Sistemas Multimídia

Aula 7: SIP em Redes Hostis
Protocolo, Operação e Desafios Práticos

Professora Ana Luiza Scharf

IFSC - SJ
Departamento de Telecomunicações

Semestre 2026.1

Sumário Detalhado

1. Contexto Histórico e Problema
2. Limitações dos Protocolos Atuais
3. Cliente-Servidor vs. Peer-to-Peer
4. SIP: Conceitos Fundamentais
5. Registro, Presença e Localização

Sumário Detalhado (continuação)

6. Métodos SIP e Códigos de Resposta
7. Negociação de Mídia: Oferta/Resposta
8. Desafios Práticos: NAT e Firewalls
9. Cenários e Exemplos Práticos
10. WebRTC: A Evolução Natural

Objetivos da Aula

Fechamento da Aula Anterior

- Revisão dos conceitos fundamentais
- Lacunas abertas nas aulas anteriores
- Integração teórico-prática

Foco Principal

- Como o SIP se adapta a redes "hostis"
- Desafios de NAT, firewalls e IPv4
- Transição do modelo ideal para o real

A Evolução das Redes IP

Mundo Ideal (Anos 70-80)

- IPv4 com 2^{32} endereços
- "Número absurdamente alto"
- Comunicação end-to-end direta
- Sem preocupações de segurança

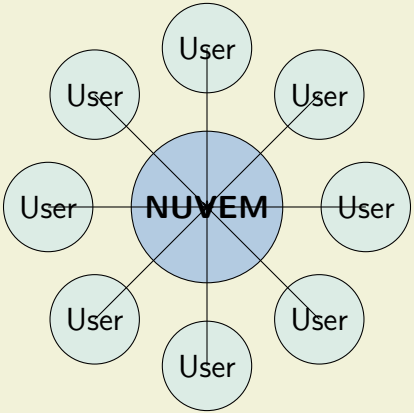
Mundo Real (Atual)

- Escassez de IPv4
- NAT em todos os lugares
- Firewalls por padrão
- Modelo cliente-servidor dominante

Mudança Fundamental

"Redes foram projetadas para segurança nem para desempenho"

Problema Central: Concentração de Serviços



Ponto único de concentração

Problema Central: Concentração de Serviços

Observação

- Tendência: centralização em poucos serviços
- Protocolos não foram projetados para isso
- HTTP se tornou padrão de mercado

IPv4: A Grande Ilusão

Projeto Original

- 1972: RFC 791
- 32 bits = 4.3 bilhões
- "Nunca acabaria"
- Endereço único por dispositivo

Realidade

- Esgotamento em 2011
- NAT em massa
- Tradução de endereços
- Perda de conectividade

Cálculo Simplificado

Dispositivos : Endereços IPv4 $\approx$ 3:1

IPv6: A Solução Ignorada

Potencial

$$2^{128} \approx 3.4 \times 10^{38} \text{ endereços}$$

- Cada grão de areia poderia ter endereço
- Fim do NAT (em teoria)

Problemas Práticos

- Adoção lenta (25% globalmente)
- Operadoras reutilizam endereços
- Custo de transição
- Compatibilidade retroativa

NAT: A Solução que Virou Problema

Vantagens

- Economia de IPv4
- "Segurança por obscuridade"
- Simplificação de redes

Desvantagens

- Quebra comunicação P2P
- Complexidade adicional
- Problemas de desempenho
- Dificulta inovações

Consequência para SIP

- Agente "some"atrás do NAT
- Necessidade de keep-alive
- Tabelas de mapeamento dinâmicas

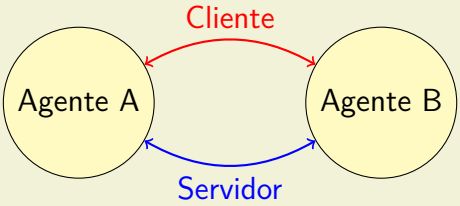
Modelo Cliente-Servidor (HTTP)

Relação Assimétrica

Características HTTP

- Papéis fixos e pré-definidos
- Cliente sempre inicia
- Servidor sempre responde
- Stateless (em teoria)

Modelo SIP: Agentes Multifuncionais



Relação Simétrica e Dinâmica

Flexibilidade SIP

- Mesmo dispositivo pode ser cliente OU servidor
- Comunicação bidirecional
- Iniciativa de qualquer lado
- Adaptável a diferentes cenários

Por que HTTP Dominou?

Vantagens Práticas

- Simplicidade de implementação
- Cache eficiente
- Escalabilidade vertical
- Segurança concentrada
- Compatível com NAT/firewalls

Consequências

- Centralização
- Dependência de servidores
- Dificuldade para P2P
- Privacidade comprometida

O que é SIP?

Definição Formal

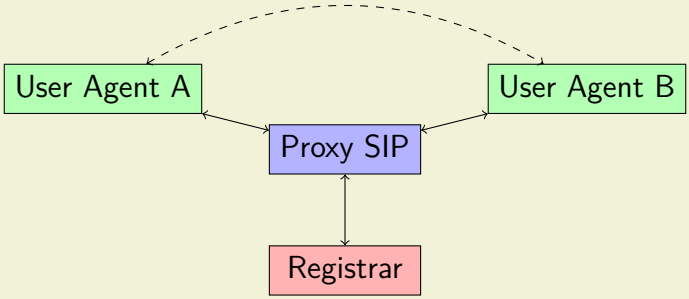
SIP (Session Initiation Protocol) é um protocolo de sinalização da camada de aplicação para criar, modificar e terminar sessões multimídia.

- RFC 3261 (padrão principal)
- Trabalha com SDP para descrição de mídia
- Usa RTP/RTCP para transporte de mídia

Analogia Telefônica

- SIP = Discagem e chamada (sinalização)
- SDP = Negociação do tipo de chamada
- RTP = Conversa em si (áudio/vídeo)

Arquitetura SIP: Componentes



+ Servidores Redirect e Location

Agentes SIP: Papéis Dinâmicos

UAC (User Agent Client)

- Inicia requisições SIP
- Envia INVITE, REGISTER
- Recebe respostas
- Pode se tornar UAS

UAS (User Agent Server)

- Recebe requisições SIP
- Processa e responde
- Envia 200 OK, 180 Ringing
- Pode se tornar UAC

Importante!

Um mesmo dispositivo alterna entre UAC e UAS durante uma sessão

Registro: "Estou Aqui!"

Propósito do REGISTER

Informar ao servidor SIP onde um usuário está localizado na rede.

Informações Enviadas

- Endereço SIP (sip:user@domain)
- Endereço IP atual
- Porta UDP/TCP
- Tempo de expiração

Resposta do Servidor

- 200 OK (sucesso)
- 401 Unauthorized (autenticação)
- 403 Forbidden (acesso negado)

Exemplo de Mensagem REGISTER

Requisição REGISTER

```
REGISTER sip:registrar.ifsc.edu.br SIP/2.0
Via: SIP/2.0/UDP 192.168.1.100:5060
Max-Forwards: 70
From: <sip:aluno1@ifsc.edu.br>;tag=12345
To: <sip:aluno1@ifsc.edu.br>
Call-ID: abc123@192.168.1.100
CSeq: 1 REGISTER
Contact: <sip:aluno1@192.168.1.100:5060>
Expires: 3600
Content-Length: 0
```

Resposta 200 OK

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.100:5060
From: <sip:aluno1@ifsc.edu.br>;tag=12345
To: <sip:aluno1@ifsc.edu.br>;tag=67890
Call-ID: abc123@192.168.1.100
CSeq: 1 REGISTER
Contact: <sip:aluno1@192.168.1.100:5060>
Expires: 3600
Content-Length: 0
```

Keep-Alive e NAT Traversal

Problema do NAT

- Tabelas NAT têm timeout (30-300s)
- Conexão inativa é removida
- Respostas não chegam ao cliente

Keep-Alive e NAT Traversal

Solução: REGISTER Periódico

- Reenvio do REGISTER antes do timeout
- Tipicamente a cada 20-60 segundos
- Mantém mapeamento ativo
- Atualiza servidor sobre presença

Custo vs. Benefício

"Regularmente fica mandando REGISTER para manter tabela NAT atualizada"

Presença: Mais que Online/Offline

Estados de Presença

- Disponível - Pronto para receber
- Ocupado - Online mas não disponível
- Ausente - Não responderá
- Em reunião - Contexto específico
- Não perturbe - Silencioso

Informações Adicionais

- Status personalizado
- Localização geográfica
- Dispositivo utilizado
- Horário de disponibilidade

Comunicação Unificada

Integração de voz, vídeo, chat, email em um único status

Principais Métodos SIP

Método	Descrição
REGISTER	Registrar localização do usuário
INVITE	Iniciar sessão multimídia
ACK	Confirmar estabelecimento de sessão
BYE	Terminar sessão
CANCEL	Cancelar requisição pendente
OPTIONS	Consultar capacidades do servidor
MESSAGE	Enviar mensagem instantânea
SUBSCRIBE	Inscrever-se para notificações
NOTIFY	Notificar sobre eventos

Códigos de Resposta SIP: Faixas

1xx Provisórias

- 100 Trying
- 180 Ringing
- 183 Session Progress

2xx Sucesso

- 200 OK
- 202 Accepted

3xx Redirecionamento

- 301 Moved
- 302 Moved Temporarily

4xx Erro Cliente

- 401 Unauthorized
- 404 Not Found
- 486 Busy Here

5xx Erro Servidor

- 500 Server Error
- 503 Service Unavailable

6xx Falha Global

- 600 Busy Everywhere
- 603 Decline

Exemplo: Fluxo INVITE Simples

SDP: Session Description Protocol

Propósito

Descrever parâmetros da sessão multimídia no corpo das mensagens SIP.

Informações Incluídas

- Tipo de mídia (áudio, vídeo)
- Codecs suportados
- Endereços IP e portas
- Atributos específicos

Negociação

- Oferta no INVITE
- Resposta no 200 OK
- ACK confirma
- Modificação com re-INVITE

Exemplo SDP Simplificado

Oferta de Mídia no INVITE

```
v=0
o=alice 2890844526 2890844526 IN IP4 192.168.1.100
s=Conversa SIP
c=IN IP4 192.168.1.100
t=0 0
m=audio 49170 RTP/AVP 0 8
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
m=video 51372 RTP/AVP 31 34
a=rtpmap:31 H261/90000
a=rtpmap:34 H263/90000
```

Exemplo SDP Simplificado

Interpretação

- Oferece áudio (PCMU, PCMA)
- Oferece vídeo (H.261, H.263)
- Portas específicas para cada mídia

O Problema do NAT para SIP

NAT Comportamentos

- Full Cone: Qualquer externo
- Restricted Cone: Só quem recebeu
- Port Restricted: Restrição porta
- Symmetric: Mapeamento único

Efeitos no SIP

- Endereço IP muda
- Respostas não chegam
- SDP contém IP errado
- Timeouts inesperados

Cenário Típico

Cliente: IP privado 192.168.1.100
NAT: Mapeia para 200.100.50.25:54321
SIP envia 192.168.1.100 no SDP $\rightarrow$ Falha!

Firewalls: Regras de Bloqueio

Comportamento Típico

- Bloqueia tudo, permite exceções
- Filtragem estado (stateful)
- Timeouts curtos para UDP
- Inspeção de conteúdo

Impacto no SIP

- Porta 5060 (SIP) pode ser bloqueada
- Portas RTP dinâmicas são problema
- Keep-alive necessário
- TCP vs. UDP diferenças

Soluções: STUN, TURN, ICE

STUN

- Descobre IP público
- Testa conectividade
- Simples e leve
- Não funciona com NAT simétrico

TURN

- Relay de mídia
- Funciona sempre
- Custo de banda
- Ponto único de falha

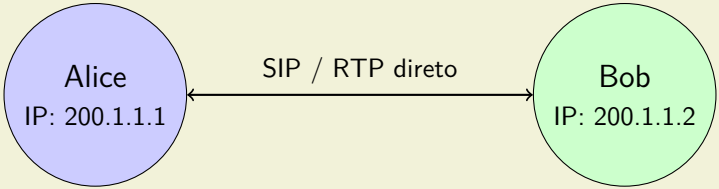
ICE

- Framework completo
- Combina STUN+TURN
- Testa vários candidatos
- Escolhe melhor caminho

WebRTC usa ICE

"ICE testa: host → STUN → TURN, escolhe o que funciona"

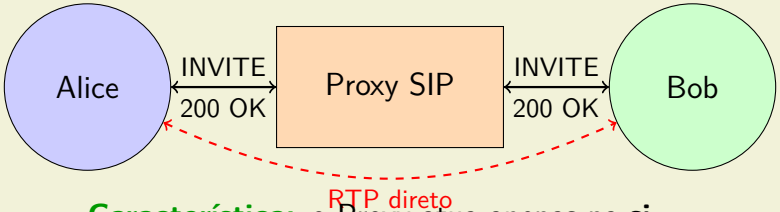
Cenário 1: Comunicação Direta (Ideal)



Vantagens: simples, rápido, baixa latência

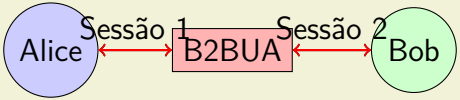
Limitação: requer IPs públicos, sem NAT/firewall

Cenário 2: Comunicação com Proxy SIP



Característica: o Proxy atua apenas na **sinalização SIP**; a mídia flui diretamente entre os usuários.

Cenário 3: Com B2BUA (Back-to-Back User Agent)



Mídia passa pelo B2BUA

Aplicações do B2BUA

- Gravação de chamadas
- Transcrição em tempo real
- Análise de tráfego
- Conversão de codecs

WebRTC: SIP Simplificado para Web

Similaridades com SIP

- Sinalização (customizável)
- SDP para negociação
- RTP/RTCP para mídia
- ICE para NAT traversal

Diferenças Principais

- API JavaScript padrão
- Sem servidor SIP obrigatório
- Foco em P2P direto
- Integração com navegadores

Comparação: SIP vs WebRTC

Aspecto	SIP	WebRTC
Complexidade	Alta (muitas RFCs)	Média (API simplificada)
NAT Traversal	STUN/TURN/ICE externos	ICE embutido no navegador
Implementação	Servidores específicos	Navegadores modernos
Uso Típico	Telefonia empresarial	Aplicações web P2P

Resumo dos Principais Pontos

1. **SIP é flexível** mas complexo para redes hostis
2. **NAT e firewalls** são desafios principais
3. **Registro periódico** mantém conectividade
4. **Oferta/Resposta** (SDP) negocia mídia
5. **STUN/TURN/ICE** resolvem NAT traversal
6. **WebRTC** é a evolução para web

Recomendações Práticas

Para Implementações

- Use bibliotecas maduras (PJSIP, Sofia-SIP)
- Implemente keep-alive robusto
- Suporte a STUN/TURN obrigatório
- Teste com diferentes tipos de NAT

Para Aprendizado

- Experimente softphones (MicroSIP, Linphone)
- Configure servidor simples (Asterisk, FreeSWITCH)
- Use Wireshark para analisar tráfego SIP
- Pratique com WebRTC simples primeiro

Próxima Aula: WebRTC na Prática

O que veremos

- Arquitetura WebRTC completa
- API JavaScript passo a passo
- Exemplo: Videoconferência P2P
- Integração com servidores de sinalização
- Desafios de escalabilidade

Preparação

Instalar: Navegador moderno, Node.js, editor de código

Obrigada pela atenção!

Perguntas e Discussão