Webrtc

# 1:、ICE



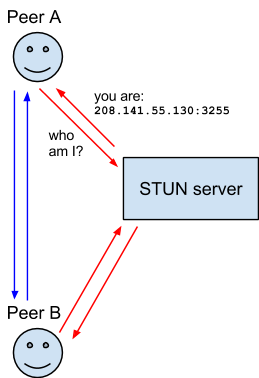
## ICE

交互式连接建立[Interactive Connectivity Establishment (ICE)](http://en.wikipedia.org/wiki/Interactive_Connectivity_Establishment) 是一个允许你的浏览器和对端浏览器建立连接的协议框架。在实际的网络当中，有很多原因能导致简单的从A端到B端直连不能如愿完成。这需要绕过阻止建立连接的防火墙，给你的设备分配一个唯一可见的地址（通常情况下我们的大部分设备没有一个公网地址），如果路由器不允许主机直连，还得通过一台服务器转发数据。ICE通过使用以下几种技术完成上述工作。

## STUN

NAT的会话穿越功能[Session Traversal Utilities for NAT (STUN)](http://en.wikipedia.org/wiki/STUN) (缩略语的最后一个字母是NAT的首字母)是一个允许位于NAT后的客户端找出自己的公网地址，判断出路由器阻止直连的限制方法的协议。

客户端通过给公网的STUN服务器发送请求获得自己的公网地址信息，以及是否能够被（穿过路由器）访问。



## NAT

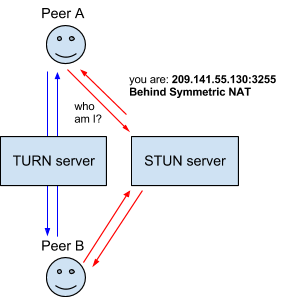
网络地址转换协议[Network Address Translation (NAT)](http://en.wikipedia.org/wiki/NAT) 用来给你的（私网）设备映射一个公网的IP地址的协议。一般情况下，路由器的WAN口有一个公网IP，所有连接这个路由器LAN口的设备会分配一个私有网段的IP地址（例如192.168.1.3）。私网设备的IP被映射成路由器的公网IP和唯一的端口，通过这种方式不需要为每一个私网设备分配不同的公网IP，但是依然能被外网设备发现。

一些路由器严格地限定了部分私网设备的对外连接。这种情况下，即使STUN服务器识别了该私网设备的公网IP和端口的映射，依然无法和这个私网设备建立连接。这种情况下就需要转向TURN协议。

## TURN

一些路由器使用一种“对称型NAT”的NAT模型。这意味着路由器只接受和对端先前建立的连接（就是下一次请求建立新的连接映射）。

NAT的中继穿越方式[Traversal Using Relays around NAT (TURN)](http://en.wikipedia.org/wiki/TURN) 通过TURN服务器中继所有数据的方式来绕过“对称型NAT”。你需要在TURN服务器上创建一个连接，然后告诉所有对端设备发包到服务器上，TURN服务器再把包转发给你。很显然这种方式是开销很大的，所以只有在没得选择的情况下采用。



## SDP

会话描述协议[Session Description Protocol (SDP)](http://en.wikipedia.org/wiki/Session_Description_Protocol) 是一个描述多媒体连接内容的协议，例如分辨率，格式，编码，加密算法等。所以在数据传输时两端都能够理解彼此的数据。本质上，这些描述内容的元数据并不是媒体流本身。

# 2、getUserMedia

# 3、RTCpeerconnection