

基于互联网的几种视频会议的通讯方式

1. NAT 类型定义

1. Full Cone NAT（完全锥形）：所有来自同一个内部 Tuple X 的请求均被 NAT 转换至同一个外部 Tuple Y，而不管这些请求是不是属于同一个应用或者是多个应用的。除此之外，当 X-Y 的转换关系建立之后，任意外部主机均可随时将 Y 中的地址和端口作为目标地址 和目标端口，向内部主机发送 UDP 报文，由于对外部请求的来源无任何限制，因此这种方式虽然足够简单，但却不那么安全

2. Restricted Cone NAT：它是 Full Cone 的受限版本：所有来自同一个内部 Tuple X 的请求均被 NAT 转换至同一个外部 Tuple Y，这与 Full Cone 相同，但不同的是，只有当内部主机曾经发送过报文给外部主机（假设其 IP 地址为 Z）后，外部主机才能以 Y 中的信息作为目标地址和目标端口，向内部 主机发送 UDP 请求报文，这意味着，NAT 设备只向内转发（目标地址/端口转换）那些来自于当前已知的外部主机的 UDP 报文，从而保障了外部请求来源的安全性

3. Port Restricted Cone NAT：它是 Restricted Cone NAT 的进一步受限版。只有当内部主机曾经发送过报文给外部主机（假设其 IP 地址为 Z 且端口为 P）之后，外部主机才能以 Y 中的信息作为目标地址和目标端 口，向内部主机发送 UDP 报文，同时，其请求报文的源端口必须为 P，这一要求进一步强化了对外部报文请求来源的限制，从而较 Restrictd Cone 更具安全性

4. Symmetric NAT：只有来自于同一个内部 Tuple 、且针对同一目标 Tuple 的请求才被 NAT 转换至同一个外部 Tuple，否则的话，NAT 将为之分配一个新的外部 Tuple；打个比方，当内部主机以相同的内部 Tuple 对 2 个不同的目标 Tuple 发送 UDP 报文时，此时 NAT 将会为内部主机分配两个不同的外部 Tuple，并且建立起两个不同的内、外部 Tuple 转换关系。与此同时，只有接收到了内部主机所发送的数据包的外部主机才能向内部主机返回 UDP 报文，这里对外部返回报文来源的限制是与 Port Restricted Cone 一致的。不难看出，如果说 Full Cone 是要求最宽松 NAT UDP 转换方式，那么，Symmetric NAT 则是要求最严格的 NAT 方式，其不仅体现在转换关系的建立上，而且还体现在对外部报文来源的限制方面。

举个例子说明：

A 机器在私网（192.168.0.4）

NAT 服务器（210.21.12.140）

B 机器在公网（210.15.27.166）

C 机器在公网（210.15.27.140）

现在，A 机器连接过 B 机器，假设是 A（192.168.0.4:5000）-> NAT（转换后 210.21.12.140:8000）-> B（210.15.27.166:2000）。

同时 A 从来没有和 C 通信过。

则对于不同类型的 NAT，有下列不同的结果：

Full Cone NAT：C 发数据到 210.21.12.140:8000，NAT 会将数据包送到 A（192.168.0.4:5000）。因为 NAT 上已经有了 192.168.0.4:5000 到 210.21.12.140:8000 的映射。

Restricted Cone：C 无法和 A 通信，因为 A 从来没有和 C 通信过，NAT 将拒绝 C 试图与 A 连接的动作。但 B 可以通过 210.21.12.140:8000 与 A 的 192.168.0.4:5000 通信，且这里 B 可以使用任何端口与 A 通信。如：210.15.27.166:2001 -> 210.21.12.140:8000，NAT 会送到 A 的 5000 端口上。

Port Restricted Cone：C 无法与 A 通信，因为 A 从来没有和 C 通信过。而 B 也只能用它的 210.15.27.166:2000 与 A 的 192.168.0.4:5000 通信，因为 A 也从来没有和 B 的其他端口通信过。该类型 NAT 是端口受限的。

Symmetric NAT：同上，

A 机器连接过 B 机器，假使是 A（192.168.0.4:5000）-> NAT（转换后 210.21.12.140:80

2.NAT 类型检测

STUN 协议定义了一些消息格式，大体上分成 Request/Response，client 向 server 发送 request，server 发送 response 给 client。Server 在收到 client 的 UDP 包以后，Server 将接收到该包的地址和端口利用 udp 传回来给 client，client 把这些地址和端口与本机的 ip 地址和端口进行比较，如果不同，说明在 NAT 后面，否则就位于 NAT 前面。为了检测不同类型的 NAT，STUN 协议定义了一些消息属性，要求 Server 有不同的动作，比如发送响应的时候使用不同的 IP 地址和端口，或者改变端口等等。STUN 协议对 NAT 有效，但是对防火墙就无能为力了，因为防火墙可能不会打开 UDP 端口。

使用 STUN 协议来检测，需要部署一个 STUN 服务器，此服务器绑定两个公网 IP(IP-1,IP-2)，并根据客户端的要求进行应答。

STUN 信息结构

STUN 由以下数据结构构成：STUN 头+STUN 有效载荷

STUN 头结构如下： 存储的值都是以网络顺序存放

字段 类型

STUN message type Short int 消息类型

Length Short int 有效载荷长度,不包含头长度

transaction ID octet[16] 连接的 ID 值, 检查 Request,和 Response

STUN 的有效载荷

SHUN 的有效载荷是一些 STUN 的属性构成, 属性的类型由信息的类型来决定。

STUN 的属性是定义好了的, 属性列表 (attribute) 如下:

MAPPED-ADDRESS 必选 用在 Binding Response, (添入 MAPING IP 和 PORT)

RESPONSEADDRESS 可选 用在 Binding Request,指定 Response,发送到哪里

如果没有指定, Response 发送到 MAPING IP 和 PORT

CHANGE-REQUEST 可选 用在 Binding Request。用来决定, CLIENT 的 NAT 类型是制 NAT, 还是端口限制 NAT, (命令服务器从不同的源端口/IP, Response 请求)

CHANGED-ADDRESS 可选 用在 Binding Responses 告诉 Client 改变的端口和 IP

SOURCE-ADDRESS 必选 只用在 Binding Responses, 标记信息的源 PORT HE IP

USERNAME 可选 Shared Secret Response/ Binding Requests

PASSWORD, 必选 SharedSecret Response

ESSAGEINTEGRITY 可选 用在 Binding Responses, Binding Request 记录信息的完整性

ERROR-CODE Binding Error Response and Shared Secret Error Response.

UNKNOWN-ATTRIBUTES

REFLECTED-FROM Binding Responses.用于追溯和防止 DDOS

```

[+] Frame 69900: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
[+] Ethernet II, Src: 04:54:16:51:68:13 (04:54:16:51:68:13), Dst: BeijingT_06:3a:f9 (00:13:32:06:3a:f9)
[+] Internet Protocol Version 4, Src: 172.16.1.75 (172.16.1.75), Dst: 74.125.127.126 (74.125.127.126)
[+] User Datagram Protocol, Src Port: 50315 (50315), Dst Port: 19302 (19302)
[+] Simple Traversal of UDP Through NAT
    [Response In: 70107]
        Message Type: Binding Request (0x0001)
        Message Length: 0x0000
        Message Transaction ID: 00000001000000020000000300000004
0000  00 13 32 06 3a f9 04 54 16 51 68 13 08 00 45 00  ..2...T .Qh...E.
0010  00 30 63 47 00 00 80 11 00 00 ac 10 01 4b 4a 7d  .0cG....KJ}
0020  7f 7e c4 8b 4b 66 00 1c 77 84 00 01 00 00 00 00  .~..Kf.. w.....
0030  00 01 00 00 00 02 00 00 00 03 00 00 00 00 04  .....
[+] 发布到LOFTER

```

消息类型是0x0001；消息长度为：0x0000；事务ID为：1234

服务器响应

```

[+] Frame 70107: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
[+] Ethernet II, Src: BeijingT_06:3a:f9 (00:13:32:06:3a:f9), Dst: 04:54:16:51:68:13 (04:54:16:51:68:13)
[+] Internet Protocol Version 4, Src: 74.125.127.126 (74.125.127.126), Dst: 172.16.1.75 (172.16.1.75)
[+] User Datagram Protocol, Src Port: 19302 (19302), Dst Port: 50315 (50315)
[+] Simple Traversal of UDP Through NAT
    [Request In: 69900]
        [Time: 0.467405000 seconds]
        Message Type: Binding Response (0x0101)
        Message Length: 0x0018
        Message Transaction ID: 00000001000000020000000300000004
    [+] Attributes
        [+] Attribute: MAPPED-ADDRESS
            Attribute Type: MAPPED-ADDRESS (0x0001)
            Attribute Length: 8
            Protocol Family: IPv4 (0x0001)
            Port: 34230
            IP: 58.215.221.82 (58.215.221.82)
        [+] Attribute: SOURCE-ADDRESS
            Attribute Type: SOURCE-ADDRESS (0x0004)
            Attribute Length: 8
            Protocol Family: IPv4 (0x0001)
            Port: 19302
            IP: 74.125.127.126 (74.125.127.126)
0000  04 54 16 51 68 13 00 13 32 06 3a f9 08 00 45 00  .T.Qh... 2.:...E.
0010  00 48 cc b8 00 00 27 11 4f 96 4a 7d 7f 7e ac 10  .H.... O.J}~..
0020  01 4b 4b 66 c4 8b 00 34 c3 c0 01 01 00 18 00 00  .KKf...4 ..
0030  00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 01  .....
0040  00 08 00 01 85 b6 3a d7 dd 52 00 04 00 08 00 01  .....
[+] 发布到LOFTER

```

响应类型是：0x0101；消息长度：0x0018；事务ID：1234，就是之前发送出去的事务ID。

NAT 检测过程:

1, STUN 客户端(101:10)向 STUN 服务器(404:40)发送请求,要求得到自身经 NAT 映射后的地址(202:20):

a,收不到服务器回复,则认为 UDP 被防火墙阻断,不能通信,网络类型:Blocked.

b,收到服务器回复,对比本地地址,如果相同(直接返回的就是源地址 101:10),则认为无 NAT 设备(没经过 NAT 映射转换),进入第 2 步,否则认为有 NAT 设备,进入 3 步.

2,(已确认无 NAT 设备)STUN 客户端向 STUN 服务器发送请求,要求服务器从其他 IP 和 PORT(505:50)向客户端回复包:

a,收不到服务器从其他 IP 地址的回复,认为包被前置防火墙阻断,网络类型:Symmetric UDPFirewall.(如果没有 NAT 的话是无论如何都能收到回复的,只有一点受到防火墙的阻断,有时候杀毒软件也阻断)

b,收到则认为客户端处在一个开放的网络上,网络类型:Opened.

3,(已确认存在 NAT 设备)STUN 客户端(101:10)向 STUN 服务器(404:40)发送请求,要求服务器从其他 IP 和 PORT(505:50)向客户端回复包:

a,收不到服务器从其他 IP 地址(包括 IP 和 Port)的回复,认为包被前置 NAT 设备阻断,进入第 4 步.(如果不是前置的就相当于全开 Opened 或 Full ConeNat 类型,无论那个 IP 和端口都能接收到回复)

b,收到则认为 NAT 设备类型为 Full Cone,即网络类型:Full Cone NAT.(此没有什么限制的基本和没有 NAT 一样 Opened)

4, STUN 客户端(101:10)向 STUN 服务器(404:40)的另外一个 IP 地址(505:40,端口不能改变)发送请求,要求得到自身经 NAT 映射后的地址(202:20,如果不是对称的应该返回这个映射地址),并对比之(与第一步中返回的映射地址比对)

a,地址不相同,则网络类型:Symmetric NAT.(如果是对称类型,则 101:10 在向一个不同的 IP 地址(505,端口不变)发送请求时会映射一个新的端口,此处相当于生成一个 202:21,比对不相同)

b,相同则认为是 Restricted NAT(受限的),进入第 5 步,进一步确认类型.

5, (已确认 RestrictedNAT 设备)STUN 客户端(101:10)向 STUN 服务器(404:40)发送请求,要求服务器从相同 IP(404)的其他 PORT(41)向客户端回复包:

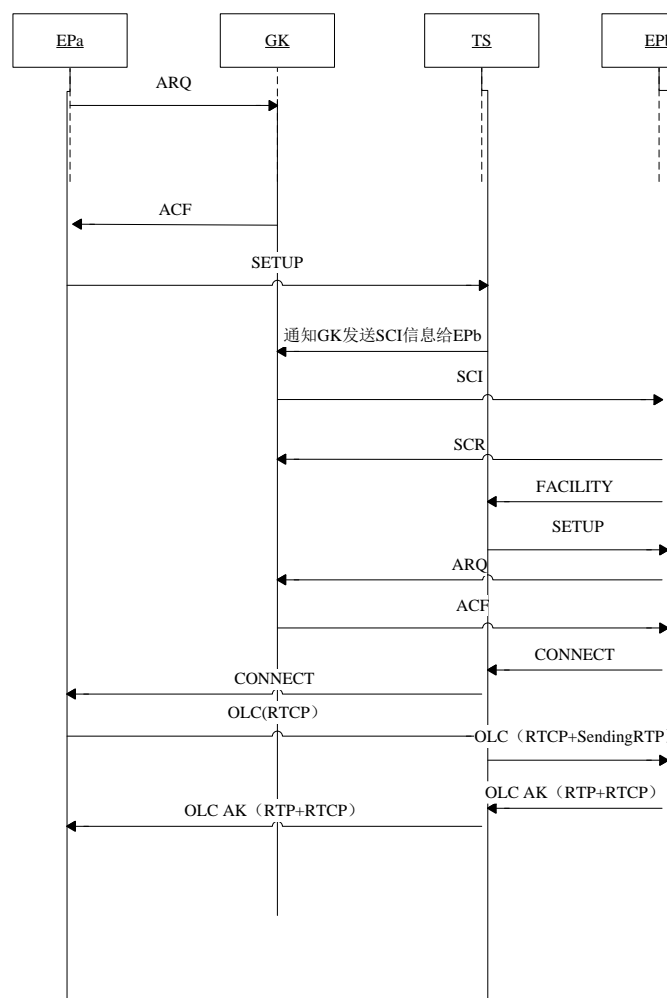
a,收不到服务器从其他 PORT 地址的回复,认为包被前置 NAT 设备阻断,网络类型:Port Restricted coneNAT.(端口改变了,端口受限相当于我一个人 A(101)向 B(404)要右手(40 端口)的苹果,而 B 左手(41 端口)有个香蕉,A 只要 B 的右手苹果,而 B 给了 A 一个左手的香蕉, A 肯定是不要的,相当于收不到回复)

b,收到则认为网络类型: Restricted cone NAT.(IP 受限,对端口没什么要求,只要是 404 这个 IP 就行,无论用那个端口都行)

3.H323/H460 通信方式

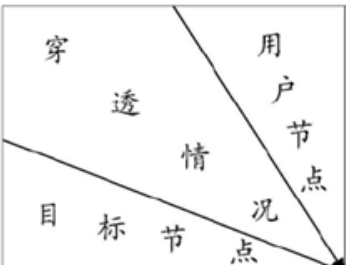
在 H.323 通信协议标准中,有专门的一个系列的标准规定了通信协议在跨 NAT 环境下的使用: H.460.x 系列, 包括: RAS 相关的 H.460.17, 呼叫信令相关的 H.460.18 , 媒体相关的 H.460.19, H.460.20 等。

其中 H.460.17 (2005 年 09 月)规定了使用 H.225.0 连接来传送 H.323 RAS 消息的规范, H.460.18 (2013 年 03 月)规定了 H.323 信号在跨网、跨防火墙环境下传输的规范, H.460.19 (Traversal of ITU-T H.323 media across network address translators and firewalls, 2013 年 03 月)规定了音视频 RTP 码流的通道 (LC) 的简单协商, 使视频会议终端可以在跨越 NAT 的环境下, 通过一个处于公网 (或者是类似各终端都可以访问到的网络) 的网守来中转协议、媒体数据, 使整个会议通路可以建立起来。



4. H323 P2P 通信方式

下表中标示为可穿透 P2P 类型的 NAT 组合。

	Full NAT	Cone NAT	Restricted Cone NAT	Port Restricted Cone NAT	Symmetric NAT
Full Cone NAT	可穿透	可穿透	可穿透	可穿透	不可穿透
Restricted Cone NAT	可穿透	可穿透	可穿透	可穿透	不可穿透
Port Restricted Cone NAT	可穿透	可穿透	可穿透	可穿透	不可穿透
Symmetric NAT	不可穿透	不可穿透	不可穿透	不可穿透	不可穿透

合并部署 GK、STUN Server 服务器。

终端注册 GK 服务器成功以后，开始 NAT 类型检测。得到自己的 NAT 类型后上报给 GK，GK 维持所有在线终端的 NAT 类型表。

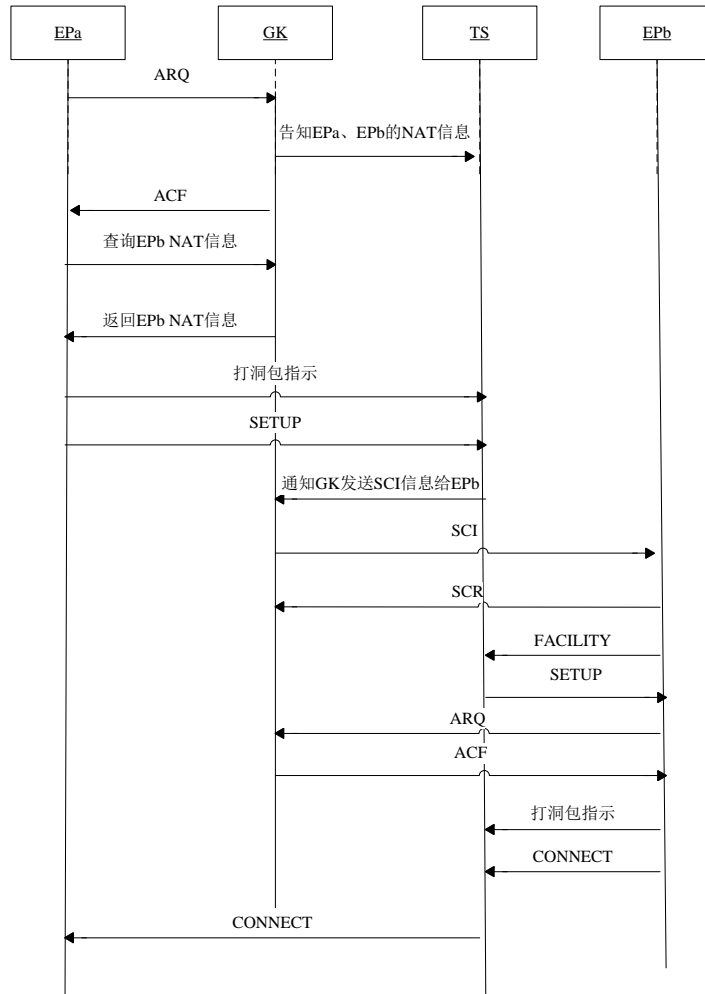
当终端向 GK 发起呼叫请求，如果双方在同一 NAT 后，GK 将目标地址重定向为被叫终端的内网地址，如果双方不在同一 NAT 后，GK 获取空闲的信令/码流服务器，将目标地址重定向为信令/码流服务器地址，终端向 GK 获取被叫 NAT 类型，如果双方在同一 NAT 后，终端向被叫发起标准 H323 IP 呼叫，双方不在同一 NAT 后，终端向被叫发起修改过的 H323/H460 呼叫。

与标准 H460 不同之处在于：主叫在发送 setup 之前，预先要收集音频、视频、双流、数据通道的 RTP/RTCP 收发地址，用这些地址分别向分配的信令/码流服务器的 UDP：2776/2777 端口（信令/码流服务器用 UDP：2776 接收/转发 RTP 流，UDP：2777 接收/转发 RTCP 流）发送自定义 stun 信令--打洞包指示。被叫在收到 ACF 以后也要收集音频、视频、双流、数据通道的 RTP/RTCP 收发地址分别向信令/码流服务器的 2776/2777 端口发送自定义 stun 信令--打洞包指示。信令/码流服务器建立起双方的 NAT 映射表。

呼叫建立后，双方互相打开媒体通道。信令/码流服务器在转发 OLC/OLC ACK 两条信令的时候，判断双方如果可以穿透 NAT，把 OLC/OLC ACK 中的终端本地 RTP/RTCP 地址转换成各自的 NAT 映射地址；双方如果不能穿透 NAT，则将 OLC/OLC ACK 中的终端本地 RTP/RTCP 地址将转换成信令/码流服务器的地址，双方通过信令/码流服务器来转发码流。

如果双方通过 P2P 方式发送码流，其中接收方是 Port Restricted Cone NAT, GK 通过 STUN 非标信令让其向发送方对应发送端口发送打洞包。

最终通道发送方保持以固定频率用本方的 RTCP 端口向对端的 RTCP 端口的 NAT 地址发送打洞包，通道接收方以固定频率用本方的 RTCP 端口向对端的 RTCP 端口的 NAT 地址发送打洞包、以固定频率用本方的 RTP 接收端口向对方的 RTP 发送端口的 NAT 地址发送打洞包，以此来维持双方 NAT 之间的通道。



5: SIP ICE 穿越