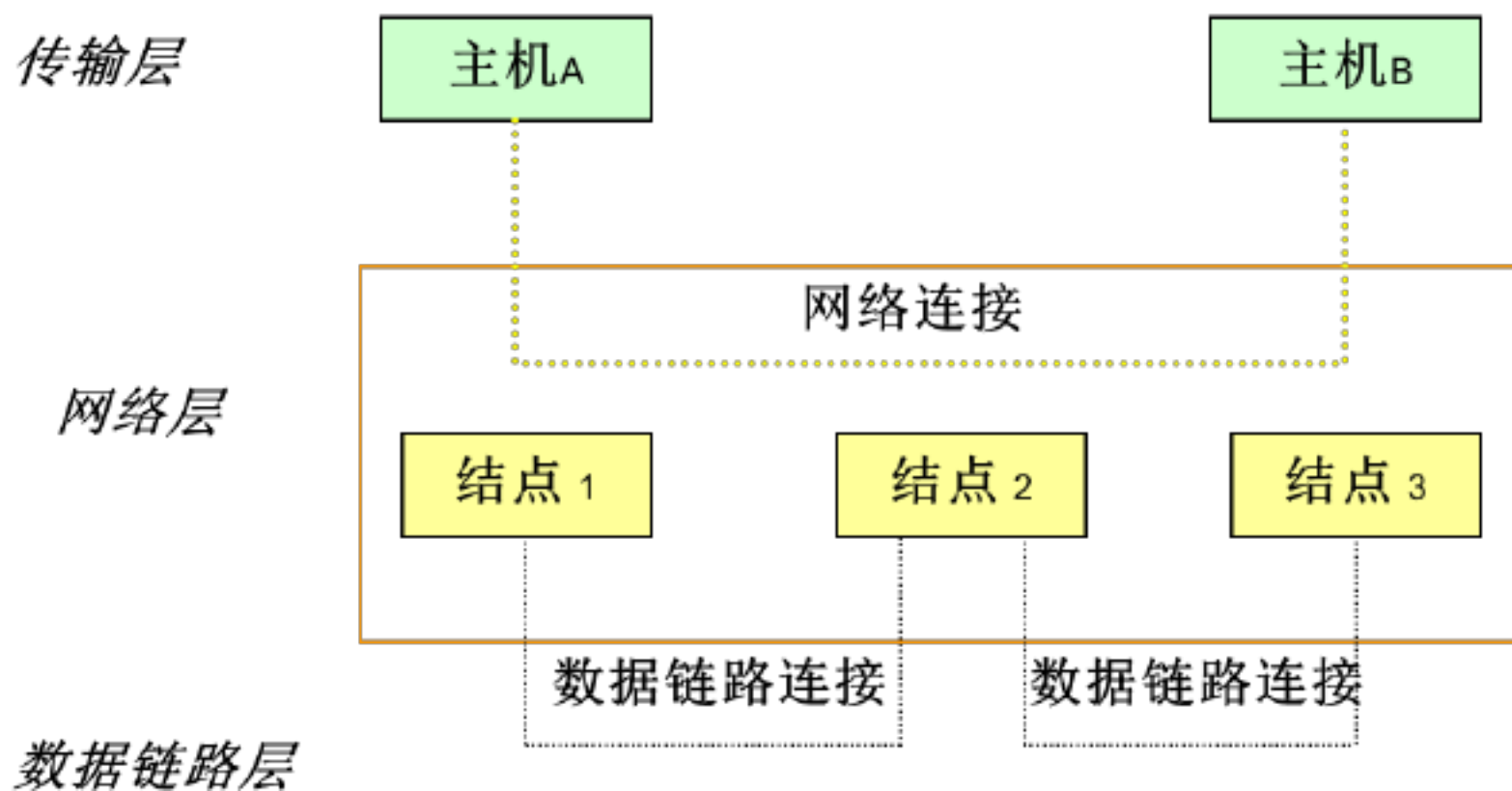


# 第 章 网络层

## 网络层概述

网络层负责数据包经过多条链路、由信源到信宿传递过程，并保证每个数据包能够成功和有效率地从出发点到达目的地。为实现端到端的传递，网络层提供了两种服务：线路交换和路由选择。线路交换是在物理链路之间建立临时的连接，每个数据包都通过这个临时链路进行传输；路由选择是选择数据包传输的最佳路径，在这种情况下，每个数据包都可以通过不同的路由到达目的地，然后再在目的地重新按照原始顺序组装起来。



网络层是通信子网的最高层，对上层用户屏蔽了子网通信的细节，如子网类型、拓扑结构、子网数目，向上层提供一致的服务、统一的地址。

### 网络层功能

为传输层提供建立、维持和释放网络连接的手段，完成路由选择、拥塞控制、网络

互联等功能。

根据传输层的要求选择网络服务质量。服务质量的参数主要包括：残留差错率、服务可用性、可靠性、吞吐量、传输延迟等。

对数据传输过程实现流量控制、差错控制以及顺序控制。

提高资源子网主机节点与通信子网的接口，向传输层提供虚电路服务和数据报服务。

网络层的主要功能是完成网络中主机间的报文传输，其关键问题之一是使用数据链路层服务将每个报文从源端传输到目的端。

**基本功能**：实现端到端的网络连接，屏蔽不同子网技术的差异，向上层提供一致的服务。

**主要功能**：

**路由选择和转发**

**通过网络连接在主机之间提供分组交换功能**

**分组的分段与成块，差错控制、顺序化、流量控制**

## 网络层提供的两种服务

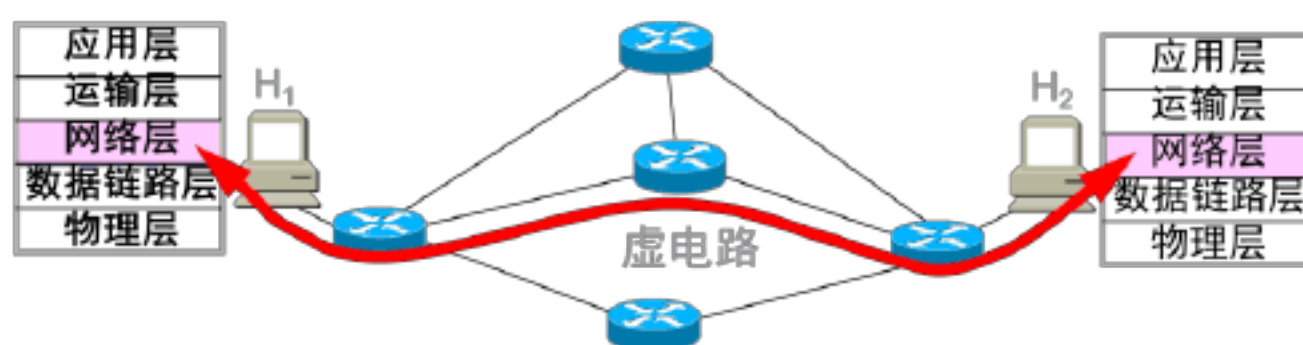
- 网络层的目的是实现两个端系统之间的数据透明传送，具体功能包括寻址和路由选择、连接的建立、保持和终止等。它提供的服务使运输层不需要了解网络中的数据传输和交换技术。
- 在计算机网络领域，网络层应该向运输层提供怎样的服务（“面向连接”还是“无连接”）曾引起了长期的争论。
- 争论焦点的实质就是：在计算机通信中，可靠交付应当由谁来负责？是网络还是端系统？

## 电信网的成功经验

### 让网络负责可靠交付

- 面向连接的通信方式
- 建立虚电路(Virtual Circuit), 以保证双方通信所需的一切网络资源。
- 如果再使用可靠传输的网络协议, 就可使所发送的分组无差错按序到达终点。

### 虚电路服务



H<sub>1</sub> 发送给 H<sub>2</sub> 的所有分组都沿着同一条虚电路传送

### 虚电路是逻辑连接

- 虚电路表示这只是一条逻辑上的连接, 分组都沿着这条逻辑连接按照存储转发方式传送, 而并不是真正建立了一条物理连接。
- 请注意, 电路交换的电话通信是先建立了一条真正的连接。因此分组交换的虚连接和电路交换的连接只是类似, 但并不完全一样。

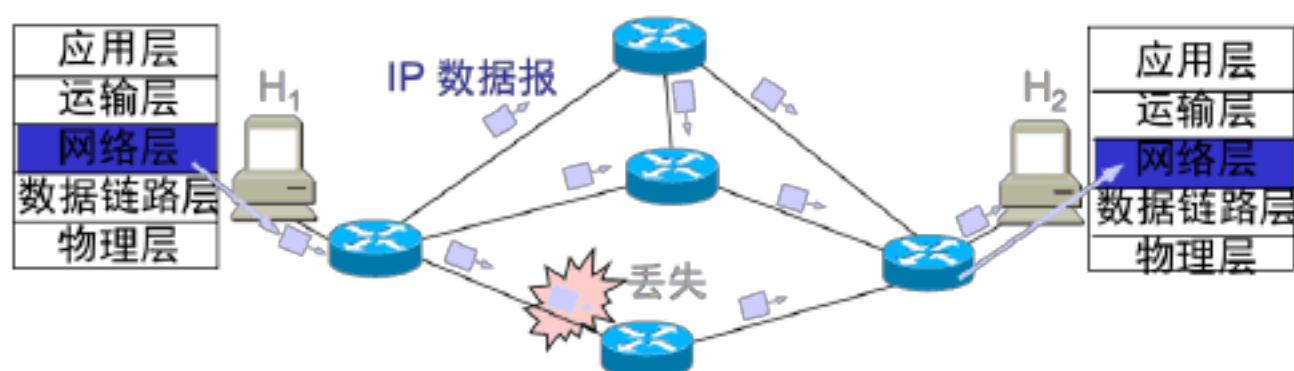
## 因特网采用的设计思路

- 网络层向上只提供简单灵活的、无连接的、尽最大努力交付的数据报服务。
- 网络在发送分组时不需要先建立连接。每一个分组（即 IP 数据报）独立发送，与其前后的分组无关（不进行编号）。
- 网络层不提供服务质量的承诺。即所传送的分组可能出错、丢失、重复和失序（不按序到达终点），当然也不保证分组传送的时限。

## 尽最大努力交付的好处

- 由于传输网络不提供端到端的可靠传输服务，这就使网络中的路由器可以做得比较简单，而且价格低廉（与电信网的交换机相比较）。
- 如果主机（即端系统）中的进程之间的通信需要是可靠的，那么就由网络的主机中的运输层负责（包括差错处理、流量控制等）。
- 采用这种设计思路的好处是：网络的造价大大降低，运行方式灵活，能够适应多种应用。
- 因特网能够发展到今日的规模，充分证明了当初采用这种设计思路的正确性。

## 数据报服务

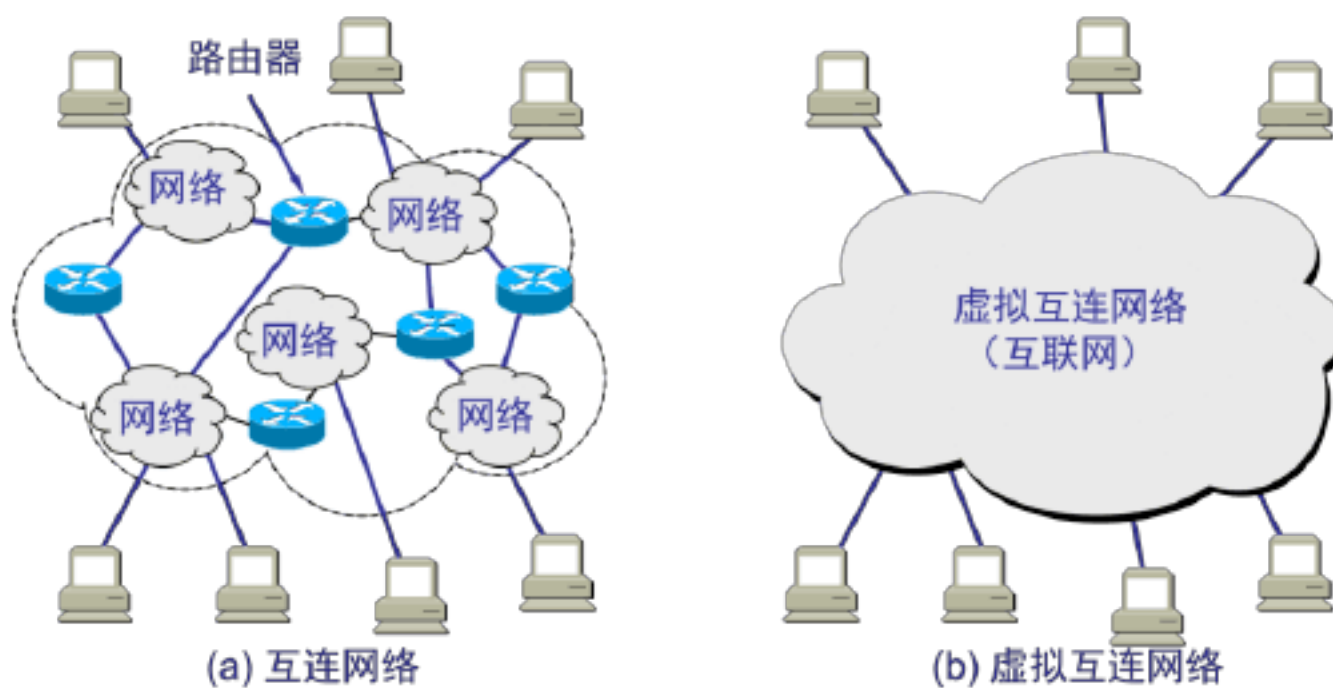


H<sub>1</sub> 发送给 H<sub>2</sub> 的分组可能沿着不同路径传送

## 虚拟互连网络的意义

- 所谓虚拟互连网络也就是逻辑互连网络，它的意思就是互连起来的各种物理网络的异构性本来是客观存在的，但是我们利用 IP 协议就可以使这些性能各异的网络从用户看起来好像是一个统一的网络。
- 使用 IP 协议的虚拟互连网络可简称为 IP 网。
- 使用虚拟互连网络的好处是：当互联网上的主机进行通信时，就好像在一个网络上通信一样，而看不见互连的各具体的网络异构细节。

## 互连网络与虚拟互连网络



对比的方面	虚电路服务	数据报服务
思路	可靠通信应当由网络来保证	可靠通信应当由用户主机来保证
连接的建立	必须有	不要
目的站地址	仅在连接建立阶段使用，每个分组使用短的虚电路号	每个分组都有目的站的全地址
分组的转发	属于同一条虚电路的分组均按照同一路由进行转发	每个分组独立选择路由进行转发
结点出故障时	所有通过出故障结点的虚电路均不能工作	出故障的结点可能会丢失分组，一些路由可能发生变化
分组的顺序	总是按发送顺序到达目的站	到达目的站不一定按发送顺序
差错控制和流量控制	可由分组交换网负责，也可由用户机负责	用用户机负责
拥塞控制	易于实现	很难实现

## 网络层服务的特点

网络层的服务有如下特点：

最重要的特点是无连接

服务是不可靠的，传送过程中可能延迟、不按顺序到达或者丢失等

服务是尽力而为的。

网络层实现这种无连接服务的分组传送机制称为网际协议，通称 IP 协议。

网络层服务应遵循以下三个原则：

服务应与通信子网技术无关。

通信子网的数量、类型和拓扑结构对传输层是隐蔽的。

传输层能获得的网络地址应采用统一的编号形式，即使跨越多个子网和域。

## 路由算法

路由算法是网络层软件的一部分，它负责确定一个进来的分组应该被传送到哪条输出线路上。

### 路由算法选择的参考标准

路由算法选择有以下参考标准：

正确性：沿着路由表所指引的路由，分组一定能够传输到最终到达的目的网络和目的主机。

最优化：指路由算法选择最佳路径的能力。

简洁性：算法设计简洁，利用最少的软件和开销，提供最有效的功能。

坚固性：路由算法处于非正常或不可预料的环境时，如硬件故障、负载过高或操作失误时，都能正确运行。

快速收敛：收敛是在最佳路径的判断上所有路由器到达一致的过程。收敛慢的路由算法会造成路径循环或网络中断。

灵活性：路由算法可以快速、准确地适应各种网络环境。

### 路由算法种类

路由算法可以分为两大类：非自适应的和自适应的。

非自适应路由算法，它是按照预先计算好的信息进行路由，它不会根据当前测量或者估计的流量和拓扑结构，来调整他们的路由决策。非自适应路由算法主要包括静态路由算法、分散通信量以及洪泛算法。

自适应路由算法，它是根据网络拓扑结构和通信量的变化等改变路由。主要有距离向量路由算法和链路状态路由算法等。

### 距离向量路由算法

距离向量路由算法要求每个路由器发送其路由表全部或部分信息，但仅发送到邻近节点上。从本质上来说，链路状态算法将少量更新信息发送至网络各处，而距离向量算法发送大量更新信息至邻接路由器。

距离向量路由算法属于动态路由算法。

缺陷：路由收敛速度慢，对好消息反应迅速，对坏消息反应迟钝；选择路由时，没有考虑线路带宽。

## 链路状态路由算法

链路状态路由算法 ( 也称最短路由算法 ) 发送路由信息到互联网上所有的结点 , 然而对于每个路由器 , 仅发送它的路由表中描述了其自身链路状态的一部分。

该路由算法是以权值作为计算路由的基础的。所谓权值是各种情况的综合考虑 , 主要包括路径长度、可靠性、路由延迟、负荷、通信代价等。

与距离向量路由不同 , 链路状态路由的信息交换准则是 : 每隔一定时间( 大约 分钟 ) , 与所有的路由器交换自己邻居的信息。

优点 :

一次性可以获得网络上所有路由器的信息 , 而不需要逐点传递 ;

该算法以权值作为基础 , 在计算路由时 , 考虑了多种因素 , 所以优于距离向量路由算法 ;

在获得了所有路由器信息之后 , 每个路由器分别采用 算法以得出它到其他各个路由器的最短路径。

二者的区别 :

这两种算法在大多数环境下都能很好的运行 , 除了以下区别 :

链路状态算法收敛更快 , 因此在一定程度上比路由算法更不容易产生路由循环。

链路状态算法要求比距离向量算法有更强的 能力和更多的内存空间 , 因此链路状态路由算法将会在实现时显得更昂贵一些。

距离向量路由算法适用于简单的网络 , 而链路状态路由算法更适合于复杂程度较高的网络

## 网络层协议

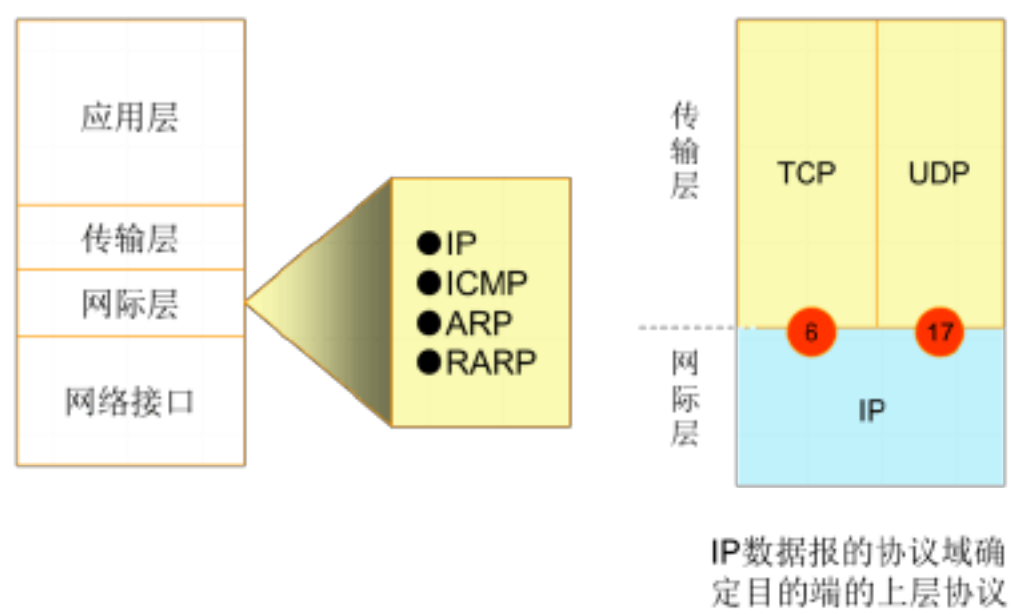


的任务是提供一种尽力投递的方法将数据报从源端传输到目标端，它并不关心源机器和目标机器是否在同样的网络中，也不关心它们之间是否还有其他网络。( 协议数据单元 )

网络层是路由选择和负责网络寻址的层。

( 网际协议 ) 是最普通的网络层协议，提供无连接的数据报传输机制。

### TCP/IP网际层的四个主要协议



协议

的地址是 位长，由 个分段的十进制组成。由网络号和主机号两部分构成。

地址的分类 (

## IP地址分类

A类	0	7bits 网络号	24 bits 主机号
B类	1 0	14 bits 网络号	16 bits 主机号
C类	1 1 0	21bits 网络号	8bits 主机号

### 地址范围

**A类 0.0.0.0 ~ 127.255.255.255**  
**B类 128.0.0.0 ~ 191.255.255.255**  
**C类 192.0.0.0 ~ 223.255.255.255**

## 保留的IP地址

以下这些IP地址具有特殊的含义:

00...00	0000 ... 0000	本机
00...00	主机号	本网中的主机
11...11	1111 ... 1111	局域网中的广播
网络号	1111 ... 1111	对指定网络的广播
网络号	0000 ... 0000	网络地址
127	任意值	回路

一般来说, 主机号部分为全“1”的IP地址保留用作广播地址;  
主机号部分为全“0”的IP地址保留用作网络地址。

地址有如下特点:

网络号可用于将数据报路由到目的网络

主机号可用于将数据报交付到本网络的主机

简化了路由表

子网 ( ) 划分:

因特网规模的急剧增长, 对 地址的需求激增。带来的问题是:

地址资源的严重匮乏

路由表规模的急速增长

解决办法：从主机号部分拿出几位作为子网号

这种在原来地址结构的基础上增加一级结构的方法称为子网划分。

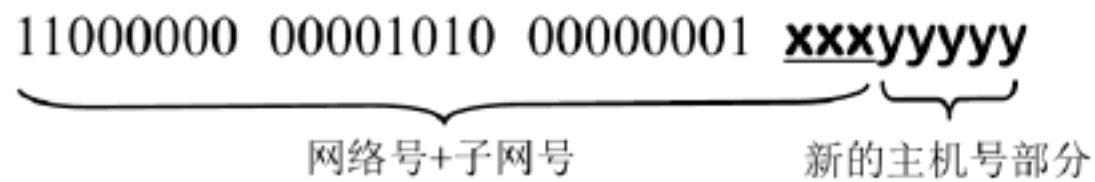
前提：网络规模较小——地址空间没有全部利用。

例如：三个，主机数为，，，均少于类地址允许的主机数。为这三个

申请个类地址显然有点浪费。

### 子网划分举例

例如：C类网络192.10.1.0，主机号部分的前三位用于标识子网号，即：



一般来说，全1和全0子网号的地址保留，因此划分出 $2^3-2=6$ 个子网，子网地址分别为：

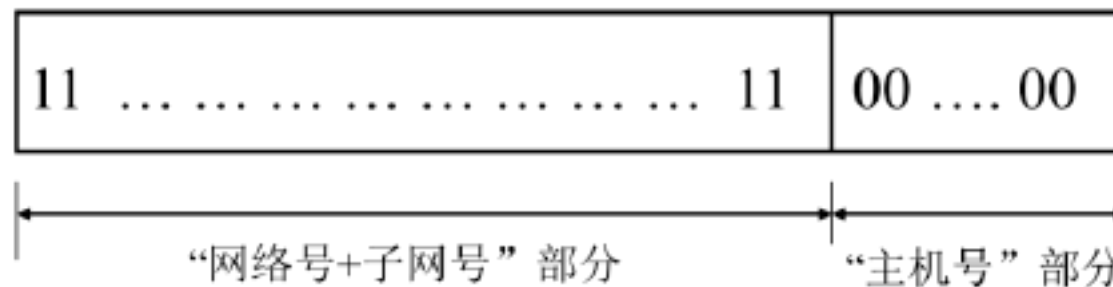
- 11000000 00001010 00000001 00100000 -- 192.10.1.32
- 11000000 00001010 00000001 01000000 -- 192.10.1.64
- 11000000 00001010 00000001 01100000 -- 192.10.1.96
- 11000000 00001010 00000001 10000000 -- 192.10.1.128
- 11000000 00001010 00000001 10100000 -- 192.10.1.160
- 11000000 00001010 00000001 11000000 -- 192.10.1.192

### •子网掩码（Subnet Mask）

子网划分后，如何识别不同的子网？

解决：采用子网掩码来分离网络号和主机号。

子网掩码格式：32比特，网络号(包括子网号)部分全为“1”，主机号部分全为“0”。



## 子网掩码计算

前面的例子中：网络号24位，子网号3位，总共27位。所以子网掩码为：

11111111 11111111 11111111 11100000  
即 255 . 255 . 255 . 224

*缺省子网掩码：A类：255.0.0.0*

*B类：255.255.0.0*

*C类：255.255.255.0*

## 子网地址计算

子网掩码∧ IP地址，结果就是该 IP地址的网络号。

例如：IP地址202.117.1.207，子网掩码255.255.255.224

11001010	01110101	00000001	110 01111
∧ 11111111	11111111	11111111	111 00000
11001010	01110101	00000001	110 00000

∴子网地址为：202.117.1.192

主机号为：15

*主机之间要能够通信，它们必须在同一子网内，否则需要使用路由器（或网关）实现互联。*

## 子网规划举例

网络分配了一个C类地址：201.222.5.0。假设需要20个子网，每个子网有5台主机。

试确定各子网地址和子网掩码。

1) 对C类地址，要从最后8位中分出几位作为子网地址：  
∵ $2^4 < 20 < 2^5$ ，∴选择5位作为子网地址，共可提供30个子网地址。

2) 检查剩余的位数能否满足每个子网中主机台数的要求：  
∵子网地址为5位，故还剩3位可以用作主机地址。

而

$2^3 > 5 + 2$ ，所以可以满足每子网5台主机的要求。

3) 子网掩码为255.255.255.248。  
(11111000B = 248)

4) 子网地址可在8、16、24、32、……、240共30个地址中任意选择20个。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/505330002023011113>