

AliceStreet Conference Center

A **real** conference room on your desktop

Firewalls, NAT's e VPN's

Versão 1.5.1

AliceStreet
Conference Center



USA Canada UK South Africa Australia Brazil Thailand
www.alicestreet.com

AliceStreet Conference Center

A real conference room on your desktop

1. Descrição geral da conectividade	
1. Descrição geral da conectividade	3
1.1 Como o cliente se conecta ao servidor	3
1.2 Como o protocolo trabalha	3
1.2.1 H.323	3
1.2.2 T 120	3
1.2.3 Complicações possíveis	4
2. Firewalls	4
2.1 Passagem de porta	4
2.2 Firewalls conscientes H.323	5
2.3 Estabeleça um VPN	5
3. Tradução do endereço da rede	5
3.1 Por que NATs podem causar problemas	5
3.2 Cliente atrás de NAT	6
3.3 Servidor atrás de NAT	6
4. VPN's	7

1. Descrição geral da conectividade

1.1 Como o cliente se conecta ao servidor

O processo de conexão geralmente trabalha da seguinte maneira :

- Quando você se conecta ao servidor usando a Internet Explorer, o servidor diz ao cliente qual o endereço do IP para se conectar.
- O cliente então se conecta àquele endereço do IP usando o protocolo H.323. H.323 é usado para comunicação de voz e de vídeo, e informação sobre a direção da tela dentro da sala.
- Uma vez que uma conexão H.323 é estabelecida, o cliente separadamente se conecta ao endereço do IP do servidor usando o protocolo T.120. T.120 é usado para comunicação de slides, nomes dos usuários, e outros dados que compartilham capacidade.

Infelizmente, enquanto os protocolos H.323 e T.120 são extremamente úteis e resistentes, eles são comparativamente complicados. O fato que você pode se conectar ao servidor usando um web browser(HTTP) não necessariamente significa que o cliente seja capaz de se conectar usando H.323 e T.120.

1.2 Como o protocolo trabalha

1.2.1 H.323

Partes do protocolo H.323 de conexão trabalha da seguinte maneira :

1. o cliente estabelece a conexão TCP ao servidor numa porta designada(1)
2. o cliente estabelece uma conexão TCP mais distante ao servidor numa porta diferente
3. o cliente e o servidor então dizem um ao outro quais portas UDP eles receberão o tráfego em tempo real (voz e vídeo).
4. Cada um então começa a transmitir os pacotes para aquelas portas UDP, contendo voz e vídeo RTP e tráfego RCTP.

A faixa das portas usadas pelos pontos 2 e 3 anteriormente citadas podem ser configuradas no servidor (veja o guia do administrador). Você precisa reservar aproximadamente 6 portas por usuário concorrente nesta faixa.

1.2.2 T 120

O protocolo T.120 (se usado) estabelece a conexão TCP ao servidor na porta 1503. O T.120 é usado somente para whiteboard e aplicação que compartilha funcionalidade.

- (1) Este padrão para 1730 do Centro de Conferência do AliceStreet, mas um padrão diferente de porta pode ser configurado no servidor. Veja o guia do administrador.

1.2.3 Complicações possíveis

Firewalls

Os firewall podem ser uma complicação porque o firewall(s) entre o cliente e o servidor poderá bloquear internamente (e em alguns casos externamente) o tráfego de algumas ou todas as portas.

Especialmente, firewalls que não entendem H.323, muitas vezes não permitirão pacotes UDP internos de alcançar seu destino e assim tanto o clientes como o servidor poderão pensar que eles estão conectados mas na realidade não serão capazes de trocar nenhum tráfego de voz e de vídeo.

NAT (Tradução do Endereço da Rede)

Embora NATs sejam bem conhecidos por causarem problemas para muitas instalações de Voice over IP, a tecnologia do AliceStreet Conference Center deverá atravessar totalmente qualquer NAT que possa ser encontrado entre o cliente e o servidor.

VPN(Rede Privada Virtual)

Geralmente, executando o Centro de Conferência do AliceStreet sobre um VPN não deveria apresentar nenhum problema. Entretanto, nós observamos alguns problemas devidos à maneira que os VPNs são implementados.

Especialmente:

- Alguns clientes VPN não lidam bem com pacotes UDP
- Alguns servidores VPN não podem lidar com o volume dos pacotes que são geralmente por voz em tempo real ou por uma aplicação de vídeo

2. Firewalls

O firewall poderá bloquear o tráfego de algumas ou de todas as portas que são usadas pelo sistema. Há várias maneiras de superar estes problemas.

2.1 Passagem de porta

Você pode evitar as questões do firewall pela passagem de portas pertinentes em seus firewalls em base permanente.

Passagem de porta externa para clientes PCs

Clientes PCs deveriam ser capazes de abrir portas externas pelo TCP :

- A porta do ouvinte (1730 por padrão mas configurável para qualquer outro valor)
- A faixa de porta especificada no servidor (se a faixa de porta não for especificada no servidor então todas as portas devem ser abertas externamente)
- 1503 (se T.120 for usado)
- 1719 (se a segurança do gatekeeper H.323 for usada , e configurada no seu gatekeeper)

Clientes PCs deveriam ser capazes de abrir portas externas pelo UDP:

- A faixa de porta especificada no servidor (se a faixa de porta não for especificada no servidor, então todas as portas devem ser abertas externamente).

Passagem de porta interna para servidores

Servidores PCs deveriam ter as portas internas abertas tanto pelo TCP como pelo UDP:

- A porta do ouvinte H.323 (1730 por padrão, mas configurável em qualquer outro valor)
- A faixa de porta especificada no servidor (se a faixa de porta não for especificada no servidor, então todas as portas devem ser abertas)
- 1503 (se T.120 for usado)
- 1719 (se você tiver implementado um gatekeeper no seu servidor).

2.2 Firewalls conscientes H.323

Algumas marcas de firewall são explicitamente conscientes do tráfego de H.323. Como resultado, quando o cliente indicar que receberá pacotes UDP em certas portas, o firewall então permitirá que os pacotes UDP do servidor passem por aquelas portas (e vice-versa) .

Note que alguns firewalls conscientes poderão apresentar incompatibilidade com o Centro de Conferência AliceStreet especialmente, se eles não foem compatíveis com –FastStart”. Por esta razão, a porta do ouvinte de default H.323 é configurada para 1730 em vez da usual porta de 1720 de H.323.

2.3 Estabeleça um VPN

Você pode usar um VPN para colocar tanto o cliente como o servidor na mesma rede virtual, assim desviando-se do firewall.

3. Tradução do endereço da rede

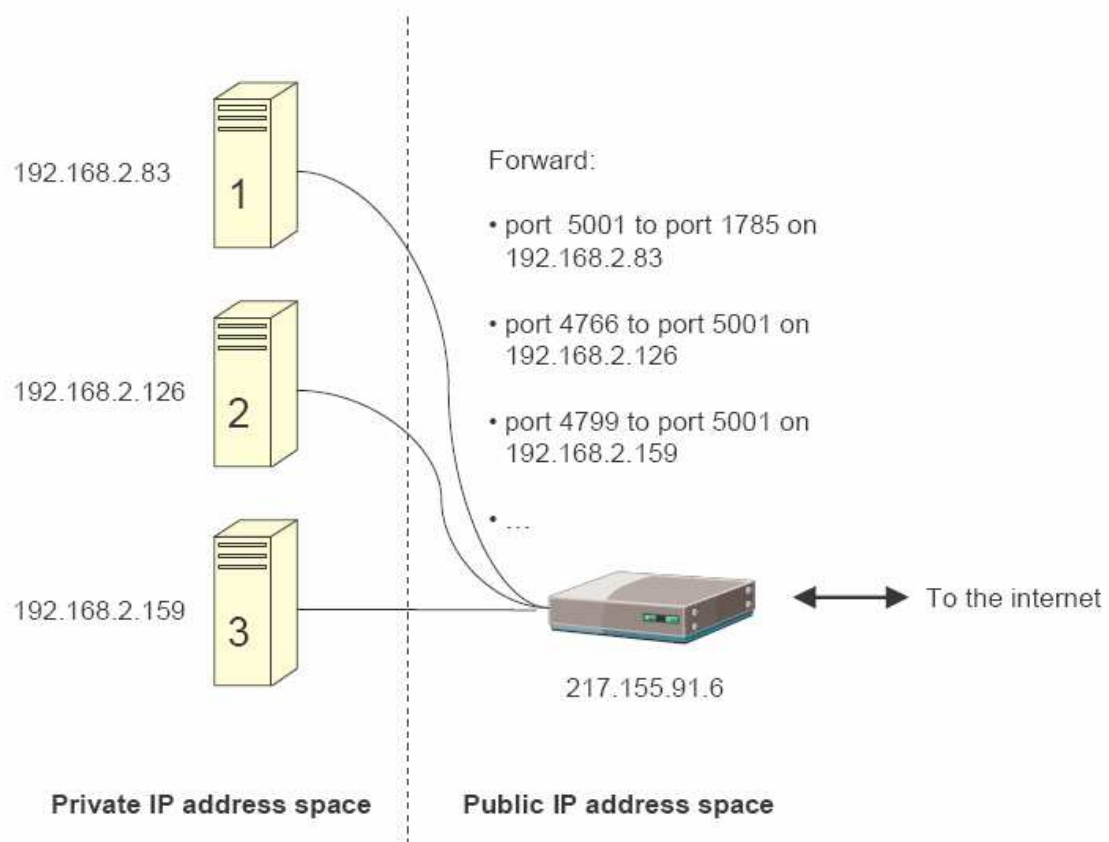
3.1 Por que NATs podem causar problemas

NATs dificultam todos os sistemas de base H.323 porque o endereço IP que o mundo externo percebe pelo PC atrás de NAT não é o mesmo endereço de IP que o próprio PC percebe.

Por exemplo, na figura abaixo, todos 3 computadores aparecem para a Internet como endereço IP 217.155.91.6, mas as próprias máquinas pensam que seus endereços IP são 192.168.xxx Padrão H.323 sinalizando que dirão a outra extremidade para enviar pacotes para 192.168.xxx mas se a outra extremidade estiver na Internet lateral ao NAT, esses endereços serão inalcançáveis.

AliceStreet Conference Center

A real conference room on your desktop



Além disso, neste exemplo, ambas máquinas 2 e 3 abrem a porta 5001 para tráfego interno UDP. Entretanto, o NAT está encaminhando os pacotes recebidos na porta 5001 para a máquina 1.

3.2 Cliente atrás de NAT

A tecnologia do AliceStreet supera os problemas acima e isto significa que o cliente atrás de NAT não deveria encontrar nenhum problema para se conectar ao servidor. Se você encontrar inesperadamente problemas para se conectar, será com maior probabilidade uma questão do firewall.

3.3 Servidor atrás de NAT

Nos casos onde o servidor do AliceStreet está atrás de um NAT, você precisará configurar tanto o servidor como o NAT apropriadamente.

Para fazer isso, no servidor :

- vá para [http://\[server\]/admin](http://[server]/admin) e logon apropriadamente
- habilite – NAT roteador” e especifique o endereço público do IP do dispositivo NAT
- Configure uma faixa de porta fixa

No NAT:

- reserve as faixas de portas fixas configuradas no servidor tanto como
 - 1730 (ou outra porta de ouvinte H.323 como configurada no servidor)
 - 1503 (se T.120 for usado)
 - 1719 (se um gatekeeper H.323 for usado)
- Configure o NAT para que ele encaminhe estas portas não traduzidas para o servidor. Consulte sua documentação do dispositivo do NAT para informações de como configurar este encaminhamento da porta.

4. VPN's

Em geral, usando um VPN (Rede Privada Virtual) é um excelente caminho para se conectar ao servidor do centro de conferência, assim como garantir segurança para a reunião.

Entretanto, há algumas coisas para se tomar cuidado devido às questões específicas relativas às implementações de VPN de diferentes vendedores.

Especialmente :

- Ao usar o Microsoft VPN cliente com L2TP/IPSec, nós descobrimos que 30%-50% de todos os pacotes RTP recebidos pelo cliente estão perdidos. Isto faz com que o uso da voz e do vídeo fique impossível.

Solução : Instale um cliente VPN diferente.

Mais geralmente :

- O uso de voz e de vídeo sobre IP tipicamente envolve o uso de um grande número de pacotes comparativamente pequenos, e o Centro de Conferência do AliceStreet não é uma exceção. Um grande número de pacotes percorrendo o VPN poderá causar problemas para alguns softwares de servidor VPNs quais poderão precisar do poder do processamento para enfrentar este número de pacotes.

Solução : use um servidor VPN mais potente.

- O uso de algumas tecnologias VPN que são baseadas em SSL(- SSL VPN") não é recomendado. Essas tecnologias VPN são fundamentalmente baseadas no TCP e isto significa que o perfil do desempenho pedido pelo UDP não é alcançado. Como resultado, você pode esperar ouvir uma interferência significativa na qualidade de seu áudio e ver um atraso significativo no seu vídeo.

Solução : execute o Centro de Conferência do AliceStreet diretamente sobre a Internet em vez de sobre o VPN.