CIP网络库

第2卷EtherNet / IP CIP的适配

1.2版

2006年5月

ODVA&ControlNet国际有限公司

CIP网络图书馆
第2卷：CIP的EtherNet / IP适配发行

号：PUB00002R2

开放DeviceNet供应商协会
1099高地驱动器，套房A，安阿伯，MI 48108-5002 USA电
话 1-734-975-8840
传真 1-734-922-0027
电子邮件 odva@odva.org
WEB www.odva.org

使用条款单个CIP网络的协议可以通过互联网在下列网站以标准收费方式获得：

www.odva.org - DeviceNet和EtherNet / IP的使用条款协议以及DeviceNet和EtherNet / IP网络的一般信息以及ODVA

www.controlnet.org - ControlNet使用协议条款以及ControlNet和ControlNet International的一般信息。

CIP网络库：卷2 CIP的EtherNet / IP适配

目录

修订

CIP网络库第2卷：CIP版本1.2的EtherNet / IP适配包含以下对版本1.1的更改。 请参阅此处所述页面上的更改栏以进行特定的修改。 注意：指定范围内的某些页面可能不包含任何更改。

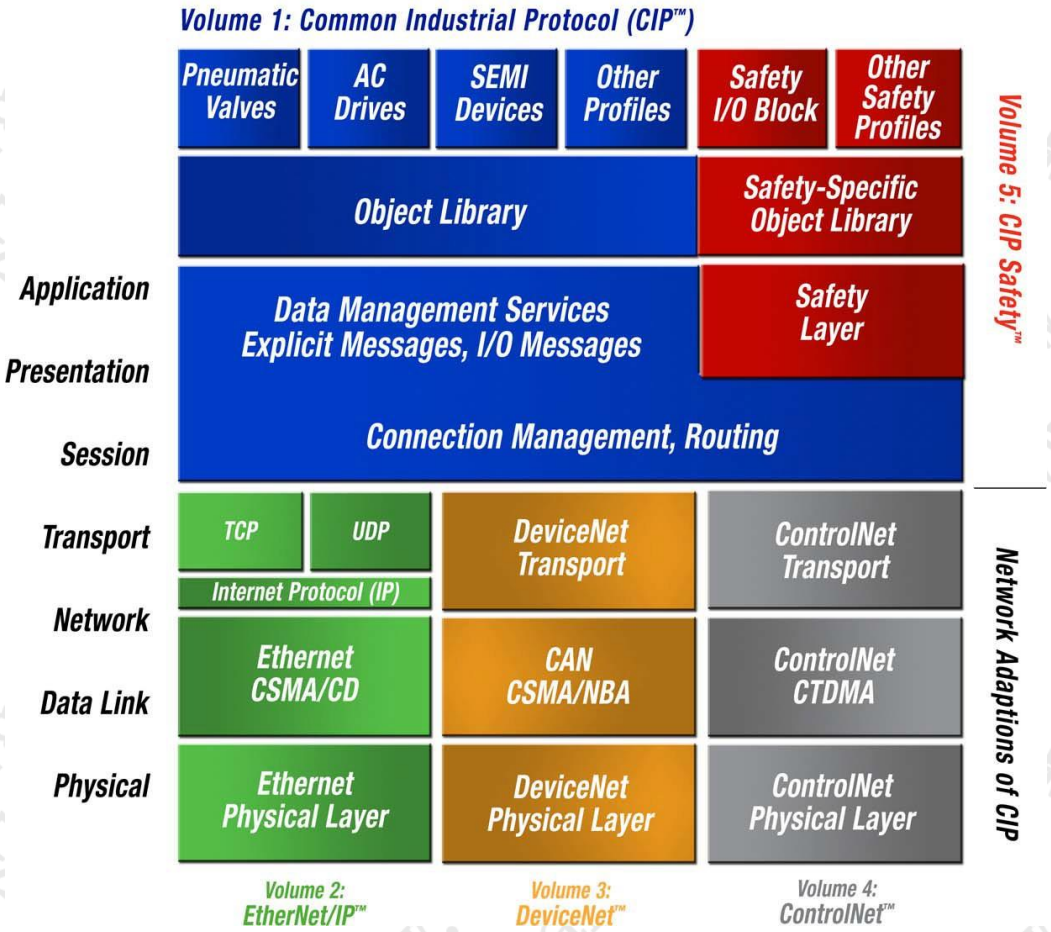
CHAPT教派	网页	描述
		TCP和EtherNet / IP I / O连接的连接
3-3.2.3	3-5	• 添加部分来描述到TCP连接的类0和1的关系
3-3.3	3-6	• 添加句子来描述到TCP连接的类2和3的关系
		IGMP行为
3-6	3-16, 17	• 添加了小节和小节
		EtherNet / IP安全参考
5-3.2.2	5-6	• 将属性7添加到实例属性列表
5-3.3.2	5-10, 11	• 修改Get_Attributes_All响应的描述
		网络连接ID的选择
3-3.7.1.1	3-8	• 将表格和新文本添加到部分。
		印刷错误/遗漏的更正
3-1	3-1	• 大写的通用工业协议
3	各个	• 将一些服务名称大写为一致

前言

CIP网络规范的组织

如今，三个网络（DeviceNet™，ControlNet™和EtherNet / IP™）使用通用工业协议（CIP）作为其网络协议的上层。 因此，管理这些网络的协会（ODVA和ControlNet国际）已经共同同意管理和分发CIP网络的规范，形成一个共同的结构，以帮助确保这些规范的一致性和准确性。

下图说明了CIP网络规范库的组织结构。 除了目前包含DeviceNet，ControlNet和EtherNet / IP的CIP网络之外，CIP Safety™还包括CIP的功能安全扩展。



这种常见的结构为CIP的每个网络适应提供了一个单独卷中的CIP。 CIP网络的规格是双卷集，配对如下所示。

EtherNet / IP规范包括：

第1卷：通用工业协议（CIP™）第2卷：CIP的EtherNet / IP适配

DeviceNet规范包括：

第1卷：通用工业协议（CIP™）第3卷：DeviceNet适配CIP

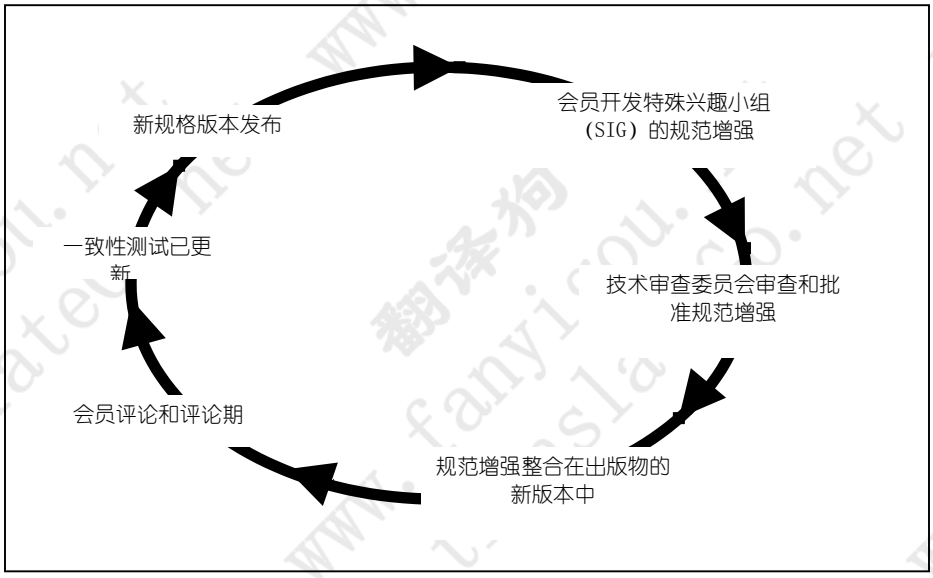
ControlNet规范包括：

第1卷：通用工业协议（CIP™）第4卷：CIP的ControlNet适配

CIP Safety™的规格分布在单一卷中：第5卷：CIP安全

规范增强过程

CIP网络的规格不断得到增强，以满足用户不断增长的特性和功能需求。 ODVA和ControlNet International也同意使用通用规范增强流程来运营，以确保所有CIP网络的开放和稳定的规范。 如下图所示，每个CIP网络规范全年都在进行此过程。 每个CIP网络规范的新版本都会定期发布。



第2卷：CIP的EtherNet / IP适配

第1章：EtherNet / IP简介

内容

1-1 介绍

EtherNet / IP（以太网/工业协议）是适用于工业环境的通信系统。 EtherNet / IP允许工业设备交换对时间要求严格的应用信息。 这些设备包括简单的I / O设备，如传感器/执行器，以及复杂的控制设备，如机器人，可编程逻辑控制器，焊机和过程控制器。

EtherNet / IP使用CIP（控制和信息协议），通用网络，传输和应用层也由ControlNet和DeviceNet共享。 EtherNet / IP则使用标准的以太网和TCP / IP技术来传输CIP通信数据包。 其结果是在开放和高度流行的以太网和TCP / IP协议之上建立了一个通用的开放式应用层。

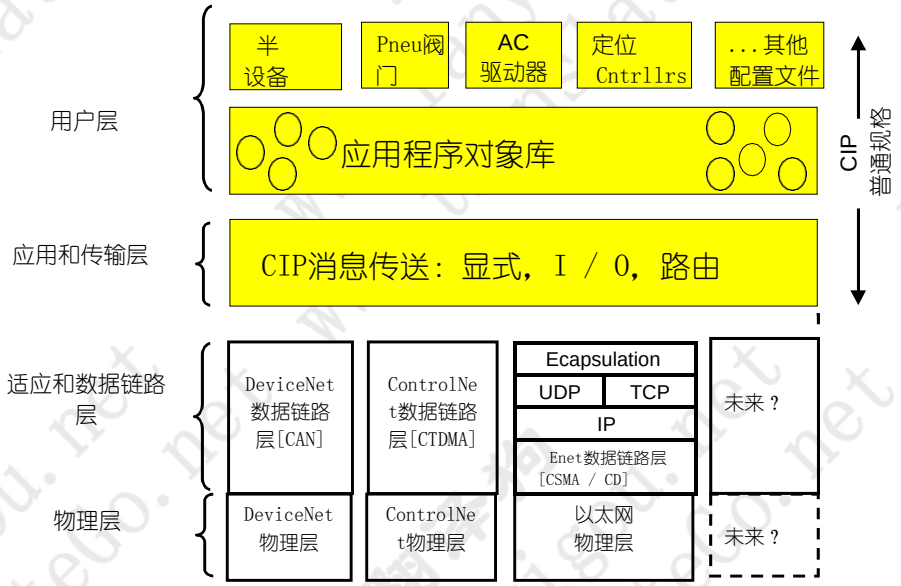
EtherNet / IP为时间关键控制数据的交换提供了生产者/消费者模型。 生产者/消费者模型允许在发送设备（例如生产者）和许多接收设备（例如消费者）之间交换应用信息，而不需要将数据多次发送到多个目的地。 对于EtherNet / IP，这是通过使用CIP网络和传输层以及IP多播技术来实现的。 许多EtherNet / IP设备可以从单个生产设备接收相同的生产应用信息。

EtherNet / IP使用标准的IEEE 802.3技术；没有非标准的增加，试图改善决定论。 相反，EtherNet / IP建议使用100 Mbps带宽和全双工操作的商用交换机技术，以提供更确定的性能。

注意：由于广泛的应用需求，EtherNet / IP不需要特定的实施或性能要求。 然而，目前正在制定一套标准的EtherNet / IP基准和度量标准，以衡量设备的性能。 这些测量可能成为产品电子数据表中的必要条目。 这些基准和指标的目标是帮助用户确定特定应用的特定EtherNet / IP设备的适用性。

下图说明了EtherNet / IP，DeviceNet和ControlNet如何共享CIP通用层。

图1-1.1 CIP公共概述



1-2 范围

EtherNet / IP规范分为以下章节：

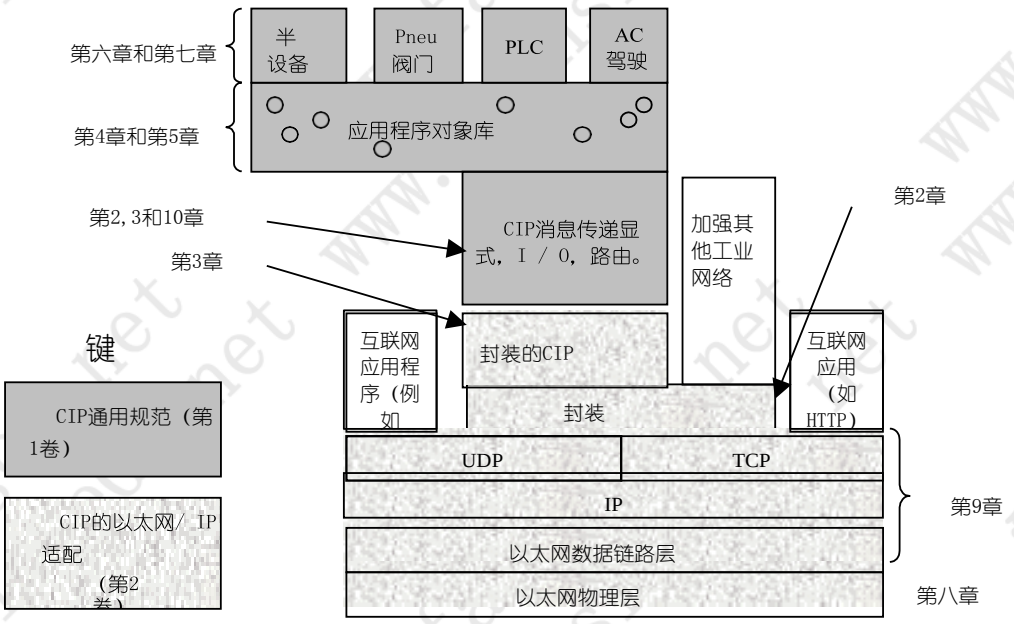
章节	标题	描述
1	介绍	规范的这一章。
2	封装协议	指定用于传输CIP数据包的封装协议通过TCP / IP网络。 本章中规定的封装协议也可以用来封装非CIP协议。
3	显式映射和I / O消息传递给TCP/IP	包含针对CIP网络和传输的EtherNet / IP特定添加层。 指定第2章中定义的封装协议用于通过TCP / IP传输CIP网络和传输层数据包网络。
4	对象模型	包含CIP对象模型的EtherNet / IP特定的添加。
5	对象库	使用特定于EtherNet / IP的对象补充CIP对象库。
6	设备配置文件	包含CIP设备配置文件库中特定于EtherNet / IP的添加。
7	电子数据表	指定添加EtherNet / IP所需的CIP EDS定义。
8	物理层	指定工业用途的媒体和物理层要求。
9	指标和中间图层	指定EtherNet / IP设备的TCP / IP要求。 这一章也是指定EtherNet / IP诊断的标准外观和行为LED指示灯。
10	桥接和路由	添加到CIP路由定义。

本章是EtherNet / IP简介。 下图显示了这些章节之间的关系以及CIP通用规范（由ODVA和ControlNet International单独出版）。 这个规范（第2卷）和CIP通用规范（第1卷）都需要完全指定一个EtherNet / IP产品。 本规范第2章中定义的封装协议也适用于封装其他工业协议，如下图所示。 但是，本发行版本中不包含封装其他协议的具体细节。

如图1-2.1所示，第2章中的封装协议使用TCP / IP层将其与网络介质隔离。 这样，封装协议可以在任何支持TCP / IP的介质上使用。 例如，封装协议可以在FDDI或PPP网络上运行。 第9章（指标和中间层）要求与RFC一致，该RFC记录了在特定网络上如何实现TCP / IP。 此外，第8章（物理层）将认证的EtherNet / IP实现范围缩小到10或100 Mb以太网上。 具体而言，章节记录了两种设备的一致性等级：一种称为“商业”，另一种称为“工业”。 其他一致性级别可以通过修改本规范来添加。

图1-2.1显示了EtherNet / IP规范的各个部分之间的关系。 如图所示，较暗的部分（第2-7章和第10章）主要由CIP共同规范（第1卷）记录。 CIP（第2卷）的EtherNet / IP适配的相应章节补充或修改了CIP通用规范的某些章节。 第2卷主要记录了浅阴影部分（第2,3,8和9章）。这些章节包含特别适用于EtherNet / IP设备的信息，但不一定适用于其他CIP网络上的信息（例如DeviceNet或ControlNet） 。

图1-2.1文档组织概览



1-3 参考

1-3.1 规范性参考文献

ISO 7498-1: 1984, 信息处理系统 - 开放系统互连 - 基本参考模型
ISO 7498 / AD1: 1987, 信息处理系统 - 开放系统互连 - 无连接数据传输
ISO 7498-3: 1987, 信息处理系统 - 开放系统互连 - 命名和寻址
ISO / IEC 8886: 1992, 信息技术 - 开放系统互连 - 系统间的电信和信息交换 - 数据链路服务定义
ISO / IEC 10039: 1990, 信息技术 - 系统间电信和信息交换 - 媒体访问控制服务定义
ISO / TR 8509: 1987, 信息处理系统 - 开放系统互连 - 服务惯例
ISO / IEC 10731: 1992, 信息技术 - 开放系统互连 - 定义OSI服务的公约
ISO 8802-2: 1989, 信息处理系统 - 局域网 - 第2部分: 逻辑链路控制
ISO / IEC 8802-3: 1993信息技术局域网和城域网第3部分: 碰撞检测载波侦听多路访问 (CSMA / CD) 接入方法和物理层规范
ISO / IEC 8802-4: 1990, 信息处理系统 - 局域网 - 第4部分: 令牌传递总线访问方法和物理层规范
ANSI X3.159-1989, 美国信息系统国家标准 - 编程语言C

1-4 额外的参考资料

"实时系统规范的策略"由DJ Hatley和IA Pirbhai CEN / CENELEC内部规定第3部分: 欧洲标准起草和呈现规则 (PNE规则) - 1991-09
RFC 768: 1980年8月, 用户数据报协议RFC
791: 1981年9月, 互联网协议
RFC 792: 1981年9月, 互联网控制消息协议RFC 793:
1981年9月, 传输控制协议
RFC 826: 1982年11月, 以太网地址解析协议
RFC 894: 1984年4月, 通过以太网传输IP数据报的标准RFC 1035: 1987, 域名 - 实施和规范
RFC 1103: 1989年6月, 通过FDDI网络传输IP数据报的建议标准RFC 1112: 1989年8月, IP多播的主机扩展
RFC 1117: 1989, 互联网号码
RFC 1122: 1989年10月, Internet主机要求 - 通信层RFC 1123: 1989年10月,
互联网主机要求 - 应用和支持RFC 1127: 1989年10月, 对主机要求的看法RFC
RFC 1171: 1990年7月, 通过点对点链接传输多协议数据报的点对点协议
RFC 1201: 1991年2月, 通过ARCNET网络传输IP流量RFC 1392: 1993年
1月, 互联网用户词汇表
RFC2236: 1997年11月, 互联网组管理协议, 版本2

1-5 定义

就本标准而言，下列定义适用。 有关其他定义，另请参见CIP通用规范第1章。

广播	网络上所有节点都愿意的特殊类型的多播包接收。 [来源：RFC1392]
广播风暴	一个不正确的数据包广播到一个网络上，导致多个主机一次全部响应，通常使用同样不正确的数据包，导致风暴的严重程度呈指数级增长。 [来源：RFC1392]
数据报	一个独立的，独立的数据实体，携带足够的信息从源端路由到目标计算机，而不依赖此源和目标计算机和传输网络之间的早期交换。 [来源：RFC1392]
封装	分层协议所使用的技术，其中一层将报头信息添加到来自上述层的协议数据单元（PDU）。 例如，在互联网术语中，一个数据包将包含一个来自物理层的头文件，其后是来自网络层（IP）的头文件，随后是来自传输层（TCP）的头文件，随后是应用程序协议数据。 [来源：RFC1208]
以太网络	最初由Xerox开发的10 Mb / s LAN标准，后来由Digital，Intel和Xerox（DIX）进行了改进。 所有的主机都连接到一个同轴电缆，在那里他们争夺网络访问使用载波侦听多路访问冲突检测（CSMA / CD）的范例。 另请参阅：802.x，局域网，令牌环。 [来源：RFC1392]
EtherNet / IP的	符合本规范的产品以及CIP通用规范被称为EtherNet / IP产品。 EtherNet / IP代表以太网工业协议。 [来源：RFC1392]
帧	单个数据传输在链路上。
MAC ID	以太网节点的48位物理地址
网络状态指示器	节点上的指示符指示物理层和数据链路层的状态。
网络地址或节点地址	链接上的节点的32位TCP / IP地址。 在大多数CIP网络中，该网络地址是MAC ID；但是，以太网并不是这种情况。 以太网的DLL有一个48位的MAC ID，它不被CIP通信栈直接使用。
港口	在EtherNet / IP特定上下文中，TCP或UDP端口是传输层解复用值。 每个应用程序都有一个唯一的端口号。 [来源：RFC1392] 有关该术语的其他定义，请参阅CIP通用规范。
多余的媒体	使用多种介质来防止通信失败的系统。
分割	在每一端通过分接头连接端接器的干线电缆部分；一个段没有活动的组件，不包括中继器。
收发器	节点内的物理组件，提供信号在介质上的传输和接收。

1-6 缩略语

对于本标准的目的，以下缩写适用。 有关其他缩写，请参阅CIP通用规范第1章。

FTP	文件传输协议。 使用TCP可靠的数据包传输在不同节点之间移动文件的Internet应用程序。 (不要和STP / FTP混淆)
LED	发光二极管
rcv	接收
RFC	征求意见稿 (RFC) – 1969年开始的文件系列，描述了互联网协议和相关实验。 并不是所有的 (实际上很少) RFC都描述了互联网标准，但是所有的互联网标准都被写成RFC。 RFC系列文件是不同寻常的，因为所提议的协议是由互联网研究和开发社区以自己的名义提出的，而不是由CCITT和ANSI等组织推动的正式审查和标准化的协议。 [来源: RFC 1392]
rx	接收
STP/FTP	屏蔽双绞线/箔双绞线
TCP	传输控制协议 (TCP) – STD 7，RFC 793中定义的Internet标准传输层协议。它是面向连接和面向流的，与UDP相反。 另请参见: 面向连接，面向流，用户数据报协议。 [来源: RFC1392]
Tx	发送
UDP	用户数据报协议 (UDP) – STD 6，RFC 768中定义的Internet标准传输层协议。它是一种无连接协议，为IP增加了可靠性和多路复用的级别。 另见: 无连接，传输控制协议。 [来源: RFC1392]
UTP	非屏蔽双绞线
Xmit	发送

第2卷：CIP的EtherNet / IP适配

第2章：封装协议

内容

2-1 介绍

本章（第2章）说明了在TCP / IP网络上封装工业协议的方法。 这种机制可以应用于CIP工业协议或其他网络。 本规范第3章详细介绍了这种封装协议在CIP中的应用。

关于OSI参考模型，这个封装协议居于第二层数据链路功能。

2-2 使用TCP和UDP

封装协议定义了所有EtherNet / IP设备都应支持的保留TCP端口号。 所有EtherNet / IP设备应在TCP端口号0xAF12上至少接受2个TCP连接。 一旦与TCP端口号0xAF12的TCP连接建立，通过TCP流发送的所有数据将按照2-3节规定的格式。

注意：TCP是基于流的协议。 允许发送几乎任何长度的IP数据包，它选择。 例如，如果将两个背靠背封装的消息传递给TCP / IP堆栈，则TCP / IP堆栈可以选择将封装的消息放在一个以太网帧中。 或者，可以选择将第一个消息的一半放在第一个以太网帧中，其余的放在下一个以太网帧中。 如图2-2所示，TCP用来封装两条消息。

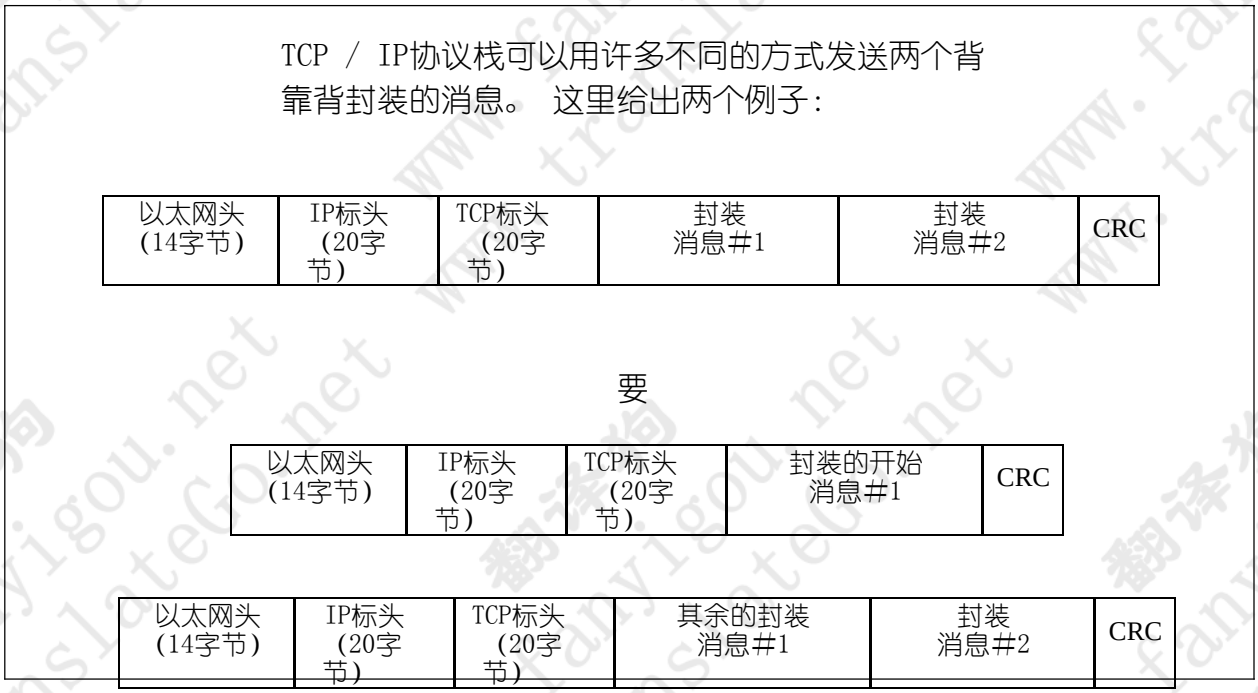


图2-2使用TCP封装两条消息

注意：本规范的目的不是记录TCP，UDP和IP传输机制的细节。 应该使用许多优秀的资源，包括整个说明书中引用的RFC来获取这些信息。

封装协议还定义了所有EtherNet / IP设备应支持的保留UDP端口号。 所有设备应接受UDP端口号0xAF12的UDP数据包。 由于与TCP不同，UDP不具有重新排序数据包的能力，因此，无论何时使用UDP发送封装的消息，整个消息都将在单个UDP数据包中发送。 在UDP端口0xAF12的单个UDP数据包中只能有一个封装的消息。

一些封装的消息只能通过TCP发送。 其他可能通过UDP或TCP发送。 有关哪些命令仅限于TCP的详细信息，请参阅“表2-3.2封装命令”。

2-3 封装消息

2-3.1 封装数据包结构

所有通过TCP发送或发送到UDP端口0xAF12的封装消息都应该由一个24字节的固定长度的头部和一个可选的数据部分组成。 总的封装消息长度（包括头部）应限制在65535字节。 其结构如下：

表2-3.1封装数据包

结构体	字段名称	数据类型	字段值
	命令	UINT	封装命令
	长度	UINT	消息数据部分的长度（以字节为单位），即消息头之后的字节数
	会话句柄	UDINT	会话标识（取决于应用）
	状态	UDINT	状态码
	发件人上下文	数组的八位字节	仅与封装命令的发送者有关的信息。 8的长度。
	选项	UDINT	选项标志
命令特定的数据	封装的数据	ARRAY 0到65511八位字节	消息的封装数据部分仅用于某些命令

封装消息长度不应该覆盖封装协议规定的长度限制。

注意：例如，即使封装，CIP UCMM消息仍然限制为504个字节。 参见CIP通用规范的第3章。

封装消息中的多字节整数字段应按小端字节顺序传输。

注意：这与标准Internet网络协议中使用的字节顺序不同，后者是big-endian。

尽管头部没有明确的信息来区分请求和回复，但是这个信息应该以两种方式之一来确定：

- 隐含地，通过命令和消息生成的上下文。 （例如，在RegisterSession命令的情况下，请求由发起者生成，目标生成应答）；
- 显式地由消息的数据部分中的封装的协议分组的内容来确定。

2-3.2 命令字段

命令代码的分配如下：

表2-3.2封装命令

码	名称	评论
0x0000	NOP	（可能仅使用TCP发送）
0x0001	预留给传统（RA）	
0x0002 和 0x0003	预留给传统（RA）	
0x0004	ListServices	（可以使用UDP或TCP发送）
0x0005	预留给传统（RA）	
0x0006 通过 0x0062	保留用于本规范的未来扩展（符合本规范的产品不得使用此范围内的命令代码）	
0x0063	ListIdentity	（可以使用UDP或TCP发送）
0x0064	ListInterfaces	可选（可以使用UDP或TCP发送）
0x0065	RegisterSession	（可能仅使用TCP发送）
0x0066	UnRegisterSession	（可能仅使用TCP发送）
0x0067 通过 0x006E	预留给传统（RA）	
0x006F	SendRRData	（可能仅使用TCP发送）
0x0070	SendUnitData	（可能仅使用TCP发送）
0x0071	预留给传统（RA）	
0x0072	IndicateStatus	可选（可能仅使用TCP发送）
0x0073	取消	可选（可能仅使用TCP发送）
0x0074 通过 0x00C7	预留给传统（RA）	
0x00C8 通过 0xFFFF	预留用于本规范的未来扩展（符合本规范的产品不得在此范围内使用命令代码）	

设备应接受它不支持的命令，而不中断会话或底层TCP连接。 指示收到不支持的命令的状态代码应该返回给消息的发送者。

注意：会话的建立在第2-5节中定义。 简而言之，一个会话在发起者和目标之间建立一个TCP / IP连接，通过这个连接可以发送封装命令。 由于TCP / IP连接被建模为一个字节流，所以封装头被预先添加到每个封装的数据包中，以便接收设备可以知道数据包开始和结束的位置。

2-3.3 长度字段

报头中的长度字段应指定消息数据部分的大小（以字节为单位）。 该字段应包含零不包含数据的消息。 消息的总长度应该是包含在长度字段中的数字加上封装头的24字节大小的总和。

即使长度对特定命令无效或超过目标的内部缓冲区，整个封装消息也应从TCP / IP连接中读取。

注意：未能读取整个消息可能会导致TCP字节流中的消息边界丢失跟踪。

2-3.4 会话句柄

会话句柄应由目标生成，并返回给发起者以响应RegisterSession请求。 发起方应将其插入到所有后续封装的数据包中（使用表2-3.2中列出的命令发送）到该特定目标。 在目标发起并向发起者发送命令的情况下，目标应该在发送给发起者的请求中包括该字段。

注：即使会话已建立，某些命令（即NOP）也不需要会话句柄。 该命令的描述中注明了是否需要特定的命令。

2-3.5 状态字段

状态字段中的值应指示接收者是否能够执行所请求的封装命令。 答复中的值为零表示成功执行该命令。 在发件人发出的所有请求中，状态字段应包含零。 如果接收方接收到一个非零状态字段的请求，则该请求将被忽略，并且不会产生应答。

注：此字段不反映消息的数据部分中包含的封装协议数据包生成的错误。 例如，在终端节点处理Set Attributes服务期间遇到的错误将通过CIP指定的错误机制返回（参见CIP公共规范的第3章）。

状态代码如下：

表2-3.3错误代码

状态码	描述
0x0000	成功
0x0001	发件人发出无效或不受支持的封装命令。
0x0002	接收器中的内存资源不足以处理命令。 这不是一个应用程序错误。 相反，只有在封装层无法获得所需内存资源的情况下才会导致此问题。
0x0003	封装消息的数据部分中的数据形成不良或不正确。
0x0004 – 0x0063	预留给传统（RA）
0x0064	向目标发送封装消息时，始发者使用了无效的会话句柄。
0x0065	目标收到一个无效长度的信息
0x0066 – 0x0068	预留给传统（RA）
0x0069	不支持的封装协议修订。
0x006A – 0xFFFF	预留用于未来扩展（符合本规范的产品不得使用此范围内的命令代码）

2-3.6 发件人上下文字段

命令的发送者应该在报头的发送者上下文字段中分配值。 接收方应在返回时不返回修改地返回该值。 没有预期回复的命令可能会忽略此字段。

注：命令的发件人可以在此字段中放置任何值。 它可以用来匹配请求和相关的回复。

2-3.7 选项字段

封装的数据包的发送者应将选项字段设置为零。 封装的数据包的接收者应验证选项字段为零。 接收方应丢弃具有非零选项字段的封装数据包。

注：该字段的意图是提供修改各种封装命令含义的位。 没有特别用于这个领域还没有被指定。

2-3.8 命令特定数据字段

注意：命令特定数据字段的结构取决于命令代码。 要组织他们的命令特定数据字段，大多数命令使用以下两种方法中的一种或两种：

1) 使用固定的结构
2) 使用通用的数据包格式（在第2-6节中描述）

通用的数据包格式允许命令以可扩展的方式构建它们的命令特定数据字段。

2-4 命令说明

2-4.1 NOP

发起者或目标可以发送NOP命令。 这个命令不会产生回复。 命令的数据部分长度应为0到65511字节。 接收方应忽略消息中包含的任何数据。

注意：NOP为发起者或目标提供了一种方式来确定TCP连接是否仍然打开。

NOP封装头应如下所示：

表2-4.1 NOP标题值

结构体	字段名称	数据类型	字段值
	命令	UINT	NOP（0x00）
	长度	UINT	数据部分的长度（从0到65511）
	会话句柄	UDINT	由于NOP命令不会生成回复，因此忽略该字段。
	状态	UDINT	应为0
	发件人上下文	数组的八位字节	由于NOP命令不会生成回复，因此忽略该字段。 8的长度。
	选项	UDINT	应为0
命令特定的数据	未使用的数据	数组的八位字节	未使用的数据

2-4.2 ListIdentity

2-4.2.1 一般

连接发起者可以使用ListIdentity命令来定位和识别潜在的目标。 这个命令应该使用UDP作为广播消息发送，不需要建立会话。

2-4.2.2 请求

ListIdentity请求应如下所示:

表2-4.2 ListIdentity请求

结构体	字段名称	数据类型	字段值
	命令	UINT	ListIdentity (0x63)
	长度	UINT	0
	会话句柄	UDINT	由于在发送ListIdentity请求之前不需要建立会话，所以该字段被忽略。
	状态	UDINT	0
	发件人上下文	数组的八位字节	0
	选项	UDINT	0

2-4.2.3 回复

为此命令定义了一个回复项目，即目标标识，项目类型代码为0x0C。 该项目应由所有支持CIP的设备支持（返回）。

List Identity命令的每个接收者都应该使用标准的封装头和数据进行回复，如下所示。 消息的数据部分应提供关于目标身份的信息。 答复应发送到收到广播请求的IP地址。

表2-4.3 ListIdentity应答

结构体	字段名称	数据类型	字段值
	命令	UINT	列表标识 (0x63)
	长度	UINT	0
	会话句柄	UDINT	忽视
	状态	UDINT	0
	发件人上下文	数组的八位字节	0
	选项	UDINT	0
	项目数量	UINT	要遵循的目标项目数量
		结构	接口信息
		UINT	项目类型代码
		UINT	物品长度
		数组的八位字节	项目数据

消息的数据部分应为通用数据包格式，其中包含一个2字节的项目计数，后跟一组提供目标身份的项目。

至少应该返回CIP身份项目，格式如表2-4.4。 该项定义的一部分遵循Identity Object的Get Attribute All服务响应定义（根据此对象的实例之一返回的数据），并且可能会在新成员添加到该服务响应时采用新成员。 与通用分组格式中的大多数字段不同，套接字地址字段应以大端顺序发送。

表2-4.4 CIP标识项

参数名称	数据类型	描述
项目类型代码	UINT	指示CIP标识的项目类型的代码（0x0C）
物品长度	UINT	后续项目中的字节数（长度因产品名称字符串而异）
封装协议版本	UINT	封装协议版本支持（也返回寄存器选择答复）。
	结构	套接字地址（请参阅第2-6.3.2节）
	INT	sin_family（big-endian）
	UINT	sin_port（big-endian）
	UDINT	sin_addr（big-endian）
	USINT的阵列	sin_zero（长度8）（big-endian）
供应商ID[1]	UINT	设备制造商供应商ID
设备类型[1]	UINT	设备产品类型
产品编号[1]	UINT	产品代码根据设备类型分配
修订[1]	USINT[2]	设备修订
状态[1]	字	设备的当前状态
序列号[1]	UDINT	设备的序列号
产品名称[1]	SHORT_STRING	设备的人类可读描述
国家[1]	USINT	设备的当前状态

[1]这些参数由Identity对象的相应实例属性进一步定义。 （参见CIP通用规范，第5章，对象库）

2-4.3 ListInterfaces

2-4.3.1 一般

连接始发者应使用可选的列表接口命令来标识与目标相关联的潜在的非CIP通信接口。无需建立会话来发送此命令。

2-4.3.2 请求

ListInterfaces请求应如下所示。

表2-4.5 ListInterfaces请求

结构体	字段名称	数据类型	字段值
	命令	UINT	列表接口 (0x64)
	长度	UINT	0
	会话句柄	UDINT	忽视
	状态	UDINT	0
	发件人上下文	数组的八位字节	0
	选项	UDINT	0

2-4.3.3 回复

如果支持，ListInterfaces请求命令的接收者应该回复一个标准的封装头和数据，如下所示。 该消息的数据部分被构造为通用分组格式，并且将提供关于与目标相关联的非CIP通信接口的信息。

表2-4.6 ListInterfaces回复

结构体	字段名称	数据类型	字段值
	命令	UINT	列表接口 (0x64)
	长度	UINT	0
	会话句柄	UDINT	忽视
	状态	UDINT	0
	发件人上下文	数组的八位字节	0
	选项	UDINT	0
	项目数量	UINT	要遵循的目标项目数量
		结构	接口信息
		UINT	项目类型代码
		UINT	物品长度
		数组的八位字节	项目数据

消息的数据部分应该是通用分组格式，其中包含一个2字节的项目计数，后面跟着提供接口信息的项目数组。 这个回复没有公开定义的项目。 被返回的特定于供应商的项目应至少返回一个由其他封装命令使用的32位接口句柄，例如SendRRData命令。

2-4.4 RegisterSession

2-4.4.1 一般

发起者应发送RegisterSession命令给目标发起会话。

注：有关建立和维护会话的详细信息，请参阅第2-5节。

2-4.4.2 请求

RegisterSession请求应如下所示：

表2-4.7 RegisterSession请求

结构体	字段名称	数据类型	字段值
	命令	UINT	RegisterSession (0x65)
	长度	UINT	4字节
	会话句柄	UDINT	0
	状态	UDINT	0
	发件人上下文	数组的八位字节	任何发件人上下文 8的长度。
	选项	UDINT	0
	协议版本	UINT	请求的协议版本应设置为1。
	选项标志	UINT	会话选项应设置为0 位0-7保留给传统 (RA) 位8-15保留给未来的扩展 注：该字段与封装标题中的选项标志不同。

2-4.4.3 回复

目标应该发送一个RegisterSession回复来表明它已经注册了发起者。 答复应与请求格式相同，如下所示：

表2-4.8 RegisterSession回复

结构体	字段名称	数据类型	字段值
	命令	UINT	RegisterSession (0x65)
	长度	UINT	4字节
	会话句柄	UDINT	由目标返回的句柄
	状态	UDINT	0
	发件人上下文	数组的八位字节	上下文从相应的RegisterSession请求中保存。 8的长度。
	选项	UDINT	0
	协议版本	UINT	请求的协议版本应设置为1。
	选项标志	UINT	会话选项应设置为0 位0-7保留给传统 (RA) 位8-15保留给未来的扩展 注：该字段与封装标题中的选项标志不同。

头部的Session Handle字段应包含一个目标生成的标识符，发起者应该保存并插入头部的Session Handle字段，以便对该目标的所有后续请求。 该字段只有在状态字段为零（0）时才有效。

报头的“发件人上下文”字段应包含原始发件人请求中存在的相同值。 如果始发者已经注册到目标，则状态字段应为零（0）。 如果目标无法注册，则状态字段应设置为0x69（不支持的封装协议修订版）。

如果发起者成功注册，协议版本字段应该等于所请求的版本。 如果目标不支持请求的协议版本，

- 该会议不得创建;
- Status字段应设置为不支持的封装协议0x69;
- 目标应返回“协议版本”字段中支持的最高版本。

如果支持所有请求的选项，Options字段将返回原始值。 该值应为零。

2-4.5 UnRegisterSession

发起者或目标都可以发送这个命令来终止会话。 当接收到这个命令时，接收器应该启动关闭TCP / IP连接。 当发起者和目标之间的传输连接终止时，会话也将被终止。 接收方应该在其最后执行任何其他相关的清理工作。 这个命令应该没有回复。

UnregisterSession命令格式如下:

表2-4.9 UnregisterSession命令

结构体	字段名称	数据类型	字段值
	命令	UINT	UnRegisterSession (0x66)
	长度	UINT	0字节
	会话句柄	UDINT	从RegisterSession回复处理
	状态	UDINT	应为0
	发件人上下文	数组的八位字节	任何发件人上下文 8的长度。
	选项	UDINT	应为0

会话句柄应设置为由原始的RegisterSession答复获得的值。 一旦客户端发送了这个命令，它将不再使用该句柄. .

注: 有关终止会话的更多详细信息，请参阅第2-5.3节。

2-4.6 ListServices

2-4.6.1 一般

ListServices命令应确定目标设备支持哪些封装服务类。

注：每个服务类都有一个唯一的类型代码和一个可选的ASCII名称。

2-4.6.2 请求

ListServices标题应如下所示：

表2-4.10 ListServices请求

结构体	字段名称	数据类型	字段值
	命令	UINT	ListServices (0x04)
	长度	UINT	0字节
	会话句柄	UDINT	忽视
	状态	UDINT	0
	发件人上下文	数组的八位字节	任何发件人上下文 8的长度。
	选项	UDINT	0

2-4.6.3 回复

接收者应该回复一个标准的封装消息，包括头部和数据，如下所示。 消息的数据部分应提供所支持服务的信息。

表2-4.11 ListServices答复

结构体	字段名称	数据类型	字段值
	命令	UINT	ListServices (0x04)
	长度	UINT	数据部分的长度
	会话句柄	UDINT	忽视
	状态	UDINT	0
	发件人上下文	数组的八位字节	从相应的ListServices请求中保存。 8的长度。
	选项	UDINT	0
	项目数量	UINT	要遵循的项目数量
	目标项目	结构	接口信息
		UINT	项目类型代码
		UINT	物品长度
		UINT	封装协议的版本应设置为1
		UINT	能力标志
		阵容16 USINT	服务名称

类型代码应按如下方式标识服务等级：

定义了一个服务类别，类型代码为0x100，名称为“Communications”。 该服务等级应指示设备支持封装CIP数据包。 所有支持封装CIP的设备都应支持ListServices请求和通信服务类。

注意：请参阅第2-6节了解项目的描述和所有保留项目代码的列表。

版本字段应指示目标支持的服务版本，以帮助维护应用程序之间的兼容性。

每个服务应该有一组不同的能力标志。 未使用的标志应被设置为零。 为通信服务定义的能力标志如下：

表2-4.12能力标志

标志值	描述
位0 – 4	保留给遗产（RA）
位5	如果设备支持通过TCP进行CIP报文封装，则应设置该位（= 1）。 否则，应清楚（= 0）
位6 – 7	保留给遗产（RA）
位8	支持CIP类0或1基于UDP的连接
位9 – 15	留作未来扩展

名称字段应允许最多16个字节，以NULL结尾的ASCII字符串，仅用于描述目的。16字节的限制应包括NULL字符。

2-4.7 SendRRData

2-4.7.1 一般

SendRRData命令应在发起者和目标之间传送封装的请求/应答包，发起者发起该命令。实际的请求/应答包应封装在消息的数据部分，由目标和发起者负责。

注：当用于封装CIP时，SendRRData请求和响应用于发送封装的UCMM消息（未连接的消息）。 更多细节见第三章。

2-4.7.2 请求

SendRRData头部应如下所示：

表2-4.13 SendRRData请求

结构体	字段名称	数据类型	字段值
	命令	UINT	SendRRData (0x6F)
	长度	UINT	数据部分的长度
	会话句柄	UDINT	Handle由RegisterSession返回
	状态	UDINT	0
	发件人上下文	数组的八位字节	任何发件人上下文 8的长度。
	选项	UDINT	0
	界面句柄	UDINT	CIP应为0
	时间到	UINT	操作超时
	封装的数据包	数组的八位字节	请参阅第2-6节中的通用数据包格式规范）

接口句柄应标识请求所针对的通信接口。 该封装CIP报文的句柄应为0。

超时到期后，目标应中止请求的操作。 当“超时”字段在1到65535之间时，超时值应设置为该秒数。 当“timeout”字段设置为0时，封装协议不应该有它自己的超时。 相反，它将依赖封装协议的超时机制。

说明：由于CIP为连接的报文提供了自己的超时机制，因此用于封装CIP报文时，超时字段通常设置为0。

封装的协议数据包应按照通用数据包格式进行编码，如第2-6部分所示。

2-4.7.3 回复

SendRRData应答如下所示，应包含响应SendRRData请求的数据。 对原始封装协议请求的回复应包含在SendRRData回复的数据部分中。

表2-4.14 SendRRData应答

结构体	字段名称	数据类型	字段值
	命令	UINT	SendRRData (0x6F)
	长度	UINT	数据结构的长度
	会话句柄	UDINT	句柄由RegisterSession返回
	状态	UDINT	0
	发件人上下文	数组的八位字节	从相应的SendRRData请求中保存。 8的长度。
	选项	UDINT	0
	界面句柄	UDINT	CIP应为0
	时间到	UINT	操作超时（未使用）
	封装的数据包	数组的八位字节	请参阅第2-6节中的通用数据包格式规范）

应答消息的数据部分的格式应与SendRRData请求消息的格式相同。

注：由于请求和回复共享一个通用格式，回复消息包含一个超时字段；但是，它不被使用。

2-4.8 SendUnitData

SendUnitData命令应发送封装的连接消息。 当封装协议具有自己的底层端到端传输机制时，可以使用此命令。 答复不予退回。 SendUnitData命令可以由TCP连接的任一端发送。

注：用于封装CIP时，SendUnitData命令用于在O T和T O两个方向上发送CIP连接的数据。

SendUnitData命令的格式如下：

表2-4.15 SendUnitData命令

结构体	字段名称	数据类型	字段值
	命令	UINT	SendUnitData (0x70)
	长度	UINT	数据部分的长度
	会话句柄	UDINT	Handle由RegisterSession返回
	状态	UDINT	0
	发件人上下文	数组的八位字节	任何发件人上下文 8的长度。
	选项	UDINT	0
	界面句柄	UDINT	应为0
	时间到	UINT	应为0
	封装的数据包	数组的八位字节	请参阅第2-6节中的通用数据包格式规范)

接口句柄和超时值应设置为零。 由于在接收到SendUnitData命令时没有生成应答，因此不使用超时字段。

2-5 会话管理

2-5.1 TCP封装会话的阶段

封装会话有三个阶段:

- 建立会议;
- 保持一个会话;
- 关闭会议。

2-5.2 建立会议

会话建立应按照以下步骤进行:

- 发起方应使用保留的TCP端口号（0xAF12）或者如果指定，从连接路径中指定TCP端口号（指定备用TCP端口号的方法在第3章）;
- 发起者应发送一个RegisterSession命令给目标（关于RegisterSession命令的描述见2-4.4节）。
- 目标应检查命令消息中的协议版本，以验证它支持与发起者相同的协议版本。 如果不是，则目标应该返回带有适当的状态字段和最高支持的协议版本的RegisterSession;
- 目标应分配一个新的（唯一的）会话ID，并向发起者发送一个RegisterSession回复。

2-5.3 终止会话

发起者或目标可以终止会话。 会议将以以下两种方式之一终止:

- 发起者或目标应关闭底层的TCP连接。 相应的目标或发起者应检测到TCP连接的丢失，并关闭其连接侧;
- 发起方或目标方应发送UnRegisterSession命令（请参阅2-4.4部分，了解UnregisterSession命令的说明），并等待检测TCP连接的关闭。 相应的目标或发起者应该关闭TCP连接的一端。 UnRegisterSession的发送者应检测到TCP连接的丢失，然后关闭其连接端。

注: 第二种方法是首选，因为它可以更及时地清理TCP连接。

2-5.4 维护一个会话

一旦会议成立，它应保持成立，直到发生下列情况之一:

- 发起者或目标关闭TCP连接;
- 发起者或目标发出UnRegisterSession命令;
- TCP连接中断。

2-5.5 TCP行为（资料性）

TCP是一种可靠的面向连接的协议。 如果连接两端的进程关闭连接的结束，则立即通知另一端的TCP。 如果从一个进程到另一个进程的消息无法在合理的时间内传递，则认为连接中断，并且在后续的所有发送和连接上接收到错误。

如果一个发起者进程检测到一个目标已经关闭了连接的结束或者连接中断了，它假定与目标的会话中断并关闭了它与目标的连接。 然后如上所述建立新的会话以恢复与目标的通信。

虽然在连接的另一端已关闭时通知始发进程，但只有在进程实际尝试通过连接发送消息时才能检测到连接断开。 在大多数情况下，发起者进程足够频繁地向目标发送消息，以及时检测到目标机器的崩溃。 同样，目标也经常发送消息给发起者，以便终止发起者进程和发起者机器崩溃。 但是，发起者或目标可能没有任何消息在相对较长的时间内在连接上发送。

TCP协议支持保活处理。 应用程序可以要求TCP确保连接在应用程序没有任何消息发送期间保持工作。 如果启用此功能，则当连接闲置一段时间后，TCP会向连接另一端的对等方发送保活消息。 如果TCP发送多个保持活动的消息并且没有收到回复，则TCP假定连接已经中断，并且通知应用程序，就好像它发送了超时的实际消息一样。

TCP / IP重试/超时处理的大多数实现都不会在连接上声明连接失败，直到它在几分钟内仍然不可用。 这是发起者主机上的TCP协议的一个特征；转身不要改变它。

2-6 通用数据包格式

2-6.1 一般

普通的数据包格式应该包括一个项目数，然后是一个地址项，然后是一个数据项（按该顺序），如下所示。 其他可选项目可能会随之而来

说明：常用的报文格式为采用封装协议传输的协议报文定义了标准格式。 常见的数据包格式是一个通用机制，旨在适应未来的数据包或地址类型。

表2-6.1通用报文格式

字段名称	数据类型	描述
项目数量	UINT	项目的数量（至少2）
地址项目	项目结构（见下文）	寻址封装数据包的信息
数据项	项目结构（见下文）	封装的数据包
可选的附加项目		

地址和数据项结构如下：

表2-6.2数据和地址项目格式

字段名称	数据类型	描述
类型ID	UINT	项目的封装类型
长度	UINT	以字节为单位的数据要遵循的长度
数据	变量	数据（如果长度> 0）

表2-6.3项目编号

物品ID号码	物品种类	描述
0x0000	地址	空（用于UCMM消息） 表示不需要封装路由。 目标是本地（以太网）或路由信息是在一个数据项。
0x0001 - 0x000B		预留给传统（RA）
0x000C		ListIdentity响应
0x000D - 0x0083		预留给传统（RA）
0x0084 - 0x0090		保留用于本规范的未来扩展（符合本规范的产品不得使用此范围内的命令代码）
0x0091		预留给传统（RA）
0x0092 - 0x00A0		保留用于本规范的未来扩展（符合本规范的产品不得使用此范围内的命令代码）
0xA1	地址	基于连接（用于连接的消息）
0x00A2 - 0x00A4		预留给传统（RA）
0x00A5 - 0x00B0		保留用于本规范的未来扩展（符合本规范的产品不得使用此范围内的命令代码）
0x00B1	数据	连接的传输包

物品ID号码	物品种类	描述
0x00B2	数据	未连接的消息
0x00B3 - 0x00FF		保留用于本规范的未来扩展（符合本规范的产品不得使用此范围内的命令代码）
0x0100		ListServices响应
0x0101 - 0x010F		预留给传统（RA）
0x0110 - 0x7FFF		保留用于本规范的未来扩展（符合本规范的产品不得使用此范围内的命令代码）
0x8000	数据	Sockaddr信息，发起者对目标
0x8001	数据	Sockaddr信息，目标发件人
0x8002		序列地址迭代
0x8003 - 0xFFFF		保留用于本规范的未来扩展（符合本规范的产品不得使用此范围内的命令代码）

2-6.2 地址项目

2-6.2.1 空地址项目

空地址项目应只包含类型ID和长度，如下所示。 长度应为零。 没有数据应该遵循这个长度。 由于空地址项不包含路由信息，所以在协议包本身包含任何必要的路由信息时应使用它。 空地址项目应该用于未连接的消息。

表2-6.4空地址项目

字段名称	数据类型	字段值
类型ID	UINT	0
长度	UINT	0

2-6.2.2 连接的地址项目

当封装的协议是面向连接的时候，这个地址项应该被使用。 数据应包含连接标识符。

注意：连接标识符在连接管理器的Forward_Open服务中进行交换。

表2-6.5连接的地址项目

字段名称	数据类型	字段值
类型ID	UINT	0xA1
长度	UINT	4
数据	UDINT	连接标识符

2-6.2.3 排序的地址项目

该地址项目应用于CIP传输类别0和类别1连接的数据。 数据应包含连接标识符和序列号。

表2-6.6顺序地址项目

字段名称	数据类型	字段值
类型ID	UINT	0x8002
长度	UINT	8
	UDINT	连接标识符
	UDINT	序列号

2-6.3 数据项目

2-6.3.1 未连接的数据项目

封装未连接消息的数据项应如下所示：

表2-6.7未连接的数据项目

字段名称	数据类型	字段值
类型ID	UINT	0xB2
长度	UINT	未连接消息的长度（以字节为单位）
数据	变量	未连接的消息

注：“数据”字段的格式取决于封装的协议。 当用于封装CIP时，**“数据”**字段的格式是消息路由器请求或消息路由器回复的格式。 有关UCMM消息封装的详细信息，请参阅本规范的第3章。 有关消息路由器请求和回复数据包的格式，请参阅CIP公共规范的第2章。

封装头中的上下文字段应用于未连接的请求/应答匹配。

2-6.3.2 关联的数据项

封装连接的传输数据包的数据项应如下所示：

表2-6.8连接的数据项目

字段名称	数据类型	字段值
类型ID	UINT	0xB1
长度	UINT	传输包的长度（以字节为单位）
数据	变量	传输包

注：“数据”字段的格式取决于封装的协议。 当用于封装CIP时，**“数据”**字段的格式是连接数据包的格式。 有关连接数据包封装的详细信息，请参阅本规范的第3章。 有关连接数据包的格式，请参阅CIP通用规范的第3章。

2-6.3.3 Sockaddr信息项目

Sockaddr Info项目应该用于封装目标和发起者之间发送数据报（连接的数据）所需的套接字地址信息。 对于发起者到目标和目标到发起者套接字信息有单独的项目。

Sockaddr信息项目应具有以下结构：

表2-6.9 Sockaddr项目

字段名称	数据类型	字段值
类型ID	UINT	O8T为0x8000，T8O为0x8001
长度	UINT	16（字节）
sin_family	INT	应为AF_INET = 2。该字段应以大端顺序发送。
sin_port	UINT	应设置为用于发送此CIP连接的数据包的TCP或UDP端口。 该字段应以大端顺序发送。
sin_addr	UDINT	应设置为将发送此CIP连接的数据包的IP地址。 该字段应以大端顺序发送。
的sin_zero	USINT的阵列	应为0.该字段应以大端顺序发送。 8的长度。

注意：Sockaddr项目的结构已从Winsock规范1.1版的sockaddr_in结构中图案化。

此页有意留为空白

第2卷：CIP的EtherNet / IP适配

第3章：显式和I / O消息传递到TCP / IP的映射

内容

3-1 介绍

EtherNet / IP规范的本章（第3章）介绍了第2章中对通用和工业协议（CIP）的封装应用。 具体来说，本章记录了UCMM和连接分组的封装；扩展路径的格式以包含IP地址；并限制哪些CIP传输参数可以组合使用。

3-2 CIP数据包通过TCP / IP

当CIP数据包的路径穿越Ethernet-TCP / IP网络时，封装的数据包将使用TCP / IP协议套件和第2章中定义的封装协议进行传输。

3-2.1 未连接的消息

UCMM包应通过TCP / IP连接，使用第2章中定义的封装协议进行传输。例如，封装的UCMM请求格式应如表3-2.1所示。

表3-2.1 UCMM请求

结构体	字段名称		数据类型	字段值
	命令		UINT	SendRRData (0x6F)
	长度		UINT	命令特定数据部分的长度
	会话句柄		UDINT	Handle由RegisterSession返回
	状态		UDINT	0
	发件人上下文		阵列8 八位字节	任何发件人上下文
	选项		UDINT	0
	界面句柄		UDINT	CIP应为0
	时间到		UINT	操作超时
		项目数量	UINT	由于使用了一个地址项目和一个数据项目，所以这个字段应该是2。
		地址类型ID	UINT	该字段应为0表示一个UCMM消息。
		地址长度	UINT	由于UCMM消息使用NULL地址项，所以该字段应为0。
		数据类型ID	UINT	该字段应该是0x00B2来封装UCMM
		数据长度	UINT	下一个字段的长度（以字节为单位）（MR请求分组的长度）
		MR请求包	USINT的阵列	该字段包含CIP公共规范第2章定义的CIP消息路由器请求包。

同样，UCMM应答的格式如表3-2.2所示。

表3-2.2 UCMM应答

结构体	字段名称		数据类型	字段值
	命令		UINT	SendRRData (0x6F)
	长度		UINT	命令特定数据部分的长度
	会话句柄		UDINT	Handle由RegisterSession返回
	状态		UDINT	0
	发件人上下文		阵列8 八位字节	从相应的UCMM请求中复制
	选项		UDINT	0
	界面句柄		UDINT	CIP应为0
	时间到		UINT	不用于回复
		项目数量	UINT	由于使用了一个地址项目和一个数据项目，所以这个字段应该是2。
		地址类型ID	UINT	该字段应为0表示一个UCMM消息。
		地址长度	UINT	由于UCMM消息使用NULL地址项，所以该字段应为0。
		数据类型ID	UINT	该字段应该是0x00B2来封装UCMM
		数据长度	UINT	下一个字段的长度（以字节为单位）（MR响应分组的长度）
		MR响应包	USINT的阵列	该字段包含CIP公共规范第2章中定义的CIP消息路由器回复包。

3-2.2 CIP传输类0和1类连接

注意：请参阅CIP通用规范，了解CIP传输类别0和类别1连接的定义和用法。

3-2.2.1 CIP传输类别0和类别1数据包

传输类0和类1连接的数据包应使用UDP和EtherNet / IP规范CIP第2章中定义的通用数据包格式进行传输。 组播连接的数据包应使用IP组播传输。

3-2.2.2 类别0和类别1连接的行为（资料性）

由于以太网没有发送调度数据的机制，所以类0和类1的几个重要方面如下所述：

在以太网上，CIP传输类别0或类1连接的数据包有可能丢失，例如由于过度的冲突。 根据定义，类0和类1连接不保证每个数据包的传递。 相反，生产者只需以指定的速率发送数据（API）。 如果数据包在类0或类1连接上丢失，则使用者从生产者接收下一个数据包。

丢包可以容忍的程度是特定于应用程序的。 以太网不适合那些不能容忍任何丢包的应用。

对于CIP传输类别1连接，消费CIP传输可以通过检查类别1数据包中的CIP序列号来检测数据包丢失。 对于0类连接，应用程序不可能知道特定的数据包已经丢失，因为0类不使用序列号。

连接超时机制在丢失太多数据包时向应用程序提供反馈。 连接超时由请求数据包间隔（RPI）和连接超时倍数决定。 如果在RPI指定的时间内没有接收到数据包，则连接超时倍数将超过连接。 例如，如果RPI为50毫秒，连接超时倍数为4，则如果在200毫秒内没有收到新的数据包（相当于丢失了4个数据包），则连接将超时。 较旧的数据包（具有较低CIP序列号的数据包）的接收将不会维持CIP连接。

任何特定连接的丢包程度将取决于与用户的以太网网络配置有关的许多因素。 进一步详细说明超出了本说明书的范围。

3-2.2.3 没有与TCP连接的链接

为了打开CIP传输类0或1连接，必须首先建立TCP连接和EtherNet / IP封装会话。 TCP连接用于发送Forward_Open服务并接收Forward_Open响应。 一旦打开TCP连接并建立了CIP传输类0和1连接，建议EtherNet / IP设备保持打开TCP连接。 如果TCP连接保持打开状态，则可用于后续通信，例如Forward_Close或其他显式消息。

虽然建议设备使TCP连接保持打开状态，但是用于打开传输类0或类1连接的TCP连接与产生的类0或类1连接之间不应有任何联系。 如果TCP连接关闭，则TCP连接的关闭不应导致目标或发起者关闭任何相应的CIP传输类0或1类连接。

3-2.3 CIP运输等级2和等级3连接

CIP传输类别2和类别3连接应通过使用第2章中定义的封装协议的TCP连接进行传输。

多个CIP连接可以通过单个TCP连接发送。 一个实现不需要支持每个TCP连接的特定数目的CIP连接。 一个实现可能会强加一个上限，如果它选择的话。

由于TCP的全双工性质，CIP发起者将目标（O T）和CIP目标发起者（T O）链路连接使用相同的TCP连接。 但是，如果一个目标随后发起一个CIP连接，那么它将被视为一个发起者，并且应该使用不同的TCP连接。

注：本标准没有定义TCP连接管理的要求，例如不活动超时，或者在所有本地连接关闭时关闭TCP连接。
但是，实现可以自由地实现这些。

3-2.4 CIP运输类别4至6

第2章中描述的封装协议不能用于封装CIP传输类别4,5和6。

3-3 连接管理器对象

3-3.1 连接参数

注：本节记录了连接管理器参数，这些参数具有特定于TCP / IP封装的要求。 连接管理器参数在CIP通用规范的第3章中有详细描述。

3-3.2 连接类型

CIP连接类型应为NULL，MULTICAST或POINT2POINT。 MULTICAST连接类型只能用于CIP传输类别0和类别1连接。

3-3.3 优先

CIP优先级应为LOW，或HIGH或SCHEDULED。 目前SCHEDULED的优先级应该和高优先级没有区别。

当相应的始发TCP连接关闭时，目标和始发者应关闭任何CIP传输类2或3连接。

注：以太网TCP / IP连接的SCHEDULED优先级可能会在未来进一步定义。

3-3.4 触发类型

CIP触发器类型应为CYCLIC，CHANGE_OF_STATE或APPLICATION。 使用CHANGE_OF_STATE触发的CIP传输类0和1类连接应使用生产禁止时间段（请参阅CIP公共规范）。

3-3.5 连接大小

CIP连接的大小不得大于65511字节。

注：Forward_Open请求将连接大小限制为511字节；但是，可选的Ex_Forward_Open允许更大的连接大小。

3-3.6 连接请求超时

为了可靠地建立延伸到TCP / IP链路上的CIP连接，连接请求超时应足够大以允许建立连接，这可能涉及解析主机名或经过多个网关。

由于TCP / IP上的连接请求处理的变化很大，连接路径中的CIP路由器不应该从连接请求超时中减去任何东西。

3-3.7 连接路径

TCP / IP连接路径段的链接地址部分应作为一个ASCII字符串编码在一个端口段中。以下表格全部得到支持：

- IP地址，例如“130.151.132.55”（IP地址的格式见RFC 1117）；
- IP地址用点符号表示，后跟一个“：”分隔符，后面跟着在指定的IP地址上使用的TCP端口号；
- 主机名称，例如“plc.controlnet.org”。 主机名应通过DNS请求解析到名称服务器（有关主机名和名称解析的信息，请参阅RFC 1035）；
- 主机名，后跟一个“：”分隔符，后面跟着在指定主机上使用的TCP端口号。

端口号应以十六进制或十进制表示。 十六进制应该用一个前导“0x”来表示。 当指定端口号时，应该使用它而不是用于封装协议（0xAF12）的标准端口号。 只有端口0xAF12保证在符合EtherNet / IP的设备中可用。

注意：其他TCP端口号可能被实现；然而，这个规范没有提供一个机制来确定设备支持哪个TCP端口号。 因此，不鼓励使用其他TCP端口号。 保证的TCP端口号0xAF12已经被互联网号码分配委员会（IANA）保留供封装协议使用。

由于端口段必须是字对齐的，因此字符串末尾可能需要填充字节。 填充字节应为0x00，不应在端口段的“可选地址大小”字段中计数。

注意：端口段的示例如表3-3.1所示（有关端口段的定义，请参见CIP通用规范）。

表3-3.1 TCP / IP链接地址示例

端口段	IP地址	笔记
[12][0D] [31][33][30][2E] [31][35][31][2E] [31][33][32][2E][31][00]	130.151.132.1	端口2，13的多字节地址 字节字符串加一个填充字节
[13][12] [70][6C][63][2E] [63][6F][6E][74][72][6F][6C][6E][65][74] [2E] [6F][72][67]	plc.controlnet.org	端口3，18的多字节地址 字节字符串，没有填充字节
[16][15] [31][33][30][2E] [31][35][31][2E] [31][33][32][2E] [35][35][3A] [30][78][33][32][31][30][00]	130.151.132.55:0x3210	端口6，21的多字节地址 字节字符串加一个填充字节
[15][17] [70][6C][63][2E] [63][6F][6E][74][72][6F][6C][6E][65][74] [2E] [图6F] [72] [67] [3A] [39][38][37][36][00]	plc.controlnet.org:9876	多字节地址端口5，32字节 字符串加上填充字节

3-3.7.1 网络连接ID 3-3.7.1.1

一般

对于EtherNet / IP连接，网络连接ID应为对选择该设备有意义的32位标识符。 网络连接ID不需要细分成任何特定的字段。

通常，消费设备选择网络连接ID来进行点对点连接，并且生产设备选择网络连接ID来进行多播连接。 下表显示哪个设备，目标或发起者，应该选择T->O和O->T网络连接ID：

表3-3.2网络连接ID选择

连接类型	哪个网络连接ID	谁选择连接ID
	发起人 - >目标	目标
	目标 - >发起者	鼻祖
	发起人 - >目标	鼻祖
	目标 - >发起者	目标

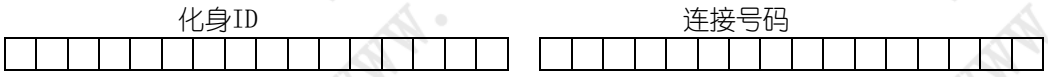
在连接关闭或超时之前，网络连接ID不能重复使用。 当设备重新启动时，不应重新使用以前打开的连接的网络连接ID，直到这些连接已关闭或超时。 只要网络中存在具有该连接ID的数据包，就不能重复使用特定的连接ID。

以下两节介绍了实现唯一网络连接ID的可能方法。

3-3.7.1.2 使用化身ID（资料）

本节介绍一种解决方案，防止设备重新启动时连接ID重复使用。 通过这个解决方案，以太网设备为类0和类1连接生成连接ID，格式如图3-3.1所示。

图3-3.1具有化身ID的连接ID



哪里：

连接号是一个16位的标识符，对于选择连接ID的设备是有意义的。

化身ID是每个设备在接受或发起任何连接之前生成的16位标识符。

当设备启动并接受连接时，化身ID仍然存在。 每个连续的加电周期都必须产生一个新的（唯一的）化身ID。 以下是生成化身ID的可接受的方法：

设备可以通过将化身ID保存在非易失性存储器中来生成唯一的化身ID：当设备加电时，其从非易失性存储器读取化身ID。 这是当前周期使用的化身ID。 然后它增加化身ID并存储下一个周期。 但是，请注意，非易失性存储器件通常对器件写入的次数有限制。根据设备的不同，每次上电写入化身ID可能是不可行的。

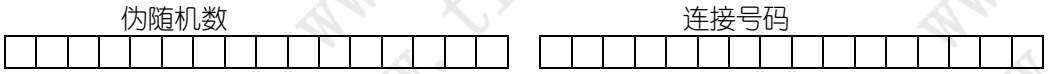
设备可以通过在上电时生成伪随机数来生成唯一的化身ID。 这种方法需要谨慎。 根据定义，生成的化身ID与前一个相同的概率是非零的。 但是，如果明智地做到了，这个概率就足够小了，不至于担心。

由于启动时间的巨大变化，诸如工作站的设备可以安全地使用系统时钟的值作为化身ID。 但是，对于嵌入式设备，使用系统时钟是不可靠的，因为固件通常在每次上电时都经历完全相同的指令序列。 这将导致相同的时钟值在选择化身ID的地方。 对于这些嵌入式设备，需要根据随机输入生成化身ID。 这最好使用伪随机数生成器（如MD5算法）完成。

3-3.7.1.3 每个连接的伪随机连接ID（资料性的）

本节介绍另一个解决方案，可以防止设备重新启动时连接ID重复使用。 使用此解决方案，每次需要类0或类1连接标识时，设备都会生成一个伪随机连接标识。 这种方法的连接ID格式如图3-3.2所示。

图3-3.2伪随机连接ID



哪里：

连接号是对选择连接ID的设备有意义的16位标识符。

伪随机数是使用适当的伪随机数生成器生成的16位数字。

使用这种方法，每次需要连接ID时，设备都会生成伪随机数部分。 应使用MD5算法[RFC 1321] [RFC 1750]等“强混合函数”生成伪随机数。 这些功能需要多个输入并产生伪随机输出。

为了防止连接ID在通电之间重复使用，MD5算法输入的种子值在连续的加电周期内必须是唯一的。 建议的方法是在收到第一个传入的连接请求时使用以下输入：

- 供应商ID，序列号，连接序列号
- sockaddr_in结构的内容（如果是出站连接，则为下一跳;如果为入站连接，则为发送者的内容）
- 系统时钟的值

注：假定以太网设备是网桥或连接的目标，如果设备是连接发起者，则不适用。 对于连接创建者来说，上述种子值在连续的通电时可能是相同的。 连接始发者必须使用另一个源来初始化种子值，否则使用化身ID方法。

根据定义，连接ID冲突仍然可能发生的概率是非零的。 但是，这个概率被降低了：

使用鲁棒的伪随机数生成器，如MD5算法。 在接下来的上电周期中确保

种子值是不同的。

3-3.8 用于CIP传输类2和类3连接的Forward_Open

CIP类2和类3连接的Forward_Open服务应使用第2章中定义的SendRRData命令通过TCP连接发送。

3-3.9 Forward_Open用于CIP传输类0和1类连接

3-3.9.1 一般

CIP传输类别0和类别1连接的Forward_Open服务应使用第2章中定义的SendRRData命令通过TCP连接发送。作为Forward_Open对话框的一部分，生产者和使用者应交换UDP端口号和IP多播地址（用于多播连接）必须发送CIP传输类别0和类别1连接的数据。 应使用第2章中定义的Sockaddr Info项来编码UDP端口号和IP多播地址。 Sockaddr信息项的使用取决于连接是多播还是点对点，以及连接发起者或连接目标是否是生产者。

对于多点传送连接，生产者应选择发送连接数据的IP多点传送地址。 端口号应为IANA分配的注册UDP端口号（0x08AE）。 IP组播地址和UDP端口号应通过Sockaddr信息项进行编码。 Sockaddr Info项目应与Forward_Open（如果连接始发者是生产者）或者Forward_pull_ply（如果连接目标是生产者）一起发送。

对于点对点连接，用户应选择一个UDP端口号，连接的数据将被发送到该端口号。 端口号可以是注册的端口号（0x08AE），或者可以是消费者选择的端口号。 端口号应该被编码在一个Sockaddr Info项中，并且应该与Forward_Open（如果连接发起者是消费者）一起发送，或者与Forward_Open_reply（如果连接目标是消费者）一起发送。

Sockaddr信息项目应置于SendRRData命令/回复中的Forward_Open和/或Forward_Open_reply数据之后。 如果Sockaddr信息项不存在或出错，则返回一个Forward_Open_reply，其状态码为0x01，扩展状态为0x205。

3-3.9.2 将连接映射到IP多播地址

注意：虽然不是必需的，但建议生产者为每个活动的多播连接使用一个唯一的IP多播地址。 根据实施情况，这可以减少消费者方面的连接筛选的数量。 它还允许消费者更均匀地服务来自多个连接的传入连接的数据。

由于不需要每个多播连接的唯一IP多播地址，消费者应能够处理来自多个多播连接的分组正被发送到相同的IP多播地址的情况。 消费者应能够根据连接ID和源IP地址来筛选传入的数据包。

注：筛选连接数据的要求在第3-4.3节中定义。

3-3.9.3 完成多播连接（资料性）

在接收到Forward_Open_reply之后，使用中的以太网设备应该加入所需的IP多播组，以接收IP多播数据报。 确切的做法取决于设备上使用的TCP / IP应用程序编程接口。

3-4 CIP传输类别0和1类连接数据

3-4.1 UDP数据报

CIP传输类别0和类别1数据包应使用第2章中定义的通用数据包格式以UDP数据报发送.CIP传输类别0和类别1数据包的UDP数据报的数据部分应如表3-4.1所示。

表3-4.1 Class 0和Class 1的UDP数据格式

字段名称	类型	值
项目数量	UINT	2
类型ID	UINT	0x8002（排序地址类型）
长度	UINT	8
	UDINT	连接ID（来自Forward_Open回复）
	UDINT	序列号
类型ID	UINT	0x00B1（连接的数据类型）
长度	UINT	数据包中的字节数
数据		0类或1类数据包

3-4.2 CIP传输类别0和类别1数据包排序

注意：根据定义，CIP类0和1类传输不检测无序数据包。 对于0类，每个数据包都被认为是新数据。 对于1级，仅检测到重复数据。 如果新的分组到达并且传输分组中的序列号与先前的分组不同，则新的分组被认为是新的数据，即使新的分组具有小于先前的序列号的序列号。

注：使用UDP传输CIP类0和1类连接的数据时，不能保证数据包以与发送的顺序相同的顺序到达。 当发送方和接收方都在同一个子网上时，数据包通常按顺序到达。 但是，当通过路由器时，当有一个数据包可能需要多个路径时，数据包可能无序到达。

对于通过以太网的0类和1类连接，设备应在3-4.1节定义的UDP有效载荷中保留一个序列号。 序列号应保持每个连接。 每当以太网设备发送一个CIP等级为1的数据包时，它应该增加该连接的序列号。 如果接收的以太网设备收到序号小于先前接收到的报文的报文，则丢弃序号较小的报文。 重复数据包应被接受并提供给传输层。

应用模块化算法对序列号进行操作，以处理序列翻转。

注意：在RFC793（TCP定义）中描述了处理32位序列号，如下所示：

要记住的是，实际的序列号空间是有限的，尽管非常大。 这个空间范围从0到2 ** 32 - 1。由于空间是有限的，所有涉及序列号的算术都必须以2 ** 32为模。 这个无符号算术保留了序列号在从2 ** 32 - 1再次循环到0时的关系。 计算机模运算有一些微妙之处，所以在编程比较这些值时应该非常小心。 符号“= <”意思是“小于或等于”（模2 ** 32）。

宏示例显示了这可能是如何完成的：

```
/*
 * TCP序列号是无符号32位整数操作
 * 与模块化算术。 这些宏可以
 * 用来比较这样的整数。
 */

#define SEQ_LT (a, b)     ( (int) ( (a) - (b) ) <0)
#define SEQ_LEQ (a, b)    ( (int) ( (a) - (b) ) <= 0)
#define SEQ_GT (a, b)     ( (int) ( (a) - (b) ) > 0)
#define SEQ_GEQ (a, b)    ( (int) ( (a) - (b) ) > = 0)
```

3-4.3 筛选传入连接的数据

接收0级和1级连接数据的以太网设备应根据发送设备的网络连接ID和IP地址对输入数据包进行屏蔽。 这是必要的，原因如下：

- 对于多播连接，没有保证的机制来防止多个设备使用相同的IP多播地址。 因此，设备可以从未建立连接的设备接收（伪造）多播连接的数据。
- 对于多播连接，允许设备为多个类0和类1多播连接使用相同的IP多播地址。
- 防止网络连接ID冲突。

当建立类0或类1连接时，目标和始发以太网设备应记录它们将接收连接数据的网络连接ID，以及连接另一端的设备的IP地址。 当设备收到连接的数据时，应确认网络连接ID对发送设备的IP地址有效。 否则，数据包将被丢弃。

3-5 IP组播范围和地址分配

3-5.1 背景（资料性的）

3-5.1.1 一般

本节讨论在以太网上实现多播连接时必须考虑的与IP多播有关的两个问题：IP多播范围和IP多播地址分配。

IP多播“范围确定”是指限制一个给定的多播数据报在网络上传播的范围。 IP多播地址分配是指应用程序如何获得IP多播地址，然后用于发送和接收多播数据报的问题。

3-5.1.2 当前的范围界定实践

在部署IP多播流量的“管理范围”的互联网标准之前（见第3-5.2节），实施将继续使用“TTL范围”将多播流量限制在某个期望的网络边界。

TTL范围是指使用IP头中的TTL字段限制组播流量的做法。 当发送IP组播流量时，主机可以根据数据包应该在网络上传播的程度将IP报头中的TTL字段设置为适当的值。 当数据包通过网络路由时，TTL字段在每一跳都递减。 路由器可以配置TTL阈值，使得它们不会转发数据包，除非剩余的TTL大于阈值。

具有一（1）的初始TTL的多播数据报实际上被限制为单个子网。

3-5.1.3 目前的地址分配实践

IP多播地址空间由互联网号码分配机构（IANA）管理。 IANA不会为EtherNet / IP所需的应用类型分配地址。 相反，IANA已经预留了多播地址空间中的一系列地址，而互联网工程任务组（IETF）已经开始设计一组协议（参见3-5.1.4节），以允许管理该地址空间在每个网站的基础上。

由于标准正在发展和尚未部署，目前应用程序唯一真正的选择是从IANA预留的地址空间中选择IP多播地址，并容忍与其他应用程序发生冲突的可能性。

3-5.1.4 不断发展的互联网标准

目前，有关IP组播地址分配和范围界定的Internet标准正在发展。 但是，似乎很清楚，最终成为标准的一般方法在下面列出的RFC和Internet草案中进行了规定（可在www.ietf.org上找到这些方法）。 请注意，互联网草案应被视为“正在进行中的作品”。

D.Meyer, “Administratively Scoped IP Multicast”, RFC 2365, July, 1998

上面的RFC定义了管理范围的IPv4多播空间，并为其管理描述了一组简单的语义。

Handley, Thaler, Estrin, “Malloc Architecture”, draft-handley-malloc-arch-00.txt, 1997年12月

上述草案提出了多播地址分配的架构。

Estrin, Govindan, Handley, Kumar, Radoslavov, Thaler, “多播地址集索赔（MASC）协议”draft-ietf-malloc-masc-01.txt, 1998年8月。

以上草案描述了一个可用于域间组播地址集分配的协议。

Handley, “Multicast Address Allocation Protocol”, draft-handley-aap-00.txt, 1997年12月。

上述草案定义了一种协议，用于解决多播地址分配服务器之间的域内多播地址分配的具体问题。

Patel, Shah, Hannah, “基于动态主机配置协议的多播地址分配”, draft-ietf-malloc-mdhcp-00.txt, 1998年8月。

上述草案定义了MDHCP协议，允许主机从组播地址分配服务器请求组播地址。MDHCP与DHCP类似。

利用上述Internet草案中指定的体系结构，以太网I / O设备将在运行时使用MDHCP来获取用于I / O连接的IP多播地址。

一旦IP多播分配体系结构变得标准化并被部署，本规范将根据情况进行更新。

3-5.2 临时范围策略

直到管理范围内的地址体系结构变得标准化和部署，发送0级或1级组播数据的设备将使用TTL范围，并将连接的数据报限制在一个单独的子网中。 这是最安全的方法，因为它可以防止不必要的多播流量影响其他子网。

采用这种方法，如果设备希望连接到不同子网上的设备，则应使用点对点连接。

3-5.3 临时分配策略

用于组播连接的IP组播地址应在IPv4组织本地范围：239.192.0.0/14（注意，高位/24保留用于相对分配）。

每台能够产生组播数据的设备都应选择一组IP地址用于组播连接。 IP组播地址的选择应采用以下两种机制之一：

- 用户可以使用一组IP地址显式地配置设备。 实际的配置机制是特定于产品的
- 设备可以根据以下算法自动选择一组基于其IP地址的组播地址：

根据主机的IP地址，每台主机都可以使用32个多播地址块。 如果正在使用子网掩码，则将子网掩码应用于IP地址以获取相对主机号：主机1使用239.192.1.0至239.192.1.31；主机2使用239.192.1.32到239.192.1.63等等。 （请注意，如上所述，范围区域中的前256个地址保留用于相关分配。）

为确保IP组播地址在组织本地范围内，如果子网掩码导致主机地址超过10位，则只使用低10位。 如果没有使用子网掩码，则使用IP地址的HOST ID部分。 对于TCP / IP类别A和B IP地址，仅使用IP地址的HOST ID部分的低10位，这使得不同的设备可以在相同的多播地址上生成数据。
接收设备必须能够容忍这个（见下文）。

没有机制阻止多个设备使用相同的IP多播地址。 因此，接收连接的组播数据的设备应根据连接ID和发送设备的IP地址来屏蔽连接的数据，如3-4.3节所述。

3-6 IGMP使用情况

3-6.1 背景（资料性的）

互联网组管理协议（IGMP）是主机用来报告其IP多播组成员身份的标准协议，并且必须由希望接收IP多播数据报的任何主机来实现。 IGMP消息由组播路由器使用，以了解哪些组播组在其所连接的网络上具有成员。 交换机也使用IGMP消息来支持“IGMP侦听”功能，交换机监听IGMP消息，并仅向已加入组播组的端口发送组播消息。

有两个版本的IGMP：

- IGMP V1在RFC1112中定义。 它定义了两条消息：主机成员查询和主机成员报告（通常称为“连接”）
- IGMP V2在RFC2236中定义。 它定义了额外的消息和行为，特别是离开组消息。

IGMP V2向后兼容V1。 RFC2236讨论了IGMP V1和V2主机和路由器之间的交互。

由于EtherNet / IP设备大量使用IP多点传送进行CIP传输级别0和1连接，所以为了创建功能良好的EtherNet / IP应用网络，EtherNet / IP设备对IGMP的一致使用至关重要。

3-6.2 IGMP成员报告消息

EtherNet / IP设备在打开CIP连接时将发出一个成员资格报告消息，在这个连接上它们将接收组播数据包。 具体来说，设备应坚持以下行为：

1. 当T> O连接类型是组播（发起者是组播消费者）时，发起者应当在收到成功的Forward_Open_reply时发布成员报告。 成员报告应包括在Forward_Open_reply中传送的IP多播地址。
2. 当O> T连接类型是组播（目标是组播消费者）时，目标应在发送成功的Forward_Open_reply时发布成员报告。 成员资格报告应包括在Forward_Open中传送的IP多播地址。

如果设备已经为IP多点传送地址发出了成员资格报告（例如，如果多点传送地址与现有连接一起使用），则设备可以（但不要求）发出另一个成员资格报告。

设备还应发送成员报告消息以响应成员查询消息，按照IGMP RFC。

3-6.3 IGMP离开组消息

支持IGMP V2的设备将在所有与消费IP多播地址关联的CIP连接已关闭或超时时发出离开组。 具体来说，设备应坚持以下行为：

1. 当T> O连接类型是组播（发起者是组播消费者）时，如果发起者在该IP组播地址上没有其他开放连接，发起者应当在收到成功的Forward_Close应答时发出离开组。
2. 当O> T连接类型是组播（目标是组播消费者）时，如果目标在该IP组播地址上没有其它打开的连接消耗，则目标应当在发送成功的Forward_Close应答时发出离开组。
3. 在连接超时的情况下，如果多播消费者没有其他连接消耗在该多播地址上，则多播消费者（无论是目标还是发起者）将发出离开组消息。

此页有意留为空白

第2卷：CIP的EtherNet / IP适配

第四章：对象模型

内容

4-1 介绍

EtherNet / IP规范的这一章包含了对EtherNet / IP特定的CIP对象模型的补充。 目前还没有这样的增加。

此页有意留为空白

第2卷：CIP的EtherNet / IP适配

第五章：对象库

内容

5-1 介绍

在这个标准中，对象建模用来表示设备的网络可见行为。 设备被建模为对象的集合。 每类对象都是相关服务，属性和行为的集合。 服务是对象执行的过程。
属性是由值表示的对象的特性，可以变化。 对象的行为是对象如何响应特定事件的指示。

规范的这一章包含了特定于EtherNet / IP的对象描述。 其余的对象描述可以在CIP公共规范中找到。 关于OSI参考模型，CIP对象执行第7层应用程序功能。 他们还提供了一个通过网络访问站点管理计数器的机制。

5-2 保留的类代码

其余类别代码在CIP通用规范中定义。

5-3 TCP / IP接口对象

分类代码：F5十六进制

5-3.1 范围

TCP / IP接口对象提供了配置设备的TCP / IP网络接口的机制。 可配置项目的示例包括设备的IP地址，网络掩码和网关地址。

与TCP / IP接口对象关联的底层物理通信接口应该是任何支持TCP / IP协议的接口。例如，TCP / IP接口对象可以与以下任何一个相关联：以太网802.3接口，ATM接口，运行SLIP的串行端口，运行PPP的串行端口等。TCP / IP接口对象提供了一个属性识别关联物理通信接口的链路专用对象。 通常期望链接专用对象提供链接专用计数器以及任何链接专用配置属性。

每个设备应该支持模块上每个支持TCP / IP的通信接口的TCP / IP接口对象的一个实例。 访问TCP / IP接口对象的实例1的请求应始终引用与接收请求的接口相关的实例。

5-3.2 属性

5-3.2.1 类属性

表5-3.1类属性

属性ID	需要实施	访问规则	名称	数据类型	属性描述	价值的语义
1至7	这些类属性是可选的，在卷1的第4章（CIP公共规范）中进行了描述。					

5-3.2.2 实例属性

表5-3.2实例属性

属性ID	需要在Implem	访问规则	名称	数据类型	属性描述	价值的语义
1	需要	得到	状态	DWORD	接口状态	见5-3.2.2.1节。
2	需要	得到	配置能力	DWORD	接口能力标志	能力标志位图。 参见5-3.2.2.2节。
3	需要	组	配置控制	DWORD	接口控制标志	控制标志的位图。参见5-3.2.2.3节

TCP/IP Object, Class Code: F5$_{Hex}$

属性 ID	需要在 Implem	访问 规则	名称	数据类型	属性描述	价值的语义
			物理链接对象	STRUCT 的:	物理链接对象的路径	参见5-3.2.2.4节
			路径大小	UINT	路径的大小	路径中的16位字的数量
			路径	填充 EPATH	标识物理链路对象的逻辑段	路径限制为一个逻辑类段和一个逻辑实例段。 最大大小是12个字节。 请参阅第1卷“逻辑段”的附录C.
			接口配置	结构:	TCP / IP网络接口配置。	见5-3.2.2.5节
			IP地址	UDINT	设备的IP地址。	值为0表示没有配置IP地址。 否则，IP地址应设置为有效的A，B或C类地址，且不得设置为环回地址（127.0.0.1）。
			网络掩码	UDINT	设备的网络掩码	值为0表示没有配置网络掩码地址。
			网关地址	UDINT	默认网关地址	值为0表示没有配置IP地址。 否则，IP地址应设置为有效的A，B或C类地址，且不得设置为环回地址（127.0.0.1）。
			名称服务器	UDINT	主要名称服务器	值为0表示没有配置名称服务器地址。 否则，名称服务器地址应设置为有效的A，B或C类地址。
			名称服务器2	UDINT	辅助名称服务器	值为0表示没有配置辅助名称服务器地址。 否则，名称服务器地址应设置为有效的A，B或C类地址。

属性ID	需要在Implem	访问规则	名称	数据类型	属性描述	价值的语义
			域名	串	默认域名称	ASCII字符。最大长度是48字符。 应该填补一个甚至字符数（垫不包括在内长度）。 长度为0应注明“不”域名是配置。
6	需要	组（Optiona湖 见5-3.2.2.6）	主机名	串	主机名	ASCII字符。最大长度是64个字符。 应填充到偶数字符（垫不包括在内长度）。 一段长度 0表示否主机名是配置。 看到第5-3.2.2.6节。
7	有条件的[1]		安全网络数	6个八位字节	请参阅CIP安全Specfication，第5卷，第3章	

1此属性是EtherNet / IP安全设备所必需的。 非安全装置不得执行此属性。

5-3.2.2.1 状态实例属性

状态属性是一个位图，应指示TCP / IP网络接口的状态。 有关与状态属性相关的对象状态的说明，请参阅第5-3.4节“行为”中的状态图。

表5-3.3状态属性

位（S）：	所谓的：	定义	
0-3	接口配置状态	指示“接口配置”属性的状态。	0 =接口配置属性尚未配置。 1 =“接口配置”属性包含有效的配置。 2-15 =保留以备将来使用。
4-31	保留的	保留以备将来使用，应设为零。	

5-3.2.2.2 配置能力实例属性

“配置能力”属性是一个位图，指示设备对可选网络配置功能的支持。 设备不需要支持任何一个特定的项目，但是必须至少支持一种获得初始IP地址的方法。

表5-3.4配置能力属性

位（S）：	所谓的：	定义
0	BOOTP客户端	1（TRUE）表示设备能够通过BOOTP获取其网络配置。
1	DNS客户端	1（TRUE）表示设备能够通过查询DNS服务器来解析主机名。
2	DHCP客户端	1（TRUE）表示设备能够通过DHCP获取其网络配置。
3	DHCP，DNS更新	1（TRUE）表示设备能够按照Internet草案<draft-ietf-dhc-dhcp-dns-12.txt>中的说明在DHCP请求中发送其主机名。
4	配置可设置	1（TRUE）表示接口配置属性是可设置的。 某些设备（例如PC或工作站）可能不允许通过TCP / IP接口对象设置接口配置。
5-31	保留的	保留以备将来使用，应设为零。

5-3.2.2.3 配置控制实例属性

配置控制属性是一个用于控制网络配置选项的位图。

表5-3.5配置控制属性

位（S）：	所谓的：	定义	
0-3	启动配置	确定设备在启动时如何获得其初始配置。	0 =设备应使用先前存储的接口配置值（例如，在非易失性存储器中或通过硬件开关等）。 1 =设备应通过BOOTP获取其接口配置值。 2 =设备在启动时应通过DHCP获取其接口配置值。 3-15 =留待将来使用。
4	DNS启用	如果为1（真），则设备应通过查询DNS服务器来解析主机名。	
5-31	保留的	保留以备将来使用，应设为零。	

设备不需要支持启动配置位的任何特定值，但设备必须至少支持一种获得初始TCP / IP接口配置的方法。

某些设备，特别是低端设备，可能会选择仅通过BOOTP或DHCP获取网络接口配置。 BOOTP和/或DHCP的使用可能不适用于所有设备。 特别是DHCP支持动态分配的IP地址，这可能导致设备每次启动时获得不同的IP地址。 此行为不适用于需要具有静态IP地址的设备。

设备可以通过BOOTP或DHCP获取其初始IP地址，然后将该地址保留在非易失性存储器中。 在通过BOOTP或DHCP接收到IP地址后，可以通过将启动配置位设置为0来保留地址。

开箱即用，设备可能希望通过除BOOTP或DHCP以外的其他方法获取其初始配置。 例如，设备可能希望通过连接的串行端口获得其初始配置。 在这种情况下，设备应该将其启动配置位设置为0，并将其接口配置属性字段设置为全0。 该设备应该等待被配置。

一旦设备启动并运行，当启动配置位的值为0时，设置接口配置属性的请求将导致设备将接口配置属性的内容存储在非易失性存储中（如果设备支持的话） 。 除非接口配置属性最低限度包含有效的IP地址，否则启动配置位不应设置为0。 否则，设备可能无法在网络上通信。

未来可能会采用其他标准配置方法，因为它们是由互联网社区开发和接受的。 非标准技术，包括依赖异常消息序列到达的各种形式的“IP拾取”，不得用于配置EtherNet / IP节点。

5-3.2.2.4 物理链接对象

该属性标识与底层物理通信接口（例如，802.3接口）关联的对象。 有两个组件属性：一个路径大小（在UINTs）和一个路径。 路径应包含逻辑段，类型类和逻辑段，类型实例标识物理链接对象。 最大路径大小是6（假设每个类和实例都有一个32位逻辑段）。

物理链路对象本身通常维护特定于链路的计数器以及任何链路特定的配置属性。 如果与TCP / IP接口对象相关的CIP端口具有以太网物理层，则该属性应指向以太网链路对象（类代码= 0xF6）的一个实例。 例如，路径可能如下所示：

表5-3.6示例路径

路径	含义
[20][F6][24][01]	[20] = 8位类段类型； [F6] =以太网链路对象类； [24] = 8位实例段类型； [01] =实例1。

5-3.2.2.5 接口配置

该属性包含作为TCP / IP节点运行所需的配置参数。 为了防止不完整或不兼容的配置，组成“接口配置”属性的参数不能单独设置。 要修改接口配置属性，用户应首先获取接口配置属性，更改所需的参数，然后设置属性。

TCP / IP接口对象应在完成Set服务后应用新的配置。 如果启动配置位（配置控制属性）的值为0，则新配置应存储在非易失性存储器中。 在值被安全地存储到非易失性存储器之前，设备不应答复设定的服务。 尝试将接口配置属性的任何组件设置为无效值（请参阅表5-3.2中的值的语义）应导致Set服务返回错误（状态码0x09）。

如果要通过BOOTP或DHCP获取初始配置，则接口配置属性组件应为全零，直到收到BOOTP或DHCP响应。 接收到BOOTP或DHCP应答后，接口配置属性应显示通过BOOTP / DHCP获得的配置。

设备不需要支持设置服务。 某些实现（例如，在PC或Workstation上运行的实现）无需支持通过TCP / IP接口对象设置网络接口配置。

接口配置属性的组件如下所述：

表5-3.7接口配置属性

名称	含义
IP地址	设备的IP地址。
网络掩码	设备的网络掩码。 当IP网络被分割成子网时，使用网络掩码。 网络掩码用于确定IP地址是否位于另一个子网上。
网关地址	设备默认网关的IP地址。 当目标IP地址在不同的子网上时，将数据包转发到默认网关以路由到目标子网。
名称服务器	主名称服务器的IP地址。 名称服务器用于解析主机名称。 例如，可能包含在CIP连接路径中。
名称服务器2	辅助名称服务器的IP地址。 辅助名称服务器用于主名称服务器不可用或无法解析主机名时使用。
域名	默认的域名。 解析未完全限定的主机名时使用默认域名。 例如，如果默认域名是“odva.org”，并且设备需要解析主机名称“plc”，则设备将尝试将主机名称解析为“plc.odva.org”。

有关IP寻址，子网，网关等的更多信息，请参阅Comer，Douglas E .； TCP / IP网络互联第1卷：协议和体系结构；恩格尔伍德悬崖，新泽西州； Prentice-Hall，1990。

5-3.2.2.6 主机名

“主机名”属性包含设备的主机名。 当设备支持DHCP-DNS更新功能并且配置为在启动时使用DHCP时，将使用主机名属性。 DHCP-DNS更新机制被指定为Internet草案<draft-ietf-dhc-dhcp-dns-12.txt>，并在Windows 2000中受支持。该机制允许DHCP客户端将其主机名传送到DHCP服务器。 DHCP服务器然后代表客户端更新DNS记录。

主机名属性不需要设置，设备正常运行。 主机名属性的值（如果已配置）应用于DHCP请求中FQDN选项的值。 如果“主机名”属性尚未配置，则设备不应在DHCP请求中包含FQDN选项。

对于不支持DHCP-DNS功能的设备，或未配置为使用DHCP的设备，则主机名称可用于提供信息。

当“接口配置”属性不可设置时，设置的访问是可选的。 某些设备（例如PC或工作站）可能不允许通过TCP / IP接口对象设置接口配置或主机名称。 如果该集合未实现，则响应于“设置属性单个”请求将返回“属性不可设置”（0x0E）错误。

5-3.3 共同服务

5-3.3.1 所有服务

TCP / IP接口对象应提供以下通用服务。

表5-3.8公共服务

服务码	需要实施		服务名称	服务描述
	类	例		
0x01	可选的	可选的	Get_Attribute_All	返回此对象属性的预定义列表（请参阅第5-3.3.2节中的Get_Attribute_All响应定义）
0x02	n/a	可选的	Set_Attribute_All	修改所有可设置的属性。
为0x0E	条件	需要	Get_Attribute_Single	返回指定属性的内容。
0x10	n/a	需要	Set_Attribute_Single	修改一个属性。

5-3.3.2 Get_Attribute_All响应

对于类属性，（因为只有一个类属性）应该返回类属性＃1。

例如属性，属性应按数字顺序返回，直到最后实现的属性。
Get_Attribute_All的回复如下：

表5-3.9 Get_Attribute_All

属性ID	字节大小	内容
1	4	状态
2	4	配置能力
3	4	配置控制
	2	物理链接对象，路径大小
	变量，最大12个字节	物理链接对象，路径（如果路径大小不为零）
	4	IP地址
	4	网络掩码
	4	网关地址
	4	名称服务器
	4	备用名称服务器
	2	域名长度
	变量， 等于域名长度	域名
	1	仅在域名长度为奇数时填充字节
	2	主机名称长度
	变量， 等于主机名长度	主机名
	1	只有主机名长度为奇数时才填充字节
7	6个八位字节	参见CIP安全技术规范第5卷第3章。 如果属性7未实现，则不存在。 当包含大于属性ID 7的附加属性时，应该为0。

物理链路对象路径，域名和主机名的长度在发出Get_Attribute_All服务请求之前是未知的。 实施者应准备接受包含物理链路对象路径（6个UINT），域名（48个USINT）和主机名（64个USINT）的最大尺寸的响应。

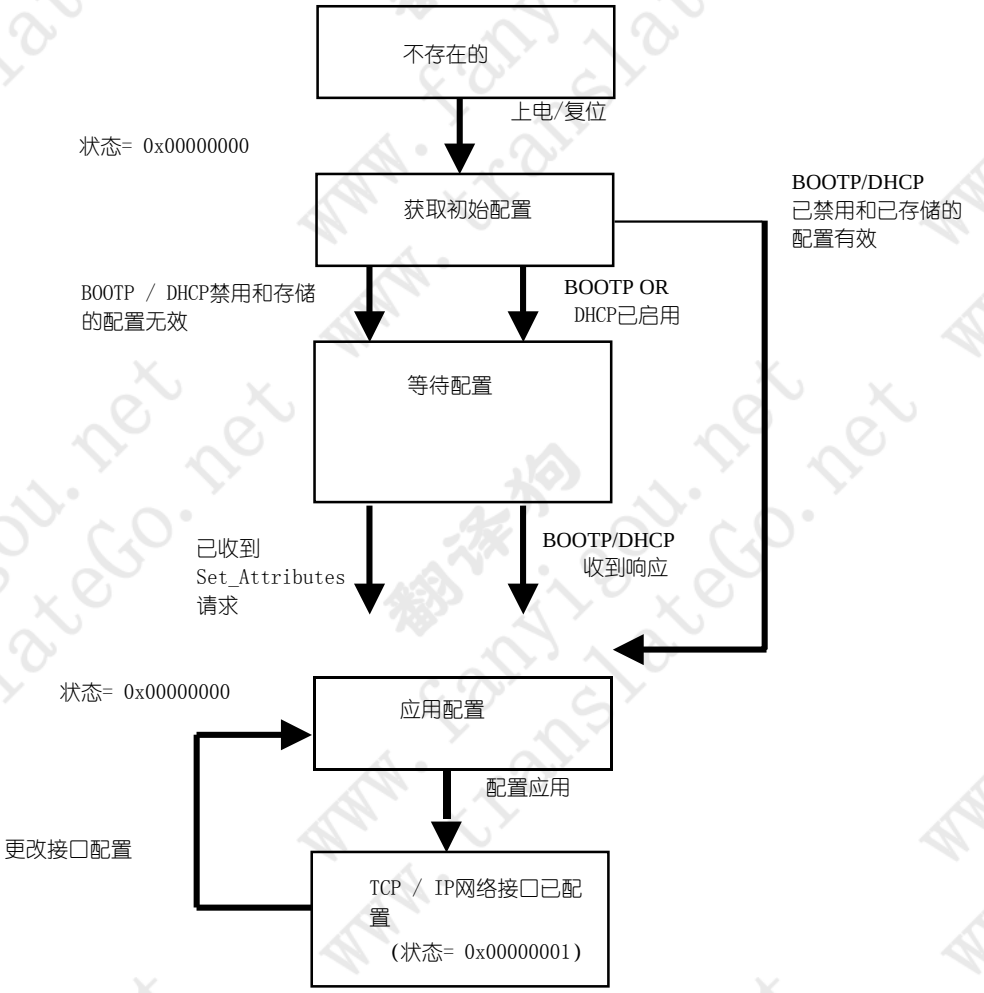
5-3.3.3 Set_Attribute_All请求

实例Set_Attribute_All请求包含“配置控制”属性，后面跟着“接口配置”属性。

5-3.4 行为

TCP / IP接口对象的行为应如下面的状态转换图所示。 请注意，通过BOOTP / TFTP获取初始可执行映像的行为不应被视为TCP / IP接口对象行为的范围之内。 设备可以自由地实现这种行为，但是应该被认为是在“不存在”状态下发生的。

图5-3.1显示TCP / IP对象行为的状态图



5-4 以太网链路对象

分类代码：F6十六进制

5-4.1 范围

以太网链路对象维护以太网的链路专用计数器和状态信息
802.3通信接口。 每个设备应该支持模块上每个以太网802.3通信接口的以太网链路对象的一个实例。 访问以太网链路对象实例1的请求应始终引用与接收请求的通信接口关联的实例。

5-4.2 属性

5-4.2.1 类属性

以太网链路对象应支持以下类属性。

表5-4.1类属性

属性ID	需要实施	访问规则	名称	数据类型	属性描述	价值的语义
1	需要	得到	调整	UINT	修改这个对象	分配给该属性的当前值是两（02）
2日至7日	这些类属性是可选的，在卷1的第4章（CIP公共规范）中进行了描述。					

读取“类修订”属性的错误意味着这是仅限修订版本1的实现。

5-4.2.2 实例属性

以太网链路对象应支持以下实例属性。

表5-4.2实例属性

属性ID	需要实施	访问规则	名称	数据类型	属性描述	价值的语义
1	需要	得到	接口速度	UDINT	目前正在使用的接口速度	以Mbps为单位的速度（例如，0, 10, 100, 1000，等等。）
2	需要	得到	界面标志	DWORD	接口状态标志	接口标志的位图。见部分5-4.2.2.1
3	需要	得到	实际地址	阵列6 USINTs	MAC层地址	见部分5-4.2.2.3

Ethernet Link Object, Class Code: $F6_{Hex}$

属性ID	需要实施	访问规则	名称	数据类型	属性描述	价值的语义
			接口计数器	STRUCT的:		见部分5-4.2.2.4
			在八位组中	UDINT	在接口上收到的八位字节	
			在Ucast数据包	UDINT	在接口上接收的单播数据包	
			在NUcast数据包	UDINT	在接口上收到非单播报文	
			在丢弃	UDINT	在接口上收到的入站数据包被丢弃	
			在错误	UDINT	包含错误的入站数据包（不包括在Discards中）	
			在未知的Protos	UDINT	具有未知协议的入站数据包	
			Out Octets	UDINT	在接口上发送的八位字节	
			出Ucast数据包	UDINT	在接口上发送的单播数据包	
			出NUcast数据包	UDINT	在接口上发送的非单播报文	
			丢弃	UDINT	出站数据包丢弃	
			出错	UDINT	包含错误的出站数据包	

属性ID	需要实施	访问规则	名称	数据类型	属性描述	价值的语义
			媒体柜台	STRUCT的:	媒体特定的计数器	见部分5-4.2.2.5
			对齐错误	UDINT	收到的帧长度不是整数个八位字节	
			FCS错误	UDINT	收到的帧没有通过FCS检查	
			单一碰撞	UDINT	成功传输经历了一次碰撞的帧	
			多重碰撞	UDINT	成功传输经历多次碰撞的帧	
			SQE测试错误	UDINT	生成SQE测试错误消息的次数	
			延期传输	UDINT	由于介质繁忙，第一次传输尝试被延迟的帧	
			迟到的碰撞	UDINT	检测到冲突的次数比传输数据包的时间晚512个比特	
			过度的碰撞	UDINT	由于过度冲突而导致传输失败的帧	
			MAC传输错误	UDINT	由于内部MAC子层传输错误而导致传输失败的帧	
			载波侦测错误	UDINT	载波侦听条件在尝试传输帧时丢失或从未断言的次数	
			框架太长	UDINT	收到的帧超过了最大允许的帧大小	
			MAC接收错误	UDINT	由于内部MAC子层接收错误，接口上接收失败的帧	
			接口控制	STRUCT的:	物理接口的配置	见部分5-4.2.2.6
			控制位	字	接口控制位	
			强制接口速度	UINT	接口强制运行的速度	以Mbps速度（10, 100, 1000等）

[1]如果Media Counters属性已实现，则需要Interface Counters属性。

5-4.2.2.1 界面标志

Interface Flags属性包含有关物理接口的状态和配置信息，如下所示:

表5-4.3接口标志

位 (S) :	所谓的:	定义
0	链接状态	指示以太网802.3通信接口是否连接到活动网络。 0表示不活动的链接； 1表示一个活动链接。 链接状态的确定是特定于实现的。 在某些情况下，设备可以通过硬件/驱动程序支持来确定链接是否处 在其他情况下，设备可能只能通过传入数据包来判断链路是否处于活动状态。
1	半/全双工	表示当前正在使用的双工模式。 0表示接口处于半双工状态； 1表示全双工。请注意，如果链接状态标志是0，那么半/全双工标志的值是不确定的。
2-4	谈判状态	链路自协商状态0 =正在进行自协商。 1 =自动协商和速度检测失败。 使用速度和双工的默认值。 默认值是依赖于产品的；推荐的默认值是10Mbps和半双工。 2 =自动协商失败，但检测到速度。 Duplex是默认的。 默认值是依赖于产品的；建议默认是半双工。 3 =成功协商速度和双工。 4 =未尝试自动协商。 强制速度和双工。
5	手动设置需要重置	0表示该接口可以自动激活链路参数变化（自动协商，双工模式，接口速度）。 1表示设备需要发送重置服务给其标识对象才能使更改生效。
6	本地硬件故障	0表示该接口没有检测到本地硬件故障。 1表示检测到本地硬件故障。 这个意思是产品特定的。 例如，AUI / MII接口检测到没有连接收发器，或者无线调制解调器检测不到连接的天线。 与链路状态的软性，可能的自我修正特性不活动相比，这被假定为需要用户干预的硬故障。
7-31	保留的	应该设置为零

5-4.2.2.2 接口速度

“Interface Speed”（接口速度）属性应指示接口当前运行的速度（例如，10 Mbps，100 Mbps，1 Gbps等）。应使用值0来指示接口的速度是不确定的。 属性的大小以Mbps为单位，所以如果接口运行速度为100 Mbps，那么接口速度属性的值应该是100.接口速度用来表示媒体带宽；如果接口运行在全双工模式下，该属性不能加倍。

5-4.2.2.3 实际地址

物理地址属性包含接口的MAC层地址。 物理地址是一个八位字节数组。 建议的显示格式是“XX-XX-XX-XX-XX-XX”，从第一个八位字节开始。 请注意，物理地址不是可设置的属性。 以太网地址应由制造商分配，并且应符合IEEE 802.3的要求。

5-4.2.2.4 接口计数器

接口计数器属性包含与在接口上接收数据包相关的计数器。 这些计数器应符合RFC 1213“MIB-II管理信息库”的定义。 接口计数器是一个条件属性；如果媒体计数器属性被执行，它们将被执行。

5-4.2.2.5 媒体柜台

媒体计数器属性包含特定于以太网媒体的计数器。 这些计数器应按照RFC 1643“类以太网接口类型的管理对象的定义”的定义。 如果实现这个属性，接口计数器也应该被实现。

5-4.2.2.6 接口控制

接口控制属性是一个由控制位和强制接口速度组成的结构，如下所示：

5-4.2.2.6.1 控制位

表5-4.4控制位

位(S)：	所谓的：	定义
0	自动协商	0表示802.3链路自协商处于关闭状态 1表示启用了自动协商。 如果禁用自动协商，则设备应使用强制双工模式和强制接口速度位指示的设置。
1	强制双面模式	如果自动协商位为0，则强制双工模式位指示接口是工作在全双工还是半双工模式。 0表示接口双工应该是半双工。 1表示接口双工应该是全双工。 不支持所请求双工的接口将返回一个GRC十六进制0x09（无效属性值）。 如果启用了自动协商，试图设置强制双工模式位将导致GRC十六进制0x0C（对象状态冲突）。
2-15	保留的	应该设置为零

5-4.2.2.6.2 强制接口速度

如果自动协商位为0，则强制接口速度位指示接口操作的速度。 速度以兆比特每秒指定（例如，对于10 Mbps以太网，接口速度应为10）。 不支持请求速度的接口应返回GRC十六进制0x09（无效属性值）。

如果启用了自动协商，试图设置强制接口速度将导致一个GRC十六进制0x0C（对象状态冲突）。

5-4.3 共同服务

5-4.3.1 所有服务

以太网链路对象应提供以下通用服务。

表5-4.5公共服务

服务码	需要实施		服务名称	服务描述
	类	例		
0x01	可选的	可选的	Get_Attribute_All	返回此对象属性的预定义列表（请参阅第5-4.3.2节中的Get_Attribute_All响应定义）
为0x0E	条件	需要	Get_Attribute_Single	返回指定属性的内容。
0x10	n/a	条件	Set_Attribute_Single	修改一个属性。

如果实现了类属性，则应该为类属性实现Get_Attribute_Single。

如果实现了接口控制属性，则应该执行Set_Attribute_Single服务。

5-4.3.2 Get_Attribute_All响应

对于类属性，由于只有一个可能的属性，因此Get_Attribute_All响应与Get_Attribute_Single响应相同。 如果没有实现类属性，则在答复的数据部分中不返回任何数据。

例如属性，属性应按数字顺序返回，直到最后实现的属性。 如果没有实现接口计数器和介质计数器属性，但是接口控制属性被实现，所有的0都应该被返回。

5-4.4 特定类别的服务

以太网链路对象应支持以下类别特定的业务：

表5-4.6特定于类别的服务

服务代码	需要实施		服务名称	服务描述
	类	例		
0x4C	n/a	条件[1]	Get_and_Clear	获取然后清除指定的属性（接口计数器或媒体计数器）。

[1]Get_and_Clear服务只有在实现接口计数器和媒体计数器的情况下才能实现。

5-4.4.1 Get_and_Clear服务

Get_and_Clear服务是一个特定于类的服务。 它只支持接口计数器和媒体计数器属性。 Get_and_Clear响应应该与指定属性的Get_Attribute_Single响应相同。 响应建立之后，属性的值应该被设置为零。

第2卷：CIP的EtherNet / IP适配

第6章：设备配置文件

内容

6-1 介绍

EtherNet / IP规范的这一章包含特定于EtherNet / IP的设备配置文件。

6-2 必需的对象

每个EtherNet / IP设备至少应实现以下每个对象的实例编号1:

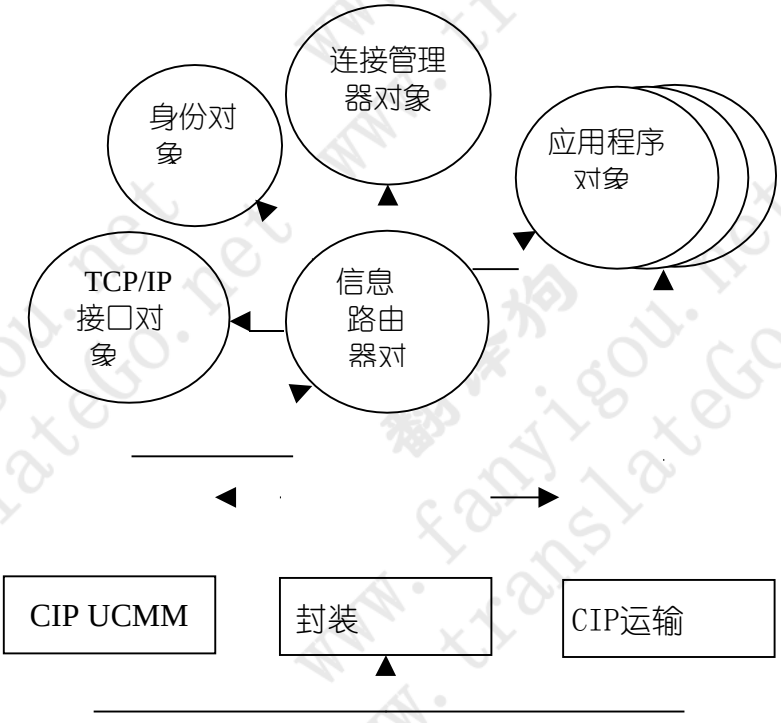
- 身份对象（类代码= 0x01）
- 消息路由器对象（类代码= 0x02）
- 连接管理器对象（类代码= 0x06）
- TCP / IP接口对象（类代码= 0xF5）和相应的链接对象

如果使用以太网介质，则相应的链路对象应为以太网链路对象（类别代码= 0xF6）。如果使用其他介质，供应商应定义供应商特定的链接对象。

注：本规范允许使用任何支持TCP / IP的介质；然而，这里只有以太网介质已经完全标准化了。 ODVA / CI未来可能会将经常使用的TCP / IP介质的其他链接对象标准化。例如，将来可能会定义一个标准化的PPP对象。

虽然它没有对象类代码，但每个设备也应实现CIP未连接消息管理器（UCMM）。

图6-2.1基础设备对象模型



此页有意留为空白

第2卷：CIP的EtherNet / IP适配

第7章：电子数据表

内容

7-1 介绍

EtherNet / IP规范的这一章包含了对EtherNet / IP特定的电子数据表（EDS）的定义的补充。 有关电子数据表格式的更多信息以及EDS相关术语（如EDS部分，EDS输入和EDS字段）的定义，请参阅CIP通用规范。

7-2 [设备分类]部分

在EDS的[Device Classification]部分中，对于任何符合EtherNet / IP的设备，至少应有一个ClassN关键字条目，其第一个字段设置为EthernetIP。 如图7-3.1所示，不存在子分类。

7-3 [端口]部分

在EDS的[Port]部分（例如参见图7-3.1），对应于EtherNet / IP兼容端口的PortN条目应设置如下：

“端口类型”字段的值应为“TCP”。

可选的“端口对象”字段应设置为此端口的TCP对象的路径。

除了CIP通用规范（第1卷）中的要求之外，没有其他要求放在**“**名称**”**和**“**端口号**”**字段中. .

注意：EtherNet / IP设备的EDS不能直接引用EtherNet / IP端口的链接对象（例如以太网链接对象），因为它可以通过端口的TCP对象引用。

图7-3.1 EtherNet / IP设备的EDS示例

```
[文件]
        DescText ="Widget EDS文
        件"; CreateData = 02-
        07-2001;
        CreateTime = 17:51:44;
        ModDate = 04-06-1997;
        ModTime = 22:07:30;
        修订版本= 2.1;
        HomeURL = "HTTP: //www.controlnet.org/EDS/12345.eds";
[设备]
        VendCode = 65535;
        VendName ="Widget-Works,
        Inc."; ProdType = 0;
        ProdTypeStr
        ="Generic"; ProdCode
        = 10;
        MajRev = 1;
        MinRev = 1;
        ProdName ="Smart-
        Widget"; 目录="1492-SW";
        Icon ="widget.ico";
[设备分类]
        Class1 = EthernetIP;

[港口]
        Port1 =
                TCP
```

第2卷：CIP的EtherNet / IP适配

第8章：物理层

内容

8-1 介绍

第8章为EtherNet / IP安装指定了EtherNet / IP介质和物理层。 在某些情况下，工业环境要求可能会超过办公室环境的要求。 可能需要增强产品和组件以提供支持工业应用所需的性能级别。 其中一些增强功能包括噪声抑制，密封，电压隔离，耐化学性，冲击，振动以及宽动态温度范围。

8-2 一般

以下部分将描述EtherNet / IP的物理层介质变体。 本标准没有规定同轴以太网组件或商用现货组件（COTS）的要求。 主要在信息系统和有限的控制应用中，同轴和COTS系统已经被部署到工业环境中。 这些系统大部分已经成功地提供了10 Mb / s的服务。 无论是提供10 Mb / s还是100 Mb / s的服务，COTS组件都被认可并被接受在本规范的指导范围内使用。 然而，测试表明，要在恶劣的环境中生存，如高噪声，多样的温度和化学品的存在，系统和组件的增强是必需的。

本文档定义了高达100 Mb / s的组件性能。 此处的组件规格针对10和100 Mb / s的数据速率进行了优化。 铜线应包括屏蔽和非屏蔽双绞线电缆技术。 第8-5.2节描述了铜双绞线的信号和耦合。

8-3 性能水平

第8-3.1节和第8-3.2节定义了两个级别的产品性能：COTS EtherNet / IP和Industrial EtherNet / IP。

注：本章中有很多部分指定了可选的要求。 这一部分将这些要求提炼成两个不同的层次：商用铜线和光纤以及工业EtherNet / IP铜线和光纤。

8-3.1 基于COTS的EtherNet / IP产品

ANSI / EIA / TIA 568 A和B应规定COTS电缆的要求。 基于铜线和光纤的COTS EtherNet / IP产品应符合EtherNet / IP规范的所有适用要求，包括第8-5节的物理层。 COTS组件的使用可能会降低系统性能。 使用此类产品或组件可能会导致工业控制应用程序的性能不理想

8-3.2 工业以太网/ IP产品

基于铜线和光纤的工业EtherNet / IP产品应符合EtherNet / IP规范的所有适用要求，包括第8-5节“工业EtherNet / IP媒体和物理层”。 对于要达到工业EtherNet / IP性能等级的产品，物理层应符合本章第8-6节所述的要求。

8-4 基于COTS的EtherNet / IP媒体和物理层

COTS组件的使用可能会降低系统性能。 使用此类产品或组件可能会导致工业控制应用程序的性能不理想。

8-4.1 铜媒体

8-4.1.1 铜介质附件（规范性引用文件）

基于ANSI / TIA / EIA-568 B.2标准的铜介质连接到EtherNet / IP网络应包括屏蔽或非屏蔽双绞线技术。 这些变体的信令和耦合应符合IEEE 802.3u / TP-PMD标准。

8-4.1.2 公开内部接口

IEEE 802.3u标准在物理层内定义了许多内部接口。 EtherNet / IP产品不需要直接实现这些接口中的每一个，而是应该表现为“好像”这些接口存在。 这些接口可以在节点内部，也可以在半导体器件内部。

8-4.1.3 电缆

屏蔽或非屏蔽双绞线电缆的性能应基于ANSI / TIA / EIA 568-B.2标准。

8-4.1.4 连接器

8-4.1.4.1 COTS RJ 45连接器变种

RJ45连接器是以太网系统的事实标准。 ANSI / TIA / EIA-568 B.2应规定COTS RJ 45连接器的要求。 另外IEC 60603-7定义了COTS RJ45连接器的机械要求。

8-4.1.5 拓扑约束

COTS双绞线系统的总永久链路长度限于90米（298英尺）。 永久链接应符合ANSI / TIA / EIA-568-B1。

COTS双绞线系统的总信道长度为100米（330英尺），包括ANSI / TIA / EIA-568-B.1中定义的跳线。 通道和跳线设计和测试应分别符合ANSI / TIA / EIA-568-B.1和B.2。

8-5 工业以太网/ IP媒体和物理层

8-5.1 环境要求

基于铜线和光纤的工业EtherNet / IP产品应符合表8-5.1中的环境要求。

表8-5.1最低环境规格

环境测试	标准	工业标准
振动（无包装）		IEC 60068-2-6
频率范围	10-500Hz	
促进	5g（可操作）	
移位	0.012英寸（pp）	
冲击（无包装）		IEC 60068-2-27
促进	30g（运营）	
	50克（不可操作）	
温度		
工作范围	-0℃分钟。 到+60℃分钟。 *	IEC 60068-2-1 IEC 60068-2-2
存储	-40至+85℃	IEC 60068-2-1 IEC 60068-2-2
湿度		IEC 60068-2-30
	5至95%的相对湿度。	
封口		
	最低IP 20	IEC 60529
耐电压（仅限连接器）		IEC 60512-1
联系人/联系方式	1000 Vd.c. 或交流高峰	
联系/测试面板	1500 Vd.c. 或交流高峰	

*温度低于0摄氏度或高于摄氏60度时，组件或拓扑结构降额

8-5.2 铜媒体

8-5.2.1 铜介质附件（规范性引用文件）

铜介质连接到EtherNet / IP网络应支持屏蔽或非屏蔽双绞线技术。 规范应包含基于ANSI / TIA / EIA_568-B类别5电缆性能等级的增强（如需要）。 这些变体的信令和耦合应符合IEEE 802.3u / TP-PMD标准中的规定，但要遵守本节（第8-5.2节）中列出的偏差。 同样，电缆的电气，机械和环境性能应符合第8-5.2.2节的规定。

8-5.2.1.1 公开内部接口

IEEE 802.3u标准在物理层内定义了许多内部接口。 EtherNet / IP产品不需要直接实现这些接口中的每一个，而是应该表现为“好像”这些接口存在。 这些接口可以在节点内部，也可以在半导体器件内部。

8-5.2.2 电缆

电缆对于在高噪声环境中影响网络性能至关重要。 为了支持工业信息系统和工业控制系统，应该有两种基本的电缆类型（COTS和工业EtherNet / IP电缆）。 只有符合本规范的电缆才有资格获得适当的性能检查标记。 两种电缆类型将具有不同的电气/机械和性能要求。

8-5.2.2.1 工业以太网/ IP电缆

工业以太网/ IP电缆应符合下表。

工业以太网/ IP电缆规格和要求		
规范	**类型**	
电动	**屏蔽**	**非屏蔽**
导线	2或4双+盾牌	2或4对
衰减	$\text{衰减}(f) \quad 1.967\sqrt{f} + 0.023f + \frac{0.050}{\sqrt{f}}$	$\text{衰减}(f) \quad 1.967\sqrt{f} + 0.023f + \frac{0.050}{\sqrt{f}}$
阻抗（装配）ASTM 4566	95 -110 Ω 1-4 Mhz 95 - 107 4 - 100 MHz	95 -110 Ω 1-4 Mhz 95 - 107 4 - 100 MHz
RL	1-10 MHz 20 + 6 Log_{10} (f) 10-20 MHz 26 20-100 MHz 26-5 * Log_{10} (f / 20)]	1-10 MHz 20 + 6 Log_{10} (f) 10-20 MHz 26 20-100 MHz 26-5 * Log_{10} (f / 20)]
下一个损失	NEXT (f) 64 - 15 * $\log_{10}$ (f) dB	NEXT (f) 64 - 15 * $\log_{10}$ (f) dB
屏蔽效能	TBD	N/A
Cupp	<= 150pf / 100米	<= 150pf / 100米
DCR	9.38 / 100米	9.38 / 100米
共模抑制	TBD	TBD
DCR不平衡	5%	5%

机械	**屏蔽**	**非屏蔽**
最小拉力	25磅	25磅
断裂强度	400 N最小	400 N最小
最小弯曲半径	1“在-20℃	1“在-20℃

尺寸的 （推荐用于RJ45兼容性）	**屏蔽**	**非屏蔽**
护套外径（双绞线护套）	0.250“最大	0.250“最大
绝缘导体	最大0.048“	最大0.048“

另外，电缆应该提供62.5MHz以上的衰减，如下段所述。 可以使用TIA / EIA 568A文件中描述的标准电缆衰减公式再现这个图形，通过将K因子代入0,0.3和0.1来重复。

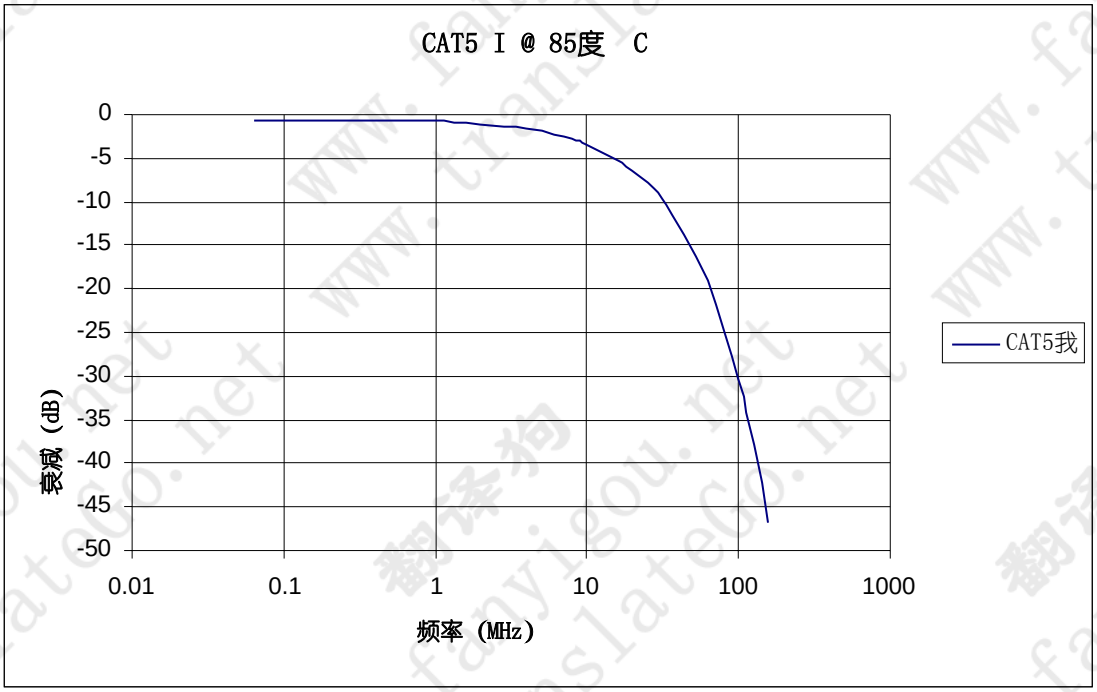
限制电缆带宽可以增加高噪声环境下的链路性能。 增加62.5 MHz以上的电缆损耗是限制噪声带宽的有效方法。 公式8-5.1列出了标准和工业加固电缆的公式和衰减因子。

公式8-5.1 UTP /屏蔽衰减

$$\mathrm{Atten}_{\mathrm{UTPCable}}(f) = -\frac{-\left(K_0\sqrt{f} + K_1 f + \frac{K_2}{\sqrt{f}}\right)}{100}$$

K_{0-2}=(1.967 0.023 0.050)　标准Cat 5E规格

K_{0-2}=(0　0.3 0.1)　　工业电缆



8-5.2.3 连接器

8-5.2.3.1 工业以太网/ IP连接器RJ 45变体

媒体的附件应通过两种工业级RJ-45连接器中的任何一种:

- 非密封工业RJ 45 EtherNet / IP连接器。 标准工业EtherNet / IP连接器应遵守第8-5.2.3.1.1节的规定
- 密封工业EtherNet / IP RJ 45连接器。 必须要求IP67密封的工业EtherNet / IP连接器符合第8-5.2.3.1.1节和第8-5.2.3.1.2节的规定

8-5.2.3.1.1 非密封工业RJ-45 EtherNet / IP连接器

标准工业硬化RJ-45连接器应符合以下规格:

工业以太网/ IP连接器规格和要求		
规范	**类型**	
电动	**RJ-45屏蔽**	**RJ-45**
导线	8 + 1盾牌	8
插入损失	ANSI/TIA/EIA-568-B.2 类别5E	ANSI/TIA/EIA-568-B.2 类别5E
RL	ANSI/TIA/EIA-568-B.2 类别5E	ANSI/TIA/EIA-568-B.2 类别5E
下一个损失	ANSI/TIA/EIA-568-B.2 类别5E	ANSI/TIA/EIA-568-B.2 类别5E
屏蔽效能	ANSI/TIA/EIA-568-B.2 类别5E	N/A
机械	**RJ-45屏蔽**	**RJ-45**
性别	插头和插座	插头和插座
交配规范	CEI IEC 60603-7	CEI IEC 60603-7
接触电镀	最小\50u英寸 黄金超过100u英寸分钟 镍或同等电镀系统	最小\50u英寸 黄金过来最小\100u英寸 镍或同等电镀系统
与LLCR联系一生	<20米	<20米
初始联系LLCR	<= 2.5 m	<= 2.5 m
联系生活	750插入和提取分钟。	750插入和提取分钟。

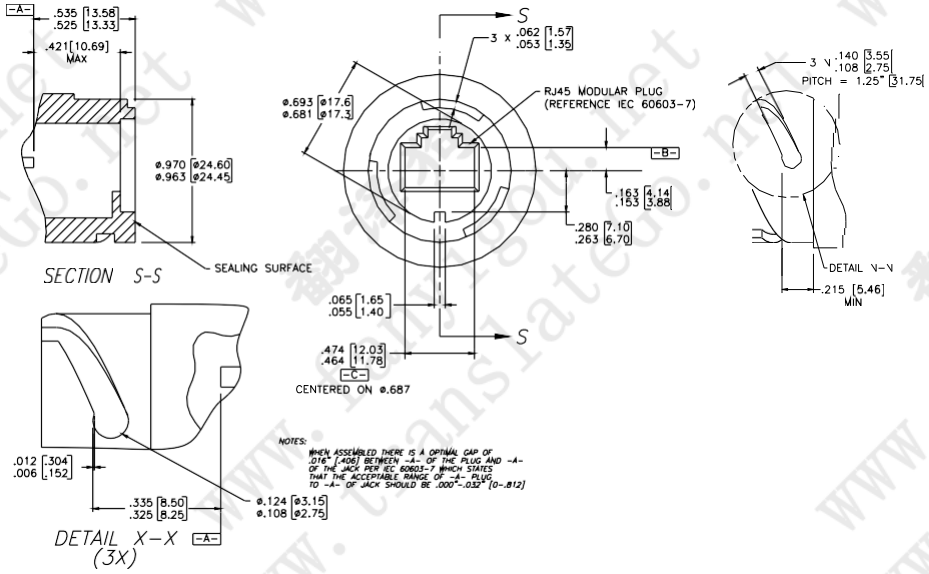
8-5.2.3.1.2 密封工业EtherNet / IP RJ-45连接器变种

密封接口应符合IEC 60529规定的最低IP67密封性能。

8-5.2.3.1.2.1 密封工业EtherNet / IP RJ 45插孔

Sealed RJ 45型号基于VG 95 234规范。 以下密封千斤顶图形充分确定了千斤顶以保持各个供应商之间的配合和密封的兼容性，这些供应商可以制造一个或两个零件 插座可以作为PCB安装，隔板和电缆端提供现场安装或制造组装。 插孔与标准的现成插头完全兼容。

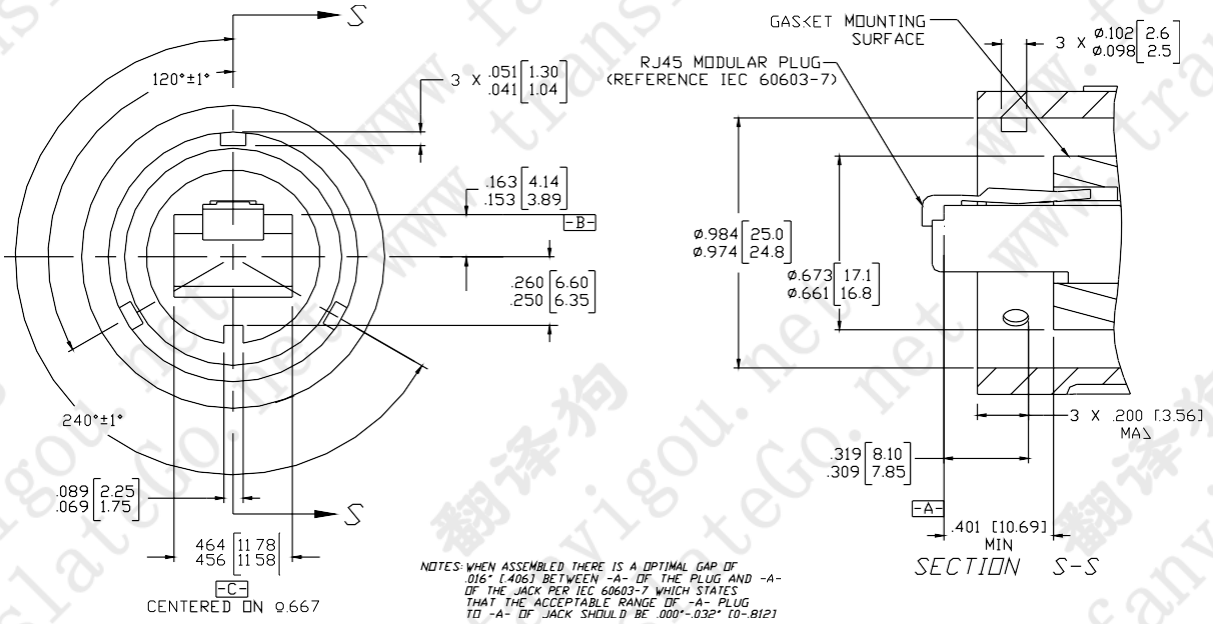
图8-5.1密封的插孔



8-5.2.3.1.2.1.1 密封工业EtherNet / IP RJ 45插头

Sealed RJ 45型号基于VG 95 234规范。 下面的密封插图充分地定义了插头以保持各个供应商之间的配合和密封的兼容性，这些供应商可以制造一个或两个部件。 插头可以作为现场安装或制造的电缆组件提供。 除了锁定机构之外，插头与标准的现成插座兼容。

图8-5.2 RJ-45密封插头



8-5.2.3.2 其他连接器

在考虑中

8-5.2.3.2.1 非密封的其他连接器

在考虑中

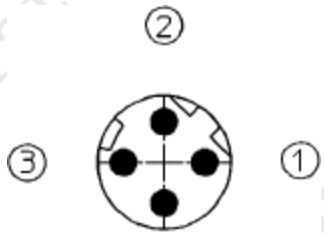
8-5.2.3.2.2 密封的其他连接器8-

5.2.3.2.2.1 M12-4“D型”

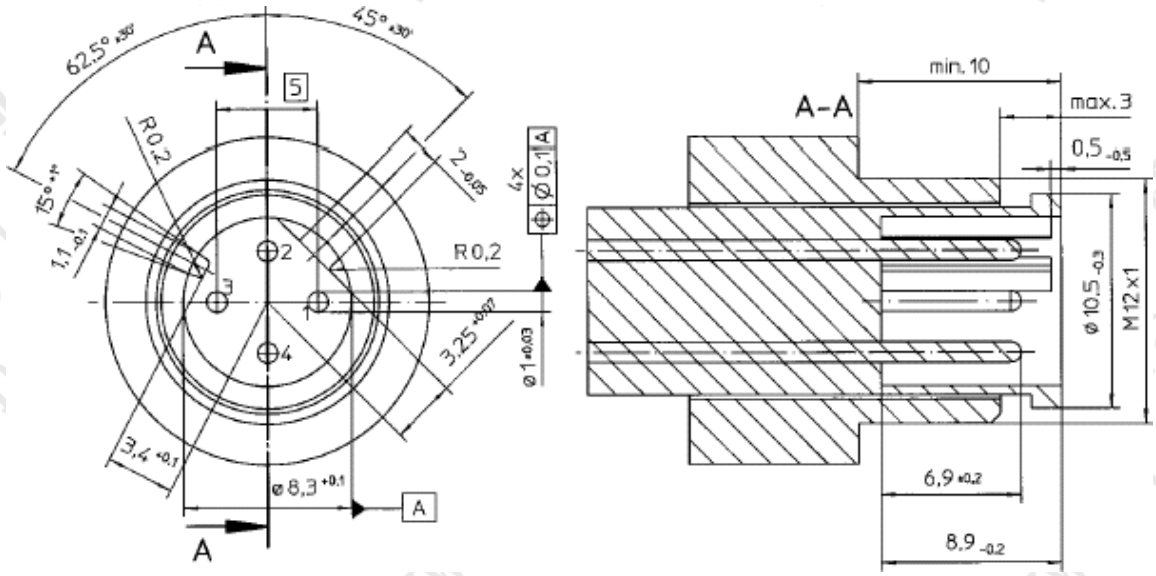
M12-4“D型”连接器是众所周知的，并在工业应用中被接受 – 20多年来，它一直是业界传感器连接的标准。 该连接器是一种替代的IP67以太网连接器，专为工业应用而设计，并被终端用户所接受。 连接器必须按照工业环境中的所有要求执行 – 机械和电气。 IEC 61076-2-101的4号“D型”修改1中也定义了连接器设计。

4针M12连接器仅适用于2对屏蔽或非屏蔽以太网电缆。

图8-5.3插头侧配合视图



销	名称	信号
1	传输数据+	TX+
3	传输数据 -	TX-
2	接收数据+	RX+
4	接收数据 -	RX-



8-5.2.4 工业以太网/ IP物理层媒体接口

连接到工业EtherNet / IP铜介质的设备应符合IEC 8802.3。

媒体接口的阻抗应符合ISO / IEC 8802.3 (ANSI / IEEE标准802.3) 和IEEE Std 802.3u-1995补充规定，但阻抗容差除外。 阻抗容差应限制在5%。 温度范围和振动应与目标环境保持一致。

8-5.2.4.1 拓扑约束

ANSI / TIA / EIA-568-B.1中定义的RJ-45系统的总信道长度为100米 (330英尺)，包括跳线。 通道和跳线设计和测试应符合ANSI / TIA / EIA-568-B.1和B.2 5E类的要求。

其他连接器系统的通道设计和测试正在考虑之中。

8-5.2.5 工业以太网/ IP组件

为了最大限度地提高噪声性能，为媒体和物理层选择的组件提供关键特性至关重要。 变压器应该（强烈推荐）在30MHz时提供至少59dB的共模抑制（CMR）。

包括以下参考框图以帮助产生统一的设计。

图8-5.4物理层框图

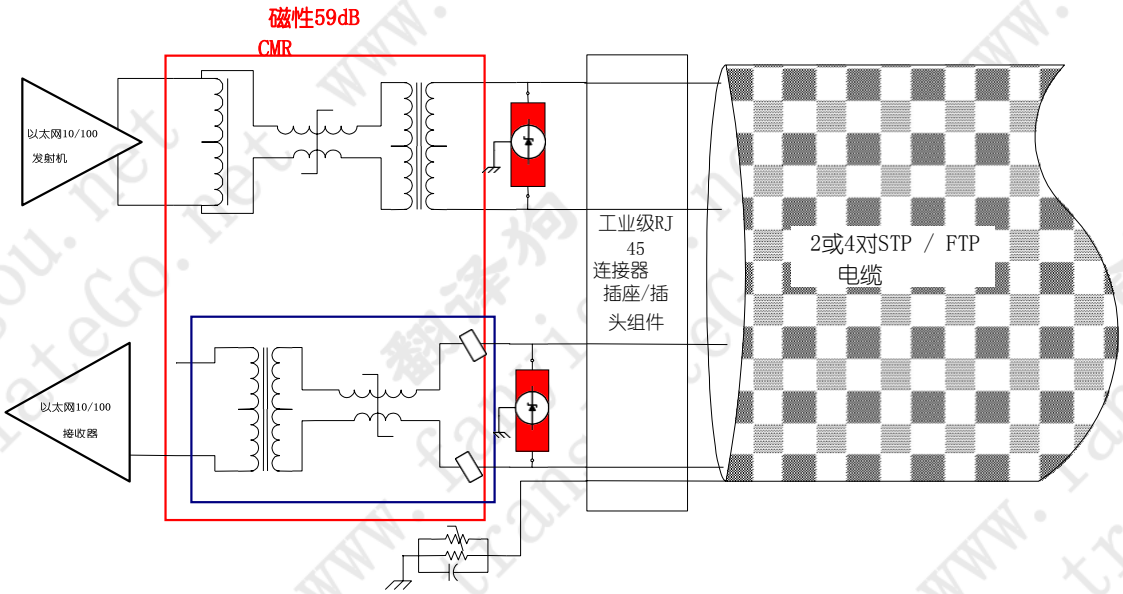
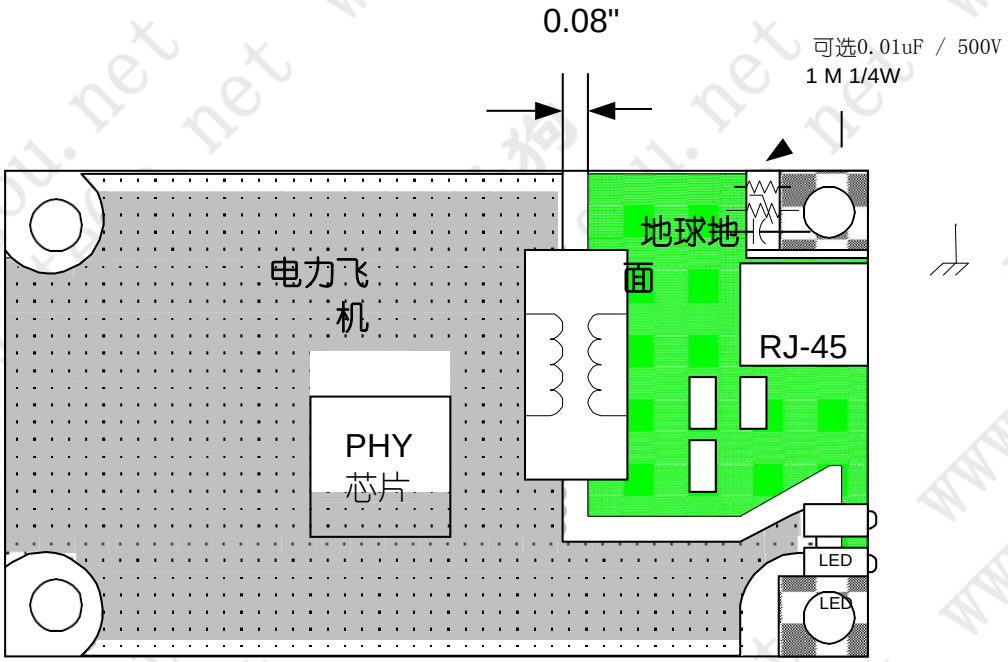


图8-5.5参考电路板布局



8-5.2.5.1 屏蔽接地

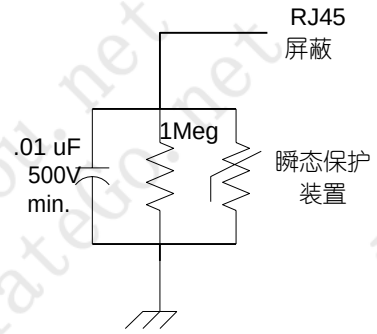
8-5.2.5.1.1 连接设备（交换机，集线器，桥接器，路由器）

所有电缆屏蔽应以两种方式中的任何一种终止：

1) 通信屏蔽应直接接地。

2) 通信屏蔽应通过并联电阻和电容组合端接到地。

图8-5.6连接设备中的屏蔽终端



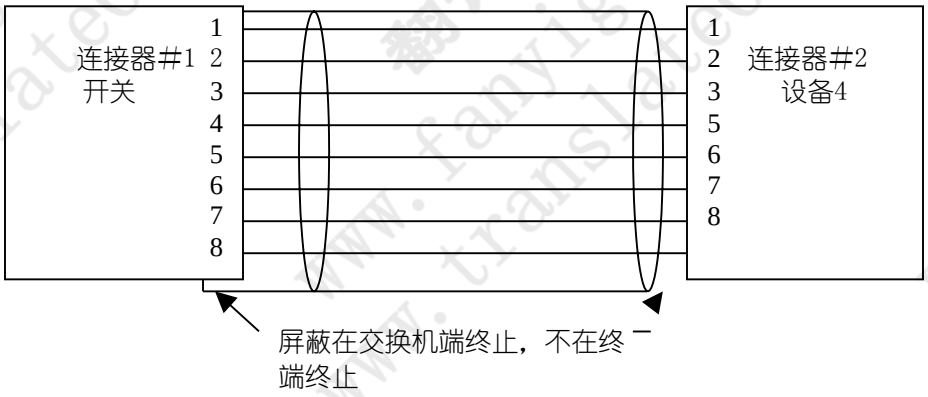
8-5.2.5.1.2 设备（传感器，PLC）

为防止屏蔽电缆引起接地回路，设备不得将屏蔽层直接接地。 所有的设备应该有以下两种方式之一的屏蔽端接：

1) 器件的屏蔽应通过并联电阻电容器组合端接。 （这与集线器/交换机的选项2相同。）

2) 如果设备通过RJ45连接器提供直接接地，则屏蔽层不应连接在RJ45插头上。

图8-5.7设备中的屏蔽终端



8-5.3 光纤媒体变种

注意：可以实施光纤物理层变体以允许在爆炸性环境中操作时符合以下要求。 可以在不牺牲距离或减少节点数量的情况下满足这些要求。

欧洲机电标准化委员会（CENELEC）欧洲共同体要求

连接到EtherNet / IP网络的光纤介质应限于SC，ST，MTRJ连接器类型。 这个变体的信令和耦合应符合IEEE 802.3u标准的规定，但要遵守本节（第8-5.3节）中列出的偏差。

8-5.3.1 连接器

光纤连接器设计应为MT-RJ，SC或ST型，并符合ANSI / TIA / EIA 568-B.3标题为“光纤布线元器件标准”的要求。

此外，连接器设计应符合相应的ANSI / TIA / EIA（光纤连接器相互适配性标准（FOCIS）文件的要求。

8-5.3.2 光纤电缆

单模和多模光缆应符合ANSI / EIA / TIA 568-B.3“光纤布线组件标准”的要求。

8-5.3.3 公开内部接口

IEEE 802.3u标准在物理层内定义了许多内部接口。 EtherNet / IP产品不需要直接实现这些接口中的每一个，而是应该表现为“好像”这些接口存在。 这些接口可以在节点内部，也可以在半导体器件内部。

8-5.3.4 拓扑约束

8-5.3.5 参考设计（资料性附录）

第2卷：CIP的EtherNet / IP适配

第9章：指标和中间层

内容

9-1 介绍

第9章规定了EtherNet / IP诊断LED的标准外观和行为。 本章还指定了EtherNet / IP设备的TCP / IP要求。

9-2 数据链路层

虽然这个规范被称为“EtherNet / IP”，但在技术上不需要以太网。 EtherNet / IP协议可用于支持Internet协议传输的任何介质。

注：例如，EtherNet / IP协议可用于FDDI，调制解调器线路（SLIP或PPP），ATM等。

使用任何特定介质时，应按照通用标准使用。 特别是使用以太网时，应按照IEEE 802.3规范的规定使用。

9-3 TCP / IP支持的要求

除了本规范中提出的各种要求之外，所有的EtherNet / IP主机都需要具有最低功能的TCP / IP协议组和传输机制。 EtherNet / IP主机的最低主机要求应符合RFC-1122，RFC-1123和RFC-1127及其后续文件的要求。 无论何时由EtherNet / IP主机实现功能或协议，该功能都应根据相应的RFC文档实施，而不管该功能或协议是否被本规范视为必需或可选。 互联网和RFC是动态的。 随着互联网和本规范的发展，将会有RFC和本节包含的要求发生变化，这些变化并不总是提供向后兼容性。

所有EtherNet / IP设备至少应支持:

- Internet协议 (IP版本4) (RFC 791)
- 用户数据报协议 (UDP) (RFC 768)
- 传输控制协议 (TCP) (RFC 793)
- 地址解析协议 (ARP) (RFC 826)
- Internet控制消息协议 (ICMP) (RFC 792)
- 互联网组管理协议 (IGMP) (RFC 1112&2236)
- IEEE 802.3 (以太网) 在RFC 894中定义

注意: 尽管封装协议适用于除了支持TCP / IP的以太网以外的其他网络，并且可以在其他网络上实现产品，但是EtherNet / IP产品的一致性测试仅限于以太网上的这些产品。 其他合适的网络包括:

- 点对点协议 (PPP) (RFC 1171)
- ARCNET (RFC 1201)
- FDDI (RFC 1103)

注: 鼓励使用EtherNet / IP设备，但不要求支持此处未指定的其他Internet协议和应用程序。 例如，可以支持HTTP，Telnet，FTP等。这个规范对这些协议和应用没有要求。

9-4 指标

9-4.1 必需的指标

产品不需要具有符合本规范的指标。 但是，为了符合第8章中描述的工业性能级别，产品应支持第9-4.2节，第9-4.3节和第9-4.4节定义的模块状态和网络状态指示器。

如果产品确实支持此处所述的任何指标，则必须遵守本节（第9-4节）中所述的规格。

可以提供两种状态指示器：

- 一个模块状态指示器；
- 一个网络状态指示器；

其他指标可能存在；但是其他指标不得使用标准指标的命名和符号约定。

注意：指示灯（通常作为LED实施）有助于维护人员快速识别故障设备或介质。 因此，红色指示灯用于指示故障状态。

注意：鼓励产品有一个指示符，用于显示链接状态（例如链接状态，tx / rx，碰撞等），遵循公认的行业惯例（如交换机等设备中使用的）。

9-4.2 共同指标要求

9-4.2.1 通用要求的适用性

通用指标要求只适用于本标准规定要求的指标。

9-4.2.2 指标的可见性

指示器应该可以看到，而不需要移除设备的盖子或部件。 指示灯在正常照明下应易于看到。 无论指示灯是否亮起，任何标签和图标均应可见。

9-4.2.3 指标闪光率

除非另有说明，否则所有指示灯的闪光速率大约为每秒1次闪光。 指示灯应亮约0.5秒，熄灭约0.5秒。 这个闪光速率规范仅适用于本章中指定的指标。

9-4.2.4 在加电指标

指示器测试在上电时执行。 为了进行目视检查，应执行以下步骤:

- 转第一个指示灯绿色，所有其他指示灯熄灭
- 将第一个指示器保持绿色约0.25秒
- 将第一个指示灯亮红色约0.25秒
- 打开绿色的第一个指标
- 将第二个指示器（如果有的话）以绿色旋转约0.25秒
- 将第二个指示器（如果存在）转换为红色大约0.25秒
- 打开第二个指示器（如果有）关闭

如果存在其他指标，则按照上述第二个指标的顺序依次测试每个指标。 如果存在模块状态指示器，则应该是序列中的第一个指示器，随后出现任何网络状态指示器。 通电测试完成后，指示灯应转为正常工作状态。

9-4.3 模块状态指示灯9-

4.3.1 描述

模块状态指示需要一个双色（红/绿）指示灯，代表整个产品的状态。

注：具有多个通信端口的产品只有一个模块状态指示灯，但多个网络状态指示灯（每个端口一个）。

9-4.3.2 标签

模块状态指示器应标有以下内容之一:

- “女士”;
- “国防部”;
- “Mod状态”;
- “模块状态”。

9-4.3.3 状态

模块状态指示灯应处于以下状态之一：

表9-4. 1模块状态指示灯

指标状态	概要	需求
稳定	没有力量	如果没有为设备供电，模块状态指示灯应该是稳定的。
绿色稳定	设备运行	如果设备运行正常，模块状态指示灯应该是绿色的。
闪烁的绿色	支持	如果设备未配置，则模块状态指示灯应呈绿色闪烁。
闪烁红色	轻微故障	如果设备检测到可恢复的轻微故障，则模块状态指示灯应呈红色闪烁。 注：不正确或不一致的配置将被视为轻微故障。
稳定的红色	重大故障	如果设备检测到不可恢复的重大故障，则模块状态指示灯应为红色。
闪烁的绿色/红色	自我测试	当设备正在进行加电测试时，模块状态指示灯应呈绿色/红色闪烁。

9-4.4 网络状态指示灯9-4. 4. 1

描述

网络状态指示需要一个双色（红色/绿色）指示灯，代表单个通信端口的状态。

注：具有多个通信端口的产品只有一个模块状态指示灯，但多个网络状态指示灯（每个端口一个）。

9-4.4.2 标签

网络状态指示器应标有以下内容之一：

- “NS”;
- “净”;
- “净状态”;
- “网络状态”。

9-4.4.3 状态

网络状态指示符的状态如下：

表9-4.2网络状态指示灯

指标状态	概要	需求
稳定	没有供电， 没有IP地址	如果设备没有IP地址（或断电），则网络状态指示灯将保持稳定。
闪烁的绿色	没有连接	如果设备没有建立连接，但已经获得IP地址，则网络状态指示灯应呈绿色闪烁。
绿色稳定	连接的	如果设备至少有一个已建立的连接（即使对于消息路由器），则网络状态指示灯应为绿色。
闪烁红色	连接超时	如果此设备为目标的一个或多个连接超时，则网络状态指示灯应呈红色闪烁。 只有在所有超时连接重新建立或设备重置的情况下，才能保留此状态。
稳定的红色	重复的IP	如果设备检测到其IP地址已被占用，则网络状态指示灯应为红色。
闪烁的绿色/红	自我测试	当设备正在进行加电测试时，网络状态指示灯应呈绿色/红色闪烁。

第2卷：CIP的EtherNet / IP适配

第10章：桥接和路由

内容

10-1 介绍

EtherNet / IP规范的这一章包含了对特定EtherNet / IP的CIP桥接和路由定义的补充。 目前还没有这样的增加。

此页有意留为空白

第2卷：CIP的EtherNet / IP适配

附录A：显式消息传递服务

内容

A-1 介绍

EtherNet / IP规范的这一章包含了对特定于EtherNet / IP的CIP显式消息服务定义的补充。 目前没有这样的补充。

此页有意留为空白

附录B：状态码

内容

B-1 介绍

EtherNet / IP规范的这一章包含了对特定于EtherNet / IP的CIP错误代码定义的补充。 目前没有这样的补充。

此页有意留为空白

第2卷：CIP的EtherNet / IP适配

附录C：数据管理

内容

C-1 介绍

EtherNet / IP规范的这一章包含了CIP数据管理规范的附加内容，这些规范是特定于EtherNet / IP的。 目前没有这样的补充。

此页有意留为空白

附录D：工程单位

内容

D-1 介绍

EtherNet / IP规范的这一章包含了EtherNet / IP特定的CIP工程单元列表。 目前还没有这样的补充。

此页有意留为空白