

参考书目

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		29
《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《C++ Primer》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。

本书主要整理和修改自：超全面的后端开发 C/C++ 面经整理分享：<https://www.nowcoder.com/discuss/489210>

整理者：Hansimov

C++

1. 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
1	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
2	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
3	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
4	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
5	指针可以有级	引用只能有一级
6	可以用 const 指针	没有 const 引用
7	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

2. 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。

2. 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。

3. 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
1	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
2	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。
3	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。
4	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
5	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）。

6	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）。
7	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

4. 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。

5. 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）在申请的空間上执行构造函数，完成对象的构造

delete: （1）在空間上执行析构函数，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）在申请的空間上执行 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	}
18	

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	
7	RTCCALLBACK(_RTC_Free_hook, (pUserData, 0));

operator delete() 的全局函数原型	
8	
9	<code>if (pUserData == NULL)</code>
10	<code>return;</code>
11	
12	<code>_mlock(_HEAP_LOCK); /* block other threads */</code>
13	<code>__TRY</code>
14	<code>/* get a pointer to memory block header */</code>
15	<code>pHead = pHdr(pUserData);</code>
16	
17	<code>/* verify block type */</code>
18	<code>_ASSERTE(_BLOCK_TYPE_IS_VALID(pHead->nBlockUse));</code>
19	
20	<code>_free_dbg(pUserData, pHead->nBlockUse);</code>
21	
22	<code>__FINALLY</code>
23	<code>_munlock(_HEAP_LOCK); /* release other threads */</code>
24	<code>__END_TRY_FINALLY</code>
25	
26	<code>return;</code>
27	<code>}</code>
28	
29	<code>/*</code>
30	<code>free 的实现</code>
31	<code>*/</code>
32	<code>#define free(p) _free_dbg(p, _NORMAL_BLOCK)</code>
33	

6. 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
1	库函数和运算符	new 和 delete 是运算符。	malloc 和 free 是库函数。
2	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。
3	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。
4	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 。

5	是否指定分配内存的大小	<code>new</code> 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。	<code>malloc</code> 需要显式地指出所需内存的大小。[5]
6	是否调用构造函数和析构函数	<code>new</code> 会调用构造函数， <code>delete</code> 会调用析构函数。[6,7]	<code>malloc</code> 不会调用构造函数。
7	处理数组	<code>new[]</code> 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 <code>new[]</code> 分配的内存必须使用 <code>delete[]</code> 释放，否则会只释放部分对象，造成内存泄露。	<code>malloc</code> 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 <code>malloc</code> 动态分配数组的内存，需要手动指定数组的大小。
8	是否可以相互调用	<code>operator new</code> 和 <code>operator delete</code> 的实现可以基于 <code>malloc</code> 和 <code>free</code> 。[8]	<code>malloc</code> 的实现不能调用 <code>new</code> 。
9	是否可以被重载	<code>operator new</code> 和 <code>operator delete</code> 可以被重载。[9]	<code>malloc</code> 不允许重载。
10	扩充已分配内存	<code>new</code> 没有相关处理方式。	使用 <code>malloc</code> 分配内存后，可以用 <code>realloc</code> 函数重新分配内存。[10]
11	内存分配时内存不足	<code>new</code> 可以指定处理函数或重新制定分配器。[11]	<code>malloc</code> 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：

```
1 int *a = (int *)malloc ( sizeof (int ));
2 if(NULL == a) {
3     ...
4 } else {
5     ...
6 }
```

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 }
```

5. new 不需要指定内存大小，malloc 则需要：

```
1 class A{...}  
2 A * ptr = new A;  
3 A * ptr = (A *)malloc(sizeof(A)); // 需要显式指定所需内存大小 sizeof(A);  
4 // 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
```

6. 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。

7. 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）。

8. 一种极简的 operator new 和 operator delete 的实现方式：

```
1 void * operator new(sieze_t size) {  
2     if(void * mem = malloc(size))  
3         return mem;  
4     else  
5         throw bad_alloc();  
6 }  
7 void operator delete(void *mem) noexcept {  
8     free(mem);  
9 }
```

9. 标准库为 operator new 和 operator delete 各定义了 4 个重载版本：

```
1 // 这些版本可能抛出异常  
2 void * operator new(size_t);  
3 void * operator new[](size_t);  
4 void * operator delete(void *) noexcept;  
5 void * operator delete[](void *0) noexcept;  
6 // 这些版本承诺不抛出异常  
7 void * operator new(size_t, nothrow_t&) noexcept;  
8 void * operator new[](size_t, nothrow_t& );  
9 void * operator delete(void *, nothrow_t& ) noexcept;
```



```
10 void * operator delete[](void *0, nothrow_t& ) noexcept;
```

10. `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。
11. 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：

```
1 namespace std {  
2     typedef void (*new_handler)();  
3 }
```

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 }
```

7. 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 `malloc/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。

8. C 和 C++的区别

9. C++和 Java 的联系与区别，包括语言特性、垃圾回收、应用场景等

10. Java 的垃圾回收机制

11. C++和 Python 的区别

12. struct 和 class 的区别

13. define 和 const 的联系与区别（编译阶段、安全性、内存占用等）

14. C++中 const 的用法（定义，用途）

15. C++ 中的 static 用法和意义

16. 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

17. 【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

18. STL 源码中的 hash 表的实现

19. 解决哈希冲突的方式

20. STL 中 unordered_map 和 map 的区别

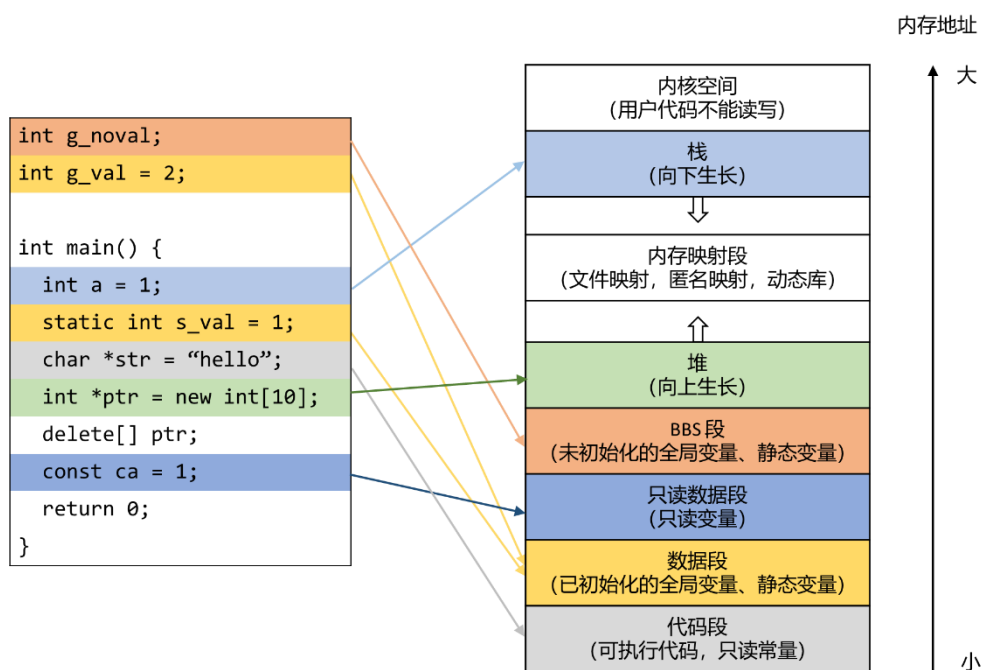
21. STL 中 vector 的实现

22. 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

23. C++ 中 vector 和 list 的区别

24. C++ 中的重载和重写的区别：

25. 【热门】C++ 内存管理



C/C++内存布局

26. 介绍面向对象的三大特性，并且举例说明每一个
27. 多态的实现（和下一个问题一起回答）
28. **【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
29. 实现编译器处理虚函数表应该如何处理
30. 基类的析构函数一般写成虚函数的原因
31. 构造函数为什么一般不定义为虚函数
32. 构造函数或者析构函数中调用虚函数会怎样
33. 纯虚函数
34. 静态绑定和动态绑定的介绍
35. 深拷贝和浅拷贝的区别（举例说明深拷贝的安全性）
36. 对象复用的了解，零拷贝的了解
37. 介绍 C++ 所有的构造函数
38. 什么情况下会调用拷贝构造函数（三种情况）
39. 结构体内存对齐方式和为什么要进行内存对齐？
40. 内存泄露的定义，如何检测与避免？
41. C++的智能指针有哪些
42. 调试程序的方法

- 43. 遇到 coredump 要怎么调试
- 44. inline 关键字说一下 和宏定义有什么区别
- 45. 模板的用法与适用场景，实现原理
- 46. 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）
- 47. 用过 C11 吗，知道 C11 新特性吗？（有面试官建议熟悉 C11）
- 48. C++的调用惯例（简单一点 C++函数调用的压栈过程）
- 49. C++的四种强制转换
- 50. string 的底层实现
- 51. 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
- 52. set，map 和 vector 的插入复杂度
- 53. 定义和声明的区别
- 54. typedef 和 define 的区别
- 55. 被 free 回收的内存是立即返还给操作系统吗？为什么？
- 56. 引用作为函数参数以及返回值的好处
- 57. 友元函数和友元类
- 58. 说一下 volatile 关键字的作用
- 59. STL 中的 sort() 算法是用什么实现的，stable_sort() 呢

60. vector 会迭代器失效吗？什么情况下会迭代器失效？

61. 为什么 C++ 没有实现垃圾回收？

操作系统

1. **【热门】** 进程与线程的区别和联系
2. 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
3. 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？
4. **【热门】** 进程之间的通信方法有哪几种
5. 进程调度方法详细介绍
6. 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
7. 操作系统的内存管理说一下
8. 实现一个 LRU 算法
9. 死锁产生的必要条件（怎么检测死锁，解决死锁问题）
10. 死锁的恢复
11. 什么是饥饿
12. 如果要你实现一个 mutex 互斥锁你要怎么实现？
13. 线程之间的通信方式有哪些？进程之间的同步方式又哪些？
14. 什么时候用多进程，什么时候用多线程
15. 文件读写使用的系统调用
16. 孤儿进程和僵尸进程分别是什么，怎么形成的？

17. 说一下 PCB / 说一下进程地址空间
18. 内核空间和用户空间是怎样区分的
19. 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）
20. 同一个进程内的线程会共享什么资源？
21. 异常和中断的区别
22. 一般情况下在 Linux / Windows 平台下栈空间的大小
23. 虚拟内存的了解
24. 服务器高并发的解决方案
25. 【热门】协程了解吗
26. 协程的底层是怎么实现的，怎么使用协程？
27. 进程的状态以及转换图
28. 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？
29. 什么是字节序？怎么判断是大端还是小端？有什么用？

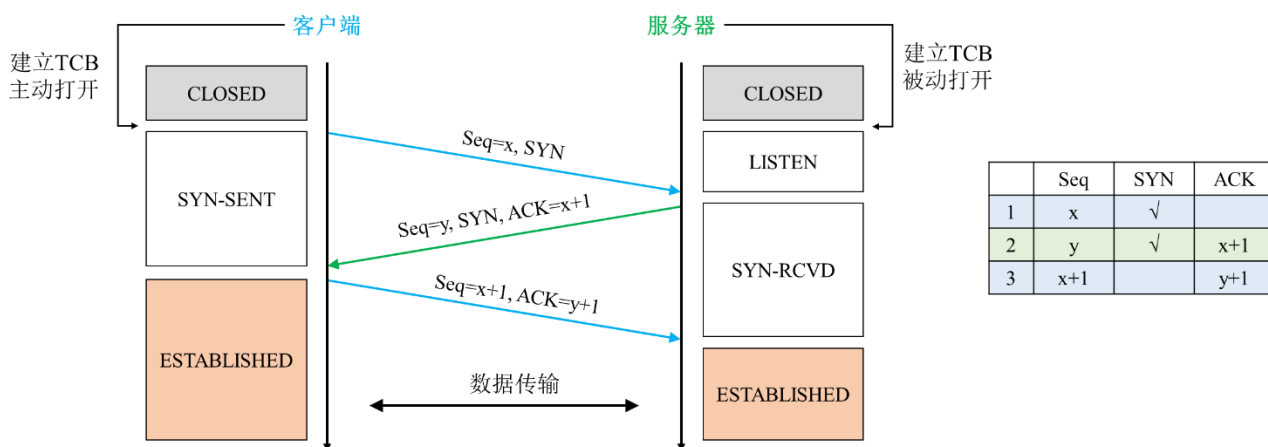
计算机网络

1. 建立 TCP 服务器的各个系统调用

2. 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？
3. 对路由协议的了解与介绍
4. UDP 如何实现可靠传输
5. TCP 和 UDP 的区别
6. TCP 和 UDP 相关的协议与端口号
7. TCP (UDP, IP) 等首部的认识 (http 请求报文构成)
8. 网页解析的过程与实现方法
9. **【热门】**在浏览器中输入 URL 后执行的全部过程
10. 网络层分片的原因与具体实现
11. **【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端均处于 **CLOSED**（关闭）状态。

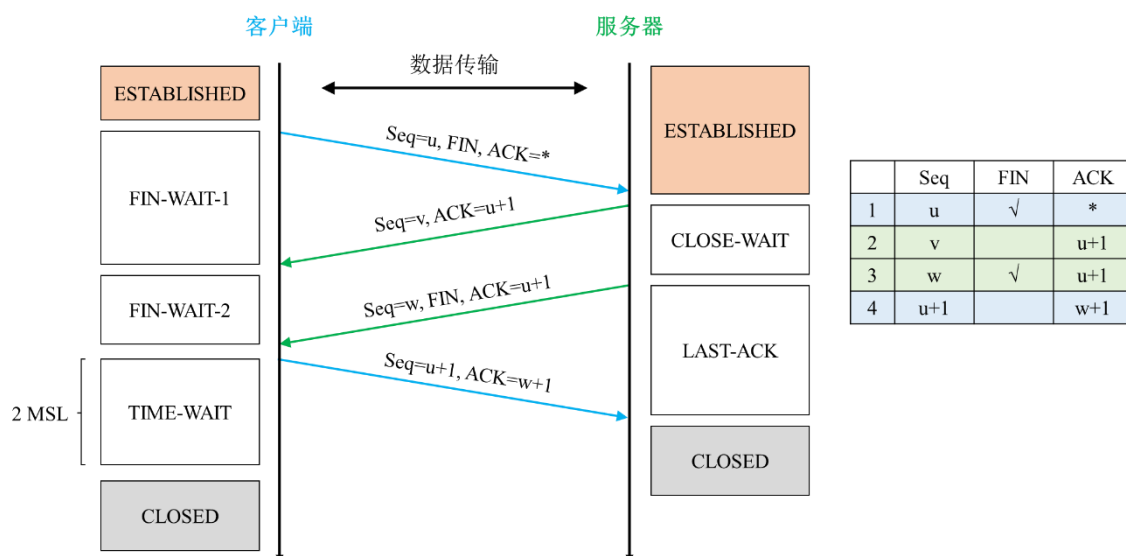
服务器进程创建传输控制块 TCB，等待接收客户端进程的连接请求，进入 **LISTEN**（监听）状态。

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端都处于 **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

12. TCP 握手以及每一次握手客户端和服务端处于哪个状态

见上题。

13. 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/tH8RFmjrvOmgLvk9hmrkw>
- <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从分辨出 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, 客户端和服务端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, 客户端和服务端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
2. 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
3. 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。

14. TCP 三次握手时的第一次的 seq 序号是怎样产生的
15. TIME_WAIT 的意义（为什么要等于 2MSL）
16. 超时重传机制（不太高频）
17. TCP 怎么保证可靠性？
18. 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）？
19. TCP 滑动窗口协议
20. 拥塞控制和流量控制的区别
21. 【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>

- 22. TCP/IP 的粘包与避免介绍一下
- 23. 说一下 TCP 的封包和拆包
- 24. HTTP 协议与 TCP 的区别与联系
- 25. HTTP/1.0 和 HTTP/1.1 的区别
- 26. http 的请求方法有哪些？get 和 post 的区别
- 27. http 的常见状态码和含义
- 28. http 和 https 的区别，由 http 升级为 https 需要做哪些操作
- 29. https 的具体实现，怎么确保安全性
- 30. 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？
- 31. 对称密码和非对称密码体系
- 32. 【热门】数字证书的了解
- 33. 服务器出现大量 close_wait 的连接的原因以及解决方法
- 34. 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？
- 35. 单条记录高并发访问的优化
- 36. 介绍一下 ping 的过程，分别用到了哪些协议
- 37. 一个 ip 配置多个域名，靠什么识别？

38. 服务器攻击（DDos 攻击）

39. DNS 的工作过程和原理

40. OSA 七层协议和五层协议，分别有哪些

41. IP 寻址和 MAC 寻址有什么不同，怎么实现的

数据库

1. 关系型和非关系型数据库的区别（低频）

2. 什么是非关系型数据库（低频）

3. 说一下 MySQL 执行一条查询语句的内部执行过程？

4. 数据库的索引类型

- mysql 四种索引类型：<https://my.oschina.net/zhangqie/blog/1618391>
- 聚集索引和非聚集索引（整理）：<https://www.cnblogs.com/aspnethot/articles/1504082.html>

逻辑分类：

- 主键索引：在关系表中定义主键时会自动创建主键索引。每张表中的主键索引只能有一个，要求主键中的每个值都唯一，即不可重复，也不能有空值。

```
alter table table_name add primary key (col1, col2, ...)
```

- 唯一索引：数据列不能有重复，但可以有空值。一张表可以有多个唯一索引，但是每个唯一索引只能有一列。（比如身份证、卡号）

```
alter table table_name add unique (col1, col2, ...)
```

- 普通索引：可以重复，可以为空值。一张表可以有多个普通索引。

```
alter table table_name add index (col1, col2, ...)
```

- 全文索引：可以加快模糊查询。可以在 varchar、char、text 类型的列上创建。

```
alter table table_name add fulltext (col1, col2, ...)
```

物理分类：

- 聚集索引 / 聚簇索引 / 主索引：数据在物理存储中的顺序和在索引中的逻辑顺序相同。
 - 比如以 ID 建立聚集索引，数据库中 ID 从小到大排列，物理存储中该数据的内存地址也从小到大排列。
 - 一般是表中的主键索引，若没有主键索引，则以第一个非空的唯一索引作为聚集索引
 - 一张表只能有一个聚集索引，但是该索引可以有多个列（组合索引）
 - 聚集索引对于经常要搜索范围值的列特别有效，找到聚集索引中包含第一个值的行后，可以确保后续索引值的行在物理上相邻
 - 当索引值唯一时，使用聚集索引查找特定的行也很有效率
- 非聚集索引 / 非聚簇索引 / 辅助索引：数据在物理存储中的顺序和在索引中的逻辑顺序不同。
 - 由于非聚集索引无法定位数据所在行，因此需要扫描两遍索引树。第一遍扫描非聚集索引的索引树，确定该数据的主键 ID，第二遍到主键索引（聚集索引）中寻找对应数据
 - 聚集索引的叶结点就是数据结点，而非聚集索引的叶结点仍然是索引结点，只不过有一个指针指向对应的数据块

5. MySQL 怎么建立索引，怎么建立主键索引，怎么删除索引

- 建立索引：alter table add 或者 create index。
- 删除索引：alter table drop 或者 drop index。

```
1 alter table table_name add primary key (col1, col2, ...) # 添加主键索引
2 alter table table_name add index (col1, col2, ...)      # 添加普通索引
3 alter table table_name add unique (col1, col2, ...)     # 添加唯一索引
4
5 create index index_name on table_name (col1, col2, ...) # 创建普通索引
6 create unique index_name on table_name (col1, col2, ...) # 创建唯一索引
7
8 alter table table_name drop index index_name # 删除普通索引
9 alter table table_name drop primary key      # 删除主键索引
10
11 drop index index_name on table_name # 删除索引
```

6. 主键、外键和索引的区别

- 关于数据库主键和外键（终于看懂啦）：<https://blog.csdn.net/harbor1981/article/details/53449435>
- MySQL 数据库的主键和外键详解 3：<https://zhuanlan.zhihu.com/p/114834741>

	主键	外键	索引
--	----	----	----

定义	主键是表中一列或多列的组合，其值能唯一地标识表中的每一行。	若一个公共关键字在某个关系中是主关键字，则该公共关键字称为另一个关系的外键。[1]	见上上题
示例	自增整数类型 全局唯一 GUID 类型		
作用	保证表的实体完整性 加快数据库的操作速度	保持数据一致性和完整性 和其他表建立联系	索引用于提高查询排序速度
个数	一张表只能有一个主键	一张表可以有多个外键	一张表可以有多个唯一索引

[1] 以该公共关键字作主关键字的表被称为主表，具有此外键的表被称为主表的从表。外键又称作外关键字。

外键举例：

student 表

id	class_id	name	age	sex
1	1	张三	16	男
2	1	李四	17	男
3	2	王五	18	女
4	1	赵六	18	男
(Auto)	(NULL)	(NULL)	(NULL)	(NULL)

class 表

id	class_name
1	高三一班
2	高三二班
(Auto)	(NULL)

- 在 student 表中，通过 class_id 字段可以把数据与另一张表 class 关联起来，这里的 class_id 就是外键。
- 由于一个班级可以有多个学生，在关系模型中，这两个表的关系称为“一对多”，即 class 表的一个记录可以对应 student 表的多个记录。
- 为了表达这种一对多的关系，我们需要在 student 表中加入一列 class_id，让它的值与 class 表的某条记录相对应。这样，我们就可以根据 class_id 这个列直接定位出 student 表的一条记录应该对应到 class 的哪条记录。

外键并不是通过列名实现的，而是通过定义外键约束实现的：

```

1  // 定义外键约束
2  ALTER TABLE student
3  ADD CONSTRAINT fk_class_id  // 外键约束的名称 fk_class_id 可以任意
4  FOREIGN KEY (class_id)      // 指定 class_id 作为外键
5  REFERENCES class (id);      // 指定这个外键关联到 class 表的 id 列（即 class 表的主键）
6
7  // 删除外键约束
8  ALTER TABLE student
9  DROP FOREIGN KEY fk_class_id;
```

由于外键约束会降低数据库的性能，大部分互联网应用程序为了追求速度，并不设置外键约束，而是仅靠应用程序自身来保证逻辑的正确性。这种情况下，class_id 仅仅是一个普通的列，只是它起到了外键的作用而已。

7. 【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

- 浅谈索引的优缺点和建立索引的原则: <https://www.jianshu.com/p/107e5bdf4148>
- 数据库中索引的优缺点（转）: <https://www.cnblogs.com/guojin705/archive/2011/06/21/2086429.html>
- 数据库的索引的优缺点: <https://programtip.com/zh/art-70024>

索引的优点:

- 可以大大加快数据的检索速度，这也是创建索引的最主要的原因
- 通过创建唯一索引，可以保证数据库表中每一行数据的唯一性
- 可以加速表和表之间的连接，特别是在实现数据的参照完整性方面很有意义
- 可以减少分组和排序子句进行数据检索的时间
- 可以在查询过程中使用优化隐藏器，提高系统性能

索引的缺点:

- 创建索引和维护索引要耗费时间，这种时间随着数据量的增加而增加
- 索引需要占用物理空间，除了数据表占数据空间之外，每个索引还要占一定的物理空间，如果要建立聚簇索引，那么需要的空间会更大
- 对表中的数据进行增加、删除和修改时，索引也要动态维护，降低了数据的维护速度

什么时候使用索引:

- 经常需要搜索的列: 可以加快搜索的速度
- 作为主键的列: 强制该列的唯一性和组织表中数据的排列结构
- 经常用在连接的列: 这些列主要是一些外键，可以加快连接的速度
- 经常需要根据范围进行搜索的列: 因为索引已经排序，其指定的范围是连续的
- 经常需要排序的列: 因为索引已经排序，可以加快排序查询速度
- 经常使用在 **WHERE** 子句中的列: 加快条件的判断速度

什么时候不能使用索引:

- 在查询中很少使用或者参考的列: 因为这些列很少用到，有无索引并不能提高查询速度。相反，由于增加了索引，反而降低了系统的维护速度，增大了空间需求。
- 只有很少数据值的列: 由于这些列的取值很少，例如人事表的性别列，在查询的结果中，结果集的数据行占了表中数据行的很大比例，即需要在表中搜索的数据行的比例很大，增加索引并不能明显加快检索速度。
- 定义为 **text**, **image** 和 **bit** 数据类型的列: 因为这些列要么数据量很大，要么取值很少。
- 当修改性能远远大于检索性能时: 因为修改性能和检索性能是互相矛盾的。当增加索引时，会提高检索性能，但是会降低修改性能；当减少索引时，会提高修改性能，降低检索性能。因此，当修改性能远远大于检索性能时，不应该创建索引。

8. 【热门】索引的底层实现

- 深入理解 MySQL 索引底层实现原理: <https://zhuanlan.zhihu.com/p/77383599>

索引是数据结构

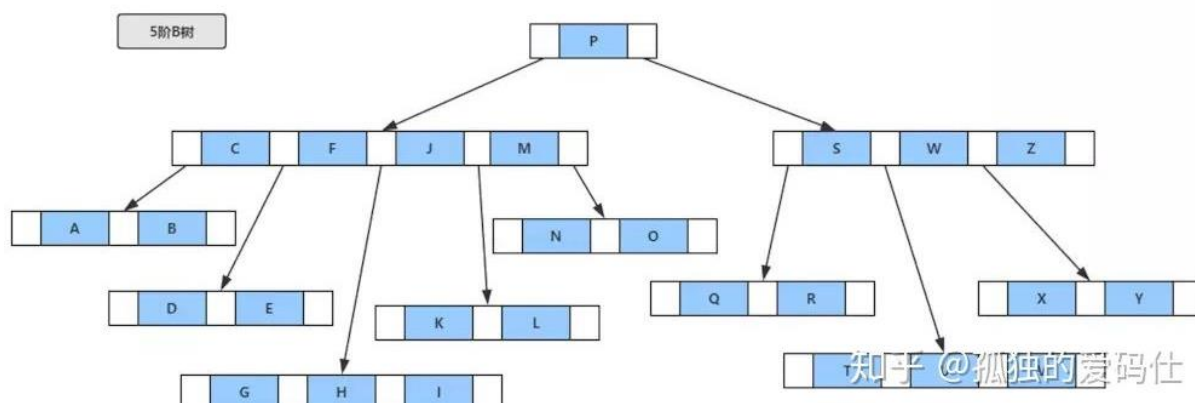
MySQL 官方对索引的定义为：索引（Index）是帮助 MySQL 高效获取数据的数据结构。

提取句子主干，就可以得到索引的本质：**索引是数据结构**。

- 数据库查询是数据库的最主要功能之一。我们都希望查询数据的速度能尽可能的快，因此数据库系统的设计者会从查询算法的角度进行优化。
- 最基本的查询算法当然是顺序查找，这种复杂度为 $O(n)$ 的算法在数据量很大时显然是糟糕的，好在计算机科学的发展提供了很多更优秀的查找算法，例如二分查找、二叉树查找等。
- 每种查找算法都只能应用于特定的数据结构之上（例如二分查找要求被检索数据有序，而二叉树查找只能应用于二叉查找树上），但是数据本身的组织结构不可能完全满足各种数据结构（例如理论上不可能同时将两列都按顺序进行组织）
- 所以，在数据之外，数据库系统还维护着满足特定查找算法的数据结构，这些数据结构以某种方式引用（指向）数据，这样就可以在这些数据结构上实现高级查找算法。
- 这种数据结构，就是索引。

B 树

B 树事实上是一种平衡的多叉查找树，也就是说最多可以开 m 个叉（ $m \geq 2$ ），称之为 m 阶 B 树，下图是一棵 5 阶 B 树。



总的来说， m 阶 B 树满足以下条件：

- 每个节点最多有 m 棵子树。
- 若根节点不是叶节点，则至少有 2 个子节点
 - 极端情况下一棵树就一个根节点，同时是根、叶、树

- 非根非叶的节点至少有 $\lceil \frac{m}{2} \rceil$ 个子树，图中 5 阶 B 树，每个节点至少有 3 个子树，也就是至少有 3 个叉。
- 有 n 个子节点的非叶节点有 n-1 个键
 - 非叶节点中的信息包括 $[n, A_1, K_1, A_2, K_2, \dots, K_{n-1}, A_{n-1}]$ ，其中 n 表示该节点中保存的节点个数，K 为关键字且 $K_i < K_{i+1}$ ，A 为指向子树的根节点的指针。
- 所有叶子节点都在同一层
 - 换句话说，从根到叶子的每一条路径都有相同的长度
 - 这些叶子节点包含的指针为空，表示找不到指定的值

B 树的查询过程和二叉排序树比较类似，从根节点依次比较每个结点，因为每个节点中的关键字和左右子树都是有序的，所以只要比较节点中的关键字，或者沿着指针就能很快地找到指定的关键字，如果查找失败，则会返回叶子节点，即空指针。

B 树搜索的伪代码如下：

```

1  BTree_Search(node, key) {
2      if(node == null) return null;
3      foreach(node.key) {
4          if(node.key[i] == key) return node.data[i];
5          if(node.key[i] > key) return BTree_Search(point[i]->node);
6      }
7      return BTree_Search(point[i+1]->node);
8  }
9  data = BTree_Search(root, my_key);

```

B 树的特点：

- 关键字集合分布在整颗树中。
- 任何一个关键字出现且只出现在一个节点中。
- 搜索有可能在非叶子节点结束。
- 其搜索性能等价于在关键字集合内做一次二分查找。
- B 树在插入删除新的数据记录会破坏 B 树的性质，因为在插入删除时，需要对树进行一个分裂、合并、转移等操作以保持 B 树性质。

B+树

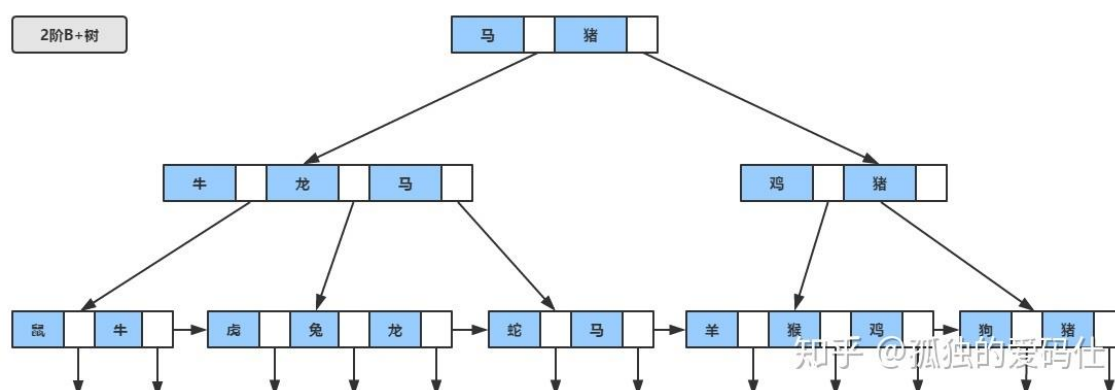
作为 B 树的加强版，B+树与 B 树的差异在于：

（详见下题）

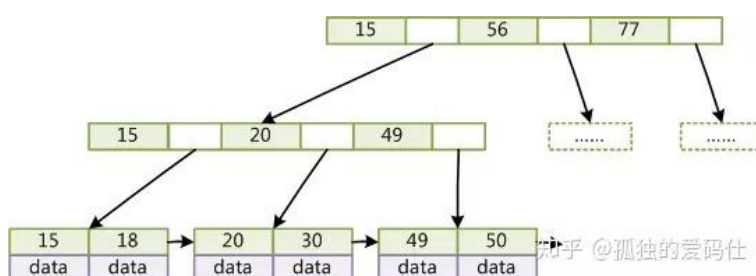
B+树的特性如下：

- 所有关键字都存储在叶子节点上，且链表中的关键字恰好是有序的。

- 查找时不可能返回非叶子节点。
- 非叶子节点相当于叶子节点的索引，叶子节点相当于是存储（关键字）数据的数据层。
- 更适合文件索引系统。



一般在数据库系统或文件系统中使用的 B+树结构都在经典 B+树的基础上进行了优化，增加了顺序访问指针。



如上图所示，在 B+树的每个叶子节点增加一个指向相邻叶子节点的指针，就形成了带有顺序访问指针的 B+树。

做这个优化的目的是为了提高区间访问的性能，例如图中要查询 key 为从 18 到 49 的所有数据记录，当找到 18 后，只需顺着节点和指针顺序遍历就可以一次性访问到所有数据节点，极大提高了区间查询效率。

MySQL 为什么使用 B/B+树

红黑树等数据结构也可以用来实现索引，但是文件系统以及数据库系统普遍采用 B 树或者 B+树。

一般来说，索引本身也很大，不可能全部存储在内存中，因此索引往往以索引文件的形式存储在磁盘上。这样的话，索引查找过程中就要产生磁盘 I/O 消耗，相对于内存存取，I/O 存取的消耗要高几个数量级，所以评价一个数据结构作为索引的优劣最重要的指标就是在查找过程中磁盘 I/O 操作次数的渐进复杂度。

换句话说，索引的结构组织要尽量减少查找过程中磁盘 I/O 的存取次数。

下面先介绍内存和磁盘存取原理，然后再结合这些原理分析 B/B+树作为索引的效率。

（该部分略）

先从 B 树分析，根据定义，可知检索一次最多需要访问 h 个节点， h 为树高。

数据库系统的设计者巧妙利用了磁盘预读原理，将一个节点的大小设为等于一个页，这样每个节点只需要一次 I/O 就可以完全载入。

B 树中一次检索最多需要 $(h-1)$ 次 I/O（根节点常驻内存），渐进复杂度为 $O(h) = O(\log_d N)$ * $O(h) = O(\log_d N)$ 。一般实际应用中，出度 d 是非常大的数字，通常超过 100，因此 h 非常小（通常不超过 3），这里的出度 d 表示树的度，即树中各个节点的度的最大值。因此用 B 树作为索引结构效率是非常高的。

为什么不用红黑树？

而红黑树这种结构， h 明显要大的多。由于逻辑上很近的节点（父子）在物理上可能很远，无法利用空间局部性，所以红黑树的 I/O 渐进复杂度也为 $O(h)$ ，效率明显比 B+树差很多。上文还说过，B+树更适合外存索引，原因和内节点出度 d 有关。从上面分析可以看到， d 越大索引的性能越好，而出度的上限取决于节点内 key 和 data 的大小：

$$d_{\max} = \lfloor \frac{\text{page_size}}{\text{key_size} + \text{data_size} + \text{point_size}} \rfloor$$

由于 B+树内节点去掉了 data 域，因此可以拥有更大的出度，性能也更好。

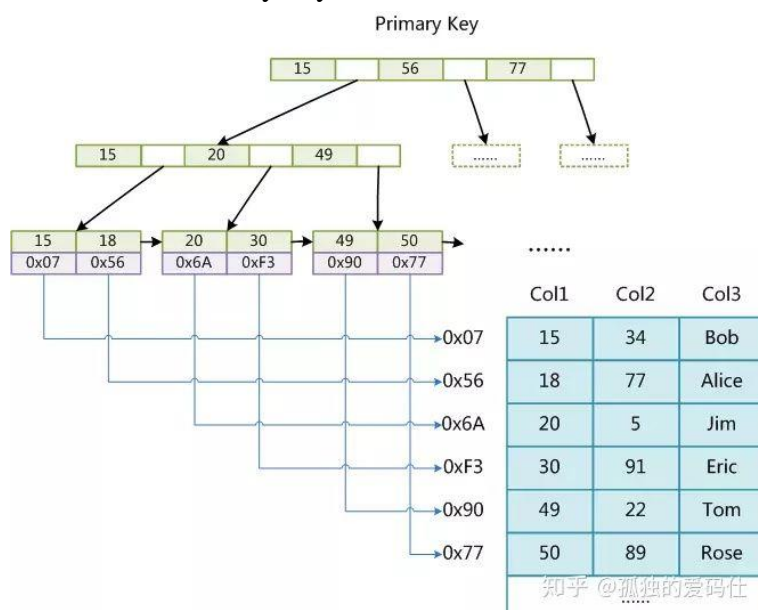
为什么不用 B 树？

- B+树把所有数据都存放在叶子节点上，内部节点保存索引，因此中间节点可以存放更多指针，树可以更矮更胖，减少了查询时的磁盘 I/O 次数，提高了查询效率。
- 叶子节点之间有指针连接，可以进行范围查询，方便区间访问

MyISAM 索引实现

MyISAM 使用 B+树作为索引结构，叶节点的 data 域存放数据记录的地址。

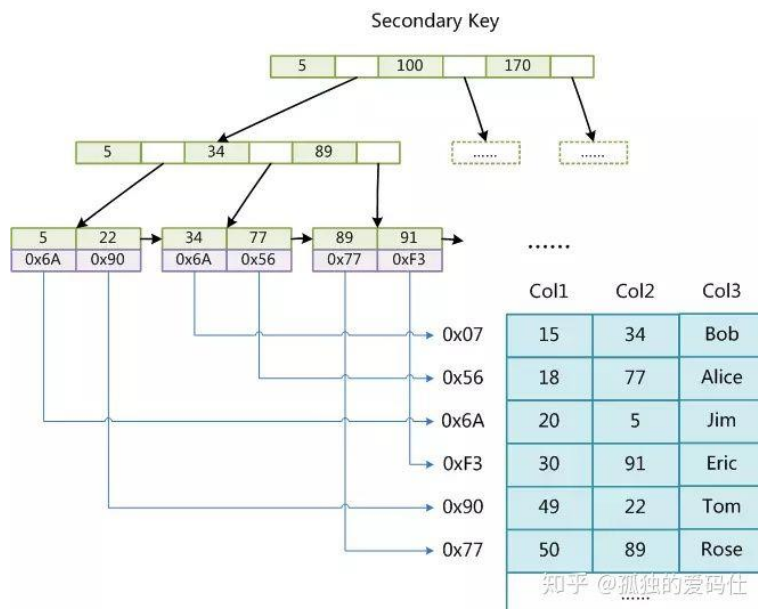
下图是 MyISAM 表的主索引（Primary key）示意图。表一共有三列，以 Col1 为主键。



MyISAM 的主索引示意图

可以看出 MyISAM 的索引文件仅仅保存数据记录的地址。在 MyISAM 中，主索引和辅助索引（Secondary Key）在结构上没有任何区别，只是主索引要求 key 是唯一的，而辅助索引的 key 可以重复。

如果在 Col2 上建立一个辅助索引，则该索引的结构如下图所示：



MyISAM 的辅助索引示意图

同样是一棵 B+树，data 域保存数据记录的地址。

MyISAM 中索引检索的算法：首先按照 B+树搜索算法搜索索引，如果指定的 Key 存在，则取出其 data 域的值，然后以 data 域的值作为地址，读取相应数据记录。

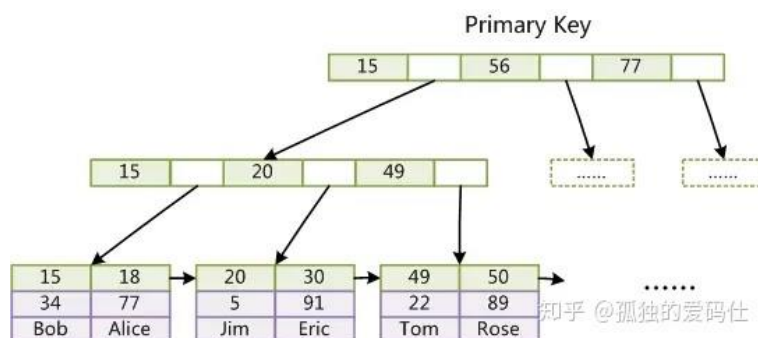
MyISAM 的采用“非聚集索引”，与 InnoDB 的“聚集索引”相区分。

InnoDB 的索引实现

虽然 InnoDB 也使用 B+树作为索引结构，但具体实现方式却与 MyISAM 截然不同。

第一个区别是，InnoDB 的数据文件本身就是索引文件。

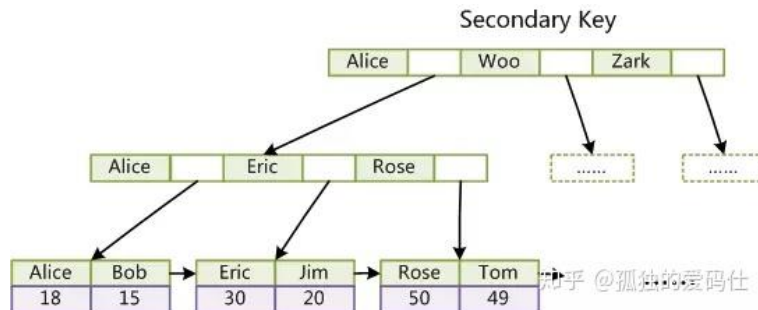
从上文知道，MyISAM 索引文件和数据文件是分离的，索引文件仅保存数据记录的地址。而在 InnoDB 中，表数据文件本身就是按 B+树组织的一个索引结构，这棵树的叶节点 data 域保存了完整的数据记录。这个索引的 key 是数据表的主键，因此 InnoDB 表数据文件本身就是主索引。



InnoDB 的主索引示意图

第二个区别是，InnoDB 的辅助索引中，data 域存储相应记录主键的值，而不是地址。换句话说，InnoDB 的所有辅助索引都引用主键作为 data 域。

下图是定义在 Col3 上的一个辅助索引：



InnoDB 的辅助索引示意图

这里以英文字符的 ASCII 码作为排序的大小比较准则。

聚集索引这种实现方式使得按主键的搜索十分高效，但是辅助索引搜索需要检索两遍索引：首先检索辅助索引获得主键，然后用主键到主索引中检索获得记录。

了解不同存储引擎的索引实现方式对于正确使用和优化索引都非常有帮助。

例如，在 InnoDB 中：

- 不建议使用过长的字段作为主键
 - 因为 InnoDB 所有辅助索引都引用主索引，过长的主索引会令辅助索引变得过大。
- 不建议使用非单调的字段作为主键
 - 因为 InnoDB 数据文件本身是一棵 B+树，非单调的主键会造成在插入新记录时数据文件为了维持 B+树的特性而频繁的分裂调整，十分低效，而使用自增字段作为主键则是一个很好的选择。

9. 【热门】B 树和 B + 树的区别（红黑树）

- B 树 - 维基百科: https://zh.wikipedia.org/wiki/B_树
- B-tree - Wikipedia: <https://en.wikipedia.org/wiki/B-tree>
- 对 B+树, B 树, 红黑树的理解: <https://www.jianshu.com/p/86a1fd2d7406>
- 面试官问你 B 树和 B+树, 就把这篇文章丢给他: <https://blog.ouyangsihai.cn/mian-shi-guan-wen-ni-b-shu-he-b-shu-jiu-ba-zhe-pian-wen-zhang-diu-gei-ta.html>
- database - What are the differences between B trees and B+ trees? : <https://stackoverflow.com/questions/870218/what-are-the-differences-between-b-trees-and-b-trees>
- 平衡二叉树、B 树、B+树、B*树 理解其中一种你就都明白了: <https://zhuanlan.zhihu.com/p/27700617>
- B+树 - 维基百科, 自由的百科全书: https://zh.wikipedia.org/wiki/B%2B_树
- b 树和 b+树的区别: <https://juejin.cn/post/6844903908985274381>
- B+树详解 | Ivanzz: <https://ivanzz1001.github.io/records/post/data-structure/2018/06/16/ds-bplustree>

B+树是 B 树的加强版，与 B 树的差别有：

		B+树	B 树
1	关键字数量	非叶子树的指针个数与关键字个数相同 有 n 个节点的子树包含 n 个关键字，关键字仅起到索引作用	n 个子节点只有 n-1 个关键字
2	存储方式	内部节点仅存储索引不存储数据 叶子节点存储了所有关键字和数据	数据存储在每个节点中
3	有序性	叶子节点根据关键字从小到大顺序连接，形成一个有序链表	
4	查询结果	通过索引找到叶子节点中的数据才能结束，也即走完了从根到叶的完整路径	找到符合条件的节点即返回
5	适用场景	数据库索引	文件索引

B+树的优点：

- 方便全表扫描，只需扫描一遍叶子节点（叶子节点保存了所有的数据）
- 方便区间查询（叶子节点间有指针连接，形成有序链表，数据紧密性和缓冲命中率更高）
- 查询效率更稳定（所有关键字数据地址都存储在叶子节点，每次查找次数相同）

B 树的优点：

- 如果频繁访问距离根结点较近的节点，效率更高（每个节点都保存数据）

10. 索引最左前缀 / 最左匹配

11. 【热门】Mysql 的优化（索引优化，性能优化）

12. 说一下事务是怎么实现的

13. MySQL 数据库引擎介绍，InnoDB 和 MyISAM 的特点与区别

- 深入理解 MySQL 索引底层实现原理：<https://zhuanlan.zhihu.com/p/77383599>
- MyISAM 和 InnoDB 的区别：<https://blog.csdn.net/daiyudong2020/article/details/104468714>
- MySQL 存储引擎——MyISAM 与 InnoDB 区别：<https://blog.csdn.net/xifeijian/article/details/20316775>
- mysql 中 innodb 和 myisam 对比及索引原理区别：https://blog.csdn.net/qq_27607965/article/details/79925288
- Mysql 中 MyISAM 和 InnoDB 的区别有哪些？<https://www.zhihu.com/question/20596402>
- MySQL 存储引擎——MyISAM 与 InnoDB 区别：<https://segmentfault.com/a/1190000008227211>

		MyISAM	InnoDB
6	默认引擎	MySQL 5.5 版本之前	MySQL 5.5 版本及之后
7	外键	×	√
8	事务	×	√（4 个事务隔离级别）
9	行锁	×（表锁）	√（也会退化为表锁）

10	全文索引	√	×（5.7 版本后支持）
11	主键	可以没有	必须有（不设为内置）
12	索引	非聚集索引 只能缓存索引	聚集索引 能缓存索引，也能缓存数据
13	数据存储	索引文件和数据文件分离 （.myi 索引文件和.myd 数据文件）	数据文件按主键聚集 （.idb 数据文件）
14	索引实现方式	见“【热门】索引的底层实现”	
15	并发	读写互相阻塞，但读不会阻塞读	读写阻塞与事务隔离级别有关
16	查询速度	更快 [1]	
17	适用场景	不需要事务支持 并发较低（只能表锁） 数据修改少（阻塞方式），读为主 数据一致性要求较低	需要事务支持 高并发（行级锁） 数据更新较为频繁 数据一致性要求较高 硬件设备内存较大（可缓存索引+数据）

MySQL 里还有：

- MEMORY 存储引擎：将表中数据保存在内存里，适合数据量较小且访问频繁的场景
- MERGE 存储引擎

[1] 为什么 MyISAM 查询更快：

- InnoDB 除了索引还要缓存数据块，MyISAM 只缓存索引，因此加载索引更快
- InnoDB 寻址先到块再到行，MyISAM 直接寻址到文件 offset
- InnoDB 要维护 MVCC（多版本并非控制）一致，即使场景没有也要检查和维护

14. 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）
15. 什么是脏读，不可重复读和幻读？
16. 【热门】数据库的隔离级别，MySQL 和 Oracle 的隔离级别分别是什么
17. MySQL 和 Redis 的区别
18. 数据库连接池的作用
19. Mysql 的表空间方式，各自特点
20. 分布式事务
21. 数据库的范式
22. 数据的锁的种类，加锁的方式
23. 什么是共享锁和排他锁
24. 分库分表的理解和简介
25. 数据库高并发的解决方案
26. 乐观锁与悲观锁解释一下
27. 乐观锁与悲观锁是怎么实现的
28. 对数据库目前最新技术有什么了解吗

Linux

1. **【热门】Linux 的 I/O 模型介绍以及同步异步阻塞非阻塞的区别**
2. **文件系统的理解（EXT4，XFS，BTRFS）**
3. **EPOLL 的介绍和了解**
4. **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？**
5. **Epoll 的 ET 模式和 LT 模式（ET 的非阻塞）**
6. **查询进程占用 CPU 的命令（注意要了解 used，buf，代表意义）**
7. **linux 的其他常见命令（kill，find，cp 等等）**
8. **shell 脚本用法**
9. **硬连接和软连接的区别**
10. **文件权限怎么看（rwx）**
11. **文件的三种时间（mtime, atime，ctime），分别在什么时候会改变**
12. **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**
13. **Linux 中线程的同步方式有哪些？**
14. **怎么修改一个文件的权限**
15. **查看文件内容常用命令**
16. **怎么找出含有关键字的前后 4 行**
17. **Linux 的 GDB 调试**

18. coredump 是什么，怎么才能 coredump

19. tcpdump 常用命令

20. crontab 命令

21. 查看后台进程

场景题、算法和数据结构

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

23. 介绍熟悉的设计模式（单例，简单工厂模式）

24. 写单例模式，线程安全版本

25. 写三个线程交替打印 ABC

26. 二维码登录的实现过程

27. 不使用临时变量实现 swap 函数

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

29. 实现快排

30. 实现一个堆排序

31. 实现一个插入排序

32. 快排存在的问题，如何优化

33. 反转一个链表

- 34. **【热门】** Top K 问题（可以采取的方法有哪些，各自优点？）
- 35. 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）
- 36. 自己构建一棵二叉树，使用带有 null 标记的前序遍历序列
- 37. 介绍一下 b 树和它的应用场景有哪些
- 38. 介绍一下 b+ 树和它的应用场景有哪些
- 39. 介绍一下红黑树和它的应用场景有哪些
- 40. 怎么写 sql 取表的前 1000 行数据
- 41. N 个骰子出现和为 m 的概率
- 42. 海量数据问题（可参考左神的书）
- 43. 一致性哈希
- 44. 希尔排序，手撕
- 45. Dijkstra 算法
- 46. 如何实现一个动态数组
- 47. 最小生成树算法说一下
- 48. 海量数据的 bitmap 使用原理
- 49. 布隆过滤器原理与优点

50. 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

51. 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

1. 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

2. 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

3. 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

4. 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

5. 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

6. 在 24 小时里面时针分针秒针可以重合几次

7. 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？

8. 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？

9. 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()
10. 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？
11. 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？
12. 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

1. 介绍一下 Hadoop
2. 说一下 MapReduce 的运行机制
3. 介绍一下 kafka
4. 为什么 kafka 吞吐量高？介绍一下零拷贝
5. 介绍一下 spark
6. 介绍一下 spark-streaming
7. spark 的 transformation 和 action 有什么区别
8. spark 常用的算子说几个

9. 如何保证 kafka 的消息不丢失
10. kafka 如何选举 leader
11. 说下 spark 中的宽依赖和窄依赖
12. 说下 spark 中 stage 是依照什么划分的
13. spark 的内存管理是怎样的
14. spark 的容错机制是什么样的

HR 面

1. 自我介绍
2. 项目中遇到的最大难点
3. 项目中的收获
4. 可以实习的时间，实习时长
5. 哪里人
6. 说一下自己的性格
7. 你的优缺点是什么
8. 有什么兴趣爱好，画的怎么样 / 球打的如何 / 游戏打的怎么样
9. 看过最好的一本书是什么
10. 学习技术中有什么难点

11. 怎么看待加班
12. 觉得深圳怎么样（或者其他地点）
13. 遇见过最大的挫折是什么，怎么解决的
14. 职业规划
15. 目前的 offer 情况
16. 你最大的优势和劣势是什么
17. 介绍在项目里面充当的角色
18. 介绍一下本科获得的全国赛奖项的情况
19. 最有成就感的事情 / 最骄傲的一件事情
20. 在实验室中担任什么角色，参加的 XXX 能聊聊吗
21. 用两个词来形容自己

项目

1. 轻量级加密服务器
2. TCP 拥塞控制
3. 轻量级数据存储（Redis）

反问