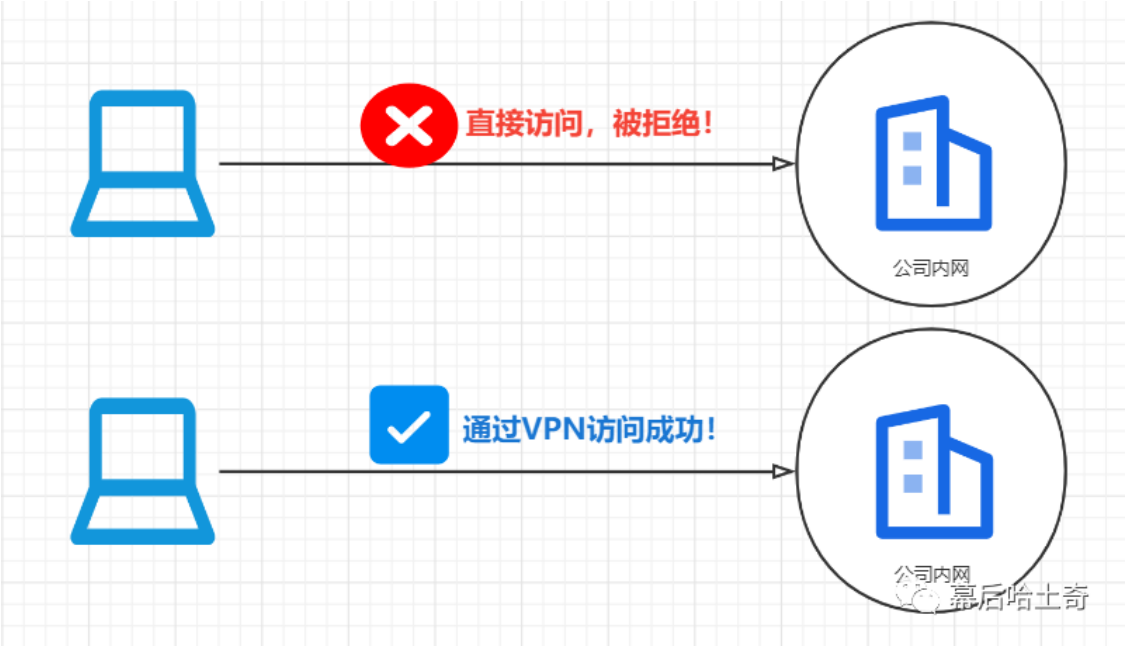
本篇继续学习跟网络层息息相关的技术，第一个来讨论常用的VPN技术，然后引入下NAT技术，初步了解下为什么要使用NAT技术。

一、虚拟局域网VPN概述

VPN：（Virtual Private Network），学名叫做虚拟专用网络。

VPN我们经常使用到，尤其是疫情肆虐的三年，需要在家办公，就需要通过VPN连入公司内网访问一些资源。

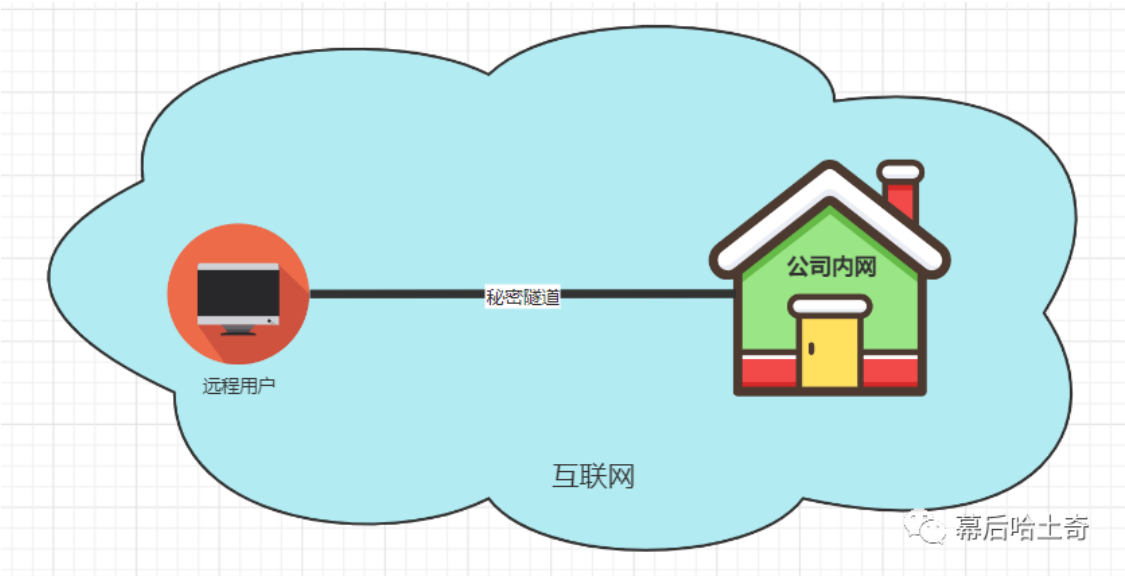


何为公司内网？即在公司内部建立一个局域网，这个网络是封闭的，正常的互联网用户甚至是黑客都无法轻易进入该网络中，一定程度上保证了公司内部数据的安全性。

我们把互联网比喻为一个广阔的天地，那么公司内网就是带围墙的房子，只有在这个房子里面的人才有权使用。

那么处于因特网中的你，不在这个房子里，又想使用里面的资源，又不能泄漏里面的资源，该如何做呢?

此时最简单的方法就是需要在你和公司内网之间建立一条”秘密隧道“。



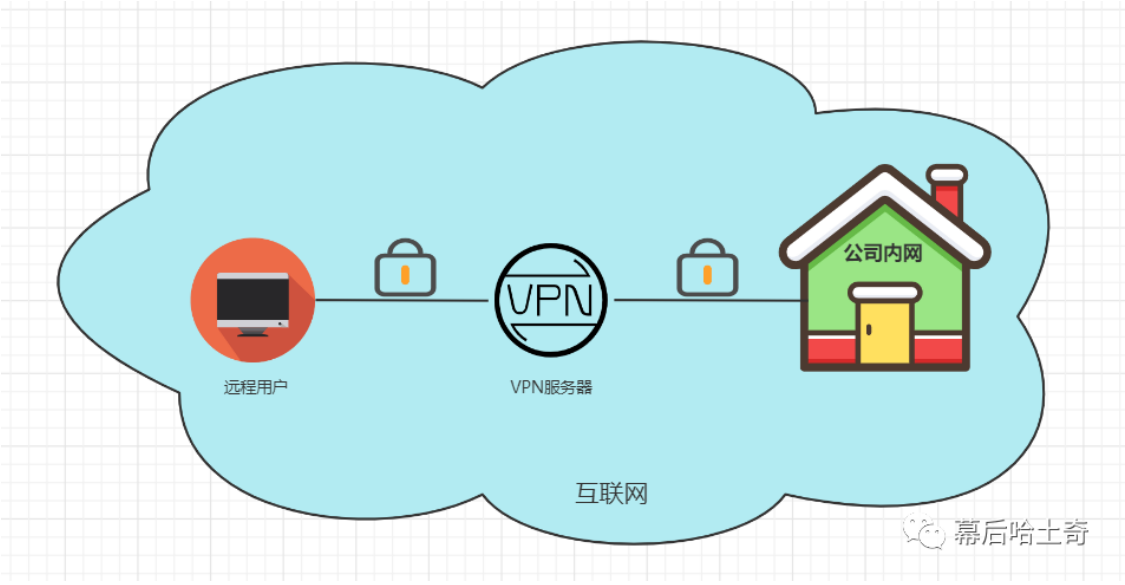
二、虚拟局域网VPN基本原理

当你通过VPN访问公司内网时，数据传递全部通过“秘密隧道”悄悄进行，这样就保证了你和公司之间的网络通讯是安全私密的。

但是这条隧道并不是真实存在的，而是通过数据加密技术封装出来的一条虚拟数据通信隧道，实际上它借用的还是互联网上的公共链路。

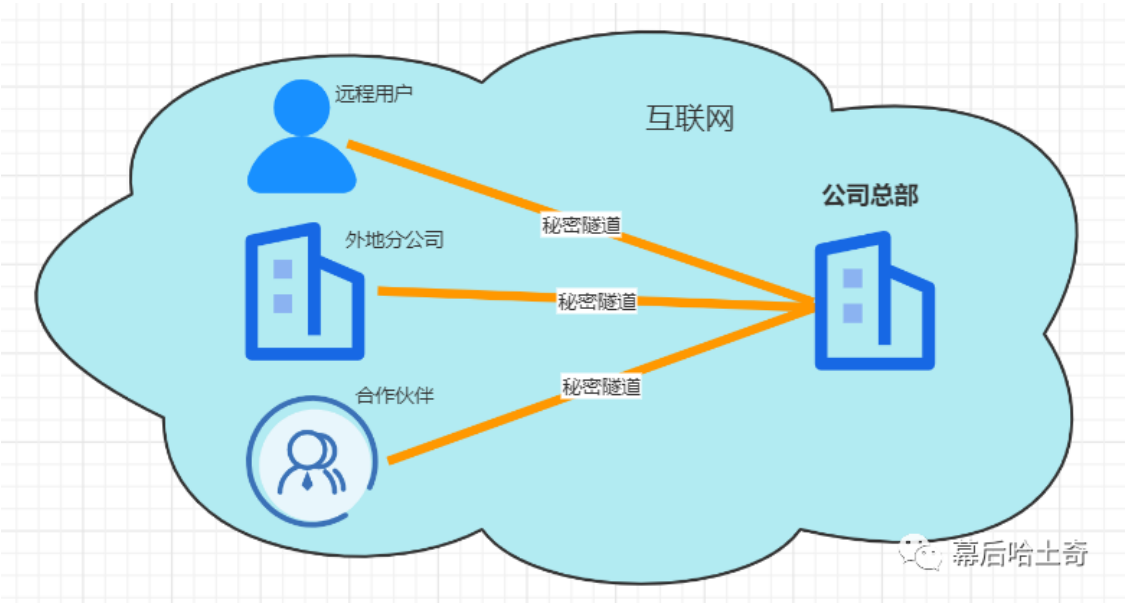
VPN会对你和公司之间传递的数据进行加密处理，加密后的数据会在一条专用的数据链路上进行安全传输，如同架设了一个专用网络一样。所以VPN称为虚拟专用网络。

- 运行员工本地PC上的VPN软件，你访问公司内网的办公网站时，不再直接访问公司内网的服务器，而是去访问VPN服务器，并给VPN服务器发一条指令“我要访问办公网站”。
- VPN服务器接到指令后，代替你去访问办公网站，收到公司办公网站的内容后，进行加密再通过“秘密隧道”将内容回传给你，这样你就通过VPN成功访问到你需要的内网资源啦。



针对不同的需求，VPN还能提供更有针对性的应用场景，比如：

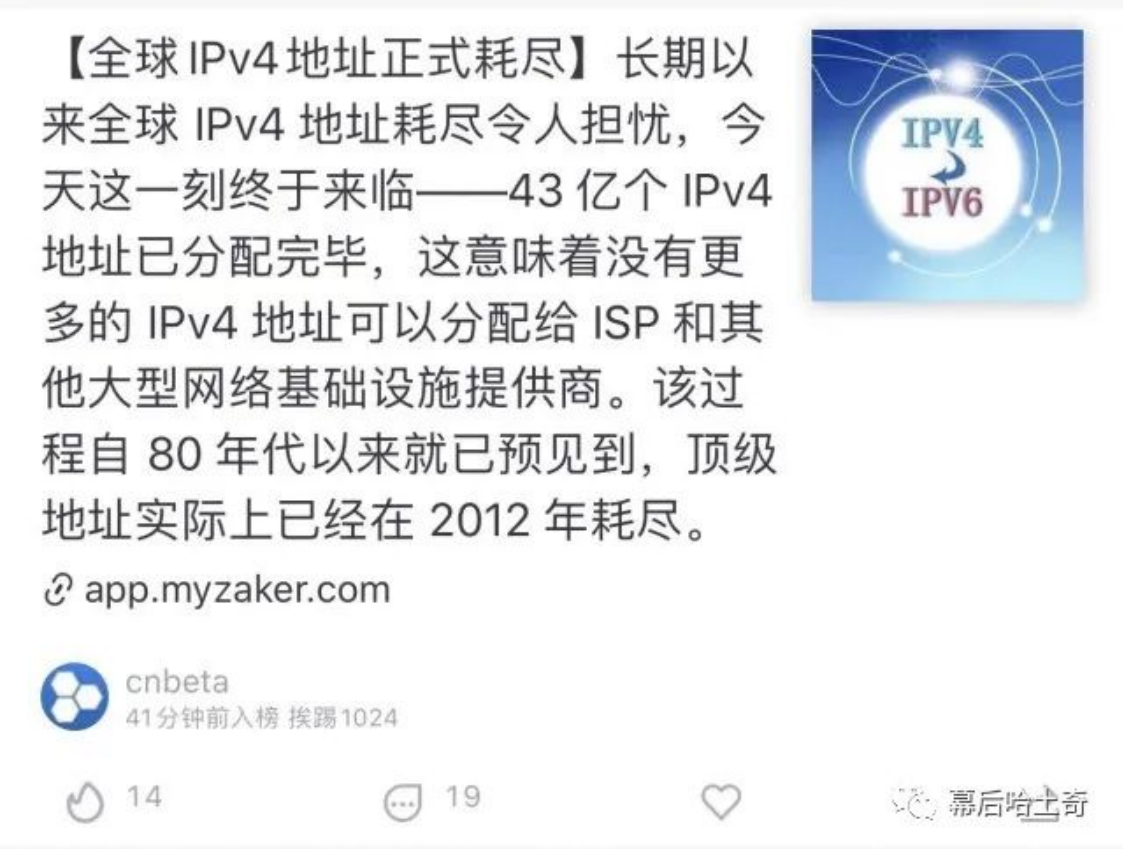
- **远程接入VPN**：用于异地办公的员工访问公司内网。
- **内联网VPN**：将企业总部和外地分公司通过虚拟专用网络连接在一起。
- **外联网VPN**：将一个公司与另一个公司的资源进行连接，与合作伙伴企业网构成外联网。



其实，除了VPN这个手段，还可以租用电信公司的专线来达到此目的，不过这种方式租金很高，没有VPN应用灵活；在安全性上，VPN通过加密技术提高了数据安全性，降低了数据在传输过程中被窃取的风险，因此，综合来看，**VPN是一种经济实用、安全有效的接入方式**。

三、IPv4地址枯竭问题

我们知道，IPV4 是32位，那么就有 2 的 32 次方个可能的取值，等于4294967296，约 43 亿。因此，全球可以有约 43 亿个 IP 地址。43亿按照互联网的发展速度仍然是不够用的，让我们看下来自2019年11月26日的地址耗尽的噩耗：



那我们是不是以后装宽带是不是也要摇号了呀?

当你意识到这个问题的时候，我们的先驱们早在90年代就发现这个问题并推动解决了，那就是IPV6发展计划。随着十多年的发展，IPv6已经被很多通信网络和终端设备厂商支持，取得了长足的进步。如今我们使用的系统比如Win7、Win8、Win10等，都已经完全支持IPv6。

IPV6，是128位，有多大呢？这个数量，即使是给地球上每一颗沙子都分配一个IP，也是妥妥够用的，写法形如：

```
2001:0db8:85a3:08d3:1319:8a2e:0370:7344
```

此外，IPV6相比较于IPV4还有其他很多很多的优点，这里暂不展开说明了。

但是！它问世已经20年了，还是没有完全替代IPv4呢？此外，既然已经耗光，为什么大家仍然还在用IPv4，对老百姓来说，并没有因为地址不够而无法上网呢？

这就是NAT在发挥作用了！NAT 是 Network Address Translation 的缩写，表示“网络地址转换”。NAT很有用，它的诞生再次缓解了IPv4地址空间即将耗尽的问题。

NAT能使大量使用内部私有地址的专用网络用户共享少量外部全球IP地址来访问因特网上的主机和资源。

关于私有地址，我们之前有学习过，这是一类特殊的地址，无需申请：

- 私有地址只能用于一个机构的内部通信，而不能用于和因特网上的主机通信
- 私有地址只能用于本地地址，而不能作为全球地址
- 在因特网中的所有路由器，对目的地址是私有地址的IP数据报一律不进行转发

四、没有NAT时发生的一个尴尬场景

现在我们要上网，假设家中的私有网络（局域网）是 192.168.0.0/24，假设你的电脑的IP地址为192.168.0.1。如果没有NAT技术，当你想连接互联网上的网站，例如 https://github.com （IP地址为13.250.177.223）时，将会发生这种情况：

DST 地址（接收方 MAC）	SRC 地址（发送方 MAC）	第 3 层使用的协议	...	源 IP 地址 192.168.0.1	目标 IP 地址 www.github.com 是 13.250.177.223	CRC

去的方向，根据目标IP是13.250.177.223，一个一个经过路由器的接力，最终到达目的地。一切顺利！但是回执呢？

github也封装了一个报文打算发给我们，但是突然发现我们的ip地址是一个192.168打头的地址，我们上面说过，这个是私有地址，不在公网上使用，那么就回不去了！

上面的问题总结下来就是，ipv4不够用，我们打算用私有地址来解决这个尴尬，但是发现一个问题就是我们的私有地址如何跟公有地址交互？解决方案当然就是我们的NAT了，千呼万唤始出来，犹抱琵琶半遮面，不行，我要你放开琵琶。

下篇文章我们来好好揭秘NAT技术细节！