



中华人民共和国国家标准化指导性技术文件

GB/Z 43728.200—2024/IEC TR 62357-200:2015

电力系统管理及其信息交换 第200 部分：从互联网协议版本4 (IPv4) 到互联网协议版本6 (IPv6) 的迁移指南

Power systems management and associated information exchange—
Part 200: Guidelines for migration from Internet Protocol version 4 (IPv4) to
Internet Protocol version 6 (IPv6)

(IEC TR 62357-200:2015, IDT)

2024-03-15发布

2024-10-01 实施

国家市场监督管理总局
国家标准化管理委员会

发布

目 次

前言 III

引言 IN

1 范围 1

2 规范性引用文件 1

3 术语、定义、缩略语和约定 5

 3.1 术语和定义 5

 3.2 缩略语 6

 3.3 约定 9

 3.4 网络图形符号 9

4 互联网技术 10

 4.1 IPv4 10

 4.2 IPv6 14

 4.3 IPv 4 和 IPv 6比较 17

5 IPv 4 到 IPv 6的过渡 19

 5.1 IPv 6迁移的必要性 19

 5.2 迁移类型 20

 5.3 IPv 6迁移对电力系统通信的影响 20

6 迁移方法 21

 6.1 迁移原则 21

 6.2 地址映射 21

 6.3 双栈设备 24

 6.4 隧道技术 28

 6.5 转换 32

 6.6 迁移计划 35

7 基于 IP 的应用协议 36

 7.1 第3层以上的应用协议 36

 7.2 IEC 61850的第3层通信 36

 7.3 IEC 61850的3层通信(承载2层流量) 39

 7.4 其他应用协议 40

 7.5 虚拟专用网络叠加 40

8 变电站自动化场景 40

 8.1 场景概述 40

 8.2 场景1:通过 IPv 6实现变电站与外部通信 41

8.3 场景2:通过 ALG 和转换器实现 IPv 6设备访问变电站 43

8.4 场景3:变电站全部或部分支持 IPv 645

8.5 场景4:中间设备作为 ALG46

8.6 场景5:传统 IPv 4网络集成仅支持IPv 6的设备 48

9 发电厂自动化场景 50

9.1 通则 50

9.2 传统 IPv 4寻址方案 51

9.3 IPv 6寻址及共存方案 51

9.4 IPv 6优势 51

9.5 问题 52

10 建议 52

10.1 给制造商的建议 52

10.2 给网络工程师的建议 52

10.3 给 IEC 标准制定工作组的建议 53

10.4 执行迁移计划的时间表 53

参考文献 54

前 言

本文件按照GB/T1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/Z43728《电力系统管理及其信息交换》的第200部分，GB/Z43728 已经发布了以下部分：

——第1部分：参考架构；

——第200部分：从互联网协议版本4(IPv4)到互联网协议版本6(IPv6)的迁移指南。

本文件等同采用IEC TR62357—200:2015《电力系统管理及其信息交换 第200部分：从互联网协议版本4(IPv4)到互联网协议版本6(IPv6)的迁移指南》，文件类型由IEC技术报告调整为我国的国家标准化指导性技术文件。

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专利的责任。

本文件由中国电力企业联合会提出。

本文件由全国电力系统管理及其信息交换标准化技术委员会(SAC/TC 82)归口。

本文件起草单位：国网浙江省电力有限公司、国网浙江省电力有限公司温州供电公司、国家电网有限公司国家电力调度控制中心、中国电力科学研究院有限公司、国网电力科学研究院有限公司、中国南方电网电力调度控制中心、国家电网有限公司华东分部、国网江苏省电力有限公司、国网浙江省电力有限公司台州供电公司、国网吉林省电力有限公司、国网河南省电力有限公司、国网天津市电力公司、江苏宏源电气有限责任公司、国电南京自动化股份有限公司、北京四方继保自动化股份有限公司、南瑞集团有限公司、上海交通大学、国网信息通信产业集团有限公司。

本文件主要起草人：陈水耀、杜奇伟、戚峰、金学奇、常乃超、朴林、李劲松、孙丹、周斌、沈健、张喜铭、李金、卞宝银、李芹、张亮、彭志强、张琦兵、畅广辉、吴佳毅、陈建、洪道鉴、奚洪磊、左建勋、郑子淮、王周虹、阮黎翔、任雁铭、崔瑶、张静、刘辉乐、黄银强、张超、徐红泉、顾建、郑翔、杨剑友、刘栋、周泰斌、俞凯、杨力强、陈培东、刘昌旭、杨松、林佳颖、王海园、张磊、吴坡、卢巍、刘文彪、施正钗、翁嘉明、陈凡、潘宇晨、李治、赵颖科、纪陵。

引 言

GB/Z43728《电力系统管理及其信息交换》旨在提升电力系统管理及其信息交换效率，拟由两个部分构成。

- 第1部分：参考架构。目的在于为本系列标准提供参考架构。
- 第200部分：从互联网协议版本4(IPv4) 到互联网协议版本6(IPv6) 的迁移指南。目的在于提供从互联网协议版本4(IPv4) 向互联网协议版本6(IPv6) 进行数据通信协议迁移的定义、指南以及建议。

本文件介绍了与迁移相关的 IPv4 和 IPv6 技术方面的教程。

本文件描述了电力通信系统通用和特定应用领域中的迁移目的以及迁移策略问题。

本文件提供了对设备制造商、网络工程师以及标准组织的建议。

本文件为电力系统数据通信标准组织给出如下时间表：

- a) 从2015年开始，所有新的或经修订的 IEC 文件都支持 IPv6 作为授权项目的选项。
- b) 在2030年之前，所有IEC 文件将同时支持IPv6 和 IPv4 作为可选项。
- c) 在2050年之后，所有IEC 文件认为 IPv4 将会被禁止。

电力系统管理及其信息交换

第200 部分：从互联网协议版本4(IPv4) 到互联网协议版本6(IPv6) 的迁移指南

1 范围

本文件适用于电力系统的信息交换，包括但不限于变电站、控制中心、运维中心、能量管理系统、基于同步相量的电网稳定系统、大型能源发电(包括化石燃料发电)、分布式能源发电(可再生能源，如风能和太阳能)、储能、负荷管理(需求侧管理和配电级消费或生产的需求响应)。

本文件解决了从互联网协议版本4(以下简称IPv4) 迁移到互联网协议版本6(以下简称 IPv6) 时遇到的问题，描述了迁移策略，包括对应用程序、通信协议栈、网络节点、配置、地址分配、网络安全及相关管理的影响。

本文件描述了从IPv4 向 IPv6 迁移的概念和必要路径，并考虑了IEC 61850 框架中若干协议的向后兼容性。

根据电力系统信息交换参考架构(IEC 62357-1)对 IEC 标准和技术报告进行审查，考虑到允许或要求 IPv6 对这些文件的影响，本文件支持因引入IPv6 对这些文件的修订。

本文件未强制要求在电力通信中使用IPv6 技术。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

ISO/IEC8602 信息技术 提供 OSI 无连接方式运输服务的协议(Information technology—Protocol for providing the OSI connectionless-mode transport service)

注：GB/T16723—1996 信息技术 提供 OSI无连接方式运输服务的协议(ISO/IEC 8602:1995, IDT)

IEC 60050-191 国际电工词汇 可信性与服务质量(International electrotechnical vocabulary; chapter 191:dependability and quality of service)

IEC 60870-5-104 远动设备及系统 第5-104部分：传输规约采用标准传输协议集的 IEC 60870-5-101网络访问(Telecontrol equipment and systems—Part 5-104:Transmission protocols -Network access for IEC 60870-5-101 using standard transport profiles)

IEC 61400-25(所有部分) 风力发电场监控系统通信(Communications for monitoring and control of wind power plants)

IEC 61588 网络测量和控制系统的精确时钟同步协议(Precision clock synchronization protocol for networked measurement and control systems)

注：GB/T25931—2010 网络测量和控制系统的精确时钟同步协议(IEC 61588:2009, IDT)

IEC 61850(所有部分) 电力自动化通信网络和系统(Communication networks and systems for power utility automation)

IEC 61850-6 电力自动化通信网络和系统 第6部分：与智能电子设备有关的变电站内通信配置

描述语言(Communication networks and systems for power utility automation—Part 6:Configuration description language for communication in electrical substations related to IEDs)

注: DL/T860.6—2012 电力自动化通信网络和系统 第6部分: 与智能电子设备有关的变电站内通信配置描述语言(IEC61850-6:2009, IDT)

IEC61850-8 (所有部分) 电力自动化通信网络和系统 特定通信服务映射(SCSM)[Communication networks and systems for power utility automation-Specific communication service mapping(SCSM)]

IEC 61850-8-1 电力自动化通信网络和系统 第8-1部分: 特定通信服务映射(SCSM)—映射到MMS(ISO 9506-1 和ISO 9506-2)及ISO/IEC 8802-3[Communication networks and systems for power utility automation—Part 8-1:Specific communication service mapping(SCSM)—Mappings to MMS(ISO 9506-1 and ISO 9506-2)and to ISO/IEC 8802-3]

注: DL/T860.81—2016 电力自动化通信网络和系统 第8-1部分: 特定通信服务映射(SCSM)—映射到MMS(ISO 9506-1 和ISO 9506-2)及ISO/IEC 8802-3(IEC 61850-8-1:2011, IDT)

IEC 61850-8-2 电力自动化通信网络和系统 第8-2部分: 特定通信服务映射(SCSM)—映射到XMPP[Communication networks and systems for power utility automation—Part 8-2:Specific communication service mapping(SCSM)—Mapping to Extensible Messaging Presence Protocol(XMPP)]

IEC TR 61850-90-1 电力自动化通信网络和系统 第90-1 部分: DL/T 860 在变电站间通信中的应用(Communication networks and systems for power utility automation—Part 90-1:Use of IEC 61850 for the communication between substations)

注: DL/T860.901—2014 电力自动化通信网络和系统 第90-1部分: DL/T 860在变电站间通信中的应用(IEC TR 61850-90-1:2010, IDT)

IEC TR 61850-90-2 电力自动化通信网络和系统 第90-2 部分: 变电站和控制中心之间使用IEC61850 通信(Communication networks and systems for power utility automation—Part 90-2:Using IEC 61850 for the communication between substations and control centres)

IEC TR 61850-90-4 电力自动化通信网络和系统 第90-4部分: 网络工程指南(Communication networks and systems for power utility automation—Part 90-4:Network engineering guidelines)

IEC TR 61850-90-5 电力自动化通信网络和系统 第90-5部分: 使用IEC 61850传输符合 IEEE C37.118的同步相量信息(Communication networks and systems for power utility automation—Part 90-5:Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118)

IEC 62351(所有部分) 电力系统管理及其信息交换 数据和通信安全(Power systems management and associated information exchange-Data and communications security)

IEC 62357-1 电力系统管理及其信息交换 第1部分: 参考架构(Power systems management and associated information exchange Part 1:Reference architecture)

IEC 62439-3 工业通信网络 高可靠性自动化网络 第3部分: 平行冗余协议(PRP) 及高可用性无缝冗余协议(HSR)[Industrial communication networks—High availability automation networks—Part 3:Parallel Redundancy Protocol(PRP)and High-availability Seamless Redundancy(HSR)]

ITU X.234 信息技术提供 OSI 无连接方式运输服务的协议(Information technology—Protocol for providing the OSI connectionless-mode transport service)

IEEE 802.1AB IEEE标准 局域网和城域网 站点和介质访问控制互连发现(IEEE Standard [or Local and metropolitan area networks—Station and Media Access Control Connectivity Discovery)

IEEE 802.1QIEEE 标准 局域网和城域网 虚拟桥接局域网(VLAN 和优先级)(IEEE standards for local and metropolitan area network;Virtual bridged local area networks(VLANs and priorities))

IEEE 1815 IEEE电力标准 系统通信 分布式网络协议[IEEE Standard for Electric Power—Systems Communications—Distributed Network Protocol (DNP3)]

RFC 0768 用户数据报协议(User Datagram Protocol)

RFC 0791 Internet 协议[Internet Protocol(IPv4)]

RFC 0792 Internet 控制报文协议[Internet Control Message Protocol(ICMP)]

RFC 0793 传输控制协议(Transmission Control Protocol,Protocol Specification)

RFC0826 以太网地址解析协议(An Ethernet Address Resolution Protocol)

RFC0894 基于以太网的 IP 数据报传输标准(A Standard for the Transmission of IP Datagrams over Ethernet Networks)

RFC 0959 文件传输协议[File Transfer Protocol(FTP)]

RFC1142 OSI 中间系统到中间系统域内路由协议(OSI IS-IS Intra-domain Routing Protocol,February 1990)

RFC1240 基于 UDP 版本1的 OSI 无连接传输服务(OSI Connectionless Transport Services on top of UDP Version 1)

RFC1305 网络时间协议版本3[Network Time Protocol(Version 3)]

RFC1918 私有网络地址分配(Address Allocation for Private Internet)

RFC1981 IPv6 路径 MTU 发现协议(Path MTU Discovery for IP version 6)

RFC 2131 动态主机配置协议[Dynamic Host Configuration Protocol(DHCPv4)]

RFC2147 基于IPv6 大包的 TCP 和 UDP(TCP and UDP over IPv6 Jumbograms)

RFC 2328 开放式最短路径优先协议版本2(OSPF Version 2)

RFC 2401 网络层安全协议(IPsec)

RFC2460 IPv6 规范[Internet Protocol,Version 6(IPv6)Specification]

RFC2464 基于以太网的IPv6 报文传输(Transmission of IPv6 Packets over Ethernet Networks)

RFC2473 IPv6 隧道通用报文规范(Generic Packet Tunneling in IPv6 Specification)

RFC2529 基于无显式隧道的 IPv6 over IPv4 传输 (Transmission of IPv6 over IPv4 Domains without Explicit Tunnels)

RFC 2663 IP 网络地址转换术语和注意事项 [IP Network Address Translator(NAT) Terminology and Considerations]

RFC2766 网络地址转换-协议转换 [Network Address Translation—Protocol Translation (NAT-PT)]

RFC 2767 基于“协议栈翻译”技术的双栈主机[Dual Stack Hosts using the“Bump-In-the-Stack” Technique(BIS)]

RFC3022 传统 IP 网络地址转换[Traditional IP Network Address Translator(Traditional NAT)]

RFC3056 通过 IPv4 云实现 IPv6 域之间的连接[Connection of IPv6 Domains via IPv4 Clouds (6to4)]

RFC3315 IPv6 动态主机配置协议[DHCP for IPv6(DHCPv6)]

RFC3338 基于“API 翻译”技术的双栈主机[Dual Stack Hosts Using“Bump-in-the-API” (BIA)]

RFC3416 简单网络管理协议版本2[Version 2 of the Protocol Operations for the Simple Network Management Protocol(SNMP)]

- RFC3736 IPv6 无状态动态主机配置协议服务[Stateless Dynamic Host Configuration Protocol (DHCP)Service for IPv6]
- RFC3921 可扩展消息与表示协议：即时消息与表示[Extensible Messaging and Presence Protocol(XMPP):Instant Messaging and Presence]
- RFC 3931 IETF 网络工作组，二层隧道协议版本3[IETF Network Working Group,Layer Two Tunneling Protocol-Version 3(L2TPv3)]
- RFC3986 统一资源标识：通用语法[Uniform Resource Identifier(URI):Generic Syntax]
- RFC4038 IPv6 迁移的应用指导(Application Aspects of IPv6 Transition)
- RFC4193 IPv6 唯一本地单播地址(Unique Local IPv6 Unicast Addresses)
- RFC4213 IPv6 主机和路由器的基本转换机制(Basic Transition Mechanisms for IPv6 Hosts and Routers)
- RFC4271 边界网关协议4[A Border Gateway Protocol 4(BGP-4)]
- RFC 4291 IPv6 寻址体系结构(IP Version 6 Addressing Architecture)
- RFC4302 IP 认证头部(IP Authentication Header)
- RFC4303 IP 封装安全载荷[IP Encapsulating Security Payload(ESP)]
- RFC4380 基于网络地址转换的 IPv6 UDP 隧道技术[Teredo:Tunneling IPv6 over UDP through Network Address Translators(NATs)]
- RFC4443 IPv6 控制报文协议[Internet Control Message Protocol(ICMPv6)for the Internet Protocol Version 6(IPv6)Specification]
- RFC4459 网络隧道中的 MTU 和分片问题(MTU and Fragmentation Issues with In-the-Network Tunneling)
- RFC4554 企业网络中使用VLAN 实现IPv4-IPv6 共存(Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks)
- RFC4632 无类域间路由：Internet 地址分配和聚合计划 [Classless Inter-domain Routing (CIDR):The Internet Address Assignment and Aggregation Plan]
- RFC4861 IPv6 邻居发现协议[Neighbor Discovery for IP version 6(IPv6)]
- RFC4862 IPv6 无状态地址自动配置(IPv6 Stateless Address Autoconfiguration)
- RFC4919 基于 IPv6 的低功耗无线个域网[IPv6 over Low-Power Wireless Personal Area Networks(6LoWPANs)]
- RFC4944 基于 IEEE 802.15.4 网络传输 IPv6 报文(Transmission of IPv6 Packets over IEEE 802.15.4 Networks)
- RFC 5214 站点内自动隧道寻址协议[Intra-Site Automatic Tunnel Addressing Protocol (ISAT-AP)]
- RFC5340 基于IPv6 的 OSPF 协议(OSPF for IPv6)
- RFC5569 基于 IPv4 架构的 IPv6 快速部署[IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)]
- RFC5641 2 层隧道协议版本3扩展电路状态值[Layer Two Tunneling Protocol-Version 3 (L2TPv3)Extended Circuit Status Values]
- RFC5771 IPv4 组播地址分配的IANA 指南(IANA Guidelines for IPv4 Multicast Address Assignments)
- RFC5905 网络时间协议版本4:协议和算法规范(Network Time Protocol Version 4:Protocol

and Algorithms Specification)

RFC5942 IPv6 子网模型: 链路和子网前缀之间的关系(IPv6 Subnet Model:The Relationship between Links and Subnet Prefixes)

RFC5991 Teredo 安全更新[Teredo Security Updates(Updates RFC 4380)]

RFC 6052 IPv4/IPv6 转换器的 IPv6 寻址(IPv6 Addressing of IPv4/IPv6 Translators)

RFC 6081 Teredo 扩展(Teredo Extensions)

RFC6144 IPv4/IPv6 转换框架[Framework for IPv4/IPv6 Translation(NATs after RFC 4966)]

RFC 6145 IP/ICMP 转换算法(IP/ICMP Translation Algorithm)

RFC6146 有状态 NAT64: 从 IPv6 客户端到 IPv4 服务器的网络寻址和协议转换(Stateful NAT64:Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers)

RFC6282 基于IEEE802.15.4 网络 IPv6 数据报的压缩格式(Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks)

RFC6333 IPv4 耗尽后的轻型双栈宽带部署(Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion)

RFC 6535 基于“主机翻译”技术的双栈主机[Dual-Stack Hosts using the“Bump-in-the-Host” Technique(BIH)]

RFC 6550 IPv6 低功耗有损网络路由协议(IPv6 Routing Protocol for Low-Power and Lossy Networks)

RFC 6775 基于低功耗无线个域网的IPv6 邻居发现优化[Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks(6LoWPANs)]

RFC 6864 更新IPv4 标识字段的规范(Updated Specification of the IPv4 ID Field)

RFC7040 公共IPv4-over-IPv6 接入网(Public IPv4-over-IPv6 Access Network)

RFC 7059 IPv6 over IPv4 隧道机制的比较(A comparison of IPv6-over-IPv4 Tunnel Mechanisms)

RFC7230 超文本传输协议(HTTP/1.1): 消息语法和路由(Hypertext Transfer Protocol (HTTP/1.1):Message Syntax and Routing)

3 术语、定义、缩略语和约定

3.1 术语和定义

IEC 60050-191 界定的以及下列术语和定义适用于本文件。

3.1.1

应用层网关 application-level gateway

使用传输信息的应用层内容, 将第一个协议接收的应用层有效载荷转换为第二个协议的应用层有效载荷的网络设备。

3.1.2

网桥 bridge

在 OSI 模型的数据链路层(第2层)连接不同网段的网络设备。

[来源: ISO/IEC 10038,ANSI/IEEE 802.1D—2004]

3.1.3

解封装 decapsulation

解析用于传输的下层网络协议, 提取上层网络协议的数据元素。

3.1.4

DHCP服务器 DHCP server

为给定时间段分配主机 IP 地址(租约)的网络服务器。

3.1.5

域名服务器 domain name server

根据给定通信对象的统一资源定位符(URL), 解析 IP 地址的网络服务器。

3.1.6

封装 encapsulation

将上层网络协议的数据元素嵌入到用于传输的下层网络协议中。

3.1.7

主机 host

应用 IP 协议的网络节点。

3.1.8

公网地址 public address

全局管理的唯一地址。

3.1.9

私网地址 private address

可在独立于公网的网络中重用的本地管理地址。

3.1.10

路由器 router

在 OSI 模型的网络层(第3层)连接不同网段的网络设备。

3.1.11

转换 translation

将一个协议转换为另一个协议的过程, 确保通信双方感知不到对方协议。

3.1.12

转换器 translator

将数据包从一个协议转换成另一个协议的设备, 而不使用来自通信双方的其他信息。

3.1.13

传输层网关 transport-level gateway

根据被传信息的传输层内容, 将所接收第一个协议的有效载荷转换成第二个协议的网络设备。

3.1.14

隧道技术 tunneling

在两个实体之间采用一种网络协议重新封装另一种网络协议的报文传输方式。

3.1.15

隧道端点 tunneler

隧道两端封装/解封装报文的设备。

3.2 缩略语

下列缩略语适用于本文件。

6LoWPAN: 基于 IPv6 的低功耗无线个域网[IPv6 over Low power Wireless Personal Area Network(RFC 4919)]

A-record:DNS 的32位IPv4 地址记录(32-bit IPv4 address record from DNS)
 AAAA:DNS 的128位IPv6 地址记录(128-bit IPv6 address record from DNS)
 ACSI:抽象通信服务接口(Abstract Communication Service Interface)
 AH: 认证头部[Authentication Header(RFC 4302)]
 ALG: 应用层网关(Application-Level Gateway)
 API: 应用程序编程接口(Application Programming Interface)
 ARP: 地址解析协议[Address Resolution Protocol(RFC 0826)]
 AS:自治系统(Autonomous System)
 BFD:双向转发检测(Bidirectional Forwarding Detection)
 BGP: 边界网关协议(互联网EGP 的继承协议)[Border Gateway Protocol(successor of EGP in Internet)]
 BIH: 主机翻译[Bump In the Host(RFC 6535)]
 CIDR: 无类域间路由[Classless Inter-domain Routing(RFC 4632)]
 CPE: 客户终端设备(Customer Premise Equipment)
 DER: 分布式能源和可再生能源(Distributed Energy and Renewable energy)
 DF:不分片位[Don't Fragment bit(IPv4)]
 DHCP: 动态主机配置协议(Dynamic Host Configuration Protocol)
 DHCPv4:DHCP 版本4[DHCP version 4(RFC 2131)]
 DHCPv6:DHCP 版本6[DHCP version 6(RFC 3315)]
 DMZ: 非军事区(DeMilitarized Zone)
 DNP3: 分布式网络协议版本3[Distributed Network Protocol version 3(IEEE 1815)]
 DNS:域名服务器(Domain Name Server)
 DSO: 配电系统运营商(Distribution System Operator)
 EGP: 外部网关协议(Exterior Gateway Protocol)
 ESP: 封装安全载荷[Encapsulating Security Payload(RFC 4303)]
 EUI-64: 扩展唯一标识符(IEEE 注册机构)LExtended Unique Identifier(IEEE Registration Authority)]
 FTP: 文件传输协议[File Transfer Protocol (RFC 0959)]
 GOOSE: 面向通用对象的变电站事件[Generic Object Oriented Substation Events(IEC 61850-8-1)]
 GRE: 通用路由封装(Generic Routing Encapsulation)
 HTTP: 超文本传输协议[Hypertext Transfer Protocol(HTTP)(RFC 7230)]
 HSR: 高可用性无缝冗余协议[High-availability Seamless Redundancy(IEC 62439-3)]
 IANA: 互联网号码分配机构(Internet Assigned Numbers Authority)
 ICMP: 互联网控制消息协议[Internet Control Message Protocol(RFC 0792)]
 ICMPv4:ICMP 版本4[ICMP version 4(RFC 0792)]
 ICMPv6:ICMP 版本6[ICMP version 6(RFC 4443)]
 ID:标识符(Identification)
 IED:智能电子设备[Intelligent Electronic Device(IEC 61850)]
 IETF: 互联网工程任务组(Internet Engineering Task Force)
 IGP:内部网关协议(Interior Gateway Protocol)
 IP: 互联网协议[Internet Protocol(RFC 0791)]

IPv4: 互联网协议版本4[Internet Protocol Version 4(RFC 0791)]
IPv6: 互联网协议版本6[Internet Protocol Version 6(RFC 2460)]
IPSec: 网络层安全协议[Internet Protocol network layer security(RFC 2401)]
IS-IS: 中间系统到中间系统协议[Intermediate System to Intermediate System(RFC 1142, ISO/OSI 8473)]
ISP: 互联网服务提供商(Internet Services Provider)
ITU: 国际电信联盟(International Telecommunication Union)
LAN: 局域网(Local Area Network)
L2TP: 2 层隧道协议[Local Area Network](Layer 2 Tunneling Protocol(RFC 3931))
LLDP: 链路层发现协议[Link Layer Discovery Protocol (IEEE 802.1AB)]
MAC: 介质访问控制(Medium Access Control)
MAP-T: 地址和端口转换映射 (Mapping of Address and Port Using Translation)
MF: 分片位(IPv4)[More Fragment(IPv4)]
MMS: 制造报文规范(Manufacturing Messaging Specification)
MPLS: 多协议标签交换(Multi-Protocol Label Switching)
MTU: 最大传输单元[Maximum Transmission Unit(RFC 0791,RFC 2460)]
NAT: 网络地址转换[Network Address Translation(RFC 3022)]
NCC: 网络控制中心(Network Control Center)
NDP: 邻居发现协议[Neighbor Discover Protocol(RFC 4861)]
NERC: 北美电力可靠性委员会[North-american Electricity Reliability Corporation(USA)]
NIST: 国家标准与技术研究院(美国)[National Institute of Standards and Technology(USA)]
NPDU: 网络协议数据单元[Network Protocol Data Unit(ISO/OSI)]
NTP: 网络时间协议[Network Timing Protocol(RFC 1305)]
OMB: 行政管理和预算局(美国)[Office of Management and Budget(IJSA)]
OSI: 开放系统互联[Open Systems Interconnection(ISO)]
OSPF: 开放式最短路径优先协议[Open Shortest Path First(RFC 2328)]
OSPFv4: IPv4 OSPF 协议[OSPF for IPv4(RFC 2328)]
OSPFv6: IPv6 OSPF 协议[OSPF for IPv6(RFC 5340)]
PDC: 相量数据集中器(Phasor Data Concentrator)
PDU: 协议数据单元[Protocol Data Unit (ISO/OSI)]
PMU: 相量测量单元(Phasor Measurement Unit)
PRP: 并行冗余协议[Parallel Redundancy Protocol (IEC 62439-3)]
PTP: 精确时钟同步协议[Precision Time Protocol (IEC 61588)]
PVID: 基于端口的 VLAN ID(Port-base VLAN ID)
RIR: 地区性互联网注册机构(Regional Internet Registry)
RPL: 低功耗及有损网络路由协议 [Routing Protocol for Low-power and lossy networks (RFC 6550)]
RTU: 远方终端设备(Remote Terminal Unit)
SCADA: 监视控制与数据采集系统(Supervisory Control And Data Acquisition)
SCD: 变电站配置描述[System Configuration Description(IEC 61850-6)]
SCL: 变电站配置描述语言[System Configuration Language(IEC 61850-6)]

SDH: 同步数字体系[Synchronous Digital Hierarchy(ITU-T)]

SED: 系统交换描述[System Exchange Description(IEC 61850-6)]

SIT: 无状态IP/ICMP 协议转换算法[Stateless IP/ICMP Translation algorithm(RFC 6145)]

SLAAC: 无状态地址自动配置[Stateless Address AutoConfiguration(RFC 4862)]

SNMP: 简单网络管理协议[Simple Network Management Protocol(RFC 3416)]

SNTP: 简单网络时间协议[Simple Network Time Protocol (RFC 5905)]

SONET: 同步光纤网络(Synchronous Optical Network)

SMV: 采样测量值[Sampled Measurement Values (IEC 61850)]

TCP: 传输控制协议[Transmission Control Protocol (RFC 0793)]

TRT: 传输中继转换器(Transport Relay Translator)

UDP: 用户数据报协议[User Datagram Protocol (RFC 0768)]

ULA: 唯一本地单播地址[Unique Local unicast Address(IPv6)]

URL: 统一资源定位符[Uniform Resource Locator(RFC 3986)]

USGv6: 美国政府互联网提议协议版本6(NIST)[United States Government Internet Protocol Version 6 Initiative(NIST)]

VID: 虚拟局域网 ID[VLAN ID(IEEE 802.1Q)]

VLAN: 虚拟局域网[Virtual Local Area Network (IEEE 802.1Q)]

VLL: 虚拟租用线路(Virtual Leased Line)

VPN: 虚拟专用网络(Virtual Private Network)

WAMPAC: 广域监测、保护和控制(Wide Area Monitoring Analysis Protection and Control System)

WAN: 广域网(Wide Area Network)

XML: 可扩展标记语言(Extended Markup Language)

XMPP: 可扩展消息与表示协议[Extensible Message and Presence Protocol (RFC 3921)]

3.3 约定

3.4 网络图形符号

图1中的图形符号适用于本文件。

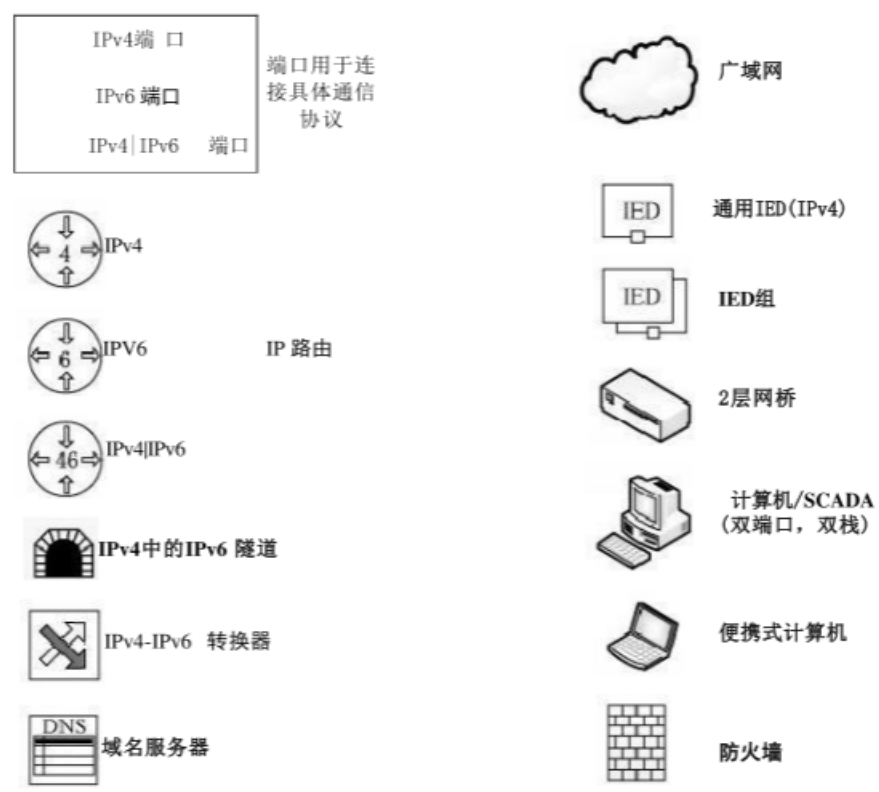


图 1 图形符号

4 互联网技术

注：第4章已从IEC TR61850-90-12中复制，以提供独立的文档。在本文件的未来版本中不会对其进行维护。

4.1 IPv4

4.1.1 来源

IPv4(RFC0791) 自1980年以来一直是互联网的基础，至今仍然是使用最广泛的网络协议。其主要特点是：

- a) IPv4 是无连接的，即路由器不保留以前的消息；
- b) IPv4 使用32位网络源地址和目的地址；
- c) IPv4 由一套路由协议支持。

4.1.2 以太网中的 IPv4 报文传输

RFC0894 定义了以太网帧中 IPv4 数据包格式。第3层报文头部位位于第2层报文头部之后，以太网帧 IP 报文头部格式见图2。

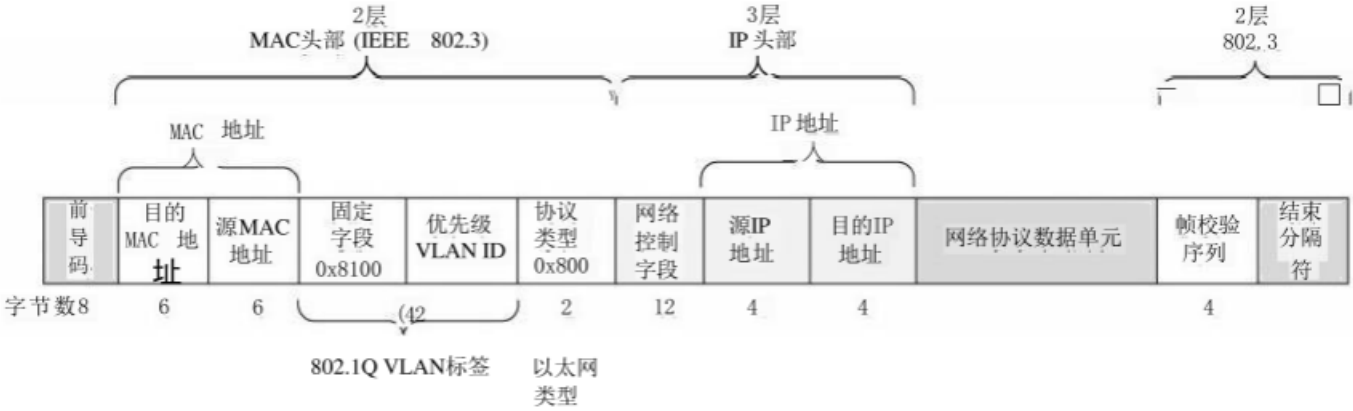


图 2 以太网帧 IP 报文头部

注：GOOSE 和 SMV 帧不携带变电站内的网络报头，但通常带有 IEEE802.1Q 标签。

4.1.3 IPv4 头部

IPv4 报文头部包含两个32位 IP 地址和一个协议类型，协议类型标识网络协议数据单元(NPDU)的有效载荷类型，以太网帧 IPv4 数据包格式见图3。

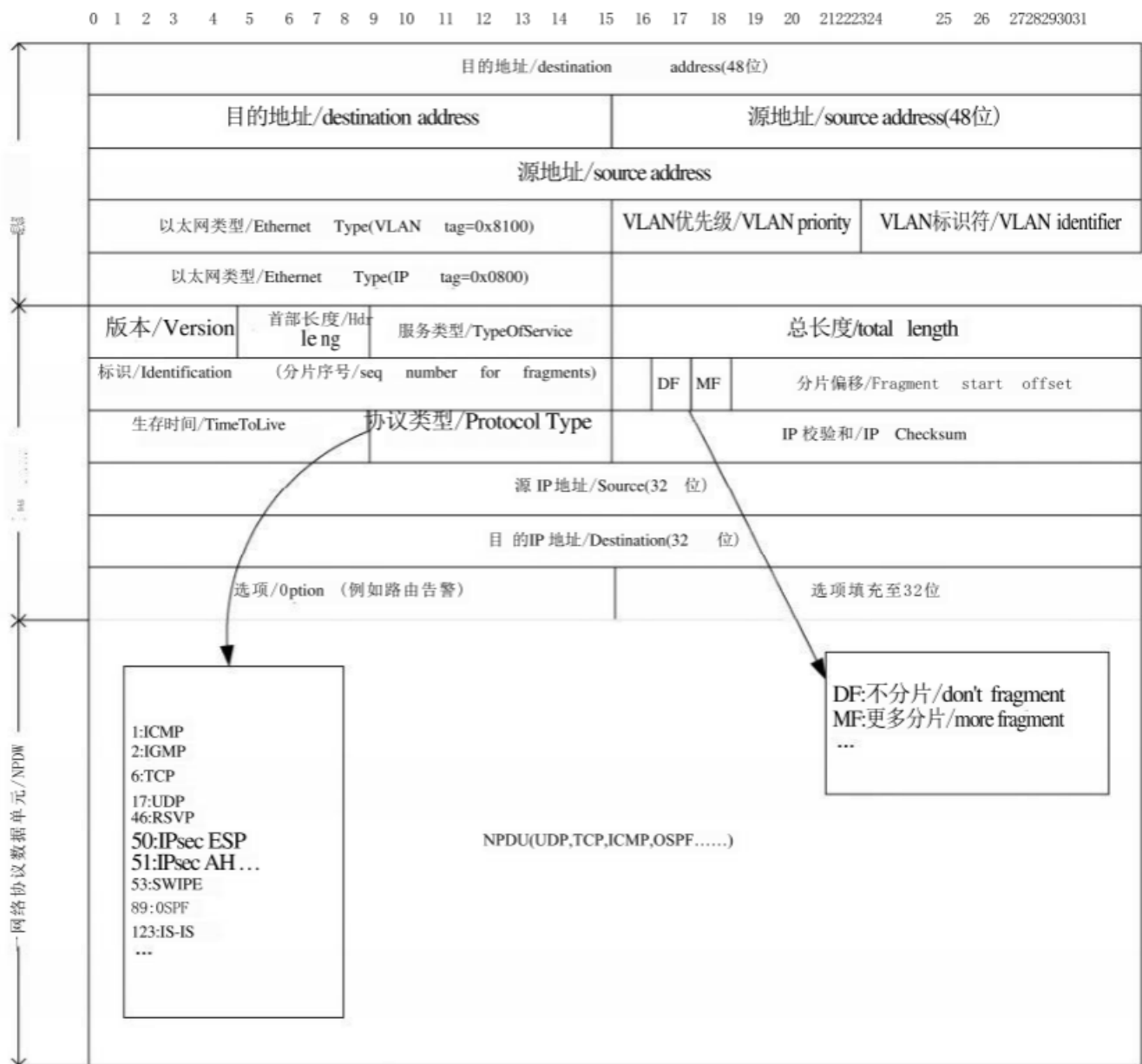


图 3 以太网帧 IPv4 数据包格式

4.1.4 IPv4 地址

IPv4 地址的长度为32位。它们的可读表示形式是由四个十进制数字组成的序列，由点分隔，每个数字代表一个八位字节。

示例1: “10.12.127.4”转换为“00001010000011000111111100000100”b。

IP 地址分为公网地址和私网地址。公网地址全球唯一，由互联网分配号码管理局(IANA) 通过区域互联网注册处(RIR) 管理；私网地址可重复使用，例如在不同的公司、工业工厂或互联网服务提供商的域中可相同。RFC 1918 制定了IPv4 地址分配的指导原则。

公网 IPv4 地址已用尽(见4.1.1)，但不影响基于私网地址或独立于公网的网络的使用。

私网地址子网边界处的路由器可按照网络地址转换(NAT) 的标准(RFC 2663/RFC 3022)将内网地址转换为公网地址，反之亦然。NAT 允许同时通过 UDP 和 TCP 通信中的端口号复用 IP 地址。NAT 通过私网地址复用和公网地址转换，延长IPv4 的生命周期。

IPv4 地址被构造造成不同大小的子网，如无类域间路由(CIDR)(RFC 4632)定义的子网。

示例2:地址10.12.127.0/24表示共享前24个相同位的所有节点属于同一个子网。

子网划分通过地址绑定构建网络并提高路由效率。

RFC 5771规定了IPv4 组播地址的分配规则。

4.1.5 IPv4 分片和报文大小

最大传输单元(MTU) 是指在没有分片的情况下, 某个节点或路由器所传输的 IP 数据包的最大字节数。

如果下一跳链路的MTU 值太小而导致报文无法转发, 则 IPv4 节点会将报文分片成长度较小的数据包, 对端节点再对分片报文进行重组。

因此, IP 报文头部包含一个16位的序列号(称为“标识”)和“分片起始偏移量”(指示原始消息中分片开始的位置)。分片位(MF) 表明这个 NPDU 不是最后一个分片。不分片位(DF) 指示下一跳路由器不应对这个 NPDU 进行分片。

在端到端节点之间的路径中, 如没有设置 DF 位, 任何IPv4 主机都可能对报文进行分片。如主机无法转发不分片的 NPDU, 将通过 ICMP 返回一个报错消息, 发送端主机应减小其 MTU 值, 直到其他主机接收它为止。IPv4 主机之间协商的 MTU 值应不小于68字节。

所有主机接收 IPv4 数据包的缓冲区空间最小是576 字节。

以太网上的 IP 数据包的 MTU 值通常为1500字节。

RFC 6864 和 RFC 4459 提供了更多详细信息。

4.1.6 IPv4 辅助协议

辅助协议允许管理 IP 网络。对于终端设备, 相关的辅助协议包括以下内容。

- a) 地址解析协议(ARP)(RFC0826) 允许主机根据IPv4 地址获取2层MAC 地址。因此, 主机广播一条2层消息“谁的 IP 地址是 X”。拥有该 IP 地址的主机使用 MAC 地址进行响应。如果发送方没有收到任何响应, 则表明它呼叫的主机和它不在同一个局域网内, 该消息会被发送到网关, 以便进一步转发。ARP 工作在第2层。
- b) 互联网控制消息协议(ICMP)(RFC 0792)允许主机询问远程主机是否存在以及响应时间。ICMP 的一个常用功能是“响应”, 其最为常见的命令是“Ping”。ICMP 还有两个功能: 报告错误和统计。ICMP 工作在第3层。
- c) 动态主机配置协议(DHCP) 向连接设备动态分配 IP 地址。因此, 当主机向DHCP 服务器请求 IP 地址时, 会收到一个有租约时间的 IP 地址。这使得客户端设备接入更便捷, 并且允许重用私网地址。服务端也可配置静态 IP 地址, 而不使用 DHCP。DHCP 版本 4(DHCPv4)(RFC 2131)在传输层使用UDP 协议, 端口号是67和68。
- d) 域名服务(DNS) 允许主机通过提交统一资源定位符(URL) 查询远程主机的 IP 地址。DNS 以包含 IPv4 地址的“A-record”作为响应, 避免在应用程序中使用硬编码 IP 地址, 并提供冗余空间。DNS 在传输层使用TCP 或 UDP 协议, 端口号是53。

4.1.7 IPv4 路由

路由器执行IP 协议中最复杂的部分。路由器之间通过交换控制消息建立路由表, 以确定数据包转发路径。

IETF 对许多路由算法进行了标准化。内部网关协议(IGP) 管理自治系统(AS) 内(如公司内部)的路由, 包括开放最短路径优先协议(OSPF)(RFC 2328)或中间系统到中间系统协议(IS-IS)(RFC 1142)。

互联网路由器连接不同的自治系统，通过使用边界网关协议(BGP)(RFC4271) 交换路由信息。

在两台设备之间，IP 协议无法确保双向转发路径是相同的(路径一致性)。

路由协议决定了网络的恢复时间。链路中断会导致长时间的重新配置，所需恢复时间为几秒甚至几分钟。IP 快速重路由和双向转发检测(BFD) 机制可加快链路恢复。

4.2 IPv6

4.2.1 IPv6 意义

由于IPv4 公网地址短缺(在2011年时已基本用尽), IETF 制 定 了IPv6 协议标准(RFC 2460), IPv6 地址有128位。 IPv6 在 IPv4 基础上进行了一些改进, 如增强了安全性和路由功能, 其中部分改进已经被移植到 IPv4。

IPv4 地址的短缺不会立即对公网造成影响, 因为有大量的私网地址都还在使用IPv4。并且在很长一段时间内, 许多工具和硬件仍会支持IPv4。

IETF 将不再支持 IPv4, 网络供应商也可能不再支持 IPv4。因此建议用户尽快开展 IPv4 到 IPv6 的迁移工作。

4.2.2 以太网中的 IPv6 报文

RFC 2464 定义了以太网帧的IPv6 数据包格式见图4。

以太网类型 “0x86dd” 标识IPv6。

IPv6 报文头部的固定长度为40字节, 唯一从 IPv4 中保留的字段是版本号, 并允许扩展头部(包括路由、安全性、隧道等参数)。

IPv4 和 IPv6 并不兼容, 可通过第2层的以太网类型和第3层的版本号来区分。

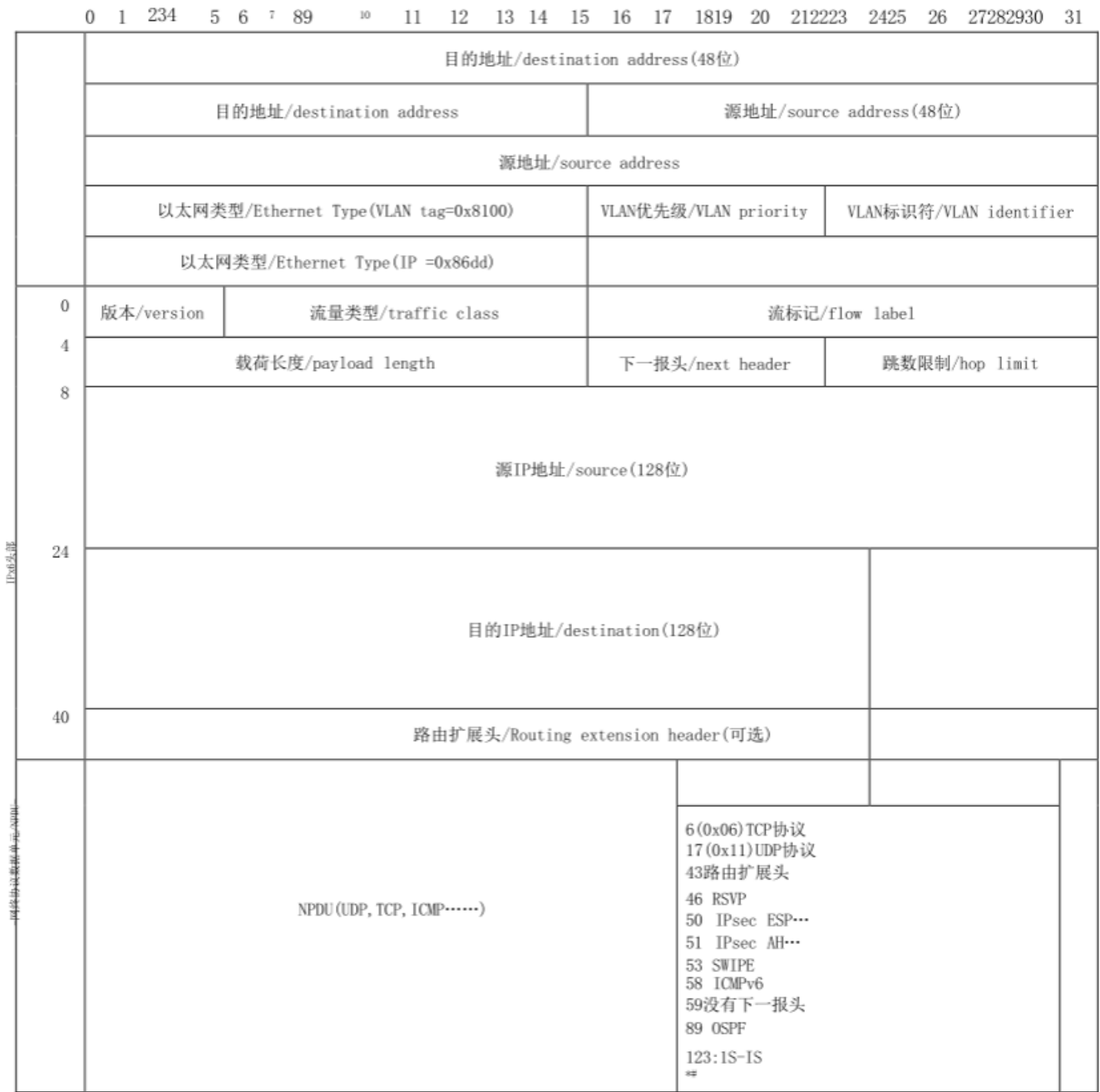


图 4 以太网帧 IPv6 数据包格式

4.2.3 IPv6 地址

4.2.3.1 IPv6 地址表示

RFC4291 定义了IPv6 地址表示方式。区别于IPv4 的“点分十进制”，IPv6 将128 位地址分为八组，每组是由四个十六进制(小写)的数字组成，每组用冒号分隔。

示例1:2001:0db8:85a3:0000:0000:8a2e:0370:7334 可表示为:
00100000000000001000011011011100010000101101000110000 000000000000
0000000000000000100010100010111000000011011100000111001100110100

此外，双冒号表示不定长的连续字符串“0”，但它最多只能出现在地址中的一个位置。

示例2:上面的地址可以表示为2001:0db8:85a3::8a2e:0370:7334

为了方便内嵌 IPv4, IPv4 地址可在IPv6 地址中出现一次，采用“点分十进制”，用点号“.” 分隔。

示例3: 192.0.2.1->64: ff9b::192.0.2.1

注: RFC5952 可能会造成地址解析问题,因为它要求 IPv6 地址中使用小写十六进制字符,这与 RFC4291 相矛盾。

4.2.3.2 IPv6 全局单播地址格式

RFC4291 规定了单播地址的格式。IPv6 的单播和广播地址包括三个字段: n 位路由、m 位子网 ID 字段和64位接口标识字段, IPv6 单播地址结构见图5。



图 5 IPv6 单播地址结构

64位接口ID 获取途径包括:

- a) 从接口的 IEEE 802.3 MAC地址衍生出来,使用EUI-64 格式;
- b) 从 DHCPv6 服务器获得(是否使用固定前缀);
- c) 自动随机配置;
- d) 手动分配。

注: 关于 EUI-64 的使用, 参见参考文献[22]。

全局单播地址由IANA 通过多个 RIR 管理。

4.2.3.3 IPv6 子网

IPv6 使用“IPv6 地址/前缀长度”的方式代替子网掩码。RFC5942 解释了 IPv4 子网掩码和 IPv6 前缀的区别。

例如: fc00::/7 表示前7位为 “1111110” 的所有地址。

4.2.3.4 IPv6 唯一本地单播地址(ULA)

RFC4193 定义了固定前缀为“fc00::/7” 的两类 ULA 地址, 由“L- 标志” (本地标志)位进行区分, fc00::/8(“L- 标志” 位设置为 ‘0’), 或者 fd00::/8(“L- 标志” 位设置为 ‘1’)。IPv6 ULA 地址结构见图 6。



图 6 IPv6 ULA 地址结构

如果前缀是本地分配的, 则将“L 标志” 设置为1(符合最通用的规则)。

ULA 地址应在私网中路由。

4.2.3.5 IPv6 本地地址

RFC4291 定义了IPv6 链路本地地址的前缀为fe80::/10,IPv6 链路本地地址结构见图7。



图7 IPv6 链路本地地址结构

链路本地地址用于单一的链路，不支持路由。

4.2.4 IPv6 辅助协议

IPv6 附带了一套辅助协议，主要包括如下内容。

- 控制消息协议版本6(ICMPv6)(RFC4443) 取代了ICMPv4 协议，是 IPv6 的强制性组件。ICMPv6 与 UDP、TCP都工作在传输层上。
- IPv6 邻居发现协议(NDPv6)(RFC 4861)提供无状态地址自动配置(SLAAC) 功能，取代了 IPv4 的 ARP 协议和 ICMPv4 协议，是ICMPv6 协议的一部分。
- DHCPv6(RFC3315) 和 DHCPv6lite(RFC 3736) 是 DHCP 的扩展协议。
- 网络层安全协议(IPsec)(RFC2401) 使用认证头部(AH)(RFC4302) 和封装安全载荷(ESP)(RFC4303)。 此协议套件部分适用于IPv4 协议。IPv6 协议中必须支持 IPsec, 但不强制使用 IPsec。
- 许多路由协议无需进行技术调整，只需改变交换信息格式即可适用于IPv6,OSPF 和 IS-IS 路由协议都在广泛使用。
- 6LoWPAN(RFC4919) 为低功耗和有损网络提供了IPv6 支持，主要包括：
 - RFC6550 提供了6LoWPAN(RPL) 的路由协议；
 - RFC4944 指定了分片；
 - RFC6282 废弃了RFC4944 中指定的报头压缩机制；
 - RFC6775 提供了对6LoWPAN 网络 NDP的适配。

4.2.5 IPv6 分片和报文大小

IPv6允许逐跳之间传输超大报文(RFC 2147),其 MTU 值远大于以太网帧的大小，但 IEC TR 61850-90-5 不支持超大报文。

所有 IPv6 主机支持接收的最小报文帧为1280 字节。

IPv6 只允许在主机(包括隧道端点)上分片，而 IPv4 支持在中间路由器上(RFC4944) 进行分片。

IPv6 协议要求主机支持路径 MTU 发现(RFC 1981),即监测端到端路径中所有网络节点的 MTU 值。

IPv6 终端主机的 MTU 值应不小于1280字节。

4.2.6 IPv6 路由

IPv6 和 IPv4 使用相同的路由协议，例如，OSPF 或 IS-IS 协议。

4.3 IPv4 和 IPv6 比较

4.3.1 主要区别

IPv4 和 IPv6 之间的主要区别见表1。

表 1 IPv4 和 IPv6 之间的差异

属性	IPv4	IPv6
地址位数	32位	128位
地址解析	ARP	NDP
报文头部长度的	可变大小，包含传输协议类型	固定大小
可选报文头部	无	可选扩展头部包含传输协议类型
报文头部压缩	无	允许
IP报文头部校验和	有	无
分片	通过路由器实现	只允许通过主机或主机模式的网络节点实现
安全支持 (IPsec)	IPsec可选	强制支持IPsec, 但不强制使用
路由协议	支持OSPF、IS-IS等，不支持RPL	支持OSPFv3、RPL和其他适用于IPv6的路由协议
ICMP	ICMPv4	ICMPv6 (强制)

4.3.2 IPv4 和 IPv6 地址分类

IPv4 和 IPv6 具有各自固定长度的地址。两者不同长度地址的转换是 IPv4 向 IPv6 迁移过程中最难处理的问题。IPv6 和 IPv4 地址对比见表2。

注：NAT通过端口和地址映射扩展IPv4地址，但这只适用于TCP和UDP协议(这几乎涵盖了所有的网络流量)。

表 2 IPv6 和 IPv4 地址的对比(RFC 4291)

地址类型	IPv4	IPv6 (RFC 4291)
未定义	0. 0. 0. 0	::
环回地址	127. 0. 0. 0/8	0::1
组播地址	224. 0. 0. 0/4	ff00::/8
链路本地地址 —— 仅在一个链路上有效； —— 不支持路由； —— 只在本地链路传输	169. 254. 0. 0/16	fe80::/10 (自动配置)
私网地址 —— 不支持路由到私网地址空间以外	10. 0. 0. 0/8 (24位块) 172. 16. 0. 0/12 (20位块) 192. 168. 0. 0/16 (16位块)	fc00::/7 fd00::/8伪随机 fc00::/8 用户指定 (ULA) (RFC4193)
全局地址 —— 向RIR注册的公共可路由地址	其他所有	2000/3
广播地址	255. 255. 255. 255	ff02::1 (不推荐)

4.3.3 IEC 61850 地址表示

系统配置语言(SCL)(IEC 61850-6)中, 配置 IPv6 网络参数部分如以下 xml 所示:

```
Address
P type="IP"2001:0db8:85a3:0000:0000:8a2e:0370:7334 /P
P type="IP-SUBNET"/56/P
P type="IP-GATEWAY"2001:0db8:85a3:0000:0000:8a2e:0370:0001/P
P type="OSI-AP-Title"1,1,999,1,1/P
P type="OSI-AE-Qualifier" 12/P
P type="OSI-PSEL"00000001/P
P type="OSI-SSEL"0001/P
P type="OSI-TSEL"0001/P
/Address
```

注: IPv6地址使用小写十六进制字符表示, 但先前也使用过大写字母表示, 因此解析器同时支持大小写。
设备可能同时配置IPv4 和 IPv6 地址(并且可能配置多个地址), 如下例所示:

```
Address
P type="IP"xsi:type="tP_IP"2001:0db8:85a3:0000:0000:8a2e:0370:7334 /P
P type="IP-SUBNET"xsi:type="tP_IP-SUBNET"/56/P
P type="IP-GATEWAY"xsi:type="tP_IP-
GATEWAY" 2001:0db8:85a3:0000:0000:8a2e:0370:0001 /P
P type="IP"xsi:type="tP_IP"10.0.0.11 /P
P type="IP-SUBNET"xsi:type="tP_IP-SUBNET"255.255.255.0 /P
P type="IP-GATEWAY"xsi:type="tP_IP-GATEWAY"10.0.0.101/P
P type="OSI-AP-Title"xsi:type="tP_OSI-AP-Title"1,1,999,1,1/P
P type="OSI-AE-Qualifier"xsi:type="tP_OSI-AE-Qualifier" 12 /P
P type="OSI-PSEL"xsi:type="tP_OSI-PSEL"00000001/P
P type="OSI-SSEL"xsi:type="tP_OSI-SSEL"0001/P
P type="OSI-TSEL"xsi:type="tP_OSI-TSEL" 0001 /P
/Address
```

5 IPv4 到 IPv6 的过渡

5.1 IPv6 迁移的必要性

随着32位IPv4 地址的耗尽, 公共互联网正在向128位的IPv6 过渡。IPv6 可提供的地址空间几乎是无限的。

IPv6 已进入快速发展阶段, 大多数新型设备均支持 IPv6, 但是大量服务器仍在使用IPv4。

公共互联网 IPv6 的流量预测趋势见图8。预计到2030年, 存在少量仅支持IPv4 的网络节点, 这些节点大部分位于私有网络中。

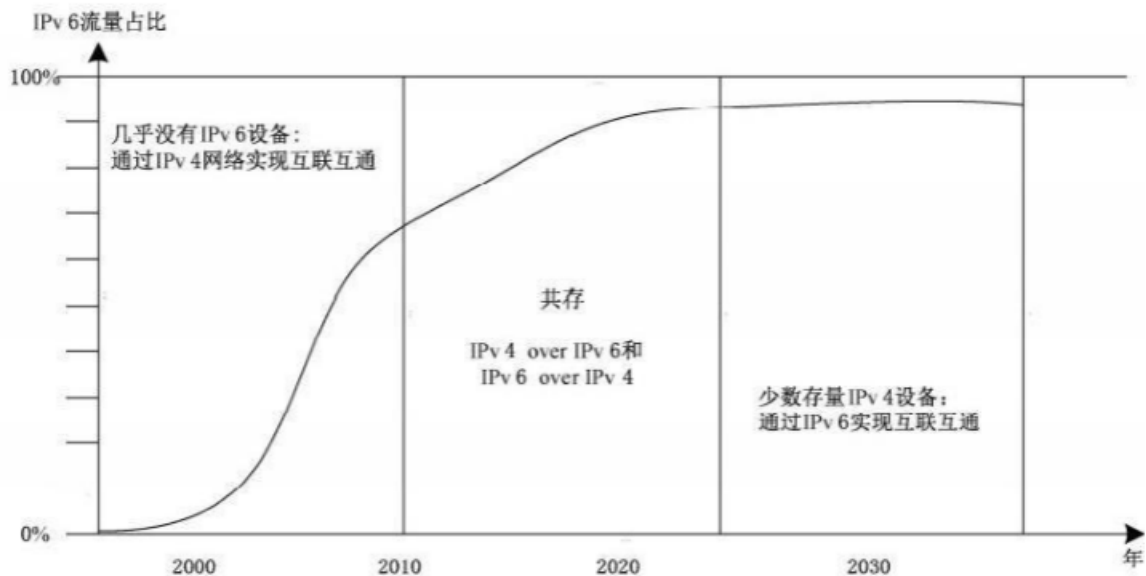


图 8 IPv6 流量趋势图

5.2 迁移类型

IETF 建议两种不同的迁移策略(RFC 4213)。

- a) 应用程序迁移：当前基于 IPv4 编写的应用程序被迁移到 IPv6 的同时，应尽可能保留与 IPv4 设备的兼容性，例如工程工具、调试及流量监控工具和遥控应用程序。在维护应用程序时需要升级软硬件。
- b) 设备和系统迁移：
 - 1) 新的IPv6 设备应能在 IPv4 体系结构上运行；
 - 2) 现存 IPv4 设备，例如路由器，应能与 IPv6 设备兼容；
 - 3) 现存 IPv6 设备不应干扰已有 IPv4 设备的正常运行；
 - 4) 新设备应同时支持访问IPv4 和 IPv6 设备(双栈)；
 - 5) 仅支持IPv4 的设备应能与仅支持 IPv6 的网络互联(通过隧道或转换技术)。

5.3 IPv6 迁移对电力系统通信的影响

对于电力系统通信，迁移至IPv6 网络的紧迫性取决于以下应用场景。

- a) 如 IFC TR 61850-90-4 所述，变电站内只使用 IPv4 私网地址，因此尚未出现地址不足的问题。
- b) 变电站的站间通信和变电站到控制中心的通信承载在电力专网上，因此只使用 IPv4 私网地址，也可能使用非 IP 化的其他通信方式。
- c) 通常使用虚拟专用网络(VPN) 对变电站设备进行维护访问，该网络只使用私网地址，只需少量公网地址就可接入 VPN 边缘设备。
- d) 控制中心需获取市场和气象信息，这些信息越来越多地仅承载在 IPv6 网络上。
- e) 分布式能源网络受配电系统运营商(DSO) 控制，可重复使用私网 IP 地址。
- f) 需要更大地址空间和基于IPv6 网络的其他服务，例如智能表计、分布式发电、需求侧管理、电动汽车等，已使用 IPv6 网络。
- g) 部分传感设备采用6LoWPAN 等通信技术，只能在 IPv6 网络上运行。

尽管电力系统通信对 IPv6 网络的依赖性不强，但网络迁移需提前准备，原因如下：

- a) IPv4 将随着技术发展而逐步淘汰，到2025年—2035年前后，IPv4 网络和设施的运行维护将

会成为电力公司的负担;

- b) IETF 所有新研究将基于IPv6 而非IPv4;
- c) 操作系统和路由器制造商可能会逐步提高 IPv4 设备的价格, 或者在指定日期停止IPv4 的技术支持;
- d) 维护双栈设备尤其是当IPv4 设备数量较少时, 成本代价过高;
- e) 由于未来缺乏 IPv4 网络知识的相关培训, IPv4 协议将被视为潜在的不安全因素;
- f) 智能电网将同时支持 IPv4 和 IPv6, 需在两种协议的边界处建立隧道或进行协议转换;
- g) 政府法规要求使用IPv6, 例如 USGv6、OMB、NIST、NERC 等。

因此, 亟需制定网络迁移策略, 以减轻未来的迁移压力。

在 IEC61850 标准体系下, 基于 IPv4 通信的网络节点仍会不断增加, 因此网络迁移策略首先需要充分考虑现存和持续增加的IPv4 节点。

同时 IPv6 迁移也为解决其他问题提供了新途径。

从 IPv4 网络迁移至IPv6 网络并非易事, 需要仔细规划。

6 迁移方法

6.1 迁移原则

大量现存IPv4 设备需逐步与 IPv6 设备通信, 面临的首个问题是两者 IP 地址长度不同, 其次是如何实现从 IPv4 到 IPv6 的地址映射。

RFC6144 定义了十几种 IPv6 过渡机制。这些过渡机制旨在将 IPv6 协议引入到现存的 IPv4 网络, 但是随着IPv6 被广泛引入, IPv4 将不会被继续使用。

RFC 4213 定义了三种基本的过渡策略:

- a) 双栈设备;
- b) 隧道技术;
- c) 转换技术。

6.2 地址映射

6.2.1 IPv4 映射到 IPv6

IPv4 和 IPv6 均未考虑到地址空间的可扩展性, 因此如何处理两者不同长度的地址是IPv4 迁移到 IPv6 的一个难题。

RFC 6052定义了从IPv4 到 IPv6 的几种映射方式, 如图9所示。但是SIT(RFC 6145)建议使用“::ffff:0:0/96” 地址格式, 具体见图9中的底部地址。

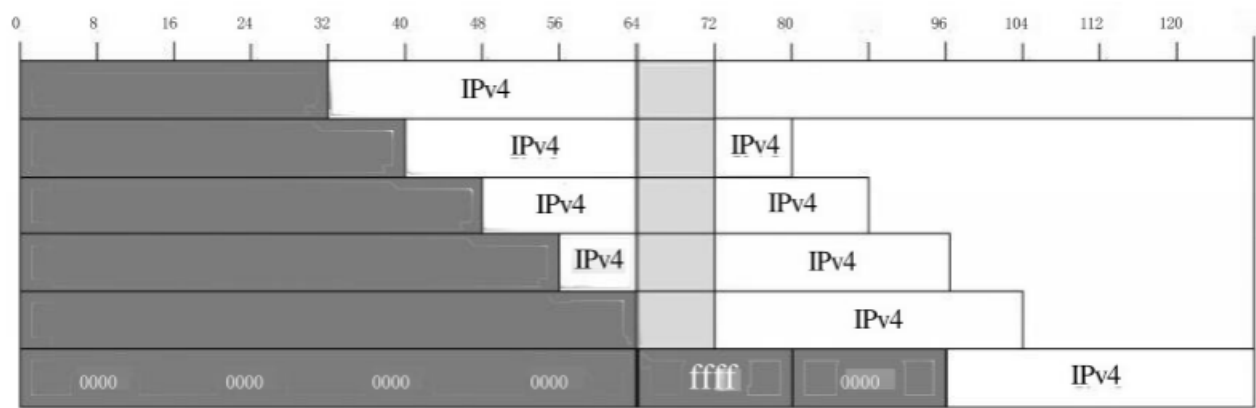


图 9 IPv4 到 IPv6 的地址映射

UDP 和 TCP 等协议的校验和包含了 IP 地址，地址改变将导致 UDP 与 TCP 校验和的重新计算，这是 IPv4-IPv6 协议转换面临的问题。为了便于从 IPv4 迁移到 IPv6,RFC 6052 提出了一种“校验和中和”转换方式，其结构前 96 位是“64:ff9b::”，后 32 位是 IPv4 地址。

示例:

64:ff9b::/96|172.16.2.33|

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0000' 0000' 0110' 0100' 1111' 1111' 1001' 1101' 0000' 0000' 0000' 0000' 0000' 0000' 0000' 0000'
0000' 0000' 0000' 0000' 0000' 0000' 0000' 0000' 1010' 1100' 0001' 0000' 0000' 0010' 0010' 0001

在协议转换时，利用校验和中和地址可避免重新计算校验和。IPv6 地址不包括原有 IPv4 地址时，则校验和中和地址失效。

“校验和中和”转换方式限制了 IPv6 地址具有固定的 96 位前缀(即只能有效使用后 32 位地址)，这违背了 IPv6 的设计初衷。

从 IPv4 地址到 IPv6 地址映射，也可使用地址静态配置的转换方式。

除此之外，每次转换需通过 DNS (或从数据库静态配置)解析全局域名(如 URL) 获取通信对端的 IP 地址。IPv6 中的 DNS 使用包含 128 位 IPv6 地址的 AAAA 记录响应 DNS 请求。

6.2.2 IPv6 地址对应用程序的普遍影响

基于 IPv4 运行的应用程序在逐步迁移至 IPv6 的过程中，应尽量减少改动。应用程序迁移应不受 IP 地址影响，但考虑到 IPv6 更长的地址长度，存在少量迁移过程受 IP 地址影响的情况，例如：

- a) 显示 IP 地址和子网掩码的长度；
- b) 程序中 IP 地址的表示方式：32 位的 IPv4 扩展至 128 位的 IPv6；
- c) 地址表和内存空间的需求；
- d) 使用硬编码地址(如 127.0.0.1, “localhost”);
- e) 处理从域名服务器接收的 AAAA 记录(IPv6 地址)；
- f) 网络服务调用函数(如 getnameinfo/getaddrinfo)。

RFC 4038 对如何检测现有代码中的潜在问题提出了建议。

6.2.3 IEC 61850 的地址迁移

6.2.3.1 总则

在 IEC61850 中，受迁移影响的不仅是 IED 设备，还包括其他应用，如 SCADA、工程工具、调试工

具、网络监视器等。

6.2.3.2 IEC 61850-8 和 IEC TR 61850-90-4 的 IPv6 映射建议

当前变电站都使用以下组别的 IPv4 私网地址：

- 10.xx.xx.xx/8,
- 172.32.xx.xx/11,
- 192.168.xx.xx/16

为了在 IPv6 公网上保持不可路由性，上述地址应被映射到 IPv6 的 ULA 地址：“fd00::/8” 或 “fc00/8”（基于TCP/UDP 伪头部保留校验和）。

IPv6 地址的应用影响了工程网络，它使网络分区变得更加灵活，利用地址前缀取代子网掩码。

注：在变电站自动化系统，根据 IEC TR61850-90-4定义的现场物理拓扑分配IPv4静态地址。只要使用合适的地址前缀，这种静态分配方式同样适用于IPv6。

设备启用IPv6 协议后，不再使用NAT 功能。

应用程序可为运行网络按地理位置划分私网地址空间(ULAs)， 例如：

<operational><region><substation><voltage level><bay><IED>

IPv6 地址规划与地址的网络部分(高64位)相关。主机部分为64位，没有定义地址规划。

网络地址部分中最低有效部分的位数可与IEC TR61850-90-4 中 IPv4 地址的位数相同，可根据区域和变电站的数量对最高有效位数进行灵活分配。

可参考以下模型：

- a) 用于虚拟电厂： <operational><region><wind park><turbine><IED>;
- b) 用于智能电网： <operational><region><sector><block><house><IED>。

管理信息大区(承载电子邮件、文件传输等业务)与生产控制大区(承载保护、远动、SCADA 等业务)的网络规划相互独立。

6.2.3.3 电力系统中其他协议的地址

IEC 61400-25 和 IEC 60870-5-104都没有定义地址分配方案。

注：其他协议尚未调查。

6.2.3.4 地址配置管理

部分应用程序在有效载荷中嵌入 IPv4 地址，这些 IP 地址参与校验和计算，这是 TCP 协议的一个问题。有效载荷中携带 IPv4 地址的多个 FTP 版本也存在同样的问题。

有效载荷中携带 IP 地址的应用协议都会受到影响，特别在 IEC 61850 中传输包含 IPv4 地址的 SCL 文件时，对端无法解析。

6.2.3.5 地址迁移评估

IPv4 地址迁移的评估结果见表3。

表 3 IPv4 地址迁移评估

实施难度	繁琐，需要核查遗留源代码
影响范围	所有应用软件

表 3 IPv4 地址迁移评估 (续)

特殊的设备	无
IPv6优势	用路由器代替NAT功能，实现端到端连接
难点	需测试和扩展认证
建议	检查有依赖IP地址和需提取IP地址的应用程序； 制造商应开始考虑其产品对IPv6的支持； 为了保持向后兼容性，解析器应能识别IPv6地址中的大写字符，并转换为小写字符以供进一步使用

6.3 双栈设备

6.3.1 通则

双栈设备同时具有 IPv4 协议栈和 IPv6 协议栈，如图10所示，路由器是第一种使用双栈的设备，它们能根据所接收报文的IP 版本进行路由。

终端设备应由应用程序选择协议栈类型。

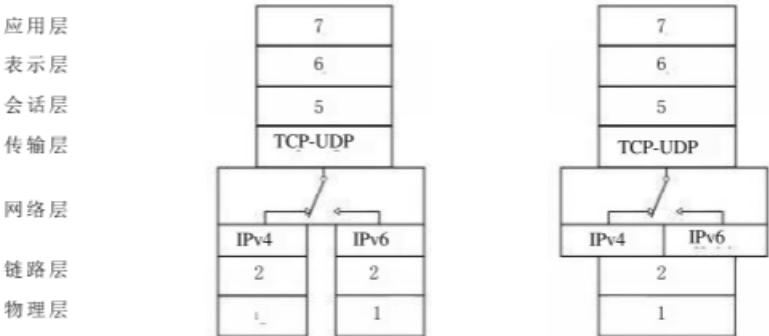


图10 两类端口的双栈设备

类双栈设备同时包含 IPv4 和 IPv6 地址集。网络层根据目的地址使用IPv4 或 IPv6 连接。在变电站内，双栈应用程序通过预先配置的地址(如IEC 61850-6 中所述的 SCD 文件的地址), 获取正确的 IP 地址和协议，混合域中的双栈设备通信连接见图11。

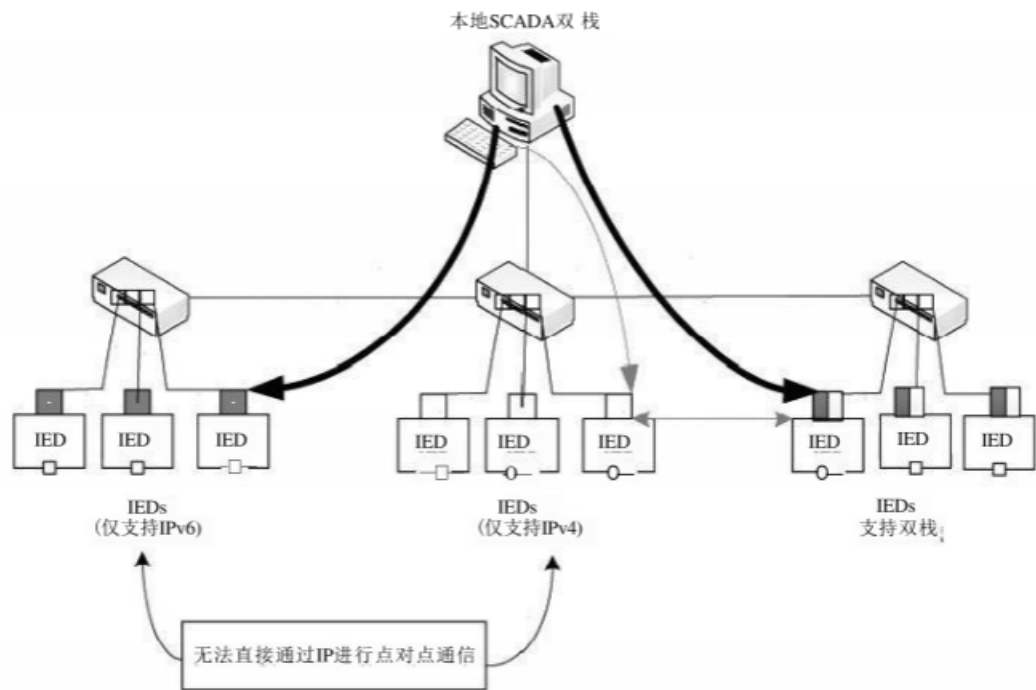


图 1 1 混合域中的双栈设备

WAN 中的双栈服务器可在 DNS 注册，因此客户端可选择正确的接口类型进行访问，跨路由器的双栈设备通信连接见图12。

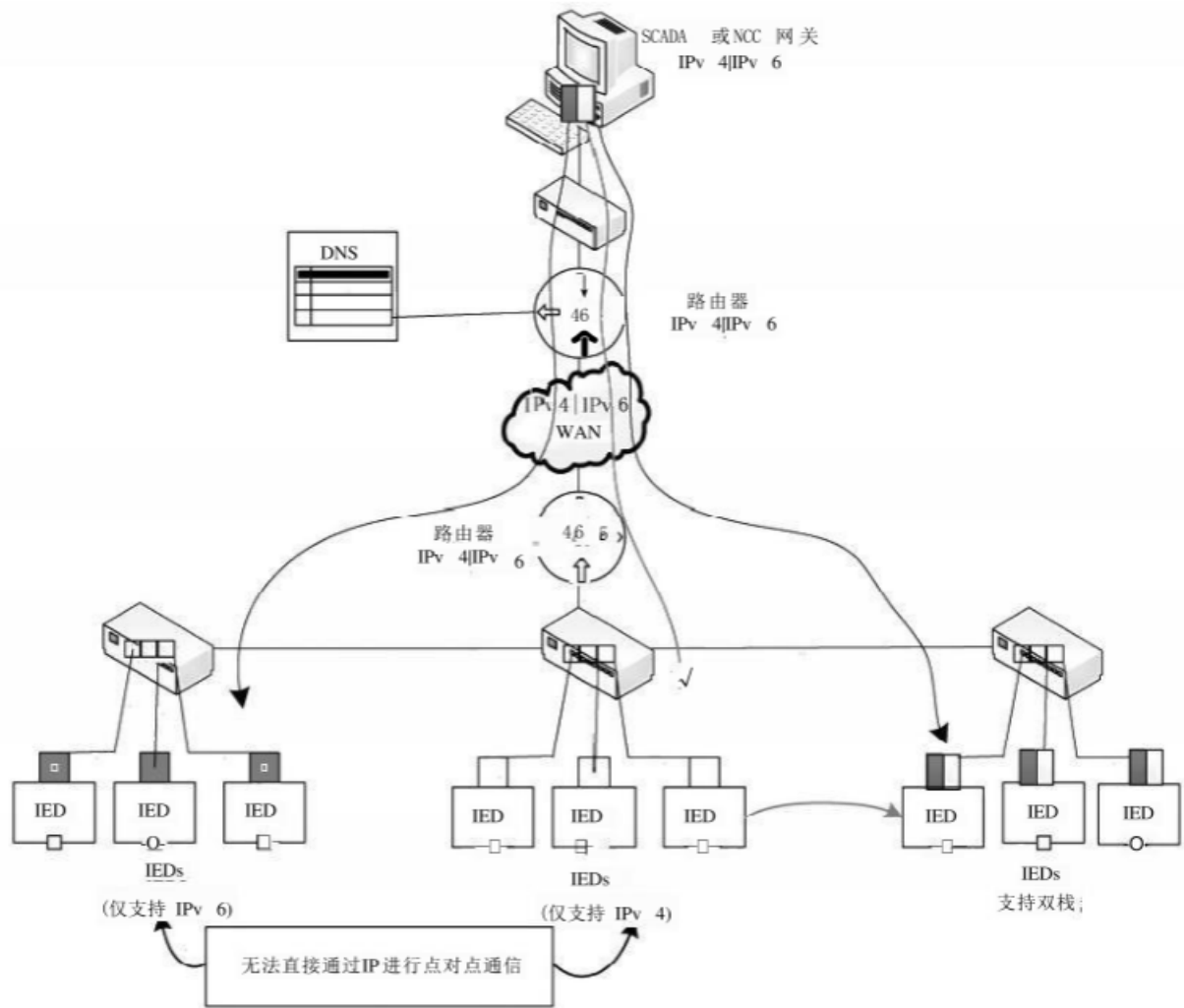


图 1 2 跨路由器的双栈设备

6.3.2 双栈规范

双栈主机同时支持IPv4 和 IPv6 协议，两种协议栈的比较见表4。

IETF 定义了两种双栈方法：双栈和轻型双栈。

“轻型双栈” (RFC 6333)机制可使 CPE(客户终端设备)利用可路由的全局 IPv6 地址传输数据包，CPE 将局域网中的私网 IPv4 地址封装到 IPv6 报文中，替代了NAT 转换功能。

DNS实现IP 地址自动获取：DNS 响应请求的 IP 地址，可能是 IPv4(A 记录)或者 IPv6(AAAA 记录)。双栈设备在会话期间使用相对应的协议栈，这种方法适用于个人电脑或智能手机等客户端，但不推荐使用。

表 4 两种协议栈的比较

方法	原则	结论
双栈	IPv4和IPv6并行使用	所有接口同时支持IPv4和IPv6, 这两种协议栈相互独立
轻型双栈	类似于双栈，但具有全局IPv6地址和运营商NAT私网IPv4地址	所有新设备都应具备的功能，此方法的前提是设备之间的整个路径都支持双栈

RFC4554 与参考文献L3]建议使用VLAN(虚拟局域网)标签来隔离IPv4 和IPv6 设备(此外，使用以太网类型也可区分 IPv4 和 IPv6)。正如 IEC TR 61850-90-4 所建议的，VLAN 使用了流量绑定技术，并减少了部分网络流量。

6.3.3 基于IPv4 和 IPv6 的 IEC 61850 协议栈

IPv4 和 IPv6 地址在 IEC61850 协议栈中的位置见图13。原则上，IPv4 或 IPv6 之上的协议，特别是硬实时协议(如 GOOSE、SMV、PTP),无需关注所使用的通信协议栈以及IP 层以下的协议(如链路层的 PRP 和 HSR)。

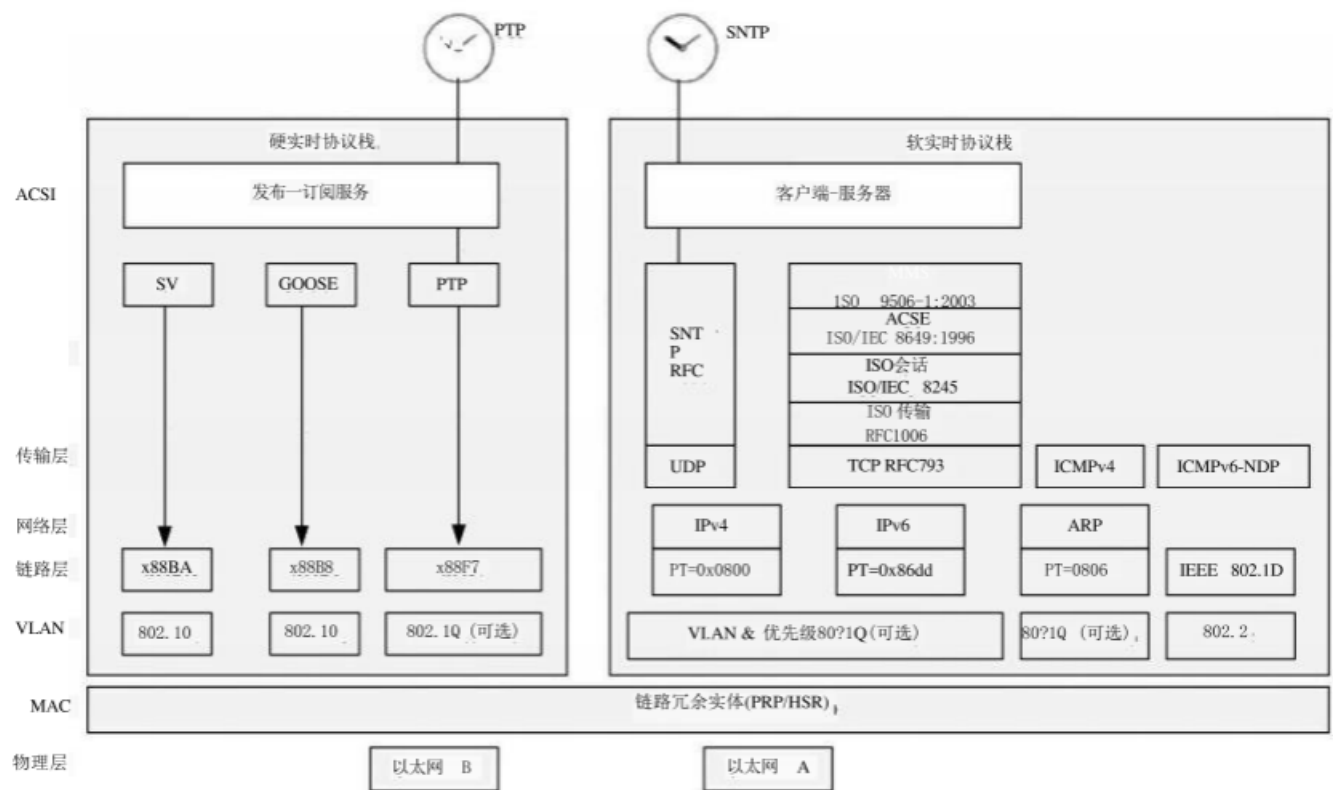


图13 IEC 61850 协议栈中的 IPv4 和 IPv6

6.3.4 BIH 双栈应用迁移

BIH(主机翻译, RFC 6535)方法允许迁移基于 IPv4 的应用程序。BIH 在 API (应用程序编程接口)或 socket (套接字)层拦截 IPv4 函数调用, 将它们指向到 IPv6 套接字(使用 IPv6 地址池中的地址), 与IPv6 主机通信。BIH 迁移方法见图14。



图14 BIH 迁移方法

BIH 替代了以前的方法, 例如“协议栈翻译”(RFC 2767)和“API 翻译”(RFC 3338)。但是, 使用该方法的应用程序仅限于:

- a) 需通过 DNS 进行地址解析;
- b) 不知道通信对端IP 地址;
- c) 可实现“NAT 穿越”。

由于变电站网络不使用DNS 且站内节点没有嵌入式“NAT 穿越”设备, 此方法不适用于变电站。

此方法只适用于应用程序迁移，同时要求相应的网络节点重新部署应用程序。

6.3.5 双栈建议

双栈设备无法解决现存 IPv4 设备迁移至 IPv6 的问题。

双栈是实现现存 IPv4 设备与IPv6 共存的技术。

在新设备上更容易实现双栈，仅支持 IPv4 的老设备无法快速迁移至IPv6，尽管同样的硬件设备均支持两种协议。

大多数操作系统(Windows、Linux 等)均支持双栈，双栈应首先应用于网关和路由器。

对于新部署或已升级的设备，支持双栈意味着：

- a) 需重新设计应用程序，以消除对地址依赖的影响；
- b) 具有双栈配置能力(许多实时操作系统已支持),但由于内存空间的原因，可能无法支持双栈同时运行；
- c) 可根据对端通信设备的 IP 协议类型，进行协议栈自适应配置。

双栈设备(例如 SCADA 系统、新设备)可实现现存 IPv4 设备与新部署或已升级的设备、系统共存。

6.4 隧道技术

6.4.1 隧道原理

隧道是一种数据封装技术，它将一种协议封装至另一种协议的有效载荷中进行数据传输。隧道至少有两个隧道端点，分别在隧道的两端，但也存在到其他 IPv4 域的分支，隧道原理见图15。图中协议1是 IPv4, 协议 2 是 IPv6。

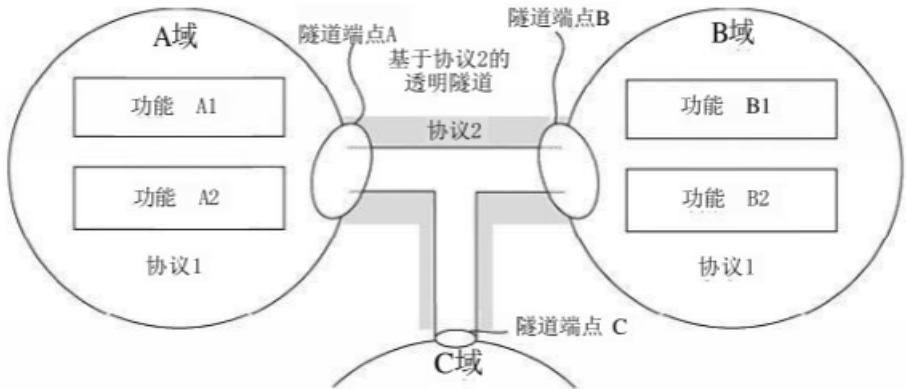


图15 隧道原理

只有隧道端点能感知协议2的特性，终端域无需关注，除非隧道端点要求限制报文帧的大小。

6.4.2 隧道协议规范

IETF 为 IPv6 规定了许多隧道协议。RFC 2473(IPv6 规范中的通用数据包隧道)总结了一些通用概念。

RFC 7059列出了以下 IETF 隧道机制：

- a) 隧道配置(隧道手工配置/6in4);
- b) 隧道自动配置;
- c) IPv6 over IPv4 不带显式隧道(6over4);
- d) 通用路由封装(GRE);

- e) 通过 IPv4 云连接 IPv6 域(6to4);
- f) 6to4 供应商管理隧道;
- g) 任何协议在其他协议中(AYIYA);
- h) 站内自动隧道寻址协议(ISATAP);
- i) UDP 上基于NAT 的 IPv6 隧道(Teredo);
- j) IPv6 快速部署(6rd);
- k) NAT44CPE 内的本地 IPv6(6a44);
- l) 定位编号分离协议(LISP);
- m) 子网封装和适配层(SEAL);
- n) 任何网络上的点对点IPv6 协议(6bed4)。

隧道协议的比较见表5和表6。

6.4.3 IPv4 over IPv6 隧道

6.4.3.1 隧道原理

IPv4 节点之间通过IPv6 网络进行通信。原则上 IPv6 网络对终端设备不可见，设备之间的路由基于 IPv4 网络，且路由器应能识别相关通信设备和域。隧道端点实现了数据的封装和解封装。

IPv4 over IPv6 隧道帧格式见图16,在数据封装过程中，IPv6 隧道不再保留IPv4 域的第2层头部。

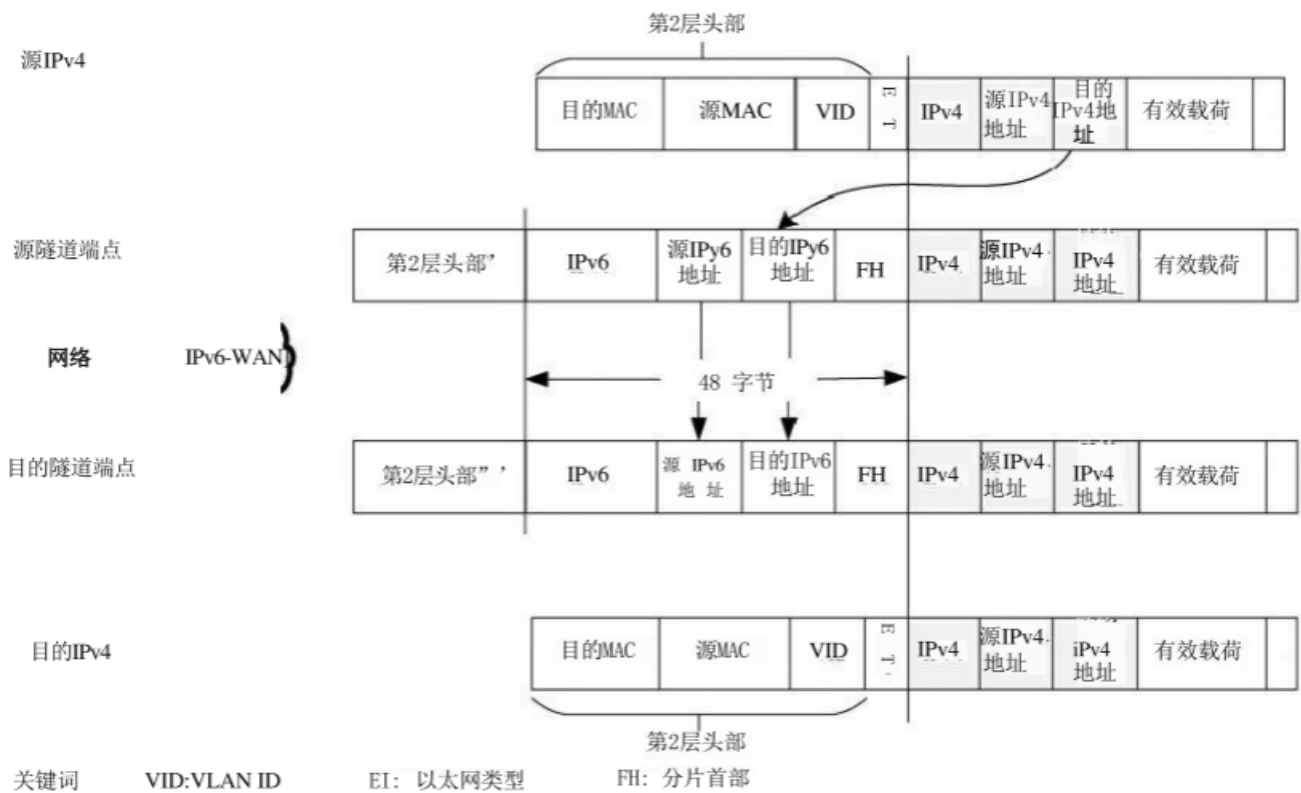


图16 IPv4 over IPv6 隧道帧格式

6.4.3.2 隧道传输和报文大小

如图16所示，IPv6 网络的帧大于IPv4 网络的帧。以太网规定的最大帧长度限制了IPv6 网络的帧大小，因此 IPv4 网络上的报文大小(包括 IPv4 报文头部)不能超过：

MTU 值 ≤ 1232 字节 (1280 字节减去 40 字节 IPv6 报文头部，再减去 8 字节分片报文头部)。

调整现存IPv4 设备的帧大小十分困难，且设备不一定支持 MTU 值减小。如果设备发送带有 DF 位的帧(见4.1.5)，则隧道不会转发，且返回错误消息给源端。

在IPv4 网络中，通常由路由器和非终端主机执行分片。如需分片，隧道端点在 IPv4 数据包封装进 IPv6 数据包之前对其进行分片，这会降低数据传输效率。

如IPv4 设备通过设置 DF 位来防止分片，则应满足以下任一条件：

- a) 数据包分片(由设备自身完成分片)；
- b) 协商MTU 值(这只是 IPv4 节点的可选功能)，且需手动调整源代码中的 MTU 值(可能涉及重新编译代码)。

不建议永久设置 DF 位 。RFC4459 和 RFC6864 阐述了如何处理分片。

6.4.3.3 基于 VLAN 的隧道端点

VLAN 是2层技术，2层隧道(例如 L2TP) 保留了VLAN 标签，但3层隧道不保留VLAN 标签。

如果隧道端点支持保留 VLAN 标签，可将VID 编码到隧道端点头部中，或者在隧道对侧通过配置重组。隧道两端的VID 可相同也可不同。

相对于将 VID 编码入 IPv6 有效载荷，将 VID 编码入源和目的 IPv6 地址更易实现(例如为远程变电站分配一组 IPv6 地址)，但该方法将限制工程化实施。

在图17中，隧道两端都保留了 VLAN 标签。边缘网桥之间的流量未打 VID 标签，目的边缘网桥处的 VID 由 PVID (基于端口的 VLAN ID)重新生成，但一个端口只能有一个 PVID。在更多情况下，源边缘网桥不会去除VID 标签，而是将它发送至源隧道端点，用于隧道选择。在目的侧，隧道端点将对 VID 重组或映射，这种方法可使多个VLAN 互连。

注：此方法也适用于基于VLL和VPLS的MPLS,在这种情况下，隧道和相应的 VID由内部 MPLS标签标识。

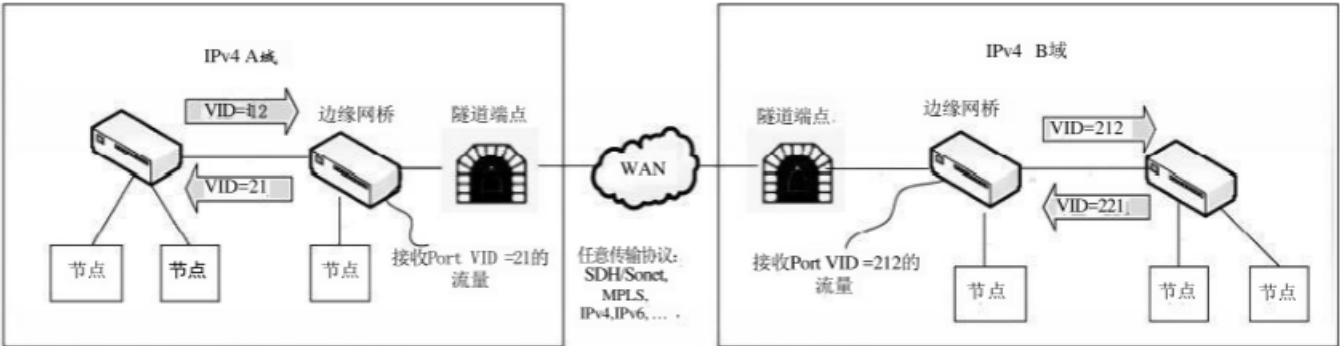


图 17 基于IPv4 over IPv6 和 VLAN 的隧道

6.4.3.4 隧道端点工作原理

隧道端点将传入的 IPv4 报文封装成 IPv6 报文。如有必要，隧道端点会调整 IPv6 链路上传输的报文大小，因为并非所有IPv4 设备都支持远程调整报文大小。

隧道端点可将每个内部 IP 地址(也称为私网地址)映射到外部IPv6 地址，从而确定对侧隧道端点。

隧道端点中的映射关系是系统管理配置的隧道表。同时隧道端点可作为 NAT 使用，将私网地址转换为公网地址。

6.4.3.5 标准的 IPv4 over IPv6 隧道协议

基于 IPv6 的隧道传输方法可实现两个 IPv4 孤岛之间的通信。该方法适用于外部网络是 IPv6 的场景，但在双栈网络中的作用有限。

IETF 定义了两 种 IPv4 over IPv6 隧道，如表5所示。
对于表6中的协议，终端设备无需感知隧道。

表5 IPv4 over IPv6 隧道

方法	运行模式	特性
4in6(RFC 2473)	IPv6中的通用分组隧道，第5章	IPv4 in IPv6隧道
4over6(RFC 7040)	公共的IPv4-over-IPv6接入网络	隧道使用全局IPv4地址进行传输，互联网服务提供商的过渡策略

6.4.3.6 自动隧道

自动隧道旨在避免静态地址配置。6in4(RFC4213) 定义了一种自动隧道机制，而6to4(RFC 3056) 中规定了一种更通用的机制，它为每个节点提供一个带有/48 IPv6 前缀的全局IPv4 地址，可满足所有应用程序的需要。

6.4.3.7 配置隧道

大多数机制未规定如何获取IPv6 或 IPv4 地址池。IEC TR61850-90-1规定在 SED 文件中配置隧道，SED 文件被加载到支持 IEC TR61850-90-1的路由器中。

6.4.4 标准的 IPv6 over IPv4 隧道协议

IETF 定义的大多数隧道协议都是考虑把IPv6 的数据包封装在IPv4 网络的隧道中进行传输，目的是让IPv6 的终端设备无需感知 IPv4 隧道的存在，以便于在现有的 IPv4 网络中引入 IPv6 技术。各类隧道协议及运行方式、特点见表6。

目前，有多种隧道技术可应用于一些特定的网络场景中，如：主机到主机，主机到网关和网关到网关的机制。静态隧道和自动隧道是比较常用的技术手段。

在电力系统通信中，终端设备和系统之间采用网关到网关的透明技术来实现，表6中的各种协议是互相独立的。

对于终端设备，若需将IPv4 网络中的各个IPv6 孤岛互连起来，使用静态网关到网关的隧道是一种较常用的方式，唯一的缺点就是静态隧道的扩展性较差，因此采用动态隧道技术是未来的发展趋势。

由于在许多情况下都需要使用自动隧道技术，所以不建议使用具有特殊格式的IPv6 地址(例如，嵌入了IPv4 地址的特殊前缀地址)。

表6 IPv6 over IPv4 隧道

标准	运行方式	特点
6in4(RFC 4213)	将IPv6报文封装在IPv4网络隧道中 RFC 2473	协议类型41, 增加20字节报文头，静态手工配置隧道
6over4(RFC 2529)	地址转换 IPv6 over IPv4传输 在IPv4网络的双栈节点之间没有显式的隧道	利用fe80::/10地址，例如192.223.16.85=>fe80::c0df:1055和IPv4的组播机制来实现虚拟链路

表6 IPv6 over IPv4 隧道(续)

标准	运行方式	特点
6to4(RFC 3056)	IPv4网络中无状态地传输IPv6数据包	使用一个内嵌了全局IPv4地址的特殊全局唯一地址前缀自动建立从路由器到路由器的隧道； 通过IPv4云连接各个IPv6域
Teredo(Meredo in Linux) (RFC4380) (RFC5991) (安全更新) (RFC 6081) (扩展)	基于NAT的IPv6 over UDP隧道	IPv6的数据包封装在IPv4-UDP报文中
ISATAP(RFC 5214)	站内自动隧道寻址协议	—
6rd(RFC 5569)	IPv4基础设施上实现IPv6的快速部署	
隧道代理		

仅支持 IPv6 的设备尚未被集成到公共 IPv4 网络中(端到端连接的 IPv4 公共网络里部署基于 6LoWPAN 传感器的网络除外), IPv6 over IPv4 隧道协议在短期内不会应用于电力自动化场景中。

6.4.5 隧道技术总结

隧道本身不是IPv4 迁移至IPv6 的方法，而是IPv4 和 IPv6 的共存技术。

终端设备应不感知隧道。

“主机-主机”和“主机-网关”的隧道端点不宜被使用。

IPv6 设备与 IPv4 设备无法通过隧道相互通信。

IPv4 设备需根据隧道 MTU 值减小其 MTU 值，以避免隧道端点强制分片。

所有新开发的设备应支持减小其 MTU 值，从而允许隧道传输。

6.5 转换

6.5.1 转换原理

通过转换，IPv4 节点可直接与 IPv6 设备通信。因此，从 IPv4 域转换到 IPv6 域，转换器应为 IPv4 域的节点模拟IPv4 网络；反之，转换器应为IPv6 域的节点模拟IPv6 网络，如图18所示。

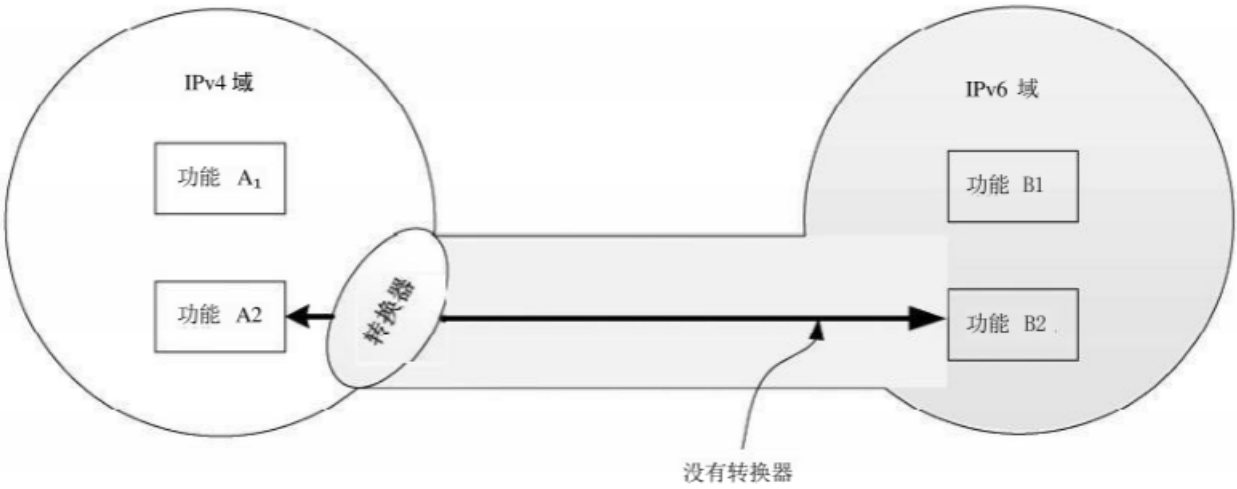


图18 转换原理

6.5.2 IPv4 到 IPv6 的转换

图19所示为IPv4 客户端和IPv6 服务器通过转换器进行数据包交换。转换器允许 IPv4 客户端以相同方式访问 IPv6 网络中的服务器，并允许IPv6 客户端访问IPv4 服务器或响应 IPv4 客户端的请求。由于IPv6 头部长度大于IPv4 头部长度，转换器将 IPv4 地址转换为更长的 IPv6 地址时，局域网上的帧长度可能超过其允许的最大长度。

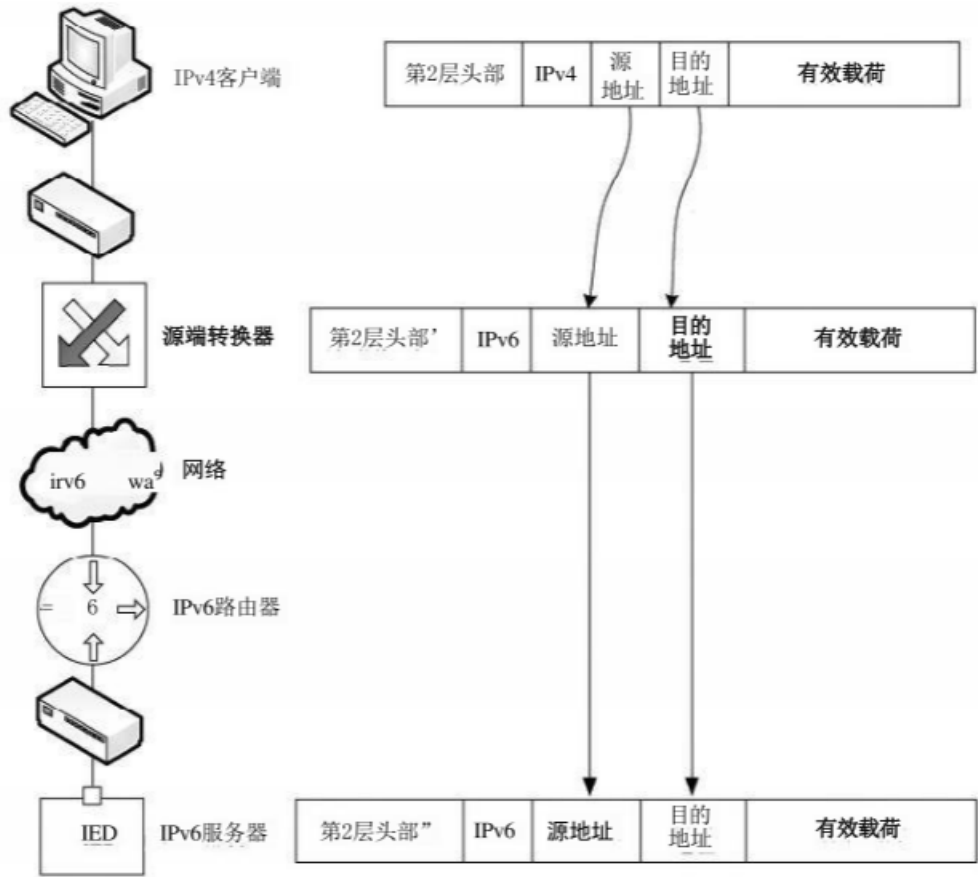


图19 IPv4 转换到 IPv6

IPv4 转换到 IPv6 的首要任务是实现短地址到长地址的映射，反之亦然。
图20所示为IPv6 到 IPv4 反向转换，处于IPv6 网络中的设备认为转换器另一侧的网络也是IPv6。

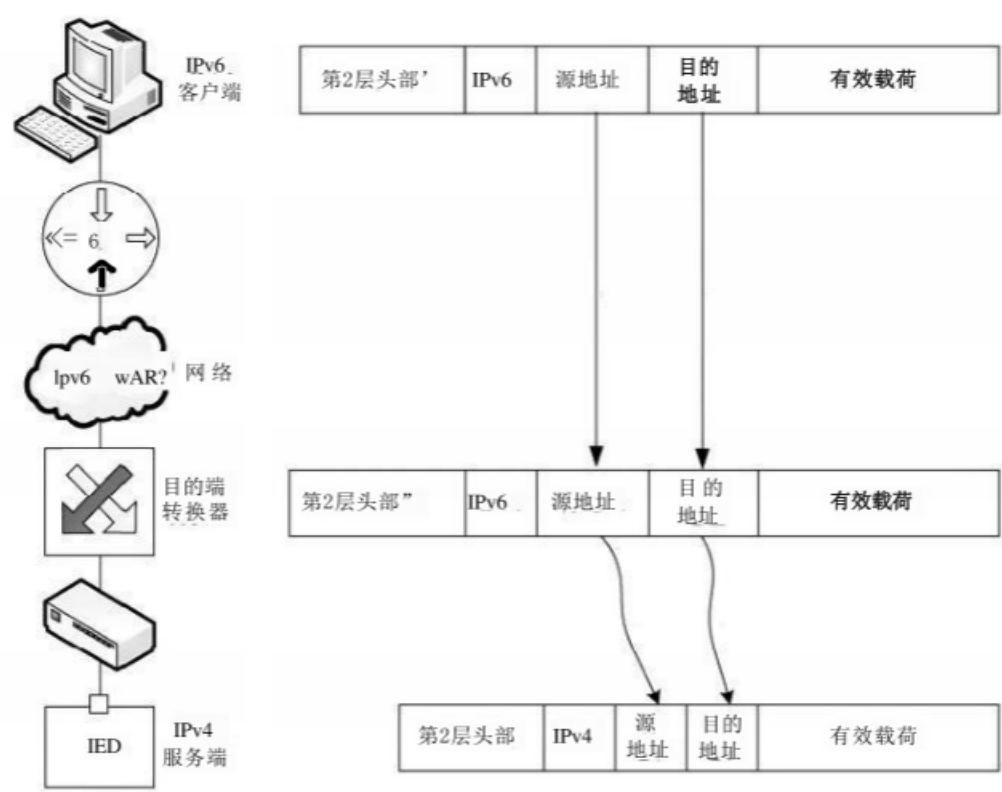


图20 IPv6 转换到 IPv4

6.5.3 转换实现

存在几个相同原理的转换器，IPv4 到 IPv6 的转换原理见图21。

通过 DNS 实现 IP 地址的动态分配，而不是在转换器上静态配置。

转换技术还存在不足，尤其是 OSI 不同层级之间的依赖性（原则上 OSI 各层级之间应相互独立）。例如，TCP-UDP 通过将部分 IP 头部嵌入其校验和（也称为“隐藏头部”，见6.2.3.4）并重新计算，这违背了分层原则。

转换器与隧道一样，都存在分片方面的问题（见6.4.3.2）。

由于某些选项在其他协议中无类似选项，某些语义会在转换过程中丢失。

由于IPv4 或 IPv6 报文头部的某些选项在另一方协议中无等同选项，某些语义会在转换过程中丢失。

注：无线设备的分片数据包较小，且在第2层对其进行重组。

转换器分为两种：有状态和无状态。有状态转换器通过建立网络会话分配临时地址，即 IP 网络层面向无连接的设计思路在这里不再适用。

转换器具有可动态添加的地址池，其一侧为 IPv6，另一侧为IPv4。

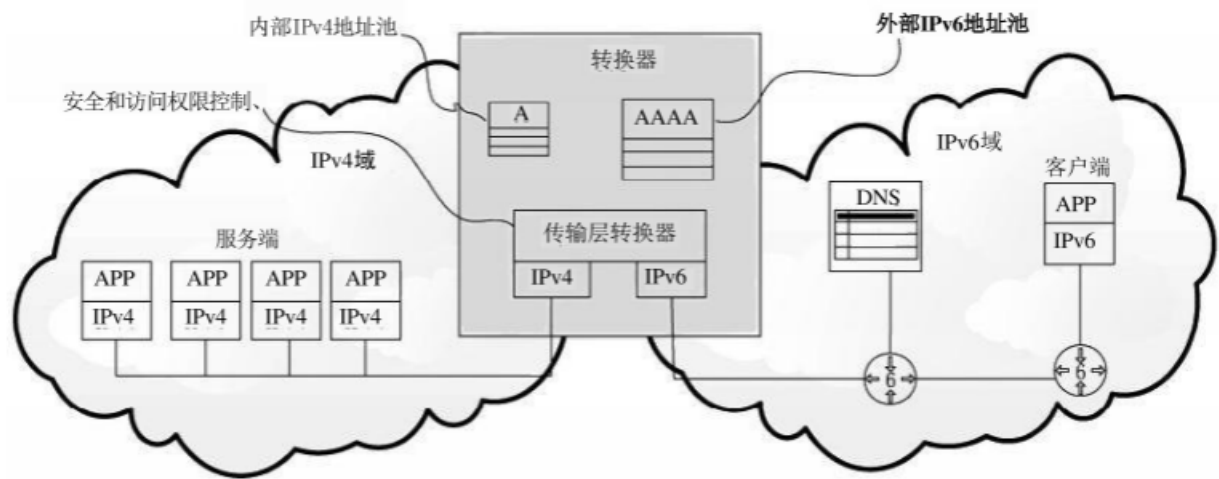


图21 IPv4 到 IPv6 的转换原理

DNS建立的会话对 URL 进行解析，并且向远程 IPv6 节点分配临时 IPv4 地址，反之也可向 IPv4 节点分配 IPv6 地址(仅对IPv6 节点可见)。

在反方向上，将较长的 IPv6 地址映射到较短的 IPv4 地址需进行网络地址转换，该技术已应用在 IPv4公网和私网边界处。

6.5.4 转换器规范

IETF 定义了几种转换器机制(其中有些正在开发中)：

- a) NAT-PT(RFC2766) (被 NAT64 替代)；
- b) NAT64(RFC 6146)；
- c) 无状态IP/ICMP 转换算法(RFC6145)；
- d) TRT；
- e) MAP-T(draft-ietf-softwire-map-t)；
- f) ALG(应用层网关)转换。

注：NAT-PT在实际应用中存在很多问题，因此 IETF提议NAT64(RFC6146)替代 RFC 2766(RFC4966)。

6.5.5 转换技术总结

很少使用转换器进行迁移。

转换器唯一适用的场景是所有新设备仅支持 IPv6, 但在最后一个IPv4 孤岛退役前，双栈设备会一直存在。

6.6 迁移计划

6.6.1 流程

迁移场景各不相同，因此没有提出明确的迁移计划。

原则上，涉及网络基础设施、设备需求规范和工具规范等变更的项目计划，应包含迁移至IPv6 的准备工作，也包括测试。

6.6.2 安全事项

在迁移过程中，可能会引发一些安全问题。

若防火墙未进行数据包深度分析，转换机制能绕过防火墙将数据包渗透到系统内。因此，隧道端点或转换器应得到相应的保护，建议在其设备内配置数据包深度检测防火墙。

迁移过程应同时遵循不同的安全机制和策略，其安全性面临严峻挑战，且相当复杂。

7 基于 IP 的应用协议

7.1 第3层以上的应用协议

应用通信协议承载多种应用数据，包括：

- a) IEC 60870-5-104(远动控制)；
- b) IEEE1815，早期称为分布式网络协议版本3 DNP3(RTU)；
- c) IEC 61850-8-1(变电站内客户端与服务器 MMS 通信)；
- d) IEC TR 61850-90-1(变电站到变电站通信)；
- e) IEC TR 61850-90-2(变电站到控制中心通信)；
- f) IEC TR 61850-90-5(相量测量单元到相量数据集中器通信)；
- g) IEC 61400-25(风力发电厂监控)；
- h) 基于第3层协议的IEC 61588(广域网的时间同步)。

以下协议显式或隐式使用了互联网协议套件：

- a) ARP；
- b) ICMP；
- c) FTP；
- d) SNMP(简单网络管理协议)(RFC 3416)；
- e) NTP(网络时间协议)(RFC 1305)；
- f) SNTP(简单网络时间协议)(RFC 5905)；
- g) HTTP(超文本传输协议)(RFC 7230)。

由于应用层协议不关注下层协议，对于IPv4到IPv6的迁移，仅涉及寻址功能和网络层支持。

注：基于第2层的应用协议，如GOOSE(IEC 61850-8-1)、SMV(IEC 61850-9-2)、PTP(IEC 61588)、LLDP不在此考虑。

7.2 IEC 61850 的第3层通信

7.2.1 第3层直接通信

IEC 61850-8-1规范了MMS(制造报文规范)和SNTP在第3层的通信方式。其他基于第3层的通信协议包括FTP,SNMP,HTTP以及与第3层相关的协议(如：ICMP)。

第3层协议原则上允许变电站外部网络直接访问所有站内设备，变电站到变电站通信方式见图22。

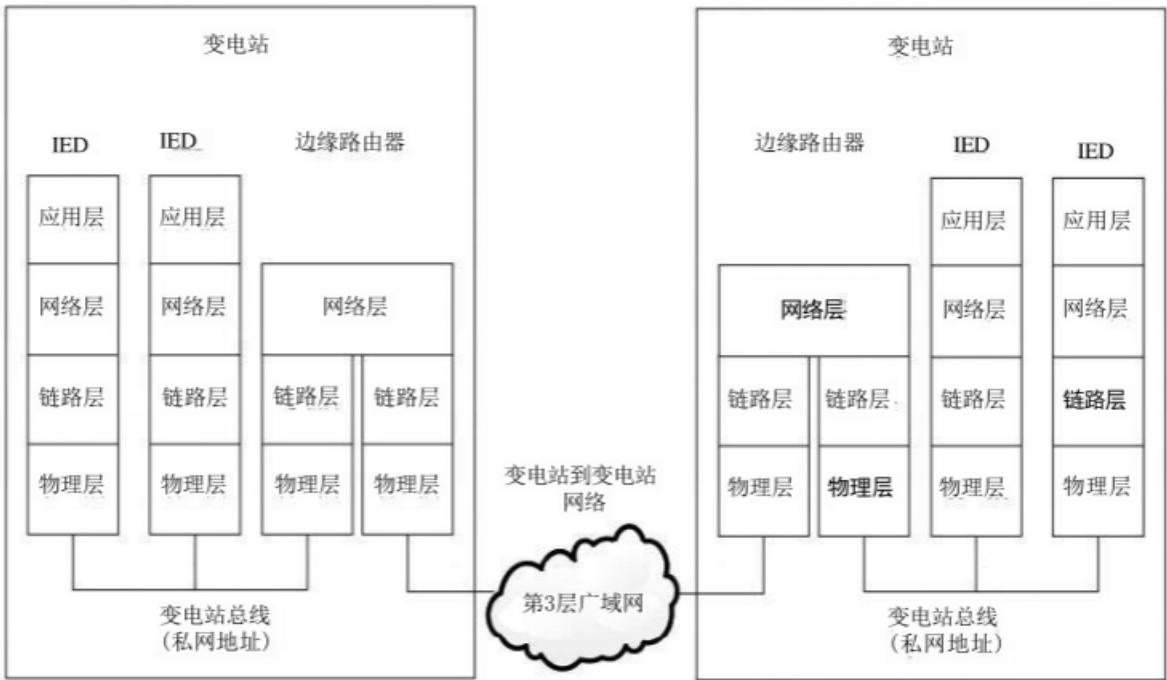


图22 第3层直接通信

变电站内设备使用IEC TR61850-90-4 建议的私网地址。该方式根据站内不同IED 所处位置对其分配静态IP 地址。相同 IP 地址有可能出现在不同的变电站，因此这些IP 地址不能用于变电站到变电站的直接通信(见7.2.2)。

私网 IPv4 地址无法在互联网上路由，因此图22的方式仅适用于统一管理的变电站。

7.2.2 第 3 层 NAT 通信

对于变电站外部网络的访问，NAT(RFC 2663)将内部地址映射到外部地址，由边缘路由器负责地址转换。

为此，边缘路由器设置外部 IPv4 地址池，实现与内部私网 IPv4 地址的映射，并可通过 TCP 和 UDP 端口号进行地址扩展(这也是 ISP 延长 IPv4 生命周期的方法)。

除地址转换之外，网络工程师也可将外部 IPv4 地址分配给内部地址，如图23所示，SCADA 站点直接使用外部 IPv4 地址，则无需 NAT 转换。

例如：SCADA 站点属于10.x.x.x/8 子网，所辖变电站属于192.168.x.x/16 子网，仅变电站需 NAT 转换。

原则上 IED 设备通过NAT 转换访问外部设备。

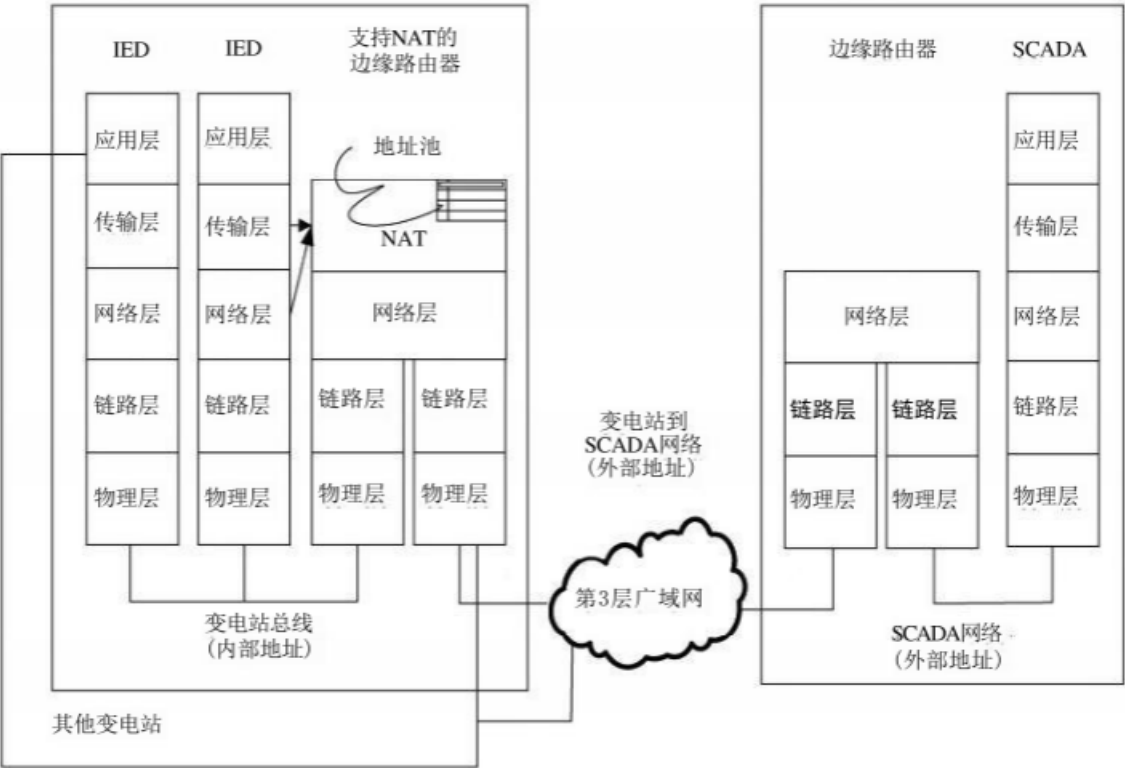


图23 第 3 层 NAT 通信

IED 设备是需要固定地址的服务端，不建议采用IPv4 地址动态分配(私网或公网)方式。在变电站内，如采用IP 地址与设备绑定方式，在设备硬件更换时会出现问题，因此采用 SCD 文件分配 IP 地址方式。

注：上述描述不适用于IED仅作为客户端的通信方式，例如类似 XMPP基础架构。

7.2.3 第 3 层 ALG（代理）通信

不宜采用外部网络直接访问站内设备的方式。即使没有恶意攻击，网络工程师也应关注外部网络直接访问站内设备存在的安全隐患。

注1:电力专网已实现与公网的物理隔离，但只要设备同时或先后连接这两个网络，就无法保证其安全性。

实际应用中不建议直接访问IED 设备(例如安全原因)，代理实现了对站内设备的访问控制，按照“按需访问”原则，只开放需要访问的对象。图24展示了变电站之间 SCADA 站点或者工作站的连接。

ALG 模拟对 IED 设备的单独访问，且 ALG 可屏蔽无需对外暴露的信息，从外部和内部观察的变电站结构不同。由于SCADA（或运维端）仅是客户端，无需部署 ALG。

注2: ALG不一定部署在边缘路由器上，其功能也能在其他设备实现，例如变电站控制器。

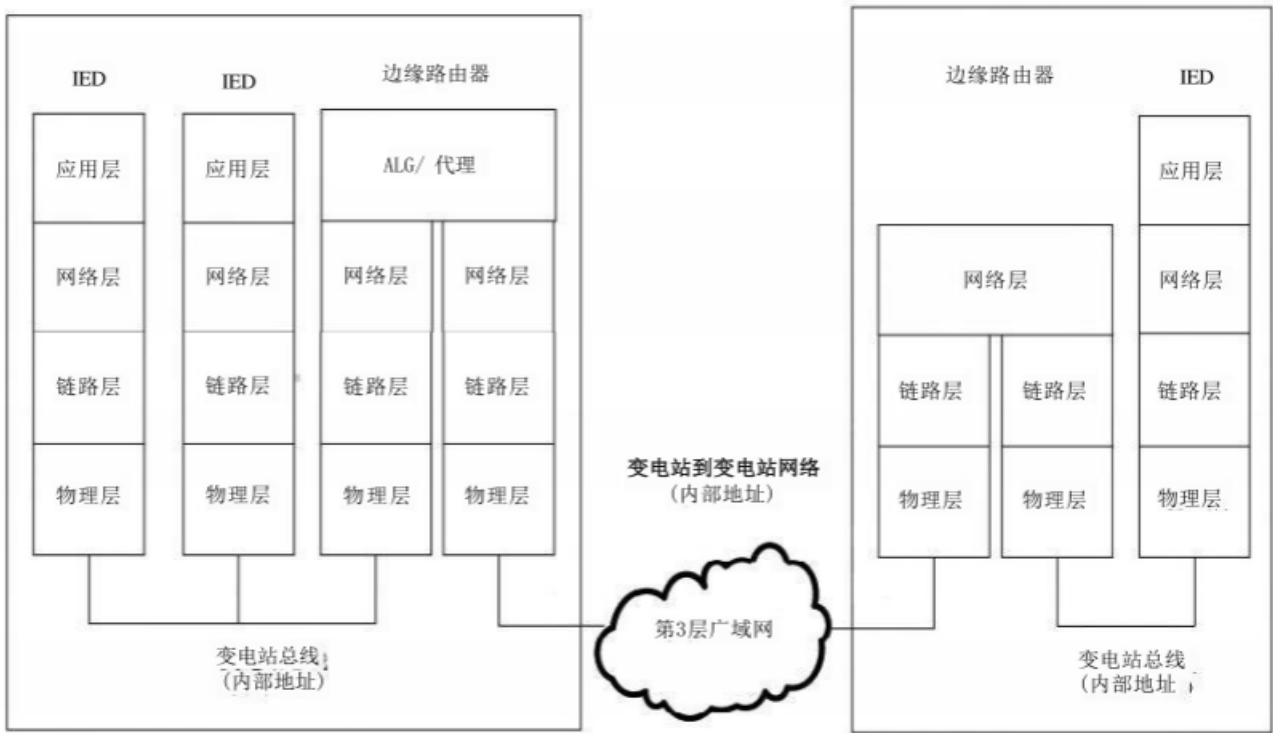


图24 第 3 层 ALG 通信

7.3 IEC 61850 的3层通信(承载2层流量)

IEC TR 61850-90-1规划了变电站之间将通过隧道交换第2层协议，但未规定隧道协议的类型(包括IP 网络、SDH/SONET 或基于 MPLS 的 VLL/VPLS)，而建议使用2层隧道 L2TP 协议(RFC 3931, RFC5641)。L2TP 协议基于 UDP，并提供身份认证机制。基于第3层广域网的2层隧道见图25。

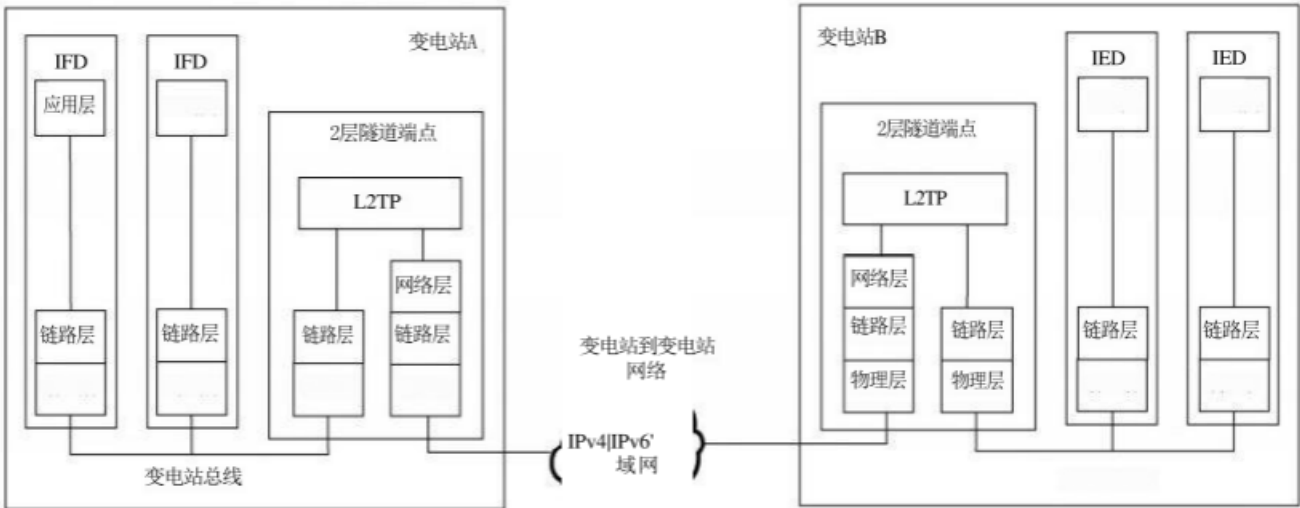


图25 基于第3层广域网的2层隧道

IEC TR 61850-90-1也规定了如8.2.3所示的 ALG 通信方式。
IEC TR 61850-90-5规定了在 IPv4 或 IPv6 上如何传输第2层流量(SMV 和 GOOSE)，采用ITU X.234(OSI 面向无连接传输)和 RFC1240 生成相应的会话头部，但未说明如何将流量映射至 IP 地址。IEC TR 61850-90-5 中基于IPv1 隧道的第2层帧格式见图26。

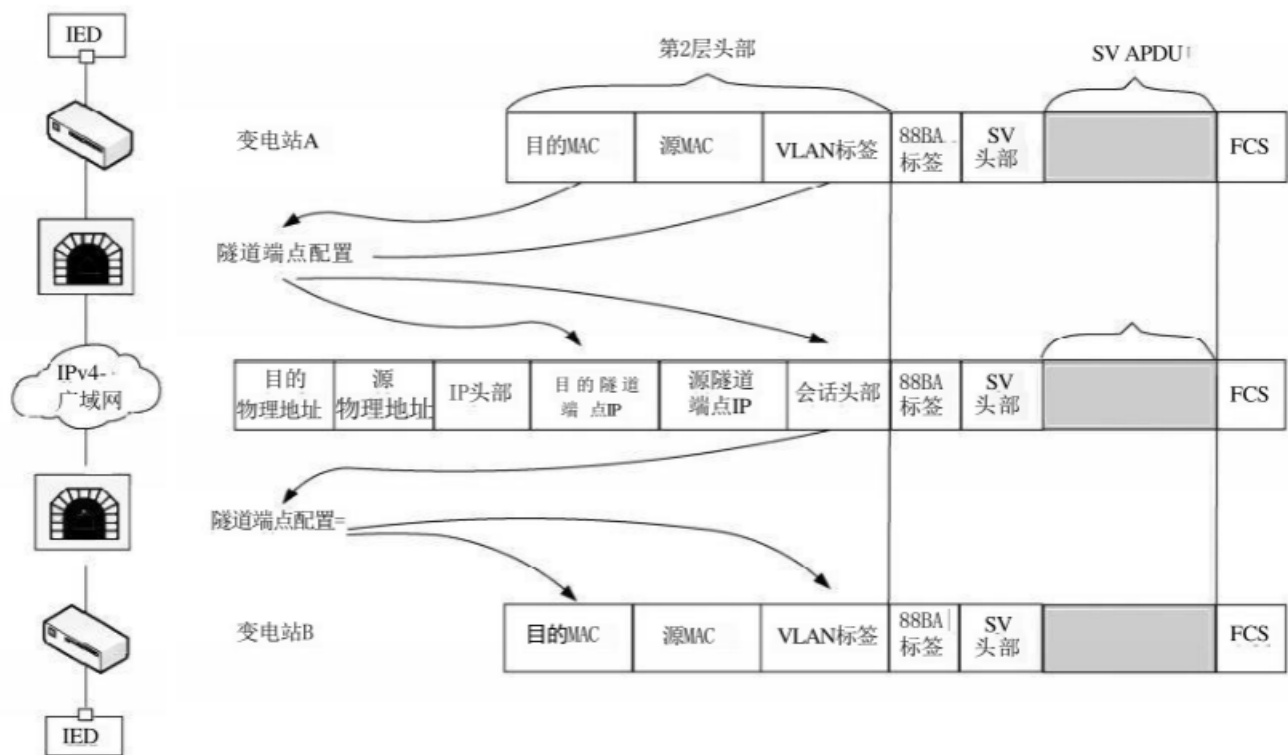


图26 IEC TR 61850-90-5 中基于 IPv4 隧道的第2层帧格式(简化版)

7.4 其他应用协议

IEC61400-25 使用了和IEC61850-8-1 相同的 IP 协议，并扩展了安全特性。
目前 IEC 60870-5-104 使用了IPv4，但未限制使用IPv6。
DNP3 over IP 使用 IPv4 和 IPv6。

7.5 虚拟专用网络叠加

IP 支持 VPN 服务，可在IPSec 隧道模式下实现，该模式允许隐藏通信双方的 IP 地址(WAN 中路由的 IP 地址是明确的)。
VPN 可承载多个虚拟连接，例如支持语音服务和视频远程监控服务。这些协议不关注下层协议，IPv6 迁移时无需考虑。

8 变电站自动化场景

8.1 场景概述

本文件涉及的场景见表7。

表 7 变电站自动化场景概览表

案例	变电站设备协议栈	网络通道	控制中心(或变电站)协议栈	方法	示例	章节
1.1	IPv4	IPv6	IPv4 (变电站)	IPv4 VPN 隧道端点	IEC TR 61850-90-1通过IP隧道传输GOOSE和SMV，也适用于 MMS	8.2.2

表 7 变电站自动化场景概览表 (续)

案例	变电站设备协议栈	网络通道	控制中心(或变电站)协议栈	方法	示例	章节
1.2	IPv4	IPv6	IPv4 (控制中心)	IPv4 VPN 隧道端点	适用于传统变电站、SCADA站 点和工程师站, 通过IPv4 over IPv6隧道传输GOOSE和SMV	8.2.3
2.1	IPv4	IPv6	IPv6 或双栈	双栈双端 口工程师站	通过双栈双端口工程师站的远 程桌面访问传统变电站	8.3.1
2.2	IPv4	IPv6	IPv6 或双栈	代理边缘路 由器作为ALG	基于IPv6的控制中心不直接访 问传统变电站内的设备	8.3.2
2.3	IPv4	IPv6	IPv6	代理边缘路 由器, 转换器	IPv6 SCADA和工程师站通过转 换器访问传统变电站设备	8.3.3
3	IPv4 和双栈	IPv6	IPv6	网关代理 转换器	现有的IPv4变电站部分迁移到 IPv6(全部迁移作为特殊案例)	8.4
4	IPv4 和IPv6	IPv4和 IPv6	IPv6	使用集中器 或中间服务 器作为ALG	通过IPv4和IPv6网络(依赖厂 站侧网络类型)分发同步相量 信息 IPv4域中的设备访问外部IPv6 网络中的服务器, 例如XMPP服 务器	8.5.1 8.5.2
5	IPv6	IPv4或 IPv6	IPv4 或IPv6	隧道转换器 (或双栈SCADA)	大量IPv6设备(通常为 6LowPAN, 比如传感器和控制 器)应与传统IPv4 SCADA或 IPv4网络通信	8.6.1 8.6.2

8.2 场景1:通过 IPv6 实现变电站与外部通信

8.2.1 场景1:描述

变电站外部的所有通信基于 IPv6 设计。

8.2.2 场景1.1:变电站到变电站 IPv4 over IPv6 的2层隧道

IEC TR 61850-90-1和 IEC TR61850-90-5 提出了变电站到变电站之间、PMU 到 PDC(相量数据集中器)之间的隧道通信支持使用IPv6。

IEC TR 61850-90-1 建议使用 L2TP (见7.3), 其中 L2TPv3 支持基于IPv6 的通信。

IEC TR 61850-90-5 建议同步相量使用基于 UDP 和 OSI 适配层的 ITU X.234(ISO/IEC 8602)协议, 该协议本身具有支持 IPv6 的隧道协议。

此外, 2层隧道协议都能在IPv6 上正常运行, 如图27所示。

IEC TR 61850-90-1 规划隧道端点可视作 IEC 61850 对象进行配置。

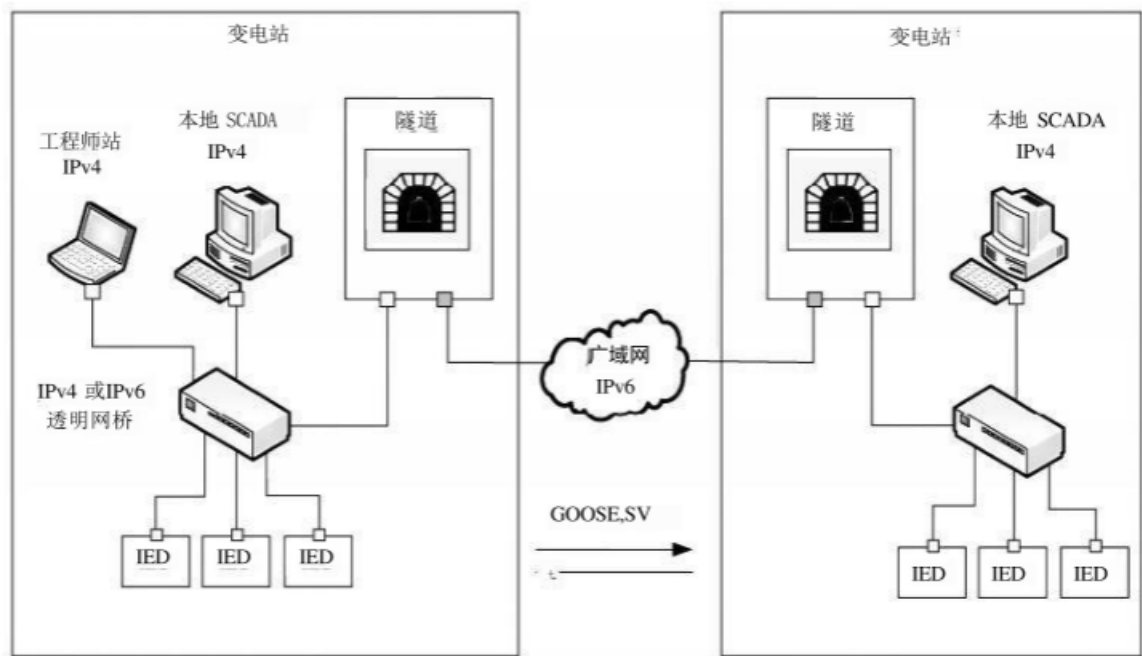


图 27 变电站到变电站的 IPv4 over IPv6 隧道

8.2.3 场景1.2:变电站到控制中心 IPv4 over IPv6 的隧道

通信双方设备仅支持 IPv4,3 层隧道提供了一个简单的解决方案。

用于传输GOOSE 或 SMV 的隧道端点可充当 NAT, 允许远程客户端访问变电站内的 IED, 变电站到控制中心的 IPv4 over IPv6 隧道见图28。

IEC TR 61850-90-1未规定将隧道端点视作 IEC61850 对象集进行配置。

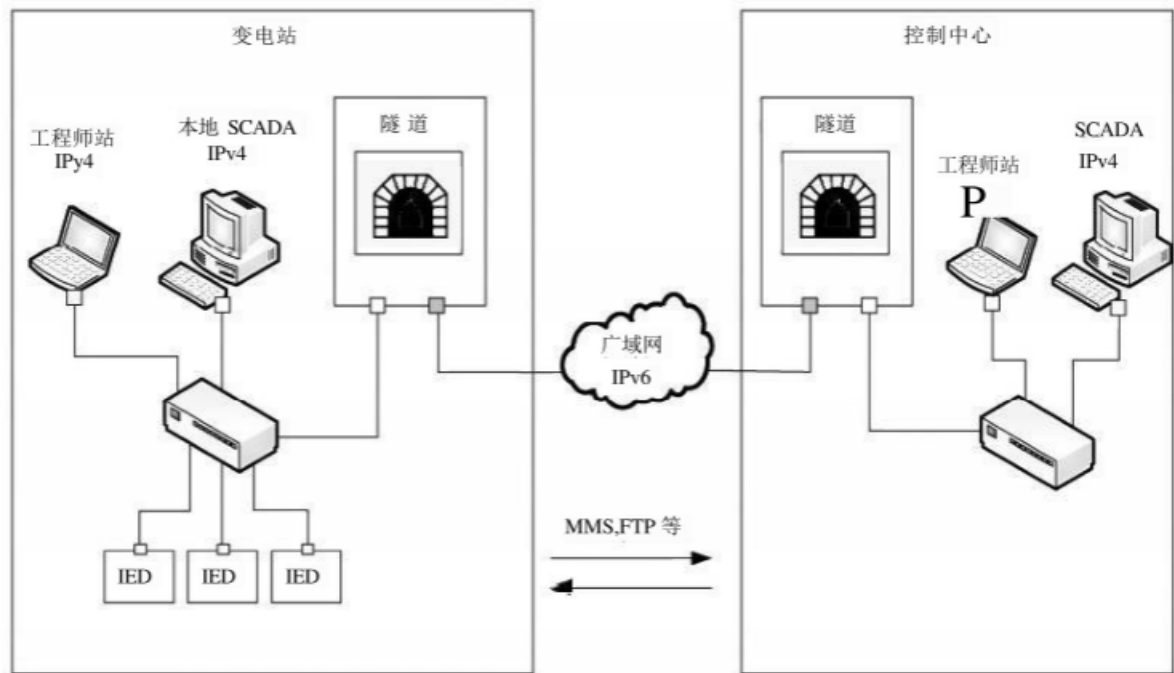


图 28 变电站到控制中心的 IPv4 over IPv6 隧道

8.2.4 场景1:评估

表8列出了IPv6 实现变电站与外部通信的评估结果。

表 8 IPv6 实现变电站与外部通信评估表

实施难度	简单
影响范围	需配置工程师站
成本	适中
特殊设备	隧道端点
IPv6优势	变电站外部的设备可仅支持IPv6
难点	网络工程，静态配置
建议	仅使用标准化的解决方案

8.3 场景2:通过 ALG 和转换器实现 IPv6 设备访问变电站

8.3.1 场景2.1:变电站到控制中心基于双栈工程师站

通信一侧的设备仅支持IPv6 时，有几种解决方案可选。

若仅通过 IPv6 进行远程访问，可采用双栈双端口工程师站作为远程访问网关。若要访问单个 IED, 工程师站(客户端)可通过远程桌面执行工程师站(服务端)的本地配置管理，IPv4 变电站到 IPv6 控制中心基于双栈工程师站通信见图29。

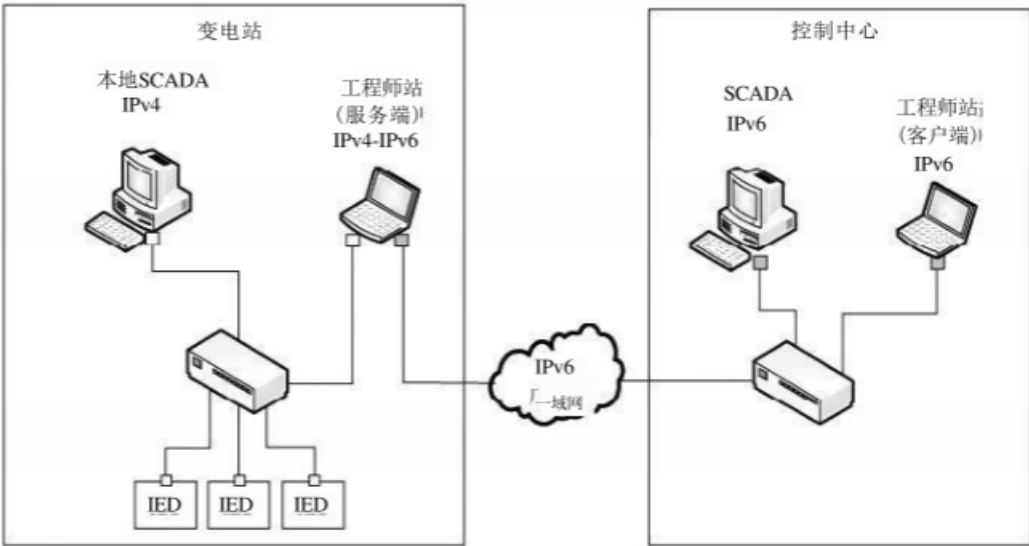


图29 IPv4 变电站到 IPv6 控制中心基于双栈工程师站

8.3.2 场景2.2:变电站到控制中心基于 ALG

如旨在访问变电站内的 IEC61850 对象，而不关注对象来自哪个设备，可使用 ALG 作为代理，通过 IPv6 接口展示 IED 对象。在 IPv6 上，可通过 MMS 访问 ALG 的数据库，IPv4 变电站到 IPv6 控制中心基于 ALG 通信见图30。

IEC 61850-8-1 未定义 IPv6 上的 MMS。

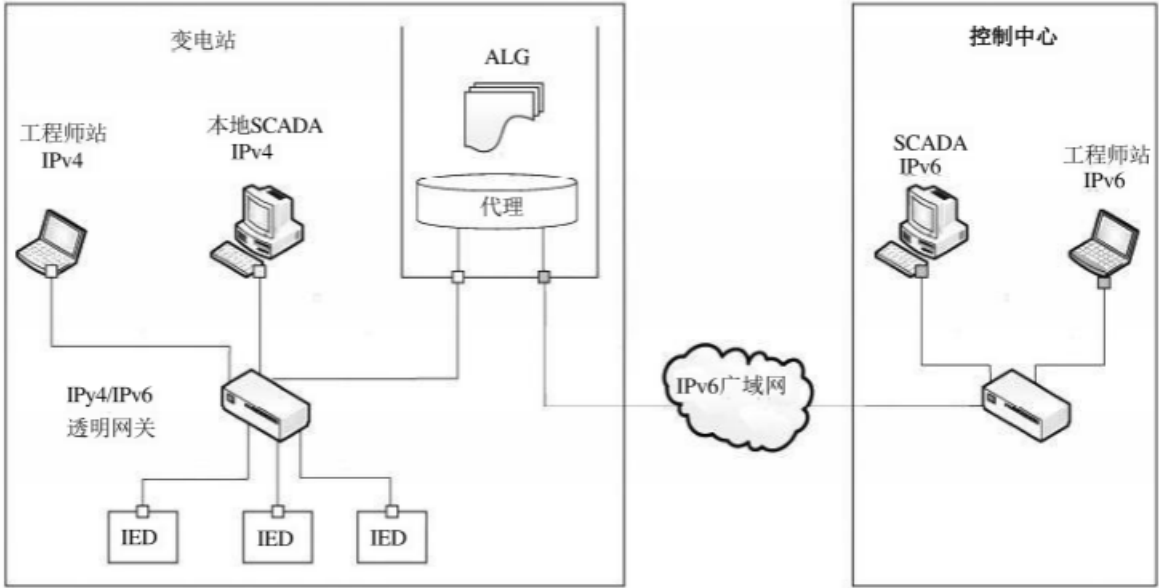


图 3 0 IPv4 变 电 站 到 IPv6 控 制 中 心 基 于 ALG

ALG 可在连接变电站与区域级或国家级控制中心的NCC 网关上实现。

8.3.3 场景2.3:变电站到 SCADA/工程师站基于转换器/代理

双栈双端口代理通过代理功能实现运行数据传输，通过转换器功能实现工程配置和设备访问，并允许使用仅支持IPv6 的工程工具，IPv4 变电站到 IPv6 控制中心基于转换器/代理通信见图31。

转换器/代理不是商用化组件，无法推广应用。
因此，只要存在IPv4 设备，工程工具就应具有双栈功能。

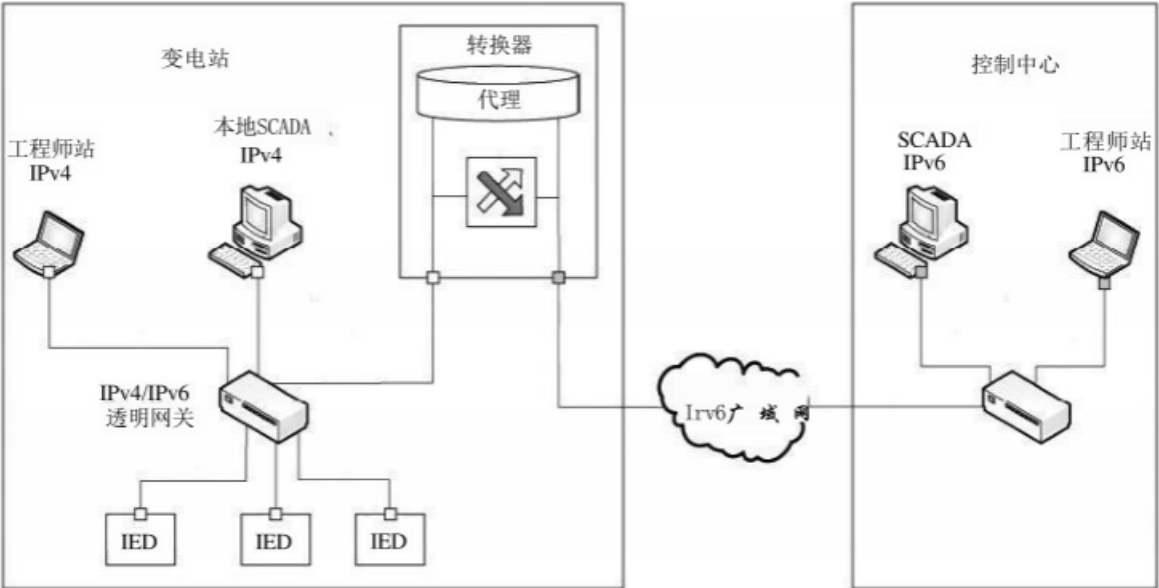


图31 IPv4 变电站到 IPv6 控制中心基于转换器/代理

8.3.4 场景2:评估

ALG 和转换器实现 IPv6 设备访问变电站的评估结果见表9。

表 9 ALG 和转换器实现 IPv6 设备访问变电站评估表

实施难度	复杂
影响范围	需配置工程师站
成本	高
特殊设备	路由器、转换器、隧道端点
IPv6优势	无
难点	面向多场景的网络管理
建议	SCADA和工具软件应长期支持双栈

8.4 场景3:变电站全部或部分支持 IPv6

8.4.1 场景3:描述

基于迁移策略或成本考虑，部分设备仅实现了单栈，因此变电站同时存在IPv4 和 IPv6 设备。

8.4.2 场景3.1:变电站存在双栈设备

除了内存限制和授权成本，目前双栈设备可广泛应用。事实上，实时内核制造商已提前规划 IPv6 通信协议栈。控制中心很有可能长期使用双栈设备。

迁移至 IPv6 对未使用路由器的变电站内部通信不会造成影响。

变电站部分 IED 不使用基于 IP 的点对点通信(GOOSE 和 SMV 直接基于第2层协议通信), 因此不是所有设备都需要支持双栈。

控制中心可直接访问变电站内的所有双栈设备，如图32所示。

控制中心访问仅支持 IPv4 的 IED, 可使用与场景2.3相同的转换器或代理；通过边缘路由器或网关可直接访问双栈 IED, 无需使用转换器。

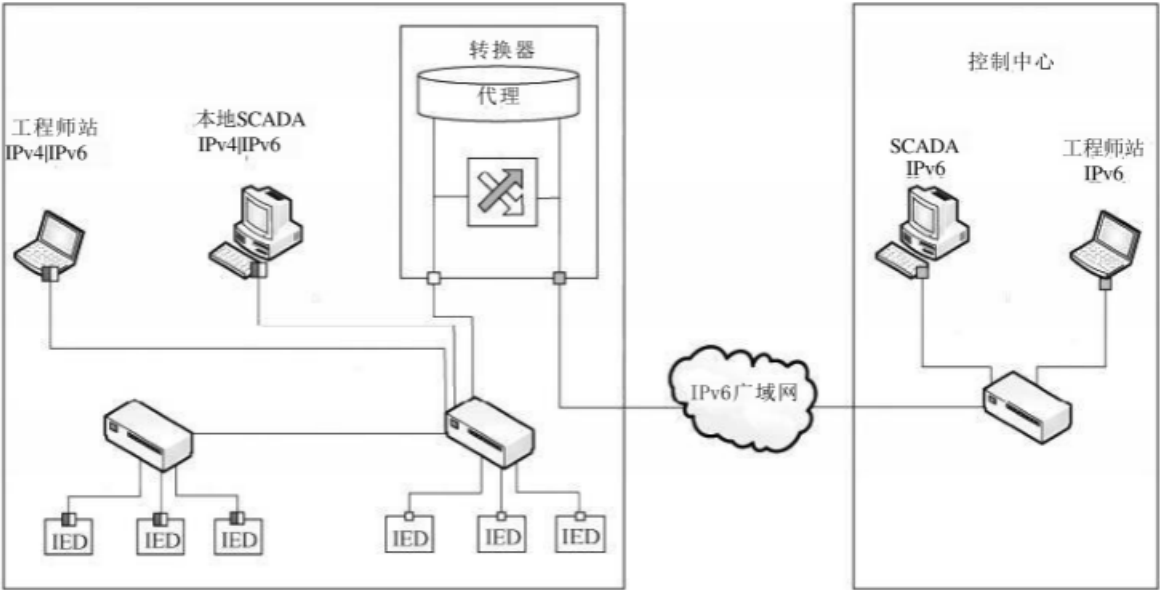


图32 IPv4 变电站存在双栈设备

变电站到变电站、变电站到控制中心的通信应使用ULA。

注：仅支持 IPv6 的 IED 在短期和中期内不会普及，因此在未来几年内不会出现 IPv4-IPv6 互操作性问题。

8.4.3 场景3:评估

变电站全部或部分支持IPv6 的评估结果见表10。

表10 变电站全部或部分支持 IPv6 评估表

实施难度	困难
影响范围	所有SCADA、工程师站设备和外部网络需支持双栈
成本	高
特殊设备	转换器
IPv6优势	控制中心的SCADA/工程师站与支持IPv6的IED之间使用端到端通信，无需NAT转换
难点	通过转换器才能实现IPv6与仅支持IPv4设备之间的对等通信
建议	所有设备都支持双栈； 在变电站的网络边缘不应使用NAT； 每个变电站具有唯一的ULA前缀，但不同变电站的子网划分和设备接口ID是类似的

8.5 场景4:中间设备作为 ALG

8.5.1 PDC 作为 ALG

在同步相量分布式网络中，双栈、多端口PDC 聚合 PMU 的数据，上传至相量数据中心。双栈 PDC 可将数据从 IPv4 设备传输到 IPv6 网络和设备，如图33 所示。

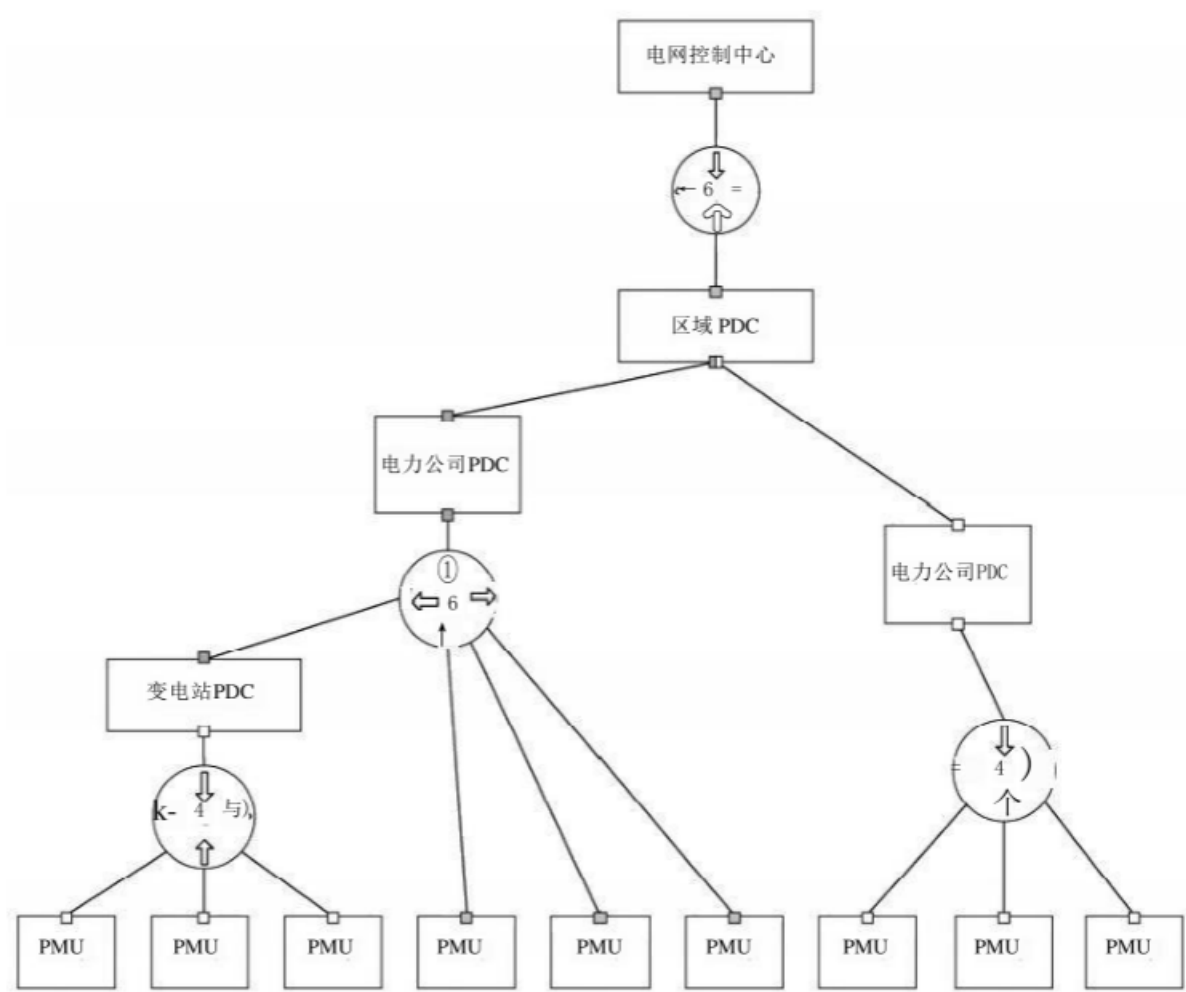


图33 PDC 作为 ALG

这不是一个通用的解决方案，原因如下：

- a) 如果网络能够提供足够的带宽，PDC 无需存在；
- b) PDC 不支持其他协议(SNMP,FTP)；
- c) 在 WAMPAC（广域监测、保护和控制）中，反向路径（访问）也需要转换，但 PDC 未定义此规则。

8.5.2 XMPP 服务器作为 ALG

IEC61850-8-2 构建的 XMPP 网络中，XMPP 服务器作为双栈设备，可通过 IPv4 访问一类客户端，同时通过 IPv6 接口访问WAN 或另一类客户端。它不完全是一个 ALG(XMPP 服务器不关注应用数据)，但仍可将其视为“中间件网关”。基于 XMPP 服务器的转换方式见图34。

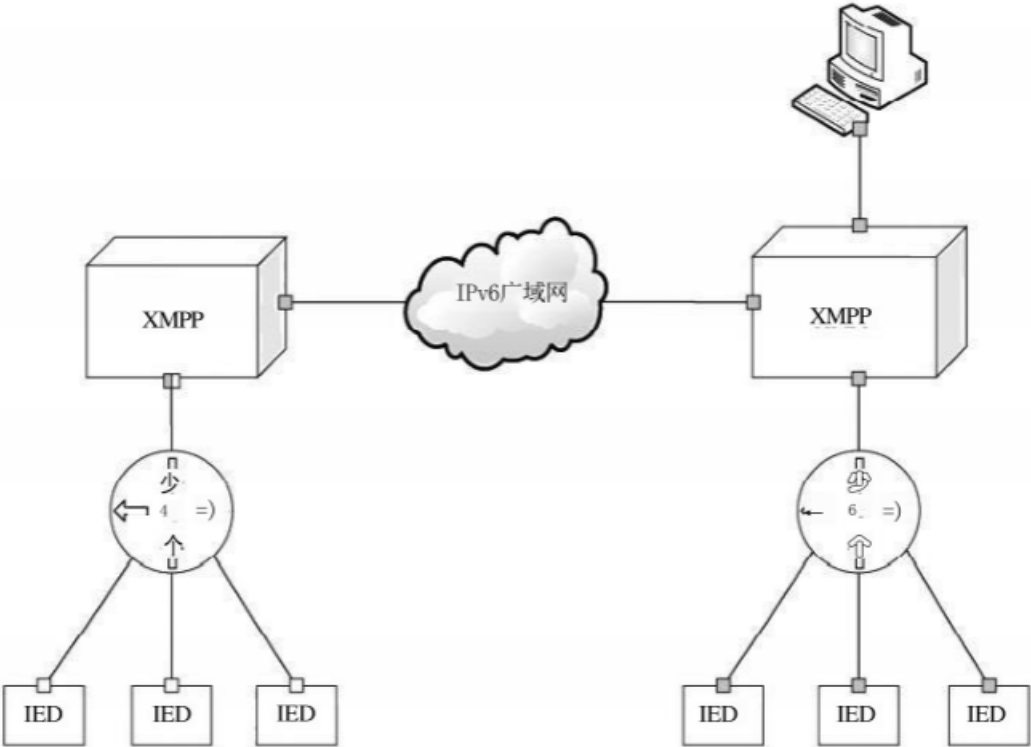


图34 基于 XMPP 服务器的转换方式

所有通信都经过 XMPP 服务器时，此方案很实用。当客户端并行使用其他协议时，这种方案没有优势。

8.5.3 场景4评估

使用中间设备作为 ALG 是一个临时解决方案，几乎没有优势，并缺乏通用性。

8.6 场景5:传统 IPv4 网络集成仅支持 IPv6 的设备

8.6.1 仅支持IPv6 的设备通过隧道连接 IPv4 网络

本场景适用于存在仅支持 IPv6 设备的网络通信，如厂站侧为6LoWPAN 智能传感器网络，主站侧为支持 IPv6 或双栈的 SCADA 或集中器。

本场景利用隧道实现通信的方式与场景2相反，仅支持 IPv6 的传感器通过隧道连接到传统 IPv4 网络见图 35。

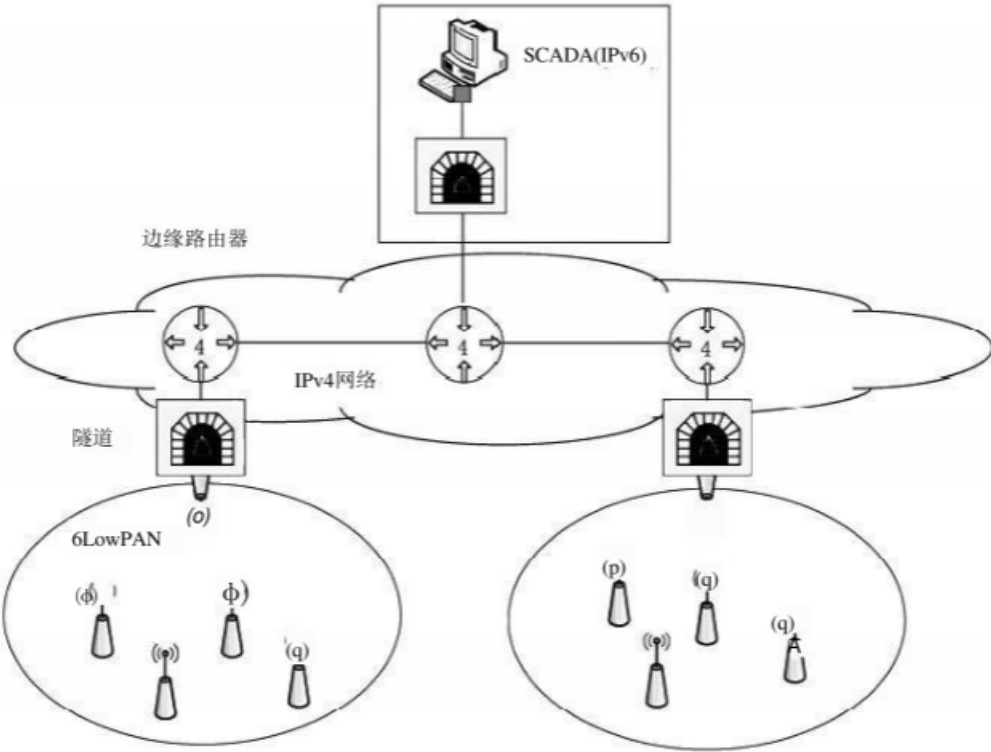


图35 仅支持 IPv6 的传感器通过隧道连接到传统 IPv4 网络

8.6.2 IPv4 SCADA 通过转换器访问仅支持 IPv6 的设备

SCADA 侧的转换器(或支持双栈的 SCADA) 会被优先使用。6LoWPAN 设备的集中器也可作为转换器使用。仅支持 IPv6 的传感器通过转换器连接到传统 IPv4 网络见图36。

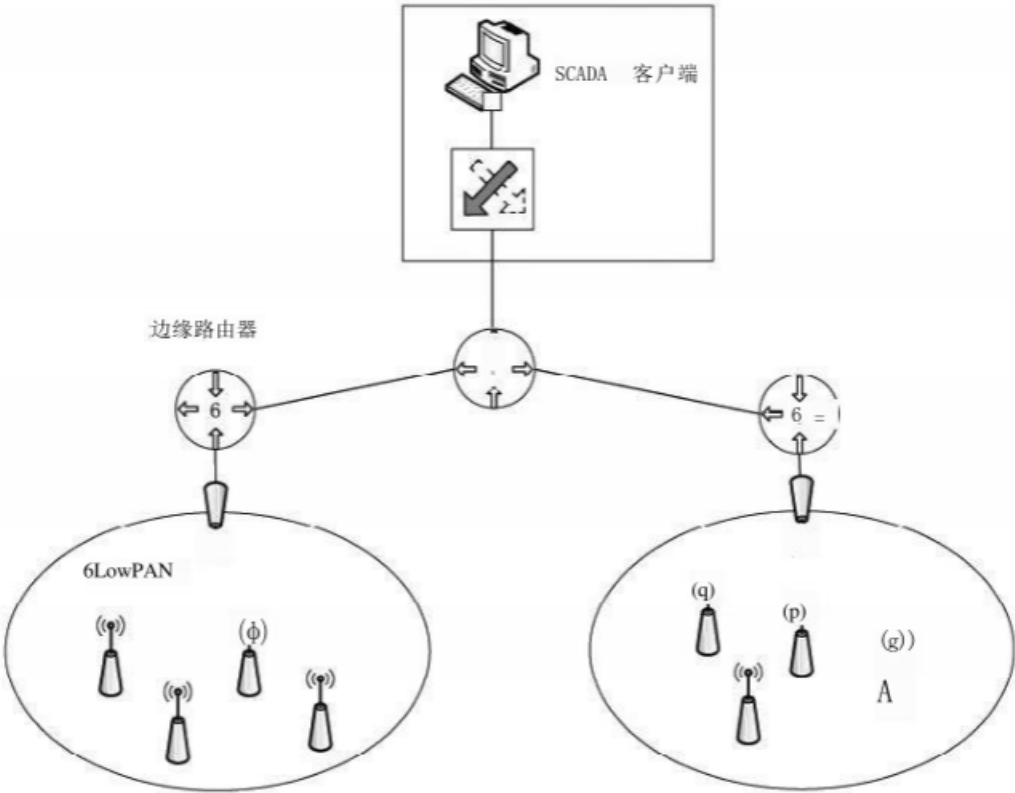


图36 仅支持 IPv6 的传感器通过转换器连接到传统 IPv4 网络

8.6.3 场景5评估

IETF 标准和商用设备已完全支持场景5。

9 发电厂自动化场景

9.1 通则

第9章中的案例涉及发电厂（如水力/可再生能源）的远程控制和自动化系统。发电系统远程控制概览见图37。

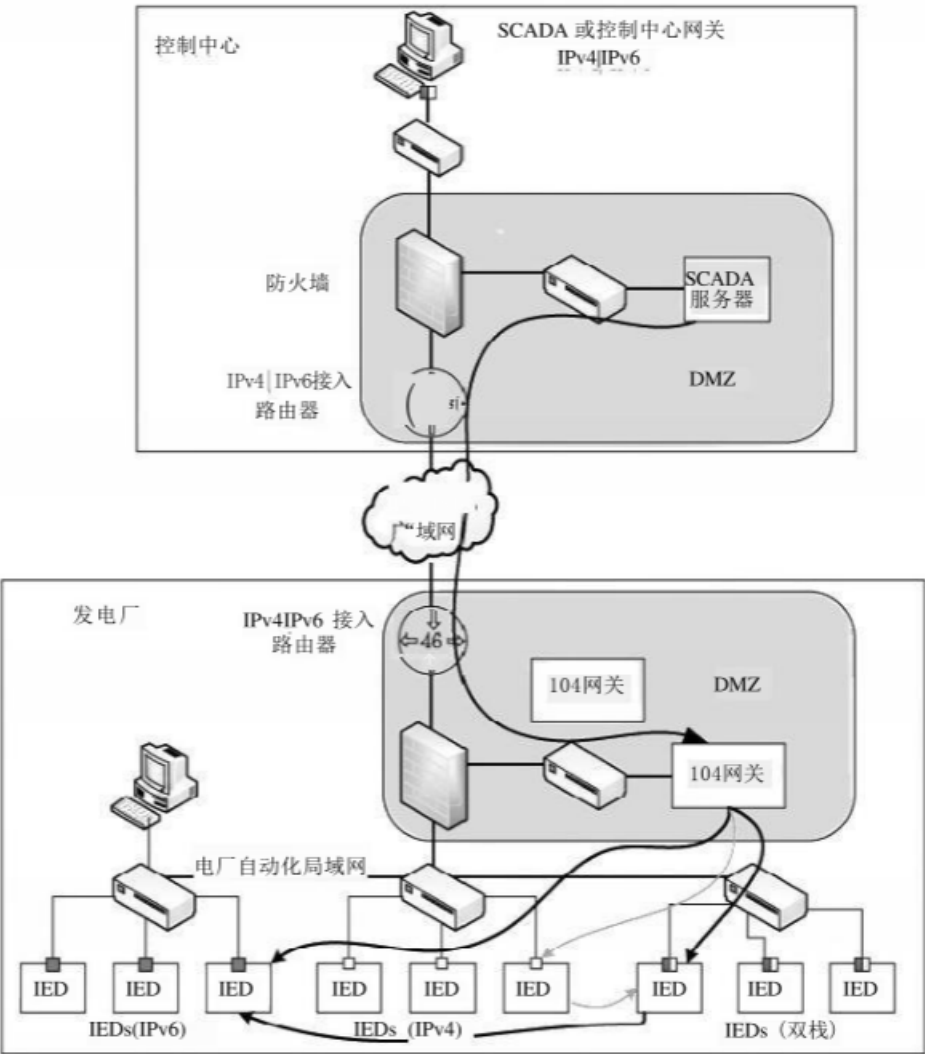


图37 发电系统远程控制概览

发电厂远程控制系统部署了支持双栈的 SCADA 系统，支持在 SCADA 应用层同时处理 IPv6 和 IPv4 协议。

本场景需考虑以下两点：

- a) 广域网将支持同时承载IPv6 和 IPv4 协议；
- b) 在操作系统和 SCADA 应用方面，SCADA 系统应已启用双栈。

本场景定义并实现四个主要的逻辑网络区：

- a) 发电厂自动化网络区，承载电厂自动化设备（如 IED）；
- b) 发电厂 DMZ 区，承载 IEC 60870-5-104 网关和其他需连接外部广域网的系统；

- c) 控制中心网络区，承载操作员控制台和控制室设备；
- d) 控制中心 DMZ 区，承载 SCADA 网关服务器和辅助系统。

每个逻辑网络区通过路由器和防火墙连接到广域网。通过防火墙策略实现网络区之间的访问控制，并且每个区的 IP 子网需独立分配。

控制中心和发电厂之间的接口是数据通信网关机，承载 IED 和传统自动化设备控制业务。

电厂自动化将同时支持传统协议和 IEC 61850 协议。

控制中心和发电厂之间远动协议的安全性依据 IEC 62351 系列标准实现。

本场景的远程控制系统可控制数百个发电厂。

多个控制中心同时运行在电力通信网，发电厂的控制功能将分布在这些控制中心中。

本网络还应支持承载 IPv6 和 IPv4 协议，即需制定双栈寻址方案，无需配置隧道。

9.2 传统 IPv4 寻址方案

传统 IPv4 寻址方案包括如下内容。

- a) 承载远程控制的 IPv4 广域网寻址方案使用企业专用网地址 10.0.0.0/8，其他业务逻辑网络也共享使用该地址，因此只有一部分地址适用于远程控制网络，例如 10.15.0.0/16；
- b) 通过将 10.15.0.0/16 网络划分为多个较小的子网而得到发电厂寻址区间。由于每个电厂只保留较小的企业子网空间（通常分配给 DMZ 区），这可能成为电厂地址分配的一个约束条件；
- c) 每个电厂有独立的自动化局域网，外部仅允许通过 DMZ 区内的防火墙对其访问。

9.2 中的方案允许使用“内部”私有地址（例如 192.168.75.0/24），该地址对于广域网不可知也无法直接访问，因此在其他类似的发电厂中可重复使用。

如任何自动化局域网设备需访问发电厂之外的设备，唯一方法是在防火墙上采用 NAT 策略。

这些传统设备无法与电厂外的其他设备直接通信。随着发电厂内逐步采用 IPv6 协议，新 IED 设备之间可直接互联。

9.3 IPv6 寻址及共存方案

随着 IPv6 广域网的逐步推广，不同的寻址方案可供选择。

在电力公司域网中，建议使用已注册的全局地址空间（例如，根据 4.2.3.2 的一个完整/48 块）。

在这个广泛的地址空间内，可为不同的网络范围保留特定的子网（例如一个/50 网络），这也同样适用于“远程控制网络”场景。

广域网中所有 IPv4 设备退役之前，IPv6 寻址方案与 IPv4 寻址方案应并行管理。电力公司全局地址方案已考虑每个 IPv6 子网划分。

每个发电厂的自动化局域网可使用 IPv6 ULA 或全局地址，并且 IPv6 设备无需使用任何 NAT 策略。

但是传统 IPv4 自动化局域网仍将可用，以确保仅支持 IPv4 设备的正常运行。

IEC 60870-5-104 定义的 RTU 网关，将转换不同协议之间以及 IPv6 和 IPv4 域之间的消息。

9.4 IPv6 优势

采用 IPv6 的主要优势是自动化局域网无需使用 NAT 策略。

控制中心可通过多种配置方式直接访问发电厂设备，这使得 IEC61850 不再只适用于电厂内部通信，也可适用于电厂之间以及电厂与控制中心之间通信。

IPv6 寻址显著提升了远程控制网络基础设施的可扩展性。随着分布式能源和可再生能源占比逐

步增大，这种可扩展性可能成为强制性要求。

上述场景无需使用隧道或专用转换设备。

9.5 问题

实现本场景较为复杂，应关注以下方面：

- a) 使用广域网IPv6 寻址和路由方案；
- b) 对网络基础设施设备(路由器、防火墙、域名服务器)的功能和规模进行适当的评估和审查，以支持 IPv4 和 IPv6 双栈传输；
- c) 对于 IPv4 和 IPv6 协议，其寻址方案和网络策略需同步管理，这也将影响网络监控、管理架构和流程；
- d) 遵循 IPv6 编码规范，手动 IP 寻址配置变得复杂且易错，应提供支持地址自动分配的工具；
- e) 为了充分发挥IPv6 的优势，电厂内的所有 IED、RTU 和局域网设备应支持IPv6。

广域网基础设施升级将面临额外的成本，有待进一步分析。

10 建议

10.1 给制造商的建议

给制造商的建议如下内容。

- a) 产品开发过程中，宜考虑产品对IPv6 的支持。
- b) 首先考虑应用程序迁移。即使没有立即部署 IPv6 的计划，后续版本的应用程序在需求和测试阶段，需考虑 IP 相关性，如相关则需支持 IPv6。
- c) SCADA、控制中心、网关等设备需支持双栈，以便它们与IPv4 和 IPv6 孤岛进行通信(假设 IPv4 和 IPv6 孤岛之间无法直接通信)，商业操作系统已支持双栈。
- d) 开发双栈 IED。由于多数实时内核已支持双栈，双栈设备研发成本不高。目前许多 RTU 也已运行在 IPv4 或 IPv6 上。
- e) 考虑测试 IPv4 设备减小包长度并支持 IPsec，提供至少作为 PICS 入口的 IP 安全协议支持。
- f) 为满足 PICS(协议实现一致性说明)要求，需测试 IPv4 设备是否可减小包长度并支持 IPsec。
- g) 开发隧道端点以实现 IPv6 网络连接传统 IPv4 设备。除合规性原因(如 NIST)外，用户不必很快切换到IPv6。因此，只要 SCADA/NCC 支持IPv4，并且监管机构允许，就可以使用隧道。最终，隧道可能会消失。
- h) 开发隧道端点，以实现通过 IPv6 网络连接 IPv4 设备。除合规性原因(如 NIST)外，用户无需立即切换至IPv6。只要SCADA/NCC 支持 IPv4，并且监管机构允许，就可使用隧道端点。隧道端点会逐步消失。
- i) 如无需从外部直接访问 IED，可开发网关以作为协议之间的桥梁。

10.2 给网络工程师的建议

给网络工程师的建议如下内容。

- a) 在部署 IPv6 组件之前需进行全面测试。
- b) 可利用IPv6 地址空间大的优势构建无NAT 的网络结构。
- c) 可利用现成的转换器实现外部直接访问IPv4 孤岛内设备。
- d) 可检查隧道端点和转换器的引入对安全性的影响。

10.3 给 IEC 标准制定工作组的建议

给IEC 标准制定工作组的建议如下内容。

- a) 确保目前 IPv4 相关的 IEC 标准将继续强制支持 IPv4, 以实现向后兼容性。
- b) 确保目前的IEC TR 61850-90-4(电压等级-间隔-IED) 寻址方案也适用于IPv6。
- c) 针对 IPv6 需提供地址分配、管理和命名(地址规划)指南。
- d) 在标准文档修订和新文档编制中需同时考虑IPv4 和 IPv6, 特别是定义映射到IPv4 的 IPv6 配置文件, 以及无需进行完全IPv6 一致性测试也能确保功能一致性。
- e) 为 SCSM 指定一个IPv6 配置文件, 作为 IEC 61850-8 的附加和可选 SCSM。如标准定义了这个选项, 特定的应用域或实用程序策略可请求 IPv6 地址(见6.3.3)。
- f) 采用隧道端点的对象模型, 作为IEC TR 61850-90-1和 IEC TR 61850-90-5 的扩展, 以简化网络工程和部署。
- g) 转换器可作为IEC 61850的一个对象, 但不宜作为IP 迁移的解决方案。
- h) 按照IEC 62351规定, 需验证隧道端点和转换器对安全性的影响。
- i) 考虑未来某个日期后需强制支持(而非使用)双栈(由网络配置程序选择协议栈类型)。
- j) 考虑未来某个日期后部分应用程序需强制使用 IPv6(参见引言)。

10.4 执行迁移计划的时间表

见引言。

参 考 文 献

- [17] IEC 61850-9-2 Communication networks and systems for power utility automation—Part 9-2:Specific communication service mapping(SCSM)—Sampled values over ISO/IEC 8802-3
- [2] IEC TR 61850-90-12 Communication networks and systems for power utility automation—Part 90-12:Wide area network engineering guidelines
- [3] ISO/IEC 10038 Information technology—Telecommunications and information exchange between systems—Local area networks—Media access control(MAC)bridges
- [4] RFC 3053 IPv6 Tunnel Broker
- [5] RFC 3068 An Anycast Prefix for 6to4 Relay Routers
- [6] RFC 3089 A SOCKS-based IPv6/IPv4 Gateway Mechanism
- [7] RFC 3142 IPv6 to IPv4 Transport Relay Translator
- [8] RFC 3376 Internet Group Management Protocol,Version 3
- [9] RFC 3547 The Group Domain of Interpretation
- [10] RFC 3596 DNS extensions to support IPv6
- 11 RFC 3964 Security Considerations for 6to4
- RFC 4007 IPv6 Scoped Address Architecture
- [13] RFC 4057 IPv6 Enterprise Network Scenarios
- 14 RFC 4477 DHCP:IPv4 and IPv6 Dual-Stack Issues
- 15 RFC 4852 IPV6 Enterprise Network Analysis-IP Layer 3 Focus
- 16 RFC 4864 Local Network Protection for IPv6(NAT obsolescence)
- [17] RFC 4942 IPv6 Transition/Coexistence Security Considerations
- 18 RFC 4966 Reasons to Move the Network Address Translator-Protocol Translator(NAT-PT)to Historic Status
- [19] RFC 5952 A Recommendation for IPv6 Address Text Representation
- 20 RFC 6147 :DNS64:DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers
- [21] RFC 6171 IP/ICMP Translation Algorithm
- [22] RFC6180 Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment
- [23] RFC 6761 Special use domain names
- [24] An introduction to IPv6,DNCPv6,transition mechanism and security,Patrick Wetterwald,CISCO,pwetterw@cisco.com
- [25] IPv6 Address,https://en.wikipedia.org/wiki/IPv6_address
- [26] IPv4-to-IPv6 Transition and Co-existence Strategies,BT Diamond IP Whitepaper.<http://ebook-browsee.net/adv.php?q=ipv4+ipv6+transition+pdf&.way=1>
- [27] <http://standards.ieee.org/development/regauth/tut/eui64.pdf>

