# 编程语言

参考链接：Github：https://github.com/huihut/interview

## C/C++

### 1.1 const

#### 1.1.1作用

1. 修饰变量，说明该变量不可以被改变；
2. 修饰指针，分为指向常量的指针和指针常量；
3. 常量引用，经常用于形参类型，即避免了拷贝，又避免了函数对值的修改；
4. 修饰成员函数，说明该成员函数内不能修改成员变量。

#### 1.1.2 const 使用

// 类class A

{private:

const int a; // 常对象成员，只能在初始化列表赋值

public:

// 构造函数

A() : a(0) { };

A(int x) : a(x) { }; // 初始化列表

// const可用于对重载函数的区分

int getValue(); // 普通成员函数

int getValue() const; // 常成员函数，不得修改类中的任何数据成员的值

};

void function()

{

// 对象

A b; // 普通对象，可以调用全部成员函数、更新常成员变量

const A a; // 常对象，只能调用常成员函数

const A \*p = &a; // 常指针

const A &q = a; // 常引用

// 指针

char greeting[] = "Hello";

char\* p1 = greeting; // 指针变量，指向字符数组变量

const char\* p2 = greeting; // 指针变量，指向字符数组常量

char\* const p3 = greeting; // 常指针，指向字符数组变量

const char\* const p4 = greeting; // 常指针，指向字符数组常量

}

// 函数

void function1(const int Var); // 传递过来的参数在函数内不可变

void function2(const char\* Var); // 参数指针所指内容为常量

void function3(char\* const Var); // 参数指针为常指针

void function4(const int& Var); // 引用参数在函数内为常量

// 函数返回值

const int function5(); // 返回一个常数

const int\* function6(); // 返回一个指向常量的指针变量，使用：const int \*p = function6();

int\* const function7(); // 返回一个指向变量的常指针，使用：int\* const p = function7();

### **1.2 static**

#### 1.2.1作用

1. 修饰普通变量，修改变量的存储区域和生命周期，使变量存储在静态区，在 main 函数运行前就分配了空间，如果有初始值就用初始值初始化它，如果没有初始值系统用默认值初始化它。
2. 修饰普通函数，表明函数的作用范围，仅在定义该函数的文件内才能使用。在多人开发项目时，为了防止与他人命名空间里的函数重名，可以将函数定位为 static。
3. 修饰成员变量，修饰成员变量使所有的对象只保存一个该变量，而且不需要生成对象就可以访问该成员。
4. 修饰成员函数，修饰成员函数使得不需要生成对象就可以访问该函数，但是在 static 函数内不能访问非静态成员。Static函数只能访问static成员。

### 1.3 this指针

#### 1.3.1 作用

1. this 指针是一个隐含于每一个非静态成员函数中的特殊指针。它指向调用该成员函数的那个对象。
2. 当对一个对象调用成员函数时，编译程序先将对象的地址赋给 this 指针，然后调用成员函数，每次成员函数存取数据成员时，都隐含使用 this 指针。
3. 当一个成员函数被调用时，自动向它传递一个隐含的参数，该参数是一个指向这个成员函数所在的对象的指针。
4. this 指针被隐含地声明为: ClassName \*const this，这意味着不能给 this 指针赋值；在 ClassName 类的 const 成员函数中，this 指针的类型为：const ClassName\* const，这说明不能对 this 指针所指向的这种对象是不可修改的（即不能对这种对象的数据成员进行赋值操作）；
5. this 并不是一个常规变量，而是个右值，所以不能取得 this 的地址（不能 &this）。
6. 在以下场景中，经常需要显式引用 this 指针：
7. 为实现对象的链式引用；
8. 为避免对同一对象进行赋值操作；
9. 在实现一些数据结构时，如 list。

### 1.4 inline 内联函数

#### 1.4.1 特征

1.相当于把内联函数里面的内容写在调用内联函数处；

2.相当于不用执行进入函数的步骤，直接执行函数体；

3.相当于宏，却比宏多了类型检查，真正具有函数特性；

4.编译器一般不内联包含循环、递归、switch 等复杂操作的内联函数；

5.在类声明中定义的函数，除了虚函数的其他函数都会自动隐式地当成内联函数。

#### 1.4.2 使用

// 声明1（加 inline，建议使用）

inline int functionName(int first, int second,...);

// 声明2（不加 inline）

int functionName(int first, int second,...);

// 定义

inline int functionName(int first, int second,...) {/\*\*\*\*/};

// 类内定义，隐式内联

class A {

int doA() { return 0; } // 隐式内联

}

// 类外定义，需要显式内联

class A {

int doA();

}

inline int A::doA() { return 0; } // 需要显式内联

#### 1.4.3 编译器对 inline 函数的处理步骤

1.将 inline 函数体复制到 inline 函数调用点处；

2.为所用 inline 函数中的局部变量分配内存空间；

3.将 inline 函数的的输入参数和返回值映射到调用方法的局部变量空间中；

4.如果 inline 函数有多个返回点，将其转变为 inline 函数代码块末尾的分支（使用 GOTO）。

#### 1.4.4 优缺点

优点

1. 内联函数同宏函数一样将在被调用处进行代码展开，省去了参数压栈、栈帧开辟与回收，结果返回等，从而提高程序运行速度。
2. 内联函数相比宏函数来说，在代码展开时，会做安全检查或自动类型转换（同普通函数），而宏定义则不会。
3. 在类中声明同时定义的成员函数，自动转化为内联函数，因此内联函数可以访问类的成员变量，宏定义则不能。
4. 内联函数在运行时可调试，而宏定义不可以。

缺点

1. 代码膨胀。内联是以代码膨胀（复制）为代价，消除函数调用带来的开销。如果执行函数体内代码的时间，相比于函数调用的开销较大，那么效率的收获会很少。另一方面，每一处内联函数的调用都要复制代码，将使程序的总代码量增大，消耗更多的内存空间。
2. inline 函数无法随着函数库升级而升级。inline函数的改变需要重新编译，不像 non-inline 可以直接链接。
3. 是否内联，程序员不可控。内联函数只是对编译器的建议，是否对函数内联，决定权在于编译器。

#### 1.4.5 虚函数（virtual）可以是内联函数（inline）吗？

1.虚函数可以是内联函数，内联是可以修饰虚函数的，但是当虚函数表现多态性的时候不能内联。

2.内联是在编译器建议编译器内联，而虚函数的多态性在运行期，编译器无法知道运行期调用哪个代码，因此虚函数表现为多态性时（运行期）不可以内联。

3.inline virtual 唯一可以内联的时候是：编译器知道所调用的对象是哪个类（如 Base::who()），这只有在编译器具有实际对象而不是对象的指针或引用时才会发生。

#### 1.4.6 虚函数内联使用

#include <iostream> using namespace std;class Base

{public:

inline virtual void who()

{

cout << "I am Base\n";

}

virtual ~Base() {}

};class Derived : public Base

{public:

inline void who() // 不写inline时隐式内联

{

cout << "I am Derived\n";

}

};

int main()

{

// 此处的虚函数 who()，是通过类（Base）的具体对象（b）来调用的，编译期间就能确定了，所以它可以是内联的，但最终是否内联取决于编译器。

Base b;

b.who();

// 此处的虚函数是通过指针调用的，呈现多态性，需要在运行时期间才能确定，所以不能为内联。

Base \*ptr = new Derived();

ptr->who();

// 因为Base有虚析构函数（virtual ~Base() {}），所以 delete 时，会先调用派生类（Derived）析构函数，再调用基类（Base）析构函数，防止内存泄漏。

delete ptr;

ptr = nullptr;

system("pause");

return 0;

}

### **1.5 volatile**

volatile int i = 10;

* volatile 关键字是一种类型修饰符，用它声明的类型变量表示可以被某些编译器未知的因素（操作系统、硬件、其它线程等）更改。所以使用 volatile 告诉编译器不应对这样的对象进行优化。
* volatile 关键字声明的变量，每次访问时都必须从内存中取出值（没有被 volatile 修饰的变量，可能由于编译器的优化，从 CPU 寄存器中取值）
* const 可以是 volatile （如只读的状态寄存器）
* 指针可以是 volatile

### 1.6 **assert()**

断言，是宏，而非函数。assert 宏的原型定义在 <assert.h>（C）、<cassert>（C++）中，其作用是如果它的条件返回错误，则终止程序执行。可以通过定义 NDEBUG 来关闭 assert，但是需要在源代码的开头，include <assert.h> 之前。

#define NDEBUG // 加上这行，则 assert 不可用

#include <assert.h>

assert( p != NULL ); // assert 不可用

### 1.7 **sizeof()**

* sizeof 对数组，得到整个数组所占空间大小。
* sizeof 对指针，得到指针本身所占空间大小。

### 1.8 **#pragma pack(n)**

#pragma pack(push) // 保存对齐状态

#pragma pack(4) // 设定为 4 字节对齐

struct test

{

char m1;

double m4;

int m3;

};

#pragma pack(pop) // 恢复对齐状态

### 1.9 **位域**

Bit mode: 2; // mode 占 2 位

类可以将其（非静态）数据成员定义为位域（bit-field），在一个位域中含有一定数量的二进制位。当一个程序需要向其他程序或硬件设备传递二进制数据时，通常会用到位域。

* 位域在内存中的布局是与机器有关的
* 位域的类型必须是整型或枚举类型，带符号类型中的位域的行为将因具体实现而定
* 取地址运算符（&）不能作用于位域，任何指针都无法指向类的位域

### 1.10 **extern "C"**

* 被 extern 限定的函数或变量是 extern 类型的
* 被 extern "C" 修饰的变量和函数是按照 C 语言方式编译和链接的

extern "C" 的作用是让 C++ 编译器将 extern "C" 声明的代码当作 C 语言代码处理，可以避免 C++ 因符号修饰导致代码不能和C语言库中的符号进行链接的问题。

#ifdef \_\_cplusplusextern "C" {

#endif

void \*memset(void \*, int, size\_t);

#ifdef \_\_cplusplus

}

#endif

### **1.11 struct 和 typedef struct**

#### 1.11.1 在C 中

// ctypedef struct Student {

int age;

} S;

等价于

// cstruct Student {

int age;

};

typedef struct Student S;

此时 S 等价于 struct Student，但两个标识符名称空间不相同。

另外还可以定义与 struct Student 不冲突的 void Student() {}。

#### 1.11.2 在**C++ 中**

由于编译器定位符号的规则（搜索规则）改变，导致不同于C语言。

一、如果在类标识符空间定义了 struct Student {...};，使用 Student me; 时，编译器将搜索全局标识符表，Student 未找到，则在类标识符内搜索。

即表现为可以使用 Student 也可以使用 struct Student，如下：

// cpp

struct Student {

int age;

};

void f( Student me ); // 正确，"struct" 关键字可省略

二、若定义了与 Student 同名函数之后，则 Student 只代表函数，不代表结构体，如下：

typedef struct Student {

int age;

} S;

void Student() {} // 正确，定义后 "Student" 只代表此函数

//void S() {} // 错误，符号 "S" 已经被定义为一个 "struct Student" 的别名

int main() {

Student();

struct Student me; // 或者 "S me";

return 0;

}

### 1.12 **C++ 中 struct 和 class**

总的来说，struct 更适合看成是一个数据结构的实现体，class 更适合看成是一个对象的实现体。

#### **区别**

* 最本质的一个区别就是默认的访问控制
  1. 默认的继承访问权限。struct 是 public 的，class 是 private 的。
  2. struct 作为数据结构的实现体，它默认的数据访问控制是 public 的，而 class 作为对象的实现体，它默认的成员变量访问控制是 private 的。

### **1.13 union 联合**

联合（union）是一种节省空间的特殊的类，一个 union 可以有多个数据成员，但是在任意时刻只有一个数据成员可以有值。当某个成员被赋值后其他成员变为未定义状态。联合有如下特点：

* 默认访问控制符为 public
* 可以含有构造函数、析构函数
* 不能含有引用类型的成员
* 不能继承自其他类，不能作为基类
* 不能含有虚函数
* 匿名 union 在定义所在作用域可直接访问 union 成员
* 匿名 union 不能包含 protected 成员或 private 成员
* 全局匿名联合必须是静态（static）的

#include<iostream>

union UnionTest {

UnionTest() : i(10) {};

int i;

double d;

};

static union {

int i;

double d;

};

int main() {

UnionTest u;

union {

int i;

double d;

};

std::cout << u.i << std::endl; // 输出 UnionTest 联合的 10

::i = 20;

std::cout << ::i << std::endl; // 输出全局静态匿名联合的 20

i = 30;

std::cout << i << std::endl; // 输出局部匿名联合的 30

return 0;

}

### 1.14 C++面向对象

C 实现 C++ 的面向对象特性（封装、继承、多态）

* 封装：使用函数指针把属性与方法封装到结构体中
* 继承：结构体嵌套
* 多态：父类与子类方法的函数指针不同

#### 封装

把客观事物封装成抽象的类，并且类可以把自己的数据和方法只让可信的类或者对象操作，对不可信的进行信息隐藏。关键字：public, protected, private。不写默认为 private。

* public 成员：可以被任意实体访问
* protected 成员：只允许被子类及本类的成员函数访问
* private 成员：只允许被本类的成员函数、友元类或友元函数访问

#### 继承

* 基类（父类）——> 派生类（子类）

#### 多态

* 多态，即多种状态（形态）。简单来说，我们可以将多态定义为消息以多种形式显示的能力。
* 多态是以封装和继承为基础的。
* C++ 多态分类及实现：
  1. 重载多态（Ad-hoc Polymorphism，编译期）：函数重载、运算符重载
  2. 子类型多态（Subtype Polymorphism，运行期）：虚函数
  3. 参数多态性（Parametric Polymorphism，编译期）：类模板、函数模板
  4. 强制多态（Coercion Polymorphism，编译期/运行期）：基本类型转换、自定义类型转换

#### **静态多态（编译期/早绑定）**

函数重载

class A

{public:

void do(int a);

void do(int a, int b);

};

#### **动态多态（运行期期/晚绑定）**

* 虚函数：用 virtual 修饰成员函数，使其成为虚函数

****注意：****

* 普通函数（非类成员函数）不能是虚函数
* 静态函数（static）不能是虚函数
* 构造函数不能是虚函数（因为在调用构造函数时，虚表指针并没有在对象的内存空间中，必须要构造函数调用完成后才会形成虚表指针）
* 内联函数不能是表现多态性时的虚函数，解释见：[虚函数（virtual）可以是内联函数（inline）吗？](https://github.com/huihut/interview" \l "%E8%99%9A%E5%87%BD%E6%95%B0virtual%E5%8F%AF%E4%BB%A5%E6%98%AF%E5%86%85%E8%81%94%E5%87%BD%E6%95%B0inline%E5%90%97)

class Shape // 形状类

{public:

virtual double calcArea()

{

...

}

virtual ~Shape();

};class Circle : public Shape // 圆形类

{public:

virtual double calcArea();

...

};class Rect : public Shape // 矩形类

{public:

virtual double calcArea();

...

};int main()

{

Shape \* shape1 = new Circle(4.0);

Shape \* shape2 = new Rect(5.0, 6.0);

shape1->calcArea(); // 调用圆形类里面的方法

shape2->calcArea(); // 调用矩形类里面的方法

delete shape1;

shape1 = nullptr;

delete shape2;

shape2 = nullptr;

return 0;

}

### 1.15 explicit（显式）关键字

* explicit 修饰构造函数时，可以防止隐式转换和复制初始化
* explicit 修饰转换函数时，可以防止隐式转换，但 [按语境转换](https://zh.cppreference.com/w/cpp/language/implicit_conversion) 除外

struct A

{

A(int) { }

operator bool() const { return true; }

};

struct B

{

explicit B(int) {}

explicit operator bool() const { return true; }

};

void doA(A a) {}

void doB(B b) {}

int main()

{

A a1(1); // OK：直接初始化

A a2 = 1; // OK：复制初始化

A a3{ 1 }; // OK：直接列表初始化

A a4 = { 1 }; // OK：复制列表初始化

A a5 = (A)1; // OK：允许 static\_cast 的显式转换

doA(1); // OK：允许从 int 到 A 的隐式转换

if (a1); // OK：使用转换函数 A::operator bool() 的从 A 到 bool 的隐式转换

bool a6（a1）;// OK：使用转换函数 A::operator bool() 的从 A 到 bool 的隐式转换

bool a7 = a1;// OK：使用转换函数 A::operator bool() 的从 A 到 bool 的隐式转换

bool a8 = static\_cast<bool>(a1); // OK ：static\_cast 进行直接初始化

B b1(1); // OK：直接初始化

B b2 = 1; // 错误：被 explicit 修饰构造函数的对象不可以复制初始化

B b3{ 1 }; // OK：直接列表初始化

B b4 = { 1 }; // 错误：被 explicit 修饰构造函数的对象不可以复制列表初始化

B b5 = (B)1; // OK：允许 static\_cast 的显式转换

doB(1); // 错误：被 explicit 修饰构造函数的对象不可以从 int 到 B 的隐式转换

if (b1); // OK：被 explicit 修饰转换函数 B::operator bool() 的对象可以从 B 到 b ool 的按语境转换

bool b6(b1); // OK：被 explicit 修饰转换函数 B::operator bool() 的对象可以从 B 到 bool 的按语境转换

bool b7 = b1; // 错误：被 explicit 修饰转换函数 B::operator bool() 的对象不可以隐式转换

bool b8 = static\_cast<bool>(b1); // OK：static\_cast 进行直接初始化

return 0;

}

### 1.16 friend 友元类和友元函数

* 能访问私有成员
* 破坏封装性
* 友元关系不可传递
* 友元关系的单向性
* 友元声明的形式及数量不受限制

### 1.17 **using 声明**

一条 using 声明 语句一次只引入命名空间的一个成员。它使得我们可以清楚知道程序中所引用的到底是哪个名字。如：

using namespace\_name::name;

### 1.18 **构造函数的 using 声明**

在 C++11 中，派生类能够重用其直接基类定义的构造函数。

using namespace\_name name;

尽量少使用 using 指示 污染命名空间

一般说来，使用 using 命令比使用 using 编译命令更安全，这是由于它****只导入了指定的名称****。如果该名称与局部名称发生冲突，编译器将****发出指示****。using编译命令导入所有的名称，包括可能并不需要的名称。如果与局部名称发生冲突，则****局部名称将覆盖名称空间版本****，而编译器****并不会发出警告****。另外，名称空间的开放性意味着名称空间的名称可能分散在多个地方，这使得难以准确知道添加了哪些名称。

尽量少使用 using 指示

using namespace std;

应该多使用 using 声明

int x;

std::cin >> x ;

std::cout << x << std::endl;

或者

using std::cin;

using std::cout;

using std::endl;

int x;

cin >> x;

cout << x << endl;

### 1.19 :: 范围解析运算符

#### **分类**

1. 全局作用域符（::name）：用于类型名称（类、类成员、成员函数、变量等）前，表示作用域为全局命名空间
2. 类作用域符（class::name）：用于表示指定类型的作用域范围是具体某个类的
3. 命名空间作用域符（namespace::name）:用于表示指定类型的作用域范围是具体某个命名空间的

int count = 0; // 全局（::）的 count

class A {public:

static int count; // 类 A 的 count（A::count）

};

int main() {

::count = 1; // 设置全局的 count 的值为 1

A::count = 2; // 设置类 A 的 count 为 2

int count = 0; // 局部的 count

count = 3; // 设置局部的 count 的值为 3

return 0;

}

### 1.20 enum 枚举类型

#### **限定作用域的枚举类型**

enum class open\_modes { input, output, append };

#### **不限定作用域的枚举类型**

enum color { red, yellow, green };enum { floatPrec = 6, doublePrec = 10 };

### 1.21 **decltype**

decltype 关键字用于检查实体的声明类型或表达式的类型及值分类。语法：

// 尾置返回允许我们在参数列表之后声明返回类型

template <typename It>auto fcn(It beg, It end) -> decltype(\*beg)

{

// 处理序列

return \*beg; // 返回序列中一个元素的引用

}// 为了使用模板参数成员，必须用 typenametemplate <typename It>auto fcn2(It beg, It end) -> typename remove\_reference<decltype(\*beg)>::type

{

// 处理序列

return \*beg; // 返回序列中一个元素的拷贝

}

### 1.22 引用

#### **左值引用**

常规引用，一般表示对象的身份。

#### **右值引用**

右值引用就是必须绑定到右值（一个临时对象、将要销毁的对象）的引用，一般表示对象的值。

右值引用可实现转移语义（Move Sementics）和精确传递（Perfect Forwarding），它的主要目的有两个方面：

* 消除两个对象交互时不必要的对象拷贝，节省运算存储资源，提高效率。
* 能够更简洁明确地定义泛型函数。

#### **引用折叠**

* X& &、X& &&、X&& & 可折叠成 X&
* X&& && 可折叠成 X&&

### 1.23 宏

* 宏定义可以实现类似于函数的功能，但是它终归不是函数，而宏定义中括弧中的“参数”也不是真的参数，在宏展开的时候对 “参数” 进行的是一对一的替换。

### 1.24 成员初始化列表

好处

* 更高效：少了一次调用默认构造函数的过程。
* 有些场合必须要用初始化列表：
  1. 常量成员，因为常量只能初始化不能赋值，所以必须放在初始化列表里面
  2. 引用类型，引用必须在定义的时候初始化，并且不能重新赋值，所以也要写在初始化列表里面
  3. 没有默认构造函数的类类型，因为使用初始化列表可以不必调用默认构造函数来初始化

initializer\_list 列表初始化

用花括号初始化器列表初始化一个对象，其中对应构造函数接受一个 std::initializer\_list 参数.

#include <iostream>

#include <vector>

#include <initializer\_list>

template <class T>struct S {

std::vector<T> v;

S(std::initializer\_list<T> l) : v(l) {

std::cout << "constructed with a " << l.size() << "-element list\n";

}

void append(std::initializer\_list<T> l) {

v.insert(v.end(), l.begin(), l.end());

}

std::pair<const T\*, std::size\_t> c\_arr() const {

return {&v[0], v.size()}; // 在 return 语句中复制列表初始化

// 这不使用 std::initializer\_list

}

};

template <typename T>void templated\_fn(T) {}

int main()

{

S<int> s = {1, 2, 3, 4, 5}; // 复制初始化

s.append({6, 7, 8}); // 函数调用中的列表初始化

std::cout << "The vector size is now " << s.c\_arr().second << " ints:\n";

for (auto n : s.v)

std::cout << n << ' ';

std::cout << '\n';

std::cout << "Range-for over brace-init-list: \n";

for (int x : {-1, -2, -3}) // auto 的规则令此带范围 for 工作

std::cout << x << ' ';

std::cout << '\n';

auto al = {10, 11, 12}; // auto 的特殊规则

std::cout << "The list bound to auto has size() = " << al.size() << '\n';

// templated\_fn({1, 2, 3}); // 编译错误！“ {1, 2, 3} ”不是表达式，

// 它无类型，故 T 无法推导

templated\_fn<std::initializer\_list<int>>({1, 2, 3}); // OK

templated\_fn<std::vector<int>>({1, 2, 3}); // 也 OK

}

### 1.25 虚函数

#### **1.25.1虚函数**

动态多态（运行期期/晚绑定）

虚函数：用 virtual 修饰成员函数，使其成为虚函数

****注意：****

* 普通函数（非类成员函数）不能是虚函数
* 静态函数（static）不能是虚函数
* 构造函数不能是虚函数（因为在调用构造函数时，虚表指针并没有在对象的内存空间中，必须要构造函数调用完成后才会形成虚表指针）
* 内联函数不能是表现多态性时的虚函数，解释见：[虚函数（virtual）可以是内联函数（inline）吗？](https://github.com/huihut/interview" \l "%E8%99%9A%E5%87%BD%E6%95%B0virtual%E5%8F%AF%E4%BB%A5%E6%98%AF%E5%86%85%E8%81%94%E5%87%BD%E6%95%B0inline%E5%90%97)

class Shape // 形状类

{public:

virtual double calcArea()

{

...

}

virtual ~Shape();

};class Circle : public Shape // 圆形类

{public:

virtual double calcArea();

...

};class Rect : public Shape // 矩形类

{public:

virtual double calcArea();

...

};int main()

{

Shape \* shape1 = new Circle(4.0);

Shape \* shape2 = new Rect(5.0, 6.0);

shape1->calcArea(); // 调用圆形类里面的方法

shape2->calcArea(); // 调用矩形类里面的方法

delete shape1;

shape1 = nullptr;

delete shape2;

shape2 = nullptr;

return 0;

}

#### **1.25.2虚析构函数**

虚析构函数是为了解决基类的指针指向派生类对象，并用基类的指针删除派生类对象。

class Shape

{public:

Shape(); // 构造函数不能是虚函数

virtual double calcArea();

virtual ~Shape(); // 虚析构函数

};class Circle : public Shape // 圆形类

{public:

virtual double calcArea();

...

};int main()

{

Shape \* shape1 = new Circle(4.0);

shape1->calcArea();

delete shape1; // 因为Shape有虚析构函数，所以delete释放内存时，先调用子类析构函数，再调用基类析构函数，防止内存泄漏。

shape1 = NULL;

return 0；

}

#### 1.25.3 纯虚函数

纯虚函数是一种特殊的虚函数，在基类中不能对虚函数给出有意义的实现，而把它声明为纯虚函数，它的实现留给该基类的派生类去做。

virtual int A() = 0;

#### 1.25.4 虚函数、纯虚函数

* 类里如果声明了虚函数，这个函数是实现的，哪怕是空实现，它的作用就是为了能让这个函数在它的子类里面可以被覆盖，这样的话，编译器就可以使用后期绑定来达到多态了。纯虚函数只是一个接口，是个函数的声明而已，它要留到子类里去实现。
* 虚函数在子类里面也可以不重载的；但纯虚函数必须在子类去实现。
* 虚函数的类用于 “实作继承”，继承接口的同时也继承了父类的实现。当然大家也可以完成自己的实现。纯虚函数关注的是接口的统一性，实现由子类完成。
* 带纯虚函数的类叫抽象类，这种类不能直接生成对象，而只有被继承，并重写其虚函数后，才能使用。抽象类被继承后，子类可以继续是抽象类，也可以是普通类。
* 虚基类是虚继承中的基类，具体见下文虚继承。https://blog.csdn.net/u012260238/article/details/53610462

#### 1.25.5 虚函数指针、虚函数表

* 虚函数指针：在含有虚函数类的对象中，指向虚函数表，在运行时确定。
* 虚函数表：在程序只读数据段（.rodata section，见：[目标文件存储结构](https://github.com/huihut/interview" \l "%E7%9B%AE%E6%A0%87%E6%96%87%E4%BB%B6%E5%AD%98%E5%82%A8%E7%BB%93%E6%9E%84)），存放虚函数指针，如果派生类实现了基类的某个虚函数，则在虚表中覆盖原本基类的那个虚函数指针，在编译时根据类的声明创建。

#### 1.25.6 虚继承

虚继承用于解决多继承条件下的菱形继承问题（浪费存储空间、存在二义性）。

底层实现原理与编译器相关，一般通过****虚基类指针****和****虚基类表****实现，每个虚继承的子类都有一个虚基类指针（占用一个指针的存储空间，4字节）和虚基类表（不占用类对象的存储空间）（需要强调的是，虚基类依旧会在子类里面存在拷贝，只是仅仅最多存在一份而已，并不是不在子类里面了）；当虚继承的子类被当做父类继承时，虚基类指针也会被继承。

实际上，vbptr 指的是虚基类表指针（virtual base table pointer），该指针指向了一个虚基类表（virtual table），虚表中记录了虚基类与本类的偏移地址；通过偏移地址，这样就找到了虚基类成员，而虚继承也不用像普通多继承那样维持着公共基类（虚基类）的两份同样的拷贝，节省了存储空间。

#### 1.25.7虚继承、虚函数

* 相同之处：都利用了虚指针（均占用类的存储空间）和虚表（均不占用类的存储空间）
* 不同之处：
  + 虚继承
    - 虚基类依旧存在继承类中，只占用存储空间
    - 虚基类表存储的是虚基类相对直接继承类的偏移
  + 虚函数
    - 虚函数不占用存储空间
    - 虚函数表存储的是虚函数地址

#### 1.25.8 模板类、成员模板、虚函数

* 模板类中可以使用虚函数
* 一个类（无论是普通类还是类模板）的成员模板（本身是模板的成员函数）不能是虚函数

#### 1.25.9 抽象类、接口类、聚合类

* 抽象类：含有纯虚函数的类
* 接口类：仅含有纯虚函数的抽象类
* 聚合类：用户可以直接访问其成员，并且具有特殊的初始化语法形式。满足如下特点：
  + 所有成员都是 public
  + 没有定义任何构造函数
  + 没有类内初始化
  + 没有基类，也没有 virtual 函数

### 1.26 **内存分配和管理**

#### 1.26.1 malloc、calloc、realloc、alloca

1. malloc：申请指定字节数的内存。申请到的内存中的初始值不确定。
2. calloc：为指定长度的对象，分配能容纳其指定个数的内存。申请到的内存的每一位（bit）都初始化为 0。
3. realloc：更改以前分配的内存长度（增加或减少）。当增加长度时，可能需将以前分配区的内容移到另一个足够大的区域，而新增区域内的初始值则不确定。
4. alloca：在栈上申请内存。程序在出栈的时候，会自动释放内存。但是需要注意的是，alloca 不具可移植性, 而且在没有传统堆栈的机器上很难实现。alloca 不宜使用在必须广泛移植的程序中。C99 中支持变长数组 (VLA)，可以用来替代 alloca。

#### 1.26.2 malloc、free

用于分配、释放内存

char \*str = (char\*) malloc(100);

assert(str != nullptr);

free(p);

p = nullptr;

#### 1.26.3 new、delete

1. new / new[]：完成两件事，先底层调用 malloc 分配了内存，然后调用构造函数（创建对象）。
2. delete/delete[]：也完成两件事，先调用析构函数（清理资源），然后底层调用 free 释放空间。
3. new 在申请内存时会自动计算所需字节数，而 malloc 则需我们自己输入申请内存空间的字节数。

int main()

{

T\* t = new T(); // 先内存分配 ，再构造函数

delete t; // 先析构函数，再内存释放

return 0;

}

#### 1.26.4 定位 new

定位 new（placement new）允许我们向 new 传递额外的地址参数，从而在预先指定的内存区域创建对象。

new (place\_address) typenew (place\_address) type (initializers)new (place\_address) type [size]new (place\_address) type [size] { braced initializer list }

* place\_address 是个指针
* initializers 提供一个（可能为空的）以逗号分隔的初始值列表

delete this 合法吗？合法，但：

1. 必须保证 this 对象是通过 new（不是 new[]、不是 placement new、不是栈上、不是全局、不是其他对象成员）分配的
2. 必须保证调用 delete this 的成员函数是最后一个调用 this 的成员函数
3. 必须保证成员函数的 delete this 后面没有调用 this 了
4. 必须保证 delete this 后没有人使用了

### 1.27 **在堆上（栈上）生成对象的类**

#### **只能在堆上**

方法：将析构函数设置为私有

原因：C++ 是静态绑定语言，编译器管理栈上对象的生命周期，编译器在为类对象分配栈空间时，会先检查类的析构函数的访问性。若析构函数不可访问，则不能在栈上创建对象。

#### **只能在栈上**

方法：将 new 和 delete 重载为私有

原因：在堆上生成对象，使用 new 关键词操作，其过程分为两阶段：第一阶段，使用 new 在堆上寻找可用内存，分配给对象；第二阶段，调用构造函数生成对象。将 new 操作设置为私有，那么第一阶段就无法完成，就不能够在堆上生成对象。

### 1.28 智能指针

#### **C++ 标准库（STL）中**

头文件：#include <memory>

#### **C++ 98**

std::auto\_ptr<std::string> ps (new std::string(str))；

#### **C++ 11**

1. shared\_ptr
2. unique\_ptr
3. weak\_ptr
4. auto\_ptr（被 C++11 弃用）

* Class shared\_ptr 实现共享式拥有（shared ownership）概念。多个智能指针指向相同对象，该对象和其相关资源会在 “最后一个 reference 被销毁” 时被释放。为了在结构较复杂的情景中执行上述工作，标准库提供 weak\_ptr、bad\_weak\_ptr 和 enable\_shared\_from\_this 等辅助类。
* Class unique\_ptr 实现独占式拥有（exclusive ownership）或严格拥有（strict ownership）概念，保证同一时间内只有一个智能指针可以指向该对象。你可以移交拥有权。它对于避免内存泄漏（resource leak）——如 new 后忘记 delete ——特别有用。

##### **shared\_ptr**

多个智能指针可以共享同一个对象，对象的最末一个拥有着有责任销毁对象，并清理与该对象相关的所有资源。

* 支持定制型删除器（custom deleter），可防范 Cross-DLL 问题（对象在动态链接库（DLL）中被 new 创建，却在另一个 DLL 内被 delete 销毁）、自动解除互斥锁

##### **weak\_ptr**

weak\_ptr 允许你共享但不拥有某对象，一旦最末一个拥有该对象的智能指针失去了所有权，任何 weak\_ptr 都会自动成空（empty）。因此，在 default 和 copy 构造函数之外，weak\_ptr 只提供 “接受一个 shared\_ptr” 的构造函数。

* 可打破环状引用（cycles of references，两个其实已经没有被使用的对象彼此互指，使之看似还在 “被使用” 的状态）的问题

##### **unique\_ptr**

unique\_ptr 是 C++11 才开始提供的类型，是一种在异常时可以帮助避免资源泄漏的智能指针。采用独占式拥有，意味着可以确保一个对象和其相应的资源同一时间只被一个 pointer 拥有。一旦拥有着被销毁或编程 empty，或开始拥有另一个对象，先前拥有的那个对象就会被销毁，其任何相应资源亦会被释放。

* unique\_ptr 用于取代 auto\_ptr

##### **auto\_ptr**

被 c++11 弃用，原因是缺乏语言特性如 “针对构造和赋值” 的 std::move 语义，以及其他瑕疵。

##### **auto\_ptr 与 unique\_ptr 比较**

* auto\_ptr 可以赋值拷贝，复制拷贝后所有权转移；unqiue\_ptr 无拷贝赋值语义，但实现了move 语义；
* auto\_ptr 对象不能管理数组（析构调用 delete），unique\_ptr 可以管理数组（析构调用 delete[] ）；

### **1.29强制类型转换运算符**

#### **static\_cast**

* 用于非多态类型的转换
* 不执行运行时类型检查（转换安全性不如 dynamic\_cast）
* 通常用于转换数值数据类型（如 float -> int）
* 可以在整个类层次结构中移动指针，子类转化为父类安全（向上转换），父类转化为子类不安全（因为子类可能有不在父类的字段或方法）

向上转换是一种隐式转换。

#### **dynamic\_cast**

* 用于多态类型的转换
* 执行行运行时类型检查
* 只适用于指针或引用
* 对不明确的指针的转换将失败（返回 nullptr），但不引发异常
* 可以在整个类层次结构中移动指针，包括向上转换、向下转换

#### **const\_cast**

* 用于删除 const、volatile 和 \_\_unaligned 特性（如将 const int 类型转换为 int 类型 ）

#### **reinterpret\_cast**

* 用于位的简单重新解释
* 滥用 reinterpret\_cast 运算符可能很容易带来风险。 除非所需转换本身是低级别的，否则应使用其他强制转换运算符之一。
* 允许将任何指针转换为任何其他指针类型（如 char\* 到 int\* 或 One\_class\* 到 Unrelated\_class\* 之类的转换，但其本身并不安全）
* 也允许将任何整数类型转换为任何指针类型以及反向转换。
* reinterpret\_cast 运算符不能丢掉 const、volatile 或 \_\_unaligned 特性。
* reinterpret\_cast 的一个实际用途是在哈希函数中，即，通过让两个不同的值几乎不以相同的索引结尾的方式将值映射到索引。

#### **bad\_cast**

* 由于强制转换为引用类型失败，dynamic\_cast 运算符引发 bad\_cast 异常。

try {

Circle& ref\_circle = dynamic\_cast<Circle&>(ref\_shape);

} catch (bad\_cast b) {

cout << "Caught: " << b.what();

}

### 1.30运行时类型信息 (RTTI)

#### **dynamic\_cast**

* 用于多态类型的转换

#### **typeid**

* typeid 运算符允许在运行时确定对象的类型
* type\_id 返回一个 type\_info 对象的引用
* 如果想通过基类的指针获得派生类的数据类型，基类必须带有虚函数
* 只能获取对象的实际类型

#### **type\_info**

* type\_info 类描述编译器在程序中生成的类型信息。 此类的对象可以有效存储指向类型的名称的指针。 type\_info 类还可存储适合比较两个类型是否相等或比较其排列顺序的编码值。 类型的编码规则和排列顺序是未指定的，并且可能因程序而异。
* 头文件：typeinfo

class Flyable // 能飞的

{public:

virtual void takeoff() = 0; // 起飞

virtual void land() = 0; // 降落

};class Bird : public Flyable // 鸟

{public:

void foraging() {...} // 觅食

virtual void takeoff() {...}

virtual void land() {...}

};class Plane : public Flyable // 飞机

{public:

void carry() {...} // 运输

virtual void take off() {...}

virtual void land() {...}

};

class type\_info

{public:

const char\* name() const;

bool operator == (const type\_info & rhs) const;

bool operator != (const type\_info & rhs) const;

int before(const type\_info & rhs) const;

virtual ~type\_info();private:

...

};

class doSomething(Flyable \*obj) // 做些事情

{

obj->takeoff();

cout << typeid(\*obj).name() << endl; // 输出传入对象类型（"class Bird" or "class Plane"）

if(typeid(\*obj) == typeid(Bird)) // 判断对象类型

{

Bird \*bird = dynamic\_cast<Bird \*>(obj); // 对象转化

bird->foraging();

}

obj->land();

};

### 1.31 **Effective C++**

1. 视 C++ 为一个语言联邦（C、Object-Oriented C++、Template C++、STL）
2. 宁可以编译器替换预处理器（尽量以 const、enum、inline 替换 #define）
3. 尽可能使用 const
4. 确定对象被使用前已先被初始化（构造时赋值（copy 构造函数）比 default 构造后赋值（copy assignment）效率高）
5. 了解 C++ 默默编写并调用哪些函数（编译器暗自为 class 创建 default 构造函数、copy 构造函数、copy assignment 操作符、析构函数）
6. 若不想使用编译器自动生成的函数，就应该明确拒绝（将不想使用的成员函数声明为 private，并且不予实现）
7. 为多态基类声明 virtual 析构函数（如果 class 带有任何 virtual 函数，它就应该拥有一个 virtual 析构函数）
8. 别让异常逃离析构函数（析构函数应该吞下不传播异常，或者结束程序，而不是吐出异常；如果要处理异常应该在非析构的普通函数处理）
9. 绝不在构造和析构过程中调用 virtual 函数（因为这类调用从不下降至 derived class）
10. 令 operator= 返回一个 reference to \*this （用于连锁赋值）
11. 在 operator= 中处理 “自我赋值”
12. 赋值对象时应确保复制 “对象内的所有成员变量” 及 “所有 base class 成分”（调用基类复制构造函数）
13. 以对象管理资源（资源在构造函数获得，在析构函数释放，建议使用智能指针，资源取得时机便是初始化时机（Resource Acquisition Is Initialization，RAII））
14. 在资源管理类中小心 copying 行为（普遍的 RAII class copying 行为是：抑制 copying、引用计数、深度拷贝、转移底部资源拥有权（类似 auto\_ptr））
15. 在资源管理类中提供对原始资源（raw resources）的访问（对原始资源的访问可能经过显式转换或隐式转换，一般而言显示转换比较安全，隐式转换对客户比较方便）
16. 成对使用 new 和 delete 时要采取相同形式（new 中使用 [] 则 delete []，new 中不使用 [] 则 delete）
17. 以独立语句将 newed 对象存储于（置入）智能指针（如果不这样做，可能会因为编译器优化，导致难以察觉的资源泄漏）
18. 让接口容易被正确使用，不易被误用（促进正常使用的办法：接口的一致性、内置类型的行为兼容；阻止误用的办法：建立新类型，限制类型上的操作，约束对象值、消除客户的资源管理责任）
19. 设计 class 犹如设计 type，需要考虑对象创建、销毁、初始化、赋值、值传递、合法值、继承关系、转换、一般化等等。
20. 宁以 pass-by-reference-to-const 替换 pass-by-value （前者通常更高效、避免切割问题（slicing problem），但不适用于内置类型、STL迭代器、函数对象）
21. 必须返回对象时，别妄想返回其 reference（绝不返回 pointer 或 reference 指向一个 local stack 对象，或返回 reference 指向一个 heap-allocated 对象，或返回 pointer 或 reference 指向一个 local static 对象而有可能同时需要多个这样的对象。）
22. 将成员变量声明为 private（为了封装、一致性、对其读写精确控制等）
23. 宁以 non-member、non-friend 替换 member 函数（可增加封装性、包裹弹性（packaging flexibility）、机能扩充性）
24. 若所有参数（包括被this指针所指的那个隐喻参数）皆须要类型转换，请为此采用 non-member 函数
25. 考虑写一个不抛异常的 swap 函数
26. 尽可能延后变量定义式的出现时间（可增加程序清晰度并改善程序效率）
27. 尽量少做转型动作（旧式：(T)expression、T(expression)；新式：const\_cast<T>(expression)、dynamic\_cast<T>(expression)、reinterpret\_cast<T>(expression)、static\_cast<T>(expression)、；尽量避免转型、注重效率避免 dynamic\_casts、尽量设计成无需转型、可把转型封装成函数、宁可用新式转型）
28. 避免使用 handles（包括 引用、指针、迭代器）指向对象内部（以增加封装性、使 const 成员函数的行为更像 const、降低 “虚吊号码牌”（dangling handles，如悬空指针等）的可能性）
29. 为 “异常安全” 而努力是值得的（异常安全函数（Exception-safe functions）即使发生异常也不会泄露资源或允许任何数据结构败坏，分为三种可能的保证：基本型、强列型、不抛异常型）
30. 透彻了解 inlining 的里里外外（inlining 在大多数 C++ 程序中是编译期的行为；inline 函数是否真正 inline，取决于编译器；大部分编译器拒绝太过复杂（如带有循环或递归）的函数 inlining，而所有对 virtual 函数的调用（除非是最平淡无奇的）也都会使 inlining 落空；inline 造成的代码膨胀可能带来效率损失；inline 函数无法随着程序库的升级而升级）
31. 将文件间的编译依存关系降至最低（如果使用 object references 或 object pointers 可以完成任务，就不要使用 objects；如果能过够，尽量以 class 声明式替换 class 定义式；为声明式和定义式提供不同的头文件）
32. 确定你的 public 继承塑模出 is-a（是一种）关系（适用于 base classes 身上的每一件事情一定适用于 derived classes 身上，因为每一个 derived class 对象也都是一个 base class 对象）
33. 避免遮掩继承而来的名字（可使用 using 声明式或转交函数（forwarding functions）来让被遮掩的名字再见天日）
34. 区分接口继承和实现继承（在 public 继承之下，derived classes 总是继承 base class 的接口；pure virtual 函数只具体指定接口继承；非纯 impure virtual 函数具体指定接口继承及缺省实现继承；non-virtual 函数具体指定接口继承以及强制性实现继承）
35. 考虑 virtual 函数以外的其他选择（如 Template Method 设计模式的 non-virtual interface（NVI）手法，将 virtual 函数替换为 “函数指针成员变量”，以 tr1::function 成员变量替换 virtual 函数，将继承体系内的 virtual 函数替换为另一个继承体系内的 virtual 函数）
36. 绝不重新定义继承而来的 non-virtual 函数
37. 绝不重新定义继承而来的缺省参数值，因为缺省参数值是静态绑定（statically bound），而 virtual 函数却是动态绑定（dynamically bound）
38. 通过复合塑模 has-a（有一个）或 “根据某物实现出”（在应用域（application domain），复合意味 has-a（有一个）；在实现域（implementation domain），复合意味着 is-implemented-in-terms-of（根据某物实现出））
39. 明智而审慎地使用 private 继承（private 继承意味着 is-implemented-in-terms-of（根据某物实现出），尽可能使用复合，当 derived class 需要访问 protected base class 的成员，或需要重新定义继承而来的时候 virtual 函数，或需要 empty base 最优化时，才使用 private 继承）
40. 明智而审慎地使用多重继承（多继承比单一继承复杂，可能导致新的歧义性，以及对 virtual 继承的需要，但确有正当用途，如 “public 继承某个 interface class” 和 “private 继承某个协助实现的 class”；virtual 继承可解决多继承下菱形继承的二义性问题，但会增加大小、速度、初始化及赋值的复杂度等等成本）
41. 了解隐式接口和编译期多态（class 和 templates 都支持接口（interfaces）和多态（polymorphism）；class 的接口是以签名为中心的显式的（explicit），多态则是通过 virtual 函数发生于运行期；template 的接口是奠基于有效表达式的隐式的（implicit），多态则是通过 template 具现化和函数重载解析（function overloading resolution）发生于编译期）
42. 了解 typename 的双重意义（声明 template 类型参数是，前缀关键字 class 和 typename 的意义完全相同；请使用关键字 typename 标识嵌套从属类型名称，但不得在基类列（base class lists）或成员初值列（member initialization list）内以它作为 base class 修饰符）
43. 学习处理模板化基类内的名称（可在 derived class templates 内通过 this-> 指涉 base class templates 内的成员名称，或藉由一个明白写出的 “base class 资格修饰符” 完成）
44. 将与参数无关的代码抽离 templates（因类型模板参数（non-type template parameters）而造成代码膨胀往往可以通过函数参数或 class 成员变量替换 template 参数来消除；因类型参数（type parameters）而造成的代码膨胀往往可以通过让带有完全相同二进制表述（binary representations）的实现类型（instantiation types）共享实现码）
45. 运用成员函数模板接受所有兼容类型（请使用成员函数模板（member function templates）生成 “可接受所有兼容类型” 的函数；声明 member templates 用于 “泛化 copy 构造” 或 “泛化 assignment 操作” 时还需要声明正常的 copy 构造函数和 copy assignment 操作符）
46. 需要类型转换时请为模板定义非成员函数（当我们编写一个 class template，而它所提供之 “与此 template 相关的” 函数支持 “所有参数之隐式类型转换” 时，请将那些函数定义为 “class template 内部的 friend 函数”）
47. 请使用 traits classes 表现类型信息（traits classes 通过 templates 和 “templates 特化” 使得 “类型相关信息” 在编译期可用，通过重载技术（overloading）实现在编译期对类型执行 if...else 测试）
48. 认识 template 元编程（模板元编程（TMP，template metaprogramming）可将工作由运行期移往编译期，因此得以实现早期错误侦测和更高的执行效率；TMP 可被用来生成 “给予政策选择组合”（based on combinations of policy choices）的客户定制代码，也可用来避免生成对某些特殊类型并不适合的代码）
49. 了解 new-handler 的行为（set\_new\_handler 允许客户指定一个在内存分配无法获得满足时被调用的函数；nothrow new 是一个颇具局限的工具，因为它只适用于内存分配（operator new），后继的构造函数调用还是可能抛出异常）
50. 了解 new 和 delete 的合理替换时机（为了检测运用错误、收集动态分配内存之使用统计信息、增加分配和归还速度、降低缺省内存管理器带来的空间额外开销、弥补缺省分配器中的非最佳齐位、将相关对象成簇集中、获得非传统的行为）
51. 编写 new 和 delete 时需固守常规（operator new 应该内涵一个无穷循环，并在其中尝试分配内存，如果它无法满足内存需求，就应该调用 new-handler，它也应该有能力处理 0 bytes 申请，class 专属版本则还应该处理 “比正确大小更大的（错误）申请”；operator delete 应该在收到 null 指针时不做任何事，class 专属版本则还应该处理 “比正确大小更大的（错误）申请”）
52. 写了 placement new 也要写 placement delete（当你写一个 placement operator new，请确定也写出了对应的 placement operator delete，否则可能会发生隐微而时断时续的内存泄漏；当你声明 placement new 和 placement delete，请确定不要无意识（非故意）地遮掩了它们地正常版本）
53. 不要轻忽编译器的警告
54. 让自己熟悉包括 TR1 在内的标准程序库（TR1，C++ Technical Report 1，C++11 标准的草稿文件）
55. 让自己熟悉 Boost（准标准库）

### **1.32 Google C++ Style Guide**

英文：Google C++ Style Guide

https://google.github.io/styleguide/cppguide.html

中文：C++ 风格指南

<https://zh-google-styleguide.readthedocs.io/en/latest/google-cpp-styleguide/contents/>



<https://blog.csdn.net/voidccc/article/details/37599203>

### 1.33 C++ lambda表达式与函数对象

lambda表达式

我们先从简答的例子开始，我们定义一个可以输出字符串的lambda表达式，表达式一般都是从方括号[]开始，然后结束于花括号{}，花括号里面就像定义函数那样，包含了lamdba表达式体：

// 定义简单的lambda表达式auto basicLambda = [] { cout << "Hello, world!" << endl; };// 调用

basicLambda(); // 输出：Hello, world!

// 指明返回类型auto add = [](int a, int b) -> int { return a + b; };// 自动推断返回类型auto multiply = [](int a, int b) { return a \* b; };

int sum = add(2, 5); // 输出：7int product = multiply(2, 5); // 输出：10

int main(){

int x = 10;

auto add\_x = [x](int a) mutable { x \*= 2; return a + x; }; // 复制捕捉x

cout << add\_x(10) << endl; // 输出 30

return 0;

}

闲话少说，归入正题，捕获的方式可以是引用也可以是复制，但是具体说来会有以下几种情况来捕获其所在作用域中的变量：

* []：默认不捕获任何变量；
* [=]：默认以值捕获所有变量；
* [&]：默认以引用捕获所有变量；
* [x]：仅以值捕获x，其它变量不捕获；
* [&x]：仅以引用捕获x，其它变量不捕获；
* [=, &x]：默认以值捕获所有变量，但是x是例外，通过引用捕获；
* [&, x]：默认以引用捕获所有变量，但是x是例外，通过值捕获；
* [this]：通过引用捕获当前对象（其实是复制指针）；
* [\*this]：通过传值方式捕获当前对象；

## STL

### 2.1参考链接

网站：<https://github.com/huihut/interview/blob/master/STL/STL.md>

### 2.2组成

* 容器（containers）
* 算法（algorithms）
* 迭代器（iterators）
* 仿函数（functors）
* 配接器（adapters）
* 空间配置器（allocator）

### 2.3 容器（containers）

array

array 是固定大小的顺序容器，它们保存了一个以严格的线性顺序排列的特定数量的元素。

Vector

vector 是表示可以改变大小的数组的序列容器。

deque

deque（['dek]）（双端队列）是double-ended queue 的一个不规则缩写。deque是具有动态大小的序列容器，可以在两端（前端或后端）扩展或收缩。

forward\_list

forward\_list（单向链表）是序列容器，允许在序列中的任何地方进行恒定的时间插入和擦除操作。

list

list，双向链表，是序列容器，允许在序列中的任何地方进行常数时间插入和擦除操作，并在两个方向上进行迭代。

stack

stack 是一种容器适配器，用于在LIFO（后进先出）的操作，其中元素仅从容器的一端插入和提取。

queue

queue 是一种容器适配器，用于在FIFO（先入先出）的操作，其中元素插入到容器的一端并从另一端提取。

priority\_queue

set

set 是按照特定顺序存储唯一元素的容器。

multiset

map

map 是关联容器，按照特定顺序存储由 key value (键值) 和 mapped value (映射值) 组合形成的元素。

#### STL 容器

| 容器 | 底层数据结构 | 时间复杂度 | 有无序 | 可不可重复 | 其他 |
| --- | --- | --- | --- | --- | --- |
| [array](https://github.com/huihut/interview/tree/master/STL" \l "array) | 数组 | 随机读改 O(1) | 无序 | 可重复 | 支持快速随机访问 |
| [vector](https://github.com/huihut/interview/tree/master/STL" \l "vector) | 数组 | 随机读改、尾部插入、尾部删除 O(1) 头部插入、头部删除 O(n) | 无序 | 可重复 | 支持快速随机访问 |
| [list](https://github.com/huihut/interview/tree/master/STL" \l "list) | 双向链表 | 插入、删除 O(1) 随机读改 O(n) | 无序 | 可重复 | 支持快速增删 |
| [deque](https://github.com/huihut/interview/tree/master/STL" \l "deque) | 双端队列 | 头尾插入、头尾删除 O(1) | 无序 | 可重复 | 一个中央控制器 + 多个缓冲区，支持首尾快速增删，支持随机访问 |
| [stack](https://github.com/huihut/interview/tree/master/STL" \l "stack) | deque / list | 顶部插入、顶部删除 O(1) | 无序 | 可重复 | deque 或 list 封闭头端开口，不用 vector 的原因应该是容量大小有限制，扩容耗时 |
| [queue](https://github.com/huihut/interview/tree/master/STL" \l "queue) | deque / list | 尾部插入、头部删除 O(1) | 无序 | 可重复 | deque 或 list 封闭头端开口，不用 vector 的原因应该是容量大小有限制，扩容耗时 |
| [priority\_queue](https://github.com/huihut/interview/tree/master/STL" \l "priority_queue) | vector + max-heap | 插入、删除 O(log2n) | 有序 | 可重复 | vector容器+heap处理规则 |
| [set](https://github.com/huihut/interview/tree/master/STL" \l "set) | 红黑树 | 插入、删除、查找 O(log2n) | 有序 | 不可重复 |  |
| [multiset](https://github.com/huihut/interview/tree/master/STL" \l "multiset) | 红黑树 | 插入、删除、查找 O(log2n) | 有序 | 可重复 |  |
| [map](https://github.com/huihut/interview/tree/master/STL" \l "map) | 红黑树 | 插入、删除、查找 O(log2n) | 有序 | 不可重复 |  |
| [multimap](https://github.com/huihut/interview/tree/master/STL" \l "multimap) | 红黑树 | 插入、删除、查找 O(log2n) | 有序 | 可重复 |  |
| hash\_set | 哈希表 | 插入、删除、查找 O(1) 最差 O(n) | 无序 | 不可重复 |  |
| hash\_multiset | 哈希表 | 插入、删除、查找 O(1) 最差 O(n) | 无序 | 可重复 |  |
| hash\_map | 哈希表 | 插入、删除、查找 O(1) 最差 O(n) | 无序 | 不可重复 |  |
| hash\_multimap | 哈希表 | 插入、删除、查找 O(1) 最差 O(n) | 无序 | 可重复 |  |

#### Stl 算法

// 简单查找算法，要求输入迭代器（input iterator）

find(beg, end, val); // 返回一个迭代器，指向输入序列中第一个等于 val 的元素，未找到返回 end

find\_if(beg, end, unaryPred); // 返回一个迭代器，指向第一个满足 unaryPred 的元素，未找到返回 end

find\_if\_not(beg, end, unaryPred); // 返回一个迭代器，指向第一个令 unaryPred 为 false 的元素，未找到返回 end

count(beg, end, val); // 返回一个计数器，指出 val 出现了多少次

count\_if(beg, end, unaryPred); // 统计有多少个元素满足 unaryPred

all\_of(beg, end, unaryPred); // 返回一个 bool 值，判断是否所有元素都满足 unaryPred

any\_of(beg, end, unaryPred); // 返回一个 bool 值，判断是否任意（存在）一个元素满足 unaryPred

none\_of(beg, end, unaryPred); // 返回一个 bool 值，判断是否所有元素都不满足 unaryPred

// 查找重复值的算法，传入向前迭代器（forward iterator）

adjacent\_find(beg, end); // 返回指向第一对相邻重复元素的迭代器，无相邻元素则返回 end

adjacent\_find(beg, end, binaryPred); // 返回指向第一对相邻重复元素的迭代器，无相邻元素则返回 end

search\_n(beg, end, count, val); // 返回一个迭代器，从此位置开始有 count 个相等元素，不存在则返回 end

search\_n(beg, end, count, val, binaryPred); // 返回一个迭代器，从此位置开始有 count 个相等元素，不存在则返回 end

// 查找子序列算法，除 find\_first\_of（前两个输入迭代器，后两个前向迭代器） 外，都要求两个前向迭代器

search(beg1, end1, beg2, end2); // 返回第二个输入范围（子序列）在爹一个输入范围中第一次出现的位置，未找到则返回 end1

search(beg1, end1, beg2, end2, binaryPred); // 返回第二个输入范围（子序列）在爹一个输入范围中第一次出现的位置，未找到则返回 end1

find\_first\_of(beg1, end1, beg2, end2); // 返回一个迭代器，指向第二个输入范围中任意元素在第一个范围中首次出现的位置，未找到则返回end1

find\_first\_of(beg1, end1, beg2, end2, binaryPred); // 返回一个迭代器，指向第二个输入范围中任意元素在第一个范围中首次出现的位置，未找到则返回end1

find\_end(beg1, end1, beg2, end2); // 类似 search，但返回的最后一次出现的位置。如果第二个输入范围为空，或者在第一个输入范围为空，或者在第一个输入范围中未找到它，则返回 end1

find\_end(beg1, end1, beg2, end2, binaryPred); // 类似 search，但返回的最后一次出现的位置。如果第二个输入范围为空，或者在第一个输入范围为空，或者在第一个输入范围中未找到它，则返回 end1

// 其他只读算法，传入输入迭代器

for\_each(beg, end, unaryOp); // 对输入序列中的每个元素应用可调用对象 unaryOp，unaryOp 的返回值被忽略

mismatch(beg1, end1, beg2); // 比较两个序列中的元素。返回一个迭代器的 pair，表示两个序列中第一个不匹配的元素

mismatch(beg1, end1, beg2, binaryPred); // 比较两个序列中的元素。返回一个迭代器的 pair，表示两个序列中第一个不匹配的元素

equal(beg1, end1, beg2); // 比较每个元素，确定两个序列是否相等。

equal(beg1, end1, beg2, binaryPred); // 比较每个元素，确定两个序列是否相等。

// 二分搜索算法，传入前向迭代器或随机访问迭代器（random-access iterator），要求序列中的元素已经是有序的。通过小于运算符（<）或 comp 比较操作实现比较。

lower\_bound(beg, end, val); // 返回一个非递减序列 [beg, end) 中的第一个大于等于值 val 的位置的迭代器，不存在则返回 end

lower\_bound(beg, end, val, comp); // 返回一个非递减序列 [beg, end) 中的第一个大于等于值 val 的位置的迭代器，不存在则返回 end

upper\_bound(beg, end, val); // 返回一个非递减序列 [beg, end) 中第一个大于 val 的位置的迭代器，不存在则返回 end

upper\_bound(beg, end, val, comp); // 返回一个非递减序列 [beg, end) 中第一个大于 val 的位置的迭代器，不存在则返回 end

equal\_range(beg, end, val); // 返回一个 pair，其 first 成员是 lower\_bound 返回的迭代器，其 second 成员是 upper\_bound 返回的迭代器

binary\_search(beg, end, val); // 返回一个 bool 值，指出序列中是否包含等于 val 的元素。对于两个值 x 和 y，当 x 不小于 y 且 y 也不小于 x 时，认为它们相等。

// 只写不读算法，要求输出迭代器（output iterator）

fill(beg, end, val); // 将 val 赋予每个元素，返回 void

fill\_n(beg, cnt, val); // 将 val 赋予 cnt 个元素，返回指向写入到输出序列最有一个元素之后位置的迭代器

genetate(beg, end, Gen); // 每次调用 Gen() 生成不同的值赋予每个序列，返回 void

genetate\_n(beg, cnt, Gen); // 每次调用 Gen() 生成不同的值赋予 cnt 个序列，返回指向写入到输出序列最有一个元素之后位置的迭代器

// 使用输入迭代器的写算法，读取一个输入序列，将值写入到一个输出序列（dest）中

copy(beg, end, dest); // 从输入范围将元素拷贝所有元素到 dest 指定定的目的序列

copy\_if(beg, end, dest, unaryPred); // 从输入范围将元素拷贝满足 unaryPred 的元素到 dest 指定定的目的序列

copy\_n(beg, n, dest); // 从输入范围将元素拷贝前 n 个元素到 dest 指定定的目的序列

move(beg, end, dest); // 对输入序列中的每个元素调用 std::move，将其移动到迭代器 dest 开始始的序列中

transform(beg, end, dest, unaryOp); // 调用给定操作（一元操作），并将结果写到dest中

transform(beg, end, beg2, dest, binaryOp); // 调用给定操作（二元操作），并将结果写到dest中

replace\_copy(beg, end, dest, old\_val, new\_val); // 将每个元素拷贝到 dest，将等于 old\_val 的的元素替换为 new\_val

replace\_copy\_if(beg, end, dest, unaryPred, new\_val); // 将每个元素拷贝到 dest，将满足 unaryPred 的的元素替换为 new\_val

merge(beg1, end1, beg2, end2, dest); // 两个输入序列必须都是有序的，用 < 运算符将合并后的序列写入到 dest 中

merge(beg1, end1, beg2, end2, dest, comp); // 两个输入序列必须都是有序的，使用给定的比较操作（comp）将合并后的序列写入到 dest 中

// 使用前向迭代器的写算法，要求前向迭代器

iter\_swap(iter1, iter2); // 交换 iter1 和 iter2 所表示的元素，返回 void

swap\_ranges(beg1, end1, beg2); // 将输入范围中所有元素与 beg2 开始的第二个序列中所有元素进行交换。返回递增后的的 beg2，指向最后一个交换元素之后的位置。

replace(beg, end, old\_val, new\_val); // 用 new\_val 替换等于 old\_val 的每个匹配元素

replace\_if(beg, end, unaryPred, new\_val); // 用 new\_val 替换满足 unaryPred 的每个匹配元素

// 使用双向迭代器的写算法，要求双向选代器（bidirectional iterator）

copy\_backward(beg, end, dest); // 从输入范围中拷贝元素到指定目的位置。如果范围为空,则返回值为 dest；否则，返回值表示从 \*beg 中拷贝或移动的元素。

move\_backward(beg, end, dest); // 从输入范围中移动元素到指定目的位置。如果范围为空,则返回值为 dest；否则,返回值表示从 \*beg 中拷贝或移动的元素。

inplace\_merge(beg, mid, end); // 将同一个序列中的两个有序子序列合并为单一的有序序列。beg 到 mid 间的子序列和 mid 到 end 间的子序列被合并，并被写入到原序列中。使用 < 比较元素。

inplace\_merge(beg, mid, end, comp); // 将同一个序列中的两个有序子序列合并为单一的有序序列。beg 到 mid 间的子序列和 mid 到 end 间的子序列被合并，并被写入到原序列中。使用给定的 comp 操作。

// 划分算法，要求双向选代器（bidirectional iterator）

is\_partitioned(beg, end, unaryPred); // 如果所有满足谓词 unaryPred 的元素都在不满足 unarypred 的元素之前，则返回 true。若序列为空，也返回 true

partition\_copy(beg, end, dest1, dest2, unaryPred); // 将满足 unaryPred 的元素拷贝到到 dest1，并将不满足 unaryPred 的元素拷贝到到 dest2。返回一个迭代器 pair，其 first 成员表示拷贝到 dest1 的的元素的末尾，second 表示拷贝到 dest2 的元素的末尾。

partitioned\_point(beg, end, unaryPred); // 输入序列必须是已经用 unaryPred 划分过的。返回满足 unaryPred 的范围的尾后迭代器。如果返回的迭代器不是 end，则它指向的元素及其后的元素必须都不满足 unaryPred

stable\_partition(beg, end, unaryPred); // 使用 unaryPred 划分输入序列。满足 unaryPred 的元素放置在序列开始，不满足的元素放在序列尾部。返回一个迭代器，指向最后一个满足 unaryPred 的元素之后的位置如果所有元素都不满足 unaryPred，则返回 beg

partition(beg, end, unaryPred); // 使用 unaryPred 划分输入序列。满足 unaryPred 的元素放置在序列开始，不满足的元素放在序列尾部。返回一个迭代器，指向最后一个满足 unaryPred 的元素之后的位置如果所有元素都不满足 unaryPred，则返回 beg

// 排序算法，要求随机访问迭代器（random-access iterator）

sort(beg, end); // 排序整个范围

stable\_sort(beg, end); // 排序整个范围（稳定排序）

sort(beg, end, comp); // 排序整个范围

stable\_sort(beg, end, comp); // 排序整个范围（稳定排序）

is\_sorted(beg, end); // 返回一个 bool 值，指出整个输入序列是否有序

is\_sorted(beg, end, comp); // 返回一个 bool 值，指出整个输入序列是否有序

is\_sorted\_until(beg, end); // 在输入序列中査找最长初始有序子序列，并返回子序列的尾后迭代器

is\_sorted\_until(beg, end, comp); // 在输入序列中査找最长初始有序子序列，并返回子序列的尾后迭代器

partial\_sort(beg, mid, end); // 排序 mid-beg 个元素。即，如果 mid-beg 等于 42，则此函数将值最小的 42 个元素有序放在序列前 42 个位置

partial\_sort(beg, mid, end, comp); // 排序 mid-beg 个元素。即，如果 mid-beg 等于 42，则此函数将值最小的 42 个元素有序放在序列前 42 个位置

partial\_sort\_copy(beg, end, destBeg, destEnd); // 排序输入范围中的元素，并将足够多的已排序元素放到 destBeg 和 destEnd 所指示的序列中

partial\_sort\_copy(beg, end, destBeg, destEnd, comp); // 排序输入范围中的元素，并将足够多的已排序元素放到 destBeg 和 destEnd 所指示的序列中

nth\_element(beg, nth, end); // nth 是一个迭代器，指向输入序列中第 n 大的元素。nth 之前的元素都小于等于它，而之后的元素都大于等于它

nth\_element(beg, nth, end, comp); // nth 是一个迭代器，指向输入序列中第 n 大的元素。nth 之前的元素都小于等于它，而之后的元素都大于等于它

// 使用前向迭代器的重排算法。普通版本在输入序列自身内部重拍元素，\_copy 版本完成重拍后写入到指定目的序列中，而不改变输入序列

remove(beg, end, val); // 通过用保留的元素覆盖要删除的元素实现删除 ==val 的元素，返回一个指向最后一个删除元素的尾后位置的迭代器

remove\_if(beg, end, unaryPred); // 通过用保留的元素覆盖要删除的元素实现删除满足 unaryPred 的元素，返回一个指向最后一个删除元素的尾后位置的迭代器

remove\_copy(beg, end, dest, val); // 通过用保留的元素覆盖要删除的元素实现删除 ==val 的元素，返回一个指向最后一个删除元素的尾后位置的迭代器

remove\_copy\_if(beg, end, dest, unaryPred); // 通过用保留的元素覆盖要删除的元素实现删除满足 unaryPred 的元素，返回一个指向最后一个删除元素的尾后位置的迭代器

unique(beg, end); // 通过对覆盖相邻的重复元素（用 == 确定是否相同）实现重排序列。返回一个迭代器，指向不重复元素的尾后位置

unique (beg, end, binaryPred); // 通过对覆盖相邻的重复元素（用 binaryPred 确定是否相同）实现重排序列。返回一个迭代器，指向不重复元素的尾后位置

unique\_copy(beg, end, dest); // 通过对覆盖相邻的重复元素（用 == 确定是否相同）实现重排序列。返回一个迭代器，指向不重复元素的尾后位置

unique\_copy\_if(beg, end, dest, binaryPred); // 通过对覆盖相邻的重复元素（用 binaryPred 确定是否相同）实现重排序列。返回一个迭代器，指向不重复元素的尾后位置

rotate(beg, mid, end); // 围绕 mid 指向的元素进行元素转动。元素 mid 成为为首元素，随后是 mid+1 到到 end 之前的元素，再接着是 beg 到 mid 之前的元素。返回一个迭代器，指向原来在 beg 位置的元素

rotate\_copy(beg, mid, end, dest); // 围绕 mid 指向的元素进行元素转动。元素 mid 成为为首元素，随后是 mid+1 到到 end 之前的元素，再接着是 beg 到 mid 之前的元素。返回一个迭代器，指向原来在 beg 位置的元素

// 使用双向迭代器的重排算法

reverse(beg, end); // 翻转序列中的元素，返回 void

reverse\_copy(beg, end, dest);; // 翻转序列中的元素，返回一个迭代器，指向拷贝到目的序列的元素的尾后位置

// 使用随机访问迭代器的重排算法

random\_shuffle(beg, end); // 混洗输入序列中的元素，返回 void

random\_shuffle(beg, end, rand); // 混洗输入序列中的元素，rand 接受一个正整数的随机对象，返回 void

shuffle(beg, end, Uniform\_rand); // 混洗输入序列中的元素，Uniform\_rand 必须满足均匀分布随机数生成器的要求，返回 void

// 最小值和最大值，使用 < 运算符或给定的比较操作 comp 进行比较

min(val1, va12); // 返回 val1 和 val2 中的最小值，两个实参的类型必须完全一致。参数和返回类型都是 const的引引用，意味着对象不会被拷贝。下略

min(val1, val2, comp);

min(init\_list);

min(init\_list, comp);

max(val1, val2);

max(val1, val2, comp);

max(init\_list);

max(init\_list, comp);

minmax(val1, val2); // 返回一个 pair，其 first 成员为提供的值中的较小者，second 成员为较大者。下略

minmax(vall, val2, comp);

minmax(init\_list);

minmax(init\_list, comp);

min\_element(beg, end); // 返回指向输入序列中最小元素的迭代器

min\_element(beg, end, comp); // 返回指向输入序列中最小元素的迭代器

max\_element(beg, end); // 返回指向输入序列中最大元素的迭代器

max\_element(beg, end, comp); // 返回指向输入序列中最大元素的迭代器

minmax\_element(beg, end); // 返回一个 pair，其中 first 成员为最小元素，second 成员为最大元素

minmax\_element(beg, end, comp); // 返回一个 pair，其中 first 成员为最小元素，second 成员为最大元素

// 字典序比较，根据第一对不相等的元素的相对大小来返回结果。如果第一个序列在字典序中小于第二个序列，则返回 true。否则，返回 fa1se。如果个序列比另一个短，且所有元素都与较长序列的对应元素相等，则较短序列在字典序中更小。如果序列长度相等，且对应元素都相等，则在字典序中任何一个都不大于另外一个。

lexicographical\_compare(beg1, end1, beg2, end2);

lexicographical\_compare(beg1, end1, beg2, end2, comp);

# 二．算法

用动画的形式呈现解LeetCode题目的思路

https://github.com/MisterBooo/LeetCodeAnimation

## 2.1排序

| 排序算法 | 平均时间复杂度 | 最差时间复杂度 | 空间复杂度 | 数据对象稳定性 |
| --- | --- | --- | --- | --- |
| [冒泡排序](https://github.com/huihut/interview/blob/master/Algorithm/BubbleSort.h) | O(n2) | O(n2) | O(1) | 稳定 |
| [选择排序](https://github.com/huihut/interview/blob/master/Algorithm/SelectionSort.h) | O(n2) | O(n2) | O(1) | 数组不稳定、链表稳定 |
| [插入排序](https://github.com/huihut/interview/blob/master/Algorithm/InsertSort.h) | O(n2) | O(n2) | O(1) | 稳定 |
| [快速排序](https://github.com/huihut/interview/blob/master/Algorithm/QuickSort.h) | O(n\*log2n) | O(n2) | O(log2n) | 不稳定 |
| [堆排序](https://github.com/huihut/interview/blob/master/Algorithm/HeapSort.cpp) | O(n\*log2n) | O(n\*log2n) | O(1) | 不稳定 |
| [归并排序](https://github.com/huihut/interview/blob/master/Algorithm/MergeSort.h) | O(n\*log2n) | O(n\*log2n) | O(n) | 稳定 |
| [希尔排序](https://github.com/huihut/interview/blob/master/Algorithm/ShellSort.h) | O(n\*log2n) | O(n2) | O(1) | 不稳定 |
| [计数排序](https://github.com/huihut/interview/blob/master/Algorithm/CountSort.cpp) | O(n+m) | O(n+m) | O(n+m) | 稳定 |
| [桶排序](https://github.com/huihut/interview/blob/master/Algorithm/BucketSort.cpp) | O(n) | O(n) | O(m) | 稳定 |
| [基数排序](https://github.com/huihut/interview/blob/master/Algorithm/RadixSort.h) | O(k\*n) | O(n2) |  | 稳定 |

* 均按从小到大排列
* k：代表数值中的 “数位” 个数
* n：代表数据规模
* m：代表数据的最大值减最小值
* 来自：[wikipedia . 排序算法](https://zh.wikipedia.org/wiki/%E6%8E%92%E5%BA%8F%E7%AE%97%E6%B3%95)

## 2.2查找

| 查找算法 | 平均时间复杂度 | 空间复杂度 | 查找条件 |
| --- | --- | --- | --- |
| [顺序查找](https://github.com/huihut/interview/blob/master/Algorithm/SequentialSearch.h) | O(n) | O(1) | 无序或有序 |
| [二分查找（折半查找）](https://github.com/huihut/interview/blob/master/Algorithm/BinarySearch.h) | O(log2n) | O(1) | 有序 |
| [插值查找](https://github.com/huihut/interview/blob/master/Algorithm/InsertionSearch.h) | O(log2(log2n)) | O(1) | 有序 |
| [斐波那契查找](https://github.com/huihut/interview/blob/master/Algorithm/FibonacciSearch.cpp) | O(log2n) | O(1) | 有序 |
| [哈希查找](https://github.com/huihut/interview/blob/master/DataStructure/HashTable.cpp) | O(1) | O(n) | 无序或有序 |
| [二叉查找树（二叉搜索树查找）](https://github.com/huihut/interview/blob/master/Algorithm/BSTSearch.h) | O(log2n) |  |  |
| [红黑树](https://github.com/huihut/interview/blob/master/DataStructure/RedBlackTree.cpp) | O(log2n) |  |  |
| 2-3树 | O(log2n - log3n) |  |  |
| B树/B+树 | O(log2n) |  |  |

## **2.3图搜索算法**

| 图搜索算法 | 数据结构 | 遍历时间复杂度 | 空间复杂度 |
| --- | --- | --- | --- |
| [BFS广度优先搜索](https://zh.wikipedia.org/wiki/%E5%B9%BF%E5%BA%A6%E4%BC%98%E5%85%88%E6%90%9C%E7%B4%A2) | 邻接矩阵 邻接链表 | O(|v|2) O(|v|+|E|) | O(|v|2) O(|v|+|E|) |
| [DFS深度优先搜索](https://zh.wikipedia.org/wiki/%E6%B7%B1%E5%BA%A6%E4%BC%98%E5%85%88%E6%90%9C%E7%B4%A2) | 邻接矩阵 邻接链表 | O(|v|2) O(|v|+|E|) | O(|v|2) O(|v|+|E|) |

## 2.4 其他算法

| **算法** | **思想** | **应用** |
| --- | --- | --- |
| [分治法](https://zh.wikipedia.org/wiki/%E5%88%86%E6%B2%BB%E6%B3%95) | 把一个复杂的问题分成两个或更多的相同或相似的子问题，直到最后子问题可以简单的直接求解，原问题的解即子问题的解的合并 | [循环赛日程安排问题](https://github.com/huihut/interview/tree/master/Problems/RoundRobinProblem)、排序算法（快速排序、归并排序） |
| [动态规划](https://zh.wikipedia.org/wiki/%E5%8A%A8%E6%80%81%E8%A7%84%E5%88%92) | 通过把原问题分解为相对简单的子问题的方式求解复杂问题的方法，适用于有重叠子问题和最优子结构性质的问题 | [背包问题](https://github.com/huihut/interview/tree/master/Problems/KnapsackProblem)、斐波那契数列 |
| [贪心法](https://zh.wikipedia.org/wiki/%E8%B4%AA%E5%BF%83%E6%B3%95) | 一种在每一步选择中都采取在当前状态下最好或最优（即最有利）的选择，从而希望导致结果是最好或最优的算法 | 旅行推销员问题（最短路径问题）、最小生成树、哈夫曼编码 |

## 2.5 算法数据结构总结

数据结构

线性

栈

队列 双端队列 循环队列 优先队列

散列表 哈希表

非线性结构

二叉树 满二叉树 完全二叉树 二叉树自平衡(红黑树，AVL树，树堆)

深度优先遍历：前序 中序 后序 广度优先遍历：层序

二叉堆(最小堆最小在最上面，最大堆最大在最上面。利用完全二叉树交换最后面一个)----可实现优先队列

算法

排序算法

冒泡 选择 插入 希尔O(n2)

快速 并归 堆 O(nlogn)

计数 桶 基数 复杂度线性

冒泡：优化可能后半有序，可设置标志位推出，保存最后一次值下次跳过 起始值跳过。

鸡尾酒排序：比较交换双向，类似钟摆，先是左到右，后是右到左。减少排序回合，适用大部分有序。

插入排序：有序和无序，将无序插入有序，进行移位操作。

选择：选择最大最右，然后最大的放在右边，依次直到排序完成。

希尔排序：选择上修改，10数增量5-2-1，每5增量形成一组，每组按大小重新挑选成一个数组，然后再按2-1增量拍寻。

快速排序：分治冒泡，交换排序，选择基准把数分两边，直到不能分。交换有双边和单边循环。双边除基数，头尾两个指针指向数和基数比较，符合分组移动指针，交换值，直到排序完成。

单边循环有一个指针进行分组

堆排序：在二叉堆上进行插入，最后输出。

计数排序：创建最大-最小范围数组，依次找数在对应下标下加1，最后根据数组大小排序。

桶排序：创建几个分组桶。(最大-最小)/桶数，分组拍寻。

详细可以去ProgramLearnig找。

# 三．操作系统

## 3.1 进程与线程

对于有线程系统：

* 进程是资源分配的独立单位
* 线程是资源调度的独立单位

对于无线程系统：

* 进程是资源调度、分配的独立单位

### 3.1.1进程之间的通信方式以及优缺点

* 管道（PIPE）
  + 有名管道：一种半双工的通信方式，它允许无亲缘关系进程间的通信
    1. 优点：可以实现任意关系的进程间的通信
    2. 缺点：
       1. 长期存于系统中，使用不当容易出错
       2. 缓冲区有限
  + 无名管道：一种半双工的通信方式，只能在具有亲缘关系的进程间使用（父子进程）
    1. 优点：简单方便
    2. 缺点：
       1. 局限于单向通信
       2. 只能创建在它的进程以及其有亲缘关系的进程之间
       3. 缓冲区有限
* 信号量（Semaphore）：一个计数器，可以用来控制多个线程对共享资源的访问
  + 优点：可以同步进程
  + 缺点：信号量有限
* 信号（Signal）：一种比较复杂的通信方式，用于通知接收进程某个事件已经发生
* 消息队列（Message Queue）：是消息的链表，存放在内核中并由消息队列标识符标识
  + 优点：可以实现任意进程间的通信，并通过系统调用函数来实现消息发送和接收之间的同步，无需考虑同步问题，方便
  + 缺点：信息的复制需要额外消耗 CPU 的时间，不适宜于信息量大或操作频繁的场合
* 共享内存（Shared Memory）：映射一段能被其他进程所访问的内存，这段共享内存由一个进程创建，但多个进程都可以访问
  + 优点：无须复制，快捷，信息量大
  + 缺点：
    1. 通信是通过将共享空间缓冲区直接附加到进程的虚拟地址空间中来实现的，因此进程间的读写操作的同步问题
    2. 利用内存缓冲区直接交换信息，内存的实体存在于计算机中，只能同一个计算机系统中的诸多进程共享，不方便网络通信
* 套接字（Socket）：可用于不同及其间的进程通信
  + 优点：
    1. 传输数据为字节级，传输数据可自定义，数据量小效率高
    2. 传输数据时间短，性能高
    3. 适合于客户端和服务器端之间信息实时交互
    4. 可以加密,数据安全性强
  + 缺点：需对传输的数据进行解析，转化成应用级的数据。

### 3.1.2 线程之间的通信方式

* 锁机制：包括互斥锁/量（mutex）、读写锁（reader-writer lock）、自旋锁（spin lock）、条件变量（condition）
  + 互斥锁/量（mutex）：提供了以排他方式防止数据结构被并发修改的方法。
  + 读写锁（reader-writer lock）：允许多个线程同时读共享数据，而对写操作是互斥的。
  + 自旋锁（spin lock）与互斥锁类似，都是为了保护共享资源。互斥锁是当资源被占用，申请者进入睡眠状态；而自旋锁则循环检测保持者是否已经释放锁。
  + 条件变量（condition）：可以以原子的方式阻塞进程，直到某个特定条件为真为止。对条件的测试是在互斥锁的保护下进行的。条件变量始终与互斥锁一起使用。
* 信号量机制(Semaphore)
  + 无名线程信号量
  + 命名线程信号量
* 信号机制(Signal)：类似进程间的信号处理
* 屏障（barrier）：屏障允许每个线程等待，直到所有的合作线程都达到某一点，然后从该点继续执行。

线程间的通信目的主要是用于线程同步，所以线程没有像进程通信中的用于数据交换的通信机制

### 3.1.3 进程之间私有和共享的资源

* 私有：地址空间、堆、全局变量、栈、寄存器
* 共享：代码段，公共数据，进程目录，进程 ID

### 3.1.4 线程之间私有和共享的资源

* 私有：线程栈，寄存器，程序寄存器
* 共享：堆，地址空间，全局变量，静态变量

### 3.1.5多进程与多线程间的对比、优劣与选择

##### **对比**

| 对比维度 | 多进程 | 多线程 | 总结 |
| --- | --- | --- | --- |
| 数据共享、同步 | 数据共享复杂，需要用 IPC；数据是分开的，同步简单 | 因为共享进程数据，数据共享简单，但也是因为这个原因导致同步复杂 | 各有优势 |
| 内存、CPU | 占用内存多，切换复杂，CPU 利用率低 | 占用内存少，切换简单，CPU 利用率高 | 线程占优 |
| 创建销毁、切换 | 创建销毁、切换复杂，速度慢 | 创建销毁、切换简单，速度很快 | 线程占优 |
| 编程、调试 | 编程简单，调试简单 | 编程复杂，调试复杂 | 进程占优 |
| 可靠性 | 进程间不会互相影响 | 一个线程挂掉将导致整个进程挂掉 | 进程占优 |
| 分布式 | 适应于多核、多机分布式；如果一台机器不够，扩展到多台机器比较简单 | 适应于多核分布式 | 进程占优 |

##### **优劣**

| 优劣 | 多进程 | 多线程 |
| --- | --- | --- |
| 优点 | 编程、调试简单，可靠性较高 | 创建、销毁、切换速度快，内存、资源占用小 |
| 缺点 | 创建、销毁、切换速度慢，内存、资源占用大 | 编程、调试复杂，可靠性较差 |

##### **选择**

* 需要频繁创建销毁的优先用线程
* 需要进行大量计算的优先使用线程
* 强相关的处理用线程，弱相关的处理用进程
* 可能要扩展到多机分布的用进程，多核分布的用线程
* 都满足需求的情况下，用你最熟悉、最拿手的方式

## 3.2 Linux 内核的同步方式

#### 原因

在现代操作系统里，同一时间可能有多个内核执行流在执行，因此内核其实象多进程多线程编程一样也需要一些同步机制来同步各执行单元对共享数据的访问。尤其是在多处理器系统上，更需要一些同步机制来同步不同处理器上的执行单元对共享的数据的访问。

#### **同步方式**

* 原子操作
* 信号量（semaphore）
* 读写信号量（rw\_semaphore）
* 自旋锁（spinlock）
* 大内核锁（BKL，Big Kernel Lock）
* 读写锁（rwlock）
* 大读者锁（brlock-Big Reader Lock）
* 读-拷贝修改(RCU，Read-Copy Update)
* 顺序锁（seqlock）

### **3.3文件系统**

* Windows：FCB 表 + FAT + 位图
* Unix：inode + 混合索引 + 成组链接

## 3.4 **主机字节序与网络字节序**

#### **主机字节序（CPU 字节序）**

##### **概念**

主机字节序又叫 CPU 字节序，其不是由操作系统决定的，而是由 CPU 指令集架构决定的。主机字节序分为两种：

* 大端字节序（Big Endian）：高序字节存储在低位地址，低序字节存储在高位地址。高字节在前低
* 小端字节序（Little Endian）：高序字节存储在高位地址，低序字节存储在低位地址。低字节在前低

##### **判断大端小端**

可以这样判断自己 CPU 字节序是大端还是小端：取低位判断。

##### **各架构处理器的字节序**

* x86（Intel、AMD）、MOS Technology 6502、Z80、VAX、PDP-11 等处理器为小端序；
* Motorola 6800、Motorola 68000、PowerPC 970、System/370、SPARC（除 V9 外）等处理器为大端序；
* ARM（默认小端序）、PowerPC（除 PowerPC 970 外）、DEC Alpha、SPARC V9、MIPS、PA-RISC 及 IA64 的字节序是可配置的。

#### **网络字节序**

网络字节顺序是 TCP/IP 中规定好的一种数据表示格式，它与具体的 CPU 类型、操作系统等无关，从而可以保证数据在不同主机之间传输时能够被正确解释。

网络字节顺序采用：大端（Big Endian）排列方式。

## 3.5 页面置换算法

在地址映射过程中，若在页面中发现所要访问的页面不在内存中，则产生缺页中断。当发生缺页中断时，如果操作系统内存中没有空闲页面，则操作系统必须在内存选择一个页面将其移出内存，以便为即将调入的页面让出空间。而用来选择淘汰哪一页的规则叫做页面置换算法。

#### **分类**

* 全局置换：在整个内存空间置换
* 局部置换：在本进程中进行置换

#### **算法**

全局：

* 工作集算法
* 缺页率置换算法

局部：

* 最佳置换算法（OPT）
* 先进先出置换算法（FIFO）
* 最近最久未使用（LRU）算法
* 时钟（Clock）置换算法

# 计算机网络

## 4.1 计算机网络体系结构

## 4.2 各层作用及协议

| 分层 | 作用 | 协议 |
| --- | --- | --- |
| 物理层 | 通过媒介传输比特，确定机械及电气规范（比特 Bit） | RJ45、CLOCK、IEEE802.3（中继器，集线器） |
| 数据链路层 | 将比特组装成帧和点到点的传递（帧 Frame） | PPP、FR、HDLC、VLAN、MAC（网桥，交换机） |
| 网络层 | 负责数据包从源到宿的传递和网际互连（包 Packet） | IP、ICMP、ARP、RARP、OSPF、IPX、RIP、IGRP（路由器） |
| 运输层 | 提供端到端的可靠报文传递和错误恢复（ 段Segment） | TCP、UDP、SPX |
| 会话层 | 建立、管理和终止会话（会话协议数据单元 SPDU） | NFS、SQL、NETBIOS、RPC |
| 表示层 | 对数据进行翻译、加密和压缩（表示协议数据单元 PPDU） | JPEG、MPEG、ASII |
| 应用层 | 允许访问OSI环境的手段（应用协议数据单元 APDU） | FTP、DNS、Telnet、SMTP、HTTP、WWW、NFS |

### 4.2.1 物理层

* 传输数据的单位：比特
* 数据传输系统：源系统（源点、发送器） --> 传输系统 --> 目的系统（接收器、终点）

通道：

* 单向通道（单工通道）：只有一个方向通信，没有反方向交互，如广播
* 双向交替通信（半双工通信）：通信双方都可发消息，但不能同时发送或接收
* 双向同时通信（全双工通信）：通信双方可以同时发送和接收信息

通道复用技术：

* 频分复用（FDM，Frequency Division Multiplexing）：不同用户在不同频带，所用用户在同样时间占用不同带宽资源
* 时分复用（TDM，Time Division Multiplexing）：不同用户在同一时间段的不同时间片，所有用户在不同时间占用同样的频带宽度
* 波分复用（WDM，Wavelength Division Multiplexing）：光的频分复用
* 码分复用（CDM，Code Division Multiplexing）：不同用户使用不同的码，可以在同样时间使用同样频带通信

### 4.2.2 **数据链路层**

主要信道：

* 点对点信道
* 广播信道

#### **点对点信道**

* 数据单元：帧

三个基本问题：

* 封装成帧：把网络层的 IP 数据报封装成帧，SOH - 数据部分 - EOT
* 透明传输：不管数据部分什么字符，都能传输出去；可以通过字节填充方法解决（冲突字符前加转义字符）
* 差错检测：降低误码率（BER，Bit Error Rate），广泛使用循环冗余检测（CRC，Cyclic Redundancy Check）

点对点协议（Point-to-Point Protocol）：

* 点对点协议（Point-to-Point Protocol）：用户计算机和 ISP 通信时所使用的协议

#### **广播信道**

广播通信：

* 硬件地址（物理地址、MAC 地址）
* 单播（unicast）帧（一对一）：收到的帧的 MAC 地址与本站的硬件地址相同
* 广播（broadcast）帧（一对全体）：发送给本局域网上所有站点的帧
* 多播（multicast）帧（一对多）：发送给本局域网上一部分站点的帧

### 4.2.3 **网络层**

* IP（Internet Protocol，网际协议）是为计算机网络相互连接进行通信而设计的协议。
* ARP（Address Resolution Protocol，地址解析协议）
* ICMP（Internet Control Message Protocol，网际控制报文协议）
* IGMP（Internet Group Management Protocol，网际组管理协议）

#### IP 网际协议

IP 地址分类：

* IP 地址 ::= {<网络号>,<主机号>}

| IP 地址类别 | 网络号 | 网络范围 | 主机号 | IP 地址范围 |
| --- | --- | --- | --- | --- |
| A 类 | 8bit，第一位固定为 0 | 0 —— 127 | 24bit | 1.0.0.0 —— 127.255.255.255 |
| B 类 | 16bit，前两位固定为 10 | 128.0 —— 191.255 | 16bit | 128.0.0.0 —— 191.255.255.255 |
| C 类 | 24bit，前三位固定为 110 | 192.0.0 —— 223.255.255 | 8bit | 192.0.0.0 —— 223.255.255.255 |
| D 类 | 前四位固定为 1110，后面为多播地址 |  |  |  |
| E 类 | 前五位固定为 11110，后面保留为今后所用 |  |  |  |

IP 数据报格式：

#### ICMP 网际控制报文协议

应用：

* PING（Packet InterNet Groper，分组网间探测）测试两个主机之间的连通性
  + TTL（Time To Live，生存时间）该字段指定 IP 包被路由器丢弃之前允许通过的最大网段数量

#### 内部网关协议

* RIP（Routing Information Protocol，路由信息协议）
* OSPF（Open Sortest Path First，开放最短路径优先）

#### 外部网关协议

* BGP（Border Gateway Protocol，边界网关协议）

#### IP多播

* IGMP（Internet Group Management Protocol，网际组管理协议）
* 多播路由选择协议

#### VPN 和 NAT

* VPN（Virtual Private Network，虚拟专用网）
* NAT（Network Address Translation，网络地址转换）

#### 路由表包含什么？

1. 网络 ID（Network ID, Network number）：就是目标地址的网络 ID。
2. 子网掩码（subnet mask）：用来判断 IP 所属网络
3. 下一跳地址/接口（Next hop / interface）：就是数据在发送到目标地址的旅途中下一站的地址。其中 interface 指向 next hop（即为下一个 route）。一个自治系统（AS, Autonomous system）中的 route 应该包含区域内所有的子网络，而默认网关（Network id: 0.0.0.0, Netmask: 0.0.0.0）指向自治系统的出口。

根据应用和执行的不同，路由表可能含有如下附加信息：

1. 花费（Cost）：就是数据发送过程中通过路径所需要的花费。
2. 路由的服务质量
3. 路由中需要过滤的出/入连接列表

### 4.2.4 运输层

#### 协议：

* TCP（Transmission Control Protocol，传输控制协议）
* UDP（User Datagram Protocol，用户数据报协议）

#### 端口：

| 应用程序 | FTP | TELNET | SMTP | DNS | TFTP | HTTP | HTTPS | SNMP |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 端口号 | 21 | 23 | 25 | 53 | 69 | 80 | 443 | 161 |

#### TCP

* TCP（Transmission Control Protocol，传输控制协议）是一种面向连接的、可靠的、基于字节流的传输层通信协议，其传输的单位是报文段。

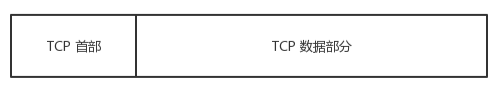
特征：

* 面向连接
* 只能点对点（一对一）通信
* 可靠交互
* 全双工通信
* 面向字节流

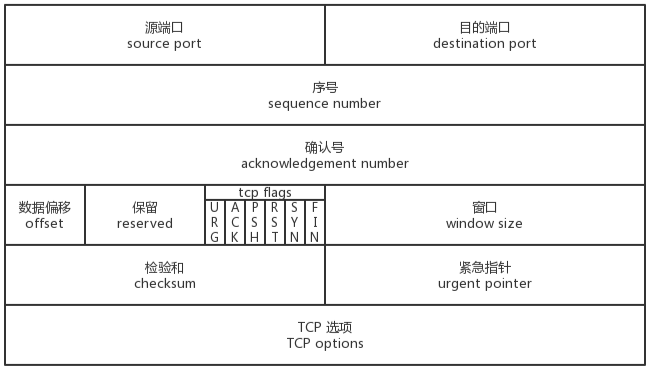
TCP 如何保证可靠传输：

* 确认和超时重传
* 数据合理分片和排序
* 流量控制
* 拥塞控制
* 数据校验

TCP 报文结构



TCP 首部



TCP：状态控制码（Code，Control Flag），占 6 比特，含义如下：

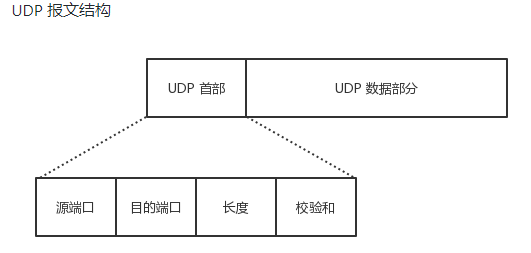
* URG：紧急比特（urgent），当 URG＝1 时，表明紧急指针字段有效，代表该封包为紧急封包。它告诉系统此报文段中有紧急数据，应尽快传送(相当于高优先级的数据)， 且上图中的 Urgent Pointer 字段也会被启用。
* ACK：确认比特（Acknowledge）。只有当 ACK＝1 时确认号字段才有效，代表这个封包为确认封包。当 ACK＝0 时，确认号无效。
* PSH：（Push function）若为 1 时，代表要求对方立即传送缓冲区内的其他对应封包，而无需等缓冲满了才送。
* RST：复位比特(Reset)，当 RST＝1 时，表明 TCP 连接中出现严重差错（如由于主机崩溃或其他原因），必须释放连接，然后再重新建立运输连接。
* SYN：同步比特(Synchronous)，SYN 置为 1，就表示这是一个连接请求或连接接受报文，通常带有 SYN 标志的封包表示『主动』要连接到对方的意思。
* FIN：终止比特(Final)，用来释放一个连接。当 FIN＝1 时，表明此报文段的发送端的数据已发送完毕，并要求释放运输连接。

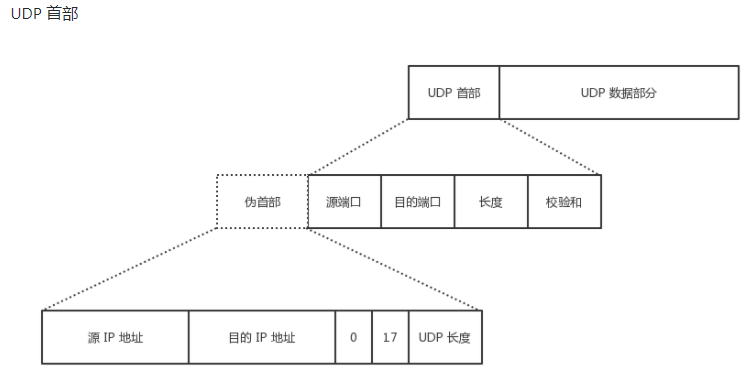
#### UDP

* UDP（User Datagram Protocol，用户数据报协议）是 OSI（Open System Interconnection 开放式系统互联） 参考模型中一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务，其传输的单位是用户数据报。

特征：

* 无连接
* 尽最大努力交付
* 面向报文
* 没有拥塞控制
* 支持一对一、一对多、多对一、多对多的交互通信
* 首部开销小





#### **TCP 与 UDP 的区别**

1. TCP 面向连接，UDP 是无连接的；
2. TCP 提供可靠的服务，也就是说，通过 TCP 连接传送的数据，无差错，不丢失，不重复，且按序到达；UDP 尽最大努力交付，即不保证可靠交付
3. TCP 的逻辑通信信道是全双工的可靠信道；UDP 则是不可靠信道
4. 每一条 TCP 连接只能是点到点的；UDP 支持一对一，一对多，多对一和多对多的交互通信
5. TCP 面向字节流（可能出现黏包问题），实际上是 TCP 把数据看成一连串无结构的字节流；UDP 是面向报文的（不会出现黏包问题）
6. UDP 没有拥塞控制，因此网络出现拥塞不会使源主机的发送速率降低（对实时应用很有用，如 IP 电话，实时视频会议等）
7. TCP 首部开销20字节；UDP 的首部开销小，只有 8 个字节

#### **TCP 黏包问题**

##### **原因**

TCP 是一个基于字节流的传输服务（UDP 基于报文的），“流” 意味着 TCP 所传输的数据是没有边界的。所以可能会出现两个数据包黏在一起的情况。

##### **解决**

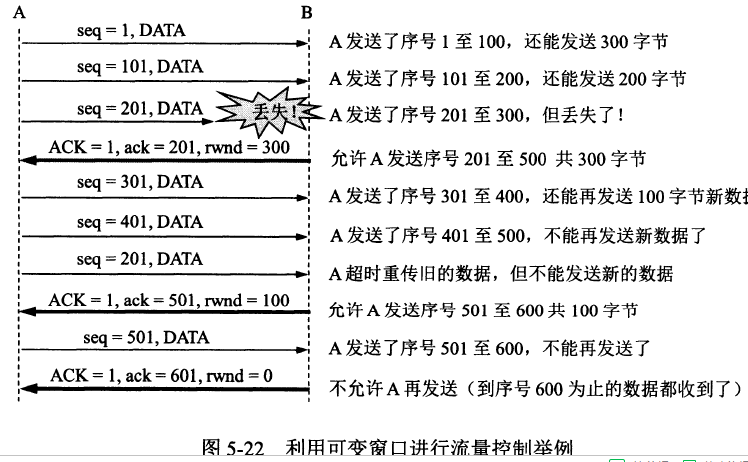
* 发送定长包。如果每个消息的大小都是一样的，那么在接收对等方只要累计接收数据，直到数据等于一个定长的数值就将它作为一个消息。
* 包头加上包体长度。包头是定长的 4 个字节，说明了包体的长度。接收对等方先接收包头长度，依据包头长度来接收包体。
* 在数据包之间设置边界，如添加特殊符号 \r\n 标记。FTP 协议正是这么做的。但问题在于如果数据正文中也含有 \r\n，则会误判为消息的边界。
* 使用更加复杂的应用层协议。

#### **TCP 流量控制**

##### **概念**

流量控制（flow control）就是让发送方的发送速率不要太快，要让接收方来得及接收。

利用可变窗口进行流量控制



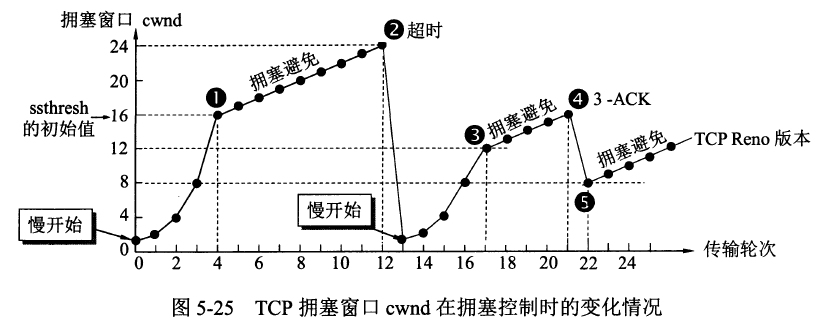
#### **TCP 拥塞控制**

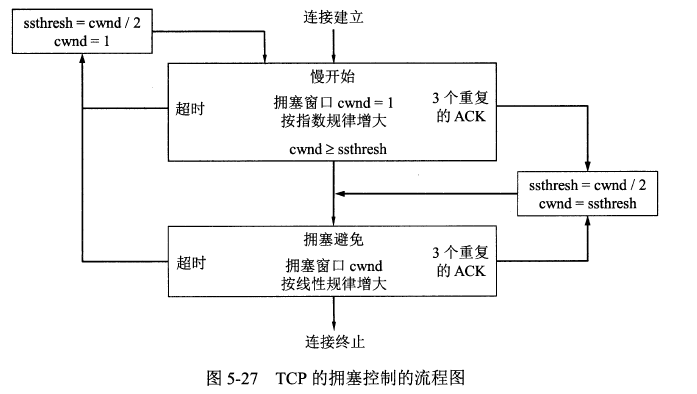
##### 概念

拥塞控制就是防止过多的数据注入到网络中，这样可以使网络中的路由器或链路不致过载。

##### **方法**

* 慢开始( slow-start )
* 拥塞避免( congestion avoidance )
* 快重传( fast retransmit )
* 快恢复( fast recovery )

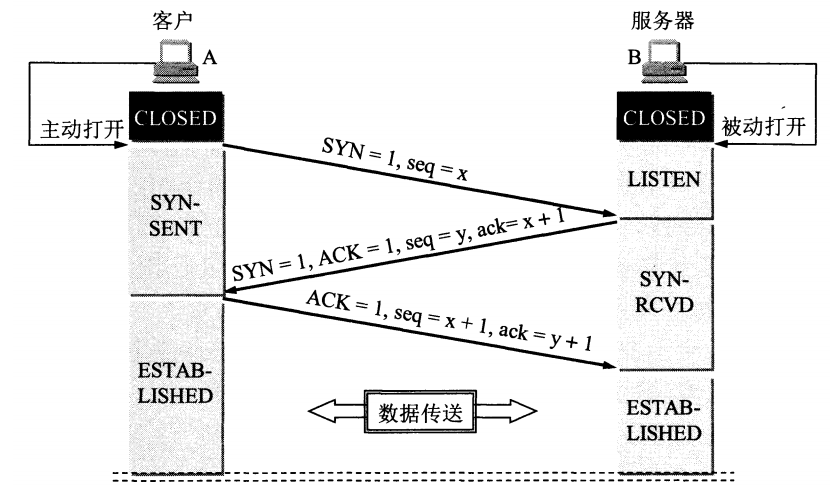




#### **TCP 传输连接管理**

因为 TCP 三次握手建立连接、四次挥手释放连接很重要，所以附上《计算机网络（第 7 版）-谢希仁》书中对此章的详细描述：<https://raw.githubusercontent.com/huihut/interview/master/images/TCP-transport-connection-management.png>

##### **TCP 三次握手建立连接**



【TCP 建立连接全过程解释】

1. 客户端发送 SYN 给服务器，说明客户端请求建立连接；
2. 服务端收到客户端发的 SYN，并回复 SYN+ACK 给客户端（同意建立连接）；
3. 客户端收到服务端的 SYN+ACK 后，回复 ACK 给服务端（表示客户端收到了服务端发的同意报文）；
4. 服务端收到客户端的 ACK，连接已建立，可以数据传输。

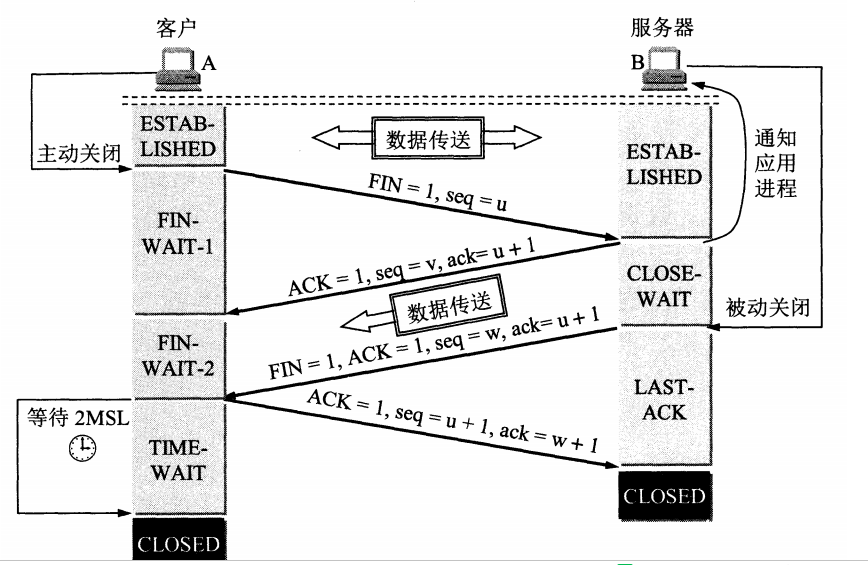
##### **TCP 为什么要进行三次握手？**

【答案一】因为信道不可靠，而 TCP 想在不可靠信道上建立可靠地传输，那么三次通信是理论上的最小值。（而 UDP 则不需建立可靠传输，因此 UDP 不需要三次握手。）

【答案二】因为双方都需要确认对方收到了自己发送的序列号，确认过程最少要进行三次通信。

【答案三】为了防止已失效的连接请求报文段突然又传送到了服务端，因而产生错误。

##### **TCP 四次挥手释放连接**



【TCP 释放连接全过程解释】

1. 客户端发送 FIN 给服务器，说明客户端不必发送数据给服务器了（请求释放从客户端到服务器的连接）；
2. 服务器接收到客户端发的 FIN，并回复 ACK 给客户端（同意释放从客户端到服务器的连接）；
3. 客户端收到服务端回复的 ACK，此时从客户端到服务器的连接已释放（但服务端到客户端的连接还未释放，并且客户端还可以接收数据）；
4. 服务端继续发送之前没发完的数据给客户端；
5. 服务端发送 FIN+ACK 给客户端，说明服务端发送完了数据（请求释放从服务端到客户端的连接，就算没收到客户端的回复，过段时间也会自动释放）；
6. 客户端收到服务端的 FIN+ACK，并回复 ACK 给客户端（同意释放从服务端到客户端的连接）；
7. 服务端收到客户端的 ACK 后，释放从服务端到客户端的连接。

##### **TCP 为什么要进行四次挥手？**

【问题一】TCP 为什么要进行四次挥手？ / 为什么 TCP 建立连接需要三次，而释放连接则需要四次？

【答案一】因为 TCP 是全双工模式，客户端请求关闭连接后，客户端向服务端的连接关闭（一二次挥手），服务端继续传输之前没传完的数据给客户端（数据传输），服务端向客户端的连接关闭（三四次挥手）。所以 TCP 释放连接时服务器的 ACK 和 FIN 是分开发送的（中间隔着数据传输），而 TCP 建立连接时服务器的 ACK 和 SYN 是一起发送的（第二次握手），所以 TCP 建立连接需要三次，而释放连接则需要四次。

【问题二】为什么 TCP 连接时可以 ACK 和 SYN 一起发送，而释放时则 ACK 和 FIN 分开发送呢？（ACK 和 FIN 分开是指第二次和第三次挥手）

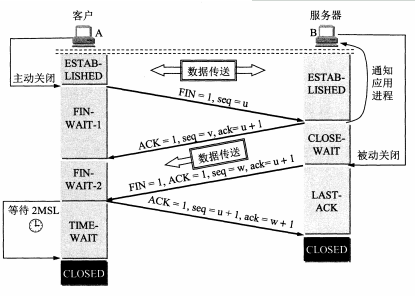
【答案二】因为客户端请求释放时，服务器可能还有数据需要传输给客户端，因此服务端要先响应客户端 FIN 请求（服务端发送 ACK），然后数据传输，传输完成后，服务端再提出 FIN 请求（服务端发送 FIN）；而连接时则没有中间的数据传输，因此连接时可以 ACK 和 SYN 一起发送。

【问题三】为什么客户端释放最后需要 TIME-WAIT 等待 2MSL 呢？

【答案三】

1. 为了保证客户端发送的最后一个 ACK 报文能够到达服务端。若未成功到达，则服务端超时重传 FIN+ACK 报文段，客户端再重传 ACK，并重新计时。
2. 防止已失效的连接请求报文段出现在本连接中。TIME-WAIT 持续 2MSL 可使本连接持续的时间内所产生的所有报文段都从网络中消失，这样可使下次连接中不会出现旧的连接报文段。

#### **TCP 有限状态机**



### 4.2.5 应用层

#### **DNS**

* DNS（Domain Name System，域名系统）是互联网的一项服务。它作为将域名和 IP 地址相互映射的一个分布式数据库，能够使人更方便地访问互联网。DNS 使用 TCP 和 UDP 端口 53。当前，对于每一级域名长度的限制是 63 个字符，域名总长度则不能超过 253 个字符。

域名：

* 域名 ::= {<三级域名>.<二级域名>.<顶级域名>}，如：blog.huihut.com

#### **FTP**

* FTP（File Transfer Protocol，文件传输协议）是用于在网络上进行文件传输的一套标准协议，使用客户/服务器模式，使用 TCP 数据报，提供交互式访问，双向传输。
* TFTP（Trivial File Transfer Protocol，简单文件传输协议）一个小且易实现的文件传输协议，也使用客户-服务器方式，使用UDP数据报，只支持文件传输而不支持交互，没有列目录，不能对用户进行身份鉴定

#### **TELNET**

* TELNET 协议是 TCP/IP 协议族中的一员，是 Internet 远程登陆服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。
* HTTP（HyperText Transfer Protocol，超文本传输协议）是用于从 WWW（World Wide Web，万维网）服务器传输超文本到本地浏览器的传送协议。
* SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP 协议属于 TCP/IP 协议簇，它帮助每台计算机在发送或中转信件时找到下一个目的地。
* Socket 建立网络通信连接至少要一对端口号（Socket）。Socket 本质是编程接口（API），对 TCP/IP 的封装，TCP/IP 也要提供可供程序员做网络开发所用的接口，这就是 Socket 编程接口。

#### **WWW**

* WWW（World Wide Web，环球信息网，万维网）是一个由许多互相链接的超文本组成的系统，通过互联网访问

##### **URL**

* URL（Uniform Resource Locator，统一资源定位符）是因特网上标准的资源的地址（Address）

标准格式：

* 协议类型:[//服务器地址[:端口号]][/资源层级UNIX文件路径]文件名[?查询][#片段ID]

完整格式：

* 协议类型:[//[访问资源需要的凭证信息@]服务器地址[:端口号]][/资源层级UNIX文件路径]文件名[?查询][#片段ID]

其中【访问凭证信息@；:端口号；?查询；#片段ID】都属于选填项  
如：https://github.com/huihut/interview#cc

##### **HTTP**

HTTP（HyperText Transfer Protocol，超文本传输协议）是一种用于分布式、协作式和超媒体信息系统的应用层协议。HTTP 是万维网的数据通信的基础。

请求方法

| 方法 | 意义 |
| --- | --- |
| OPTIONS | 请求一些选项信息，允许客户端查看服务器的性能 |
| GET | 请求指定的页面信息，并返回实体主体 |
| HEAD | 类似于 get 请求，只不过返回的响应中没有具体的内容，用于获取报头 |
| POST | 向指定资源提交数据进行处理请求（例如提交表单或者上传文件）。数据被包含在请求体中。POST请求可能会导致新的资源的建立和/或已有资源的修改 |
| PUT | 从客户端向服务器传送的数据取代指定的文档的内容 |
| DELETE | 请求服务器删除指定的页面 |
| TRACE | 回显服务器收到的请求，主要用于测试或诊断 |

状态码（Status-Code）

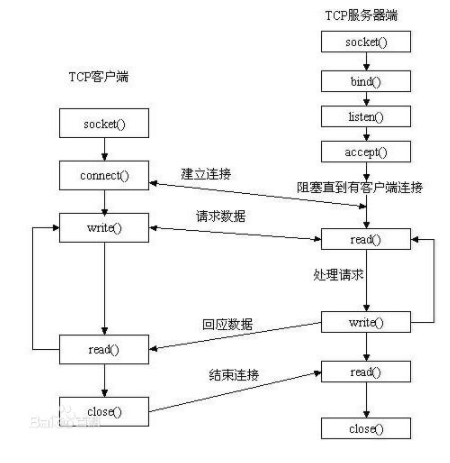
* 1xx：表示通知信息，如请求收到了或正在进行处理
  + 100 Continue：继续，客户端应继续其请求
  + 101 Switching Protocols 切换协议。服务器根据客户端的请求切换协议。只能切换到更高级的协议，例如，切换到 HTTP 的新版本协议
* 2xx：表示成功，如接收或知道了
  + 200 OK: 请求成功
* 3xx：表示重定向，如要完成请求还必须采取进一步的行动
  + 301 Moved Permanently: 永久移动。请求的资源已被永久的移动到新 URL，返回信息会包括新的 URL，浏览器会自动定向到新 URL。今后任何新的请求都应使用新的 URL 代替
* 4xx：表示客户的差错，如请求中有错误的语法或不能完成
  + 400 Bad Request: 客户端请求的语法错误，服务器无法理解
  + 401 Unauthorized: 请求要求用户的身份认证
  + 403 Forbidden: 服务器理解请求客户端的请求，但是拒绝执行此请求（权限不够）
  + 404 Not Found: 服务器无法根据客户端的请求找到资源（网页）。通过此代码，网站设计人员可设置 “您所请求的资源无法找到” 的个性页面
  + 408 Request Timeout: 服务器等待客户端发送的请求时间过长，超时
* 5xx：表示服务器的差错，如服务器失效无法完成请求
  + 500 Internal Server Error: 服务器内部错误，无法完成请求
  + 503 Service Unavailable: 由于超载或系统维护，服务器暂时的无法处理客户端的请求。延时的长度可包含在服务器的 Retry-After 头信息中
  + 504 Gateway Timeout: 充当网关或代理的服务器，未及时从远端服务器获取请求

##### **他协议**

* SMTP（Simple Main Transfer Protocol，简单邮件传输协议）是在 Internet 传输 Email 的标准，是一个相对简单的基于文本的协议。在其之上指定了一条消息的一个或多个接收者（在大多数情况下被确认是存在的），然后消息文本会被传输。可以很简单地通过 Telnet 程序来测试一个 SMTP 服务器。SMTP 使用 TCP 端口 25。
* DHCP（Dynamic Host Configuration Protocol，动态主机设置协议）是一个局域网的网络协议，使用 UDP 协议工作，主要有两个用途：
  + 用于内部网络或网络服务供应商自动分配 IP 地址给用户
  + 用于内部网络管理员作为对所有电脑作中央管理的手段
* SNMP（Simple Network Management Protocol，简单网络管理协议）构成了互联网工程工作小组（IETF，Internet Engineering Task Force）定义的 Internet 协议族的一部分。该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。

## 4.3网络编程

### **Socket** [Linux Socket 编程（不限 Linux）](https://www.cnblogs.com/skynet/archive/2010/12/12/1903949.html)



#### **Socket 中的 read()、write() 函数**

ssize\_t read(int fd, void \*buf, size\_t count);

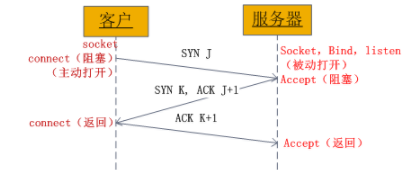
ssize\_t write(int fd, const void \*buf, size\_t count);

##### **read()**

* read 函数是负责从 fd 中读取内容。
* 当读成功时，read 返回实际所读的字节数。
* 如果返回的值是 0 表示已经读到文件的结束了，小于 0 表示出现了错误。
* 如果错误为 EINTR 说明读是由中断引起的；如果是 ECONNREST 表示网络连接出了问题。

##### **write()**

* write 函数将 buf 中的 nbytes 字节内容写入文件描述符 fd。
* 成功时返回写的字节数。失败时返回 -1，并设置 errno 变量。
* 在网络程序中，当我们向套接字文件描述符写时有俩种可能。
* （1）write 的返回值大于 0，表示写了部分或者是全部的数据。
* （2）返回的值小于 0，此时出现了错误。
* 如果错误为 EINTR 表示在写的时候出现了中断错误；如果为 EPIPE 表示网络连接出现了问题（对方已经关闭了连接）。



# 数据库

### 5.1**基本概念**

* 数据（data）：描述事物的符号记录称为数据。
* 数据库（DataBase，DB）：是长期存储在计算机内、有组织的、可共享的大量数据的集合，具有永久存储、有组织、可共享三个基本特点。
* 数据库管理系统（DataBase Management System，DBMS）：是位于用户与操作系统之间的一层数据管理软件。
* 数据库系统（DataBase System，DBS）：是有数据库、数据库管理系统（及其应用开发工具）、应用程序和数据库管理员（DataBase Administrator DBA）组成的存储、管理、处理和维护数据的系统。
* 实体（entity）：客观存在并可相互区别的事物称为实体。
* 属性（attribute）：实体所具有的某一特性称为属性。
* 码（key）：唯一标识实体的属性集称为码。
* 实体型（entity type）：用实体名及其属性名集合来抽象和刻画同类实体，称为实体型。
* 实体集（entity set）：同一实体型的集合称为实体集。
* 联系（relationship）：实体之间的联系通常是指不同实体集之间的联系。
* 模式（schema）：模式也称逻辑模式，是数据库全体数据的逻辑结构和特征的描述，是所有用户的公共数据视图。
* 外模式（external schema）：外模式也称子模式（subschema）或用户模式，它是数据库用户（包括应用程序员和最终用户）能够看见和使用的局部数据的逻辑结构和特征的描述，是数据库用户的数据视图，是与某一应用有关的数据的逻辑表示。
* 内模式（internal schema）：内模式也称为存储模式（storage schema），一个数据库只有一个内模式。他是数据物理结构和存储方式的描述，是数据库在数据库内部的组织方式。

### **5.2常用数据模型**

* 层次模型（hierarchical model）
* 网状模型（network model）
* 关系模型（relational model）
  + 关系（relation）：一个关系对应通常说的一张表
  + 元组（tuple）：表中的一行即为一个元组
  + 属性（attribute）：表中的一列即为一个属性
  + 码（key）：表中可以唯一确定一个元组的某个属性组
  + 域（domain）：一组具有相同数据类型的值的集合
  + 分量：元组中的一个属性值
  + 关系模式：对关系的描述，一般表示为 关系名(属性1, 属性2, ..., 属性n)
* 面向对象数据模型（object oriented data model）
* 对象关系数据模型（object relational data model）
* 半结构化数据模型（semistructure data model）

### **5.3常用 SQL 操作**

|  |  |  |
| --- | --- | --- |
| 对象类型 | 对象 | 操作类型 |
| 数据库模式 | 模式 | CREATE SCHEMA |
| 基本表 | CREATE SCHEMA，ALTER TABLE |
| 视图 | CREATE VIEW |
| 索引 | CREATE INDEX |
| 数据 | 基本表和视图 | SELECT，INSERT，UPDATE，DELETE，REFERENCES，ALL PRIVILEGES |
| 属性列 | SELECT，INSERT，UPDATE，REFERENCES，ALL PRIVILEGES |

### **5.4关系型数据库**

* 基本关系操作：查询（选择、投影、连接（等值连接、自然连接、外连接（左外连接、右外连接））、除、并、差、交、笛卡尔积等）、插入、删除、修改
* 关系模型中的三类完整性约束：实体完整性、参照完整性、用户定义的完整性

#### **索引**

* 数据库索引：顺序索引、B+ 树索引、hash 索引
* [MySQL 索引背后的数据结构及算法原理](http://blog.codinglabs.org/articles/theory-of-mysql-index.html)

### **5.5数据库完整性**

* 数据库的完整性是指数据的正确性和相容性。
  + 完整性：为了防止数据库中存在不符合语义（不正确）的数据。
  + 安全性：为了保护数据库防止恶意破坏和非法存取。
* 触发器：是用户定义在关系表中的一类由事件驱动的特殊过程。

### **5.6关系数据理论**

* 数据依赖是一个关系内部属性与属性之间的一种约束关系，是通过属性间值的相等与否体现出来的数据间相关联系。
* 最重要的数据依赖：函数依赖、多值依赖。

#### **范式**

* 第一范式（1NF）：属性（字段）是最小单位不可再分。
* 第二范式（2NF）：满足 1NF，每个非主属性完全依赖于主键（消除 1NF 非主属性对码的部分函数依赖）。
* 第三范式（3NF）：满足 2NF，任何非主属性不依赖于其他非主属性（消除 2NF 主属性对码的传递函数依赖）。
* 鲍依斯-科得范式（BCNF）：满足 3NF，任何非主属性不能对主键子集依赖（消除 3NF 主属性对码的部分和传递函数依赖）。
* 第四范式（4NF）：满足 3NF，属性之间不能有非平凡且非函数依赖的多值依赖（消除 3NF 非平凡且非函数依赖的多值依赖）。

### **5.7数据库恢复**

* 事务：是用户定义的一个数据库操作序列，这些操作要么全做，要么全不做，是一个不可分割的工作单位。
* 事物的 ACID 特性：原子性、一致性、隔离性、持续性。
* 恢复的实现技术：建立冗余数据 -> 利用冗余数据实施数据库恢复。
* 建立冗余数据常用技术：数据转储（动态海量转储、动态增量转储、静态海量转储、静态增量转储）、登记日志文件。

### **5.8并发控制**

* 事务是并发控制的基本单位。
* 并发操作带来的数据不一致性包括：丢失修改、不可重复读、读 “脏” 数据。
* 并发控制主要技术：封锁、时间戳、乐观控制法、多版本并发控制等。
* 基本封锁类型：排他锁（X 锁 / 写锁）、共享锁（S 锁 / 读锁）。
* 活锁死锁：
  + 活锁：事务永远处于等待状态，可通过先来先服务的策略避免。
  + 死锁：事物永远不能结束
    - 预防：一次封锁法、顺序封锁法；
    - 诊断：超时法、等待图法；
    - 解除：撤销处理死锁代价最小的事务，并释放此事务的所有的锁，使其他事务得以继续运行下去。
* 可串行化调度：多个事务的并发执行是正确的，当且仅当其结果与按某一次序串行地执行这些事务时的结果相同。可串行性时并发事务正确调度的准则。

# 六．设计模式

## 6.1 单例模式

// 懒汉式单例模式class Singleton

{private:

Singleton() { }

static Singleton \* pInstance;public:

static Singleton \* GetInstance()

{

if (pInstance == nullptr)

pInstance = new Singleton();

return pInstance;

}

};

// 线程安全的单例模式class Singleton

{private:

Singleton() { }

~Singleton() { }

Singleton(const Singleton &);

Singleton & operator = (const Singleton &);public:

static Singleton & GetInstance()

{

static Singleton instance;

return instance;

}

};

## 6.2 抽象工厂模式

## 6.3 适配器模式

## 6.4 桥接模式

## 6.5 观察者模式

## 6.6 设计模式的六大原则

* 单一职责原则（SRP，Single Responsibility Principle）
* 里氏替换原则（LSP，Liskov Substitution Principle）
* 依赖倒置原则（DIP，Dependence Inversion Principle）
* 接口隔离原则（ISP，Interface Segregation Principle）
* 迪米特法则（LoD，Law of Demeter）
* 开放封闭原则（OCP，Open Close Principle）

# 七．编译链接装载

## 7.1 内存、栈、堆

一般应用程序内存空间有如下区域：

* 栈：由操作系统自动分配释放，存放函数的参数值、局部变量等的值，用于维护函数调用的上下文
* 堆：一般由程序员分配释放，若程序员不释放，程序结束时可能由操作系统回收，用来容纳应用程序动态分配的内存区域
* 可执行文件映像：存储着可执行文件在内存中的映像，由装载器装载是将可执行文件的内存读取或映射到这里
* 保留区：保留区并不是一个单一的内存区域，而是对内存中受到保护而禁止访问的内存区域的总称，如通常 C 语言讲无效指针赋值为 0（NULL），因此 0 地址正常情况下不可能有效的访问数据

#### **栈**

栈保存了一个函数调用所需要的维护信息，常被称为堆栈帧（Stack Frame）或活动记录（Activate Record），一般包含以下几方面：

* 函数的返回地址和参数
* 临时变量：包括函数的非静态局部变量以及编译器自动生成的其他临时变量
* 保存上下文：包括函数调用前后需要保持不变的寄存器

#### **堆**

堆分配算法：

* 空闲链表（Free List）
* 位图（Bitmap）
* 对象池

#### **“段错误（segment fault）” 或 “非法操作，该内存地址不能 read/write”**

典型的非法指针解引用造成的错误。当指针指向一个不允许读写的内存地址，而程序却试图利用指针来读或写该地址时，会出现这个错误。

普遍原因：

* 将指针初始化为 NULL，之后没有给它一个合理的值就开始使用指针
* 没用初始化栈中的指针，指针的值一般会是随机数，之后就直接开始使用指针

## 7.2 编译链接

#### **各平台文件格式**

| 平台 | 可执行文件 | 目标文件 | 动态库/共享对象 | 静态库 |
| --- | --- | --- | --- | --- |
| Windows | exe | obj | dll | lib |
| Unix/Linux | ELF、out | o | so | a |
| Mac | Mach-O | o | dylib、tbd、framework | a、framework |

#### **编译链接过程**

1. 预编译（预编译器处理如 #include、#define 等预编译指令，生成 .i 或 .ii 文件）
2. 编译（编译器进行词法分析、语法分析、语义分析、中间代码生成、目标代码生成、优化，生成 .s 文件）
3. 汇编（汇编器把汇编码翻译成机器码，生成 .o 文件）
4. 链接（连接器进行地址和空间分配、符号决议、重定位，生成 .out 文件）

现在版本 GCC 把预编译和编译合成一步，预编译编译程序 cc1、汇编器 as、连接器 ld

MSVC 编译环境，编译器 cl、连接器 link、可执行文件查看器 dumpbin

#### **目标文件**

编译器编译源代码后生成的文件叫做目标文件。目标文件从结构上讲，它是已经编译后的可执行文件格式，只是还没有经过链接的过程，其中可能有些符号或有些地址还没有被调整。

可执行文件（Windows 的 .exe 和 Linux 的 ELF）、动态链接库（Windows 的 .dll 和 Linux 的 .so）、静态链接库（Windows 的 .lib 和 Linux 的 .a）都是按照可执行文件格式存储（Windows 按照 PE-COFF，Linux 按照 ELF）

##### **目标文件格式**

* Windows 的 PE（Portable Executable），或称为 PE-COFF，.obj 格式
* Linux 的 ELF（Executable Linkable Format），.o 格式
* Intel/Microsoft 的 OMF（Object Module Format）
* Unix 的 a.out 格式
* MS-DOS 的 .COM 格式

PE 和 ELF 都是 COFF（Common File Format）的变种

##### **目标文件存储结构**

| 段 | 功能 |
| --- | --- |
| File Header | 文件头，描述整个文件的文件属性（包括文件是否可执行、是静态链接或动态连接及入口地址、目标硬件、目标操作系统等） |
| .text section | 代码段，执行语句编译成的机器代码 |
| .data section | 数据段，已初始化的全局变量和局部静态变量 |
| .bss section | BSS 段（Block Started by Symbol），未初始化的全局变量和局部静态变量（因为默认值为 0，所以只是在此预留位置，不占空间） |
| .rodata section | 只读数据段，存放只读数据，一般是程序里面的只读变量（如 const 修饰的变量）和字符串常量 |
| .comment section | 注释信息段，存放编译器版本信息 |
| .note.GNU-stack section | 堆栈提示段 |

#### **链接的接口————符号**

在链接中，目标文件之间相互拼合实际上是目标文件之间对地址的引用，即对函数和变量的地址的引用。我们将函数和变量统称为符号（Symbol），函数名或变量名就是符号名（Symbol Name）。

## 7.3 Linux 的共享库（Shared Library）

Linux 下的共享库就是普通的 ELF 共享对象。

共享库版本更新应该保证二进制接口 ABI（Application Binary Interface）的兼容

#### **命名**

libname.so.x.y.z

* x：主版本号，不同主版本号的库之间不兼容，需要重新编译
* y：次版本号，高版本号向后兼容低版本号
* z：发布版本号，不对接口进行更改，完全兼容

#### **路径**

大部分包括 Linux 在内的开源系统遵循 FHS（File Hierarchy Standard）的标准，这标准规定了系统文件如何存放，包括各个目录结构、组织和作用。

* /lib：存放系统最关键和最基础的共享库，如动态链接器、C 语言运行库、数学库等
* /usr/lib：存放非系统运行时所需要的关键性的库，主要是开发库
* /usr/local/lib：存放跟操作系统本身并不十分相关的库，主要是一些第三方应用程序的库

动态链接器会在 /lib、/usr/lib 和由 /etc/ld.so.conf 配置文件指定的，目录中查找共享库

#### **环境变量**

* LD\_LIBRARY\_PATH：临时改变某个应用程序的共享库查找路径，而不会影响其他应用程序
* LD\_PRELOAD：指定预先装载的一些共享库甚至是目标文件
* LD\_DEBUG：打开动态链接器的调试功能

#### **so 共享库的编写**

创建一个名为 MySharedLib 的共享库

CMakeLists.txt

cmake\_minimum\_required(VERSION 3.10)project(MySharedLib)

set(CMAKE\_CXX\_STANDARD 11)

add\_library(MySharedLib SHARED library.cpp library.h)

library.h

#ifndef MYSHAREDLIB\_LIBRARY\_H

#define MYSHAREDLIB\_LIBRARY\_H

// 打印 Hello World!void hello();

// 使用可变模版参数求和template <typename T>

T sum(T t)

{

return t;

}template <typename T, typename ...Types>

T sum(T first, Types ... rest)

{

return first + sum<T>(rest...);

}

#endif

library.cpp

#include <iostream>

#include "library.h"

void hello() {

std::cout << "Hello, World!" << std::endl;

}

#### **so 共享库的使用（被可执行项目调用）**

创建一个名为 TestSharedLib 的可执行项目

CMakeLists.txt

cmake\_minimum\_required(VERSION 3.10)project(TestSharedLib)

# C++11 编译set(CMAKE\_CXX\_STANDARD 11)

# 头文件路径set(INC\_DIR /home/xx/code/clion/MySharedLib)# 库文件路径set(LIB\_DIR /home/xx/code/clion/MySharedLib/cmake-build-debug)

include\_directories(${INC\_DIR})link\_directories(${LIB\_DIR})link\_libraries(MySharedLib)

add\_executable(TestSharedLib main.cpp)

# 链接 MySharedLib 库target\_link\_libraries(TestSharedLib MySharedLib)

main.cpp

#include <iostream>

#include "library.h"using std::cout;using std::endl;

int main() {

hello();

cout << "1 + 2 = " << sum(1,2) << endl;

cout << "1 + 2 + 3 = " << sum(1,2,3) << endl;

return 0;

}

执行结果

Hello, World!

1 + 2 = 3

1 + 2 + 3 = 6

## 7.4 Windows 应用程序入口函数

* GUI（Graphical User Interface）应用，链接器选项：/SUBSYSTEM:WINDOWS
* CUI（Console User Interface）应用，链接器选项：/SUBSYSTEM:CONSOLE

## 7.5 Windows 的动态链接库（Dynamic-Link Library）

#### **用处**

* 扩展了应用程序的特性
* 简化了项目管理
* 有助于节省内存
* 促进了资源的共享
* 促进了本地化
* 有助于解决平台间的差异
* 可以用于特殊目的

#### **注意**

* 创建 DLL，事实上是在创建可供一个可执行模块调用的函数
* 当一个模块提供一个内存分配函数（malloc、new）的时候，它必须同时提供另一个内存释放函数（free、delete）
* 在使用 C 和 C++ 混编的时候，要使用 extern "C" 修饰符
* 一个 DLL 可以导出函数、变量（避免导出）、C++ 类（导出导入需要同编译器，否则避免导出）
* DLL 模块：cpp 文件中的 \_\_declspec(dllexport) 写在 include 头文件之前
* 调用 DLL 的可执行模块：cpp 文件的 \_\_declspec(dllimport) 之前不应该定义 MYLIBAPI

#### **加载 Windows 程序的搜索顺序**

1. 包含可执行文件的目录
2. Windows 的系统目录，可以通过 GetSystemDirectory 得到
3. 16 位的系统目录，即 Windows 目录中的 System 子目录
4. Windows 目录，可以通过 GetWindowsDirectory 得到
5. 进程的当前目录
6. PATH 环境变量中所列出的目录

#### **DLL 入口函数**

BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)

{

switch(fdwReason)

{

case DLL\_PROCESS\_ATTACH:

// 第一次将一个DLL映射到进程地址空间时调用

// The DLL is being mapped into the process' address space.

break;

case DLL\_THREAD\_ATTACH:

// 当进程创建一个线程的时候，用于告诉DLL执行与线程相关的初始化（非主线程执行）

// A thread is bing created.

break;

case DLL\_THREAD\_DETACH:

// 系统调用 ExitThread 线程退出前，即将终止的线程通过告诉DLL执行与线程相关的清理

// A thread is exiting cleanly.

break;

case DLL\_PROCESS\_DETACH:

// 将一个DLL从进程的地址空间时调用

// The DLL is being unmapped from the process' address space.

break;

}

return (TRUE); // Used only for DLL\_PROCESS\_ATTACH

}

#### **载入卸载库**

LoadLibrary、LoadLibraryExA、LoadPackagedLibrary、FreeLibrary、FreeLibraryAndExitThread 函数声明

#### **显示地链接到导出符号**

GetProcAddress 函数声明

#### **DumpBin.exe 查看 DLL 信息**

在 VS 的开发人员命令提示符 使用 DumpBin.exe 可查看 DLL 库的导出段（导出的变量、函数、类名的符号）、相对虚拟地址（RVA，relative virtual address）。如：

DUMPBIN -exports D:\mydll.dll

#### **LoadLibrary 与 FreeLibrary 流程图**

LoadLibrary 与 FreeLibrary 流程图

#### **DLL 库的编写（导出一个 DLL 模块）**

DLL 库的编写（导出一个 DLL 模块）

#### **DLL 库的使用（运行时动态链接 DLL）**

DLL 库的使用（运行时动态链接 DLL）

## 7.6 运行库（Runtime Library）

#### **典型程序运行步骤**

1. 操作系统创建进程，把控制权交给程序的入口（往往是运行库中的某个入口函数）
2. 入口函数对运行库和程序运行环境进行初始化（包括堆、I/O、线程、全局变量构造等等）。
3. 入口函数初始化后，调用 main 函数，正式开始执行程序主体部分。
4. main 函数执行完毕后，返回到入口函数进行清理工作（包括全局变量析构、堆销毁、关闭I/O等），然后进行系统调用结束进程。

一个程序的 I/O 指代程序与外界的交互，包括文件、管程、网络、命令行、信号等。更广义地讲，I/O 指代操作系统理解为 “文件” 的事物。

#### **glibc 入口**

\_start -> \_\_libc\_start\_main -> exit -> \_exit

其中 main(argc, argv, \_\_environ) 函数在 \_\_libc\_start\_main 里执行。

#### **MSVC CRT 入口**

int mainCRTStartup(void)

执行如下操作：

1. 初始化和 OS 版本有关的全局变量。
2. 初始化堆。
3. 初始化 I/O。
4. 获取命令行参数和环境变量。
5. 初始化 C 库的一些数据。
6. 调用 main 并记录返回值。
7. 检查错误并将 main 的返回值返回。

#### **C 语言运行库（CRT）**

大致包含如下功能：

* 启动与退出：包括入口函数及入口函数所依赖的其他函数等。
* 标准函数：有 C 语言标准规定的C语言标准库所拥有的函数实现。
* I/O：I/O 功能的封装和实现。
* 堆：堆的封装和实现。
* 语言实现：语言中一些特殊功能的实现。
* 调试：实现调试功能的代码。

#### **C语言标准库（ANSI C）**

包含：

* 标准输入输出（stdio.h）
* 文件操作（stdio.h）
* 字符操作（ctype.h）
* 字符串操作（string.h）
* 数学函数（math.h）
* 资源管理（stdlib.h）
* 格式转换（stdlib.h）
* 时间/日期（time.h）
* 断言（assert.h）
* 各种类型上的常数（limits.h & float.h）
* 变长参数（stdarg.h）
* 非局部跳转（setjmp.h）

# 八．Linux高级网络编程系列教程

**https://blog.csdn.net/u011545382/article/details/80348210**

**网络应用层编程**

## 8.1 网络协议入门



物理层：就是把电脑连接起来的物理手段。它主要规定了网络的一些电气特性，作用是负责传送 0 和 1 的电信。可以用光缆、电缆、双绞线、无线电波等方式。

链接层：链接层”的功能，它在“物理层”的上方，确定了 0 和 1 的分组方式。每家公司都有自己的电信号分组方式。逐渐地，一种叫做“以太网”（Ethernet）的协议，占据了主导地位。以太网规定，一组电信号构成一个数据包，叫做“帧”（Frame）。每一帧分成两个部分：标头（Head）和数据（Data）。“标头”的长度，固定为 18 字节。"数据"的长度，最短为 46 字节，最长为 1500 字节。因此，整个"帧"最短为 64 字节，最长为 1518 字节。如果数据很长，就必须分割成多个帧进行发送。网卡的地址，就是数据包的发送地址和接收地址，这叫做 MAC 地址。

网络层：以太网协议，依靠 MAC 地址发送数据。但是，这样做有一个重大的缺点。以太网采用广播方式发送数据包，所有成员人手一“包”，不仅效率低，而且局限在发送者所在的子网络。也就是说，如果两台计算机不在同一个子网络，广播是传不过去的。这种设计是合理的，否则互联网上每一台计算机都会收到所有包，那会引起灾难（广播风暴）。因此，必须找到一种方法，能够区分哪些 MAC 地址属于同一个子网络，哪些不是。如果是同一个子网络，就采用广播方式发送，否则就采用“路由”方式发送。这就导致了“网络层”的诞生。它的作用是引进一套新的地址，使得我们能够区分不同的计算机是否属于同一个子网络。这套地址就叫做“网络地址”，简称“网址”。网络地址帮助我们确定计算机所在的子网络，MAC 地址则将数据包送到该子网络中的目标网卡。因此，从逻辑上可以推断，必定是先处理网络地址，然后再处理 MAC 地址。互联网上的每一台计算机，都会分配到一个 IP 地址。这个地址分成两个部分，前一部分代表网络，后一部分代表主机。所谓“子网掩码”，就是表示子网络特征的一个参数。它在形式上等同于 IP 地址，也是一个 32 位二进制数字，它的网络部分全部为1，主机部分全部为0，并且1和0分别连续。知道“子网掩码”，我们就能判断，任意两个 IP 地址是否处在同一个子网络。方法是将两个 IP 地址与子网掩码分别进行 AND 运算（两个数位都为1，运算结果为1，否则为0），然后比较结果是否相同，如果是的话，就表明它们在同一个子网络中，否则就不是。比如，已知 IP 地址 172.16.254.1 和 172.16.254.233 的子网掩码都是 255.255.255.0，请问它们是否在同一个子网络？两者与子网掩码分别进行 AND 运算，结果都是 172.16.254.0，因此它们在同一个子网络。总结一下，IP 协议的作用主要有两个，一个是为每一台计算机分配 IP 地址，另一个是确定哪些地址在同一个子网络。IP 数据包也分为“标头”和“数据”两个部分。“标头”部分主要包括版本、长度、IP 地址等信息，“数据”部分则是 IP 数据包的具体内容。它放进以太网数据包后，以太网数据包就变成了下面这样。IP 数据包的“标头”部分的长度为 20 到 60 字节，整个数据包的总长度最大为 65,535字节。因此，理论上，一个 IP 数据包的“数据”部分，最长为 65,515字节。前面说过，以太网数据包的“数据”部分，最长只有 1500 字节。因此，如果 IP 数据包超过了 1500 字节，它就需要分割成几个以太网数据包，分开发送了。我们需要一种机制，能够从 IP 地址得到 MAC 地址。这里又可以分成两种情况。第一种情况，如果两台主机不在同一个子网络，那么事实上没有办法得到对方的 MAC 地址，只能把数据包传送到两个子网络连接处的“网关”（gateway），让网关去处理。第二种情况，如果两台主机在同一个子网络，那么我们可以用 ARP 协议，得到对方的 MAC 地址。ARP 协议也是发出一个数据包（包含在以太网数据包中），其中包含它所要查询主机的 IP 地址，在对方的 MAC 地址这一栏，填的是 FF:FF:FF:FF:FF:FF，表示这是一个“广播”地址。它所在子网络的每一台主机，都会收到这个数据包，从中取出 IP 地址，与自身的 IP 地址进行比较。如果两者相同，都做出回复，向对方报告自己的 MAC 地址，否则就丢弃这个包。总之，有了 ARP 协议之后，我们就可以得到同一个子网络内的主机 MAC 地址，可以把数据包发送到任意一台主机之上。

传输层：我们还需要一个参数，表示这个数据包到底供哪个程序（进程）使用。这个参数就叫做“端口”（port），它其实是每一个使用网卡的程序的编号。每个数据包都发到主机的特定端口，所以不同的程序就能取到自己所需要的数据。“端口”是 0 到 65535 之间的一个整数，正好 16 个二进制位。0到 1023 的端口被系统占用，用户只能选用大于 1023 的端口。不管是浏览网页还是在线聊天，应用程序会随机选用一个端口，然后与服务器的相应端口联系。“传输层”的功能，就是建立“端口到端口”的通信。相比之下，“网络层”的功能是建立“主机到主机”的通信。只要确定主机和端口，我们就能实现程序之间的交流。因此，Unix 系统就把主机+端口，叫做“套接字”（socket）。有了它，就可以进行网络应用程序开发了。在，我们必须在数据包中加入端口信息，这就需要新的协议。最简单的实现叫做 UDP 协议，它的格式几乎就是在数据前面，加上端口号。UDP 数据包，也是由“标头”和“数据”两部分组成。“标头”部分主要定义了发出端口和接收端口，“数据”部分就是具体的内容。然后，把整个 UDP 数据包放入 IP 数据包的“数据”部分，而前面说过，IP 数据包又是放在以太网数据包之中的。UDP 数据包非常简单，“标头”部分一共只有 8 个字节，总长度不超过 65,535字节，正好放进一个 IP 数据包。UDP 协议的优点是比较简单，容易实现，但是缺点是可靠性较差，一旦数据包发出，无法知道对方是否收到。为了解决这个问题，提高网络可靠性，TCP 协议就诞生了。这个协议非常复杂，但可以近似认为，它就是有确认机制的 UDP 协议，每发出一个数据包都要求确认。如果有一个数据包遗失，就收不到确认，发出方就知道有必要重发这个数据包了。TCP 数据包和 UDP 数据包一样，都是内嵌在 IP 数据包的“数据”部分。TCP 数据包没有长度限制，理论上可以无限长，但是为了保证网络的效率，通常 TCP 数据包的长度不会超过 IP 数据包的长度，以确保单个 TCP 数据包不必再。

应用层：应用程序收到“传输层”的数据，接下来就要进行解读。由于互联网是开放架构，数据来源五花八门，必须事先规定好格式，否则根本无法解读。“应用层”的作用，就是规定应用程序的数据格式。举例来说，TCP 协议可以为各种各样的程序传递数据，比如 Email、WWW、FTP 等等。那么，必须有不同协议规定电子邮件、网页、FTP 数据的格式，这些应用程序协议就构成了“应用层”。

## 8.2 无连接和面向连接协议的区别

网络编程中最基本的概念就是面向连接（connection-oriented）和无连接（connectionless）协议。这些术语指的并不是物理介质本身，而是用来说明如何在物理介质上传输数据的。它们的本质区别在于，对无连接协议来说，每个分组的处理都独立于所有其他分组，而对面向连接的协议来说，协议实现则维护了与后继分组有关的状态信息。

无连接协议中的分组被称为数据报（datagram），每个分组都是独立寻址，并由应用程序发送的。从协议的角度来看，每个数据报都是一个独立的实体，与在两个相同的对等实体之间传送的任何其他数据报都没有关系，这就意味着协议很可能是不可靠的。也就是说，网络会尽最大努力传送每一个数据报，但并不保证数据报不丢失、不延迟或者不错序传输。另一方面，面向连接的协议则维护了分组之间的状态，使用这种协议的应用程序通常都会进行长期的对话。记住这些状态，协议就可以提供可靠的传输。比如，发送端可以记住哪些数据已经发送出去了但还未被确认，以及数据是什么时候发送的。如果在某段时间间隔内没有收到确认，发送端可以重传数据。接收端可以记住已经收到了哪些数据，并将重复的数据丢弃。如果分组不是按序到达的，接收端可以将其保存下来，直到逻辑上先于它的分组到达为止。

典型的面向连接协议有三个阶段。第一阶段，在对等实体间建立连接。接下来是数据传输阶段，在这个阶段中，数据在对等实体间传输。最后，当对等实体完成数据传输时，连接被拆除。一种标准的类比是：使用无连接协议就像寄信，而使用面向连接的协议就像打电话。既然无连接协议有这么多的缺点，大家可能会奇怪，为什么还要使用这种协议呢？我们会看到，在很多情况下，使用无连接协议构建应用程序都是有意义的。比如，使用无连接协议可以很方便地支持一对多和多对一通信，而面向连接协议通常都需要多个独立的连接才能做到。但更重要的是，无连接协议是构建面向连接协议的基础。TCP 和 UDP 都是构建在 IP 之上的。因此，IP 是构建整个 TCP/IP 协议族的基础。但 IP 提供的是一种尽力而为的、不可靠的无连接服务。它接收来自其上层的分组，将它们封装在一个 IP 分组中，根据路由为分组选择正确的硬件接口，从这个接口将分组发送出去。一旦将分组发送出去了，IP 就不再关心这个分组了。和所有无连接协议一样，它将分组发送出去之后就不再记得这个分组了。

为了提供这种可靠性，TCP 向基本的 IP 服务中添加了三项功能：

首先，它为 TCP 段中的数据提供了校验和。这样有助于确保抵达目的地的数据在传输过程中不会被网络损坏。

第二，它为每字节分配了一个序列号，这样，如果数据抵达目的地时真的错序了，接收端也能够按照恰当的顺序将其重装起来。当然，TCP 并没有为每字节都附加一个序列号。实际上，每个 TCP 段的首部都包含了段中第一字节的序列号。这样，就隐含地知道了段中其他字节的序列号。

第三，TCP 提供另一方面，UDP 为编写应用程序的程序员提供了一种不可靠的无连接服务。事实上，UDP 只向底层的 IP 协议中添加了两项功能。

首先，它提供了一个可选的校验和来检测数据的损坏情况。尽管 IP 也有校验和，但它只对 IP 分组首部进行计算，所以，TCP 和 UDP 也都提供了校验和来保护它们自己的首部和数据。

其次，UDP 向 IP添加的第二项特性就是端口的概念。了一种确认-重传机制，以确保最终每个段都会被传送出去。

## 8.3 网络字节序、地址转换

字节序是指多字节数据的存储顺序，在设计计算机系统的时候，有两种处理内存中数据的方法：大端格式、小端格式。

小端格式(Little-Endian)：将低位字节数据存储在低地址。

大端格式(Big-Endian)：将高位字节数据存储在低地址。

网络字节序定义：收到的第一个字节被当作高位看待，这就要求发送端发送的第一个字节应当是高位。而在发送端发送数据时，发送的第一个字节是该数字在内存中起始地址对应的字节。可见多字节数值在发送前，在内存中数值应该以大端法存放。

所以，网络协议指定了通讯字节序：大端。只有在多字节数据处理时才需要考虑字节序，运行在同一台计算机上的进程相互通信时，一般不用考虑字节序，异构计算机之间通讯，需要转换自己的字节序为网络字节

## 8.4 套接字的介绍

套接字的特性有三个属性确定，它们是：域（domain），类型（type），和协议（protocol）。

域：

指定套接字通信中使用的网络介质。最常见的套接字域是 AF\_INET（IPv4）或者AF\_INET6(IPV6)，它是指 Internet 网络，许多 Linux 局域网使用的都是该网络，当然，因特网自身用的也是它。

套接字类型：

流套接字（SOCK\_STREAM）：

流套接字用于提供面向连接、可靠的数据传输服务。该服务将保证数据能够实现无差错、无重复发送，并按顺序接收。流套接字之所以能够实现可靠的数据服务，原因在于其使用了传输控制协议，即TCP（The Transmission Control Protocol）协议。

数据报套接字（SOCK\_DGRAM）：

数据报套接字提供了一种无连接的服务。该服务并不能保证数据传输的可靠性，数据有可能在传输过程中丢失或出现数据重复，且无法保证顺序地接收到数据。数据报套接字使用UDP（User Datagram Protocol）协议进行数据的传输。由于数据报套接字不能保证数据传输的可靠性，对于有可能出现的数据丢失情况，需要在程序中做相应的处理。

原始套接字（SOCK\_RAW）：

原始套接字与标准套接字（标准套接字指的是前面介绍的流套接字和数据报套接字）的区别在于：原始套接字可以读写内核没有处理的IP数据包，而流套接字只能读取TCP协议的数据，数据报套接字只能读取UDP协议的数据。因此，如果要访问其他协议发送数据必须使用原始套接字。

套接字协议（协议类别）：

只要底层的传输机制允许不止一个协议来提供要求的套接字类型，我们就可以为套接字选择一个特定的协议。通常使用默认即可（也就是最后一个参数填“0”）。

#include <sys/socket.h>

int socket(int family,int type,int protocol);

family：协议族（AF\_UNIX、AF\_INET、AF\_INET6、PF\_PACKET等）

type：套接字类型（SOCK\_STREAM、SOCK\_DGRAM、SOCK\_RAW等）

protocol：协议类别（0、IPPROTO\_TCP、IPPROTO\_UDP等），设为 0 表示使用默认协议。

## 8.5 浅谈 C/S 和 B/S 架构

C/S架构软件（即客户机/服务器模式）分为客户机和服务器两层：第一层是在客户机系统上结合了表示与业务逻辑，第二层是通过网络结合了数据库服务器。简单的说就是第一层是用户表示层，第二层是数据库层。

B/S型模式，即浏览器/服务器结构。它是C/S架构的一种改进，可以说属于三层C/S架构。主要是利用了不断成熟的WWW浏览器技术，用通用浏览器就实现了原来需要复杂专用软件才能实现的强大功能，并节约了开发成本，是一种全新的软件系统构造技术。

## 8.6 UDP编程

客户端：创建fd，绑定server 得ip，sendto数据

服务端：创建fd，bind绑定网卡ip，recvfrom数据

绑定( bind )端口需要注意的问题

需要注意的是，一个网络应用程序只能绑定一个端口( 一个套接字只能 绑定一个端口 )。如果客户端想绑定端口号，一定要调用发送信息函数之前绑定( bind )端口，因为在发送信息函数( sendto, 或 write )，系统会自动给当前网络程序分配一个随机端口号，这相当于随机绑定了一个端口号，这里只会分配一次，以后通信就以这个随机端口通信，我们再绑定端口号的话，就会绑定失败。如果我们放在发送信息函数( sendto, 或 write )之前绑定，那样程序将以我们绑定的端口号发送信息，不会再随机分配一个端口号。

## 8.7 广播

网络上的广播指：由一台主机向该主机所在子网内（同一个[局域网](http://baike.baidu.com/link?url=o-mzKpdjU2rkaEAPcvsUVDBl1Lp-y_TD3IyWox716eADVkOg0oVNNrJRFcuw6JXsgzMaUm5qBBwfUtU1OHSJQK)）的所有主机发送数据的方式。如下图的 1 号主机广播给 2、3、4、5 号主机发送数据。广播地址(Broadcast Address)是专门用于同时向网络中（通常指同一子网）所有工作站进行发送的一个地址。

在使用TCP/IP 协议的网络中，主机标识段host ID（简称主机 ID） 为全 1 的 IP 地址为广播地址，广播的分组传送给同一个子网的所有计算机。对于10.1.1.0 （255.255.255.0 ）网段，其广播地址为10.1.1.255 （255 即为 2 进制的 11111111 ），当发出一个目的地址为10.1.1.255 的数据包时，它将被分发给该网段上的所有计算机。广播地址应用于网络内的所有主机。

广播地址主要有两类：

1)受限广播

路由器不会转发受限广播的数据包，但同一个子网的所有主机都会接收到受限广播的数据包。IP 地址的网络字段和主机字段全为 1 就是受限广播地址255.255.255.255。

1. 直接广播（也叫定向广播）

直接广播可以被路由转发，发送到目标网络的所有主机，如：ip地址为 192.168.2.1 的主机也可以发送广播到192.168.1.0这个网络。当然不是所有的路由器，傻瓜式路由器是默认阻止直接广播的。IP 地址的网络字段定义这个网络，主机字段通常全为 1，如192.168.10.0/24 的直接广播（定向广播）地址为：192.168.10.255。

四种 IP 广播地址

受限的广播地址

受限的广播地址是255.255.255.255。该地址用于主机配置过程中IP数据包的目的地址，此时，主机可能还不知道它所在网络的网络掩码，甚至连它的IP地址也不知道。在任何情况下，路由器都不转发目的地址为受限的广播地址的数据报，这样的数据报仅出现在本地网络中。

指向网络的广播

指向网络的广播地址是主机号为全1的地址。A类网络广播地址为netid.255.255.255，其中netid为A类网络的网络号。一个路由器可以设置是否转发这个广播地址的数据。

指向子网的广播

指向子网的广播地址为主机号为全1且有特定子网号的地址。作为子网直接广播地址的IP地址需要了解子网的掩码。例如，如果路由器收到发往128.1.2.255的数据报，当B类网络128.1的子网掩码为255.255.255.0时，该地址就是指向子网的广播地址；但如果该子网的掩码为255.255.254.0，该地址就不是指向子网的广播地址。在划分为子网的网络中指向子网的广播地址限于表示特定子网上的主机。

指向所有子网的广播

指向所有子网的广播也需要了解目的网络的子网掩码，以便与指向网络的广播地址区分开。指向所有子网的广播地址的子网号及主机号为全1。例如，如果目的子网掩码为255.255.255.0，那么IP地址128.1.255.255是一个指向所有子网的广播地址。然而，如果网络没有划分子网，这就是一个指向网络的广播。这一类型的地址现在已经基本不使用了，而由D类组播地址所取代。

广播特点

对于一个带网卡设备的主机，它能接收到哪些网络数据包呢？

1）网卡会接收目的 ip 和它的 ip 地址相同的数据包（至于能不能到应用层我们暂时不管，至于MAC地址如何确定我们暂时也不管），这个就是单播传输数据。

2）网卡会接收到目的 ip 为广播地址数据包，这个广播地址的 MAC 地址为：ff:ff:ff:ff:ff:ff 。

3）如果这个主机加入了多播组，它也会接收该多播组地址的数据包

UDP 广播特点如下：处于同一子网的所有主机都必须处理数据。UDP 数据包会沿协议栈向上一直到 UDP 层，因为到 UDP 层，端口不匹配的话，数据才丢弃，如下图，所以，运行音视频等较高速率工作的应用，会带来较大的负担。

默认的情况下，不允许发送广播数据包，需要修改套接口选项：

int setsockopt( int sockfd, int level, int optname, const void \*optval, socklen\_t optlen);

设置套接字选项



## 8.8 多播

IP 多播（也称多址广播或组播）技术，是一种允许一台或多台主机（多播源）发送单一数据包到多台主机（一次的，同时的）的 TCP/IP 网络技术。多播是 IPv6 数据包的 3 种基本目的地址类型之一，多播是一点对多点的通信,　IPv6 没有采用 IPv4 中的组播术语，而是将广播看成是多播的一个特殊例子。

IP 多播应用大致可以分为三类: 点对多点应用，多点对点应用和多点对多点应用。

1）点对多点应用是指一个发送者，多个接收者的应用形式，这是最常见的多播应用形式。典型的应用包括：媒体广播、媒体推送、信息缓存、事件通知和状态监视等。

2）多点对点应用是指多个发送者，一个接收者的应用形式。通常是双向请求响应应用，任何一端（多点或点）都有可能发起请求。典型应用包括：资源查找、数据收集、网络竞拍、信息询问等。

3）多点对多点应用是指多个发送者和多个接收者的应用形式。通常，每个接收者可以接收多个发送者发送的数据，同时，每个发送者可以把数据发送给多个接收者。典型应用包括：多点会议、资源同步、并行处理、协同处理、远程学习、讨论组、分布式交互模拟（DIS）、多人游戏。

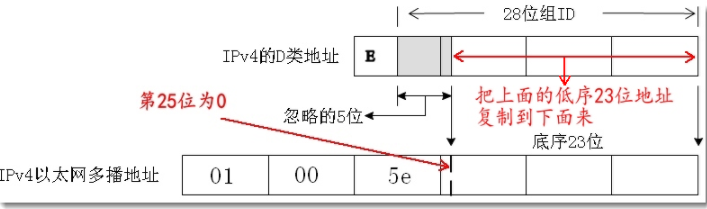
IP 多播通信必须依赖于 IP 多播地址，在 IPv4 中它是一个 D 类 IP 地址，范围从 224.0.0.0 到 239.255.255.255，并被划分为局部链接多播地址、预留多播地址和管理权限多播地址三类：

1）局部链接多播地址范围在 224.0.0.0~224.0.0.255，这是为路由协议和其它用途保留的地址，路由器并不转发属于此范围的IP包；

2）预留多播地址为 224.0.1.0~238.255.255.255，可用于全球范围（如Internet）或网络协议；

3）管理权限多播地址为 239.0.0.0~239.255.255.255，可供组织内部使用，类似于私有 IP 地址，不能用于 Internet，可限制多播范围。

使用同一个 IP 多播地址接收多播数据包的所有主机构成了一个主机组，也称为多播组。一个多播组的成员是随时变动的，一台主机可以随时加入或离开多播组，多播组成员的数目和所在的地理位置也不受限制，一台主机也可以属于几个多播组。多播地址与 MAC 地址的映射：IPv4 的 D 类地址是多播地址。IEEE 把一块以太网多播组地址分给 IANA 以支持IP多播。块的地址都以 01:00:5e 开头，第 25 位为 0，低 23 位为 IPv4 多播地址( D类地址 )的低 23 位。IPv4 多播地址与 MAC 地址的映射关系如图所示：



由于多播地址( D类地址 )中的最高 5bit 在映射过程中被忽略，因此每个以太网多播地址对应的多播组是不唯一的。32 个不同的多播组号被映射为一个以太网地址。例如，多播地址 224.128.64.32（十六进制 e0.80.40.20）和 224.0.64.32（十六进制 e0.00.40.20）都映射为同一以太网地址 01:00:5e:00:40:20。既然地址映射是不唯一的，那么设备驱动程序或 IP 层就必须对数据报进行过滤。

Setsockopt



多播只能用 UDP 或原始 IP 实现，不能用 TCP。

struct ip\_mreq mreq; // 多播地址结构体

// 加入多播组，相当于创建一个QQ群，某人加入此群

mreq.imr\_multiaddr.s\_addr = inet\_addr(group); // 多播地址，类似于 QQ 群号

mreq.imr\_interface.s\_addr = htonl(INADDR\_ANY);// 将本机加入多播组，类似于某人加入此群

// 加入多播组

err = setsockopt(sockfd, IPPROTO\_IP, IP\_ADD\_MEMBERSHIP,&mreq, sizeof(mreq));

## 8.9 TCP客户端

TCP（Transmission Control Protocol 传输控制协议）是一种面向连接的、可靠的、基于字节流的传输层通信协议。

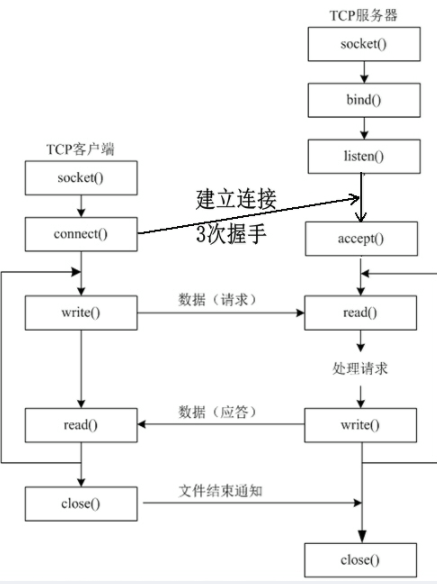
TCP 具有以下特点：

1）电话系统服务模式的抽象

2）每一次完整的数据传输都要经过建立连接、使用连接、终止连接的过程

3）可靠、出错重传、且每收到一个数据都要给出相应的确认，保证数据传输的可靠性

基于 TCP 的网络编程开发分为服务器端和客户端两部分，常见的核心步骤和流程如下：



对于 TCP 客户端编程流程，有点类似于打电话过程：

1.找个可以通话的手机(socket() )

2.拨通对方号码并确定对方是自己要找的人（ connect() ）

3.主动聊天（ send() 或 write() ）

4.或者，接收对方的回话（ recv() 或read() ）

5.通信结束后，双方说再见挂电话（close() ）

## 8.10 TCP服务器

1.具备一个可以确知的地址（ bind() ）：相当于我们要明确知道移动客服的号码，才能给他们电话;

2.让操作系统知道是一个服务器，而不是客户端（ listen() ）：相当于移动的客服，他们主要的职责是被动接听用户电话，而不是主动打电话骚扰用户；

3.等待连接的到来（ accept() ）：移动客服时刻等待着，来一个客户接听一个。

1.找个可以通话的手机（socket() ）

2.插上电话卡固定一个号码（ bind() ）

3.职责为被动接听，给手机设置一个铃声来监听是否有来电（ listen()）

4. 有来电，确定双方的关系后，才真正接通不挂电话（ accept() ）

5. 接听对方的诉说（ recv() ）

6.适当给些回话（ send() ）

7.通信结束后，双方说再见挂电话（ close()）。

int bind( int sockfd, const struct sockaddr \*myaddr，socklen\_t addrlen );

将本地协议地址与 sockfd 绑定，这样 ip、port 就固定了.注意：bind只能绑定自身的地址及端口

int listen(int sockfd, int backlog);

将套接字由主动修改为被动，使操作系统为该套接字设置一个连接队列，用来记录所有连接到该套接字的连接。

int accept( int sockfd, struct sockaddr \*cliaddr, socklen\_t \*addrlen ); //返回值是从socket中establish中建立连接的fd

从已连接队列中取出一个已经建立的连接，如果没有任何连接可用，则进入睡眠等待（阻塞）。

使用 close() 函数即可关闭套接字，关闭一个代表已连接套接字将导致另一端接收到一个 0 长度的数据包。做服务器时关闭监听套接字（ socket()和listen()之后的套接字 ）将导致服务器无法接收新的连接，但不会影响已经建立的连接；关闭 accept()返回的已连接套接字将导致它所代表的连接被关闭，但不会影响服务器的监听（ socket()和listen()之后的套接字 ）。做客户端时关闭连接就是关闭连接，不意味着其他。

如果客户端和服务器已经连接成功的前提下，通常的情况下，先关闭客户端，再关闭服务器，如果是先关闭服务器，立马启动服务器是，服务器绑定的端口不会立马释放（如下图），要过 1 分钟左右才会释放。

## 8.11 tcp、udp迭代服务器

目前最常用的服务器模型有：

迭代服务器：服务器在同一时刻只能响应一个客户端的请求

并发服务器：服务器在同一时刻可以响应多个客户端的请求

UDP 循环服务器每次从套接字上读取一个客户端的请求 -> 处理 -> 然后将结果返回给客户机。

TCP 迭代服务器接受一个客户端的连接，然后处理，完成了这个客户的所有请求后，断开连接。TCP 迭代服务器一次只能处理一个客户端的请求，只有在这个客户的所有请求满足后，服务器才可以继续后面的请求。如果有一个客户端占住服务器不放时，其它的客户机都不能工作了，因此，TCP 服务器一般很少用迭代服务器模型的。

## 8.12 浅谈 TCP三次握手和四次挥手

tcp协议格式



16位源端口号：16位的源端口中包含初始化通信的端口。源端口和源IP地址的作用是标识报文的返回地址。

16位目的端口号：16位的目的端口域定义传输的目的。这个端口指明报文接收计算机上的应用程序地址接口。

32位序号：32位的序列号由接收端计算机使用，重新分段的报文成最初形式。当SYN出现，序列码实际上是初始序列码（Initial Sequence Number，ISN），而第一个数据字节是ISN+1。这个序列号（序列码）可用来补偿传输中的不一致。

32位确认序号：32位的序列号由接收端计算机使用，重组分段的报文成最初形式。如果设置了ACK控制位，这个值表示一个准备接收的包的序列码。

4位首部长度：4位包括TCP头大小，指示何处数据开始。

保留（6位）：6位值域，这些位必须是0。为了将来定义新的用途而保留。

标志：6位标志域。表示为：紧急标志、有意义的应答标志、推、重置连接标志、同步序列号标志、完成发送数据标志。按照顺序排列是：URG、ACK、PSH、RST、SYN、FIN。

16位窗口大小：用来表示想收到的每个TCP数据段的大小。TCP的流量控制由连接的每一端通过声明的窗口大小来提供。窗口大小为字节数，起始于确认序号字段指明的值，这个值是接收端正期望接收的字节。窗口大小是一个16字节字段，因而窗口大小最大为65535字节。

16位校验和：16位TCP头。源机器基于数据内容计算一个数值，收信息机要与源机器数值 结果完全一样，从而证明数据的有效性。检验和覆盖了整个的TCP报文段：这是一个强制性的字段，一定是由发送端计算和存储，并由接收端进行验证的。

16位紧急指针：指向后面是优先数据的字节，在URG标志设置了时才有效。如果URG标志没有被设置，紧急域作为填充。加快处理标示为紧急的数据段。

选项：长度不定，但长度必须为1个字节。如果没有选项就表示这个1字节的域等于0。

数据：该TCP协议包负载的数据。

在上述字段中，6位标志域的各个选项功能如下。

URG：紧急标志。紧急标志为"1"表明该位有效。

ACK：确认标志。表明确认编号栏有效。大多数情况下该标志位是置位的。TCP报头内的确认编号栏内包含的确认编号（w+1）为下一个预期的序列编号，同时提示远端系统已经成功接收所有数据。

PSH：推标志。该标志置位时，接收端不将该数据进行队列处理，而是尽可能快地将数据转由应用处理。在处理Telnet或rlogin等交互模式的连接时，该标志总是置位的。

RST：复位标志。用于复位相应的TCP连接。

SYN：同步标志。表明同步序列编号栏有效。该标志仅在三次握手建立TCP连接时有效。它提示TCP连接的服务端检查序列编号，该序列编号为TCP连接初始端（一般是客户端）的初始序列编号。在这里，可以把TCP序列编号看作是一个范围从0到4，294，967，295的32位计数器。通过TCP连接交换的数据中每一个字节都经过序列编号。在TCP报头中的序列编号栏包括了TCP分段中第一个字节的序列编号。

FIN：结束标志。

三次握手

在 TCP/IP 协议中，TCP 协议提供可靠的连接服务，采用三次握手建立一个连接。

第一次握手：建立连接时，客户端发送 syn 包(tcp协议中syn位置1，序号为J)到服务器，并进入 SYN\_SEND 状态，等待服务器确认；

第二次握手：服务器收到 syn 包，必须确认客户的 SYN，同时自己也发送一个 SYN 包，即 SYN+ACK包（tcp协议中syn位置1，ack位置1，序号K，确定序号为J+1），此时服务器进入 SYN\_RECV 状态；

第三次握手：客户端收到服务器的 SYN＋ACK 包，向服务器发送确认包 ACK(tcp协议中ack位置1，确认序号K+1)，此包发送完毕，客户端和服务器进入 ESTABLISHED 状态，完成三次握手。

通过这样的[三次握手](http://baike.baidu.com/link?url=eZXiFRQOKsO6NUMErlv_ourWMexrPfxtUhSw1f5waWf_gVDDeOpI7xFga2VygpC-qZWFVkj-XTcQeKx7UQO7fq)，客户端与服务端建立起可靠的双工的连接，开始传送数据。 ****三次握手的最主要目的是保证连接是双工的，可靠更多的是通过重传机制来保证的。****

四次挥手

由于 TCP 连接是全双工的，因此每个方向都必须单独进行关闭。这好比，我们打电话（全双工），正常的情况下（出于礼貌），通话的双方都要说再见后才能挂电话，保证通信双方都把话说完了才挂电话。

1）客户端 A 在应用层调用close时会激发底层发送一个 FIN（tcp协议中FIN位置1、序号为M，结合上图分析）请求，用来关闭客户 A 到服务器 B 的数据传送，客户端A此时处于半关闭状态（应用层无法接收数据但底层还可以接收数据）；

2）服务器 B 底层收到客户端A的FIN时会做两件事

2.1)第1件事：收到客户端A的FIN时底层会主动回发一个ACK（tcp协议中ACK位置1，确认序号M+1）

2.2)第2件事：收到客户端A的FIN时，导致服务器B的应用层read()返回0（告诉服务器B应用层：客户端A关闭了）

3）服务器B应用层调用close()激发底层给客户端 A 发送一个 FIN（tcp协议中FIN位置1、序号为N）,这是服务器B已处于半关闭状态;

4）客户端 A 底层回发 ACK（tcp协议中ACK位置1，确认序号N+1） 给服务器B，这是客户端A、服务器B都处于完全关闭状态，回收相应的资源。

****为什么建立连接协议是三次握手，而关闭连接却是四次握手呢？****

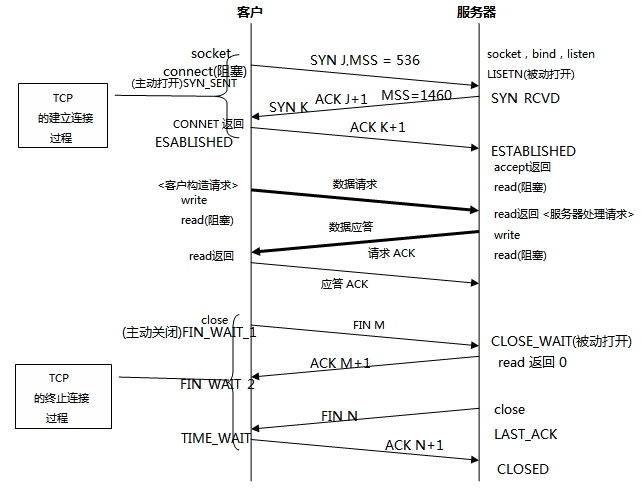
这是因为服务端的 LISTEN 状态下的 SOCKET 当收到 SYN 报文的建连请求后，它可以把 ACK 和 SYN（ACK 起应答作用，而 SYN 起同步作用）放在一个报文里来发送。但关闭连接时，当收到FIN 报文通知时，如果能将ACK、FIN放在一个报文里那么就有了三次挥手，但是这是不可能，因为ACK是服务器B一收到FIN报文底层就回发的，而服务器B的FIN是应用层调用close()激发的，所以它这里的 ACK 报文和 FIN 报文在发送的时间上都是分开的，不可能同时发送。

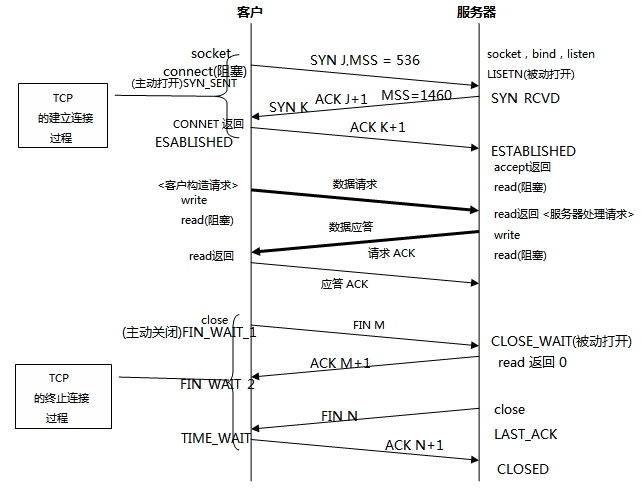
****为什么 TIME\_WAIT 状态还需要等 2MS L后才能返回到 CLOSED 状态？****

这是因为虽然双方都同意关闭连接了，而且握手的 4 个报文也都协调和发送完毕，按理可以直接回到 CLOSED 状态（就好比从 SYN\_SEND 状态到 ESTABLISH 状态那样）；但是因为我们必须要假想网络是不可靠的，你无法保证你最后发送的 ACK 报文会一定被对方收到，因此对方处于 LAST\_ACK 状态下的 SOCKET 可能会因为超时未收到 ACK 报文，而重发 FIN 报文，所以这个 TIME\_WAIT 状态的作用就是用来重发可能丢失的 ACK 报文。

## 8.13 TCP 通信过程中各步骤的状态

<https://blog.csdn.net/lianghe_work/article/details/46460463>





CLOSED: 这个没什么好说的了，表示初始状态。

LISTEN: 这个也是非常容易理解的一个状态，表示服务器端的某个 SOCKET 处于监听状态，可以接收连接了。

SYN\_RCVD: 这个状态表示接收到了 SYN 报文，在正常情况下，这个状态是服务器端的SOCKET 在建立 TCP 连接时的三次握手会话过程中的一个中间状态，很短暂，基本上用 netstat 你是很难看到这种状态的，除非你特意写了一个客户端测试程序，故意将三次 TCP 握手过程中最后一个 ACK 报文不予发送。因此这种状态时，当收到客户端的 ACK 报文后，它会进入到 ESTABLISHED 状态。

SYN\_SENT: 这个状态与 SYN\_RCVD 相呼应，当客户端 SOCKET 执行 CONNECT 连接时，它首先发送 SYN 报文，因此也随即它会进入到了 SYN\_SENT 状态，并等待服务端的发送三次握手中的第 2 个报文。SYN\_SENT 状态表示客户端已发送 SYN 报文。

ESTABLISHED：这个容易理解了，表示连接已经建立了。

FIN\_WAIT\_1: 这个状态要好好解释一下，其实 FIN\_WAIT\_1 和 FIN\_WAIT\_2 状态的真正含义都是表示等待对方的 FIN 报文。而这两种状态的区别是：FIN\_WAIT\_1 状态实际上是当 SOCKET 在 ESTABLISHED 状态时，它想主动关闭连接，向对方发送了 FIN 报文，此时该 SOCKET 即进入到 FIN\_WAIT\_1 状态。而当对方回应 ACK 报文后，则进入到 FIN\_WAIT\_2 状态，当然在实际的正常情况下，无论对方何种情况下，都应该马 上回应 ACK 报文，所以 FIN\_WAIT\_1 状态一般是比较难见到的，而 FIN\_WAIT\_2 状态还有时常常可以用 netstat 看到。

FIN\_WAIT\_2：上面已经详细解释了这种状态，实际上 FIN\_WAIT\_2 状态下的 SOCKET，表示半连接，也即有一方要求 close 连接，但另外还告诉对方，我暂时还有点数据需要传送给你，稍后再关闭连接

TIME\_WAIT: 表示收到了对方的 FIN 报文，并发送出了 ACK 报文，就等 2MSL 后即可回到 CLOSED 可用状态了。如果 FIN\_WAIT\_1 状态下，收到了对方同时带 FIN 标志和ACK 标志的报文时，可以直接进入到 TIME\_WAIT 状态，而无须经过 FIN\_WAIT\_2 状态。

CLOSING(图中没有标志这种状态): 这种状态比较特殊，实际情况中应该是很少见，属于一种比较罕见的例外状态。正常情况下，当你发送 FIN 报文后，按理来说是应该先收到（或同时收到）对方的 ACK 报文，再收到对方的 FIN 报文。但是 CLOSING 状态表示你发送 FIN 报文后，并没有收到对方的 ACK 报文，反而却也收到了对方的 FIN 报文。什么情况下会出现此种情况呢？其实细想一下，也不难得出结论：那就是如果双方几乎在同时close一个 SOCKET 的话，那么就出现了双方同时发送 FIN 报文的情况，也即会出现 CLOSING 状态，表示双方都正在关闭 SOCKET 连接。

CLOSE\_WAIT: 这种状态的含义其实是表示在等待关闭。怎么理解呢？当对方 close 一个 SOCKET 后发送 FIN 报文给自己，你系统毫无疑问地会回应一个 ACK 报文给对方，此时则进入到 CLOSE\_WAIT 状态。接下来呢，实际上你真正需要考虑的事情是察看你是否还有数据发送给对方，如果没有的话，那么你也就可以 close 这个 SOCKET，发送 FIN 报文给对方，也即关闭连接。所以你在 CLOSE\_WAIT 状态下，需要完成的事情是等待你去关闭连接。

LAST\_ACK: 这个状态还是比较容易好理解的，它是被动关闭一方在发送 FIN 报文后，最后等待对方的 ACK 报文。当收到 ACK 报文后，也即可以进入到 CLOSED 可用状态了。

## 8.14 connect()、listen()和accept()三者之间的关系

对于客户端的 connect() 函数，该函数的功能为客户端主动连接服务器，建立连接是通过三次握手，而这个连接的过程是由内核完成，不是这个函数完成的，这个函数的作用仅仅是通知 Linux 内核，让 Linux 内核自动完成 TCP 三次握手连接（三次握手详情，请看《浅谈 TCP 三次握手》），最后把连接的结果返回给这个函数的返回值（成功连接为0， 失败为-1）。

通常的情况，客户端的 connect() 函数默认会一直阻塞，直到三次握手成功或超时失败才返回（正常的情况，这个过程很快完成）。

对于服务器，它是被动连接的。举一个生活中的例子，通常的情况下，移动的客服（相当于服务器）是等待着客户（相当于客户端）电话的到来。而这个过程，需要调用listen()函数。listen() 函数的主要作用就是将套接字( sockfd )变成被动连接的监听套接字（被动等待客户端的连接），至于参数 backlog 的作用是设置内核中连接队列的长度（这个长度有什么用，后面做详细的解释），TCP 三次握手也不是由这个函数完成，listen()的作用仅仅告诉内核一些信息。这里需要注意的是，listen()函数不会阻塞，它主要做的事情为，将该套接字和套接字对应的连接队列长度告诉 Linux 内核，然后，listen()函数就结束。这样的话，当有一个客户端主动连接（connect()），Linux 内核就自动完成TCP 三次握手，将建立好的链接自动存储到队列中，如此重复。所以，只要 TCP 服务器调用了 listen()，客户端就可以通过 connect() 和服务器建立连接，而这个连接的过程是由内核完成。

这里详细的介绍一下 listen() 函数的第二个参数（ backlog）的作用：告诉内核连接队列的长度。

为了更好的理解 backlog 参数，我们必须认识到内核为任何一个给定的监听套接口维护一个队列，该队列由两部分构成，分别是完成连接接队列、未完成连接队列：

1、未完成连接队列（incomplete connection queue），当服务器每收到客户端的一个SYN分节，就会将该客户端放入未完成连接队列，而服务器套接口处于 SYN\_RCVD 状态。

2、已完成连接队列（completed connection queue），当客户端和服务器彻底完成三次握手过程，客户端将从未完成连接队列升级成已完成连接队列，并从未完成连接队列中清空该客户端，这些套接口处于 ESTABLISHED 状态。

accept()函数功能是，从连接队列头部取出一个已经完成的连接，如果这个队列没有已经完成的连接，accept()函数就会阻塞，直到取出队列中已完成的用户连接为止。如果，服务器不能及时调用 accept() 取走队列中已完成的连接，队列满掉后会怎样呢？UNP（《unix网络编程》）告诉我们，服务器的连接队列满掉后，服务器不会对再对建立新连接的syn进行应答，所以客户端的 connect 就会返回 ETIMEDOUT。但实际上Linux的并不是这样的！TCP 的连接队列满后，Linux 不会如书中所说的拒绝连接，只是有些会延时连接，写程序时服务器的 listen() 的第二个参数最好还是根据需要填写，写太大不好（具体可以看cat /proc/sys/net/core/somaxconn，默认最大值限制是 128），浪费资源，写太小也不好，延时建立连接。

## 8.15 I/O复用之select详解

I/O复用概念：解决进程或线程阻塞到某个 I/O 系统调用而出现的技术，使进程不阻塞于某个特定的 I/O 系统调。

I/O复用使用的场合：

1.当客户处理多个描述符（通常是交互式输入、网络套接字）时，必须使用I/O复用。

2.tcp服务器既要处理监听套接字，又要处理已连接套接字，一般要使用I/O复用。

3.如果一个服务器既要处理tcp又要处理udp，一般要使用I/O复用。

4.如果一个服务器要处理多个服务或多个服务时，一般要使用I/O复用。

select函数介绍：

int select(int maxfd, fd\_set \*readset, fd\_set \*writeset, fd\_set \*exceptset, const struct timeval \*timeout);

功能：轮询扫描多个描述符中的任一描述符是否发生响应，或经过一段时间后唤醒

参数：

参数 名称 说明

maxfd 指定要检测的描述符的范围 所检测描述符最大值+1

readset可读描述符集监测该集合中的任意描述符是否有数据可读

writeset可写描述符集监测该集合中的任意描述符是否有数据可写

exceptset异常描述符集监测该集合中的任意描述符是否发生异常

timeout超时时间超过规定时间后唤醒

返回值：

0：超时

-1：出错

>0：准备好的文件描述符数量

select()函数能对多个文件描述符进行监测，如果一个参数对应一个描述符，那么select函数的4个参数最多能监测4个文件描述，那他如何实现对多个文件描述符的监测的呢？大家想一想文件描述符基本具有3种特性（读、写、异常），如果我们统一将监测可读的描述符放入可读集合（readset），监测可写的描述符放入可写集合（writeset），监测异常的描述符放入异常集合（exceptset）。然后将这3个集合传给select函数，是不是就可监测多个描述符呢.

集合操作函数

/初始化描述符集

void FD\_ZERO(fd\_set \*fdset);

//将一个描述符添加到描述符集

void FD\_SET(int fd, fd\_set \*fdset); FD\_SET(0, &rset);//将标准输入添加到文件描述符聚合变量中

//将一个描述符从描述符集中删除

void FD\_CLR(int fd, fd\_set \*fdset);

//检测指定的描述符是否有事件发生

int FD\_ISSET(int fd, fd\_set \*fdset);

while(1)

{

fd\_set rset;//创建一个描述符集rset

FD\_ZERO(&rset);//对描述符集rset清零

FD\_SET(0, &rset);//将描述符0加入到描述符集rset中

FD\_SET(4, &rset);//将描述符4加入到描述符集rset中

FD\_SET(5, &rset);//将描述符5加入到描述符集rset中

if(select(5+1, &rset, NULL, NULL, NULL) > 0)

{

if(FD\_ISSET(0, &rset))

{

//描述符0可读及相应的处理代码

}

if(FD\_ISSET(4, &rset))

{

//描述符4可读及相应的处理代码

}

if(FD\_ISSET(5, &rset))

{

//描述符5可读及相应的处理代码

}

}

}

select优点：

目前几乎在所有的平台上支持，其良好跨平台支持也是它的一个优点

select缺点：

1.每次调用 select()，都需要把 fd 集合从用户态拷贝到内核态，这个开销在 fd 很多时会很大，同时每次调用 select() 都需要在内核遍历传递进来的所有 fd，这个开销在 fd 很多时也很大。

2.单个进程能够监视的文件描述符的数量存在最大限制，在 Linux 上一般为 1024，可以通过修改宏定义甚至重新编译内核的方式提升这一限制，但是这样也会造成效率的降低

## 8.16 I/O复用之poll函数

select() 和 poll() 系统调用的本质一样，poll() 的机制与 select() 类似，与 select() 在本质上没有多大差别，管理多个描述符也是进行轮询，根据描述符的状态进行处理，但是 poll() 没有最大文件描述符数量的限制（但是数量过大后性能也是会下降）。poll() 和 select() 同样存在一个缺点就是，包含大量文件描述符的数组被整体复制于用户态和内核的地址空间之间，而不论这些文件描述符是否就绪，它的开销随着文件描述符数量的增加而线性增大。

int poll(struct pollfd \*fds, nfds\_t nfds, int timeout);

监视并等待多个文件描述符的属性变化

fds:指向一个结构体数组的第0个元素的指针，每个数组元素都是一个struct pollfd结构，用于指定测试某个给定的fd的条件

struct pollfd{

int fd; //文件描述符

short events; //等待的事件

short revents; //实际发生的事件

};

fd：每一个 pollfd 结构体指定了一个被监视的文件描述符，可以传递多个结构体，指示 poll() 监视多个文件描述符。

events：指定监测fd的事件（输入、输出、错误），每一个事件有多个取值，如下

revents：revents 域是文件描述符的操作结果事件，内核在调用返回时设置这个域。events 域中请求的任何事件都可能在 revents 域中返回.



注意：每个结构体的 events 域是由用户来设置，告诉内核我们关注的是什么，而 revents 域是返回时内核设置的，以说明对该描述符发生了什么事件

nfds:用来指定第一个参数数组元素个数

timeout: 指定等待的毫秒数，无论 I/O 是否准备好，poll() 都会返回.

返回值：

成功时，poll() 返回结构体中 revents 域不为 0 的文件描述符个数；如果在超时前没有任何事件发生，poll()返回 0；

失败时，poll() 返回 -1，并设置 errno 为下列值之一：

EBADF：一个或多个结构体中指定的文件描述符无效。

EFAULT：fds 指针指向的地址超出进程的地址空间。

EINTR：请求的事件之前产生一个信号，调用可以重新发起。

EINVAL：nfds 参数超出 PLIMIT\_NOFILE 值。

ENOMEM：可用内存不足，无法完成请求。

// 监视并等待多个文件（标准输入，udp套接字）描述符的属性变化（是否可读）

// 没有属性变化，这个函数会阻塞，直到有变化才往下执行，这里没有设置超时

ret = poll(fds, 2, -1);

if( ( fds[0].revents & POLLIN ) == POLLIN ){ // 标准输入循环查询

## 8.17 I/O复用函数之epoll

epoll 是在 2.6 内核中提出的，是之前的 select() 和 poll() 的增强版本。相对于 select() 和 poll() 来说，epoll 更加灵活，没有描述符限制。epoll 使用一个文件描述符管理多个描述符，将用户关系的文件描述符的事件存放到内核的一个事件表中，这样在用户空间和内核空间的 copy 只需一次。

epoll操作过程需要的四个接口函数

#include <sys/epoll.h>

int epoll\_create(int size);

int epoll\_ctl(int epfd, int op, int fd, struct epoll\_event \*event);

int epoll\_wait(int epfd, struct epoll\_event \*events, int maxevents, int timeout);

int close(int epfd);

int epoll\_create(int size);

功能：

该函数生成一个epoll专用的文件描述符（其余的接口函数一般都用使用这个专用的文件描述符）

参数：

size: 用来告诉内核这个监听的数目一共有多大，参数 size 并不是限制了 epoll 所能监听的描述符最大个数，只是对内核初始分配内部数据结构的一个建议。自从 linux 2.6.8 之后，size 参数是被忽略的，也就是说可以填只有大于 0 的任意值。需要注意的是，当创建好 epoll 句柄后，它就是会占用一个 fd 值，在 linux 下如果查看 /proc/ 进程 id/fd/，是能够看到这个 fd 的，所以在使用完 epoll 后，必须调用 close() 关闭，否则可能导致 fd 被耗尽

返回值：

成功：epoll 专用的文件描述符

失败：-1

int epoll\_ctl(int epfd, int op, int fd, struct epoll\_event \*event);

功能：

epoll 的事件注册函数，它不同于 select() 是在监听事件时告诉内核要监听什么类型的事件，而是在这里先注册要监听的事件类型

参数：

epfd: epoll 专用的文件描述符，epoll\_create()的返回值

op: 表示动作，用三个宏来表示：

EPOLL\_CTL\_ADD：注册新的 fd 到 epfd 中；

EPOLL\_CTL\_MOD：修改已经注册的fd的监听事件；

EPOLL\_CTL\_DEL：从 epfd 中删除一个 fd；

fd: 需要监听的文件描述符

event: 告诉内核要监听什么事件，struct epoll\_event 结构如下：

// 保存触发事件的某个文件描述符相关的数据（与具体使用方式有关）

typedef union epoll\_data {

void \*ptr;

int fd;

\_\_uint32\_t u32;

\_\_uint64\_t u64;

} epoll\_data\_t;

// 感兴趣的事件和被触发的事件

struct epoll\_event {

\_\_uint32\_t events; /\* Epoll events \*/

epoll\_data\_t data; /\* User data variable \*/

};

events 可以是以下几个宏的集合：

EPOLLIN ：表示对应的文件描述符可以读（包括对端 SOCKET 正常关闭）；

EPOLLOUT：表示对应的文件描述符可以写；

EPOLLPRI：表示对应的文件描述符有紧急的数据可读（这里应该表示有带外数据到来）；

EPOLLERR：表示对应的文件描述符发生错误；

EPOLLHUP：表示对应的文件描述符被挂断；

EPOLLET ：将 EPOLL 设为边缘触发(Edge Triggered)模式，这是相对于水平触发(Level Triggered)来说的。

EPOLLONESHOT：只监听一次事件，当监听完这次事件之后，如果还需要继续监听这个 socket 的话，需要再次把这个 socket 加入到 EPOLL 队列里

返回值：

成功：0

失败：-1

int epoll\_wait(int epfd, struct epoll\_event \*events, int maxevents, int timeout);

功能：

等待事件的产生，收集在 epoll 监控的事件中已经发送的事件，类似于 select() 调用。

参数：

epfd: epoll 专用的文件描述符，epoll\_create()的返回值

events: 分配好的 epoll\_event 结构体数组，epoll 将会把发生的事件赋值到events 数组中（events 不可以是空指针，内核只负责把数据复制到这个 events 数组中，不会去帮助我们在用户态中分配内存）。

maxevents: maxevents 告之内核这个 events 有多大 。

timeout: 超时时间，单位为毫秒，为 -1 时，函数为阻塞

返回值：

成功：返回需要处理的事件数目，如返回 0 表示已超时。

失败：-1

epoll 对文件描述符的操作有两种模式：LT（level trigger）和 ET（edge trigger）。LT 模式是默认模式，LT 模式与 ET 模式的区别如下：

LT 模式：当 epoll\_wait 检测到描述符事件发生并将此事件通知应用程序，应用程序可以不立即处理该事件。下次调用 epoll\_wait 时，会再次响应应用程序并通知此事件。

ET 模式：当 epoll\_wait 检测到描述符事件发生并将此事件通知应用程序，应用程序必须立即处理该事件。如果不处理，下次调用 epoll\_wait 时，不会再次响应应用程序并通知此事件。

ET 模式在很大程度上减少了 epoll 事件被重复触发的次数，因此效率要比 LT 模式高。epoll 工作在 ET 模式的时候，必须使用非阻塞套接口，以避免由于一个文件句柄的阻塞读/阻塞写操作把处理多个文件描述符的任务饿死

int close(int epfd);

在用完之后，记得用close()来关闭这个创建出来的epoll句柄

举例：

int epfd = epoll\_create(10); // 创建一个 epoll 的句柄，参数要大于 0， 没有太大意义

event.data.fd = 0; // 标准输入

event.events = EPOLLIN; // 表示对应的文件描述符可以读

// 事件注册函数，将标准输入描述符 0 加入监听事件

ret = epoll\_ctl(epfd, EPOLL\_CTL\_ADD, 0, &event);

// 监视并等待多个文件（标准输入，udp套接字）描述符的属性变化（是否可读）

// 没有属性变化，这个函数会阻塞，直到有变化才往下执行，这里没有设置超时

ret = epoll\_wait(epfd, &wait\_event, 2, -1);

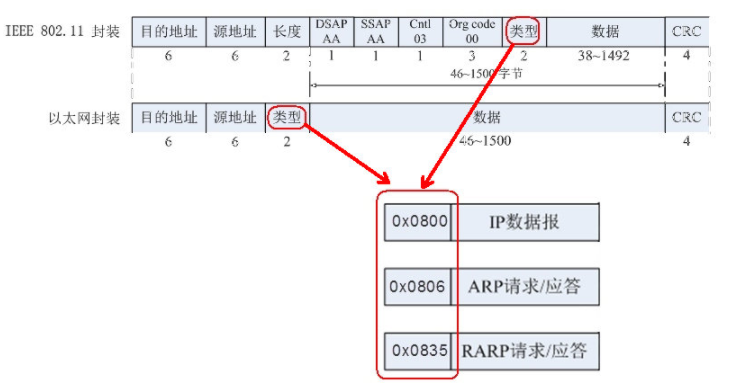
if( ( 0 == wait\_event.data.fd ) && ( EPOLLIN == wait\_event.events & EPOLLIN ) )

为什么要，父子进程中多次的关闭ｓｏｃｋｅｔ，其实是ｆｏｒｋ函数调用之后，子进程会导致父进程中ｓｏｃｋｅｔ引用计数＋１，ｃｌｏｓｅ的时候只有当引用计数为０时才会真正关闭ｓｏｃｋｅｔ。文中提到的防止子进程共享父进程，是原因之一，但不是最重要的原因。最重要的原因是防止内存泄露。 同时，这个代码也不够完善，子进程退出，会导致大量的僵尸进程，应在父亲进程中添加处理僵尸进程。

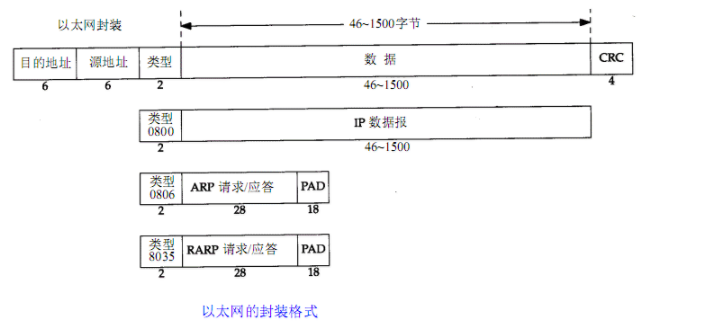
## 8.18 原始套接字

原始套接字（SOCK\_RAW）可以用来自行组装数据包，可以接收本机网卡上所有的数据帧（数据包），对于监听网络流量和分析网络数据很有作用。原始套接字是基于 IP 数据包的编程（SOCK\_PACKET 是基于数据链路层的编程）。另外，必须在管理员权限下才能使用原始套接字。

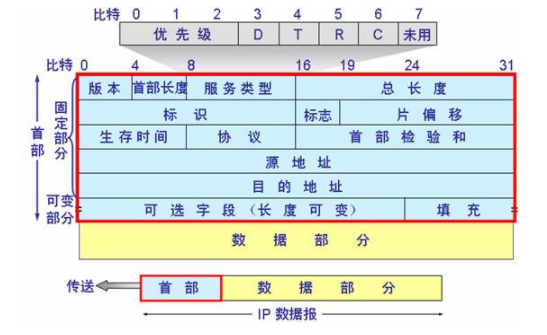
链路层封包格式



MAC 头部（有线局域网）



IP 数据报首部



TCP/IP 协议定义了一个在因特网上传输的包，称为 IP 数据报 (IP Datagram)。这是一个与硬件无关的虚拟包，由首部和数据两部分组成。

首部的前一部分是固定长度，共 20 字节，是所有 IP 数据报必须具有的。在首部的固定部分的后面是一些可选字段，其长度是可变的。首都中的源地址和目的地址都是 IP 协议地址。

1）版本：占4位，指IP协议的版本。

通信双方使用的 IP 协议版本必须一致。日前广泛使用的 IP 协议版本号为 4 (即 IPv4)。IPv6 目前还处于起步阶段。

2）首部长度：占 4 位，可表示的最大十进制数值是 15。

请注意，这个字段所表示数的单位是32位字 ( 1 个 32 位字长是 4  字节)，因此，当 IP 的首部长度为 1111 时 ( 即十进制的 15 )，首部长度就达到 60 字节。

当 IP 分组的首部长度不是 4 字节的整数倍时，必须利用最后的填充字段加以填充。因此数据部分永远在 4 字节的整数倍开始，这样在实现 IP 协议时较为方便。首部长度限制为 60 字节的缺点是有时可能不够用。这样做的目的是希望用户尽量减少开销。最常用的首部长度就是 20 字节 (即首部长度为 0101)，这时不使用任何选项。

1. 服务：占 8 位，用来获得更好的服务，一般不使用。

服务类型字段实际上被划分为 2 个部分，一部分为优先权一部分为 TOS。优先权用来设定报文的优先级，就像邮包分为挂号和平信一样。TOS 允许按照吞吐量、时延、可靠性和费用方式选择传输服务，在早期的时候，TOS 还被用来进行路由选择。在 QOS 中有时也会使用优先权，常见的优先权队列。

这个字段在旧标准中叫做服务类型，但实际上一直没有被使用过。1998 年 IETF 把这个字段改名为区分服务 DS ( DifferentiatedServices )。只有在使用区分服务时，这个字段才起作用。

1. 总长度：总长度指首都及数据之和的长度，单位为字节。

因为总长度字段为 16 位，所以数据报的最大长度为 65535 字节。在 IP 层下面的每一种数据链路层都有自己的帧格式，其中包括帧格式中的数据字段的最大长度，即最大传送单元 MTU (Maximum Transfer Unit)。当一个数据报封装成链路层的帧时，此数据报的总长度 ( 即首部加上数据部分 )一定不能超过下面的数据链路层的 MTU 值。

如果报文总长度大于数据链路可传输的最大传输单元（MTU），那么就会对报文进行分片，详情请看《IP 分片丢失重传》。

5）标识 ( Identification )：占 16位。

IP 软件在存储器中维持一个计数器，每产生一个数据报，计数器就加 1，并将此值赋给标识字段。但这个“标识”并不是序号，因为 IP 是无连接的服务，数据报不存在按序接收的问题。

当数据报由于长度超过网络的 MTU 而必须分片时，这个标识字段的值就被复制到所有的数据报的标识字段中。相同的标识字段的值使分片后的各数据报片最后能正确地重装成为原来的数据报。

6）标志 ( Flag )：占3 位，但目前只有2位有意义，  其中第一位没有被使用。

 第二位是不分片位，当 DF 位被置1，表示路由器不能对数据报文进行分片处理，如果报文由于不能被分片而不能被转发，那么路由器将丢弃这个数据包，并向源地址发送错误报告。这一功能可以用来测试线路的最大传输单元。只有当 DF = 0 时才允许分片。

第三位为 MF，当路由器对数据进行分片时，除了最后一个分片的 MF 位为 0 外，其他所有的 MF 全部为 1，表示其后面还有其他的分片。

MF = 1 即表示后面 “还有分片” 的数据报。

MF = 0表示这已是若干数据报片中的最后一个。

7）片偏移：占 13位。较长的分组在分片后，某片在原分组中的相对位置。

也就是说，相对用户数据字段的起点，该片从何处开始。片偏移以 8 个字节为偏移单位。这就是说，每个分片的长度一定是 8 字节 ( 64 位)的整数倍。

8）生存时间：占 8 位，生存时间字段常用的英文缩写是 TTL ( Time To Live )，其表明数据报在网络中的寿命。

由发出数据报的源点设置这个字段。其目的是防止无法交付的数据报无限制地在因特网中兜围子，因而白白消耗网络资源。

最初的设计是以秒作为 TTL 的单位。每经过一个路由器时，就把 TTL 减去数据报在路由器消耗掉的一段时间。若数据报在路由器消耗的时间小于 1 秒，就把 TTL 值减 1。当 TTL 值为 0 时，就丢弃这个数据报。当 TTL 为零的时候，就会丢弃这个报文，同时向源地址发送错误报告，促使重新发送。

1. 协议：占 8 位，协议字段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 层知道应将数据部分上交给哪个处理过程，常用的有ICMP(1), IGMP(2), TCP(6), UDP(17), IPv6（41）

10）首部检验和：占 16 位。这个字段只检验数据报的首部，但不包括数据部分。

这是因为数据报每经过一个路由器，都要重新计算一下首都检验和 ( 一些字段，如生存时间、标志、片偏移等都可能发生变化 )。不检验数据部分可减少计算的工作量。

11）源地址：发送方IP地址

12）目的地址：接收方IP地址

Tcp 控制位

紧急 URG：此位置 1，表明紧急指针字段有效，它告诉系统此报文段中有紧急数据，应尽快传送。

确认 ACK：仅当 ACK = 1 时确认号字段才有效，TCP 规定，在连接建立后所有传达的报文段都必须把 ACK 置 1。

推送 PSH：当两个应用进程进行交互式的通信时，有时在一端的应用进程希望在键入一个命令后立即就能够收到对方的响应。在这种情况下，TCP 就可以使用推送（push）操作，这时，发送方 TCP 把 PSH 置 1 ，并立即创建一个报文段发送出去，接收方收到 PSH = 1 的报文段，就尽快地（即“推送”向前）交付给接收应用进程，而不再等到整个缓存都填满后再向上交付。

复位 RST：用于复位相应的 TCP 连接

同步 SYN：仅在三次握手建立 TCP 连接时有效。当 SYN = 1 而 ACK = 0 时，表明这是一个连接请求报文段，对方若同意建立连接，则应在相应的报文段中使用 SYN = 1 和 ACK = 1。因此，SYN 置 1 就表示这是一个连接请求或连接接受报文。

终止 FIN：用来释放一个连接。当 FIN = 1 时，表明此报文段的发送方的数据已经发送完毕，并要求释放运输连接。

伪首部，又称为伪包头（Pseudo Header）：是指在 TCP 的分段或 UDP 的数据报格式中，在数据报首部前面增加源 IP 地址、目的 IP 地址、IP 分组的协议字段、TCP 或 UDP 数据报的总长度等共12字节，所构成的扩展首部结构。此伪首部是一个临时的结构，它既不向上也不向下传递，仅仅只是为了保证可以校验套接字的正确性。

