Sistemas Multimídia

Aula 6: Protocolo SIP – Arquitetura e NAT Traversal

Professora Ana Luiza Scharf

IFSC - São José
Departamento de Telecomunicações

Semestre 2026.1

Agenda da Aula

1. Revisão Arquitetura SIP
2. Cabeçalhos SIP Fundamentais
3. Modelos de Comunicação
4. Desafios do NAT
5. Soluções Práticas
6. Segurança
7. Conclusão

Contexto e Motivação

Problema Real

Sistemas embarcados (sensores, câmeras IP) precisam de:

- Comunicação em tempo real
- Conexão através de NAT
- Segurança adequada
- Baixo consumo de recursos

Situação Comum

"Sistemas tão pequenos que não permitem manutenção frequente... precisam ser protegidos mesmo com recursos limitados."

Revisão: Arquitetura SIP - RFC 3261

Componentes SIP

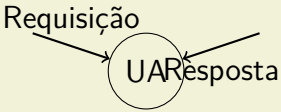
- User Agent (UA)
- Proxy Server
- Registrar Server
- Redirect Server

Mensagens SIP

- Requests: INVITE, ACK, BYE
- Responses: 1xx, 2xx, 3xx
- Transações e Diálogos

Característica Importante: SIP não depende das camadas inferiores - usa cabeçalhos próprios para roteamento.

Agentes SIP: Comportamento Dual



User Agent
Cliente & Servidor

- **UAC**: Inicia requisições
- **UAS**: Responde requisições
- Mesmo agente pode ser ambos
- Diferente do HTTP

Cabeçalho Via: Circuitos Lógicos

Funcionamento

1. Requisição passa pelo Proxy 1
2. Proxy 1 adiciona: `Via: proxy1`
3. Requisição passa pelo Proxy 2
4. Proxy 2 adiciona: `Via: proxy2`
5. Resposta volta pelo caminho inverso

Importante

"Empilhando cabeçalhos Via para criar circuitos onde mensagens de requisição e resposta passem pelos mesmos equipamentos."

Cabeçalhos SIP Fundamentais

Call-ID

- Identificador único do diálogo
- Ex: `Call-ID: 12345@host`

CSeq

- Número de sequência
- Ex: `CSeq: 1 INVITE`

From/To

- Identificam participantes
- Ex: `sip:alice@domain.com`

Contact

- Endereço para contato direto
- Crítico para NAT
- Ex: `Contact: alice@192.168.1.10`

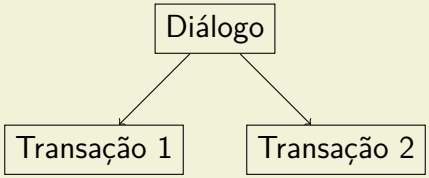
Exemplo de Mensagem SIP

Mensagem REGISTER

REGISTER sip:proxy.ifsc.edu.br SIP/2.0
Via: SIP/2.0/UDP 192.168.0.10:5060
From: <sip:alice@ifsc.edu.br>
To: <sip:alice@ifsc.edu.br>
Call-ID: 12345@192.168.0.10
CSeq: 1 REGISTER
Contact: <sip:alice@200.100.50.1:5060>
Expires: 3600
Content-Length: 0

- Problema: Contact tem IP privado (192.168.0.10)
- Solução: Contact deve ter IP público após NAT

Diálogos e Transações SIP



- **Diálogo**: Sessão completa (ex: uma chamada telefônica)
- **Transação**: Par requisição-resposta (ex: INVITE + 200 OK)
- Várias transações podem compor um diálogo

Comparação: SIP vs HTTP

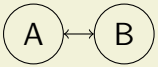
Característica	SIP	HTTP
Modelo	Peer-to-Peer	Cliente-Servidor
Conexões	Bidirecionais	Unidirecionais
NAT	Complexo	Simples
Portas	5060/5061	80/443
Estado	Com estado	Sem estado

Diferencial

"No HTTP o cliente sempre inicia. No SIP, qualquer agente pode iniciar comunicação."

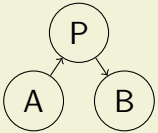
Modelos de Comunicação SIP

Ponto-a-Ponto



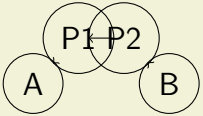
- Inviável com NAT
- Sem intermediários

Triângulo



- Comum na prática
- Registro obrigatório

Trapézio



- Múltiplos proxies
- Entre domínios

O Problema do NAT

O que é NAT?

- Network Address Translation
- Traduz IPs privados para públicos
- Necessário por escassez de IPv4
- Cria tabelas de mapeamento temporárias

Exemplo Prático

"Guilherme (192.168.0.10) quer falar com Eduarda (192.168.1.20). Ambos atrás de NATs. Como conectar?"

Funcionamento do NAT

Tabela NAT

IP Interno:Porta	IP Externo:Porta
192.168.0.10:5060	200.100.50.1:5060
192.168.0.11:5060	200.100.50.1:5061
192.168.0.12:80	200.100.50.1:8080

Por que NAT é Problema para SIP?

1. **Bidirecionalidade**: SIP precisa que ambos lados iniciem comunicação
2. **Endereços nos cabeçalhos**: Contact header contém IP:porta
3. **Tempo limitado**: Entradas NAT expiram (30s-5min)
4. **Tipos diferentes**: NAT Full Cone, Restricted, Port Restricted

Citação

"O SIP diferente do HTTP precisa manter aberta a via de comunicação."

Exemplo: Comunicação com NAT

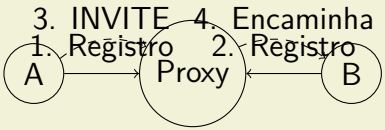
Cenário:

- Cliente A: Casa, NAT
- Cliente B: Casa, NAT
- Proxy SIP: Campus IFSC
- Objetivo: Ligação SIP

Passos:

1. A e B registram no Proxy
2. Proxy conhece IPs públicos
3. A chama B via Proxy
4. Proxy encaminha para B
5. Mídia estabelecida

Exemplo: Comunicação com NAT



Registro Periódico - Solução para NAT

Como Funciona?

- Cliente manda REGISTER a cada 60s
- Mantém entrada NAT ativa
- Atualiza Contact header
- Proxy sempre sabe onde alcançar cliente

Registros

- T0: Cliente registra (NAT criado)
- T60: Cliente re-registra (NAT mantido)
- T120: Cliente re-registra (NAT mantido)
- Se parar: NAT expira após timeout

Protocolos Auxiliares para NAT

STUN

- Session Traversal Utilities for NAT
- Descobre IP público
- Testa tipo de NAT
- Simples mas limitado

TURN

- Traversal Using Relays
- Relé central
- Último recurso
- Latência maior

ICE

- Interactive Connectivity
- Combina STUN+TURN
- Encontra melhor caminho
- Usado em WebRTC

Na Prática

- Muitos sistemas: Só registro periódico
- Sistemas críticos: + STUN
- Último caso: TURN

Segurança em Sistemas SIP

Problemas Comuns

- Sistemas embarcados vulneráveis
- Ataques por escalada
- Interceptação de chamadas
- Negação de serviço (DoS)

Caso Real

"Telefones IP com ramais especiais para ligações internacionais. Preocupação com acesso não autorizado."

Boas Práticas de Segurança

Autenticação

- Senhas fortes
- TLS para SIP
- SRTP para mídia
- Certificados digitais

Hardening

- Firewalls configurados
- Atualizações regulares
- Logs e monitoramento
- Segmentação de rede

IoT

"Câmeras IP, sensores... se não protegidos, viram porta de entrada para ataques."

Casos de Uso - Quando Proteger?

Análise de Risco

- **Sensor de temperatura**: Baixo risco
- **Câmera segurança**: Alto risco
- **Controle de acesso**: Altíssimo risco
- **Telefonia executiva**: Alto risco

Exemplo da Aula

"Se a informação não é sensível, como temperatura, talvez não precise. Mas controle de acesso precisa proteção máxima."

Ferramentas para Testes

Análise

- Wireshark
- tcpdump
- sipp (teste carga)
- sngrep (visualização)

Implementação

- Asterisk
- FreeSWITCH
- pjsip
- Kamailio

Prática na Próxima Aula

Configuração básica e análise de tráfego com Wireshark.

Desafios da Parte de Mídia

Aviso Importante

"Tudo isso que falamos hoje é só 10% do problema. Os outros 90% são a parte de mídia."

- RTP/RTCP: Protocolos de mídia
- Codecs: Compressão áudio/vídeo
- QoS: Qualidade de Serviço
- Sincronização
- NAT traversal para RTP

Perguntas Frequentes

P: Por que não usar HTTP?

R: HTTP é cliente-servidor. SIP é peer-to-peer. Qualquer agente pode iniciar.

P: IPv6 resolve NAT?

R: Sim, mas transição lenta. NAT continuará por anos.

P: Qual modelo no projeto?

R: Cenário triângulo com proxy. Mais viável na prática.

Resumo dos Conceitos Chave

Arquitetura SIP

- Agentes com dupla função
- Independente de rede
- Cabeçalhos para roteamento
- Diálogos/transações

NAT Traversal

- Registros periódicos
- Cabeçalho Contact
- STUN/TURN/ICE
- Keep-alive

Mensagem Principal

"SIP precisa de mecanismos específicos para NAT porque qualquer agente pode iniciar comunicação."

Próximos Passos

Para Próxima Aula

- Configurar ambiente
- Instalar ferramentas
- Capturar tráfego
- Analisar cabeçalhos

Leituras

- RFC 3261 (SIP)
- RFC 5389 (STUN)
- RFC 5766 (TURN)
- RFC 5245 (ICE)

Dúvidas?

Próxima aula: Configuração prática

Material no repositório da disciplina