# 基本概念

内网穿透是指在一个局域网（通常是内网）中，某台设备通过特定技术手段，使得外部网络（例如互联网）能够访问内网中的服务或设备。因为内网通常是通过路由器、网关进行NAT（网络地址转换），内网设备在外部看不到直接的IP地址，所以在没有内网穿透的情况下，外部网络无法直接访问内网的服务。

# 内网穿透的需求

内网设备通常是无法被外部直接访问的，因为：

路由器通过\*\*NAT（网络地址转换）\*\*将内网IP与外网IP进行转换，外网无法知道内网设备的具体IP。

许多企业或家庭的局域网通过防火墙或路由器进行保护，禁止外部直接访问内网资源。

但有时候，我们希望从外部网络访问内网服务，例如：

家里的网络摄像头或智能设备需要远程控制。

本地开发的Web服务需要在外网进行调试。

使用云服务搭建的系统，需要与本地设备或网络进行交互等。

在这些场景下，我们需要通过内网穿透技术来实现外网与内网的通信。

# 实现原理

## （1）端口映射（Port Forwarding）

在路由器中进行端口映射，将外网的某个端口指向内网中指定的设备和端口。这样，外部用户访问路由器公网IP的特定端口时，路由器会将流量转发到内网设备。

**优点**：简单直接。

**缺点**：需要对路由器进行配置，并且内网设备的IP地址必须是固定的。

## （2）反向代理（Reverse Proxy）

反向代理服务器是指外部请求会先发送到一台代理服务器，代理服务器将请求转发到内网的相应服务上。外网访问的是代理服务器，而不是直接访问内网设备。

**常用工具**：NGINX、Apache、Caddy等。

## （3）VPN（虚拟私人网络）

通过在内网设备和外网设备之间搭建一个虚拟的专用网络，所有通信都通过这个虚拟网络进行。这种方式可以让外网设备像在内网中一样访问内网资源。

**优点**：安全性较高，适用于企业级应用。

**缺点**：配置复杂，需要更多的计算和网络资源。

## （4）第三方内网穿透服务

这是目前非常流行的一种解决方案，使用一些第三方内网穿透工具来实现。用户不需要配置路由器或VPN，只需要在内网设备上安装客户端，通过这些工具提供的服务将内网的服务暴露到外网。

**常见工具**：

**Ngrok**：可以快速将本地开发的服务暴露到外网，支持HTTP、HTTPS和TCP协议。

**FRP**：一个高性能的反向代理应用，广泛用于内网穿透，可以通过简单的配置将内网服务暴露到外网。

**ZeroTier**：通过创建虚拟网络，将内网设备与外网设备连接起来。

**花生壳**：一款常用的内网穿透工具，适合个人和小型企业使用。

## （5）STUN/TURN协议（用于P2P穿透）

这种方式是通过STUN（Session Traversal Utilities for NAT）和TURN（Traversal Using Relays around NAT）协议帮助设备穿越NAT，让两台设备建立P2P连接。STUN服务器帮助设备知道其公网IP地址，而TURN服务器则作为中介转发数据。

**优点**：能直接建立P2P连接，不需要额外的服务器支持。

**缺点**：需要STUN/TURN服务器的支持，可能受到NAT类型的影响。

# 应用场景

## 远程访问

如在公司内网中有一个Web服务，想要通过外网进行远程访问和管理。

## 游戏主机/设备

例如在家中搭建的游戏服务器，想要朋友通过外网访问。

## 远程桌面

如果有台计算机需要从外网远程控制，可以通过内网穿透技术实现远程桌面连接。

## IoT设备管理

例如家里的智能设备或摄像头，想要从外部控制。

# 安全性问题

暴露内网服务：通过内网穿透，外部设备能够访问内网的服务，如果没有足够的安全措施，可能被恶意攻击者利用。

身份验证：建议在穿透的服务上启用强身份验证和加密通信。

使用加密通道：如通过HTTPS、VPN等方式保护数据传输的安全。

# frp官网

https://github.com/fatedier/frp

# 使用教程

https://www.baimeidashu.com/15654.html

https://blog.csdn.net/bacawa/article/details/134027987