Ethernet/IP工业以太网
概述

阮于东

上海电器科学研究所（集团）有限公司

2008.8.15

工业网络的发展方向

- 更大的范围,单链路向多层局域网、广域网发展
- 多种物理介质
- 更丰富的信息
- 更快的速度,更精确的控制（准确的时间标记）
- 控制网络与信息管理网的统一，计划，财务，生产，维修信息的交互
- 高性能低成本－使用现成的技术

基于以太网的工业通信是当前的技术潮流

- Ethernet/IP
- Profinet
- MODBUS－RTPS
- FF HSC
- SERCOSⅢ
- EtherCAT
- IEC61850

通过IEC61784-2用于测量与控制的数字通信扩展IEC61158，已进入PAS文件的实时以太网如下：

- PAS 62030 Ed1　实时以太网MODBUS－RTPS
- PAS 62405 Ed1　实时以太网Vnet/IP
- PAS 62406 Ed1　实时以太网TCnet
- PAS 62407 Ed1　实时以太网 EtherCAT
- PAS 62408 Ed1　实时以太网 PowerLink
- PAS 62409 Ed1　实时以太网 EPA
- PAS 62410 Ed1　实时以太网 SERCOSⅢ
- PAS 62411 Ed1　实时以太网 PROFINET
- PAS 62412 Ed1　实时以太网 P－NET
- PAS 62413 Ed1　实时以太网 Ethernet/IP

现场总线标准

IEC61158:

Type1- FF H1

Type2- ControlNet EtherNet/IP

Type3- Profibus

Type4- P-net

Type5- FF HSE

Type6- SwiftNet

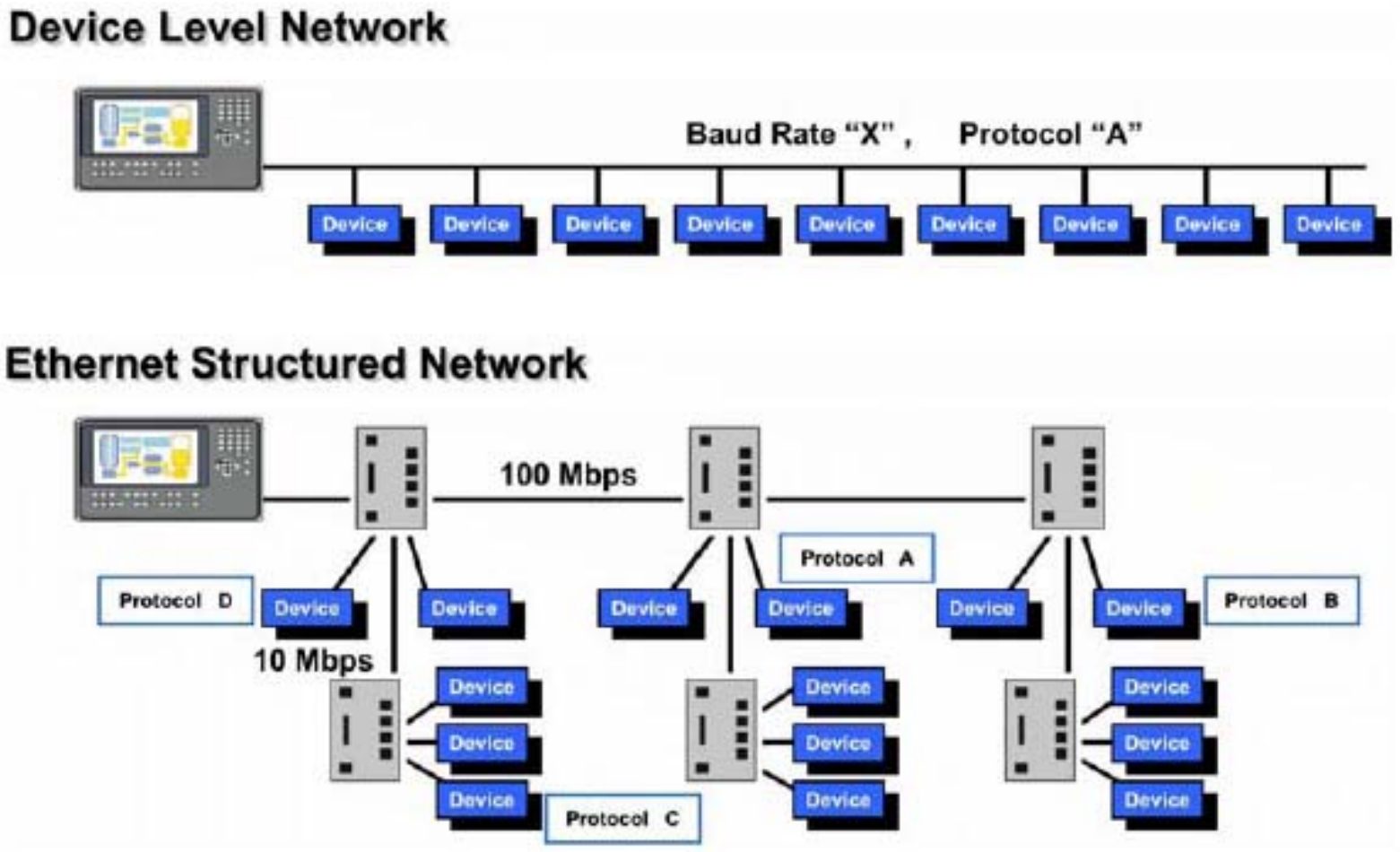
Type7- WordFIP

Type8- Interbus-S

Type10- ProfiNet

IEC62026：DeviceNet， ASI

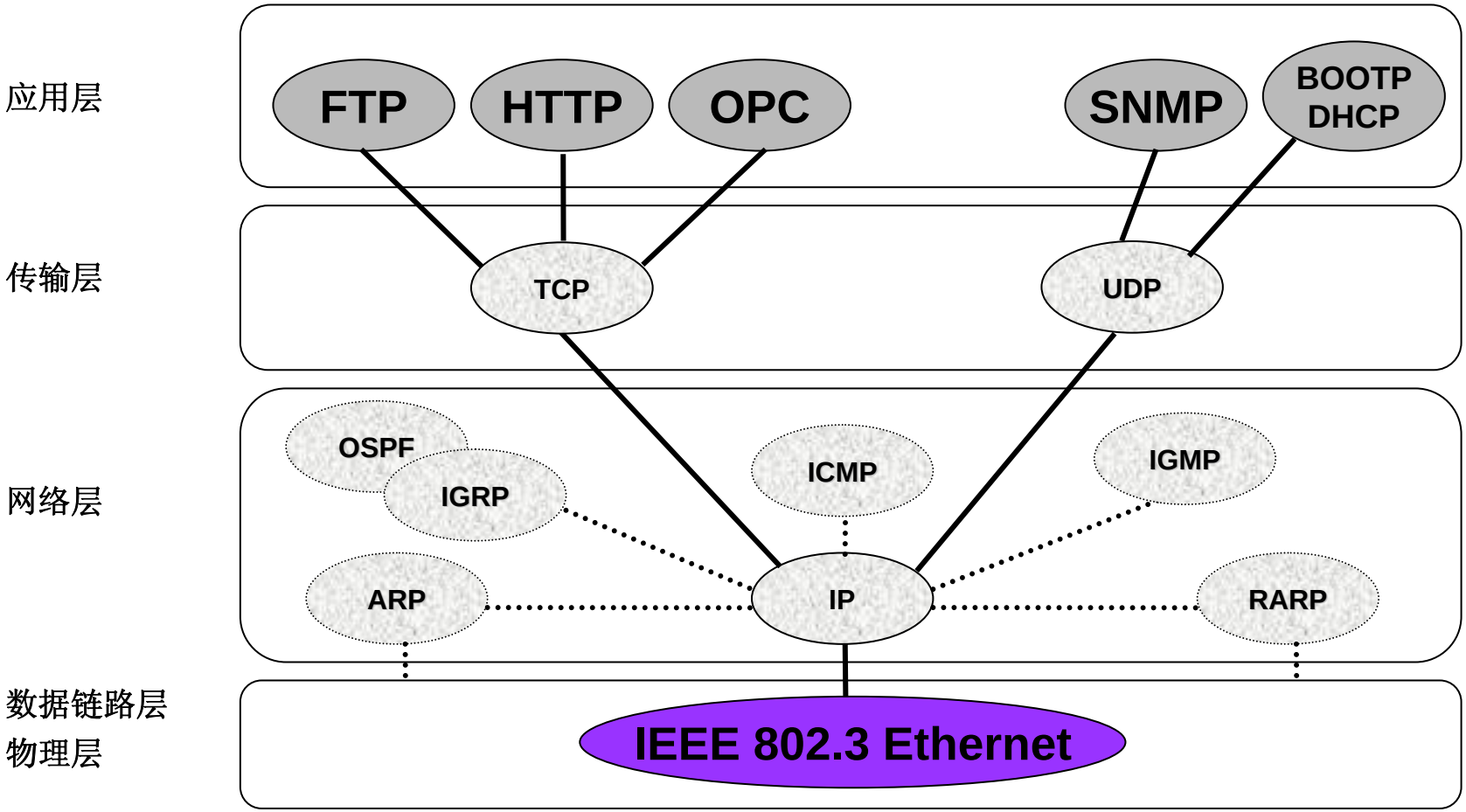
设备层总线网和结构化的Ethernet 网络



Ethernet

- 数据传输速度
  - 10Mbps、100Mbps、1Gbps.....
- 拓扑结构和介质
  - 更灵活的拓扑结构和介质选择，各网段可使用不同介质
  - 全双向交换机网络，自动选择报文路径
  - 增加可用带宽和性能
  - 更好的网络分段、诊断安全等
  - 可实现多连接的通信
- 持续的技术改进
- 广泛应用的硬件（每年产量2亿8千万节点） – 低成本
- 国际标准
- 现成的技术

以太网协议族的支持


应用层
FTP
HTTP
OPC
SNMP
BOOTP
DHCP
传输层
TCP
UDP
网络层
OSPF
IGRP
ICMP
IGMP
ARP
IP
RARP
数据链路层
物理层
IEEE 802.3 Ethernet

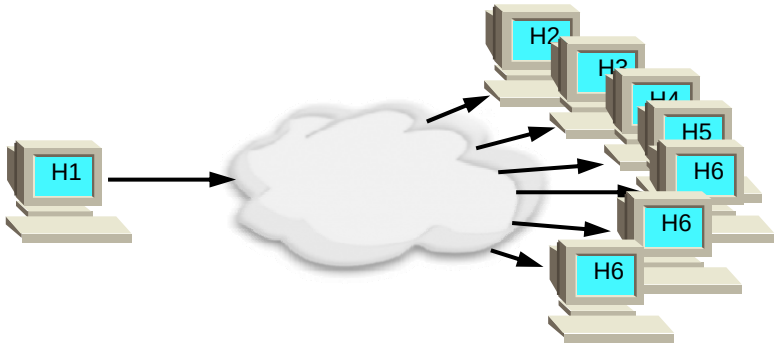
IP功能

- 提供跨链路寻址和数据交换的机制
- 通过ARP，RARP，ICMP，IGMP的支持实现网际互连
- 通过无连接的包传输尽力送达
  - 数据包可能丢失、不按正常顺序到达、重复的分段；些问题由更高级别的协议处理
- 提供IP路由，这是不同物理网络互连时实现路由的基本机制
- 分段和重新组装数据包

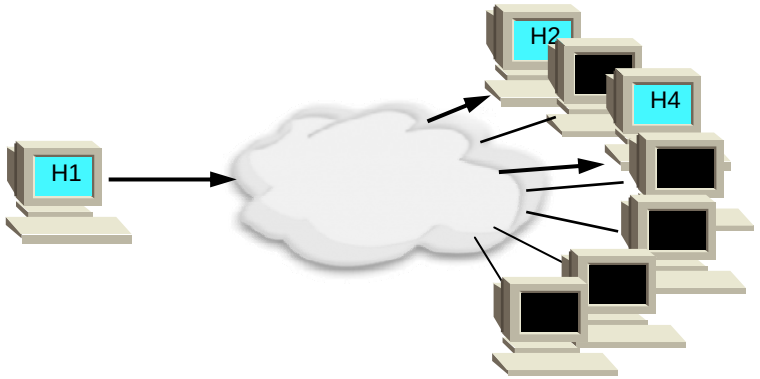
IP 地址类型

单点发送－报文到达单一目的地

广播发送－到达子网的所有节点



多点发送－到达一组节点



TCP 作用

- 传输控制协议 (TCP)
  - 为IP层提供基于连接的应用程序接口
  - 在传送数据包之前，先要建立连接
  - 所有的数据包都需要确认
  - 提供可靠的送达机制包括错误恢复和流量控制

UDP 作用

- 用户数据报协议 (UDP)
  - 为IP层提供无连接的应用程序接口
  - 不能保证可靠送达，无流量控制或者错误恢复,需要应用程序承担这一个责任
  - UDP 的低开销因此非常快速
  - 用于实现多播通信

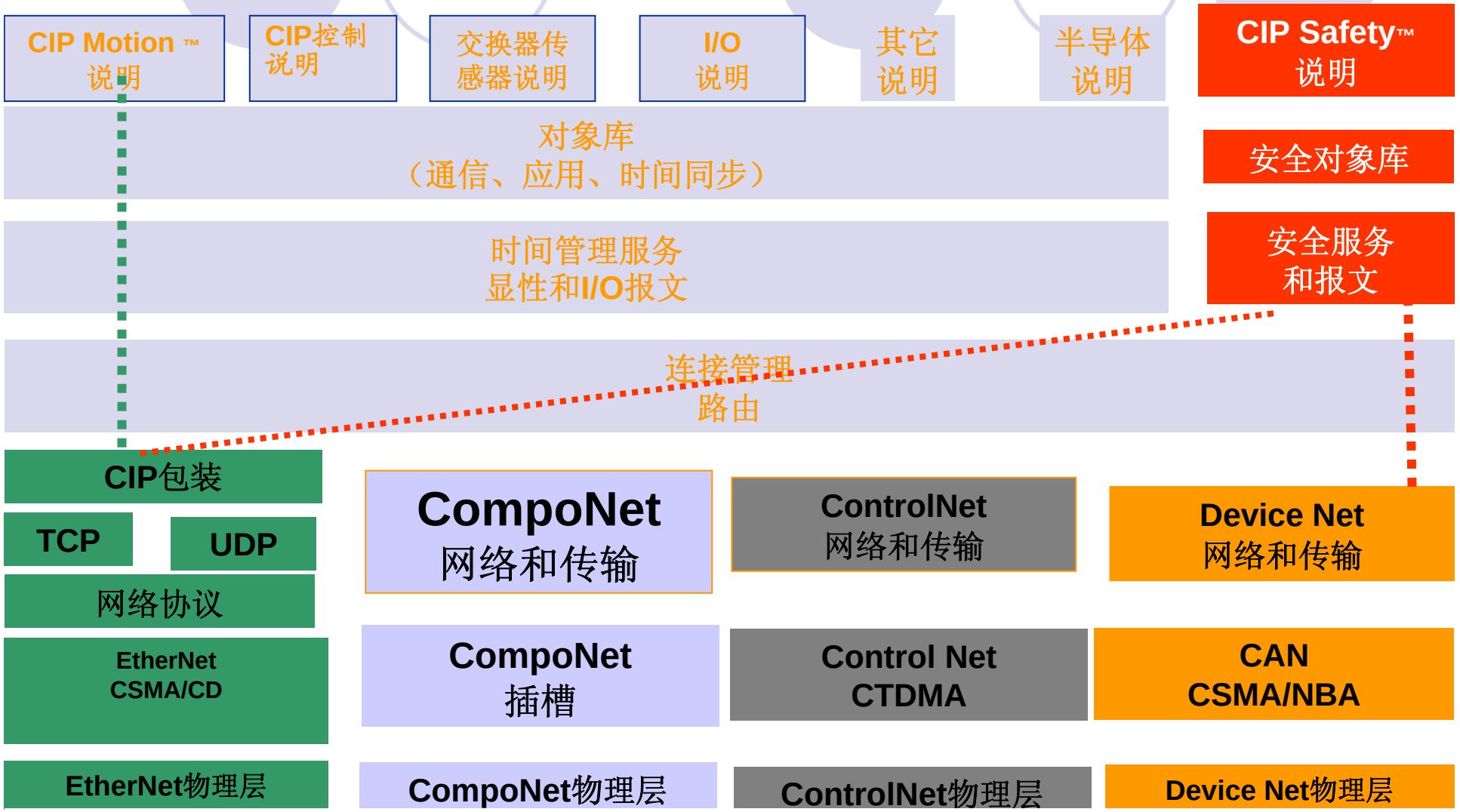
IGMP、ARP、OSPF、HTTP等协议支持

- IGMP网络组管理协议，被用在一个网络上的特定多播组中,创立主机隶属关系
- ARP地址解析协议被用来映射 IP地址 与物理的网络地址(Ethernet MAC地址)
- 最短路径优先协议（Open Shortest Path First）
- 用于网页浏览的超文本传送协议HTTP
- 简单网络管理协议SNMP
- 时间同步协议NTP，SNTP，IEEE1588

工业以太网具有性能优势

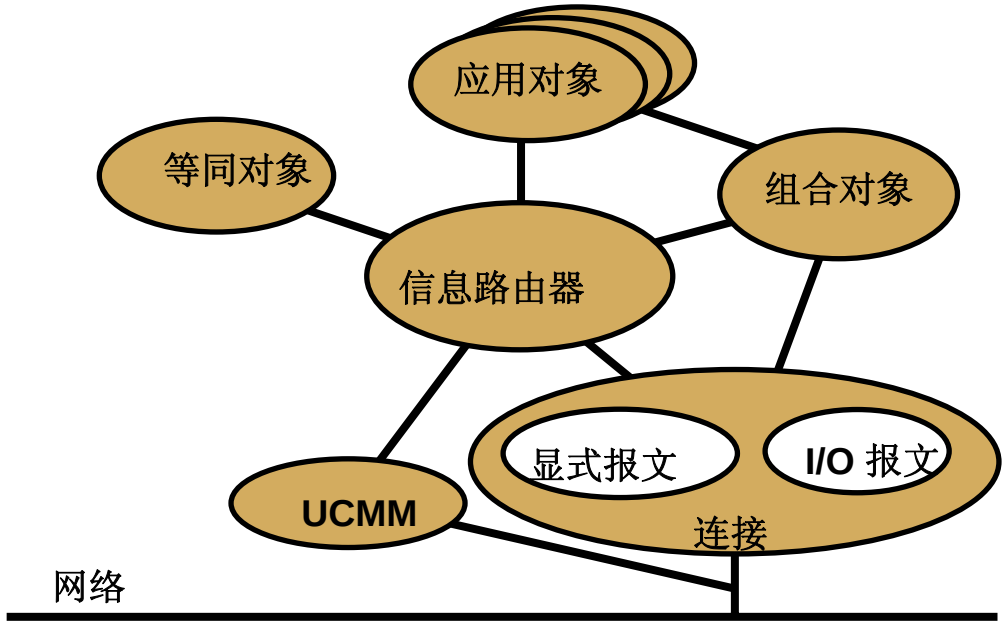
	Ethernet/IP	Devicenet	Profibus-DP
波特率	10M/100Mbps	500Kbps	12Mbps
网络范围	多层网络	单网段	单网段
最大数据包	1500字节	8字节	256字节
报文优先级	802.1Q	有	无
周期报文	UDP/IP	隐式报文	有
非周期报文	TCP/IP	显式报文	DPV1以上有
网络供电	有	有	无
时间同步	SNTP，1588	无	无
运动控制	CIP Motion	无	无

CIP的支持的技术


CIP Motion ™ 说明
CIP控制 说明
交换器传 感器说明
I/O 说明
其它 说明
半导体 说明
CIP Safety™ 说明
对象库 （通信、应用、时间同步）
安全对象库
时间管理服务 显性和I/O报文
安全服务 和报文
连接管理 路由
CIP包装
TCP
UDP
网络协议
EtherNet CSMA/CD
EtherNet物理层
CompoNet 网络和传输
CompoNet 插槽
CompoNet物理层
ControlNet 网络和传输
Control Net CTDMA
ControlNet物理层
Device Net 网络和传输
CAN CSMA/NBA
Device Net物理层
EtherNet/IP™
CompoNet™
ControlNet™
DeviceNet™

CIP对象模型

- CIP应用对象模式描述设备
  - 用一个对象的集合描述设备的行为
  - 用对象将设备的功能分成逻辑相关的子集，每个都有确切定义的行为



服务

- 定义一组公共服务，用于访问数据和控制设备操作

Get_Attributes_All
Set_Attributes_All
Request
Get_Attribute_List
Set_Attribute_List
Reset
Start

Get_Attribute_Single
Set_Attribute_Single
Find_Next_Object_Instance
Restore
Save
No Operation

设备描述

设备描述通过以下方面说明设备特性：

- 必需和可选对象的特定组合，以及它们如何相互作用
- 决定可以访问那些对象服务和属性
- 设备交换的输入/输出数据的结构
- 设备的配置数据

电子数据文件（EDS）

- 供货商提供的文档，以便了解设备：
  - 结构和I/O数据含义
  - 有哪些I/O数据传输类型
  - 可访问网络应用配置参数
  - 支持复杂设备的组件化产品
    - 说明框架系统的结构和模块：机架、模块和通信适配器

生产者/消费者通信与源/目的通信

- 源/目的（点对点）
- 因数据到达各节点时间不一，难以实现不同节点的同步反应
  - 对不同目的地需要多次传送相同数据导致带宽浪费
  - 需要多个网络

- 生产者/消费者（数据的标识）
  - 多节点能够同时从单一生产者消费相同数据以确保各节点同步
  - 带宽使用更有效率
  - 更高的确定性和可重复性

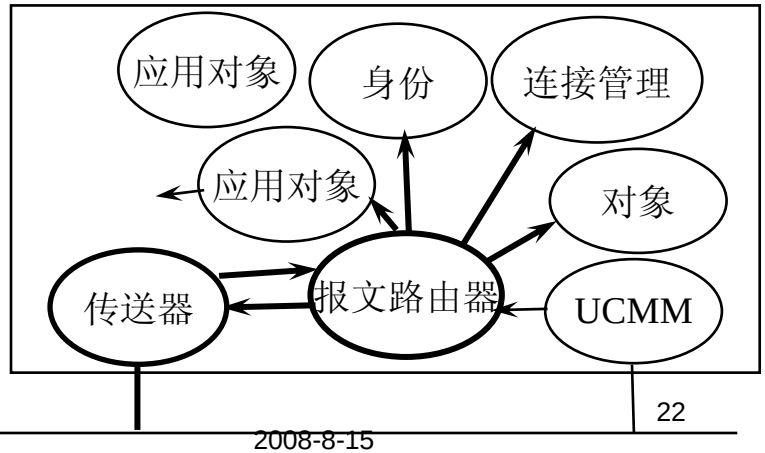
Ethernet/IP 通信模型

Ethernet/IP使用一种非常高效灵活的数据交换模式，称为生产者/消费者模式。

- 生产者是数据的发送者
  - 生产者在网络上传送数据包，数据包带有能指示包裹内容的唯一的识别符
- 消费者是数据的接收者
  - 任何感兴趣的消费者通过对信息包标识符的过滤从网络上接受数据
  - 可以由多个消费者接收和利用这些数据
- Ethernet/IP的I/O报文使用UDP/IP，UDP多播是发送到IP多播组地址，参加这个多播组的成员度可接收这个报文

报文类型－显式报文

- 显式报文应用于点对点、客户－服务器类传送
  - 用于命令执行指定的服务和报告执行的结果
    - 可访问所有内部资源
  - 基于请求－响应方式
    - 需要时向服务器发出请求
  - 可使用有连接或非连接通信



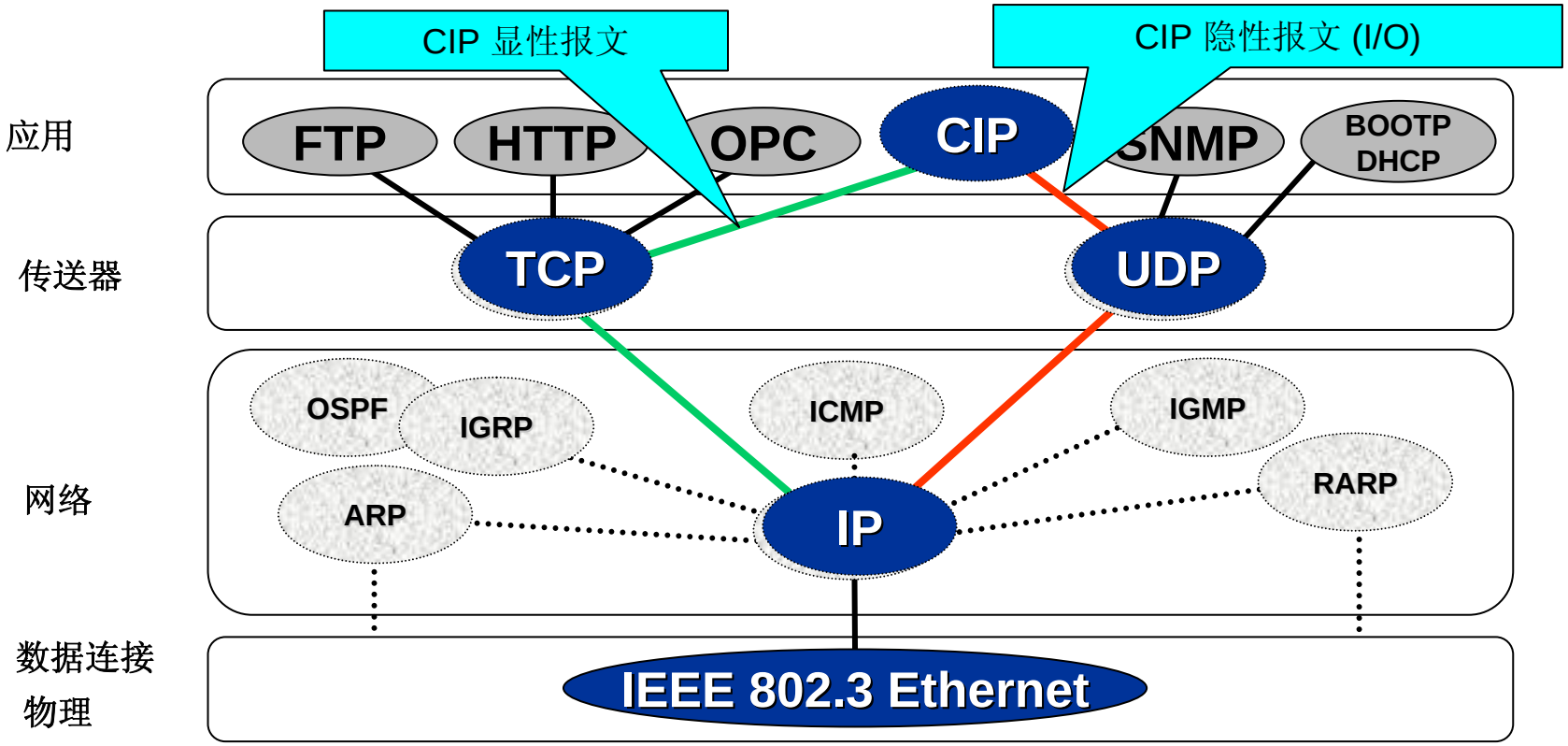
报文类型－隐式报文

隐式报文传递应用特定的 I/O 数据

- 源－目的数据是应用对象（例：组合对象）
- 在报文的数据部分没有协议数据－全部是I/O数据
  - 在设备描述中说明数据格式，在电子数据文件(EDS)也有说明
- 预知数据含义所以数据传输更有效率
- 基于时间(循环) 或数值变化（状态变化）的传输
- 连接定时机制提醒对方中止通讯
- 只在连接状态下－没有非连接隐性报文

EtherNet/IP是CIP在TCP/UDP/IP上的应用

CIP显性报文（配置、收集、诊断）利用流量控制和TCP的点对点特性

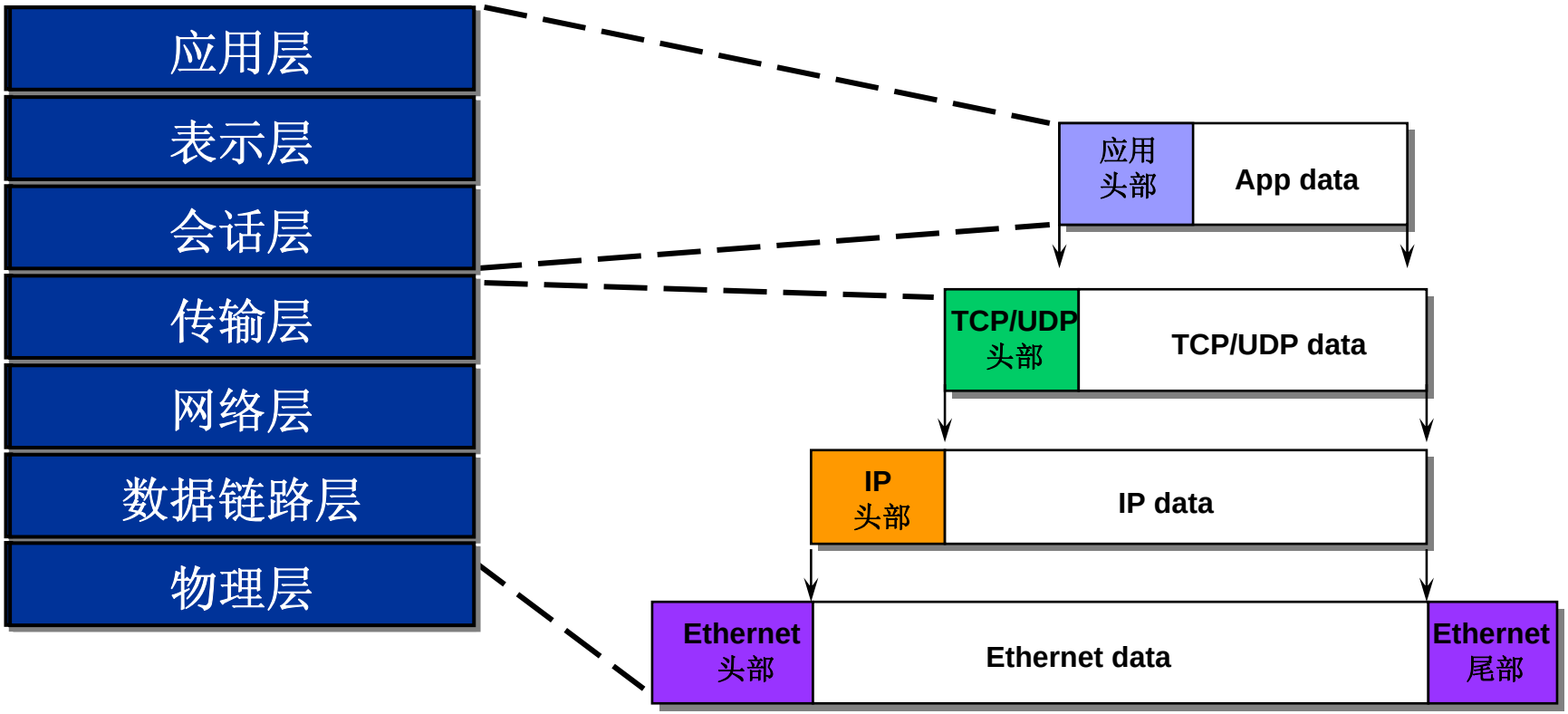


- I/O控制使用UDP支持了CIP生产者－消费者模式，通过绘制IP多点传送以达到I/O高效交换

协议封装

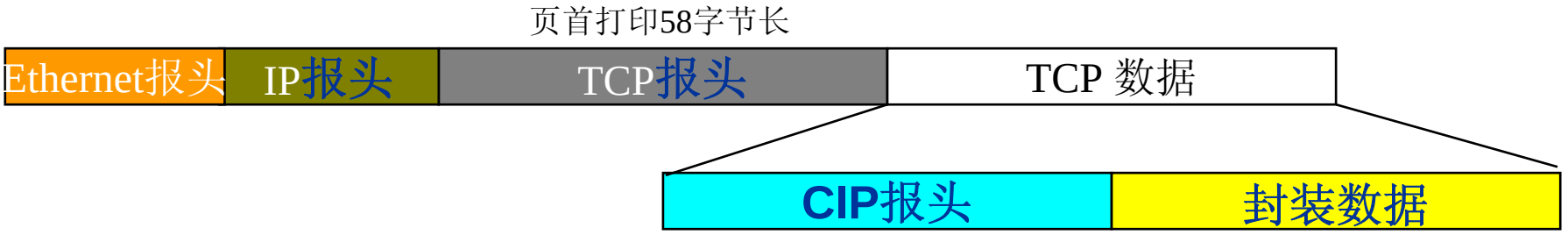
OSI 模式

TCP/IP包结构



在TCP/IP内封装CIP

- Ethernet报文是多协议串联结构
  - Ethernet、IP、TCP（UDP）等
  - EtherNet/IP定义了适合于TCP数据的包装协议，通过端口号表示这是Ethernet/IP报文
  - TCP（UDP）数据由两部分组成:
    - 报头，封装数据



在TCP 协议打包CIP数据

Two back-to-back encapsulated messages could be sent in many different ways by the TCP/IP stack. Two examples are given here:

Ethernet header (14 bytes)	IP header (20 bytes)	TCP header (20 bytes)	Encapsulation message #1	Encapsulation message #2	CRC

or

Ethernet header (14 bytes)	IP header (20 bytes)	TCP header (20 bytes)	Start of encapsulation message #1	CRC

Ethernet header (14 bytes)	IP header (20 bytes)	TCP header (20 bytes)	Rest of encapsulation message #1	Encapsulation message #2	CRC

常用的封装命令

代码	名称	说明
0x0000	NOP	（只能使用 TCP 发送）
0x0004	ListService 列举支持的封装服务	（可使用 TCP 或 UDP 发送）
0x0063	ListIdentity 查询潜在的目标	（可使用 TCP 或 UDP 发送）
0x0065	RegisterSession 登录会话	（可使用 TCP 或 UDP 发送）
0x0066	UnRegisterSession 取消会话	（可使用 TCP 或 UDP 发送）
0x006F	SendRRData 传送 UCMM 数据包	（可使用 TCP 或 UDP 发送）
0x0070	SendUnitData 传送有连接的数据包	（可使用 TCP 或 UDP 发送）

CIP封装包的结构

Structure	Field Name	Data Type	Field Value
Encapsulation header	Command	UINT	Encapsulation command
	Length	UINT	Length, in bytes, of the data portion of the message, i.e., the number of bytes following the header
	Session handle	UDINT	Session identification (application dependent)
	Status	UDINT	Status code
	Sender Context	ARRAY of octet	Information pertinent only to the sender of an encapsulation command. Length of 8.
	Options	UDINT	Options flags
Command specific data	Encapsulated data	ARRAY of 0 to 65511 octet	The encapsulation data portion of the message is required only for certain commands

SendRRData发送Forword Open请求

1，SendRRData 发送 Forword Open 请求

结构	字段名		数据类型	字段值
封装头部	命令		UINT	SendRRData (0x6F)
	长度		UINT	数据部分长度
	会话句柄		UDINT	保持由RegisterSession处理返回的值
	状态		UDINT	0
	发送者上下关系		ARRAY of USHORT	（无关）
	选项		UDINT	0
命令特定数据	接口句柄		UDINT	0（表示是CIP包）
	Timeout		UINT	超时值
	封装包（命令包格式）	Item Count	UINT	2
		地址类ID	UINT	0（指示这是UCMM报文）
		地址长度	UINT	0
		数据类ID	UINT	0x00B2（无连接传送包）
		数据长度	UINT	6+xxxx
		请求包路由	ARRAY of USHORT	请求包路由格式如下表

Forword Open命令

参数名称	数据类型	说明
请求/响应	BYTE	0（Bit7=0 表示请求，1 表示应答）
服务代码		54（Forword Open 请求）（Bit6~0 表示服务代码）
请求路径尺寸 请求路径 请求数据	USINT EPATH Aray of octer	4 20 06 24 01（ClassID=6 连接管理器对象，Instance ID=1） Forword Open Request（格式如下）

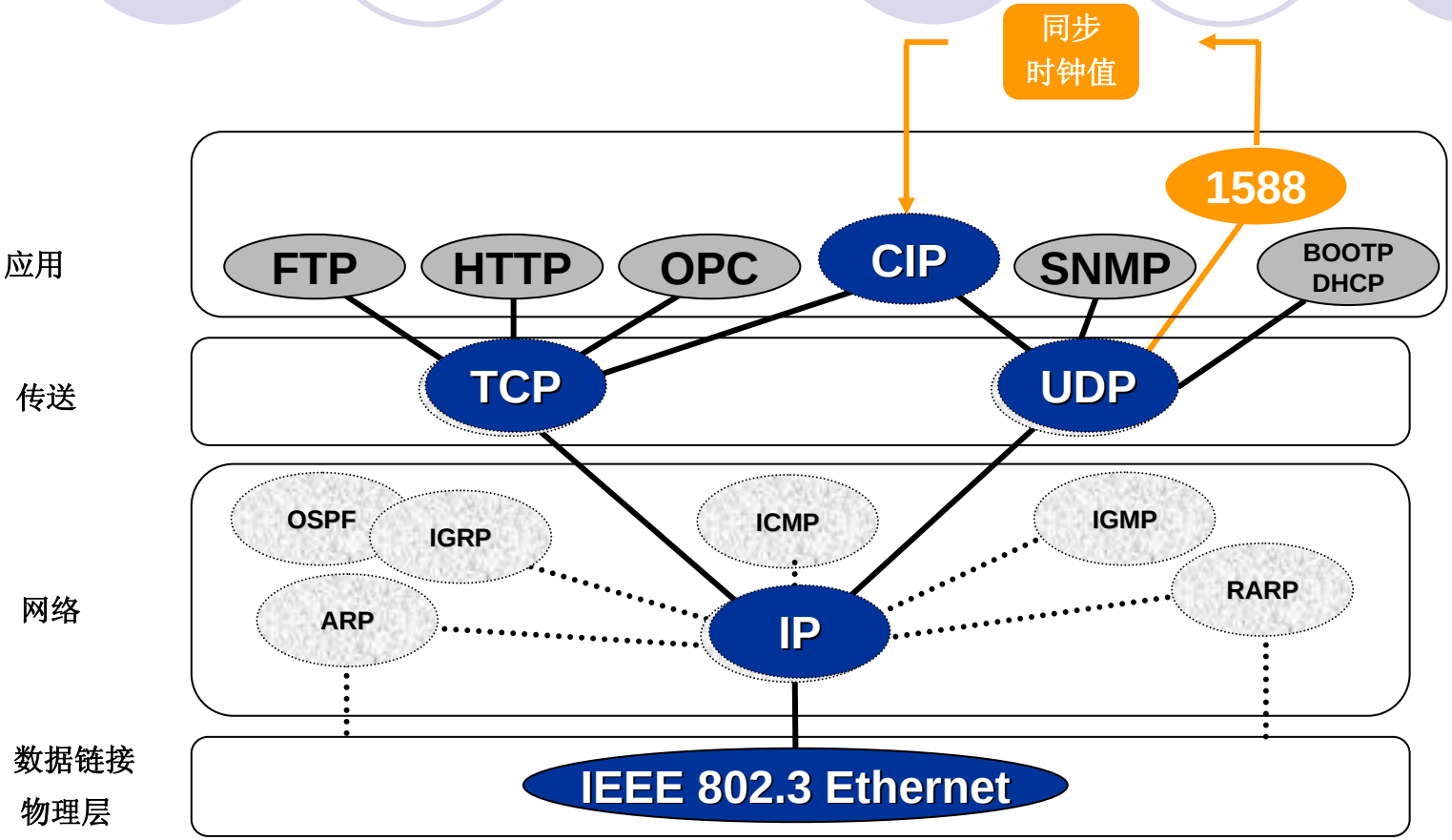
时间 同步

- 分散的智能节点的控制，测量或对事件的描述可能与其它节点的行为相关，它们需要相同的时间基准。
- 通过网络传递时间信息并非难事，但要求毫秒级的时间同步就相当不同容易，微秒级的同步精度需要专门研究，是近年实现的技术。
- NTP，SNTP协议可以实现几十毫秒的同步进度
- IEEE1588是“用于网络测量和控制系统的精确时钟同步协议”--IEC61588，可以实现微秒级的精度，通常是在以太网上实现的。

时间同步

- 使用64位二进制数表示时间，前32位是秒计数可表示136年的年、月、日、分、秒，后32位是秒的分数，可表示到纳秒（10^{-9}秒）
- 基于软件的协议，使用Sync，Follow_up,Delay_Req,Delay_Resp四种报文实现同步
- 通过硬件辅助提高同步精度

CIP 同步: CIP + IEEE 1588



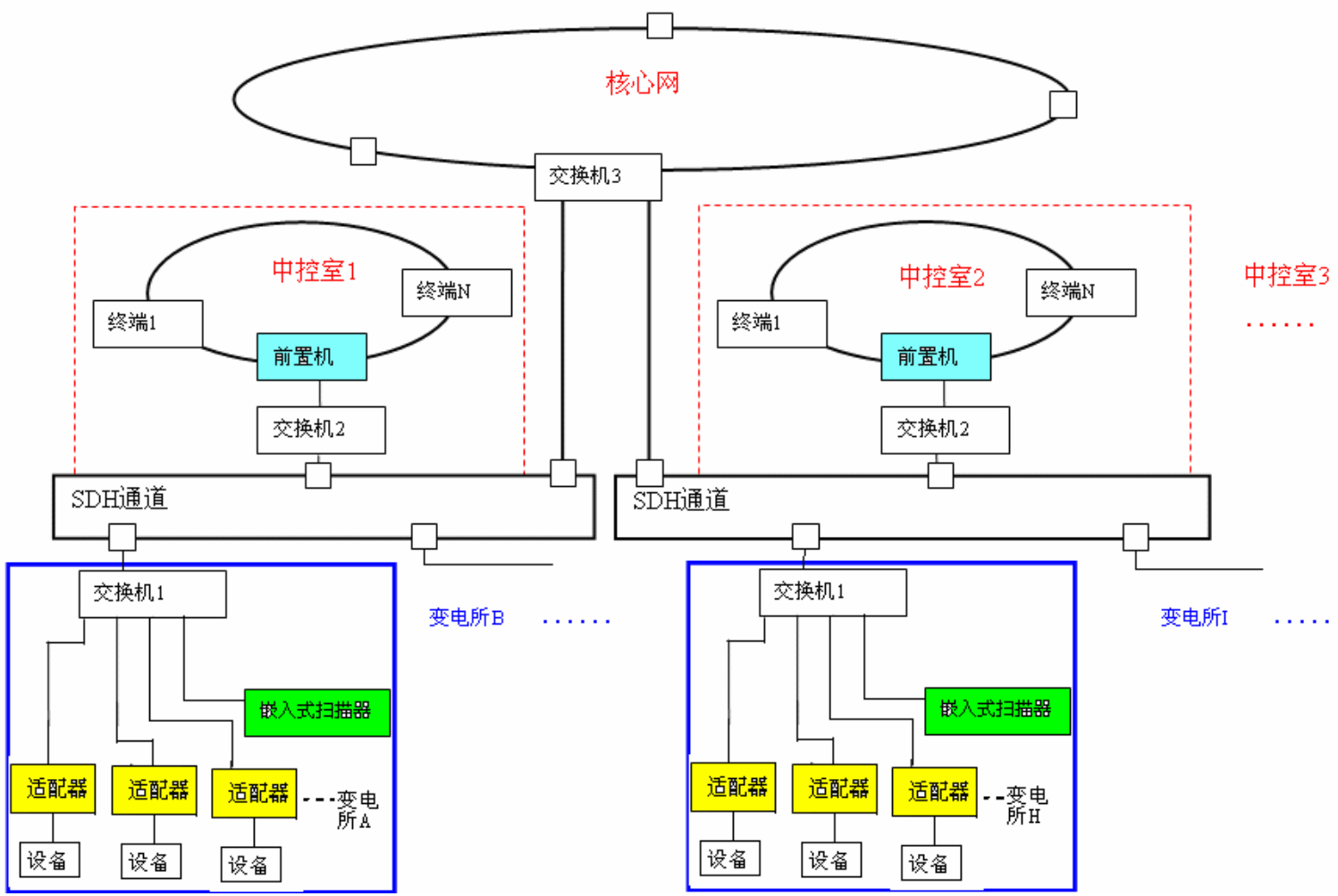
Ethernet/IP设备的开发

- Ethernet/IP是基于标准以太网，可使用带有以太网接口的芯片，如ARM或类似芯片
- 操作系统提供以太网驱动程序和接口
- 开发Ethernet/IP应用层
- 使用标准的网络部件

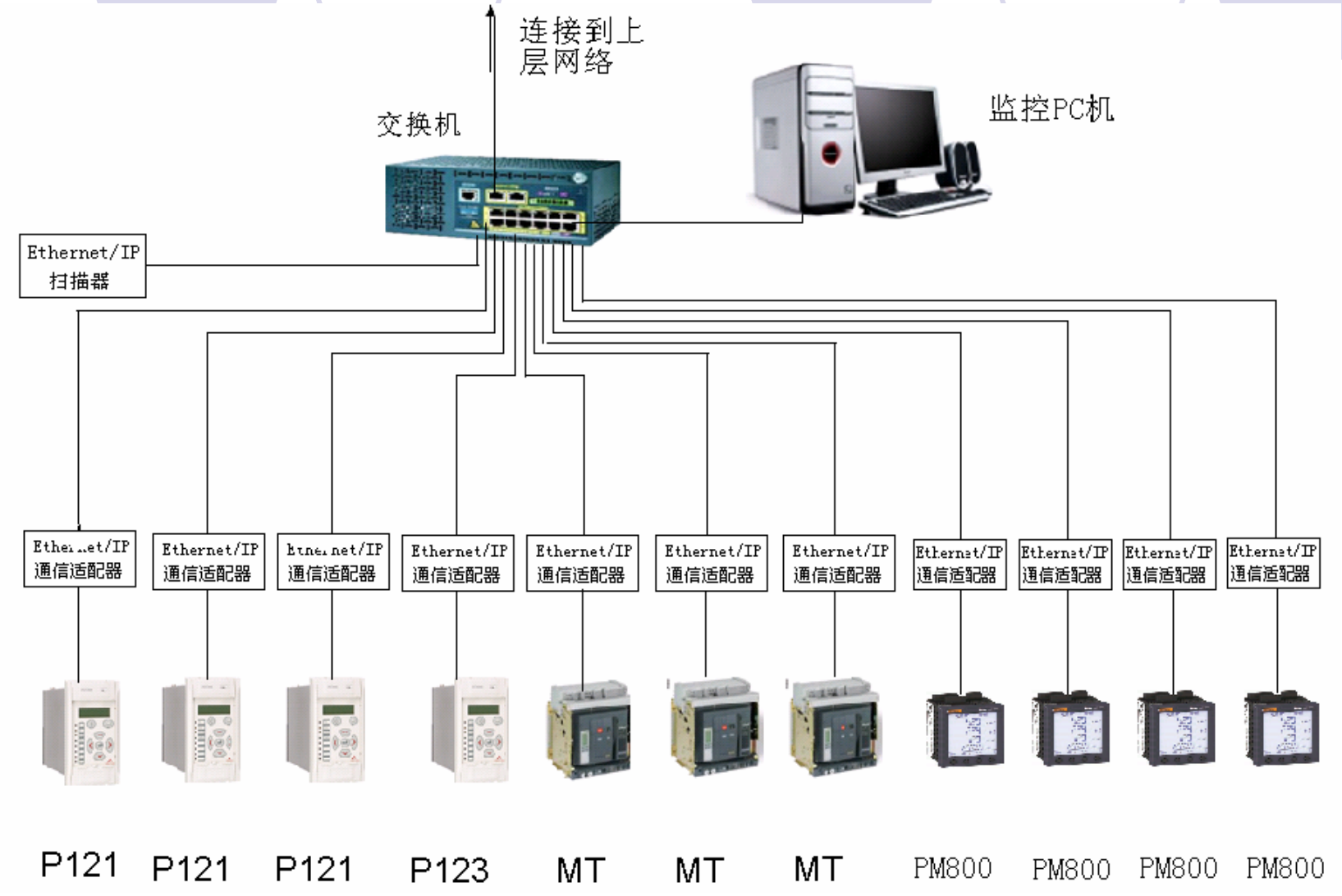
使用Ethernet/IP通信的例子

- 所有设备通过Ethernet/IP通信适配器接入，每个设备都是标准的Ethernet/IP节点，可以独立于网络上的设备交换信息。
- 使用通用的以太网交换机和网络设备，电缆或光缆10M/100M/1G
- Ethernet/IP报文可在通常的以太网上传输，网络距离也不是问题
- 使用Ethernet/IP扫描器集中周期数据，提高通信效率。

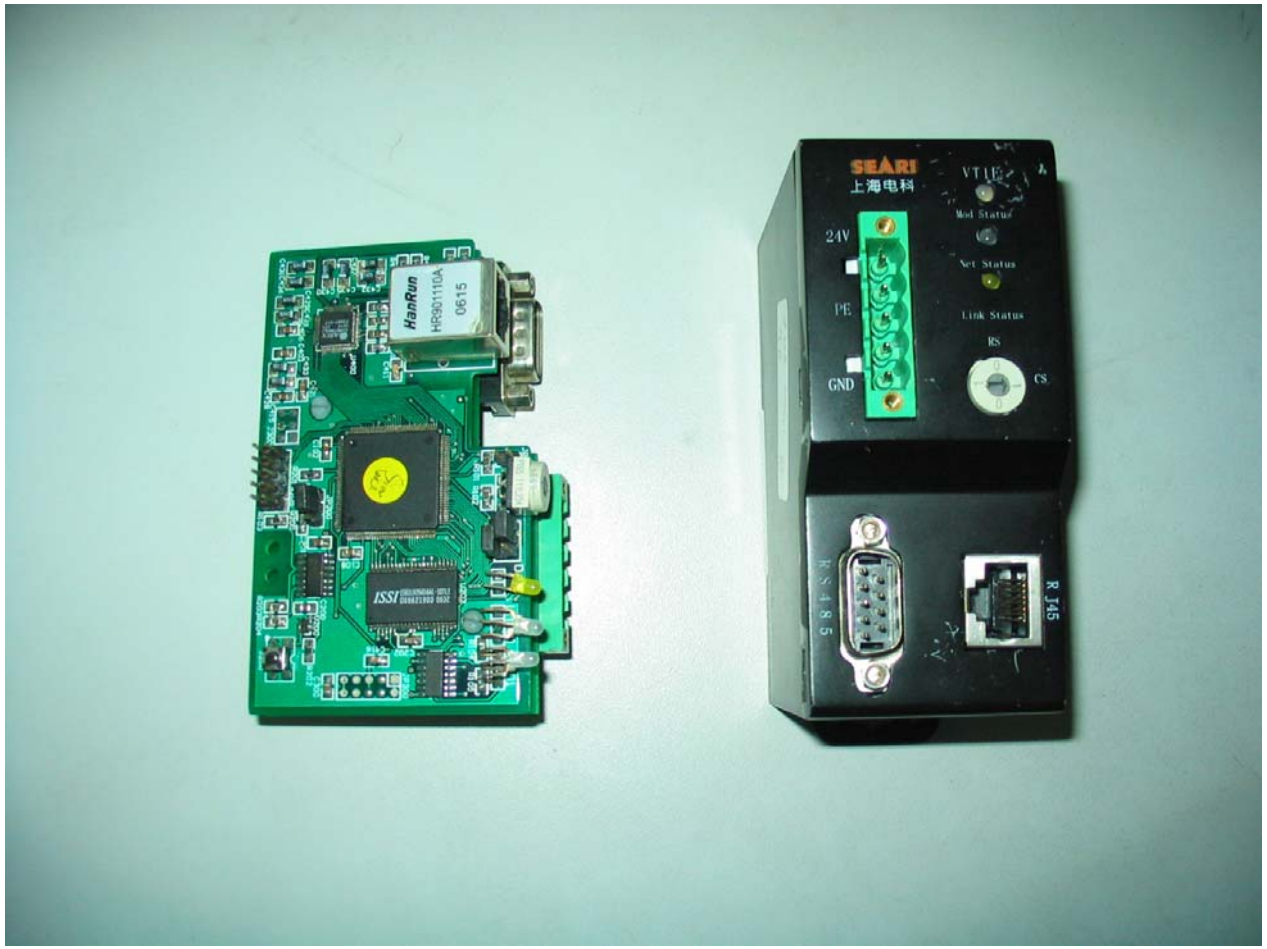
电力监控系统示意图


核心网
交换机3
中控室1
终端N
终端1
前置机
交换机2
中控室2
终端N
终端1
前置机
交换机2
中控室3
.....
SDH通道
SDH通道
交换机1
变电所B .....
嵌入式扫描器
适配器
适配器
适配器
变电所A
设备
设备
设备
交换机1
变电所I .....
嵌入式扫描器
适配器
适配器
适配器
变电所H
设备
设备
设备

使用Ethernet/IP通信的变电站配置

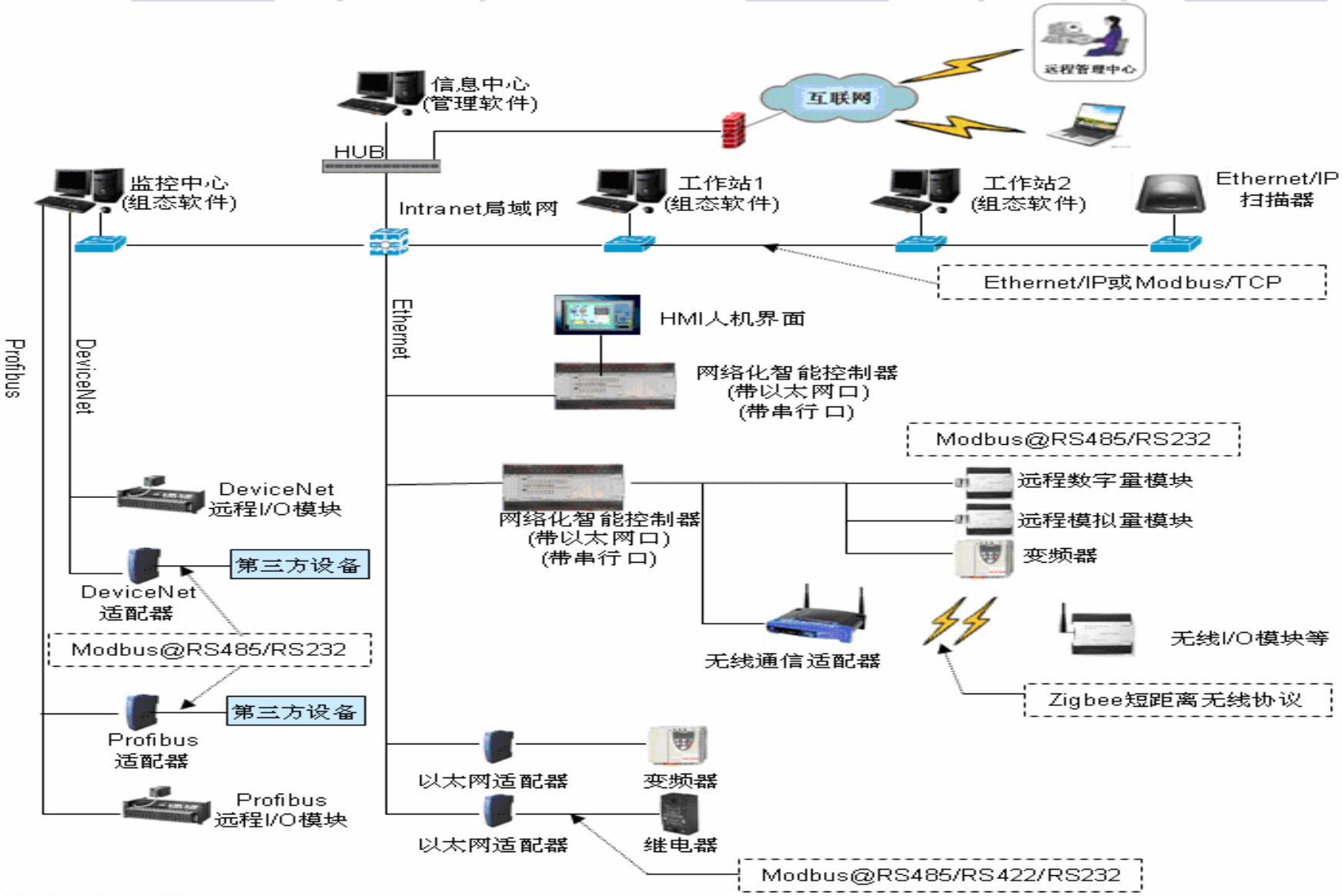


嵌入式Ethernet/IP通信适配器



嵌入式Ethernet/IP扫描器

可能的控制网络


远程管理中心
互联网
信息中心
(管理软件)
HUB
监控中心
(组态软件)
Intranet局域网
工作站1
(组态软件)
工作站2
(组态软件)
Ethernet/IP
扫描器
Ethernet/IP或Modbus/TCP
Profibus
DeviceNet
Ethernet
HMI人机界面
网络化智能控制器
(带以太网口)
(带串行口)
Modbus@RS485/RS232
远程数字量模块
远程模拟量模块
变频器
DeviceNet
远程I/O模块
网络化智能控制器
(带以太网口)
(带串行口)
第三方设备
DeviceNet
适配器
Modbus@RS485/RS232
无线通信适配器
无线I/O模块等
Zigbee短距离无线协议
第三方设备
Profibus
适配器
以太网适配器
变频器
Profibus
远程I/O模块
以太网适配器
继电器
Modbus@RS485/RS422/RS232

总结

- 以太网是当前应用最广的网络
- 基于以太网技术的工业网络即工业以太网具有性能和价格优势，是新一代工业网络的主流
- 工业以太网可以满足当前工业自动化的要求，而且具有很好的发展前景

感谢各位的关注

谢谢！