

ICS 33.040.40

M 32

YD

中华人民共和国通信行业标准

YD/T 1452-2014

代替 YD/T 1452-2006

IPv6 网络设备技术要求 边缘路由器

Technical specification for edge router equipment supporting IPv6

2014-10-14 发布

2014-10-14 实施

中华人民共和国工业和信息化部 发布

目 次

前 言..... II

1 范围..... 1

2 规范性引用文件..... 1

3 术语、定义和缩略语..... 4

4 路由器功能..... 10

5 物理层接口规范..... 11

6 链路层..... 12

7 Internet层..... 13

8 传输层..... 21

9 应用层——路由协议..... 22

10 应用层——网络管理协议..... 26

11 IPv6的安全..... 27

12 对移动IP的支持..... 28

13 运行与维护..... 28

14 技术指标..... 31

15 环境要求..... 33

16 电源与接地..... 33

附录A（规范性附录） PPP上的IPv6..... 34

附录B（规范性附录） 在以太网上传输IPv6数据包..... 39

前 言

本标准是支持IPv6的路由器设备系列标准之一，该系列标准的结构和名称如下：

——YD/T 1452 《IPv6 网络设备技术要求 边缘路由器》

——YD/T 1453 《IPv6 网络设备测试方法 边缘路由器》

——YD/T 1454 《IPv6 网络设备技术要求 核心路由器》

——YD/T 1455 《IPv6 网络设备测试方法 核心路由器》

与本系列标准相关的标准还有支持 IPv4 的路由器设备系列标准，该系列标准的结构和名称如下：

——YD/T 1096-2009 《路由器设备技术要求 边缘路由器》

——YD/T 1097-2009 《路由器设备技术要求 核心路由器》

——YD/T 1098-2009 《路由器设备测试方法 边缘路由器》

——YD/T 1156-2009 《路由器设备测试方法 核心路由器》

本标准编制依据 GB/T 1.1-2009 给出的规则起草。

本标准代替YD/T 1452-2006《IPv6网络设备技术要求 边缘路由器》，本标准与YD/T 1452-2006相比主要技术变化如下：

——根据以下主要技术变化修改规范性引用文件、术语、定义和缩略语内容；

——在物理层接口规范中删除 ISDN 通信接口、X.21 接口、X.21bis 接口、V.24 接口、G 系列接口、V.35 接口技术内容，增加 10GE 接口和 10G POS 接口的技术内容；

——删除链路层中有关帧中继端口和 ISDN 接口的链路层协议技术内容；

——删除 IPv6 扩展头中 0 型路由头的技术内容；

——修改第 8.2、8.4 和 10.4 节的技术内容为可选；

——修改第 15 和第 16 章技术内容的规范性引用标准；

——删除附录 C 在帧中继网络上传输 IPv6 数据包技术内容；

——删除附录 D ATM 网络上的 IPv6 技术内容。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、中兴通讯股份有限公司。

本标准主要起草人：赵 锋、张宇华、陈 丹、彭海清、高 飞、常 城、李红阳、黄春秀。

本标准于2006年06月首次发布，本次为第一次修订。

IPv6网络设备技术要求

边缘路由器

1 范围

本标准规定了支持IPv6的边缘路由器的技术要求，主要包括功能、指标、通信接口、通信协议、环境要求等。

本标准适用于支持IPv6的边缘路由器设备。

本标准下文中所有对路由器的规定均特指对支持IPv6的边缘路由器。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB3483	电子设备雷击试验导则
GB4943.1	信息技术设备的安全 第1部分：通用要求
GB19286-2003	电信网络设备的电磁兼容性要求及测量方法
YD/T 1162.1	多协议标记交换（MPLS）技术要求
YD/T 1295	支持IPv6的路由协议技术要求——开放最短路径优先协议（OSPF）
YD/T 1341	IPv6基本协议——IPv6协议
YD/T 1342	IPv6路由协议——支持IPv6的边界网关协议（BGP4）
YD/T 1454	IPv6网络设备技术要求——支持IPv6的核心路由器
YD/T 1466	IP安全协议（IPSec）技术要求
YD/T 1712-2007	中小型电信机房环境要求
YD/T 5098	通信局（站）防雷与接地工程设计规范
YDN065	邮电部电话交换设备总技术规范书
IETF RFC768	用户数据包协议（User Datagram Protocol）
IETF RFC793	传输控制协议（Transmission Control Protocol）
IETF RFC1089	以太网上的SNMP（SNMP over Ethernet）
IETF RFC1122	对 Internet 主机的要求——通信层（Requirements for Internet Hosts - Communication Layers）
IETF RFC1142	OSI ISIS域内路由协议（OSI IS-IS Intra-domain Routing Protocol）
IETF RFC1155	用于TCP/IP互联网的管理信息的结构与识别（Structure and identification of management information for TCP/IP-based internets）
IETF RFC1195	使用OSI IS-IS为TCP/IP和双栈环境提供路由（Use of OSI IS-IS for routing in TCP/IP and dual environments）
IETF RFC1212	MIB的简明定义（Concise MIB definitions）

IETF RFC1213	TCP/IP 基本网络管理的管理信息库 (Management Information Base for Network Management of TCP/IP-based internets: MIB-II)
IETF RFC1224	用于管理异步产生的告警的技术要求 (Techniques for managing asynchronously generated alerts)
IETF RFC1229	扩展的通用接口管理信息库 (Extensions to the generic-interface MIB)
IETF RFC1230	IEEE 802.4令牌总线MIB (IEEE 802.4 Token Bus MIB)
IETF RFC1231	IEEE 802.5令牌总线MIB (IEEE 802.5 Token Ring MIB)
IETF RFC1304	定义的管理对象为SIP接口类型 (Definitions of Managed Objects for the SIP Interface Type)
IETF RFC1317	定义的管理对象为与RS-232类似的硬件设备 (Definitions of Managed Objects for RS-232-like Hardware Devices)
IETF RFC1333	PPP链路质量监视 (PPP Link Quality Monitoring)
IETF RFC1334	PPP认证协议 (PPP Authentication Protocols)
IETF RFC1398	对以太网链路接口类型管理对象的定义 (Definitions of Managed Objects for the Ethernet-Like Interface Types)
IETF RFC1406	定义的管理对象为DS1和E1接口类型 (Definitions of Managed Objects for the DS1 and E1 Interface Types)
IETF RFC1407	定义的管理对象为DS3和E3接口类型 (Definitions of Managed Objects for the DS3/E3 Interface Type)
IETF RFC1418	SNMP应用于OSI模型之上 (SNMP over OSI)
IETF RFC1471	对PPP链路控制协议管理对象的定义 (The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol)
IETF RFC1472	对PPP安全协议管理对象的定义 (The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol)
IETF RFC1473	管理对象的定义为IP网络控制协议的点对点协议 (The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol)
IETF RFC1513	令牌环扩展到远程网络监控的管理信息库 (Token Ring Extensions to the Remote Network Monitoring MIB)
IETF RFC1661	点到点协议 (The Point-to-Point Protocol)
IETF RFC1757	远程网络监控MIB (Remote Network Monitoring Management Information Base)
IETF RFC1771	BGP4协议的问题修改 (Issues in Revising BGP-4)
IETF RFC1772	应用在互联网的BGP4 (Application of the Border Gateway Protocol in the Internet)
IETF RFC1902	SNMPv2 的管理信息结构 (Structure of Management Information for Version 2 of the Simple Network Management Protocol)

IETF RFC1907	用于SNMPv2的MIB (Management Information Base for Version 2 of the Simple Network Management Protocol)
IETF RFC1981	IPv6路径MTU发现协议 (Path MTU Discovery for IP version 6)
IETF RFC1994	PPP握手认证协议 (CHAP) (PPP Challenge Handshake Authentication Protocol (CHAP))
IETF RFC1997	BGP协议的团体属性 (BGP Communities Attribute)
IETF RFC2021	使用SMIv2的远程网络监控MIBv2 (Remote Network Monitoring Management Information Base Version 2 using SMIv2)
IETF RFC2080	IPv6 RIPng (RIPng for IPv6)
IETF RFC2115	在帧中继网络使用的管理信息库 (Management Information Base for Frame Relay DTEs Using SMIv2)
IETF RFC2373	IPv6的寻址体系结构 (IP Version 6 Addressing Architecture)
IETF RFC2439	BGP路由振荡抑制 (BGP Route Flap Damping)
IETF RFC2460	互联网协议第6版规范 (Internet Protocol, Version 6 (IPv6) Specification)
IETF RFC2461	IPv6的邻居发现协议 (Neighbor Discovery for IP Version 6 (IPv6))
IETF RFC2462	IPv6无状态地址自动配置 (IPv6 Stateless Address Autoconfiguration)
IETF RFC2465	IPv6 管理信息库: 文本约定和通用组 (Management Information Base for IP Version 6: Textual Conventions and General Group)
IETF RFC2466	IPv6 管理信息库: ICMPv6 组 (Management Information Base for IP Version 6: ICMPv6 Group)
IETF RFC2472	PPP上的IPv6 (IP Version 6 over PPP)
IETF RFC2573	SNMPv3的应用 (SNMP Applications)
IETF RFC2574	SNMPv3基于用户的安全模型 (User-based Security Model (USM) for version 3 of the Simple Network Management Protocol)
IETF RFC2675	IPv6超长包 (IPv6 Jumbograms)
IETF RFC2710	IPv6 组播监听者发现协议 (Multicast Listener Discovery (MLD) for IPv6)
IETF RFC2711	IPv6 路由器警告选项 (IPv6 Router Alert Option)
IETF RFC2894	IPv6路由器重编号协议 (Router Renumbering for IPv6)
IETF RFC3019	用于MLD的IPv6 MIB (IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol)
IETF RFC3484	IPv6缺省地址选择 (Default Address Selection for Internet Protocol version 6)
IETF RFC3513	IPv6地址结构 (Internet Protocol Version 6 Addressing Architecture)
IETF RFC3775	IPv6对移动性的支持 (Mobility Support in IPv6)
IETF RFC4022	TCP 协议的管理信息库 (Management Information Base for the Transmission Control Protocol)
IETF RFC4113	UDP 协议的管理信息库 (Management Information Base for the User Datagram Protocol)

IETF RFC4273	管理对象的定义为BGP4 (Definitions of Managed Objects for BGP-4)
IETF RFC4293	IP协议的管理信息库 (Management Information Base for the Internet Protocol)
IETF RFC4444	ISIS管理信息库 (Management Information Base for Intermediate System to Intermediate System)
IETF RFC4456	替代全连接型IBGP的BGP路由反射 (BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP))
IETF RFC4760	BGP4的多协议扩展 (Multiprotocol Extensions for BGP-4)
IETF RFC5095	IPv6协议中弃用0型路由头 (Deprecation of Type 0 Routing Headers in IPv6)
IETF RFC5308	用于IPv6的ISIS (Routing IPv6 with IS-IS)
IEEE802.3	以太网介质访问控制协议 (CSMA/CD) 及物理层技术规范
IEEE802.3u	百兆以太网标准 (100Base-T/100Base-FX)
IEEE802.3z	千兆以太网标准 (1000Base-LX/1000Base-SX)

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

路由器 Routers

通过转发数据包来实现网络互连的设备。

路由器可以支持多种协议 (例如 TCP/IP、SPX/IPX、AppleTalk)，可以在多个层次上转发数据包 (例如数据链路层、网络层、应用层)。如果没有特殊指明，本文件正文中的路由器特指基于 TCP/IP 协议簇、工作在 IP 层上的网络设备。

路由器需要连接两个或多个由 IPv6 链路本地地址或点到点协议标识的逻辑端口，至少拥有一个物理端口。路由器根据收到的数据包中网络层地址以及路由器内部维护的路由表，决定输出端口以及下一条路由器地址或主机地址并且重写链路层数据包头。

路由表应动态维护来反映当前的网络拓扑。路由器通常通过与其他路由器交换路由信息来完成动态维护路由表。

路由器只提供数据包传输服务。为实现路由选择的通用性和鲁棒性 (Robust)，路由器的实现应使用最少状态信息来维持上述服务。

3.1.2

边缘路由器 Edge Routers

位于网络边缘，用作接入边缘网的路由器。除非特别指出，否则边缘路由器应符合 3.1.1 中路由器的要求。

3.1.3

协议分层 Protocol Layers

通常按照互联网的 5 层结构或者开放系统互连 (OSI) 7 层参考协议描述。本文件按照互联网 5 层结构来描述。互联网上的协议分层如下所述：

- 应用层 Application Layer

应用层位于互联网协议栈中最高层。应用层通常包括 OSI 7 层参考模型中的表达层和应用层的功能，以及会话层的部分功能。

应用层协议可以分为直接为用户提供服务的用户协议和提供通用系统功能的支持协议。用户协议包括 Telnet（远程登录）、FTP（文件传输协议）、SMTP（简单邮件传递协议）等。支持协议可以包括 SNMP（简单网络管理协议）、BOOTP（启动捆绑协议）、TFTP（平凡文件传输协议）和大量的路由协议。

● 传输层 Transport Layer

传输层协议提供端到端的通信服务。该层协议除完成 OSI 7 层参考模型中传输层功能外，还包含少量的会话层功能。

目前，主要有两种传输层协议：传输控制协议（TCP）和用户数据包协议（UDP）。

TCP 是面向连接的可靠传输服务，提供端到端可靠性、正确次序以及流量控制。UDP 是无连接的传输服务。

● 互联网层 Internet Layer

所有互联网传输协议都使用互联网协议（IPv6）将数据从数据源传送到目的地。IP 是基于无连接或数据包的网际服务，不提供端到端的传递保证。IP 数据包到达时可能损坏、重复、失序或者部分丢失。需要时，IP 层以上的层负责可靠的数据传递。该层相当于 OSI 参考模型中的网络层。

互联网控制消息协议（ICMPv6）是一种控制协议。ICMPv6 位于 IP 层，封装在 IP 数据包中。ICMPv6 提供差错报告、拥塞报告和路由器重定向等功能。

组播监听者发现协议（MLD）是为 IP 组播（multicasting）建立动态主机组的网络层协议。

● 链路层 Link Layer

链路层协议包含物理层之上、网络层之下的所有内容，负责正确传递数据包。

互联网链路层标准通常只描述用于在指定链路层协议上传输 IP 数据包的地址解析原则。

3.1.4

自治系统 Autonomous System

自治系统包含一组由一系列路由器互连而成的子网（子网上连接主机），并构成网络拓扑一个可连接的分段。这些子网和路由器一般都由一个单一的操作维护（O&M）管理组织来控制维护。在一个 AS 内，路由器可以使用一个或多个内部路由协议，通常有几种度量（metric）方式。每个 AS 对外部网络一般都有一个统一的内部路由计划、精简的可达路由。一个 AS 由 AS 号来标识。

3.1.5

IP 组播 IP Multicasting

IP 组播是链路层组播的扩展。使用组播技术，一个数据包能传送到多个主机（并非全部主机）。在扩展情况下，这些主机可以在不同的地址域中，这些主机称为组播组。每个组播组有一个 IPv6 组播地址标识。发送给每个组播成员的 IPv6 数据包具有与 IPv6 单播业务流相同的服务质量。数据包发送者可以不属于组播成员。

3.1.6

数据包 Packet

数据包是一组互联网模块之间的传输单元。从源到目的地的数据称为数据包。IP 不提供可靠的传输机制，也没有端到端、段到段的概念，没有出错重传，也没有流量控制。

3.1.7

缺省路由 Default Route

路由表中的一条记录，指明数据包的目的地不在路由表中时的路由，是一种特殊的静态路由，简单地说，就是在没有找到匹配的路由时使用的路由。在路由表中，缺省路由以目的网络为 0.0.0.0、子网掩码为 0.0.0.0 的形式出现。如果数据包的目地址不能与任何路由相匹配，那么系统将使用缺省路由转发该数据包。

3.1.8

转发器 Forwarder

路由器中负责在各接口间交换包的逻辑实体。转发器决定对本地分发的包或传出到另一接口的包排队。

3.1.9

转发 Forwarding

转发是路由器对每个收到包的处理。包可能由路由器接收，可能送到另一个或多个端口，或者两者皆有。转发包括决定如何处理包的过程：排入队列输出或者内部接收。

3.1.10

转发信息表 Forwarding Information Base

包括转发 IP 数据包所需要的信息，在本文件中称为 FIB。该表中至少包含接口标识和到每一个可达目标网络前缀的下一跳信息。

3.1.11

分段 Fragment

包含上层数据包一部分内容的 IPv6 数据包。该上层数据包太大，不能整个放入输出网络的一个数据包中。

3.1.12

通用串口 Universal Serial Interface

一个能连接两个系统的物理媒体，能配置成点到点链路，同样也能支持使用例如 LAPS 协议的链路层网络。链路层网络连接到另一系统或交换机，在连接上可能存在高层复用虚电路通信，参见点到点线路。

3.1.13

内部网关协议 Interior Gateway Protocol

在自治系统内分发路由信息的协议。

3.1.14

接口 IPv6 地址 Interface IP Address

赋予路由器一个特定接口的 IPv6 地址以及网络前缀长度。

3.1.15

互联网地址 Internet Address

在互联网上标识一台主机的数。包含两部分：IPv6 地址以及前缀长度。前缀长度指多少比特作为网络地址。

3.1.16

互联网协议第 6 版 IPv6

由 IETF RFC2460 定义的包交换协议。IPv6 不提供可靠的通讯机制，即没有段到段、端到端的概念。

3.1.17

IPv6 数据包 IPv6 Data Packet

互联网协议端到端的传输单元。IPv6 数据包中包含 IPv6 头、扩展头和高层数据（例如 TCP、UDP、ICMPv6 等）。IPv6 数据包是 IPv6 头、扩展头以及后面紧接的消息。

IPv6 数据包是完全的 IP 端到端的传输单元。

IPv6 数据包包含一个或多个 IP 分段。

3.1.18

IP 分段 IP Fragment

IPv6 数据包的一部分。IP 分段包括 IPv6 头、扩展头以及 IPv6 数据包中高层信息的部分或全部。

一个或多个 IP 分段组成 IPv6 数据包。

3.1.19

最大传输单元 Maximum Transmission Unit

通过逻辑接口收发的最大尺寸包。该数值包含 IPv6 头和扩展头，不包含链路层头或帧。

3.1.20

组播地址 Multicast Address

由组播主机识别的一种特殊类型地址。

组播地址有时称为功能地址或组地址。

3.1.21

网络前缀 Network Prefix

IPv6 地址中标识网络的部分。在设置地址中表示网络的比特。

3.1.22

始发 Originate

从路由器发出的包有两种，一种是收到后转发的包；另一种是路由器产生的包（例如路由通告）。由路由器产生的包称为始发于路由器。

3.1.23

路径 Path

从一个路由器到一特定目标的包需要穿过的路由器及（子）网的序列。路径是单向的，在一对主机间路径不同是可能的。

3.1.24

链路 Link

通信中介或媒体。节点可以通过链路在数据链路层（紧接在 IPv6 的下层）进行通信。

3.1.25

邻居 Neighbors

连接在同一链路上的路由器或主机。

3.1.26

链路最大传输单元 Link MTU

能通过链路完整传输的数据包的最大传输单元。

3.1.27

路径最大传输单元 Path MTU

源节点和目的节点之间的一条路径上所有链路最大传输单元中的最小值。

3.1.28

物理网络 Physical Network

邻近链路层的网络。其内部结构（如果存在）对互联网层是透明的。由于对 IP 层透明，可以由多种设备例如桥、转发器连接多种媒体。

3.1.29

物理网络接口 Physical Network Interface

连接网络的物理接口，拥有（可能唯一）链路层地址。在同一路由器上的物理网络地址可能共享同一个链路层地址，但同一网络上不同路由器的链路层地址应是唯一的。

3.1.30

点到点线路 Point to Point line

能且仅能连接两个系统的物理媒体。

3.1.31

反向路径转发 Reverse Path Forwarding

对组播包指定下一跳目标的方法。

3.1.32

悄悄丢弃 Silently Discard

路由器应不作任何进一步处理而丢弃该包，且不发 ICMP 差错消息。然而为诊断差错，路由器应提供将差错及包内容写入日志，并具有对差错计数的能力。

3.1.33

稀疏模式 Sparse Mode

初始转发状态与密集模式相反，假设所有的网络都不需要该数据。

3.1.34

子网 Subnet

网络的一部分，在物理上可能是独立的，与网络的其他部分共享一个网络地址，由子网号区分。子网对于网络正如网络对于互联网。

3.1.35

子网号 Subnet Number

互联网地址的一部分，用于区分子网。在互联网路由时不被理睬，用于企业网内路由。

3.1.36

跳数限制 Hop Limit

IPv6 头中的跳数限制域，表示数据包还能够被转发经过的路由器的数目。

3.1.37

运维 Operation and Maintenance

设备的运行和维护，简称 O&M。

3.2 缩略语

下列缩略语适用于本文件。

ACCM	Asynchronous Control Character Map	异步控制字符映射
ANSI	American National Standard Institute	美国国家标准研究所
ARP	Address Resolution Protocol	地址解析协议
AS	Autonomous System	自治系统
BACP	Bandwidth Allocation Control Protocol	带宽分配控制协议
BAP	Bandwidth Allocation Protocol	带宽分配协议
BGP	Border Gateway Protocol	边界路由协议
CHAP	Challenge-Handshake Authentication Protocol	握手认证协议
CIDR	Classless Inter Domain Routing	无类域间路由选择
CLP	Cell Loss Priority	信元丢失优先级
ECP	Encryption Control Protocol	保密控制协议
EGP	Exterior Gateway Protocol	外部路由协议
FCS	Frame Check Sequence	帧校验序列
FIB	Forwarding Information Base	转发信息表
FTP	File Transmission Protocol	文件传输协议
HDLC	High-Level Data Link Control	高级数据链路控制协议
ICMP	Internet Control Message Protocol	互联网控制消息协议
IGP	Interior Gateway Protocol	内部路由协议
IPv6	Internet Protocol Version 6	互联网协议-第 6 版
IPCP	IP Control Protocol	IP 控制协议
IPv6CP	IPv6 Control Protocol	IPv6 控制协议
IPXCP	The PPP Internetwork Packet Exchange Control Protocol	网间数据包交换控制协议
IS-IS	Intermediate System to Intermediate System	中间系统—中间系统
LAN	Local Area Network	局域网
LAPS	Link Access Protocol-SDH	链路接入协议—SDH
LCP	Link Control Protocol	链路控制协议
LQM	Link Quality Monitor	链路质量监视
MIB	Management Information Base	管理信息库
MRU	Maximun Receive Unit	最大接收单元
MTU	Maximun Transmission Unit	最大传输单元
NCP	Network Control Protocol	网络控制协议
NHRP	Next Hop Routing Protocol	下一跳路由协议

NIC	Network Interface Card	网络接口卡
NOC	Network Operation Center	网络运行中心
NTP	Network Time protocol	网络时间协议
O&M	Operation and Maintenance	运行与维护
OOB	Out Of Band	带外
OSPF	Open Shortest Path First	开放最短路径优先
PAP	Password Authentication Protocol	密码认证协议
PPP	Point to Point Protocol	点到点协议
RPF	Reverse Path Forwarding	反转路径转发
SDH	Synchronous Digital Hierarchy	同步数字体系
SNMP	Simple Network Management Protocol	简单网络管理协议
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial file transfer protocol	平凡文件传输协议
UDP	User Datagram Protocol	用户数据包协议
WAN	Wide Area Network	广域网

4 路由器功能

4.1 路由器功能划分

路由器并非应实现下列所有功能中的所有内容，但应实现所有功能中基本内容。

路由器功能可分成如下几方面。

4.1.1 接口功能

该功能用作将路由器连接到网络。可以分为局域网接口及广域网接口两种。局域网接口主要包括以太网接口等；广域网主要包括 SDH、E1/T1 网络接口。

4.1.2 通信协议功能

该功能负责处理通信协议，可以包括 TCP/IP、MPLS、PPP 等协议。

4.1.3 数据包转发功能

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

4.1.4 路由信息维护功能

该功能负责运行路由协议，维护路由表。路由协议可包括 RIPng、OSPFv3、ISISv6、BGP4+等协议。

4.1.5 管理控制功能

路由器管理控制功能包括 4 个功能，SNMP 代理功能、Telnet 服务器功能、本地管理和远端监控（RMON）功能。通过 5 种不同的途径对路由器进行控制管理，并且允许记录日志。

4.1.6 安全功能

用于完成数据包过滤、地址转换、访问控制、数据加密、防火墙、地址分配等功能。

4.2 路由器功能实现

路由器需要实现如下基本功能：

- a) 实现本标准规定的互联网协议，包括 IPv6，邻居发现，ICMPv6。

b) 连接到两个或多个数据包交换的网络。对每个连接到的网络，路由器应实现该网络所要求的功能。这些功能包括：

- IPv6 数据包封装到链路层帧或从链路层帧中取出 IPv6 数据包。
- 按照该网络所支持的最大数据包大小发送或接收 IPv6 数据包。该大小是网络最大传输单元 (MTU)。

- 将 IPv6 地址与相应网络的链路层地址相互转换，例如将 IPv6 地址转换成以太网硬件地址。
- 实现网络支持的流量控制和差错指示。

c) 接收及转发数据包，在收发过程中实现缓冲区管理，拥塞控制以及公平性处理。

- 出现差错时辨认差错并产生 ICMPv6 差错及必要的差错消息。
- 丢弃跳数限制域为 0 的数据包。
- 必要时将数据包分段。

d) 按照路由表信息，为每个 IPv6 数据包选择下一跳目的地。

e) 应支持至少一种内部网关协议 (IGP) 与其他同一自治域中路由器交换路由信息及可达性信息；可以支持外部网关协议 (exterior gateway protocol EGP) 与其他自治域交换拓扑信息。

f) 提供网络管理和系统支持机制，包括存储/上载配置、诊断、升级、状态报告、异常情况报告及控制等。

5 物理层接口规范

5.1 概述

本章规定路由器应支持的接口类型以及接口特性。

路由器如果拥有下列类型接口，则应符合本标准的规定或者本标准引用的规范性引用文件。

注：对本标准没有涉及的接口类型应符合相关国家标准、行业标准或国际标准。

路由器应至少拥有一个物理接口。

5.2 PSTN E1 接口（可选）

采用 2048 kbit/s 速率的数字接口，见 YDN 065。

5.3 以太网接口（必选）

路由器可以拥有 10Mbit/s 以太网接口（符合 IEEE802.3），100Mbit/s 快速以太网接口（符合 IEEE802.3u），千兆以太网接口（符合 IEEE802.3z）。

10Mbit/s 以太网接口电缆可采用 10Base-5，10Base-2，10Base-T，10Base-F。

100Mbit/s 以太网接口可采用三类传输介质：100Base-T4、100Base-TX 和 100Base-FX。

1000Mbit/s 以太网物理接口可选支持 1000Base-CX，1000Base-SX，1000Base-LX 和 1000Base-T。

10Gbit/s 以太网物理接口可选支持 10GBase-R、10GBase-W，见 YD/T 1454 第 5.4 节。

5.4 串行同步物理层接口（可选）

包括 64kbit/s，2048 kbit/s 等速率接口，见 YDN 065。

5.5 SDH 接口（可选）

边缘路由器可选支持 SDH STM-1 接口、SDH STM-4 接口、SDH STM-16 接口和 SDH STM-64 接口中的一种或多种。STM-1 有光接和电接口两种，STM-1 电接口适用于局内干扰信号弱的情况。STM-4、STM-16、STM-64 应采用光接口，见 YD/T 1454 第 5.7 节。

6 链路层

6.1 链路层/Internet 层接口

对每个收到的数据包，链路层应将下列信息传输到上层：

- a) IP 包；
- b) 链路层数据包的数据部分长度；
- c) 收到该数据包的物理接口标识；
- d) 数据包目的地物理地址的分类：普通包、组播包；
- e) 源物理地址。

对每个需要传输的数据包，Internet 层应提供下列信息：

- a) IP 包；
- b) IP 包长度；
- c) 目的地物理地址；
- d) 下一跳 IP 地址；
- e) 链路层优先级值。

6.2 链路层附加要求

6.2.1 Ethernet 与 802.3 共存

具有 10Mbit/s 以太网的路由器应符合 IETF RFC1122 中对以太网的要求。

6.2.2 最大传输单元——MTU

每个逻辑端口的 MTU 应在该链路层合法的 MTU 范围内可配置。

由于一些链路层协议定义了可以发送的最大帧尺寸，在这种情况下，路由器不允许发送超过链路层最大帧尺寸的 MTU。然而路由器应当允许接收最大的链路层帧，即使其尺寸大于 MTU。

6.2.3 点到点协议——PPP（可选）

点到点协议的实现应符合 IETF RFC1661、IETF RFC2472、IETF RFC1334 和 IETF RFC1994。

点到点接口是使用点到点线路传输数据的接口，这样的接口包括专线和复合接口等。复合接口通常使用特殊的物理接口。

实现点到点接口或通用串行接口的路由器应实现 PPP。

路由器应在所有的通用串行接口上实现 PPP。路由器可以允许线路配置成点到点链路协议来替代 PPP。点到点链路接口应缺省使用 PPP（当使能时），在使能以前要求配置链路层协议。通用串行接口应要求在使能以前配置链路协议。

LCP 协议提供一系列可以协商的任选域，这些任选域包括地址和控制字段压缩、协议字段压缩、异步控制字符映射（ACCM）、最大接收单元（MRU）、链路质量监视（LQM）、幻数（用于环回检测）、PAP 和 CHAP 和 32 位的 FCS。

路由器可以在同步或异步链路上使用地址和控制字段压缩、协议字段压缩。如果路由器指示它能接收这些压缩，也应能接收非压缩的 IP 头信息。

路由器可以在异步 PPP 链路上协商 ACCM，但不应在同步 PPP 链路上协商 ACCM。如果路由器在同步 PPP 链路上收到一个 ACCM 协商试图，它应确认这个任选域，然后不理睬它。

路由器应正确协议最大接收单元（MRU）。如果路由器协商的 MRU 小于 1500 字节，它应有能力接

收一个 1500 字节的帧。

路由器应实现和协商用于环回检测的幻数。

路由器应支持 PAP 和 CHAP。

路由器可选实现 IETF RFC1333。

路由器应支持 16 位的 FCS，可以支持 32 位的 FCS。

路由器可以执行 IPv6 接口标识协商。如果对端不支持 IPv6 接口协商规程，路由器应采取正确的措施。

PPP 上有关 IPv6 的规定见附录 A。

6.2.4 接口测试

路由器应提供一种机制允许路由软件决定某物理接口是否可用；在复合接口上，路由器通常需要判断虚电路是否可用。路由器应当提供一种机制允许路由软件判断物理接口质量。路由器应提供一种机制来通知路由软件：接口可用或由管理操作决定其不可用。路由器应提供一种机制在检测到链路层接口可用或不可用时通知路由软件。

6.3 串行线上的链路层协议（可选）

当路由器使用串行线路互连时，建议支持 HDLC 帧（同步线路）链路层协议。

7 Internet 层

7.1 Internet 协议——IPv6

7.1.1 定义

路由器应实现 IPv6 协议，并符合 YD/T 1341。

在某些情况下，要求路由器在丢弃数据包时不作任何处理（即不发送 ICMPv6 差错消息），然而为了诊断故障，路由器应提供将差错写入日志（包括所丢弃数据包的内容）的能力，以及具有对丢弃数据包进行计数的能力。

7.1.2 协议概述

YD/T 1341 对 IPv6 协议作了描述。路由器应实现该协议。

7.1.2.1 跳数限制

路由器应丢弃收到的跳数限制为 0 的数据包。当路由器转发数据包时应将跳数限制域的值减 1。

7.1.2.2 扩展头的分类

路由器应能识别并处理以下几种扩展头：

- 逐跳选项头；
- 目的地选项头；
- 路由头；
- 分段头。

路由器可以识别并处理以下几种扩展头：

- 认证头；
- 封装安全载荷头。

除了以下两种情况之外，路由器只能检查或处理接收数据包中的逐跳选项头：

- 接收数据包的接口的地址与数据包的 IPv6 头中的目的地址相同；

- 数据包的 IPv6 头中的目的地址是组播地址，并且该路由器是组播节点组中的一个节点。

路由器应严格按照扩展头在数据包中出现的顺序来检查或处理接收数据包中的扩展头。路由器不能在数据包中搜索一个特定的扩展头，并且在处理完所有排在它前面的头之前处理它。

如果路由器处理一个头的结果是要进行下一个头的处理，但这个头的“下一个头”域的值不能被路由器所识别，则路由器将丢弃这个数据包并向数据包的源节点发送一个 ICMP “参数错误”消息，ICMP 代码值为 1（不能识别下一个头的类型），ICMP 指针域包含源数据包中不能被识别的域的偏移量。若一个路由器遇到除 IPv6 头外的任一个头的“下一个头”域为 0，则它对这个数据包也应按上面的方法进行处理。

7.1.2.3 扩展头的顺序

当路由器发送的数据包带有多个扩展头时，扩展头应按下面的顺序出现：

- IPv6 头
- 逐跳选项头
- 目的地选项头（注 1）
- 路由头
- 分段头
- 认证头
- 封装安全载荷头
- 目的地选项头（注 2）
- 上层头

注 1：这些选项要在 IPv6 目的地址域所列出的第一个目的地进行处理，也要在路由头所列出的后续目的地进行处理。

注 2：这些选项只在数据包的最终目的地进行处理。

路由器应接收并处理同一个数据包中以任何顺序、任何次数出现的扩展头，只有逐跳选项头才应严格地接在 IPv6 头之后。

7.1.2.4 选项

路由器在处理一个扩展头时，应严格按照每个选项在扩展头中出现的顺序来处理它们。

路由器对逐跳选项头或目的地选项头中未知选项的处理应符合 YD/T 1341 中的规定。

路由器可选支持逐跳选项头中的超长包载荷选项。该选项的格式和用法应符合 IETF RFC2675 的规定。

路由器应支持逐跳选项头中的路由器警告选项。该选项的格式和用法应符合 IETF RFC2711 的规定。

7.1.3 扩展头的处理

7.1.3.1 路由头

路由器在处理接收到的数据包时，如果遇到一个路由头包含有不能识别的“路由类型”值，则它应该依据“剩余段”域的值采取措施。具体方法如下：

- 如果“剩余段”的值为 0，则路由器忽略这个路由头，继续处理数据包中的下一个头（其类型由路由头的“下一个头”域的值标识）。
- 如果“剩余段”的值不为 0，则路由器应丢弃这个数据包，并且向数据包的源地址发送一个 ICMP “参数错误”消息（代码值为 0），ICMP 指针指向不能识别的“路由类型”。

如果一个路由器在处理完接收数据包的路由头后，决定应将该数据包转发到一条链路 MTU 小于该包长度的链路上，那么该节点应丢弃此数据包并向该包的源地址发送一个 ICMP “数据包过大” 消息。

路由器只能检查或处理 “目的地址” 域与接收数据包的接口地址相同的 IPv6 数据包中的路由头。

出于安全性考虑，在 IETF RFC5095 中对 IETF RFC2460 进行了更新，要求路由器禁用 IPv6 扩展头中的 0 型路由头。

7.1.3.2 分段头

如果路由器需要发送一个大于路径 MTU 的数据包到目的节点，则它应将该数据包分段，并将每个分段作为一个独立的数据包传送。路由器在进行数据包分段时应符合 IETF RFC2460 中 4.5 节的相应规定。

路由器应支持将发送给自己的分段 IPv6 数据包重组。路由器在重组数据包时应符合 IETF RFC2460 中 4.5 节的重组原则。

如果路由器在接收到第一个到达的分段之后的 60s 内，一个数据包所有要重组的分段没有全部到达，则路由器应放弃重组该数据包，并且丢弃所有已接收的分段。在这种情况下，如果第一个分段数据包已接收到，则路由器要向那个分段数据包的源地址发送一个 ICMP “超时—段重组超时” 消息。

如果路由器从分段数据包 “载荷长度” 域中得到的分段长度不是 8 个字节的整数倍，并且这个段的 M 标志位是 1，则路由器应丢弃这个段，并且要向段的源地址发送一个 ICMP “参数错误” 消息（代码为 0），ICMP 指针指向分段数据包的 “载荷长度” 域。

如果路由器收到的一个分段的长度和偏移导致出现这种情况，即由这个分段重组的数据包 “载荷长度” 超过 65535 个字节，则路由器应丢弃这个分段，并且向分段的源地址发送一个 ICMP “参数错误” 消息（代码为 0），ICMP 指针指向分段数据包的 “段偏移” 域。

7.1.4 数据包的长度

路由器任一接口的链路 MTU 均不得小于 1280 字节。如果与某一接口相连的链路不支持 1280 字节的数据包，则路由器应在 IPv6 层以下的一层提供与链路相关的分段和重组功能。

为了发送长度大于路径 MTU 的数据包，路由器应使用 IPv6 分段头给数据包分段。

7.1.5 流标签

对于不支持流标签域功能的路由器来说，当发送一个数据包时，在流标签域填入 0 值；当转发数据包时，对流标签域不作任何改动；当接收数据包时，忽略流标签域。

7.1.6 业务等级

支持业务等级域的特殊应用的路由器可以在生成、转发或接收数据包时根据特殊应用的需要改变这一域的值。不具备此能力的路由器应忽略此域并且不能对其进行修改。

7.2 邻居发现协议

7.2.1 协议功能

邻居发现协议是 IPv6 协议的一个基本的组成部分，它实现了在 IPv4 中的地址解析协议（ARP）、控制报文协议（ICMP）中的路由器发现部分、重定向协议的所有功能，并具有邻居不可达检测机制。

路由器应实现邻居发现协议中的路由器和前缀发现、地址解析、下一跳地址确定、重定向、邻居不可达检测、重复地址检测功能，可选实现链路层地址变化、输入负载均衡、泛播地址和代理通告等功能。

7.2.2 消息类型

路由器应实现邻居发现协议的 5 种消息类型。邻居发现协议使用 5 种类型的 IPv6 控制信息报文

(ICMPv6) 来实现邻居发现协议的各种功能，这 5 种消息是：

- 路由器请求 (Router Solicitation)：当接口工作时，主机发送路由器请求消息，要求路由器立即产生路由器通告消息，而不必等待下一个预定时间。
- 路由器通告 (Router Advertisement)：路由器周期性地通告它的存在以及配置的链路和网络参数，或者对路由器请求消息作出响应。路由器通告消息包含在连接 (on-link) 确定、地址配置的前缀和跳数限制值等。
- 邻居请求 (Neighbor Solicitation)：节点发送邻居请求消息来请求邻居的链路层地址，以验证它先前所获得并保存在缓存中的邻居链路层地址的可达性，或者验证它自己的地址在本地链路上是否是唯一的。
- 邻居通告 (Neighbor Advertisement)：邻居请求消息的响应；节点也可以发送非请求邻居通告来指示链路层地址的变化。
- 重定向 (Redirect)：路由器通过重定向消息通知主机，对于特定的目的地址，自己并不是最佳路由，并通知主机到达目的地的最佳下一跳。

7.2.3 路由器和前缀发现

路由器应无条件丢弃不满足有效性检查的路由器请求和路由器通告消息。

路由器发现功能用来标识与给定链路相连的路由器，并获取与地址自动配置相关的前缀和配置参数。

作为对请求消息的响应，路由器应周期地发送组播路由器通告消息，来通告链路上节点的可达性。路由器发出路由器通告消息，指示该发送方是否愿意为缺省路由器。路由器通告还包括前缀信息选项，这些选项列出了一组确认“在连接”IP 地址的前缀。路由器通告消息应包含一些标志位，这些标志位通知主机怎样执行地址的自动配置。另外路由器通告消息中还应包含网络管理的参数，例如主机产生的数据包中使用的跳数限制参数的缺省值，或链路 MTU 值。

当主机向路由器发出路由器请求消息时，路由器应立刻发送路由器通告消息。

7.2.4 地址解析

路由器通过邻居请求和邻居通告消息将 IPv6 地址解析成链路层地址，对组播地址不执行地址解析。

路由器通过组播邻居请求消息来激活地址解析过程，邻居请求消息用来请求目标路由器返回它的链路层地址。源路由器在邻居请求消息中包含了它的链路层地址，并将邻居请求消息组播到与目标地址相关的请求节点组播地址，目标路由器在单播的邻居通告消息中返回它的链路层地址。这一对消息使源和目标路由器能解析出相互的链路层地址。

7.2.5 下一跳地址确定

当路由器向目的地发送数据包时，使用目的地缓存、前缀列表、默认路由器列表确定合适的下一跳的 IP 地址，然后路由器查询邻居缓存确定邻居的链路层地址。

IPv6 单播地址的下一跳确定操作如下：发送者使用前缀列表中的前缀进行最长前缀匹配，确定包的目的地是在连接的还是非连接的。如果下一跳是在连接的，下一跳地址就和目的地地址相同，否则发送者从默认路由器列表中选择下一跳。如果默认路由器列表是空，发送者认为目的地是在连接的。

下一跳确定的信息存储在目的地缓存中，下一个包可以使用这些信息。当路由器发送包时，首先检查目的地缓存，如果目的地缓存没有相关信息存在，就激活下一跳确定过程。

在学习到下一跳路由器的 IPv6 地址后，发送者检查邻居缓存以决定链路层地址。如果没有下一跳

IPv6 地址的表项存在，路由器的工作如下：

- 创建一个新表项，并设置其状态为不完全；
- 开始进行地址解析；
- 对传送的包进行排队。

当地址解析结束时，获得链路层地址，存储在邻居缓存中。此时表项到达新的可达状态，排队的包能够传送。

对于组播包，下一跳总是认为在连接，确定组播 IPv6 地址的链路层地址取决于链路类型。

当邻居缓存开始传送单播包时，发送者根据邻居不可达检测算法检测相关的可达性信息，验证邻居的可达性。

当邻居不可达时，再次执行下一跳确定，验证到达目的地的另一条路径是否是可达的。

7.2.6 重定向功能

当包应发送到一个非连接的目的地时，需要选择转发包的路由器。当选择的路由器作为消息传送的下一跳，并不是最好的下一跳时，路由器需产生重定向消息，通知源节点到达目的地存在一个更佳的下一跳路由器。

路由器应能够确定每个邻居路由器的本地链路（link-local）地址，以保证重定向消息里的目标地址根据本地链路地址来识别邻居路由器。

在源端没有正确应答重定向消息，或者源端选择忽略没有被验证的重定向消息的情况下，为了节省频带和处理的费用，路由器应限定发送重定向消息的速率。

在收到重定向消息时，路由器不能更新路由表。

7.2.7 邻居不可达检测

路由器应进行邻居不可达性检测，以检测邻居或邻居前向路径发生的故障。

如果路由器最近收到确认，邻居的 IP 层已经收到最近发送到它的数据包，那么该邻居是可达的。邻居不可达检测使用两种方法进行确认：一种是上层协议从上层协议来的提示，提供“连接正在处理”的确认；另一种是路由器发送单播邻居请求消息，收到了应答的邻居通告消息。为了减少不必要的网络流量，探测消息仅发送到邻居。

邻居不可达性检测与向邻居发送数据包同时进行。在邻居可达性确认期间，路由器继续向缓存链路层地址的邻居发送数据包。如果没有数据包发向邻居，则不发送检测。

7.3 路径 MTU 发现协议

为了充分利用网络带宽资源并尽量减少 IP 分段的发生，有必要发现端到端的 MTU。在 RFC1981 中描述了发现路径 MTU 的机制。路由器可选支持路径 MTU 发现协议。如果路由器不支持该协议，则在转发数据包时应以缺省的 IPv6 最小链路 MTU（1280 字节）作为最大包长。

在路由器发送 IPv6 数据包时，应以发送下一跳链路的 MTU 作为路径 MTU 的初始预测值并根据 IETF RFC1981 中描述的方法修改此预测值。

当路由器的路径 MTU 的预测值小于或等于实际的路径 MTU 时，路由器应中止发现路径 MTU 的处理过程。

当数据包的目的地址是组播地址时，路由器应选择所有组播路径的路径 MTU 的最小值作为转发数据包时的路径 MTU。

7.4 互联网控制消息协议——ICMPv6

7.4.1 定义

在路由器中 ICMPv6 用来报告处理报文过程中遇到的错误，以及实现一些网络层功能，如诊断（ICMPv6 “Ping”）等。ICMPv6 是 IPv6 的一个必要组成部分，路由器应实现 ICMPv6 协议。

7.4.2 消息类型

路由器应实现两类 ICMPv6 消息：差错消息和信息消息。差错消息的消息类型字段高位比特为 0，所以差错消息的消息类型代码为 0~127，信息消息的消息类型代码为 128~255。

ICMPv6 差错消息：

- 目的不可达（类型 1）；
- 包长超长（类型 2）；
- 超时（类型 3）；
- 参数错误（类型 4）。

ICMP 信息消息：

- 回显请求（类型 128）；
- 回显应答（类型 129）。

7.4.3 消息源地址的确定

发送 ICMPv6 消息的路由器应在对 IPv6 报头计算校验和之前确定消息源和目的的 IPv6 地址。如果该路由器具有多个单播地址，那么它需要依据以下原则选择消息的源地址：

a) 如果要发送的消息是对发送到这个路由器某个单播地址的报文响应，那么源地址应与该单播地址相同。

b) 如果要发送的消息是对发送到这个路由器所属组的组播或泛播组地址的报文响应，那么响应消息的源地址应是接收组播包的接口的一个单播地址。

c) 如果如果一个发送到非本路由器地址的报文发生了错误，路由器应该发送一个 ICMPv6 消息作为响应，这个 ICMPv6 消息的源地址应该是本路由器的一个单播地址，并且这个地址应该与错误报文的目地址具有最大的相关性。例如，如果待发送的 ICMPv6 消息是对一个数据包无法成功传送情况的响应，那么 ICMPv6 消息的源地址应该是该数据包转发失败的那个接口的单播地址。

d) 另外，传送消息时应根据其目的地址检查路由器的路由表，以确定转发接口，并且消息的源地址应该是这个接口上的一个单播地址。

7.4.4 消息校验和计算

路由器对校验和的计算是将 ICMPv6 消息分成 16 比特长的段，每段计算其二进制补码，然后对其求和，这里的 ICMPv6 消息从 ICMPv6 消息类型字段开始，它由 IPv6 报头中的“伪报头”指明，在伪报头中的“下一报头”值为 58。

在计算校验和之前，校验和字段要先置为 0。

7.4.5 消息处理规则

路由器对 ICMPv6 消息的处理应符合以下规则：

- 如果接收到带有未知类型的 ICMPv6 差错消息，应将其交至上层。
- 如果接收到带有未知类型的信息消息，应将其丢弃。

c) 每个 ICMPv6 差错消息（类型值 <128 ）的消息体中将包含导致错误的那个 IPv6 数据包，但要保证最后的差错消息长度不超过 IPv6 最小 MTU 的限制。

d) 当网络层协议要求将 ICMPv6 差错消息传送给上层进程时，从原始数据包中取出（包含在 ICMPv6 差错消息的消息体中）上层协议的类型，根据协议的类型选择适当的上层进程来处理差错。如果原始数据包含有过多的扩展报头，由于要满足 IPv6 最小 MTU 的要求，在 ICMPv6 消息中可能不包含上层协议类型。这种情况下，这个差错消息将在 IPv6 层处理后丢弃。

当接收到如下报文时，不能发送 ICMPv6 差错消息：

a) ICMPv6 差错消息。

b) 发往某 IPv6 组播地址的报文（对这个规则有两种例外情况：（1）包长过大消息—使用 IPv6 组播的路径 MTU 发现机制进行工作；（2）代码为 2 的参数错误消息—表明有一个未知的 IPv6 选项，且选项类型的最高位的两个比特为 10）。

c) 链路层组播包。

d) 链路层广播包。

e) 数据包的源地址不是 IPv6 单播地址，也就是说，其源地址是一个非 IPv6 定义的地址，一个 IPv6 组播地址或是一个 ICMP 消息发送者已知的 IPv6 “泛播”地址。

e) 最后，为了限制发送 ICMPv6 差错消息所用的带宽，减少开销，每个 IPv6 路由器都应限制 ICMPv6 差错消息的发送速率。有几种方法可以实现速率限制的功能，例如：

- 基于定时器。例如，限制将差错消息发往指定信源或任何信源的速率，最多每 T 毫秒发送一次。
- 基于带宽。例如限制在某个接口上发送差错消息的速率为与其相连的链路带宽的某一比例 (F)。

在该路由器上限制参数（上边例子中的 T 和 F ）应该配置一个保守的缺省值（例如， $T=1s$ ，而不是 0，或 $F=2\%$ ，而不是 100%）

7.4.6 ICMPv6 差错消息

7.4.6.1 目的不可达消息

目的不可达消息应该由路由器或路由器的 IPv6 层产生，作为对数据包由于非阻塞的原因无法送达目的端的响应。（如果数据包由于网络阻塞而被丢弃，则不能发送 ICMPv6 消息）

如果传送失败的原因是在传送路由器上没有匹配的路由表项，则代码值应置为 0（注意：这种错误只能在路由器上没有“缺省路由”时才会发生）。

如果传送失败是由于网络管理上的原因，如存在“防火墙”，则代码值应置为 1。

如果传送失败是由于其他原因引起，例如无法将 IPv6 地址解析为响应的链路层地址，或由于链路层的某些原因，则代码值应置为 3。

当目的路由器上的传输层协议（如 UDP）对数据包并没有接收者，并且传输层协议本身也没有措施去通知发送端，则接收端应该发送一个代码为 4 的目的不可达消息。

当路由器接收到以自身为目的地 ICMPv6 目的不可达消息之后应通知高层进程。

7.4.6.2 包长超长消息

当数据包大于出口链路的 MTU 而无法传送时，路由器应该发送一个包长超长消息作为响应。消息中的信息用来作为路径 MTU 发现过程的一部分。

在如下情况下路由器需要发送包长超长响应消息：接收到一个目的地址为 IPv6 组播地址的报文，或

者一个链路层组播报文，或者一个链路层广播报文。

当路由器接收到以自身为目的地的包长超长消息时，应送交上层处理。

7.4.6.3 超时消息

如果路由器接收到跳数限制为 0 的包，或路由器将数据包的跳数限制减至 0，则应丢弃这个数据包，并向信源发送代码为 0 的 ICMPv6 超时消息，这个消息指明出现了路由环路或跳数初始值过小。

当路由器接收到以自身为目的地的超时消息时，应送交上层处理。

7.4.6.4 参数错误消息

如果路由器在处理报文时，发现报文的头部或扩展头中发生错误，以至于无法进行处理，则该路由器应丢弃这个报文，并应该向信源发送一个 ICMPv6 参数错误消息，以指明错误的类型和位置。

指针指示了原始数据包中发生错误的位置（以字节为标志）。例如，类型为 4，代码为 1，指针域为 40 的 ICMPv6 消息表明在原始数据包中紧跟着 IPv6 报头的扩展报头中存在一个未知的“下一报头”值。

当路由器接收到以自身为目的地的参数错误消息时，应送交上层处理。

7.4.7 ICMPv6 信息消息

7.4.7.1 回显请求消息

每个路由器应实现 ICMPv6 回显响应功能，当收到回显请求时能够发送相应的回显应答。同时，路由器应实现应用层的接口，以发送回显请求，接收回显应答，作为一种诊断的手段。

回显请求消息可以送交上层进行 ICMP 消息的处理。

7.4.7.2 回显应答消息

每个路由器都应实现 ICMPv6 的回显功能，以接收回显请求消息并发送相应的回显应答。同时，路由器应该实现应用层接口，用来发送回显请求并接收回显应答，以达到诊断的目的。

与发往单播地址的回显请求消息相对应的回显应答消息的源地址应与该回显请求消息中的目的地址相同。

对于发往 IPv6 组播地址的回显请求消息，也应该发送回显应答作为响应。回显应答应使用接收到该回显请求的接口的一个单播地址作为源地址。

回显应答消息应交付给路由器上产生回显请求的进程进行处理，它也可能交付给那些没有产生回显请求的进程。

7.5 IPv6 寻址

7.5.1 IPv6 地址结构

路由器应支持 IETF RFC3513 规定的 IPv6 地址结构。

7.5.2 IPv6 无状态地址自动配置

IETF RFC2462 规定了 IPv6 的无状态地址自动配置协议。无状态地址自动配置协议主要适用于 IPv6 主机。为了支持 IPv6 主机的无状态地址自动配置，使主机可以即插即用，不必手工配置地址，路由器应支持以下功能：

- 路由器应该能根据 IETF RFC2462 中的规定生成链路本地地址；
- 路由器应该支持重复地址发现（DAD）；
- 路由器应该接受 IPv6 主机为完成重复地址发现操作而发来的 Neighbor Solicitation 消息，检查主机生成的临时地址在链路上的唯一性；

— 路由器应该周期性地向主机发送 Router Advertisement 消息，其中包含主机生成站点本地地址和全局地址所需要的地址前缀；

— 路由器应该接受主机为尽快获得地址前缀而发来的 Router Solicitation 消息，发送 Router Advertisement 响应消息，其中包含主机生成站点本地地址和全局地址所需要的地址前缀。

具体实现见附录 B。

7.5.3 IPv6 缺省地址选择

在一个接口上拥有多个 IPv6 地址或拥有多个 IPv6 接口的路由器可以支持 IPv6 缺省地址选择协议，并符合 IETF RFC3484。

7.6 IPv6 路由器重编号

路由器可选支持 IPv6 路由器重编号协议，支持该协议的路由器应符合 IETF RFC2894。

7.7 组播监听者发现协议（MLD）

MLD 是用于主机和组播路由器之间的协议，应用于一个物理网络上以建立特定组播组中的主机成员关系。组播路由器使用该信息和组播路由协议一起支持互联网上的 IP 组播转发。

路由器应该支持组播监听者发现协议，并符合 IETF RFC2710。

路由器应该实现 MLD 中的主机部分要求。

8 传输层

路由器应该支持传输控制协议（TCP）和用户数据包协议（UDP）。

8.1 用户数据报协议——UDP

用户数据包协议在 IETF RFC768 中规定。

路由器实现的 UDP 应符合 IETF RFC768 的要求。

本标准不规定不同协议层之间的接口。

路由器应该产生 UDP 校验和。路由器应计算数据包和伪头上的 UDP 校验和，其中伪头中的地址使用 IPv6 的 128 比特地址。如果计算结果为 0，则应修改为 0xFFFF 放在 UDP 头中。路由器应丢弃接收到的包含 0 校验和的 UDP 数据包，并记录下错误。

8.2 UDP 超长包（jumbogram）的处理（可选）

支持 IPv6 超长包协议（IETF RFC2675）的路由器在发送包长（包括 UDP 头与数据）超过 65535 字节的 UDP 数据包时，应将 UDP 长度域的值设为 0；接收到这样的数据包的路由器如果支持 IPv6 超长包协议，则应从 IPv6 载荷长度域的值得到 UDP 数据包的实际长度。

支持 IPv6 超长包协议的路由器在收发 UDP 超长包时应符合 IETF RFC2675 第 4 章的规定。

8.3 传输控制协议——TCP

传输控制协议在 IETF RFC793 中规定。

路由器实现的 TCP 应符合 IETF RFC793 的要求。

本标准不规定不同协议层之间的接口。

路由器在计算 TCP 校验和时，应用 IPv6 的 128 比特地址替代 IPv4 的 32 比特地址。计算方法参见 YD/T 1341。

实现路径 MTU 发现协议的路由器只有在路径 MTU 未知时使用 516 作为发送 MSS 的缺省值；如果路径 MTU 已知，发送 MSS 缺省值是路径 MTU-60。

8.4 TCP 超长包 (jumbogram) 的处理 (可选)

支持 IPv6 超长包协议 (IETF RFC2675) 的路由器应符合以下的规定。

8.4.1 MSS 选项

当路由器发送 TCP 数据包时,如果路径 MTU-60 的值大于或等于 65535,则应将 MSS 的值设为 65535。

当路由器收到 MSS 的值为 65535 的 TCP 数据包时,应使用路径 MTU-60 的值作为真实的 MSS 值。

8.4.2 紧急指针

当路由器发送/接收带有紧急指针的 TCP 数据包时,应根据 IETF RFC2675 5.2 节的规定进行处理。

9 应用层——路由协议

9.1 定义

互联网路由系统包含两部分-内部路由与外部路由。自治域 (AS) 允许描述一组路由器从内部路由到外部路由的转变。IP 数据包通常要穿过两个或多个 AS 的路由器才能到达目的地,AS 系统应相互提供拓扑信息才能允许这种转发。内部网关协议用作在 AS 内部分发路由信息 (即 AS 内部路由)。外部网关协议用作在 AS 间交换路由信息 (即 AS 间路由)。

9.1.1 路由安全性考虑

路由器应提供将路由信息源由最值得信赖到最不值得信赖排列的能力,并首先从最值得信赖的路由信息源接收路由信息。上述规定在使用外部路由网关 EGP 和其他内部路由协议的始发核心/末梢 (core/stub) AS 系统中隐含使用。

路由器应提供一种机制来过滤过时无效的路由 (例如 127 网络)。

缺省情况下,路由器不能分发不是该路由器使用、信任或认为有效的路由信息。有时路由器需要分发值得怀疑的路由信息,但由管理员直接人为干预。

路由器应谨慎接收来自其他路由器的路由信息。

9.1.2 优先级

除非特殊路由协议的指定,路由器应将携带路由信息流量的 IP 数据包的优先级设置成 6 (互联网控制)。

9.1.3 消息确认

对等实体之间 (peer-to-peer) 的认证涉及多种测试。对通行字 (password) 消息的申请和可接收相邻路由器列表的使用有效地提高了路由数据库的鲁棒性。路由器应实现允许显式指定有效相邻路由器的管理控制。路由器应对支持的路由协议实现对等实体之间 (peer-to-peer) 认证。

路由器应能基于原地址和接收数据包的端口来检验相邻路由器。路由器与直接相连的子网上的路由器应严格按照相连接口或者通过非编号接口进行通信。从其他接口上得到的信息应悄悄丢弃。

9.2 内部网关协议

9.2.1 定义

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,但应实现下列功能:

- a) 应能迅速反映 AS 内部拓扑的改变;
- b) 提供一种机制使电路振荡时不引起连续的路由更新;
- c) 提供快速收敛成无环回 (loop-free) 路由;

- d) 使用最少的带宽;
- e) 提供等效路由以便负荷分担;
- f) 提供一种认证的路由更新方法。

路由器除实现静态路由外,应实现 RIPng 协议,路由器应至少支持 OSPFv3、IS-ISv6 协议中的一种。

9.2.2 开放最短路径优先——OSPFv3

基于最短路径优先 (SPF) 是一类基于链路状态算法的协议,它们基于 Dijkstra 的最短路径算法。在基于 SPF 的系统中,每个路由器通过称为洪泛 (flooding) 算法的过程得到完整的拓扑数据库。泛滥过程确保信息可靠传输。每一个运行 SPF 算法的路由器在数据路上建立 IP 路由表。

路由器应支持可变长子网掩码 (VLSM),支持广播网络,支持非广播多接入网络 (NBMA),支持虚链路,支持 Stub 域和 NSSA,支持等开销多路径,具体要求见 YD/T 1295。

实现 OSPFv3 的路由器应实现 OSPFv3 MIB。

9.2.3 中间系统到中间系统——双重 IS-ISv6

IS-ISv6 是基于链路状态 (SPF) 路由算法,拥有所有该类协议的优点。

路由器可选实现双重 IS-ISv6。

双重 IS-IS 在 IETF RFC1142 和 IETF RFC1195, IETF RFC5308 中规定。

实现双重 IS-ISv6 的路由器应实现 IETF RFC4444 中规定。

9.2.4 路由信息协议 RIPng

RIPng 应用极其广泛,是自治域内路由协议的事实标准之一。

路由器可选实现 RIPng 协议。路由器对 RIPng 协议的支持应符合 IETF RFC2080。

9.3 外部网关协议

9.3.1 定义

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。

路由器可选实现 BGP4+。

9.3.2 边缘网关协议——BGP4+

9.3.2.1 定义

边缘网关协议 (BGP4+) 是自治域间路由协议,是在 BGP 运行者之间交换网络可达性信息。网络信息包含流量到达某个网络所应经过的完整 AS 列表。该信息应确保路径内没有环路。该信息应足够丰富以用作构建 AS 互连图,在 AS 互连图中,应裁减路由环回,应被实施 AS 层的策略决定。

路由器应实现 BGP4 在 IETF RFC1771 中的规定,以及 YD/T 1342。

实现 BGP4+ 的路由器应实现 BGP4 MIB (IETF RFC4273)。

建议实现 BGP4+ 的路由器遵从 IETF RFC1772 第 6 章中的规定。

9.3.2.2 协议介绍

BGP4+ 提供对非常复杂的路由策略的支持,但不要求所有对 BGP4+ 的实现都支持这样的策略。BGP4+ 至少要实现:

- a) 应允许 AS 控制 BGP4+ 学到的路由是否广播到相邻 AS。BGP4+ 的实现应至少在单个网络粒度上实现上述规定。BGP4+ 的实现同样应在自治系统粒度上实现上述规定,上述自治系统可能是产生路由的自治系统,或者可能是将路由广播到本地系统的自治系统 (相邻自治系统)。

b) 应允许 AS 当存在多条路径时倾向于使用某条特定路径。该功能应通过允许管理员向自治系统赋度来实现，使路由选择进程选择一条最低度量的路由（路由的度量定义为有关该路由 AS_PATH 路径属性所有 AS 的度量之和）。

c) 应允许 AS 忽略 AS_PATH 路径属性中包含某特定 AS 的路由。这样的功能可以使用 2) 中提到的技术实现：将某 AS 度量赋为无限大。路由选择进程应不理睬度量为无限大的路由。

d) 提供 BGP4+路由反射，并符合 IETF RFC4456 的规定。

e) 提供 BGP4+区域属性，并符合 IETF RFC1997 的规定。

f) 提供自治系统联合。

g) 支持 IETF RFC2439 规定的路由振荡抑制。

h) 支持 IETF RFC4760 规定的 BGP4+的多协议扩展。

i) 支持 IPv6 的 BGP4+路由协议利用 BGP4 多协议扩展定义的 MP_REACH_NLRI 和 MP_UNREACH_NLRI BGP 属性来传送 IPv6 的路由信息。具体的规定见 YD/T 1342。

9.3.3 没有外部协议的自治系统间路由

在两个独立的标准内部路由协议间不使用标准外部路由协议交换两个自治域中的路由信息是可能的。这样做通常的方法是在一个边缘路由器上独立运行两个内部路由协议进程，在两个进程间交换路由信息。

如同 EGP 与 BGP 交换信息，如果没有适当的控制，在一个路由器两个 IGP 间交换路由信息很容易产生路由环路。

9.4 静态路由

静态路由提供一种途径来显示定义到一个特定目的地的下一跳路由器。路由器应提供一种途径来定义到特定目的地的静态路由，其中目的地由网络前缀定义。该机制应允许对每一条静态路由指定度量（metric）。一个支持动态路由协议的路由器应允许静态路由定义成任何路由协议使用的有效的度量。路由器应允许用户规定一组静态路由是否通过路由协议扩散。另外如果路由器支持使用下列信息的路由协议，应在静态路由中支持这些附加信息。这些信息是：

a) 前缀长度；

b) 对给定路由协议引入静态路由的特定度量。

9.5 策略路由

策略路由提供一种通过用户自定义的规则来进行数据包转发的路由方式，路由器应可选支持策略路由，策略路由的方式有：基于源地址的策略路由、基于目的地址的策略路由、基于源端口的策略路由、基于目的端口的策略路由、基于高层协议的策略路由。

9.6 路由信息的过滤

网络中每个路由器基于转发数据库中包含的信息作转发决定。在一个简单网络中数据库内的信息可以静态配置。当网络变得复杂时，动态更新转发数据库对网络有效运行至关重要。

如果要求通过网络的数据流尽可能地高效，则需要一种机制来控制那些路由器用作创建转发数据库的信息的传播。这种控制任务可以通过哪一个路由信息源可以信任，选择相信那一条消息的形式来实现。转发数据库是可用的路由消息经过过滤后的结果。

除有效性之外，控制路由消息传播可以通过阻止不正确或错误的路由信息的扩散而增加转发数据库

的稳定性。

在某些情况下，本地策略可能要求不能广泛传播整个路由信息。

这些过滤器要求只用于非 SPF 协议（对不实现距离矢量协议的路由器没有影响）。

9.7 路由确认

当路由更新宣告中路由违反本标准的规定时，路由器应作为差错写入日志，除非接收的更新路由协议使用这些值编码那些特殊路由编码（例如缺省路由）。

9.7.1 基本路由过滤

过滤路由信息允许对路由器用作转发报的路径进行控制。路由器应可以配置从那一个路由信息源接收路由消息，那一条路由可以信任，因此路由器应指定：

- 路由信息可以从哪个逻辑接口接收，从每个逻辑接口上可以接收哪些路由；
- 在一个逻辑接口上传播所有路由或者只传播缺省路由。

某些路由协议不能将逻辑接口作为路由信息源，在这种情况下，路由器应指定：从哪一个相邻路由器可以接收路由信息。

9.7.2 高级路由过滤

当网络拓扑变得越复杂时，越需要对复杂的路由进行过滤，因此路由器应对每个路由协议分别提供：

- a) 从哪一个逻辑端口或路由器可以接收路由信息，那些路由可以信任；
- b) 哪些路由将通过哪个逻辑接口来发送；
- c) 路由信息将发送到哪个路由器。

在许多环境下，需要将其他路由器上收到的路由信息赋予可信任度。路由器可以指定：对收到的每条路由赋予可信度或优先级。无论每个路由所关联的路由度量如何，赋予高可行度的路由将优先选择。

如果路由器支持赋予优先级值，路由器不允许传播不作为第一方信息选择的路由。如果路由器使用的路由协议不支持区分第一方与第三方信息，路由器不能传播任何不能优先选择的路由。

如果路由器不使用某路由信息中的路由，则路由器不能传播给其他路由器。

9.8 路由协议间信息交换

如果这些独立的 IP 路由进程能运行在同一路由器上，路由器应能在独立的 IP 内部路由协议之间交换路由信息。如果路由器配置成在独立内部路由协议间双向交换路由信息，则应提供某些机制来防止路由环回。路由器应提供优先级机制，在独立的路由进程中选择路由。当穿过管理边界时，路由器应提供 IGP-IGP 交换的管理控制。

路由器应提供某种机制来翻译或转变基于每个网络的度量。路由器（或路由协议）可以允许在 IGP 中引入外部路由的全局（程）优先级。

9.9 组播路由协议

路由器应实现组播路由协议，应支持组播监听者发现协议 MLD（IETF RFC2710）和协议无关组播协议-稀疏模式（PIM-SM）。

9.10 MPLS 协议（可选）

路由器可选支持 MPLS，支持 MPLS LER 功能，支持 MPLS 显式路由 LSP，支持 LDP，能配置备份 LSP，支持负荷分担的多路径 LSP，支持标记压栈，支持基于约束的路径计算，能基于源/目的地址，协议，源/目的端口，选项域，TOS/优先级（Precedence）域，TCP 标志，根据路由表的下一跳等参数将包

路由至输出 LSP。

有关 MPLS 协议具体要求见 YD/T 1162.1。

10 应用层——网络管理协议

10.1 简单网络管理协议——SNMP

路由器应支持 IETF RFC1902 至 IETF RFC1907 中规定的 SNMPv2。

路由器可选支持 IETF RFC2573、IETF RFC2574 中规定的 SNMPv3。

SNMP 应使用 UDP/IP 作为传输层/网络层协议。也可以使用其他协议（例如 IETF RFC1418 和 IETF RFC1089）。

SNMP 管理请求向路由器任何一个接口的 IP 发出时，该操作应生效。实际的管理动作应由路由器或路由器的代理完成。

支持 SNMPv2 协议的路由器应实现 SNMPv2 MIB（IETF RFC1907）。

路由器应实现所有的 SNMP 操作。

路由器应提供一种机制来限制 SNMP 陷阱（trap）消息的产生速率。路由器可以通过 IETF RFC1224 中描述的异步告警管理算法来实现上述机制。

10.2 区域表格

为本标准描述方便，假设路由器中存在一个抽象的区域表格。该表格包含多个条目，每个条目给一个特定区域，包含完全定义该区域属性需要的参数。对抽象区域表格的实现方法在本标准范围之外，由实现者决定。

路由器的区域表格建议至少包含两个条目。

路由器应允许用户手工（即不使用 SNMP）检查、增、删、改 SNMP 区域表格中的条目。用户应能够设置区域名，或者构造 MIB 视图。用户应能以只读（即不允许 SET）或者读写（允许 SET）的方式配置区域。

用户应能定义至少一个 IP 地址，当使用自陷（trap）时，对每个捕获或 MIB 视图的通知将送到该 IP 地址。这些 IP 地址应定义在区域或 MIB 视图库内。允许或不允许在区域或 MIB 视图库上发通知应是可配置的。

路由器应提供为特定团体提供有效管理员列表的能力。如果提供上述列表，路由器应检验 SNMP 数据包源地址的有效性，如果该地址没有在上述列表中出现则应丢弃该数据包。如果数据包被丢弃，路由器应采取 SNMP 认证失败时的相应措施。

区域表格应存储在非-不稳定的存储器内。

区域表格的初始状态应包含一个条目，其中区域名串为 Public，访问权限为只读。该条目的缺省状态为不允许发送自陷（trap）。如果实现，该条目应保存在区域表格中，直到管理员改变或者删除。

10.3 标准 MIBS

所有关于路由器配置的 MIB 都应实现：

- MIB-II STD16, IETF RFC1213) 中的系统、接口、组应实现。
- 接口扩展 MIB (IETF RFC1229) 应实现。
- IPv6 TCP MIB (IETF RFC4022) 应实现。
- IPv6 UDP MIB (IETF RFC4113) 应实现。

- IP MIB 在 (IETF RFC4293) 应实现。
- IPv6 MIB 的文本约定和通用组 (IETF RFC2465) 应实现。
- IPv6 MIB 的 ICMPv6 组 (IETF RFC2466) 应实现。
- 支持 MLD 协议的路由器应实现用于 MLD 的 IPv6 MIB (IETF RFC3019)。
- 如果路由器有以太网, 802.3, STARLAN 接口, 以太网链路 MIB (IETF RFC1398) 应实现。
- 如果路由器有 802.4 接口, 802.4MIB (IETF RFC1230) 应实现。
- 如果路由器有 802.5 接口, 802.5MIB (IETF RFC1231) 应实现。
- 如果路由器由使用 V.24 信令的接口, 例如 RS-232, V.10, V.11, V.35, 或者 RS-422/423/449, RS-232 (IETF RFC1317) 应实现。
- 如果路由器有 T1/DS1 接口, T1/DS1 MIB (IETF RFC1406) 应实现。
- 如果路由器有 T3/DS3 接口, T3/DS3 MIB (IETF RFC1407) 应实现。
- 如果路由器有 SMDS 接口, SMDS 接口协议 MIB (IETF RFC1304) 应实现。
- 如果路由器在任何接口上支持 PPP, PPP MIB (IETF RFC1471, IETF RFC1472 和 IETF RFC1473) 应实现。
- 如果路由器在任何接口上支持 FrameRelay, FrameRelay MIB (IETF RFC1513, IETF RFC2115) 应实现。

10.4 RMON MIBS (可选)

路由器应支持 RMON MIB (IETF RFC1757 和 IETF RFC2021)。

其中, 路由器应支持 RMON 第 1 组 (以太网统计数据组)、第 2 组 (历史记录控制组)、第 3 组 (以太网历史记录组)、第 4 组 (告警组) 和第 10 组 (事件组)。可以选择支持第 5 组 (主机组)、第 6 组 (前 N 个主机组)、第 7 组 (矩阵组)、第 8 组 (筛选组) 和第 9 组 (包捕获组)。

10.5 厂商指定的 MIBS

互联网标准和根据实验的 MIB 不能完全覆盖网络单元统计、状态、配置和控制信息。路由器厂商可以自己开发覆盖上述信息的 MIB 扩展, 这些 MIB 扩展称为厂商特定的 MIB。

由于这些信息不能由标准或实验得到的 MIB 得到, 厂商特定的 MIB 应提供存取这些统计、状态、配置和控制信息的方法, 而且这些信息能用于监视和控制操作。

厂商应根据 IETF RFC1155 的规定使所有厂商特定的 MIB 变量可用, 并以 IETF RFC1212 规定的方式来描述。

10.6 保存改变

通过 SNMP 调整的参数可以存储在非-不稳定存储器中。

11 IPv6 的安全

IPSec 是在 IP 层提供通信安全而制定的一套协议族, 它可有效地保护 IP 数据包的安全, 它采取的具体保护形式包括: 数据起源地验证; 无连接数据的完整性验证; 数据内容的机密性; 抗重播保护; 以及有限的数据流机密性保证。

路由器应支持 AH 协议, 在实现 AH 协议时需要实现下列算法:

- a) 使用 MD5 的 HMAC 算法 (必选);
- b) 使用 SHA-1 的 HMAC 算法 (可选)。

路由器可选支持 ESP 协议，支持 ESP 协议的路由器需要实现下列算法：

- a) 使用 MD5 的 HMAC 算法（必选）；
- b) 使用 SHA-1 的 HMAC 算法（可选）。

路由器应支持手工密钥管理，可选支持 IKE。

路由器在进行路由协议包交换时，应支持使用 AH 头通过 MD5 进行加密认证的功能。

IPSec 具体的规定见 YD/T 1466。

12 对移动 IP 的支持

路由器可选支持 IETF RFC3775 中对于所有路由器的通用要求。路由器可选支持其中家乡代理的功能。

13 运行与维护

13.1 定义

路由器的 O&M 中应包含以下措施：

- a) 设备资源利用率；
- b) 网络接口带宽利用率；
- c) 丢包率；
- d) 设备软件运行情况；
- e) 路由器的配置情况；
- f) 开关机配置；
- g) 安装或升级新硬件；
- h) 安装或升级新软件；
- i) 监视路由器及相连网络的状态及性能；
- j) 流量统计的收集；
- k) 以及上述措施的协调等；
- l) 诊断路由器的处理器、网络接口、相连的网络、或通信链路的硬件问题；
- m) 故障定位、记录和存储；
- n) 故障告警；
- o) 在宕机后重新启动或重新引导路由器；
- p) 配置（重新配置）路由器；
- q) 发现及诊断互联网问题例如拥塞、路由环回、差错 IP 地址、黑洞、包雪崩、主机的错误行为；
- r) 暂时的或者永久的网络拓扑改变；
- s) 运行软件的故障检查及记录等。

路由器以及相连的通信链路通常作为一个系统由集中的 O&M 组织来维护运行。该组织可能通过一个网络运行中心（NOC）来执行 O&M 功能。由于路由器可能与 NOC 连接在不同网上，路由器支持 NOC 从互联网远程监视及控制非常重要。由于网络故障通常会终止网络访问，NOC 要求路由器应支持通过一条备用途径，通常是接在路由器配置口上的调制解调器来实现网络管理。

因为在互联网中传输的 IP 包通常会使用多于一个 NOC 控制下的路由器，互联网故障诊断将牵涉到

多个 NOC 的合作。在某些情况下，路由器需要超过一个 NOC 来监视，但由于过多的监视会损害路由器性能，因此只有在必要时才可以这样做。

13.2 路由器初始化

13.2.1 最少路由器配置

在路由器能转发包以前，存在一个最少的路由器配置条件：

- 路由器知道该物理接口上相关联的至少一个逻辑接口的 IP 地址和网络前缀长度；
- 路由器知道该接口是非编号接口，并且路由器知道其路由器 ID；
- 路由器不允许使用厂商配置的缺省 IP 地址，前缀长度，路由器 ID；
- 路由器不允许假设一个没有配置的接口是一个非编号接口。

13.2.2 地址及前缀初始化

路由器应允许静态配置 IP 地址，前缀长度，并存储在非-不稳定存储器中。

路由器在系统初始化前应保证没有配置 IP 地址和前缀长度，并允许开启和配置动态获取地址的功能，如 DHCP 协议，路由器可以在系统初始化过程中动态得到 IP 地址和前缀长度，用于网络管理员登录设备。

13.3 运行和维护具体规定

13.3.1 定义

在路由器上实施 O&M 功能有多个可用的模型：一个是仅在本地模型，该模型要求 O&M 功能只能在本地执行（例如，接在路由器上的终端）；一个是完全远程管理，在本地只允许作最少的操作（例如，强迫引导），大多数 O&M 从远端由 NOC 执行；另一个是中间模型，例如 NOC 人员可以登录到路由器上作为一个主机，使用 Telenet 协议执行本地也能申请的功能。仅在本地模型一般在路由器安装时使用，路由器通常需由 NOC 远端操作，所以路由器应实现远端操作。

远端 O&M 功能可以通过控制代理（程序）实现。在直接应用中，O&M 功能直接由 NOC 通过标准互联网协议实现（例如，SNMP，UDP，TCP）。在间接应用中，控制代理支持这些协议并控制路由器使用恰当的协议。建议使用直接应用的方式。

厂商应提供这样一种环境：用户使用控制代理或其他 NOC 软件应象在标准操作系统中编程一样。使用标准互联网协议 TCP 和 UDP 应能帮助实现上述要求。

路由器远程监视和远程控制存在重要的访问控制问题：一方面应确保应用这些功能时路由器资源的有效控制，例如路由器监视时应不过分占用 CPU 资源；另一方面，O&M 功能应具有相对高的优先级，因为路由器拥塞的时候通常是最需要 O&M 操作的时候。

13.3.2 带外访问

路由器应提供带外（OOB）访问。OOB 访问应提供所有带内访问的功能。带外访问应实现访问控制，防止非法访问。

13.3.3 路由器 O&M 功能

13.3.3.1 维护——硬件诊断

在本地硬件维护时，每个路由器应作为一个独立设备来操作，在路由器处应提供运行诊断程序的工具和方法。路由器应能在故障情况时运行诊断程序。

13.3.3.2 控制——下载内存和重新引导

路由器应同时提供带内和带外的机制来使网络管理员重新装载、停止、重新启动路由器。路由器应提供一种机制（例如 watchdog 定时器），当路由器因为软硬件差错挂起一定时间后，自动重新启动。

路由器应实现一种机制将路由器的内存（和/或路由器宕机后所有对厂家调试有用的状态信息）保存到本地稳定存储设备或者通过在线转储机制保存到另一台主机中。

13.3.3.3 控制——配置路由器

每台路由器都有需要配置的参数。路由器参数更新后应不需要重新引导，最坏情况下需要重新启动。可能存在某些情况，改变参数后应重启路由器（例如改变某接口的 IP 地址）。这些情况下，应小心将对路由器和周边网络的影响减少到最小。

应存在一种方法自动或人工地从网络配置路由器。路由器应能从另一台路由器或主机下载/上载配置参数。路由器应提供一种方法，无论作为应用程序方式或者路由器功能方式，能相互转换配置参数格式和人工可编辑格式。路由器应具有某种稳定的存储器存储配置。

13.3.3.4 网络引导系统软件

路由器应将系统软件保存在非-不稳定存储器中，例如 PROM，EPROM，或者磁盘中。路由器可以通过网络从其他主机或路由器下载系统软件。

能将系统软件保存在本地非-不稳定存储器中的路由器可以实现配置成从网络引导系统软件。实现上述功能的路由器应配置成当无法从网络引导系统时可以从本地引导系统。

路由器可以给予不同系统软件区分不同配置。如果不同版本软件的配置命令有所改变，路由器应能兼容上一版本的配置命令。

13.3.3.5 对差错配置的检查与反应

路由器应实现一种机制检测差错配置并做出响应。如果命令不正确运行，路由器应给出差错消息。路由器不应接受差错格式的命令，即使该命令本身是正确的。

另一种差错是对路由器连接网络的差错配置。路由器可以实现检测网络的误配置。路由器可以将发现的差错记录到日志或者网络上其他路由器或主机，管理员可以看到可能存在的问题。

13.3.3.6 最少干扰

对路由器配置的改变应最小程度地影响网络。当在路由器上作很小的改动时，路由表不应没有必要地刷新。如果路由器上运行多个路由协议，停止一个路由协议不应干扰其他路由协议，除非某网络需要通过多个路由协议获得路由。

13.4 安全性考虑

13.4.1 数据过滤

当路由器用于局域网时，应提供以下数据过滤功能：

- a) 路由器的每个端口应可以配置 ACL 访问控制列表功能；
- b) 路由器的每个端口应提供基于源 IP 地址的数据过滤；
- c) 路由器的每个端口应提供基于目的 IP 地址的数据过滤；
- d) 路由器的每个端口应提供基于端口的数据过滤。

13.4.2 路由器防攻击

路由器应具有防范非法攻击的功能（如 LAND 攻击、TCP SYN 攻击、Smurf 攻击、水滴攻击等）。路由器应能过滤收到的 ICMPv6 数据包。路由器可以为 ICMPv6 数据包的透传设定门限。

13.4.3 配置安全

路由器应实现以下配置安全：

- 认证 SNMP 报文诊断；
- 普通用户和特权用户的登录身份检验；
- 定期检查配置信息。

13.4.4 审计与审计记录

a) 安全性审计

路由器应提供一种机制审计与安全性相关的故障与冲突：

- 授权（Authorization）失败：差错通行字，无效的 SNMP 通信，无效的授权令牌；
- 对控制策略的违反：禁止的源路由，被过滤掉的目的地；
- 授权通过：正确通行字，远程登录带内访问，控制台访问等。

b) 配置改变

路由器应提供一种方法来记录配置的改变，该记录内容包括登录时间、账号、实施的操作和时间等信息。

13.4.5 配置控制

在为路由器装载软件/固件时，厂商应负责使用良好的配置控制。如果允许在互联网上更新或下载则，应提供一种方法是客户能验证下载的内容有效。这种验证可以通过检查下载内容校验和来实现。如果厂商提供用户远程改变路由器配置的能力，例如通过远程登录，这种能力应是可配置的，缺省情况应是不允许远程配置。在允许远程配置前，路由器应要求有效的认证。这种认证不应在网络上传输认证明文，例如，如果实现远程登录，厂商应实现 Kerberos、S-Key 或者其他类似认证机制。

路由器不允许存在未记载于文档的访问后门，或通用密码。厂商应确保这种用于调试或者开发产品的访问途径在产品分销到客户之前已删除。

13.4.6 监控

路由器应能基于 IP 接口或进行合法的信息截取。

13.5 计费信息统计功能

路由器应提供包数、字节数、端口、业务类型等信息统计功能。

14 技术指标

14.1 物理层接口技术指标

路由器的物理层接口技术指标详见第 5 章的规定。

14.2 路由器的丢包率（packet loss rate）

丢包率是指路由器在稳定的持续负荷下由于资源缺少在应该转发的数据包中不能转发的数据包所占比例。

丢包率通常用作衡量路由器在超负荷工作时路由器的性能。

14.3 路由器吞吐量（throughput）

吞吐量是路由器的包转发能力。

吞吐量与路由器端口数量、端口速率、数据包长度、数据包类型、路由计算模式（分布或集中）以及测试方法有关。一般泛指处理器处理数据包的能力。由于路由器设计使用在不同目的和应用环境，对

吞吐量作范围限制没有意义。本标准对吞吐量不作规范。只作为重要的性能指标供比较。

14.4 路由器的时延 (latency)

路由器时延指需转发的数据包最后一比特进入路由器端口到该数据包第一比特出现在端口链路上的时间间隔。

该时间间隔是存储转发方式工作的路由器的处理时间。对于 cut through 方式工作的设备可能会得到负的时延。(该种设备在收到部分数据包后即开始转发)。

通常所测试的时延是指测试仪表发出数据包到经过路由器转发后收到该数据包的时间间隔。上述时延与测试数据包的长度、链路速率及吞吐量都相关。

时延对网络性能影响较大。特此作如下规范:

64byte IP 包时延小于 1ms (暂定)

512byte IP 包时延小于 15ms (暂定)

1518 byte IP 包时延小于 350ms (暂定)

14.5 错序比 (out-of-sequence ratio)

错序比指路由器转发数据包时错序包所占总包数的比例。

本标准对错序比不作规范, 只作为重要的性能指标供比较。

14.6 路由器认证技术指标

路由器支持 PPP 等协议时应当支持连接认证技术: 应支持 PAP/CHAP 认证。PAP/CHAP 认证符合 IETF RFC1994 规范。

认证的平均响应时间 < 6s。

14.7 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。

由于路由器设计使用在不同目的和应用环境, 对路由表容量作范围限制没有意义。本标准对路由表容量不作规范。只作为重要的性能指标供比较。

14.8 背靠背帧数 (back-to-back frame)

路由器能够处理的最大背靠背帧数。

背靠背帧是指一组固定长度的帧, 帧间间隔是媒体所允许的最小帧间隔。

由于路由器设计使用在不同目的和应用环境, 对背靠背帧数作范围限制没有意义。本标准对背靠背帧数不作规范。只作为重要的性能指标供比较。

14.9 计费

路由器可以通过例如 Radius 协议提供计费数据。

14.10 同步

边缘路由器同步方式: 采用主从同步方式。

边缘路由器内部时钟应采用四级时钟设备。

边缘路由器内部时钟主要性能要求如下:

a) 时钟单元可采用一般晶体时钟。

b) 自由运行频率准确度: $\pm 50 \times 10^{-6}$ 。

c) 牵引范围: $\pm 50 \times 10^{-6}$ 。

14.11 可靠性指标

系统的无故障工作时间：MTBF>8760h。

系统故障恢复时间<0.5h。

建议对关键设备进行备份。

15 环境要求

15.1 环境要求

15.1.1 温湿度、气压条件

机房内温湿度、气压条件要求见YD/T 1712第3.1节。

15.1.2 洁净度条件

机房内洁净度条件要求见 YD/T 1712 第 3.2 节。

15.1.3 电磁环境

机房内的电磁场强度要求见 YD/T 1712 第 3.4 节。

15.2 路由器抗电磁干扰的能力

路由器设备抗电磁干扰的能力要求见 GB19286-2003 第 11 章和第 12 章。

15.3 路由器防雷击能力

路由器设备防雷击能力应当符合 GB3483 和 YD/T 5098 的要求。

16 电源与接地

电源和路由器接地应当符合GB4943.1和YD/T 5098的要求。

广东省网络空间安全协会受控资料

附 录 A
(规范性附录)
PPP 上的 IPv6

A.1 介绍

PPP 主要由 3 部分组成:

在串行链路上封装数据报文的方法。

用于建立、配置、测试数据链路连接的链路控制协议。

用于建立和配置不同网络层协议的网络控制协议簇。

为了在 PPP 的连接上建立通信, PPP 连接的两端都应首先发送 LCP 包来配置和测试数据链路。当建链完毕, 同时可选能力也通过 LCP 进行了必要的协商之后, PPP 应发送 NCP 包选择和配置一个或多个网络层协议。当被选中的每一个网络层协议配置完成后, 每个网络层协议上的数据报文可以通过该链路来发送。

在本附录中, 建立和配置基于 PPP 连接的 IPv6 协议的 NCP 指的是 IPv6 控制协议 (IPv6CP)。

链路将会保持通信直到明确的 LCP 包或 NCP 包关闭链路, 或者是发生了某些外在的事件 (另一端电力中断, 载波中断等等)。

A.2 发送IPv6 的报文

任何 IPv6 数据包传送之前 PPP 应达到网络层协议的阶段, 同时 IPv6 控制协议应达到开放的状态。

IPv6 包被封装在 PPP 数据链路层帧的消息域中, 此时协议域的类型为 0x0057 (IPv6)。

通过 PPP 链路传输的最大 IPv6 包长和 PPP 数据链路层帧的消息域的最大长度是一样的。支持 IPv6 的 PPP 链路的消息域的大小至少和 IPv6 要求的链路最小的 MTU 一样大, 即 1280byte。

A.3 IPv6 的PPP网络控制协议

在 PPP 链路的两端, IPv6CP 可以可靠的配置, 激活, 停止 IPv6 协议模块。它和链路控制协议采用同样的包交换机制。在 PPP 达到网络层协议阶段之前, IPv6CP 包可能不进行交换。在此阶段到达之前收到的 IPv6CP 的包将会被丢弃。

IPv6CP 同链路控制协议在以下特例中是完全一致的:

a) 数据链路层协议域。IPv6CP 包被封装在 PPP 数据链路层帧的消息域中, 此时协议域的类型为 0x8057 (IPv6 控制协议)。

b) 编码域。IPv6CP 只使用了 1~7 的编码 (Configure-Request, Configure-Ack, Configure-Nak, Configure-Reject, Terminate-Request, Terminate-Ack and Code-Reject)。IPv6CP 应把其他的编码看作是無法识别的, 并且在 Code-Rejects 中加以拒绝。

c) 超时。在 PPP 达到网络层协议阶段之前, IPv6CP 包可能不进行交换。一个实现应该在等待 Configure-AcK 或其他响应超时之前准备等待认证和链路质量决定阶段的完成。建议只有在用户干预或经过一段可配置的时间之后实现才能放弃建链的过程。

d) 配置选项类型。IPv6CP 有一套独特的配置选项集。

A.4 IPv6CP配置选项

A.4.1 概述

IPv6CP 配置选项允许对 IPv6 的参数进行协商。它有一套单独的选项，使用与 LCP 相同的配置选项格式。如果在 Configure-Request 包中没有配置选项，则将假设使用默认的配置选项值。

最近在“IANA 协议值与指定服务网页”中定义了 IPv6CP 选项类型域的最新值。当前值分配如下：
接口标识符；
IPv6 压缩协议。

在本附录中只定义了接口标识符和 IPv6 压缩协议这两个 IPv6 选项。将来任何其他的 IPv6CP 配置选项将在独立的文档中定义。

A.4.2 接口标识符

在链路的本地端点进行地址自动配置时采用惟一的 64 比特的接口标识符，这个配置选项提供了协商该接口标识符的方法（见第 5 章）。一个 Configure-Request 消息应包含一个正确的接口标识选项的实例。在 PPP 链路上接口标识符应是惟一的，也就是说，完成协商后，在 PPP 链路的两端选择不同的接口标识符的值。接口标识符可能在更广的范围内也是惟一的。

在请求这个配置选项之前，实现需要选择一个暂定接口标识符。应该选择非 0 值的暂定接口标识符以保证该值对于链路来讲是惟一的，而且有可能的话，这个值在 IPv6CP 有限状态机初始化过程中应该是可重新生成的（管理性的关闭，重新开放，重启动。等等）。与选择完全随机的接口标识符相比，选择可重新生成的接口标识符更为合理，这样在通过接口标识符构造全局地址时就能提供一定的稳定性。

假定接口标识符比特是按照从 0 到 63 这种规范的 bit 顺序，最高比特位是 0，第六比特位是 u 比特（IEEE EUI-64 中定义的通用/本地比特），该比特位用来指示接口标识符是否为全球惟一的 IEEE 标识符。如果是全球惟一的 IEEE 标识符，则该位置 1，否则置 0）。

以下为按优先选择顺序选择暂定接口标识符的方法：

a) 如果节点的 IEEE 全球性标识符（EUI-48 或 EUI-64）是可用的，那么由于它的惟一性，IEEE 全球性标识符将要被用来构造暂定接口标识符。当从节点上的其他设备提取 IEEE 全球性标识符时，应该按照规范的比特顺序进行提取。

对于 EUI-64 标识符来说，只需要反转“u”比特即可。图 A.1 所示一个全球惟一的 EUI-64 标识符。

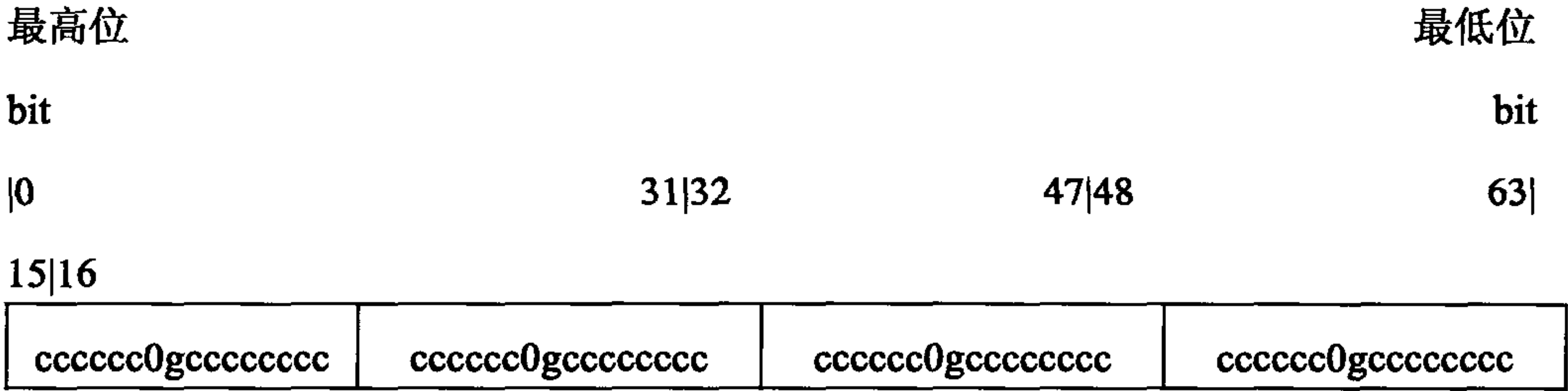


图 A.1 全球惟一的 EUI-64 标识符格式

“c” 比特的位置被分配给 company_id，“0” 值表示这是一个全局地址，“g” 比特表示组/个体，“e” 比特的位置被分配给 extension-identifier。

它对应的 IPv6 接口标识符的格式如图 A.2 所示。

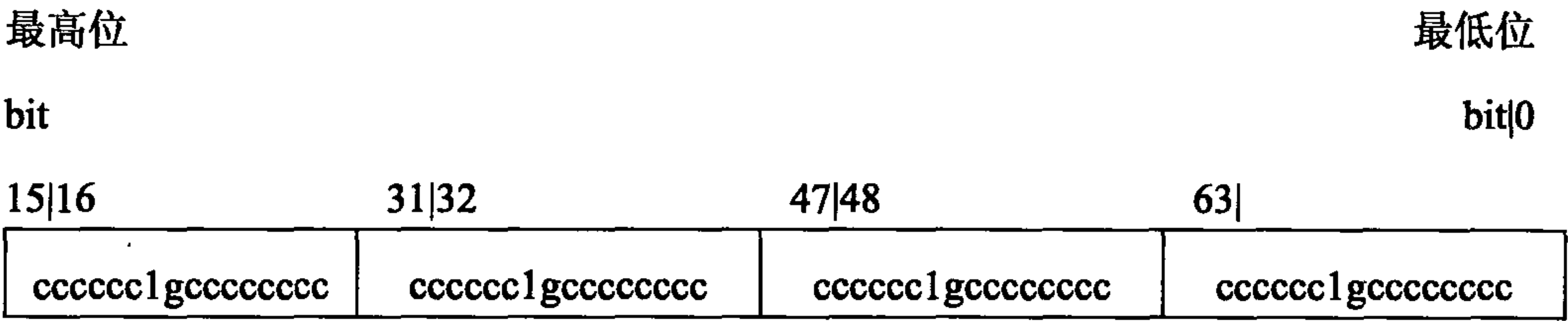


图 A.2 EUI-64 标识符对应的 IPv6 接口标识符格式

与 EUI-64 相比，惟一的变化是反转了通用的/本地比特的值。

要转变为 EUI-64 格式，EUI-48 标识符应首先在 48 比特 MAC 地址的中部（在 company_id 和 EUI-48 的 extension-identifier 值之间）插入两个字节 0xFF 和 0xFE。图 A.3 所示为全球惟一的 48 比特的 EUI-48 标识符格式。它所对应的 IPv6 接口标识符格式如图 A.4 所示。

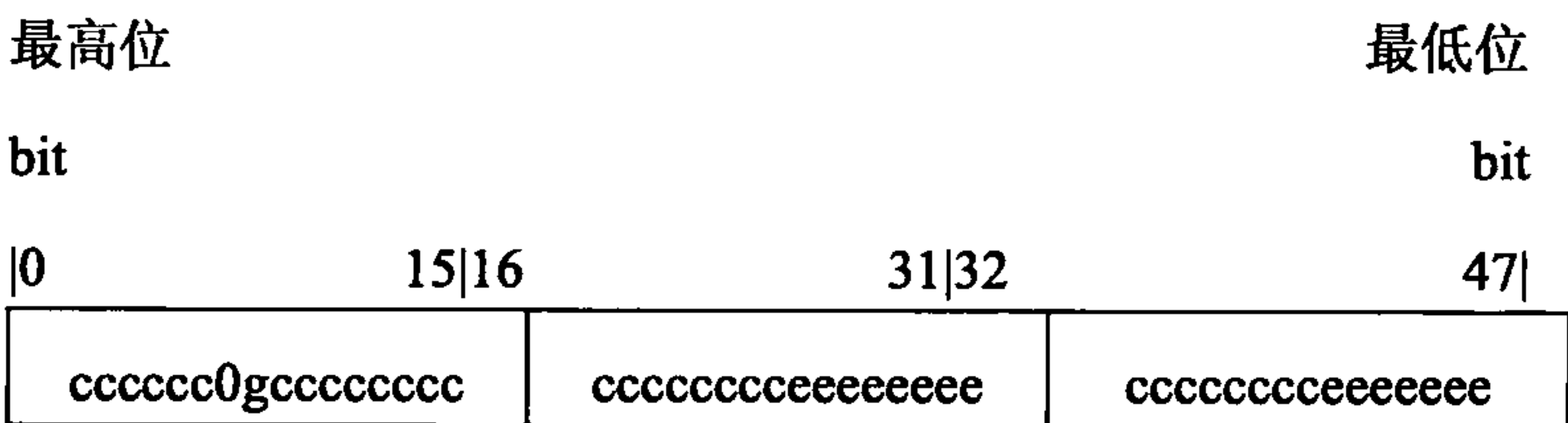


图 A.3 全球惟一的 48 比特的 EUI-48 标识符格式

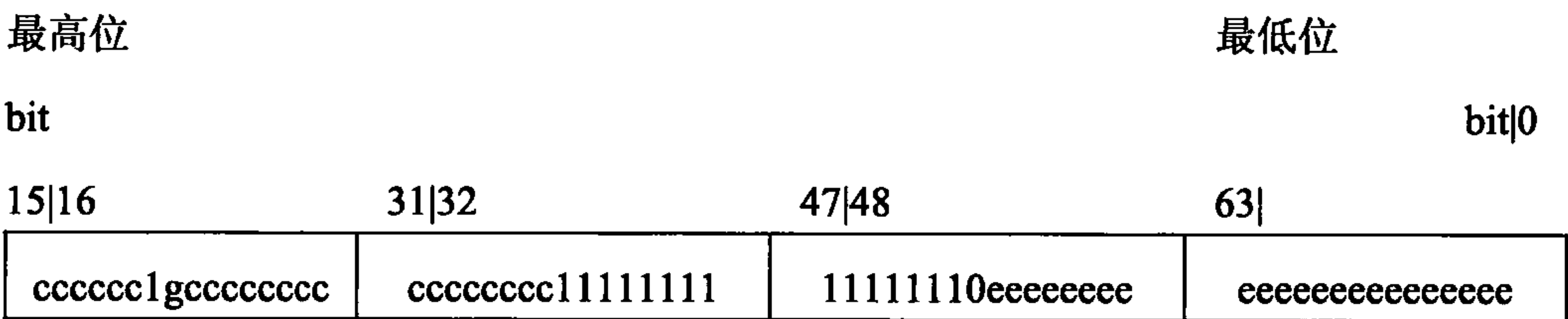


图 A.4 EUI-48 标识符对应的 IPv6 接口标识符格式

- b) 如果一个 IEEE 的全球性的标示符不可用，那么应选择不同的惟一的标识符源。建议使用链路层的地址，机器的串口号等标识符。这时接口标识符的“u”比特应被设置为 0。
- c) 如果无法找到合适的惟一的标识符源，建议生成一个随机的数。这时接口标识符的“u”比特应被设置为 0。

要成功协商接口标识符就需要有惟一的或随机的标识符源。如果既不产生惟一数字也不是产生随机数字，那么在 Configure-Request 中就推荐用 0 值作为端口标识符。作为响应，PPP 对端可能会提供一个合法的非零值。如果至少有 PPP 的一端可以为本身和它的对端产生不同的非零值，那么标识符的协商将会成功。

当收到包含接口标识符配置选项消息的 Configure-Request 时，如果接收端实现了此选项，则它应把发送到对端的最后一个 Configure-Request 中的接口标识符与收到的接口标识符进行比较。按照比较的结果，接收端应按以下方式响应：

如果两个接口标识符不同但收到的接口标识符为 0，则向对端发送一个 Configure-Nak 消息，其中带有建议对端使用的不同的非零接口标识符。这个接口标识符应同发送到对端的最后一个 Configure-Request 中的接口标识符不同。建议该值在 IPv6CP 有限状态机初始化过程中始终应该是可复制的。该接口标识符中的“u”比特应置 0，除非从 EUI-48/EUI-64 中提取的标识符是由远端提供用于特殊的用途。

如果两个接口标识符不同并且收到的接口标识符不为 0，那么收到的接口标识符应得到确认，也就是说，发送一个包含接收到的接口标识符的 Configure-Ack，这意味着接收端认可请求的接口标识符。

如果两个接口标识符相同并且非零，则应向对端发送一个 Configure-Nak 消息，其中带有建议对端使用的不同的非零接口标识符。这个接口标识符应同发送到对端的最后一个 Configure-Request 中的接口标识符不同。建议该值在 IPv6CP 有限状态机初始化过程中始终应该是可复制的。该接口标识符中的“u”比特应置 0，除非从 EUI-48/EUI-64 中提取的标识符是由远端提供用于特殊的用途。

如果两个接口标识符都为 0，那么应发送 Configure-Reject 消息终止协商，其中的接口标识符的值设置为 0。这种情况下，不能通过协商得到惟一的接口标识符。

当收到包含接口标识符配置选项消息的 Configure-Request 时，如果接收端不支持此选项，那么应发送 Configure-Reject 消息。

在请求端发送了 Configure-Request 消息后，如果收到 Configure-Nak 消息或计时器超时，则应发送一个新的 Configure-Request 消息。

如果收到一个含合法接口标识符的 Configure-Reject 消息，那么新的 Configure-Request 中应不包含接口标识符选项。

如果接收到的 Configure-Nak 消息中的接口标识符与前一个发送给对端的 Configure-Nak 中的接口标识符不同，则该消息指明了一个惟一的接口标识符。在这种情况下，新的 Configure-Request 应发送前一个来自对端的 Configure-Nak 中建议的标识符值。但是如果收到的接口标识符和最后发送的 Configure-Nak 中的相同，那么应选择一个新的接口标识符。这时，接收端将发送一个包含新的暂定标识符值的 Configure-Request 消息。这种过程（发送 Configure-Request 消息，接收 Configure-Request 消息，发送 Configure-Nak 消息，接收 Configure-Nak 消息）可能会发生几次，但是极不可能重复出现。最有可能的情况是，PPP 两端选择的接口标识符可能很快会出现分歧，从而导致链路被中断。

如果需要协商接口标识符，而对端的 Configure-Request 消息中又没有提供这一选项，那么这个选项应该被附加在 Configure-Nak 消息中。其中暂定的接口标识符的值应能被远端所接受，也就是它应该和 PPP 链路的本端所选定的接口标识符不同。发自对端的下一个 Configure-Request 消息可能包括这个选项，如果收到的下一个 Configure-Request 消息仍不包含这一选项，则接收端不能再发送包含此选项的 Configure-Nak 消息，这时它将假设对端不支持这个选项。

在默认情况下 PPP 的实现应该尝试在 PPP 端点之间协商接口标识符。

接口标识符配置选项的格式如图 A.5 所示。比特的传输顺序由低向高。

0	8	16	31
(bit)			
类型		长度	接口标识符 (MS 字节)
接口标识符 (未完)			
接口标识符 (LS 字节)			

图 A.5 接口标识符配置选项的格式

类型：1。

长度：10。

接口标识符：如果不能找到合适的惟一标识符源，链路上很可能会出现零值或惟一的 64 比特的接口标识符。

默认：如果合法的接口标识符没有协商成功，则不能使用默认的接口标识符的值。本附录没有规定在这种情况下进行恢复的方法。这时可以通过手动的方法来配置接口的接口标识符。

A.4.3 IPv6压缩协议

这个配置选项提供了一种协商使用特定的 IPv6 包压缩协议的方法。IPv6 压缩协议配置选项被用来表明接收压缩数据包的能力。如果双向都要求压缩那么链路上的每个端点应单独请求这个选项。在缺省的情况下，压缩不可用。

通过这一选项的协商而进行的 IPv6 压缩只对 IPv6 数据报有效，不应该把它与通过 CCP 协商得到的

压缩结果相混淆，后者的协商结果可能会影响所有的数据报。

IPv6 压缩协议配置选项格式如图 A.6 所示。比特的传输顺序由低向高。

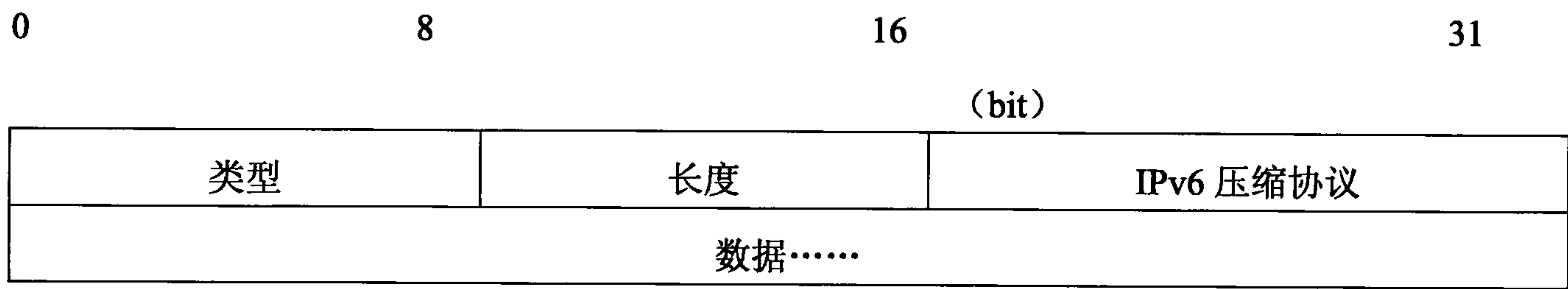


图 A.6 IPv6 压缩协议配置选项格式

类型：2。

长度：≥4。

IPv6 压缩协议：该域由 2 个字节构成，表明希望使用的压缩协议。由于使用同样的压缩协议，所以这个域值和 PPP 数据链路层协议域的值经常是相同的。目前没有分配 IPv6 压缩协议域的值。特定的分配将在定义特定压缩算法的文档中给出。

数据：数据域为 0 或更多的字节，在数据域中包含由特殊压缩协议决定的附加数据。

默认：无 IPv6 压缩协议可用。

A.5 无状态自动配置和链路本地地址

PPP 接口的 IPv6 单播地址的接口标识符应该在 PPP 建链的 IPv6CP 阶段进行协商。如果合法的接口标识符没有协商成功，本附录没有规定在这种情况下进行恢复的方法。这时可以通过手动的方法来配置接口的接口标识符。

只要接口标识符在 PPP 建链的 IPv6CP 阶段进行了协商，那么再在 IPv6 无状态自动配置协议中执行重复地址检测就是多余的。因此建议在支持 IPv6CP 接口标识符选项协商的 PPP 链路中 DupAddrDetectTransmits 自动配置变量的值为零。

PPP 接口的链路本地地址格式如图 A.7 所示。

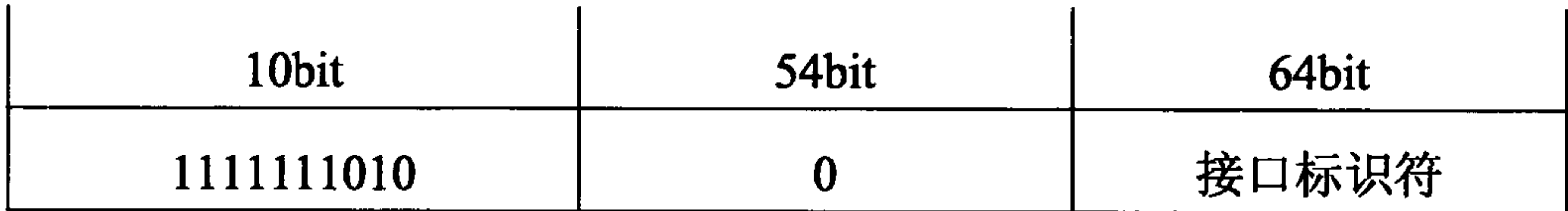


图 A.7 PPP 接口的链路本地地址格式

最高位的 10 比特是链路本地地址的前缀 FE80::。在链路本地前缀和接口标识符域之间填充了 54 个 0 比特。

A.6 安全考虑

PPP 的 IPv6 控制协议扩展可以与所有规定的 PPP 认证和加密机制共同使用。

附 录 B
(规范性附录)
在以太网上传输 IPv6 数据包

注：本附录规范了在以太网上 IPv6 数据包传输的帧格式，IPv6 链路本地地址的构成方法以及无状态自动配置的地址。本附录还规范了源/目的链路层地址选项的内容，在以太网上传输路由器请求、路由器广告、邻居请求、邻居广告、重定向消息时会使用到这一选项。

B.1 最大传输单元

在以太网上 IPv6 数据包的默认 MTU 值是 1500 字节。这一个值可以通过包含指定较小 MTU 的 MTU 选项的路由器广告；或者通过在每个节点上手工配置来缩减。如果一个以太网端口上接收到的路由器广告中包含一个 MTU 选项并且 MTU 大于 1500，或者大于手工配置的值，则上述 MTU 选项可以被记录在系统管理日志中，但是应被忽略。

在本文档中，从 DHCP 上接收到的信息被认为是“手动配置”，以太网则包含 CSMA/CD 和基于 ISO/IEC 8802-3 的具有多种速率的全双工子网。

B.2 帧格式

IPv6 数据包在标准的以太网帧中传输。以太网包头包含目的以太网地址、源以太网地址和以太网类型编码。该以太网类型编码的值应为十六进制的 86DD。以太网包的数据域包含 IPv6 包头和紧接 IPv6 包头的载荷，其后可能会有填充字节以满足以太网链路最小帧大小的要求。帧格式如图 B.1 所示。

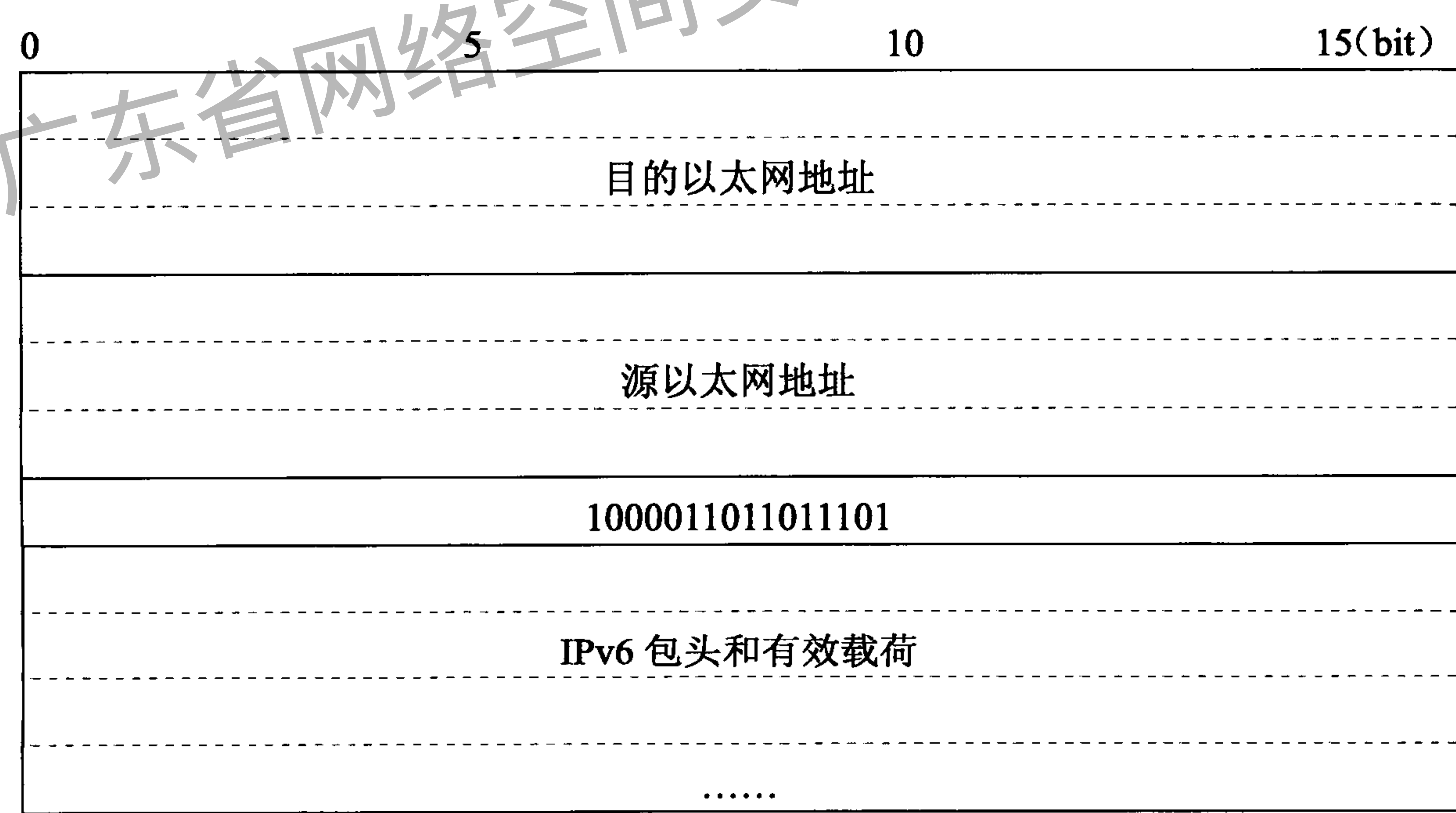


图 B.1 帧格式

B.3 无状态自动配置

以太网接口的接口标识基于由接口内置的 48 比特 IEEE 802 地址得到的 EUI-64 标识。EUI-64 的构成如下所示。

EUI-64 的公司标识（即 EUI-64 的前三个字节）使用以太网地址的 OUI（即以太网地址的前三个比特）。EUI 的第四和第五字节设置为十六进制的 FFFE。EUI-64 的最后三个字节使用以太网地址的最后三

个字节。

接口标识在 EUI-64 基础上设置了通用/本地 (U/L) 比特, U/L 是 EUI-64 第一个字节的次低比特。由于接口的内置地址通常来自统一管理的地址空间, 是全球惟一的, 所以设置该比特通常将值 0 改为 1。统一管理的 IEEE 802 地址或 EUI-64 的 U/L 比特设置为 0; 而全球惟一性 IPv6 接口标识 U/L 比特设置为 1, 见 IETF RFC2373。例如, 以太网接口内置地址是十六进制的 34-56-78-9A-BC-DE, 则接口标识为 36-56-78-FF-FE-9A-BC-DE。

通过手工或者软件配置的不同的 MAC 地址不应被用于构造接口标识。如果一定要使用这样的 MAC 地址, 则该地址的全球惟一性将在 U/L 比特值中反映出来。

用于以太网接口无状态自动配置的 IPv6 地址前缀的长度应为 64bit。

B.4 链路本地地址

根据上面的定义, 以太网接口的 IPv6 链路本地地址应通过在 FE80::/64 前缀后添加接口标识来构成, 如图 B.2 所示。

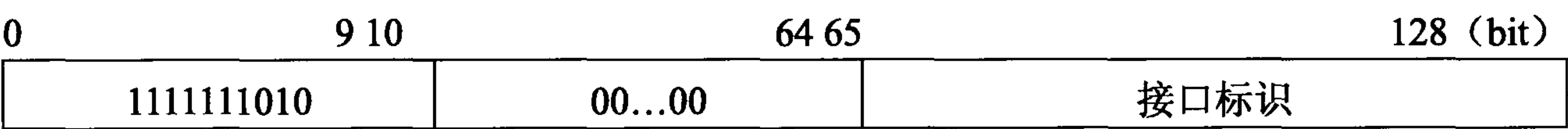


图 B.2 以太网接口的 IPv6 链路本地地址

B.5 地址映射——单播

将 IPv6 单播地址映射到以太网链路层地址的方法详见 IETF RFC2461。当链路层是以太网时, 源/目的链路层地址选项格式如图 B.3 所示。

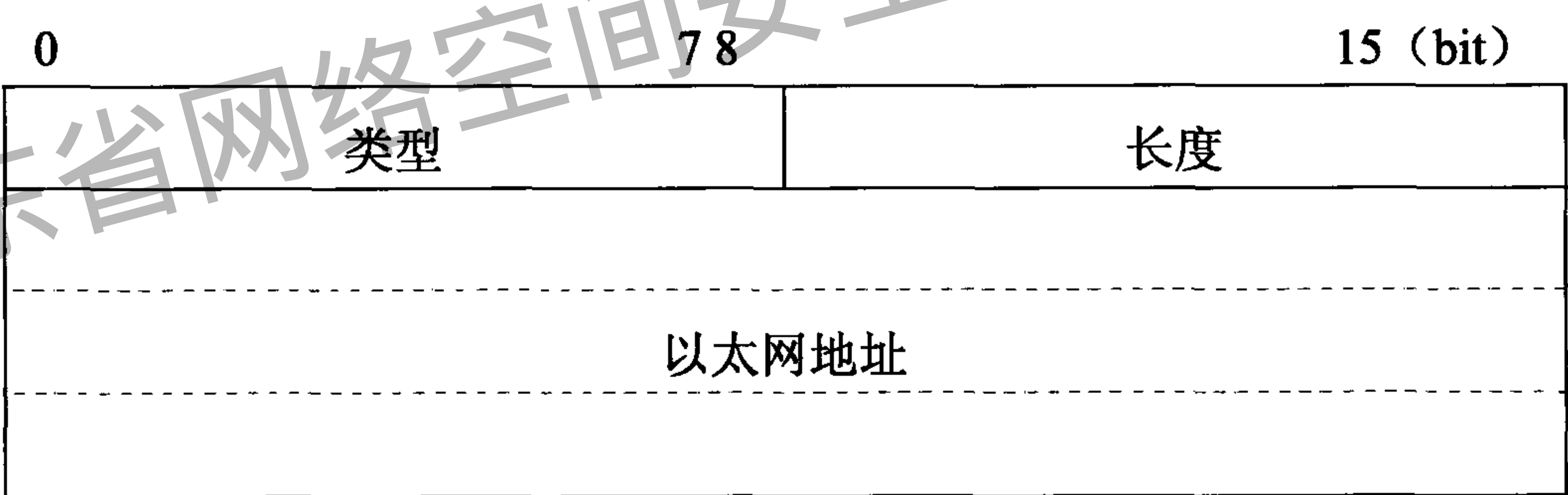


图 B.3 源/目的链路层地址选项格式

选项域:

类型: 1 表示源链路层地址; 2 表示目的链路层地址。

长度: 1 (一个单位为 8 个字节)。

以太网地址: 48 比特以太网 IEEE 802 地址使用规范的比特次序。上述地址是接口当前响应的地址, 可能与用于构造接口标识的内置地址不同。

B.6 地址映射——组播

带有由 16 个字节组成 (从 DST[1]到 DST[16]) 的组播目的地址 (DST) 的 IPv6 数据包被传输到前两个字节为十六进制的 3333, 最后 4 个字节是 IPv6 组播目的地址的最后 4 个字节的以太网组播目的地址。格式如图 B.4 所示。

0	7	8	15 (bit)
00110011		00110011	
DST (13)		DST (14)	
DST (15)		DST (16)	

图 B.4 带有组播目的地址的 IPv6 数据包格式

广东省网络空间安全协会受控资料

广东省网络空间安全协会受控资料

中华人民共和国
通信行业标准
IPv6 网络设备技术要求
边缘路由器

YD/T 1452-2014

*

人民邮电出版社出版发行
北京市丰台区成寿寺路1号邮电出版大厦
邮政编码：100164
北京康利胶印厂印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2015年12月第1版
印张：3 2015年12月北京第1次印刷
字数：80千字

15115·499

定价：30元

本书如有印装质量问题，请与本社联系 电话：(010)81055492