第2章 计算机及网络基础

东南大学 网络空间安全学科
胡爱群 教授/博导
二o一九年九月十日

主要内容

- 计算机基础知识
  1. 计算机发展简史
  2. 计算机硬件
  3. 计算机软件
  4. 计算机安全性分析
- 网络基础知识
  1. 网络发展简史
  2. 网络体系结构
  3. 网络安全性分析

一、计算机基础

✓ 计算机是网络安全防护的对象，也是实施网络安全所依赖的基础平台。了解计算机的硬件和软件体系结构，对理解网络安全具有重要的作用。

1. 计算机发展简史

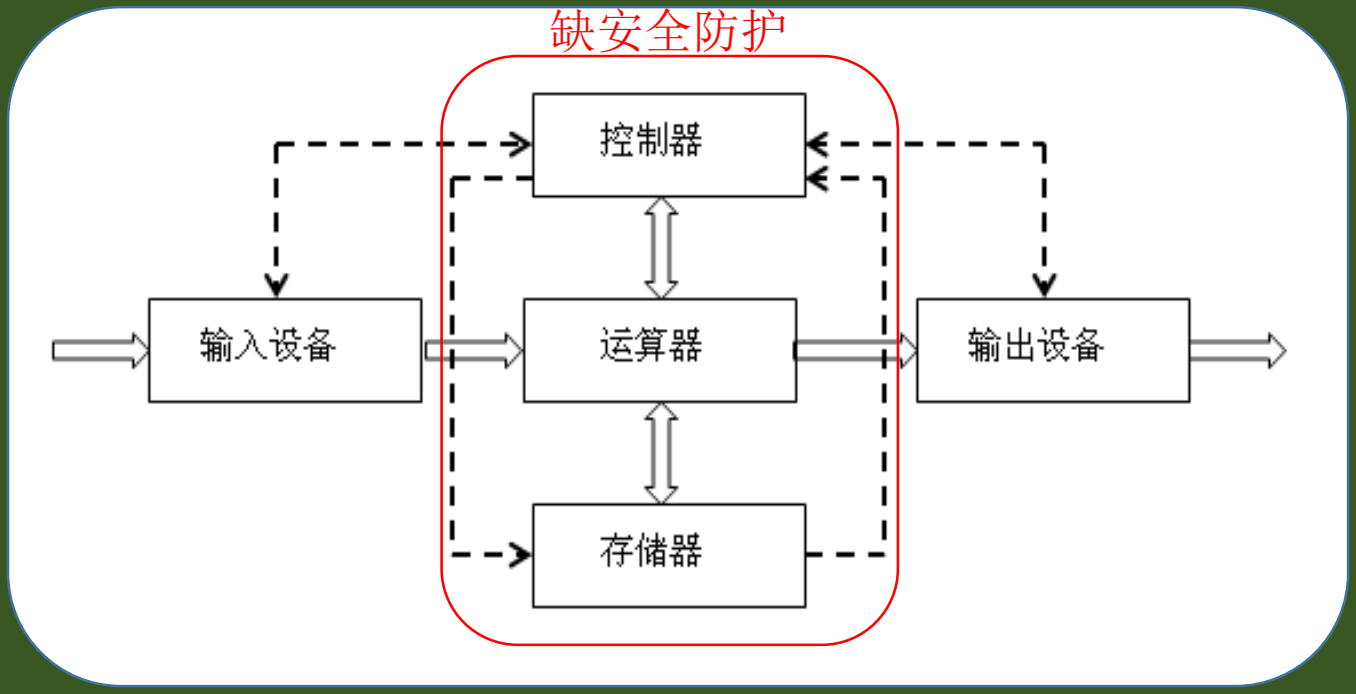
- 1946年2月,世界上第一台电子计算机ENIAC (Electronic Numerical Integrator and Computer)问世.

早期将计算机分为：巨型机、大型机、中型机、小型机、微型机等。





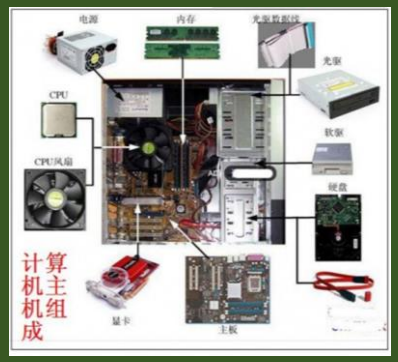
计算机结构原理



冯．诺依曼型计算机

- 冯．诺依曼型计算机由5部分组成：运算器、控制器、存储器、输入设备和输出设备。

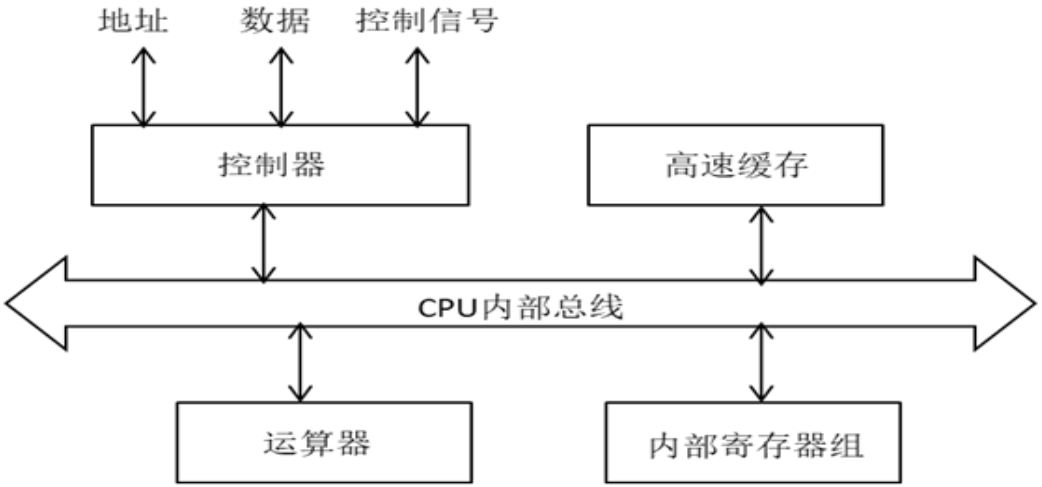
计算机组成



- 计算机系统
  - 硬件
    - 主机
      - 处理器(CPU)
      - 内存储器
      - 总线
      - 输入输出接口
    - 外部设备
      - 外存储器（U盘、硬盘、光盘等）
      - 输入设备（键盘、鼠标、扫描仪等）
      - 输出设备（显示器、打印机、音箱等）
      - 其他（网卡、声卡、显卡等）
  - 软件
    - 系统软件
      - 操作系统
      - 系统应用软件（数据库管理系统、编译器等）
    - 应用软件

CPU

- CPU一般包括四部分：运算器、控制逻辑单元（或控制器）、内部寄存器组、高速缓存(cache)，它们通过CPU内部总线连接在一起，并集成到一片硅片上。
- 除了CPU外，很多计算机中还配有称为“协处理器”的配套芯片，以完成特定功能，如浮点运算。现代CPU芯片很多已集成了一个或多个协处理器。
- 今天的CPU或微处理器芯片多采取双核、四核、六核或更多处理核心(core)的多核体系结构，以实现指令级并行或事务级并行处理，从而获得更高性能。

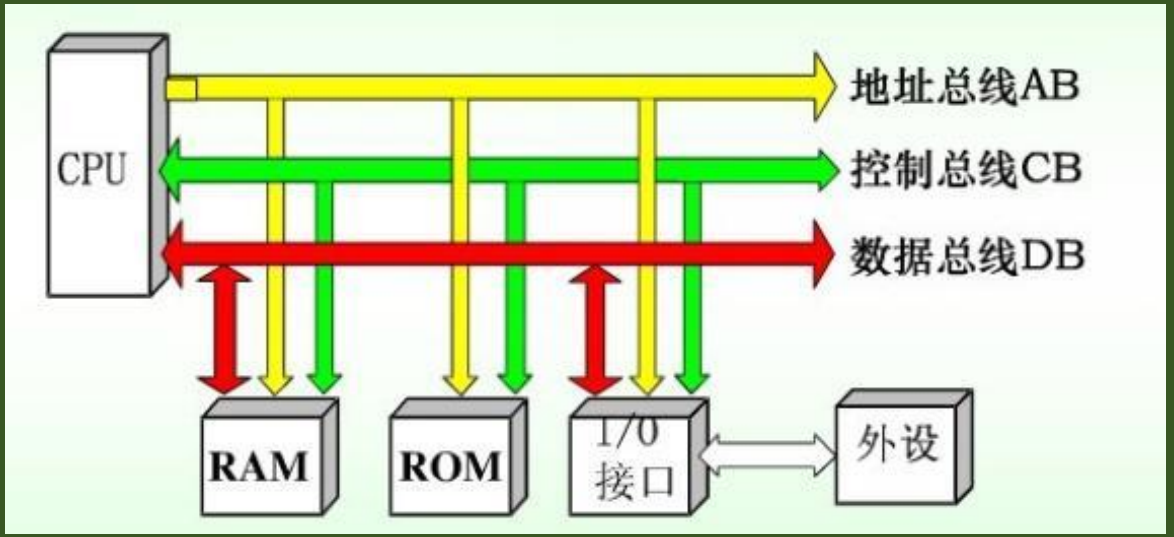


GPU

(Graphics Processing Unit)

- 传统的CPU只由几个核构成，然而一个现代GPU通常采用成百上千的简单核心的众核体结构，拥有一个慢速执行多并发线程的大规模并行吞吐体系结构。
- 早期的GPU仅限于加速图形和视频编码，但现代GPU的作用不仅如此，还可用于处理大批量并行浮点计算。
- 某种程度上讲，GPU让CPU摆脱了所有数据密集型计算，而不只是那些视频处理相关的计算。因此，GPU在大规模并行计算得到了广泛应用。

总线

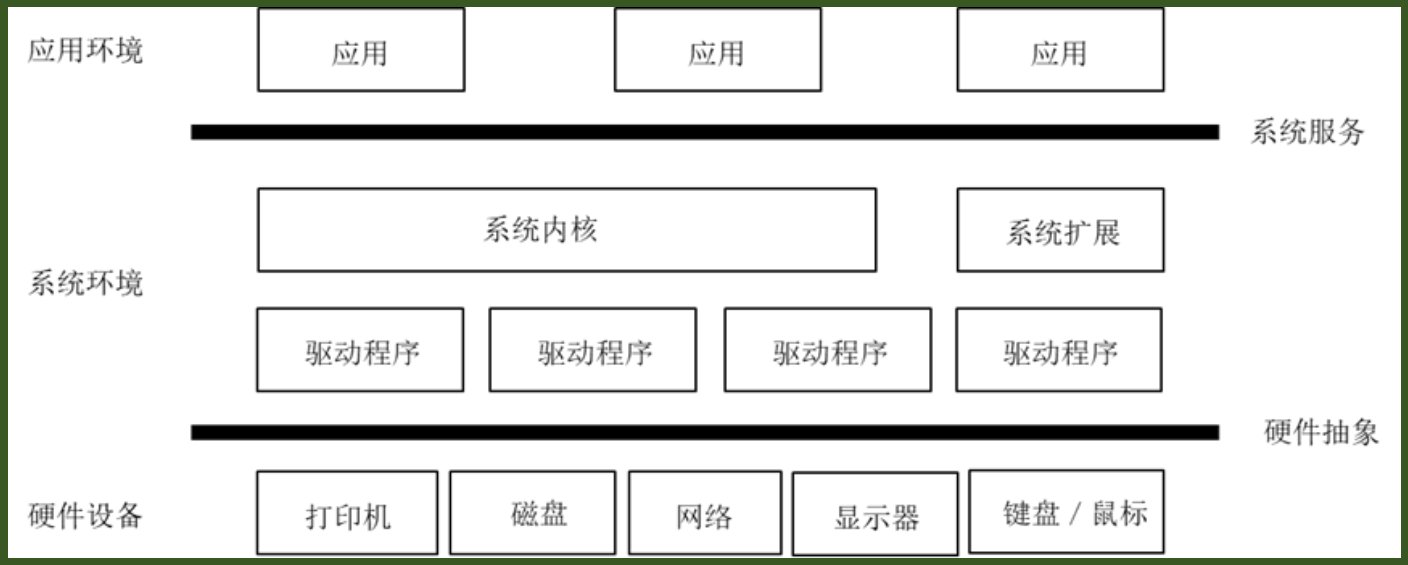


- 总线主要分为微处理器级总线，包括地址总线(AB, Address Bus)、数据总线(DB, Data Bus)和控制总线(CB, Control Bus)，用来实现CPU与外围控制芯片（如主存、Cache）之间的信息交互。
- 不同CPU的地址总线的位数不同，通常的位数有：8位、16位、32位、64位；
- 系统级总线，也称为“I/O通道总线”，同样包括AB、DB、CB三种，用于CPU与接口卡的连接，为方便各种接口卡能够在各种系统中实现“即插即用”，系统总线的设计要求与具体的CPU无关，相关标准有：ISA总线、PCI总线、AGP总线等；
- 外设总线，是指计算机主机与外部设备接口的总线，常见的接口标准有：IDE 、EIDA 、 、USB等。

计算机软件

- 包括系统软件和应用软件。

  - 系统软件中的操作系统是整个计算机系统的核心。操作系统位于硬件和用户之间，是专门管理计算机硬件资源的软件。
  - 应用软件是针对特定应用需求，利用各种编程语言（如C/C++，Java, Python, C#等）编写的、在操作系统上运行的各种软件。



操作系统架构

操作系统

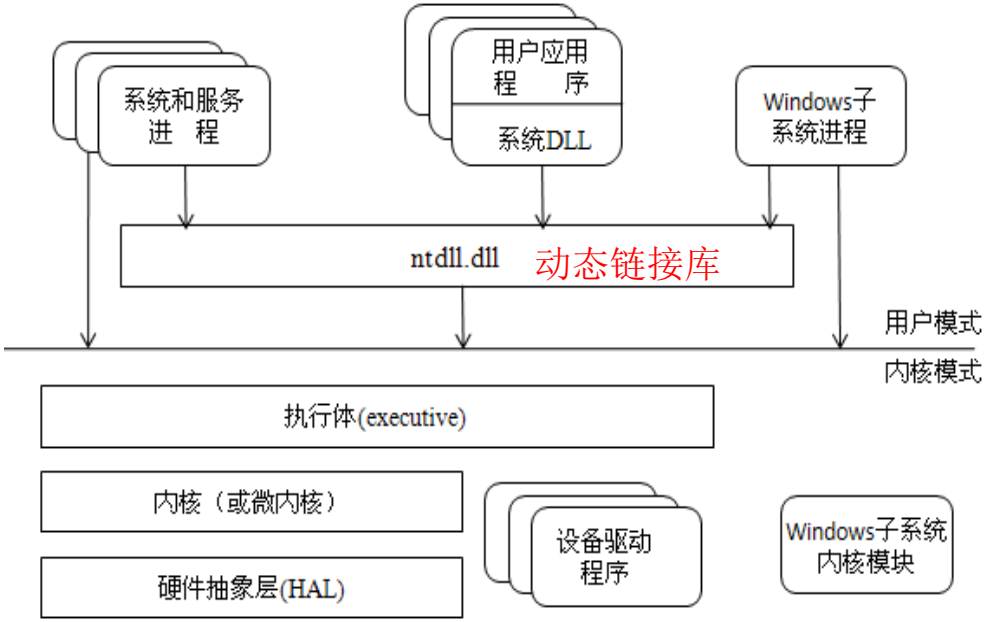
- 主要有两类：UNIX操作系统和Windows操作系统。

操作系统的任务：

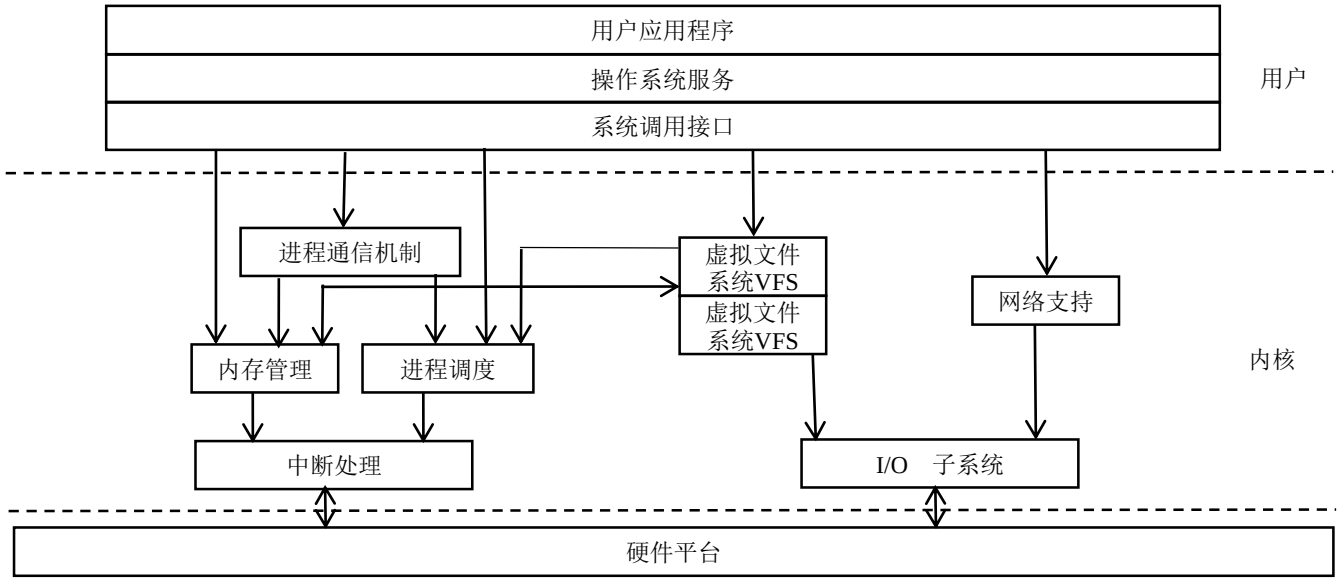
- 处理器管理：管理多个程序同时在一个处理器上运行，以进程(process)为基本单位。以进程为最小单位分配资源，以线程为基本单位执行程序。
- 存储器管理：内存分配、内存保护、地址映射和内存扩充等。
- 设备管理：缓存管理、设备分配、设备驱动程序和虚拟设备管理等。
- 文件管理：文件存储内容的管理、目录管理、文件的读 / 写管理以及文件的保护等。
- 用户接口：命令接口、程序接口（或系统调用接口）和图形接口。

Windows操作系统

- Windows采用用户模式和内核模式的双模式(dual mode)来保护操作系统免受应用程序错误的影响。
- 操作系统的核心在内核模式(kernel mode)中运行；应用程序的代码则运行在用户模式(user mode)下。
- 应用程序通过指令在用户模式和内核模式间切换。
- 内核模式和用户模式的运行环境是相互隔离的，它们可以访问的内存空间也并不相同。

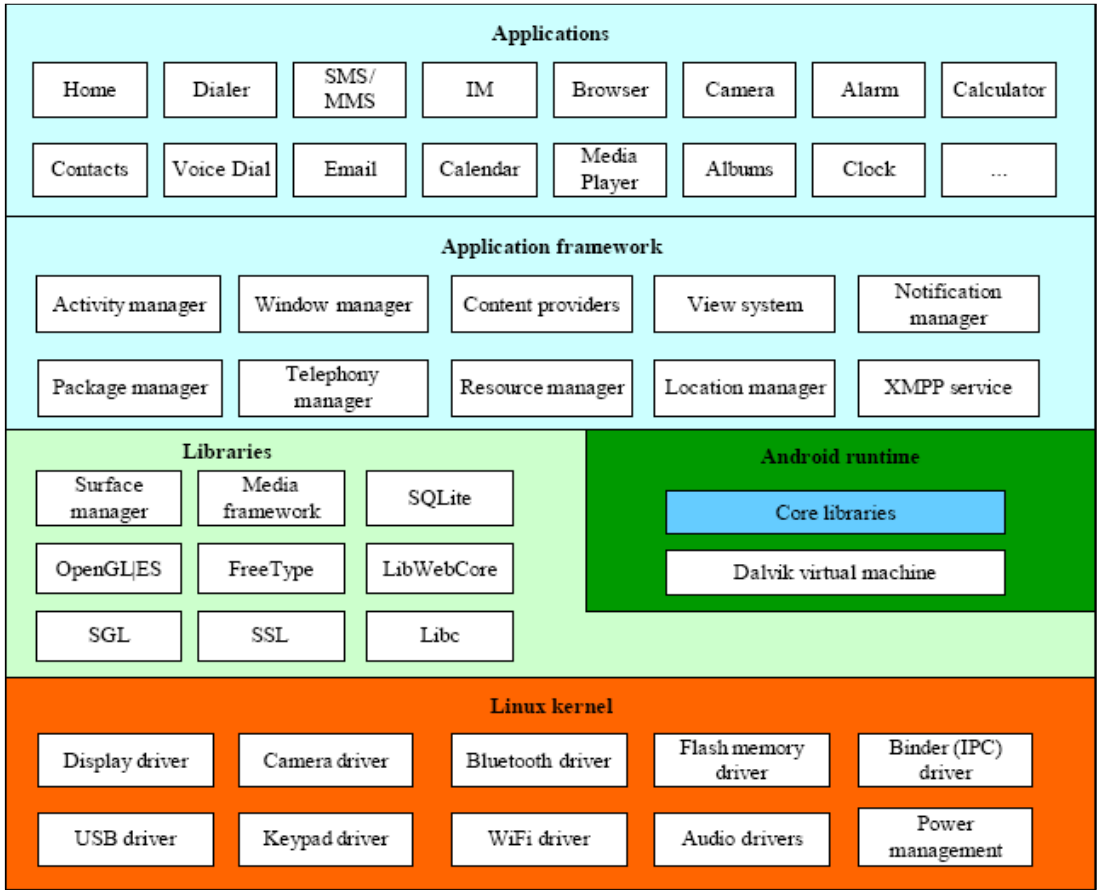


Linux操作系统



- ✓ Linux内核采用单内核(monolithic kernel)模式；
- ✓ Linux使用简单的基于优先级的进程调度算法来完成进程的调度；
- ✓ Linux支持虚拟内存，并负责进程虚拟内存到物理内存间的映射；
- ✓ Linux支持多种进程间通信机制，这些机制支持多进程资源的互斥访问、进程间同步和消息传递等；
- ✓ 操作系统服务由shell和实用程序组成，属于特定的用户程序。shell介于系统调用接口和应用程序之间，是用户和Linux内核之间的接口。

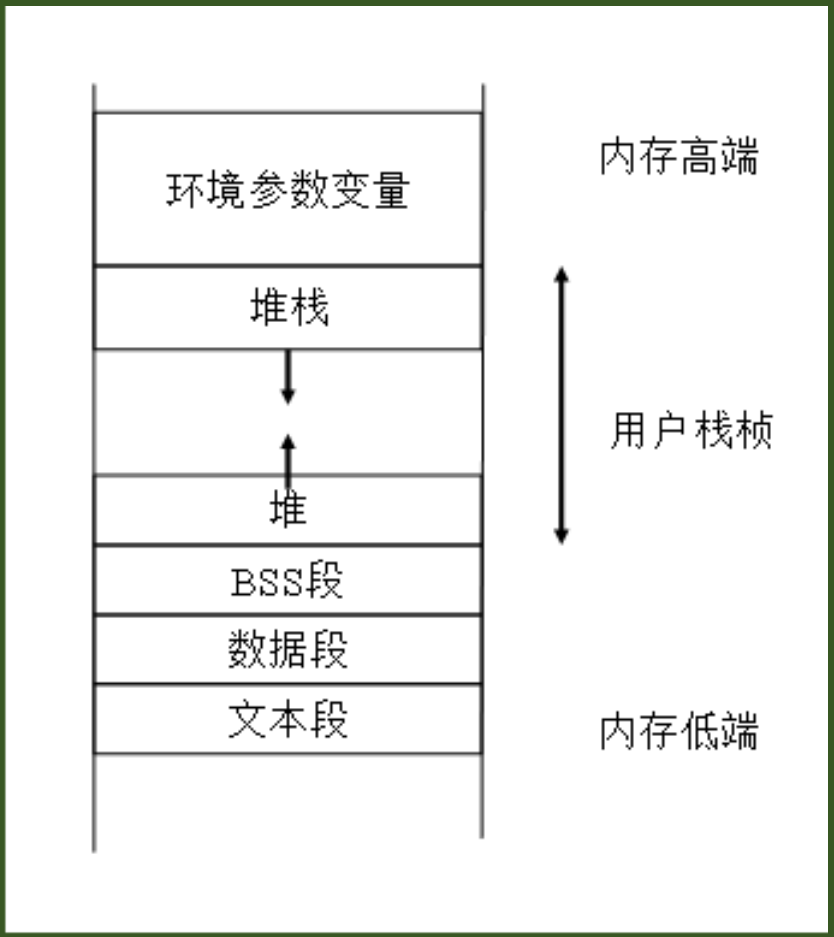
Android操作系统



- 系统的最底层是Linux内核层(Linux kernel)，Google对原有的Linux内核进行了改进，以适应移动智能终端设备的硬件环境。
- Linux内核提供最基本的功能，包括内存管理、进程调度、设备驱动器和文件系统。
- Android的很多安全机制都是基于Linux内核的。
- Android自身也有一套安全机制，包括：沙箱或沙盒(sandbox)、权限(rights)和签名(signature)。

软件在计算机内存中的布局

- 计算机软件中的很多安全问题与软件在内存中的布局有关。
- 在大多数操作系统中，系统在创建一个软件进程时，会一次性给该进程分配一块内存（通常称为“静态分配”），这块内存在进程运行期间保持不变。
- 除了上述一次性分配的内存外，进程还可以动态申请内存，这就是堆(Heap)分配。
- 栈的增长方向是从内存高端向内存低端增长，而大多数的内存拷贝是从内存低端到内存高端。这为栈溢出攻击提供了条件。



计算机安全性分析

- 计算机系统自身的脆弱和不足（或称为“安全漏洞”）是造成信息系统安全问题的内部根源，攻击者正是利用系统的脆弱性使各种威胁变成现实危害。

（1）计算机系统硬件系统的故障。

（2）各类计算机软件故障或安全缺陷。

（3）网络和通信协议自身的缺陷导致的安全问题。

（4）配置和管理不当等人为因素导致计算机存在安全风险。

软件漏洞

在设计、开发过程中有很多因素会导致系统、软件漏洞的出现，主要包括：

（1）系统基础设计错误导致漏洞。例如，因特网在设计时未考虑认证机制，使得假冒IP地址很容易。

（2）编码错误导致漏洞。例如，缓冲区溢出、格式化字符串漏洞、脚本漏洞等都是由于在编程实现时没有实施严格的安全检查而产生的漏洞。

（3）安全策略实施错误导致漏洞。例如，在设计访问控制策略时，若不对每一处访问都进行访问控制检查，则会导致漏洞。

（4）实施安全策略对象歧义导致漏洞，即实施安全策略时，处理的对象和最终操作处理的对象不一致，如IE浏览器的解码漏洞。

（5）系统开发人员刻意留下的后门。一些后门是开发人员为调试而留，而另一些则是开发人员为后期非法控制而设置的。这些后门一旦被攻击者获悉，将严重威胁系统的安全。

（6） 除了上述设计实现过程中产生的系统安全漏洞外，不正确的安全配置也会导致安全事故，例如弱口令、开放Guest用户、安全策略配置不当等。

软件漏洞难以克服的原因

（1）方案的设计可能存在缺陷。

（2）从理论上证明一个程序的正确性是非常困难的。

（3）一些产品测试不足，匆匆投入市场。

（4）为了缩短研制时间，厂商常常将安全性置于次要地位。

（5）系统中运行的应用程序越来越多，相应的漏洞也就不可避免地增多。

（6）现代软件外包生产方式带来的安全问题。

（7）软件的高复杂度。

二、网络基础知识

- 网络发展简史

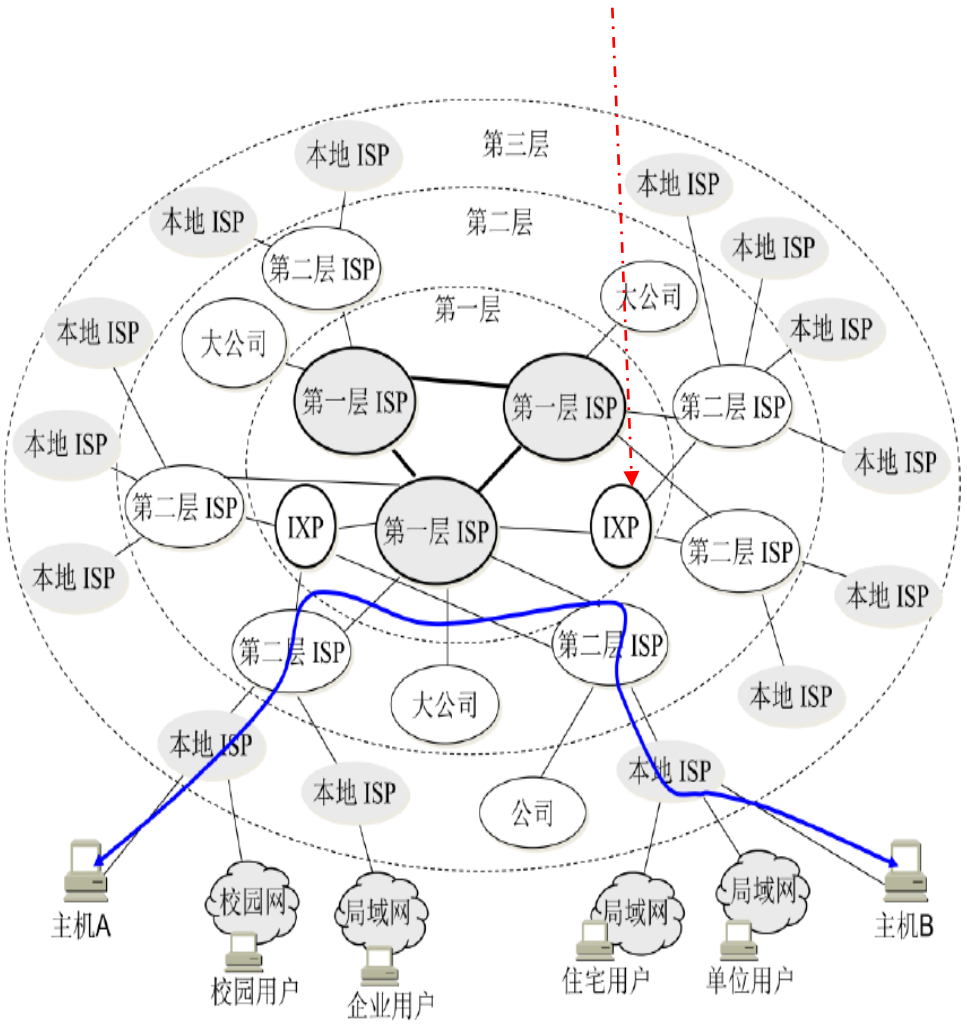
电信网络→电视网络→计算机网络

“三网合一” 话音、视频、数据业务

- ✓ 计算机网络由若干节点(node)和连接这些节点的链路(link)组成。
- ✓ 节点主要包括两类：端系统和中间节点。
- ✓ 端系统(end system)，也称主机(host)，通常是指网络边缘的节点，可以是传统的计算机，也可以是非传统计算机设备，如智能手机、个人数字助手(PDA)、电视、汽车、家用电器、摄像机、传感设备等。
- ✓ 中间节点，主要包括集线器、交换机、路由器、自治系统、虚拟节点和代理等网络设备或组织。链路则可以分为源主机到目的主机间的端到端路径(path)和两个节点之间的跳(hop)。

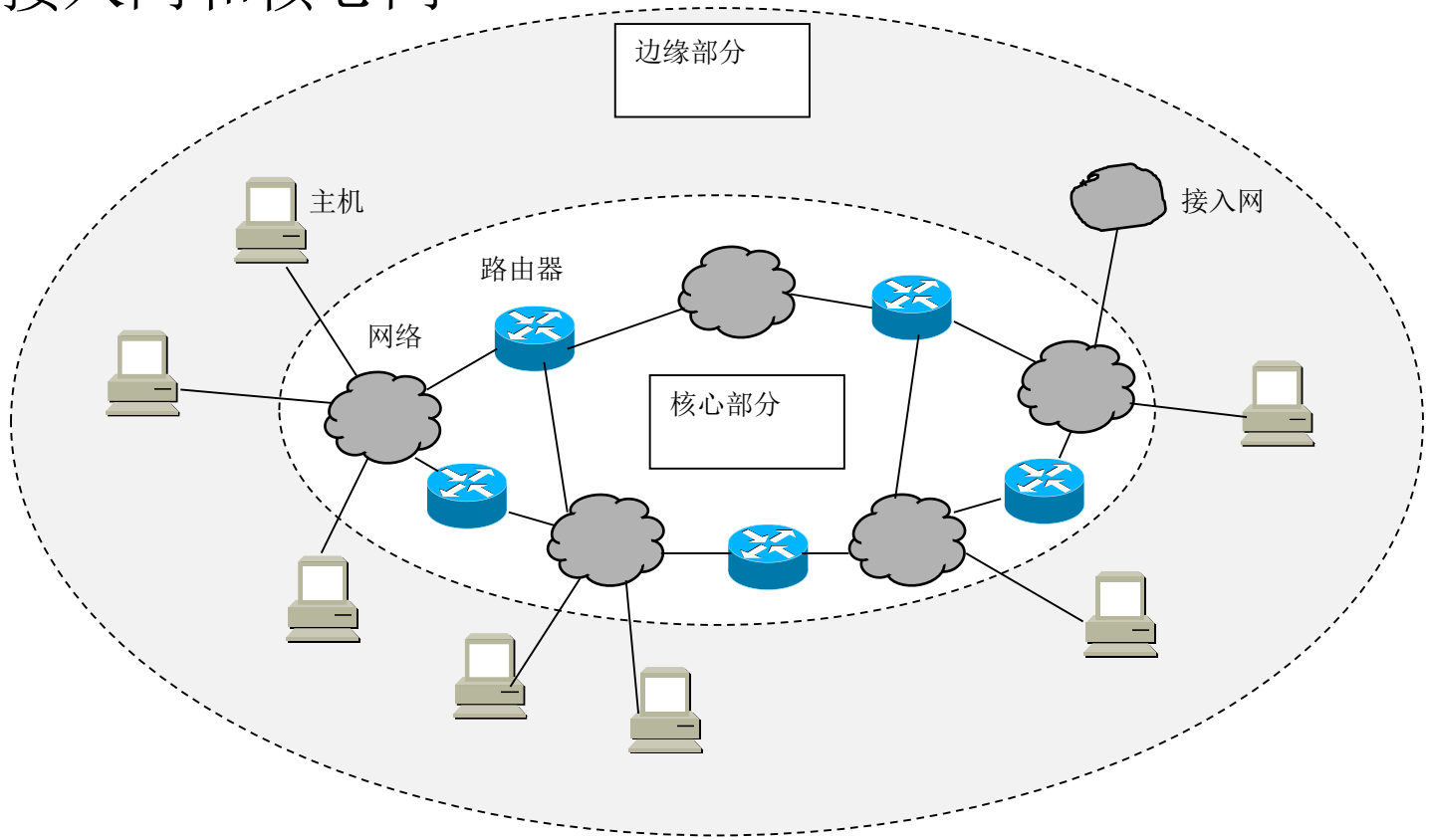
Internet

- 网络和网络通过互联设备（路由器，router）互连起来，构成一个覆盖范围更大的网络，即互联网(internet或internetwork)。
- 因特网(Internet)是全球最大的、开放的互联网，它采用TCP/IP协议族作为通信的规则，且其前身是美国的ARPANET。
- 因特网是一个多层次ISP(Internet Service Provider)结构的网络。



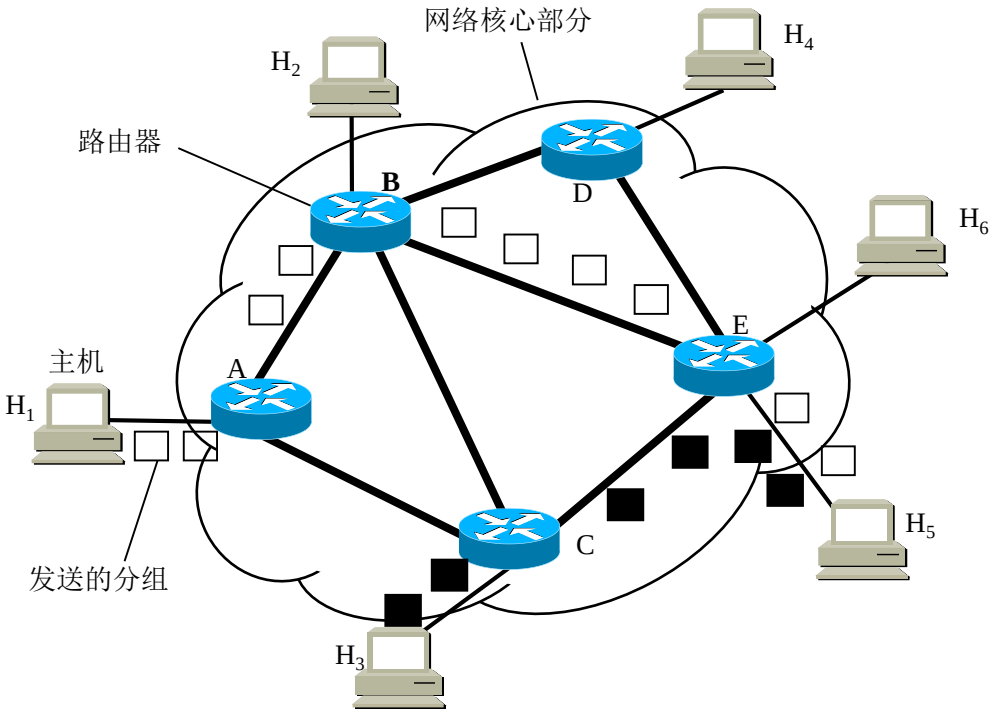
Internet的简化结构

--接入网和核心网



✓ 网络边缘的主机或端系统之间的通信方式通常分为两类：客户－服务器方式（C/S方式）和对等方式（P2P方式）。

分组交换



- 主机H1发送给主机H5的报文被划分成分组后，经过路由器A、B、E，到达目的主机H5；
- 主机H3发送给主机H5的报文被划分成分组后，经过路由器C、E，到达目的主机H5。
- 网络在转发分组的过程中，可能会根据当前网络中的流量分布情况，动态调整分组所通过的路径。
- 分组交换在传送数据之前不必占用一条端到端的通信资源。
- 与电路交换、报文交换相比，分组交换在数据通信过程中采用了动态分配传输带宽的策略，特别适合传输突发式的计算机网络数据，使得通信线路的利用率大大提高了，可靠性和灵活性也较好。

网络体系结构

- 计算机网络之所以能够做到有条不紊地交换数据，是因为网络中的各方都遵守一些事先约定好的规则。
- 这些规则明确规定了所交换的数据的格式以及有关的同步问题。
- 这些为进行网络中的数据交换而建立的规则、标准或约定即称为网络协议。
- 网络协议主要有三个要素：语法、语义和同步。
- 在网络协议中，可以将交换的报文（也称为协议数据单元或PDU)分为两种：用于传输用户数据的数据报文和用于协议控制的控制报文。

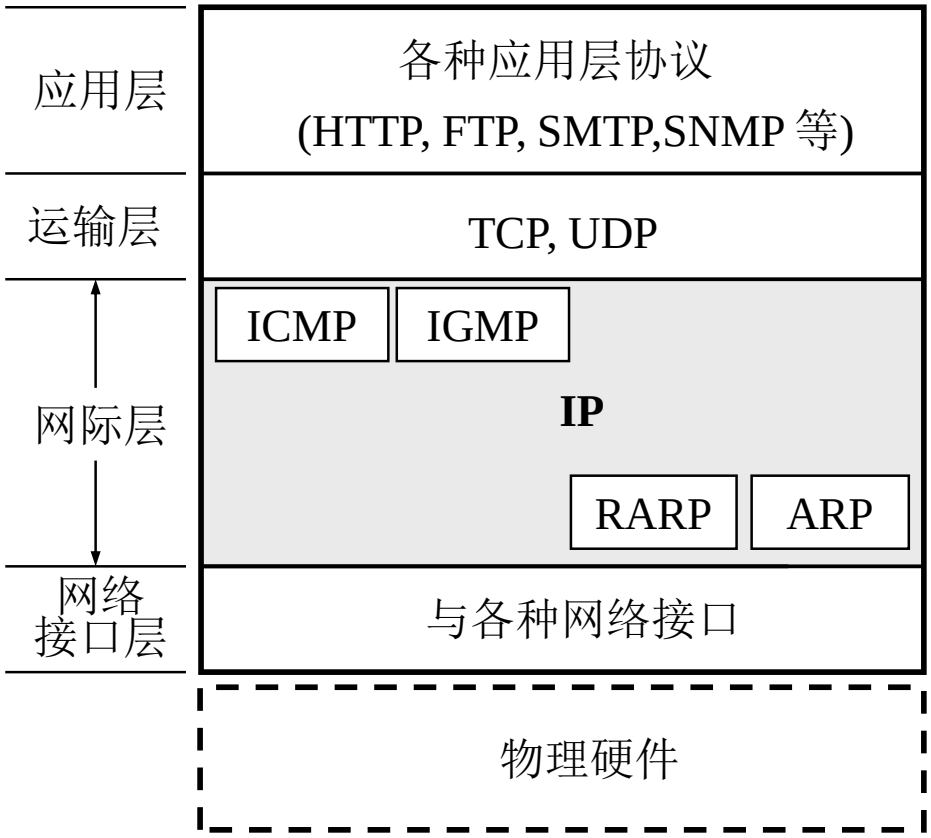
网络协议的语义

- 可以理解为协议数据报文中的控制信息和控制报文所约定的含义，即需要发出何种控制信息，完成何种动作以及做出何种响应。
- 例如：报文首部控制信息中的目的地址信息指明了报文的目的地，接收到此报文的网络节点均将其作为进行路由选择的依据，因而规定在首部控制信息中在给定域给出目标节点地址就是一种语义。
- 又例如，为了实现有连接的传输服务，设计了一套实现连接的控制报文。发起连接方构造一个请求连接的协议控制报文，这个“请求连接”就是该控制报文的语义。收端收到这个控制报文后，根据已知的格式分析规定域中报文的类型码就可了解这个“请求连接”的语义，从而给出“允许连接”或“拒绝连接”的响应。

网络协议的同步

- 同步是指通信过程中各种控制报文传送的顺序关系;
- 例如“允许连接”或“拒绝连接”报文必须是作为请求连接报文的一种响应来发送，“拆除连接”报文也必须在建立连接后的某种条件下发送等等。
- 这种控制报文发送的时序关系，也决定了通信双方所处的通信状态(发送状态、接收状态、等待状态等)的制约关系。
- 在有些文献中，也将这种同步关系视为协议语法的一部分。

TCP/IP体系结构



与IP配合使用的还有四个协议:

- ✓ ICMP (Internet Control Message Protocol), ICMPv4和ICMPv6.
- ✓ IGMP (Internet Group Management Protocol)
- ✓ ARP (Address Resolution Protocol)
- ✓ RARP (Reverse Address Resolution Protocol)。

ARP: 局域网中根据IP获取MAC；
RARP：根据MAC获取IP（新机安装时）。

网络安全性分析

因特网的以下几个特性易被攻击者利用：

(1) 分组交换

(2) 认证与可追踪性

(3) 尽力而为(best-effort)的服务策略

(4) 匿名与隐私

(5) 对全球网络基础实施的依赖

(6) 无尺度网络

(7) 互联网的级联特性

分组交换

- 所有用户共享所有资源，给予一个用户的服务会受到其它用户的影响；
- 攻击数据包在被判断为是否恶意之前都会被转发到受害者；
- 路由分散决策，流量无序等。

认证与可追踪性

- 因特网没有认证机制，任何一个终端接入即可访问全网，这导致一个严重的问题就是IP欺骗：攻击者可以伪造数据包中的任何区域的内容，然后发送数据包到Internet中。
- 通常情况下，路由器不具备数据追踪功能，因此很难去验证一个数据包是否来自于其所声称的地方。通过IP欺骗隐藏来源，攻击者就可以发起攻击而无须担心对由此造成的损失负责。

尽力而为的服务策略

- 因特网采取的是尽力而为策略，即只要是交给网络的数据，不管其是正常用户发送的正常数据，还是攻击者发送的攻击流量，网络都会尽可能地将其送到目的地。
- 把网络资源的分配和公平性完全寄托在终端的自律上。
- 在现在看来，这显然是不现实的。

匿名与隐私

- 网络上的身份是虚拟的，普通用户无法知道对方的真实身份，也无法拒绝来路不明的信息（如邮件）。
- 20年前，美国《纽约客》杂志以黑色幽默方式直指网络虚拟化之弊——“在互联网上，没有人知道你是一条狗”。

对全球网络基础实施的依赖

全球网络基础设施不提供可靠性、安全性保证，这使得攻击者可以放大其攻击效力：

- 首先，一些不恰当的协议设计导致一些（尤其是畸形的）数据包比其它数据包耗费更多的资源（如TCP 协议的连接请求SYN包比其它的TCP包占用的目标资源更多）；
- 其次，Internet是一个大“集体”，其中存在的很多不安全系统会严重威胁整个网络的安全。

无尺度网络

因特网是一种无尺度网络。

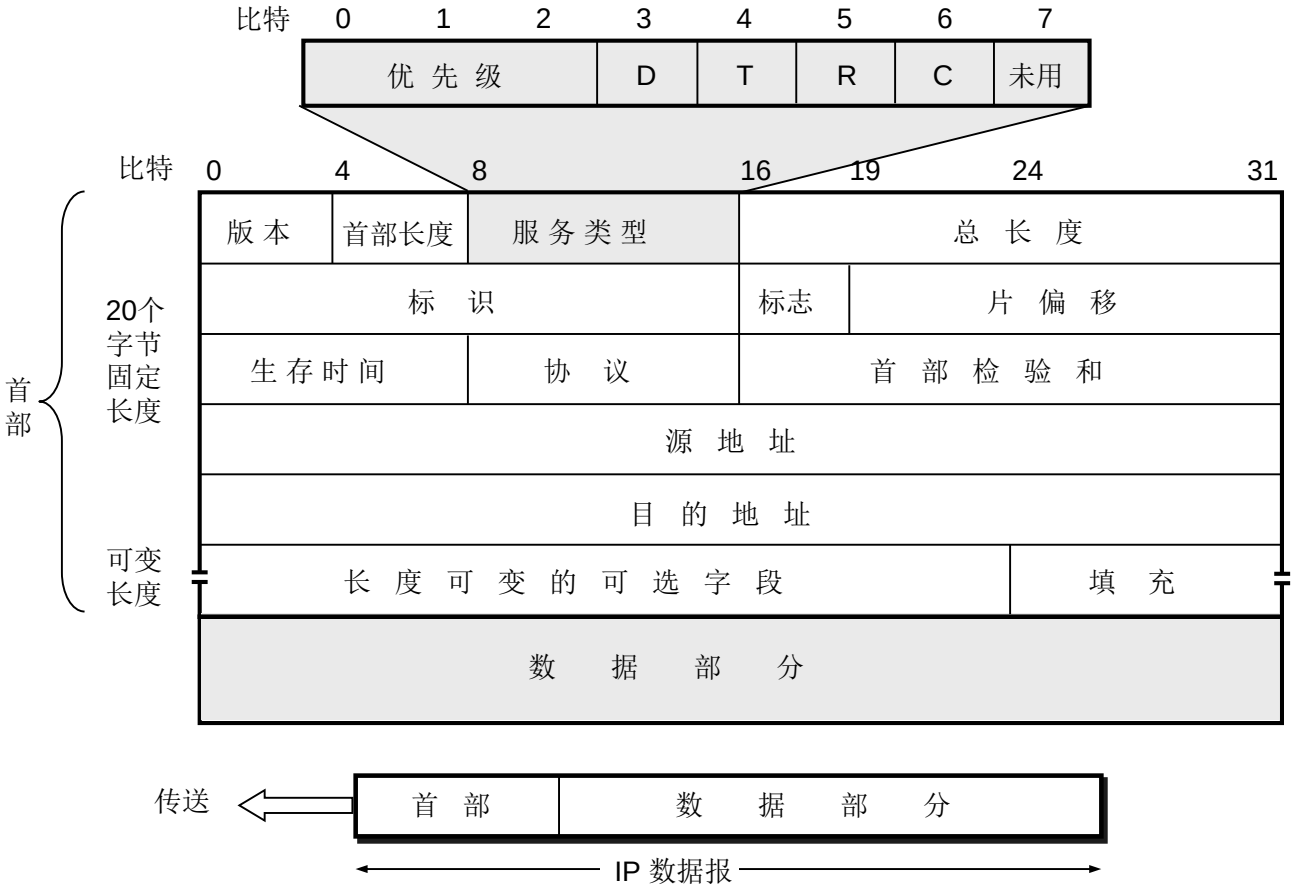
- 无尺度网络的典型特征是网络中的大部分节点只和很少节点连接，而有极少数节点与非常多的节点连接。
- 这种关键节点（称为“枢纽”或“集散节点”）的存在使得无尺度网络对意外故障有强大的承受能力（删除大部分网络节点而不会引发网络分裂），但面对针对枢纽节点的协同性攻击时则显得脆弱（删除少量枢纽节点就能让无尺度网络分裂成微小的孤立碎片）。

互联网的级联特性

互联网是一个由路由器将众多小的网络级联而成的大网络。

- 当网络中的一条通讯线路发生变化时，附近的路由器会通过“边界网关协议(BGP)”向其邻近的路由器发出通知。
- 这些路由器接着又向其他邻近路由器发出通知，最后将新路径的情况发布到整个互联网。也就是说，一个路由器消息可以逐级影响到网络中的其它路由器，形成“蝴蝶效应”。
- “网络数字大炮”就是针对互联网的这种级联结构发起的一种拒绝服务攻击武器，它利用伪造的BGP协议消息攻击路由器，导致网络中几乎所有路由器都被占用，正常的路由中断无法得到修复，最终瘫痪整个互联网。

IPv4协议


比特 0 1 2 3 4 5 6 7
优 先 级
D
T
R
C
未用
比特 0 4 8 16 19 24 31
首部
20个字节固定长度
可变长度
版 本
首部长度
服 务 类 型
总 长 度
标 识
标志
片 偏 移
生 存 时 间
协 议
首 部 检 验 和
源 地 址
目 的 地 址
长 度 可 变 的 可 选 字 段
填 充
数 据 部 分
传送
首 部
数 据 部 分
IP 数据报

IPv4协议内容

（1）版本。指IP协议的版本，值4表示IPv4，6表示IPv6。

（2）首部长度。可表示的最大数值是15个单位(一个单位为4字节)，因此IP的首部长度的最大值是60B。

（3）服务类型。用来获得更好的服务。

（4）总长度。指首部和数据之和的长度，单位为B。总长度字段为16 bit，因此数据报的最大长度为65535B（即64 KB）。

（5）标识(identification)。它是一个计数器，用来产生数据报的标识。

（6）标志(flag)。

（7）片偏移。指出较长的分组在分片后，某片在原分组中的相对位置。

（8）生存时间，记为TTL (Time To Live)。用来控制数据报所通过路由器的最大跳数。

（9）协议。指出此数据报携带的数据是使用何种协议，以便使目的主机的IP层知道应将此数据报上交给哪个进程。

（10）首部检验和。只检验数据报的首部，不包括数据部分。

（11）源地址。数据报的源IP地址，占32bit。

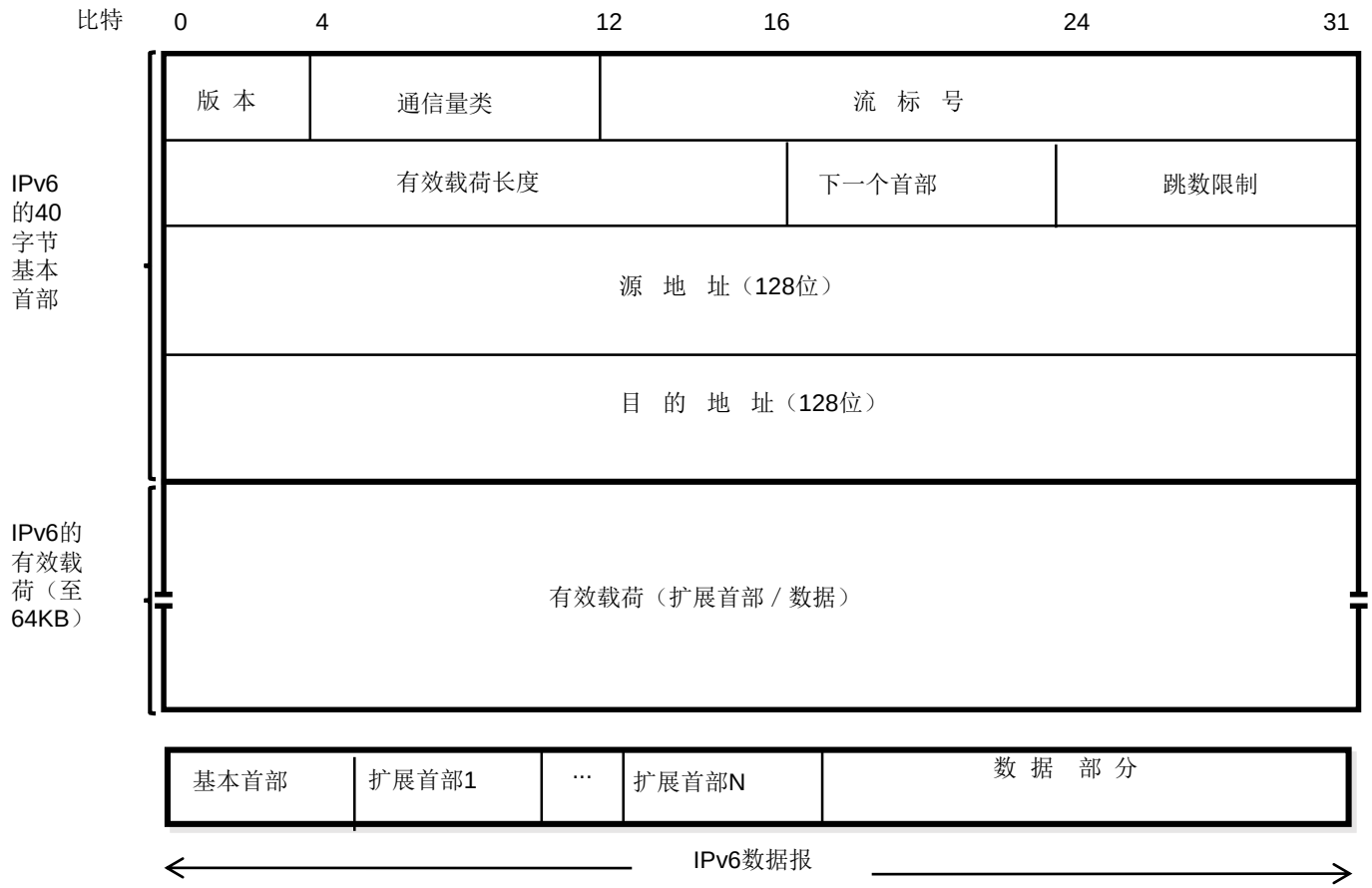
（12）目的地址。数据报的目的IP地址，占32bit。

IPv4协议安全性分析

IPv4协议是无状态、无认证协议，其自身有很多特性易被攻击者利用。

- IPv4协议没有认证机制：由于IPv4没有来源认证，IP包中的所有字段几乎都可以伪造。
- 数据包分片：IP数据报可能需要先分片，到达目的地后再重组。这一机制可以被攻击者利用，例如：借此攻击那些不能正确处理数据报分片异常（如分片重叠）的主机，用于绕过防火墙，或逃避入侵检测系统的检查。
- 寻址与协议选项：数据报的寻址信息以及协议选项的信息泄露了部分网络拓扑信息。记录路由或时戳的协议选项可被攻击者用于网络侦察。
- 访问控制与带宽控制：IPv4协议没有访问控制机制，使得攻击者可以查看上层协议（如，TCP、UDP等）的内容；攻击者还可以利用IPv4协议没有带宽控制的缺陷，进行数据包风暴攻击来消耗网络带宽、系统资源，从而导致拒绝服务攻击.

IPv6协议


比特
0
4
12
16
24
31
版 本
通信量类
流 标 号
有效载荷长度
下一个首部
跳数限制
源 地 址（128位）
目 的 地 址（128位）
IPv6的40字节基本首部
IPv6的有效载荷（至64KB）
有效载荷（扩展首部 / 数据）
基本首部
扩展首部1
…
扩展首部N
数 据 部 分
IPv6数据报

IPv6协议内容

（1）版本(version)。指IP协议的版本，值4表示IPv4，6表示IPv6。

（2）通信量类(traffic class)。主要用于区分不同的IPv6数据报的类别或优先级。

（3）流标号(flow label)。用来标识同一个流里面的报文。IPv6提出了流(flow)的概念，是指互联网络上从特定源点到特定终点（单播或多播）的一系列数据报，而在这个“流”所经过的路径上的路由器都能保证指明的服务质量。所有属于同一个流的数据报都具有相同的流标号。

（4）有效载荷长度(payload length)。表明该IPv6包基本首部后包含的字节数，包含扩展首部。

（5）下一个首部(next leader)。该字段用来指明报头后接的报文头部的类型，若存在扩展首部，表示第一个扩展首部的类型，否则表示其上层协议的类型。

（6）跳数限制（hop limit）。该字段类似于IPv4中的TTL，每次转发跳数减1，该字段达到0时包将会被丢弃。

（7）源地址。标识该报文的来源地址，占128位。

（8）目的地址。标识该报文的目的地址，占128位。

IPv4到IPv6的过渡

从IPv4向IPv6过渡采用逐步演进的方法，IETF推荐的过渡方案主要有：

- ✓双协议栈(dual stack):同时装备IPv4和IPv6协议栈；
- ✓隧道(tunneling)：隧道机制是指将IPv6数据报作为数据封装在IPv4数据报里；
- ✓网络地址转换(NAT, Network Address Translator)等机制：内部的IPv4主机要和外部的IPv6主机通信时，在NAT服务器中将IPv4地址（相当于内部地址）变换成IPv6地址（相当于全局地址），服务器维护一个IPv4与IPv6地址的映射表。反之，当内部的IPv6主机和外部的IPv4主机进行通信时，则IPv6主机映射成内部地址，IPv4主机映射成全局地址。

IPv6安全性分析

在安全性方面，与IPv4相比，IPv6通过IPSec协议保证IP层的传输安全，在网络保密性、完整性方面有了更好的改进，在可控性、抗否认性方面有了新的保证，主要改进措施如下：

(1) 包头认证(AH, Authentication Header)。IPv6将AH作为可选首部，提供数据完整性和分组的鉴权。

(2) 安全包头封装。同AH一样，IPv6将封装安全净荷(ESP, Encapsulating Security Payload)作为可选首部，以支持IP分组的私密和数据完整性。根据用户的不同需求，它既可用于传送层（如TCP、UDP、ICMP）的加密，称为“传输层模式ESP”，同时又可用于整个分组的加密，称为“隧道模式ESP”。

(3) ESP DES-CBC方式。ESP处理一般必须执行DES-CBC加密算法，数据分为以64位为单位的块进行处理，解密逻辑的输入是现行数据和先前加密数据块的与或。

(4) 鉴权加私密方式。根据不同的业务模式，两种IP安全机制可以按一定的顺序结合，从而达到分组传送加密的目的。按顺序的不同，分为鉴权之前加密和加密之前鉴权。

IPv6带来的新的安全风险

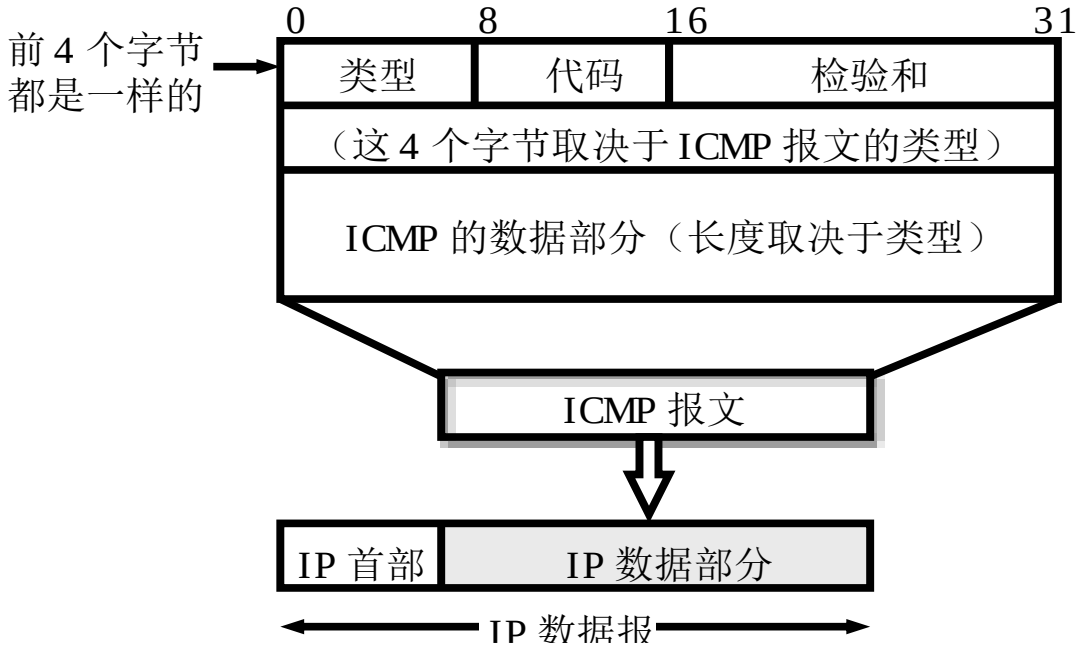
尽管IPv6协议采取多种措施来加强安全性，同时还会伴随其产生新的安全问题：

- IPv4向IPv6过渡技术的安全风险；
- 无状态地址自动配置的安全风险；
- 邻居发现协议的安全风险；
- IPv6中组播技术缺陷的安全风险；
- IPv6中PKI管理系统的安全风险；
- IPv6编址机制的隐患；
- IPv6的安全机制对网络安全体系的挑战所带来的安全风险等。

ICMP协议及其安全缺陷

ICMP(Internet Control Message Protocol)

为了提高IP数据报交付成功的机会，IETF在网际层设计了ICMP (Internet Control Message Protocol)协议。ICMP允许主机或路由器报告差错情况、提供有关异常情况的报告。



ICMP协议安全缺陷

ICMP协议本身的特点决定了它非常容易被用于攻击网络上的路由器和主机，因而被广泛应用。例如：

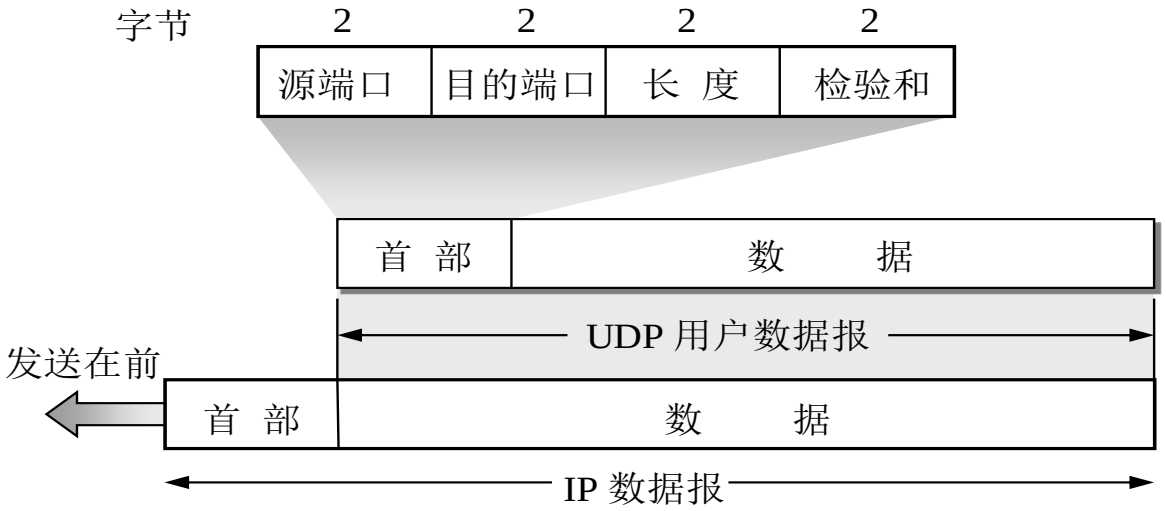
（1）利用“目的不可达”报文对攻击目标发起拒绝服务攻击。

（2）利用“改变路由”报文破坏路由表，导致网络瘫痪。

（3）木马利用ICMP协议报文进行隐蔽通信。

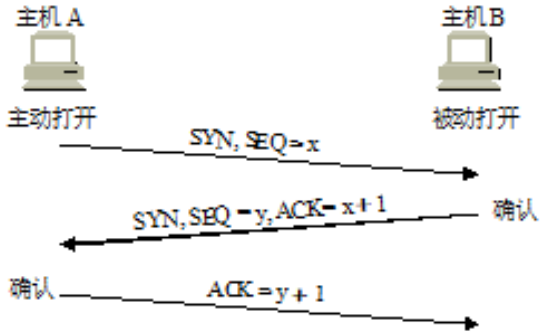
（4）利用“回送(Echo)请求或回答”报文进行网络扫描或拒绝服务攻击。

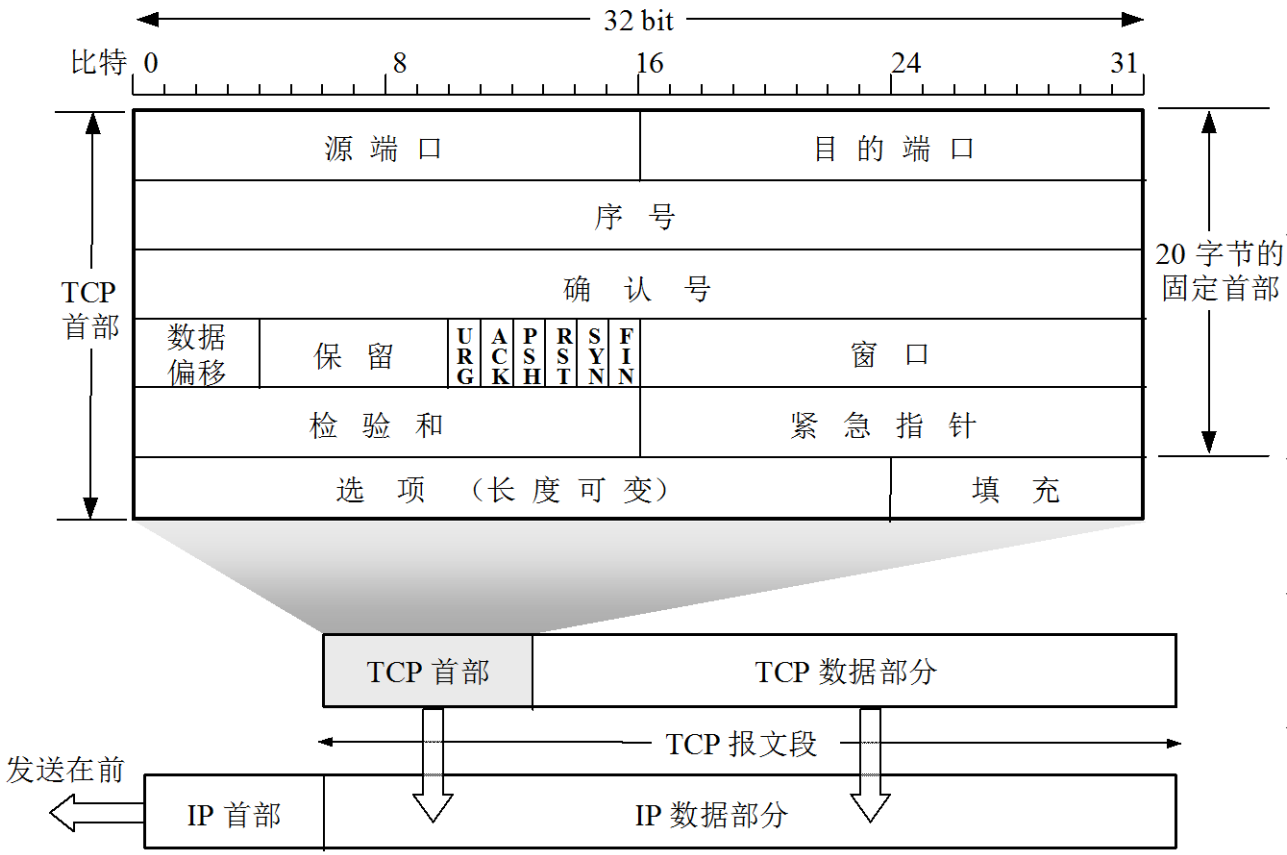
UDP协议及其安全缺陷



- ✓ 尽管UDP协议提供的是不可靠数据传输服务，但由于其简单高效，因此有很多应用层协议利用UDP作为传输协议，如简单网络管理协议(SNMP)、域名解析协议(DNS)、动态主机配置协议(DHCP)、网络文件系统(NFS)、简单文件传送协议(TFTP)和路由信息协议(RIP)。
- ✓ 如果某一应用层协议需要可靠传输，则可根据需要在UDP基础上加入一些可靠机制，如重传、超时、序号等，或直接利用TCP协议。
- ✓ UDP协议可以用来发起风暴型拒绝服务攻击。

TCP协议及其安全缺陷





- ✓ 主机A的TCP向主机B的TCP发出连接请求报文段，其首部中的同步比特SYN应置为1，同时选择一个序号x，表明在后面传送数据时的第一个数据字节的序号是x。
- ✓ 主机B的TCP收到连接请求报文段后，如同意，则发回确认。在确认报文段中应将SYN置为1，确认号应为x □ 1，同时也为自己选择一个序号y。
- ✓ 主机A的TCP收到此报文段后，还要向B给出确认，其确认号为y □ 1。
- ✓ 运行客户进程的主机A的TCP通知上层应用进程，连接已经建立(或打开)。
- ✓ 当运行服务器进程的主机B的TCP收到主机A的确认后，也通知其上层应用进程，连接已经建立。

TCP协议的安全性

（1）由于一台主机或服务器所允许建立的TCP连接数是有限的，因此，攻击者常常用TCP全连接（完成三次握手过程）或半连接（只完成二次握手过程）来对目标发起拒绝服务攻击，如SYN Flood攻击、TCP连接耗尽型攻击等。

（2）序号预测。TCP报文段的初始序号（ISN）在TCP连接建立时产生，攻击者向目标主机发送连接请求可得到上次的序号，再通过多次测量来回传输路径得到进攻主机到目标主机间数据包传送的来回时间（RTT）。已知上次连接的序号和RTT，就能预测下次连接的序号。若攻击者推测出正确的序号就能伪造有害数据包并使目标主机接受。

（3）网络扫描。攻击者可以利用TCP连接请求来进行端口扫描，从而获得目标主机上的网络服务状态，进一步发起有针对性的攻击。

ARP协议及其安全缺陷

- ARP用于将计算机的网络地址（32位IP地址）转化为物理地址（48位MAC地址）。
- 在以太网中的数据帧从一个主机到达网内的另一台主机是根据48位的以太网地址（硬件地址）来确定网络接口的，而不是根据32位的IP地址。因此，内核（如驱动）必须知道目的端的硬件地址才能发送数据。
- 每台主机均有一个ARP高速缓存(ARP Cache)，保存主机知道的所有IP地址和MAC地址的对应关系。
- 在Windows系统中，使用arp -a命令就可以查看本地的ARP高速缓存的内容。
- 一台主机的网络驱动程序要发送上层交来的数据时，会查看其ARP缓存中的IP地址和MAC地址的映射表。如果表中已有目的IP地址对应的MAC地址，则获取MAC地址，构建网络包发送，否则就发送ARP请求，等待拥有该IP的主机给出响应。发出请求的主机在收到响应后，更新其ARP缓存。

ARP协议安全性

ARP协议对收到的ARP响应不作任何验证就更新其ARP缓存，即允许未经请求的ARP广播或单播对缓存中的IP-MAC对应表表项进行删除、添加或修改。这一严重的安全缺陷，经常被攻击者用来进行各种网络攻击，例如：

（1）网络嗅探。攻击者可以伪造ARP响应，从本地或远程发送到本局域网中，修改ARP缓存，从而重定向IP数据流到攻击者主机，达到窃听、假冒或拒绝服务（如，IP地址冲突、网络数据包定向到非目的主机）等目的。

（2）阻止数据包通过网关。局域网一般通过网关与外网联接，所有与外网计算机有通信关系的计算机上的ARP缓存中都存在网关IP地址和MAC地址的映射记录。如果该记录被攻击者用假冒的ARP响应更改，那么该计算机向外发送的数据包将总被发送到错误的网关MAC地址上，导致该计算机就不能够与外网通信。

作业

1、比较IPv4协议与IPv6协议，并对它们进行安全性分析。

2、阐述Android操作系统中的安全机制。