ICS 25.040
N 10

中华人民共和国国家标准化指导性技术文件

GB/Z 20177.4—2006

控制网络 LONWORKS 技术规范 第 4 部分：基于隧道技术在 IP 信道上传输控制网络协议的规范

Control network LONWORKS technology specification—Part 4: Specification of tunneling component network protocols over internet protocol channels

2006-05-08 发布

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目　　次

前　言

GB/Z 20177 总标题为《控制网络 LONWORKS 技术规范》，目前包括以下 4 个部分：

——第 1 部分：协议规范；

——第 2 部分：电力线信道规范；

——第 3 部分：自由拓扑双绞线信道规范；

——第 4 部分：基于隧道技术在 IP 信道上传输控制网络协议的规范。

本部分是 GB/Z 20177《控制网络 LONWORKS 技术规范》指导性技术文件的第 4 部分。

本部分修改采用 ANSI/CEA852《基于隧道技术在 IP 信道上传输控制网络协议的规范》。

本部分与 ANSI/CEA852 的主要差异：

a) 凡是出现 ANSI/CEA852 的地方都用本部分代替；

b) 根据 GB/T 1.1 进行编辑性修改；

c) 为方便使用，在原文的基础上增加了引言部分。

本部分的附录 A 是规范性附录。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量和控制标准化技术委员会第四分技术委员会归口。

本部分起草单位：机械工业仪器仪表综合技术经济研究所、西南大学、北京交通大学现代通信研究所、北京宽网社区数字化建设有限公司、威世达通信控制技术(北京)有限公司、埃施朗公司。

本部分主要起草人：梅恪、王春喜、王玉敏、杨玉柱、刘枫、孙昕、史学玲、欧阳劲松、刘运基、戴恋、刘永生、李翔宇。

引　言

《控制网络 LONWORKS 技术规范》基于 OSI 参考模型(GB T 9387.1—1998),是一个 7 层模型。GB/Z 20177 由四个部分组成。

——第 1 部分:协议规范;

——第 2 部分:电力线信道规范;

——第 3 部分:自由拓扑双绞线信道规范;

——第 4 部分:基于隧道技术在 IP 信道上传输控制网络协议的规范。

第 1 部分是整个技术规范的核心,后三部分是第 1 部分的补充。

GB/Z 20177《控制网络 LONWORKS 技术规范》四个部分的关系见图 1。

本部分是 GB/Z 20177 的第 4 部分,是基于隧道技术在 IP 信道上传输控制网络协议的规范,针对网络层作了补充说明,并描述了控制网到 IP 信道的隧道技术以及相关设备的规范。

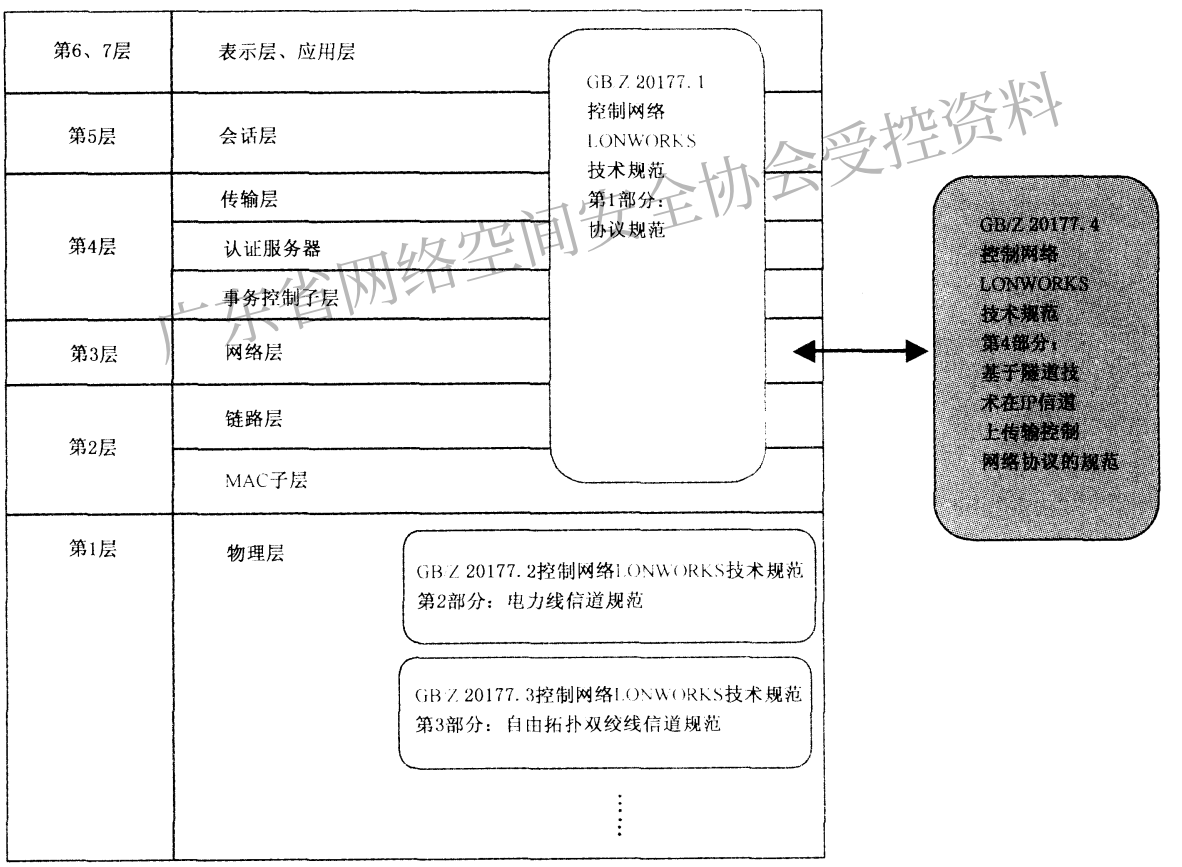

图 1　GB/Z 20177 四个部分的关系

控制网络 LONWORKS 技术规范 第 4 部分：基于隧道技术在 IP 信道上传输控制网络协议的规范

1 范围

GB/Z 20177 的本部分定义了基于隧道技术在 IP 信道上传输控制网络协议的规范，在隧道机制中将控制网络数据包封装在 IP 包中。本部分的目的是保证使用 IP 信道进行通信的各种 LONWORKS 控制网络设备间的可互操作性。

本部分适用于自动化控制系统及产品的设计、制造、集成、安装和维护等。

2 规范性引用文件

下列文件中的条款通过 GB/Z 20177 的本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB/T 9387(所有部分) 信息技术 开放系统互连 基本参考模型(idt ISO 7498)

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 17963—2000 信息技术 开放系统互连网络层安全协议(idt ISO/IEC 11577:1995)

GB/Z 20177.1—2006 控制网络 LONWORKS 技术规范 第 1 部分：协议规范

RFC 768 用户数据报协议(UDP)

RFC 791 因特网协议(IP)

RFC 792 因特网控制报文协议(ICMP)

RFC 793 传输控制协议(TCP)

RFC 822 ARPA 因特网文本信息格式

RFC 826 以太网地址解析协议(ARP)

RFC 919 广播因特网数据报

RFC 922 子网广播因特网数据报

RFC 950 因特网标准子网进程

RFC 951 引导协议(BOOTP)

RFC 959 文件传输协议(FTP)

RFC 1112 因特网组管理协议(IGMP)

RFC 1122 因特网主机要求——通信层

RFC 1155 基于 TCP/IP 因特网的管理信息结构和标识

RFC 1157 简单网络管理协议(SNMP)

RFC 1212 简明 MIB 定义

RFC 1213 基于 TCP/IP 因特网网络管理的管理信息库：MIB-Ⅱ

RFC 1215 使用 SNMP 定义陷阱的协定

RFC 1305 网络时间协议(Version 3)，规范，执行和分析

RFC 1321 MD5 报文密文算法

RFC 1533　DHCP 选项和 BOOTP 制造商扩展协议
RFC 1541　动态主机组态协议(DHCP)
RFC 1643　与以太网接口类型有关的被管理对象的定义
RFC 1661:1994　点对点协议(PPP)
RFC 2030　简单网络时间协议(SNTP)
RFC 2131　动态主机配置协议(DHCP)
RFC 1157　简单网络管理协议(SNMP)

3　术语和定义

3.1

控制网络　component network;CN

在本部分中,控制网络(CN)也称为设备网络。CN 定义为一个由节点(设备)组成的网络,可以完成计算、探测和执行的功能。通常情况下,这些设备用于控制和遥测等目的的应用,如 HVAC、安防、能源管理、机器控制等。这些设备一般不用来进行数据处理和常规情况下的计算目的。与常规的数据网络相比,CN 具有以下的特性:

a)　通常要求的信道带宽较低;
b)　小的数据包/报文;
c)　对报文的可靠性和处理的响应时间要求高。

3.2

隧道技术　tunneling

将一个协议包封装在另一个协议包的有效负载内传输的一种技术。

3.3

信道　channel

公共通信传输机制,特定控制网络设备集合能共享该机制,并通过该机制互相通信而无需使用路由器。信道用于在控制网络协议栈链路层下传输控制网络包。信道主要是指一些物理媒体类型,例如:电力线、RF 或双绞线,但在 IP 网络情况下,信道不是物理的而是一个协议“隧道”。

3.4

控制网络设备　CN device

任何使用 CN 协议与其他 CN 设备通信的设备。CN/IP 设备通过 IP 信道与其他 CN 设备通信。

3.5

控制网络路由器　CN router

特殊类型 CN 设备,在两个或两个以上的信道间为 CN 协议包选择路由。“CN /IP 路由器”是一个 CN 路由器,只是它为数据包选择路由中至少一个信道是 IP 信道。

3.6

CN 节点　CN node

一个特殊类型 CN 设备,该设备能够发送或接收 CN 协议包,但不能在信道间为它们选择路由。“CN /IP 节点”是一个 CN 节点,只是它接收和发送数据包的信道中至少一个是 IP 信道。

所有 CN 设备或是路由器或是节点,或同时是路由器和节点。

3.7

CN 组　CN group

共享公共多播地址的 CN 设备集合。

3.8

地址解析协议　address resolution protocol;ARP

一个用于将 IP 地址转换成物理地址(例如:以太网地址)的 TCP/IP 协议。希望获得物理地址的主机向 TCP/IP 网广播一个 ARP 请求。在网络上具有该请求中的 IP 地址的主机就以其物理硬件地址应答。

3.9

反向地址解析协议　reverse address resolution protocol;RARP

主机使用这个反向 ARP(RARP)协议寻找其 IP 地址。在这种情况下,主机广播其物理地址,并且 RARP 服务器以该主机 IP 地址应答。

3.10

因特网控制报文协议　internet control message protocol;ICMP

是 RFC792 定义的因特网协议(IP)的扩展。ICMP 支持包含差错、控制和信息报文的包。例如:PING 命令使用 ICMP 测试因特网连接。

3.11

因特网组管理协议　internet group management protocol;IGMP

在 RFC1112 中被定义为因特网上进行多播的 IP 标准。用于在单个网络上建立特定多播组中的主机成员。协议机制允许主机使用主机成员报告向本地路由器通知它要接收对特定多播组寻址的报文。所有符合 IP 多播规范第 2 级的主机都需要 IGMP。

4　缩略语

IP	Internet Protocol	因特网协议
MBZ	Must Be Zero	必须为零
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议
NAT	Network Adderss Translation	网络地址翻译
SNTP	Simple Network Time Protocol	简单网络时间协议
FTP	File Transfer Protocol	文件传输协议
HTTP	Hypertext Transfer Protocol	超文本传送协议
IGMP	Internet Group Management Protocol	因特网组管理协议
IANA	Internet Assigned Numbers Authority	因特网号码分配机构

5　概述

本部分提供使用隧道机理在 IP 网络上传输 CN 数据包的规范,在该隧道机制中将 CN 包封装在 IP 包中。该规范适用于 CN 节点和 CN 路由器。

该规范的主体与 IP 网上传输的 CN 协议无关。对于本部分特定的规范,见附录 A。

可能连接到 IP 网络的 CN 设备和网络的配置见图 2。

图 2 描述两种 CN 设备:CN 节点和 CN 路由器。值得注意的是,图中示出的路由器能够在典型 CN 信道(例如:双绞线或电力线)和 IP 信道之间进行数据包路由选择,或者在两个 IP 信道之间进行 CN 包路由选择。在本部分中,IP 信道的定义方式和其他 CN 信道的定义方式一样。

在图 2 中,IP 网可以被认为是一个或多个 IP 信道。本规范仅说明 CN 包如何在 IP 信道上被传输。本规范没有说明在标准 CN 信道和 IP 信道间如何进行 CN 包路由选择。本规范没有说明标准 CN 或 IP 信道的低层(物理、MAC 和链路层)。

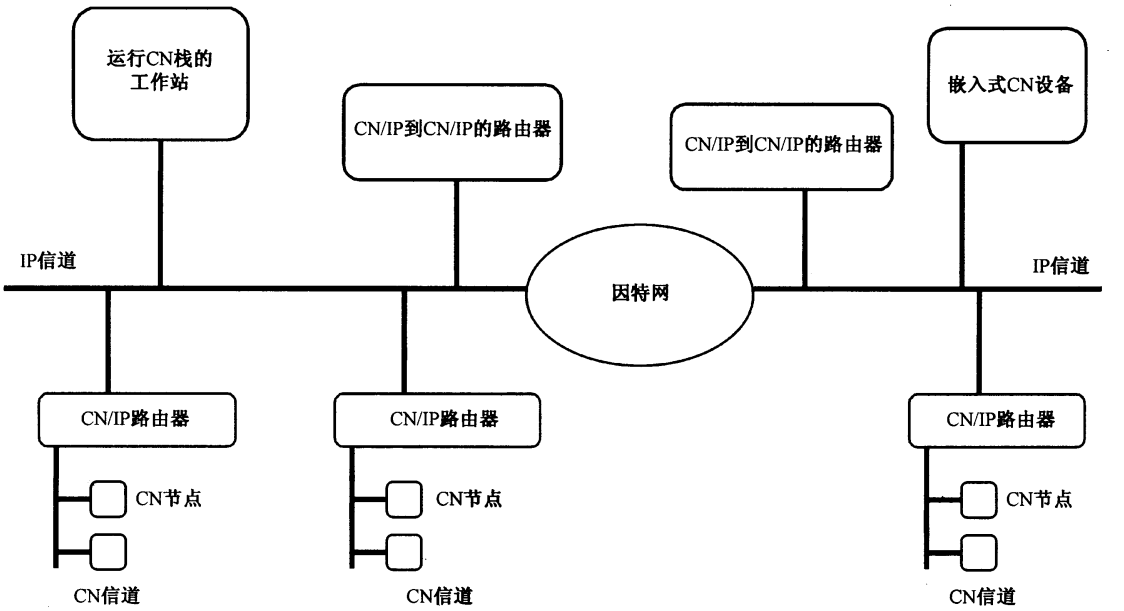

图 2　典型 CN/IP 应用

6　要求

下述是 IP 信道上传输 CN 数据包的通用要求：

——尽可能有效，以便实现准实时操作；

——与用于接收数据包的应用层接口独立，例如：隧道协议不应依赖于套接字接口的存在或如何使用该接口；

——保证保持 CN 包的顺序；

——保证不转发“陈旧”(超出 IP 信道的最大超时)CN 包；

——检测 IP 网中重复的包；

——支持使 IP 包优先的 IP 路由设备；

——防止恶意用户损害设备的可选安全措施；

——可扩展的；

——允许从 CN/IP 设备提取状态信息；

——支持 CN/IP 设备和配置服务器之间的配置信息交换。

7　CN/IP 设备规范

7.1　与 IP 相关的设备规范

CN/IP 必须像任何标准 IP 主机一样操作，能够在相同 IP 子网上或因特网能覆盖到的任何地方，与任何其他 IP 主机交换 IP 数据包。CN/IP 设备必须有单个的单播 IP 地址并可以归属于多达 32 个多播组。CN/IP 设备是否支持多播是可选的。本部分不阐述子网之间或通过因特网的 IP 包路由。CN/IP 设备必须与要求执行 IP 路由功能的任何标准机制(IP 路由器和交换机等)兼容。

7.2　与 CN 相关的设备规范

7.2.1　数据包格式

IP 信道上使用隧道技术的 CN 包通用格式是从 CN 协议栈的链路层(第 2 层)接收的或向其发送的数据包格式。特定 CN 协议的数据包格式的准确规范见附录 A。

7.2.2　编址方式

不同 CN 协议通常使用不同的编址方式交换数据包。为了在 IP 上使用隧道技术传输 CN 包，尽管

通常不需要理解 CN 包的内容或其地址，但在配置过程中会反映出 CN 编址方式的某些方面。当建立 IP 信道时，用于隧道技术传输是非常重要的。因为 CN 协议使用不同编址方式，所以本规范主体部分中用于描述地址的术语是通用的和丰富的，以便能够描述所有 CN 协议中使用的编址方式的超集。本规范中使用下列 CN 编址术语。

——“唯一 ID”：是指在一个特定协议中所有设备具有唯一的标识。实际上，唯一 ID 通常是固定的，在设备的整个生命周期中不改变。

——“域”：是 3 级分层编址方式的最高级。在特定网络中，域 ID 应是唯一的。这就意味着在使用域的特定网络中，如果两个设备有相同的域 ID，那么它们属于相同域，域 ID 通常在本质上是逻辑的，且可以改变和配置。

——子网：是 3 级分层编址方式的中间级。在特定域中子网 ID 应是唯一的。这就意味着在使用子网 ID 的特定网络中，如果两个设备有相同域 ID 和相同子网 ID，那么它们属于相同子网。一些 CN 不使用域，在这种情况下，子网可以是设备地址的最高级。子网 ID 通常在本质上是逻辑的，且可以改变和配置。

——节点：是任何分层编址方式中的最低级。在特定子网中节点 ID 应当是唯一的。在同一子网内不应有 2 个设备具有相同的节点 ID。节点 ID 通常在性质上是逻辑的，且可以改变和配置。

——组：组是与上述域/子网/节点分层编址方式不同的另一种编址方式。组用于报文多播。一些 CN 可以不支持组地址和那些与其他编址方式有关的不同规则的地址。本规范不涉及到这些问题。

上述定义是相当通用的，并作为特定 CN 协议和这些术语配合的指南。一般说来，在 CN 协议内不同编址方式如何工作与本规范无关。只需要了解各个编址术语的含义。

8 IP 信道规范

IP 信道与现存典型 CN 信道不同。典型 CN 信道在本质上是物理信道。这意味着信道上所有设备默认接收所有在该信道上传输的数据包。此外，当将新设备加入到信道时，没有必要使该信道上的其他设备在交换数据包之前就知道该设备。为了在信道上传输数据包，设备必须能够在信道上以物理方式传输数据包。如果一个设备以简单的物理方式连接至信道，该设备就能够与信道上的其他设备交换数据包。

与之相比，IP 信道实质上不是物理信道，而是逻辑信道。有一些支持 IP 通信的不同物理媒体，其中任何一种媒体应能够支持 CN 信道。因为我们正在描述逻辑信道，所以必须“构建”信道，通过向信道上的每个设备通知该信道上有其他设备的存在。换句话说，在设备可以将数据包传输给 IP 信道上的其他设备之前，它必须知道如何将一个数据包发送给该设备，即：其 IP 地址。

物理信道和逻辑信道之间的另一个重要区别为：在典型物理信道上，当数据包在信道上传输时，能够计算数据包从一个设备到另一个设备所需时间的固定上限。对于 IP 网络，有时是不可能的。IP 网上 CN 设备之间的数据包传递时间偏差远大于典型 CN 信道上的数据包传递时间。

如图 2 所示，各种 CN/IP 设备使用 IP 信道作为 CN 包的中间传输机制。当在 IP 信道上传输 CN 包时，将封装 CN 包的 IP 报文发送给 IP 信道上其他 CN/IP 设备。CN/IP 设备接收到一个 IP 报文时，提取和处理 CN 包。单个 IP 报文可以包括多个 CN 包。因此，必须以允许提取单个 CN 包的方式格式化 IP 报文。这种情况称为包“重组”。CN/IP 设备必须支持重组包的接收。同样地，必须以重组 IP 报文中包含的每个 CN 包是完整的方式进行重组，即：重组结果不应使 CN 包超过 IP 报文边界。另一个要求是，中间 IP 设备能够分开已重组的 CN 包并在转发前以不同方式将其重组。

单播 IP 地址列表规定 IP 信道，每个 CN/IP 设备对应一个 IP 地址。在单个 IP 信道上，CN/IP 设备数量没有上限。

如果 IP 信道上的每个 CN/IP 设备含有该 IP 信道上每个其他 CN/IP 设备的单播 IP 地址列表，这

就是实现 CN 包隧道技术所需的。在大部分情况下，对于 IP 信道上转发的每个 CN 包，必须强制在信道上向每个 CN/IP 设备发送单独的单播 IP 报文。这种情况不能灵活变化，因此使用下列技术减少 IP 流量：

——IP 多播组；

——选择性转发。

IP 多播组允许将单个 IP 报文发送至多个 CN/IP 设备。因此，IP 或 CN/IP 信道的完整定义应不仅包含信道上所有 CN/IP 设备的单播 IP 地址，而且还包含它们所属的 IP 多播组。每个 CN/IP 设备能够属于多达 32 个多播地址。

选择性转发是指在转发 CN 包之前检查其内容，以便决定是否应将其发送至一个特定 CN/IP 设备。为了进行这个动作，必须知道每个潜在目的地的附加 CN 特定信息。如果 CN/IP 设备是一个路由器，那么实现选择性转发的必要信息是该 CN/IP 路由器的路由列表。如果设备只是一个节点，那么应知道该节点所属的域、子网、节点 ID、唯一 ID 和 CN 组。因此，所有这些信息都是完整 IP 信道定义的一部分。简言之，一个完整 IP 信道定义包含了与 IP 信道上将数据包转发至其他 CN/IP 设备有关的所有已知信息。这就是有关 IP 信道知识的全部。

强调指出，不管 IP 或 CN/IP 设备使用哪种转发方式，下列条件成立：

——CN 协议包一直由 IP 信道上的所有 CN/IP 设备接收，不管这些 CN/IP 设备是路由器或节点。当 CN/IP 设备应接收 CN 包时，如果出现不确定或不清楚的情况，那么应根据设备的特定实施策略决定可以或不可以丢弃该数据包。设备可以将数据包转发至信道上的所有设备，或者简单地将其丢弃并不转发至任何设备。

——除非由于 CN 协议栈链路层上的一些重试机制，不应将特定 CN 包两次发送至相同 CN/IP 设备。由于 IP 网络性质，可能发生这样的情况：CN/IP 设备可以接收重复的 IP 报文，但不应是从另一个 CN/IP 设备多次传输报文的结果。

此外，如果根据某些标准构成组，那么可以在多播组中进行选择性转发。例如：多播组“A”可以包含所有属于域 ID“W”的 CN/IP 设备。如果一个 CN 包发往域“W”，那么仅将它转发至多播组“A”就足够了。为了在多播地址上进行选择性转发，必须知道这些组是否根据一些准则构成。

当认识到完整 IP 信道定义难以被使用和维护时，不要求 IP 或 CN/IP 设备使用它转发数据包。在每个 CN/IP 设备中能够保持另一种被称为“发送列表”的数据结构。发送列表可以同时包含单播地址和多播地址，并且是服从于上述相同条件。它可以使用第三方配置工具创建并装载至 CN/IP 设备，该配置工具更适合根据一些准则创建多播组。发送列表表示正确转发 CN 包所需的最小信息量，构建发送列表简化转发过程，以便 CN/IP 设备仅需要将数据包转发至发送列表上的每个地址（单播或多播）。为了允许 IP 或 CN/IP 设备能转发数据包至列表中的每个地址，必须满足下列条件：

a) CN 协议包必须被所有需要接收 CN 协议包的 CN/IP 设备接收，不管这些设备是路由器或节点。

b) 不能将特定 CN 包两次传输至相同 CN/IP 设备。

c) 如果设备 A 是设备 B 发送列表中的目的地，那么设备 B 应是设备 A 发送列表中的目的地。这对于支持 CN 协议的确认服务是必需的。

通过将特征和列表中多播表项结合起来，使用发送列表实现简单形式的选择性转发是可能的。

值得注意的是，一般说来，IP 信道定义表示 IP 信道的完整全局信息，而发送列表是根据一些特性从设备智能组合产生的。发送列表的主要目的是使 CN/IP 设备高效运行而不需要它们深入处理完整信道定义列表。更值得注意的是，发送列表是 IP 或 CN/IP 设备的配置属性，意味着通过显式配置过程可将其控制并输入到一个设备中。尽管发送列表是一个配置属性，但它不能阻止 IP 或 CN/IP 设备进行自身配置和计算自身发送列表。

为了严格控制 CN/IP 设备的行为和它们如何转发数据包，应能够配置 IP 或 CN/IP 设备，以便使

用显式发送列表，忽略任何 IP 信道配置信息。

8.1 IP 传输机制

IP 是图 3 所示的网络层协议，设计成运行在多种物理媒体和链路层协议之上。因此，本部分没有对 IP 栈的链路层或物理层作任何规定。

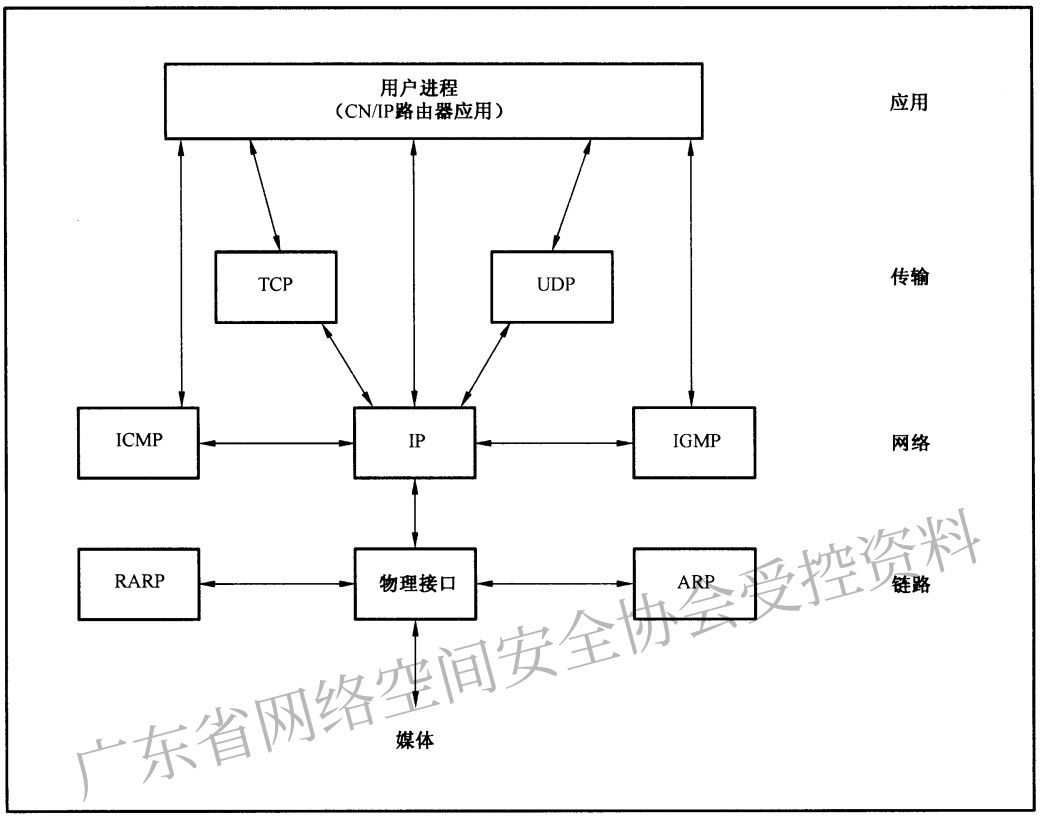

图 3 IP 协议栈

如图 3 所示，下列是 3 个用于传输 IP 包的最通用机制：

——原始 IP；

——TCP；

——UDP。

TCP 和 UDP 是基于 IP 的传输协议。关于 CN 数据报文的传输，假定 UDP 能增强效率并且支持多播寻址，它可用于 CN/IP 设备之间的通信。所有 CN/IP 设备必须支持 UDP。在配置过程中使用 TCP 有一些优点，并且 TCP 可以支持 UDP 之外的某些报文。CN/IP 设备中的 TCP 支持是可选的。

为了阐述顺序问题，在数据包的首部上加一个顺序号，以便有助于排序。所有 UDP 数据报必须带着有效的“校验和”传输。

为了通过 TCP/UDP 发送一个数据包，除 IP 地址外，必须定义一个端口号。一般来说，端口号是可配置的，并用于下列定义的不同目的。

本部分推荐使用的端口号见附录 A。

当使用 UDP 时，可使用单播或多播寻址发送数据报。单播是点到点的，这就意味着将数据报从一个 IP 主机发送到其他单个 IP 主机。当发送相同数据报到多个 IP 主机时，使用多播寻址更为有效。因此，建议 CN/IP 设备支持单播和多播寻址。IP 信道是由 IP 地址列表定义的。信道定义或发送列表可包含单播地址和多播地址的任意组合。为了与 IP 或 CN/IP 设备相互操作，IP 或 CN/IP 支持多播是不要求的。

为了使 IP 或 CN/IP 路由器在整个 IP 路由器上使用多播寻址，CN/IP 设备必须向 IP 路由器通知加入多播组的意图。有成熟的方法进行这种操作，本部分不对这种方法进行规定。

8.1.1 注意事项(资料性)

一些 IP 网包含 NAT 路由器。除非专门设计路由器，否则这些路由器不能处理将 IP 地址嵌入有效载荷中的协议，这同样适用于本部分规定的隧道协议。一般来说，该协议不能在所有 NAT 路由器上工作。只要有一个能处理该协议的路由器，该协议仍可用于使用 NAT 路由器的网络。它可以是 NAT 路由器本身或在网络相同区域作为 NAT 路由器的另一个 CN/IP 到 CN/IP 路由器。

9 CN/IP 设备配置

CN/IP 设备有双重特性。从 CN 观点来看，它是 CN 信道上的节点，并具有一切应有特征。可以使用标准 CN 网络管理程序和报文配置，并管理这些参数。

从 IP 观点来看，CN/IP 设备是 IP 网络上的一个 IP 主机，因此它必须像 IP 网络上的任何其他主机一样被配置。

此外，还有与该 CN/IP 设备一起定义的逻辑 IP 信道配置信息。

本章只描述与配置 IP 主机和 IP 信道参数相关的要素。

一般来说，一系列技术和协议可用来配置所有 IP 主机和信道参数。所有 CN/IP 设备必须至少支持对该设备转发机制的手工配置，以便保证可以用不同方法配置的设备之间的最小等级可互操作性。转发意味着通过如上所述的隧道技术发送到 IP 信道上其他设备。

9.1 配置参数

本条定义 CN/IP 设备用于(或可以用于)操作的参数。本条不定义用于存储信息的数据结构或定义用于数据交换的报文。本条集中定义和标识了所有 CN/IP 设备参数。本条还讨论设备之间传送信息的机制。

有三个相关数据集，该数据集构成 CN/IP 设备中所包含的参数。

——第 8 章中描述的 CN/IP 信道定义。

——第 8 章中描述的发送列表。

——与 CN/IP 信道上的设备相关的设备参数。

9.1.1 信道定义参数

完整信道定义在逻辑上是信道上每个 CN/IP 设备的列表。信道上每个设备可与下述类型信息有关系。

——多播支持(是或否)。因为这是可选的，所以必须有是否支持的指示。

——TCP 支持(是或否)。因为这是可选的，所以必须有是否支持的指示。

——CN/IP 设备类型(路由器、节点、代理等)。

——CN 路由器类型(中继器、自学习、配置等)。

——CN“要求所有广播”标志。

——名称。用于识别的简单文本字符串。

——信道超时。该参数对信道而言是全局性的，每个设备有这个值，但对所有设备相同。

——IP 地址。这是设备的单播 IP 地址。

——侦听数据的单播端口。

——CN/IP 设备侦听的多播地址/端口号对的列表。

——CN 特定唯一设备 ID1(路由器近侧或节点)。

——CN 特定唯一设备 ID2(路由器远侧)。

——CN 特定唯一设备 ID3(用于辅助配置的)。

——每个域的 CN 域长度和 ID、子网、节点地址。

——对节点特定的参数为:CN 组成员信息。

——对路由器特定的参数为:CN 路由表。

注:这个列表实质上是有代表性的。在本部分后续章节中讨论所要求的全部细节。

在规范中定义的隧道协议不需要任何特定 CN 寻址方式。支持下列 CN 地址类型:

——唯一设备 ID;

——域 ID;

——子网 ID;

——节点 ID;

——组 ID。

与上述地址类型相应的特定编址规定见附录 A。

9.1.2 发送列表参数

下列参数用于定义发送列表:

——单播 IP 地址和端口列表;

——多播 IP 地址和端口列表。

9.1.3 设备参数

——IP 网关地址;

——IP 子网掩码;

——配置服务器 IP 地址/端口;

——SNTP 服务器 IP 地址。

9.2 配置技术

本条描述可用于设置上条定义的参数的各种方法。

这些参数可用许多方法设置。CN/IP 设备不需要支持所有这些方法,但如果它支持任何一种方法,那么它应以标准方式支持。

9.2.1 手工配置

手工配置不需要配置服务器。所有要求的信道定义参数、发送列表参数以及设备参数必须是手工输入的。没有标准方法进行这种操作。这是由厂商专门规定的,可用下列任何一种方法完成:

——配置文档;

——终端接口;

——Telnet 接口;

——FTP 文档传输;

——HTTP 接口。

9.2.2 BOOTP 和 DHCP

9.2.2.1 背景

有两种机制使设备获得 IP 地址而不需要预先配置:DHCP 和 BOOTP。

DHCP 实际上是 BOOTP 和 BOOTP 服务器端的扩展,它遵守 RFC951,能理解来自 DHCP 客户端的报文并对这些报文正确地响应。

系统启动时,发送 DHCP 请求向 DHCP 服务器请求 IP 地址。DHCP 服务器端以一个有效的、DHCP 客户端目前可使用但尚未使用的 IP 地址响应。

9.2.2.2 符合性

符合本规范并希望获得 IP 地址而不需要预先配置的设备必须成为一个 DHCP 客户端,并可以成为 BOOTP 客户端。

9.2.3 配置服务器

希望 CN/IP 信道上的设备尽可能是“即插即用”的。假设给出了 CN/IP 设备用于操作的大量配置

信息，希望有一种机制将其分配，以便不需要将其单独输入各个设备。允许这种机制工作的设备被称作配置服务器。

使用配置服务器的设备必须与不使用配置服务器的设备相互操作。然而，配置服务器不需要支持本规范中描述的所有交互作用。特别是不必支持信道路由数据包。

配置服务器使用 IP 报文自动配置 CN/IP 客户。一般来说，配置服务器可以支持下列功能：

——不同客户 CN/IP 参数的配置。

——将 IP 信道定义和发送列表分配给 CN/IP 设备。信道列表描述整个网络，而发送列表对于每个 CN/IP 设备是唯一的。

——通过检测 CN/IP 设备何时在线和离线，自动维护信道定义列表。

除 9.1 描述的参数外，CN/IP 还必须具有配置服务器的 IP 地址和使用配置服务器通信的端口。

当上电、复位和设备信道定义列表中的参数改变时，CN/IP 设备必须发送一个设备注册报文给配置服务器。

本条没有规定服务器如何管理分配给用户的参数列表。事实上，应使用任何期望的管理方法来维护这些参数。当客户端在线和离线时需要服务器有能力动态建立和维护参数。为达到这个目的，配置协议和报文格式将被设计成允许服务器支持这个功能。

10 CN/IP 报文和操作方式

本章目的是：

——规定 IP 信道上 CN/IP 设备之间可交换的所有报文；

——定义报文内容；

——规定协议和设备交换报文时的动作。

第 11 章将规定本章中定义报文的准确数据包格式。

CN/IP 设备使用 IP 信道用于各种目的和操作方式。本规范的各章分别讨论每种情况。操作方式包括下列内容：

——交换(使用隧道技术)CN 数据包；

——与配置服务器交换配置信息；

——多种状态报文；

——厂商特定的报文和协议。

对于每种操作方式，将定义一个 CN/IP 设备之间交换的报文集。

10.1 通用报文首部

每个由 IP 信道上设备交换的 IP 报文的开头有一个固定首部，该首部带有对所有 CN/IP 报文通用的格式。该首部包含下列字段：

——版本；

——协议标志；

——厂商代码；

——包类型；

——数据包长度；

——首部大小；

——会话 ID；

——序列号；

——时间戳；

——安全密钥。

在第 11 章中描述具体报文格式。

假设具有相同版本号的所有数据包总是可以被解析。如果接收到一个版本号未知的数据包，应丢弃这个数据包不进行进一步处理。

协议标志规定有关数据包的信息，例如：将哪个 CN 协议包封装在报文中以及是否使用安全机制发送报文。

厂商代码允许厂商特定的数据包。对根据本规范规定的标准定义的所有数据包，应设置该值为 0。通过唯一厂商代码（除 0 以外）部分地识别厂商特定数据包。

将唯一数据包类型代码分配给 11.1 所述的每项功能。本规范中定义的标准数据包类型代码的范围为 0x00 至 0x7F。本规范定义的作为标准功能扩展用于传递信息的厂商特定包，可以作为标准功能使用相同数据包类型代码，然而厂商代码必须设置成对应该厂商的唯一标识符。与本规范中定义的现有标准功能无关的厂商特定代码必须使用 0x80 至 0xFF 范围中的包类型代码。

数据包长度和首部大小分别规定包大小和首部大小。

会话 ID 与序列号一起，使出现重复序列号的概率最小。

时间戳用于检测“陈旧”数据包，它基于和 CN/IP 信道上所有设备间同步的时间基准，像 10.3.3 定义的那样。

安全密钥用于保护 10.7 描述的数据包。

所有 CN/IP 报文可以使用 UDP 数据报发送。每个 UDP 数据报可以包含一个或多个 CN/IP 报文。如果在单个 UDP 数据报中有多个 CN/IP 报文（重组），那么每个报文将有其自身的首部。因为每个首部具有报文大小信息，所以能够分别提取每个报文。

所有 CN/IP 设备必须支持包重组。图 4 描述了单个 UDP 数据报中的多个 CN/IP 报文（包重组）。

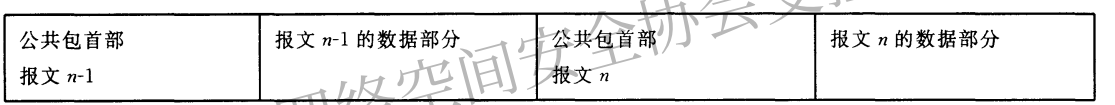

图 4　包重组

某个 CN/IP 报文可以越过 UDP 数据报边界。在这种情况下，定义了用于方便传输的特定分段协议。越过 UDP 数据报边界并使用特定分段方式的报文一定不能与其他包重组。

10.2　包分段

10.2.1　概述

某个 CN/IP 数据结构配置请求的响应比单个 UDP 中要携带的数据多，由于每个 UDP 包有效载荷最多 548 字节。本段描述了能够传输这些数据结构的通用方法。值得注意的是，这种方法不能防止在分段传送中，整个数据结构的某些部分发生变化时，数据本身出现偏差。在本协议的所有配置响应包定义中，采用以下两种方法之一：专门定制响应包格式以便消除对数据偏差的敏感性；或提供一个能检测潜在的数据偏差的简单方法。

该协议包括 SEGMENT（分段）包类型。任何其他配置包类型可以作为一系列分段包中的有效载荷被携带。选择有效载荷包的字节序列，以便将最后形成的分段包装入到一个 UDP 帧中，并提供这些段作为响应。如果将请求的包装入到 UDP 帧中，那么它就可被发送而不用封装。

以分段包形式发送的包被完整地发送。这就是有效载荷包具有通用包首部，该首部带有有效载荷包的包长度。所有分段包具有相同的包类型。

为了便于使用这种方法，每个调用配置响应的配置请求包应包含一个分段 ID 字段，并且每个分段包应在标志字段中包含一个有效比特和一个最终比特以及一个日期指示器。

——请求 ID 字段是由应答服务器从“对分段包的请求”中复制的。它表示请求源应用的标志值，以便它可以唯一地识别出请求的响应。因此，多个请求就可以同时离开至相同目的地。请求 ID 字段是 16 比特，以便请求号以外的任何设备信息都可用一种执行相关方式包含在该字段内。

——分段 ID 是完整数据结构中局部数据块的参照符。参照第 1 个局部数据块的分段 ID 是 0x0。

——分段包中的有效比特表示与被指示分段 ID 有关的包中数据的有效性。有效比特置位意味着数据是有效的。有效比特被清除意味着对于被指示的分段 ID 没有有效数据。

——分段包中的最终比特表示在分段 ID 值大于该包中返回值的结构中有附加数据，最终比特置位表示没有附加数据。

——日期时间指示器用于检测已获得的数据偏差。该字段表示何时一个特定数据结构有效。它不是数据何时请求传输的指示器。对于对其敏感的配置数据来说，可以通过比较每个代表完整数据结构的响应包中返回的日期时间段检测数据偏差。如果在所有包中日期时间字段不相同，那么表示已获得数据的某些部分发生了偏差。在 11.5 中规定日期时间字段的格式。

10.2.2 分段交换

获得配置数据的典型方法如下：

a) 请求节点发送一个分段 ID=0 的请求包。它可以可选地设置 REQUEST_ALL 标志，以便指示所有分段包将被发送而不需要等待附加请求包。

b) 如果响应报文恰好装入一个帧中，那么发送该帧。当接收方接收到请求类型的包时，它撤回请求 ID 并处理响应。

c) 如果响应包无法装入单个帧中，响应节点发出一个分段包，该包的分段 ID 等于请求包的分段 ID。此外，如果该分段没有数据，那么就发送响应包，最终比特置位、有效比特被清除。如果该分段出现数据，有效比特置位。此外，如果在已指示的分段 ID 以外出现更多数据，那么将当前包的数据部分充满到它最大容量，并且最终比特标志被清除。

d) 如果请求节点并没有接收到响应，那么请求报文就被重复发送，直到接收到响应为止。重复间隔以指数方式增加，最长间隔为 30 s。

e) 请求节点检查响应报文的标志字段。如果有效比特被清除，那么剩余的响应包就可被忽略。转入步骤 g)。

f) 如果有效比特为真，那么数据被处理。如果检测出数据偏差，那么检验日期时间字段。

g) 如果最终比特置位，那么该数据结构的请求序列就被终止，并且已获得的结构被标记为有效。

h) 如果最终比特被清除，那么发送另一个请求包，该包的分段 ID 等于前一个请求包的分段 ID 加 1。从步骤 c)继续该过程。如果任何接收到包的日期时间都不相同，那么从步骤 a)开始这个过程。

用任何分段 ID 值来开始数据结构采集是同样有效的，然而分段 0 的请求通常产生带有有效数据的响应。即使请求以非 0 分段开始，如果将响应恰好装入单个 UDP 帧中，那么响应不使用分段包，但仅以响应包进行响应。

当请求节点已接收到一串分段包时，且所有分段包中都带有完整的分段 ID 集和相同日期时间，它组合有效载荷包并对其加以处理。如果任何部分有不同的日期时间，那么将丢弃整个集，并从步骤 a)重新开始这个过程。因为响应可以包含具有完整的新日期时间的段，所以不保存任何段。

10.2.2.1 请求 ID 值

服务器从不发送未被请求的分段包。

请求 ID 值在请求包中被从设备发送到服务器，并且其值完全受请求设备的控制。被请求的 ID 可以是包括 0 的任何值，它将在服务器发送的段包中被复制。对于同时活动的请求，请求 ID 值必须是唯一的。如果该值不是唯一的，那么在服务器中另一个段的请求将是不明确的。在这种情况下，服务器的行为是未定义的。

10.2.3 实施要求

本段进一步详细描述了分段过程。同时还描述了这个设计的体系结构含义以及服务器和设备的实施要求。

10.2.3.1 目的和范围

这个分段方案使任意格式的包能在链路上以有限的帧长可靠地交换。在一个分段序列被接收后，将每个分段的有效载荷连接起来形成字节流，该字节流被认为是数据包。这个数据包包含另一个带有包类型码和包长的通用包首部。

未来任何数据包都可以用同样方法被封装和分段。在通用包首部中不要求附加字段，在每个当前或未来的包格式中也不要求附加字段。

包分段目的不专门应用于数据包。

包分段可按任何顺序被请求，也可重复请求，如果服务器以带有相同日期时间的包进行响应，那么每个有同样日期时间和分段 ID 的响应必须包括与其他任何这类响应相同的字节。

10.2.3.2 服务器实施要求

服务器中的各种实施要求能保证日期时间字段指明请求 ID 的包序列是固定不变的。其中有：

——在任何不满足的请求存在期间锁定数据库，并在前一个请求结束时更新数据库。

——保留请求数据快照，如果最终包已被发出，或者由于没有完成请求/响应序列而超时，那么，该快照过期。

10.2.3.3 设备实施要求

设备中的各种实施要求能保证未完整应答的请求不继续消耗资源。其中有：

当分段到达时，将其隔离，并当下述情况发生时，收回这些段和控制数据：

a) 发生超时表明服务器没有应答请求(在适当重传后)。

b) 适当非分段包的响应表明已满足请求。(没有将显式请求 ID 字段加入到包首部上，但该状态是无歧义的，因为设备仅与单个配置服务器通信，所以不需要该服务器支持多个同样类型的更新请求。)

c) 分段包序列已被接收，带有正确请求 ID，所有分段包序列带有相同日期时间。将这些分段的有效载荷解码成一个数据包，该包是对请求的响应。

10.3 数据包交换

本条定义如何在 IP 信道上交换 CN 数据包。本条明确地定义如何将 CN 包转发到另一个 CN/IP 设备。本条没有说明如何决定转发 CN 数据包至哪个 CN/IP 设备。假设这个决定是使用 IP 信道定义或发送列表做出的。为了便于讨论，定义“转发”列表为接收特定 CN 数据包的 IP 地址列表。值得注意的是，转发列表包含单播 IP 地址和多播 IP 地址。如何确定这种转发列表与下述讨论无关。

因为 CN 使用端到端的确认服务，所以作出下列假设：

——不必将确认加入至被转发的 CN/IP 数据包；

——不必重发被丢失的 IP 包。

另一方面，为了 CN 正确操作，必须满足下列条件：

——必须保持 CN 包的包排序；

——CN 包的发送方不能将多个 CN 包的复制发送到 CN/IP 信道上每个其他设备；

——接收方必须检测重复的 CN/IP 包，并不能将其转发；

——信道上超时的包不能被转发。这些包被称作“陈旧”包。

使用基于 UDP 的隧道技术在 CN/IP 设备间相互交换 CN 数据包。将带有首部的每个 CN 包封装到 UDP 数据报中。将首部和 CN 数据包有效载荷的组合称为“CN/IP 数据报文”。首部的部分被称为 CN/IP 数据报文首部，而 CN 数据包被称为 CN/IP 数据报文有效载荷。值得注意的是，单个 UDP 数据报可以包含多个 CN/IP 数据报文。

假设特定转发列表 IP 或 CN/IP 设备简单地使用 UDP 将相同 CN/IP 数据报文转发到列表上的每个地址。因为 IP 网络和 UDP 简单转发的特点，所以报文将不能保证目的地主机没有接收到重复的、失序的或陈旧的包。因此，CN/IP 数据报文的发送方必须包括附加信息，以保证接收方能适当地处理每

种状况。下面阐述这些内容。

10.3.1 失序包

接收方不能转发已检测为失序的包，CN/IP 设备应该设法将接收到的包重新排序，以便纠正排序问题，但如果知道它们失序，那么决不应该转发它们。如果不支持或不可能重新排序，那么这些数据包必须被丢弃。

应该使用下列算法保证接收方不转发失序的包。

——对于每个数据包 IP 目的地地址，每个 CN/IP 数据源含有一个会话 ID(SID)和一个无符号 32 位包序列号(PSN)。每个通过数据源发送至特定 IP 目的地地址的 CN/IP 数据报文包含这个 SID/PSN 对。在报文被发送之后，每个 PSN 加 1，而 SID 在连续 CN/IP 数据报文之间不发生变化。对于 CN/IP 将报文发往的各种 IP 目的地地址，SID 可以是公共的。

——如果 CN/IP 设备正在对特定目的地地址发起新“会话”(即：在上电或重启之后)，那么它必须使用与前一个已被使用 SID 不同的 SID。一般来说，对于连续报文，SID 保持不变，而 PSN 增加。

——PSN 的取值从 0xFFFFFFFF 回至 0x00000000。因此，设 X 和 Y 为 PSN，可以得出：假设使用无符号 32 位算法，如果(X－Y)＜0x80000000，那么 X＜Y。

——对于每个接收数据包的 IP 源地址/目的地地址(SA/DA)对，每个 CN/IP 数据接收方提供“前一个转发序列”号(LFS)。

——设置每个 SA/DA 的初始 LFS 值为 SA/DA 刚接收到 CN/IP 数据报文的 PSN，如果下列任何一个条件成立：

a) 在启动数据接收设备之后；

b) 如果 SID 与从 SA/DA 接收到的前一个 CN/IP 数据报文不同。

——数据接收设备接收 PSN＝LFS＋1 的 CN/IP 数据报文引起数据包被转发，LFS 增加 1。

——数据接收设备接收 PSN＞LFS＋1 的 CN/IP 数据报文可以造成包被保持在等待状态，等待所有其他(LFS＋1)＜PSN＜(第 1 个被保持等待状态包的 PSN)包的到达和顺序转发。

——如果满足如下两个条件：数据接收设备中有被保持等待状态的包存在；第 1 个被保持等待状态的包被接收后的时间大于信道超时时间(小于极大值 1.5 秒)，那么所有在间隙中的 PSN 在(LFS＋1)和(第 1 个被保持等待状态的包的 PSN)之间的包将放弃等待。设置 LFS 等于第 1 个被保持等待状态包的 PSN-1。下一个序列的包的转发继续进行，不管被保持等待状态或正在传输中。

——数据接收设备接收到的 PSN＜(LFS＋1)的 CN/IP 数据包作为重复包被丢弃。

——来自一个 SA/DA 的 CN/IP 数据包被保持在等待状态，并不影响来自另一 SA/DA 的 CN/IP 数据包的转发或被保持在等待状态。

10.3.2 重复包检测

检测确定为重复的包必须由接收方丢弃。这种情况可以使用与 10.3.1 中保证排序相同的算法来完成。

10.3.3 陈旧包检测

CN/IP 设备必须能检测陈旧包。CN/IP 设备还必须支持关闭陈旧包检测的能力，因为在某些情况下陈旧包检测是不必要的，例如，单段以太网 LAN 中没有 IP 路由器造成网络通信业务量的未知延时情况。假设启动了陈旧包检测，被检测为陈旧的包必须由接收方丢弃。如果一个包从发送方传输到接收方的时间大于信道超时时间间隔(CTP)，该包即被认为是陈旧的。CTP 表示包在 IP 信道上从发送方到接收所需时间的合理上限。本部分并不叙述信道超时时间间隔是如何确定的。值得注意的是，它的单位是毫秒，并且 IP 信道上每个 CN/IP 设备都知道。单个超时时间间隔适用于信道上的每个 CN/IP 设备。

为了使设备能检测何时包已陈旧，必须确定包传输到IP信道上以后经过了多少时间。在本部分中规定的方法是：在包转发到IP信道上之前由发送方给每个数据包分配一个时间戳。在CN/IP到CN/IP路由器的情况下，包在转发到下一个IP信道之前要以最新时间重新打印时间戳。在将包转发到相同IP信道上的代理节点的情况下，包就不重复打印时间戳。同时应注意的是：所有接收到特定包的CN/IP地址必须有相同的时间戳。

为使时间戳有效，IP信道上的所有设备必须保持时钟同步。同步精度并未规定。根据所用的IP网络类型，可用的精度范围是很广泛的。值得注意的是，时间同步的任何不精确将反映在利用隧道技术协议的传输延时抖动上。在本规范的相应附录中叙述与特定协议相关的范围。

使全体CN/IP设备时钟同步的方法是RFC-2030中规定的SNTP。这就意味着IP网络的某个地方有一个SNTP时间服务器并且CN/IP设备已被配置成可访问其IP地址。RFC-1305规定的时间戳的格式是32位整数秒和32位整数皮秒。该格式没有对符合要求的精度和算术属性进行定义。因此，在本规范中时间戳的格式是32位毫秒。它与当前SNTP时间是一致的。时间戳每隔49.7天复位一次。

只要与时间服务器维持着通信，那么设备始终应同步，并且可以正常进行陈旧包检测。如果与时间服务器的通信由于某种原因中断，那么将会出现问题。在这种情况下，设备可以继续转发包，只要确信其时钟与网上其他设备的偏差未超出范围。因为时间服务器是网络上时间的公共参考，所以设备就可以继续转发包，只要确信在离线之前其时间是在时间服务器的容差范围内。如果设备知道它自己的时钟偏差率，那么这是能够做到的。如果设备不能估计自己的时钟和网络上其他设备的时钟容差范围，那么它不能将包转发到IP信道上。

虽然NTP时间的分辨率是基于皮秒(ps)，但是系统中时间的实际精度是以计时器的中断来计算，通常为10ms或16ms。时间戳的精度为毫秒(ms)，但是低3位或4位是没有值的。这意味着取整或舍位不是一个问题。同样地，值得注意的是：CN的最小接收事务定时器值是128ms，因此，两个时间戳之间的微小差值是无关紧要的。

10.4 配置服务器交互作用

10.4.1 通用设备交互作用

下列是CN/IP设备(客户端)和配置服务器之间的会话操作：

a) 设备发送一个注册报文到配置服务器。该报文中包含一些配置参数。该报文不断重发，直到从服务器接收到响应为止。重发时间间隔以指数方式增加，最大达到30s。如果设备具有有效配置，那么当设备等待来自服务器的响应时，设备可以利用该配置为报文选择路由。

b) 服务器必须用两个可能报文中的一个进行应答。如果不希望在信道上增加客户端，确认报文含有值ACK_DEVICE_REFUSED；或者设备配置报文包含某些配置参数。服务器没有重发确认包。如果设备没收到它，那么设备将重发原始请求。

c) 设备必须确认它接收到步骤b)中向它发送的设备配置报文。确认报文可能有各种值：值ACK_OK表示设备接受配置，值ACK_FIXED表示设备有固定配置，值ACK_BAD_MESSAGE表示接收到的报文已被破坏，值ACK_CANT_COMPLY表示设备不能使用该配置参数。

d) 注册后，设备可以向服务器发送一系列请求报文。

e) 服务器必须以合适的响应报文应答这些请求。

本部分中没有规定服务器如何响应不同的确认，但服务器应记录该报文以方便调试。

10.4.1.1 来自服务器的主动包

服务器可以发送一个未请求的设备配置报文到一个设备。设备以上述同样方法确认该报文。最佳实施方法是：服务器应避免使带有主动包的在线设备超负荷，直到设备结束发送请求包为止。实施细节是选择问题。其他配置包从不以未请求方式被发送。以未请求方式发送的设备配置报文从不被分段。

来自服务器的未请求设备配置报文用于向设备表明信道配置的某些部分已发生变化。设备配置报文中的日期时间字段在这些报文中是有效的，并且表明最新发送列表和信道成员列表包的日期时间。在将这些日期时间与设备当前存储的包日期时间比较之后，设备必须从服务器请求信道成员列表、发送列表和信道路由包，以便获得最新版本。

CN/IP 信道配置可以是静态的，即使使用了配置服务器。事先知道配置并固定在配置服务器中就是这种情况。这是理由之一，说明为什么服务器可以用 CN/IP 设备拒绝的报文应答客户注册报文。与服务器一起注册的设备可以不是固定配置的一部分。服务器决定以什么方式应答客户注册报文是厂商特定的。

10.4.1.2 来自设备或其他节点的请求

设备必须应答来自其他节点或设备的请求。除了分段以外，没有为其他设备请求的数据或不是设备、服务器的节点提供保证。通过分段，保证意味着各系列包将有相同日期时间和固定字节集。设备必须在和服务器通信方面保持全局完整性。

例如，对于信道路由包来说，如果设备(A)响应另一个设备(B)，并且在交换信息期间，设备(A)路由信息改变，设备(A)不负责通知设备(B)它不能对设备(B)响应或通知设备(B)通过改变日期时间表明数据已经改变(除非在交换期间数据的剩余部分是来自已改变的数据集)。设备(A)的唯一全责是向服务器通知更新的信息。

设备不负责应答或处理来自服务器设备以外的其他设备的主动配置报文。它们必须应答来自设备而不来自服务器的主动的请求报文。这就意味着，如果设备接收到来自服务器以外节点的主动的信道成员列表、发送列表、信道路由或设备配置报文，那么设备可以将它们丢弃。

10.4.1.3 日期时间

所有配置包都含有日期时间。它是数据有效的日期和时间。可以用 1 秒的分辨率通过寻找字段确定该数据的新或旧版本。字段是受到约束的，以便如果在同一秒内多个数据版本被创建，那么它们具有该字段的唯一递增值。

如果网络支持 SNTP 或 NTP，日期时间值是 RFC-1305 中 NTP 数据时间的秒部分。它是 1900 年 1 月 1 日以来的秒数量。该时间将在 2036 年结束。详见 RFC-2030 的第 3 章。

如果网络不支持 SNTP 或 NTP 协议，日期时间可以是一个不包括 0 的小整数。在 20 世纪早期，这些日期时间显然不是壁钟的时间，而是受到约束的，以便要服从上文提到的在所有时间内都是唯一的要求。即这样设备发送的数值永不重复。

日期时间是以 UTC(格林尼治通用时间)或与其相当的 GMT(格林尼治标准时间)表示的，因此时区并不影响该值。同样地，也不进行夏时制的调整。在使用 UTC 后，如果设备在不同时区间移动，或者如果执行夏时制，那么为配置包所报告的时间始终是单调增加的。

当时钟漂移且人工或自动复位时，设备中设置的时间可能变得超前或滞后。设备不能发出这样一个配置包，该包的日期时间早于它以前发出的任何包的日期时间。可以用几种方式完成，一种方式是使设备将最近发出配置包的日期时间保存在非易失性存储器中。当每次配置包被发出时，设备选择最新的当前日期时间并将最近保存日期时间加 1。如果设备以小于每秒 1 个的平均速率发出新的配置包，那么配置日期时间和系统日期时间最终将交叉，并且系统日期时间将滞后。

10.4.2 通用协议交互作用

每个发出的包有一个预期响应。响应可能是协议交换中的一个 ACK 或另一个报文。其他报文的接收应被解释为前一个报文的 ACK_OK。

——使用 back-off 算法重发包几次，以避免拥塞。例如，可以设置重发定时器为 1s，每次重发定时器就成倍增加，直到 30s 为止。

——ACK 不被重发，但设备中的状态变化始终如此，协议中复制前一个报文的接收不会引起状态变化，而会引起相应的 ACK 重发。

配置服务器可以支持多个信道。在这种情况下，利用每个信道的设备 IP 地址列表对配置服务器进行配置。设备注册报文包含设备 IP 地址，因此可确定设备的信道成员。对于所有其他报文，可以将正在发送的 IP 地址确定为 UDP 帧的源地址或 TCP 连接的源地址。

10.4.3 包分段

10.4.3.1 UDP

约 548 字节长度的 UDP 有效载荷造成信道成员的限制，并且当考虑到节点时还会引起其他一些问题。处理较长包受限于配置协议，下列是主要考虑的包类型：

——网络上设备超过 128 个的信道成员包；

——网络上设备超过 64 个的发送列表包；

——节点带有超过 4 个域的信道路由信息。

当这些数据集超过 548 字节 UDP 包大小限制时，使用 10.2 描述的分段方式。

10.4.3.2 TCP

TCP 是与服务器通信的可选方法。设备注册包的 IP_PROTOCOL 字段指示 TCP 或 TCP 和 UDP 时，服务器可以使用 TCP 链路与设备交换数据。

在这种情况下：

a) 不使用分段包。不管包大小发送整个包。

b) 不在 TCP 连接上发送 ACK 报文。

c) 不在 TCP 连接上进行重发。

d) 可以使用 TCP 或 UDP 将请求从设备发送到服务器。这样的请求可以由服务器使用 TCP 或 UDP 来处理。如果设备使用 TCP 连接到服务器，并且服务器支持 TCP，那么服务器必须使用 TCP 应答。

e) 当配置服务器检测出配置变化时，它可以通过 TCP 链路主动发送配置数据给设备。信道成员包总是首先被发送，随后是任何相关的更新包。可以用这种方式发送下列包：发送列表、设备配置包或信道路由包。

f) 当 TCP 连接突然断开时，设备而不是服务器负责重建连接。假设设备故障或与网络隔离。当出现新更新值时，配置服务器再次设法尝试与设备建立连接，以便转发更新值。设备应连续设法尝试，在一些与实施有关的期间与服务器建立连接，并基于任何现有配置数据继续为报文选择路由。当使用 TCP 时，设备或服务器可以启动连接。在一些与实施有关的期间，连接保持开放，等待更多通信业务来使用。在自身超时之后，每侧都可以终止连接。应该正确关闭 TCP 连接，但不强制要求。

当支持 TCP 的设备首次开始与服务器通信时，它不知道服务器是否支持 TCP。设备可以使用下列机制决定是否使用 TCP：

a) 设备设法与配置服务器建立 TCP 连接。

b) 在通过 UDP 向服务器发出请求之前，设备不必等待连接成功或超时。例如，设备可以开始 TCP 连接，然后立即将设备注册包发送到服务器。注意，设备注册包含有说明设备支持 TCP 的 IP 协议字段。

设备确定配置服务器是否支持 TCP 的唯一方法是使一个连接成功。该机制假设不支持 TCP 的节点不能以“拒绝连接”来响应。

如果服务器支持的同时连接数量小于信道上的设备数量，那么设备在尝试连接时可能从服务器接收到“拒绝连接”报文。这种响应表明服务器上资源不足。在这种情况下，在适当时间之后，它们会再次尝试或选择使用 UDP。

服务器应该储存 TCP 连接的超时，以便为新设备对话提供一个或多个开放式连接。

10.4.4 设备注册

这个交互作用设计用于使设备将其身份码通知服务器并从服务器获得 IP 操作参数。

设备需要下列信息，以便开始与服务器交互作用。所有其他信息都能根据数据唯一性从服务器获得：

a) 设备的 IP 地址/端口；

b) 配置服务器的 IP 地址/端口。

利用这种交互作用解决下列情况：

a) 设备有一些标识信息，并需要从服务器获得其余信息。服务器认识设备。

b) 设备有一个固定的、可能是本地输入的配置，需要利用服务器注册并获得发送列表和/或信道成员列表。

c) 设备可能或不可能遵守服务器建议的配置信息。协议不允许进行配置商议。如果设备不能遵守服务器建议的配置，那么报告这种情况并停止操作。

d) 当设备停止操作时，它继续处理来自配置服务器的报文，但是不为报文选择路由。它不再促使与服务器进一步活动，而是处理设备响应报文。

表 1 描述了本协议。

表 1 使用配置服务器的设备注册协议

设备	←→	服务器
发送设备注册包	→	加入配置或拒绝
停止运行直到复位为止	←	用 ACK_DEVICE_REFUSED 拒绝，或
用新参数开始运行，和	←	设备配置包
ACK_OK 开始运行，或	→	停止设备配置的重发，在数据库中指示设备是成员
ACK_CANT_COMPLY 停止运行直到复位	→	无进一步动作，数据库无变化
执行下一步	←	发送主动的设备配置包
发送 ACK_OK 或 ACK_CANT_COMPLY	→	请求更多信息，必要时基于设备响应中的日期时间

在被动的情况下，服务器没有重发设备配置包。如果客户没有及时接收到设备配置包，那么它将重发设备注册包到服务器。

在主动的情况下，如果服务器没有从客户端接收到 ACK_OK 或 ACK_CANT_COMPLY，那么服务器应重发设备配置包。

配置服务器也可以使用那些报文将配置服务器的变化通知信道成员。如果配置服务器的 IP 地址或端口发生变化，就要这样做。表 2 中描述该协议。这还不是安全操作。设备可能拒绝这个请求，因此，必须以一些相关实现方式为配置管理员标识进行配置。本协议本身不允许对安全作出重大妥协，然而由于 IP 电子欺骗是可能的，另一个节点能够在任何脱网时候占用 IP 标识并扮演配置管理员角色。

表 2 服务器到设备主动配置报文协议

设备	←→	服务器
建立响应	←	发送配置请求包
发送设备配置包	→	建立设备配置包
—	←	发送设备配置包
采用配置服务器和时间服务器的新 IP 地址/端口发送 ACK_OK	→	作为配置服务器正常进行
发送 ACK_CANT_COMPLY 停止运行以便不干涉信道的进一步运行	→	标明设备不再是信道成员

如果设备采用了一种策略，以便当它接收到不能遵守的服务器变化时还能继续运行，那么设备只能与类似设备可互操作。这是因为新配置管理员必须信赖所有服从它的指令和信息的设备，或必须依赖故障后以某种方法被人工更新的设备。

服务器应在发送新的配置包之前请求客户端配置。不要求客户端在处理来自服务器的新设备配置包之前接收到这样一个请求。

10.4.5 信道成员

交互作用的目的是允许设备能获得信道上其他设备的完整列表。表3描述该协议。

如果在一些设备工作之后信道成员列表改变，那么服务器可以为信道成员列表发送一个带有新日期时间的主动设备配置包。

表3 设备到服务器信道成员请求协议

设备	←→	服务器
发送信道成员请求包	→	在数据库中寻找设备并标识信道
停止运行直到复位	←	ACK_DEVICE_REFUSED 如果没有被定义的信道或设备不是任何信道的成员，或
用新参数开始运行	←	发送信道成员包

信道成员包不是由服务器重发的。如果设备没有接收到包，那么它就再次进行请求。

当配置发生任何改变时，服务器就向每个成员通知改变。有三类改变：

a) 将一个设备加入列表；

b) 将一个设备从列表中移出；

c) 一个设备改变了其配置，要求其他节点更新它们的发送列表或该节点的路由信息。

这些情况都由服务器来处理，服务器向所有设备发送带有更新的信道成员包日期时间的主动设备配置包。然后，设备请求一个新信道成员包。如果接收到包的节点发现它不在成员中，那么它停止为包选择路由并等待新的配置报文。如果节点没有信道成员列表，意味着它刚被加入到信道中，那么它可以请求信道路由包或发送列表包。

信道成员包的每个表项包含一个日期时间，该日期时间表明信道路由包的最近有效日期时间。它还包含一个 SendListDateTime 发送列表最近有效时间和一个 DeviceRequestDateTime 设备的这个数据包最近有效时间。设备使用这些日期时间请求新信息。

10.4.6 发送列表

这个交互作用使设备能获得信道的发送列表。表4描述这个协议。

如果在一些设备工作之后发送列表发生改变，那么协议首先使服务器发送设备配置包作为主动报文。见10.4.4。

发送列表是一个可选方式，通过这种方式路由器可以转发包。通过使用发送列表，配置服务器可以集中管理信道的多播地址。服务器必须支持发送列表包的创建，并且必须响应设备对这些包的请求。设备对发送列表包的支持是可选的，并且设备不需要从服务器请求这些包。

发送列表被如何得到或配置到服务器中是由实施决定的，只要它遵守第7章中规定的三项规则。当缺乏已配置的发送列表或缺乏将其推导出来的更复杂算法时，服务器可以使用下列算法来产生一个发送列表。

发送列表产生方法：

当且仅当 CN/IP 信道中的每个设备属于相同多播组，使用算法 A，否则使用算法 B。值得注意的是，设备属于哪个多播组是服务器完全知道的设备配置的一部分。有关知识来自设备发送的设备注册包或服务器发送到设备的设备配置包。

算法 A(高度优化)：

选择单个多播组，CN/IP 信道上的每个设备都属于该多播组。为这个组选择一个多播 IP 地址，作为发送列表中唯一的表项。值得注意的是，这个算法取决于 CN/IP 信道上每个属于发送列表中规定的多播组的设备。如果由于某种原因，这种情况不能成立，那么必须相应地修改发送列表。

算法 B(强制算法)：

对于信道成员列表中的每个设备，将相应设备的单播 IP 地址加入发送列表。在这种情况下，发送列表必须与信道成员列表保持一一对应。如果从信道成员列表中增加或删除设备，必须相应地修改发送列表。

当使用发送列表时，将设备转发的每个包无条件地发送至列表中每个地址。设备监听设备配置报文中规定的端口和地址。

表 4　设备到服务器的发送列表请求协议

设备	←→	服务器
发送列表请求包被发送	→	在数据库中寻找设备并标识发送列表
停止运行直到复位	←	ACK_DEVICE_REFUSED 如果没有定义任何信道或设备不是任何信道的成员，或
用新参数开始运行	←	发送列表包被发送

发送列表包不是由服务器重发的。如果设备没有接收到包，那么它就再次请求。

10.4.7　信道路由

这个相互作用允许设备获得设备的信道路由信息，或允许设备发送信道路由信息到服务器，用于发送到其他设备。表 5 和表 6 分别描述这个协议。

这些包是在 CN/IP 设备之间被交换的并表示报文中指示的设备路由信息。当一个配置服务器发送几个包时，每个单播 IP 地址与信道成员列表中的 IP 地址对应。路由信息指向那个节点。信道成员的所有 IP 地址必须是唯一的。

支持信道路由包是可选的。

具体地说，在这个包中发送由子网和组掩码构成的路由表。如果由于某些原因，在 IP 网络上不允许路由器之间多播寻址，那么路由器可以使用子网和组掩码信息，以避免发送每个包到其他路由器，否则就要浪费带宽。

如果路由器能路由选择多个 CN 域或作为代理，那么可以在包中重复子网掩码，组掩码和域结构。

如果在一些设备工作之后信道路由信息发生改变，那么协议可以首先使服务器发送主动设备配置报文。见 10.4.4。

当设备支持信道路由包时，并且它有新信道路由信息，设备就创建一个新信道路由包。然后，将这个包发送到服务器。

表 5　设备到服务器信道路由更新协议

设备	←→	服务器
发送信道路由包	→	在数据库中寻找设备并标识路由列表
停止运行直到复位	←	ACK_DEVICE_REFUSED 如果没有定义任何信道或设备不是任何信道的成员，或
停止信道路由包的重发	←	发送 ACK_OK

当设备支持信道路由包时，它需要信道上其他设备的路由包。设备以表 6 中示出的方式获得这些包。

表 6　设备到服务器信道路由请求协议

设备	←→	服务器
发送信道路由请求包	→	在数据库中寻找设备并标识路由列表
停止运行直到复位	←	ACK_DEVICE_REFUSED 如果没有定义任何信道或设备不是任何信道的成员，或
用新参数开始操作	←	发送信道路由包

服务器不重复进行传送，并且设备不能完成 ACK。如果设备没有接收到报文，那么它再次请求。

信道路由请求报文包含对服务器请求的两个字段：

a) 日期时间：表明如果任何数据比该日期时间新，那么发送数据。零表示总是发送数据。

b) IP 单播地址：如果非零，表示仅发送这台设备的信道路由信息。如果是零，表示向信道的所有成员发送所有的信道路由信息。

可以使用这些选项优化对服务器的请求。例如，如果一个路由器请求信道成员列表，并在列表中发现一个新设备，它可能仅为那台设备请求信道路由信息。

10.4.7.1 到子网/节点地址的路由

信道路由包含有一个子网/节点地址列表和一个带有子网掩码的域列表。路由器可以使用这些列表以下列方式实现最佳路由：

使用子网/节点寻址方式的报文被发送到相匹配域/子网/节点地址的相应设备。匹配子网广播和被寻址的唯一 ID 指向的子网报文被转发到那个子网中所有节点。不能将这样的子网设置在域的子网掩码中。域/子网/节点地址通常是唯一的，但在一些情况下（某种差错情况或瞬时状况）可以有多个声明相同地址的设备。在这些情况下，报文将被路由到多个设备。

10.4.7.2 要求全部广播的语义

信道路由包的 CN 标志字段包含 1 个比特称为 WANTS_ALL_BROADCASTS。该字段根据以下情况优化路由：

所有设备将至少代表一个 CN 可寻址的节点。例如，对于 CN/IP 路由器，这个节点在与 IP 信道连接的路由器侧。如果设备至少有一个处于未被配置状态的 CN 可寻址节点，那么它必须报告要求全部广播（全域或子网），不考虑广播报文中的域 ID。这是因为当 CN 节点处于未配置状态时，CN 节点响应全部广播，而不考虑域 ID。

10.5 其他状态报文

这些报文用于允许网络工具从设备中提取报文，以便帮助管理和调试网络上的设备。一般情况下，通过本部分中描述的报文可以获得所有有关设备正常、统计和配置等有用报文。这些报文不要用于设备的配置或代替已为配置服务器定义的功能。

支持下列通用操作：

——请求 CN/IP 设备的通用正常/状态；

——请求 CN/IP 设备的通用正常/状态/统计，并当将它们发送至请求者时清除统计；

——请求设备配置；

——请求设备发送列表；

——请求设备信道成员；

——请求设备信道路由信息。

所有这些操作是以简单的请求/响应事务形式进行。在适当的时候，重新使用为客户端/服务器交互作用定义的报文格式。在本条描述的任何请求/响应事务中，值得注意的是，不是配置服务器的节点不应响应与正在被请求设备不相应的请求。例如，设备 A 不应响应对设备 B 信息的请求，除非设备 A 是一个配置服务器。

10.5.1 CN/IP 设备状态

所有信息是可选的。这意味着不规定以任何方式提供这个信息。访问这个信息的可能性包括，但不限于：

——路由器上的局部串行线；

——CN 参数访问；

——CN 网络变量访问；

——IP 上的专用（未定义的）报文；

——路由器上运行的 HTML 服务器。

这些数据不要被复制，或参与路由器 TCP/IP 栈中对 SNMP MIB-Ⅱ任何可选的支持。

10.5.1.1 状态信息

一般来说，统计信息是无符号 32 位定点整数格式。如果不支持统计信息，那么将统计值设置为 0xFFFFFFFF。如果统计量处于溢出状态，那么将其设置为 0xFFFFFFFE。任何单个统计的支持是可选的，然而，任何 CN/IP 节点必须用这个包对请求信息响应。厂商自由地增加实现特定统计作为附加响应包。厂商特定报文扩展的信息见 10.6。

——从前一个计数器复位开始的时间。(格式:32 位无符号整数，秒)

——前一个计数器复位的时间。用 GMT。(格式:日期时间。见 11.4)

——信道上的成员数。(格式:32 位无符号整数)

——最近发送报文的信道上的成员数。(测量方法未定义。)(格式:32 位无符号整数)

——被接收的 CN 包数(从 CN 信道接收的包数)。(格式:32 位无符号整数)

——由于选择转发接收但丢弃的 CN 包数。(格式:32 位无符号整数)

——接收到的 CN 总字节数。(格式:32 位无符号整数)

——发送的 CN 包数。(发送到 CN 信道上的包数。)(格式:32 位无符号整数)

——发送的 CN 总字节数。(格式:32 位无符号整数)

——发送到 IP 信道上的 CN 包数。(格式:32 位无符号整数)

——发送到 IP 信道上的 CN 字节数。(格式:32 位无符号整数)

——从 IP 信道接收到的 CN 包数。(格式:32 位无符号整数)

——从 IP 信道接收到的 CN 字节数。(格式:32 位无符号整数)

——发送到 IP 网络上含有 LT 包的 IP 包数。(格式:32 位无符号整数)

——来自 IP 网络的含有 LT 包的 IP 包数。(格式:32 位无符号整数)

——至 IP 信道的平均聚合。(值被表示为一对 32 位无符号整数。)整个 LT 包＜第 10 项＞/整个 IP 包＜第 14 项＞。

——来自 IP 信道的平均聚合。(值被表示为一对 32 位无符号整数。)整个 LT 包＜第 12 项＞/整个 IP 包＜第 15 项＞。

注：由于所有参数是可选的，复制数据格式不是问题。可以选择不支持第 12 项、第 15 项，而支持第 17 项。

——已发送的 UDP 包的数目。(格式:32 位无符号整数)

——已发送的 TCP 包的数目。(格式:32 位无符号整数)

——已发送的多播包的数目。(格式:32 位无符号整数)

——从 IP 丢弃的陈旧 LT 包数。(格式:32 位无符号整数)

注：陈旧意味着在 IP 网络中的时间过长。

——TCP 连接失败的次数。(格式:32 位无符号整数)

——具有不同 TCP 连接失败的主机数。(格式:32 位无符号整数)

——已发送的路由器配置报文数目。(格式:32 位无符号整数)

——已接收到的路由器配置报文数目。(格式:32 位无符号整数)

——配置改变的次数。(格式:32 位整数)

——已发送的 UDP 包/秒的连续平均数。(格式:32 位整数)

——已接收到的 UDP 包/秒的连续平均数。(格式:32 位整数)

——已发送的 TCP 包/秒连续平均数。(格式:32 位整数)

——已收接到的 TCP 包/秒连续平均数。(格式:32 位整数)

10.5.2 设备配置

设备配置可以由一些主机来请求。如果它规定设备接收请求，那么必须响应这样的请求。

设备配置请求/响应事务使用与 10.4.4 中所描述相同的包，如表 7 所示。

表 7　请求设备配置的协议

IP 主机	←→	设备
发送配置请求包	→	证实请求有效
完成	←	以 ACK_DEVICE_REFUSED 拒绝，或
完成	←	发送设备配置包

10.5.3　设备发送列表

设备发送列表可以由一些主机来请求。如果它规定设备接收请求，那么必须响应这样的请求。

设备发送列表请求/响应处理使用与 10.4.6 中所描述相同的包，如表 8 所示。

表 8　请求设备发送列表的协议

IP 主机	←→	设备
发送列表请求包被发送	→	证实请求有效
完成	←	以 ACK_DEVICE_REFUSED 拒绝，或
完成	←	发送列表包被发送

10.5.4　信道成员列表

设备信道成员列表可以由一些主机来请求。如果它规定设备接收请求，那么必须响应这样的请求。

设备信道成员列表请求/响应事务使用与 10.4.5 所描述相同的包，如表 9 所示。

表 9　请求设备信道定义的协议

IP 主机	←→	设备
发送信道成员请求包	→	证实请求有效
完成	←	以 ACK_DEVICE_REFUSE 拒绝，或
完成	←	发送信道成员包

10.5.5　信道路由信息

设备的信道路由报文可以由一些主机请求。如果它规定设备接收请求，那么必须响应这样的请求。

设备配置请求/响应事务使用与 10.4.7 所描述相同的包，如表 10 所示。

表 10　请求设备信道路由信息的协议

IP 主机	←→	设备
发送信道路由请求包	→	证实请求有效
完成	←	以 ACK_DEVICE_REFUSED 拒绝，或
完成	←	发送信道路由包

10.6　厂商特定报文

通用包首部中的厂商代码用于厂商特定包。对于根据本规范定义的所有标准包，必须设置这个值为 0。唯一厂商代码可以部分地识别厂商特定包(除 0 以外)。

对 11.1 中详细描述的每个功能分配唯一包类型码。本规范中定义的标准包类型代码的范围是 0x00 至 0x7F。传输信息作为本规范中定义的标准功能扩展的厂商特定包可以使用与标准功能相同的包类型代码，然而必须设置厂商代码为该厂商唯一标识符。与本规范中定义的现有标准功能无关的厂商特定包必须使用 0x80 至 0xFF 范围中的包类型代码。

设备所接收到的不能识别厂商代码/包类型组合的厂商特定包必须丢弃。

10.7　CN 包的鉴别

CN/IP 设备中的安全性是可选的。如果设置 CN/IP 首部协议标志字段中的安全位(见 11.2 通用

CN/IP 首部),那么必须像本条描述的那样执行下列鉴别方案。

本条描述的安全性等级是鉴别。将使用本条描述的方案所发送的报文鉴别为来自可靠的信息源。报文中的信息没被加密且不禁止检查。这个方案保证发送方使用有效共享密钥构成包,并且保证发送过程中不受破坏。对于这个方案的更多信息,见 RFC1321。

图 5 说明了对 CN 首部中安全位设置的包编码和解码过程。

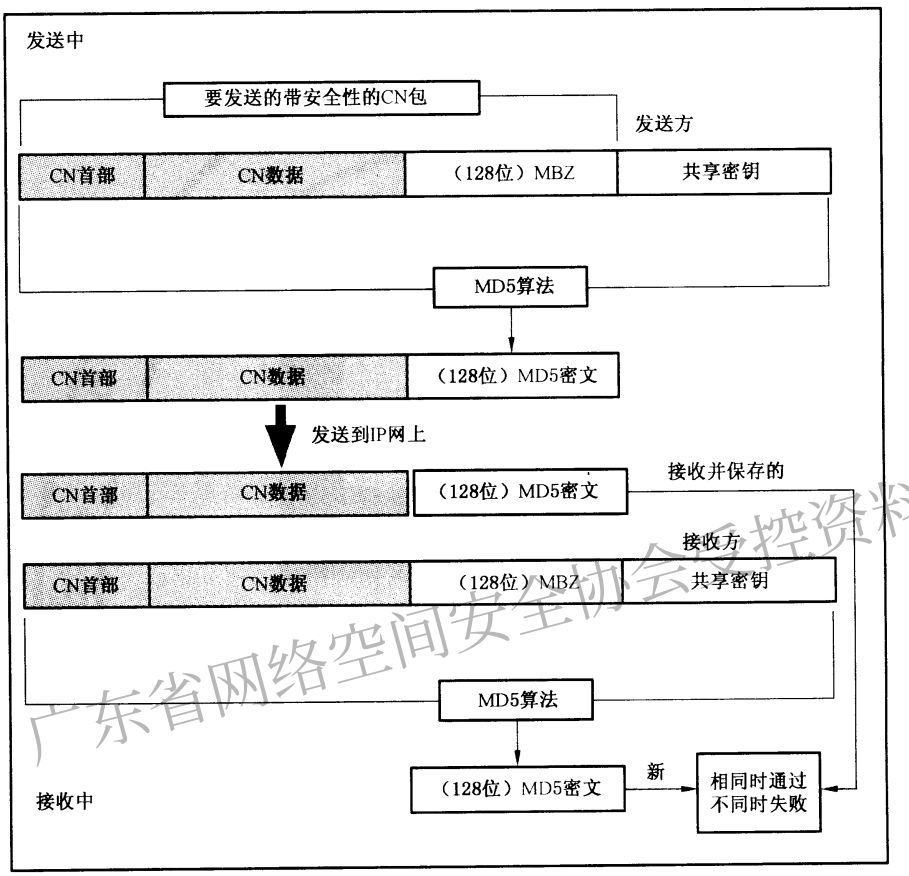

图 5 CN 包鉴别的编码和解码

在发送一个安全的报文之前,像上述所示的那样,发送方向报文添加一个共享密钥。

"共享密钥"必须至少代表一个包含 128 个自由度的值。例如,对选择所有比特有效的 16 字节阵列或每字节 6 比特有效的 22 字节字符串都能满足 CN "共享密钥"的最小要求。然而,CN"共享密钥"不限于 128 个自由度,可以更大。

"共享密钥"的其他要求为:

——不应该在网络上公开传送"共享密钥";

——CN 设备必须允许人工设置和更新设备密钥的安全方法;

——当且仅当在设备执行中出现鉴别问题,那么 CN 设备必须至少提供单个用于确认请求的"共享密钥";

——制造商最初可以有选择地利用默认"共享密钥"制造产品,随后可以利用安全网络报文更新该"共享密钥"。

然后,通过将 MD5 报文密文算法加入到带有"共享密钥"的完整 CN/IP 包上生成包密文。将生成的 MD5 密文插入到上述 MBZ 密钥字段,并且将不带有密钥的包发送至网络。

正在接收的设备对入向包执行相同过程。

a) 存储入向密文并用 0 替代密文字段;

b) 用自身的“共享密钥”制作包密文；

c) 将入向密文和它生成的新密文比较；

d) 匹配 MD5 密文表示包有效；

e) CN 设备应该丢弃未被鉴别包并且可以记录未被鉴别包。

11 包格式

本章对所有 CN/IP 包的内容和格式进行详细描述。对于如何使用本章中描述的各种包，见第 9 章。

所有 CN/IP 包由一个首部和其后的数据部分组成。所有 CN/IP 报文的首部格式是相同的。数据部分与 CN/IP 包的类型有关。

除了有注解的以外，所有字段都按网络字节顺序。

11.1 包类型

表 11 是系统中使用的所有包的交叉引用。

使用下列缩略语描述各种数据集合：

DC——设备配置

CM——信道成员列表

SL——发送列表

CR——信道路由

表 11 报文类型交叉引用

包名称	格式(第 11 章)	使用的事务(第 10 章)	代码
数据包	11.4	CN 数据包交换(10.3)	0x01
设备配置请求	11.8	对服务器的 DC 请求(10.4.4) 对设备的 DC 请求(10.5.2)	0x63
设备注册	11.5	设备对服务器注册(10.4.4)	0x03
设备配置	11.5	来自服务器的 DC 响应(10.4.4) 来自设备的 DC 响应(10.5.2) 服务器的主动的设备配置更新(10.4.1.1)	0x71
信道成员请求	11.8	对服务器的 CM 请求(10.4.5) 对设备的 CM 请求(10.5.4)	0x64
信道成员	11.6	来自服务器的 CM 响应(10.4.5) 来自设备的 CM 响应(10.4.6)	0x04
发送列表请求	11.8	对服务器的 SL 请求(10.4.6) 对设备的 SL 请求(10.5.3)	0x66
发送列表	11.10	来自服务器的 SL 响应(10.4.6) 来自设备的 SL 响应(10.5.3)	0x06
信道路由请求	11.8	对服务器的 CR 请求(10.4.7) 对设备的 CR 请求(10.5.5)	0x68
信道路由	11.7	来自服务器的 CR 响应(10.4.7) 来自设备的 CR 响应(10.5.5)	0x08
确认	11.9	10.4.2	0x07
分段	11.3	10.4 和 10.5 节中的所有 CM、SL 和 CR 事务	0x7F
状态/正常/统计请求	11.8	对设备的状态请求(10.5.1)	0x60
状态/正常/统计响应	11.11	来自设备的状态响应(10.5.1)	0x70

11.2 通用 CN/IP 首部

所有 CN/IP 包带有表 12 中示出的通用首部。

表 12 通用包首部格式

字节 0	字节 1	字节 2	字节 3
数据包长度		版本	包类型
扩展首部大小	协议标志	厂商代码(16 位)	
会话 ID			
顺序号			
时间戳			

该首部出现在所有包上。以下是对每个字段的描述。

版本

这是包的版本号。假设一直可以对带有相同版本号的包进行分解。如果节点接收到一个带有未知版本号的首部,它将丢弃该包而不再对包中的内容进行进一步的处理。当前版本号是 0x01。版本号是这个字节的低 5 位。高 3 位被定义如下:

比特位 5～6:MBZ

保留

比特位 7:后面有无厂商特定包

在此之后的包含厂商代码要与这个包同时被处理。

协议标志

这些标志是用于描绘各种隧道技术协议的比特位标志。使用下列比特位:

比特位 7(MSB)——保留,MBZ

比特位 6——保留,MBZ

比特位 5——安全位。如 10.7 描述的那样,如果将这个位设置为 1,那么这个包含有鉴别信息。

比特位 4-0——协议代码。这个字段规定了在包中利用隧道技术的协议。支持下列协议:

0x00—GB/Z 20177.1

厂商代码

该字段用于指示厂商特定代码。值 0x0000 表示该包符合本规范。除 0x0000 以外的任何值表示这个包是一个厂商特定包。厂商特定报文的详细信息见 10.6。

相关机构分配和管理每个厂商代码。要求在特定协议中厂商代码是唯一的。

包类型

这决定了包的类型。本规范中定义的包类型代码的范围是从 0x00 至 0x7F。能够传送信息作为本规范定义的标准功能扩展的厂商特定包可以使用与标准功能相同的厂商特定代码,然而必须将厂商代码设置为该厂商唯一的标识符。与本规范中定义的现有标准功能无关的厂商特定包必须使用一个范围为 0x80 至 0xFF 的包类型代码。厂商特定报文的详细信息见 10.6。

数据包长度

这个字段表示包的字节长度,包括通用包首部中的字节。如果当前帧中有多个字段值,那么加入地址的字段值是后续包的下一个版本字段的偏移量。

扩展首部大小

这个字段是超过标准首部大小4字节记录为单位的包首部长度。如果通用首部没有扩展，那么这个字段为0。这就意味着首部必须是4字节的倍数并且与4字节的边界对齐。该字段考虑到允许对未来协议版本的后向兼容。本协议版本1生成的所有包必须将首部大小设置为0。

会话ID

会话ID与顺序号一起使用，保证按标准UDP信道上发送数据包的顺序接收数据包。每个CN/IP节点随机地选择一个会话ID。如果CN/IP节点进行重新启动和复位等并忘记其正在使用的顺序号，那么节点使用新的会话ID向目的地发送下一个报文。可以有限制地被随机选择新会话ID，这个限制是新会话ID与重启/复位事件之前节点所使用的会话ID不同。

当节点从信息源接收到一个带有不同会话ID的报文时，而该会话ID与来自于同一信息源的前一个报文中的会话ID不同，节点就假设报文是有顺序的新报文。此外，为了顺序保存后续报文，接收方记忆新报文中包含的会话ID/顺序号对。

顺序号

当前包的顺序号。算法的细节见10.3.1～10.3.3。

时间戳

被分配给当前数据包的时间戳，如果没有时间戳，则为零。这个时间戳表明在这个IP信道上发出这个包的时间。

对于配置包，时间戳字段总是为零。它仅对数据包有效。

11.3 分段包

这个包用于封装超过单个UDP数据报大小的其他CN/IP报文。

表13示出了分段包格式。

表13 分段包格式

字节0	字节1	字节2	字节3
通用包首部			
日期时间			
标志	请求ID		分段ID
有效载荷字节	有效载荷字节	有效载荷字节	有效载荷字节
有效载荷字节	有效载荷字节	有效载荷字节	有效载荷字节
有效载荷字节	有效载荷字节	有效载荷字节	有效载荷字节
有效载荷字节	有效载荷字节	有效载荷字节	有效载荷字节
有效载荷字节	有效载荷字节	有效载荷字节	有效载荷字节

下面是对这个包中所有字段的描述。

包类型

见11.1。

日期时间

日期时间格式的详细说明见11.5。日期时间字段是被封装包日期时间的拷贝。特定被封装包的所有分段有相同的日期时间，该包中的数据元素是一致的。在分段传输封装包过程中，如果构成被封装包的任何数据发生了变化，那么受影响分段包中的日期时间也改变为新数据集的日期时间。

标志

比特位7：有效位

该比特位置位，表示分段ID所指示的数据包中存在有效数据。

比特位 6:最终位

该比特位置位,指示分段 ID 值大于该包中返回值的包中没有数据存在。

比特位 5～0:保留。

请求 ID

产生这个响应的请求报文中请求 ID 值的复制。

分段 ID

产生这个响应的请求报文中分段 ID 的复制。它是这个响应中包含的数据标识符。

11.4 CN 数据包

表 14 示出了 CN/IP 数据包的格式。

表 14 格式

CN/IP 通用首部	CN 数据包

CN/IP 首部

见 11.2。

CN 数据包

这是附录 A 中描述的完整 PDU 包。构成 PDU 的字节数等于包字节数减去首部字节数。

注:如 10.3.1 中描述的那样,CN 数据包处理顺序必须与其产生的顺序相同。这样,在将未按顺序到达的 IP 包发送到 CN 协议栈之前,应该将该 IP 包重新排序。如果不支持重新排序,必须忽略未按顺序接收的包。

11.5 CN/IP 设备注册/配置包

如果正在使用配置服务器,那么 CN/IP 设备向服务器发送设备注册包,以便向服务器通知 CN/IP 设备的存在。然后,服务器利用设备配置包进行响应。服务器使用注册包,以便配置 CN/IP 设备并可能维护 IP 信道上所有 CN/IP 设备的列表。

设备配置包是配置服务器唯一主动发送到设备的包。

表 15 示出了 CN/IP 设备注册和设备配置包格式。

表 15 设备注册/配置包格式

字节 0	字节 1	字节 2	字节 3
通用包首部			
日期时间			
IP 标志	CN 路由器类型	CN 标志	节点类型
多播地址计数[M]	MBZ	信道超时	
唯一 ID 总字节数[U]		IP 单播端口	
IP 单播地址			
信道成员日期时间			
发送列表日期时间			
配置服务器 IP 地址			
主时间服务器 IP 地址			
次时间服务器 IP 地址			
配置服务器 IP 端口		主时间服务器 IP 端口	
次时间服务器 IP 端口		MBZ	

表 15(续)

字节 0	字节 1	字节 2	字节 3
IP 多播地址[0]			
IP 多播端口[0]		MBZ[0]	
IP 多播地址[M-1]			
IP 多播端口[M-1]		MBZ[M-1]	
唯一 ID[0]	唯一 ID[1]	唯一 ID[2]	唯一 ID[3]
唯一 ID[4]	唯一 ID[5]	唯一 ID[6]	...[U-1]
名称长度[N]	名称[0]	名称[1]	名称[2]
名称[3]	名称[4]	名称[5]	...[N-1]

包类型

见 11.1。

日期时间

它是数据有效的日期和时间。可以用 1 秒的分辨率通过寻找字段确定该数据的新或旧版本。字段是受到约束的,以便如果在同一秒内多个数据版本被创建,那么它们具有该字段的唯一递增值。

如果网络支持 SNTP 或 NTP,日期时间值是 RFC-1305 中 NTP 数据时间的秒部分。它是 1900 年 1 月 1 日以来的秒数量。该时间将在 2036 年结束。详见 RFC-2030 的第 3 章。

如果网络不支持 SNTP 或 NTP 协议,日期时间可以是一个不包括 0 的小整数。在 20 世纪早期,这些日期时间显然不是壁钟的时间,而是受到约束的,以便要服从上文提到的在所有时间内都是唯一的要求。即这样设备发送的数值永不重复。

IP 标志:

掩码值包括:

0x01——支持 UDP

0x02——支持 TCP

0x04——支持多播

CN 路由器类型

在设备节点类型是一个路由器的情况下,该字段表示下列操作模式:

0x00——配置:对于每个被规定域,如果设置子网掩码位,那么将子网/节点、子网广播和子网唯一 ID 报文(非零子网)转发至设备。在上述任何报文中,如果子网为 0,那么应该像设置子网 0 比特位为 1 那样转发该报文。对于组报文,如果比特位被设置在组掩码中,那么将其转发。

0x01——自学习:对于每个被规定域,如果子网掩码位被设置,那么将子网/节点、子网广播和子网唯一 ID 报文(非零子网)转发至设备。在上述任何报文中,如果子网为 0,那么应该像设置掩码中子网 0 比特位为 1 那样转发报文。对正在或可能在“另一侧”的子网,设置子网掩码位,并且对不知道在“这一侧”的子网,不设置子网掩码位。对于组报文,总是转发(组比特位被忽略)。

0x02——网桥:对于每个被规定域,转发所有报文(子网和组比特位被忽略)。

0x03——中继器:转发所有报文(域/子网/组信息被忽略)。

CN 标志:

掩码值包括:

0x01——WANTS_ALL_BROADCASTS. 这个功能的细节见 10.4.7.2。

0x02——支持 10.7 中描述的安全性。

节点类型

设备类型。目前，这些类型的行为是未被规定的。

0x01——非 IP 信道至 IP 信道路由器。

0x02——IP 信道节点。

0x03——IP 信道代理服务器。

0x04——IP 信道至 IP 信道路由器。

多播地址计数

多播 IP 地址和端口号的数目。

信道超时

10.3.3 和 10.3.1 中超时值的单位是毫秒(ms)。值 1 ms～1 500 ms 是有效的。尽管可能规定这个参数小于 1 ms，但是由于 SNTP 性质，不能保证这个精度等级。可能使用的最小精度等级的范围为 10 ms～16 ms。

唯一 ID 总字节数

随后唯一 ID 的字节总数。必须是 6 个字节(唯一 ID 的大小)的倍数。至少必须有一个表项。如果设备是节点，那么唯一 ID 与 GB/Z 20177.1 中规定的唯一 ID 对应。一个路由器设备可以有三个唯一 ID，路由器每侧使用一个唯一 ID，一个唯一 ID 用于配置。本字段中要求规定的唯一 ID 是与路由器侧对应的唯一 ID，该路由器被直接连接至 CN/IP 信道。

IP 单播端口

侦听单播 IP 报文时 CN/IP 设备使用的端口号。

IP 单播地址

按网络字节顺序的 CN/IP 设备的单播 IP 地址。CN/IP 设备将侦听这个地址上的入向单播 IP 包。

信道成员日期时间

服务器的最近信道成员包的日期时间。该日期时间用于决定：当设备从服务器接收到主动的设备响应包时，是否应向配置服务器请求新的信道成员包。当从设备向服务器发送包时，其内容是没有意义的。

发送列表日期时间

设备的最近发送列表包的日期时间。该日期时间被用于决定：当设备从服务器接收到一个主动的设备响应包时，是否应向配置服务器请求新的发送列表包。当从设备向服务器发送包时，其内容是没有意义的。

配置服务器 IP 地址

配置服务器的 IP 地址。这个信道的新配置服务器可以发送一个设备配置包来设置配置服务器和时间服务器的 IP 地址和端口号。

主/次时间服务器 IP 地址

NTP 时间服务器的 IP 地址。如上所述，这些地址是由配置服务器设置的。如果设备能够访问主时间服务器，那么就使用主时间服务器，否则使用次时间服务器。这就保证设备使用一个可预知服务器。

配置服务器 IP 端口

配置服务器的 IP 端口号。设置如上。

主/次时间服务器 IP 端口

时间服务器的 IP 端口号。只要条件允许就应该使用标准 NTP 端口号 123。

IP 多播地址

CN/IP 设备的多播 IP 地址。如果不支持多播地址计数，那么多播地址计数为零。CN/IP 设备将侦听该地址上的入向多播 IP 包。将 8 个字节的地址、端口、MBZ 重复“多播地址计数”次。

IP 多播端口

当侦听多播 IP 包时，CN/IP 设备使用的端口号。

唯一 ID

唯一 ID 被打包在一起，每个包 6 个字节，用 CN 网络字节顺序表示。

名称长度

名称字段的长度。名称必须以零终止，并且这个计数包括零。

名称

这是可变长度的名称，最多 128 字节，不包括零终止符。它与设备有关。在设备中，名字不必是唯一的。

11.6 信道成员包

配置服务器使用这个包将信道成员通知给设备。为了简明起见，这个报文包括 IP 信道上所有 CN/IP 设备的 IP 地址和端口号。一旦设备有 IP 地址列表，它就能将设备请求报文发送至请求完整配置列表中的每个设备。

表 16 示出信道成员包格式。

表 16 信道成员包格式

字节 0	字节 1	字节 2	字节 3
通用包首部			
日期时间			
发送列表日期时间			
MBZ			
列表大小		MBZ	
对于每个 CN/IP 设备，将下列字段重复一次			
IP 单播地址			
IP 单播端口		MBZ	
设备信道路由包的日期时间			

下面是对这个包中所有字段的描述。

日期时间

对这个信道建立信道成员包的日期时间。见 11.4 。

发送列表日期时间

对这个设备建立发送包的日期时间。见 11.4 。

MBZ

列表大小

CN/IP 设备表中的设备数量。

IP 单播地址

按网络字节顺序的 CN/IP 设备的单播 IP 地址。CN/IP 设备将侦听该地址上的入向单播 IP 包。

IP 单播端口

侦听单播 IP 报文时 CN/IP 设备使用的端口号。

设备信道路由包的日期时间

对能够访问配置服务器的设备来说，这是最新信道路由包的日期时间。用于决定是否从配置服务

器请求一个新信道路由包。

11.7 信道路由包

表 17 示出了信道路由包格式。

表 17 信道路由包格式

字节 0	字节 1	字节 2	字节 3
带有包类型的通用包首部（0x08）			
日期时间			
IP 多播端口		IP 单播端口	
IP 多播地址			
IP 单播地址			
IP 标志	CN 路由器类型	CN 标志	节点类型
唯一 ID 总字节数[U]		MBZ	
子网节点总字节数[S]		域总字节数[D]	
唯一 ID[0]	唯一 ID[1]	唯一 ID[2]	唯一 ID[3]
唯一 ID[4]	唯一 ID[5]	唯一 ID[6]	...[U-1]
对于每个节点地址(CN 节点地址)，重复下列字段			
子网号[0]	节点号[0]	域索引[1]	
唯一 ID 索引[0]		子网号[1]	节点号[1]
域索引[1]		唯一 ID 索引[1]	
子网号[S-1]	节点号[S-1]	域索引[S-1]	
唯一 ID 索引[S-1]		...	...
对于每个域(CN 域列表)，将下列字段重复一次			
子网掩码[0]	子网掩码[1]	子网掩码[2]	子网掩码[3]
子网掩码[4]	子网掩码[5]	子网掩码[6]	子网掩码[7]
...	...	...	...
子网掩码[28]	子网掩码[29]	子网掩码[30]	子网掩码[31]
组掩码[0]	组掩码[1]	组掩码[2]	组掩码[3]
...	...	...	...
组掩码[28]	组掩码[29]	组掩码[30]	组掩码[31]
域长度	MBZ	域[0]	域[1]
域[2]	域[3]	域[4]	域[5]

下面是对这个包中字段的描述。

日期时间

该字段的详细描述见 11.4。

IP 多播端口

当侦听多播 IP 包时，正在进行发送的 CN/IP 设备所使用的端口号。

IP 单播端口

侦听单播 IP 报文时正在进行发送的 CN/IP 设备所使用的端口号。

IP 多播地址

CN/IP 设备的多播 IP 地址。如果不支持，则为零。CN/IP 设备将侦听该地址上的入向多播 IP 包。

IP 单播地址

按网络字节顺序的 CN/IP 设备的单播 IP 地址。CN/IP 设备将侦听该地址上的入向单播 IP 包。

IP 标志

这个标志表示支持的 IP 功能，见 11.5。

CN 路由器类型

如果节点类型是一个路由器，该字段表示路由器的类型，见 11.5。

CN 标志

CN 标志掩码，见 11.5。

节点类型

该字段表示设备类型，见 11.5。

唯一 ID 总字节数

唯一 ID 的字节数目。必须是 6 个字节的倍数，6 个字节是唯一 ID 的大小。允许为零。

子网节点总字节数

CN 子网节点元素的字节总数。必须是 6 个字节的倍数，6 个字节是子网节点元素的大小。允许为零。

域总字节数

该字节表示报文中域元素的大小。根据要求，可以表示多个域。传递大于 548 个字节的包，见 10.2。每个域元素为：32＋32＋2＋6＝72 个字节，并且是固定长度。

唯一 ID

唯一 ID 被打包在一起，每个 6 个字节，用 CN 网络字节顺序表示。

CN 节点地址

这是一个 CN 节点地址列表，每个结构中都有一个字段。字段是：

a) CN 子网号(字节)；

b) CN 节点号(字节)；

c) 域列表的索引(16 比特位字)；

d) 对前面唯一 ID 列表的索引(16 比特位字)。

注：当全部考虑这 4 部分时，表中的每个表项必须是唯一的，但是如果任何部分不同，那么可以在表项中复制其他任何部分。例如，如果唯一 ID 索引不同，{域、子网、节点}可以出现多次。这就表示这个 CN 地址有多个唯一 ID。这是合法的，但很少使用。通常是，带有相同唯一 ID 索引，但 D、S 、N 部分不同的表项指示相同唯一 ID 的多重{域、子网、节点}地址。

CN 域列表

域的列表。每个域通过一个子网掩码、一个组掩码和一个域标识符表示。域的数目等于域总字节数字段除以报文的域结构大小(72 个字节)。报文中可以有多个域，受到包大小的限制。有关长报文的分段见 10.2。每个域用 72 个字节固定长度结构来表示。

子网掩码(CN 子网掩码)

子网掩码数组是一个 256 比特位(32 个字节)数组，每个子网掩码位对应一个 CN 子网。如果在数组中设置该比特位，那么路由器通过自身将包从 IP 信道转发至子网。

组掩码(CN 组掩码)

组掩码数组是一个 256 比特位数组，每个组掩码位对应一个 CN 组地址。如果在数组中设置该比特位，那么路由器通过自身将包从 IP 信道转发至该组。

域长度(CN 域长度)

域长度是0、1、3或6中的一个，并且与用字节表示的CN域标识符长度对应。

域(CN域标识符)

CN域标识符是以CN网络字节顺序表示的6个字节数组。如果域长度小于6个字节，那么用零填充标识符后面未使用的域字节成为6个字节。

11.8 请求包

表18详细说明了配置请求包的格式。根据正在请求哪种数据结构，改变通用包首部中的包类型值。

表18 配置请求包格式

字节0	字节1	字节2	字节3
通用包首部			
日期时间			
原因	请求ID		分段ID
当前日期时间			
IP单播地址			

日期时间

该字段的描述见11.4。

标志

比特位1,0:原因

如表19所示，原因代码可修改请求。

表19 请求原因代码

原因代码	描述	代码
REQUEST_NORMAL	如果数据是新的或数据为零，发送正常请求	0x00
REQUEST_VERIFY	请求验证数据，总是发送数据	0x01

比特位2:请求所有

如表20所示，原因代码可修改请求。

表20 请求数量代码

原因代码	描述	代码
REQUEST_ONE	如果要求多个分段，则请求一个分段	0x00
REQUEST_ALL	请求立即发送所有分段	0x01

比特位3:请求并删除

如表21所示，原因代码可修改请求。

表21 请求动作代码

原因代码	描述	代码
REQUEST_COPY	拷贝统计	0x00
REQUEST_MOVE	拷贝并清除统计	0x01

比特位4～7:保留。

请求ID

该请求源所应用的标签值，以便它可以唯一地区分对该请求的响应，见10.2。

分段ID

在请求可以包括多个响应包的信息中使用，见 10.2.2。

当前日期时间

该字段的描述见 11.4。如果有效数据比这个日期时间新，那么指示接收方发送数据。零表示总是发送被请求的数据。

单播 IP 地址

仅用于信道路由请求报文。否则 MBZ。表示将仅发送这个特定设备的信道路由。零表示将发送所有路由信息。(仅当 TCP 用于配置服务器通信时，这个选项有效。)

11.9 确认包

当对从其他设备接收到的报文进行响应时，CN/IP 设备使用这些报文。表 22 示出了确认报文的格式。TCP 连接上 ACK 的使用见 10.4.3.2。

表 22 确认包格式

字节 0	字节 1	字节 2	字节 3
带有包类型的通用包首部			
日期时间			
ACK 类型	请求 ID		分段 ID

下面是对这个包中字段的描述。

日期时间

这个字段的描述见 11.4。

ACK 类型

CN/IP 设备使用这个参数，以便在服务器上进一步进行请求。有效值包括：

——ACK_OK(0)

——ACK_FIXED(1)

——ACK_BAD_MESSAGE(2)

——ACK_CANT_COMPLY(3)

——ACK_DEVICE_REFUSED(4)

——ACK_NOT_SUPPORTED(5)

请求 ID

从请求返回的标签值，以便它可以唯一地区分对该请求的响应，见 10.2。如果不适用就为零。

分段 ID

从请求返回，表示与请求方的关联性，见 10.2。如果不适用就为零。

11.10 发送列表包

当设备请求获得 CN/IP 设备中的发送列表时，配置服务器发送该报文。

表 23 给出了发送列表包的格式。

表 23 发送列表包格式

字节 0	字节 1	字节 2	字节 3
通用包首部			
日期时间			
IP 地址端口对的数目	MBZ	MBZ	
对于每个地址/端口对，将下列字段重复一次			
IP 地址			
IP 端口		MBZ	

下面是对这个包中字段的描述。

日期时间

见 11.4。

IP 地址/端口对的数目

发送列表中 CN/IP 设备带有的 IP 地址/端口对的数目。允许为零。这里表示为多播或单播地址。

IP 地址

CN/IP 设备的 IP 地址或多播地址。CN/IP 设备将包发送至该地址。

IP 端口

发送包时 CN/IP 设备使用的端口号。

11.11 节点状态/正常/统计响应报文

表 24 给出了状态包的格式。

表 24 节点状态/正常/统计响应报文

字节 0	字节 1	字节 2	字节 3
通用包首部			
从前一个计数器复位开始的时间			
前一个计数器复位的时间,用 GMT			
信道成员数			
最近发送报文的信道上的成员数			
被接收的 CN 包数			
由于选择转发接收而丢弃的 CN 包数			
接收到的 CN 总字节数			
发送的 CN 包数			
发送的 CN 总字节数			
发送到 IP 信道上的 CN 包数			
发送到 IP 信道上的 CN 字节数			
IP 信道接收到的 CN 包数			
IP 信道接收到的 CN 字节数			
发送到 IP 网络上含有 LT 包的 IP 包数			
来自 IP 网络的含有 LT 包的 IP 包数			
至 IP 信道的平均聚合			
来自 IP 信道的平均聚合			
已发送的 UDP 包的数目			
已发送的 TCP 包的数目			
已发送的多播包的数目			
从 IP 丢弃的陈旧 LT 包数			
TCP 连接失败的次数			
具有不同 TCP 连接失败的主机数目			
已发送的路由器配置报文数目			
已接收到的路由器配置报文数目			

表 24(续)

字节 0	字节 1	字节 2	字节 3
配置改变的次数			
已发送的 UDP 包/秒的连续平均数			
已接收到的 UDP 包/秒的连续平均数			
已发送的 TCP 包/秒的连续平均数			
已接收到的 TCP 包/秒的连续平均数			

——从前一个计数器复位开始的时间。(格式:32 位无符号整数,秒)

——前一个计数器复位的时间。用 GMT。(格式:日期时间。见 11.4)

——信道上的成员数。(格式:32 位无符号整数)

——最近发送报文的信道上的成员数。(测量方法未定义。)(格式:32 位无符号整数)

——被接收的 CN 包数(从 CN 信道接收的包数)。(格式:32 位无符号整数)

——由于选择转发接收但丢弃的 CN 包数。(格式:32 位无符号整数)

——接收到的 CN 总字节数。(格式:32 位无符号整数)

——发送的 CN 包数。(发送到 CN 信道上的包数。)(格式:32 位无符号整数)

——发送的 CN 总字节数。(格式:32 位无符号整数)

——发送到 IP 信道上的 CN 包数。(格式:32 位无符号整数)

——发送到 IP 信道上的 CN 字节数。(格式:32 位无符号整数)

——从 IP 信道接收到的 CN 包数。(格式:32 位无符号整数)

——从 IP 信道接收到的 CN 字节数。(格式:32 位无符号整数)

——发送到 IP 网络上含有 LT 包的 IP 包数。(格式:32 位无符号整数)

——来自 IP 网络的含有 LT 包的 IP 包数。(格式:32 位无符号整数)

——至 IP 信道的平均聚合。(值被表示为一对 32 位无符号整数。)整个 LT 包<第 10 项>/整个 IP 包<第 14 项>。

——来自 IP 信道的平均聚合。(值被表示为一对 32 位无符号整数。)整个 LT 包<第 12 项>/整个 IP 包<第 15 项>。

注:由于所有参数是可选的,复制数据格式不是问题。可以选择不支持第 12 项、第 15 项,而支持第 17 项。

——已发送的 UDP 包的数目。(格式:32 位无符号整数)

——已发送的 TCP 包的数目。(格式:32 位无符号整数)

——已发送的多播包的数目。(格式:32 位无符号整数)

——从 IP 丢弃的陈旧 LT 包数。(格式:32 位无符号整数)

注:陈旧意味着在 IP 网络中的时间过长。

——TCP 连接失败的次数。(格式:32 位无符号整数)

——具有不同 TCP 连接失败的主机数。(格式:32 位无符号整数)

——已发送的路由器配置报文数目。(格式:32 位无符号整数)

——已接收到的路由器配置报文数目。(格式:32 位无符号整数)

——配置改变的次数。(格式:32 位整数)

——已发送的 UDP 包/秒的连续平均数。(格式:32 位整数)

——已接收到的 UDP 包/秒的连续平均数。(格式:32 位整数)

——已发送的 TCP 包/秒连续平均数。(格式:32 位整数)

——已收接到的 TCP 包/秒连续平均数。(格式:32 位整数)

附 录 A
（规范性附录）
与 GB/Z 20177.1 的关系

IP 信道上封装的包格式包括 CRC 字段在内的 L2Hdr 字段。它不包括前置码、BitSync 字段或 ByteSync 字段或 LineCodeViolation 位。在 GB/Z 20177.1 中可以找到这些包的规范。

如 GB/Z 20177.1 中定义的那样，本规范支持下列引用的寻址方式：

——唯一设备 ID-神经元 ID；

——域 ID-域 ID；

——子网 ID-子网 ID；

——节点 ID-节点 ID；

——组 ID-组 ID。

当使用 GB/Z 20177.1 时，关于同步的注意事项：

GB/Z 20177.1 是一个为设备实时控制设计的通信协议。因此，预期的结果是，在规定时间以内交付报文（根据应用要求）并且在该规定时间附近有最小的时间抖动。作为协议差错检测/恢复部分，具有重复报文检测特点，因此仅执行一次报文，不考虑单个报文传输事务中接收到的报文数目。

GB/Z 20177.1 中的重复检测是一个在发送方和接收方使用的算法。该标准中全面地描述了这个算法，这里仅给出简单概述，以便解决时间同步问题。

当发送方构建报文时，发送方查看其配置来决定协议服务。如果协议服务规定重复检测，发送方分配事务号，该事务号在发送方与接收方最近的通信中没有被使用，然后发送带有该事务号的报文。发送方还启动一个被称作事务定时器的定时器。当该定时器定时时间到时，将进行报文重试，除非被配置重试计数已被使用完或已经接收到一个响应。

当接收到报文时，接收方要查看该报文是否有现存事务。如果有现存事务，报文是重复的，是有响应的但不作处理。如果没有现存事务，分配新事务并启动接收定时器。当接收定时器定时时间到时，删除事务。一旦删除事务，任何带有与被删除事务中事务号相同号的新报文将被看作是新报文。

IP 网络没有设计成具有实时控制功能。为了支持实时应用，例如：IP 信道上的话音，利用帧首部中的 QOS（服务质量）字段扩展 IP 协议。但是该字段的含义没有标准化，因此不是所有的路由器都能适当地处理该字段。在本部分中，不能通过可靠地设置包中的 QOS 字段，在公共因特网上发送这个包，来实现较低时延、小的时间抖动的端到端服务。

如果在 IP 网络上对 GB/Z 20177.1 中的包使用隧道技术，随机延时就会加到这些包上，那么由于交付接收方解释为新包而不是重复的陈旧包，将导致 GB/Z 20177.1 协议失败。这些失败严重地影响应用。为了防止这些协议失败，所有 GB/Z 20177.1/IP 节点的时间同步选项能够依据本部分中的指令得以实现。为了确定同步必须达到何种精度，必须在整个 IP 分段上检查 GB/Z 20177.1 协议定时器，这个 IP 分段可能发生随机延时。GB/Z 20177.1 中的 B.3 表是 GB/Z 20177.1 网络的定时器值的表项集。按下列公式计算允许的最大抖动：

min（正在使用的接收事务定时器值-（重试 * 事务定时器值））

在检查所有节点对的地方，检查 IP 信道上的通信，通过设置配置定时器确定允许的最小时间抖动。此后，就能确定网络上所有节点必须为何种时间精度。进行这种计算要求知道抖动 IP 信道上通信的所有 GB/Z 20177.1 节点配置。这意味着在某种网络数据库中拥有所有配置信息。当没有这个配置信息时，可以使用另一种方法来避免陈旧包检测问题。如果连接至因特网的每个 LAN 上有一个时间服务器，该因特网能够从卫星或无线资源获得原子钟时间并将其用于 LAN 上的节点，每个 LAN 分段就能有极精确的时间，使未检出的陈旧包不成为一个问题。

CN/IP 设备应该使用下列端口号中的一个，已由 IANA 分配的端口号：

——1628/TCP；

——1628/UDP；

——1629/TCP；

——1629/UDP。

中 华 人 民 共 和 国
国家标准化指导性技术文件
控制网络 LONWORKS 技术规范
第 4 部分:基于隧道技术在 IP 信道上
传输控制网络协议的规范
GB/Z 20177.4—2006
*
中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.bzcbs.com
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.75 字数 80 千字
2006 年 11 月第一版 2006 年 11 月第一次印刷
*
书号:155066·1-28056 定价 19.00 元

GB/Z 20177.4-2006