通 信 安 全

L11—TCP/IP隐患及安全通信协议

- 教师：崔爱娇

- 编号：ELEC3019
- 学时：32学时

概 要

TCP/IP隐患及安全通信协议

计算机网络概述

TCP/IP协议

安全威胁与防范

概 要

TCP/IP隐患及安全通信协议

计算机网络概述

TCP/IP协议

安全威胁与防范

计算机网络的演变

第一阶段 理论基础研究的阶段

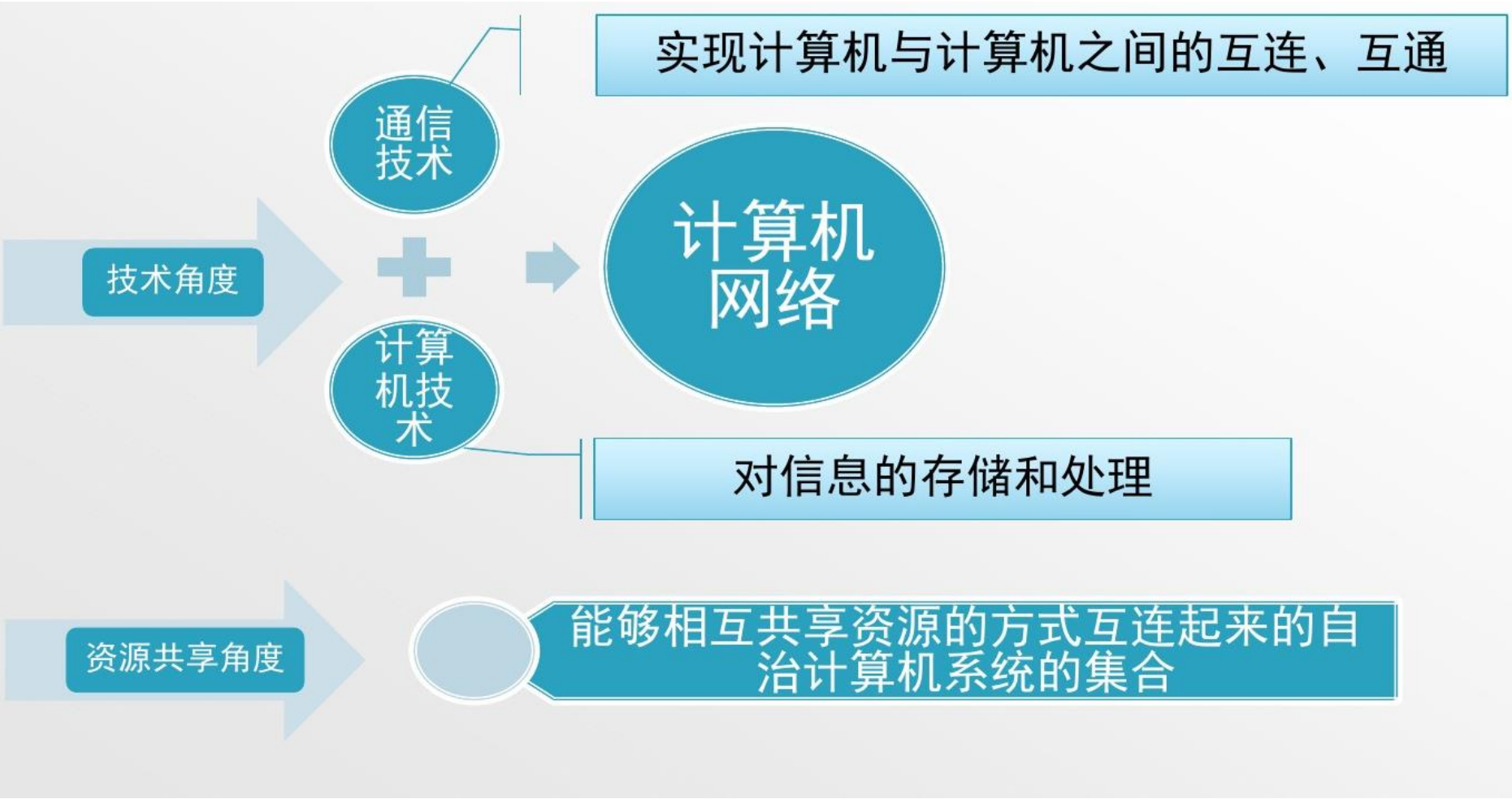
第二阶段 新型分组交换技术的诞生

标志着计算机网络与通信技术的结合基本成型

第三阶段 TCP/IP协议的提出

标志着通信与计算机技术的结合基本完成

计算机网络的概念


技术角度
通信技术
计算机技术
计算机网络
实现计算机与计算机之间的互连、互通
对信息的存储和处理
资源共享角度
能够相互共享资源的方式互连起来的自治计算机系统的集合

计算机网络的性质

- **分散性**：计算机网络所连接的计算机系统可以是分布在不同地理位置的多台独立的计算机系统
- **异构性**：计算机网络中所包含的计算机不论是在组成上，还是在功能上，都可以有显著的不同
- **自治性**：参与连接计算机网络的计算机应该是“自治计算机系统”，即所有计算机应该实行自我管理

计算机网络协议

网络协议包含上基本要求

语法	• 用来规定信息格式
语义	• 用来说明通信双方应当怎么做
时序规则	• 消息说明事件的先后顺序

计算机网络分类

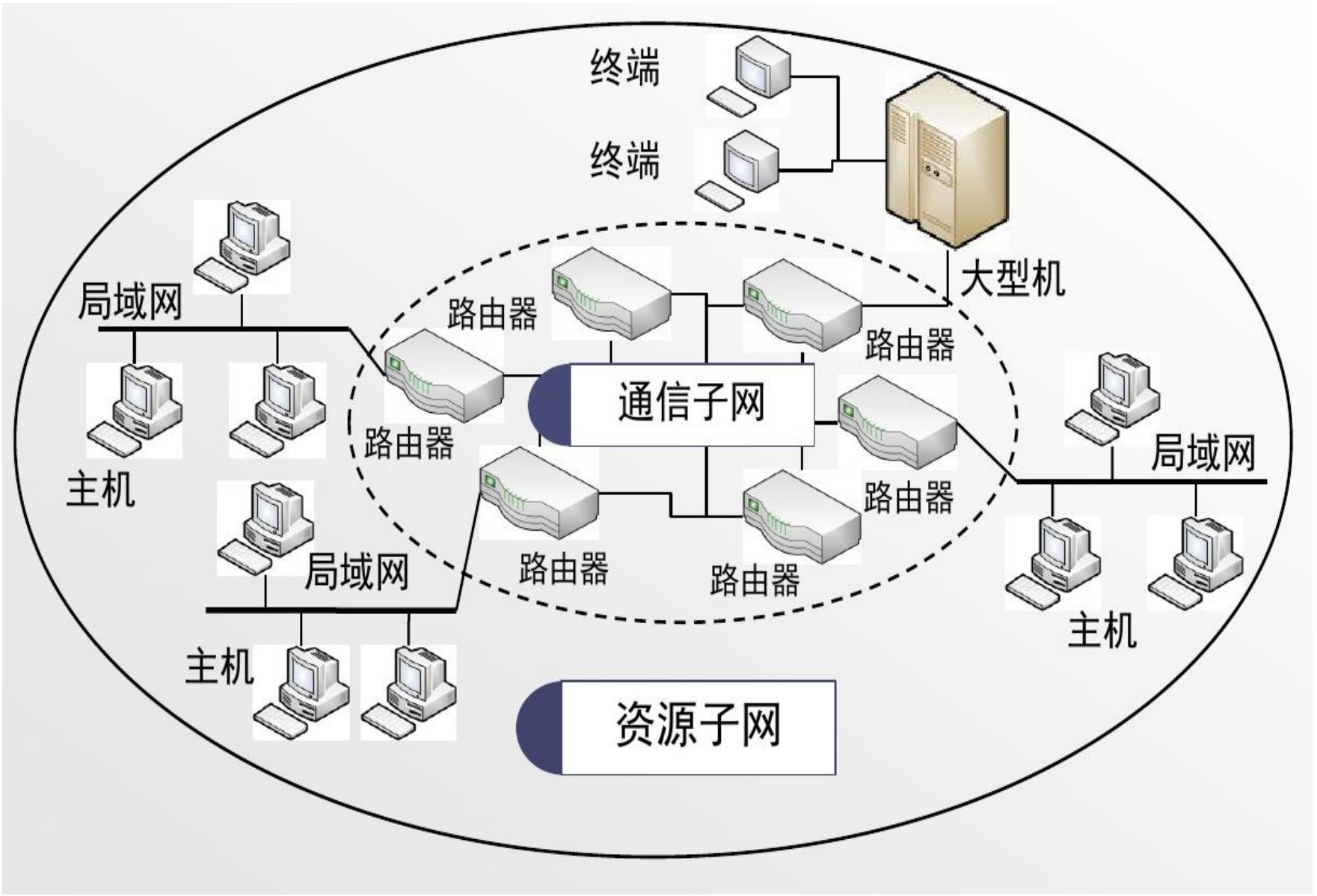
按传输技术分类

广播式网络（Broadcast Networks）
点对点网络（Point-to-point networks）

按网络的覆盖范围与规模分类

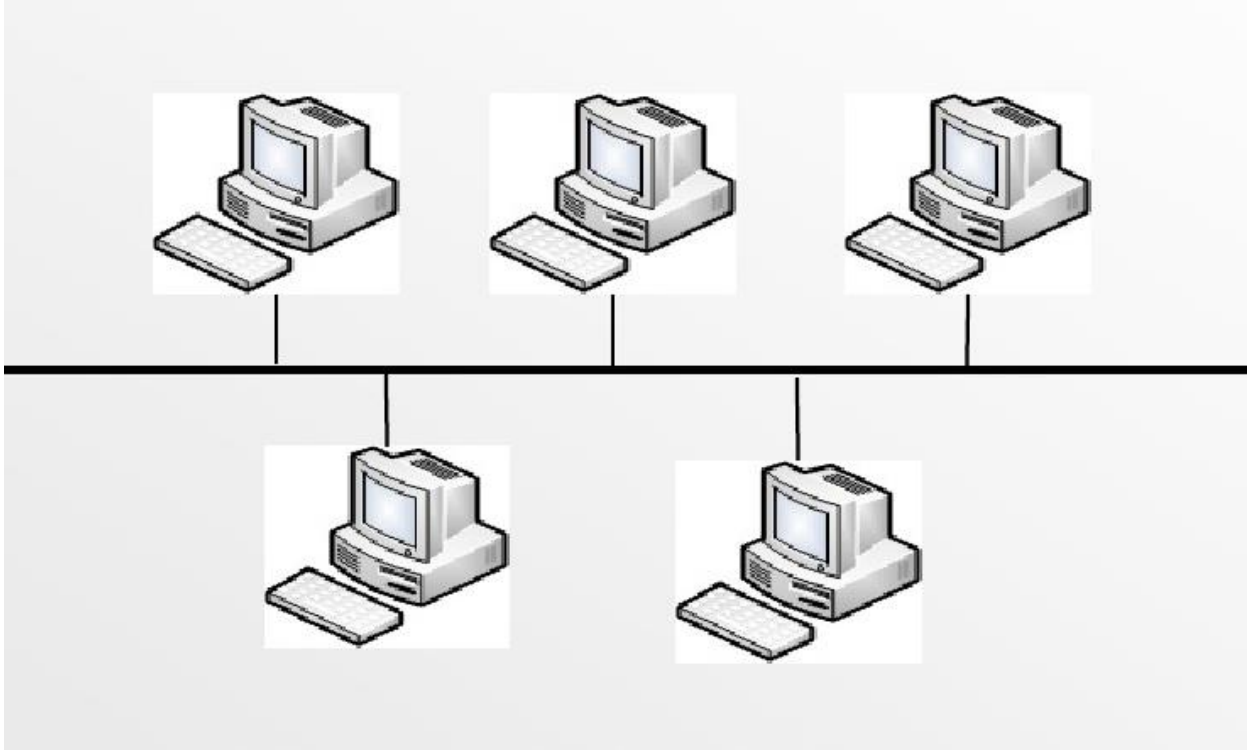
局域网（LAN）
城域网（MAN）
广域网（WAN）

计算机网络的组成与结构



常见计算机网络拓扑结构

总线结构

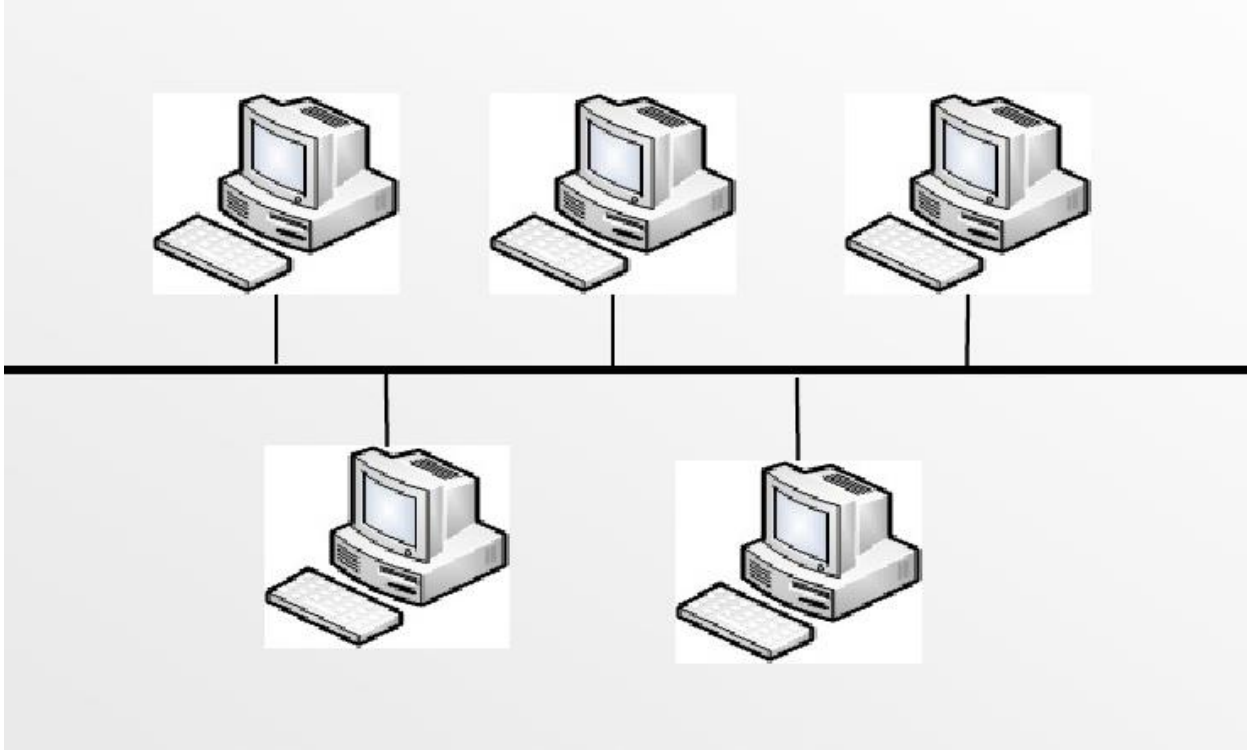


优点

(1)总线结构所需要的电缆数量少，线缆长度短，易于布线和维护。
(2)总线结构简单,又是元源工作,有较高的可靠性。传输速率高，可达1~100Mbps。
(3)易于扩充,增加或减少用户比较方便，结构简单，组网容易，网络扩展方便
(4)多个节点共用一条传输信道，信道利用率高。

常见计算机网络拓扑结构

总线结构

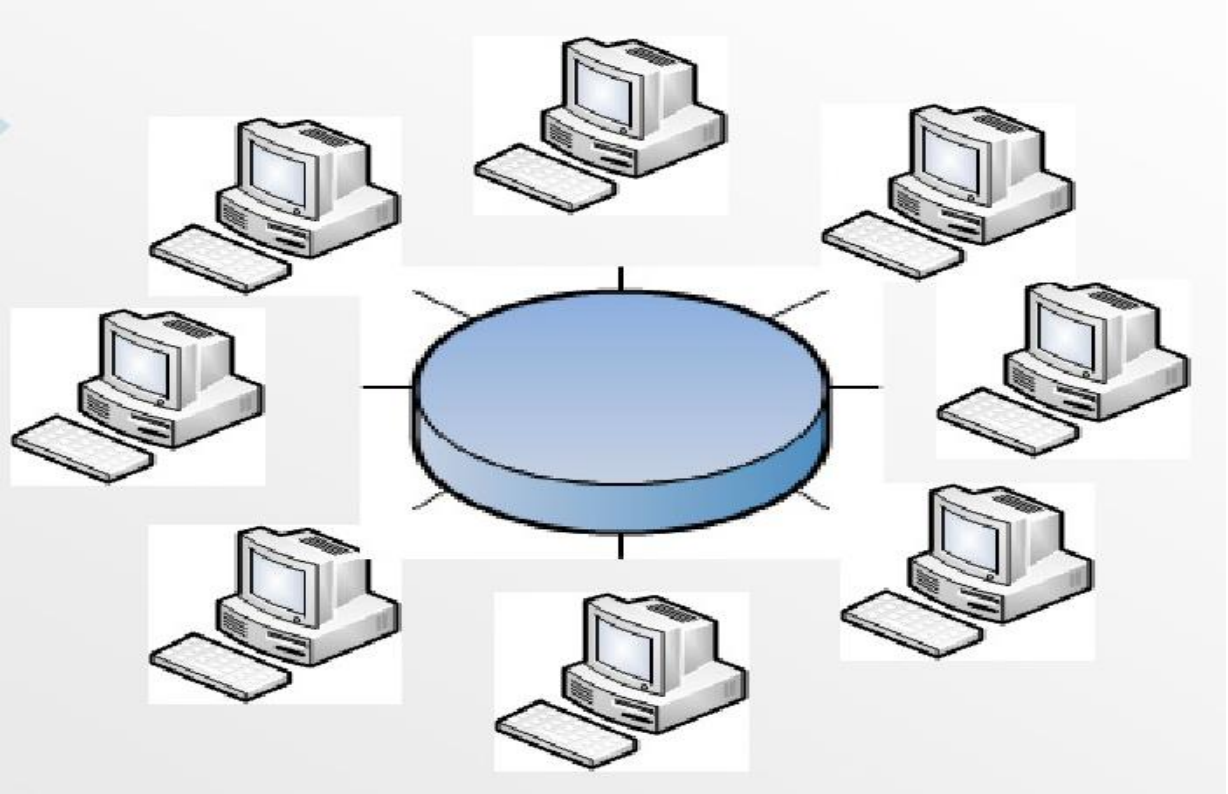


缺点

(1)总线的传输距离有限,通信范围受到限制。
(2)故障诊断和隔离较困难。
(3)分布式协议不能保证信息的及时传送，不具有实时功能。站点必须是智能的,要有媒体访问控制功能,从而增加了站点的硬件和软件开销。

常见计算机网络拓扑结构

环状结构

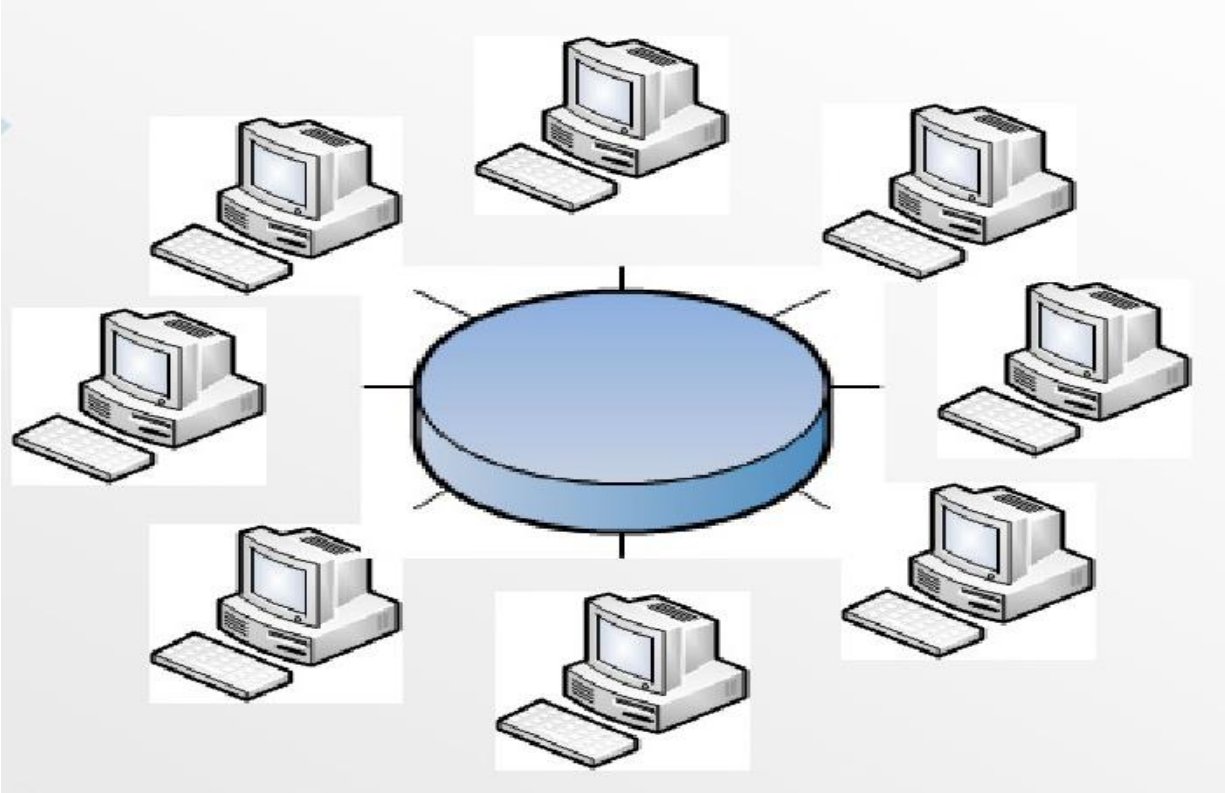


优点

(1)电缆长度短。环型拓扑网络所需的电缆长度和总线拓扑网络相似，但比星形拓扑网络要短得多。
(2)增加或减少工作站时，仅需简单的连接操作。
(3)可使用光纤。光纤的传输速率很高，十分适合于环型拓扑的单方向传输。

常见计算机网络拓扑结构

环状结构

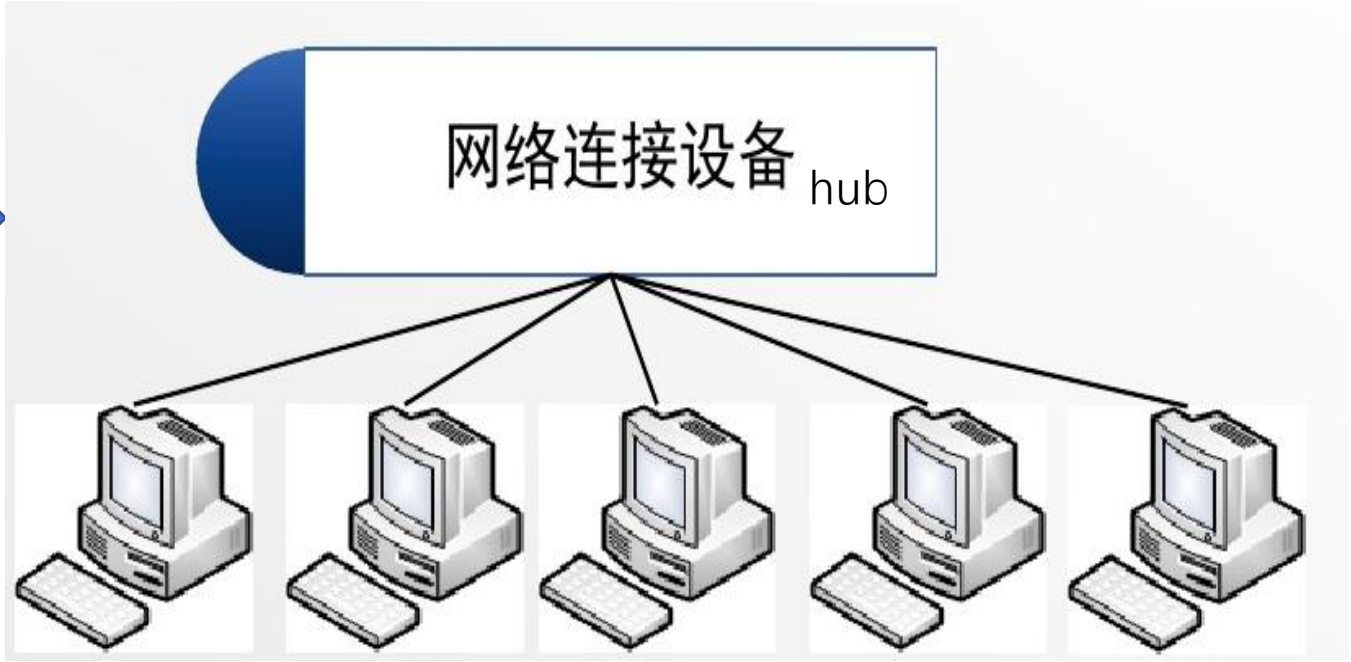


缺点

(1)节点的故障会引起全网故障。这是因为环上的数据传输要通过接在环上的每一个节点,一旦环中某一节点发生故障就会引起全网的故障。
(2)故障检测困难。这与总线拓扑相似,因为不是集中控制,故障检测需在网上各个节点进行,因此就不很容易。
(3)环型拓扑结构的媒体访问控制协议都采用令牌传递的方式,在负载很轻时,信道利用率相对来说就比较低。

常见计算机网络拓扑结构

星状结构

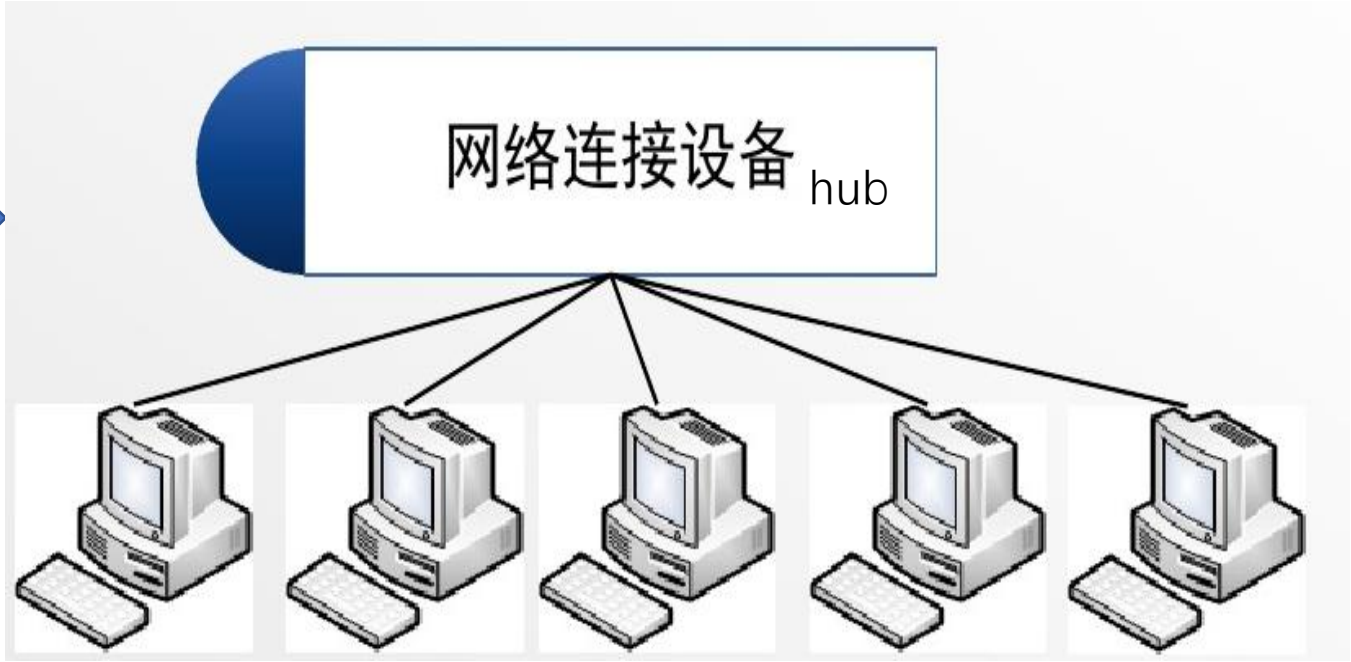


优点

（1）结构简单，连接方便，管理和维护都相对容易，而且扩展性强。
（2）网络延迟时间较小，传输误差低。
（3）在同一网段内支持多种传输介质，除非中央节点故障，否则网络不会轻易瘫痪。
（4）每个节点直接连到中央节点，故障容易检测和隔离，可以很方便地排除有故障的节点。
因此，星型网络拓扑结构是目前应用最广泛的一种网络拓扑结构。

常见计算机网络拓扑结构

星状结构

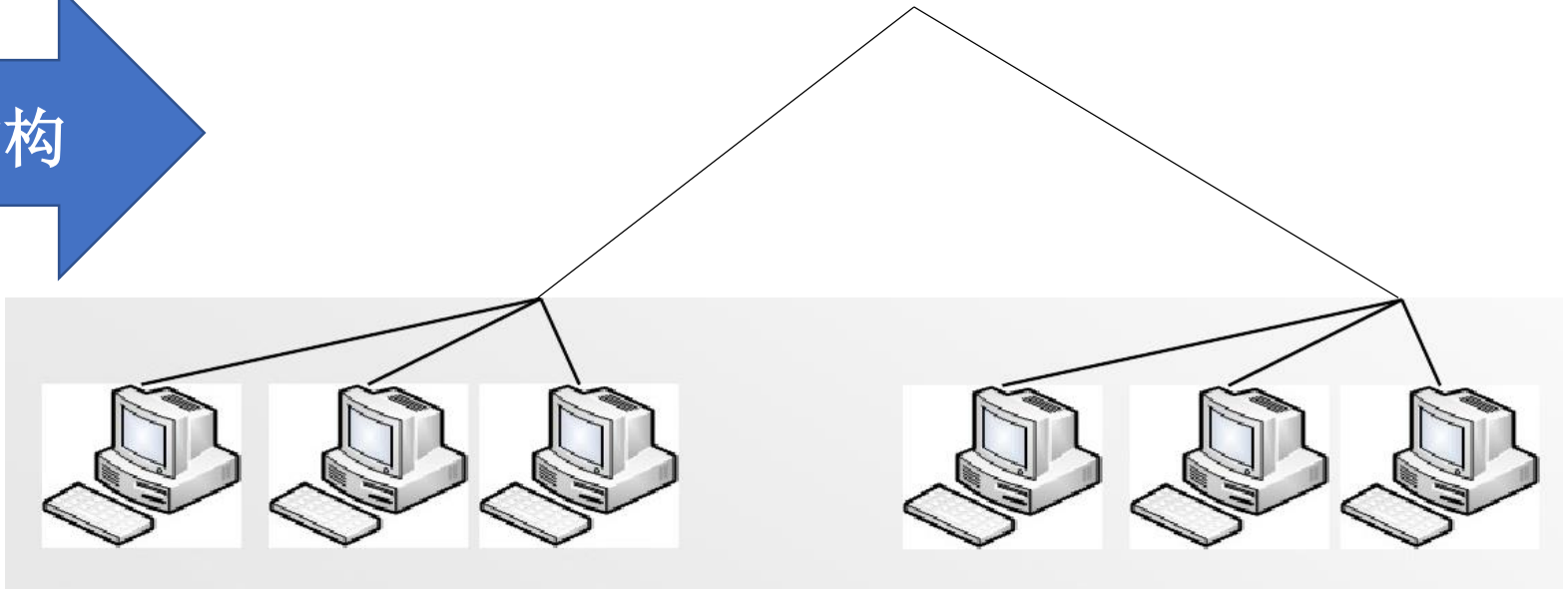


缺点

（1）安装和维护的费用较高
（2）共享资源的能力较差
（3）一条通信线路只被该线路上的中央节点和边缘节点使用，通信线路利用率不高
（4）对中央节点要求相当高，一旦中央节点出现故障，则整个网络将瘫痪。

常见计算机网络拓扑结构

树状结构

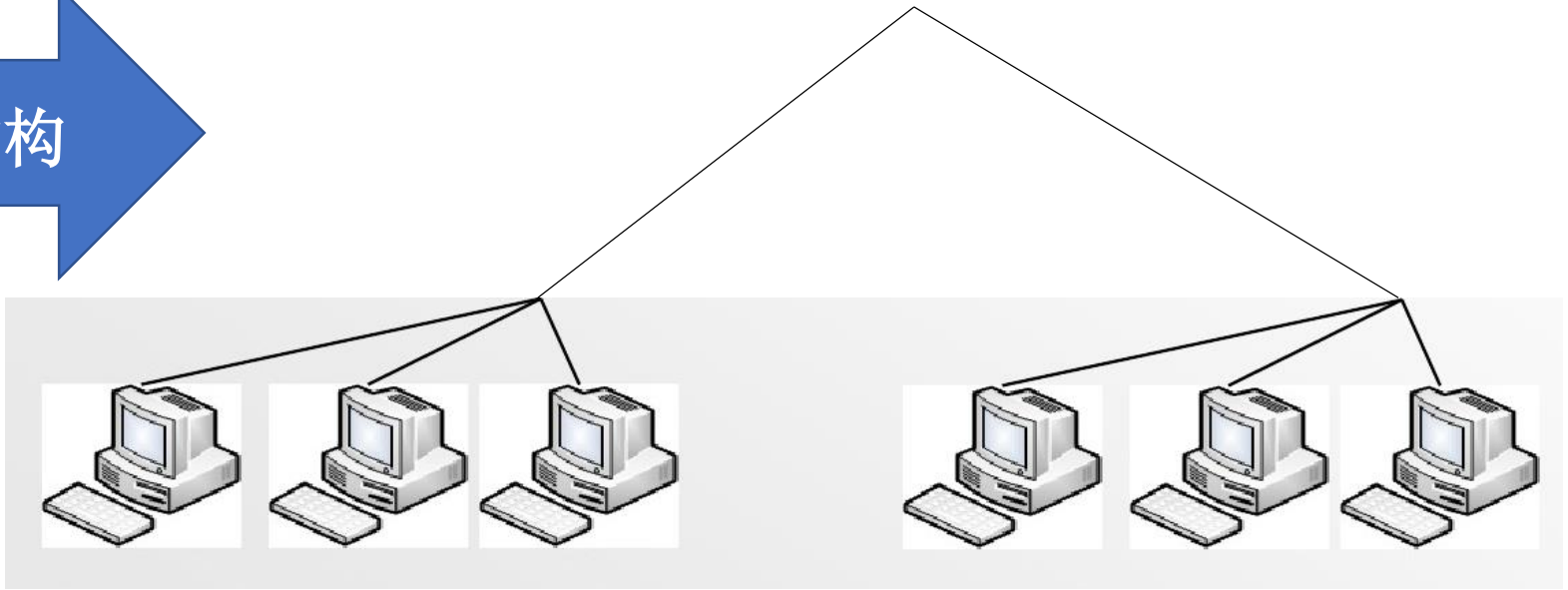


优点

(1)易于扩展。这种结构可以延伸出很多分支和子分支,这些新节点和新分支都能容易地加入网内。
(2)故障隔离较容易。如果某一分支的节点或线路发生故障,很容易将故障分支与整个系统隔离开来。

常见计算机网络拓扑结构

树状结构

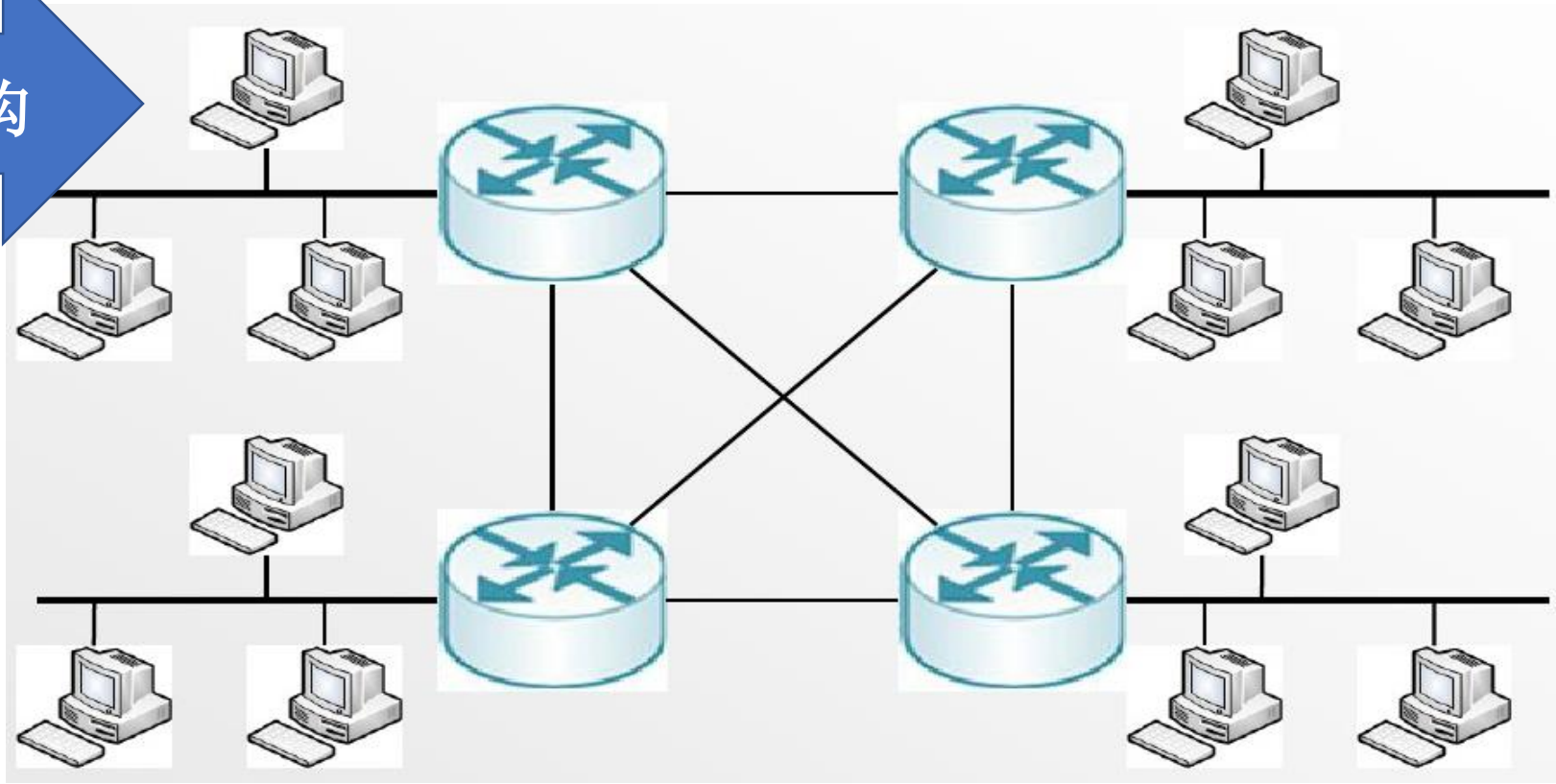


缺点

各个节点对根的依赖性太大，如果根发生故障，则全网不能正常工作。从这一点来看，树型拓扑结构的可靠性有点类似于星型拓扑结构。

常见计算机网络拓扑结构

网状结构



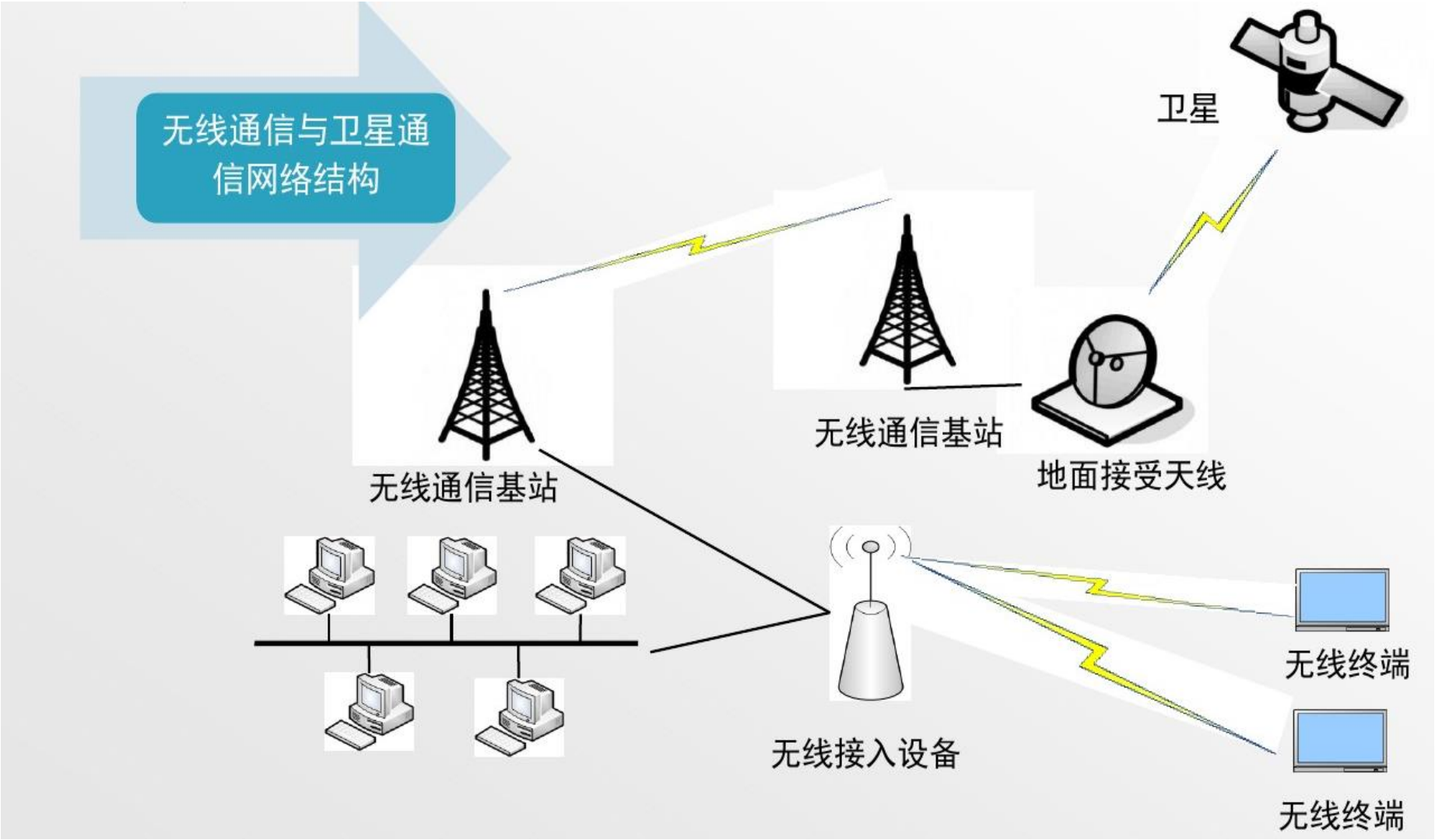
优点

(1)节点间路径多，碰撞和阻塞减少。
(2)局部故障不影响整个网络，可靠性高。

缺点

(1)网络关系复杂，建网较难，不易扩充。
(2)网络控制机制复杂，必须采用路由算法和流量控制机制。

常见计算机网络拓扑结构



概 要

TCP/IP隐患及安全通信协议

计算机网络概述

TCP/IP协议

安全威胁与防范

第7层应用层：OSI中的最高层。为特定类型的网络应用提供了访问OSI环境的手段。应用层确定进程之间通信的性质，以满足用户的需要。应用层不仅要提供应用进程所需要的信息交换和远程操作，而且还要作为应用进程的用户代理，来完成一些为进行信息交换所必需的功能。

第4层传输层：传输层是网络体系结构中高低层之间衔接的一个接口层。传输层不仅仅是一个单独的结构层，而是整个分析体系协议的核心。传输层为会话层用户提供一个端到端的可靠、透明和优化的数据传输服务机制。

第3层网络层：本层通过寻址来建立两个节点之间的连接，为源端的运输层送来的分组，选择合适的路由和交换节点，正确无误地按照地址传送给目的端的运输层。它包括通过互连网络来路由和中继数据；除了选择路由之外，网络层还负责建立和维护连接，控制网络上的拥塞以及在必要的时候生成计费信息。

第2层数据链路层：在此层将数据分帧，并处理流控制。屏蔽物理层，为网络层提供一个数据链路的连接，在一条有可能出差错的物理连接上，进行几乎无差错的数据传输（差错控制）。本层指定拓扑结构并提供硬件寻址。常用设备有网桥、交换机;

第1层物理层：处于OSI参考模型的最底层。物理层的主要功能是利用物理传输介质为数据链路层提供物理连接，以便透明的传送比特流。常用设备有（各种物理设备）网卡、集线器、中继器、调制解调器、网线、双绞线、同轴电缆。

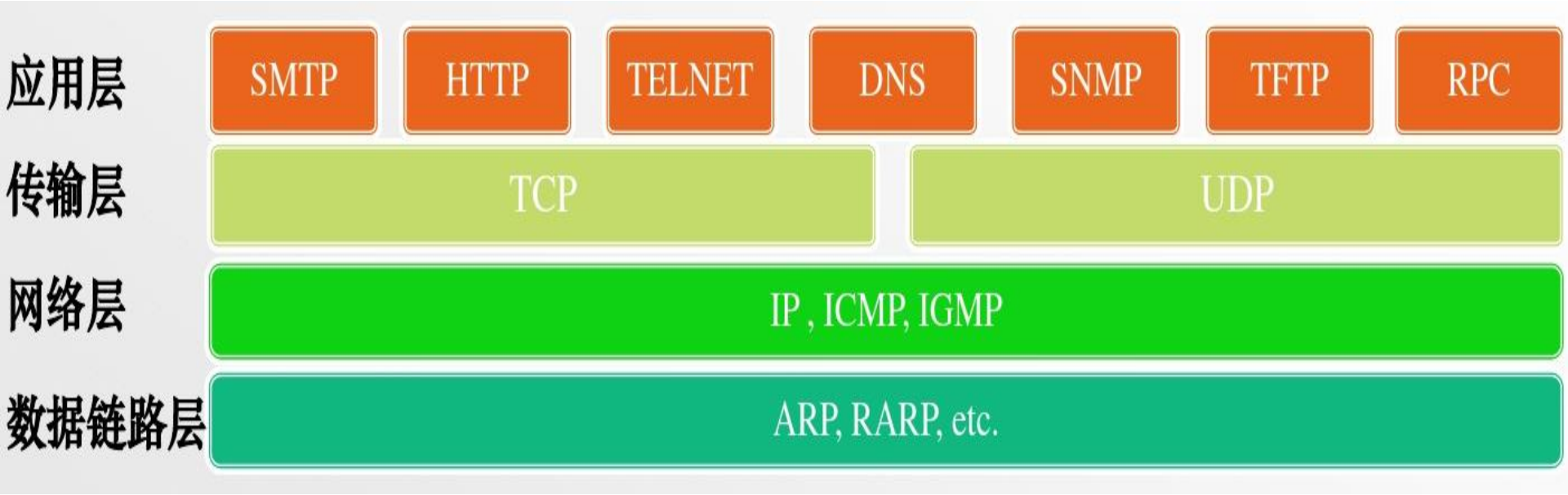
TCP/IP协议基础——OSI参考模型

应用层	• 应用进程访问网络服务的窗口
表示层	• 解释不同控制码、字符集和图形字符等
会话层	• 负责建立、维护和同步通信设备之间的交互操作
传输层	• 负责整个消息无差错、按顺序地的从信源到信宿传递过程
网络层	• 负责数据包成功和有效率地经过多条链路、 • 由信源到信宿的传递过程
数据链路层	• 负责将数据帧无差错地从一个站点送达下一个相邻站点
物理层	• 数据链路实体间透明的比特（Bit）流传输

TCP/IP协议基础——协议栈

应用层	• 直接为网络应用提供服务，使得应用程序能通过网络收发数据
传输层	• 提供面向连接的服务和无连接的服务
网络层	• 提供无连接服务。网络层负责对数据包进行路由选择
数据链路层	• 负责在物理媒介中传输端到端数据包
物理层	• 实现端到端比特流传输

TCP/IP协议基础——协议栈



概 要

TCP/IP隐患及安全通信协议

计算机网络概述

TCP/IP协议

安全威胁与防范

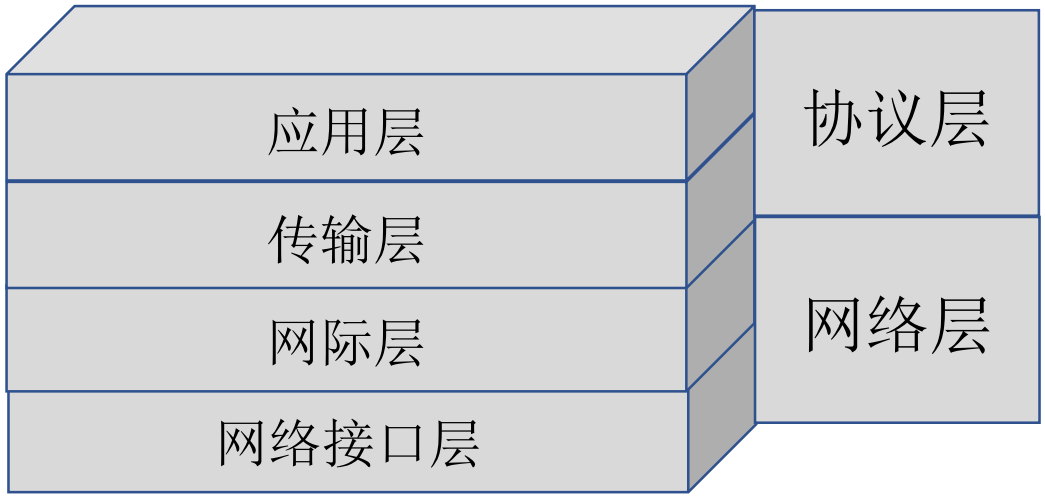
TCP/IP体系

TCP/IP开始仅仅是两个协议：TCP(Transfer Control Protocol，传输控制协议)和IP（Internet Protocol，网际协议）。

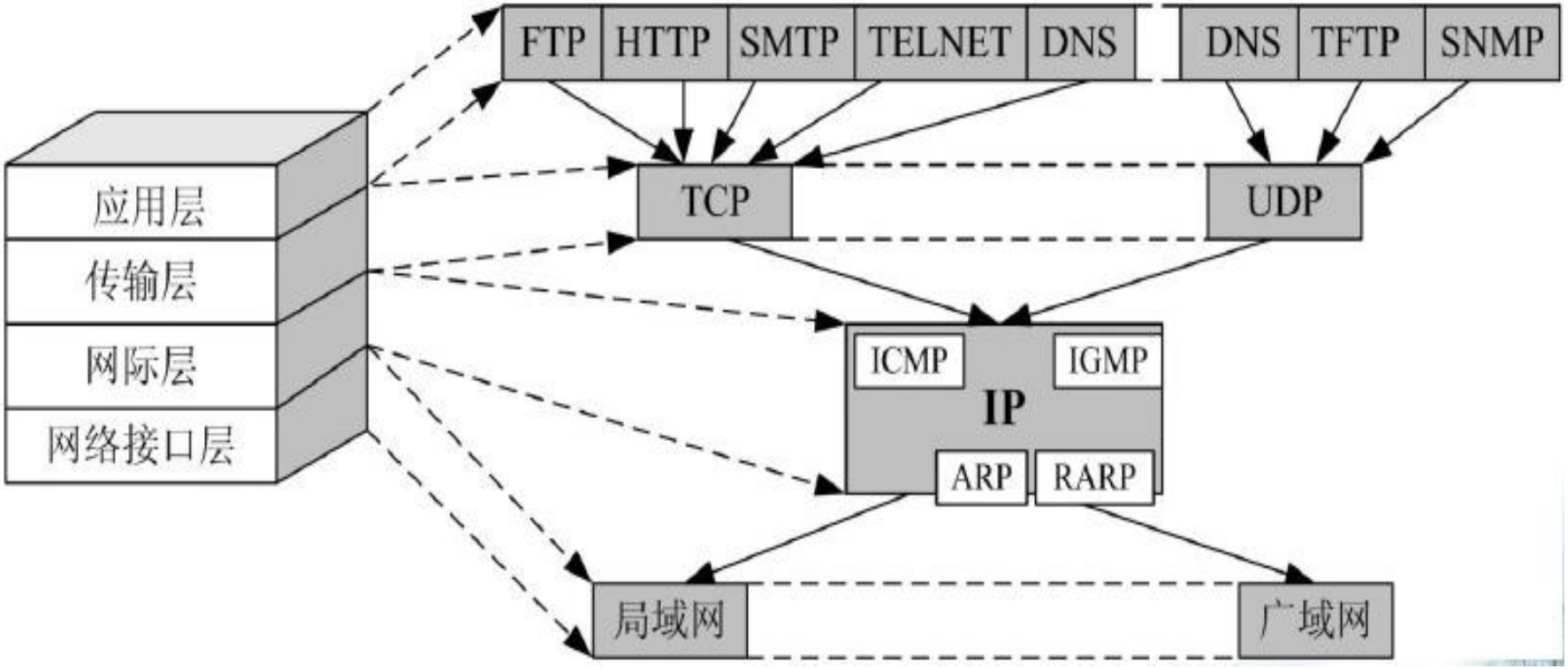
后来，TCP/IP演变为一种体系结构，即TCP/IP参考模型。现在的TCP/IP已成为一个工业标准的协议集，它最早应用于ARPAnet。

与OSI参考模型不同，TCP/IP模型由应用层（Application Layer）、传输层（Transport Layer）、网际层（Internet Layer，也称Internet层）和网络接口层（Network Interface Layer）四部分组成。

TCP/IP体系



TCP/IP协议族



TCP/IP体系中的主要协议及与各层的对应关系

TCP/IP各层的主要功能

TCP/IP体系也称为TCP/IP参考模型，该模型从下到上分为网络接口层、网际层、传输层和应用层，共4个子层。各层的主要功能如下。

1. 网络接口层：在TCP/IP参考模型中，网络接口层属于最低的一层，它负责通过网络发送和接收分组。

2. 网际层：网际层也称为“互联网络层”，它相当于OSI参考模型网络层的无连接网络服务。网际层的任务是：允许位于同一网络或不同网络中的两台主机之间以分组的形式进行通信。。

TCP/IP各层的主要功能

3. 传输层：在TCP/IP参考模型中，传输层位于网际层与应用层之间，其设计目标是：允许在源和目的主机的对等体之间进行对话，负责会话对等体的应用进程之间的通信。TCP/IP参考模型的传输层功能类似于OSI参考型传输层的功能。

4. 应用层：应用层属于TCP/IP参考模型的最高层。应用层包括根据应用需要开发的一些高层协议，如telnet、FTP、SMTP、DNS、SNMP、HTTP等。而且，随着网络应用的不断发展，新的应用层协议还会不断出现。

TCP/IP网络中的分组传输示例

（1）子网：一个大型的通信网络由多个子网（subnetwork）组成，每一个子网属于某一种特定类型的网络，如局域网中的以太网、令牌环网、FDDI，广域网中的 x.25、帧中继等。

（2）网络接入协议：当计算机接入网络时，必须使用这一子网中规定的接入协议。通过网络接入协议，可以让一台主机将数据通过子网发送到其他的主机。

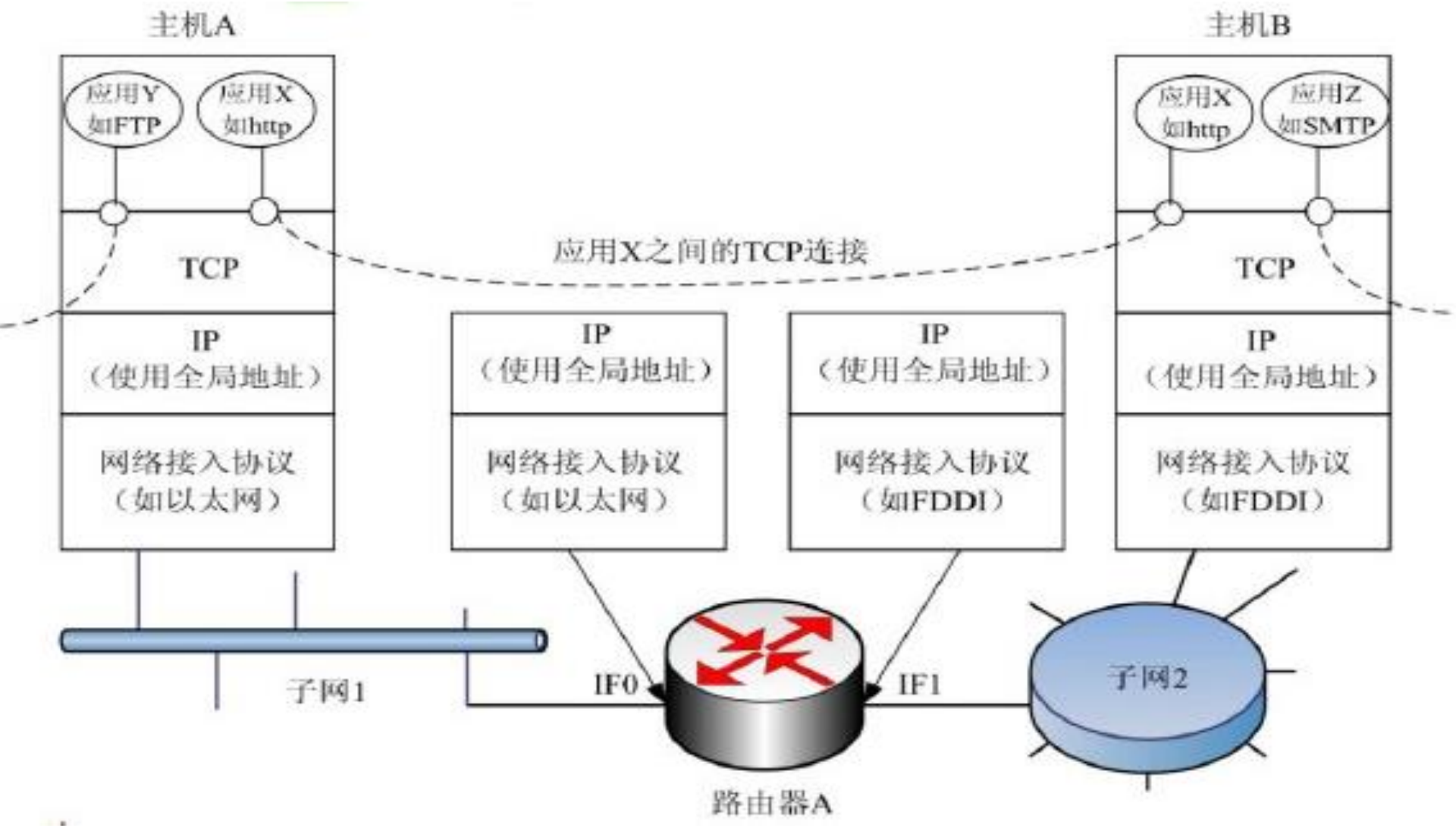
（3）路由器：它是连接不同子网的设备，一台路由器相当于一个中继站，将一个IP分组从某一子网中的一台主机通过一个或多个子网发送到目的主机。

TCP/IP网络中的分组传输示例

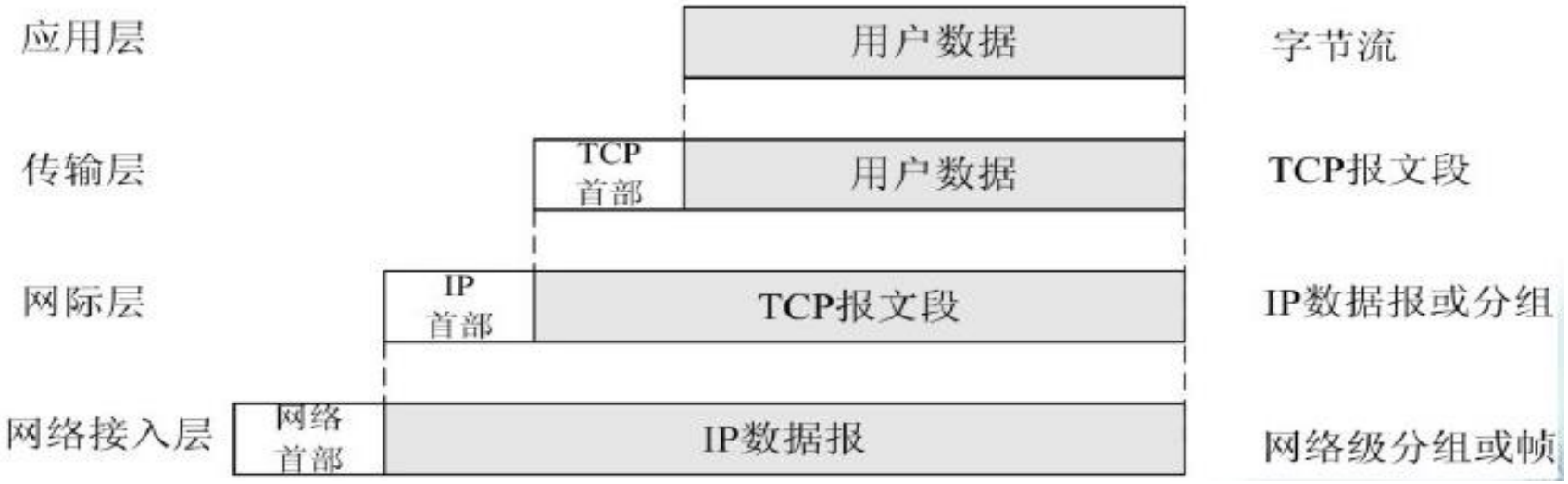
（4）全局地址：对于Internet等互联网络来说，每一台主机必须拥有一个全网唯一的IP地址作为其身份的唯一标识，这个IP地址称为全局地址。当源主机发送数据到目的主机时，源主机首先要知道目的主机的IP地址。

（5）端口：主机中的每一个进程必须具有一个在本主机中唯一的地址，这个地址称为端口(port)。通过端口，端到端的协议（如TCP）才能够将数据正确地交付给相应的进程。

TCP/IP网络中数据的传输过程



在TCP/IP参考模型中，每一次的数据称为协议数据单元（PDU）,例如TCP报文段也称为TCP PDU。在数据发送端，在每一次添加首部信息的过程称为数据封装。在数据接收端，每一层去掉首部信息的过程称为数据解封。



TCP/IP网络中数据的封装过程

ARP安全

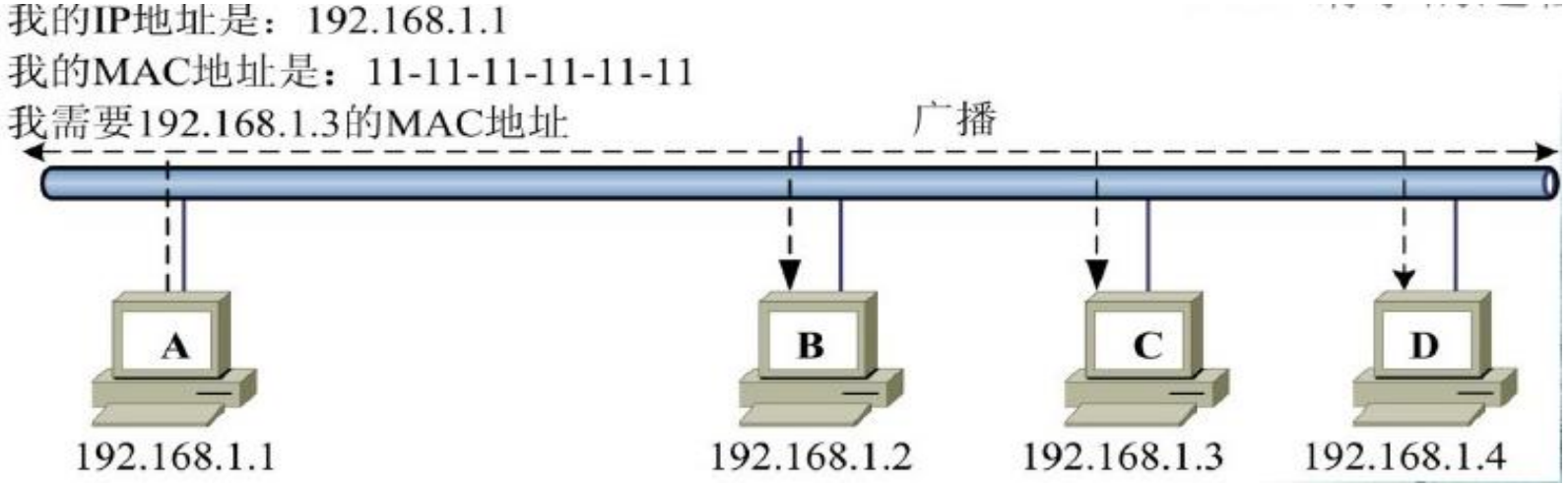
ARP(Address Resolution Protocol，地址解析协议)用来将IP地址映射到MAC地址，以便设备能够在共享介质的网络（如以太网）中通信。

ARP协议的实现中还有一些应该注意的事项：
（1）每天计算机上都有一个ARP缓冲，它保存了一定数量的从IP地址到MAC地址的映射，同时当一个ARP广播到来时，虽然这个ARP广播可能与它无关，但ARP协议软件也会把其中的物理地址与IP地址的映射记录下来，这样做的好处是能够减少ARP报文在局域网上发送的次数。

（2）按照缺省设置，ARP高速缓存中的项目是动态的，ARP缓冲中IP地址与物理地址之间的映射并不是一旦生成就永久有效的，每一个ARP映射表项都有自己的寿命，如果在一段时间内没有使用，那么这个ARP映射就会从缓冲中被删除，这一点和交换机MAC地址表的原理一样。这种老化机制，大大减少了ARP缓存表的长度，加快了查询速度。

ARP安全

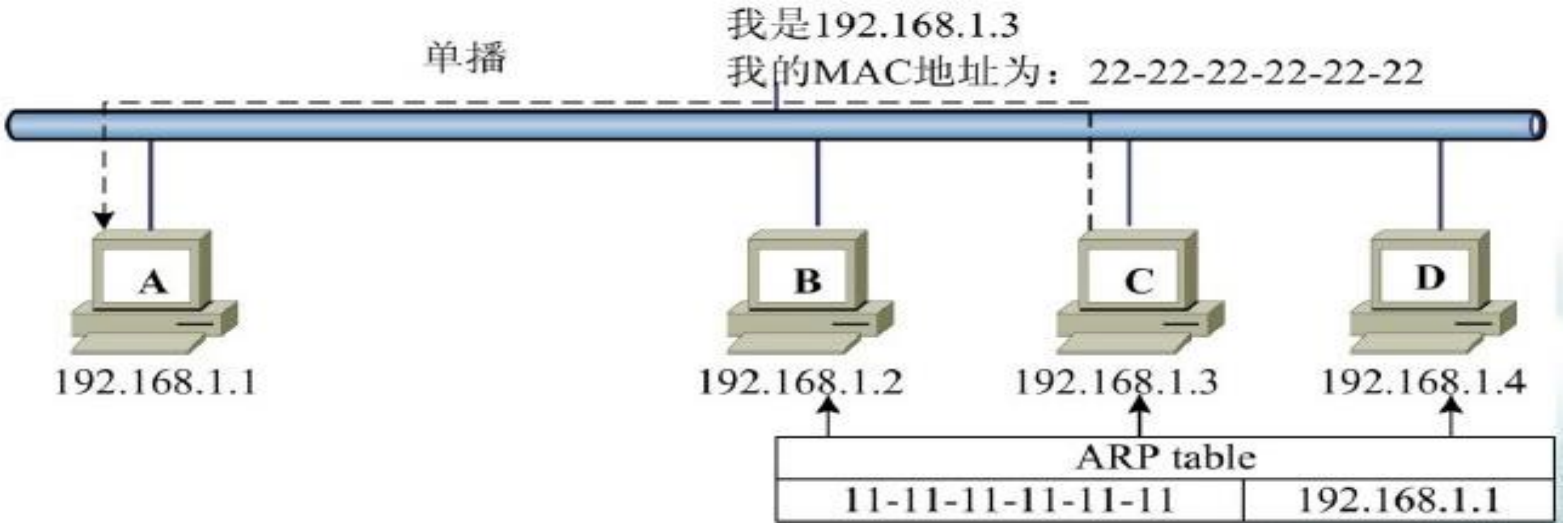
在以太网中，当主机要确定某个IP地址的MAC地址时，它会先检查自己的ARP缓冲表，如果目标地址不包含在该缓冲表中，主机就会发生一个ARP请求（广播形式），网段上的任何主机都可以接收到该广播，但是只有目标主机才会响应此ARP请求。由于目标主机在收到ARP请求时可以学习到发送方的IP地址到MAC地址的映射，因此它采用一个单播消息来回应请求。



ARP请求的过程

ARP安全

主机B、主机D收到主机A发来的ARP请求时，他们发现这个请求不是发给自己的，因此他们忽略这个请求，但是他们还是将主机A的IP地址到MAC地址的映射记录到自己的ARP表中。当主机C收到主机A发来的ARP请求时，它发现这个ARP请求时发给自己的，于是它用单播消息回应ARP请求，同时记录下其IP地址到MAC地址的映射。



ARP回应的过程

ARP欺骗的概念和现状

由于ARP协议在设计中存在的主动发送ARP报文的漏洞，使得主机可以发送虚假的ARP请求报文或响应报文，报文中的源IP地址和源MAC地址均可以进行伪造。在局域网中，即可以伪造成某一台主机（如服务器）的IP地址和MAC地址的组合，也可以伪造成网关的IP地址和MAC地址的组合，等等。

针对计算机的ARP欺骗

假设主机A向主机B发送数据。在主机A中，当应用程序要发送的数据到了TCP/IP参考模型的网际层与网络接口层之间时，主机A在ARP缓存表中查找是否有主机B的MAC地址（其实是主机B的IP地址与MAC地址的对应关系），如果有，则直接将该MAC地址（22-22-22-22-22-22）作为目的MAC地址添加到数据单元的网络首部（位于网络接口层），成为数据帧。

由于ARP协议在设计中存在的主动发送ARP报文的漏洞，使得主机可以发送虚假的ARP请求报文或响应报文，报文中的源IP地址和源MAC地址均可以进行伪造。在局域网中，即可以伪造成某一台主机（如服务器）的IP地址和MAC地址的组合，也可以伪造成网关的IP地址和MAC地址的组合，等等。（同一IP网段，如本例的192.168.1.x）中，主机利用MAC地址作为寻址的依据，所以主机A根据主机B的MAC地址，将数据帧发送给主机B。

针对计算机的ARP欺骗

由于ARP协议在设计中存在的主动发送ARP报文的漏洞，使得主机可以发送虚假的ARP请求报文或响应报文，报文中的源IP地址和源MAC地址均可以进行伪造。在局域网中，即可以伪造成某一台主机（如服务器）的IP地址和MAC地址的组合，也可以伪造成网关的IP地址和MAC地址的组合，等等。（同一IP网段，如本例的192.168.1.x）中，主机利用MAC地址作为寻址的依据，所以主机A根据主机C的MAC地址，将数据帧发送给主机C 。

主机	IP地址	MAC地址
主机A	192.168.1.1	11-11-11-11-11-11
主机B	192.168.1.2	22-22-22-22-22-22
主机C	192.168.1.3	33-33-33-33-33-33
主机D	192.168.1.4	44-44-44-44-44-44
主机E	192.168.1.5	55-55-55-55-55-55

主机中IP地址与MAC地址的对应关系示意图

针对计算机的ARP欺骗

如果主机A在ARP缓存表中没有找到目标主机C的IP地址对应的MAC地址

主机A就会再网络上发送一个广播帧，该广播帧的目的MAC地址是“FF. FF. FF. FF. FF. FF”，表示向局域网内的所有主机发出这样的询问：IP地址为192.168.1.3的MAC地址是什么？

在局域网中所有的主机都会接受到该广播帧，但在正常情况下因为只有主机B的IP地址是192.168.1.3，所以主机C会对该广播帧进行ARP响应，即向主机A发送一个ARP响应帧：我（ IP地址是192.168.1.3 ）的MAC地址是“33-33-33-33-33-33”。

针对计算机的ARP欺骗

如果现在主机D要对主机A进行ARP欺骗，冒充自己是主机C。

具体实施中，当主机A 要与主机C进行通信时，主机D主动告诉主机A自己的IP地址和MAC地址的组合是“192.168.1.3+44-44-44-44-44-44-”，

这样当主机A要发送给主机C数据时，会将主机D的MAC地址44-44-44-44-44-44-添加到数据帧的目的MAC地址中，从而将本来要发给主机C的数据发给了主机D,实现了ARP欺骗。

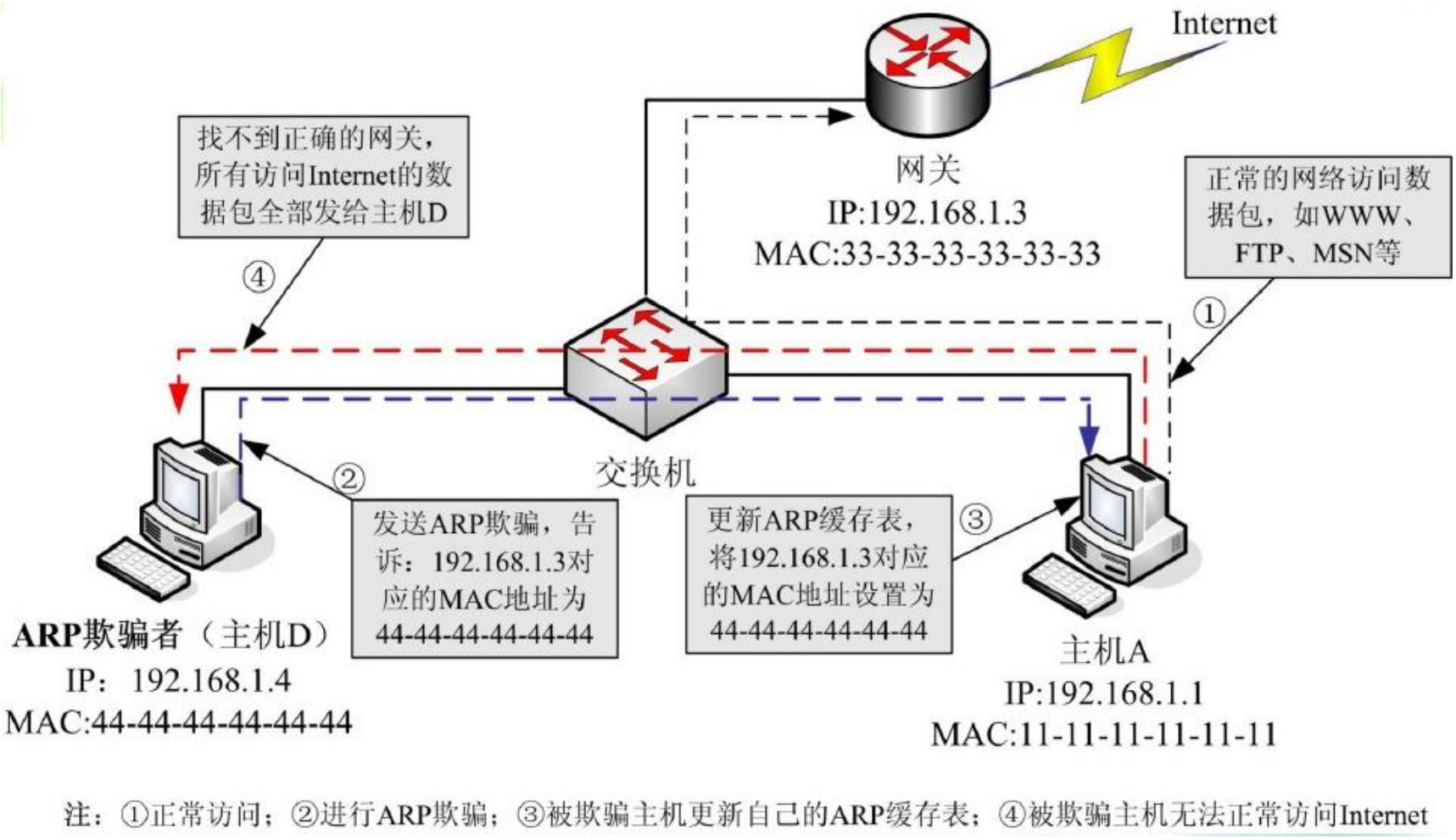
在整个ARP欺骗过程中，主机D称为“中间人”（man in the middle）,对这一中间人的存在主机A根本没有意识到。

针对计算机的ARP欺骗

通过以上的ARP欺骗，使主机A与主机C之间断开了联系。

现在假设主机C是局域网中的网关，而主机D为ARP欺骗者。这样，当局域网中的计算机要与其他网络进行通信（如访问Internet）时，所以发往其他网络的数据全部发给了主机D，而主机D并非真正的网关，这样整个网络将无法与其他网络进行通信。

这种现象在ARP欺骗中非常普遍。


Internet
网关
IP:192.168.1.3
MAC:33-33-33-33-33-33
找不到正确的网关，所有访问Internet的数据包全部发给主机D
④
正常的网络访问数据包，如WWW、FTP、MSN等
①
交换机
②
发送ARP欺骗，告诉：192.168.1.3对应的MAC地址为44-44-44-44-44-44
更新ARP缓存表，将192.168.1.3对应的MAC地址设置为44-44-44-44-44-44
③
ARP欺骗者（主机D）
IP：192.168.1.4
MAC:44-44-44-44-44-44
主机A
IP:192.168.1.1
MAC:11-11-11-11-11-11
注：①正常访问；②进行ARP欺骗；③被欺骗主机更新自己的ARP缓存表；④被欺骗主机无法正常访问Internet

ARP欺骗的实现过程

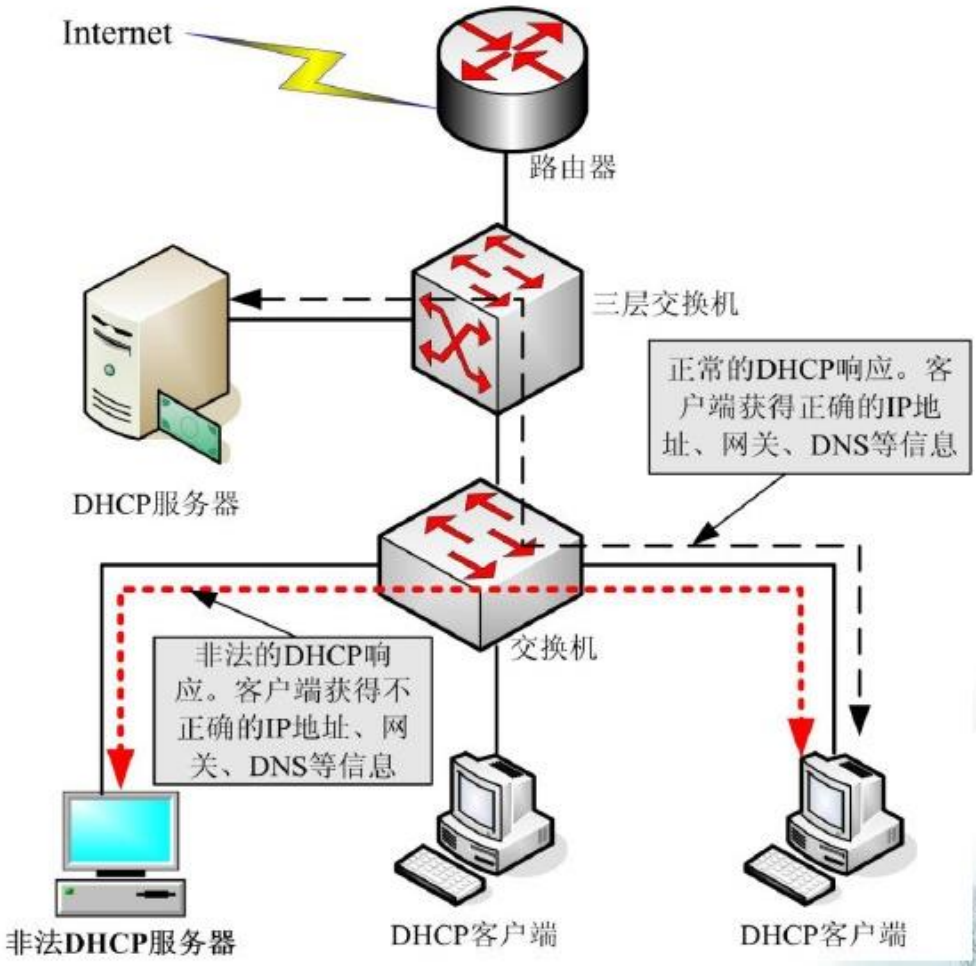
DHCP安全

DHCP(Dynamic Host configuration Protocol，动态主机配置协议)是一个客户机/服务器协议，在TCP/IP网络中对客户机动态分配和管理IP地址等配置信息，以简化网络配置，方便用户使用及管理员的管理。

DHCP概述

一台DHCP服务器可以是一台运行Windows 2000 Server、UNIX或Linux的计算机，也可以是一台路由器或交换机。DHCP的工作过程如图所示。

如图所示，一台非法DHCP服务器接入到了网络中，并“冒充”为一这个网段中的合法DHCP服务器。



非法DHCP服务器的工作原理

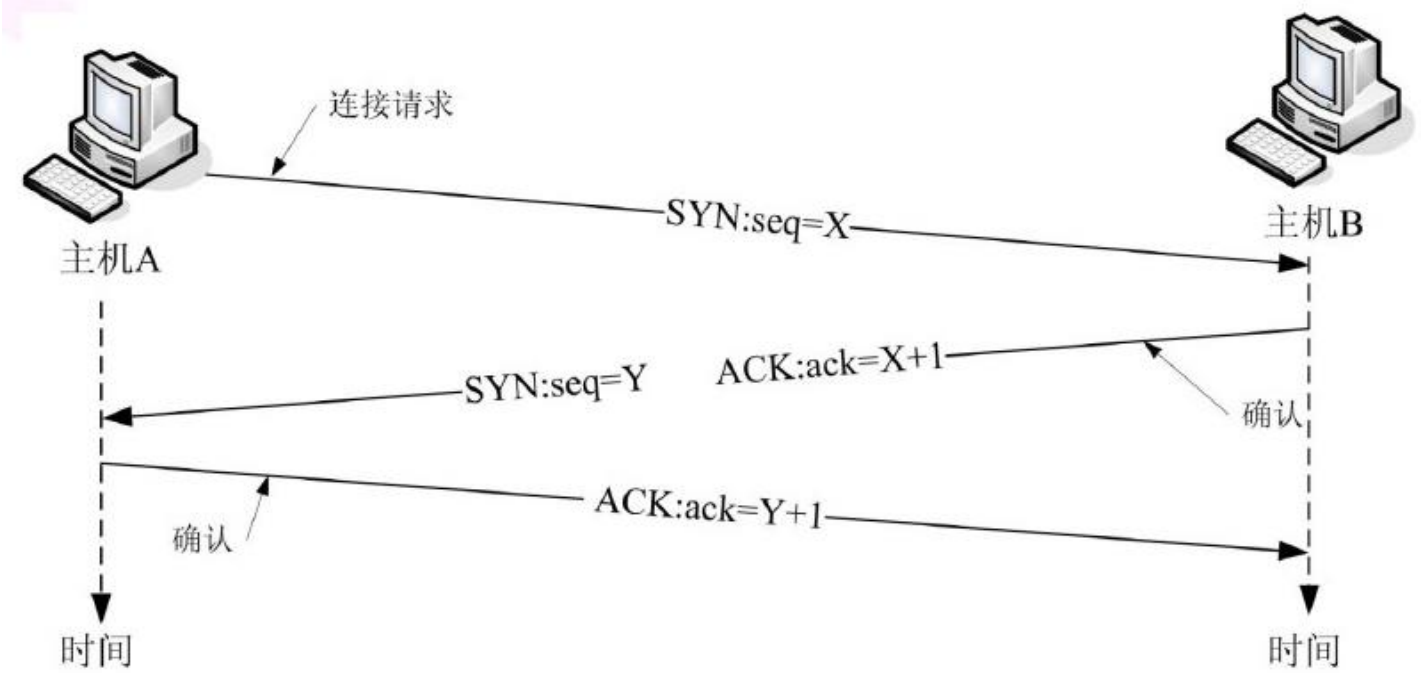
TCP安全

TCP协议涉及到TCP报文段的结构、TCP连接的建立与终止、TCP数据的传输、流量控制、差错控制、数据重传等内容。

1.连接建立

TCP是面向连接的。在面向连接的环境中，开始传输数据之前，在两个终端之间必须先建立一个连接。建立连接的过程可以确保通信双方在发送用户数据之前已经准备好了传送和接收数据。对于一个要建立的连接，通信双方必须用彼此的初始化序列号SEQ和来自对方成功传输确认的确认序列号ACK来同步。(ACK号指明希望收到的下一个字节的编号)习惯上将同步信号写成SYN，应答信号写为ACK.

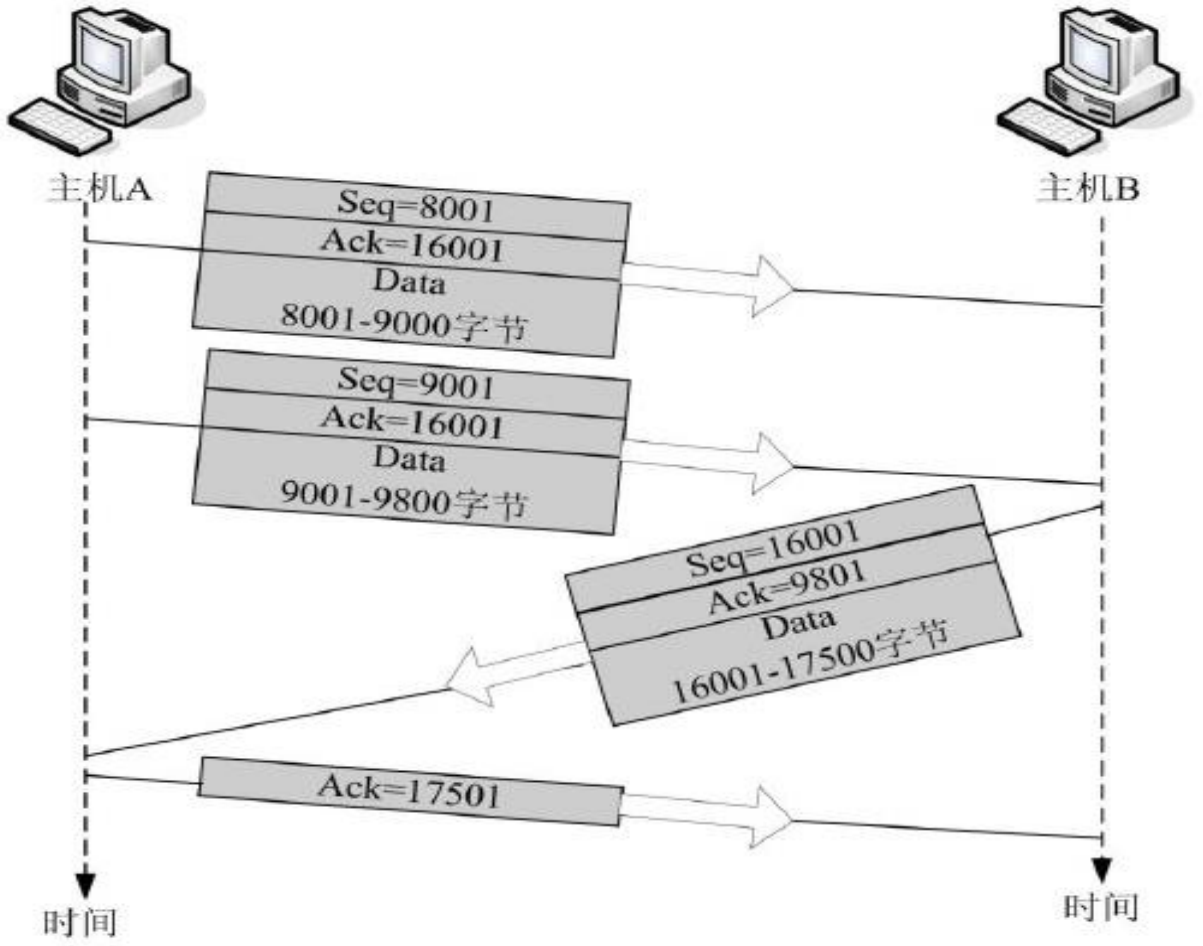
TCP连接建立



TCP连接建立时的三次握手

数据传输

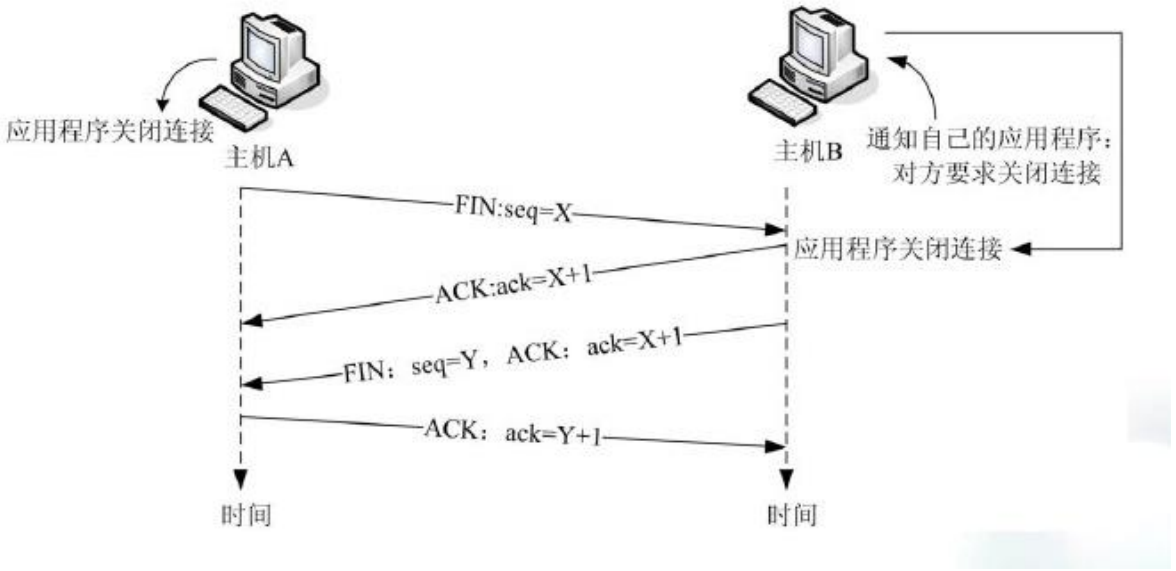
在连接建立后，TCP将以全双工方式传送数据，在同一时间主机A与主机B之间可以同时进行TCP报文段的传输，并对接收到的TCP报文段进行确认。如图所示，当通过三次握手建立了主机A与主机B之间的TCP连接后，现在假设主机A要向主机B发送1800字节的数据，主机B要向主机A发送1500字节的数据。



TCP报文段的传输过程

连接终止

对于一个已经建立的连接，TCP使用改进的三次握手来释放连接（使用一个带有FIN附加标记的报文段，即在TCP报文段首部中将FIN字段的值置为1）。TCP关闭连接的步骤如图所示。



TCP使用改进的三次握手来释放连接

TCP的安全问题

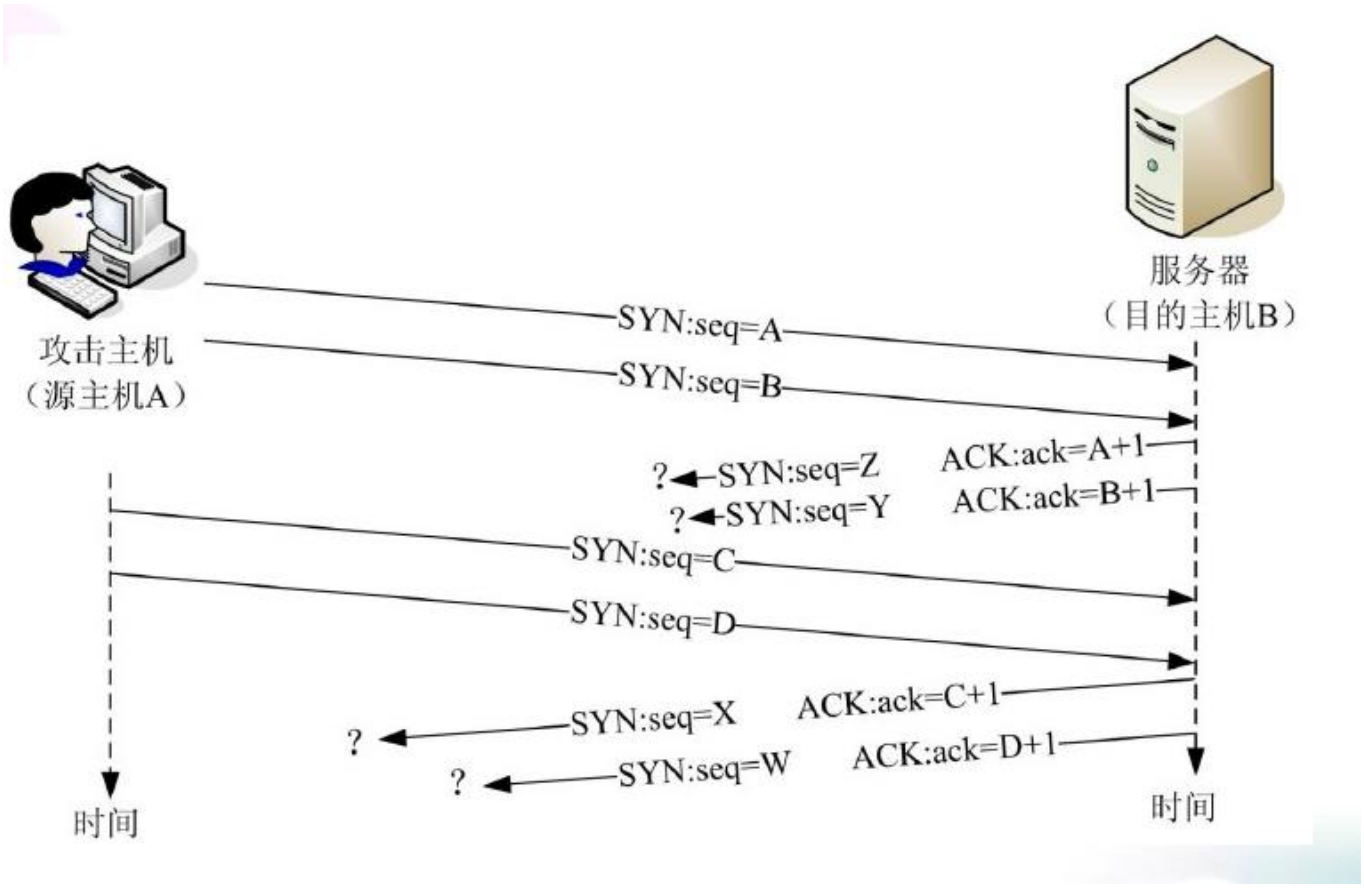
在TCP/IP网络中，如果两台主机之间要实现可靠的数据传输，首先要通过三次握手方式建立主机之间的TCP连接，但在TCP连接过程中很容易出现一个严重的安全问题：TCP SYN泛洪攻击。

按照TCP连接建立时三次握手的协议约定，当源主机A要建立与目的主机B之间的TCP连接时，源主机A首先发送一个用于同步的SYN报文段（第一次握手）。当目的主机B接收到这个报文段时，在正常情况下目的主机会打开连接端口，并给源主机A返回一个SYN+ACK的报文段（第二次握手）。

TCP的安全问题

TCP SYN泛洪攻击的工作过程如图所示。如果在第一次握手过程中，源主机A发送给目的主机B的SYN报文段中的IP地址是伪造的，源主机A同时向目的主机B发送大量的SYN报文段。这时，对于目的主机B来说会正常接收这些SYN报文段，并发送SYN+ACK确认报文段。由于目的主机B接收到的SYN报文段中的IP地址都是伪造的，所以发送出去的SYN+ACK确认报文段全部得不到回复。在目的主机B的队列中存在大量的“半开放状态”的连接，最终将队列的存储空间填满，并因资源耗尽而瘫痪。

TCP的安全问题



TCP SYN泛洪攻击的工作过程

DNS安全

为了解决主机IP地址与主机之间的对应关系，InterNIC(Internet Network Information Center, Internet网络信息中心)制定了一套称为域名系统（Domain Name System, DNS）的分层名字解析方案，当DNS用户提出IP地址查询请求时，就可以由DNS服务器中的数据库提供所需的数据。DNS技术目前已广泛的应用于Internet和Intranet中。

DNS概述

DNS的功能及组成

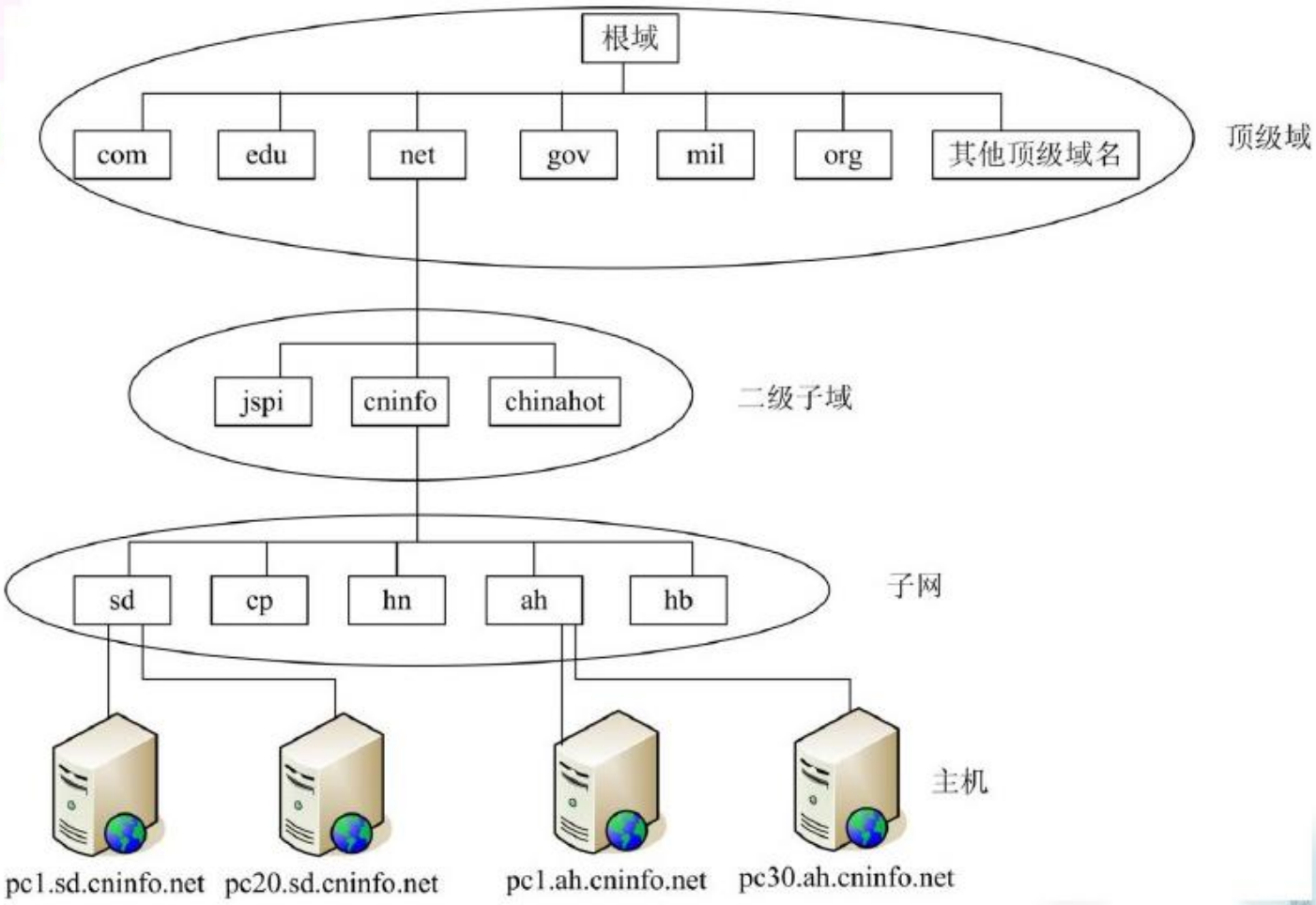
简单的讲，DNS协议的最基本的功能是对主机名与对应的IP地址之间建立映射关系。例如，新浪网站的一个IP地址是202.106.184.200，几乎所有浏览该网站的用户都是使用www.sina.com.cn，而并非使用IP地址来访问。使用主机名（域名）比直接使用IP地址具有以下两点好处：

主机名便于记忆，如sina.com.cn

数字形式的IP地址可能会由于各种原因而改变，而主机名可以保持不变。

DNS概述

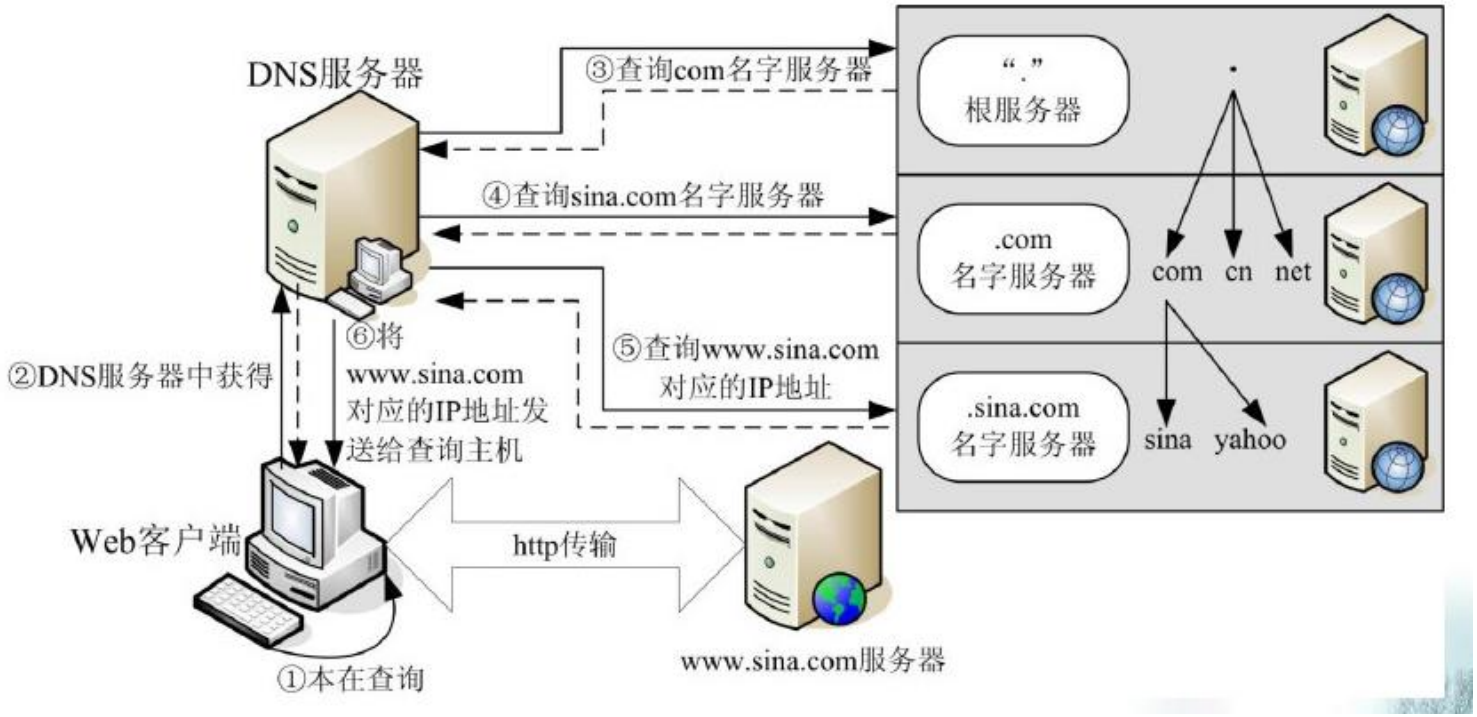
下图显示了顶级域的名字空间及下一级子域之间的树型结构关系，图中的每一个节点以及其下的所有节点叫做一个域。域可以有主机（计算机）和其他域（子域）。例如，pc1.sd.cninfo.net就是一个主机，而sd.cninfo.net则是一个子域。一般在子域中含有多个主机，例如，ah.cninfo.net子域下就含有pc1.ah.cninfo.net和pc30.ah.cninfo.net两台主机。



Internet的域名结构

DNS的解析过程

现在假设客户端Web浏览器要访问网站www.sina.com，整个访问过程如图所示。



DNS的安全问题——缓存中毒

DNS缓存中毒利用了DNS缓存机制，在DNS服务器的缓存中存入大量错误的数据记录主动供用户查询。由于缓存中大量错误的记录是攻击者伪造的，而伪造者可能会根据不同的意图伪造不同的记录，例如将查询指向某一个特定的服务器，使所有通过该DNS查询的用户都访问某一个网站的主页；或将所有的邮件指向某一台邮件服务器，拦截利用该DNS进行解析的邮件，等等。

由于DNS服务器之间会进行记录的同步复制，所以在TTL内，缓存中毒的DNS服务器有可能将错误的记录发送给其他的DNS服务器，导致更多的DNS服务器中毒。正如DNS的发明者Paul Mockapetris所说：中毒的缓存就像是“使人们走错方向的假冒路牌”。

DNS的安全问题

2. 拒绝服务攻击

DNS服务器在互联网中的关键作用使它很容易成为攻击者进行攻击的目标，加上DNS服务器对大量的攻击没有相应的防御能力，所以攻击过程很容易实现，且造成的后果非常严重。现在使用的DNS采用了树型结构，一旦DNS服务器不能提供服务，其所辖的子域都将无法解析客户端的域名查询请求。

3. 域名劫持

域名劫持通常是指通过采用非法手段获得某一个域名管理员的账号和密码，或者域名管理邮箱，然后将该域名的IP地址指向其他的主机（该主机的IP地址有可能不存在）。域名被劫持后，不仅有关该域名的记录会被改变，甚至该域名的所有权可能会落到其他人的手里。

DNS安全扩展（DNSSEC）

1. DNSSEC的基本原理

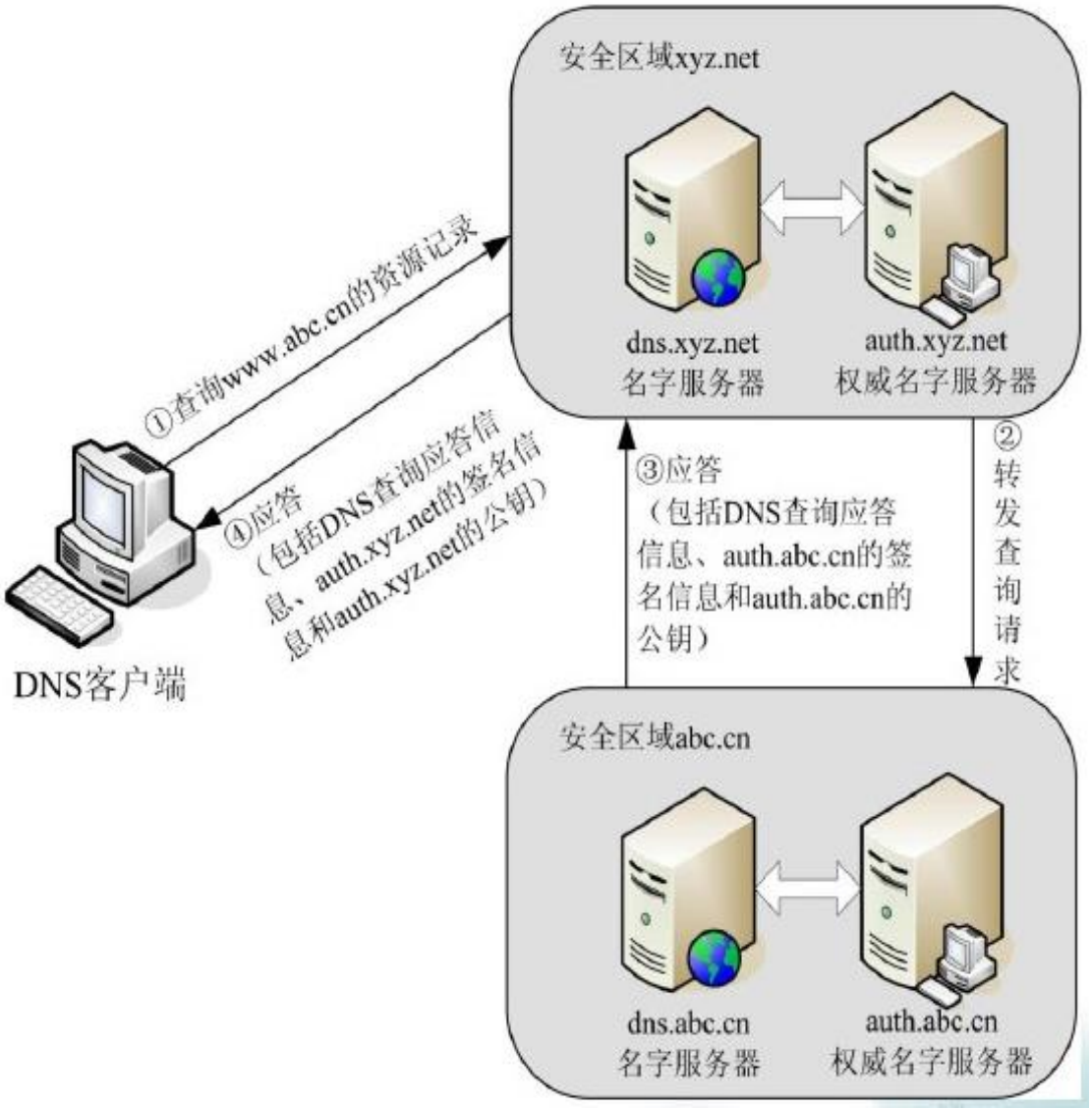
域名系统安全扩展（DNSSEC）是在原有的域名系统（DNS）上通过公钥技术，对DNS中的信息进行数字签名，从而提供DNS的安全认证和信息完整性检验。具体原理为：发送方：首先使用hash函数对要发送的DNS信息进行计算，得到固定长度的“信息摘要”；然后对“信息摘要”用私钥加密，此过程实现了对“信息摘要”的数字签名；最后将要发送的DNS信息、该DNS信息的“信息摘要”以及该“信息摘要”的数字签名，一起发送出来。

DNS安全扩展（DNSSEC）

接收方：

首先采用公钥系统中的对应公钥对接收到的“信息摘要”的数字签名进行解密，得到解密后的“信息摘要”；接着用与发送方相同的hash函数对接收到的DNS信息进行运算，得到运算后的“信息摘要”；最后，对解密后的“信息摘要”和运算后的“信息摘要”进行比较，如果两者的值相同，就可以确认接收到的DNS信息是完整的，即是由正确的DNS服务器得到的响应。

DNS安全扩展（DNSSEC）



DNSSEC相同的查询和应答过程

DNSSEC的工作机制

其中，相同中的所有客户端和服务器都支持DNSSEC，区域abc.cn的权威名字服务器为auth.abc.cn，区域xyz.net的权威名字服务器为auth.xyz.net

DNSSEC的应用现状

DNSSEC作为对目前DNS的安全扩展，可有效的防范DNS存在的各种攻击，保证客户端收到的DNS记录的真实性和完整性。此外，DNSSEC与原有的DNS具有向下的兼容性，在实现上具有可行性。但是，由于Internet的特殊性，从DNS到DNSSEC的转换不可能在短期内完成，需要一个渐进的过程。可以先有针对性的建立一些安全区域，如.cn、.net等，然后再向其他区域扩展。当整个internet部署了DNSSEC后，所有的信任将集中到根域下。

DNSSEC的应用现状

目前在推广DNSSEC上存在许多问题或困难：
一是由于整个Internet上的DNS记录非常庞大，如果要部署适用于整个Internet的DNSSEC，需要投入大量时间和设备，同时还要得到所有区域服务器提供商的支持；

二是DNSSEC只是提供了对DNS记录真实性的验证，只是有限的程度上为用户通信的安全提供了保证；

三是DNSSEC在DNS请求和应答 中添加了数字签名，一方面增加了通信的流量和复杂性，另一方面安全性主要依赖于公钥技术的安全性，所以对于DNSSEC系统来说是否会存在新的安全问题也是一个未知数。

作业

- 从ARP欺骗攻击，DHCP攻击，泛洪攻击，DNS攻击中选择两种攻击方式，基于图，示意攻击过程和原理。