# 书籍信息

|  |  |  |  |
| --- | --- | --- | --- |
| 书名 | 版本 | 简写 | 偏移量\* |
| 《C++ Primer》 | 中文第5版 |  | 26 |
| 《深入理解计算机系统》 | 中文第3版 | CSAPP |  |
| 《现代操作系统》 | 中文第4版 |  |  |
| 《计算机网络：自顶向下方法》 | 中文第6版 |  |  |
| 《Unix网络编程 卷1：套接字联网API》 | 中文第3版 | UNP | 14 |
| 《数据库系统概念》 | 中文第6版 |  |  |
| 《超全面的后端C/C++面经整理》 |  |  |  |
| 《TCP/IP详解 卷1：协议》 | 中文第2版 |  | 20 |
| 《Linux高性能服务器编程》 |  |  | 18 |

* \*偏移量：指本人所用电子版PDF的页码和书籍实际页码的差值，比如PDF中为第71页，书籍实际页码为45页，那么差值为71-45=26。本文出于阅读和跳转方便，标注的页码均为电子版PDF的页码。

# C++

## 指针和引用的区别

1. 《C++ Primer》第71~75页
2. 浅谈C++中指针和引用的区别：<https://www.cnblogs.com/dolphin0520/archive/2011/04/03/2004869.html>

|  |  |  |
| --- | --- | --- |
|  | 指针 | 引用 |
|  | 指针本身就是一个对象 | 引用本身并非对象，它只是为一个已经存在的对象所起的别名 |
|  | 允许对指针赋值和拷贝，在指针的生命周期内其可以先后指向不同的对象，给指针赋值就是令其存放一个新地址，指向一个新对象 | 一旦定义了引用，就无法令其再绑定到另外的对象，之后每次使用该引用都是访问其最初绑定的那个对象 |
|  | 指针无需在定义时赋初值，指针可以为空 | 引用必须初始化，且引用不能为空 |
|  | sizeof得到的是指针自身的大小，一般为4字 | sizeof得到的引用大小取决于被引用对象大小 |
|  | 指针可以有多级 | 引用只能有一级 |
|  | 可以用const指针 | 没有const引用 |
|  | 指针传参时需要解引用才能修改参数 | 引用传参时可以直接修改参数 |

## 在函数参数传递时，何时用指针，何时用引用，二者的区别

1. **使用指针传递的场景**

需要返回函数内局部变量的内存的时候用指针（返回局部变量的引用是没有意义的）。使用指针传参需要开辟内存，用完要记得释放指针，不然会内存泄漏。

1. **使用引用传递的场景**

（1）对栈空间大小比较敏感（比如递归）时使用引用，使用引用传递无需创建临时变量，开销更小。

（2）类对象作为参数传递的时候使用引用，这是 C++ 类对象传递的标准方式。

* C++ 值传递、指针传递、引用传递详解： https://www.cnblogs.com/yanlingyin/archive/2011/12/07/2278961.html

1. **值传递：**形参是实参的拷贝，改变形参的值并不会影响外部实参的值。从被调用函数的角度来说，值传递是单向的（实参->形参），参数的值只能传入，不能传出。当函数内部需要修改参数，并且不希望这个改变影响调用者时，采用值传递。
2. **指针传递：**形参为指向实参地址的指针，当对形参的指向操作时，就相当于对实参本身进行的操作。
3. **引用传递：**形参相当于是实参的“别名”，对形参的操作其实就是对实参的操作，在引用传递过程中，被调函数的形式参数虽然也作为局部变量在栈中开辟了内存空间，但是这时存放的是由主调函数放进来的实参变量的地址。被调函数对形参的任何操作都被处理成间接寻址，即通过栈中存放的地址访问主调函数中的实参变量。正因为如此，被调函数对形参做的任何操作都影响了主调函数中的实参变量。

## 堆和栈有什么区别

C++ 堆和栈的区别，内存分配方式理解：<https://blog.csdn.net/qq_35637562/article/details/78550953>

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | 堆 | 栈 |
|  | 管理方式 | 程序员手动分配，容易产生内存泄露 | 编译器自动管理，无需手动控制 |
|  | 空间大小 | 堆的空间较大，在32位系统下，堆内存可达4 GB，几乎不存在限制。 | 栈的空间较小，比如VC6下默认为1 MB。 |
|  | 碎片问题 | 堆空间有频繁的分配（new）和释放（delete）操作，这会导致内存空间不连续，产生内存碎片 | 栈中的块先进后出，始终只有栈顶的块最先被弹出。 |
|  | 生长方向 | 堆的生长方向向上↑，也即内存地址不断增加 | 栈的生长方向向下↓，也即内存地址不断减小 |
|  | 分配方式 | 堆都是动态分配的，没有静态分配的堆 | 栈既有静态分配，也有动态分配。静态分配由编译器完成，比如局部变量的分配。动态分配由malloc函数完成，且由编译器释放，无需手动实现（和堆不同）。 |
|  | 分配效率 | 堆的分配效率低，因为是由C/C++函数库提供的，机制较为复杂。在为一个堆分配内存时，需要按照一定的算法搜索可用的足够大的空间，没有的话还要特地增加程序数据段的内存空间。 | 栈的分配效率高，因为是机器系统提供的数据结构，会在底层提供对栈的支持（比如分配专门的寄存器存放栈的地址，入栈出栈都有专门的指令）。 |
|  | 适用场景 | 需要分配大量内存空间时使用堆 | 在大部分情况下使用栈，因为优点很多 |

## 堆和栈哪个更快，为什么

栈更快一点。

* 操作系统在底层对栈提供支持，专门的寄存器存放栈的地址，专门的入栈出栈指令。
* 堆的操作是由C/C++函数库提供的，分配堆内存时需要使用相关算法寻找大小合适的内存，并且获取堆的内容需要两次访问，第一次访问指针，第二次依据指针保存的地址访问内存。

## new和delete是如何实现的

* C++：new和delete背后的实现原理：https://blog.csdn.net/tonglin12138/article/details/85699115
* C++学习——深度剖析new和delete原理：<https://blog.csdn.net/weixin_41028343/article/details/102952840>
* C++ new/delete详解及原理：<https://www.cnblogs.com/Duikerdd/p/11687621.html>
* new和delete的底层实现原理：<https://blog.csdn.net/qq_42719751/article/details/90084812>

new/new[] 和delete/delete[] 都是C++用来实现动态内存管理的操作符。new/new[] 申请空间，delete/delete[] 释放空间。operator new和operator delete是系统提供的全局函数，new和delete在底层调用全局函数来申请和释放空间。

**1、对于内置类型**

相同之处：申请内置类型的空间时，new和malloc基本类似，delete和free基本类似。

不同之处：（1）new和delete申请和释放的是单个元素的空间，new[] 和delete[] 申请和释放的是连续空间。（2）new在申请空间失败时会抛出异常，malloc会返回NULL。

**2、对于自定义类型**

**new：**（1）调用operator new函数申请空间，该函数实际上通过malloc来申请空间；（2）在申请的空间上执行构造函数，完成对象的构造

**delete：**（1）在空间上执行析构函数，完成对象中资源的清理工作；（2）调用operator delete函数释放对象的空间，该函数实际上通过free来释放空间

**new [N]：**（1）调用operator new[] 函数，在operator new[] 中实际调用operator new函数完成N个对象空间的申请；（2）在申请的空间上执行N次构造函数

**delete [N]：**（1）在释放的对象空间上执行N次析构函数，完成N个对象中资源的清理；（2）调用operator delete[] 释放空间，在operator delete[] 中实际调用operator delete来释放空间

**问：那么在new[N] 和delete[N] 过程中如何确定本次调用的是第几次函数？**

答：在使用new[] 时，调用operator new[](size\_t size) 函数，传参时传入的不是 sizeof(类型)\* 对象个数；而是**在对象数组的大小上加上一个额外数据，用于编译器区分对象数组指针和对象指针以及对象数组大小**。在VS2008下这个额外数据占4个字节，一个int大小。

但是，这个额外数据对外是不可见的。

|  |
| --- |
| operator new() 的全局函数原型 |
| 1. /\* 2. operator new： 3. 该函数实际通过 malloc 来申请空间，当 malloc 申请空间成功时直接返回； 4. 申请空间失败，尝试执行空间不足应对措施，如果改应对措施用户设置了，则继续申请，否则抛异常。 5. \*/ 6. void \*\_\_CRTDECL **operator** new(size\_t size) \_THROW1(\_STD bad\_alloc) { 7. // try to allocate size bytes 8. void \*p; 9. **while** ((p = malloc(size)) == 0) 10. **if** (\_callnewh(size) == 0) { 11. // report no memory 12. // 如果申请内存失败了，这里会抛出 bad\_alloc 类型异常 13. **static** **const** std::bad\_alloc nomem; 14. \_RAISE(nomem); 15. } 16. **return** (p); 17. } |

| operator delete() 的全局函数原型 |
| --- |
| 1. /\* 2. operator delete: 该函数最终是通过 free 来释放空间的 3. \*/ 4. void **operator** delete(void \*pUserData) { 5. \_CrtMemBlockHeader \* pHead; 6. RTCCALLBACK(\_RTC\_Free\_hook, (pUserData, 0)); 7. **if** (pUserData == NULL) 8. **return**; 9. \_mlock(\_HEAP\_LOCK); /\* block other threads \*/ 10. \_\_TRY 11. /\* get a pointer to memory block header \*/ 12. pHead = pHdr(pUserData); 13. /\* verify block type \*/ 14. \_ASSERTE(\_BLOCK\_TYPE\_IS\_VALID(pHead->nBlockUse)); 15. \_free\_dbg(pUserData, pHead->nBlockUse); 16. \_\_FINALLY 17. \_munlock(\_HEAP\_LOCK); /\* release other threads \*/ 18. \_\_END\_TRY\_FINALLY 19. return; 20. } 21. /\* 22. free的实现 23. \*/ 24. #define free(p) \_free\_dbg(p, \_NORMAL\_BLOCK) |

## new和malloc的异同

**※ 细说new与malloc的10点区别：**<https://www.cnblogs.com/qg-whz/p/5140930.html>

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | new/delete | malloc/free |
|  | 库函数和运算符 | new和delete是运算符。 | malloc和free是库函数。 |
|  | 分配内存的位置 | new从**自由存储区（free store）**上为对象动态分配内存空间。[1,2] | malloc从**堆**上动态分配内存。 |
|  | 内存分配成功的返回值 | new内存分配成功时，返回**对象类型的指针**，类型严格与对象匹配，无须进行类型转换，故new是类型安全的操作符。[3] | malloc内存分配成功时，返回**void \***，需要通过强制类型转换将void \* 指针转换成我们需要的类型。 |
|  | 内存分配失败的返回值 | new内存分配失败时抛出**bad\_alloc异常**，不会返回NULL。[4] | malloc内存分配失败时会返回**NULL**。 |
|  | 是否指定分配内存的大小 | new分配内存无需指定内存块的大小，编译器会根据类型信息自动计算。 | malloc需要显式地指出所需内存的大小。[5] |
|  | 是否调用构造函数和析构函数 | new会调用构造函数，delete会调用析构函数。[6,7] | malloc不会调用构造函数。 |
|  | 处理数组 | new[] 会分别调用构造函数初始化每一个数组元素，释放时为每个对象调用析构函数。使用new[] 分配的内存必须使用 delete[] 释放，否则会只释放部分对象，造成内存泄露。 | malloc不知道在内存上申请的是数组还是别的什么，只会给你一块原始内存和地址。因此要用malloc动态分配数组的内存，需要手动指定数组的大小。 |
|  | 是否可以相互调用 | operator new和operator delete的实现可以基于malloc和free。[8] | malloc的实现不能调用new。 |
|  | 是否可以被重载 | operator new和operator delete可以被重载。[9] | malloc不允许重载。 |
|  | 扩充已分配内存 | new没有相关处理方式。 | 使用malloc分配内存后，可以用realloc函数重新分配内存。[10] |
|  | 内存分配时内存不足 | new可以指定处理函数或重新制定分配器。[11] | malloc没有相关处理方式。 |

一些说明：

1. 凡是通过new申请的内存，该内存即为自由存储区。
2. 自由存储区能否是堆？

该问题等价于new能否在堆上动态分配内存。这取决于operator new 的实现细节。自由存储区可以是堆，也可以是静态存储区，取决于operator new 在何处为对象分配内存。特别地，new甚至可以不为对象分配内存，比如**定位new**：

1. new (place\_address) type;
2. void \* operator new (size\_t, void \*) // 不允许重定义该版本的 operator new
3. 类型安全很大程度上等价于内存安全，类型安全的代码不会试图访问未被授权的内存区域。
4. 使用C语言时，习惯在malloc分配内存后用NULL判断分配是否成功：
5. int \*a = (int \*)malloc ( sizeof (int ));
6. if(NULL == a) {
7. ...
8. } else {
9. ...
10. }

使用C++时，则不应在new后使用NULL判断，而应捕捉bad\_alloc异常：

1. try {
2. int \*a = new int();
3. } catch (bad\_alloc) {
4. ...
5. }
6. new不需要指定内存大小，malloc则需要：
7. class A{...}
8. A \* ptr = new A;
9. A \* ptr = (A \*)malloc(sizeof(A)); // 需要显式指定所需内存大小sizeof(A);
10. // 当然，这里仅作示意，实际上不应使用 malloc 来处理自定义数据类型
11. new分配对象内存有3步：

（1）调用operator new（或者new[]）函数分配一块足够大的、原始的、未命名的空间存储特定类型的对象；

（2）编译器执行相应的构造函数以构造对象，并传入初值；

（3）对象构造完成后，返回一个指向该对象的指针。

delete分配对象内存有2步：

（1）调用对象的析构函数；

（2）编译器调用operator delete（或者delete[]）函数释放内存空间。

1. 不应使用malloc和free函数处理C++中的自定义数据类型（包括标准库中需要构造和析构的数据类型）。
2. 一种极简的operator new和operator delete的实现方式：
3. void \* operator new(sieze\_t size) {
4. if(void \* mem = malloc(size))
5. return mem;
6. else
7. throw bad\_alloc();
8. }
9. void operator delete(void \*mem) noexcept {
10. free(mem);
11. }
12. 标准库为operator new和operator delete各定义了4个重载版本：
13. // 这些版本可能抛出异常
14. void \* operator new(size\_t);
15. void \* operator new[](size\_t);
16. void \* operator delete(void \*) noexcept;
17. void \* operator delete[](void \*0) noexcept;
18. // 这些版本承诺不抛出异常
19. void \* operator new(size\_t, nothrow\_t&) noexcept;
20. void \* operator new[](size\_t, nothrow\_t& );
21. void \* operator delete(void \*, nothrow\_t& ) noexcept;
22. void \* operator delete[](void \*0, nothrow\_t& ）noexcept;
23. realloc先判断当前指针所指内存是否有足够的连续空间，如果有，原地扩大可分配的内存地址，并且返回原来的地址指针；如果空间不够，先按照新指定的大小分配空间，再将原有数据从头到尾拷贝到新分配的内存区域，最后释放原来的内存区域。
24. 在operator new因为申请的内存不足从而抛出异常之前，会先调用一个用户指定的错误处理函数new\_handler，这是一个指针类型，指向一个没有参数和返回值的错误处理函数：
25. namespace std {
26. typedef void (\*new\_handler)();
27. }

使用者需要调用set\_new\_handler指定错误处理函数，这是声明于std的一个标准库函数。set\_new\_handler的参数为new\_handler指针，指向operator new 无法分配足够内存时应当调用的函数；其返回值也是指针，指向set\_new\_handler被调用前正在执行（但马上就要被替换）的那个new\_handler函数。

1. namespace std {
2. new\_handler set\_new\_handler(new\_handler p) throw();
3. }

## 既然有了malloc/free，C++中为什么还需要new/delete

有了malloc/free为什么还要new/delete ：<https://blog.csdn.net/liubing8609/article/details/85568356>

由于内部数据类型没有构造与析构的过程，因此对它们而言malloc/free和new/delete是等价的。

对于非内部数据类型的对象而言，光用maloc/free无法满足动态对象的要求。对象在创建的同时要自动执行构造函数，对象在消亡之前要自动执行析构函数。

由于malloc/free是库函数而不是运算符，不在编译器控制权限之内，不能够把执行构造函数和析构函数的任务强加于malloc/free。因此C++语言需要一个能完成动态内存分配和初始化工作的运算符new，以及一个能完成清理与释放内存工作的运算符delete。

注意：malloc/free是库函数，而new/delete是运算符。

**问：既然new/delete的功能完全覆盖了malloc/free，为什么C++不摒弃malloc/free呢？**

答：因为C++程序经常要调用C函数，而C程序只能用malloc/free管理动态内存。

**问：free和delete能否换用？**

答：如果用free释放“new创建的动态对象”，那么该对象因无法执行析构函数而可能导致程序出错。如果用delete释放“malloc申请的动态内存”，理论上讲程序不会出错，但是该程序的可读性很差。所以new/delete和malloc/free应该配对使用。

## C和C++的区别

## C++和Java的联系与区别，包括语言特性、垃圾回收、应用场景等

## Java的垃圾回收机制

## C++和Python的区别

## struct和class的区别

## define和const的联系与区别（编译阶段、安全性、内存占用等）

## C++中const的用法（定义，用途）

## C++ 中的 static 用法和意义

## 计算下面几个类的大小：

1. class A {};
2. int main(){
3. cout<<sizeof(A)<<endl; // 输出 1;
4. A a;
5. cout<<sizeof(a)<<endl; // 输出 1;
6. return 0;
7. }

空类的大小是 1， 在 C++ 中空类会占一个字节，这是为了让对象的实例能够相互区别。具体来说，空类同样可以被实例化，并且每个实例在内存中都有独一无二的地址，因此，编译器会给空类隐含加上一个字节，这样空类实例化之后就会拥有独一无二的内存地址。当该空白类作为基类时，该类的大小就优化为 0 了，子类的大小就是子类本身的大小。这就是所谓的空白基类最优化.

空类的实例大小就是类的大小，所以 sizeof(a)=1 字节, 如果 a 是指针，则 sizeof(a) 就是指针的大小，即 4 字节

1. class A { virtual Fun(){} };
2. int main(){
3. cout<<sizeof(A)<<endl; // 输出 4(32位机器)/8(64位机器);
4. A a;
5. cout<<sizeof(a)<<endl; // 输出 4(32位机器)/8(64位机器);
6. return 0;
7. }

因为有虚函数的类对象中都有一个虚函数表指针 \_\_vptr，其大小是 4 字节

1. class A { static int a; };
2. int main(){
3. cout<<sizeof(A)<<endl;// 输出 1;
4. A a;
5. cout<<sizeof(a)<<endl;// 输出 1;
6. return 0;
7. }

静态成员存放在静态存储区，不占用类的大小, 普通函数也不占用类大小

1. class A { int a; };
2. int main(){
3. cout<<sizeof(A)<<endl;// 输出 4;
4. A a;
5. cout<<sizeof(a)<<endl;// 输出 4;
6. return 0;
7. }
8. class A { static int a; int b; };;
9. int main(){
10. cout<<sizeof(A)<<endl;// 输出 4;
11. A a;
12. cout<<sizeof(a)<<endl;// 输出 4;
13. return 0;
14. }

静态成员 a 不占用类的大小，所以类的大小就是 b 变量的大小 即 4 个字节

## 【热门】C++ 的 STL 介绍（这个系列很重要，建议侯捷的书籍和视频），包括内存管理 allocator，函数，实现机理，多线程实现等

## STL 源码中的 hash 表的实现

## 解决哈希冲突的方式

## STL 中 unordered\_map 和 map 的区别

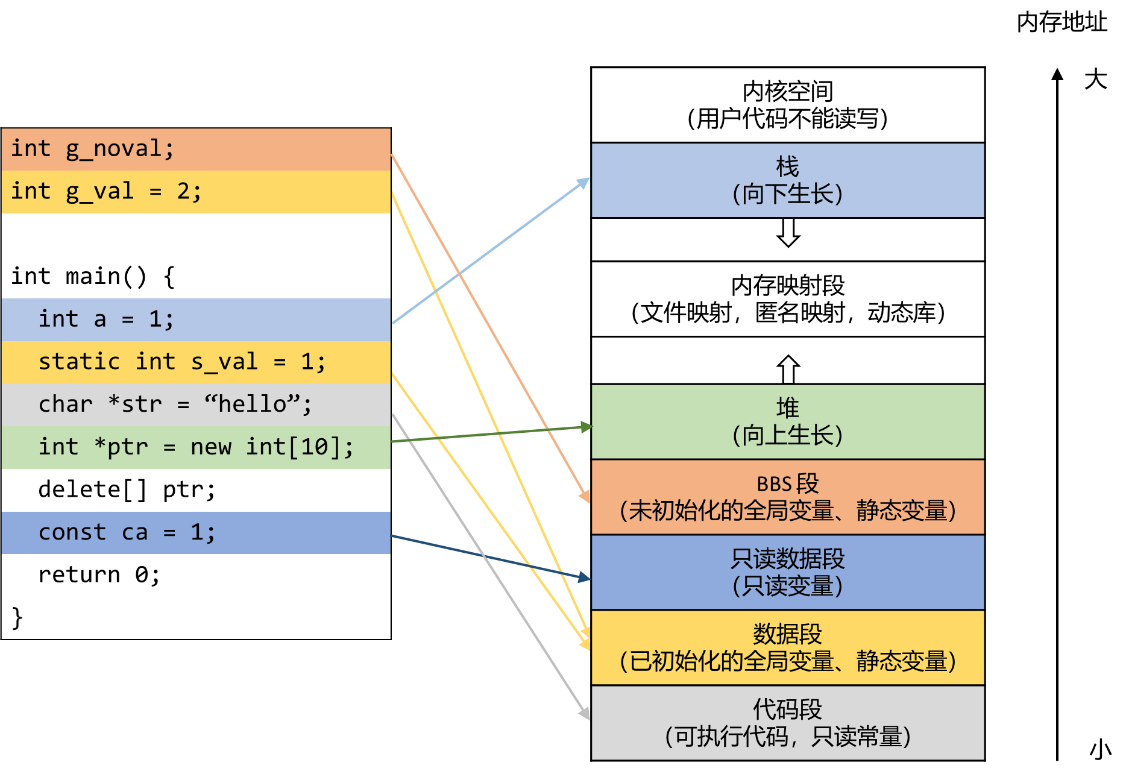
## STL 中 vector 的实现

## vector 使用的注意点及其原因，频繁对 vector 调用 push\_back() 对性能的影响和原因

## C++ 中 vector 和 list 的区别

## C++ 中的重载和重写的区别：

## 【热门】C ++ 内存管理



C/C++内存布局

## 介绍面向对象的三大特性，并且举例说明每一个

## 多态的实现（和下个问题一起回答）

## 【热门】C++ 虚函数相关（虚函数表，虚函数指针），虚函数的实现原理

## 实现编译器处理虚函数表应该如何处理

## 基类的析构函数一般写成虚函数的原因

## 构造函数为什么一般不定义为虚函数

## 构造函数或者析构函数中调用虚函数会怎样

## 纯虚函数

## 静态绑定和动态绑定的介绍

## 深拷贝和浅拷贝的区别（举例说明深拷贝的安全性）

## 对象复用的了解，零拷贝的了解

## 介绍 C++ 所有的构造函数

## 什么情况下会调用拷贝构造函数（三种情况）

## 结构体内存对齐方式和为什么要进行内存对齐？

## 内存泄露的定义，如何检测与避免？

## C++的智能指针有哪些

## 调试程序的方法

## 遇到coredump要怎么调试

## inline关键字说一下 和宏定义有什么区别

## 模板的用法与适用场景，实现原理

## 成员初始化列表的概念，为什么用成员初始化列表会快一些（性能优势）

## 用过C11吗，知道C11新特性吗？（有面试官建议熟悉 C11）

## C++的调用惯例（简单一点C++函数调用的压栈过程）

## C++的四种强制转换

## string的底层实现

## 一个函数或者可执行文件的生成过程或者编译过程是怎样的

## set，map和vector的插入复杂度

## 定义和声明的区别

## typdef和define的区别

## 被free回收的内存是立即返还给操作系统吗？为什么？

## 引用作为函数参数以及返回值的好处

## 友元函数和友元类

## 说一下volatile关键字的作用

## STL中的sort() 算法是用什么实现的，stable\_sort() 呢

## vector会迭代器失效吗？什么情况下会迭代器失效？

## 为什么C++没有实现垃圾回收？

# 操作系统

## 【热门】进程与线程的区别和联系

## Linux 理论上最多可以创建多少个进程？一个进程可以创建多少线程，和什么有关

## 冯诺依曼结构有哪几个模块？分别对应现代计算机的哪几个部分？

## 【热门】进程之间的通信方法有哪几种

## 进程调度方法详细介绍

## 进程的执行过程是什么样的，执行一个进程需要做哪些工作

## 操作系统的内存管理说一下

## 实现一个LRU算法

## 死锁产生的必要条件（怎么检测死锁，解决死锁问题）

## 死锁的恢复

## 什么是饥饿

## 如果要你实现一个mutex互斥锁你要怎么实现？

## 线程之间的通信方式有哪些？进程之间的同步方式又哪些？

## 什么时候用多进程，什么时候用多线程

## 文件读写使用的系统调用

## 孤儿进程和僵尸进程分别是什么，怎么形成的？

## 说一下PCB / 说一下进程地址空间

## 内核空间和用户空间是怎样区分的

## 线程是如何同步的（尤其是如果项目中用到了多线程，很大可能会结合讨论）

## 同一个进程内的线程会共享什么资源？

## 异常和中断的区别

## 一般情况下在 Linux / Windows 平台下栈空间的大小

## 虚拟内存的了解

## 服务器高并发的解决方案

## 【热门】协程了解吗

## 协程的底层是怎么实现的，怎么使用协程？

## 进程的状态以及转换图

## 在执行malloc申请内存的时候，操作系统是怎么做的？/ 内存分配的原理说一下 / malloc函数底层是怎么实现的？/ 进程是怎么分配内存的？

## 什么是字节序？怎么判断是大端还是小端？有什么用？

# 计算机网络

## 建立 TCP 服务器的各个系统调用

## 继上一题，说明 socket 网络编程有哪些系统调用？其中 close 是一次就能直接关闭的吗，半关闭状态是怎么产生的？

## 对路由协议的了解与介绍

## UDP如何实现可靠传输

## TCP和UDP的区别

## TCP和UDP相关的协议与端口号

## TCP（UDP，IP）等首部的认识（http请求报文构成）

## 网页解析的过程与实现方法

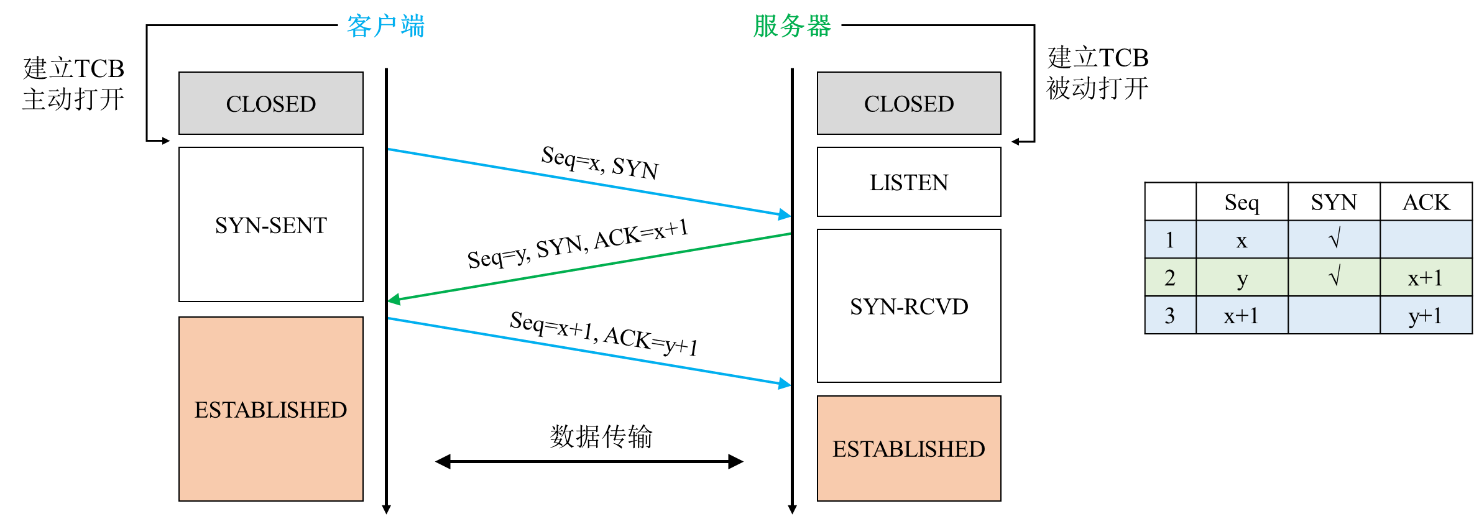
## 【热门】在浏览器中输入URL后执行的全部过程

## 网络层分片的原因与具体实现

## 【热门】TCP 的三次握手与四次挥手的详细介绍

* 《TCP/IP 详解 卷1》“第13章 TCP连接管理”：“13.2 TCP连接的建立与终止”，第443~451页
* 《Unix网络编程 卷1》“第2章 传输层：TCP、UDP和SCTP”：“2.6 TCP连接的建立和终止”，第45~50页
* 《Linux高性能服务器编程》“第3章 TCP协议详解”：“3.3 TCP连接的建立和关闭”，第55~62页
* **两张动图-彻底明白TCP的三次握手与四次挥手：<https://blog.csdn.net/qzcsu/article/details/72861891>**
* 面试官，不要再问我三次握手和四次挥手：<https://juejin.cn/post/6844903958624878606>
* TCP 协议·笔试面试知识整理：<https://hit-alibaba.github.io/interview/basic/network/TCP.html>

### TCP三次握手



TCP建立连接：三次握手

TCP建立连接过程为三次握手。

初始时客户端和服务器均处于CLOSED（关闭）状态。

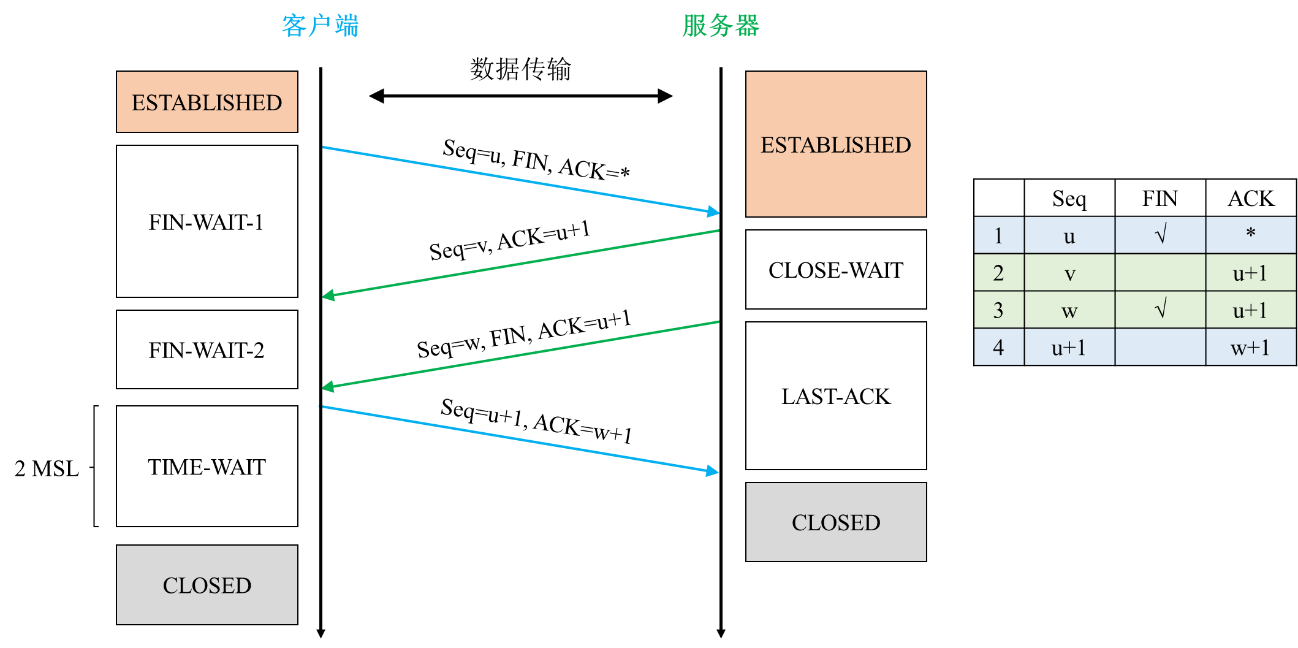
服务器进程创建传输控制块TCB，等待接收客户端进程的连接请求，进入LISTEN（监听）状态。

1. 客户端进程创建传输控制块TCB，向服务器发出连接请求报文，进入SYN-SENT（同步发送）状态
   * 客户端发送①客户端初始序列号Seq=x；②同步序列报文段SYN
2. 服务器收到请求报文，若同意连接，发出确认报文，进入SYN-RCVD（同步收到）状态
   * 服务器发送①服务器初始序列号Seq=y；②SYN；③确认号ACK=x+1
3. 客户端收到确认报文，再给服务器发送确认报文，进入ESTABLISHED（连接建立）状态
   * 客户端返回①Seq=x+1；②ACK=y+1
   * 服务器收到客户端的确认报文后，也进入ESTABLISHED（连接建立）状态，此时双方就可以通信了。

报文速记：

* 三次都携带本方序列号Seq
* 前两次有SYN，后两次有ACK
* 确认号ACK都是对方上次的序列号Seq+1

### TCP四次挥手



TCP关闭连接：四次挥手

TCP关闭连接的过程为四次挥手。

初始时客户端和服务器都处于ESTABLISHED（连接建立）状态。

1. 客户端停止发送数据，发送连接释放报文，进入FIN-WAIT-1（终止等待1）状态
   * 客户端发送①客户端序列号Seq=u；②终止报文段FIN；③确认号ACK=\*。
2. 服务器收到连接释放报文，发送确认报文，进入CLOSE-WAIT（关闭等待）状态
   * 服务器发送①服务器序列号Seq=v；②确认号ACK=u+1。
   * 此时客户端往服务器的方向已释放，连接处于半关闭状态，客户端没有数据要发送给服务器，但是如果服务器要发送数据，客户端仍要接收服务器最后发送的数据。
   * 客户端收到服务器的确认报文，进入FIN-WAIT-2（终止等待2）状态，等待服务器发送连接释放报文，在这段时间内还要继续接收服务器发送的数据。
3. 服务器发送完最后的数据，向客户端发送连接释放报文，进入LAST-ACK（最后确认）状态
   * 服务器发送①服务器序列号Seq=w；②终止报文段FIN；③确认号ACK=u+1。
4. 客户端收到服务器的连接释放报文，回复确认报文，进入TIME-WAIT（时间等待）状态
   * 客户端发送①客户端序列号Seq=u+1；②确认号ACK=w+1。
   * 此时TCP连接还没有释放，需经过2\*MSL（最大报文段寿命）时间后，客户端撤销了相应的传输控制块TCB，才进入CLOSED（关闭）状态。
   * 服务器一旦收到该确认报文，立刻进入CLOSED（关闭）状态，撤销TCB后，此次TCP连接结束。

报文速记：

* 四次都携带本方序列号Seq和确认号ACK
* 第1、3次有FIN
* ACK都是对方上次的序列号Seq+1

## TCP 握手以及每一次握手客户端和服务器端处于哪个状态

见上题。

## 为什么使用三次握手，两次握手可不可以？

* TCP 为什么是三次握手，而不是两次或四次？ - 知乎：<https://www.zhihu.com/question/24853633>
* <https://www.zhihu.com/question/24853633/answer/1279799682>
* 近 40 张图解被问千百遍的 TCP 三次握手和四次挥手面试题：https://mp.weixin.qq.com/s/tH8RFmjrveOmgLvk9hmrkw
* <https://www.zhihu.com/question/24853633/answer/573627478>
* RFC 793: Transmission Control Protocol：<https://www.rfc-editor.org/rfc/rfc793.html#page-32>
* TCP 为什么三次握手而不是两次握手（正解版）：<https://blog.csdn.net/lengxiao1993/article/details/82771768>

两种常见的说法是：

* 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。（谢希仁《计算机网络》）
* 为了解决“网络中存在延迟的重复分组”问题。（Tanenbaum《计算机网络》）

在RFC 793的第28、29、32页回答了三次握手的原因：

[p.28] A three way handshake is necessary **because sequence numbers are not tied to a global clock in the network, and TCPs may have different mechanisms for picking the ISN's.** The receiver of the first SYN has no way of knowing whether the segment was an old delayed one or not, unless it remembers the last sequence number used on the connection (which is not always possible), and so it must ask the sender to verify this SYN. The three way handshake and the advantages of a clock-driven scheme are discussed in [3].

[p.29] The three-way handshake **reduces the possibility of false connections.** It is the implementation of **a trade-off between memory and messages to provide for this checking.**

[p.32] The principle reason for the three-way handshake is **to prevent old duplicate connection initiations from causing confusion.**

To deal with this, a special control message, reset, has been devised.

* If the receiving TCP is in a non-synchronized state (i.e., SYN-SENT, SYN-RECEIVED), it returns to LISTEN on receiving an acceptable reset.
* If the TCP is in one of the synchronized states (ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, TIME-WAIT), it aborts the connection and informs its user.

We discuss this latter under "half-open" connections below.

两次握手的过程：

1. A发送①序列号Seq=a；②同步信号SYN；
2. B发送①序列号Seq=b；②同步信号SYN；③确认信号ACK

（如果四次握手，那么实际上是将三次握手中的ACK和SYN拆开发送。）

这时我们就能回答为什么使用三次握手：

**1. 防止旧的重复连接初始化造成混乱（主要）**

* 如果一个旧的SYN报文比最新的SYN报文早到达了服务端，那么此时服务端会返回一个SYN + ACK报文给客户端
* 如果是两次握手，无法判断当前连接是否是历史连接
* 如果是三次握手，客户端（发送方）在准备发送第三次报文时，有足够的上下文来判断当前连接是否是历史连接：
  + 如果是历史连接（序列号过期或超时），则第三次握手发送RST报文，中止历史连接
  + 如果不是历史连接，则第三次握手发送ACK报文，通信双方成功建立连接

**2. 同步双方的序列号**

TCP连接握手，实际上握的是通信双方数据原点的序列号。TCP需要序列号Seq来做可靠重传或接收，而避免连接复用时无法分辨出Seq是延迟的或是旧连接的Seq，因此需要三次握手来约定确定双方的 ISN（初始序列号）。

TCP协议的通信双方都必须维护一个序列号，序列号是可靠传输的一个关键因素，它的作用如下：

* 接收方可以去除重复数据
* 接收方可以根据数据包的序列号按序接收
* 可以标识发送出去的数据包中，哪些是已经被对方收到的。

可见序列号在TCP连接中具有重要作用：

* 当客户端发送携带初始序列号的SYN报文时，需要服务端返回一个ACK应答报文，表示客户端的SYN报文已被服务端成功接收；
* 当服务端发送初始序列号给客户端的时候，依然也要得到客户端的应答回应，这样一来一回，才能确保双方的初始序列号能被可靠的同步。

两次握手只保证了一方的初始序列号能被对方成功接收，没办法保证双方的初始序列号都能被确认接收。具体来说，客户端和服务器对客户端的序列号达成了共识，但是并没有对服务器的序列号达成共识。也即，服务器无法知道客户端是否已经接收到自己的同步信号，如果这个同步信号丢失了，客户端和服务器将无法对服务器的初始序列号达成一致。

拓展内容：

* TCP的设计者将SYN这个同步标志位SYN设计成占用一个字节的编号（FIN标志位也是），既然是一个字节的数据，按照TCP对有数据的TCP字段必须确认的原则，所以在这里客户端必须给服务器一个确认，以确认客户端已经接收到服务器的同步信号。
* SYN位字段会消耗一个序列号，消耗一个序列号也意味着使用重传进行可靠传输。故SYN和应用程序字节（还有FIN）是被可靠传输的。不消耗序列号的ACK则不是。（《TCP/IP 详解 卷1》第439页）

**3. 避免资源浪费**

（其实第3点我认为和第1点是一个意思。）

如果只有两次握手，当客户端的SYN请求连接在网络中阻塞，客户端没有接收到服务器的ACK报文，就会重新发送SYN，由于没有第三次握手，服务器不清楚客户端是否收到了自己发送的建立连接的ACK确认信号，所以每收到一个SYN就只能先主动建立一个连接。

因此如果客户端的SYN阻塞了，就会重复发送多次SYN报文，那么服务器在收到请求后就会建立多个冗余的无效链接，造成不必要的资源浪费。

顺便补充一下三次握手中丢包的情形：

1. 第一个包，即A发给B的SYN中途被丢，没有到达B

* A会周期性超时重传，直到收到B的确认

1. 第二个包，即B发给A的SYN +ACK中途被丢，没有到达A

* B会周期性超时重传，直到收到A的确认

1. 第三个包，即A发给B的ACK中途被丢，没有到达B

* A发完ACK，单方面认为TCP为 ESTABLISHED状态，而B显然认为TCP为Active状态：
  + 假定此时双方都没有数据发送，B会周期性超时重传，直到收到A的确认，收到之后B的TCP 连接也为ESTABLISHED状态，双向可以发包。
  + 假定此时A有数据发送，B收到A的数据+ ACK，自然会切换为ESTABLISHED状态，并接受A的数据。
  + 假定B有数据发送，则数据事实上是发送不了的，而是一直周期性超时重传SYN + ACK，直到收到A的ACK后才能发送数据。

## TCP 三次握手时的第一次的seq序号是怎样产生的

## TIME\_WAIT 的意义（为什么要等于 2MSL）

## 超时重传机制（不太高频）

## TCP 怎么保证可靠性？

## 流量控制的介绍，采用滑动窗口会有什么问题（死锁可能，糊涂窗口综合征）？

## TCP滑动窗口协议

## 拥塞控制和流量控制的区别

## 【热门】TCP 拥塞控制，算法名字？

* 《TCP/IP详解 卷1：协议》“第16章 TCP拥塞控制”，第537~583页
* TCP流量控制、拥塞控制：https://zhuanlan.zhihu.com/p/37379780

## TCP/IP 的粘包与避免介绍一下

## 说一下 TCP 的封包和拆包

## HTTP协议与TCP的区别与联系

## HTTP/1.0和HTTP/1.1 的区别

## http 的请求方法有哪些？get 和 post 的区别

## http 的常见状态码和含义

## http 和 https 的区别，由 http 升级为 https 需要做哪些操作

## https 的具体实现，怎么确保安全性

## 一个机器能够使用的端口号上限是多少，为什么？可以改变吗？那如果想要用的端口超过这个限制怎么办？

## 对称密码和非对称密码体系

## 【热门】数字证书的了解

## 服务器出现大量close\_wait的连接的原因以及解决方法

## 消息摘要算法列举一下，介绍 MD5 算法，为什么 MD5 是不可逆的，有什么办法可以加强消息摘要算法的安全性让它不那么容易被破解呢？

## 单条记录高并发访问的优化

## 介绍一下 ping 的过程，分别用到了哪些协议

## 一个ip配置多个域名，靠什么识别？

## 服务器攻击（DDos 攻击）

## DNS 的工作过程和原理

## OSA 七层协议和五层协议，分别有哪些

## IP 寻址和 MAC 寻址有什么不同，怎么实现的

# 数据库

## 关系型和非关系型数据库的区别（低频）

## 什么是非关系型数据库（低频）

## 说一下MySQL执行一条查询语句的内部执行过程？

## 数据库的索引类型

## 说一下事务是怎么实现的

## MySQL 怎么建立索引，怎么建立主键索引，怎么删除索引

## 【热门】索引的优缺点，什么时候使用索引，什么时候不能使用索引

## 【热门】索引的底层实现

## 【热门】B 树和 B + 树的区别

## 索引最左前缀 / 最左匹配

## 【热门】Mysql 的优化（索引优化，性能优化）

## MYSQL 数据库引擎介绍，innodb 和 myisam 的特点与区别

## MySQL和Redis的区别

## 数据库中事务的 ACID（四大特性都要能够举例说明，理解透彻，比如原子性和一致性的关联，隔离性不好会出现的问题）

## 什么是脏读，不可重复读和幻读？

## 数据库的隔离级别，mysql 和 Oracle 的隔离级别分别是什么（重点）

## 数据库连接池的作用

## Mysql 的表空间方式，各自特点

## 分布式事务

## 数据库的范式

## 数据的锁的种类，加锁的方式

## 什么是共享锁和排他锁

## 分库分表的理解和简介

## 数据库高并发的解决方案

## 乐观锁与悲观锁解释一下

## 乐观锁与悲观锁是怎么实现的

## 对数据库目前最新技术有什么了解吗

# Linux

## 【热门】Linux 的 I/O 模型介绍以及同步异步阻塞非阻塞的区别

## 文件系统的理解（EXT4，XFS，BTRFS）

## EPOLL 的介绍和了解

## IO 复用的三种方法（select,poll,epoll）深入理解，包括三者区别，内部原理实现？

## Epoll 的 ET 模式和 LT 模式（ET 的非阻塞）

## 查询进程占用 CPU 的命令（注意要了解到 used，buf，代表意义）

## linux 的其他常见命令（kill，find，cp 等等）

## shell 脚本用法

## 硬连接和软连接的区别

## 文件权限怎么看（rwx）

## 文件的三种时间（mtime, atime，ctime），分别在什么时候会改变

## Linux 监控网络带宽的命令，查看特定进程的占用网络资源情况命令

## Linux 中线程的同步方式有哪些？

## 怎么修改一个文件的权限

## 查看文件内容常用命令

## 怎么找出含有关键字的前后 4 行

## Linux的GDB调试

## coredump 是什么，怎么才能 coredump

## tcpdump 常用命令

## crontab 命令

## 查看后台进程

# 场景题、算法和数据结构

## leetcode hot100 至少刷两遍，剑指 offer 至少刷两遍 重中之重！！

## 介绍熟悉的设计模式（单例，简单工厂模式）

## 写单例模式，线程安全版本

## 写三个线程交替打印 ABC

## 二维码登录的实现过程

## 不使用临时变量实现 swap 函数

## 实现一个 strcpy 函数（或者 memcpy），如果内存可能重叠呢

## 实现快排

## 实现一个堆排序

## 实现一个插入排序

## 快排存在的问题，如何优化

## 反转一个链表

## 【热门】Top K 问题（可以采取的方法有哪些，各自优点？）

## 8G 的 int 型数据，计算机的内存只有 2G，怎么对它进行排序？（外部排序）

## 自己构建一棵二叉树，使用带有 null 标记的前序遍历序列

## 介绍一下 b 树和它的应用场景有哪些

## 介绍一下 b+ 树和它的应用场景有哪些

## 介绍一下红黑树和它的应用场景有哪些

## 怎么写 sql 取表的前 1000 行数据

## N 个骰子出现和为 m 的概率

## 海量数据问题（可参考左神的书）

## 一致性哈希

## 希尔排序，手撕

## Dijkstra 算法

## 如何实现一个动态数组

## 最小生成树算法说一下

## 海量数据的 bitmap 使用原理

## 布隆过滤器原理与优点

## 布隆过滤器处理大规模问题时的持久化，包括内存大小受限、磁盘换入换出问题

## 实现一个队列，并且使它支持多线程，队列有什么应用场景

# 智力题

## 100 层楼，只有 2 个鸡蛋，想要判断出那一层刚好让鸡蛋碎掉，给出策略

## 毒药问题，1000 瓶水，其中有一瓶可以无限稀释的毒药，要快速找出哪一瓶有毒，需要几只小白鼠

## 先手必胜策略问题：100 本书，每次能够拿 1-5 本，怎么拿能保证最后一次是你拿

## 放 n 只蚂蚁在一条树枝上，蚂蚁与蚂蚁之间碰到就各自往反方向走，问总距离或者时间

## 瓶子换饮料问题：1000 瓶饮料，3 个空瓶子能够换 1 瓶饮料，问最多能喝几瓶

## 在 24 小时里面时针分针秒针可以重合几次

## 有一个天平，九个砝码，一个轻一些，用天平至少几次能找到轻的？

## 有十组砝码每组十个，每个砝码重 10g，其中一组每个只有 9g，有能显示克数的秤最少几次能找到轻的那一组砝码？

## 生成随机数问题：给定生成 1 到 5 的随机数 Rand5()，如何得到生成 1 到 7 的随机数函数 Rand7()

## 赛马：有 25 匹马，每场比赛只能赛 5 匹，至少要赛多少场才能找到最快的 3 匹马？

## 烧 香 / 绳子 / 其他 确定时间问题：有两根不均匀的香，燃烧完都需要一个小时，问怎么确定 15 分钟的时长？

## 掰巧克力问题 N\_M 块巧克力，每次掰一块的一行或一列，掰成 1\_1 的巧克力需要多少次？（1000 个人参加辩论赛，1V1，输了就退出，需要安排多少场比赛）

# 大数据

## 介绍一下 Hadoop

## 说一下 MapReduce 的运行机制

## 介绍一下 kafka

## 为什么 kafka 吞吐量高？介绍一下零拷贝

## 介绍一下 spark

## 介绍一下 spark-streaming

## spark 的 transformation 和 action 有什么区别

## spark 常用的算子说几个

## 如何保证 kafka 的消息不丢失

## kafka 如何选举 leader

## 说下 spark 中的宽依赖和窄依赖

## 说下 spark 中 stage 是依照什么划分的

## spark 的内存管理是怎样的

## spark 的容错机制是什么样的

# HR面

## 自我介绍

## 项目中遇到的最大难点

## 项目中的收获

## 可以实习的时间，实习时长

## 哪里人

## 说一下自己的性格

## 你的优缺点是什么

## 有什么兴趣爱好，画的怎么样 / 球打的如何 / 游戏打的怎么样

## 看过最好的一本书是什么

## 学习技术中有什么难点

## 怎么看待加班

## 觉得深圳怎么样（或者其他地点）

## 遇见过最大的挫折是什么，怎么解决的

## 职业规划

## 目前的 offer 情况

## 你最大的优势和劣势是什么

## 介绍在项目里面充当的角色

## 介绍一下本科获得的全国赛奖项的情况

## 最有成就感的事情 / 最骄傲的一件事情

## 在实验室中担任什么角色，参加的 XXX 能聊聊吗

## 用两个词来形容自己

# 项目

## 轻量级加密服务器

## TCP拥塞控制

## 轻量级数据存储（Redis）

# 反问