队)
QoS	Quality of Service (服务质量保证)
RADIUS	Remote Authorization Dial In User Service (远程认证拨号用户服务)
RDI	Remote Defect Indication (远端故障指示)
RDM	Russian Dolls Model (俄罗斯套娃带宽约束模型)
RED	Random Early Detection (随机早期检测)
RIP	Routing Information Protocol (路由信息协议)
RPR	Resilient Packet Ring (弹性分组环)
SDH	Synchronous Digital Hierarchy (同步数字序列)
SDN	Switched Data Network (交换数据网)
SNAP	Service Network Access Point (业务网络接入点)
SNMP	Simple Network Management Protocol (简单网络管理协议)
SR	Service Router (业务路由器)
TE	Traffic Engineering 流量工程
ToS	Type Of Service 业务类型
uRPF	unicast Reverse Path Forwarding (单播反向路径转发)
VLAN	Virtual LAN (虚拟局域网)
VC	Virtual Channel (虚通道)
VP	Virtual Path (虚通路)

VPDN	Virtual Private Dial_up Network (虚拟拨号专网)
VPLS	Virtual Private LAN Service (虚拟专用以太网服务)
VPN	Virtual Private Network (虚拟专用网)
VR	Virtual Router (虚拟路由器)
VRF	Virtual Route Forwarding Table (VPN 路由转发表)
WRED	Weighted Random Early Detection (加权随机早期检测)
WRR	Weighted Round-Robin (加权循环队列调度)

2 概述

2.1 SR 的定位

SR 在 IP 城域网中，处于城域骨干网的业务接入控制层。

SR 向下接口：

- (1) SR 可以通过 ATM 接口连接 ATM 网络或直接连接 ADSL 局端 DSLAM 设备或专线用户接入设备，实现专线用户的汇接。
- (2) SR 可以通过 GE/10GE 接口连接汇聚交换机，实现以太网 LAN 专线用户的汇接。
- (3) SR 可以通过 MSTP 网络连接大客户接入设备，实现大客户专线用户的汇接。
- (4) SR 可以通过 GE/10GE 接口连接 OLT 设备，实现 FTTx 专线用户的汇接。
- (5) SR 可以提供直联政企客户的高速接口。

SR 向上接口：

- (1) SR 通常以 GE 接口(或 10GE 接口)、2.5G PoS 接口(或 10GPoS)连接城域网骨干路由器，实现业务的上行。
- (2) SR 可通过 GE 接口(或 10GE 接口)、2.5G PoS 接口(或 10GPoS)连接到 CN2 骨干网业务路由器，进而连接到 CN2 骨干网中，用于实现 MPLS VPN 的跨域互通。

使用独立以太网或 PoS 承载三层网络上行流量，可使用双链路提供冗余。

典型的网络拓扑如下图 2-1 所示：

网关业务功能。

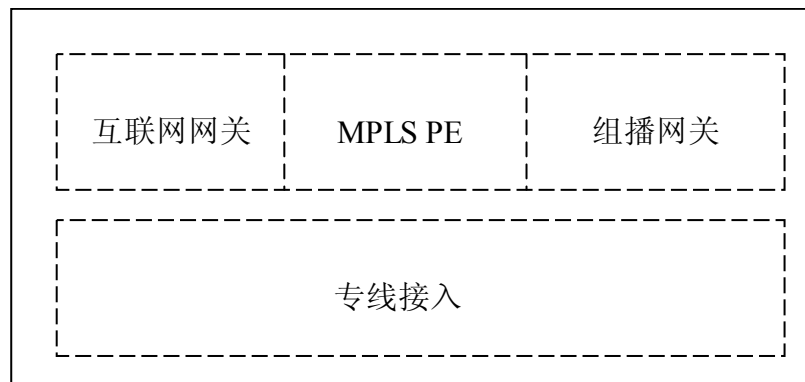


图 2-2 SR的业务功能模块

SR 各组成模块的主要功能如下：

(1) 专线接入功能模块

提供用户接入端口（物理端口或逻辑端口）以及在端口上的接入控制功能，如 Diffserv 标记、速率限制或流量整形、ACL、uRPF 等安全控制、流量采集和统计等。

(2) 互联网网关业务功能模块

用户 IP 地址和路由提供。

实现大客户专线接入互联网的业务，用户可直接通过 MSTP/RPR 和以太汇聚网接入 SR，也可采用光纤直连接入 SR 进行业务接入控制，实现专线接入网关功能。

(3) MPLS VPN PE 业务功能模块

二三层 MPLS VPN 业务功能，主要实现 MPLS L3 VPN 的 PE、PE ASBR 和 VPN RR 的功能，实现 VPLS 的 PE 功能。

(4) 组播网关业务功能模块

组播路由，IGMP 控制，组播用户管理和控制，组播复制。

综上所述，SR 接入功能模块主要是专线接入。SR 业务功能模块主要实现互联网网关业务功能，提供互联网业务；实现 PE 业务功能，提供 MPLS 二三层 VPN 业务；实现组播网关业务功能，提供 IPTV 等基于组播等业务。

2.3 SR 能够提供的业务

目前 SR 主要是基于 xDSL/LAN 的专线接入业务，也可以充当城域网的 PE

设备，基于 SR 还可以实现 IP VPN/VPDN，构建企业内部 Intranet 等应用。

2.3.1 互联网业务的实现思路

互联网业务为用户提供到城域网的宽带接入并连接到 CHINANET、CN2 以及 INTERNET 的业务，是城域网最基本的业务。

xDSL/LAN 专线用户接入 DSLAM 或二层交换机，通过 ATM 网或以太网汇聚到 SR，对于光纤直连的大客户专线通过 MSTP/RPR/SDN 网络接入到 SR，SR 提供路由，并实现 ACL、uRPF 等安全控制和速率限制，实现 DSCP 标记等 QoS 控制。

2.3.2 VPN 业务等实现思路

(1) 二/三层 MPLS VPN

SR 作为 PE，通过城域核心的 P 路由器(对开启 MPLS 的城域网)或 CN2 的 PE 路由器(对不开启 MPLS 的城域网)实现本地或跨域的二/三层 MPLS VPN 业务。

(2) VPDN

用户可通过二次拨号发起 IPSec 或其它形式的隧道，终结于 SR，实现用户远程接入 MPLS 三层 VPN。

2.3.3 组播业务的实现思路

当城域网内 BRAS 设备无法满足组播业务开展的功能和性能要求时，可以在 SR 上实现组播业务。

SR 是 PIM 路由协议的边界，IGMP 请求的终结点，负责组播业务的接入控制，通过静态组加入配置将所有组播流量推送到 SR。

二层汇聚网络为组播业务提供专用 VLAN，组播包由 SR 向用户接入点的逐级复制，并最终由用户接入点实现面向用户的跨 VLAN 组播复制。

2.4 设备分类

根据支持的用户规模，设备分为以下 A、B 两类。

	A 类	B 类
单槽交换及可配置容量(单向)	≥20G	≥20G
整机端口线速配置容量(单向)	≥240G	≥120G
上联端口	10GPOS/2.5G POS/10GE/GE	2.5G PoS/10GE/GE
下联端口	10GE/GE/FE/ STM-1 ATM	

部署位置	业务密集的地方	业务较密集的地方
------	---------	----------

3 接口要求

3.1 常规

SR 必须具备通过 RS-232C VT-100 类型终端访问的控制接口。

SR 应该具备冗余 BITS 外部时钟输入接口。

SR 必须能够从通道化接口取得时钟。

所有接口必须能够用于用户接入或网络上而不影响接口的功能。

SR 必须支持在所有 SONET/SDH/TDM 端口的物理端口 loopback。

SR 必须支持 100Base-T/GE/2.5G PoS 接口，必须支持 10GE、10G PoS 接口，建议支持 STM-1/STM-4 的 ATM 接口。

A 类设备必须在不更换任何硬件设备(机箱、引擎、电源、风扇等等)的条件下具备支持未来 20G 的业务卡。

3.2 以太网接口

SR 必须支持由“IEEE Std 802.3, 2005 Edition, Carrier sense multiple access with collision detection(CSMA/CD) access method and physical layer specifications”所定义的 10/100Mbps 和 1000Mbps 双绞线及光纤要求。

建议 SR 支持“IEEE802.3ae, 2002 Edition, Media Access Control(MAC) Parameters, Physical Layers, and Management Parameters for 10Gb/s Operation”。

设备必须在 GE/10GE 以太网物理端口上支持超长帧(Jumbo Ethernet frame)。

要求以下各种类型接口的 MTU 可配置，支持 L3 MTU 值必须不小于 1500；GE/10GE 接口的 MTU 应不小于 9178。

3.2.1 接口类型及特性

3.2.1.1 10Mbit/s 和 100M bit/s 以太网接口

10Mbit/s 以太网接口应符合 IEEE802.3。

100Mbit/s 以太网接口应符合 IEEE802.3u。100Base-T 技术中可采用三类传输介质：100Base-T4、100Base-TX 和 100Base-FX。

SR 必须支持 10/100Base-T 自适应接口。

3.2.1.2 1000Mbit/s 以太网接口

SR 必须支持千兆以太网(1000Mbit/s)接口。1000Mb/s 以太网物理接口可以支

持 1000Base-Sx、1000Base-LX 以及 1000Base-T。其中，1000Base-SX 和 1000Base-LX 接口特性应符合 YD/T1097-2001 的 5.2.2 节的要求。1000Base-T 接口应符合 IEEE802.3ab。

千兆以太网光接口必须支持 GBIC 或 SFP 模块。

3.2.1.3 10Gbit/s 以太网接口

建议 SR 支持 10Gbit/s 以太网接口，应支持 10GBase-R，建议支持 10GBase-W。所支持的 10Gbit/s 以太网接口特性应符合 IEEE802.3ae。

安装在路由器设备上的 10Gbit/s 接口卡，应只占用一个槽位，除非特殊原因，不建议使用占用双（多）槽位的 10Gbit/s 接口卡。

3.2.2 功能要求

必须支持 IEEE802.1Q VLAN，和 IEEE 802.1p 的优先级设定功能。

SR 必须支持符合 IEEE802.1ad 的 VLAN 堆叠 (Stack VLAN)，其外层以太网帧协议标识为 0x88A8，建议设备端口支持对该字段参数可配置。

SR 必须支持 QinQ 透传功能。

SR 必须支持 QinQ 直接终结入三层功能，三层 IP 口必须是可路由可调度接口。

SR 必须支持单口 SVLAN 的内外层可配置范围均在 1-4096。

在最高速接口上应支持长达 15 分钟的比特计数而不溢出。

支持流控功能。

SR 必须支持在一个物理端口上通过逻辑接口同时实现 L2 和 L3 功能。

SR 应该支持在物理端口上的 IEEE 802.3ad 链路汇聚/负载分担功能。设备在启用链路聚合功能时必须实现对 VLAN 及 SVLAN 的透传承载。

SR 必须支持 VRRP 功能。设备在启用 VRRP 功能时必须实现对 VLAN 及 SVLAN 的透传承载。设备必须支持 BFD for VRRP。

SR 必须支持在 GE/10GE 接口上的 MPLS。

3.3 PoS 接口

3.3.1 接口类型及特性

PoS 接口的 SDH 帧封装应符合标准 ITU-T G.707 (1996)；接口性能应符合标准 ITU-T G.957 (1995)；误码率应符合标准 ITU-T G.826 (1996)；抖动与漂移应符合标准 ITU-T G.825 (1993)。

接口类型必须支持 STM-1 接口，STM-4 接口和 STM-16 接口，建议支持

STM-64 接口,其中 STM-1 和 STM-4 接口必须符合 YD/T973-1998 规定的 SDH 155 Mb/s、622Mb/s 光发送和接收模块的技术条件要求; STM-16 接口必须符合 YD/T 1111.1-2001 和 YD/T 1111.2-2001 规定的 SDH 2.488320Gb/s 光接收模块和光发送模块技术要求; STM-64 接口则必须符合 YD/T 1199.1-2002 和 YD/T 1199.2-2002 规定的 SDH 10Gb/s 光接收模块和光发送模块技术要求, 安装在路由器设备上的 10Gbit/s 接口卡, 应只占用一个槽位, 除非特殊情况, 不建议使用占用双 (多) 槽位的 10Gbit/s 接口卡。

设备的 PoS 接口必须支持 1+1 自动保护倒换。

所有的光接口必须支持单模和多模。

3.3.2 链路层及功能要求

PoS 端口链路层协议要求支持 HDLC 和 PPP over SONET/SDH (RFC1662、RFC2615) 。

PPP 协议由标准 RFC1661 描述。IP 数据包也可以遵循 YD/T 1061-2000 同步数字体系 (SDH) 上传送 IP 的 LAPS 技术要求, 先转换成 LAPS 帧结构, 再映射到 SDH 虚容器中。IPv6 数据包遵循 RFC2472。

能通过调度排队算法提供 QoS (或 CoS)。

必须支持基于 IP 的拥塞管理。

必须支持 PoS 上的 MPLS。

3.4 ATM 接口

3.4.1 接口类型及特性

路由器的 ATM 接口必须支持 STM-1 接口标准、STM-4 接口标准。

ATM 接口应支持光接口和电接口两种类型, 电接口适用于局内、干扰信号弱的情况; 光接口必须符合 YD/T 976-1998 中的相关要求; 物理层采用两种速率接口: 155520Kbit/s 和 622080Kbit/s。

必须支持 APS 1+1 保护。

应支持光接口和电接口两种类型, 电接口适用于局内、干扰信号弱的情况。

3.4.2 ATM 层要求

ATM 层应该符合 YDN 052-1997 的规定; ATM 适配层必须符合 YDN 053.4-1997 中的规定; ATM 接口必须按照 RFC2684 规定将 IP 包封装到 AAL5 的帧格式中。

必须支持 LLC/SNAP 和 IP 复用 PVC(路由协议的 LLC 封装)。

SR 应该支持 ATM 论坛用户-网络互联接口(UNI)规范，版本 3.1。

SR 必须支持 ATM 论坛流量管理规范 4.1 所定义的 ATM CBR 服务等级、UBR 业务等级、ATM nrt-VBR 服务等级和 ATM rt-VBR 服务等级；应该支持 ATM 流量管理规范 4.1 补遗所定义的带有 MDCR 参数的 ATM UBR 服务等级。

SR 应该支持 I.610 所规定的 ATM OAM VC 管理。

SR 必须在所有 ATM 端口上支持 ITU-T I.610 所规定的 ATM F4 和 F5 OAM。

SR 必须支持 PVC，建议支持 SVC。

输出队列必须支持对每条虚电路分段和业务整形功能。

3.5 其它接口

建议支持信道化 DS3/E3、STM-1、STM-4。

信道化的 PoS 接口可以灵活而高密度地提供多种低速接口，包括 E1、E3 等。

建议支持速率为 155Mbit/s、622Mbit/s、2.5Gbit/s 的 RPR 接口。

4 用户管理

SR 必须支持用户的认证、授权、IP 地址分配及计费功能、支持策略控制和动态授权，支持用户唯一性标识功能。

4.1 用户认证方式

设备必须支持 RADIUS 认证、本地认证、不认证等多种认证方式。

设备必须支持 PPPoE、PPPoA 等 PPP 拨号认证。支持 PAP、CHAP 验证方式，PAP、CHAP 验证顺序可灵活配置。

设备必须支持 802.1X 认证，支持 EAP-MD5 认证和 EAP-SIM 认证。

设备必须支持 IPOE 接入认证。在 IPoE 的接入环境下，SR 必须能够同时支持 DHCP+WEB 的接入认证方式和基于 DHCP option 扩展的接入认证方式。认证流程必须符合中国电信的“我的 E 家”业务采用 PPPOE 和 IPOE 用户管理的解决方案。

设备支持 DHCP+WEB 认证方式时，支持强推 Portal 门户。强制用户在拨号认证通过后第一次打开浏览器的时候前往指定页面，门户网站内容可以由运营商自行制定。

设备支持基于 DHCP option 扩展的接入认证方式时，SR 必须能够照中国电信的要求将包含用户终端信息和物理线路信息的 DHCP Option 映射成 Radius 属性并发送至 Radius Server 实现接入认证，并根据认证鉴权结果，控制用户接入。可以通过 Radius 服务器向用户下发接入属性（带宽、业务优先级等）。

设备必须支持 IPOE 接入认证方式下对 session 管理功能，包括 IPoE 用户的上线速率、IPoE 用户下线管理机制、IPoE 用户异常掉线机制处理。

支持 DHCP Relay 及 DHCP Proxy 功能。

设备可以同时支持 PPP、802.1X、IPOE 认证，每个端口可以指定某种或某几种认证方式。

设备必须支持普通用户的认证，支持加域名后缀的用户认证方式，满足用户对多 ISP 的选择，对本地用户能够支持按 VLAN-ID 或者 PVC-ID 认证的方式。

4.2 IPOE 认证方式

设备必须支持 IPOE 接入认证。在 IPoE 的接入环境下，SR 必须能够同时支持基于 DHCP option 扩展（Circuit-id）的接入认证方式和 DHCP+WEB 的接入认证方式。

基于 DHCP option 扩展的接入认证流程要求如图 4-1：

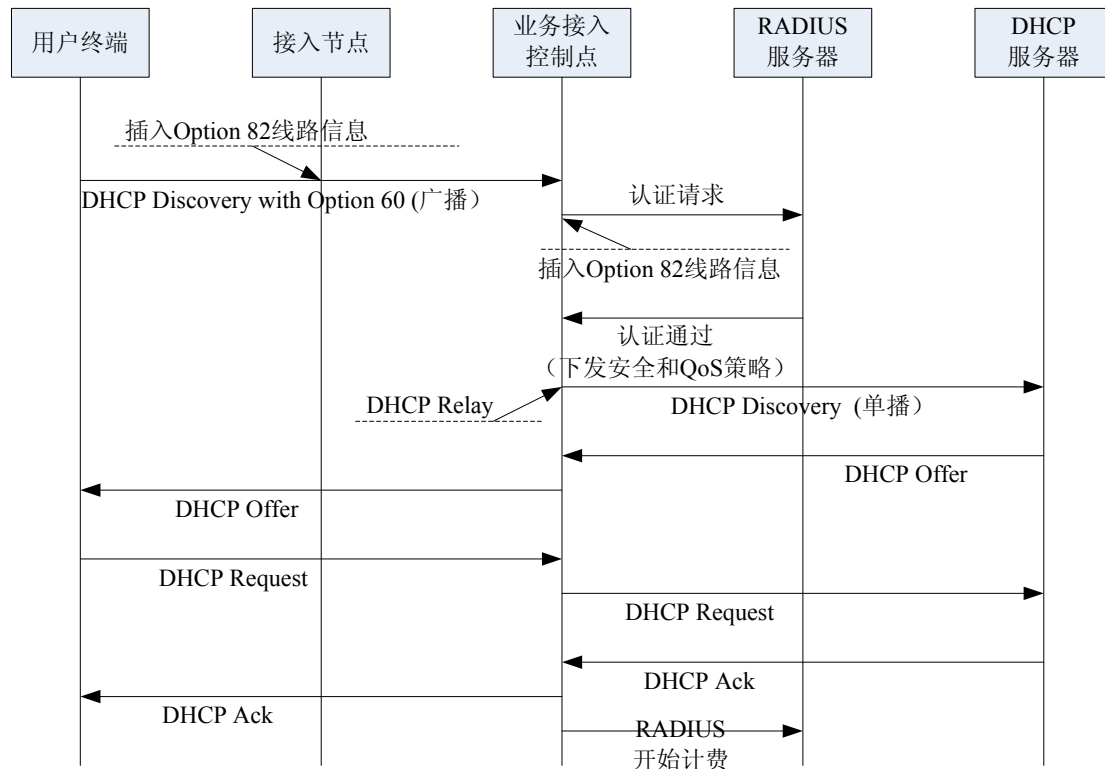


图 4-1 基于 DHCP option 扩展的接入认证流程

基于 DHCP option 扩展的接入认证的具体过程如下：

- 用户终端发出携带有 DHCP Option 60 字段的 DHCP 发现消息；
- 接入节点（DSLAM 或接入交换机）在 DHCP 发现消息里插入 DHCP Option 82（包含物理线路号信息），然后再把修改过的 DHCP 发现消息转发到后面的业务接入控制点（BRAS/SR）；

c) 业务接入控制点检测到这是一个新用户,为该用户创建 IP 会话上下文,此时 IP 地址还未获得配置。业务控制点为该 IP 会话创建一个 RADIUS 接入请求消息,并向 RADIUS 服务器发送 RADIUS 请求消息。RADIUS 接入请求消息必须包含 Username、Nas-Port-id、Nas-Port-Address 等属性;

d) 如果通过 RADIUS 服务器的认证, RADIUS 服务器将向控制点回复接受接入消息,同时传送与该用户的 IP 会话有关的业务策略。控制点接收到接受接入消息,该 IP 会话获得授权,执行该 IP 会话的业务策略,包括 QoS 参数配置和安全策略;

e) 接入控制点向 DHCP 服务器中继转发 DHCP 发现消息;

f) DHCP 服务器接收到 DHCP 发现消息后,回应 DHCP 提供消息;

g) 业务接入控制点接收到 DHCP 提供消息,中继转发到用户终端。业务控制点把获得的 IP 地址与已建立的 IP 会话相关联,完成该 IP 会话的全部配置。后续的针对该用户的所有动态策略都将针对此 IP 会话进行操作。在 IP 会话过程中,业务控制点不断进行 IP 会话的心跳检测,如果几次未得到用户终端的响应,就断开 IP 会话,释放资源,终止计费;

h) 用户终端接收到 DHCP 提供消息,响应以 DHCP 请求消息;

i) DHCP 服务器收到 DHCP 请求消息后,响应以 DHCP 确认消息。用户终端收到 DHCP 确认消息,完成 DHCP 配置过程;

j) 业务接入控制点对该 IP 会话进行统计,并把统计参数发送给 RADIUS 服务器用于后台的统计计费。

设备必须支持在接收到终端发出的 DHCP Discovery 报文中插入 Option 82 线路信息。建议用户的 SVLAN 信息或 DSLAM 上用户端口信息作为设备插入的 Option 82 线路信息。Option 82 用于标识用户位置信息,用于认证时对应于 RADIUS 属性 Nas-Port-id (attribute 87)。

设备必须支持根据 Option 60 做为业务分类标识。设备必须可以使用 Option 82 作为线路信息进行认证。

设备必须能够获取 DHCP Discovery 报文中的 MAC 地址(发送 DHCP 请求的终端 MAC 地址)作为用户名,并使用 DHCP Discovery 报文中的 Option 60 字段作为域名地址(@domain),构建 IPOE 接入认证的 Username: MAC@option 60。

建议设备支持的认证方式为:

Username: MAC@option 60;

Password: 可修改的任意字符。

建议设备支持 Option 43 和 Option 120。

当设备内置 DHCP Server 时,建议设备能够根据不同的 Option 60 值分配不同网段的 IP 地址。

当设备外置 DHCP Server，且不同业务 DHCP 地址管理平台分离时，建议设备能够分析识别 DHCP Discovery 报文中的 Option 60 字段，并把具有不同的 Option 60 值的 DHCP Discovery 报文送到相对应的 DHCP 平台的能力。

必须支持 DHCP Snooping 功能，实现 IP 地址、MAC 地址和 VLAN 逻辑端口的动态绑定，避免出现地址私配和地址盗用。

必须支持针对源 MAC 地址的 DHCP DISCOVERY 报文的 DDOS 攻击，必须支持接口级的 DHCP discovery 请求报文的限速功能，建议支持用户级的 DHCP DISCOVERY 的报文限速功能。

必须支持 IPoE 用户正常下线管理机制及 IPoE 用户异常掉线处理机制。

4.3 授权

设备必须支持带宽控制。

设备必须支持访问权限控制，包括认证前与认证后。

设备必须支持 QoS 优先级分类。

设备必须支持动态授权。

设备必须支持主备 DNS。

4.4 计费

设备必须支持按使用时长、流量等计费方式，建议支持按业务等级、业务类型等计费方式及实时计费功能。生成的计费信息包中应包括用户的帐号、分配的 IP 地址、Session ID、登录时间、离线时间、上网时长、设备号、端口号、PVC 或 VLAN Id (SVLAN Id)、MAC 地址、上/下载字节、上/下载包数量、不同 QoS 等级的流量信息和丢包信息等关键信息。为配合计费系统按流量计费的功能，在标准 RADIUS 断线包标准属性中，SR 必须能提供用户准确的进和出流量。

设备必须支持限制向 RADIUS 服务器发送请求的速率，设备必须丢弃超出所配置最大请求速率的 RADIUS 请求。必须支持 RADIUS 记帐请求的复制功能，可以将同一个记帐请求同时送往两个不同的 RADIUS 记帐服务器。必须支持计费报文的重传机制。

设备必须支持当与远端的 Radius 失去联系时可实现本地计费，保证话单数据不会丢失。

设备可以设置用户最大连接时长，该值可以由配置时设定，也可以从计费系统的 RADIUS 返回包中取得。当用户的连接时间达到允许的最大时长时，SR 能主动撤除与用户的链接，并能正确的送出计费停止包。

设备的计费精度必须小于 1 秒。

4.5 地址管理与分配

SR 必须支持多种 IP 地址管理和分配方式，从地址类型来看，必须支持固定 IP（ADSL 专线）、静态 IP（用户每次拨号登录网络时分配到相同的 IP 地址）和动态 IP。

SR 必须支持 DHCP 方式、PPP 方式和静态配置方式分配和管理 IP 地址。

（1）分配静态地址。

设备必须在地址池耗尽的情况下拒绝用户的分配地址请求。

设备必须支持缺省地址池。

设备必须支持通过本地配置为指定域名的用户分配特定的地址池地址。

设备必须支持根据 RADIUS 响应属性为用户分配特定的地址池地址。

设备必须保证用户不能私配地址。

（2）分配动态地址

设备必须支持用户从本地地址池分配地址。

设备必须支持用户从 RADIUS server 分配地址。

设备必须支持用户从外部 DHCP Server 统一分配地址。

设备必须支持在本地配置用于 PPP 和 DHCP 用户的地址池。设备必须支持在地址池中使用私有（保留）地址。IP 地址池必须可以包含多个 CIDR 地址块。

SR 必须支持 RADIUS Client 功能，支持由 RADIUS Server 分配 IP 地址，设备必须支持将 RADIUS 应答中的 Framed-IP-Address 作为分配给用户的地址。设备必须支持 SR 本身来分配 IP 地址。必须能支持 20 个以上的 IP Pool。支持根据 RADIUS 应答中的属性为用户使用特定的地址池。设备必须支持缺省地址池，如果在 RADIUS 回应中指定了一个未命名的地址池，设备必须从缺省地址池中为用户分配地址。

SR 必须内置 DHCP 服务器，由 SR 直接分配地址；必须支持 DHCP Relay 和 DHCP Proxy 功能，通过远程 DHCP 服务器分配地址。必须支持 IP 地址、MAC 地址和 VLAN 逻辑端口的动态绑定，避免地址冲突和盗用。要求支持 DHCP+WEB 方式和基于 DHCP option 扩展的接入认证方式提供用户认证、授权；要求支持 DHCP 请求转换为 RADIUS 请求功能，实现 DHCP 地址管理和 PPP 拨号地址管理的集中管理。

必须支持多个地址池，对于不同的用户类型，SR 可以根据 RADIUS 的要求分发不同地址池的 IP 地址，以达到控制用户上网的访问范围。SR 的每个接入单元应该能够根据用户名、接入端口等信息自动为用户分组，每组具有不同的 IP 地址池，在每组内地址池为用户选择 IP 地址。必须支持通过 RADIUS 返回 IP Pool Name 而实现对用户选择 IP Pool 分配 IP 地址的方式。

通过多域选择，可为不同的 ISP 分配不同的 IP Pool。设备必须支持为任意可路由端口分配 IPv4 地址（固定地址）。设备必须支持为单个可路由端口分配多个 IPv4 地址。设备必须支持在本地配置为指定的域名用户使用特定的地址池。

设备必须遵循 RFC 828，使用地址解析协议（ARP）构造 ARP 表。设备必须支持反欺骗机制（如 secure ARP 或 Proxy ARP）。设备必须允许网络管理员在 ARP 表中手工添加表目，将一个或多个 IP 地址与 MAC 地址关联。

设备必须过滤流量，保证用户不能使用私配地址。

设备必须支持每 VR 至少 20 个或整机 2000 个地址池。

A、B 类 SR 支持的地址数量分别大于 64K、32K。

4.6 RADIUS

SR 必须支持与 RADIUS 服务器一起共同完成用户的认证、授权、IP 地址分配及计费功能。

设备必须支持主备 RADIUS 及负荷分担功能。必须支持认证与计费 RADIUS 分开。支持主、备 RADIUS 的自动切换，当主 RADIUS 出现故障时，系统须能自动产生告警，并将认证计费信息请求发送到备用 RADIUS，由备用 RADIUS 服务器负责完成认证和产生计费信息。当主用 RADIUS 恢复后，不须人工干预，BRAS 能重新指回主用 RADIUS。整个切换过程无服务中断和计费信息丢失。

SR 发出的包必须符合标准 RADIUS 协议，必须支持认证、授权、计费、VPN 等 RADIUS 属性，支持 RADIUS 扩展属性。

5 策略控制

设备必须支持通过策略控制平台对基于用户名、PVC、VLAN、MAC 地址、IP 地址、逻辑端口、物理端口、MPLS 标签等属性绑定的接入控制策略。控制策略应能实现业务流分类、标记、速率限制、带宽保证、流量整形、队列调度、拥塞避免等基本的 QoS 机制。

必须实现用户业务 QoS 的动态调整策略。

设备建议支持通过策略控制平台实现层次化 QoS。

设备必须支持通过策略控制平台实现标准的 5 元组 ACL；建议设备支持通过策略控制平台实现扩展 ACL（EACL），分类规则含端口、VLAN、MAC 等；建议设备支持基于帐号和基于用户的扩展 ACL（UACL），对用户实施访问权限控制。

设备必须支持通过策略控制平台实现用户带宽 CAR 控制，并支持将 CAR 控制信息送往 RADIUS，以便实现不同带宽不同费率。

设备必须支持通过访问外部服务器得到基本用户信息（用户名、用户类型、

付费方式等)、用户订购业务、用户 QoS profiles、用户线路信息。

设备必须支持 Push 模式策略控制。

设备建议支持 Pull 模式的策略控制。

设备必须支持用户/业务策略通过策略控制平台强制激活方式、用户通过 Portal 界面订购业务的手工激活方式、自定义触发条件满足时(如:时长、流量、非法/非正常业务流)的自动激活方式。

设备必须允许指定用户使用的访问控制策略,对用户实施访问权限控制。

设备必须支持按 Domain 实施控制策略,包括:认证计费策略,带宽控制策略,访问权限,QoS 策略,路由策略等。

设备必须支持同一帐号下的不同业务权限的控制及部分业务权限的透传至 DSLAM 的功能。

设备必须支持不同的用户帐号实现不同的 ACL 和路由策略。

设备必须支持不同的业务类型实现不同的路由策略。

设备必须支持动态授权,支持以 COPS、DIAMETER 或 RADIUS 为主的业务控制协议。

设备提供 COPS 接口协议时必须支持 COPS 规定的多种消息类型,按照功能可以划分为两类:COPS 链路状态建立/维护消息与业务处理消息。

a) COPS 链路状态建立/维护消息包括:

- Client-Open (OPN) 消息
- Client-Accept (CAT) 消息
- Client-Close (CC) 消息
- Keep-Alive (KA) 消息

b) 业务处理消息包括:

- 请求 (REQ) 消息
- 删除请求状态 (DRQ) 消息
- 策略下发 (DEC Install) 消息
- 策略删除 (DEC Remove) 消息
- 状态一致性请求 (SSQ) 消息
- 状态一致性完成 (SSC) 消息
- 状态上报 (RPT) 消息

提供 COPS 接口的策略控制过程采用 PUSH 方式如图 5-1 所示,整个描述过程如下:

a) BRAS/SR 和策略控制平台之间建立 TCP 链路;

b) BRAS/SR 和策略控制平台将发生一些消息的交互以验证 TCP 链路的合法性;

c) 验证通过后，当接收到业务管理平台发送的 QoS 请求，或者 BRAS/SR 发送的用户上线请求，策略控制平台根据网络运营商定义的策略等信息进行决策，形成策略数据放在 DECInstall/Remove 消息中下发给 BRAS/SR；

d) BRAS/SR 收到 DEC Install/Remove 消息后，在本地进行策略信息的执行，完毕后向策略控制平台发送 RPT 消息报告执行的状态（成功/失败）；

e) 当用户不再使用某个业务时，由 BRAS/SR 向策略控制平台发出 DRQ 消息，要求删除某个用户的状态信息；BRAS/SR 将删除本地的状态信息，策略控制平台将删除本地的状态信息并回收分配给用户的资源。

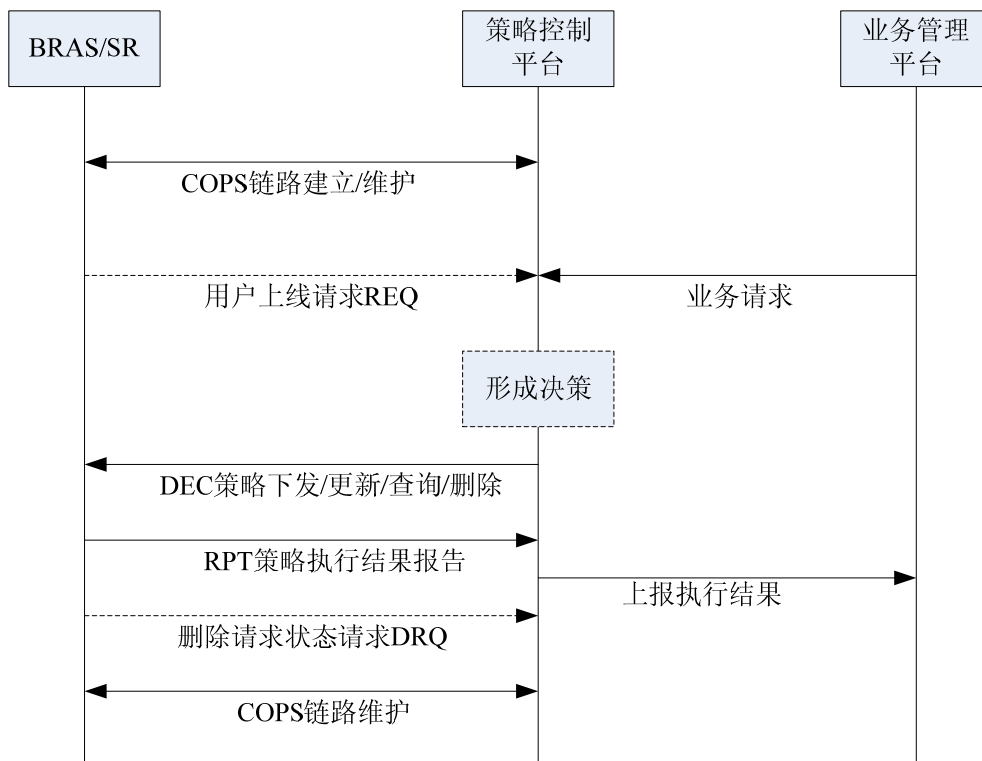


图5-1 COPS接口上的策略控制过程

设备提供 DIAMETER 接口协议的功能要求待定。

设备应能在配套的增值业务系统的管理下，动态修改用户的各种策略，以提供动态 QoS 等增值业务功能，要求用户和 SR、PORTAL 三者之间实现一次连接、一次用户认证、多次业务选择功能。

设备必须支持基于 RFC3576 的 DADIUS 扩展动态授权：

必须支持 RADIUS 扩展中的用户下线（DM）和动态授权（COA）消息，符合 RFC3576 规定的消息交互框架；

必须支持 SR 和 RADIUS server 之间的密钥检查，对密钥检查不通过的请求直接丢弃；

必须支持以 Username（1）为关键字的 DM 和 COA 消息；

必须支持以 Acct-Session-Id (44) 为关键字的 DM 和 COA 消息；

建议支持对 NAS-Port (5)、Framed-IP-Address (8)、Calling-Station-Id (31)、NAS-Port-Type (61)、NAS-Port-Id (87) 的校验检查；

动态授权必须支持的标准属性：Filter-Id (11)、Session-Timeout (27)；

动态授权建议支持的标准属性：Idle-Timeout (28)；

动态授权必须支持的厂商属性：用户的上下行带宽、用户的 QoS 配置变化；

动态授权建议支持的厂商属性：用户 TCP 会话数限制、流量预付费时的剩余流量。

建议设备支持通过策略控制平台动态调整用户使用的带宽或业务优先级，限制用访问特定的资源。当用户业务使用完毕后，释放带宽资源并删除相应的配置信息。

建议设备支持可用资源（如可用带宽、CPU 利用率、队列缓存大小）和用户资源使用状况实时上报到策略服务器，策略服务器根据设备的资源利用情况及用户使用资源情况决定对用户的接纳控制和策略控制。

6 路由功能

本章中的路由功能规定为基于 IPv4 的路由功能，但应当支持通过软件可升级 IPv6 协议。

6.1 常规要求

6.1.1 协议和地址

SR 必须支持下列链路层协议：ARP/RARP、PPP、ATM、PoS。

SR 必须支持下列互联网层协议：IP、ICMP、IGMP。

SR 必须支持下列应用层协议：FTP、Telnet、SNMP 等。

IP 地址必须支持下列规定：

- 必须支持 A、B、C、D、E 类地址的配置及使用规定。
- 必须支持与地址分配和汇总策略相关的无类别域内路由 CIDR。
- 必须支持私网地址使用的规定。

SR 必须支持在主端口上配置 primary/secondary IP 地址。

SR 必须支持使用 unnumbered IP 端口。

SR 应当支持静态及动态 NAT 功能(可选，放置在有 NAT 业务需求的城域网的 SR 需支持)。

SR 必须支持实现 DHCP Server 的功能。

6.1.2 路由

SR 必须支持静态路由配置和动态路由协议。

SR 必须支持基于 IPv4 的域内动态路由协议(RIPv1/v2、OSPFv2、ISIS)和域间路由协议(BGP4)。

SR 必须支持为静态路由配置如下参数：ToS、子网掩码(或前缀长度)、路径权值；在配置某静态路由时，必须允许静态路由定义成任何路由协议使用的路径权值；必须允许用户规定一组静态路由是否通过某路由协议扩散；SR 必须支持基于用户定义的策略，提供静态配置的策略路由能力。

SR 必须支持多条缺省路由和静态路由的 ECMP；必须支持允许配置路由是否公告的时间间隔。

SR 必须支持根据逻辑或物理端口过滤进出路由信息；必须支持路由汇总；必须支持路由协议的重分发功能。

SR 应能够实现重设 ToS/DSCP 域、指定下一跳、指定输出端口、指定 IP 到 MPLS 等功能。

SR 必须支持禁止直接域广播。

SR 必须支持 BFD 功能，包括 BFD for 静态路由、BFD for Vlan、BFD for VRRP、BFD for OSPF、BFD for ISIS、BFD for BGP、BFD for LDP。基本功能应符合 draft-ietf-bfd-base-08 规定的各项要求，包括 BFD 检测的承载协议及使用的端口号，BFD 的包类型、包格式，检测模式、发送周期及检测时间、参数修改过程、会话初始化和建立等内容；应支持 draft-ietf-bfd-v4v6-1hop-08 和 draft-ietf-bfd-multihop-06 的相关规定。

必须支持 PoS 对 SDH Section、Line 和 Path 故障信号的检测支持，并根据这些信号触发 IP 接口状态，触发机制和相关时间参数可以配置。

建议设备根据传输误码率判断链路状态的能力。

必须支持 SPF 计算中的快速收敛 ISPF 和 PRC 算法。

必须支持 OSPF/ISIS/BGP/LDP 路由协议的 NSR 功能，当设备在当前激活的主路由引擎或软件突然失效而进行主备切换时，能够保持路由协议的稳定性和数据包持续的转发。

建议设备支持 IP FRR 功能，能够将备份路由表下发到转发表中。

6.2 OSPF 路由协议功能要求

SR 必须支持 RFC2328 OSPFv2 路由协议的全部功能和要求，其中包括：链路状态数据库、自治系统内对区的分割、域内路由功能、自治系统外部路由的处理、路由协议包格式、基本功能实现要求(定时器、IP 组播包接收和发送、可变长子网掩码支持、IP 超网支持、低层协议支持、非广播低层协议支持、操作原语列表、激活其它过程的任务支持)、协议数据结构、区数据结构、邻居路由器状态维护、收发协议包的处理、接口数据结构、邻居数据结构、路由表结构、LSA 包数据结构及处理、虚链路要求、路由表计算等。

SR 必须支持如下 OSPF LSA：

- type1: router-LSA;
- type2: Network-LSA;
- type3: Network Summary-LSA;
- type4: ASBR Summary-LSA;
- type5: AS-External-LSA;
- type6: Group Membership LSA;
- type7: NSSA External LSA;
- type8: External Attributes LSA;
- type9: Opaque LSA (link-local scope) ；
- type10: Opaque LSA (area-local scope) ；
- type11: Opaque LSA (AS scope) 。

SR 在满足作为 stub 路由器的条件下，必须能发布 OSPF Stub Route。

SR 必须能够实现作为 ABR 和 ASBR 的功能。

SR 建议支持规定 OSPF 平滑重启功能。当路由控制平面重新启动时，网络拓扑未发生变化，则必须启动 OSPF 平滑重启过程；若检测到网络发生了变化，则必须能转换到正常到 OSPF 重启过程。路由器必须能够实现平滑重启的发起者功能，也必须能够在作为平滑重启发起者的邻居时，运行在平滑重启助手模式下。无论作为平滑重启的发起者还是作为助手，路由器必须提供 OSPF 平滑重启的后向兼容能力，能够感知在邻居无法作为助手时，进入正常的 OSPF 重启状态。整个平滑重启过程必须符合 RFC3623 的规定。

必须支持 OSPF 在 BGP/MPLS IP VPN 网络环境中，在 PE 和 CE 之间启用 OSPF 协议时的操作要求；必须支持在一个 VPN 的两个 PE 上的 VRF 之间建立 sham Link 的功能；要求支持的 OSPF Instance 数量不少于 VR 数量，OSPF 在 BGP/MPLS IP VPN 中的操作、功能等必须符合 RFC4577 的规定。

在启动了 OSPF 的邻居之间必须支持协议消息的保密认证功能。

必须支持 OSPF 多路径负载分担，其分担误差要求在 10%之内。

必须支持对路由协议优先级/管理距离的调整。

必须支持 OSPF 多进程。

可选支持 OSPF 多拓扑路由功能,符合 RFC4915 的要求。

6.3 ISIS 路由协议功能要求

SR 必须遵守 RFC1195 中的规定，包括：与子网无关的功能，与子网相关的功能，PDU 的结构和编码，路由信息的类型和编码，序列号分组编码及路由算法；对路由信息的 QoS 设置必须符合 RFC2474 中的规定；SR 必须支持 RFC1195 中的 IS-IS 路由信息的简单认证功能和 RFC3567 中的加密认证功能，以保证路由信息的安全。

在点到点链路之间建立 ISIS 链路时，必须通过 3 次握手机制实现，实现方式应符合 RFC3373 中的规定。

必须支持 RFC2763 规定的动态主机名 TLV(类型 137)，以便于运维管理。

必须支持 RFC2966 规定的两层 ISIS 域范围的前缀分发功能；必须支持 Level2 到 Level1 的路由泄漏特性。

必须支持 RFC3277 ISIS 瞬时黑洞避免功能，即在重启时，给建立了邻接关系的路由器快速发出带有 Overload bit 置位的 LSP 消息，在该路由器同步路由数据库完成后，再次发布 LSP 消息时，应清除 Overload 比特位的原置位。

必须支持 ISIS 多路径负载分担及其管理，分担误差在 10%之内。

必须支持 ISIS 协议的快速路由收敛机制，相关参数可配置：

- ✓ 必须支持 ISIS PRC（部分路由计算）和 I-SPF（增量 SPF）。
- ✓ ISIS 可配置的时间参数应包括 hello 间隔时间、LSP 发送间隔时间、SPF 初始时间、SPF 间隔时间。
- ✓ 必须支持 POS 对 SDH Section、Line 和 Path 故障信号的检测，并根据这些信号触发 IP 接口状态，触发机制和相关时间参数可以配置。
- ✓ 必须支持 10GE、GE 接口 keeplive 发送间隔可配置为不大于 1 秒，要求具备物理端口故障快速检测能力（不大于 100ms）。
- ✓ 必须支持设备根据传输误码率判断链路状态的能力。
- ✓ 必须支持物理端口的 damping 功能，打开该功能不影响端口状态变化 TRAP 的发送。

必须支持 RFC3847 中规定 ISIS 的重启信令,即增加相关的定时器 T1/T2/T3,及 Restart TLV(类型 211),在重启(或启动)的路由器及其邻居在重启(启动)过程中的操作(如邻居的获得、多层间操作、数据库同步等),要符合该 RFC 文档的规定。

建议支持在 RFC3784 和 RFC4205 中规定扩展 TLV 及其 sub-TLV,其中 (1) — (3)为 IS-IS 用于 TE 的扩展;(4)则为 ISIS 用于 GMPLS 的扩展:

(1) extended IS Reachability TLV(类型 22)及其 sub-TLV(子类型 3,4,6,8-11,18, 20, 21);

(2) extended IP Reachability TLV(类型 135);

(3) The TE Router ID TLV(类型 134);

(4) shared Risk Link Group(类型 138);

可选支持 ISIS 的多拓扑路由功能,符合 RFC5120 的要求。

可选支持链路状态路由协议 LAN 上的点到点操作,符合 RFC5309 的要求。

6.4 RIPv1/v2 路由协议功能要求

SR 必须支持 RFC2453 RIP Version 2 规定的各项功能要求、各项协议消息封装格式、协议算法。

SR 必须支持 RFC2091,以保证 RIPv2 在与邻接设备通过面向连接的电路连接时的可用性。

SR 必须支持只向客户 CPE 发送 RIP 更新,但不接收由 CPE 传来的更新。

SR 必须支持 RIPv2 的加密认证功能;在启用 RIPv2 版本时,必须支持与 RIPv1 版本的后向兼容。

6.5 BGP-4 路由协议功能要求

SR 必须符合 RFC4271-BGP4 协议中规定的全部功能和要求,包括:

(1) 路由发布和存储规定。

(2) BGP 各类消息包(OPEN、UPDATE、KEEPALIVE、NOTIFICATION 和 ROUTE- REFRESH 消息类型)格式规定,并支持 BGP 各类消息包所包含的内容。

- 对于 OPEN 消息,必须支持 RFC4271 第 4.2 节的规定,同时必须支持 RFC3392 中规定的能力选项格式,建议支持 draft-ietf-idr- restart-13 中的 BGP 平滑重启的能力选项参数规定。

- 对于 UPDATE 消息,必须支持下列 Path Attribute (通道属性)类型:

- Type Code 1: ORIGIN;

- Type Code 2: AS_PATH;
- Type Code 3: NEXT_HOP;
- Type Code 4: MULTI_EXIT_DISC;
- Type Code 5: LOCAL_PREF;
- Type Code 6: ATOMIC_AGGREGATE;
- Type Code 7: AGGREGATION;
- Type Code 8: COMMUNITY;
- Type Code 9: ORIGINATOR_ID;
- Type Code 10: CLUSTER_LIST;
- Type Code 14: MP_REACH_NLRI;
- Type Code 15: MP_UNREACH_NLRI。

其中, TypeCode1~7 必须符合 RFC4271 中第 4.3 节和第 5 章的相关规定; 对 TypeCode8—Community 属性值的范围、操作、聚合和使用, 必须符合 RFC1997 的规定, 属性值应可配置; TypeCode 9、10 在路由反射功能实现时, 避免出现路由信息环路, 其格式和使用, 必须符合 RFC4456 的规定; TypeCode 14、15 则用于 BGP-4 的多协议扩展, 其功能实现在 RFC2858 中规定。

- 对于 KEEPALIVE 消息, 必须支持 RFC4271 第 4.4 节的规定。
- 对于 NOTIFICATION 消息, 必须支持 RFC4271 中第 4.5 节中对错误码和错误子码的规定和第 6 章对各类 NOTIFICATION 消息的处理, 必须支持 RFC4486 的 Cease Notification 的 8 个子编码(subcode)的定义和处理。
- 对于 ROUTE-REFRESH 消息, 消息格式和操作过程必须符合 RFC2918 中的规定。

(3) BGP 版本协商的规定。

(4) BGP 中有限状态机规定。

(5) BGP 内所有定时器相关规定。

SR 除了支持基于 AS 配置 BGP, 还必须支持能够实现基于团体配置 BGP, 相关措施应该符合 RFC1998 的规定。

SR 必须支持 BGP 路由振荡抑制, 符合 RFC2439 的规定。提供限制发布路由的相关定时器; 支持实现稳定发布路由的方法; 所有的定时器参数及动作均应可配置。

SR 必须支持 BGP-4 多协议扩展, 必须支持多协议可达 NLRI 属性(类型码为 14)和多协议不可达 NLRI 属性(类型码为 15), 对这两个属性的编码格式、后续地

址族标识(单播、多播、组播)、发布和处理,以及错误码的处理均要符合 RFC2858 的规定;网络层协议为 IPv6 的 BGP 多协议扩展则必须支持 RFC2545。

SR 必须支持自治系统联盟的功能,支持 RFC3065 中规定的 AS_PATH 新增段类型,即 AS_CONFED_SEQUENCE(value=3)和 AS_CONFED_SET(value=4),相关的操作、管理、兼容性、部署等均要符合 RFC3065 中的规定。

SR 必须支持 RFC2385 定义的,新增 TCP 选项携带 MD5 摘要,通过 TCP 的这项扩展功能增强 BGP 的安全性,MD5 加密涵盖的内容、相关语法、发送/接收操作,以及有关面向无连接复位的处理、性能、TCP 头的长度、MD5 算法、密钥的设置等,必须要符合 RFC2385 中的规定。

SR 必须支持 IBGP 路由反射功能,其路由反射的操作、路由反射器的备份、路由信息环路的避免等过程,均必须符合 RFC4456 的规定。

SR 必须支持在 BGP-4 消息中携带 MPLS 标签的功能,有关标签携带和功能实现方式均必须符合 RFC3107 的规定。

SR 必须支持在 BGP/MPLS IP VPN 环境中,SR 必须支持通过 BGP 分发 VPN 内部的路由,并保证来自各不同 VPN 的路由清晰明了,互相隔离(并保证不同 VPN 地址重叠时路由分发不受影响);必须支持 PE 之间路由反射;必须不能约束 CE 和 PE 之间 VPN 路由操作,即当 CE 和 PE 之间为静态路由、或 RIP、或 OSPF 时,必须支持 BGP 与相应路由协议的重分发,也必须支持 CE 和 PE 之间为 BGP Peer 时的路由学习;必须支持骨干为多 AS 时的 VPN 路由的分发;上述所有的操作必须支持 RFC4364 的规定。

SR 必须支持 IBGP/EBGP 多路径负载分担,分担误差在 10%之内。

SR 必须支持 IBGP/EBGP 的路由收敛优先级区分功能,能够保证高优先级业务路由在故障时优先收敛。

必须支持 BGP 的策略路由功能,能基于源地址、源地址+目的地址、源地址+目的地址+TCP/UDP 端口、IPP 值进行路由重定向;必须支持策略路由至少 8 条负载分担,分担误差在 10%以内;并当策略路由失效时,可配置路由器是否通过其它有效路由到达目的。

必须支持 BGP 的日常配置和维护操作功能;必须支持灵活丰富的路由控制和过滤功能。

建议 SR 支持 BGP 的平滑重启功能,其能力消息格式、发起者和接收者的操作过程、状态转换等应符合 RFC 4724 的规定。

7 QoS

7.1 QoS 机制

设备必须实现 DiffServ QoS 机制, 包括分类、标记、速率限制、带宽保证、流量整形、策略和测量等, 符合 RFC2475 的规定; 设备必须支持 RFC2597 定义的 AF 转发功能; 必须支持 RFC3246 定义 EF 转发功能, 并保证对此类业务流对转发时延低于 30ms; 必须支持 RFC2474 定义的 BF 转发功能; 必须支持 RFC3662 中规定的为属于 BF 的某服务进一步降低服务的功能; 必须支持 RFC2697 和 RFC2698 中规定的单速率三色标记 (1R3C) 和双速率三色标记 (2R3C) 的业务合同参数, 以及不同情况下的令牌桶算法规定。

(1) 分类

设备必须支持基于多种方式对数据流进行分类功能, 包括:

- IPv4 及 IPv6 的 DSCP;
- 用户会话接入的物理/逻辑端口;
- 源 IP 地址;
- 目的 IP 地址;
- IP 协议字段;
- 源 TCP/UDP 端口号;
- 目的 TCP/UDP 端口号;
- 802.1p 的 CoS 字段;
- 802.1Q 的 VLAN ID 字段;
- SVLAN 各层堆栈的 VLAN ID 和 CoS 字段;

(2) 标记和映射

基于上述的分类字段, 设备必须支持根据配置的策略控制, 提供对 IP 包的 DSCP 字段、802.1p 以太帧中的 CoS 字段和 MPLS 的 EXP 字段进行标记的功能, 并能够实现这三层之间各 CoS 字段的相互映射。设备必须支持在 MPLS 网络里, 可以将不同等级的数据流量加上 MPLS-EXP 的 QoS 定义, 建议可以对第二层的 MPLS VPN 线路做 MPLS-EXP 的 QoS 定义。必须支持 SHORT PIPE/PIPE/UNIFORM/模式的 MPLS QoS。

通过 ATM 接口接入的用户业务, 则设备必须支持特定 PVC 和 DSCP 的映射。

(3) 速率限制和带宽保证

设备必须具备在任意端口、会话和应用流上加载控制策略的能力, 支持对物理端口、子端口的流量进行限速, 支持对基于 IP 地址的流量限速。要求 10/100

Mbit/s 接口颗粒度最少 64kbit/s; 1000Mbit/s 接口速率限制颗粒度最小为 1Mbit/s, 误差小于 5%。

设备必须支持基于物理端口/子端口、PVC 和 IP 地址的可配置最小吞吐量以保证不会出现完全无法得到带宽的情况。

(4) 流量整形

设备必须支持基于流分类加载流量整形的控制功能, 并根据配置实现流量整形功能; 设备必须实现对每个队列的整形能力; 设备必须实现对 L2TP 隧道的流量整形功能。设备中的分级调度器必须能够基于网络拓扑模型对下行流量进行整形以保证下行的二层端口无拥塞。

(5) 统计功能

设备具备对实施分类后的数据包进行统计的手段。

(6) 动态调整 QoS 策略

设备应该能够提供对外部策略服务器的接口, 利用标准协议(如 COPS、RADIUS 或 DIAMETER 协议), 支持向外部策略服务平台通知状态(如申请/释放 QoS 资源的结果、用户掉线异常通知等), 并接受外部策略控制平台的控制, 动态改变在 ATM 层、IP 层的 QoS 策略及整形参数, 而无需重建会话。

(7) 队列调度和拥塞控制

设备必须支持多种队列调度技术, 如 PQ/CQ/LLQ/WRR/CBWFQ 等队列调度技术, 并为每个队列提供不同的控制策略; 设备必须支持速率限制、RED、WRED、尾丢弃(TAILDROP)等拥塞控制技术。

(8) 层次化 QoS 要求

SR 必须支持层次化 QoS 功能, 实现分级调度, 分级调度必须能有效利用资源, 任何流量必须可以使用分配给其它流量等级的未使用带宽。

设备应符合 TR-059 描述的层次化 QoS 处理的主要过程:

- BRAS 感知流量类型, 并且根据流分类结果把流量分别打入不同的 Session 队列, 同时根据配置或策略对不同的流分别进行流量监管和限制, 并支持如 PQ/CQ/LLQ/WRR/CBWFQ 等多种调度算法;
- 物理端口调度器根据端口速率从下属调度器 (VP 调度器) “pull”报文, 同时根据配置或策略对不同 VP 分别进行流量监管和限制;
- 每个 VP 调度器将得到调度, 同时每个 VP 调度器根据 VP 速率从下属调度器 (VC 组调度器) “pull”报文, 根据配置或策略对不同 VC 分别进行流量监管和限制;

按照这个方法, VP 调度器、VC 调度器、Session 调度器将依次得到调度,

一旦 Session 调度器得到调度，它将从对应 Session 队列中“pull”一个报文，并让报文从 BRAS/路由器的物理端口发送出去。

(9) ATM 流量管理

设备必须支持 VBR 服务的超额订购。

设备必须支持 PVC 和 IP/MPLS QoS 队列的映射。

设备必须支持每 VC 的信元整形以符合该 ATM PVC 所对应的流量描述，这些流量描述由其使用的 ATM 服务等级定义，包括 PCR, SCR, MBS 等。

设备必须支持双漏桶信元整形。

设备的性能在流量整形开启时必须不受任何影响。

7.2 QoS 能力

要求队列数量大于等于 8k 个/单板，ACL 大于 8K 个/单板（具备拆分为进出各 4K 能力），数据缓冲内存大于 256MB/STM-64（或者 64MB/STM-16 端口），最大延时小于 100us、最大抖动小于 30us，要求每队列带宽保证误差小于 5%。

与外部的策略服务器直连且无阻塞时，设备必须支持并应用每秒至少 50 条策略的改变；策略规则由策略条件和策略动作构成，设备必须支持对每个用户加载 10 个策略规则或者整机支持至少 10,000 个策略规则的应用。

设备必须能够在每个端口(任意的物理或逻辑端口)应用至少 2 个策略(进和出方向，每个策略包含至少 10 个规则)，而不影响设备的性能。

设备的性能在流量整形开启时必须不受任何影响；设备必须支持 RED、基于 IP 优先级、DSCP 的 WRED 或尾丢弃，必须支持能根据 IP 优先级、DSCP 值执行相应的拥塞处理能力。

对于层次化 QoS 要求 SR 必须支持四层 QoS 控制，各层次调度器的数目视系统规格而定，并实现基于类(或队列)的每级限速，即实现对每类(或队列)的最高速率限制，能够实现 QoS 的二级限速和三级限速功能；对每层均实现拥塞控制，支持拥塞处理和拥塞避免等 QoS 功能；对每个层次都能够进行流量监管或整形。

7.3 DPI 功能

建议支持 DPI（Deep Packet Inspection，深度包检测）功能，可在网络层识别应用层信息，以便细化安全策略。

支持对 HTTP、FTP、DNS、POP3、SMTP、ICMP 等多种基本协议的识别。

支持 P2P（Skype、BitTorrent、eDonkey、MSN 等）应用层协议的识别。

支持对识别出的应用进行控制，并能对网络流量进行统计。

开启 DPI 功能时对设备性能的影响不大。

8 MPLS 功能

SR 的体系结构必须支持 MPLS，必须支持 MPLS 协议的基本功能，支持 MPLS LER 和 LSR 功能，支持 MPLS 显式路由。SR 必须支持标准的 LDP 和 RSVP-TE 信令协议，不应使用厂商私有的协议。

SR 必须能配置备份 LSP；支持多路径 LSP 的负荷分担；支持标签堆栈；支持基于约束的路径计算，能够基于源/目的 IP 地址、协议、源/目的端口号、ToS/优先级、TCP 标志、路由表的下一跳等参数将数据包路由至输出 LSP。必须支持将任意三个 IP Precedence 值映射到一个 EXP 中，并支持相应的层次化 QoS 部署。

SR 必须支持 MPLS 流量工程。

SR 必须支持 MPLS 虚拟专用网。

SR 必须支持 MPLS IP VPN 业务，必须支持作为 MPLS IP VPN 的 PE 路由器。

应当支持标准公开的 MPLS VLL 二层隧道协议(Martini 方案)，及 GRE 三层隧道协议，不应使用厂商私有的 VPN 标准。

SR 应支持虚拟专用 LAN 承载服务，即支持 VPLS 功能。

SR 在任意类型的线卡和端口上都必须支持 MPLS 三层 VPN 功能，应该支持 MPLS 二层 VPN 功能、VPLS、GRE 隧道 VPN 功能，使由该 SR 所构成的网络能同时提供多种 VPN 服务，以最大限度地满足不同企业用户的需求。

SR 在支持 MPLS 二层 VPN 时，应同时支持 Martini 标准和 Lasserer-vKompella 标准。SR 在支持 RFC4364 MPLS IP VPN 时，必须支持自治域内和跨自治域 AS 的功能，SR 在支持 MPLS 三层 VPN 时，必须支持 VPN 内部的 QoS 功能。

SR 必须能够根据所配置的策略，把输入的业务量自动分配到不同的 TE LSP 中；建议采用硬件来完成该功能，在完成该功能时，仍然能以线速转发 MPLS 数据包。

建议 SR 在支持 IP FRR 的基础上，支持 LDP 的 FRR 功能。

8.1 MPLS 基本功能

MPLS 帧的封装格式必须符合 RFC3032 的规定，能够确定网络层协议类型、能够产生打标签的 ICMP 包、能够正确处理超大 IP 报文、能够在 PPP 链路上传递打标签的 IP 包；标签值的使用必须符合 RFC3032 和 RFC4182 的规定；MPLS 帧格式的 TTL 字段的处理必须符合 RFC3032 和 RFC3443 的规定；SR 的 MPLS 标签堆栈应该支持至少 3 层标签；必须支持符合 RFC3035 的使用 LDP 或 ATM VC

交换的 MPLS。

SR 必须支持 LDP 协议，LDP 协议的实现必须符合 RFC3036 的规定：

- 能够作为 LDP Peer 实现 LDP 消息(发现、会话、通告和通知消息)的交换；
- 能够实现 LDP 协议的各项操作，包括：FEC 的确定；标签空间、LDP 标识符；LDP 发现；LDP 会话的维护和建立；非直连 LSR 之间 LDP 会话的实现；和 LDP 传送的实现；标签的分发和管理；LDP 环回检测；LDP 消息的真实性和完整性验证；显式路由 LSP 的标签分发等；
- 协议规范：包括 LDP PDU 格式；LDP 过程；TLV 编码；LDP 消息的构成等。

SR 建议支持 RFC3478 规定的 LDP 的平滑重启机制。

必须支持 BFD for LDP，BFD for RSVP。

必须支持 LDP 和 RSVP 协议的无中断路由功能。

SR 必须具备 LSP 环回检测和防止功能，必须支持 RFC3063 规定的 MPLS 环回检测机制提供的 Thread 功能；SR 必须支持 RFC4379 规定的 MPLS 数据平面故障检测功能，并应能与 draft-ietf-bfd-mpls-07 中规定的 BFD 在 MPLS LSP 中的应用相结合,实现对 MPLS LSP 的故障检测功能。

标签保持模式必须使用自由(liberal)标签保持模式，参见 RFC3031 的 3.8 节。

SR 必须支持 LDP 过滤。

SR 应支持基于标签对数据包的转发，并可通过手动配置或标签分配协议 (LDP)建立 LSP。

SR 建议支持 RFC3270 定义的 L-LSPs 的各项功能操作；建议支持把 MPLS 封装在 GRE 中，符合 RFC4023 中将 MPLS 封装到 GRE 中的规定。

8.2 MPLS 流量工程

必须支持基本的 MPLS 流量工程(TE)标准，必须支持 RSVP-TE 信令协议。必须支持符合 RFC4124 规定的差分服务感知 TE (DS-TE) 功能，为每类业务级别 (Class-Type,CT) 保证带宽。建议支持符合 RFC4125 规定的最大分配带宽约束模型 (Maximum Allocation Model, MAM)、符合 RFC4127 规定的俄罗斯套娃带宽约束模型 (Russian Dolls Model, RDM) 以及符合 RFC4126 规定的基于带宽预留的最大分配带宽约束模型 (Maximum Allocation with Reservation,MAR)。必须支持 E-LSP，在 E-LSP 中，一条 LSP 承载多个 CoS 类别的数据包，使用 EXP 比特来区别不同的 CoS 数据。

SR 必须支持实现符合 RFC2702 的 MPLS 上 TE 需求；必须符合 RFC3181 规

定的抢占通知的优先级策略要素；必须符合 RFC3272 互联网流量工程的概述和原则；必须符合 RFC3346 使用 MPLS 实现链路工程的适用性描述；必须支持 MPLS 流量工程的差分服务感知要求。

SR 必须支持 RSVP 协议，必须实现 RFC2205 中 RSVPv1 功能的规定，RSVPv1 的消息处理必须符合 RFC2209 的规定。

SR 必须支持 RSVP-TE 功能，该功能实现必须符合 RFC3209 规定的支持 LSP 隧道的 RSVP 扩展、RFC3396 规定的修改 RSVP 的过程。

SR 必须支持 CSPF，约束条件可以是链路可用带宽、时延、链路属性、管理权重等。

必须支持 RFC3630 规定的 OSPFv2 流量工程扩展功能。

必须支持 RFC3784 规定的 IS-IS 流量工程扩展功能。

SR 必须支持 LSP 的 RSVP-TE 的快速重路由(FRR)功能，符合 RFC4090 的规定，当链路或节点发生故障时，从故障链路或节点切换到备份链路的时间小于或等于 50ms；必须支持 RFC4561,以实现 TE LSP 的跨域倒换。SR 必须支持 MPLS-TE FRR 中 Facility 和 Detour 两种方式，支持 1:N 和 1:1 的备份，必须支持手工配置保护通道，建议支持通过自动计算实现。

SR 必须支持根据所配置策略，将输入的业务量自动分配到不同的 TE LSP 中。建议采用硬件来完成该功能，在使用该功能时，SR 必须能以线速转发。

9 VPN

9.1 L2 VPN

9.1.1 L2TP

9.1.1.1 L2TP 基本要求

设备必须支持 L2TPv2 功能，符合 RFC2661，建议支持 L2TPv3,其功能要求、实现等要符合 RFC3931。

设备必须支持 RFC2661，在 UDP 上承载 L2TP 报文。

设备必须支持 RFC2809，通过 RADIUS 实现 L2TP 强制隧道的功能。

设备必须遵循 RFC2867，支持 RADIUS 的隧道计费；必须遵循 RFC2868，支持隧道协议的 RADIUS 属性。

设备必须能够作为 LAC；建议设备可以作为 LNS。

建议设备支持 L2TP 隧道交换功能，允许终结在 L2TP LNS 上的会话和另一个 L2TP LAC 发起的会话之间交换数据包。

设备必须支持使用设备本身的环回地址发起和终结 L2TP 隧道。

设备必须支持 RFC3145 规定的 L2TP 断开连接的原因信息提供。

设备必须支持 RFC3193，即支持结合 IPSec 加密的 L2TP 隧道。

9.1.1.2 LAC 和 LNS

SR 必须支持 RFC2661 中所有有关代理 LCP 和鉴权 AVP 的 LAC 及 LNS 功能。当 SR 作为 LAC 时，必须允许 LNS 强制 LCP 重协商。

设备必须支持静态和动态隧道的建立；静态隧道建立指 L2TP 隧道在正确配置后即建立，动态隧道建立是指 L2TP 隧道在有相应的 PPP 会话要求时才建立。

在作为 LAC 使用时，设备必须能够将来自 PPPoA、PPPoE 和 L2TP 的 PPP 会话汇聚到单个 L2TP 隧道中，有关操作要遵循 RFC2661 中的规定。

SR 必须支持根据 RADIUS 返回的“隧道服务器末端”属性，将 PPP 会话终结到 LNS 或 LNS 组。

当 PPPoE 或者 PPPoA 在用户和设备之间建立后，设备必须能够根据用户 NAI 中的域名来选择(或创建)一个 L2TP 用于承载 PPPoE 或 PPPoA 来的 PPP 流量。

SR 必须将所有的 PPP 用户 ID 和认证信息通过 L2TP 隧道传递给 LNS。

如果 PPP 会话和 L2TP 隧道已经达到最大数量(每端口、每设备等)，设备必须拒绝新的 PPPoE 或 PPPoA 请求。

如果 L2TP 隧道中已经没有了 PPP 会话，设备必须能够动态终结该隧道。

设备必须支持在物理或逻辑断开上的多个 L2TP 隧道；必须支持静态配置及通过 RADIUS 返回多个隧道参数。

设备必须支持隧道组功能，在一对 LAC 和 LNS 之间可以创建多个 L2TP 隧道并被指派到一个隧道组中，设备必须支持将一个隧道配置为承载多个 FQDN PPP 会话。

设备必须支持按照严格优先级使用隧道承载 PPP 会话，当隧道组或者 LNS 组中当第一条隧道充满时(或达到配置的负载阈值时)，才开始使用该组中的第二条隧道。

设备必须支持在隧道组或者 LNS 组内均衡分配 PPP 会话。

设备必须支持基于权重在多个隧道之间对 PPP 会话进行负载平衡(例如 75%

的会话请求使用隧道 1，另外 25%使用隧道 2)；如果隧道组中一条隧道失效，设备必须继续使用剩余的隧道对 PPP 会话进行负载均衡；如果 LNS 组中的一个 LNS 不可用，PPP 会话必须在剩余的 LNS 之间负载均衡。

设备必须支持动态增加或删除隧道组中的隧道而不影响其它的隧道及其中的 PPP 会话；设备必须支持隧道组或者 LNS 组之间的故障切换。

9.1.2 基于 IP/MPLS 二层的 VPN

(1) 设备必须支持 PWE3，RFC3985 规定的 PWE3 体系架构的规定，满足 RFC3916 规定的 PWE3 需求。

(2) 设备必须支持以下业务：

- ATM over MPLS
- Bridged Ethernet over MPLS
- Frame Relay over MPLS
- Ethernet/VLAN over MPLS
- PPP over MPLS
- DDN over MPLS
- SDH over MPLS

设备建议实现不同介质的互通功能。要求满足以下几种介质的互通：

- Ethernet /VLAN 与 Frame Relay 互通
- Frame Relay 与 ATM 互通
- Ethernet/VLAN 与 ATM 互通

(3) 设备必须支持 Martini 方案，遵循下列 RFC 标准的规定：

RFC 4906 - Transport of Layer 2 Frames Over MPLS, MPLS 上二层帧的传送。

RFC 4905 - Encapsulation Methods for Transport of Layer 2 Frames Over MPLS, MPLS 网络上二层帧传送的封装方法。

必须支持基于 MPLS LSP EXP 的 QoS，建议支持基于 VCID 的 QoS 功能。

(4) 设备可以支持 Kompella 方案，遵循 RFC 草案标准的规定：draft-kompella-ppvpn-l2vpn-04，隧道上的二层 VPN。

(5) 设备必须支持多点方式的 L2 MPLS VPN 业务，即虚拟专用 LAN 业务 VPLS，若支持 Martini 方式，则必须符合 RFC 4762，使用 LDP 信令的 VPLS；若支持 Kompella 方式，则必须符合 RFC 4761，使用 BGP 自动发现和信令的 VPLS。

设备必须支持以下三种方式接入 VPLS：基于物理端口方式；基于 IEEE 802.1Q 方式；基于 QinQ 方式。

设备必须支持两种外层隧道方式：LDP 和 RSVP-TE。

当CE通过多条链路连接PE站点时，建议PE采用STP或者水平分割机制来避免环路问题。

设备作为VPLS PE在处理VLAN标识的时候，必须遵循RFC4448中的在MPLS网络上传送以太网帧的封装规定。当设备作为入口PE时，可以将标识（802.1q或者QinQ）传递到出口PE，或者重写外层标识后传递到出口PE，操作行为必须可配置。当设备作为出口PE时，可以对传递过来的标识（802.1q或者QinQ）的外层标签进行重写，保留内层标签不变。

必须支持基本的OAM功能，包括LSP ping；LSP trace；MAC ping和MAC trace，建议遵循ITU-T Y.1731和IEEE 802.1ag等OAM功能。

设备必须支持VPLS分层架构。

设备应支持跨自治域VPLS业务的实现。在LDP信令跨域互通时，可采用STP冗余方式下的H-VPLS域间互通；在BGP信令跨域互通时，应支持OPTION A方式和OPTION C方式的域间互通；在不同信令域间VPLS（一个域为LDP信令，一个域为BGP信令），应支持背靠背VPLS域间互通的实现。

9.2 L3 VPN

设备必须支持在每个VPN内的ping和traceroute。

9.2.1 MPLS VPN

SR必须支持基于RFC4364定义的MPLS/BGP三层VPN的功能，提供单域、跨域和运营商的运营商的VPN服务，同时，不能约束PE-CE连接上的路由协议，允许PE-CE连接使用以下路由协议：BGP/OSPF/ISIS/RIP/静态路由。

SR必须能作为RFC4364中定义的PE路由器和P路由器使用；必须支持对从CE学习到对路由数目进行限制，在超过时必须告警。

SR必须支持每个VRF对loopback端口及其地址配置。

SR必须支持MPLS VPDN的实现机制，允许VPN用户通过拨号发起某种隧道（如IPSec或L2TP等），终结于SR（即VPN的PE路由器），实现用户远程接入MPLS IP VPN。

必须支持VPN业务流的QoS功能，必须基于不同的8个EXP实现QoS队列的部署，必须支持将用户的任意三个IP Precedence值映射到同一个EXP的功能，必须支持基于EXP和IP Precedence值的层次化QoS处理。用户VPN业务

流的 IP Precedence 值在整个 VPN 内的传递过程不能发生改变，即 SR 必须支持来自 CE 的用户 QoS 透传功能，在 VPN 出口的 PE 的 QoS 处理必须可选择配置为基于 EXP 或用户的 IP Precedence。必须能够同时支持多种 QoS 策略，如端口速率限制和优先级队列技术等的同时配置。

SR 必须支持基于 BGP community 或 AS Path 实现速率限制的功能。

SR 必须支持 BGP 的源站点属性和 AS Override 属性在 VPN 中的应用。

SR 必须支持作为 PE ASBR，支持 VPN 的跨自治域互通的功能，必须支持跨自治域的 OPTION A 和 OPTION B 方式互通，可选支持 OPTION C 方式互通。

SR 必须实现作为 VPN RR 的功能。

建议支持 VPN FRR 功能。

9.2.2 IPSec

SR 必须支持 IPSec 功能，其中认证头(AH)的格式、处理和审核要符合 RFC4302 的规定；安全载荷封装(ESP)的 ESP 格式、处理和审核要符合 RFC4303 的规定；对于 AH 和 ESP 使用的加密和认证的算法，则必须符合 RFC4305 的规定。

SR 实现互联网密钥交换(IKE)必须要符合 RFC4306 的规定，IKE 的加密算法应符合 RFC4307 的规定。

SR 必须支持下列加密算法，并正确应用于 IPSec 中：

- NULL 加密(RFC2410)；
- 3DES-CBC 加密算法(RFC2451)；
- 128 比特密钥的 AES-CBC 加密算法(RFC3602)；
- AES-CTR 加密算法(RFC3686)；
- DES-CBC 加密算法(RFC2405)；

SR 必须支持下列认证算法，并正确应用于 IPSec 中：

- HMAC-SHA1-96 算法(RFC2404)；
- AES-XCBC-MAC-96 算法(RFC3566)；
- HMAC-MD5-96 算法(RFC2403)；

上述算法的实现应通过硬件实现，并不能影响设备的性能。

9.2.3 GRE

建议支持 RFC2784 规定的 GRE 标准，支持符合 RFC1702 的在 IPv4 网络中的 GRE 封装。

10 组播

设备必须实现 RFC1112，必须实现 RFC2236 规定的 IGMPv2，必须实现 RFC3376 规定的 IGMPv3。必须支持 IGMP Proxy。

设备必须支持 RFC2362，PIM-SM 模式；必须支持 PIM-SM 中的集合点(RP)自动发现。设备必须支持 PIM-DM、MSDP(RFC3618 组播源发现协议)等组播协议；设备必须支持 IP 定源组播(SSM)。

设备所支持的三层功能必须同样适用于组播，例如速率限制和过滤等。

设备须具有灵活的组播业务控制机制，如组播组访问控制、组播用户数限制、每个用户加入的组播组数限制等。能通过 Radius 属性提供灵活的组播业务控制，可控制每个用户的组播权限、控制每个用户的组播带宽和 QoS。建议通过策略控制平台提供灵活的组播业务控制。设备必须对静默丢弃所有上行用户组播流量功能可配置。

设备必须支持 IGMP 快速离开机制。

建议设备支持 PIM-SM 隧道；建议设备应支持在 MPLS 环境实现组播业务，并实现 RFC4364 中描述的组播 VPN 业务。

设备支持由 RPT 模式切换到 SPT 过程中不丢包。支持包转发依赖硬件完成，不影响主控板的 CPU 性能。必须支持对组播流量的 QoS 功能而不影响性能。

为支持 IPTV 业务，SR 设备还需具备以下功能：

设备必须支持静态用户组播业务权限控制功能，用户根据配置时是否关联业务权限来识别组播用户。支持 Radius 提供动态返回组播权限功能和控制端口上的动态加入的功能。

设备必须支持组播用户接入封装类型包括：Ethernet，IEEE 802.1q，ATM Bridge 和 IP 包。

设备必须支持 DHCP 方式接入用户的组播认证（利用 Option60 或电路认证）计费功能，包括对该 DHCP 用户的动态组播加入业务权限控制和面向该 DHCP 用户接入电路连接的组播流复制，计费功能同普通 DHCP 上网用户。

设备必须支持对上送到控制层处理的 IGMP、PIM 等组播协议报文流进行限速，防止产生组播攻击。

设备必须支持组播业务防盗用，在组播用户进行 IGMP 接入请求操作时，对用户的电路，MAC 地址，源 IP 地址，等进行一致性检查，只有检查通过才允许加入组播组。

设备必须提供动态组播 QoS 功能，在用户加入组播组后，自动按配置对该

用户的单播流进行限速。或通过动态修改用户带宽或业务流优先级方式保证组播流优先转发。

设备应能提供组播 VLAN/VC 功能，为二层接入网络提供组播数据的专用 VLAN/VC。组播包由 SR 向用户接入点的逐级复制，并最终由用户接入点（DSLAM 或接入交换机）实现面向用户的跨 VLAN 组播复制。

设备必须支持端口及用户上加入组播组数目限制，通过配置命令可以控制端口及用户允许加入组播组数目。建议通过策略控制平台控制端口及用户允许加入组播组数目。

设备必须支持用户的频道访问权限功能，频道访问权限分为禁止、预览和允许三种。频道预览应能够配置针对单次预览的持续时长、预览次数、预览间隔时长以及预览总时长参数。

设备应支持组播源地址检查功能，以避免在用户端口下存在多个 STB 时单一 STB 离开某组播组造成的观看同一组播组的其他 STB 点播中断的现象。

设备建议支持根据用户申请带宽的使用情况对组播请求进行接纳控制，当用户的剩余带宽不够时，用户的组播请求应不成功。

设备应支持 CDR（Call Detail Record）呼叫信息记录功能，记录用户的基本访问信息（包括 IGMP 请求成功/失败，用户标识，何时加入，何时离开，离开方式（强制、自主离开），访问的频道，频道权限，CDR 记录产生时间等）。

设备应支持 CDR 信息定时同步到 RADIUS 或 IPTV 业务管理系统，确保 CDR 信息不丢失。

11 IPv6

设备必须支持 IPv6 协议，主要包括 IPv6 数据包线速转发，IPv6 动态路由协议，过渡机制等。

必须支持 IPv6 基本协议，符合 RFC2460—互联网协议(版本六)。

必须支持 IPv6 地址结构的规定，符合 RFC4291—IP v6 地址体系结构。

必须支持基于 IPv6 的邻居发现机制，包括路由器和前缀发现，地址解析和邻居不可达检测，重定向等功能要求，符合 RFC2461 和 RFC3122 中邻居发现的相关规定。支持在同一链路上使用邻居发现协议来获知其它节点的存在，从而确定彼此的链路层地址，并发现路由器以及维护通向活动邻居的可达性信息。

必须支持 RFC4443 规定的 ICMPv6。

建议支持 IPv6 静态路由和动态路由，支持的动态路由包括：ISISv6、OSPFv3、

BGP4+、RIPng 等。

路由器必须支持 IPv6 的静态路由。到特定目的地的静态路由由网络前缀定义。支持 IPv6 静态路由中附加信息，包括：前缀长度、对给定路由协议引入静态路由的特定度量。

对应于 IPv6 的路由协议，路由器应支持 IS-ISv6 协议，应符合 RFC5308 中的规定。支持为适应 IPv6 协议增加的两个 TLV，即 IPv6 可达性 TLV 和 IPv6 接口地址 TLV。支持增加的 IPv6 协议标志符。

路由器必须实现在 RFC5340 中规定的 OSPFv3。支持 IPv6 OSPF 包格式，并直接运行在 IPv6 上。支持路由器 LSA 选项字段中增加的两个选项比特：R 比特和 V6 比特。支持 LSA 的格式变化。在 LSA 头和路由器 LSA、网络 LSA 中删去所有地址语义，这两个 LSA 以网络协议无关的方式描述路由域的拓扑。支持新增加的用于分布 IPv6 地址信息的新 LSA，以及进行下一跳解析所需要的数据。

路由器支持 BGP4+，符合 RFC2545 的规定。BGP4 用作传达 IPv6 可达性信息时下一跳属性可能需要包含全局地址以及本链路地址。用作构造 MP_REACH_NLRI 属性中下一跳域网络地址需要遵守 IPv6 特定的规则。满足在下一跳域 IPv6 地址中向对等实体传送下一跳全局 IPv6 地址，并且后接下一跳本链路 IPv6 地址。如果下一跳地址字段包含本链路地址，则地址长度值等于 32。

路由器必须支持 RIPng，并符合 RFC2080 的规定。

必须支持 IPv6 端口的 CoS/QoS 分类，并实施 QoS 策略控制。

必须支持在 IPv4 的 L2TP 隧道中承载 IPv6，必须支持 IPv6 LNS。

建议支持 IPv6 的 PPP 拨号，建议支持 RFC2472 规定的 IPv6 over PPP，建议支持 IPv6 NCP over PPPoA and PPPoE，建议支持 IPv6 CP。

设备必须支持 IPv4 到 IPv6 的过渡机制，主要包括双栈方式、手工隧道方式及 6to4 隧道方式，其它还应支持 IPv4/IPv6 NAT-PT/ALG 方式过渡机制，应具有双向 NAT-PT 和 DNS ALG、FTP ALG 功能(IPv4 到 IPv6 和 IPv6 到 IPv4)，支持 TCP、UDP 和其它端口复用的应用程序。可选支持 6PE 方式过渡机制，满足 RFC4659 的要求。

设备必须支持 IPv6 下的 IPSec 功能，符合 RFC4302/4303/4305 的规定要求。

必须支持 IPV6 的各种安全特性，支持 IPV6 的 uRPF 功能，应线速支持 IPv6 DDOS 攻击限制和过滤功能。

建议支持 IPv6 上的协议 PIM-SM, MLD, IPv6 based LDP for MPLS 等。。

建议设备硬件支持 IPv6 数据包转发, 端口转发达到线速。

建议设备支持基于 IPv6 的 IPOE 接入认证方式。

12 设备管理功能

12.1 基本管理功能

设备必须提供配套网元管理系统: 系统能自动发现设备, 可以管理多台设备。

网管系统必须具有配置管理、故障管理、性能管理、计费管理和安全管理功能: 管理系统可以通过图形化管理界面实现完全的配置操作, 建议系统支持 web 方式进行配置; 能够收集、显示、设置告警阈值、编排、过滤、处理和清除等告警管理; 能够收集、统计、显示所有的性能参数; 系统能提供认证、授权、控制、审计等安全管理功能; 系统必须提供北向接口如 CORBA/COPS/LDAP, 可以无缝地集成在第三方网管平台上。

设备要求具备可管理性, 设备必须支持通过 Console Port 或 Telnet 的模式实现配置管理。

设备必须支持 SNMPv1, 符合 RFC1155 和 RFC1157 的规定。

设备必须支持 SNMPv2, 符合 RFC2578、RFC2579、RFC2580、RFC3416 及 RFC3417 的规定。

设备必须支持 SNMPv3, 符合 RFC3410 的规定。

设备必须支持带外网管, 可以将管理流量与用户流量从物理或逻辑上分开, 带外网管与带内网管具有同等的功能。

设备必须支持 NTP, 必须支持在本地存放多个版本的软件和配置文件。

必须对一些重要的操作提供操作撤消功能。

建议具备 QoS 流量、故障、安全、配置等关键统计信息的本地存储功能, 并以 XML 的形式表达、通过 FTP 方式传送到指定的 FTP 服务器。

建议支持基于 XML 的 Network Configuration(NETCONF)网管协议。

必须支持流量采样, 在 10GE/GE/10G POS/2.5G POS 接口开启流采样功能, 所有端口按照 1000:1 的采样比进行 xFlow 采样的情况下仍保持线速转发, 只开启此项功能时 CPU 利用率不超过 30%, 采样精度大于 90%。建议支持针对子端口的 xFlow 采样。

12.2 SNMP MIB

设备必须支持 ATM MIB，包括：RFC2515 和 ATM 论坛的 SNMP-M4-MIB-AF-NM- 0095.1 中规定的管理目标定义。

设备必须支持分布式管理 MIB，即对 Remote Ping，Traceroute 和 Loopback 操作的管理目标定义，符合 RFC4560 的规定。

设备必须支持以太网 MIB，符合 RFC3635 中的规定。

设备必须支持接口组 MIB，符合 RFC2863 的接口组 MIB 的规定。

设备必须支持 IP MIB，包括 RFC1213 基于 TCP/IP 的互联网网络管理 MIB (MIB-II)、RFC2011 使用 SMIV2 的 IP SNMPv2 MIB、RFC2012 使用 SMIV2 的 TCP SNMPv2 MIB、RFC2013 使用 SMIV2 的 UDP SNMPv2 MIB、RFC4292 IP 转发表 MIB、RFC4087 IP 隧道 MIB。

设备必须支持组播 MIB，包括：RFC2932 中 IPv4 组播路由 MIB、RFC2933 中 IGMP MIB、RFC2934 中 IPv4 PIM MIB 的规定。

设备必须支持 PPP MIB，包括：RFC1471 的 PPP LCP 的管理目标定义；RFC1472 的 PPP 的安全协议管理目标定义；RFC1473 的 PPP IPCP 管理目标定义；

设备必须支持 RIP MIB，符合 RFC1724 的规定。

设备必须支持 OSPF MIB，符合 RFC1850 的 OSPFv2 MIB 的规定，符合 OSPFv3 MIB draft-ietf-ospf-ospfv3-mib-11 的规定。

设备必须支持 ISIS MIB，符合 RFC4444 的规定。

设备必须支持 BGP-4 MIB，符合 RFC4273 的规定。

设备必须支持 MPLS MIB，包括： RFC3814 MPLS FEC 到 NHLFE MIB；RFC3815 的 LDP 管理目标定义；RFC3813 MPLS LSR MIB；RFC3812 MPLS TE MIB；RFC4220 TE LINK MIB；RFC4368 MPLS 受控标签 ATM 和帧中继管理接口定义；RFC4687 对 MPLS 及其相关内容的管理必须符合 RFC4377 MPLS 网络的 OAM 需求、RFC4378 的 MPLS OAM 框架及点到多点 MPLS 网络 OAM 需求。建议支持 MPLS 快速重路由 MIB，符合 draft-ietf-mpls-fastreroute-mib-06.txt 的规定。

设备必须支持 MPLS L3 VPN MIB，符合 RFC4382 的规定。

设备必须支持 BFD MIB，符合 draft-ietf-bfd-mib-03 草案的规定。

设备必须支持 VRRP MIB，符合 RFC2787 规定的 VRRP 管理目标定义。

设备必须支持事件 MIB，符合 RFC2981 的规定。

设备必须支持通告 MIB，符合 RFC3014 的规定。

设备必须支持统计 MIB，符合 RFC2513 对面向连接对网络计费信息收集和存储的 controls 的管理目标定义。

设备必须支持 SNMP MIB，符合 RFC3418 SNMP MIB 的规定。

设备必须支持 SNMPv3 MIB，符合 RFC3411 规定的 SNMP 管理框架的体系架构；符合 RFC3412 规定的 SNMP 消息处理和分发；符合 RFC3413 SNMP 应用规定；RFC3414 SNMPv3 的基于用户安全模型(USM)；RFC3415 SNMP 基于视图接入控制模型(VACM)。

设备提供商必须提供所有相关 QoS 相关的 MIB，若含定义 MIB，则必须符合下述要求。

设备提供商自定义的 MIB 必须符合 RFC1155 B 标准，并符合 RFC1212 定源的描述和命名机制；必须能有效地支持特定对象的状态显示、统计、配置和控制，可通告一定途径获取其自定义 MIB 信息，并能对设备进行写操作。

12.3 故障管理

设备必须能够向网元管理系统发送告警信息；在告警信息中提供足够的信息以协助排障，例如日期时间戳、严重程度、部件标识、软件/硬件/固件版本等。

设备的故障告警必须至少要有以下几个严重级别的分类：紧急(critical)，主要(major)；次要(minor)和通知(informational)，并可以定制。

设备对以下情况必须发送告警：当 Radius 服务器不可用时；当设备的组成部分、逻辑端口或服务控制不可用时；设备必须支持对系统资源(例如 CPU 利用率)检测，在资源利用达到配置对阈值时。

故障事件的发生与事件的告警报告时间相差要小于 5 秒钟；当故障被修正时，设备将自动清除该故障的当前告警，并将改故障转存至历史告警信息中。

设备必须具备预先维护监测功能，例如事件审计、内存使用情况的监控、进程“丢失”或软件故障的监察等，并能采取适当的故障恢复措施。

设备必须允许通过用户名、IP、MAC 等进行会话的查找；设备必须支持 ping、traceroute 等工具辅助故障的处理；设备必须支持回退能力，如将操作系统软件/配置退回到先前的版本。

设备必须在网元管理系统无法工作时提供远程访问的手段；必须提供自检测或者故障诊断手段/工具，可完成连通性测试、性能测试、业务测试、硬件故障的检测及定位等；设备必须支持用户定位。

12.4 配置管理

网管系统必须实现对设备系统、端口和业务数据的配置、查询和修改；必须支持远程系统软件升级，建议设备支持在升级过程中不中断业务；设备必须提供软件备份、配置文件备份功能并能恢复；设备必须支持从 FTP 或 TFTP 服务器下载软件/配置文件。

网管系统必须支持 QoS 管理，支持对 IEEE 802.1p 的 CoS 字段、LSP EXP 字段、IP Precedence 字段等的配置，支持这些字段之间相互映射关系的配置，支持层次化 QoS 的配置，支持 VPN QoS 的配置，支持 QoS 队列、拥塞策略的配置。

12.5 计费管理

对于账号用户，应能协助 Radius 服务器完成用户的计费工作。

对于专线或 VPN 用户，应能根据业务实现的流量或时长的统计，并通过开放的通用接口提交给计费系统。

实现本地计费的设备对计费数据形成原始话单，以文本等方式在本地存储计费数据，未实现本地计费的设备的计费数据以标准 MIB 的形式存储于 MIB 库中，计费服务器通过 SNMP 周期性地查询设备的 MIB 计数器获取计费数据。设备厂商应开放其 MIB 库，使计费系统能通过标准的 SNMP 协议实时读取数据并进行相应处理。

12.6 性能管理

设备必须能够对系统内部对资源进行统计，如 CPU 及内存利用率等；设备必须支持对 QoS 策略对的实施进行统计；设备必须支持与业务相关对统计功能。

设备必须支持可设定一个端口每秒钟处理数据包个数的基本阈值，当超过时必须提供告警信息。

设备必须提供流量镜像功能；必须支持对基于单个用户流对监控和统计功能，包括应用层端口、会话连接数等。

12.7 安全管理

设备必须支持管理的安全功能，必须支持能够通过用户名和口令实现对设备对管理和控制；必须支持远程 telnet 访问功能；必须支持采用加密的方式进行安全的远程访问，如 SSH。对于远程访问必须提供访问超时控制，同时远程访问连接数限制，远程登录尝试次数限制，远程访问的相关信息记录(如访问终端的地址，端口，用户名和密码)等。

对于通过 console 端口的访问，也应提供访问超时、访问连接数、登录尝试次数等安全控制。

设备必须支持分级分权管理。

设备必须支持 RADIUS 进行网管登录密码认证，对密码进行集中管理。

设备应提供对登录口令长度的控制要求，建议至少不少于 8 个字符。

设备必须具有良好的访问控制，对设备所有网管操作都可配置为需要经过认证和授权方可进行，设备还必须支持 SNMP 对访问级别，必须支持网管日志功能，对超越权限或者失败的关键操作进行登记并作为安全告警；失败必须提供安全性审计的功能，并提供一种方法来记录配置的改变及操作人员改变配置的时间。

设备不允许存在未记载于文档的访问后门或通用密码。厂商必须确保这种用于调试或开发的途径在产品分销到客户手中之前已删除。

13 安全

13.1 访问控制和流量控制

设备必须支持源地址校验功能，支持单播反向路径转发/查找 uRPF 功能。

设备必须支持标准的五元组(源/目的 IP 地址、IP 协议字段、源/目的端口)的访问控制列表功能，还必须提供基于 MAC 地址(包括源和目的地址)的访问控制策略手段。访问控制列表必须可定制为在设备全局生效还是在端口生效。

设备必须提供流量监管功能。

13.2 路由协议安全

设备必须路由协议安全功能，支持 OSPF、ISIS、BGP 等路由协议的 MD5 认证，保证路由信息的可信度。

对于 MPLS LSP 的标签分配，使用 LDP/CR-LDP 的标签交换使用 UDP 协议承载，对于基本 hello 消息，设备应只接受与可信 LSR 直接相连的接口上的基本 hello 消息，忽略地址不是到该子网组播组的所有路由器的基本 hello 消息的地址；对于扩展 hello 消息，可利用 ACL 只接受允许的源发送来的扩展 hello 消息。LDP 会话过程使用的消息由 TCP 协议承载，应通过 TCP MD5 签名选项对会话消息进行真实性和完整性验证；使用 RSVP-TE 时，则应通过加密散列函数支持邻居验证，应支持 HMAC-MD5 算法，建议实现 HMAC-SHA1 算法。

13.3 抗攻击能力

设备必须支持抵抗大流量攻击的能力，包括过路流量和对设备本身对攻击。对于第一种攻击，路由器应能采取限速策略；对于第二种攻击，路由器必须丢弃攻击流，并生成告警日志。在此情况下，路由器必须完成对正常路由协议和管理报文的发送和接收处理。

设备必须支持抵抗畸形包的能力，能够检测超短/超长报文，并采取丢弃策略，同时对这种报文进行统计；能够检测到链路层错误并采取丢弃策略，同时进行日志记录和统计；能够检测网络层报文并采取丢弃策略，同时进行错误报文统计；设备不能由于错误报文/畸形报文而崩溃；设备本身必须不能发出错误报文/畸形报文。

设备必须支持对定向广播报文攻击的防范，禁止该类报文转发或者以广播形势转发，对于分布式 DOS 攻击，设备必须提供简单策略阻止这种分布式 DOS 攻击向设备扩散。

设备必须支持对 IP 地址哄骗的防范，必须支持单播逆向路径转发(URPF)功能限制这类报文在网络中出现。

设备必须支持至少一种针对去往/来自用户的流量，基于包类型(如 TCP SYN、ICMP 等)的机制(如可配置的速率限制)，以防护来自被黑的/恶意的用户主机的 flooding 拒绝服务攻击。

设备必须支持对 IP spoofing 的诊断和阻断；必须支持对 IP 源路由选项攻击对诊断和阻断；必须支持对 IP Address sweep 攻击的诊断和阻断；必须支持对端口扫描的诊断和阻断。

13.4 网络地址/端口翻译

设备必须支持网络地址翻译和网络地址/端口翻译；必须支持混合编址方式，对于来自私网的非私网地址的报文直接进行转发；支持黑名单功能，对黑名单中的地址不进行地址转换和报文转发；支持对不同级别用户并发连接数的限制。

设备必须支持 NAT 日志的输出。

13.5 MPLS VPN

不管是 L2 VPN 还是 L3 VPN，数据应严格基于标签沿着 LSP 分发，除非特殊需要，一个 VPN 的数据不得进入另一个 VPN 中；当支持 VPN 服务和互联网服务时，特别时在同一个物理接口上通过不同的逻辑接口支持 VPN 服务和互联网服务时，可基于逻辑接口对接入速率进行限制。

对于 L2 VPN, VPN 之间 MAC 地址和 VLAN 信息应相互隔离, VPN 之间或 VPN 和 MPLS 骨干之间可以复用 MAC 地址空间和 VLAN 空间;除非需要, VPN 之间或 VPN 或 MPLS 骨干之间的交换信息应相互隔离;可实现 VPN 使用的路由器资源(CPU、内存等)的相互隔离,防止因一个 VPN 独占资源而造成对其它 VPN 的 DOS 攻击。

对于 L3 VPN, 通过 BGP 协议约束路由信息的分配, 应支持静态路由和动态路由算法, 对于动态路由, IGP 和 EGP 协议都应支持 MD5 加密验证, 并可基于 VRF 实例限制路由更新的速度; VPN 之间的拓扑和编址信息应相互隔离, 一个 VPN 应可以使用所有互联网地址范围, VPN 和 MPLS 骨干之间应可以复用 IP 地址空间;应为每个 VPN 维持一个独立的 VRF 实例, 除非需要, VPN 之间或 VPN 和 MPLS 骨干之间的路由信息及其分发和处理应相互独立、互不干扰;可实现 VPN 使用的路由器资源的相互隔离, 防止因一个 VPN 独占资源而造成对其它 VPN 的 DOS 攻击。

13.6 冗余

设备必须支持冗余服务器的故障切换机制, 包括: Radius 服务器、LDAP 服务器(如果支持 LDAP)和 COPS 服务器(如果支持 COPS)。

设备必须支持 VRRP 功能。

所有元件必须支持热插拔;对于关键部件必须提供冗余备份功能, 如主控卡、路由控制卡等;必须支持从故障板卡到冗余板卡到自动切换, 手工切换应该作为选项支持;设备中的所有元件必须能够提供 1:1、N:1 或分布式设备冗余能力, 这些元件的倒换应是自动的, 并且不能影响业务(除第 8 项), 设备元件包括:

- (1) 交换单元;
- (2) 包转发引擎;
- (3) 控制和路由处理器;
- (4) 管理系统/管理接口;
- (5) 馈电接口;
- (6) 电源转换模块/供电单元;
- (7) 风扇;
- (8) 物理接口模块包括 APS(如 SONET GR253)的冗余能力。所有各种速率(up to OC-48)的 ATM、PoS 和通道化接口模块必须支持 N:1 冗余。

14 性能

14.1 设备容量要求

每个 ATM 端口 VP \geq 32 条;单个模块的 ATM PVC \geq 8000 条;整机 PVC \geq 64000。

每个以太网端口 VLAN 数量 \geq 4000。

设备转发引擎的吞吐能力,以 PPS 计,应等于设备有效配置的所有类型端口速率的总和;PPS 性能应该足以满足所有被支持的端口以限速转发混合长度的 IP 包;轻载条件下(端口吞吐量 10%),设备的 IP 包丢包率为 0;重载条件下(端口吞吐量 90%),设备的 IP 包丢包率小于 0.1%;路由器吞吐量在系统满负荷时,所有端口必须能够以线速处理 64 字节的包;在整机满负荷情况下,接口转发时延,转发 1518 字节及其以下长度的 IP 包时延均应小于 1ms。

流量整形能力,接口板上应可以支持 2048 个队列,当支持 2048 个队列时仍能做到线速转发,应支持 8 个等级的丢弃优先级。

14.2 路由性能

设备应该支持至少 100,000 条 RIB 表目,建议支持至少 250K 条 RIB 表目;应该支持至少 100,000 条 FIB 表目,建议支持至少 250K 条 FIB 表目;支持至少 20,000 条 IGP 路由,必须同时维持至少 100 个 IGP 邻居关系。

当设备容纳 10,000 条 IGP 路由时,建议路由更新收敛时间不大于 500ms。

OSPF 协议路由性能要求:

- (1) 至少应支持 100 个邻居/ospf instance;
- (2) 至少支持每个 OSPF 区里有 5000 条路由。

IS-IS 协议路由性能要求:

- (1) 至少应支持 100 个邻居/ospf instance;
- (2) 至少支持每个 ISIS 区里有 5000 条路由;
- (3) ISIS 单 Level 必须支持 1500 条 LSP,1 万条路由表处理能力。

RIP 协议路由性能要求:

- (1) RIB 至少可以支持 50,000 条,建立至少支持 250,000 条;
- (2) FIB 至少可以支持 50,000 条,建立至少支持 250,000 条。

BGP 协议路由性能要求:

- (1) 至少支持 500 个 BGP Peer;

- (2) BGP 会话数量大于 500,000;
- (3) 路由表容量大于 300,000 条;
- (4) Path 容量大于 1,500,000 条;
- (5) BGP/MP-BGP 路由波动对内存占用不能超过 50%, 对 CPU 使用影响不超过 10%。

MPLS 相关性能要求:

- (1) 在 25 个 LDP 邻居的情况下, 要求至少 2000 个标签/秒的更新能力, 单台设备故障切换造成包转发中断施加不大于 500ms;
- (2) 建立和拆除 LSP 的速度, 要求大于 2000LSP/秒;
- (3) 设备必须支持快速重路由功能, 当链路或节点发生故障时, 在建立 4000 条 LSP 的情况下, 从故障链路或节点切换到备份链路的时间小于或等于 50ms;
- (4) 当设备作为 MPLS 网络 LSR 路由器时, 必须支持 ≥ 32000 条 LSP; 当设备作为 MPLS 边缘路由器 LER 时, 必须支持至少 16000 条 LSP。当设备在支持最多的 LSP 数量时, 应仍然能以限速转发 MPLS 数据包;
- (5) 设备必须支持至少 2000 个 LSP, 至少支持 10,000 个标签表容量。

14.3 VPN 性能

■ MPLS L3 VPN 性能

要求 A 类 SR 支持至少 2000 个 VRF, VPN 路由表容量至少 20 万条; B 类 SR 支持至少 1000 个 VRF, VPN 路由表容量至少 10 万条, 同时对 MPLS IP VPN 的支持应为硬件线卡实现。在大量开展 MPLS IP VPN 业务后, 路由器的整体性能应不受影响。

SR 必须支持在每个 MPLS IP VPN 中支持至少 2000 个用户站点参与双向动态路由协议。

(2) L2 VPN

1) L2TP

SR 必须支持至少 4000 个 L2TP 隧道; 每个 L2TP 隧道中支持至少 8000 个 PPP 会话(不要求与隧道数相关); 每个隧道组中必须支持至少 8 个隧道。

L2TP 的平均建立响应时间 < 10 秒; 连接保持时间 > 12 秒

2) MPLS L2 VPN

MPLS VLL 的隧道支持数量要求不少于 64K。

设备支持 VPLS 的数量不少于 4000 个。

14.4 组播性能

要求设备在由 RPT 模式切换到 SPT 过程不能丢包。

单播路由切换后，组播路由切换的时间小于 1 秒。

组播组快速离开时延应小于 100 毫秒；频道切换时间小于 100 毫秒。

要求设备必须至少 2000 个组播组；至少支持 10,000 条组播路由；在承载 1000 个组，每组 2Mbps 流量的业务时，能稳定运行，要求包转发依赖硬件完成，不影响主控板 CPU 的性能；在启动了组播流量的 QoS 功能后，不能影响业务路由器的性能。

14.5 整机业务叠加性能

要求整机满配置下无阻塞交换，交换容量与端口容量之比大于 2，背板容量大于交换容量(端口容量指可配置的最大数量端口的总带宽；交换容量指交换矩阵最大交换能力；背板容量指背板单位时间内可传输的最大数据量)。

设备在多种功能同时开启时对设备性能的影响不明显，且必须不导致业务质量的下降。

设备的业务量叠加性能要求时指设备在用户数量和硬件满配置下，在提供专线接入、组播、MPLS 二三层 VPN 等业务并且针对全部在线用户提供 uRPF、ACL、QoS 等业务功能情况下，所具备的总体性能。设备在满配并叠加各种业务时性能应该不能明显下降，时延和丢包都应很小，CPU 利用率不能过高，并且能够长期稳定地运行。

15 设备其它要求

15.1 机箱要求

任何接口模块必须可以被不受限制地插入任何非保留给控制/交换模块地槽位中。

冷却系统必须是冗余和可热插拔的，当一个风扇故障时，剩余的风扇必须能够维持对满载系统的冷却。

必须使用温度传感器监测系统的温度，当系统温度超过预设的阈值时，必须产生一个告警指示，并发送给适当的告警/故障管理系统；必须提供视觉指示(LED)用于显示设备的冷却系统或温度情况(如风扇工作/故障，温度正常/过热等)。

设备应该提供多种机箱以应用于小型、中型及大型接入节点。本规范的要求适用于大型节点的部署，本规范中的功能要求(规模要求除外)适用于任何规模的设备。

15.2 线缆管理

设备应该在机箱的背部提供适当的线缆管理，使用户可以方便地对线缆进行操作。

15.3 设备可用性

设备应该具备 99.999% 的总体可用性(软、硬件)；例行维护时间不计算在内；系统无故障连续工作时间(MTBF)必须大于 69,000 小时。

必须允许对运行系统进行所有适当的配置更改和软件升级而不影响在线用户。

所有元件必须支持热插拔；必须支持关键部件冗余，及从故障板卡到备份板卡的自动切换，详细内容可参见 12.6 节；建议支持不同业务转发板的端口备份；从主用电源到备用电源的切换必须是自动的，不能引起业务的中断；设备应该支持以太网冗余，可以在 800ms 内恢复点对点的千兆以太网连接；在切换到冗余控制板卡时，建议设备能维护 VC、PPP 或 RFC1483/2684 会话的状态，并保持与之相关的所有功能或协议；满配的设备冷启动后应该在 10 分钟内完全正常运作；在有冗余配置的情况下，从机箱中抽走控制板卡时及重新插入控制板卡时，设备必须能够继续转发流量。

15.4 定时与同步要求

设备必须支持采用主从同步方式。

设备应设置外定时源输入接口，从通信楼定时供给设备（BITS）获得定时。同步接口可以为 2048kbit/s 或 2048kHz，优选 2048kbit/s 接口。

设备应具有从线路信号中恢复定时，并用于同步功能。当不能使用外定时方式时，采用线路定时。可从 STM-N 线路信号中获得，帧结构应符合 ITU-T 建议 G.707 的要求。

设备内部时钟应采用二或三级时钟。时钟单元可采用有保持功能的高稳晶体时钟。二级时钟的自由运行频率准确度优于： $\pm 4 \times 10^{-7}$ ；三级时钟的自由运行频率准确度优于： $\pm 4.6 \times 10^{-6}$ 。

设备在失去全部输入频率基准时钟信号时，内部时钟应能自动进入保持工作方式。时钟能在 24 小时内仍能维持相对于外定时中断瞬间时钟频率不劣于 $\pm 1 \times 10^{-8}$ 的时钟准确度。

设备的定时信号可从下列信号中提取：

- (1) 从外同步接口获取；
- (2) 从线路信号中获取；
- (3) 设备内部时钟产生的可用定时信号中获取。

定时信号的提取顺序为：先（1）后（2）再（3）提取定时信号。

15.5 网络时间同步

设备必须支持网络时间同步协议 NTP，支持 NTP 认证和 NTP 服务器/客户端。

15.6 OAM 要求

SR 设备必须支持 MPLS OAM 以及 ETHERNET OAM。

OAM 标准化协议应满足以下规范：

- RFC 4377 : Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks
- RFC 4378: A Framework for Multi-Protocol Label Switching (MPLS) Operations and Management (OAM)
- RFC4379: Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
- Ethernet OAM: IEEE 802.1ag & ITU-T Y.1731

15.7 设备硬件要求

1. 设备应支持不同业务处理板的混插，提高插槽的通用性和灵活性。
2. 系统交换引擎、总线带宽和到每个业务槽位的连接带宽必须能够满足目前和未来多种业务的发展需要，如，支持组播业务线速转发、频道的快速切换，保证视频业务质量和带宽。

3. 设备应具有网络故障和硬件故障告警功能。
4. 当软件升级时，应不影响硬件结构。
5. 对主控模块的要求：
 - 主控模块应具有软硬件故障告警功能。
 - 主控模块应具有故障脱机自动诊断功能以及负荷控制措施。
6. 设备应提供过流、过压保护措施。
7. 设备必须具备冗余的 Stratum3(或更佳)内部振荡器用于内部时钟，需满足或高于 Issue1 revision 2 of Telcordia GR-1110-Core 第 4.6 节中指定的同步要求。

15.8 设备软件要求

1. 软件要求保证安全可靠，具有容错能力。
2. 软件系统须提供数据接口，提供进行二次开发的文档。
3. 软件应采用模块化结构，模块之间的通信应按规定的接口进行。
4. 应具有软件故障的监视功能，一旦软件出现死循环等重大故障时，应能自动再启动，并做出即时故障报告信息。
5. 配置数据与处理程序应有相对的独立性，配置数据的任何变更都不应引起运行版本的变更。
6. 软件应有完善、方便的人机通信控制功能。
7. 软件应具备方便、迅速地恢复到原来版本的功能。
8. 系统软件应能在线升级，不需重新启动。
9. 软件应在不中断通信的情况下，完成程序打补丁的功能。
10. 不同时期软件版本应能向下兼容，软件版本易于升级
11. 软件升级必须可以在线获得
12. 设备必须支持从 FTP 或 TFTP 服务器下载软件/配置文件
13. 设备应该通过 CMM Level 3 认证，满足对软件开发和质量保证过程的要求
14. 设备应该通过 ISO 9001 认证，满足对软件开发和质量保证过程的要求
15. 设备的工程和制造过程应该通过 TL-9000 认证

15.9 环境要求

室内型设备必须能够在以下环境条件下正常运行：环境温度：5℃～45℃，每小时变化<10℃；相对湿度：10%～90%(非凝露、非结霜)。

在以下灰尘环境下，设备应能正常工作：直径大于 $5\text{ }\mu\text{m}$ 的灰尘浓度 $\leq 3\times 10^4$ 粒/ m^3 ；灰尘粒子是非导电、导磁和腐蚀性的。

设备的电磁兼容性应符合国标 GB 9254-1998《信息技术设备无线电骚扰限值和测试方法》和 GB/T 17618-1998《信息技术设备抗扰度限值和测试方法》。设备产生的电磁辐射建议符合 FCC Class A、EN55022/CISPR-22 Class A、VCCI Class A 等标准。

抗震措施：按 8 级烈度进行计算。

机械振动：4.9 牛顿/平方米(50 赫兹至 200 赫兹)。

应提供双电源备份和负载分担功能，必须支持-48V 直流电源，直流电压及其波动范围要求：直流电压及其波动范围要求：额定电压-48V，允许变动范围为-40V~-57V；建议支持-220V 交流电源，交流电压及其波动范围要求：单相 220V $\pm 10\%$ ，频率 50Hz $\pm 5\%$ ，线电压波形畸变率小于 3%。

15.10 绿色要求

15.10.1 设备管理要求

(1) 基本要求

1. 对于机框插槽式设备，设备应有高温报警功能。
2. 对于机框插槽式设备，应具备能源监控及管理功能。在设备管理员需要时，可检测到设备当前能耗状态。
3. 对于机框插槽式设备，应支持根据实际情况中断未用板卡供电或进入微电状态。
4. 设备电源反灌杂音应满足通信电源 YD/T 1051-2000《通信局站电源系统总技术要求》的要求。

(2) 扩展要求

1. 对于机框插槽式设备，能通过查询方式监控到目前工作状态下能耗，以及设备各个组件，如各板卡、机框、风扇，所消耗的能耗比例。
2. 对于机框插槽式设备，设备可通过命令行或网管工具远程关闭设备部分模块或功能以减少其工作能耗。
3. 对于机框插槽式设备，可根据实际情况动态调整风扇转速。
4. 对于机框插槽式设备和服务器设备，宜具有可根据用户需求和不同应用场合配置交流或直流供电的选择。

15.10.2 设备环保与包装要求

(1) 设备环保要求

设备设计阶段，设备的主要部分（如电路板、机箱、电缆等）应尽量减少铅、镉、汞、六价铬、溴化耐燃剂等有害物质，并严格按 ROHS 规范进行产品生产与设计。

(2) 设备包装要求

实行包装减量化（Reduce）。绿色包装在满足保护、方便、销售等功能的条件下，应是用量最少的适度包装。

包装应易于重复利用（Reuse）或易于回收再生（Recycle）。

包装废弃物可以降解腐化（Degradable）。为了不形成永久的垃圾，不可回收利用的包装废弃物要能分解腐化，进而达到改善土壤的目的。

包装材料对人体和生物应无毒无害，包装材料中不应含有有毒物质或有毒物质的含量应控制在有关标准以下。

包装材料应尽量减少木材的使用。

在包装产品的整个生命周期中，均不应对环境产生污染或造成公害。

(3) 其它要求

设备内部应有合理的气流组织，应采用前进后出或垂直通风方式，不宜从侧面进出通风。

同时，机框式数据设备内风扇应具有自动调节速率的功能，机架内采用防热风回流等技术，降低对机房环境的局部制冷要求。

机架门开孔率：考虑到通风和散热的需求，在保证门的强度和刚度要求前提下，机架正面门和背面门开孔率至少不得低于 30%，以获得良好的排吸风效果。

15.10.3 能耗分级标准

设备能耗等级应达到最新版本的中国电信《绿色数据设备技术规范》所定义的标准。

附录 A CE 设备技术要求

A1 CE 的定位

CE 在 IP 城域网中用于承载 CDMA 3G 业务、NGN 业务或大客户专线，可连接城域网的骨干网内的业务接入控制设备 SR，或连接 CN2 的 PE，实现各类业务的接入汇聚与路由转发，并接入本地或跨域的各种二、三层 MPLS VPN。

A2 CE 设备的技术要求

A2.1 设备分类及接口要求

根据业务发展趋势及 CE 产品现状，将 CE 分为两类：A 类和 B 类。

A 类：放置在业务密集的地方；双引擎配置条件下可配置端口容量（单向）不小于 140Gbps，交换矩阵和背板容量 $\geq 320\text{Gbps}$ ，必须支持 10GE、GE、FE 等以太网类型端口，建议支持 10G POS、2.5G POS、STM-1 POS、155M ATM 端口，所有端口在 QoS、ACL、Accounting 等功能同时应用时，保证语音/视频/INTERNET 多业务承载下稳定线速转发。设备具有良好的可扩展能力。A 类 CE 必须是 10G 平台，主控冗余条件下至少具备 6 个业务插槽。

B 类：放置在业务量较小的地方；双引擎配置条件下可配置端口可配置容量（单向）不小于 60Gbps，交换矩阵和背板容量 $\geq 120\text{Gbps}$ ，必须支持 10GE、GE、FE 等以太网类型端口、建议支持 10G POS、2.5G POS、STM-1 POS、155M ATM 端口。所有端口在 QoS、ACL、Accounting 等功能同时应用时，保证语音/视频/INTERNET 多业务承载下稳定线速转发。设备具有良好的可扩展能力。B 类 CE 必须是 10G 平台，主控冗余条件下至少具备 3 个业务插槽。

A2.2 基本功能要求

A2.2.1 链路聚合

必须支持网络侧的基于 802.3ad 链路聚合功能，必须支持，捆绑链路不少于 8 条。

必须能够在单 VLAN 或启用 SVLAN 条件下支持端口聚合功能。

链路故障时的收敛时间必须小于 800ms，建议达到 50ms 以内。

A2.2.2 生成树协议

设备必须支持符合 IEEE 802.1d 标准的生成树协议，简单拓扑环境下（网络

层次不大于 2 层) 链路收敛时间不大于 45 秒。

设备必须支持快速生成树协议, 简单拓扑环境下 (网络层次不大于 2 层) 链路收敛时间不大于 3 秒。

设备必须支持多生成树协议, 为交换机上的每个 VLAN 或多个 VLAN 建立对方的生成树, 链路收敛时间达到快速生成树协议的标准。

在支持的各种生成树协议环境下, 设备必须支持对节点权值和端口权值可配置, 以实现网络根网桥和设备根端口的灵活选择。同时还必须具备良好的兼容性, 可和支持该标准的其他厂家设备互通。

A2.2.3 VALN/SVLAN

设备必须支持 VLAN 功能, 必须支持 IEEE802.1q 协议规定的 VLAN 帧封装形式。

设备必须支持基于端口划分 VLAN, 各物理端口可通过配置不同的 VLAN ID 分属不同 VLAN。设备所有端口必须支持 VLAN tagged 和 untagged 两种工作方式。

建议设备支持 VLAN ID 交换功能, 即将进入设备的数据包所携带的 VLAN ID 映射为指定的其他 VLAN ID 并转发。

建议设备支持 VLAN 聚合, 即将多个 VLAN ID 聚合为一个 VLAN ID。

设备必须支持 SVLAN 功能, 为带有 VLAN 标记的数据包加入第二层 VLAN 标记。

一台设备必须可同时支持标准 VLAN 业务和 SVLAN 业务, 可使用同一个上行端口传送两种业务。设备启用 SVLAN 的端口必须可正常配置访问控制和 QOS 等各种策略。

SVLAN 以太网帧的外层 VLAN 标签的 ETHERNET TYPE 必须设置为 0x88a8, 建议设备支持外层 VLAN 标签的 ETHERNET TYPE 字段可配置。

设备必须通过硬件实现支持选择性 SVLAN 功能, 即在同一个物理端口上支持根据单层 VLAN ID 灵活加载外层 VLAN ID; 同时能够透传标准 VLAN (单 VLAN) 流量。

建议设备支持 SVLAN 的以下操作: 根据入端口、内层 VLAN 中 802.1p 参数、内层 VLAN ID 添加外层 VLAN ID 及 802.1p 参数。

建议设备能够对双层 VLAN 报文中的内、外层 VLAN 信息进行灵活的识别和处理, 便于对用户的上下流量进行管理。

A2.2.4 VRRP 功能

必须支持 VRRP (virtual router redundancy protocol)。

设备应能同时支持多组（不少于 100 组）VRRP 配置，每组可独立配置参数。主从 VRRP 设备之间的最短倒换时间应低于 500ms。

设备应能配置优先级，并支持优先级抢占或不抢占两种配置方式，当工作在优先级抢占方式时，可配置抢占延迟时间。

设备应能支持 VRRP 跟踪接口状态功能，即允许通过配置命令将 VRRP 与接口状态绑定，当被跟踪接口状态发生变化时，CE 能自动调整 VRRP 优先级，从而引起主从接入设备的倒换。

建议设备支持 BFD for VRRP。

A2.3 路由功能要求

具体要求参见本规范中第 5 章的路由功能要求。

A2.4 QoS 要求

具体要求参见本规范中第 6 章的 QoS 功能要求。

A2.5 VPN 要求

具体要求参见本规范中第 8 章的 VPN 功能要求。

A2.6 组播要求

具体要求参见本规范中第 9 章的组播功能要求。

A2.7 IPv6 要求

具体要求参见本规范中第 10 章的 IPv6 技术要求。

A2.8 设备管理功能要求

具体要求参见本规范中第 11 章的设备管理功能要求。

A2.9 安全要求

具体要求参见本规范中第 12 章的安全要求。

A2.10 BFD 功能要求

SR 必须支持 BFD 功能，基本功能应符合 draft-ietf-bfd-base-08 规定的各项要求，包括 BFD 检测的承载协议及使用的端口号，BFD 的包类型、包格式，检测模式、发送周期及检测时间、参数修改过程、会话初始化和建立等内容；SR 必

须支持单跳 BFD 功能的实现，并符合 draft-ietf-bfd-v4v6-1hop-08 的相关规定，建议支持 draft-ietf-bfd-multihop-06 的相关规定。SR 必须支持 BFD for OSPF, BFD for ISIS, BFD for Static、BFD for BGP、BFD for LDP。

A2.11 OAM 要求

具体要求参见本规范中 14.6 节中的 OAM 要求。

A2.12 定时与同步要求

具体要求参见本规范中 14.4 节中的定时与同步要求。

A2.13 性能要求

可参考本规范中第 13 章中的性能要求。

中国电信集团公司技术标准

Q/CT 2078-2008

中国电信 IP 城域网设备技术规范 (宽带接入服务器) (V3.0)

2008-12-31 发布

2009-1-1 实施

中国电信集团公司 发布

目 录

1	编制说明	1
1.1	范围.....	1
1.2	引用标准.....	1
1.3	定义、术语和缩写.....	6
1.3.1	定义.....	6
1.3.2	术语和缩写.....	7
2	概述.....	9
2.1	BRAS 的定位	9
2.2	BRAS 的功能和业务组成	10
2.3	业务实现思路.....	11
2.3.1	互联网业务的实现思路.....	12
2.3.2	VPN 业务的实现思路.....	12
2.3.3	组播业务的实现思路.....	12
3	设备分类	13
4	接口要求	13
4.1	常规.....	13
4.2	以太网接口.....	14
4.3	POS 接口	14
4.4	ATM 接口	15
4.5	其它接口.....	16
5	接入方式及用户管理	16
5.1	接入方式.....	16
5.1.1	以太网接入.....	16
5.1.2	ATM 接入	17
5.1.3	专线接入.....	17
5.1.4	宽带用户接入线路标识编码格式定义.....	18
5.2	用户管理.....	19
5.2.1	用户认证方式.....	19
5.2.2	IPOE 接入认证方式.....	20
5.2.3	授权.....	22
5.2.4	计费.....	22
5.2.5	地址管理与分配.....	23

5.2.6	RADIUS.....	24
5.2.7	断线码.....	24
5.2.8	策略控制.....	27
5.2.9	DHCP.....	30
5.2.10	用户端口绑定和唯一性标识.....	31
5.2.11	DPI 功能.....	31
5.2.12	SBC (Session Border Control) 功能 (可选)	31
6	QoS 功能.....	31
6.1	QoS 机制.....	31
6.2	QoS 能力.....	35
7	路由功能.....	36
7.1	开放最短路径优先 OSPF.....	37
7.2	中间系统到中间系统 ISIS.....	38
7.3	路由信息协议 RIP V1/2.....	39
7.4	边界网关协议 BGP4.....	39
7.5	VR 功能.....	41
8	MPLS 及 VPN 功能.....	41
8.1	MPLS.....	41
8.2	L2 VPN.....	42
8.2.1	L2TP.....	42
8.2.2	LAC 和 LNS.....	43
8.2.3	基于 IP/MPLS 的二层 VPN.....	44
8.2.4	BRAS 对二层 VPN 的终结功能.....	45
8.3	L3 VPN.....	45
8.3.1	MPLS VPN.....	45
8.3.2	IPSec.....	46
8.3.3	GRE.....	46
9	组播.....	46
10	IPv6.....	48
11	性能要求.....	49
11.1	设备容量要求.....	49
11.2	呼叫处理能力.....	50
11.3	服务质量.....	51
11.4	路由表容量.....	51

11.5	VPN 性能指标.....	51
11.6	组播性能指标.....	52
11.7	整机业务叠加性能.....	52
11.8	计费要求.....	53
12	安全和可靠性	53
12.1	设备自身安全.....	53
12.2	业务安全.....	54
12.3	可靠性和可用性要求.....	55
13	设备管理功能	56
13.1	基本管理功能.....	56
13.2	SNMP MIB	57
13.3	故障管理.....	59
13.4	配置管理.....	60
13.5	计费管理.....	60
13.6	性能管理.....	60
14	互通性要求	61
15	其它要求	62
15.1	定时与同步要求.....	62
15.2	网络时间同步.....	62
15.3	OAM 要求	62
15.4	设备硬件要求.....	63
15.5	机箱要求.....	63
15.6	线缆管理.....	64
15.7	设备软件要求.....	64
15.8	环境要求.....	64
15.9	绿色要求.....	65
15.9.1	设备管理要求	65
15.9.2	设备环保与包装要求	65
15.9.3	能耗分级标准	66

1 编制说明

1.1 范围

本技术规范以 RFC 文档以及 IEEE 标准为依据,针对中国电信实际情况和具体要求,对 IP 城域网中宽带网络接入服务器的定义、网络定位、业务功能等进行了说明,对设备分类、接口要求、用户接入方式、用户管理、QoS 功能、路由功能、MPLS 及 VPN 功能、组播、IPv6 功能、设备性能指标、安全和可靠性、设备管理、互通性及其它方面的要求进行了规定。

本技术规范适用于中国电信集团宽带网络接入服务器的研制、生产和引进。
在本规范中:

- (1) 必须: 表示该条目是本规范必须。违反这样的要求是原则性错误。
- (2) 必须实现: 表示该要求必须实现,但不要求缺省使能。
- (3) 不允许(不可以): 表示该条目绝对禁止。
- (4) 应当(建议): 表示在某些特定条件下存在忽视该条目的理由,但是忽视或违反该条目时必须仔细衡量。
- (5) 应当(建议)实现: 与应当(建议)类似,实现时不必要缺省使能。
- (6) 不应当(不建议): 表示在某些特定条件存在所描述行为可接受或有效的理由,但实现该行为时必须仔细衡量。
- (7) 可以: 表示该条目确实可选。

1.2 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。

GB/T17625.1-2003	《电磁兼容 限值 谐波电流发射限值(设备每相输入电流≤16A)》
GB17625.2-1999	《电磁兼容 限值 对额定电流不大于 16A 的设备在低压供电系统中产生电压波动和闪烁的限制》
YD/T 1051-2000	《通信局站电源系统总技术要求》
SPECpower_ssj2008	标准效能公司能耗测试标准
能源之星 4.0	主要针对消费性电子产品的能源节约计划。
COC on Energy Consumption of Broadband Equipment	宽带设备能源消耗管理

GB2423-89	电工电子产品的基本环境试验规程试验
GB4798.3-90	电工电子产品应用环境条件--有气候防护场所固定使用
YD/T 767-1995	同步数字系列设备和系统的光接口技术要求
YD/T 877-1996	同步数字体系（SDH）利用设备和系统的电接口技术要求
YD/T 976-1998	B-ISDN 用户网络接口物理层规范
YD/T 1045-2000	网络接入服务器（NAS）技术规范
YD/T 1061-2000	SDH 上传送 IP 的 LAPS 技术要求
YD/T 1109-2001	ATM 交换机设备技术规范
YD/T 1148-2001	网络接入服务器（NAS）技术要求—宽带网络接入服务器
YD/T 1162.1-2005	多协议标记交换（MPLS）总体技术要求
YD/T 1162.2-2001	在 ATM 上实现 MPLS 的技术要求
YD/T 1190-2002	基于网络的虚拟 IP 专用网（IP-VPN）框架
YDN 052-1997	B-ISDN ATM 层技术规范
YDN 053.4-1997	B-ISDN ATM 适配层（AAL）类型 5 技术规范
IEEE 802.2/3	局域网协议标准
IEEE 802.3u	快速以太网标准
IEEE 802.3ab/802.3z	千兆比以太网标准
IEEE 802.3ac	VLAN 标记
IEEE 802.3ad	以太网链路聚集
IEEE 802.1d	生成树协议
IEEE 802.1p	服务等级和优先级标准
IEEE 802.1q	虚拟局域网标准
IEEE 802.3x	流量控制
IEEE 802.17	RPR 标准
IEEE Std 802.1X(2001)	基于端口的网络接入控制
ITU-T G.703(1991)	系列数字接口的物理/电特性
ITU-T G.707(1996)	用于 SDH 的网络节点接口
ITU-T I.731	ATM 设备的类型与一般特性
ITU-T I.732	ATM 设备的功能特性
RFC 768	UDP 协议
RFC 791	IP 协议
RFC 792	ICMP 协议
RFC 793	TCP 协议
RFC 826	以太网 ARP
RFC 854	TELNET 协议
RFC 894	在以太网上传输 IP 数据包的标准
RFC 896	IP/TCP 互联网拥塞控制
RFC 922	IP 广播
RFC 950	IP 相关子网

RFC 959	FTP 协议
RFC 1042	在 IEEE802 网络上的 IP 数据报传输标准
RFC 1058	RIPv1 协议
RFC 1112	IP 组播中的主机扩展
RFC 1122	互联网主机要求-通信层
RFC 1142	IS-IS 协议
RFC 1155	基于 TCP/IP 的互连网管理信息的结构和标识
RFC 1156	基于 TCP/IP 的互联网网络管理的管理信息库：MIB-I
RFC 1157	简单网络管理协议（SNMP）
RFC 1195	用于在 TCP/IP 和双重环境中 OSI IS-IS 路由
RFC 1212	简明 MIB 定义
RFC 1213	基于 TCP/IP 的互连网的网络管理信息库：MIB-II
RFC 1256	ICMP 路由器发现消息
RFC 1321	MD5 算法
RFC 1332	IPCP 协议
RFC 1334	PAP 协议
RFC 1471	点到点协议上的链路控制协议管理对象定义
RFC 1473	点到点协议上的网络控制协议管理对象定义
RFC 1483/2684	AAL5 上的多协议封装
RFC 1490	FRAME RELAY 上的多协议封装
RFC 1519	CIDR：一种地址分配和聚合的策略
RFC 1573	MIB-II 接口组扩展
RFC 1631	IP 网络地址转换器（NAT）
RFC 1643	以太网链路 MIB
RFC 1657/4273	BGP4 管理对象定义
RFC 1661	PPP 协议
RFC 1662	在类 HDLC 帧中的 PPP 协议
RFC 1695	ATM 接口、设备和业务对象
RFC 1702	IPv4 网络上的通用路由封装
RFC 1771	BGPv4 协议
RFC 1724	RIP 管理信息库
RFC 1829	ESP DES-CBC 转换
RFC 1850	OSPF 管理信息库
RFC 1851	ESP 3DES 转换
RFC 1990	PPP 多链协议
RFC 1994	CHAP 协议
RFC 1997	BGP 团体属性
RFC 2080	IPv6 的 RIPng
RFC 2082	RIP v2 MD5 认证（Authentication）

RFC 2115	帧中继管理信息库
RFC 2131	动态主机配置协议 (DHCP)
RFC 2185	IPv6 路由方面过渡
RFC 2205	RSVP 功能描述
RFC 2236	互联网组管理协议 IGMPv2
RFC 2328	OSPF v2 协议
RFC 2338	虚拟冗余路由协议 (VRRP)
RFC 2362	协议无关组播-稀疏模式
RFC 2364	AAL5 上的 PPP
RFC 2375	IPv6 组播地址分配
RFC 2401~12	互联网协议安全体系
RFC 2402	IP 认证头
RFC 2406	IP 安全负荷封装
RFC 2409	因特网密钥交换 (IKE)
RFC 2420	PPP 3DES 封装协议
RFC 2439	BGP4 路由振荡抑制
RFC 2452/4022	IPv6 TCP MIB
RFC 2453	RIP v2 协议
RFC 2454/4113	IPv6 UDP MIB
RFC 2460	互联网协议-第六版 (IPv6) 规范
RFC 2461	IPv6 的邻居发现
RFC 2464	在以太网上传送 IPv6 分组
RFC 2472	PPP 上的 IPv6
RFC 2474	在 IPv4 与 IPv6 的 Diff-Serv 字段 (DS) 的定义
RFC 2475	Diff-Serv 体系结构
RFC 2509	PPP 上 IP 头压缩
RFC 2513	用于面向连接网络中计费信息的采集、保存的管理对象
RFC 2515	ATM 管理对象定
RFC 2516	传输 PPPoE 之方法
RFC 2529	在 IPv4 域中不使用显式隧道传输 IPv6
RFC 2545	用于 IPv6 域内选路的 BGP4 多协议扩展
RFC 2547/4346	BGP/MPLS VPN 规范
RFC 2578~2580	SMIv2 规范
RFC 2615	PPP over SONET/SDH 协议
RFC 2661	L2TP 协议
RFC 2665/3635	对以太网接口类型管理对象的定义
RFC 2667/4087	IP 隧道 MIB
RFC 2684	AAL5 上的多协议封装
RFC 2685	VPN 标识

RFC 2705	MPLS 流量工程
RFC 2764	IP VPN 框架
RFC 2766	NAT-PT
RFC 2784	GRE 隧道协议
RFC 2787	VRRP 的管理对象定义
RFC 2809	L2TP 的强制隧道
RFC 2858	BGP-4 多协议扩展
RFC 2863	接口组 MIB
RFC 2865	RADIUS 协议（认证）
RFC 2866	RADIUS 协议（计费）
RFC 2867	RADIUS 协议（隧道协议的计费）
RFC 2868	RADIUS 协议（隧道协议的认证）
RFC 2869	RADIUS 协议扩展
RFC 2932	IPv4 组播路由管理信息库
RFC 2933	IGMP 管理信息库
RFC 2934	PIM 管理信息库
RFC 2981	事件管理信息库
RFC 3014	通告管理信息库
RFC 3031	MPLS 体系结构
RFC 3032	MPLS 标记栈编码
RFC 3036	LDP 协议
RFC 3063	MPLS 环路预防机制
RFC 3065	BGP 自治域联盟
RFC 3145	L2TP 断开原因信息
RFC 3162	RADIUS 和 IPv6
RFC 3193	使用 IPSec 的安全 L2TP
RFC 3209	RSVP-TE: RSVP 的 LSP 隧道扩展
RFC 3270	MPLS 支持 DiffServ
RFC 3315	DHCPv6
RFC 3376	互联网组管理协议 IGMPv3
RFC 3410	简单网络管理协议介绍
RFC 3411~3415	简单网络管理协议第三版（SNMPv3）规范
RFC 3416~3417	简单网络管理协议第二版（SNMPv2）规范
RFC 3418	SNMP 管理信息库
RFC 3576	RADIUS 动态认证扩展
RFC 3587	IPv6 的可聚合全球单播地址格式
RFC 3623	OSPF 快速重启动
RFC 3633	DHCPv6 中 IPv6 前缀选项
RFC 3646	在 IPv6 的 DHCP 协议中实现 DNS 自动配置

RFC 3784	流量工程中 IS-IS 扩展
RFC 3916	PWE3 需求
RFC 3931	L2TPv3
RFC 3985	PWE3 结构
RFC 4090	LSP 隧道对 RSVP-TE 的快速重路由扩展
RFC 4271	BGP-4 协议
RFC 4291	IPv6 协议的地址结构
RFC 4292	IP 转发表管理信息库
RFC 4293	IP 管理信息库
RFC 4443	用于 IPv6 的 ICMP 协议 ICMPv6
RFC 4444	IS-IS 管理信息库
RFC 4560	RPING, Traceroute 和 Lookup 管理对象定义
RFC 4659	BGP-MPLS IP VPN 在 IPv6 VPN 中的扩展
RFC 4905	MPLS 网络上二层帧传送的封装方法
RFC 4906	MPLS 上二层帧的传送
RFC 4762	使用 LDP 信令的 VPLS
RFC 4761	使用 BGP 自动发现和信令的 VPLS
RFC 4724	BGP 的平滑重启功能
RFC 4915	OSPF 多拓扑路由功能
RFC 5304	IS-IS 加密认证
RFC 5308	Routing IPv6 with IS-IS
RFC 5120	ISIS 多拓扑路由功能
RFC 5309	链路状态路由协议 LAN 上的点到点操作要求
RFC 5340	OSPF for Ipv6
draft-kompella-ppvpn-l2vpn-04	Layer 2 VPNs Over Tunnels
draft-ietf-ospf-ospfv3-mib-11	OSPFv3 管理信息库
draft-ietf-bfd-base-08	双向转发检测
draft-ietf-bfd-v4v6-1hop-08	IPv4/v6 双向转发检测（单跳）
draft-ietf-bfd-multihop-06	多跳路径的双向转发检测
draft-ietf-bfd-mpls-07	MPLS LSP 中的双向转发检测

1.3 定义、术语和缩写

1.3.1 定义

宽带网络接入服务器（Broadband Remote Access Server，简称 BRAS）是面

向宽带网络应用的新型接入网关，是 IP 网络业务的接入控制点，位于城域网的接入层。

1.3.2 术语和缩写

AAA	Authentication, Authorization & Accounting （认证、授权和计费）
ACL	Access Control List （访问控制列表）
ADSL	Asymmetric Digital Subscriber Line （非对称数字用户线）
AIS	Alarm Indication Signal （告警指示信号）
APS	Auto-Protection Switching （自动保护倒换）
ARP	Address Resolution Protocol （地址解析协议）
ATM	Asynchronous Transfer Mode （异步传递模式）
BFD	Bidirectional Forwarding Detection （双向转发检测）
BGP	Border Gateway Protocol （边界网关协议）
BITS	Building Integrated Timing Source （通信楼综合定时供给系统）
BRAS	Broadband Remote Access Server （宽带接入服务器）
CE	Customer Edge(用户边缘)
CHAP	Challenge-handshake Authentication Protocol （握手认证协议）
CPE	Customer Premises Equipment （客户端设备）
CIDR	Classless Inter-Domain Routing （无类域间路由选择）
COPS	Common Open Policy Service （通用开放策略服务）
DHCP	Dynamic Host Configuration Protocol （动态主机配置协议）
DiffServ	Differentiate Service （差分服务）
DSCP	DiffServ codepoint （差分服务代码点）
DSLAM	Digital Subscriber Line Access Multiplexer （数字用户线接入复用器）
EAP	Extensible Authentication Protocol （扩展认证协议）
EGP	Exterior Gateway Protocol （外部网关协议）
FIB	Forwarding Information Base （转发信息库）
FTP	File Transfer Protocol （文件传输协议）
GBIC	GigaBit Interface Converter （吉比特接口转换器）
GE	Gigabits Ethernet （千兆以太网）
GRE	Generic Routing Encapsulation （通用路由协议封装）
ICMP	Internet Control Message Protocol （互联网控制消息协议）
ICP	Internet Content Provider （互联网内容提供商）
IGMP	Internet Group Management Protocol （互联网组管理协议）
IGP	Interior Gateway Protocol （内部网关协议）
IPoE	IP over Ethernet
IPSEC	IP Security Protocol （IP 网络安全协议）

IPTV	IP Television (IP 电视)
IPv6	Internet Protocol Version 6 (互联网协议第 6 版)
IPv6CP	IP Control Protocol (IPv6 控制协议)
IS-IS	Intermediate System to Intermediate System (中间系统到中间系统)
ISP	Internet Service Provider (互联网服务提供商)
L2TP	Layer 2 Tunnelling Protocol (第二层隧道协议)
LAC	L2TP Access Concentrator (L2TP 访问集中器)
LAN	Local Area Network (局域网)
LCP	Link Control Protocol (链路控制协议)
LDP	Label Distribution Protocol (标签分发协议)
LLC	Logical Link Control (逻辑链路控制)
LNS	L2TP Network Server (L2TP 网络服务器)
LSP	Label Switch Path (标签交换路径)
MAC	Media Access Control (介质访问控制)
MBGP	Multi-Protocol BGP (多协议 BGP)
MIB	Management Information Base (管理信息库)
MPLS	Multi-Protocol Label Switching (多协议标签交换)
MPLS EXP	MPLS experimental Field (MPLS 试验字段)
MTBF	Mean Time Between Failure (平均无故障工作时间)
NAT	Network Address Translate (网络地址转换)
NAT-PT	Network Address Translate + Protocol Translation (网络地址翻译/协议翻译)
OAM	Operation And Maintenance (操作和维护)
OLT	Optical Line Terminal (光线路终端)
ONU	ONU Optical Network Unit (光网络单元)
OSPF	Open Shortest Path First Protocol (开放式最短路径优先协议)
PAP	Password Authentication Protocol (密码认证协议)
PE	Provider Edge (运营商边缘)
PHB	Per-Hop Behavior (每跳行为)
PIM-SM	Protocol Independent Multicast - Sparse Mode (协议无关组播协议—稀疏模式)
POS	Packet Over SDH
PPP	Point To Point Protocol (点到点协议)
PPPoA	PPP Over ATM
PPPoE	PPP Over Ethernet
PPS	Packets Per Second (每秒分组数)
PVC	Permanent virtual circuit (永久虚连接)
QoS	Quality Of Service (服务质量保证)
RADIUS	Remote Authorization Dial In User Service (远程认证拨号用户服务)
RDI	Remote Defect Indication (远端故障指示)

RIB	Routing Information Base（路由信息库）
RIP	Routing Information Protocol（路由信息协议）
SDH	Synchronous Digital Hierarchy（同步数字序列）
SNAP	Service Network Access Point（业务网络接入点）
SNMP	Simple Network Management Protocol（简单网络管理协议）
TE	Traffic Engineering 流量工程
TOS	Type Of Service 业务类型
uRPF	Unicast Reverse Path Forwarding（单播反向路径查找）
VLAN	Virtual LAN（虚拟局域网）
VPDN	Virtual Private Dial-Up Network（虚拟拨号专网）
VPLS	Virtual Private Lan Service（虚拟专用以太网服务）
VPN	Virtual Private Network（虚拟专用网）
VR	Virtual Router（虚拟路由器）
VRF	Virtual Route Forwarding Table（VPN 路由转发表）
WRED	Weighted Random Early Dectection (加权随机早期检测)

2 概述

2.1 BRAS 的定位

BRAS 通常以 ATM 接口连接 ATM 网络或直接连接 ADSL 局端 DSLAM 设备，实现 ADSL 用户的汇接；以 GE/10GE 接口连接二层汇聚交换机，实现以太网上行 DSLAM 或者 LAN 用户的汇接；以 GE/10GE 接口连接 OLT 设备，实现 FTTX 用户的汇接。

BRAS 通常以 GE/10GE 接口或 2.5G/10G POS 接口连接城域网骨干路由器，实现业务的上行。

典型的网络拓扑如下图 2-1 所示：

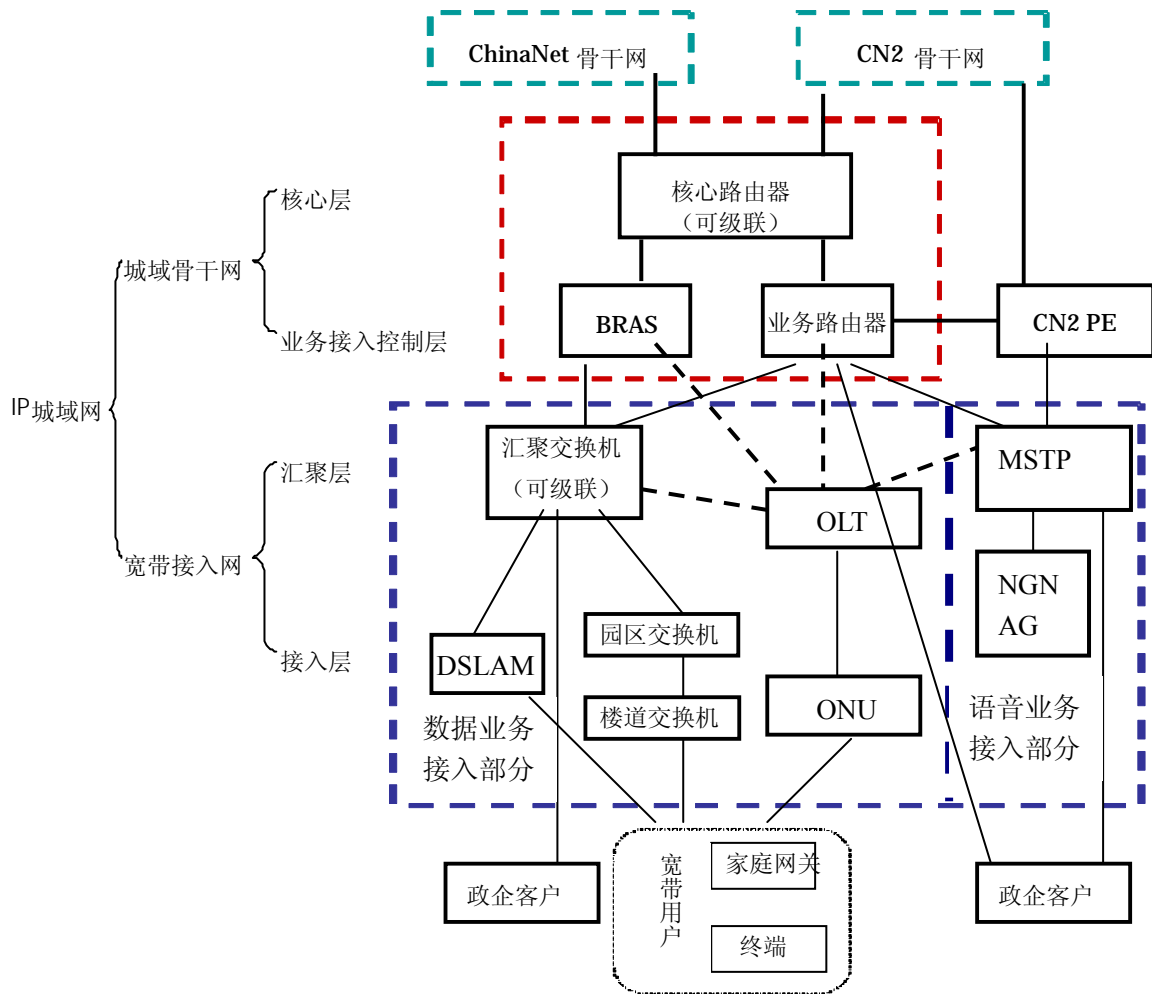


图 2-1 城域网拓扑

2.2 BRAS 的功能和业务组成

BRAS 作为 IP 网络业务的接入控制点，是宽带接入网和城域骨干网的衔接点，其功能分为两部分：业务功能模块（网络业务的实现，偏重于与城域骨干网的配合和衔接）和接入功能模块（接入方式的终结和控制，偏重于与宽带接入网的配合和衔接）。业务功能模块和接入功能模块处于相对独立的层次上，能够自由组合，实现不同接入方式和不同网络业务的灵活组合。

BRAS 的接入功能模块包括：拨号接入功能、专线接入功能。

BRAS 的业务功能模块包括：互联网网关业务功能、组播网关业务功能和 MPLS PE 业务功能。

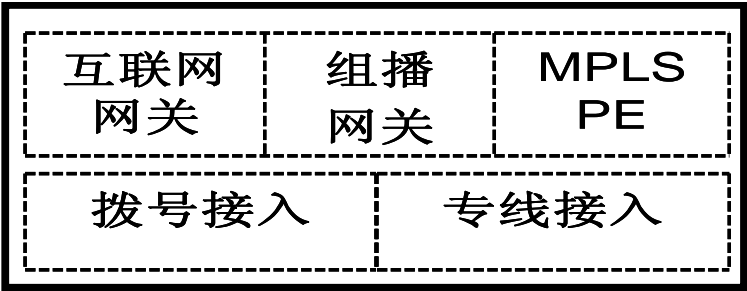


图 2-2 BRAS 的业务功能模块

BRAS 各组成模块的主要功能如下：

(1) 拨号接入功能模块

主要是 PPPoE 拨号接入控制功能，包括 PPPoE 请求响应和会话控制、用于认证和计费的 RADIUS client 功能，以及常规的 Diffserv 标记、速率限制和流量整形、ACL、uRPF 等安全控制、流量采集和统计等。

(2) 专线接入功能模块

提供用户端口（物理端口或逻辑端口）以及在端口上的接入控制功能，如 Diffserv 标记、速率限制和流量整形、ACL、uRPF 等安全控制、流量采集和统计等。

(3) 互联网网关业务功能模块

用户 IP 地址和路由提供。

(4) 组播网关业务功能模块

组播路由，IGMP 控制，组播用户管理和控制，组播复制。

(5) MPLS VPN PE 业务功能模块

二三层 MPLS VPN 业务功能，具体功能包括三层 VPN 的 MBGP、VRF 以及二层 VPN 的 VPLS PE 功能。

BRAS 主要的接入功能模块是拨号接入，次要接入功能模块是专线接入；

BRAS 主要的业务功能模块是互联网网关业务，次要业务功能模块是组播网关业务和 MPLS VPN PE 业务。

BRAS 主要实现互联网网关业务功能，提供互联网业务。在设备功能和性能允许的前提下，可以用 BRAS 实现 PE 业务功能，提供 MPLS 二三层 VPN 业务。BRAS 实现组播网关业务功能，提供 IPTV 等基于组播的业务。

2.3 业务实现思路

BRAS 作为业务接入控制点设备，实现的主要业务包括：互联网业务、VPN 业务和组播业务，各种业务的实现思路如下：

2.3.1 互联网业务的实现思路

互联网业务为用户提供到城域网的宽带接入并连接到 CHINANET、CN2 以及 INTERNET 的业务，是城域网最基本的业务。

ADSL/LAN 拨号用户接入 DSLAM 或楼道交换机，通过 ATM 网或以太网汇聚到 BRAS，BRAS 终结 PPPoE，为拨号用户分配地址，提供认证、授权和计费功能，提供路由，并实现 ACL、uRPF 等安全控制和速率限制，实现 DSCP 标记等 QoS 控制。

2.3.2 VPN 业务的实现思路

(1) L2TP VPN

主要用于构建企业的 VPDN 网络。

用户通过 ADSL/LAN 拨号接入，发起 PPP Session 连接到 BRAS，BRAS 充当 L2TP 的 LAC 角色，封装用户的 PPP Session 到 L2TP 隧道，L2TP 隧道穿过公共 IP 网络，终止于企业内部的 LNS，PPP Session 也终结在 LNS 上。用户的 PPP Session 经企业内部的认证服务器认证通过后即可访问企业的内部网络资源。

(2) 三层 MPLS VPN

对于 ADSL/LAN 拨号用户，BRAS 终结 PPP Session 后，将用户的 PVC/VLAN 绑定到相应的 VRF 里，对于 ADSL/LAN 专线用户，BRAS 直接将用户的 PVC/VLAN 绑定到相应的 VRF 里，BRAS 充当 PE 的角色，通过城域核心的 P 路由器（对开启 MPLS 的城域网）或 CN2 的 PE 路由器（对不开启 MPLS 的城域网）实现本地或跨域的 MPLS VPN 业务。

2.3.3 组播业务的实现思路

BRAS 是 PIM 路由协议的边界，IGMP 请求的终结点，负责组播业务的 AAA 请求和控制，支持基于 PPP 和端口的复制。在 BRAS 设备能力和带宽允许的情况下，优先采用 BRAS 实现 PPP 复制提供组播业务。通过静态组加入配置将所有组播流量推送到 BRAS。在业务开展初期，在用户比较少的情况下，由 BRAS 为组播用户进行复制；当用户数量发展到比较密集的时候，二层汇聚网络为组播业务提供专用 VLAN，组播包由 BRAS/SR 向用户接入点的逐级复制，并最终由用户接入点实现面向用户的跨 VLAN 组播复制。

3 设备分类

根据支持的用户规模，BRAS 分为以下 A、B 两类。

	A 类	B 类
最大在线用户数	48000	32000
最大配置用户数	96000	64000
每用户保证带宽	200Kbps	200Kbps
单槽交换及可配置容量（单向）	10Gbps	2.5Gbps
整机端口线速配置容量（单向）	120Gbps	60Gbps
槽位数	12	8
上联端口	10GPOS/2.5G POS/10GE/GE	2.5G PoS/10GE/GE
下联端口	10GE/GE/FE/ATMOC-3	GE/FE/ATMOC-3

4 接口要求

4.1 常规

BRAS 用户侧必须支持 GE/100BaseT/ATM 等多种业务物理接口，网络侧必须支持 2.5G POS/GE/100BaseT/ATM 等多种上行接口，其中 A 类 BRAS 必须支持的 10GE 上行接口，建议支持 10G POS 上行接口和 10GE 下行接口；B 类 BRAS 建议支持 10GE 上行接口。

A 类设备必须在不更换任何硬件设备(机箱、引擎、电源、风扇等等)的条件下具备支持未来 20G 的业务卡能力。

10GE/GE/100BaseT/ATM 等接口必须能够用于用户接入或网络上行而不影响接口的功能。

设备必须支持在所有 SONET/SDH/TDM 端口的物理端口 loopback。

设备必须具备通过 RS-232 VT-100 类型终端访问的控制面板。

设备必须具备冗余的 BITS（Building Integrated Timing Source）外部时钟输入接口。

设备必须能够从通道化接口取得时钟。

4.2 以太网接口

BRAS 必须支持 FE 接口：

- (1) 10/100Base-T 接口：符合 IEEE802.3/IEEE802.3u 标准。

或：

- (2) 100Base-FX 接口：符合 IEEE802.3u 定义的 100Base-FX 以太网标准。
- (3) 100Base-TX 接口：符合 IEEE802.3u 定义的 100Base-TX 以太网标准。

设备必须支持在 100Base-TX 端口上的自动协商功能。

BRAS 必须支持 GE 接口：

- (1) 1000Base-T 接口：符合 IEEE802.3ab 定义的 1000Base-T 以太网标准。
- (2) 1000Base-LX 接口：符合 IEEE802.3z 定义的 1000Base-LX 以太网标准。
- (3) 1000Base-SX 接口：符合 IEEE802.3z 定义的 1000Base-SX 以太网标准。
- (4) 1000Base-ZX 接口：符合 IEEE802.3z 定义的 1000Base-ZX 以太网标准。

GE 光接口必须支持 GBIC (GigaBit Interface Converter) 或 SFP (Small Form-factor Pluggable) 模块。

建议设备提供只支持三层转发功能的 GE 接口。

A 类设备必须支持 10GE 接口：符合 IEEE802.3ae 定义的万兆以太网标准。

建议设备支持在物理端口上的 IEEE 802.3ad 链路汇聚/负载分担功能。设备在启用链路聚合功能时必须实现对 VLAN 及 SVLAN 的透传承载。链路故障时的收敛时间必须小于 800ms，建议达到 50ms 以内。

设备必须在以太网物理端口上支持至少 1550 字节的以太网有效载荷，以保证将 1500 字节的 IP 包置入 L2TP 封装中而无需分段。

设备必须在以太网物理端口上支持超长帧 (Jumbo Ethernet frame)。

设备在最高速接口上应支持长达 15min 的比特计数而不溢出。

设备必须支持 VLAN 堆叠 (Stack Vlan)，且每端口必须支持 4096×4096 个 VLAN。

接口在连接光纤发生故障时，告警自动发出 Console log 和 SNMP TRAP。

业务板卡建议支持 BFD (Bidirectional Forwarding Detection, BFD)，并且在 BFD 检测到链路故障时能够自动切换到预先设定的备份链路或者 VLAN 去。

4.3 POS 接口

POS 接口应支持 STM-1、STM-4、STM-16 接口标准，A 类设备建议支持 STM-64 接口标准。

设备的 POS 接口必须支持 1+1 自动保护切换（APS）。

所有光接口必须支持单模。

所有光接口必须支持多模。

在 POS 接口中，PPP 映射到 SDH 应遵循 RFC2615 和 RFC1662。

PPP 协议由标准 RFC1661 描述。IP 数据包也可以遵循 YD/T 1061-2000 同步数字体系（SDH）上传送 IP 的 LAPS 技术要求，先转换成 LAPS 帧结构，再映射到 SDH 虚容器 VC 中。IPv6 数据包遵循 RFC 2472。

其 POS 接口的 SDH 帧封装应符合标准 ITU-T G.707（1996）；接口性能应符合标准 ITU-T G.957（1995）；误码率应符合标准 ITU-T G.826（1996）；抖动与漂移应符合标准 ITU-T G.825（1993）。

接口在连接光纤发生故障时，告警自动发出 Console log 和 SNMP TRAP。

4.4 ATM 接口

设备用于用户侧的 ATM 接口必须支持 STM-1 接口标准，建议支持 STM-4 接口标准。

设备用于网络侧的 ATM 接口必须支持 STM-1 和 STM-4 接口标准。

设备应支持光接口和电接口两种，电接口适用于局内、干扰信号弱的情况。物理层采用两种速率的接口：155520 kbit/s 或 622080 kbit/s。光接口必须符合 YD/T976-1998 的规定。

ATM 层必须符合 YDN052-1997 的规定。ATM 适配层必须符合 YDN 053.4-1997 的规定。ATM 接口必须按照 RFC1483 的规定将 IP 包封装到 AAL5 的帧格式中。

设备必须支持 ATM 论坛用户-网络互联接口（UNI）规范，版本 3.1。支持 RFC 1483 规定的 AAL5 上的多协议封装。支持 LLC/SNAP 和 IP 复用 PVC（路由协议的 LLC 封装）。

设备必须支持 ATM 论坛流量管理规范（Traffic Management Specification）4.1（AF-TM-0121.000）所定义的 ATM CBR 服务等级、UBR 服务等级、nrt-VBR 服务等级、rt-VBR 服务等级及 ATM 论坛流量管理规范 4.1 补遗

（AF-TM-0150.000）所定义的带有 MDCR（Minimum Desired Cell Rate）参数的 ATM UBR 服务等级。

建议设备支持 ITU-T I.610 所规定的 ATM OAM VC 管理。设备必须在所有 ATM 端口上支持 ITU-T I.610 所规定的 ATM F4 和 F5 OAM loopback、AIS、以及 RDI（remote defect indication）。

设备 ATM 接口建议支持 APS 1+1 保护。

4.5 其它接口

建议支持速率为 155Mbit/s、622Mbit/s、2.5Gbit/s 的 RPR 接口。

5 接入方式及用户管理

5.1 接入方式

BRAS 必须支持以太网接入方式、ATM 接入方式及专线接入。

5.1.1 以太网接入

设备必须支持 PPPoE 接入，可限制逻辑端口或子端口的最大 PPP Session 数且可配置。

设备必须支持以太网端口的 MAC 地址学习与老化。只向学习到该 MAC 地址的端口发送单播流量，以防止用户的 MAC 地址被其它端口窥探（snoop）。如果设备在某个时间段没有从这个地址收到或者向这个地址发出流量，设备必须老化动态学习到的 MAC 地址并将其从 MAC 地址表中删除。设备必须允许 MAC 地址老化时间可配置。

设备必须在 RFC 2684 逻辑以太网端口上支持至少 1550 字节的以太网有效载荷。

设备必须支持 IEEE Std 802.1q-1998 所定义的 VLAN。必须支持基于端口、PPP 用户划分 VLAN，支持 tagged 和 untagged 两种工作方式。每个端口支持的最大 VLAN 数为 4096。建议设备能够把 802.1q VLAN 端口作为逻辑 IP 端口使用（如 IP VPN 环境中）。

设备必须支持以太网控制帧（如生成树协议）的 tunneling。设备应支持标准虚拟冗余路由器协议（VRRP），并符合 RFC2338 的要求。

设备必须支持多端口的以太网桥接功能（802.1d）。设备必须有能力阻断在同一桥接组中两个用户间的所有通信（基于二层或三层机制）。如果允许用户流量在不同的用户之间桥接的话，设备必须支持 MAC 层的 ACL，可以基于 Ethertype 准许或拒绝。设备必须允许操作员清除桥接表中的单个用户而无需清除整个表。设备必须能禁止某个以太网 MAC 地址在同一时刻与多个 VLAN 相关联。设备必须允许通过用户登录、IP 地址（如果有）和 MAC 地址来查找一个

VLAN 中的所有会话。

设备必须支持 VLAN 堆叠（将用户的 802.1q VLAN 置于运营商 VLAN 中的能力），遵循 IEEE 802.1ad 标准的规定。VLAN 堆叠技术用于采用 VLAN ID 实现用户唯一性标识和定位的宽带接入网，以实现 VLAN 资源的扩展。每个以太网端口及每个 PPP 用户都必须支持 Stack VLAN，且每个以太网端口必须支持 4K*4K 个 VLAN。设备在进行 VLAN 堆叠时 ethertype 字段为 0x88A8，必须支持可配置的 ethertype 字段。

设备必须支持两层 VLAN 自动生成功能。

设备必须支持以太网端口的 802.3x 规定的流量控制协议。设备必须支持以太网端口的基于 IEEE 802.1p 优先级设定。

设备必须支持 VRRP 功能。设备在启用 VRRP 功能时必须实现对 VLAN 及 SVLAN 的透传承载。设备必须支持 BFD for VRRP。

5.1.2 ATM 接入

设备必须支持 PPPoA 接入，可限制逻辑端口的最大 PPP Session 数且可配置。

设备必须支持 ATM VP 及 VC 的汇聚和终结。设备必须支持 ATM VP 及 VC 的交叉接合（cross-connect）能力。设备必须在提供 VP/VC 的交叉接合功能时保持 ATM 的服务等级（service class）。必须支持 PVC、建议支持 SVC。必须支持 AAL5，支持 CBR、UBR 和 VBR 业务，支持业务流量整形。

设备必须支持通过 ARP 从 RFC 1483/2684 桥接 ATM PVC 端口动态学习 MAC 地址。设备必须维护一个静态 VLAN 到 PVC 的映射关系，以及一个动态学习的 ATM PVC 到 MAC 地址的映射关系。设备必须允许对动态学习到的 MAC 地址到 ATM PVC 映射的超时间隔进行调整。设备必须支持映射多个 MAC 地址到单个 ATM PVC。

每个物理端口支持 4 个队列或 4 个以上队列。输出队列必须支持对每条 VC 分段和业务整形功能。必须能在独立的 VC 上，或在单条 VC 上排队发送属于同一个下一跳路由器的区分业务流。

支持 ATM 上的 MPLS（MPLS over ATM）。

5.1.3 专线接入

设备必须支持 ADSL 通过 RFC1483/2684 桥接和路由的方式专线接入方式。必须支持以太网专线接入方式。

设备必须支持通过 VPI/VCI 统计用户流量，对以太网接入的专线用户根据 VLAN ID 或 IP 地址或 IP 子网或物理端口统计数据流量，并通过 RADIUS 定期将流量信息发送 RADIUS 服务器。

5.1.4 宽带用户接入线路标识编码格式定义

宽带用户接入线路标识的编码格式必须符合中国电信有关规定，从 DSLAM 设备接收该编码，并统一上报给后台管理系统。其统一编码格式为：

```
{atm|eth|trunk} NAS_slot/NAS_subslot/NAS_port:XPI.XCI  
AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port[:A  
NI_XPI.ANI_XCI]
```

说明：

- atm|eth|trunk: BRAS 端口类型，ATM 接口、以太网接口或 trunk 类型的以太网接口；
- NAS_slot: BRAS 槽号 0~31；
- NAS_subslot: BRAS 子槽号 0~31；
- NAS_Port: BRAS 端口号 0~63；
- XPI: 如接口类型为 atm，XPI 对应于 VPI，XPI 为 0~255；如接口类型为 eth（或 trunk），XPI 对应于 PVLAN，XPI 为 0~4095；
- XCI: 如接口类型为 atm，XCI 对应于 VCI，XCI 为 0~65535；如接口类型为 eth（或 trunk），XCI 对应于 CVLAN，XCI 为 0~4095；
- AccessNodeIdentifier: 接入节点标识（如 DSLAM 设备），长度不超过 50 个字符的字符串，字符串中间不能有空格；
- ANI_rack: 接入节点机架号（如支持紧耦合的 DSLAM 设备）0~15；
- ANI_frame: 接入节点机框号 0~31；
- ANI_slot: 接入节点槽号 0~127；
- ANI_subslot: 接入节点子槽号 0~31；
- ANI_port: 接入节点端口号 0~255；
- ANI_XPI: 可选项，如接口类型为 atm，XPI 对应于 VPI，XPI 为 0~255；如接口类型为 eth，XPI 对应于 PVLAN，XPI 为 0~4095；
- ANI_XCI: 如接口类型为 atm，XCI 对应于 VCI，XCI 为 0~65535；如接口类型为 eth，XCI 对应于 CVLAN，XCI 为 0~4095；
- ANI_XPI.ANI_XCI，主要是携带 CPE 侧的业务信息，可用于标识未来的业务类型需求，如在多 PVC 应用场合下可标识具体的业务。

字符串之间用一个空格隔开，要求字符串中间不能有空格。花括号{ }中的内容是必选的，|表示并列的关系，多选一。[]表示可选项。对于某些设备没有机架、框、子槽的概念，相应位置应统一填 0，对于无效的 VLAN ID 值都填 4096。

如接口类型为 ATM，则 AccessNodeIdentifier、ANI_rack、ANI_frame、ANI_slot、ANI_subslot、ANI_port 域可统一填 0。

如运营商未使用 SVLAN 技术，则 XPI=4096，XCI=VLAN，取值为 0~4095。

如运营商未使用 VLAN 技术区分用户（用户 PC 直连 BAS 端口），则 XPI=4096，XCI=4096。

5.2 用户管理

BRAS 必须支持用户的认证、授权、IP 地址分配及计费功能、支持策略控制和动态授权，支持用户唯一性标识功能。

5.2.1 用户认证方式

设备必须支持 RADIUS 认证、本地认证、不认证等多种认证方式。

设备必须支持 PPPoE、PPPoA 等 PPP 拨号认证。支持 PAP、CHAP 验证方式，PAP、CHAP 验证顺序可灵活配置。

设备必须支持 802.1X 认证，支持 EAP-MD5 认证和 EAP-SIM 认证。

设备必须支持 IPOE 接入认证。在 IPoE 的接入环境下，BRAS 必须能够同时支持 DHCP+WEB 的接入认证方式和基于 DHCP option 扩展（Circuit-id）的接入认证方式。认证流程必须符合中国电信的“我的 E 家”业务采用 PPPOE 和 IPOE 用户管理的解决方案。

设备支持 DHCP+WEB 认证方式时，支持强推 Portal 门户。强制用户在拨号认证通过后第一次打开浏览器的时候前往指定页面，门户网站内容可以由运营商自行制定。

设备支持基于 DHCP option 扩展的接入认证方式时，BRAS 必须能够照中国电信的要求将包含用户终端信息和物理线路信息的 DHCP Option 映射成 Radius 属性并发送至 Radius Server 实现接入认证，并根据认证鉴权结果，控制用户接入。可以通过 Radius 服务器向用户下发接入属性（带宽、业务优先级等）。

设备必须支持 IPOE 接入认证方式下对 session 管理功能，包括 IPoE 用户的上线速率、IPoE 用户下线管理机制、IPoE 用户异常掉线机制处理。

支持 DHCP Relay 及 DHCP Proxy 功能。

设备可以同时支持 PPP、802.1X、DHCP+WEB 认证，每个端口可以指定某

种或某几种认证方式。

设备必须支持普通用户的认证，支持加域名后缀的用户认证方式，满足用户对多 ISP 的选择，对本地用户能够支持按 VLAN-ID 或者 PVC-ID 认证的方式。

建议支持用户一次拨号、多次动态选择应用服务或同时提供多个应用服务（不需断线或重新建立新的 PPP 连接）。

支持用户输入值的某些特殊符号，如支持用户登录名中的“@”、“/”等可显示的 ASCII 符号。

5.2.2 IPOE 接入认证方式

设备必须支持 IPOE 接入认证。在 IPoE 的接入环境下，BRAS 必须能够同时支持基于 DHCP option 扩展（Circuit-id）的接入认证方式和 DHCP+WEB 的接入认证方式。

基于 DHCP option 扩展的接入认证流程要求如图 5-1：

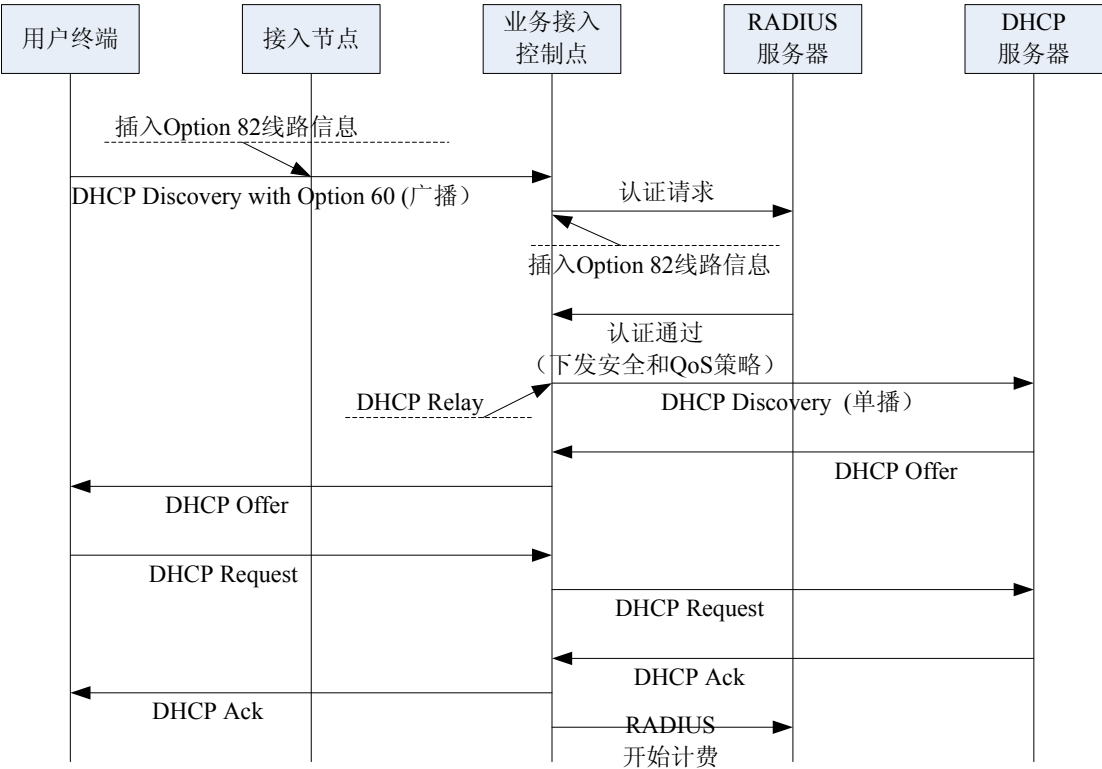


图 5-1 基于 DHCP option 扩展的接入认证流程

基于 DHCP option 扩展的接入认证的具体过程如下：

- a) 用户终端发出携带有 DHCP Option 60 字段的 DHCP 发现消息；

b) 接入节点（DSLAM 或接入交换机）在 DHCP 发现消息里插入 DHCP Option 82（包含物理线路号信息），然后再把修改过的 DHCP 发现消息转发到后面的业务接入控制点（BRAS/SR）；

c) 业务接入控制点检测到这是一个新用户，为该用户创建 IP 会话上下文，此时 IP 地址还未获得配置。业务控制点为该 IP 会话创建一个 RADIUS 接入请求消息，并向 RADIUS 服务器发送 RADIUS 请求消息。RADIUS 接入请求消息必须包含 Username、Nas-Port-id、Nas-Port-Address 等属性；

d) 如果通过 RADIUS 服务器的认证，RADIUS 服务器将向控制点回复接受接入消息，同时传送与该用户的 IP 会话有关的业务策略。控制点接收到接受接入消息，该 IP 会话获得授权，执行该 IP 会话的业务策略，包括 QoS 参数配置和安全策略；

e) 接入控制点向 DHCP 服务器中继转发 DHCP 发现消息；

f) DHCP 服务器接收到 DHCP 发现消息后，回应 DHCP 提供消息；

g) 业务接入控制点接收到 DHCP 提供消息，中继转发到用户终端。业务控制点把获得的 IP 地址与已建立的 IP 会话相关联，完成该 IP 会话的全部配置。后续的针对该用户的所有动态策略都将针对此 IP 会话进行操作。在 IP 会话过程中，业务控制点不断进行 IP 会话的心跳检测，如果几次未得到用户终端的响应，就断开 IP 会话，释放资源，终止计费；

h) 用户终端接收到 DHCP 提供消息，响应以 DHCP 请求消息；

i) DHCP 服务器收到 DHCP 请求消息后，响应以 DHCP 确认消息。用户终端收到 DHCP 确认消息，完成 DHCP 配置过程；

j) 业务接入控制点对该 IP 会话进行统计，并把统计参数发送给 RADIUS 服务器用于后台的统计计费。

设备必须支持在接收到终端发出的 DHCP Discovery 报文中插入 Option 82 线路信息。建议用户的 SVLAN 信息或 DSLAM 上用户端口信息作为设备插入的 Option 82 线路信息。Option 82 用于标识用户位置信息，用于认证时对应于 RADIUS 属性 Nas-Port-id（attribute 87）。

设备必须支持根据 Option 60 做为业务分类标识。设备必须可以使用 Option 82 作为线路信息进行认证。

设备必须能够获取 DHCP Discovery 报文中的 MAC 地址（发送 DHCP 请求的终端 MAC 地址）作为用户名，并使用 DHCP Discovery 报文中的 Option 60 字段作为域名地址（@domain），构建 IPOE 接入认证的 Username: MAC@option 60。

建议设备支持的认证方式为：

Username: MAC@option 60；

Password: 可修改的任意字符。

建议设备支持 Option 43 和 Option 120。

当设备内置 DHCP Server 时，建议设备能够根据不同的 Option 60 值分配不同网段的 IP 地址。

当设备外置 DHCP Server，且不同业务 DHCP 地址管理平台分离时，建议设备能够分析识别 DHCP Discovery 报文中的 Option 60 字段，并把具有不同的 Option 60 值的 DHCP Discovery 报文送到相对应的 DHCP 平台的能力。

必须支持 DHCP Snooping 功能，实现 IP 地址、MAC 地址和 VLAN 逻辑端口的动态绑定，避免出现地址私配和地址盗用。

必须支持针对源 MAC 地址的 DHCP DISCOVERY 报文的 DDOS 攻击，必须支持接口级的 DHCP discovery 请求报文的限速功能，建议支持用户级的 DHCP DISCOVERY 的报文限速功能。

必须支持 IPoE 用户正常下线管理机制及 IPoE 用户异常掉线处理机制。

5.2.3 授权

设备必须支持带宽控制。

设备必须支持访问权限控制，包括认证前与认证后。

设备必须支持 QoS 优先级分类。

设备必须支持动态授权。

设备必须支持主备 DNS。

5.2.4 计费

设备必须支持按使用时长、流量等计费方式，建议支持按业务等级、业务类型等计费方式及实时计费功能。生成的计费信息包中应包括用户的帐号、分配的 IP 地址、Session ID、登录时间、离线时间、上网时长、设备号、端口号、PVC 或 VLAN Id (SVLAN Id)、MAC 地址、上/下载字节、上/下载包数量、不同 QoS 等级的流量信息和丢包信息等关键信息。为配合计费系统按流量计费的功能，在标准 RADIUS 断线包标准属性中，BRAS 必须能提供用户准确的进和出流量。

设备必须支持限制向 RADIUS 服务器发送请求的速率，设备必须丢弃超出所配置最大请求速率的 RADIUS 请求。必须支持 RADIUS 记帐请求的复制功能，可以将同一个记帐请求同时送往两个不同的 RADIUS 记帐服务器。必须支持计费报文的重传机制。

设备必须支持当与远端的 Radius 失去联系时可实现本地计费，保证话单数据不会丢失。

设备可以设置用户最大连接时长，该值可以由配置时设定，也可以从计费系统的 RADIUS 返回包中取得。当用户的连接时间达到允许的最大时长时，BRAS 能主动撤除与用户的 PPP 链接，并能正确的送出计费停止包。

设备的计费精度必须小于 1 秒。

5.2.5 地址管理与分配

BRAS 必须支持多种 IP 地址管理和分配方式，从地址类型来看，必须支持固定 IP (ADSL 专线)、静态 IP (用户每次拨号登录网络时分配到相同的 IP 地址) 和动态 IP。

BRAS 必须支持 DHCP 方式、PPP 方式和静态配置方式分配和管理 IP 地址。

(1) 分配静态地址。

设备必须在地址池耗尽的情况下拒绝用户的分配地址请求。

设备必须支持缺省地址池。

设备必须支持通过本地配置为指定域名的用户分配特定的地址池地址。

设备必须支持根据 RADIUS 响应属性为用户分配特定的地址池地址。

设备必须保证用户不能私配地址。

(2) 分配动态地址

设备必须支持用户从本地地址池分配地址。

设备必须支持用户从 RADIUS server 分配地址。

设备必须支持用户从外部 DHCP Server 统一分配地址。

设备必须支持在本地配置用于 PPP 和 DHCP 用户的地址池。设备必须支持在地址池中使用私有（保留）地址。IP 地址池必须可以包含多个 CIDR 地址块。

BRAS 必须支持 RADIUS Client 功能，支持由 RADIUS Server 分配 IP 地址，设备必须支持将 RADIUS 应答中的 Framed-IP-Address 作为分配给用户的地址。设备必须支持 BRAS 本身来分配 IP 地址。必须能支持 20 个以上的 IP Pool。支持根据 RADIUS 应答中的属性为用户使用特定的地址池。设备必须支持缺省地址池，如果在 RADIUS 回应中指定了一个未命名的地址池，设备必须从缺省地址池中为用户分配地址。

BRAS 必须内置 DHCP 服务器，由 BRAS 直接分配地址；必须支持 DHCP Relay 和 DHCP Proxy 功能，通过远程 DHCP 服务器分配地址。必须支持 IP 地址、MAC 地址和 VLAN 逻辑端口的动态绑定，避免地址冲突和盗用。要求支持 DHCP

+WEB 方式提供用户认证、授权；要求支持 DHCP 请求转换为 RADIUS 请求功能，实现 DHCP 地址管理和 PPP 拨号地址管理的集中管理。

必须支持多个地址池，对于不同的用户类型，BRAS 可以根据 RADIUS 的要求分发不同地址池的 IP 地址，以达到控制用户上网的访问范围。BRAS 的每个接入单元应该能够根据用户名、接入端口等信息自动为用户分组，每组具有不同的 IP 地址池，在每组内地址池为用户选择 IP 地址。必须支持通过 RADIUS 返回 IP Pool Name 而实现对用户选择 IP Pool 分配 IP 地址的方式。

通过多域选择，可为不同的 ISP 分配不同的 IP Pool。设备必须支持为任意可路由端口分配 IPv4 地址（固定地址）。设备必须支持为单个可路由端口分配多个 IPv4 地址。设备必须支持在本地配置为指定的域名用户使用特定的地址池。

设备必须遵循 RFC 828，使用地址解析协议（ARP）构造 ARP 表。设备必须支持反欺骗机制（如 secure ARP 或 Proxy ARP）。设备必须允许网络管理员在 ARP 表中手工添加表目，将一个或多个 IP 地址与 MAC 地址关联。

设备必须过滤流量，保证用户不能使用私配地址。

设备必须支持每 VR 至少 20 个或整机 2000 个地址池。

A、B 类 BRAS 支持的地址数量分别大于 64K、32K。

5.2.6 RADIUS

BRAS 必须支持与 RADIUS 服务器一起共同完成用户的认证、授权、IP 地址分配及计费功能。

设备必须支持主备 RADIUS 及负荷分担功能。必须支持认证与计费 RADIUS 分开。支持主、备 RADIUS 的自动切换，当主 RADIUS 出现故障时，系统须能自动产生告警，并将认证计费信息请求发送到备用 RADIUS，由备用 RADIUS 服务器负责完成认证和产生计费信息。当主用 RADIUS 恢复后，不须人工干预，BRAS 能重新指回主用 RADIUS。整个切换过程无服务中断和计费信息丢失。

BRAS 发出的包必须符合标准 RADIUS 协议，必须支持认证、授权、计费、VPN 等 RADIUS 属性，支持 RADIUS 扩展属性。

5.2.7 断线码

设备必须符合中国电信 BRAS 断线代码规范。中国电信 BRAS 断线代码规范见下表：

代码	定义	说明	场景举例
----	----	----	------

代码	定义	说明	场景举例
1	User Request. 用户请求下线。	PPPoE 认证用户主动要求终止连接。PPPoE 的 LCP（链路控制协议）发出链路终止数据包给 BRAS，要求终止连接。	正常关机、用户主动断开连接等。 注：在系统挂起、休眠时，不同拨号器、操作系统情况会有差异，如果用户发送了下线请求，使用此原因；如果没有，BRAS 通过 LCP 发现用户下线，BRAS 返回代码 2，例如，Win2000 下使用拨号软件 RasPPPoE、WinXP 自带拨号软件，系统休眠或者挂起时，拨号软件没有发出断线请求。
2	Lost Carrier. 载波丢失。	PPPoE 协议握手报文丢失。 一般指 BRAS 下一级网络设备（含该设备）到 PPPoE 拨号设备间的故障。	用户线路断、PC 断电、PC 异常关机、网卡禁用等。
3	Lost Service. 业务不再提供。	业务服务器（例如：VPN）主动发起终止用户业务服务的报文。	BRAS 接收到 VPN 业务服务器发起的 L2TP StopCCN 包。
4	Idle Timeout. 闲置切断。	用户在规定时间内流量没有达到设定值。	用户长时间没有使用联网的电脑。
5	Session Timeout. 会话超时。	用户上线时间达到了规定值或者用户的流量达到了规定值。	预付费用户上线时间达到了规定值或者用户的流量达到了规定值。
6	Admin Reset. 管理员复位	由于管理的需要，暂时中断用户的链接。	1、命令行/网管复位或者禁用端口 2、命令行/网管切断在线用户

代码	定义	说明	场景举例
	端口, 或者删除会话。		3、命令行/网管删除L2TP隧道 4、删除、修改配置参数
7	Admin Reboot. 管理员重启BRAS。	在重启BRAS前, 发送断线信息。	
8	Port Error. BRAS检测到端口错误。	BRAS主动检测到用户接入端口的错误。一般指BRAS到下一级网络设备间(包括BRAS)的故障。	1、BRAS用户单板异常 2、BRAS用户端口异常 3、BRAS到下一级网络设备间物理线路断 4、BRAS用户端口PVC异常中断
9	BRAS Error. BRAS内部处理异常。	由于BRAS内部软件处理异常造成的用户掉线。	
10	BRAS Re-quest. BRAS因其它无法识别原因中止会话。	未规定的掉线原因。	
11	BRAS Reboot. BRAS异常导致设备重启。	BRAS异常重启前发送断线信息, 以进行非管理性的重启。	

说明:

在断线原因分类中, 代码2、8、9、10、11属于异常断线。

代码2一般指BRAS下一级网络设备(含该设备)到PPPoE拨号设备间的故障, 代码8一般指BRAS到下级网络设备间(包括BRAS)的故障。

代码8的故障也会引起代码2的故障, 如果代码8和代码2同时出现, 应认定为

代码8故障。

要求代码10在实际情况中尽量少的出现。

BRAS 探测 PPPoE 协议状态的 ECHO 报文应每分钟发送三次，如果连续发了三次而 PPPoE 用户没有一次响应的话（需 20 秒之内响应），BRAS 就认为该用户已经下线。

5.2.8 策略控制

设备必须支持通过策略控制平台对基于用户名、PVC、VLAN、MAC 地址、IP 地址、逻辑端口、物理端口、MPLS 标签等属性绑定的接入控制策略。控制策略应能实现业务流分类、标记、速率限制、带宽保证、流量整形、队列调度、拥塞避免等基本的 QoS 机制。

必须实现用户业务 QoS 的动态调整策略。

设备建议支持通过策略控制平台实现层次化 QoS。

设备必须支持通过策略控制平台实现标准的 5 元组 ACL；建议设备支持通过策略控制平台实现扩展 ACL（EACL），分类规则含端口、VLAN、MAC 等；建议设备支持基于帐号和基于用户的扩展 ACL（UACL），对用户实施访问权限控制。

设备必须支持通过策略控制平台实现用户带宽 CAR 控制，并支持将 CAR 控制信息送往 RADIUS，以便实现不同带宽不同费率。

设备必须支持通过访问外部服务器得到基本用户信息（用户名、用户类型、付费方式等）、用户订购业务、用户 QoS profiles、用户线路信息。

设备必须支持 Push 模式策略控制。

设备建议支持 Pull 模式的策略控制。

设备必须支持用户/业务策略通过策略控制平台强制激活方式、用户通过 Portal 界面订购业务的手工激活方式、自定义触发条件满足时（如：时长、流量、非法/非正常业务流）的自动激活方式。

设备必须允许指定用户使用的访问控制策略，对用户实施访问权限控制。

设备必须支持按 Domain 实施控制策略，包括：认证计费策略，带宽控制策略，访问权限，QoS 策略，路由策略等。

BRAS 设备必须支持同一帐号下的不同业务权限的控制及部分业务权限的透传至 DSLAM 的功能。

设备必须支持不同的用户帐号实现不同的 ACL 和路由策略。

设备必须支持不同的业务类型实现不同的路由策略。

设备必须支持动态授权，支持以 COPS、DIAMETER 或 RADIUS 为主的业务控制协议。

设备提供 COPS 接口协议时必须支持 COPS 规定的多种消息类型，按照功能可以划分为两类：COPS 链路状态建立/维护消息与业务处理消息。

a) COPS 链路状态建立/维护消息包括：

- Client-Open (OPN) 消息
- Client-Accept (CAT) 消息
- Client-Close (CC) 消息
- Keep-Alive (KA) 消息

b) 业务处理消息包括：

- 请求 (REQ) 消息
- 删除请求状态 (DRQ) 消息
- 策略下发 (DEC Install) 消息
- 策略删除 (DEC Remove) 消息
- 状态一致性请求 (SSQ) 消息
- 状态一致性完成 (SSC) 消息
- 状态上报 (RPT) 消息

提供 COPS 接口的策略控制过程采用 PUSH 方式如图 5-2 所示，整个描述过程如下：

a) BRAS/SR 和策略控制平台之间建立 TCP 链路；

b) BRAS/SR 和策略控制平台将发生一些消息的交互以验证 TCP 链路的合法性；

c) 验证通过后，当接收到业务管理平台发送的 QoS 请求，或者 BRAS/SR 发送的用户上线请求，策略控制平台根据网络运营商定义的策略等信息进行决策，形成策略数据放在 DECInstall/Remove 消息中下发给 BRAS/SR；

d) BRAS/SR 收到 DEC Install/Remove 消息后，在本地进行策略信息的执行，完毕后向策略控制平台发送 RPT 消息报告执行的状态（成功/失败）；

e) 当用户不再使用某个业务时，由 BRAS/SR 向策略控制平台发出 DRQ 消息，要求删除某个用户的状态信息；BRAS/SR 将删除本地的状态信息，策略控制平台将删除本地的状态信息并回收分配给用户的资源。

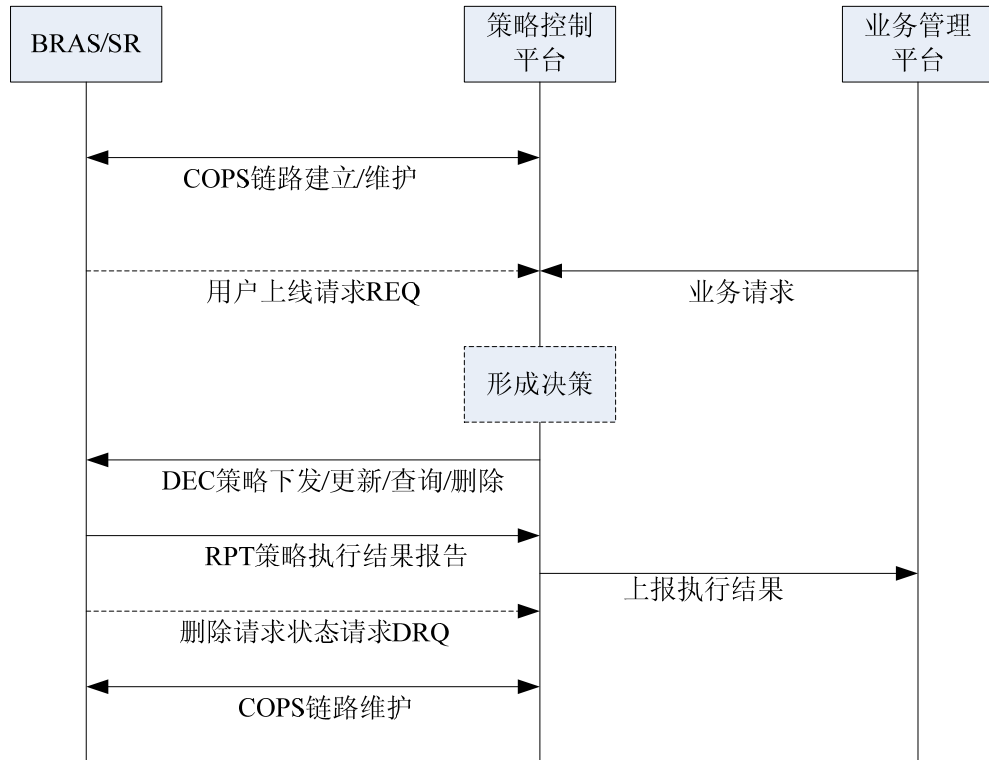


图 5-2 COPS 接口上的策略控制过程

设备提供 DIAMETER 接口协议的功能要求待定。

设备应能在配套的增值业务系统的管理下，动态修改用户的各种策略，以提供动态 QoS 等增值业务功能，要求用户和 BRAS、PORTAL 三者之间实现一次连接、一次用户认证、多次业务选择功能。

设备必须支持基于 RFC3576 的 DADIUS 扩展动态授权：

- 必须支持 RADIUS 扩展中的踢用户下线（DM）和动态授权（COA）消息，符合 RFC3576 规定的消息交互框架；
- 必须支持 BRAS 和 RADIUS server 之间的密钥检查，对密钥检查不通过的请求直接丢弃；
- 必须支持以 Username（1）为关键字的 DM 和 COA 消息；
- 必须支持以 Acct-Session-Id（44）为关键字的 DM 和 COA 消息；
- 建议支持对 NAS-Port（5）、Framed-IP-Address（8）、Calling-Station-Id（31）、NAS-Port-Type（61）、NAS-Port-Id（87）的校验检查；
- 动态授权必须支持的标准属性：Filter-Id（11）、Session-Timeout（27）；
- 动态授权建议支持的标准属性：Idle-Timeout（28）；
- 动态授权必须支持的厂商属性：用户的上下行带宽、用户的 QoS 配置变化；
- 动态授权建议支持的厂商属性：用户 TCP 会话数限制、流量预付费时的

剩余流量。

建议设备支持通过策略控制平台动态调整用户使用的带宽或业务优先级，限制访问特定的资源。当用户业务使用完毕后，释放带宽资源并删除相应的配置信息。

建议设备支持可用资源（如可用带宽、CPU 利用率、队列缓存大小）和用户资源使用状况实时上报到策略服务器，策略服务器根据设备的资源利用情况及用户使用资源情况决定对用户的接纳控制和策略控制。

5.2.9 DHCP

设备必须支持 RFC 2131，在设备本地实现 DHCP 服务器功能。

设备本地的 DHCP 服务器必须能够为客户提供以下 DHCP 选项：

- 子网掩码
- 缺省路由
- DNS 服务器
- 域名
- NetBIOS 名字服务器
- NetBIOS 节点类型
- 租借时间

DHCP proxy:

设备必须支持 DHCP 代理，在 DHCP 用户请求地址时，设备作为 DHCP 客户端向 DHCP 服务器获得地址，然后分配给用户；

每个 VR 都必须可以独立作为 DHCP 代理；

设备在支持 DHCP 代理时必须可以指定至少 3 个 DHCP 服务器。

DHCP Relay:

设备必须支持 RFC 3046 DHCP 中继代理消息选项，能够作为 DHCP 中继代理为用户分配 IP 地址；

设备中的 DHCP 中继代理必须检查上行数据包，发现 IP 地址和以太网 MAC 地址，构造 ARP 表；

设备中的 DHCP 中继代理必须作为客户和 DHCP 服务器产生点对点的 DHCP 请求；

设备中的 DHCP 中继代理必须跟随租借时间和租借更新协商，能够在租借时间期满时终止用户会话。

5.2.10 用户端口绑定和唯一性标识

设备必须支持用户帐号与用户端口绑定（可以根据 Stack VLAN ID 和 PVC ID 来标识用户和定位用户的物理位置），建议支持 VBAS、PPPoE+和 DHCP Option82 等技术实现用户端口精确定位。

设备必须支持 SVLAN（IEEE 802.1ad）的用户端口绑定解决方案，且每 GE 端口的 VLAN 数量为 4096×4096。设备在进行 VLAN 堆叠时 ethertype 字段为 0x88A8，必须支持可配置的 ethertype 字段。

5.2.11 DPI 功能

建议支持 DPI（Deep Packet Inspection，深度包检测）功能，可在网络层识别应用层信息，以便细化安全策略。

支持对 HTTP、FTP、DNS、POP3、SMTP、ICMP 等多种基本协议的识别。

支持 P2P（Skype、BitTorrent、eDonkey、MSN 等）应用层协议的识别。

支持对识别出的应用进行控制，并能对网络流量进行统计。

开启 DPI 功能时对设备性能的影响不大。

5.2.12 SBC（Session Border Control）功能（可选）

建议支持 SIP、MGCP、H.248、H.323 等信令代理功能，能够接受各终端的注册，并可作为主叫或被叫进行会话通讯。

建议支持 NAT/防火墙穿越功能。不需要对网络中原有的 NAT/防火墙做任何改动。

建议支持 ACL 和包过滤，防止 IP 层 DOS 攻击及信令攻击，具有呼叫接入控制功能。

6 QoS 功能

6.1 QoS 机制

设备必须实现 DIFSEV QoS 机制，包括分类、标记、速率限制、带宽保证、流量整形、策略和测量等，并符合 RFC 2475 的规定。

（1）分类

设备必须支持基于多种方式对数据流进行分类功能。基于以下字段的包分类：

- IPv4 及 IPv6 的 DSCP
- 用户会话接入的物理/逻辑端口
- 源 IP 地址
- 目的 IP 地址
- IP 协议
- 源 TCP/UDP 端口
- 目的 TCP/UDP 端口
- 802.1P
- 802.1q
- TCP flag
- ICMP type
- 用户帐号（每 PPPoE 或 PPPoA 会话）
- SVLAN
- MAC 地址

（2）标记及其映射

基于前述的分类字段，设备必须提供对 DSCP、802.1P 或 MPLS EXP 字段进行标记的手段，并支持三者之间的相互映射。

设备必须支持 SVLAN 环境中内、外层 VLAN 标签间 802.1P 的双向（内层到外层，外层到内层）映射。

如果某个用户有多条 PVC，设备必须支持 DSCP 与特定 PVC 的映射。

必须支持 RFC 3270 中对 MPLS QOS 的定义，要求支持 Uniform mode、Short pipe mode、Pipe mode。可以针对内层和外层 MPLS 标签单独设置标签 EXP。

（3）速率限制

设备必须具备在任意端口、会话、用户和应用流上应用（加载）策略的能力，支持对物理端口、每个用户/子端口的流量进行限速，要求颗粒度最少 64k，速率限制误差小于 5%。

设备必须支持入方向和出方向的速率限制，对超过限制要求的流量能选择处理方式，如允许转发、丢弃、修改优先级等。

应支持基于 VLAN 和用户的二级限速功能。

（4）带宽保证

设备必须支持针对每个会话可以提供最小保证的带宽。必须支持 RFC2697 和 RFC2698 中规定的单速率三色标记（1R3C）和双速率三色标记（2R3C）的业务合同参数，以及不同情况下的令牌桶算法规定。

（5）流量整形

设备必须支持每个终结和非终结 PPP 会话的流量整形。

设备必须支持对每个 L2TP/GRE/IPSEC 隧道的流量整形。

设备必须实现对每个队列的整形能力。

(6) 统计和计费

设备具备对实施分类后的数据包进行统计的手段。

设备必须支持 RADIUS 扩展属性实现带宽、等级、流量、时长等 QoS 参数的原始计费信息上传给 RADIUS 服务器。

(7) 动态调整 QoS 策略

设备必须支持 COPS 协议、DIAMETER 或 RADIUS 协议，实现动态带宽控制和管理。设备必须能够基于由外部策略服务器（如策略决策点）提供的信息，利用 COPS 协议、DIAMETER 或 RADIUS 协议，动态改变在 ATM 层、IP 层和 PPP 层的策略及整形等 QoS 参数，而无需重建会话。

设备必须支持向 QoS 业务平台通知状态（如申请/释放 QoS 资源的结果、用户掉线异步通知等）。

(8) 队列要求

设备必须支持将不同等级的业务映射到相应的队列中，并为每个队列配置相应的带宽保证和转发优先级。

设备必须支持严格优先级和轮询等队列技术，可保证严格优先级队列的带宽和延时，并按比例为轮询队列分配带宽。

设备必须支持速率限制，设备应支持 Tail-Drop、RED、WRED 等拥塞避免技术。

设备必须达到每个逻辑端口进出方向支持的队列数都不小于 8 个。每用户支持不少于 4 个业务队列并实施不同的质量保证和控制，要求至少有一个是严格优先队列。

BRAS 是 QoS 保证和控制的关键点，必须具备足够的数据缓存来实现。要求支持双向的数据缓存。

(9) 层次化 QoS 的要求

设备必须支持层次化 QoS，对于每个用户，设备必须提供至少 4 个独立的用户优先级别。

设备必须支持感知 Diffserv 的分级调度器（见 DSL Forum TR-059）以避免接入网中在设备与 RG 之间任何潜在的拥塞。

设备应符合 TR-059 描述的层次化 QoS 处理的主要过程：

- BRAS 感知流量类型，并且根据流分类结果把流量分别打入不同的 Session 队列，同时根据配置或策略对不同的流分别进行流量监管和限制，

并支持如 PQ/CQ/LLQ/WRR/CBWFQ 等多种调度算法；

- 物理端口调度器根据端口速率从下属调度器（VP 调度器）“pull”报文，同时根据配置或策略对不同 VP 分别进行流量监管和限制；
- 每个 VP 调度器将得到调度，同时每个 VP 调度器根据 VP 速率从下属调度器（VC 组调度器）“pull”报文，根据配置或策略对不同 VC 分别进行流量监管和限制；

按照这个方法，VP 调度器、VC 调度器、Session 调度器将依次得到调度，一旦 Session 调度器得到调度，它将从对应 Session 队列中“pull”一个报文，并让报文从 BRAS/路由器的物理端口发送出去。

设备中的分级调度器必须能够对至少两层 ATM 节点进行拥塞点的建模，如果设备不包括 ATM 交换功能，则设备中的分级调度器必须能够对至少三层 ATM 节点进行拥塞点的建模。

设备中的分级调度器必须能够对至少两层以太网节点进行拥塞点的建模。

分级调度必须能够有效利用资源，任何等级流量必须可以使用分配给其它等级流量的未使用带宽。

设备中的分级调度器必须能够结合某条 ADSL 线路的同步速率来为相应的 VC 实施流量调度。

设备中的分级调度器必须能够基于网络拓扑模型对下行流量进行整形以保证下行的二层端口无拥塞。

（10）对多 PPPoE SESSION 的 QOS 保证

必须支持单 VLAN 多 PPPoE SESSION 的 QOS 保证，建议支持多 VLAN 多 SESSION 的 QOS 保证。

（11）ATM 流量管理

设备必须支持 VBR 服务的超额订购。

设备必须支持每 VC 排队（queuing）。

设备必须支持层次化的 QoS。

设备必须支持每 VC 的信元整形以符合该 ATM PVC 所对应的流量描述，这些流量描述由其使用的 ATM 服务等级定义，包括 PCR、SCR、MBS 等。

设备必须支持双漏桶信元整形。

设备的性能在流量整形开启时必须不受任何影响。

设备必须在 VC 和 VP 层次同时支持对于从 BRAS 发出或对于穿透 BRAS（ATM 交叉互联）的 ATM 流量进行整形。

设备必须支持在 ATM 流量交叉互联时的早期包丢弃（early packet discard）。

6.2 QoS 能力

要求队列数量大于等于 8k 个/单板。端口队列数量大于 8 个/物理端口，ACL 大于 3000 个/物理端口。建议至少支持单向 32Mbyte/GE 端口、128MB/OC-48 端口的数据缓存。最大延时小于 100us、最大抖动小于 30us，要求每队列带宽保证误差小于 5%。

与外部的策略服务器直连且无阻塞时，设备必须支持并应用每秒至少 50 条策略的改变。

策略规则由策略条件和策略动作构成，设备必须支持对每个用户加载 10 个策略规则或者整机支持至少 10,000 个策略规则的应用。

设备必须能够在每个端口（任意的物理或逻辑端口）应用至少 2 个策略（进和出方向，每个策略包含至少 10 个规则），而不影响设备的性能。

设备的性能在流量整形开启时必须不受任何影响。

层次化 QoS 指标：

- 调度器的层次最少要求有四个层次，理想是五个层次；各个层次调度器的数目视系统规格而定，例如子端口调度器的数目就和支持层次化 QoS 的物理端口数目相等。设备的 GE/10GE 接口必须支持物理端口、SVLAN（外层 VLAN）、CVLAN（内层 VLAN）、用户不同业务流四个层面的 QoS 队列管理和调度。
- 队列的层次、各个层次的队列数目、队列的深度。理想情况下，每个层次都有队列，即有 5 层队列，最低层次必须要有队列。一般要求层次化 QoS 能够缓存 200ms 的报文数目。
- 拥塞处理——调度器或队列之间的调度。理想情况下，在每个层次需要能够灵活支持 PQ、CBWFQ 等调度算法。
- 拥塞避免。进队列前需进行 RED 或 WRED 处理。设备必须支持基于 IP Precedence、DSCP 的 WRED，必须支持能根据 IP Precedence、DSCP 值执行相应的拥塞处理能力。
- 流量监管和整形。需要在每个层次进行流量监管或整形。
- 优先级域的映射。BRAS/路由器需要能够根据流分类后的报文优先级，设置报文二层头中的优先级域，保证“实时性”业务对时延和时延抖动的需求。
- 设备必须支持基于类（基于队列）的限速能力，即实现对每个队列的最高速率限制。
- 统计。为了提高可维护性以及满足计费需求，在层次化 QoS 处理过程中，

需要能够在每个层次统计被“pull”和“discard”的报文数目和字节数。

7 路由功能

设备必须支持静态路由和动态路由。

根据是否在一个自治域内部使用，动态路由协议分为内部网关协议（IGP）和外部网关协议（EGP）。自治域内部采用的路由选择协议称为内部网关协议，外部网关协议主要用于多个自治域之间的路由选择。

内部网关协议（IGP）用作在特定 AS 内部路由器间分发路由信息。对特定 IGP 算法的实现相对独立，但必须实现下列功能：

- 能迅速反映 AS 内部拓扑的改变；
- 提供一种机制使链路振荡时不引起连续的路由更新；
- 提供快速收敛成无环回（loop-free）路由；
- 使用最少的带宽；
- 提供等价路由以便负荷分担；
- 提供一种认证的路由更新方法。

设备除实现静态路由外，必须实现 OSPFv2，IS-IS，RIPv1/2。

外部网关协议在自治系统间使用，为特定自治系统内一组网络与相邻自治系统交换可达性信息。设备必须实现 BGP4。

设备必须支持静态路由、动态路由（包括 RIP、OSFP、IS-IS、BGP4 等）的负荷分担和冗余功能。

必须支持 BFD 功能，包括 BFD for 静态路由、BFD for Vlan、BFD for OSPF、BFD for ISIS、BFD for BGP、BFD for LDP。基本功能应符合 draft-ietf-bfd-base-08 规定的各项要求，包括 BFD 检测的承载协议及使用的端口号，BFD 的包类型、包格式，检测模式、发送周期及检测时间、参数修改过程、会话初始化和建立等内容；应支持 draft-ietf-bfd-v4v6-1hop-08 和 draft-ietf-bfd-multihop-06 的相关规定。

必须支持 OSPF/ISIS/BGP/LDP 路由协议的 NSR 功能，当设备在当前激活的主路由引擎或软件突然失效而进行主备切换时，能够保持路由协议的稳定性和数据包持续的转发。

必须支持 POS 对 SDH Section、Line 和 Path 故障信号的检测支持，并根据这些信号触发 IP 接口状态，触发机制和相关时间参数可以配置。

建议设备根据传输误码率判断链路状态的能力。

必须支持 SPF 计算中的快速收敛 ISPF 和 PRC 算法。

建议设备支持 OSPF/ISIS/BGP 路由协议的 NSR 功能，当设备的路由相关部

件出现故障时，仍能维持配置了路由协议的端口能够与邻居保持一定时间的 keepalive。

建议设备支持 IP FRR 功能，能够将备份路由表下发到转发表中。

7.1 开放最短路径优先 OSPF

设备必须支持 RFC 2328 规定的 OSPFv2 路由协议的全部功能和要求，其中包括：链路状态数据库、自治系统内对区的分割、域内路由功能、自治系统外部路由的处理、路由协议包格式、基本功能实现要求（定时器、IP 组播包接收和发送、可变长子网掩码支持、IP 超网支持、低层协议支持、非广播低层协议支持、操作原语列表、激活其它过程的任务支持）、协议数据结构、区数据结构、邻居路由器状态维护、收发协议包的处理、接口数据结构、邻居数据结构、路由表结构、LSA 包数据结构及处理、虚链路要求、路由表计算等。

设备必须支持如下 OSPF LSA：

- type1: router-LSA;
- type2: Network-LSA;
- type3: Network Summary-LSA;
- type4: ASBR Summary-LSA;
- type5: AS-External-LSA;
- type6: Group Membership LSA;
- type7: NSSA External LSA;
- type8: External Attributes LSA;
- type9: Opaque LSA (link-local scope);
- type10: Opaque LSA (area-local scope);
- type11: Opaque LSA (AS scope)。

设备在满足作为 stub 路由器的条件下，必须能发布 OSPF Stub Route。

设备必须能够实现作为 ABR 和 ASBR 的功能。

设备建议支持 RFC 3623 规定 OSPF Graceful Restart 功能。当路由控制平面重新启动时，网络拓扑未发生变化，则必须启动 OSPF Graceful Restart 过程；若检测到网络发生了变化，则必须能转换到正常到 OSPF Restart 过程。路由器必须能够实现 Graceful Restart 的发起者功能，也必须能够在作为 Graceful Restart 发起者的邻居时，运行在 Graceful Restart helper mode 模式下。无论作为 Graceful Restart 的发起者还是 Helper。设备必须提供 OSPF Graceful Restart 的后向兼容能力，能够感知在邻居无法作为 helper 时，进入正常的 OSPF Restart 状态。整个 Grace Restart 过程必须符合 RFC3623 的规定。

必须支持 OSPF 的 NSR 功能，当设备在当前激活的主路由引擎或软件突然

失效而进行主备切换时，能够保持路由协议的稳定性和数据包持续的转发。

必须支持 OSPF 在 BGP/MPLS IP VPN 网络环境中，在 PE 和 CE 之间启用 OSPF 协议时的操作要求；必须支持在一个 VPN 的两个 PE 上的 VRF 之间建立 sham Link 的功能；要求支持的 OSPF Instance 数量不少于 VR 数量。

在启动了 OSPF 的邻居之间必须支持协议消息的保密认证功能。

必须支持 OSPF 多路径负载分担，其分担误差要求在 10%之内。

必须支持对路由协议优先级/管理距离的调整。

必须支持 OSPF 多进程。

7.2 中间系统到中间系统 ISIS

设备必须实现在 RFC1142 中规定的 ISIS。

设备必须遵守 RFC1195 中的规定，包括：与子网无关的功能，与子网相关的功能，PDU 的结构和编码，路由信息的类型和编码，序列号分组编码及路由算法。对路由信息的 QoS 设置必须符合 RFC2474 中的规定。

设备必须支持 RFC1195 中的 IS-IS 路由信息的简单认证功能和 RFC3567 中的加密认证功能，以保证路由信息的安全。

在点到点链路之间建立 ISIS 链路时，必须通过 3 次握手机制实现，实现方式应符合 RFC3373 中的规定。

必须支持 RFC2763-ISIS 的动态主机交换机制规定的 Dynamic hostname TLV(类型 137)，以便于运维管理。

必须支持 RFC 2966 规定的 Domain-wide Prefix Distribution with Two-Level ISIS 功能；必须支持 Level2 到 Level1 的路由泄漏特性。

必须支持 RFC3277 ISIS Transient Blackhole Avoidance 功能，即在重启时，给建立了邻接关系的路由器快速发出带有 Overload bit 置位的 LSP 消息，在该路由器同步路由数据库完成后，再次发布 LSP 消息时，应清除 Overload bit 原置位。

必须支持 ISIS 多路径负载分担及其管理，分担误差在 10%之内。

必须支持 RFC 3847 中规定 ISIS 的重启信令，即增加相关的定时器 T1/T2/T3，及 Restart TLV（类型 211），在重启（或启动）的设备及其邻居在重启（启动）过程中的操作（如邻居的获得、多层间操作、数据库同步等），要符合该 RFC 文档的规定。

建议支持在 RFC3784 和 RFC4205 中规定扩展 TLV 及其 sub-TLV，其中（1）—（3）为 IS-IS 用于 TE 的扩展；（4）则为 ISIS 用于 GMPLS 的扩展。

（1）extended IS Reachability TLV（类型 22）及其 sub-TLV（子类型 3,4,6,8-11,18, 20, 21）；

- (2) extended IP Reachability TLV (类型 135);
- (3) The TE Router ID TLV (类型 134);
- (4) shared Risk Link Group (类型 138)。

7.3 路由信息协议 RIP V1/2

设备必须支持 RIP version 1/2。

设备必须支持 RFC 2453 RIP Version 2 规定的各项功能要求、各项协议消息封装格式、协议算法。

设备必须支持 RFC 2091 的规定，以保证 RIPv2 在与邻接设备通过面向连接的链路连接时的可用性。

设备必须支持只向客户 CPE 发送 RIP 更新，但不接收由 CPE 传来的更新。

设备在启用 RIPv2 版本时，必须支持与 RIPv1 版本的后向兼容

设备必须支持 RIPv2 的加密认证功能。

7.4 边界网关协议 BGP4

设备必须实现在 RFC4271 中规定的 BGP4。必须符合其规定的全部功能和要求：

(1) 符合路由发布和存储规定；

(2)符合 BGP 各类消息包(OPEN、UPDATE、KEEPALIVE、NOTIFICATION 和 ROUTE- REFRESH 消息类型) 格式规定，并支持 BGP 各类消息包所包含的内容。

对于 OPEN 消息，必须支持 RFC 4271 第 4.2 节的规定，同时必须支持 RFC3392 中规定的的能力选项格式，建议支持 draft-ietf-idr-restart-13.txt 中的 BGP Graceful Restart 的能力选项参数规定；

对于 UPDATE 消息，必须支持下列 Path Attribute（通道属性）类型：

- Type Code 1: ORIGIN
- Type Code 2: AS_PATH
- Type Code 3: NEXT_HOP
- Type Code 4: MULTI_EXIT_DISC
- Type Code 5: LOCAL_PREF
- Type Code 6: ATOMIC_AGGREGATE
- Type Code 7: AGGREGATION
- Type Code 8: COMMUNITY
- Type Code 9: ORIGINATOR_ID

- Type Code 10: CLUSTER_LIST
- Type Code 14: MP_REACH_NLRI
- Type Code 15: MP_UNREACH_NLRI

其中, TypeCode1~7 必须符合 RFC4271 中第 4.3 节和第 5 章的相关规定。

对 TypeCode8—COMMUNITY 属性值的范围、操作、聚合和使用, 必须符合 RFC 1997 的规定, 属性值应可配置。

TypeCode 9、10 是路由反射功能实现时, 避免出现路由信息环路使用的, 其格式和使用, 必须符合 RFC4456 的规定。

TypeCode 14、15 则用于 BGP-4 的多协议扩展, 参见下面的第 (4) 点。

对于 KEEPALIVE 消息, 必须支持 RFC4271 第 4.4 节的规定。

对于 NOTIFICATION 消息, 必须支持 RFC4271 中第 4.5 节中对错误码和错误子码的规定和第 6 章对各类 NOTIFICATION 消息的处理, 必须支持 RFC4486 的 Cease Notification 的 8 个子编码 (subcode) 的定义和处理。

对于 ROUTE-REFRESH 消息, 消息格式和操作过程必须符合 RFC2918 中的规定。

- (3) 符合 BGP 版本协商的规定;
- (4) 符合 BGP 中有限状态机规定;
- (5) 符合 BGP 内所有定时器相关规定。

设备除了支持基于 AS 配置 BGP, 还必须支持能够实现基于 community 配置 BGP, 相关措施应该符合 RFC 1998 的规定。

设备必须支持 BGP 路由振荡抑制, 符合 RFC 2439 的规定。提供限制发布路由的相关定时器; 支持实现稳定发布路由的方法; 所有的定时器参数及动作均应可配置。

设备必须支持 BGP-4 多协议扩展, 必须支持多协议可达 NLRI 属性

(MP_REACH_NLRI, type code 为 14) 和多协议不可达 NLRI 属性

(MP_UNREACH_NLRI, type code 为 15), 对这两个属性的编码格式、后续地址族标识(单播、多播、组播)、发布和处理, 以及错误码的处理均要符合 RFC2858 的规定; 网络层协议为 IPv6 的 BGP 多协议扩展则必须支持 RFC 2545。

设备必须支持自治系统联盟的功能, 支持 RFC3065 中规定的 AS_PATH 新增段类型, 即 AS_CONFED_SEQUENCE (value=3) 和 AS_CONFED_SET (value=4), 相关的操作、管理、兼容性、部署等均要符合 RFC3065 中的规定。

设备必须支持 RFC2385 定义的, 新增 TCP 选项携带 MD5 摘要, 通过 TCP 的这项扩展功能增强 BGP 的安全性, MD5 加密涵盖的内容、相关语法、发送/接收操作, 以及有关面向无连接复位的处理、性能、TCP 头的长度、MD5 算法、

密钥的设置等，必须要符合 RFC2385 中的规定。

设备必须支持 IBGP 路由反射功能，其路由反射的操作、路由反射器的备份、路由信息环路的避免等过程，均必须符合 RFC4456 的规定。

设备必须支持在 BGP-4 消息中携带 MPLS Label 的功能，有关标签携带和功能实现方式均必须符合 RFC 3107 的规定。

设备必须支持在 BGP/MPLS IP VPN 环境中，通过 BGP 分发 VPN 内部的路由，并保证来自各不同 VPN 的路由清晰明了，且是隔离（并保证不同 VPN 地址重叠时路由分发不受影响）；必须支持 PE 之间路由反射；必须支持不限制 CE 和 PE 之间 VPN 路由操作，即当 CE 和 PE 之间为静态路由、或 RIP、或 OSPF 时，必须支持 BGP 与相应路由协议的重分发，也必须支持 CE 和 PE 之间为 BGP Peer 时的路由学习；必须支持骨干为多 AS 时的 VPN 路由的分发；所有的操作必须支持 RFC 4364 的规定。

设备必须支持 IBGP/EBGP 多路径负载分担，分担误差在 10%之内。

必须支持灵活丰富的路由控制和过滤功能。

建议支持 BGP 的平滑重启功能，其能力消息格式、发起者和接收者的操作过程、状态转换等应符合 RFC4724 的规定。

7.5 VR 功能

设备必须支持虚拟路由器（VR）相关功能：

设备必须支持每个 VR 有自己独立的路由信息表（RIB），转发信息表（FIB）以及管理信息表（MIB）。单个 VR 必须支持多 IP POOL，多个 Loopback 地址。

设备必须支持所有 Session/PVC 可以终结在一个 VR 上。必须支持 Session 可以动态或静态地与 VR 实现绑定。

设备必须支持根据域名、VC、VLAN 或端口类型实现 VR 的绑定。

设备必须支持同一端口捆绑多种业务封装（PPPoE、1483B、1483R），并绑定到不同的 VR。

设备必须支持 RADIUS 请求报文的本机 IP 地址标识可配置。

设备必须支持无域标识及无指定 VR 的用户业务由 default VR 处理。

8 MPLS 及 VPN 功能

8.1 MPLS

设备必须支持 RFC 3031-Multiprotocol Label Switching Architecture。

设备必须支持 RFC 3032-MPLS Label Stack Encoding。

设备必须支持 RFC 3036-LDP Specification。

设备必须使用 RFC 3036 中的 independent label distribution control。

设备必须支持 RFC 3036 中定义的 Downstream Unsolicited label distribution。

设备必须支持 RFC 3063-MPLS Loop Prevention Mechanism。

设备必须支持 RFC 4090 中规定的 LSP 的快速重路由能力。

设备必须使用 RFC 3031 中的 liberal label retention。

设备必须支持 RFC 3270 定义的 E-LSP。

设备必须支持 RFC 2858-Multi-protocol Extensions for BGP-4。

设备必须支持 BGP Site of Origin。

设备必须支持 BGP AS Override。

设备必须支持 LDP 过滤。

设备必须支持 RFC 3209-RSVP-TE: Extensions to RSVP for LSP Tunnels。

设备应支持基于标签对数据包的转发，并可通过手工配置或标签分配协议（LDP）建立 LSP。

设备必须支持 3 层标签（标签堆叠）。

设备必须支持 RFC 3270 定义的 L-LSPs。

设备支持把 MPLS 封装在 GRE 中。

8.2 L2 VPN

8.2.1 L2TP

设备必须支持 L2TPv2，符合 RFC 2661；建议支持 L2TPv3，符合 RFC 3931；

设备必须支持 RFC 2661，Layer Two Tunneling Protocol 中定义的 L2TP over the User Datagram Protocol （UDP） over Internet Protocol （IP） （UDP/IP）。

设备必须支持 RFC 2809 Implementation of L2TP Compulsory Tunneling via RADIUS，通过 RADIUS 实现强制隧道。

设备必须遵循 RFC 2868，支持隧道协议的 RADIUS 属性。

设备必须遵循 RFC 2867，支持 RADIUS 的隧道计费。计费信息应包括用户名、Session ID、主叫 ID、Tunnel 类型、Tunnel 媒介类型、Tunnel 客户端终结点、Tunnel 服务器端终结点、出/入字节数、连接时间、出/入数据包数、丢包数、和 Tunnel 撤除原因等。

设备必须可以作为 LAC。

建议设备可以作为 LNS。

建议设备支持 L2TP tunnel switching，允许终结在 L2TP LNS 上的会话和另一个从 L2TP LAC 发起的会话之间交换数据包。

设备必须支持使用设备的 loopback 地址发起和终结 L2TP 隧道。

设备必须支持每个 VR 中多个 loopback 地址。

设备必须支持 RFC 3145，L2TP Disconnect Cause Information。

设备必须支持 RFC 3193（Securing L2TP using IPsec），即支持结合 IPsec 加密的 L2TP 隧道。

8.2.2 LAC 和 LNS

当 BRAS 作为 LAC 时，必须允许 LNS 强制 LCP 重协商。BRAS 必须支持 RFC 2661 中所有有关代理 LCP 和鉴权 AVPs 的 LAC 及 LNS 功能。

设备必须支持静态和动态的隧道建立。静态隧道建立指 L2TP 隧道在正确配置后即建立，动态隧道建立指 L2TP 隧道在有相应的 PPP 会话要求时才建立。

当作为 LAC 使用时，设备必须能够将来自 PPPoA，PPPoE 和 L2TP 的 PPP 会话汇聚到单个 L2TP 隧道中，详见 RFC 2661。

设备必须支持在物理或逻辑端口上的多个 L2TP 隧道。

设备必须支持静态配置及通过 RADIUS 返回多个隧道参数。

设备必须支持隧道组，在一对 LAC 和 LNS 之间可以创建多个 L2TP 隧道并被指派到一个隧道组中。设备必须支持将一个隧道配置为承载多个 FQDNs（domains/realms）PPP 会话。

设备必须支持根据 RADIUS 返回的 Tunnel Server Endpoint 属性将 PPP 会话终结到 LNS 或者 LNS 组。

设备必须将所有的 PPP 用户 ID 和认证信息通过 L2TP 隧道传递给 LNS。

如果 PPP 会话和 L2TP 隧道已经达到最大数量（每端口，每设备等），设备必须拒绝新的 PPPoE 或 PPPoA 会话。

如果 L2TP 隧道中已经没有 PPP 会话，设备必须能够动态终结该隧道。

设备必须支持在隧道组或者 LNS 组内均衡分配 PPP 会话。

设备必须支持按照严格优先级使用隧道承载 PPP 会话，当隧道组或者 LNS 组中的第一条隧道充满时，才开始使用该组中的第二条隧道。

设备必须支持基于权重在多个隧道之间对 PPP 会话进行负载平衡（例如 75% 的会话请求使用隧道 1，另外 25% 使用隧道 2）。

如果隧道组中一条隧道失效，设备必须继续使用剩余的隧道对 PPP 会话进

行负载平衡。

如果 LNS 组中的一个 LNS 不可用, PPP 会话必须在剩余的 LNS 之间负载均衡。

设备必须支持动态增加或者删隧道组中的隧道而不影响其它的隧道及其中的 PPP 会话。

设备必须支持隧道组或者 LNS 组之间的故障切换。

8.2.3 基于 IP/MPLS 的二层 VPN

(1) 设备建议支持 PWE3, RFC 3985 规定的 PWE3 体系架构的规定, 满足 RFC 3916 规定的 PWE3 需求。

(2) 设备建议支持以下业务:

- ATM over MPLS
- Frame Relay over MPLS
- PPP/HDLC over MPLS
- Ethernet over MPLS

(3) 设备建议支持点到点的 L2 MPLS VPN (即 PPVPN)。

- 如果设备采用 Martini 方式, 则遵循下列 RFC 标准的规定:

RFC 4906 - Transport of Layer 2 Frames Over MPLS, MPLS 上二层帧的传送;

RFC 4905 - Encapsulation Methods for Transport of Layer 2 Frames Over MPLS, MPLS 上二层帧传送的封装方法。

- 如果设备支持 Kompella 方式, 则遵循下列 RFC 草案标准的规定:

draft-kompella-ppvpn-l2vpn-04, 隧道上的二层 VPN。

(4) 设备必须支持多点方式的 L2 MPLS VPN (即虚拟专用 LAN 业务 VPLS)。

- 如果设备采用 Martini 方式, 则遵循下列 RFC 标准的规定:

RFC 4762 - Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling.

- 如果设备支持 Kompella 方式, 则遵循下列 RFC 标准的规定:

RFC 4761 - Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling.

设备必须支持以下三种方式接入 VPLS: 基于物理端口方式, 基于 802.1Q

方式；基于 QinQ 方式。建议支持两种外层隧道方式：LDP 和 RSVP-TE。

建议支持二层组播功能，即基于 VC 的 IGMP snooping/proxy,以及基于本地 AC 的 IGMP snooping/proxy。建议支持组播快速加入和快速离开功能。

建议支持分层的 VPLS（即 H-VPLS）。

建议遵循 ITU-T Y.1731 和 IEEE 802.1ag，全面支持 OAM 功能。

8.2.4 BRAS 对二层 VPN 的终结功能

- (1) 建议 BRAS 支持 VLL 接入终结功能，并能够根据用户接入信息，将二层 VLL 隧道终结至不同的业务 VPN 中；
- (2) 建议 BRAS 支持 VPLS 接入终结功能，并能够根据用户接入信息，将二层 VPLS 隧道终结至不同的业务 VPN 中；
- (3) 建议 BRAS 支持将 L2TP 隧道终结，并能够根据用户接入信息，终结至不同的业务 VPN 中；
- (4) 建议 BRAS 支持将 IPsec 隧道终结，并能够根据用户接入信息，终结至不同的业务 VPN 中。

8.3 L3 VPN

8.3.1 MPLS VPN

设备必须支持 RFC 4364 定义的 BGP/MPLS VPN。

当使用 RFC 4364 来提供基于网络的 IP VPN 时，设备必须支持在 PE-CE 连接上的以下协议：

- BGP
- OSPF
- RIP
- 静态路由

当使用 RFC4364 来提供基于网络的 IP VPN 时，设备必须在 PE-CE 连接上支持 IS-IS。

设备必须能够同时作为 RFC 4364 中定义的 PE 路由器和 P 路由器。

设备必须支持对从 CE 学习到的路由数目进行限制。

设备必须支持在从 CE 学习到的路由数目超过限制时告警。

设备必须支持每 VRF 的 Loop back 端口。

8.3.2 IPSec

必须支持 IPSec 协议，符合 RFC2401-2412 的规定。路由器应实现的安全性包括隧道模式和透明模式。符合 RFC2402（IP 身份验证头）中对 AH 的规定，符合 RFC 2406（IP 封装安全性净荷 ESP）中对 ESP 的规定。符合 RFC2409（IKE）规定的密钥管理协议。

支持 DES、3DES 和 DES56 等（RFC1829、RFC1851、RFC2420）加密算法，并且加密由硬件实现，不影响设备性能。

8.3.3 GRE

建议支持 RFC 2784 规定的 GRE 标准，支持 IPv4 GRE 封装，符合 RFC1702。

9 组播

设备必须实现 RFC 1112，必须实现 RFC 2236 规定的 IGMPv2，建议实现 RFC 3376 规定的 IGMPv3。设备必须支持对 PPPoE 用户的 IGMP 控制协议，必须支持 IGMP Proxy。

设备必须支持 RFC2362，PIM-SM 模式。必须支持 PIM-SM 中的 RP 自动发现。设备必须支持 PIM-DM、MSDP 等组播协议。设备必须支持 IP 定源组播（Source-Specific Multicast-SSM）。

设备必须支持基于 PPP、VLAN、PVC 和端口的组播包复制。

设备必须支持 IGMP FastLeave 功能。

设备所支持的三层功能必须同样适用于组播，例如速率限制和过滤等。

设备须具有灵活的组播业务控制机制，如组播组访问控制、组播用户数限制、每个用户加入的组播组数限制等。能通过 Radius 属性提供灵活的组播业务控制，可控制每个用户的组播权限、控制每个用户的组播带宽和 QoS。建议通过策略控制平台提供灵活的组播业务控制。

设备必须支持 PIM-SM 隧道。设备必须实现 RFC 4364 中描述的组播 VPN 业务。

设备支持由 RPT 模式切换到 SPT 过程中不丢包。支持包转发依赖硬件完成，不影响主控板的 CPU 性能。必须支持对组播流量的 QoS 功能而不影响性能。

为支持 IPTV 业务，BRAS 设备还需具备以下功能：

设备必须支持静态用户组播业务权限控制功能，设备根据配置时是否关联业务权限来识别组播用户。支持 Radius 提供动态返回组播权限功能和控制端口上的

动态加入的功能。

设备必须支持 PPP 接入用户的组播认证计费功能，包括对该 PPP 用户的动态组播加入业务权限控制和面向该 PPP 连接的组播流复制，计费功能同普通 PPP 上网用户。

设备必须支持 DHCP 接入用户的组播认证（利用 Option60 或电路认证）计费功能，包括对该 DHCP 用户的动态组播加入业务权限控制和面向该 DHCP 用户接入电路连接的组播流复制，计费功能同普通 DHCP 上网用户。

设备必须支持 STB IPoE 接入，DSLAM 复制时用户侧动态组播加入功能。

设备必须支持组播用户接入封装类型包括：Ethernet，VLAN，ATM Bridge，Router。

设备必须支持对上送到控制层处理的 IGMP、PIM 等组播协议报文进行限速，防止产生组播攻击。

设备必须支持组播业务防盗用，在组播用户进行 IGMP 接入请求操作时，对用户的电路，MAC 地址，源 IP 地址，PPP Session ID 进行一致性检查，只有检查通过才允许加入组播组。

设备必须提供动态组播 QoS 功能，在用户加入组播组后，自动按配置对该用户的单播流进行限速。或通过动态修改用户带宽或业务流优先级方式保证组播流优先转发。

设备应能提供组播 VLAN/VC 功能，为 DSLAM 复制提供组播数据。当用户通过 IGMP 加入组时，数据（一份）通过组播 VLAN/VC 传递到 DSLAM，由 DSLAM 复制给最终用户。

设备必须支持端口及用户上加入组播组数目限制，通过配置命令可以控制端口及用户下允许加入组播组数目。

设备必须支持用户的频道访问权限功能，频道访问权限分为禁止、预览和允许三种。频道预览应能够配置针对单次预览的持续时长、预览次数、预览间隔时长以及预览总时长参数。

设备应支持组播源地址检查功能，以避免在用户端口下存在多个 STB 时单一 STB 离开某组播组造成的观看同一组播组的其他 STB 点播中断的现象。

设备建议支持根据用户申请带宽的使用情况对组播请求进行接纳控制，当用户的剩余带宽不够时，用户的组播请求应不成功。

设备应支持 CDR（Call Detail Record）呼叫信息记录功能，记录用户的基本访问信息（包括 IGMP 请求成功/失败，用户标识，何时加入，何时离开，离开方式（强制、自主离开），访问的频道，频道权限，CDR 记录产生时间等）。

设备应支持 CDR 信息定时同步到 RADIUS 或 IPTV 业务管理系统，确保 CDR

信息不丢失。

10 IPv6

建议设备支持 IPv6 协议，主要包括 IPv6 数据包线速转发，IPv6 动态路由协议，以及支持用户 IPv6 PPP 拨号：

建议支持 IPv6 基本协议，符合 RFC 2460 的规定。

建议支持 IPv6 地址结构的规定，符合的规定。

建议支持基于 IPv6 的邻居发现机制，包括路由器和前缀发现，地址解析和邻居不可达检测，重定向等功能要求，必须符合 RFC2461 和 RFC3122 中邻居发现部分。支持在同一链路上使用邻居发现协议来获知其他节点的存在，从而确定彼此的链路层地址，并发现路由器以及维护通向活动邻居的可达性信息。建议支持 RFC 4443 规定的 ICMPv6。

建议支持 IPv6 的 PPP 拨号，建议支持 RFC 2472 规定的 IPv6 over PPP，建议支持 IPv6 NCP over PPPoA and PPPoE，建议支持 IPv6CP。

用户 IPv6 地址的分配方式有三种：无状态地址自动分配、有状态地址自动分配和前缀代理方式。为适应不同的网络应用环境，BRAS 设备应支持这三种方式。对于单个 IP 地址的分配，BRAS 经 PPPoE、PPPoA 或 RADIUS 认证授权后，应支持无状态地址自动分配，符合 RFC2462 标准。还应支持主机经 DHCP 实现有状态地址自动分配，符合 DHCPv6 (RFC3315)，建议设备支持 RFC 3646，即在 IPv6 的 DHCP 协议中实现 DNS 自动配置。需要支持 DHCP Relay 功能。与 IPv4 地址分配不同，IPv6 地址分配除分配单个 IPv6 地址外，还应支持分配地址前缀。对于地址前缀的分配，CPE 路由器与 BRAS 之间采用前缀授权方式，符合 RFC 3633，IPv6 Prefix Options for DHCPv6。由 BRAS 分配给用户/48 到/64 长度的地址前缀。

建议支持 IPv6 静态路由和动态路由，支持的动态路由包括：ISISv6、OSPFv3、BGP4+、RIPng 等。

建议支持 IPv6 的静态路由。到特定目的地的静态路由由网络前缀定义。支持 IPv6 静态路由中附加信息，包括：前缀长度、对给定路由协议引入静态路由的特定度量。

对应于 IPv6 的路由协议，应支持 IS-ISv6 协议，应符合 RFC5308 中的规定。支持为适应 IPv6 协议增加的两个 TLV，即 IPv6 可达性 TLV 和 IPv6 接口地址 TLV。支持增加的 IPv6 协议标志符。实现 IS-IS 的 BRAS 应实现 IS-IS MIB，符合 RFC 4444 的规定。

建议实现在 RFC5340 中规定的 OSPFv3。支持 IPv6 OSPF 包格式，并直接运行在 IPv6 上。支持 LSA 选项字段中增加的两个选项比特：R 比特和 V6 比特。支持 LSA 的格式变化。在 LSA 头和路由器 LSA、网络 LSA 中删去所有地址语义，这两个 LSA 以网络协议无关的方式描述路由域的拓扑。支持新增加的用于分布 IPv6 地址信息的新 LSA，以及进行下一跳解析所需要的数据。符合 OSPFv3 MIB draft-ietf-ospf-ospfv3-mib-11.txt 的规定。

建议支持 BGP4+，符合 RFC2545 的规定。BGP4 用作传达 IPv6 可达性信息时下一跳属性可能需要包含全局地址以及本链路地址。用作构造 MP_REACH_NLRI 属性中下一跳域网络地址需要遵守 IPv6 特定的规则。满足在下一跳域 IPv6 地址中向对等实体传送下一跳全局 IPv6 地址，并且后接下一跳本链路 IPv6 地址。如果下一跳地址字段包含本链路地址，则地址长度值等于 32。

建议支持 RIPng，并符合 RFC2080 的规定。

建议支持 IPv6 端口的 CoS/QoS 分类，并实施 QoS 策略控制。

建议支持 IPv6 over L2TP over IPv4。建议支持 IPv6 LNS。

建议设备支持 IPv4 到 IPv6 的过渡机制，主要包括双栈方式、隧道方式及 NAT-PT/ALG 方式。

可选支持 IPv6 上的组播协议 PIM-SM，MLD 等。

建议设备硬件支持 IPv6 数据包转发，端口转发达到线速。

建议设备支持基于 IPv6 的 IPOE 接入认证方式。

11 性能要求

11.1 设备容量要求

(1) A 类：

系统交换容量（单向） $\geq 120\text{G}$ ；每槽带宽（单向） 10G ；

最大在线用户数 ≥ 48000 ；

最大配置用户数 ≥ 96000 ；

每用户保证带宽 200K ；

(2) B 类：

系统交换容量（单向） $\geq 60\text{G}$ ；每槽带宽（单向） 2.5G ；

最大在线用户数 ≥ 32000 ；

最大配置用户数 ≥ 64000 ；

每用户保证带宽 200K;

(3) VP/VC 数

每 ATM 端口 VP 数 ≥ 32 ;

单板 PVC 数 ≥ 8000 ;

整机 PVC 数 ≥ 64000 。

(4) 虚拟路由器数目

整机虚拟路由器 (VR) ≥ 64 。

11.2 呼叫处理能力

(1) 呼叫建立时间

呼叫建立时间指从用户终端发起 (PPPoE 或者 PPPoA) 呼叫到认证通过进行地址配置所经历的时间 (不包括和认证服务器之间的交互时间)。

呼叫建立时间 $\leq 3s$ (含 RADIUS 认证时间)

PPP 建链时间 $< 300ms$ (不含 RADIUS 认证时间)

(2) 呼叫建立速率

每秒至少能完成 100 个 PPPoE 或 PPPoA 的建立;

或:

PPP 每秒同时建链数: 每秒同时建链数 $>$ 标称最大活动会话数的 2%。

(3) 接通率

接通率: PPPoE 或 PPPoA 拨号接通/拨号总次数;

在本地认证前提下, 并发会话 (PPP Session) 数达到设备标称值 70% 时, 接通率 $\geq 99.99\%$ 。

注: 接通即用户认证通过, 正确获得 IP 地址或者 IPv6 地址前缀, 并能获得正常的网络服务。

平均呼叫接通率应大于 98%。

(4) 掉线率

10% 标称最大并发会话数占用率下 6 小时掉线率应小于 0.5%。

10% 标称最大并发会话数占用率下 12 小时掉线率应小于 1%。

90% 标称最大并发会话数占用率下 6 小时掉线率应小于 1%。

90% 标称最大并发会话数占用率下 12 小时掉线率应小于 2%。

(5) 最大并发会话数

- A、B 类 BRAS 的整机 PPP 最大活动会话数分别为 48K、32K, 配置用户数分别为 96K、64K。建议 10*GE 单板 PPPoE/IPoE 并发数支持 24000。

11.3 服务质量

(1) 包转发时延

1518byte 长度及以下包时延均应 $<1\text{ms}$ 。

(2) 丢包率

设备在轻载条件下（吞吐量 10%），丢包率应为 0。

设备在重载条件下（吞吐量 90%），丢包率小于 10^{-3} 。

(3) 设备吞吐量

当系统满负荷时，所有的端口必须能够以线速处理 40 字节的 IP 包。

设备转发引擎的吞吐能力，以 PPS（Packets Per Second）计，应等于设备有效配置的所有类型端口速率的总和。

PPS 性能必须足以满足所有被支持的端口以线速转发混合 IP 包。

11.4 路由表容量

路由表容量指路由器运行中可以容纳的路由数量。

设备必须支持至少 100K 条 FIB 表目，建议支持至少 250K 条 FIB 表目。

设备必须支持至少 100K 条 RIB 表目，建议支持至少 250K 条 RIB 表目。

平均每个目的地址至少可以提供 2 条路径。

设备必须支持至少 10,000 条 IGP 路由。

设备必须支持至少 300,000 条 BGP 路由。

设备必须支持至少 100 个 IGP 邻居，分别包括 OSPF 和 IS-IS。

设备必须支持每个 AREA 中至少 5000 条路由，分别包括 OSPF 和 IS-IS。

ISIS 单 Level 必须支持 1500 条 LSP、1 万条路由表处理能力。

设备必须支持至少 50 个 BGP 对等。

11.5 VPN 性能指标

(1) MPLS:

设备必须支持至少 10,000 个 LSP。

标签更新和收敛性能。A、B 类设备在 10 个 LDP 邻居的情况下，要求至少 200 个标签/秒的更新能力，单台设备时故障切换造成包转发中断时间小于 500ms。

建立和拆掉 LSP 的速度，要求大于 200 LSP/秒。

(2) 2 层 MPLS VPN

设备必须支持至少 8K L2 VPN。

(3) L2TP

设备必须支持至少 16K L2TP 隧道，32KPPP 会话。

设备必须在每个 VR 中支持至少 1000 个 L2TP 隧道。

设备必须在每个 L2TP 隧道中支持至少 8000 个 PPP 会话（不要求与上一项相关）。

设备在每个隧道组中必须支持至少 8 个隧道。

L2TP 的平均建立响应时间 < 10 秒。

至少有 50% 的标称 PPP 会话数可以建立 L2TP。

L2TP 连接保持时间 > 12 小时。

(4) 3 层 MPLS VPN

设备必须支持在每个 MPLS VPN 中支持至少 2,000 个用户站点参与双向动态路由协议。

要求 A 类 BRAS 支持至少 1000 个 VRF，VPN 路由表容量至少 10 万条；B 类 BRAS 支持至少 500 个 VRF，VPN 路由表容量至少 5 万条。

11.6 组播性能指标

组播数据的转发能力：设备必须支持端口上的组播复制为线速复制转发。

系统支持组播频道组播组：必须支持至少 8K 个组播组。

整机支持组播用户数：A 类 BRAS 至少达到 16000 用户，B 类 BRAS 至少达到 12000 用户。

系统组播路由表容量：必须支持至少 10K 组播路由。

组播加入离开性能：必须在 100 毫秒内完成对 IGMP 加入和离开信息的处理。

11.7 整机业务叠加性能

要求整机满配置下无阻塞交换，交换容量与端口配置容量之比大于 2，背板容量大于交换容量。（端口容量指可配置的最大数量端口的总带宽；交换容量指交换矩阵最大交换能力；背板容量指背板单位时间内可传输的最大数据量）。

设备在多种功能同时开启时对设备性能的影响不明显，且必须不导致业务质量的下降。

设备的业务叠加性能要求是指设备在用户数量和硬件满配置下，在提供 PPPoE 接入、IPoE 接入、专线接入、组播、MPLS 二三层 VPN 等业务并且针对全部在线用户提供 uRPF、ACL、QoS 等业务功能等情况下所具备的总体性能。

设备在满配并叠加各种业务时性能必须不能明显下降，时延和丢包都应很小，CPU 利用率不能过高，并且能够长期稳定地运行。

11.8 计费要求

BRAS 计费精度为 1s。

基于时长的计费误差不大于 1 分钟。

基于流量的计费误差不大于 1%，且最大不超过 1Mbyte。

在 RADIUS 记帐信息中，应可提供每个 PPP 拨号用户或者 VLAN 专线用户不同 QoS 等级的流量信息和丢包信息，同时也可以通过 SNMP 进行采集。

12 安全和可靠性

安全功能包括设备自身安全和设备所提供业务的安全。

12.1 设备自身安全

设备必须保证自身的安全性。设备的安全性主要基于设备自身系统安全、数据过滤、路由认证、异常流量识别和限制、异常报文的处理、安全监控等几个方面。设备要求有充分的安全措施，以保障系统的可靠及可用性和信息的完整性。

设备必须支持分级分权管理，不同的用户名和密码，授予不同的管理权限。

必须支持采用加密的方式进行安全的远程 Telnet 访问，如 SSH。

设备必须支持冗余服务器的故障切换机制，包括：

- RADIUS Server
- LDAP服务器（如果支持LDAP）
- COPS服务器（如果支持COPS）

设备必须支持标准五元组的 ACL（源 IP、目的地 IP、TCP/UDP、源端口、目的地端口），还必须提供基于 MAC 地址（包括目的和源地址）的访问控制策略手段。

设备必须具有防攻击的功能，可防止 DDOS 攻击、ARP 攻击、TCP 半连接攻击及恶意 ping 攻击等方式的攻击，能够限制这些攻击流量的带宽，并且保证已建立的用户连接保持正常工作，新的用户连接可以建立。在遭到攻击时，控制板和业务板的 CPU 利用率不会上升很多。

设备必须支持 RIP、OSPF、ISIS、BGP 等路由协议的 MD5 认证，保证路由信息的可信度。

设备必须具有良好的访问控制。对设备的所有网管操作都可配置为需要经过认证和授权方可进行。设备还必须支持 SNMP 的访问级别。

必须支持 RADIUS 进行网管登录口令认证，对口令进行集中管理。

必须支持网管日志，对超越权限或失败的关键操作进行登记并作为安全告警。设备必须提供安全性审计的功能，必须提供一种方法来记录配置的改变及操作人员改变配置的时间。

设备不允许存在未记载于文档的访问后门或通用密码。厂商必须确保这种用于调试或开发的访问途径在产品分销到客户手中之前已删除。

设备必须支持对 IP spoofing 的侦测和阻断。

设备必须支持对 IP 源路由选项攻击的侦测和阻断。

设备必须支持对 IP address sweep 攻击的侦测和阻断。

设备必须该支持对端口扫描的侦测和阻断。

设备必须支持防火墙功能。建议支持状态防火墙。

设备应在发现安全问题时，通过 SNMP Trap 方式发送简单报警信息，并通过 syslog 传送详细安全报警信息。

12.2 业务安全

在 DHCP 地址管理模式下，设备应有完善的 IP 地址盗用的防范措施。设备必须支持对每 PVC/VLAN 可分配的 IP 地址数量可配置，设备必须支持用户下线检测并及时释放 IP 地址。

设备应具有用户帐号和物理端口绑定功能，对 IP 上行的 DSLAM 用户进行唯一性标识。

设备应能对某一端口、某一 VLAN、某条 PVC 实现用户接入数限制功能。对于 ADSL 用户，设备必须支持限制每条 PVC 上最大允许接入用户数，包括 PPP 连接数限制。对于 LAN 接入用户，必须支持限制每个 VLAN 上最大允许接入用户数，包括 PPP 连接数限制。对于账号用户支持对用户允许的 TCP/UDP 连接数进行限制。设备必须实现对某一用户的四层连接数进行限制，限制数量的大小可配置，限制某用户的 TCP Session 数和单位时间里 TCP Session 的增长数。

设备必须具备控制单位时间内 Flow 连接的频率，该 flow 可以通过 ACL 类定义，频率可配置。例如 1 分钟内最多只能发起 5 个针对地址为 202.97.1.1 的信令服务器的 SIP 信令呼叫请求。

设备必须具有通过端口镜像方式实现对某用户、某 VLAN、某端口流量的监控的能力。

设备应提供灵活的、基于用户的 ACL 访问控制机制，开启 ACL 功能时对设

备性能的影响不大。设备应能提供防火墙包过滤功能，既只允许符合 ACL 条件的数据包通过，将不符合 ACL 条件的数据包丢弃。设备应具备根据以太帧中的 `ethertype` 字节进行包过滤的功能，并且不影响性能。

设备应具备针对某一用户、端口和子端口的严格的单播反向通道转发检查（strict uRPF）功能，要求开启 uRPF 时性能不下降。

设备应能够按照不同的用户权限向用户提供不同的接入能力。

建议具备业务感知的功能。

12.3 可靠性和可用性要求

设备必须具备 99.999% 的总体可用性（软硬件），例行维护时间不计算在内。

系统无故障连续工作时间（MTBF）必须大于 69,000 小时。故障恢复时间 < 30 分钟。

设备应提供过流、过压保护措施，保证器件不受损坏。设备应具有良好的散热性能。

所有部件必须支持热插拔。

必须允许对运行系统进行所有适当的配置更改和软件升级而不影响在线用户。建议支持不同业务转发板的端口备份。

设备应具备冗余性和容错性等安全措施，关键部件应采用冗余设计，以保证电信级的可靠性。设备中的所有部件必须能够提供 1:1、N:1 或分布式设备冗余能力，设备部件包括：

- 交换单元
- 包转发引擎
- 控制和路由处理器
- 物理接口模块，包括 APS（如 SONET GR253）的冗余能力。所有各种速率（up to OC-48）的 ATM、POS 和通道化接口模块必须支持 N:1 冗余
- 管理系统/管理接口
- 馈电接口
- 电源转换模块/供电单元
- 风扇

必须支持从故障板卡到冗余板卡的自动切换，建议手工切换作为选项支持。从主用电源到备用电源的切换必须是自动的，不能引起业务的中断。

设备必须支持以太网冗余，可以在 800ms 内恢复点对点的 GE 连接。

在切换到冗余控制板卡时，建议设备能维护 VC、PPP 或 RFC 1483/2684 会话的状态，并保持与之相关的所有功能或协议。

满配的设备冷启动后必须在 10 分钟内完全正常运作。

在有冗余配置的情况下，从机箱中抽走控制板卡时及重新插入控制板卡时，设备必须能够继续转发流量。

必须支持 BRAS 之间的冗余备份。

建议所有的以太网端口、POS 端口都支持双向故障检测协议 BFD 功能，基本功能应符合 draft-ietf-bfd-base-08 规定的各项要求，包括 BFD 检测的承载协议及使用的端口号，BFD 的包类型、包格式，检测模式、发送周期及检测时间、参数修改过程、会话初始化和建立等内容；应支持对单跳和多跳链路的 BFD 检测，符合 draft-ietf-bfd-v4v6-1hop-08 和 draft-ietf-bfd-multihop-06 的相关规定。应支持在 BFD 检测到链路故障时能够自动切换到预先设定的备份链路上。可以在同一 BRAS 上，指定互为备用的端口。检测周期可设定，可设为 10ms，连续检测 3 次。要求能与其他厂家的设备实现互通。

13 设备管理功能

13.1 基本管理功能

设备必须提供配套网元管理系统：

系统能自动发现设备，可以管理多台设备；

该系统可以通过图形化管理界面实现完全的配置操作，建议系统支持 WEB 方式进行配置管理；

该系统具有故障管理、配置管理、计费（accounting）、性能管理和安全管理（FCAPS）功能；

该系统能提供收集、显示、极限、编排、过滤、处理和清除等告警管理；

该系统能够收集、统计、显示所有的性能参数；

系统能提供认证、授权、控制、审计等安全管理功能；

系统必须提供 northbound 接口如 CORBA/COPS/LDAP，可以被无缝地集成在第三方网管平台上；

设备要求具备可管理性，设备必须支持通过 Console Port 或 Telnet 的模式实现配置管理。

设备必须支持 SNMP V1，符合 RFC 1155 及 RFC 1157 的规定。

设备必须支持 SNMP V2，符合 RFC 2578、RFC 2579、RFC 2580、RFC 3416

及 RFC 3417 的规定。

设备必须支持 SNMP V3，符合 RFC 3410 的规定。

设备必须支持带外网管，可以将管理流量与用户流量从物理或逻辑上分开。带外网管与带内网管具有同等的功能。

设备必须支持基于 RADIUS 的管理员集中认证、授权和记帐管理，必须可以配置不同于普通接入用户的 RADIUS 服务器完成。支持基于命令行的集中授权。

设备必须支持 NTP。

设备必须支持在本地存放多个版本的软件和配置文件。

必须对一些重要的操作提供操作撤消功能。

建议具备 QoS 流量、故障、安全、配置等关键统计信息的本地存储功能，并以 XML 的形式表达、通过 FTP 方式传送到指定的 FTP 服务器。

建议支持基于 XML 的 Network Configuration (NETCONF) 网管协议。

必须支持流量采样，采样精度大于 90%，建议支持针对子端口的 xFlow 采样。

13.2 SNMP MIB

设备必须支持 ATM MIB，包括：

RFC 2515-Definitions of Managed Objects for ATM Management (February 1999)；

设备必须支持 BGP-4 MIB：RFC 4273-Definitions of Managed Objects for BGP-4 (January 2006)。

设备必须支持分布式管理 MIB：RFC 4560 - Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (June 2006)。

设备必须支持以太网 MIB：RFC 3635 - Definitions of Managed Objects for the Ethernet-like Interface Types (September 2003)。

设备必须支持事件 MIB：RFC 2981 - Event MIB (October 2000)。

设备必须支持通告 MIB：RFC 3014 - Notification Log MIB (November 2000)。

设备必须支持帧中继 MIB：RFC 2115 - Management Information Base for Frame Relay DTEs Using SMIV2 (September 1997)。

设备必须支持 IGMP MIB：RFC 2933 - Internet Group Management Protocol MIB (October 2000)。

设备必须支持端口 MIB: RFC 2863 - The Interfaces Group MIB (June 2000)。

设备必须支持 IP MIB, 包括:

RFC 1213 - Management Information Base for Network Management of TCP/IP-based Internets: MIB-II (March 1991);

RFC 2932 - IPv4 Multicast Routing MIB (October 2000)。

RFC 4022 - Management Information Base for the Transmission Control Protocol (TCP) (March 2005);

RFC 4113 - Management Information Base for the User Datagram Protocol (UDP) (June 2005);

RFC 4292 - IP Forwarding Table MIB (April 2006);

RFC 4293 - Management Information Base for the Internet Protocol (IP) (April 2006);

RFC 4087 - IP Tunnel MIB (June 2005)。

设备必须支持 OSPF MIB: RFC 1850 - OSPF Version 2 Management Information Base (November 1995)。

设备必须支持 PIM MIB: RFC 2934 - Protocol Independent Multicast MIB for IPv4 (October 2000)。

设备必须支持 PPP MIB, 包括:

RFC 1471 - The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol (June 1993);

RFC 1473 - The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol (June 1993)。

设备必须支持 RIP MIB: RFC 1724 - RIP Version 2 MIB Extension (November 1994)。

设备必须支持 SNMP MIB, 包括:

RFC 1213 - Management Information Base for Network Management of TCP/IP-based Internets: MIB-II (March 1991);

RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) (December 2002)。

设备必须支持 SNMPv3 MIB, 包括:

RFC 3411 - An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks (December 2002);

RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) (December 2002);

RFC 3413 - Simple Network Management Protocol (SNMP) Applications

(December 2002);

RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) (December 2002);

RFC 3415 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) (December 2002)。

设备必须支持统计 MIB: RFC 2513 - Managed Objects for Controlling the Collection and Storage of Accounting Information for Connection-Oriented Networks (February 1999)。

设备必须支持 VRRP MIB: RFC 2787 - Definitions of Managed Objects for the Virtual Router Redundancy Protocol (March 2000)。

厂商自定义的 MIB 必须符合 RFC1155 (STD16) 标准, 并遵照 RFC1212 (STD16) 定义的描述与命名机制。

厂商自定义 MIB 必须能有效地支持特定对象的状态显示、统计、配置和控制, 可通过一定途径提取厂商自定义 MIB 信息并能对设备进行写操作。

13.3 故障管理

设备必须能够向网元管理系统发送告警。

设备必须在告警中提供足够的信息以协助排障, 例如日期时间戳, 严重程度, 部件的标识, 硬件/软件/固件版本等。

设备的故障告警必须至少要有以下几个严重级别的分类: 紧急 (critical), 主要 (major), 次要 (minor) 和通知 (informational), 并可以定制。

设备对以下情况必须发送告警:

当 RADIUS 服务器不可用时;

当设备的组成部件、逻辑端口或服务控制不可用时;

设备必须支持对系统资源 (例如 IP 地址池) 的检测, 在资源利用达到配置的阈值时。

故障事件的发生与该事件的告警报告的时间相差要小于 5 秒钟。

当故障被修正时, 设备将自动清除该故障的告警。

设备必须具备预先维护监测功能, 例如事件审计、内存使用情况的监控、进程“丢失”或软件故障的监察等, 并能采取适当的恢复措施。

设备必须允许通过 VC、VP、VR、用户名、IP、MAC 等进行会话的查找。

设备必须支持使用 Ping、Traceroute 等工具辅助故障的处理。

设备必须支持回退能力, 如将操作系统软件/配置退回到先前的版本。

设备必须在网元管理系统无法工作时提供远程访问的手段。

设备必须支持命令显示 PPP 会话信息和 L2TP 隧道信息。

设备必须支持在 L2TP 隧道的 LAC 侧查看 L2TP 的状态和统计。

设备必须提供自检测试或者故障诊断手段/工具。可完成连通性测试、性能测试、业务测试、硬件故障的检测及定位等。

设备必须支持用户定位。

13.4 配置管理

可实现对设备系统、端口和业务数据的配置、查询和修改。

可完成系统软件升级，建议设备支持不中断业务升级。

应能通过网元管理系统对设备集中进行软件升级。

设备必须提供软件备份、配置文件备份功能并能恢复。

设备必须支持从 FTP 或 TFTP 服务器下载软件/配置文件。

13.5 计费管理

对帐号用户，应能协助 RADIUS 服务器完成用户的计费工作。

对专线或 VPN 用户，应能根据业务实现对流量或时长的统计，并通过开放的通用接口提交给计费系统。

实现本地计费的设备对计费数据形成原始话单，以文本等方式在本地存储计费数据，未实现本地计费的设备的计费数据以标准 MIB 的形式存储于 MIB 库中，计费服务器通过 SNMP 周期性地查询设备的 MIB 计数器获取计费数据。设备厂商应开放其 MIB 库，使计费系统能通过标准的 SNMP 协议实时读取数据并进行相应处理。

13.6 性能管理

设备必须对 ATM PVC、L2TP 隧道、PPPoE 会话和 PPPoA 会话的接受和发送数据包进行监测和统计。

设备应能监测和统计 PPP 用户的呼叫性能数据：用户发起的呼叫次数、呼叫成功完成的次数、呼叫失败或放弃的次数并说明其原因。

设备必须支持命令用于汇总在设备上配置的所有 PVC，并显示其封装类型。

设备必须能够对系统内部的资源使用进行统计，如 CPU 及内存利用率等。

设备必须支持对 QoS 策略的实施进行监控和统计。可基于用户、端口、PVC 或 VLAN、IP 地址或应用的 QoS 实施效果如吞吐量、丢包率性能进行监控和统计。

设备必须支持与业务相关的统计功能。

设备必须支持对基于单个用户业务流的监控和统计功能，包括应用层端口、会话连接数等。

当用户超过最大会话连接数限制时，设备必须将该信息及时写到日志文件。

设备必须支持可配置的 IP 地址池使用情况高低阈值，并能够将超出阈限的情况报告给管理系统。

设备必须支持可设定一个端口每秒种处理多少个包的基本阈值，但超过时必须提供告警。建议每个 VLAN、PVC、虚端口、PPP Session 都可设置。

设备必须在用户会话（PPPoE/PPPoA）提供流量镜像功能，例如将特定用户会话的上行和/或下行流量拷贝到指定的目的端口，能够开启镜像的用户会话数必须不少于系统配置数的 2%。

必须能够提供统计分析功能，包括对 Ethernet、ATM、SDH 端口的物理特性的统计，统计每个端口接收帧/信元计数、可纠正帧/信元计数，帧/信元丢失率；对时延性能的统计包括传输时延，信元时延抖动等。

14 互通性要求

设备应能够与现有的其他网络设备（DSLAM、ATM 交换机、以太网交换机、路由器等）实现物理层互通。

设备应能和主流交换机厂家的设备实现 VLAN、SVLAN 的互通，可实现 SVLAN 外层标识的灵活设置。

设备必须能与主流路由器厂家的设备实现路由协议（RIPv1、RIPv2、OSPFv2、ISIS、BGPv4）的互通。

设备必须能和主流路由器厂家的设备实现 MPLS 及相关协议的互通。

设备必须能与其他厂家设备实现 L2/L3 MPLS VPN、VPLS、GRE、IPSec、L2TP 等 VPN 业务的互通。

如支持 IPv6，要求设备必须能与其他厂家设备的 IPv6 及 IPv6 相关协议的互通。

15 其它要求

15.1 定时与同步要求

设备必须支持采用主从同步方式。

设备应设置外定时源输入接口，从通信楼定时供给设备（BITS）获得定时。同步接口可以为 2048kbit/s 或 2048kHz，优选 2048kbit/s 接口。

设备应具有从线路信号中恢复定时，并用于同步功能。当不能使用外定时方式时，采用线路定时。可从 STM-N 线路信号中获得，帧结构应符合 ITU-T 建议 G.707 的要求。

设备内部时钟应采用二或三级时钟。时钟单元可采用有保持功能的高稳晶体时钟。二级时钟的自由运行频率准确度优于： $\pm 4 \times 10^{-7}$ ；三级时钟的自由运行频率准确度优于： $\pm 4.6 \times 10^{-6}$ 。时钟能在 24 小时内仍能维持相对于外定时中断瞬间时钟频率不劣于 $\pm 1 \times 10^{-8}$ 的时钟准确度。

设备在失去全部输入频率基准时钟信号时，内部时钟应能自动进入保持工作方式。

设备的定时信号可从下列信号中提取：

- （1）从外同步接口获取；
- （2）从线路信号中获取；
- （3）设备内部时钟产生的可用定时信号中获取。

定时信号的提取顺序为：先（1）后（2）再（3）提取定时信号。

15.2 网络时间同步

设备必须支持网络时间同步协议 NTP，支持 NTP 认证和 NTP 服务器/客户端。

15.3 OAM 要求

设备必须支持 MPLS OAM 以及 ETHERNET OAM。

OAM 标准化协议应满足以下规范：

RFC 4377 : Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks

RFC 4378 : A Framework for Multi-Protocol Label Switching (MPLS) Operations and Management (OAM)

RFC4379: Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

Ethernet OAM: IEEE 802.1ag & ITU-T Y.1731

15.4 设备硬件要求

1. 设备应支持不同业务处理板的混插，提高插槽的通用性和灵活性。
2. 系统交换引擎、总线带宽和到每个业务槽位的连接带宽必须能够满足目前和未来多种业务的发展需要，如，支持组播业务线速转发、频道的快速切换，保证视频业务质量和带宽。
3. 设备应具有网络故障和硬件故障告警功能。
4. 当软件升级时，应不影响硬件结构。
5. 对主控模块的要求：
 - 主控模块应具有软硬件故障告警功能。
 - 主控模块应具有故障脱机自动诊断功能以及负荷控制措施。
6. 设备应提供过流、过压保护措施。
7. 设备必须具备冗余的 Stratum 3（或更佳）内部振荡器用于内部时钟，需满足或高于 Telcordia GR-1110-Core 第 4.6 节中指定的同步要求。

15.5 机箱要求

任何端口模块必须可以被不受限制地插入任何非保留给控制/交换模块的槽位中。

冷却系统必须是冗余和可热插拔的，当一个风扇故障时，剩余的风扇必须能够维持对满载系统的冷却。

必须使用温度传感器监测系统的温度，当系统温度超过预设的阈值时，必须产生一个告警指示，并发送给适当的告警/故障管理系统。

必须提供视觉指示（LED）用于显示设备的冷却系统或温度情况（如风扇工作/故障，温度正常/过热等）。

建议设备提供多种机箱设计以应用于小型、中型及大型接入节点。本规范中的要求适用于大型接入节点的部署，本规范中的功能要求（规模要求除外）适用

于任何规模的设备。

15.6 线缆管理

设备必须在机箱的背部提供适当的线缆管理，使用户可以方便地对线缆进行操作。

15.7 设备软件要求

1. 软件要求保证安全可靠，具有容错能力。
2. 软件系统须提供数据接口，提供进行二次开发的文档。
3. 软件应采用模块化结构，模块之间的通信应按规定的接口进行。
4. 应具有软件故障的监视功能，一旦软件出现死循环等重大故障时，应能自动再启动，并做出即时故障报告信息。
5. 配置数据与处理程序应有相对的独立性，配置数据的任何变更都不应引起运行版本的变更。
6. 软件应有完善、方便的人机通信控制功能。
7. 软件应具备方便、迅速地恢复到原来版本的功能。
8. 系统软件应能在线升级，不需重新启动。
9. 软件应在不中断通信的情况下，完成程序打补丁的功能。
10. 不同时期软件版本应能向下兼容，软件版本易于升级
11. 软件升级必须可以在线获得
12. 设备必须支持从 FTP 或 TFTP 服务器下载软件/配置文件
13. 设备应该通过 CMM Level 3 认证，满足对软件开发和质量保证过程的要求
14. 设备应该通过 ISO 9001 认证，满足对软件开发和质量保证过程的要求
15. 设备的工程和制造过程应该通过 TL-9000 认证

15.8 环境要求

室内型设备必须能够在以下环境条件下正常运行：

环境温度： 5℃～45℃，每小时变化<10℃

相对湿度： 10%～90% （非凝露、非结霜）

在以下灰尘环境下，设备应能正常工作：直径大于 5 μm 的灰尘浓度≤3×10⁴ 粒/m³；灰尘粒子是非导电、导磁和腐蚀性的。

设备的电磁兼容性应符合国标 GB 9254-1998 《信息技术设备无线电骚扰限

值和测试方法》和 GB/T 17618-1998《信息技术设备抗扰度限值和测试方法》。设备产生的电磁辐射建议符合 FCC Class A、EN55022/CISPR-22 Class A、VCCI Class A 等标准。

抗震措施：按 8 级烈度进行计算；

机械振动：4.9 牛顿/平方米（50 赫兹至 200 赫兹）

应提供双电源备份和负载分担功能，必须支持-48V 直流电源。直流电压及其波动范围要求：

直流电压及其波动范围要求：额定电压-48V，允许变动范围为-40V~-57V。

15.9 绿色要求

15.9.1 设备管理要求

（1）基本要求

1. 对于机框插槽式设备，设备应有高温报警功能。
2. 对于机框插槽式设备，应具备能源监控及管理功能。在设备管理员需要时，可检测到设备当前能耗状态。
3. 对于机框插槽式设备，应支持根据实际情况中断未用板卡供电或进入微电状态。
4. 设备电源反灌杂音应满足通信电源 YD/T 1051-2000《通信局站电源系统总技术要求》的要求。

（2）扩展要求

1. 对于机框插槽式设备，能通过查询方式监控到目前工作状态下能耗，以及设备各个组件，如各板卡、机框、风扇，所消耗的能耗比例。
2. 对于机框插槽式设备，设备可通过命令行或网管工具远程关闭设备部分模块或功能以减少其工作能耗。
3. 对于机框插槽式设备，可根据实际情况动态调整风扇转速。
4. 对于机框插槽式设备和服务器设备，宜具有可根据用户需求和不同应用场合配置交流或直流供电的选择。

15.9.2 设备环保与包装要求

（1）设备环保要求

设备设计阶段，设备的主要部分（如电路板、机箱、电缆等）应尽量减少铅、镉、汞、六价铬、溴化耐燃剂等有害物质，并严格按 ROHS 规范进行产品生产与设计。

（2） 设备包装要求

实行包装减量化（Reduce）。绿色包装在满足保护、方便、销售等功能的条件下，应是用量最少的适度包装。

包装应易于重复利用（Reuse）或易于回收再生（Recycle）。

包装废弃物可以降解腐化（Degradable）。为了不形成永久的垃圾，不可回收利用的包装废弃物要能分解腐化，进而达到改善土壤的目的。

包装材料对人体和生物应无毒无害，包装材料中不应含有有毒物质或有毒物质的含量应控制在有关标准以下。

包装材料应尽量减少木材的使用。

在包装产品的整个生命周期中，均不应对环境产生污染或造成公害。

（3） 其它要求

设备内部应有合理的气流组织，应采用前进后出或垂直通风方式，不宜从侧面进出通风。

同时，机框式数据设备内风扇应具有自动调节速率的功能，机架内采用防热风回流等技术，降低对机房环境的局部制冷要求。

机架门开孔率：考虑到通风和散热的需求，在保证门的强度和刚度要求前提下，机架正面门和背面门开孔率至少不得低于 30%，以获得良好的排吸风效果。

15.9.3 能耗分级标准

设备能耗等级应达到最新版本的中国电信《绿色数据设备技术规范》所定义的标准。

中国电信集团公司技术标准

Q/CT 2080-2008

中国电信 IP 城域网设备技术规范 (汇聚交换机)

(V3.0)

2008-12-31 发布

2009-1-1 实施

中国电信集团公司 发布

目 录

1. 编制说明	1
1.1 范围	1
1.2 引用标准	1
1.3 定义、术语和缩写	2
1.3.1 定义	2
1.3.2 术语和缩写	2
2. 概述及总体要求	3
3. 设备容量、接口及可靠性要求	3
3.1 接口类型要求	3
3.1.1 百兆以太网接口	3
3.1.2 千兆以太网接口	4
3.1.3 万兆以太网接口	4
3.1.4 PON 接口	4
3.1.5 管理接口	5
3.2 设备容量要求	5
3.3 可靠性和可用性	5
4. 功能要求	6
4.1 以太网基本功能要求	6
4.2 生成树协议	6
4.3 VLAN 功能	7
4.4 VLAN 堆叠	8
4.5 端口聚合	9
4.6 广播抑制	9
4.7 二层组播	9
4.8 策略控制及 QoS 功能	10
4.8.1 访问控制	10
4.8.2 业务分类	10
4.8.3 队列技术	11
4.8.4 速率限制	11
4.8.5 拥塞避免	11
4.9 MAC 地址限制	11
4.10 以太环网	11
4.11 T-MPLS	12
4.12 三层功能要求（可选）	12
4.13 其他功能要求	12
4.13.1 DHCP OPTION 82	12
4.13.2 Private VLAN	12
4.13.3 VLAN 交换	13
4.13.4 MAC IN MAC	13
5. MPLS 功能（可选）	13
5.1 MPLS 基本功能	13
6. 性能要求	14

6.1 MAC 地址学习和缓存能力.....	14
6.1.1 MAC 地址学习速度.....	14
6.1.2 MAC 地址表容量.....	14
6.2 VLAN 能力.....	15
6.3 转发性能.....	15
6.4 组播处理能力.....	15
6.5 访问控制表条目.....	15
7. 运行与维护.....	16
7.1 命令行功能.....	16
7.2 WEB 配置界面.....	16
7.3 远程访问.....	16
7.4 用户认证.....	16
7.5 日志记录.....	16
7.6 流量镜像.....	17
7.7 以太网 OAM.....	17
7.8 链路故障检测及保护切换.....	18
7.9 设备集群与堆叠.....	18
7.9.1 设备集群.....	18
7.9.2 设备堆叠.....	18
8. 网络管理.....	19
8.1 网管协议.....	19
8.2 管理信息库.....	19
8.3 网管系统.....	20
8.3.1 配置管理.....	20
8.3.2 性能管理.....	21
8.3.3 故障管理.....	21
8.3.4 安全管理.....	22
9 设备其他要求.....	23
9.1 硬件结构要求.....	23
9.2 设备软件要求.....	23
9.3 供电和环境要求.....	24
9.3.1 供电要求.....	24
9.3.2 接地.....	24
9.3.3 工作环境.....	25
9.3.4 设备抗震加固.....	25
9.3.5 防雷.....	25
9.3.6 防电磁干扰.....	25
9.4 绿色要求.....	25
9.4.1 设备管理要求.....	25
9.4.2 设备环保与包装要求.....	26
9.4.3 能耗分级标准.....	26

1. 编制说明

1.1 范围

本技术规范以 RFC 文档、ITU-T 以及 IEEE 标准为依据，针对中国电信实际情况和具体要求，对 IP 城域网中汇聚交换机的软硬件结构、功能、性能、运维与管理等进行了规定。

本技术规范适用于中国电信集团城域网汇聚交换机设备的研制、生产和引进。

在本规范中：

- (1) 必须：表示该条目是本规范必须。违反这样的要求是原则性错误。
- (2) 必须实现：表示该要求必须实现，但不要求缺省使能。
- (3) 不允许（不可以）：表示该条目绝对禁止。
- (4) 应当（建议）：表示在某些特定条件下存在忽视该条目的理由，但是忽视或违反该条目时必须仔细衡量。
- (5) 应当（建议）实现：与应当（建议）类似，实现时不必要缺省使能。
- (6) 不应当（不建议）：表示在某些特定条件存在所描述行为可接受或有效的理由，但实现该行为时必须仔细衡量。
- (7) 可以：表示该条目确实可选。

1.2 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。在标准出版时，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的最新版本的可能性。

GB/T17625.1-2003	《电磁兼容 限值 谐波电流发射限值(设备每相输入电流≤16A)》
GB17625.2-1999	《电磁兼容 限值 对额定电流不大于 16A 的设备在低压供电系统中产生电压波动和闪烁的限制》
YD/T 1051-2000	《通信局站电源系统总技术要求》
SPECpower_ssj2008	标准效能公司能耗测试标准
能源之星 4.0	主要针对消费性电子产品的能源节约计划。
COC on Energy Consumption of Broadband Equipment	宽带设备能源消耗管理
IEEE802.1d	媒体访问控制(MAC)网桥

IEEE802.1q	虚拟桥接局域网
IEEE802.1ad	供应商桥接
IEEE802.1ag	以太网连接故障管理
IEEE802.1ah	供应商骨干桥接
IEEE802.3	局域网协议标准
IEEE802.3ad	多链路段聚合
IEEE802.3ah	第一公里以太网
ITU Y.1731	以太网 OAM 和性能管理
RFC826	以太网地址解释协议 ARP
RFC1213	管理信息库(MIB-II)
RFC1256	ICMP 路由发现消息
RFC1643	用于以太网接口类型的管理对象的定义
RFC1901	SNMPv2 协议
RFC1902	SNMPv2 的 SMI
RFC1905	SNMPv2 协议操作
RFC1907	用于 SNMPv2 的 MIB
RFC2233	使用 SMIv2 的接口组 MIB
RFC2236	互联网组管理协议 IGMP 版本 2

1.3 定义、术语和缩写

1.3.1 定义

以太交换机（Switch）是 IP 网络业务的接入设备，位于城域网的接入层，起到业务接入和汇聚功能。

1.3.2 术语和缩写

ACL	访问控制列表
ANSI	美国国家标准研究所
ARP	地址解析协议
FCS	帧校验序列
FIB	转发信息表
GE	千兆以太网
ICMP	互联网消息协议
IGMP	互联网组消息协议
IP	互联网协议
IPv4	互联网协议——第 4 版
LAN	局域网
MIB	管理信息库
MTU	最大传输单元
OA & M	运行管理与维护
PDU	协议数据单元

PPP	点到点协议
RADIUS	远程认证拨号用户服务
SNMP	简单网络管理协议
SVLAN	堆叠 VLAN
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
VLAN	虚拟局域网
WAN	广域网

2. 概述及总体要求

城域网中使用的汇聚以太网交换机位于城域网三层业务接入点以下，用于组成公众接入平面的以太网交换汇聚网络，完成公众业务的汇聚，并传送至三层网络。

城域汇聚交换机只启用二层功能，总体技术要求如下：

- 1) 具有较强的二层交换能力，提供较高的链路带宽和接口密度。
- 2) 能够完成对互联网、NGN、IPTV 等业务的区分，上传至 BRAS、SR 等相应的三层设备。
- 3) 具备用户唯一性标识技术，实现对用户的识别和定位。
- 4) 支持一定的策略控制手段，基于用户、业务提供差异化服务。

3. 设备容量、接口及可靠性要求

3.1 接口类型要求

3.1.1 百兆以太网接口

交换机必须支持符合 IEEE802.3/802.3u 的 10M/100M 快速以太网接口。

物理层传输方式包括 100BASE-TX 和 100BASE-FX，其中光接口模块必须可替换，以满足不同传输波长和传输距离的要求。

3.1.2 千兆以太网接口

交换机必须支持符合 IEEE802.3z 的千兆以太网接口。

物理层传输方式包括 1000BASE-SX、1000BASE-LX 和 1000BASE-T，其中光接口模块必须可替换，以满足不同传输波长和传输距离的要求。

3.1.3 万兆以太网接口

建议设备支持符合 IEEE802.3ae 的万兆以太网接口。

3.1.4 PON 接口

建议设备支持 EPON 或者 GPON 接口，具备 OLT 的功能。EPON 接口应符合标准 YD/T 1475-2006《接入网技术要求——基于以太网方式的无源光网络（EPON）》。

提供 EPON 接口的设备应采用动态带宽分配机制（DBA）来提高系统带宽利用率以保证业务公平性和 QoS，至少应能根据 LLID 分配带宽授权，最小带宽分配粒度不应大于 256kbit/s。

提供 EPON 接口的设备应能区分不同类型业务的优先级，上行和下行方向都应能根据 SLA 协议保证高优先级业务的 QoS。

提供 EPON 接口的设备应对用户信息进行加密，其中下行方向应支持加密功能，上行方向可选支持。

提供 EPON 接口的设备应具有对 ONU 进行认证的能力，应拒绝非法 ONU 的接入。

提供 EPON 接口的设备应支持 IEEE 802.1Q 协议，应支持按照 PON 端口或以太网端口划分 VLAN。

提供 EPON 接口的设备应支持基于端口或 MAC 地址的以太网帧过滤。

提供 EPON 接口的设备应支持对广播帧和组播帧的抑制功能。

提供 EPON 接口的设备应实现各 ONU 之间的二层隔离。

提供 EPON 接口的设备应支持 IGMP Snooping 或 IGMP Proxy 功能。

提供 EPON 接口的设备建议采用光纤保护倒换机制。

3.1.5 管理接口

设备必须提供用于本地维护管理的串行管理接口（Console 口）。

设备必须提供基于以太网的带外网管接口。

3.2 设备容量要求

- 1) 设备可采用集中转发或分布交换的转发处理方式，整机容量对于 A 类设备不小于 256Gbps，对于 B 类设备不小于 64Gbps。。
- 2) 设备最大支持的接口数量要求为：百兆接口不小于 48 个，千兆接口不小于 32 个。

3.3 可靠性和可用性

- 1) 采用集中转发结构的设备主控板必须支持冗余备份功能，主控板切换时业务中断时间不大于 50ms。
- 2) 采用交换结构的设备的交换矩阵必须支持冗余备份功能。对于交换矩阵集成于主控板的设备，主控板切换时板内业务无中断，板间业务中断时间不大于 50ms；对于主控板和交换矩阵分离的设备，主控板切换时业务无中断，交换矩阵切换时板内业务无中断，板间业务中断时间不大于 50ms。
- 3) 设备必须支持电源模块的冗余。工作电源模块切换时业务无中断。
- 4) 设备必须支持在不中断通信的情况下，可带电进行板卡的热插拔操作。热插拔操作必须对整机及其他业务板卡无影响。
- 5) 设备平均无故障工作时间（MTBF）必须大于 17520 小时，系统故障恢复时间（MTTR）必须小于 1 小时。
- 6) 满配置环境下，设备重启动时间不大于 10 分钟。

4. 功能要求

4.1 以太网基本功能要求

1) 以太网帧封装和转发

设备必须支持 IEEE 802.3 和 ETHERNET II 帧封装形式，并支持以存储转发模式完成数据包的交换转发。

2) 端口速率

以太网端口必须支持全双工/半双工模式及端口速率可配，并支持设备间端口工作模式的自协商（AUTO-NEGOTIATION）。建议电口能支持 MDI/MDI-X 自适应。

3) MAC 地址学习

设备必须支持 MAC 地址的手工配置和动态学习功能，动态学习模式下地址老化时间可调。

4) 异常帧检测

设备必须具备异常帧检测功能，可识别并过滤超短帧、CRC 校验错帧等各种异常帧，同时保证正常帧的转发。

5) 超常帧转发

设备必须支持超常帧转发（帧长大于 1518BYTE），可转发的最大帧长不小于 1536BYTE。建议设备支持最大 9000BYTE 的巨帧（JUMBO 帧）的转发。

6) 流量控制

设备百兆和千兆端口必须支持流量控制功能，在产生拥塞时可向发送源发出通告要求其降速或暂停发送。

在全双工方式下必须支持 802.3x 规定的流量控制协议，在产生拥塞时可向发送源发出 PAUSE 帧，禁止对端在一定时间内发送除 MAC 控制帧以外的帧。

在半双工方式下必须支持反压流控功能，产生拥塞时在输入端口产生强制的冲突，迫使远端设备放弃此数据帧的发送。

4.2 生成树协议

1) 设备必须支持符合 IEEE 802.1d 标准的生成树协议（STP），简单拓扑环境

下（网络层次不大于 2 层）链路收敛时间不大于 45 秒。

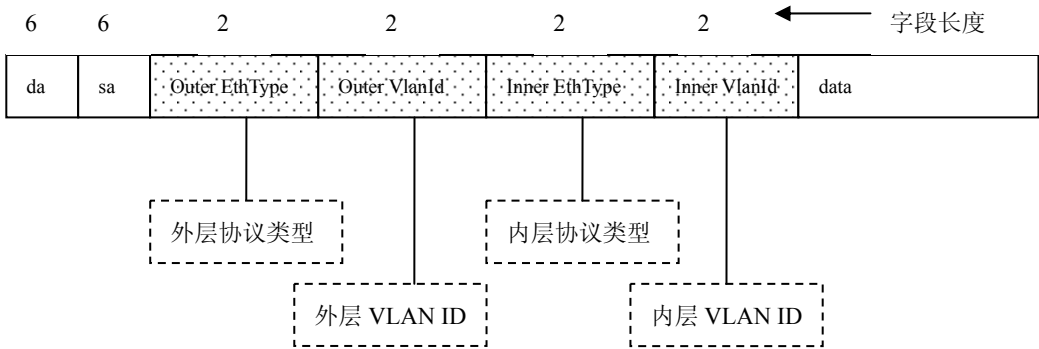
- 2) 设备必须支持快速生成树协议（RSTP），简单拓扑环境下（网络层次不大于 2 层）链路收敛时间不大于 3 秒。
- 3) 设备必须支持多生成树协议（MSTP），为交换机上的每个 VLAN 或多个 VLAN 建立对方的生成树，链路收敛时间达到快速生成树协议的标准。
- 4) 在支持的各种生成树协议环境下，设备必须支持对节点权值和端口权值可配置，以实现网络根网桥和设备根端口的灵活选择。同时还必须具备良好的兼容性，可和支持该标准的其他厂家设备互通。

4.3 VLAN 功能

- 1) 设备必须支持 VLAN 功能，必须支持 IEEE802.1q 协议规定的 VLAN 帧封装形式。各 FE 和 GE 端口支持 VLAN tagged 和 untagged 两种工作方式，其中 tagged 端口可配置允许通过 VLAN 范围，并支持 VLAN 的修剪(VLAN PRUNING)。
- 2) 设备必须支持基于端口划分 VLAN，各物理端口可通过配置不同的 VLAN ID 分属不同 VLAN。设备所有端口必须支持 VLAN tagged 和 untagged 两种工作方式，tagged 方式下默认 VLAN（NATIVE VLAN）的 VLAN ID 可配置。
- 3) 可选支持通过 MAC 地址、上层协议等其他方式划分 VLAN。
- 4) 设备必须支持通过配置启用或禁用指定的 VLAN，可配置的 VLAN ID 范围为 1-4094。
- 5) 设备必须支持端口隔离功能，同一 VLAN 中不同端口之间可配置为隔离状态，互相不能通信。
- 6) 建议设备支持一般属性注册协议（GARP）和 VLAN 注册协议（GVRP），实现多设备间 VLAN 的自动发现和配置。
- 7) 建议设备支持 VLAN ID 交换功能，即将进入设备的数据包所携带的 VLAN ID 映射为指定的其他 VLAN ID 并转发。
- 8) 建议设备支持 VLAN 聚合，即将多个 VLAN ID 聚合为一个 VLAN ID。

4.4 VLAN 堆叠

VLAN 堆叠（STACKING VLAN）功能在带有 VLAN 标记（用户侧 VLAN/内层 VLAN）的数据包上加入第二层 VLAN 标记（网络侧 VLAN/外层 VLAN）具有二层 VLAN 标记的以太网帧结构如下图所示：



VLAN 堆叠技术用于采用 VLAN ID 实现用户唯一性标识和定位的宽带接入网，以实现二层以太交换网络 VLAN 资源的扩展。设备要求如下：

- 1) 设备必须支持 VLAN 堆叠功能，为带有 VLAN 标记的数据包加入第二层 VLAN 标记。
- 2) 一台设备必须可同时支持标准 VLAN 业务和 SVLAN 业务，可使用同一个上行端口传送两种业务。设备启用 SVLAN 的端口必须可正常配置访问控制和 QOS 等各种策略。
- 3) 设备的 SVLAN 功能必须具有和其他厂家的交换机、BRAS 设备良好的互通性。SVLAN 以太网帧的外层 VLAN 标签的 ETHERNET TYPE 必须设置为 0x88a8，建议设备支持外层 VLAN 标签的 ETHERNET TYPE 字段可配置。
- 4) 设备必须通过硬件实现支持选择性 SVLAN 功能，即在同一个物理端口上支持根据单层 VLAN ID 灵活加载外层 VLAN ID；同时能够透传标准 VLAN（单 VLAN）流量。
- 5) 建议设备支持 SVLAN 的以下操作：根据入端口、内层 VLAN 中 802.1p 参数、内层 VLAN ID 添加外层 VLAN ID 及 802.1p 参数。
- 6) 建议设备能够对双层 VLAN 报文中的内、外层 VLAN 信息进行灵活的识别

和处理，便于对用户的上下流量进行管理。

- 7) 设备可选支持基于流的选择性 SVLAN 功能，可根据流的特征，如 MAC 地址、IP 地址、优先级或四层端口等分配相应外层 VLAN 标签。

4.5 端口聚合

- 1) 设备的百兆端口和千兆端口必须支持符合 IEEE 802.3ad 规定的端口聚合功能，即将多个以太网端口捆绑为一个聚合端口使用，以实现带宽扩展和链路保护的功能。设备的板内 FE 端口和 GE 端口必须能够在单 VLAN 或启用 SVLAN 条件下支持端口聚合功能。
- 2) 设备必须支持通过静态配置实现端口聚合，聚合端口可支持 VLAN tagged 和 untagged 两种工作方式。建议设备支持通过动态配置实现端口聚合。
- 3) 百兆端口最大可聚合的端口数必须不小于 8 个，千兆端口最大可聚合的端口数不小于 4 个。设备在各种聚合链路数目情况下，必须能实现各链路间的负载均分，达到 100%的带宽利用率。设备必须支持根据数据流的源目的地址进行负载分担，建议支持逐包负载分担方式。
- 4) 链路故障时的收敛时间必须小于 800ms，建议达到 50ms 以内。
- 5) 建议设备支持板间接口的端口的聚合功能。
- 6) 在静态配置环境下，可与其他支持该标准的厂家设备实现良好互通。

4.6 广播抑制

- 1) 设备必须具备广播过滤功能，可通过配置限制每个端口允许通过的最大广播包速率和比例。对广播数据流的带宽限制误差不大于 5%。
- 2) 设备必须支持对组播和未知单播的限制和过滤功能，可限制每个端口允许通过的最大组播包或未知单播包的速率和比例，带宽限制误差不大于 5%。

4.7 二层组播

- 1) 设备必须支持 IGMP SNOOPING 二层组播功能，以实现组播包的二层复制。
- 2) 设备必须支持 VLAN UNTAG 和 VLAN TAG 接口下的组播复制功能，以及组播组的快速加入和离开。组播组离开延时应小于 20ms。
- 3) 设备必须具备一定的组播业务控制机制，如组播组访问控制、组播用户数

限制、单个用户加入的组播组数限制等。

- 4) 设备必须支持跨 VLAN 的组播复制能力，可将一个 VLAN 组播业务复制到多个不同的用户 VLAN 中。
- 5) 设备必须支持 IGMP PROXY 二层组播复制功能。
- 6) 建议设备具备 ANCP 的相关功能，以实现交换机与 BRAS/SR 间交互信息，实现对组播的控制。

4.8 策略控制及 QoS 功能

4.8.1 访问控制

- 1) 设备必须能够在百兆和千兆端口上实现对流量的访问控制功能。
- 2) 设备必须支持二层和三层的访问控制表，可匹配的字段包括：
 - 源 MAC 地址、目的 MAC 地址；
 - 标准 VLAN 环境中的 VLAN ID；
 - SVLAN 环境中的内层和外层 VLAN ID；
 - 802.1P 优先级字段；
 - 源 IP 地址、目的 IP 地址；
 - 四层协议类型及源、目的端口号；
- 3) 设备必须支持端口入方向和出方向的访问控制。
- 4) 建议支持基于 VLAN 端口的访问控制（在 VLAN 端口下，根据 MAC、IP 地址等进行访问控制）；

4.8.2 业务分类

- 1) 设备必须能够识别物理端口、VLAN/SVLAN、IEEE 802.1D 优先级标签（原 IEEE802.1p）、Ethernet 类型、IP 地址、IP 类型、四层协议端口等信息，作为划分业务等级的依据。建议支持报文的深度检测（80 个字节）功能。
- 2) 设备必须可根据数据包所属的业务等级改写其 802.1P COS 等级，以作为其在网络中传递时的业务优先级标识。
- 3) 设备必须支持 802.1P 和 IP TOS 之间的映射，以及 SVLAN 环境中内、外层

VLAN 标签间 802.1P 的双向（内层到外层，外层到内层）映射。

4.8.3 队列技术

- 1) 设备必须支持将不同等级的业务映射到相应的队列中，并为每个队列配置相应的带宽保证和转发优先级。
- 2) 设备必须支持严格优先级和轮询等队列技术，可保证严格优先级队列的带宽和延时，并按比例为轮询队列分配带宽。
- 3) 每个物理端口必须支持的 8 个硬件队列数不小于 4 个。

4.8.4 速率限制

- 1) 设备必须支持基于物理端口和访问控制表等条件进行流量的速率限制。
- 2) 设备必须支持入方向和出方向的速率限制，对超过限制要求的流量能选择处理方式，如允许转发、丢弃、修改优先级等。
- 3) 速率限制最小可配置带宽不大于 64Kbps，增量颗粒度不大于 64Kbps；限制结果精确，误差不大于 5%。
- 4) 端口应能在进行速率限制的同时，提供访问控制、队列调度等功能。

4.8.5 拥塞避免

建议设备支持 WRED 拥塞避免机制。

4.9 MAC 地址限制

设备必须具备对指定端口下的 MAC 地址数量进行限制的功能，且地址数量可灵活配置。对于超过限制值的 MAC 地址不会被加入设备 MAC 地址表，对应的数据流量不被转发。

4.10 以太环网

建议设备支持以太环网，并实现以下功能：

—支持环网拓扑自动发现，可动态地增加、减少环路节点；环上各节点具有统一的、可更新的环路拓扑结构图；

—提供环保护和网络拓扑自愈恢复功能，在环路或节点发生故障时（光纤中

断、节点设备故障等), 能够实现自动环保护功能, 保护切换时间小于 50ms;

—支持环上各节点业务带宽的公平算法。当环上出现拥塞或重负荷时, 可保证各节点发送业务的公平性。

4.11 T-MPLS

建议设备支持 T-MPLS。实现 T-MPLS 的设备必须遵循以下标准:

- G.8110.1: T-MPLS 层网络架构
- G.8112: T-MPLS 传送网 NNI
- G.8121: T-MPLS 设备功能块特性
- G.8131: T-MPLS 网络的线性保护倒换
- G.8113/Y.1372: T-MPLS 的 OAM 需求
- G.8114/Y.1373: T-MPLS 的 OAM 机制
- G.8132/Y.1382: T-MPLS 网络的环保护倒换
- G.8151/Y.1374: T-MPLS 网元管理

4.12 三层功能要求 (可选)

- 1) 建议支持 ARP 及 ARP PROXY;
- 2) 建议支持 RIP1/2、OSPFv2 等路由协议;
- 3) 建议支持 IGMP、PIM-DM/SM 等组播路由协议;
- 4) 建议支持 VLL、VPLS 等 L2 MPLS VPN;
- 5) 建议支持 IPv6 基本协议, 符合 RFC2460—互联网协议(版本六)。

4.13 其他功能要求

4.13.1 DHCP OPTION 82

设备必须支持 DHCP OPTION 82 功能, 可将物理端口信息插入 DHCP Discovery 消息中, 传给上层网络设备。

4.13.2 Private VLAN

设备必须支持 Private VLAN 功能, 可以隔离属于同一 VLAN 的物理端口间

的互访。

4.13.3 VLAN 交换

建议设备支持 VLAN 交换功能，将进入设备的数据包所携带的 VLAN ID 替换为指定的其他 VLAN ID 并转发。

4.13.4 MAC IN MAC

设备可选支持 IEEE 802.1ah 规定的 MAC in MAC 功能，为一个以太网帧加上第二层（外层）MAC 封装。

5. MPLS 功能（可选）

设备建议支持 MPLS，支持 MPLS 协议的基本功能，支持 MPLS LER 和 LSR 功能，支持 MPLS 显式路由。

设备建议能配置备份 LSP；支持多路径 LSP 的负荷分担；支持标签堆栈；能够基于源/目的 IP 地址、协议、源/目的端口号、ToS/优先级、TCP 标志、路由表的下一跳等参数将数据包路由至输出 LSP。支持将任意三个 IP Precedence 值映射到一个 EXP 中，并支持相应的层次化 QoS 部署。

建议支持标准公开的 MPLS VLL 二层隧道协议(Martini 方案)。

设备建议支持虚拟专用 LAN 承载服务，即支持 VPLS 功能。

设备在支持 MPLS 二层 VPN 时，应同时支持 Martini 标准和 Lasserer-vKompella 标准。

设备能够根据所配置的策略，把输入的业务量自动分配到不同的 TE LSP 中；建议采用硬件来完成该功能，在完成该功能时，仍然能以线速转发 MPLS 数据包。

建议设备在支持 IP FRR 的基础上，支持 LDP 的 FRR 功能。

5.1 MPLS 基本功能

MPLS 帧的封装格式必须符合 RFC3032 的规定，能够确定网络层协议类型、能够产生打标签的 ICMP 包、能够正确处理超大 IP 报文、能够在 PPP 链路上传递打标签的 IP 包；标签值的使用必须符合 RFC3032 和 RFC4182 的规定；MPLS 帧格式的 TTL 字段的处理必须符合 RFC3032 和 RFC3443 的规定。

设备建议支持 LDP 协议，LDP 协议的实现必须符合 RFC3036 的规定：

- 能够作为 LDP Peer 实现 LDP 消息(发现、会话、通告和通知消息)的交换；
- 能够实现 LDP 协议的各项操作，包括：FEC 的确定；标签空间、LDP 标识符；LDP 发现；LDP 会话的维护和建立；非直连 LSR 之间 LDP 会话的实现；和 LDP 传送的实现；标签的分发和管理；LDP 环回检测；LDP 消息的真实性和完整性验证；显式路由 LSP 的标签分发等；
- 协议规范：包括 LDP PDU 格式；LDP 过程；TLV 编码；LDP 消息的构成等。

建议支持 BFD for LDP，BFD for RSVP。

建议支持 LDP 和 RSVP 协议的无中断路由功能。

设备应具备 LSP 环回检测和防止功能，支持 RFC3063 规定的 MPLS 环回检测机制提供的 Thread 功能；建议支持 RFC4379 规定的 MPLS 数据平面故障检测功能，并能与 draft-ietf-bfd-mpls-07 中规定的 BFD 在 MPLS LSP 中的应用相结合,实现对 MPLS LSP 的故障检测功能。

标签保持模式建议使用自由(liberal)标签保持模式，参见 RFC3031 的 3.8 节。

设备应支持基于标签对数据包的转发，并可通过手动配置或标签分配协议(LDP)建立 LSP。

6. 性能要求

6.1 MAC 地址学习和缓存能力

6.1.1 MAC 地址学习速度

设备百兆和千兆端口的 MAC 地址学习速度不低于 1000 个/秒。

6.1.2 MAC 地址表容量

采用集中转发结构的设备整机 MAC 地址表容量 A 类不小于 64K 个，B 类不小于 32K 个；采用分布转发结构的设备 MAC 地址表容量 A 类不小于 64K 个/业务板，B 类不小于 32K 个/业务板。

6.2 VLAN 能力

- 1) 单台设备必须支持4094个VLAN同时启用，在开启大量VLAN的情况下不影响设备转发性能。
- 2) 开启选择性SVLAN功能时，汇聚交换机必须能够并发识别外层4K个VLAN标识、内层4K个VLAN标识。
- 3) 设备所有接口同时开启选择性SVLAN功能时，每端口可识别的用户标签数量不低于4094个，识别和分配标签过程不能影响设备转发性能。

6.3 转发性能

- 1) 设备的百兆端口和千兆端口对于各种帧长的数据流具备 100%线速转发能力。无拥塞情况下，64 字节数据包转发延时小于 100us。
- 2) 同一业务板内各端口间必须实现无阻塞转发；不同业务板间交换能力大于 16Gbps（双向）。
- 3) 设备长期性能要求为：在高负载条件下（端口流量大于 90%），64 字节以太网帧丢失率小于 10^{-5} 。

6.4 组播处理能力

- 1) 设备可同时支持的组播组数目不少于 200 个。
- 2) 端口加入/离开某个组播组的时间小于 20ms。
- 3) 设备各端口必须实现对组播流的线速转发，且转发单、组播混合流量时不出现性能下降。
- 4) 每 GE 端口的跨 VLAN 组播复制能力不小于 200 条，且不影响设备性能。

6.5 访问控制表条目

- 1) 设备每个端口至少可应用一个访问控制表。
- 2) 分布式转发结构交换机单板访问控制列表至少 1000 条；集中式转发结构交换机整机访问控制列表至少 1000 条。
- 3) 在应用的访问控制表条目较多时设备的转发性能不出现下降。

7. 运行与维护

7.1 命令行功能

- 1) 设备必须支持提供命令行方式的维护管理界面。管理者可通过本地串行接口或远程网络接口登录和操作设备。
- 2) 命令行模式下必须完成设备所有功能的配置。
- 3) 必须具备以下维护功能：
 - 可查询设备当前的软硬件版本、各模块及端口工作状态
 - 可对 MAC 缓存表、ARP 缓存表、端口流量统计等系统表项完成显示、查询和清除的操作
 - 可查询当前运行协议的工作状态
 - 提供 ICMP PING、TRACEROUTE 等 OAM 工具

7.2 WEB 配置界面

建议设备提供 WEB 配置管理界面，客户端可通过浏览器对设备进行配置。

7.3 远程访问

- 1) 设备必须支持 TELNET 方式的远程访问功能。
- 2) 必须提供源地址限制、最大连接数限制等访问控制功能。
- 3) 设备必须支持以 SSH 方式的远程访问功能。

7.4 用户认证

- 1) 设备必须能对登录用户进行认证，并提供本地账号管理和远程认证的功能。
- 2) 设备必须支持 RADIUS 远程认证协议，并支持 RADIUS 扩展属性，可从 RADIUS 返回信息中确定用户的级别和权限。

7.5 日志记录

设备必须支持日志记录（SYSLOG）的功能，可对各类事件记录保存到日志中，并发送给指定服务器。必须支持的记录项目包括：

- 端口状态变化
- 告警
- 设备或模块重启动
- 用户登录及命令操作
- 配置改变

7.6 流量镜像

- 1) 设备必须支持端口镜像功能，可分别将指定端口入方向和出方向的流量镜像到相应端口。
- 2) 必须支持对 VLAN tagged 端口和 untagged 端口的流量镜像。
- 3) 设备必须支持基于流的镜像功能，可基于访问控制表等手段将符合匹配条件的数据流镜像到指定端口。
- 4) 建议设备支持远程流量镜像功能。

7.7 以太网 OAM

建议设备支持以下标准规定的以太网 OAM 功能：

- IEEE802.1ag
- IEEE802.3ah
- ITU Y.1731

遵循 ITU Y.1731 标准的设备建议支持如下以太网 OAM 故障管理功能：

- 以太网连续性检查 (ETH-CC)
- 以太网环回 (ETH-LB)
- 以太网链路跟踪 (ETH-LT)
- 以太网警告指示信号 (ETH-AIS)
- 以太网远端缺陷指示 (ETH-RDI)
- 以太网锁定信号 (ETH-LCK)
- 以太网测试信号 (ETH-Test)
- 以太网自动保护倒换 (ETH-APS)
- 以太网维护通讯通道 (ETH-MCC)
- 以太网实验用的OAM (ETH-EXP)

遵循 ITU Y.1731 标准的设备建议支持如下以太网 OAM 性能监控功能：

- 帧丢失测量(ETH-LM)
- 帧延时测量(ETH-DM)
- 吞吐量测量

遵循 ITU Y.1731 标准的设备必须符合标准规定的以太网 OAM 的帧格式。

7.8 链路故障检测及保护切换

建议设备所有类型的以太网端口支持双向故障检测协议（Bidirectional Forwarding Detection, draft-ietf-bfd-base-02.txt, BFD），并且在通过 BFD 检测到链路故障时能够执行预先设定的动作（如进行保护切换等）。可以在交换机上指定互为备份的链路或 VLAN。

7.9 设备集群与堆叠

7.9.1 设备集群

设备必须支持在多台汇聚交换机之间实现集群管理功能。具体要求如下：

- 1) 可只使用一个管理地址，对集群内的设备进行远程管理。（在主设备上可切换到不同设备进行管理）
- 2) 可通过命令行方式在集群内所有成员间切换管理，并可在主设备上实现对从设备的相关操作，如批量下载、保存、删除从设备的配置，软件升级，重启从设备等功能。
- 3) 可同时支持的集群设备数量不小于 8 台。

7.9.2 设备堆叠

设备必须支持在多台园区交换机之间实现堆叠功能。具体要求如下：

- 1) 可只使用一个管理地址，实现对所有堆叠设备的管理。
- 2) 可在主设备上查询、配置所有堆叠设备的端口。
- 3) 可在主设备上查询、配置所有堆叠设备的 VLAN、生成树协议。
- 4) 可同时支持的堆叠设备数量不小于 8 台。

8. 网络管理

8.1 网管协议

- 1) 设备必须支持SNMP v1、SNMPv2网络管理协议,并符合RFC 1157、RFC 1902 - RFC 1906 标准的规定。
- 2) 建议设备支持SNMP v3网管协议。
- 3) 设备必须支持SNMP访问地址限制,只允许特定地址范围的主机对设备的访问。
- 4) 设备必须支持安全视图的功能,为不同的网络管理者设置相应的MIB视图浏览权限。

8.2 管理信息库

- 1) 设备必须支持RFC 1213规定的标准管理信息库。
- 2) 设备必须支持以下标准规定的管理信息库:
 - RFC 2665 - Definitions of Managed Objects for the Ethernet-like Interface Types (August 1998)
 - RFC 2863 - The Interfaces Group MIB (June 2000)
 - RFC 2933 - Internet Group Management Protocol MIB (October 2000)
 - RFC 2981 - Event MIB (October 2000)
 - RFC 3014 - Notification Log MIB (November 2000)
 - RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) (December 2002)
 - RFC 3411 - An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks (December 2002)
 - RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) (December 2002)
 - RFC 3413 -Simple Network Management Protocol (SNMP) Applications (December 2002)
 - RFC 3414 - User-based Security Model (USM) for version 3 of the Simple

Network Management Protocol (SNMPv3) (December 2002)

RFC 3415 - View-based Access Control Model (VACM) for the Simple

Network Management Protocol (SNMP) (December 2002)

RFC 2513 - Managed Objects for Controlling the Collection and Storage of

Accounting Information for Connection-Oriented Networks

(February 1999)

- 3) 厂家私有MIB库必须符合RFC 1155和RFC 1212标准的规定。

私有MIB必须包括以下内容：

- 端口
- VLAN信息
- CPU、内存占用率
- 物理资源
- 访问控制和QOS
- 二层组播
- VLAN堆叠（SVLAN）

- 4) 设备必须提供可查看QOS各队列的包/字节计数、流速以及丢包计数的MIB接口。

8.3 网管系统

网管系统必须具备故障管理、配置管理、性能管理和安全管理等主要网管功能。必须提供与第三方网管系统的接口，可以无缝地集成在第三方网管系统上。

8.3.1 配置管理

- 1) 网管系统必须能够自动发现网络拓扑，显示网元间连接关系，并能够动态、实时显示被管网元的运行状态和状况。
- 2) 网管系统必须能够在网络拓扑中创建、删除、查询修改设备。
- 3) 网管系统必须能够对设备软件进行升级，建议网管系统支持集群升级。
- 4) 网管系统必须提供对设备配置信息的上载和下载功能，并支持对配置信息合法性和一致性的检查。
- 5) 网管系统必须能够完成以下功能的配置：

- 业务端口的打开和关闭、协商参数设置、流控等
- VLAN的创建、删除、与相应业务端口的关联、VLAN堆叠的配置等
- 各种生成树功能的开启和关闭、节点和端口权值的设置
- 二三层访问控制表的配置、应用
- 业务分类、优先级队列、速率限制等QOS功能配置
- 二层组播功能（IGMP SNOOPING）的配置
- 网管协议、地址的设置

8.3.2 性能管理

- 1) 网管系统必须对网元的重要性能参数（CPU 利用率、内存利用率、数据包
的分类统计）进行监控。
- 2) 网管系统必须提供性能门限管理，支持对一个监测对象的某个性能参数设
置上限和（或）下限，当该监测对象的性能参数超过设定的上限或下限时，
产生越限告警。
- 3) 网管系统必须提供查询性能数据的功能，并以表格和图形如折线图、直方
图、饼图等方式显示查询结果和统计结果。必须能对查询统计结果进行打
印输出。
- 4) 允许指定网元性能监测的属性，并可进行查询/修改，包括：性能监测对象、
需要监测的参数名称、监测周期（15 分钟或者 24 小时）、监测状态（打
开/关闭）、开始时间、结束时间、是否自动上报。
- 5) 网管系统必须提供性能趋势分析功能，通过对当前和历史性能测量数据的
分析，预测性能监测参数今后的变化趋势。
- 6) 性能数据在网管存储设备上保存一定期限的 15 分钟和 24 小时性能。测量
周期为 15 分钟的测量数据至少 30 天；测量周期为 24 小时的测量数据至
少 60 天。当性能数据的存储超过期限或容量时必须提示用户归档和删除。

8.3.3 故障管理

- 1) 网管系统必须支持对告警类型、告警级别和告警状态的分类定义。
告警类型包括：设备告警、服务质量告警、通信告警、环境告警、处理

失败告警

告警级别包括：紧急告警、主要告警、次要告警、提示告警、清除告警

告警状态包括：当前告警、历史告警、已确认告警、未确认告警、锁定

告警

- 2) 网管系统必须能够在网络拓扑图中以不同形式显示告警发生的位置及告警信息，并提示用户对告警进行确认。
- 3) 网管系统必须能够对告警信息进行确认、清除、合并、过滤。
- 4) 网管系统必须具有告警相关性抑制功能。根据网络配置信息，以及接收的告警信息频度和种类，对告警信息的关联进行综合分析，在多个告警中确定故障根源。并能以图形显示方式或文本显示方式将设备或通信故障定位在设备板卡或端口上，同时给出可能的故障原因。
- 5) 网管系统必须能够对当前告警或者历史告警提供查询和统计功能。
- 6) 网管系统必须支持告警信息的同步，将显示的告警状态与网元实际的告警状态进行核准，必须提供人工和自动两种校正模式。

8.3.4 安全管理

- 1) 网管系统必须能够对用户进行管理，包括增加用户、删除用户、锁定用户、解锁用户、查询用户信息、修改用户密码。
- 2) 网管系统必须对用户的访问进行认证、授权。
- 3) 网管系统必须对用户划分等级，不同级别的管理员必须具有不同的权限，访问者只能在自己的权限范围内进行管理操作。敏感信息、或固定用户终端鉴权属性、数据库和配置数据只能由有授权的个人或管理系统进行操作。
- 4) 网管必须提供操作日志记录，以记录网管配置的改变及网管操作人员登录、注销的时间。

9 设备其他要求

9.1 硬件结构要求

- 1) 设备必须采用模块化结构设计，所有板卡可替换升级，且各版本硬件良好兼容，提供较高的可用性和可扩展性。
- 2) 设备控制板卡、业务卡、交换矩阵和电源等模块必须支持在线热插拔。
- 3) 设备应支持不同业务处理板的混插，提高插槽的通用性和灵活性。
- 4) 对于单播组播转发、VLAN 堆叠、策略控制等功能必须采用独立硬件实现，减轻 CPU 压力，确保设备的性能要求。
- 5) 采用交换结构的设备具备头端阻塞避免机制。
- 6) 设备应具有网络故障和硬件故障告警功能。
- 7) 当软件升级时，应不影响硬件结构。
- 8) 对主控模块的要求：
 - 主控模块应具有软硬件故障告警功能。
 - 主控模块应具有故障脱机自动诊断功能以及负荷控制措施。
- 9) 设备应提供过流、过压保护措施。
- 10) 机箱冷却系统必须冗余且可热插拔，当一个风扇故障时，剩余的风扇必须能够维持对满载系统的冷却。必须提供视觉指示(LED)用于显示设备的冷却系统或温度情况(如风扇工作/故障，温度正常/过热等)。
- 11) 设备必须适合安装在标准 19 英寸的机架上，所需机柜深度不超过 600mm。
- 12) 设备必须提供直观、方便的指示灯，建议包括电源指示灯、运行状态指示灯、端口连接状态指示灯、端口工作模式指示灯、链路活动指示灯等。

9.2 设备软件要求

- 1) 软件要求保证安全可靠，具有容错能力。
- 2) 软件系统须提供数据接口，提供进行二次开发的文档。
- 3) 软件应采用模块化结构，模块之间的通信应按规定的接口进行。
- 4) 应具有软件故障的监视功能，一旦软件出现死循环等重大故障时，应能自动再启动，并做出即时故障报告信息。

- 5) 配置数据与处理程序应有相对的独立性，配置数据的任何变更都不应引起运行版本的变更。
- 6) 软件应有完善、方便的人机通信控制功能。
- 7) 软件应具备方便、迅速地恢复到原来版本的功能。
- 8) 系统软件应能在线升级，不需重新启动。
- 9) 软件应在不中断通信的情况下，完成程序打补丁的功能。
- 10) 不同时期软件版本应能向下兼容，软件版本易于升级
- 11) 软件升级必须可以在线获得。
- 12) 设备必须支持从 FTP 或 TFTP 服务器下载软件/配置文件。
- 13) 设备必须该通过 CMM Level 3 认证，满足对软件开发和质量保证过程的要求。
- 14) 设备必须该通过 ISO 9001 认证，满足对软件开发和质量保证过程的要求。

9.3 供电和环境要求

9.3.1 供电要求

- 1) 直流电压及其波动范围要求：

-额定电压：-48V

-电压波动：在直流输入端子处测试的-48V 电压允许变化范围为-57V 至 -40V。要求设备在此电压范围内正常工作。

- 2) 交流电压及其波动范围要求：

单相 220V，变化范围为 10%，频率 50Hz，变化范围为 5%，线电压波形畸变率小于 5%。要求设备在此电压范围内正常工作。

9.3.2 接地

- 1) 接地方式必须符合工作地、保护地和建筑防雷接地-组接地体的联合接地方式。
- 2) 接地线截面积根据可能通过的最大电流负荷确定。
- 3) 联合接地电阻值必须小于 5Ω 。

9.3.3 工作环境

- 1) 温度：5℃~45°
- 2) 相对湿度：10%~90%
- 3) 温度变化率：≤10℃/h，不结露
- 4) 海拔高度：-500~5000 米
- 5) 防尘：静态条件下测试，主机房空气中≥0.5μm 的尘粒数，少于 18000 粒/升

9.3.4 设备抗震加固

设备应具备抗震加固特性。要求抗震设防烈度按 8 度考虑。

9.3.5 防雷

设备防雷击能力必须符合 GB3483-1983 《电子设备雷击实验》。

9.3.6 防电磁干扰

- 1) 设备在受到 0.01-1000MHZ 频率范围内电场强度为 140dBuV/m 的外界电磁干扰时不出现故障和性能下降。
- 2) 在直流或交流电源线受到 0.01-100MHZ 频率范围的外界电磁干扰电流使不出现故障和性能下降。

9.4 绿色要求

9.4.1 设备管理要求

(1) 基本要求

1. 对于机框插槽式设备，设备应有高温报警功能。
2. 对于机框插槽式设备，应具备能源监控及管理功能。在设备管理员需要时，可检测到设备当前能耗状态。
3. 对于机框插槽式设备，应支持根据实际情况中断未用板卡供电或进入微电状态。
4. 设备电源反灌杂音应满足通信电源 YD/T 1051-2000 《通信局站电源系统

总技术要求》的要求。

(2) 扩展要求

1. 对于机框插槽式设备，能通过查询方式监控到目前工作状态下能耗，以及设备各个组件，如各板卡、机框、风扇，所消耗的能耗比例。
2. 对于机框插槽式设备，设备可通过命令行或网管工具远程关闭设备部分模块或功能以减少其工作能耗。
3. 对于机框插槽式设备，可根据实际情况动态调整风扇转速。
4. 对于机框插槽式设备和服务器设备，宜具有可根据用户需求和不同应用场合配置交流或直流供电的选择。

9.4.2 设备环保与包装要求

(1) 设备环保要求

设备设计阶段，设备的主要部分（如电路板、机箱、电缆等）应尽量减少铅、镉、汞、六价铬、溴化耐燃剂等有害物质，并严格按 ROHS 规范进行产品生产与设计。

(2) 设备包装要求

实行包装减量化（Reduce）。绿色包装在满足保护、方便、销售等功能的条件下，应是用量最少的适度包装。

包装应易于重复利用（Reuse）或易于回收再生（Recycle）。

包装废弃物可以降解腐化（Degradable）。为了不形成永久的垃圾，不可回收利用的包装废弃物要能分解腐化，进而达到改善土壤的目的。

包装材料对人体和生物应无毒无害，包装材料中不应含有有毒物质或有毒物质的含量应控制在有关标准以下。

包装材料应尽量减少木材的使用。

在包装产品的整个生命周期中，均不应对环境产生污染或造成公害。

(3) 其它要求

设备内部应有合理的气流组织，应采用前进后出或垂直通风方式，不宜从侧面进出通风。

同时，机框式数据设备内风扇应具有自动调节速率的功能，机架内采用防热风回流等技术，降低对机房环境的局部制冷要求。

机架门开孔率：考虑到通风和散热的需求，在保证门的强度和刚度要求前提下，机架正面门和背面门开孔率至少不得低于 30%，以获得良好的排吸风效果。

9.4.3 能耗分级标准

设备能耗等级应达到最新版本的中国电信《绿色数据设备技术规范》所定义

的标准。

中国电信集团公司技术标准

Q/CT 2081-2008

中国电信 IP 城域网设备技术规范 (园区交换机)

(V3.0)

2008-12-31 发布

2009-1-1 实施

中国电信集团公司 发布

目 录

1. 编制说明	1
1.1 范围	1
1.2 引用标准	1
1.3 定义、术语和缩写	2
1.3.1 定义	2
1.3.2 术语和缩写	2
2. 概述及总体要求	3
3. 设备容量、接口及可靠性要求	3
3.1 接口类型要求	3
3.2 设备容量要求	4
3.3 可靠性和可用性	4
4. 功能要求	4
4.1 基本功能要求	4
4.2 生成树协议	5
4.3 VLAN 功能	5
4.4 VLAN 堆叠	6
4.5 端口聚合	7
4.6 广播抑制	7
4.7 二层组播	7
4.8 策略控制功能	8
4.8.1 访问控制	8
4.8.2 业务分类	8
4.8.3 队列技术	8
4.8.4 速率限制	9
4.8.5 拥塞避免	9
4.9 网络安全	9
4.9.1 地址绑定	9
4.9.2 地址数量限制	9
4.9.3 VLAN 隔离	9
4.9.4 报文过滤及抑制	9
4.10 以太环网	10
4.11 三层功能要求（可选）	10
4.12 其他功能要求	10
4.12.1 DHCP OPTION 82	10
4.12.2 Private VLAN	10
4.12.3 VLAN 交换	10
4.12.4 MAC IN MAC	10
5. 性能要求	11
5.1 MAC 地址学习和缓存能力	11
5.2 VLAN 能力	11
5.3 转发性能	11
5.4 组播处理能力	11
5.5 访问控制表条目	12

6. 运行与维护	12
6.1 设备集群与堆叠	12
6.1.1 设备集群	12
6.1.2 设备堆叠	12
6.2 命令行功能	12
6.3 WEB 配置界面	13
6.4 远程访问	13
6.5 用户认证	13
6.6 日志记录	13
6.7 流量镜像	13
6.8 以太网 OAM	14
6.9 链路故障检测及保护切换	14
7. 网络管理	15
7.1 网管协议	15
7.2 管理信息库	15
7.3 网管系统	16
7.3.1 配置管理	16
7.3.2 性能管理	17
7.3.3 故障管理	17
7.3.4 安全管理	18
8 设备其他要求	18
8.1 硬件结构要求	18
8.2 设备软件要求	19
8.3 供电和环境要求	19
8.3.1 供电要求	19
8.3.2 接地	19
8.3.3 工作环境	20
8.3.4 设备抗震加固	20
8.3.5 防雷	20
8.3.6 防电磁干扰	20
8.4 绿色要求	20
8.4.1 设备管理要求	20
8.4.2 设备环保与包装要求	21
8.4.3 能耗分级标准	22

1. 编制说明

1.1 范围

本技术规范以 RFC 文档、ITU-T 以及 IEEE 标准为依据，针对中国电信实际情况和具体要求，对 IP 城域网中园区交换机的软硬件结构、功能、设备性能、运维与管理等进行了规定。

本技术规范适用于中国电信集团城域网园区交换机设备的研制、生产和引进。

在本规范中：

- (1) 必须：表示该条目是本规范必须。违反这样的要求是原则性错误。
- (2) 必须实现：表示该要求必须实现，但不要求缺省使能。
- (3) 不允许（不可以）：表示该条目绝对禁止。
- (4) 应当（建议）：表示在某些特定条件下存在忽视该条目的理由，但是忽视或违反该条目时必须仔细衡量。
- (5) 应当（建议）实现：与应当（建议）类似，实现时不必要缺省使能。
- (6) 不应当（不建议）：表示在某些特定条件存在所描述行为可接受或有效的理由，但实现该行为时必须仔细衡量。
- (7) 可以：表示该条目确实可选。

1.2 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。在标准出版时，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的最新版本的可能性。

GB/T17625.1-2003	《电磁兼容 限值 谐波电流发射限值(设备每相输入电流≤16A)》
GB17625.2-1999	《电磁兼容 限值 对额定电流不大于 16A 的设备在低压供电系统中产生电压波动和闪烁的限制》
YD/T 1051-2000	《通信局站电源系统总技术要求》
SPECpower_ssj2008	标准效能公司能耗测试标准
能源之星 4.0	主要针对消费性电子产品的能源节约计划。
COC on Energy Consumption of Broadband Equipment	宽带设备能源消耗管理

IEEE802.1d	媒体访问控制(MAC)网桥
IEEE802.1q	虚拟桥接局域网
IEEE802.1ad	供应商桥接
IEEE802.1ag	以太网连接故障管理
IEEE802.1ah	供应商骨干桥接
IEEE802.3	局域网协议标准
IEEE802.3ad	多链路段聚合
IEEE802.3ah	第一公里以太网
ITU Y.1731	以太网 OAM 和性能管理
RFC826	以太网地址解释协议 ARP
RFC1213	管理信息库(MIB-II)
RFC1256	ICMP 路由发现消息
RFC1643	用于以太网接口类型的管理对象的定义
RFC1901	SNMPv2 协议
RFC1902	SNMPv2 的 SMI
RFC1905	SNMPv2 协议操作
RFC1907	用于 SNMPv2 的 MIB
RFC2233	使用 SMIv2 的接口组 MIB
RFC2236	互联网组管理协议 IGMP 版本 2

1.3 定义、术语和缩写

1.3.1 定义

园区以太网交换机(Switch)是 IP 网络业务的接入设备,位于城域网的接入层,起到业务接入和汇聚功能。

1.3.2 术语和缩写

ACL	访问控制列表
ANSI	美国国家标准研究所
ARP	地址解析协议
FCS	帧校验序列
FIB	转发信息表
GE	千兆以太网
ICMP	互联网消息协议
IGMP	互联网组消息协议

IP	互联网协议
IPv4	互联网协议——第 4 版
LAN	局域网
MIB	管理信息库
MTU	最大传输单元
OA&M	运行管理与维护
PDU	协议数据单元
PPP	点到点协议
RADIUS	远程认证拨号用户服务
SNMP	简单网络管理协议
SVLAN	堆叠 VLAN
TCP	传输控制协议
TOS	服务类型
TTL	生存时间

2. 概述及总体要求

园区以太网交换机位于城域汇聚交换机以下，用于组成组建城域宽带接入网，完成公众业务的初步汇聚。园区交换机下联楼道交换机，并可就近汇接 DSLAM，为用户提供至以太网汇聚网络的上行通路。

城域园区交换机只启用二层功能，总体技术要求如下：

- 1) 具备百兆到千兆的业务汇聚能力，提供多条高带宽上行链路。
- 2) 支持足够数量的 VLAN，用于区分用户和业务。
- 3) 提供一定的 QoS 能力，可实现对用户、业务的识别和控制。
- 4) 具备较强的组播控制和处理能力，在技术层面保证 IPTV 业务的开展。

3. 设备容量、接口及可靠性要求

3.1 接口类型要求

3.1.1 百兆以太网接口

交换机必须支持符合 IEEE802.3/802.3u 的 10M/100M 快速以太网接口。

物理层传输方式包括 100BASE-TX 和 100BASE-FX，其中光接口模块必须

可替换，以满足不同传输波长和传输距离的要求。

3.1.2 千兆以太网接口

交换机必须支持符合 IEEE802.3z 的千兆以太网接口。

物理层传输方式包括 1000BASE-SX、1000BASE-LX 和 1000BASE-T，其中光接口模块必须可替换，以满足不同传输波长和传输距离的要求。

3.1.3 PON 接口

交换机建议支持 PON 接口，具备 ONU 的功能。

3.1.4 管理接口

设备必须提供用于本地维护管理的串行管理接口（Console 口）。

3.2 设备容量要求

- 1) 要求整机交换容量大于 8Gbps。
- 2) 设备可提供的接口数量要求为：百兆接口不小于 24 个，千兆接口不小于 2 个。

3.3 可靠性和可用性

- 1) 设备平均无故障工作时间（MTBF）必须大于 17520 小时，系统故障恢复时间（MTTR）必须小于 1 小时。
- 2) 满配置环境下，设备重启动时间不大于 5 分钟。

4. 功能要求

4.1 基本功能要求

1) 以太网帧封装和转发

设备必须支持 IEEE 802.3 和 ETHERNET II 帧封装形式，并支持以存储转发模式完成数据包的交换转发。

2) 端口速率

以太网端口必须支持全双工/半双工模式及端口速率可配，并个支持设备间端口工作模式的自协商（AUTO-NEGATIATION）。建议电口支持 MDI/MDI-X 自适应。

3) MAC 地址学习

设备必须支持 MAC 地址的手工配置和动态学习功能，动态学习模式下地址

老化时间可调。

4) 异常帧检测

设备必须具备异常帧检测功能，可识别并过滤超短帧、CRC 校验错帧等各种异常帧，同时保证正常帧的转发。

5) 超常帧转发

设备必须支持超常帧转发（帧长大于 1518BYTE），可转发的最大帧长不小于 1536BYTE。建议设备支持最大 9000BYTE 的巨帧（JUMBO 帧）的转发。

6) 流量控制

设备百兆和千兆端口必须支持流量控制功能，在产生拥塞时可向发送源发出通告要求其降速或暂停发送。

在全双工方式下必须支持 802.3x 规定的流量控制协议，在产生拥塞时可向发送源发出 PAUSE 帧，禁止对端在一定时间内发送除 MAC 控制帧以外的帧。

在半双工方式下必须支持反压流控功能，产生拥塞时在输入端口产生强制的冲突，迫使远端设备放弃此数据帧的发送。

4.2 生成树协议

- 1) 设备必须支持符合 IEEE 802.1d 标准的生成树协议（STP），简单拓扑环境下（网络层次不大于 2 层）链路收敛时间不大于 45 秒。
- 2) 设备必须支持快速生成树协议（RSTP），简单拓扑环境下（网络层次不大于 2 层）链路收敛时间不大于 3 秒。
- 3) 设备必须支持多生成树协议（MSTP），为交换机上的每个 VLAN 或多个 VLAN 建立对应的生成树，链路收敛时间达到快速生成树协议的标准。
- 4) 在各种支持的生成树协议环境下，设备必须支持对节点权值和端口权值可配置，以实现网络根网桥和设备根端口的灵活选择。同时还必须具备良好的兼容性，可和支持该标准的其他厂家互通。

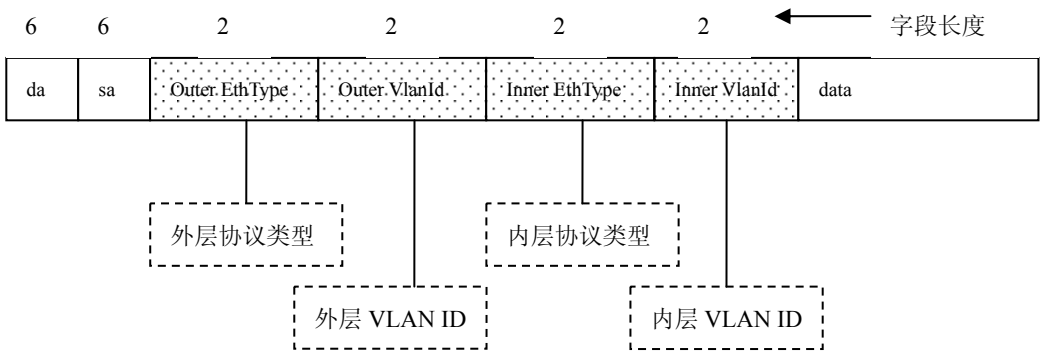
4.3 VLAN 功能

- 1) 设备必须支持 VLAN 功能，必须支持 IEEE802.1q 协议规定的 VLAN 帧封装形式。各 FE 和 GE 端口支持 tagged 和 untagged 两种工作方式，其中 tagged 端口可配置允许通过 VLAN 范围，并支持 VLAN 的修剪（VLAN PRUNING）。
- 2) 设备必须支持基于端口划分 VLAN，各物理端口可通过配置不同的 VLAN ID 分属不同 VLAN。设备所有端口必须支持 tagged 和 untagged 两种工作方式，tagged 方式下默认 VLAN（NATIVE VLAN）的 VLAN ID 可配置。

- 3) 可选支持通过 MAC 地址、上层协议等其他方式划分 VLAN。
- 4) 设备必须支持通过配置启用或禁用指定的 VLAN，可配置的 VLAN ID 范围为 1-4094。
- 5) 设备必须支持端口隔离功能，同一 VLAN 中不同端口之间可配置为隔离状态，互相不能通信。
- 6) 建议设备支持一般属性注册协议（GARP）和 VLAN 注册协议（GVRP），实现多设备间 VLAN 的自动发现和配置。
- 7) 建议设备支持 VLAN ID 交换功能，即将进入设备的数据包所携带的 VLAN ID 映射为指定的其他 VLAN ID 并转发。
- 8) 建议设备支持 VLAN 聚合，即将多个 VLAN ID 聚合为一个 VLAN ID。

4.4 VLAN 堆叠

VLAN 堆叠（STACKING VLAN）功能在带有 VLAN 标记（用户侧 VLAN/内层 VLAN）的数据包上加入第二层 VLAN 标记（网络侧 VLAN/外层 VLAN）。具有二层 VLAN 标记的以太网帧结构如下图所示：



VLAN 堆叠技术用于采用 VLAN ID 实现用户唯一性标识和定位的宽带接入网，以实现二层以太交换网络 VLAN 资源的扩展。设备要求如下：

- 1) 设备必须支持 VLAN 堆叠功能，为带有 VLAN 标记的数据包加入第二层 VLAN 标记。
- 2) 一台设备必须同时支持标准 VLAN 业务和 SVLAN 业务，可使用同一个上行端口传送两种业务。设备启用 SVLAN 的端口必须可正常配置访问控制和 QOS 等各种策略。
- 3) 设备的 SVLAN 功能必须具有和其他厂家的交换机、BRAS 设备良好的互通性。SVLAN 以太网帧的外层 VLAN 标签的 ETHERNET TYPE 必须设置为

0x88a8, 建议设备支持 SVLAN 外层 ETHERNET TYPE 字段可配置。

- 4) 建议设备必须支持通过硬件实现支持选择性 SVLAN 功能, 即在同一个物理端口上支持根据单层 VLAN ID 灵活加载外层 VLAN ID; 同时能够透传标准 VLAN (单 VLAN) 流量。
- 5) 建议设备支持 SVLAN 的以下操作: 根据入端口、内层 VLAN 中 802.1p 参数、内层 VLAN ID 添加外层 VLAN ID 及 802.1p 参数。
- 6) 建议设备能够对双层 VLAN 报文中的内层进行灵活的识别和处理, 便于对用户的上下流量进行管理。
- 7) 设备可选支持基于流的选择性 SVLAN 功能, 可根据流的特征, 如 MAC 地址、IP 地址、优先级或四层端口等分配相应外层 VLAN 标签。

4.5 端口聚合

- 1) 设备的百兆端口和千兆端口必须支持符合 IEEE 802.3AD 规定的端口聚合功能, 即将多个以太网端口捆绑为一个聚合端口使用, 以实现带宽扩展和链路保护的功能。设备的板内 FE 端口和 GE 端口必须能够在单 VLAN 或启用 SVLAN 条件下支持端口聚合功能。
- 2) 设备必须支持通过静态配置实现端口聚合, 建议支持通过动态配置实现端口聚合。聚合端口可支持 VLAN tagged 和 VLAN untagged 两种工作方式。
- 3) 对于园区交换机, 设备必须支持 FE 端口最大可聚合的端口数应不小于 4 个, GE 端口最大可聚合的端口数不小于 2 个, 并保证在普通 VLAN 或启用 SVLAN 条件下各聚合链路内流量的均衡。
- 4) 链路故障时的收敛时间必须小于 800ms, 建议达到 50ms 以内。
- 5) 建议设备支持板间接口的端口的聚合功能。
- 6) 在静态配置环境下, 必须可与其他支持该标准的厂家设备实现良好互通。

4.6 广播抑制

- 1) 设备必须具备广播帧过滤功能, 可通过配置限制每个端口允许通过的最大广播包速率和比例。对广播数据流的带宽限制误差不大于 5%。
- 2) 设备必须支持对组播和未知单播的限制和过滤功能, 可限制每个端口允许通过的最大组播包或未知单播包的速率和比例, 带宽限制误差不大于 5%。

4.7 二层组播

- 1) 设备必须支持 IGMP SNOOPING 二层组播功能, 以实现组播包的二层复

制。

- 2) 设备必须支持 VLAN UNTAG 和 VLAN TAG 接口下的组播复制功能，以及组播组的快速加入和离开。组播组离开延时应小于 20ms。
- 3) 设备必须具备一定的组播业务控制机制，如组播组访问控制、组播用户数限制、单个用户加入的组播组数限制等。
- 4) 设备必须支持跨 VLAN 的组播复制能力，可将一个 VLAN 组播业务复制到多个不同的用户 VLAN 中。
- 5) 设备必须支持 IGMP PROXY 二层组播复制功能。
- 6) 建议园区交换机具备 ANCP 的相关功能，以实现交换机与 BRASE/SR 间交互信息，实现对组播的控制。

4.8 策略控制功能

4.8.1 访问控制

- 1) 设备必须能够在百兆和千兆端口上实现对流量的访问控制功能。
- 2) 设备必须支持二层和三层的访问控制表，可匹配的字段包括：
 - 源 MAC 地址、目的 MAC 地址；
 - 标准 VLAN 环境中的 VLAN ID
 - SVLAN 环境中的内层和外层 VLAN ID；
 - 802.1P 优先级字段；
 - 源 IP 地址、目的 IP 地址；
 - 四层协议类型及源、目的端口号
- 3) 建议园区交换机支持基于 VLAN 端口的访问控制（在 VLAN 端口下，根据 MAC、IP 地址等进行访问控制）；
- 4) 设备必须支持端口入方向和出方向的访问控制。

4.8.2 业务分类

- 1) 设备必须能够识别物理端口、VLAN/SVLAN、IEEE 802.1D 优先级标签（原 IEEE802.1p）、Ethernet 类型、IP 地址、IP 类型、四层协议端口等信息，作为划分业务等级的依据。建议支持报文的深度检测（80 个字节）功能。
- 2) 设备必须可根据数据包所属的业务等级改写其 802.1P COS 等级，以作为其在网络中传递时的业务优先级标识。
- 3) 建议支持 802.1P 优先级和 IP TOS 之间的映射，以及 SVLAN 环境中内、外层 VLAN 标签间 802.1P 的双向（内层到外层，外层到内层）映射。

4.8.3 队列技术

- 1) 设备必须支持将不同等级的业务映射到相应的队列中，并为每个队列配

置相应的带宽保证和转发优先级。

- 2) 设备必须支持严格优先级和轮询等队列技术，可保证严格优先级队列的带宽和转发延时，并可按比例为轮询队列分配带宽。
- 3) 每个端口支持的硬件队列数不小于 4 个，建议支持 8 个。

4.8.4 速率限制

- 1) 设备必须支持基于物理端口和访问控制表等条件进行流量的速率限制。
- 2) 设备必须支持入方向和出方向的速率限制，对超过限制要求的流量能选择处理方式，如允许转发、丢弃、修改优先级等。
- 3) 要求速率限制最小可配置带宽必须不大于 64Kbps，增量颗粒度必须不大于 64Kbps；限制结果必须精确，误差不大于 5%。
- 4) 端口应能在进行速率限制的同时，提供访问控制、队列调度等功能。

4.8.5 拥塞避免

建议设备支持 WRED 拥塞避免机制。

4.9 网络安全

4.9.1 地址绑定

设备必须支持端口与用户 MAC 地址绑定的功能，即该端口只允许源 MAC 为指定 MAC 地址的数据流通过。

建议支持设备端口与用户 IP 地址的绑定。

4.9.2 地址数量限制

设备必须具备对指定端口下的 MAC 地址数量进行限制的功能，且地址数量可灵活配置。对于超过限制值的 MAC 地址不会被加入设备 MAC 地址表，对应的数据流量不被转发。

4.9.3 VLAN 隔离

设备必须支持 VLAN 隔离功能，可以隔离属于同一 VLAN 的物理端口间的互访。

4.9.4 报文过滤及抑制

设备应支持以下报文过滤及抑制功能：

- 过滤来自用户的 DHCP OFFER/ACK/NAK、IGMP 查询报文；
- 可配置丢弃或透传用户侧 BPDU 报文；
- 过滤来自用户端口的组播流；
- 对来自网络侧的非法组播源进行配置和过滤；

- 对特定协议（如 DHCP、IGMP、ARP、PPPoE）的报文进行速率配置。

4.10 以太环网

建议设备支持以太环网，并实现以下功能：

支持环网拓扑自动发现，可动态地增加、减少环路节点；环上各节点具有统一的、可更新的环路拓扑结构图；

提供环保护和网络拓扑自愈恢复功能，在环路或节点发生故障时（光纤中断、节点设备故障等），能够实现自动环保护功能，保护切换时间小于 50ms；

支持环上各节点业务带宽的公平算法。当环上出现拥塞或重负荷时，可保证各节点发送业务的公平性。

4.11 三层功能要求（可选）

- 1) 建议支持 ARP 及 ARP PROXY；
- 2) 建议支持 RIP1/2、OSPFv2 等路由协议；
- 3) 建议支持 IGMP、PIM-DM/SM 等组播路由协议；
- 4) 建议支持 VLL、VPLS 等 L2 MPLS VPN；
- 5) 建议支持 IPv6 基本协议，符合 RFC2460—互联网协议(版本六)。

4.12 其他功能要求

4.12.1 DHCP OPTION 82

设备必须支持 DHCP OPTION 82 功能，可将物理端口信息插入 DHCP Discovery 消息中，传给上层网络设备。

4.12.2 Private VLAN

设备必须支持 Private VLAN 功能，可以隔离属于同一 VLAN 的物理端口间的互访。

4.12.3 VLAN 交换

建议设备支持 VLAN 交换功能，将进入设备的数据包所携带的 VLAN ID 替换为指定的其他 VLAN ID 并转发。

4.12.4 MAC IN MAC

设备可选支持 IEEE 802.1ah 规定的 MAC in MAC 功能，为一个以太网帧加

上第二层（外层）MAC 封装。

5. 性能要求

5.1 MAC 地址学习和缓存能力

5.1.1 MAC 地址学习速度

设备百兆和千兆端口的 MAC 地址学习速度不低于 1000 个/秒。

5.1.2 MAC 地址表容量

设备 MAC 地址表容量不小于 16000 个/设备。

5.2 VLAN 能力

- 1) 单台设备必须支持4094个VLAN同时启用，在开启大量VLAN的情况下不影响设备转发性能。
- 2) 开启选择性SVLAN功能时，园区交换机必须能够并发识别外层4K个VLAN标识、内层4K个VLAN标识。
- 3) 设备所有接口同时开启选择性SVLAN功能时，每端口可识别的用户标签数量必须支持不低于4094个，识别和分配标签过程不能影响设备转发性能。

5.3 转发性能

- 1) 设备的百兆端口和千兆端口对于各种帧长的数据流具备 100%线速转发能力。无拥塞情况下，64 字节数据包转发延时小于 100us。
- 2) 设备长期性能要求为：在高负载条件下（端口流量大于 90%），64 字节以太网帧丢失率小于 10^{-5} 。

5.4 组播处理能力

- 1) 设备可同时支持的组播组数目至少达到 200 个。
- 2) 要求端口加入/离开某个组播组的时间小于 20ms。
- 3) 设备各端口必须实现对组播流的线速转发，且转发单、组播混合流量，以及启用跨 VLAN 组播功能时不出现性能下降。
- 4) 每 FE 端口的跨 VLAN 组播复制能力不小于 8 条，且不影响设备性能。

5.5 访问控制表条目

- 1) 设备每个端口至少可应用一个访问控制表。
- 2) 分布式转发结构交换机单板访问控制列表至少 1000 条；集中式转发结构交换机整机访问控制列表至少 1000 条。
- 3) 要求在应用的访问控制表条目较多时设备的转发性能不出现下降。

6. 运行与维护

6.1 设备集群与堆叠

6.1.1 设备集群

设备必须支持在多台园区交换机之间实现集群管理功能。具体要求如下：

- 1) 可只使用一个管理地址，对集群内的设备进行远程管理。（在主设备上可切换到不同设备进行管理）
- 2) 可通过命令行方式在集群内所有成员间切换管理，并可在主设备上实现对从设备的相关操作，如批量下载、保存、删除从设备的配置，软件升级，重启从设备等功能。
- 3) 可同时支持的集群设备数量不小于 8 台。

6.1.2 设备堆叠

设备必须支持在多台园区交换机之间实现堆叠功能。具体要求如下：

- 1) 可只使用一个管理地址，实现对所有堆叠设备的管理。
- 2) 可在主设备上查询、配置所有堆叠设备的端口。
- 3) 可在主设备上查询、配置所有堆叠设备的 VLAN、生成树协议。
- 4) 可同时支持的堆叠设备数量不小于 8 台。

6.2 命令行功能

- 1) 设备必须支持提供命令行方式的维护管理界面。管理者可通过本地串行接口或远程网络接口登录和操作设备。
- 2) 命令行模式下必须完成设备所有功能的配置。
- 3) 必须具备以下维护功能：
 - 可查询设备当前的软硬件版本、各端口工作状态
 - 可对 MAC 缓存表、ARP 缓存表、端口流量统计等系统表项完成显

- 示、查询和清除的操作
- 可查询当前运行协议的工作状态
- 提供 ICMP PING、TRACEROUTE 等 OAM 工具

6.3 WEB 配置界面

建议设备提供WEB配置管理界面，客户端可通过浏览器对设备进行配置。

6.4 远程访问

- 1) 设备必须支持以 TELNET 方式的远程访问功能。
- 2) 设备必须支持以 SSH 方式的远程访问功能。
- 3) 必须提供源地址限制、最大连接数限制等访问控制功能。

6.5 用户认证

- 1) 设备必须能对登录用户进行认证，并提供本地账号管理和远程认证的功能。
- 2) 设备必须支持 RADIUS 远程认证协议，并支持 RADIUS 扩展属性，可从 RADIUS 返回信息中确定用户的级别和权限。

6.6 日志记录

设备必须支持日志记录（SYSLOG）的功能，可对各类事件记录保存到日志中，并发送给指定服务器。必须支持的记录项目包括：

- 端口状态变化
- 告警
- 设备或模块重启动
- 用户登录及命令操作
- 配置改变

6.7 流量镜像

- 1) 设备必须支持端口镜像功能，可分别将指定端口入方向和出方向的流量镜像到相应端口。
- 2) 必须支持对 VLAN tagged 端口和 untagged 端口的流量镜像。

- 3) 建议支持基于流的镜像功能，可基于访问控制表等手段将符合匹配条件的数据流镜像到指定端口。
- 4) 建议设备支持远程流量镜像功能。

6.8 以太网 OAM

建议设备支持以下标准规定的以太网 OAM 功能：

- IEEE802.1ag
- IEEE802.3ah
- ITU Y.1731

遵循 ITU Y.1731 标准的设备建议支持如下以太网 OAM 故障管理功能：

- 以太网连续性检查 (ETH-CC)
- 以太网环回 (ETH-LB)
- 以太网链路跟踪 (ETH-LT)
- 以太网警告指示信号 (ETH-AIS)
- 以太网远端缺陷指示 (ETH-RDI)
- 以太网锁定信号 (ETH-LCK)
- 以太网测试信号 (ETH-Test)
- 以太网自动保护倒换 (ETH-APS)
- 以太网维护通讯通道 (ETH-MCC)
- 以太网实验用的OAM (ETH-EXP)

遵循 ITU Y.1731 标准的设备建议支持如下以太网 OAM 性能监控功能：

- 帧丢失测量 (ETH-LM)
- 帧延时测量 (ETH-DM)
- 吞吐量测量

遵循 ITU Y.1731 标准的设备必须符合标准规定的以太网 OAM 的帧格式。

6.9 链路故障检测及保护切换

建议设备所有类型的以太网端口支持双向故障检测协议（Bidirectional Forwarding Detection, draft-ietf-bfd-base-02.txt, BFD），并且在通过 BFD 检测到链路故障时能够执行预先设定的动作（如进行保护切换等）。可以在交换机上指定互为备份的链路或 VLAN。

7. 网络管理

7.1 网管协议

- 1) 设备必须支持SNMP v1、SNMPv2网络管理协议,并符合RFC 1157、RFC 1902 - RFC 1906 标准的规定。
- 2) 设备建议支持SNMP v3网管协议。
- 3) 设备必须支持SNMP访问地址限制, 只允许特定地址范围的主机对设备的访问。
- 4) 设备必须支持安全视图的功能, 为不同的网络管理者设置相应的MIB视图浏览权限。

7.2 管理信息库

- 1) 设备必须支持RFC 1213规定的标准管理信息库。
- 2) 设备必须支持以下标准规定的管理信息库:
 - RFC 2513 - Managed Objects for Controlling the Collection and Storage of Accounting Information for Connection-Oriented Networks (February 1999)
 - RFC 2665 - Definitions of Managed Objects for the Ethernet-like Interface Types (August 1998)
 - RFC 2863 - The Interfaces Group MIB (June 2000)
 - RFC 2933 - Internet Group Management Protocol MIB (October 2000)
 - RFC 2981 - Event MIB (October 2000)
 - RFC 3014 - Notification Log MIB (November 2000)
 - RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) (December 2002)
 - RFC 3411 - An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks (December 2002)
 - RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) (December 2002)
 - RFC 3413 -Simple Network Management Protocol (SNMP) Applications (December 2002)
 - RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) (December 2002)

RFC 3415 - View-based Access Control Model (VACM) for the Simple
Network Management Protocol (SNMP) (December 2002)

3) 厂家私有MIB库必须符合RFC 1155和RFC 1212标准的规定。

私有MIB必须包括以下内容：

- 端口
- VLAN信息
- CPU、内存占用率
- 物理资源
- 访问控制和QOS
- 二层组播
- VLAN堆叠（SVLAN）

7.3 网管系统

网管系统必须具备故障管理、配置管理、性能管理和安全管理等主要网管功能。必须提供与第三方网管系统的接口，可以无缝地集成在第三方网管系统上。

7.3.1 配置管理

- 1) 网管系统必须能够自动发现网络拓扑，显示网元间连接关系，并能够动态、实时显示被管网元的运行状态和状况。
- 2) 网管系统必须能够在网络拓扑中创建、删除、查询修改设备。
- 3) 网管系统必须能够对设备软件进行升级，建议网管系统支持集群升级。
- 4) 网管系统必须提供对设备配置信息的上载和下载功能，并支持对配置信息合法性和一致性的检查。
- 5) 网管系统必须能够完成以下功能的配置：
 - 业务端口的打开和关闭、协商参数设置、流控等
 - VLAN的创建、删除、与相应业务端口的关联、VLAN堆叠的配置等
 - 各种生成树功能的开启和关闭、节点和端口权值的设置
 - 二三四层访问控制表的配置、应用
 - 业务分类、优先级队列、速率限制等QOS功能配置
 - 二层组播功能（IGMP SNOOPING）的配置
 - 设备集群和堆叠功能的配置
 - 网管协议、地址的设置

7.3.2 性能管理

- 1) 网管系统必须对网元的重要性能参数（CPU 利用率、内存利用率、数据包分类统计）进行监控。
- 2) 网管系统必须提供性能门限管理，支持对一个监测对象的某个性能参数设置上限和（或）下限，当该监测对象的性能参数超过设定的上限或下限时，产生越限告警。
- 3) 网管系统必须提供查询性能数据的功能，并以表格和图形如折线图、直方图、饼图等方式显示查询结果和统计结果。必须能对查询统计结果进行打印输出。
- 4) 允许指定网元性能监测的属性，并可进行查询/修改，包括：性能监测对象、需要监测的参数名称、监测周期（15 分钟或者 24 小时）、监测状态（打开/关闭）、开始时间、结束时间、是否自动上报。
- 5) 网管系统必须提供性能趋势分析功能，通过对当前和历史性能测量数据的分析，预测性能监测参数今后的变化趋势。
- 6) 性能数据在网管存储设备上保存一定期限的 15 分钟和 24 小时性能。测量周期为 15 分钟的测量数据至少 30 天；测量周期为 24 小时的测量数据至少 60 天。当性能数据的存储超过期限或容量时必须提示用户归档和删除。

7.3.3 故障管理

- 1) 网管系统必须支持对告警类型、告警级别和告警状态的分类定义。
告警类型包括：设备告警、服务质量告警、通信告警、环境告警、处理失败告警
告警级别包括：紧急告警、主要告警、次要告警、提示告警、清除告警
告警状态包括：当前告警、历史告警、已确认告警、未确认告警、锁定告警
- 2) 网管系统必须能够在网络拓扑图中以不同形式显示告警发生的位置及告警信息，并提示用户对告警进行确认。
- 3) 网管系统必须能够对告警信息进行确认、清除、合并、过滤。
- 4) 网管系统必须具有告警相关性抑制功能。根据网络配置信息，以及接收的告警信息频度和种类，对告警信息的关联进行综合分析，在多个告警中确定故障根源。并能以图形显示方式或文本显示方式将设备或通信故障定位在设备板卡或端口上，同时给出可能的故障原因。
- 5) 网管系统必须能够对当前告警或者历史告警提供查询和统计功能。
- 6) 网管系统必须支持告警信息的同步，将显示的告警状态与网元实际的告

警状态进行核准，必须提供人工和自动两种校正模式。

7.3.4 安全管理

- 1) 网管系统必须能够对用户进行管理，包括增加用户、删除用户、锁定用户、解锁用户、查询用户信息、修改用户密码。
- 2) 网管系统必须对用户的访问进行认证、授权。
- 3) 网管系统必须对用户划分等级，不同级别的管理员必须具有不同的权限，访问者只能在自己的权限范围内进行管理操作。敏感信息、或固定用户终端鉴权属性、数据库和配置数据只能由有授权的个人或管理系统进行操作。
- 4) 网管必须提供操作日志记录，以记录网管配置的改变及网管操作人员登录、注销的时间。

8 设备其他要求

8.1 硬件结构要求

- 1) 设备可采用模块化或非模块化结构设计。模块化设备所有板卡必须可替换升级，且各版本硬件良好兼容，提供较高的可用性和可扩展性。模块化设备的板卡、电源等部件必须支持在线热插拔。
- 2) 交换机的总线带宽必须超过其上所有端口带宽之和，实现无阻塞交换。
- 3) 设备应支持不同业务处理板的混插，提高插槽的通用性和灵活性。
- 4) 对于单播组播转发、VLAN 堆叠、策略控制等功能必须采用独立硬件实现，减轻 CPU 压力，确保设备的性能要求。
- 5) 建议设备电源模块支持冗余备份。
- 6) 设备应具有网络故障和硬件故障告警功能。
- 7) 当软件升级时，应不影响硬件结构。
- 8) 对主控模块的要求：
 - 主控模块应具有软硬件故障告警功能。
 - 主控模块应具有故障脱机自动诊断功能以及负荷控制措施。
- 9) 设备应提供过流、过压保护措施。
- 10) 设备机箱必须提供视觉指示(LED)用于显示设备的工作状态和故障告警等情况。
- 11) 设备必须适合安装在标准 19 英寸的机架上。
- 12) 设备必须提供直观、方便的指示灯，建议包括电源指示灯、运行状态指

示灯、端口连接状态指示灯、端口工作模式指示灯、链路活动指示灯等。

8.2 设备软件要求

- 1) 软件要求保证安全可靠，具有容错能力。
- 2) 软件系统须提供数据接口，提供进行二次开发的文档。
- 3) 软件应采用模块化结构，模块之间的通信应按规定的接口进行。
- 4) 应具有软件故障的监视功能，一旦软件出现死循环等重大故障时，应能自动再启动，并做出即时故障报告信息。
- 5) 配置数据与处理程序应有相对的独立性，配置数据的任何变更都不应引起运行版本的变更。
- 6) 软件应有完善、方便的人机通信控制功能。
- 7) 软件应具备方便、迅速地恢复到原来版本的功能。
- 8) 系统软件应能在线升级，不需重新启动。
- 9) 软件应在不中断通信的情况下，完成程序打补丁的功能。
- 10) 不同时期软件版本应能向下兼容，软件版本易于升级
- 11) 软件升级必须可以在线获得。
- 12) 设备必须支持从 FTP 或 TFTP 服务器下载软件/配置文件。
- 13) 设备必须该通过 CMM Level 3 认证，满足对软件开发和质量保证过程的要求。
- 14) 设备必须该通过 ISO 9001 认证，满足对软件开发和质量保证过程的要求。

8.3 供电和环境要求

8.3.1 供电要求

- 1) 交流电压及其波动范围要求：
单相 220V，变化范围为 10%，频率 50Hz，变化范围为 5%，线电压波形畸变率小于 5%。要求设备在此电压范围内正常工作。
- 2) 直流电压及其波动范围要求：
-额定电压：-48V
-电压波动：在直流输入端子处测试的-48V 电压允许变化范围为-57V 至 -40V。要求设备在此电压范围内正常工作。

8.3.2 接地

- 1) 接地方式必须符合工作地、保护地和建筑防雷接地-组接地体的联合接地

方式。

- 2) 接地线截面积根据可能通过的最大电流负荷确定。
- 3) 联合接地电阻值必须小于 5Ω 。

8.3.3 工作环境

- 1) 温度: $5^{\circ}\text{C}\sim 45^{\circ}$
- 2) 相对湿度: $10\%\sim 90\%$
- 3) 温度变化率: $\leq 10^{\circ}\text{C/h}$, 不结露
- 4) 海拔高度: $-500\sim 5000$ 米
- 5) 防尘: 静态条件下测试, 主机房空气中 $\geq 0.5\mu\text{m}$ 的尘粒数, 少于 18000 粒/升

8.3.4 设备抗震加固

设备应具备抗震加固特性。要求抗震设防烈度按 8 度考虑。

8.3.5 防雷

设备防雷击能力必须符合 GB3483-1983 《电子设备雷击实验》。

8.3.6 防电磁干扰

- 1) 设备在受到 0.01-1000MHZ 频率范围内电场强度为 140dBuV/m 的外界电磁干扰时不出现故障和性能下降。
- 2) 在直流或交流电源线受到 0.01-100MHZ 频率范围的外界电磁干扰电流使不出现故障和性能下降。

8.4 绿色要求

8.4.1 设备管理要求

(1) 基本要求

1. 对于机框插槽式设备, 设备应有高温报警功能。
2. 对于机框插槽式设备, 应具备能源监控及管理功能。在设备管理员需要时, 可检测到设备当前能耗状态。
3. 对于机框插槽式设备, 应支持根据实际情况中断未用板卡供电或进入微电状态。

4. 设备电源反灌杂音应满足通信电源 YD/T 1051-2000《通信局站电源系统总技术要求》的要求。

(2) 扩展要求

1. 对于机框插槽式设备，能通过查询方式监控到目前工作状态下能耗，以及设备各个组件，如各板卡、机框、风扇，所消耗的能耗比例。
2. 对于机框插槽式设备，设备可通过命令行或网管工具远程关闭设备部分模块或功能以减少其工作能耗。
3. 对于机框插槽式设备，可根据实际情况动态调整风扇转速。
4. 对于机框插槽式设备和服务器设备，宜具有可根据用户需求和不同应用场合配置交流或直流供电的选择。

8.4.2 设备环保与包装要求

(1) 设备环保要求

设备设计阶段，设备的主要部分（如电路板、机箱、电缆等）应尽量减少铅、镉、汞、六价铬、溴化耐燃剂等有害物质，并严格按 ROHS 规范进行产品生产与设计。

(2) 设备包装要求

实行包装减量化（Reduce）。绿色包装在满足保护、方便、销售等功能的条件下，应是用量最少的适度包装。

包装应易于重复利用（Reuse）或易于回收再生（Recycle）。

包装废弃物可以降解腐化（Degradable）。为了不形成永久的垃圾，不可回收利用的包装废弃物要能分解腐化，进而达到改善土壤的目的。

包装材料对人体和生物应无毒无害，包装材料中不应含有有毒物质或有毒物质的含量应控制在有关标准以下。

包装材料应尽量减少木材的使用。

在包装产品的整个生命周期中，均不应对环境产生污染或造成公害。

(3) 其它要求

设备内部应有合理的气流组织，应采用前进后出或垂直通风方式，不宜从侧面进出通风。

同时，机框式数据设备内风扇应具有自动调节速率的功能，机架内采用防热风回流等技术，降低对机房环境的局部制冷要求。

机架门开孔率：考虑到通风和散热的需求，在保证门的强度和刚度要求前提下，机架正面门和背面门开孔率至少不得低于 30%，以获得良好的排吸风效果。

8.4.3 能耗分级标准

设备能耗等级应达到最新版本的中国电信《绿色数据设备技术规范》所定义的标准。

中国电信集团公司技术标准

Q/CT 2079-2008

中国电信 IP 城域网设备技术规范 (DSLAM)

(V3.0)

2008-12-31 发布

2009-1-1 实施

中国电信集团公司 发布

目 录

1	编制说明.....	1
1.1	范围.....	1
1.2	引用标准.....	1
1.3	定义、术语和缩写.....	3
1.3.1	定义.....	3
1.3.2	术语和缩写.....	3
2	概述.....	4
2.1	定位.....	4
2.2	功能和业务组成.....	4
3	设备容量和接口要求.....	4
3.1	设备容量.....	4
3.2	用户侧接口.....	5
3.3	网络侧接口.....	5
3.4	级联接口.....	5
3.5	管理接口.....	5
3.6	测试总线接口.....	6
4	功能.....	6
4.1	基本功能.....	6
4.1.1	业务接入功能.....	6
4.1.2	DSL 线路功能.....	6
4.1.3	以太网端口功能.....	6
4.1.4	EPON 接口功能.....	6
4.1.5	级联组网功能.....	6
4.2	ATM-DSLAM 功能.....	6
4.2.1	ATM 连接功能.....	6
4.2.2	QoS 功能.....	7
4.2.3	流量控制和拥塞处理.....	7
4.2.4	环回监测功能.....	7
4.2.5	IMA.....	7
4.3	二层 IP-DSLAM 功能.....	7
4.3.1	数据封装功能.....	7
4.3.2	PPPoE 透传功能.....	8
4.3.3	专线业务功能.....	8
4.3.4	VLAN/SVLAN 功能.....	8
4.3.5	用户端口隔离与互访.....	9
4.3.6	端口速率控制.....	9
4.3.7	MAC 地址限制与绑定.....	9
4.3.8	IP 地址与端口绑定.....	9
4.3.9	用户端口标识和可溯源性.....	9
4.3.10	流量控制.....	10
4.3.11	拥塞处理.....	10
4.3.12	报文过滤.....	10

4.3.13	报文抑制.....	10
4.3.14	端口汇聚（TRUNK）	10
4.3.15	端口镜像.....	10
4.3.16	生成树（Spanning Tree）协议.....	11
4.3.17	安全.....	11
4.3.18	组播功能.....	11
4.3.19	QoS 功能.....	12
4.4	三层 IP-DSLAM 功能（可选）	13
5	设备性能.....	14
5.1	基本性能.....	14
5.1.1	传输性能.....	14
	参见中国电信接入网相关技术规范。	14
5.1.2	多 PVC 处理能力	14
5.1.3	线路同步时间.....	14
	参见中国电信接入网相关技术规范。	14
5.1.4	误码性能.....	14
5.1.5	业务兼容性.....	14
5.1.6	设备恢复.....	14
5.2	ATM-DSLAM 性能	14
5.2.1	ATM 信元传送性能指标	14
5.2.2	视频业务性能.....	15
5.3	二层 IP-DSLAM 性能.....	15
5.3.1	MAC 地址缓存能力.....	15
5.3.2	VLAN 性能.....	15
5.3.3	转发性能.....	16
5.3.4	SAR 转发能力	16
5.3.5	组播性能.....	16
5.3.6	视频业务性能.....	16
5.4	三层 IP-DSLAM 性能（可选）	17
5.4.1	最大活动连接数.....	17
5.4.2	并发用户数.....	17
5.4.3	认证平均建链时间.....	17
5.4.4	每秒同时建链次数.....	17
5.4.5	包转发能力.....	17
5.4.6	IP 丢包率	18
5.4.7	NAT 数据包转发能力	18
5.4.8	NAT 最大连接数	18
5.5	设备恢复时间.....	18
6	设备管理功能.....	18
6.1	一般要求.....	18
6.1.1	设备的管理方式.....	18
6.1.2	管理的安全要求.....	19
6.2	基本管理功能.....	19
6.3	配置管理功能.....	20

6.4	故障管理功能.....	22
6.5	性能管理功能.....	23
6.6	安全管理功能.....	24
6.7	DSL 线路自动测试功能	24
6.8	DSL 终端远程管理功能	25
7	设备其他要求.....	25
7.1	设备硬件要求.....	25
7.2	机箱要求.....	26
7.3	线缆管理.....	26
7.4	设备可用性.....	26
7.5	设备软件要求.....	27
7.6	环境要求.....	28
7.7	绿色要求.....	28
7.7.1	设备管理要求.....	28
7.7.2	设备环保与包装要求.....	29
7.7.3	能耗分级标准.....	30

1 编制说明

1.1 范围

本技术规范以 RFC 文档、ITU-T 以及 IEEE 标准为依据，针对中国电信实际情况和具体要求，对 IP 城域网中 DSLAM 设备在 IP 组网方面的硬件要求、接口要求、功能、设备性能、设备管理功能等进行了规定，重点放在 IP 城域网整体框架要求下对 DSLAM 设备网络侧联网所需功能和参数的规范上，用户侧各类接入技术的具体参数指标要求、用户环路的管理等内容请详见中国电信接入网相关技术规范的规定。

本技术规范适用于中国电信集团 DSLAM 设备的引入和改造。

在本规范中：

- (1) 必须：表示该条目是本规范必须。违反这样的要求是原则性错误。
- (2) 必须实现：表示该要求必须实现，但不要求缺省使能。
- (3) 不允许（不可以）：表示该条目绝对禁止。
- (4) 应当（建议）：表示在某些特定条件下存在忽视该条目的理由，但是忽视或违反该条目时必须仔细衡量。
- (5) 应当（建议）实现：与应当（建议）类似，实现时不必要缺省使能。
- (6) 不应当（不建议）：表示在某些特定条件存在所描述行为可接受或有效的理由，但实现该行为时必须仔细衡量。
- (7) 可以：表示该条目确实可选。

1.2 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。

GB/T17625.1-2003	《电磁兼容 限值 谐波电流发射限值(设备每相输入电流≤16A)》
GB17625.2-1999	《电磁兼容 限值 对额定电流不大于 16A 的设备在低压供电系统中产生电压波动和闪烁的限制》
YD/T 1051-2000	《通信局站电源系统总技术要求》
SPECpower_ssj2008	标准效能公司能耗测试标准
能源之星 4.0	主要针对消费性电子产品的能源节约计划。
COC on Energy Consumption of	宽带设备能源消耗管理

Broadband Equipment

GB2423-89	电工电子产品的基本环境试验规程试验
GB4798.3-90	电工电子产品应用环境条件 有气候防护场所固定使用
YD/T 1082-2000	接入网设备过电压过电流防护及基本环境适应性技术条件
YD/T 1185-2002	接入网技术要求—单线对高比特率数字用户线（SHDSL）
YD/T 1244-2002	数字用户线（XDSL）设备电磁兼容性要求和测量方法
YD/T 1348-2005	接入网技术要求—不对称数字用户线（ADSL）自动测试系统
YD/T 1475-2006	《接入网技术要求——基于以太网方式的无源光网络（EPON）》
ITU-T G.992.5	频谱扩展的第二代不对称数字用户线（ADSL2+）收发器
ITU-T G.993.2	第二代甚高速数字用户线（VDSL2）收发器
RFC0768(1990)	UDP 协议
RFC0791(1990)	IP 协议
RFC0792(1990)	ICMP 协议
RFC0793(1990)	TCP 协议
RFC0854(1990)	TELNET 协议
RFC0855(1990)	Telnet 协议选项规范
RFC0858(1990)	Telnet 抑制前进选项
RFC0894(1990)	在以太网上传输 IP 数据包的标准
RFC1155 (1990)	基于 TCP/IP 的互连网管理信息的结构和标识
RFC1157(1990)	简单网络管理协议（SNMP）
RFC1213 (1991)	基于 TCP/IP 的互连网的网络管理信息库：MIB-II
RFC1321(1992)	MD5 算法
RFC1332(1992)	IPCP 协议
RFC1334(1992)	PAP 协议
RFC1631(1994)	IP 网络地址转换器(NAT)
RFC1661(1994)	PPP 协议
RFC1990(1996)	PPP 多链协议
RFC1994 (1996)	CHAP 协议
RFC1662(1994)	在类 HDLC 帧中的 PPP 协议
RFC2364 (1998)	PPP Over AAL5
RFC 2516 (1999)	传输 PPPoE 之方法
RFC 2615 (1999)	PPP over SONET/SDH 协议

RFC 1483 (1993)	AAL5 上的多协议封装
RFC 2138(1997)	RADIUS 协议
RFC 2139(1997)	RADIUS 计费协议
RFC1112	组播管理协议 V1
RFC2236	组播管理协议 V2
RFC2933	IGMP MIB
RFC3046	DHCP 中继代理信息选项

1.3 定义、术语和缩写

1.3.1 定义

数字用户线接入复用器 (Digital Subscriber Liner Multiplexer, 简称 DSLAM) 是面向宽带网络应用的接入设备, 它是 DSL 接入复用设备, 位于 DSL 宽带接入的局端。

1.3.2 术语和缩写

ACL	Access Control List (访问控制列表)
ADSL	Asymmetric Digital Subscriber Line (非对称数字用户线)
ADSL2+	(频谱扩展第二代不对称数字用户线)
ATM	Asynchronous Transfer Mode (异步传递模式)
BS	Bit Switch (比特交换)
CDR	Call Detail Record (呼叫记录信息)
DSLAM	Digital Subscriber Line Access Multiplexer (数字用户线接入复用器)
DPBO	Downstream Power back-of (下行功率下调)
EPON	Passive Optical Network Based on Ethernet (无源以太光网络)
GE	Gigabits Ethernet (千兆以太网)
IGMP	Internet Group Management Protocol (互联网组管理协议)
MAN	Metropolitan Area Network (城域网)
PPP	Point To Point Protocol (点到点协议)
PPPOA	PPP Over AAL5
PPPOE	PPP Over Ethernet
POTS	(Plain Old Telephone Service) 普通电话业务

PSD	PowerSpectralDensity（功率谱密度）
PVC	Permanent virtual circuit (永久虚连接)
QOS	Quality Of Service （服务质量保证）
RADIUS	Remote Authorization Dial In User Service （远程认证拨号用户服务）
SNMP	Simple Network Management Protocol （简单网络管理协议）
SHDSL	Symmetrical High-Speed Digital Subscriber Loop（对称高速数字用户线）
UPBO	Upstream Power back-of（上行功率下调）
VDSL	Very-high-bit-rate Digital Subscriber loop （甚高速数字用户环路）
VDSL2	Very High Speed Digital Subscriber Line 2（第二代甚高速数字用户线）
VLAN	Virtual LAN

2 概述

2.1 定位

城域网 DSLAM 设备主要需要具备二层功能。内置 BAS 功能、或/和三层路由功能的 DSLAM 设备不是主流方式,可根据业务发展需要在一些特殊场合少量使用。鉴于 ATM 资源的紧张和网络 IP 化的趋势,城域网 DSLAM 应以 IP-DSLAM 为主, ATM-DSLAM 作为一种补充,可以用于满足部分对安全性和 QoS 要求高的大客户业务需要。

2.2 功能和业务组成

DSLAM 作为 DSL 业务的局端设备,其功能分为两部分:线路功能模块和业务功能模块,线路功能模块和业务功能模块处于相对独立的层次上,能够自由组合,实现不同线路接入方式和不同业务功能的灵活组合。DSLAM 设备除了支持好普通宽带上网的同时,应能很好地支持视频、组播业务;能够提供差异化服务,根据不同的业务需求提供相应的 QoS 保证;能实现端口和用户绑定功能;能为大客户提供较完善的安全解决方案;能提供足够的交换能力、总线带宽、上联接口,以支持高带宽的应用。

3 设备容量和接口要求

3.1 设备容量

1. 同一厂家必须可同时提供大容量机框式、小容量盒式两种类型的设备。
2. 建议机框式设备的单板容量为: ADSL 在 32 线以上, VDSL2 在 24 线以

上。

3.2 用户侧接口

1. 用户侧接口要求参见中国电信接入网相关技术规范。

3.3 网络侧接口

1. 网络侧接口必须支持 Ethernet 接入方式，可选支持 ATM 接入方式。
2. IP-DSLAM 设备至少应提供一个以太网（FE/GE）上行接口，如果单节点 DSL 端口容量超过 100 线，IP-DSLAM 必须支持两个以上的 GE 上联接口；必须支持两个或两个以上同时工作的上联接口，以使不同的业务走不同的上联接口。
3. 建议设备提供 10GE 接口。
4. 对于小容量（满配置小于 100 线）设备建议提供 EPON 上联接口。
5. 以太网上行接口要求
 - FE 接口应符合 IEEE 802.3u 规范的 100Base-T/100Base-FX 接口。
 - GE 接口应符合 IEEE 802.3z 规范的 1000Base-X（SX、LX、CX）和 1000Base-T 接口。
 - 10GE 接口应符合 IEEE 802.3ae 规范。
6. ATM 上行接口要求
 - ATM-DSLAM 上行接口必须支持 ATM 155Mb/s 接口，可选支持 ATM 622Mb/s 接口。ATM STM-1/4 接口应为符合 YD/T 1109-2001 《ATM 交换机技术规范》 6.4.1.3 节和 6.4.1.4 节相关要求的接口。

3.4 级联接口

1. DSLAM 设备必须至少提供一个用于级联的接口，建议提供多个级联接口。
2. 设备必须支持星型级联方式。

3.5 管理接口

1. DSLAM 设备必须提供用于本地维护管理的管理接口（Console 口）。
2. DSLAM 必须提供用于远程集中维护管理的带外管理接口（100BASE-T）。
3. 网管接口应支持 SNMP v1（RFC1157）和 SNMPv2，建议支持 SNMPv3。

3.6 测试总线接口

大容量设备（满配置大于300线）应具备测试总线接口，符合YD/T 1348-2005《接入网技术要求—不对称数字用户线（ADSL）自动测试系统》的相关规定。

4 功能

4.1 基本功能

4.1.1 业务接入功能

参见中国电信接入网相关技术规范。

4.1.2 DSL 线路功能

参见中国电信接入网相关技术规范。

4.1.3 以太网端口功能

参见中国电信接入网相关技术规范。

4.1.4 EPON 接口功能

参加中国电信接入网相关技术规范。

4.1.5 级联组网功能

参加中国电信接入网相关技术规范。

4.2 ATM-DSLAM 功能

DSLAM 设备必须具有 ATM 层、物理层的传输会聚（TC）子层和物理媒质（PM）子层的功能。

4.2.1 ATM 连接功能

ATM 连接功能应支持 ATM VP 和 VC 连接，具体连接功能包括：

1. ATM PVC

DSLAM 设备应支持 ATM PVC 连接，系统应能支持 VP 级或/和 VC 级的 ATM 交叉连接，并且支持下列两种连接结构：

- 双向点对点连接（必选）

- 单向点对多点连接（可选）

2. ATM SVC

DSLAM 设备可选支持 ATM SVC 连接, 和 ITU-T E.164 寻址方式。支持 ATM SVC 连接时系统应能支持两种连接结构:

- 双向点对点连接（必选）
- 单向点对多点连接（可选）

4.2.2 QoS 功能

DSLAM 设备应支持针对每个 VC 的 ATM-QoS 机制, 且 ATM-QoS 机制能支持 CBR（必选）、UBR（必选）、rt-VBR（可选）、nrt-VBR（可选）、ABR（可选）等类型, 并能根据业务发展需要进行任意配置。

4.2.3 流量控制和拥塞处理

ATM-DSLAM 设备必须提供以下流量控制和拥塞控制功能:

- 使用参数控制（UPC/NPC）（必选）
- 优先级控制（PC）（必选）
- 选择信元丢弃（必选）
- 连接接纳控制（CAC）（必选）
- 网络资源管理（NRM）（可选）
- 流量整形（可选）

4.2.4 环回监测功能

设备必须支持业务的 F4、F5 环回监测功能。

4.2.5 IMA

DSLAM 必须应支持 ATM E1 IMA(Inverse Multiplexing over ATM)功能。厂家应说明其设备支持的 IMA E1 的最大数目。

4.3 二层 IP-DSLAM 功能

4.3.1 数据封装功能

当提供 ADSL、ADSL2+或 SHDSL 接入时, IP-DSLAM 必须支持 RFC1483 桥接/路由的数据包封装功能。

4.3.2 PPPoE 透传功能

设备必须支持二层桥接的 PPPoE 数据包的透传。

4.3.3 专线业务功能

设备必须支持基于用户端口的桥接或路由专线业务。

4.3.4 VLAN/SVLAN 功能

4.3.4.1 基本功能要求

(1) 对于来自用户侧的 untagged 报文，设备必须能够根据需要添加 SVLAN-Tag 或 (SVLAN-Tag+CVLAN-Tag) 标记；

(2) 对于来自用户侧的携带有 CVLAN-Tag 标记的报文，设备必须能够根据需要添加 SVLAN-Tag 标记；

(3) 对于来自网络侧的报文，在发送到用户端口以前，设备必须能够根据需要删除 SVLAN-Tag 标记或 (SVLAN-Tag+CVLAN-Tag) 标记；

(4) 802.1ad VLAN tag 中的 EtherType 字段，应至少支持 0x88a8；为了向上兼容性考虑，该字段在 DSLAM 上必须可配置。

4.3.4.2 VLAN tagged 报文处理机制

(1) 对于配置为接收“VLAN Tagged”报文的端口，设备应具有端口的 VLAN 成员表配置功能。设备应丢弃所接收到的与 VLAN 成员表不匹配的 VLAN Tagged 报文。

(2) 对于配置为接收“VLAN Tagged”报文的端口，设备应支持为 VLAN 成员表配置相应的 VLAN 转换表，该表可以有以下两种情况：

- 指定 S-VID 替换用户侧的 C-VID

- 指定 (C-VID+S-VID) 替换用户侧的 C-VID

(3) 对于端口 VLAN 成员表中的每一个 C-VID，设备必须支持以下两种配置方式：

- 接受所接收到的 VLAN 优先级标记

- 根据规则重置优先级标记

(4) 下行方向，设备必须完成反向 VLAN 转换和必要的标记修改功能，还原用户侧的 C-VID。但时，下行报文的 C-Tag 优先级标记则不需要修改。

4.3.4.3 VLAN 映射要求

(1) 用户侧为多 PVC 应用场景：

- 对于 untagged 报文，设备应支持同一端口的不同 PVC 到不同 SVLAN-Tag 以及不同 PVC 到相同 SVALN-Tag 的映射；
- 对于 VLAN tagged 报文，设备应支持 PVC 到 SVLAN-Tag 映射的唯一性，而 CVLAN-Tag 保持不变。

(2) 用户侧为 untagged/priority-tagged 的单 PVC 应用场景：

- 对于同一端口的不同报文，设备应支持根据以太网类型进行 SVLAN-Tag 映射；并支持 priority-tag 到 SVLAN-Tag 的映射。

4.3.5 用户端口隔离与互访

IP-DSLAM 设备必须支持同一 VLAN 的不同用户端口的二层隔离，并能支持特定业务发展情况下同一 VLAN 下不同用户的互联互通。

4.3.6 端口速率控制

IP-DSLAM 必须具有对用户上下行接入速率进行控制的能力，接入速率控制颗粒度应不超过 64kb/s，速率控制误差小于 5%。

4.3.7 MAC 地址限制与绑定

1. IP-DSLAM 必须具有限制单端口下用户 MAC 地址数量的功能，且 MAC 地址数量可以灵活配置。
2. IP-DSLAM 必须具有支持端口与用户 MAC 地址的静态绑定的功能，可以选择支持端口与用户 MAC 地址动态绑定的功能。

4.3.8 IP 地址与端口绑定

IP-DSLAM 必须具有支持端口与用户 IP 地址的静态绑定的功能，可以选择支持端口与用户 IP 地址动态绑定的功能。

4.3.9 用户端口标识和可溯源性

1. IP-DSLAM 设备必须能实现用户的唯一标识和定位功能，能配合 BRAS 设备实现根据用户 MAC/IP 地址，查找用户所在端口的功能。
2. 设备必须支持选择性 SVLAN 和 DHCP option82 方式实现用户端口标识和可溯源性，建议支持 PPPoE+、VBAS 方式实现用户端口标识和可溯源性。
3. IP-DSLAM 设备向 BRAS 提供的用户接入线路信息应满足中国电信企业标准《中国电信宽带用户接入线路标识编码格式要求》。

4.3.10 流量控制

1. 设备应在不对设备整体性能存在影响的前提下，支持 10/100M 全双工、10/100M 半双工和千兆端口的流量控制功能。
2. 设备应支持全双工方式下的 802.3x 规定的 pause 流量控制协议，支持半双工方式下的反压流量控制功能。

4.3.11 拥塞处理

1. 当用户流量总和不大于上/下行端口设定速率时，设备应能实现数据无丢包转发。
2. 当用户流量总和大于上/下行端口设定速率时，设备应具有高性能的数据处理芯片和比较大的缓存区，保证数据的及时处理并尽量减少数据突发情况下的丢包。

4.3.12 报文过滤

设备应支持以下报文过滤功能：

- 基于源/目的MAC地址、以太网类型、VLAN、源/目的IP地址、IP层协议类型、源/目的L4（TCP/UDP）端口的过滤；
- 过滤来自用户的DHCP OFFER/ACK/NAK、IGMP查询报文；
- 可配置丢弃或透传用户侧BPDU报文；
- 过滤来自用户端口的组播流。
- 对来自网络侧的非法组播源进行配置和过滤。

4.3.13 报文抑制

为防止形成广播风暴，设备应支持对广播/组播包进行速率抑制，并支持针对特定协议（如DHCP、IGMP、ARP、PPPoE）的报文进行速率配置。

4.3.14 端口汇聚（TRUNK）

当设备提供 2 个或多个可同时使用的 FE 或 GE 以太网上联接口时，设备应支持端口汇聚功能，实现链路备份和流量分担。设备实现该功能时应支持 IEEE 802.3ad 标准，并能与其他支持该标准的厂家设备互通。

4.3.15 端口镜像

建议设备支持以太网端口镜像功能，包括一对一和一对多两种方式。

4.3.16 生成树（Spanning Tree）协议

1. 设备必须支持符合 IEEE 802.1d 标准的生成树协议，简单拓扑环境下（网络层次不大于 2 层）链路收敛时间不大于 50 秒。
2. 设备必须支持快速生成树协议，简单拓扑环境下（网络层次不大于 2 层）链路收敛时间不大于 3 秒。
3. 建议支持 IEEE 802.1Q 规定的 MSTP 协议。

4.3.17 安全

（1）MAC 地址控制

- 对于来自用户端口的目的地址为保留地址的MAC帧，设备应按照缺省行为及可配置的方式进行处理。
- 为防止MAC洪泛（flooding）攻击，设备应能够限制每个用户端口学习到的源MAC地址数，限制的MAC地址数量应能够基于用户端口进行配置。
- 为防止MAC地址盗用，设备对MAC地址重复的用户应可设置为正常提供业务或拒绝提供业务。

（2）防 DoS 攻击

建议设备支持防止Ping of Death、SYN flood、Land攻击、IP欺骗等DoS攻击。

4.3.18 组播功能

4.3.18.1 组播协议

设备应支持IGMP V1（RFC 1112）、IGMP V2（RFC 2236）协议，可选支持IGMP V3和组播管理协议的MIB（RFC2933）。

设备应支持IGMP SNOOPING和IGMP PROXY功能，在IGMP PROXY下，IP地址可配置。

4.3.18.2 组播传送方式

设备应支持组播业务静态直接送抵DSLAM和动态申请送抵DSLAM的两种业务传输方式。

设备应支持专用组播VLAN，即组播业务使用独立的、专用的VLAN与其他业务相隔离的应用方式。

设备应支持不同VLAN/SVLAN间的组播复制功能。

4.3.18.3 组播控制

(1) 组播权限控制

- 设备应具有本地和远程查询、配置用户频道访问权限的功能，用户的频道访问权限分为禁止、预览和允许三种。
- 频道预览应能够配置针对单次预览的持续时长、预览次数、预览间隔时长以及预览总时长参数。
- 设备应支持预览权限复位功能，可通过设定时间方式进行自动复位。
- 建议设备具备ANCP的相关功能，以实现DSLAM与BRAS/SR间交互信息，实现对组播的控制。

(2) 组播业务管理

- 设备应支持用户端口同时请求的组播数可配置。
- 用户端口在带宽不够的情况下,用户的组播请求应不成功。
- 设备应支持组播源地址检查功能，以避免在用户端口下存在多个STB时单一STB离开某组播组造成的观看同一组播组的其他STB点播中断的现象。
- 设备应支持组播业务暂停、恢复功能，方便进行欠费用户的配置管理。

4.3.18.4 CDR要求

设备应支持CDR（Call Detail Record）呼叫信息记录功能，记录用户的基本访问信息（包括IGMP请求成功/失败，用户标识，何时加入，何时离开，离开方式（强制、自主离开），访问的频道，频道权限，CDR记录产生时间等）。短时间的组播加入离开可不作CDR记录要求，具体时间参数可配置；短时间的组播预览可不作计时要求，具体时间参数可配置。

设备应支持CDR信息定时同步到管理系统，确保CDR信息不丢失。

4.3.19 QoS 功能

4.3.19.1 流分类

设备应支持以下流分类方法：

- 基于物理端口
- 基于PVC
- 基于用户CVLAN-Tag
- 基于Ethernet类型，（例如PPPoE、IPoE等）
- 基于IP地址
- 基于TCP、UDP端口

建议支持基于报文的深度检测（80个字节）分类。

4.3.19.2 业务流标记功能

设备应根据报文分类实现S-Tag或（S-Tag+C-Tag）的标记；
设备应根据报文分类实现802.1D优先级标记功能；
建议设备支持根据报文分类实现IP字段的TOS及DSCP标记功能。

4.3.19.3 优先级队列管理

设备应支持优先级队列与优先级标签之间的映射；
网络侧每个端口应支持8个优先级调度队列；
用户侧每个端口应至少支持4个优先级调度队列，建议支持6个优先级调度队列；
平均每个端口的队列长度应不小于512Kbytes，建议每调度队列Buffer长度可配置；
建议支持队列缓存的板卡级动态统计复用功能；
设备应支持不同优先级队列之间的严格优先级队列调度算法SP；
设备应支持同一优先级队列内部的加权循环队列调度算法WRR或SP+WRR；
建议支持加权公平队列调度WFQ。

4.3.19.4 业务流限速

设备应支持针对不同分类流的速率控制功能，速率控制精度优于5%。
设备应支持以下几种业务流限速方法：

- 基于VLAN/SVLAN
- 基于PVC
- 基于用户端口

对超速的数据包应可选择丢弃和优先级重标记两种处理方式。

4.3.19.5 拥塞避免

设备应支持 Tail-Drop、RED、WRED 算法中的一种，建议支持 WRED 算法。

4.4 三层 IP-DSLAM 功能（可选）

设备可以选择支持以下一些三层功能：

1. 内置 BAS 功能，支持 PPPoE、WEB 或 802.1x 认证。
2. 支持用户 IP 地址动态和静态两种分配方式，并能够对用户端口获得的 IP 地址数量进行限制。
3. 支持 L2TP 协议和 VPDN LAC 功能。
4. 支持静态路由、RIPv2 或 OSPF。
5. 支持 IP 组播 IGMPv2 或 PIM-SM（RFC2362）。

5 设备性能

5.1 基本性能

5.1.1 传输性能

参见中国电信接入网相关技术规范。

5.1.2 多 PVC 处理能力

设备应具有单端口的多PVC处理能力，每个用户端口可同时配置的PVC数目应不少于6条。

5.1.3 线路同步时间

参见中国电信接入网相关技术规范。

5.1.4 误码性能

参见中国电信接入网相关技术规范。

5.1.5 业务兼容性

参见中国电信接入网相关技术规范。

5.1.6 设备恢复

指设备断电后重新上电到业务恢复的过程。设备恢复后必须返回到设备断电前的运行状态。

建议设备恢复时间不超过 3 分钟。

5.2 ATM-DSLAM 性能

5.2.1 ATM 信元传送性能指标

本技术规范定义了 3 个 QoS 级别的 ATM 信元传送性能指标：QoS 级 1、QoS 级 3 和 QoS 4。QoS 级 1 对应对信元丢失要求严格的应用，QoS 级 3 对应延迟低、面向连接的数据传送应用，QoS 级 4 对应延迟低、无连接的数据传送应用。表 1 定义了 STM-1 和 STM-4 接口的 3 个 QoS 级别的性能指标，QoS 级 1、3、4 的性能指标是按照 ATM 连接所通过的接口在 80% 负荷条件下确定的。

表一 对发送信元到 STM-1 或 STM-4 接口的 ATM 连接经过一个 ATM 交换部分性能指标

性能参数	CLP	QOS级1连接	QOS级3连接	QOS级4连接
信元丢失率CLR	0	$\leq 2 \times 10^{-10}$	$\leq 10^{-7}$	$\leq 10^{-7}$
信元丢失率CLR	1	不规定	不规定	不规定
信元差错率CER	1/0	$\leq 10^{-12}$	$\leq 10^{-12}$	$\leq 10^{-12}$
信元传输时延 CTD (99%概率)	1/0	150 μ s	150 μ s	150 μ s
信元传输时延抖动CDV(10^{-10} 量级)	1/0	250 μ s	不规定	不规定
信元传输时延抖动CDV(10^{-7} 量级)	1/0	不规定	250 μ s	250 μ s

5.2.2 视频业务性能

1. DSLAM 设备从背板容量、业务引擎、设备转发能力和网络侧接口等方面应确保视频业务所需要的带宽。
2. DSLAM 设备业务端口、系统应能提供足够大的缓存 (Buffer)、具有抵抗网络流量瞬间突变的能力，确保视频业务的性能。
3. 建议设备支持专门的视频/组播总线。

5.3 二层 IP-DSLAM 性能

5.3.1 MAC 地址缓存能力

IP-DSLAM 的 MAC 地址缓存能力应不低于 4096 个, 平均每用户端口的 MAC 地址缓存能力应不低于 8 个, 每个用户端口的最大 MAC 地址缓存能力应不低于 64 个。

5.3.2 VLAN 性能

- (1) 对于大容量设备 (GE、ATM STM-4 及以上接口), 每个上联端口支持的 VLAN 数目应不少于 4K, 对于中小容量设备, 每个上联端

口支持的 VLAN 数目应不少于 2K，且设备支持的 VLAN ID 应能够在 0~4095 之间灵活配置。

- (2) 在开启大量 VLAN 的情况下不影响设备转发性能。

5.3.3 转发性能

设备主交换板应支持全GE线速转发；

各类线卡转发能力参见中国电信接入网相关技术规范。

设备用户单板槽位带宽应大于设备用户板卡的处理能力。

5.3.4 SAR 转发能力

指 IP-DSLAM 上行将 ATM 信元转化成以太网帧和下行将以太网帧转化成 ATM 信元的能力，应该支持支持线速转发。

5.3.5 组播性能

- 设备每用户板卡应同时支持不少于255个组播组数，单个用户端口同时支持组播组数量不少于4个。
- 设备每秒处理IGMP协议报文的能力应不小设备端口数量的25%（暂定）。
- 设备应具备每用户端口最大连接速率下的线性复制能力。
- 在组播流已递送到设备的情况下，用户终端从发送IGMP请求报文到设备开始向该用户终端发送组播数据报文的时间应不超过100ms。
- 在fast leave模式下，用户终端从发送IGMP离开报文到DSLAM设备停止向该用户终端发送组播数据报文的时间应不超过100ms。
- 设备上联端口应能实现对组播流的线速转发，并且在处理单播和组播混合流量时不出现性能的下降。
- 建议设备支持专门的视频/组播总线。

5.3.6 视频业务性能

1. DSLAM 设备从背板容量、业务引擎、设备转发能力和网络侧接口等方面应确保视频业务所需要的带宽。
2. DSLAM 设备业务端口、系统应能提供足够大的缓存、具有抵抗网络流量瞬间突变的能力，确保视频业务的性能。
3. 建议设备支持专门的视频/组播总线。

5.4 三层 IP-DSLAM 性能（可选）

5.4.1 最大活动连接数

最大活动连接数指内置于 IP-DSLAM 的 BAS 功能能够同时支持的活动连接数量。

建议 IP-DSLAM 支持的最大活动连接数量在 2000 个以上。

5.4.2 并发用户数

并发用户数指 IP-DSLAM 支持的同时发起认证请求并成功建立连接的最大用户数。

建议并发用户数不少于单节点 IP-DSLAM 最大容量的 5%。

5.4.3 认证平均建链时间

认证平均建链时间指在一定负荷条件下，一段时间内每次从发起认证请求到建立连接的平均时间。

本技术规范规定为在 30%最大活动连接数的成功连接条件下，以每秒 2%的最大活动连接数速度向 IP-DSLAM 发起 10%最大活动连接数的认证请求，计算认证成功次数的平均每次建链时间。

建议认证的平均建链时间不超过 5 秒。

5.4.4 每秒同时建链次数

每秒同时建链次数指一段时间内，认证连接成功建立总次数与所花时间的比。

本技术规范规定每次同时发起 2%的最大活动连接数，直到达到 IP-DSLAM 的最大活动连接数，计算成功建立认证连接的总数与所占用的时间的比。

每秒同时建链次数应不少于最大活动连接数的 2%。

5.4.5 包转发能力

包转发能力指 IP-DSLAM 在建立认证连接的情况下，上联以太网口对数据包的转发能力。

本技术规范规定单个上行以太网口的包转发能力在 64Byte 长度情况下应达到 100kpps，建议达到线速转发能力。

5.4.6 IP 丢包率

指 IP-DSLAM 在稳定的持续负荷条件下，应该转发的数据包中不能转发的数据包所占的比例。

本技术规范规定 IP-DSLAM 在 10%吞吐量的负荷条件下的 IP 丢包率不超过 0.05%；在 90%吞吐量的负荷条件下的 IP 丢包率不超过 2%。

5.4.7 NAT 数据包转发能力

指在启用 NAT 功能的情况下，上行以太网端口对数据包的转发能力。

本技术规范规定在 64Bytes 长度的报文下，单个以太网接口 NAT 的数据包转发能力应能达到 100Kpps，建议达到线速转发。

5.4.8 NAT 最大连接数

建议 IP-DSLAM 的 NAT 最大连接数能够同时支持最大活动连接用户数建立连接。

5.5 设备恢复时间

设备恢复时间指设备断电后重新上电到业务恢复整个过程所花的时间。设备恢复后必须返回到设备断电前的运行状态。

设备恢复时间应不超过 3 分钟。

6 设备管理功能

6.1 一般要求

6.1.1 设备的管理方式

1. 设备必须能通过其所带的 Console 口以接受本地维护终端对其的管理维护操作。
2. 设备必须支持经 Telnet 方式远程对其进行管理。
3. 设备可以支持远程 WEB 方式的管理。
4. 设备必须支持通过管理系统远程进行集中管理。其管理软件建议可以单独操作，也可以在第三方网管平台上运行，网管系统应提供与上一级网络管理系统相对接的接口。带外访问与带内访问方式应提供一致的管理功能。厂家应说明网管系统采用的硬件和软件平台。

6.1.2 管理的安全要求

5. 设备必须提供一种方法来记录配置的改变，记录操作人员改变配置的动作和时间。设备必须提供安全性审计的功能。
6. 设备必须具有良好的访问控制。对设备的所有网管操作都必须能配置成需要经过认证和授权。建议设备支持设置 SNMP 的访问级别。设备不允许存在未记载于文档的访问后门或通用密码。
7. 设备的远程配置能力缺省情况下应是不允许的。在允许远程配置前，设备必须通过本地操作终端进行有效的授权。
8. 设备必须能被 SNMP RFC1157 (STD0015) 管理；必须支持 SNMP v2，建议支持 SNMP v2C 或 v3 的管理。所有的 SNMP 操作必须实现。

6.2 基本管理功能

1. 设备必须提供配套网元管理系统：
 - 网管系统应支持分级、分权、分域管理。
 - 网管系统必须具有网络拓扑结构的自动发现功能，并能够清晰的显示设备各面板视图，并对各种板卡进行清晰标识。
 - 网管系统应具备对设备进行配置管理、故障管理、性能管理和安全管理方面的功能。
 - 网管系统应支持不少于 5 台远程终端同时对设备进行管理，管理能力应不少于 60 万 DSL 端口。
 - 网管系统应提供环境电源监控管理、ADSL 线路自动测试、ADSL 用户终端远程管理等功能。
 - 网管系统应具有在线下载版本、在线版本升级等版本管理功能，保存数据、下载数据、上载数据等数据管理功能及主备倒换、主备同步数据等备机管理功能。
 - 网管应提供 DSLAM 设备软件在线升级功能，该功能不应对用户业务造成大的影响。
 - 网管系统应具有良好的图形用户界面和在线帮助、网络软件下载、手动和自动参数配置等功能。
 - 建议网管系统采用中文界面。
2. 设备应具备可管理性，设备应支持通过 CONSOLE 口对其进行带外方式的操作维护，应支持经 TELNET 方式远程对其进行操作管理维护，应支持通过网管系统进行操作管理维护，可选支持远程 WEB 方式的管理维护。

6.3 配置管理功能

a) 应支持对网络侧、用户侧端口的接口参数配置，包括：接口类型、管理状态和操作状态、用户端口的接入速率等；

b) 应支持对ADSL2+功能特性和线路端口参数进行配置和操作，其中，功能特性的配置和操作包括：

- 比特交换
- 无缝速率适配
- L2低功率管理
- 双端线路测试（DELT）
- 单端线路测试（SELT）

线路端口参数包括：

- 目标噪声余度（Target Noise Margin）
- 最大噪声余度（Maximum Noise Margin）
- 最小噪声余度（Minimum Noise Margin）
- 速率适配模式（Rate Adaptation Mode）
- 期望最大速率（Desired Maximum Rate）
- 期望最小速率（Desired Minimum Rate）
- 最大交织深度（Maximum Interleave Depth）
- 告警（事件）门限（Alarm（Event）Thresholds），超过下述任一事件的15分钟计数门限将引起系统告警：
 - 信号丢失（Loss of Signal）
 - 帧丢失（Loss of Frame）
 - 电源丢失（Loss of Power）
 - 链路丢失（Loss of Link）
- 每秒误帧门限，业务数据传输过程中每秒错误帧达到此门限开始报警。

c) 应支持对VDSL2功能特性和线路端口参数的配置和操作，其中功能特性的配置操作包括：

- 比特交换（BS）
- MIB PSD 模板（MIB PSD mask）
- 虚拟噪声（Virtual Noise）
- 单端线路测试（SELT）
- 双端线路测试（DELT）

线路端口参数的配置包括：

- 基本参数集配置 (Base Profile) :
 - 传输模式 (Transmode)
 - Profile参数集 (Standard Profile)
 - 频段划分 (BandPlan)
 - RFI陷波频段 (RFI notching Bands)
 - 子载波关断 (Sub-Carrier Blackout)
 - 下行标称最大集总发送功率 (Maximum nominal Aggregate Transmit Power in Down Stream)
- 业务参数集配置 (Service Profile) :
 - 目标噪声余度 (Target Noise Margin)
 - 最大噪声余度 (Maximum Noise Margin)
 - 最小噪声余度 (Minimum Noise Margin)
 - 速率适配模式 (Rate Adaptation Mode)
 - 期望最大速率 (Desired Maximum Rate)
 - 期望最小速率 (Desired Minimum Rate)
 - 最大交织深度 (Maximum Interleave Depth)
 - 最小脉冲噪声保护 (Minimum Impulse Noise Protection)
- UPBO参数集配置 (Upstream Power Back Off Profile) :
 - UPBO参考PSD配置参数集 (reference parameter of UPBO reference PSD per-Band)
 - UPBO使能控制 (Force CO-MIB electrical loop length)
- DPBO参数集配置 (Downstream Power Back Off Profile) :
 - 交换局侧功率谱密度模板 (Assumed Exchange PSD mask)
 - 交换局侧电气长度 (E-side Electrical Length)
 - 交换局侧电缆模型配置参数集 (E-side Cable Model scalers)
 - 最小有效电平 (Minimum Usable Signal)
 - DPBO最小频率 (DPBO span Minimum frequency)
 - DPBO最大频率 (DPBO span Maximum frequency)
- d) 应支持对ATM参数配置, 至少包括:
 - 每端口PVC条数
 - 针对单个PVC的业务类型
 - 针对单个PVC的速率限制值
- e) 应支持对以太网参数进行配置, 至少包括:
 - 基于端口的最大MAC学习数
 - MAC地址老化时间

- 安全配置
- VLAN/SVLAN配置，如VLAN ID、VLAN成员表等
- VLAN的速率限制值等
- f) 应支持通过网管对系统软件进行升级；
- g) 应支持对组播相关功能的配置，至少包括：
 - IGMP SNOOPING和IGMP PROXY使能
 - IGMP PROXY IP地址设定
 - 用户端口IGMP协议报文抑制使能和抑止比
 - CDR使能
 - CDR最大记录数
 - CDR上报时间间隔
 - 用户频道访问权限（禁止、预览和允许）
 - 频道预览参数（预览的持续时长、预览次数、预览间隔时长、预览总时长、预览权限复位时间等）
- h) 应支持对QoS、多业务相关功能的配置，至少包括：
 - 配置入端口信任或替换优先级标签
 - 流分类（按物理端口、PVC、IEEE 802.1D、VLAN ID、Ethernet类型/IP类型等分类）
 - 流的速率、突发容量、超速处理方式（丢弃、优先级重新标记）和优先级标签等配置
 - 优先级标签和队列映射关系
 - 队列调度算法选择（SP，WRR）
 - 队列加权参数
 - 拥塞控制方法设定
 - 流与VLAN/SVLAN的映射关系
- i) 所有配置操作应记录到日志文件；
- j) 可选支持对环境监控参数进行配置。

6.4 故障管理功能

1. 网管系统应能够对各种不同的告警/故障分不同级别实时显示出来，并且可正确记录各种告警/故障事件和状态（未确认/已确认/已清除等）。
2. 当设备发现 DSL 线路出现故障时，网管应能收集到此类告警。
3. 当设备和网管平台之间出现通信故障时，网管应能收集到此类告警。
4. 当某些环境变量（如电源电压、温度、湿度等）超出设备所允许的范围时，网管应能收集到环境告警。

5. 网管应能对产生的故障告警及事件消息进行记录，以便用户对历史告警进行查询。告警日志的操作功能应包括查询、分类统计、备份和删除。
6. 网管应提供告警统计门限设定功能。主要包括以下超过 15 分钟计数门限的信息：
 - 信号丢失（Loss of Signal）
 - 帧丢失（Loss of Frame）
 - 电源丢失（Loss of Power）
 - 链路丢失（Loss of Link）
 - 误码秒（Errored Seconds）
7. 网管系统告警统计列表应可对故障类型基于故障严重程度、故障原因、时间段进行分级处理，应具备周期性的告警统计。

6.5 性能管理功能

- a) ADSL2+性能管理应具备对下述系统性能管理事件的当天和前一天的每 15 分钟计数以及 24 小时计数功能，其中参数“块”定义为一个 ADSL2+ 复帧（superframe）：
 - 信号丢失（Loss of Signal）
 - 帧丢失（Loss of Frame）
 - 电源丢失（Loss of Power）
 - 链路丢失（Loss of Link）
 - 发送块（Transmitted Blocks）
 - 接收块（Received Blocks）
 - 已纠正块（Corrected Blocks）
 - 未纠正块（Uncorrected Blocks）
- b) VDSL2 性能管理应具备对下述系统性能管理事件的当天和前一天的每 15 分钟计数以及 24 小时计数功能，包括：
 - 前向纠错秒（FEC Second）
 - 误码秒（Error Second）
 - 严重误码秒（Serious Error Second）
 - 信号丢失秒（Loss of Signal Second）
 - 不可用秒（Unavailable Second）
 - 已纠正块（Corrected Blocks）
 - 未纠正块（Coding Violations）
- c) ADSL2+应具备记录特定线路端口的以下信息：
 - 当前线路衰减（Line Attenuation （current））

- 当前噪声余度 (Noise Margin (current))
 - 总输出功率 (Total Output Power)
 - 最大可行速率 (Maximum Attainable Rate)
 - 当前速率 (Current Rate)
 - 信道数据块长度 (Channel Data Block Length)
 - 交织深度 (Interleave Depth)
- d) VDSL2应具备记录特定线路端口的以下信息:
- 实际频谱规格 (Actual Standard Profile)
 - 当前各频段线路衰减 (Line Attenuation (current) per Band)
 - 当前各频段噪声余度 (Noise Margin (current) per Band)
 - 实际总输出功率 (Actual Aggregate Transmit Output Power)
 - 最大可达速率 (Maximum Attainable Rate)
 - 当前速率 (Current Rate)
 - 交织深度 (Interleave Depth)
- e) 应具备对网络侧端口特定连接的性能统计分析功能, 至少包括:
- 输入的总字节数
 - 输入的单播包数
 - 输入的非单播包数
 - 丢弃的输入包数
 - 包含错误的输入包数
 - 输出的总字节数
 - 输出的单播包数
 - 输出的非单播包数
 - 丢弃的输出包数
 - 包含错误的输出包数

6.6 安全管理功能

网管系统应通过定义个人访问权限的方式, 提供对于网管系统访问的安全措施, 不同级别的管理员应具有不同的权限, 访问者只能在自己的权限范围内进行管理操作。敏感信息、或固定用户终端鉴权属性、数据库和配置数据只能由有授权的个人或管理系统进行操作。

6.7 DSL 线路自动测试功能

1. DSLAM 设备必须具备测试总线以及内置抓线矩阵支持内置测试总线, 支持标准的 APP 协议、TL1 协议/接口。

2. DSLAM 设备应能配合测试设备和测试服务器，完成窄带线路电气特性测试，宽带线路电气性能测试（包括频率响应、时域反射、噪声测试、DMT 测试和纵向平衡测试）和仿真测试功能（包括物理层仿真测试、用户端 PPPoE 仿真测试、用户端 PING 仿真测试）。
3. 设备能提供 DSL 线路自动测试功能，其功能应满足中国电信企业标准《ADSL 自动测试技术要求（暂行）》的相关要求。

6.8 DSL 终端远程管理功能

1. 设备应具有远程终端管理功能。
2. DSLAM 应支持 EOC 和 PVC 中的一种管理通道，终端设备支持两种管理通道。
3. 应支持 SNMP over AAL5 over PVC 或 SNMP over HDLC over EOC 的管理协议承载通道，HTTP over IP over PVC 可作为一种补充手段实现对不常用功能的管理。
4. 设备应支持以下一些 DSL 终端远程管理功能
 - 查看终端详细信息
版本号、以太网端口状态和速率、NAT 状态、PVC 信息等
 - 配置终端
VPI/VCI、封装协议、DHCP Client、NAT 功能等
 - 配置终端管理的 IP 地址
 - 终端重启
 - 终端升级
 - 终端版本校验
 - 终端测试
 - 激活终端发起 PING、FTP、PPP 等仿真测试
 - 终端即插即用
5. 设备具备的自动测试功能应满足中国电信企业标准《ADSL 终端远程管理技术要求》的相关要求。
6. 设备应支持终端综合管理系统（ITMS）对 DSL 终端的远程管理功能。

7 设备其他要求

7.1 设备硬件要求

1. 设备应支持不同业务处理板的混插，提高插槽的通用性和灵活性。
2. 系统交换引擎、总线带宽和到每个业务槽位的连接带宽必须能够满足目

前和未来多种业务的发展需要，如，支持组播业务线速转发、频道的快速切换，保证视频业务质量和带宽。

3. 设备应具有网络故障和硬件故障告警功能。
4. 当软件升级时，应不影响硬件结构。
5. 对主控模块的要求：
 - 主控模块应具有软硬件故障告警功能。
 - 主控模块应具有故障脱机自动诊断功能以及负荷控制措施。
6. 设备应提供过流、过压保护措施。
7. DSLAM 设备应适合安装在 19 英寸的机架上，机架规格宽度及深度不超过 600mm。

7.2 机箱要求

1. 冷却系统必须是冗余和可热插拔的，当一个风扇故障时，剩余的风扇必须能够维持对满载系统的冷却。
2. 必须使用温度传感器监测系统的温度，当系统温度超过预设的阈值时，必须产生一个告警指示，并发送给适当的告警/故障管理系统。
3. 必须提供视觉指示(LED)用于显示设备的冷却系统或温度情况(如风扇工作/故障，温度正常/过热等)。
4. 设备应该提供多种机箱设计以应用于各种类型节点。本规范中的功能要求(规模要求除外)适用于任何规模的设备。
5. 设备必须提供直观、方便的指示灯，建议包括电源指示灯、运行状态指示灯、端口连接状态指示灯、端口工作模式指示灯、链路活动指示灯等。

7.3 线缆管理

1. 设备应该在机箱的背部提供适当的线缆管理，使用户可以方便地对线缆进行操作

7.4 设备可用性

1. 设备应该具备 99.999%的总体可用性(软硬件)，例行维护时间不计算在内。
2. 系统无故障连续工作时间(MTBF)必须大于 17520 小时，系统故障恢复时间 (MTTR) 应小于 1 小时。
3. 设备所有业务单板必须支持热插拔功能。
4. 必须允许对运行系统进行所有适当的配置更改和软件升级而不影响在线用户。

5. 必须支持从故障板卡到冗余板卡的自动切换，手工切换应该作为选项支持。
6. 设备中的所有元件必须能够提供 1:1、N:1 或分布式设备冗余能力，设备元件包括：
 - 系统主控板
 - 控制处理器
 - 电源转换模块/供电单元
 - 风扇
7. 系统主控板等核心模块必须支持冗余保护和备份功能。可以支持用户端口的冗余保护和备份功能。
8. 设备必须具有主备用电源输入，且具有支持电源热备份的能力。
9. 从主用电源到备用电源的切换必须是自动的，不能引起业务的中断。
10. 满配置环境下，设备重新启动时间不大于 5 分钟。
11. 在有冗余配置的情况下，从机箱中抽走控制板卡时及重新插入控制板卡时，设备必须能够继续转发流量。

7.5 设备软件要求

1. 软件要求保证安全可靠，具有容错能力。
2. 软件系统须提供数据接口，提供进行二次开发的文档。
3. 软件应采用模块化结构，模块之间的通信应按规定的接口进行。
4. 应具有软件故障的监视功能，一旦软件出现死循环等重大故障时，应能自动再启动，并做出即时故障报告信息。
5. 配置数据与处理程序应有相对的独立性，配置数据的任何变更都不应引起运行版本的变更。
6. 软件应有完善、方便的人机通信控制功能。
7. 软件应具备方便、迅速地恢复到原来版本的功能。
8. 系统软件应能在线升级，不需重新启动。
9. 软件应在不中断通信的情况下，完成程序打补丁的功能。
10. 不同时期软件版本应能向下兼容，软件版本易于升级。
11. 软件升级必须可以在线获得。
12. 设备必须支持从 FTP 或 TFTP 服务器下载软件/配置文件。
13. 设备应该通过 CMM Level 3 认证，满足对软件开发和质量保证过程的要求。
14. 设备应该通过 ISO 9001 认证，满足对软件开发和质量保证过程的要求。
15. 设备的工程和制造过程应该通过 TL-9000 认证。

7.6 环境要求

1. 设备应满足 YD/T 1082-2000《接入网设备过电压过电流防护及基本环境适应性技术条件》规定的环境要求。
2. 室内型设备必须能够在以下环境条件下正常运行：
 - 环境温度：5℃～45℃，每小时变化<10℃
 - 相对湿度：10%～90%（非凝露、非结霜）
3. 在以下灰尘环境下，设备应能正常工作：直径大于 5 μm 的灰尘浓度 ≤3×10⁴ 粒/m³；灰尘粒子是非导电、导磁和腐蚀性的。
4. 设备的电磁兼容性指标应满足 YD/T 1244《数字用户线（xDSL）设备电磁兼容性要求和测量方法》的相关要求，应符合国标 GB 9254-1998《信息技术设备无线电骚扰限值和测试方法》和 GB/T 17618-1998《信息技术设备抗扰度限值和测试方法》。设备产生的电磁辐射建议符合 FCC Class A、EN55022/CISPR-22 Class A、VCCI Class A 等标准。
5. 抗震措施：按 8 级烈度进行计算；
6. 机械振动：4.9 牛顿/平方米（50 赫兹至 200 赫兹）
7. 应提供双电源备份和负载分担功能，应支持-48VDC 和~220VAC 电源。
直流电压及其波动范围要求：
 - 直流电压及其波动范围要求：额定电压-48V，允许变动范围为-40V~-57V。
 - 交流电压及其波动范围要求：单相 220V±10%，频率 50Hz±5%，线电压波形畸变率小于 3%。
8. 设备应满足 YD/T 1082-2000《接入网设备过电压过电流防护及基本环境适应性技术条件》对模拟雷电冲击、电力线感应、电力线接触等指标的要求。
9. 正常情况下，设备的绝缘电阻不应小于 50MΩ，设备的接地电阻应小于 5Ω。

7.7 绿色要求

7.7.1 设备管理要求

（1）基本要求

1. 对于机框插槽式设备，设备应有高温报警功能。
2. 对于机框插槽式设备，应具备能源监控及管理功能。在设备管理员需要时，可检测到设备当前能耗状态。

3. 对于机框插槽式设备，应支持根据实际情况中断未用板卡供电或进入微电状态。
4. 应支持将端口设置为低功耗模式（L0、L2、L3 模式）。
5. 设备电源反灌杂音应满足通信电源 YD/T 1051-2000《通信局站电源系统总技术要求》的要求。

（2）扩展要求

1. 对于机框插槽式设备，能通过查询方式监控到目前工作状态下能耗，以及设备各个组件，如各板卡、机框、风扇，所消耗的能耗比例。
2. 对于机框插槽式设备，设备可通过命令行或网管工具远程关闭设备部分模块或功能以减少其工作能耗。
3. 对于机框插槽式设备，可根据实际情况动态调整风扇转速。
4. 可根据电缆长度调整端口工作功率。

7.7.2 设备环保与包装要求

（1）设备环保要求

设备设计阶段，设备的主要部分（如电路板、机箱、电缆等）应尽量减少铅、镉、汞、六价铬、溴化耐燃剂等有害物质，并严格按 ROHS 规范进行产品生产与设计。

（2）设备包装要求

实行包装减量化（Reduce）。绿色包装在满足保护、方便、销售等功能的条件下，应是用量最少的适度包装。

包装应易于重复利用（Reuse）或易于回收再生（Recycle）。

包装废弃物可以降解腐化（Degradable）。为了不形成永久的垃圾，不可回收利用的包装废弃物要能分解腐化，进而达到改善土壤的目的。

包装材料对人体和生物应无毒无害，包装材料中不应含有有毒物质或有毒物质的含量应控制在有关标准以下。

包装材料应尽量减少木材的使用。

在包装产品的整个生命周期中，均不应对环境产生污染或造成公害。

（3）其它要求

设备内部应有合理的气流组织，应采用前进后出或垂直通风方式，不宜从侧面进出通风。

同时，机框式数据设备内风扇应具有自动调节速率的功能，机架内采用防热风回流等技术，降低对机房环境的局部制冷要求。

机架门开孔率：考虑到通风和散热的需求，在保证门的强度和刚度要求前提下，机架正面门和背面门开孔率至少不得低于 30%，以获得良好的排吸风效果。

7.7.3 能耗分级标准

DSLAM 设备能耗等级应达到最新版本的中国电信《绿色数据设备技术规范》所定义的标准。

抄送公司内部：集团公司网络发展部、国际部、技术部、采购部、移动建设部、网络运行维护事业部、无线网络优化中心。

拟文部门：技术部

会签部门：网络发展部、网络运行维护事业部。

中国电信集团公司综合部

2008年12月26日印发
