第 1 章　计算机网络技术

本章介绍在计算机网络工程规划设计、网络组建和网络运维管理过程中所必须理解和掌握的网络基础知识，并重点介绍了 TCP/IP 模型和 TCP/IP。

1.1　计算机网络基本概念

计算机网络是计算机技术和通信技术发展的必然产物。进入 20 世纪 90 年代以后，以因特网(Internet)为代表的计算机网络得到了飞速发展，加速了全球数字化、网络化、信息化和智能化革命的进程。计算机网络正日益影响和改变着人们的生活方式、工作方式和学习方式，现在人们的生活、工作、学习和交往都已离不开计算机网络了。

1.1.1　计算机网络的定义与分类

1. 计算机网络的定义

计算机网络是指利用无线或有线(Wi-Fi 及 3G、4G、5G 无线信号)传输介质，将分布在不同地理位置且自治的计算机互联起来而构成的计算机集合。组建网络的目的是实现资源共享和通信。

目前最大的计算机网络就是因特网，它是利用传输介质和网络互联设备，将分布在全球范围内的计算机和计算机网络互联起来，而形成的一个覆盖全球的计算机网络。

2. 计算机网络的分类

可以从不同的角度对计算机网络进行分类。

(1) 根据网络的交换功能的不同，计算机网络可分为电路交换网、报文交换网、分组交换网和混合交换网。混合交换就是在一个数据网络中同时采用了电路交换技术和分组交换技术。

目前计算机网络主要采用分组交换技术，而传统的电话网采用电路交换技术。

(2) 根据网络覆盖的地理范围的大小，计算机网络可分为局域网、城域网和广域网。

- 局域网(local area network，LAN)：指网络覆盖范围在几百米至几千米的网络，网络覆盖的地理范围较小，如校园网、企事业单位内部网等。

  局域网可运行的协议主要有以太网协议(IEEE 802.3)、令牌总线(IEEE 802.4)、令

牌环(IEEE 802.5)和光纤分布式数据接口(FDDI)。目前局域网最常用的是以太网协议,因此,在没有特别说明的情况下,局域网通常是指以太局域网。以太网是指运行以太网协议的网络。

- 城域网(metropolitan area network,MAN):指网络覆盖范围在几千米至几十千米的网络,其作用范围为一个城市。
- 广域网(wide area network,WAN):指网络覆盖范围在几十至几千千米的网络,可以跨越不同的国家或洲。因特网是全球最大的一个广域网,因特网通信采用TCP/IP簇,该协议簇就是为因特网而设计的。目前局域网也采用TCP/IP来通信。

(3) 根据网络的使用者,计算机网络可划分为公用网络和专用网络。

3. 网络的性能指标

计算机网络的主要性能指标有带宽和时延。

(1) 带宽。在模拟信号中,带宽是指通信线路允许通过的信号频率范围,其单位为赫兹。

在数字通信中,带宽是指数字信道发送数字信号的速率,其单位为比特每秒(b/s),因此带宽有时也称为吞吐量,常用每秒发送的比特数来表示。比如,通常说某条链路的带宽或吞吐量为100Mb/s,实际上是指该条链接的数据发送速率为100Mb/s,即每秒钟可传送100M比特的数据。

注意:*在数字通信中,单位换算关系与计算机领域是不相同的,其换算关系为*

$$1kb/s=1000b/s$$
$$1Mb/s=1000kb/s$$
$$1Gb/s=1000Mb/s$$

(2) 时延。时延是指一个报文或分组从链路的一端传送到另一端所需的时间。时延由发送时延、传播时延和处理时延三部分构成。

发送时延是使数据块从发送节点进入传输介质所需的时间,即从数据块的第一个比特数据开始发送算起,到最后一个比特发送完毕所需的时间,其值为数据块的长度除以信道带宽。因此,在发送的数据量一定的情况下,带宽越大,则发送时延越小,传输越快。发送时延又称传输时延。

传播时延是指电磁波在信道中传输一定的距离所花费的时间。一般情况下,这部分时延可忽略不计,但如果通过卫星信道传输,则这部分时延较大。电磁波在铜线电缆中的传播速度约为2.3×10^5km/s,在光纤中的速度约为2.0×10^5km/s,1000km长的光纤线路产生的传播时延约为5ms。

处理时延是指数据在交换节点为存储转发而进行一些必要处理所花费的时间。在处理时延中,排队时延占的比重较大,通常可用排队时延作为处理时延。

1.1.2 网络拓扑结构

网络拓扑结构是指用传输介质互联的各节点的物理布局。在网络拓扑结构图中,通常用点来表示联网的计算机,用线来表示通信链路。

在计算机网络中，网络拓扑结构主要有总线型、星形、环形、网状和树形，最常用的主要是星形。

1. 总线型结构网络

总线型结构网络使用同轴电缆细缆或粗缆作为公用总线来连接其他节点。总线的两端安装一对 50Ω 的终端电阻，以吸收剩余的电信号，避免产生有害的反射电信号。采用细同轴电缆时，每一段总线的长度一般不超过 185m。其网络拓扑结构如图 1.1 所示。总线结构网络可靠性差，速率慢(10Mb/s)，目前已不再使用。

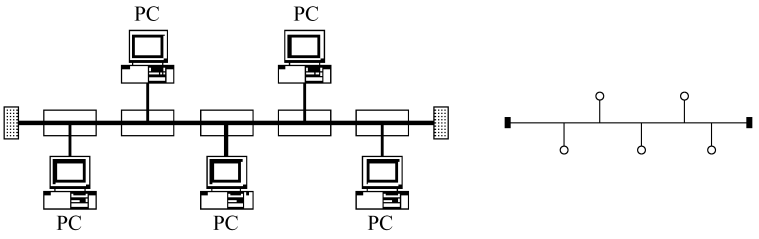

图 1.1　总线型的网络拓扑结构

主要优点：结构简单，所需电缆数量较少。

主要缺点：故障诊断和隔离较困难，可靠性差，传输距离有限，共享带宽，速度慢。

2. 星形结构网络

星形结构网络中，各节点以星形方式连接到中心交换节点，通过中心交换节点，实现各节点间的相互通信，是目前局域网的主要组网方式。中心交换节点可以用集线器或交换机，集线器是共享带宽设备，已淘汰，目前主要采用交换机来作为中心交换节点。其网络拓扑结构如图 1.2 所示。

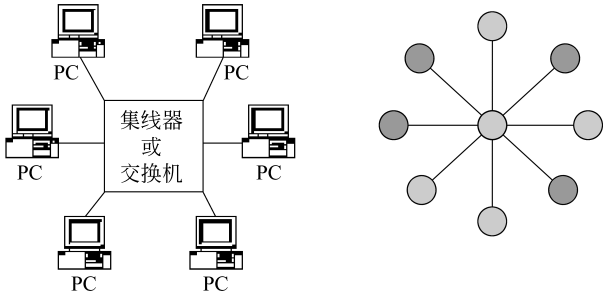

图 1.2　星形的网络拓扑结构

主要优点：控制简单，故障诊断和隔离容易，易于扩展，可靠性好。

主要缺点：需要的电缆较多，交换节点负荷较重。

3. 环形结构网络

环形结构网络由通信线路将各节点连接成一个闭合的环，数据在环上单向流动，网络中

用令牌控制来协调各节点的发送,任意两节点都可通信。其网络拓扑结构如图1.3所示。

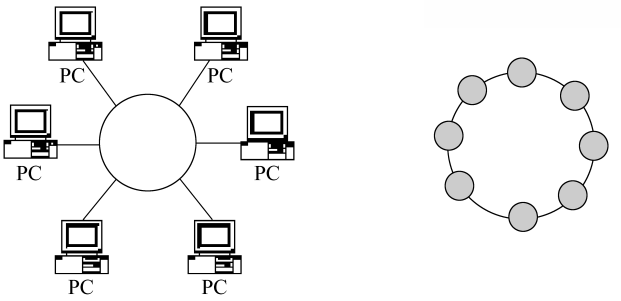

图1.3 环形的网络拓扑结构

主要优点:所需线缆较少,易于扩展。

主要缺点:可靠性差,一个节点的故障会引起全网故障,故障检测困难。

4. 网状结构网络

网状结构网络在所有设备间实现点对点的互联,如图1.4所示。

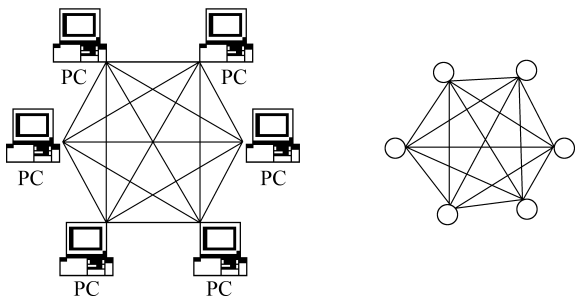

图1.4 网状的网络拓扑结构

在局域网中,使用网状结构较少;在因特网中,骨干路由器彼此间的互联可采用网状结构,以提供到目标网络的多种路径选择和链路冗余。

5. 树形结构网络

树形结构网络像一棵倒置的树,顶端是树根,树根以下带分支,每个分支还可再进行分支。树形结构网络易于扩展,故障隔离较容易,其缺点是各个节点对根的依赖性较大。

1.1.3 网络通信协议

1. 网络通信协议的概念

在计算机网络中,要做到有条不紊地交换数据和通信,就必须共同遵守一些事先约定好的规则,这些为进行网络数据交换而建立的规则、标准或约定就称为网络协议。

网络协议由语法、语义和同步三个要素组成。语法规定了数据与控制信息的结构或格式；语义则定义了所要完成的操作，即完成何种动作或做出何种响应；同步则是事件实现顺序的详细说明。

2. 常用的网络通信协议

在局域网中，常用的协议主要有 NetBEUI 和 TCP/IP 协议集，用得最广泛的主要是 TCP/IP 协议集。

(1) NetBEUI 协议。NetBEUI(NetBIOS extended user interface，NetBIOS 用户扩展接口)是 IBM 于 1985 年开发的一种体积小、效率高、速度快的通信协议，但不具备跨网段工作的能力，主要用于小型网络。

(2) TCP/IP 协议集。TCP/IP 是因特网的标准通信协议，支持路由和跨平台特性。在局域网中，也广泛采用 TCP/IP 来工作。TCP/IP 是一个大的协议集，并不仅是 TCP 和 IP 这两个协议。

1.2　计算机网络体系结构

相互通信的两个计算机系统必须高度协调一致才能正常工作，而这种协调过程是相当复杂的，因此，计算机网络实际上是个非常复杂的系统。

对计算机网络体系结构进行分层，可将庞大而复杂的问题，转化为若干较小的局部问题，这样就比较容易研究和处理。

对计算机网络体系结构的分层模型有 OSI 模型和 TCP/IP 模型两种。OSI 属于国际标准，由于分层较多，实现较复杂，主要用于理论研究。TCP/IP 模型分层较少，实现较容易，成为事实上的国际标准和工业生产标准。

1.2.1　OSI 模型

OSI(open system interconnection reference model，开放系统互联参考模型)是国际标准化组织 ISO 于 1983 年正式推出的参考模型，即著名的 ISO 7498 国际标准。

在 OSI 模型中，将网络体系结构分成了七层，由低层到高层，依次是物理层、数据链路层、网络层、传输层(运输层)、会话层、表示层和应用层。每一层均向相邻的上一层通过层间接口提供服务，上一层要在下一层所提供的服务的基础上实现本层的功能，因此服务是垂直的。而协议是水平的，它是控制对等层实体之间通信的规则，即只有对等的层才能相互通信。比如 A 计算机的数据链路层与 B 计算机的数据链路层之间通信，A 计算机的传输层与 B 计算机的传输层之间通信。

应用层为用户提供所需的各种应用服务，如 HTTP 服务、FTP 服务、邮件服务、域名服务等。

表示层主要用于数据的表示、编码和解码，实现信息的语法语义表示和转换，如加密

解密、转换翻译、压缩与解压缩等。

会话层用于为不同机器上的应用进程建立和管理会话。

传输层解决数据在网络之间的传输问题,用于提高网络层服务质量,提供点对点的数据传输。它从会话层接收数据,并在必要时将数据分割成适合在网络层传输的数据单元,然后将这些数据交给网络层,再由网络层负责将数据传送到目的主机。该层的数据传输单位为数据报。

网络层解决网络与网络之间的通信问题,主要功能有逻辑编址、分组传输、路由选择等。此层的数据传送单位为IP数据包。

数据链路层为网络层接供一条无差错的数据传输链路。在发送数据时,接收网络层传递来的数据包,封装成数据帧;在接收数据时,数据链路层将物理层传递来的二进制比特流,还原为数据帧。数据链路层传送的基本单位为数据帧,使用物理地址进行寻址。

物理层负责传送原始比特流,并屏蔽传输介质的差异,使数据链路层不必考虑传输介质的差异,实现数据链路层的透明传输。另外,物理层还必须解决比特同步的问题。

1.2.2 TCP/IP模型

1. TCP/IP模型体系结构

OSI的七层体系结构仅是一个纯理论的分析模型,本身并不是一个具体协议的真实分层,具有四层体系结构的TCP/IP模型得到了广泛应用,成为事实上的国际标准和工业生产标准。

在TCP/IP模型中,网络体系结构由低层到高层,依次为网络接口层、网络层、传输层(运输层)和应用层,其网络体系结构与OSI七层结构的对应关系如图1.5所示。

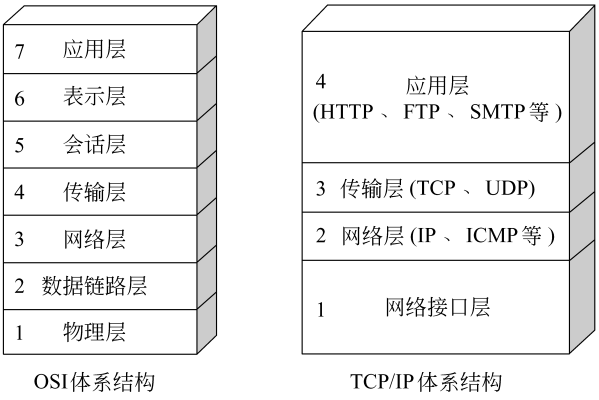

图1.5 OSI与TCP/IP体系结构的对应关系

在TCP/IP体系结构中,网络接口层整合了OSI体系结构中的物理层和数据链路层的功能,因此,从协议的层次结构看,TCP/IP模型实际上是一个具有五层协议的体系结构。

在实际应用中，网络接口层的功能主要由网络接口（网卡）来实现，它实现了数据链路层和物理层的功能。网络层主要由路由器或三层交换机来实现。传输层（运输层）由用户主机中的应用进程（比如 QQ 服务进程、IIS 服务进程等）来实现，它存在于分组交换网之外的主机中，传输层的任务就是负责两个主机中的服务进程之间的通信。传输层之上的应用层就不再关心信息的传输问题了。通常也将分组交换网称为通信子网，而将用户主机的集合称为资源子网。

2. 各层常用的协议

1）应用层协议

常用协议主要有 HTTP（hypertext transfer protocol，超文本传输协议）、HTTPS（hypertext transfer protocol over secure socket layer，安全的超文本传输协议）、SMTP（simple mail transfer protocol，简单邮件传输协议）、IMAP4（internet message access protocol version 4，交互式数据消息访问协议第 4 版）、POP3（post office protocol version 3，邮局协议第 3 版）、Telnet（终端仿真协议）、SSH（secure shell）、FTP（file transfer protocol，文件传输协议）、TFTP（trivial file transfer protocol，简单文件传输协议）、DNS（domain name system，域名系统）、DHCP（dynamic host configuration protocol，动态主机配置协议）、SNMP（simple network management protocol，简单网络管理协议）等。

2）传输层协议

传输层提供端到端（主机服务进程对另一主机服务进程）的数据传输，提供可靠传输协议 TCP（transmission control protocol，传输控制协议）和不可靠传输协议 UDP（user datagram protocol，用户数据报协议）两种。

TCP 提供面向连接的、可靠的传输服务。利用 TCP 传输数据时，必须先建立 TCP 连接，连接建立成功后，才能传输数据。TCP 提供传输可靠性控制机制，通过流量控制、分段/重组和差错控制功能，能对传送的分组进行跟踪，对在传输过程中丢失的报文，会要求重传，从而保证传输的可靠性。

UDP 是一种无连接的传输层协议，提供面向事务的、简单、不可靠的信息传送服务。UDP 无法跟踪报文的传输过程，当报文发送之后，是无法得知其是否安全完整地到达目标主机的，故是不可靠的传输协议，常用于数据量大且对可靠性要求不高的传输应用，比如音频或视频信号的传输。

3）网络层协议

网络层协议主要是 IP。IP 的作用是将数据封装成 IP 数据包，并运行必要的路由算法，对 IP 数据包进行路由转发，实现网络与网络之间的通信。

网络层协议除了 IP 之外，还有两个附属协议，分别是 ICMP（Internet control message protocol，因特网控制报文协议）和 IGMP（Internet group management protocol，因特网组管理协议），它们可视为工作在网络层和传输层之间，其数据采用 IP 数据包进行封装。对这两个协议，没有严格定义它们是属于网络层还是传输层，一般习惯上将其视为网络层协议。

ICMP 是一种无连接的协议，用于在 IP 主机、路由器之间传递控制消息，这些控制消

息包括网络是否通畅,主机是否可达,路由是否可用等。检测网络是否通畅的 ping 命令和 tracert 路由追踪命令就是基于 ICMP 工作的。

IGMP 是因特网协议家族中的一个组管理协议,用于组播通信,属于组成员管理协议,管理组播组成员的加入和离开。主机和组播路由器之间通过 IGMP 来实现组播组成员信息的交互。

4) 网络接口层协议

网络接口层完成了 OSI 中的数据链路层和物理层的功能,在进行数据分组传送时,负责建立无差错的数据传输链路。

数据链路层常用的协议主要有 LLC(logical link control,逻辑链路控制)协议、MAC(medium access control,介质访问控制)协议、ARP(address resolution protocol,地址解析协议)、RARP(reverse address resolution protocol,反向地址解析协议)、MPLS(multiprotocol label switch,多协议标签交换)协议等。

ARP、RARP 和 MPLS 协议工作时涉及数据链路层和网络层,可视为工作在数据链路层和网络层之间的协议。

数据链路层分为 LLC 和 MAC 两个子层。LLC 子层是数据链路层的上层部分,为网络层提供统一的接口,LLC 子层实现与硬件无关的功能,比如流量控制、差错恢复等。在 LLC 子层下面是 MAC 子层,MAC 子层提供与物理层之间的接口。

ARP 用于将目的 IP 地址解析为数据链路层物理寻址所需的 MAC 地址,解析成功后,IP 地址与 MAC 地址的对应关系将保存在主机的 ARP 缓冲区中,从而建立起一个 ARP 列表,以供下次查询使用。ARP 缓冲区中的 ARP 列表有老化期,以保证列表的有效性。

RARP 用于将 MAC 地址解析为对应的 IP 地址,功能与 ARP 相反。

MPLS 是一种标记(label)机制的包交换技术,通过简单的 2 层交换来集成 IP 路由的控制功能。利用 MPLS 技术与 VPN 技术相结合,可实现 MPLS VPN。

目前国内使用较多的仍是 TCP/IP 的第 4 版,即 IPv4,新版的 IPv6 已在骨干网络中部署和应用;IPv4 与 IPv6 将共同存在较长的时间;IPv6 是未来发展和应用的方向,也是物联网发展的基础。

3. 数据在各层间的传递过程

为简化问题,假设计算机 1 和计算机 2 直接相连,现在计算机 1 的应用进程 AP_1 要向计算机 2 的应用进程 AP_2 发送数据,下面分析该数据在发送端和接收端的各层间的传递和处理过程。

应用进程 AP_1 将要传送的数据交给应用层,应用层在数据首部加上必要的控制信息 H_5,然后将数据传递给下面的传输层,数据和控制信息就成为下一层的数据单元。

传输层接收到这个数据单元后,在首部加上本层的控制信息 H_4,再交给下面的网络层,成为网络层的数据单元。

网络层接收到这个数据单元后,在首部加上 IP 包头 H_3,再交给下面的数据链路层。

数据链路层收到这个数据单元后,在首部和尾部分别加上控制信息 H_2 和 T_2,将数据

单元封装成数据帧，然后交给物理层进行传送。

对于 HDLC 数据帧，在首部和尾部各加上 24bit 的控制信息；对于 Ethernet V2 格式的 MAC 帧，首部添加 14(6＋6＋2)字节，尾部添加 4 字节的帧校验序列(frame check sequence，FCS)。

物理层直接进行比特流的传送，不再加控制信息。当这一串比特流经网络传输介质到达目的主机时，就从第 1 层依次交付给上一层进行处理。每一层根据控制信息进行必要的操作，然后将本层的控制信息剥去，将剩下的数据单元再交付给上一层进行处理，最后，应用进程 AP_2 就可收到来自 AP_1 应用进程传送的数据。

从中可见，数据在发送时从高层向低层流动，每一层(物理层除外)都给收到的数据单元套上一个本层的“信封”(控制信息)；数据在被接收时从低层向高层流动，每一层(物理层除外)进行必要处理后，去掉本层的“信封”，将“信封”中的数据单元再上交给上一层进行处理。整个传递过程如图 1.6 所示。

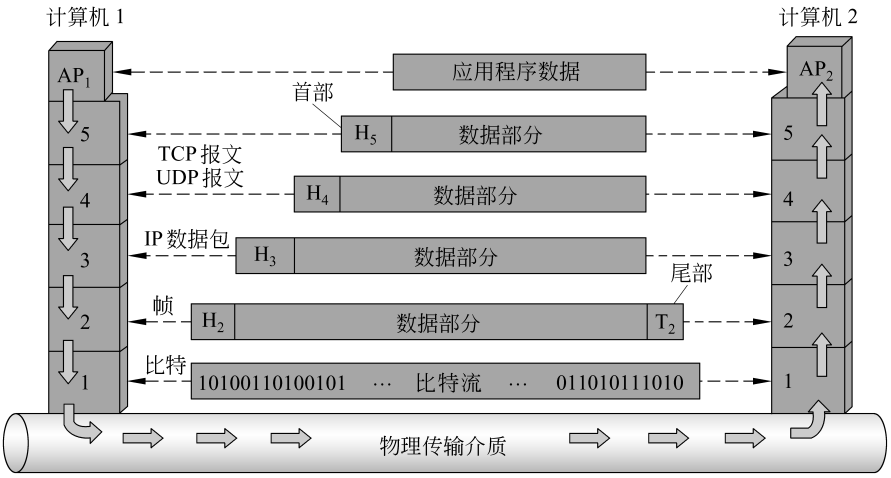

图 1.6　数据在各层间的传递过程

1.3　以太网简介

1. 以太网标准

以太网是美国施乐(Xerox)公司于 1975 年研制成功的，是一种基于基带总线的局域网，采用无源电缆作为总线来传送数据帧，当时的数据速率为 2.94Mb/s。

1980 年，DEC、Intel 和施乐公司联合提出了 10Mb/s 速率的以太网规范(DIX V1)。1982 年修改为第二版(DIX Ethernet V2)，成为世界上第一个局域网规范。

在此基础上，IEEE 802 委员会于 1983 年制定了第一个以太网标准，编号为 IEEE 802.3，数据速率为 10Mb/s。该标准仅对帧格式做了很小的调整，允许基于这两种标准的

硬件可以在同一个局域网上互操作。由于这两个标准差异很小,通常不严格区分。因此目前存在两个以太网协议标准,即国际标准的IEEE 802.3和DIX Ethernet V2标准。

由于商业竞争,IEEE的802委员会并未形成统一的局域网标准,除了以太网局域网标准(IEEE 802.3)外,还有令牌总线(IEEE 802.4)和令牌环网(IEEE 802.5)的局域网标准。目前局域网主要采用以太网协议标准,称为以太局域网。

2. 以太网工作原理

以太网使用带冲突检测的载波侦听和载波侦听多路访问/冲突检测(carrier sense multiple access with collision detection,CSMA/CD)协议进行工作。

载波侦听是指每一个站点在发送数据之前,都要先检测总线是否空闲,是否有其他计算机在发送数据,如果有,则暂时不要发送数据,以免发生碰撞冲突。

冲突检测是指站点应边发送数据边检测信道上的信号电压的大小,以判断当前是否有冲突产生。如果有碰撞冲突产生,信号将产生严重失真,此时就必须立即停止发送,并等待一段随机时间后,再重新进行载波侦听和发送。

从中可见,使用CSMA/CD协议工作时,一个站点不能同时发送数据和接收数据,属于半双工通信。连接在同一总线上的所有站点,均在同一个冲突域范围内,站点越多,碰撞冲突的概率就越大,网络通信速率和效率就会大大降低。

早期使用集线器设备连接构建的局域网属于同一个冲突域,因此通信速度和效率很低下。

3. 高速以太网

传统以太网的速率为10Mb/s,且以半双工方式工作。速率达到或超过100Mb/s的以太网统称为高速以太网。

1) 快速以太网

快速以太网(fast ethernet)是指速率达到100Mb/s的以太网,采用星形拓扑结构,在双绞线(100Base-TX)或光纤(100Base-FX)上传送100Mb/s的基带信号。1995年IEEE正式将快速以太网定为国际标准,编号为IEEE 802.3u。

快速以太网的MAC帧格式仍采用IEEE 802.3标准规定的帧格式,由于速率提高了10倍,为了保持最短帧长(64字节)不变,将网段的最大电缆长度减小到100m,帧间时间间隔也从原来的9.6μs改为0.96μs。

快速以太网是对IEEE 802.3标准的补充,能自动识别和适应10Mb/s和100Mb/s网速。

2) 吉比特以太网

吉比特以太网又称千兆以太网。IEEE于1997年通过了吉比特以太网标准,编号为IEEE 802.3z,1998年成为正式标准。

吉比特以太网允许在1Gb/s速率下以全双工或半双式两种模式工作,向后兼容10Base-T和100Base-T。使用IEEE 802.3协议规定的帧格式,在半双工模式工作时使用CSMA/CD协议。