# 6. přednáška

**SIP**

# Obsah

1. Charakteristika a historie protokolu
2. Architektura protokolu
3. Bezpečnostní otázky
4. Konfigurace SIP na Cisco směrovačích

# Charakteristika a historie protokolu

- Protokol řízení aplikační vrstvy vycházející z textu ASCI
- Vyvinutý IETF pro multimediální (hlasové, obrazové, textové) konference přes IP
- Konkrétně nabízí vytvoření a udržování relace (session), což je výměna dat uvnitř seskupení účastníků
- Je určen pro aplikace, kde
  - uživatelé se přesunují mezi koncovými body
  - uživatelé adresovatelní více jmény
- Nejde o samostatný komunikační systém, SIP je spíše komponenta, kterou lze použít společně s dalšími protokoly IETF (RTP, RTSP, MGCP, SDP) k sestavení úplné multimediální architektury. Také používá URL pro adresování, DNS pro vyhledávání služeb a TRIP (Telegraphy Routing over IP) pro směrování hovorů. Podpůrné služby mohou poskytovat i LDAP servery databázové servery, aplikace XML atd.
- Základní funkčnost a provoz SIP ale na jiných protokolech nezávisí

# Jak a proč SIP funguje

- Funguje na principu pozvání k relacím založeným na transakčním modelu „požadavek – reakce“ podobnému HTTP. Transakce je tvořena požadavkem, ten aktivuje na druhé straně nějakou funkci (metodu) a min. jednu reakci
- SIP patří do kategorie „peer-to-peer“ (end-to-end) protokolů. Normálně používá UDP port 5060, ale stejný port může fungovat i pro TCP.
- Proč brány SIP jako hlasové brány? Výhody:
  - číslování se konfiguruje přímo na bráně – volání na přímo připojená zařízení lze zpravovávat přímo na bráně a nemusí se přeposílat na speciální zařízení (např. CUCM). Obdobně se lze vyhnout i směrování na speciálních zařízeních v případě volání na zaregistrovaná místa přímo na bráně
  - překlady lze definovat na jednotlivých branách á tím uplatnit regionální požadavky (např. formáty speciálních čísel)
  - integrace hlasových bran různých výrobců (např. komunikace hlasové brány Cisco IOS – s hlasovou branou Alcatel-Lucent)

# Historie vzniku protokolu SIP

Work began in 1995 in IETF mmusic WG

02/1996: draft-ietf-mmusic-sip-00: 15 stran

12/1996: -01: 30 stran, dva typy request

01/1999: -12: 149 stran, 6 metod

03/1999: RFC2543, 153 stran, 6 metod

11/1999: SIP WG

11/2000: draft-ietf-sip-rfc2543bis-02, 171 stran, 6 metod

04/2001: rozdělení na skupinySIP WG a SIP a SIPPING

02/2002: RFC3261 – 269 stran (jádro protokolu)

03/2010: RFC5727 – změny

# Dokumenty 1

**Core SIP Documents**

| RFC | Document Title |
|---|---|
| RFC 2543 | SIP: Session Initiation Protocol (obsolete) |
| RFC 3261 | SIP: Session Initiation Protocol |
| RFC 3262 | Reliability of Provisional Responses |
| RFC 3263 | Locating SIP Servers |
| RFC 3264 | An Offer/Answer Model with the Session Description Protocol (SDP) |
| RFC 3265 | SIP-Specific Event Notification |

**SDP-Related Documents**

| RFC | Document Title |
|---|---|
| RFC 2327 | Session Description Protocol (SDP) (obsolete: see RFC 4566) |
| RFC 3266 | Support of IPv6 in SDP |
| RFC 3388 | Grouping Media Lines in SDP |
| RFC 3407 | Session Description Protocol (SDP) Simple Capability Declaration |
| RFC 3556 | SDP Bandwidth Modifiers for RTCP Bandwidth |
| RFC 3605 | Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) |
| RFC 3890 | A Transport Independent Bandwidth Modifier |
| RFC 4091 | An Alternative NAT Semantics for SDP |
| RFC 4145 | TCP-Based Media Transport in the SDP |
| RFC 4566 | Session Description Protocol (SDP) |
| RFC 4567 | Key Management Extensions for SDP and RTSP |
| RFC 4568 | SDP Security Descriptions for Media Streams |
| RFC 4570 | SDP Source Filters |
| RFC 4572 | Connection-Oriented Media Transport over TLS in SDP |
| RFC 4574 | SDP Label Attribute |
| RFC 4756 | FEC Grouping Semantics in SDP |
| RFC 5027 | Security Preconditions for SDP |
| RFC 5432 | QoS Mechanism Selection in SDP |
| RFC 5547 | SDP Offer/Answer Mechanism to Enable File Transfer |
| RFC 5576 | Source-Specific Media Attributes in SDP |

# Dokumenty 2

**RTP-Related Documents**

| RFC | Document Title |
|---|---|
| RFC 1889 | RTP: Transport Protocol for Real-Time Applications (obsolete: see RFC 3550) |
| RFC 1890 | RTP Profile for Audio and Video Conferences with Minimal Control (obsolete: see RFC 3551) |
| RFC 2198 | RTP Payload for Redundant Audio Data |
| RFC 2733 | An RTP Payload Format for Generic Forward Error Correction (obsolete: see RFC 5109) |
| RFC 2793 | RTP Payload for Text Conversation (obsolete: see RFC 4103) |
| RFC 2833 | RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals (obsolete: see RFC 4733) |
| RFC 2959 | Real-Time Transport Protocol Management Information Base |
| RFC 3389 | RTP Payload for Comfort Noise |
| RFC 3611 | RTP Control Protocol Extended Reports (RTCP XR) |
| RFC 3711 | The Secure Real-time Transport Protocol (SRTP) |
| RFC 4103 | RTP Payload for Text Conversation |
| RFC 4571 | Framing RTP and RTCP Packets over Connection-Oriented Transport |
| RFC 4585 | Extended RTP Profile for RTCP-Based Feedback (RTP/AVPF) |
| RFC 4586 | RTP/AVPF: Results of the Timing Rule Simulations |
| RFC 4588 | RTP Retransmission Payload Format |
| RFC 4771 | Integrity Transform Carrying Roll-Over for SRTP |
| RFC 4733 | RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals |
| RFC 4961 | Symmetric RTP / RTP Control Protocol |
| RFC 3550 | RTP: Transport Protocol for Real-Time Applications |
| RFC 3551 | RTP Profile for Audio and Video Conferences with Minimal Control |
| RFC 5109 | RTP Payload Format for Generic Forward Error Correction |
| RFC 5117 | RTP Topologies |
| RFC 5450 | Transmission Time Offsets in RTP Streams |
| RFC 5506 | Support for Reduced-Size RTCP: Opportunities and Consequences |

# Dokumenty 3

**HTTP-Related Documents**

| RFC | Document Title |
|---|---|
| RFC 2616 | Hypertext Transfer Protocol -- HTTP/1.1 |
| RFC 2617 | HTTP Authentication: Basic and Digest Access Authentication |
| RFC 3310 | HTTP Digest Authentication Using Authentication and Key Agreement (AKA) |

**MIME-Related Documents**

| RFC | Document Title |
|---|---|
| RFC 1847 | Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted |
| RFC 2045 | MIME Part One: Format of Internet Message Bodies |
| RFC 2046 | MIME Part Two: Media Types |
| RFC 2047 | MIME Part Three: Message Header Extensions for Non-ASCII Text |
| RFC 2048 | MIME Part Four: Registration Procedures (obsolete: see RFC 4288 and RFC 4289) |
| RFC 2633 | S/MIME Version 3 Message Specification |
| RFC 3204 | MIME media types for ISUP and QSIG Objects |
| RFC 3420 | Internet Media Type message/sipfrag |
| RFC 3555 | MIME Type Registration of RTP Payload Formats |
| RFC 4288 | Media Type Specifications and Registration Procedures |
| RFC 4289 | Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures |

# Dokumenty 4

**SIP Standards Track Documents (Options, Extensions, etc.)**

| RFC | Document Title |
|---|---|
| RFC 2976 | The SIP INFO Method |
| RFC 3048 | Extensions for IP Access to Telephone Call Services |
| RFC 3050 | CGI for SIP |
| RFC 3311 | UPDATE Method |
| RFC 3312 | Integration of Resource Management and SIP |
| RFC 3313 | Private SIP Extensions for Media Authorization |
| RFC 3319 | DHCPv6 Options for SIP Servers |
| RFC 3323 | A Privacy Mechanism for SIP |
| RFC 3324 | Short Term Requirements for Network Asserted Identity |
| RFC 3325 | Private Extensions to SIP for Asserted Identity within Trusted Networks |
| RFC 3326 | The Reason Header Field |
| RFC 3327 | Extension Header Field for Registering Non-Adjacent Contacts |
| RFC 3329 | Security Mechanism Agreement |
| RFC 3361 | DHCP-for-IPv4 Option for SIP Servers |
| RFC 3372 | SIP for Telephones (SIP-T): Context and Architectures |
| RFC 3398 | ISUP to SIP Mapping |
| RFC 3428 | SIP Extension for Instant Messaging |
| RFC 3455 | Private Header Extensions for 3GPP |
| RFC 3515 | The Session Initiation Protocol (SIP) Refer Method |
| RFC 3578 | Mapping ISUP Overlapped Signalling to SIP |
| RFC 3581 | Extension to SIP for Symmetric Response Routing |
| RFC 3608 | Extension Header Field for Service Route Discovery During Registration |
| RFC 3680 | SIP Event Package for Registrations |
| RFC 3840 | Indicating User Agent Capabilities in SIP |
| RFC 3841 | Caller Preferences for SIP |
| RFC 3842 | Message Summary and Message Waiting Indication Event Package |
| RFC 3856 | Presence Event Package |
| RFC 3857 | A Watcher Information Event Template-Package |
| RFC 3891 | "Replaces" Header |
| RFC 3892 | Referred-By Mechanism |
| RFC 3893 | SIP Authenticated Identity Body (AIB) |
| RFC 3911 | SIP "Join" Header |
| RFC 3903 | Event State Publication |
| RFC 3959 | Early Session Disposition Type |
| RFC 3960 | Early Media and Ringing Tone Generation |
| RFC 4028 | Session Timers in the Session Initiation Protocol (SIP) |
| RFC 4235 | An INVITE-Initiated Dialog Event Package for SIP |
| RFC 4244 | Extension for Request History Information |
| RFC 4320 | Actions Addressing Identified Issues with the SIP Non-INVITE Transaction |
| RFC 4411 | Extending the SIP Reason Header for Preemption Events |
| RFC 4412 | Communications Resource Priority for SIP |
| RFC 4474 | Enhancements for Authenticated Identity Management in SIP |
| RFC 4483 | A Mechanism for Content Indirection in SIP |
| RFC 4488 | Suppression of SIP REFER Method Implicit Subscription |
| RFC 4575 | SIP Event Package for Conference State |
| RFC 4662 | SIP Event Notification Extension for Resource Lists |
| RFC 4730 | Event Package for KPML |
| RFC 4780 | MIB for SIP |
| RFC 4904 | Representing Trunk Groups in tel/sip URIs |
| RFC 4916 | Connected Identity in SIP |
| RFC 4967 | Dial String Parameter for the SIP URI |
| RFC 4975 | Message Session Relay Protocol (MSRP) |
| RFC 4976 | Relay Extension for MSRP |
| RFC 5079 | Rejecting Anonymous Requests in SIP |
| RFC 5196 | SIP User Agent Capability Extension to Presence Information Data Format (PIDF) |
| RFC 5263 | SIP Extension for Partial Notification of Presence Information |
| RFC 5264 | Publication of Partial Presence Information |
| RFC 5373 | Requesting Answering Modes for SIP |
| RFC 5478 | IANA Registration of new SIP Resource-Priority Namespaces |
| RFC 5509 | IANA Registration Instant Messaging and Presence DNS SRV RRs for SIP |
| RFC 5552 | SIP Interface to VoiceXML Media Services |
| RFC 5589 | SIP Call Control - Transfer |
| RFC 5627 | Obtaining and Using Globally Routable User Agent URIs (GRUUs) in SIP |
| RFC 5628 | Registration Event Package Extension for SIP GRUUs |
| RFC 5629 | A Framework for Application Interaction in SIP |
| RFC 5630 | The Use of the SIPS URI Scheme in SIP |
| RFC 5631 | SIP Session Mobility |
| RFC 5658 | Addressing Record-Route Issues in SIP |

# Dokumenty 5

**SIP Informational RFCs and BCP Documents**

| RFC | Document Title |
|---|---|
| RFC 3087 | Control of Service Context using SIP Request-URI |
| RFC 3351 | User Requirements for SIP in Support of Speech/Hearing Impaired |
| RFC 3603 | Private SIP Proxy-to-Proxy Extensions for PacketCable Distributed Call Signaling |
| RFC 3665 | SIP Basic Call Flow Examples |
| RFC 3702 | Authentication, Authorization, and Accounting Requirements for SIP |
| RFC 3824 | Using E.164 numbers with SIP |
| RFC 3966 | IANA Registry for SIP Header Field |
| RFC 3969 | IANA Registry for SIP URI |
| RFC 3976 | Interworking SIP and IN Applications |
| RFC 4117 | Transcoding Services Invocation using SPCC |
| RFC 4123 | SIP-H.323 Interworking Requirements |
| RFC 4168 | SCTP as a transport for SIP |
| RFC 4189 | Requirements for End-to-Middle Security for SIP |
| RFC 4240 | Basic Network Media Services with SIP |
| RFC 4245 | High-Level Requirements for Tightly Coupled SIP Conferencing |
| RFC 4317 | SDP Offer/Answer Examples |
| RFC 4321 | Problems Identified Associated with the SIP Non-INVITE Transaction |
| RFC 4353 | A Framework for Conferencing with SIP |
| RFC 4354 | SIP Event Package and Data Format for Push-to-Talk over Cellular (PoC) Service |
| RFC 4453 | Requirements for Consent-Based Communications in the SIP |
| RFC 4457 | SIP P-User-Database Private-Header (P-Header) |
| RFC 4458 | SIP URIs for Applications such as Voicemail and Interactive Voice Response (IVR) |
| RFC 4475 | SIP Torture Test Messages |
| RFC 4484 | Trait-Based Authorization Requirements for SIP |
| RFC 4504 | SIP Telephony Device Requirements and Configuration |
| RFC 4538 | Request Authorization through Dialog Identification in SIP |
| RFC 4596 | Guidelines for Usage of the SIP Caller Preferences Extension |
| RFC 4579 | SIP Call Control - Conferencing for User Agents |
| RFC 4964 | The P-Answer-State Header Extension to SIP |
| RFC 5002 | SIP P-Profile-Key Private Header (P-Header) |
| RFC 5009 | Private Header (P-Header) Extension to SIP for Authorization of Early Media |
| RFC 5039 | SIP and Spam |
| RFC 5057 | Multiple Dialog Usages in SIP |
| RFC 5118 | SIP Torture Test Messages for IPv6 |
| RFC 5194 | Framework for Real-Time Text using SIP |
| RFC 5411 | A Hitchhiker's Guide to SIP |
| RFC 5479 | Requirements and Analysis of Media Security Management Protocols |
| RFC 5502 | SIP P-Served-User Private-Header (P-Header) for the 3GPP Core Network |

**SIP-Related Documents**

| RFC | Document Title |
|---|---|
| RFC 3219 | Telephony Routing over IP (TRIP) (tutorial) |
| RFC 3320 | Signaling Compression |
| RFC 3321 | Signaling Compression - Extended Operations |
| RFC 3322 | Signaling Compression - Requirements and Assumptions |
| RFC 3485 | Compressing the Session Initiation Protocol (SIP) |
| RFC 3485 | SIP and SDP Static Dictionary for Signaling Compression |
| RFC 3603 | Private SIP Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture (obsolete, see RFC 5503) |
| RFC 3725 | Best Current Practices for 3PCC in SIP |
| RFC 3764 | enumservice registration for SIP Addresses-of-Record |
| RFC 4077 | A Negative Acknowledgement Mechanism for Signaling Compression |
| RFC 4083 | 3GPP Release 5 Requirements on SIP |
| RFC 4092 | Usage of SDP Alternative NAT Semantics in SIP |
| RFC 4465 | Signaling Compression (SigComp) Torture Tests |
| RFC 4497 | Interworking between the SIP and QSIG |
| RFC 4740 | Diameter SIP Application |
| RFC 5049 | Applying Signaling Compression to SIP |
| RFC 5112 | The Presence-Specific Static Dictionary for Signaling Compression |
| RFC 5115 | TRIP attribute for Resource Priority |
| RFC 5503 | Private SIP Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture |

**Directory Services Documents**

| Standard | Document Title |
|---|---|
| H.350 | Directory Services Architecture for Multimedia Conferencing |
| H.350.4 | Directory Services Architecture for SIP |

# RFC 3261 – 269 stran!

Network Working Group
Request for Comments: 3261
Obsoletes: 2543
Category: Standards Track

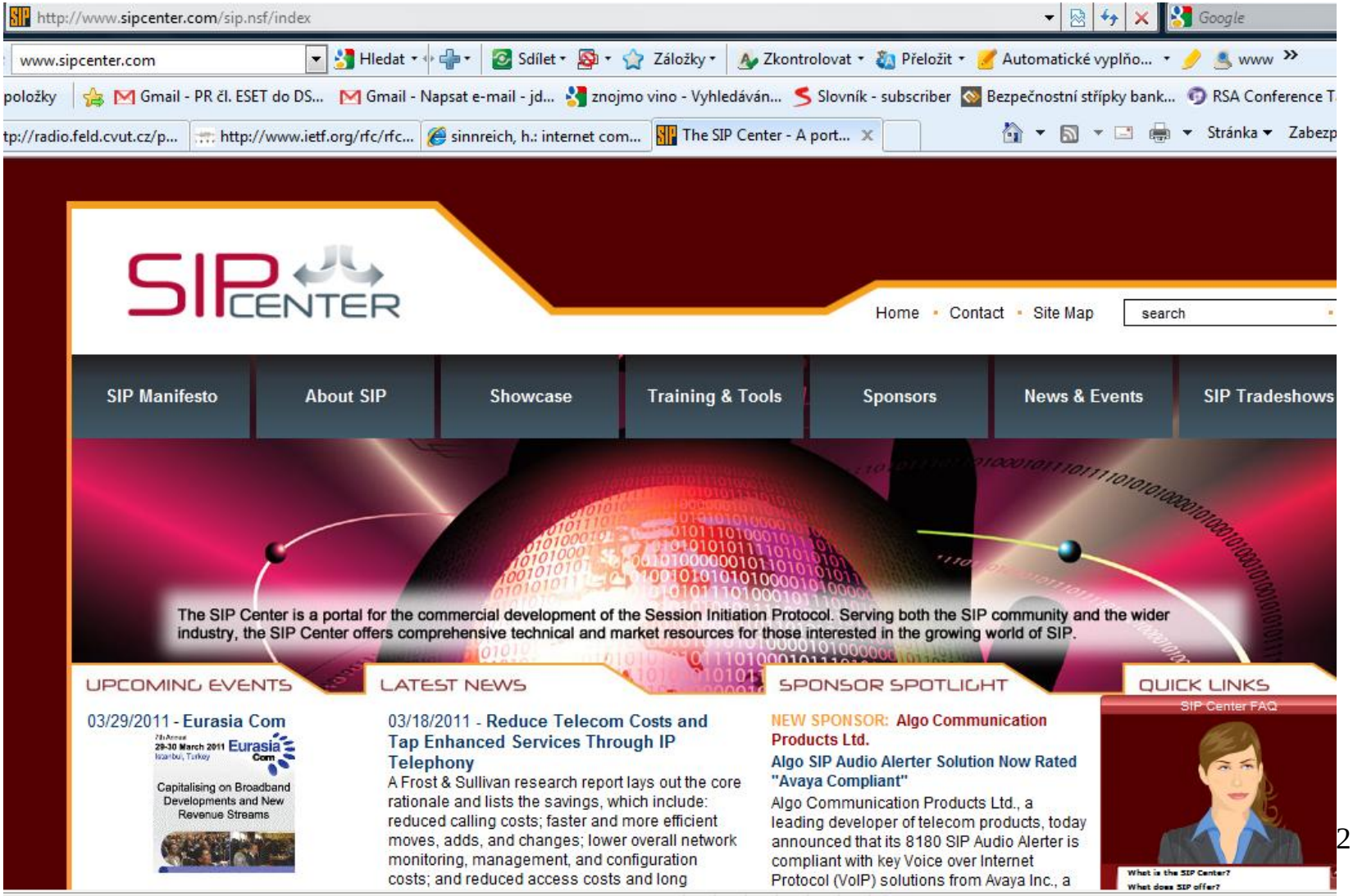
J. Rosenberg
dynamicsoft
H. Schulzrinne
Columbia U.
G. Camarillo
Ericsson
A. Johnston
WorldCom
J. Peterson
Neustar
R. Sparks
dynamicsoft
M. Handley
ICIR
E. Schooler
AT&T
June 2002

SIP: Session Initiation Protocol

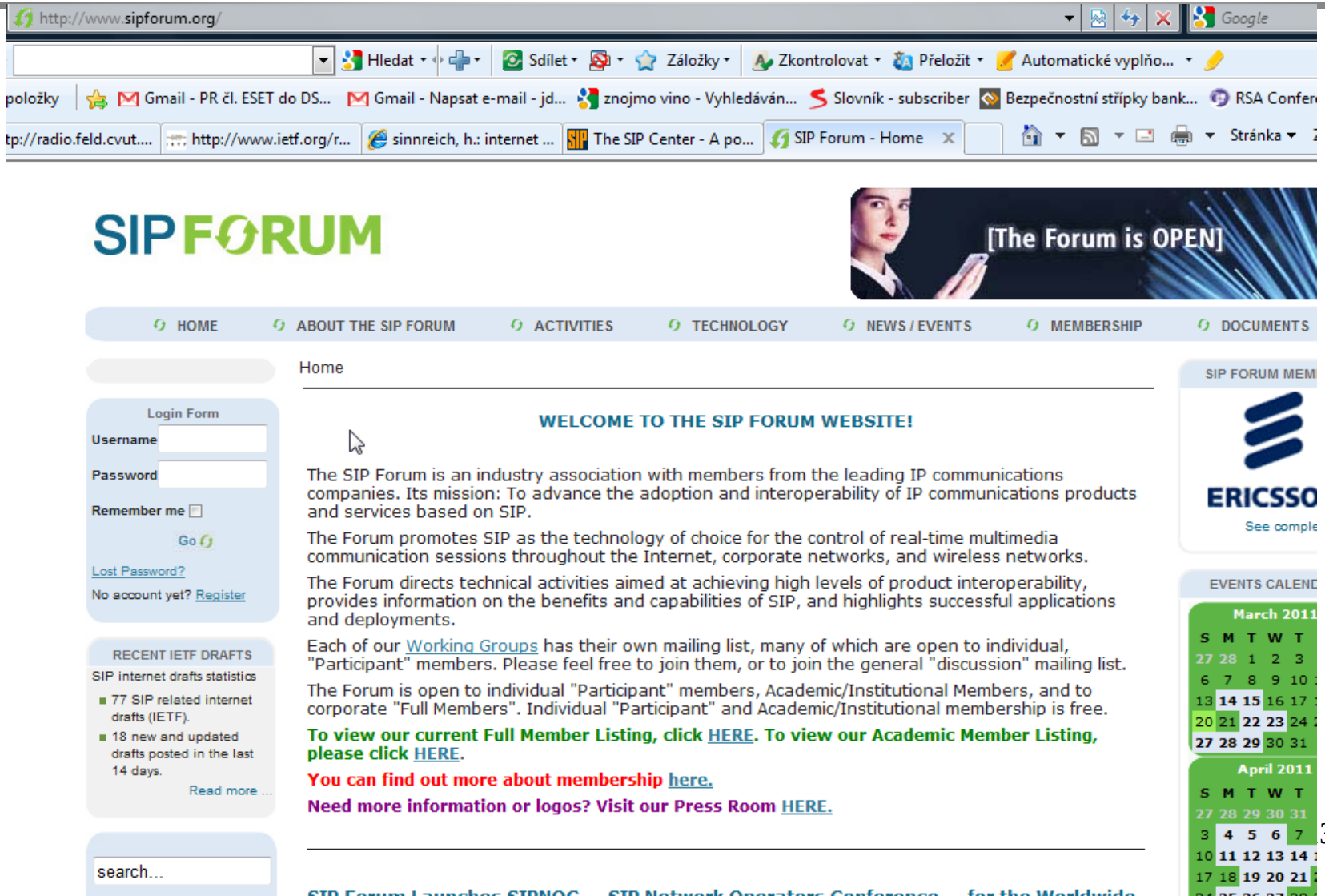
Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

# SIP center


http://www.sipcenter.com/sip.nsf/index
www.sipcenter.com
The SIP Center - A port...
SIP CENTER
Home · Contact · Site Map
search
SIP Manifesto
About SIP
Showcase
Training & Tools
Sponsors
News & Events
SIP Tradeshows
The SIP Center is a portal for the commercial development of the Session Initiation Protocol. Serving both the SIP community and the wider industry, the SIP Center offers comprehensive technical and market resources for those interested in the growing world of SIP.
UPCOMING EVENTS
LATEST NEWS
SPONSOR SPOTLIGHT
QUICK LINKS
03/29/2011 - Eurasia Com
29-30 March 2011 Eurasia Com
Capitalising on Broadband Developments and New Revenue Streams
03/18/2011 - Reduce Telecom Costs and Tap Enhanced Services Through IP Telephony
A Frost & Sullivan research report lays out the core rationale and lists the savings, which include: reduced calling costs; faster and more efficient moves, adds, and changes; lower overall network monitoring, management, and configuration costs; and reduced access costs and long
NEW SPONSOR: Algo Communication Products Ltd.
Algo SIP Audio Alerter Solution Now Rated "Avaya Compliant"
Algo Communication Products Ltd., a leading developer of telecom products, today announced that its 8180 SIP Audio Alerter is compliant with key Voice over Internet Protocol (VoIP) solutions from Avaya Inc., a
SIP Center FAQ
What is the SIP Center?
What does SIP offer?

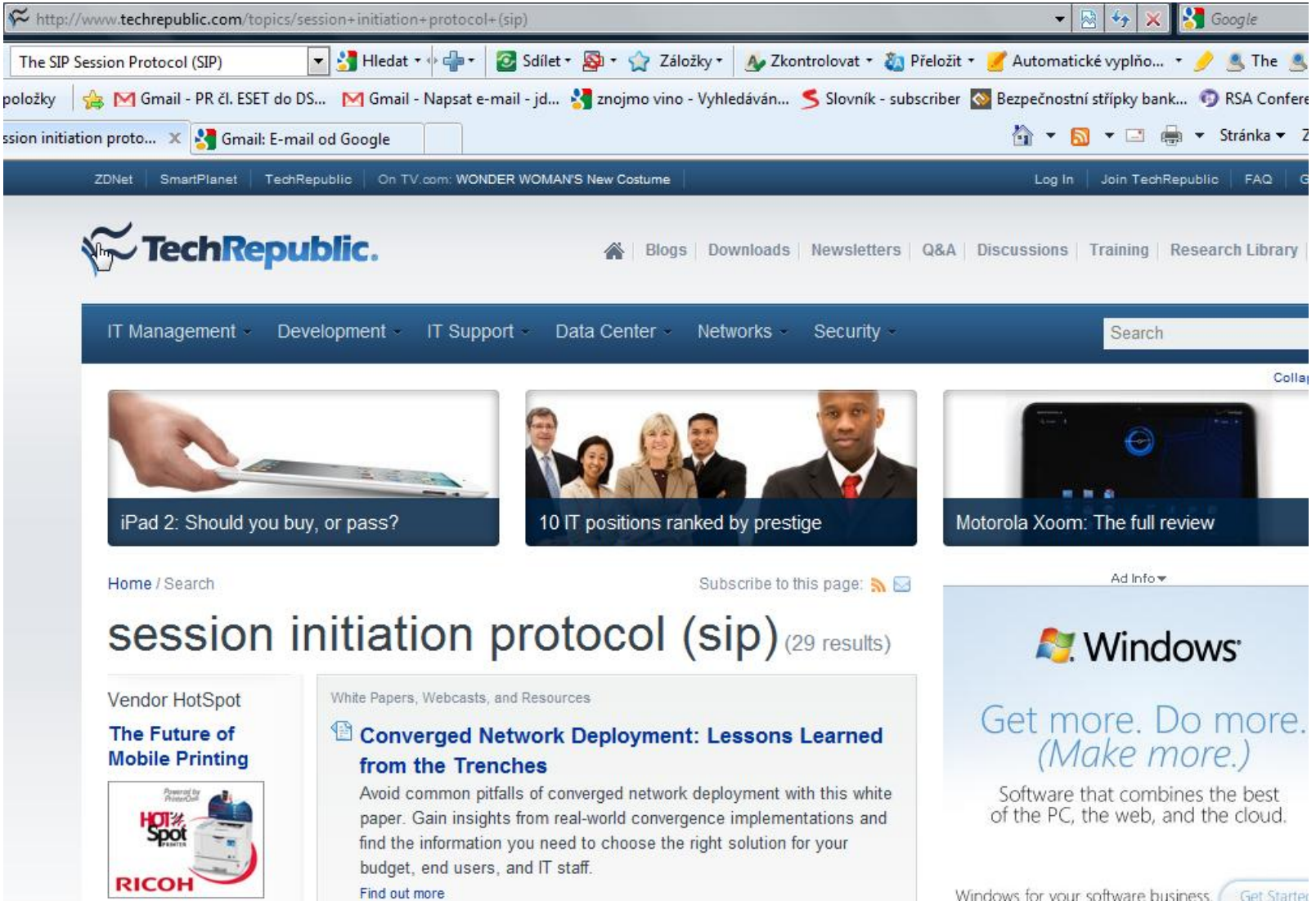
# SIP Forum


http://www.sipforum.org/
Google
Hledat
Sdílet
Záložky
Zkontrolovat
Přeložit
Automatické vyplňo...
položky
Gmail - PR čl. ESET do DS...
Gmail - Napsat e-mail - jd...
znojmo vino - Vyhledáván...
Slovník - subscriber
Bezpečnostní střípky bank...
RSA Confer
tp://radio.feld.cvut....
http://www.ietf.org/r...
sinnreich, h.: internet ...
The SIP Center - A po...
SIP Forum - Home
Stránka
SIP FORUM
[The Forum is OPEN]
HOME
ABOUT THE SIP FORUM
ACTIVITIES
TECHNOLOGY
NEWS / EVENTS
MEMBERSHIP
DOCUMENTS
Home
Login Form
Username
Password
Remember me
Go
Lost Password?
No account yet? Register
RECENT IETF DRAFTS
SIP internet drafts statistics
77 SIP related internet drafts (IETF).
18 new and updated drafts posted in the last 14 days.
Read more ...
search...
WELCOME TO THE SIP FORUM WEBSITE!
The SIP Forum is an industry association with members from the leading IP communications companies. Its mission: To advance the adoption and interoperability of IP communications products and services based on SIP.
The Forum promotes SIP as the technology of choice for the control of real-time multimedia communication sessions throughout the Internet, corporate networks, and wireless networks.
The Forum directs technical activities aimed at achieving high levels of product interoperability, provides information on the benefits and capabilities of SIP, and highlights successful applications and deployments.
Each of our Working Groups has their own mailing list, many of which are open to individual, "Participant" members. Please feel free to join them, or to join the general "discussion" mailing list.
The Forum is open to individual "Participant" members, Academic/Institutional Members, and to corporate "Full Members". Individual "Participant" and Academic/Institutional membership is free.
To view our current Full Member Listing, click HERE. To view our Academic Member Listing, please click HERE.
You can find out more about membership here.
Need more information or logos? Visit our Press Room HERE.
SIP FORUM MEM
ERICSSO
See comple
EVENTS CALEND
March 2011
S M T W T
27 28 1 2 3
6 7 8 9 10
13 14 15 16 17
20 21 22 23 24
27 28 29 30 31
April 2011
S M T W T
27 28 29 30 31
3 4 5 6 7
10 11 12 13 14
17 18 19 20 21

# OpenSIP


Google Tato stránka je v jazyce anglicky. Chcete ji přeložit pomocí lišty Google Toolbar? Další informace Nejedná se o jazyk anglicky? Pomozte nám zlepšit se
Přeložit
Vždy překládat jazyk anglic
Currently you are not logged in.
Login | Register
opensips
the new breed of communication engine
GO
Main
News
License
Releases
2.0 Design
About
Contact
Resources
Downloads
Install
Documentation
Webinars
Performance tests
Features
Mailing lists
Public meetings
View History Print
Welcome to the OpenSIPS Project - Former OpenSER Project
Headline news:
Load an performance monitoring: New statistics and traps for monitoring and debugging the load and performance of OpenSIPS
OpenSIPS 2.0 code release: first code for OpenSIPS 2.0 was released. You can download and give it a try - please note the first release has a limited functionality
OpenSIPS eBootcamp: remote learning for OpenSIPS via eBootcamps - starting on 28th of February
OpenSIPS 1.6.4 released: a new major stable release is available for download - learn more about the new additions
What OpenSIPS is
OpenSIPS (Open SIP Server) is a mature Open Source implementation of a SIP server. OpenSIPS is more than a SIP proxy/router as it includes application-level functionalities. OpenSIPS, as a SIP server, is the core component of any SIP-based VoIP solution. With a very flexible and customizable routing engine, OpenSIPS 'unifies voice, video, IM and presence services in a highly efficient way, thanks to its
Your VoIP Account
Login / Register
News
Load and performance monitoring
22nd of February 2011 New statistics and traps for OpenSIPS monitoring.
Read more...
OpenSIPS 2.0
17th of February 2011
OpenSIPS 2.0 first code release.
Internet | Chráněný režim: Vypnuto
100%

# TechRepublic



# P2P SIP

## Peer-to-Peer Session Initiation Protocol (p2psip)

Documents | Charter | List Archive » | Tools WG Page »

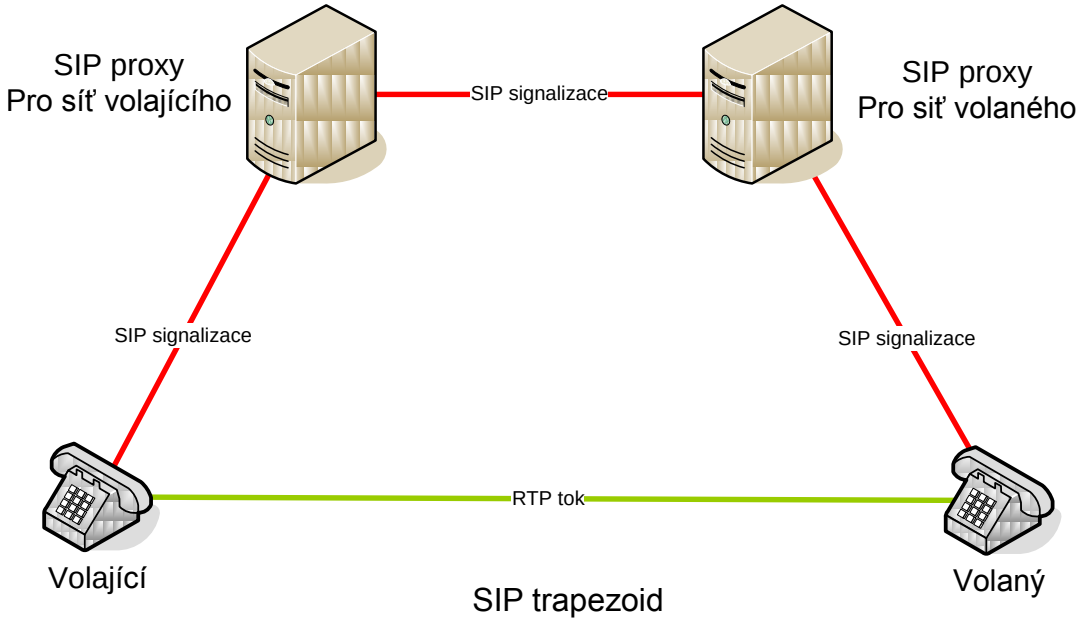
| Document | Title | Date | Status |
|---|---|---|---|
| **Active Internet-Drafts** | | | |
| draft-ietf-p2psip-base-12 | REsource LOcation And Discovery (RELOAD) Base Protocol | 2010-11-10 | I-D Exists |
| draft-ietf-p2psip-concepts-03 | Concepts and Terminology for Peer to Peer SIP | 2010-10-25 | I-D Exists |
| draft-ietf-p2psip-diagnostics-05 | P2PSIP Overlay Diagnostics | 2011-01-11 | I-D Exists |
| draft-ietf-p2psip-self-tuning-03 | A Self-tuning Distributed Hash Table (DHT) for REsource LOcation And Discovery (RELOAD) | 2011-01-07 | I-D Exists |
| draft-ietf-p2psip-service-discovery-02 | Service Discovery Usage for REsource LOcation And Discovery (RELOAD) | 2011-01-07 | I-D Exists |

| Related Documents | Title | Date | Status |
|---|---|---|---|
| **Active Internet-Drafts** | | | |
| draft-chen-p2psip-psc-00 | Public Security Channel(PSC): An Alternative Key Management Mode in RELOAD | 2010-10-15 | I-D Exists |
| draft-jiang-p2psip-relay-05 | An extension to RELOAD to support Direct Response and Relay Peer routing | 2011-03-10 new | I-D Exists |
| draft-knauf-p2psip-disco-01 | A RELOAD Usage for Distributed Conference Control (DisCo) | 2010-12-30 | I-D Exists |

# 2. Architektura protokolu

# Architektura protokolu SIP

- účastnické stanice (User agent – UA)
- SIP proxy server (zástupný server)



# Účastnické stanice

- Účastnické stanice (User Agent – UA) jsou zařízení implementující protokol SIP používané zejména k uskutečnění a příjmu hovorů umístěné na konci sítě internetové telefonie.
- Alternativně mohou být za účastnickou stanici považovány brány do dalších sítí jako například brána do sítě PSTN, umožňující volání a příjem hovorů ze sítě PSTN.
- Častým případem jsou také účastnické stanice používané výhradně pro IM (Instant Messaging).
- Uživatelské stanice mohou být ve formě software na klasických PC (softwarové telefony), popřípadě se může jednat o specializovaná zařízení pro IP telefonii (hardwarové telefony).
- Účastnické stanice musejí být schopny obsluhovat celou řadu protokolů používaných ve světe internetové telefonie (SIP, RTP, RTCP, STUN atd.).
- Účastnické stanice jsou rovněž zodpovědné za kódování signálu před přenosem a musejí tak implementovat některé přenosové kodeky.

# Složení účastnické stanice

- Každá **účastnická stanice** se skládá ze dvou částí:
  - *Klientská část* (UAC – User Agent Client) je část zodpovědná za vytváření volání,  za registraci stanice atd.
  - *Serverová část* (UAS – User Agent Server) je část zodpovědná za příjem požadavků a generování odpovídajících odezev.

  Všechna koncová zařízení a servery implementují jak UAC, tak i UAS.

# SIP proxy server

- *SIP proxy server* (zástupný server) je zařízení zodpovědné za příjem požadavků od uživatelských stanic a ostatních SIP proxy a jejich následné směřování na další SIP proxy popřípadě přímo na cílovou uživatelskou stanici tehdy, kdy je cílová stanice registrována na této SIP proxy.
- Vyhledání další SIP proxy je možné pomocí DNS systémů popřípadě pomocí fixního směrování nastaveném v dané proxy.
- Rozdělení: stateless a statefull (poznají opakující se zprávy, smyčky, větvení atd.)

  Stateful jsou transakční (do ukončení transakce) a dialogové (do ukončení dialogu)

# Další prvky architektury

- redirect (přesměrování) server
- register (registrační) server
- location (lokační) server
- STUN
- RTP proxy

# Redirect, Register a Location servery

- *Redirect server* (přesměrovací server) po přijetí zprávy INVITE provede vyhledání ve vlastní databázi a následně odpoví uživatelské stanici zprávou ze skupiny přesměrování (REDIRECT 3xx) která obsahuje novou adresu, kam by měla uživatelská stanice poslat novou zprávu INVITE.
- *Register server* (registrační server) je zodpovědný za příjem a zpracování REGISTER zpráv popisujících okamžitou lokalizaci uživatelské stanice (její IP a port). Registrační servery bývají spojeny s lokačními servery a SIP proxy servery v jeden homogenní celek.
- *Location server* (server umístění) využívá databáze pro uložení informace o lokalizaci účastnické stanice (IP adresa, port), která je location serveru poskytnuta registračním serverem na základě přijaté REGISTER zprávy. K vyhledání koncového uživatele může použít různé protokoly (finger, rwhois, LSDAP…)

# STUN a RTP proxy

- *STUN* (Simple Traversal of UDP over NAT) je protokol umožňující překonat problém protokolu SIP nebo přesněji protokolu SDP (Session Description Protokol) užívaného uvnitř protokolu SIP (například uvnitř metody INVITE) k popisu cílové IP adresy a portu pro RTP stream.

  Prochází-li pak paket nesoucí metody INVITE přes NAT, je privátní IP adresa paketu nahrazena adresou veřejnou.

- *RTP proxy* jsou užity pro řešení problémů s překladem adres v případech, kdy například oba účastnící jsou v různých privátních sítích za symetrickým NAT.

  RTP proxy se rovněž používají pro zvýšení úrovně zabezpečení v sítích.

  RTP proxy spolupracuje se SIP proxy. SIP proxy provádí náhradu adres pro RTP stream v SDP a instruuje RTP proxy k otevření příslušného RTP kanálu.

# SIP URI

| URI | použití adresy | doporučení |
|---|---|---|
| sip: nebo sips: | SIP a Secure SIP adresa | RFC 3261 |
| tel: | Telefonní čísla | RFC 3999 |
| pres: | Prezence | RFC 3861 |
| im: | Instant Message | RFC 3861 |
| http: | Web | RFC 2616 |
| h323 | H.323 URL | RFC 3508 |

**sip: user: password@host:port;uri-parameters?headers**

# Základní metody protokolu SIP

| Typ zprávy | Popis |
|---|---|
| INVITE | Slouží k žádosti o sestavení spojení |
| ACK | Acknowledgment – potvrzení INVITE (volaným). – realizuje třífázový handshaking |
| BYE | Ukončení spojení |
| CANCEL | Ukončení nesestaveného spojení |
| REGISTER | Registrace UA |
| OPTIONS | Dotaz na možnosti a schopnosti serveru |

# Rozšíření metod protokolu SIP

| smysl žádosti | název metody | doporučení |
|---|---|---|
| sestavení relace | INVITE | RFC 3261 |
| potvrzení na INVITE | ACK | RFC 3261 |
| získání schopností entity | OPTIONS | RFC 3261 |
| zrušení dosud nevyřízené žádosti | CANCEL | RFC 3261 |
| ukončení existující relace | BYE | RFC 3261 |
| registrace (device URI a user URI) | REGISTER | RFC 3261 |
| přihlášení k odběru informací (presence) | SUBSCRIBE | RFC 3265 |
| doručení informace (presence) | NOTIFY | RFC 3265 |
| aktualizace stavu informace na server (presence) | PUBLISH | RFC 3903 |
| požadavek jiného UA k relaci (např. inicializace spojení přes web nebo call transfer) | REFER | RFC 3515 |
| přenos zpráv Instant Message (chat) | MESSAGE | RFC 3428 |
| aktualizace stavu relace | UPDATE | RFC 3311 |
| dočasné potvrzení prozatímní odpovědi | PRACK | RFC 3262 |
| přenos signalizačních informací během relace (např. ISUP SS7) | INFO | RFC 2976 |

# Příklad metody INVITE

```
INVITE sip:darda@sip.domainB.cz SIP/2.0
Via: SIP/2.0/UDP
195.122.198.236:5065;rport;branch=z9hG4bK1441F37B74154C09BD150D68AD
8B83F7
From: markl <sip:jarda@sip.domainA.cz:5065>;tag=1603324369
To: <sip:darda@sip.domainB.cz>
Contact: <sip:jarda@195.122.198.236:5065>
Call-ID: 650ADF5C-0EB4-499A-9744-2B2561B30C94@192.168.2.111
CSeq: 9126 INVITE
Max-Forwards: 70
Content-Type: application/sdp
User-Agent: SIPphone Lite release 1104v
Content-Length: 321
v=0
o=markl 212548077 212548116 IN IP4 195.122.198.236
s=SIPphone Lite
c=IN IP4 195.122.198.236
t=0 0
m=audio 8000 RTP/AVP 0 8 3 98 97 101
a=rtpmap:0 pcmu/8000
a=rtpmap:8 pcma/8000
a=rtpmap:3 gsm/8000
a=rtpmap:98 iLBC/8000
a=rtpmap:97 speex/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

# Analýza požadavku

- Metoda INVITE se používá pro inicializaci volání určitým uživatelem.
- Volající ji posílá INVITE volanému pro nastavení nejrůznějších parametrů volání.

```
INVITE sip:darda@sip.domainB.cz SIP/2.0
Via: SIP/2.0/UDP 195.122.198.236:5065;rport;branch=z9hG4bK1441F37B74154C09BD150D68AD8B83F7
Via umožňuje dopručení odpovědi po stejné trase, branch slouží pro detekci smyček
From: jarda <sip:jarda@sip.domainA.cz:5065>;tag=1603324369… pro rozeznání,kdo odpovídá u forku
To: <sip:darda@sip.domainB.cz>
Contact: sip:jarda@195.122.198.236:5065.. Některé metody mi posílej přímo
Call-ID: 650ADF5C-0EB4-499A-9744-2B2561B30C94@192.168.2.111....identifikátor stejného dialogu
CSeq: 9126 INVITE … pořadové číslo žádosti
Max-Forwards: 70 - omezení počtu skoků (70 default)
```

# Popis základních polí

| Pole | Popis |
|---|---|
| Request line | Skládá se ze tří parametrů: Method, Request-URI and protocol version. Například: `INVITE sip:novak@sip.domainB.cz SIP/2.0` |
| Method | Indikace SIP metody. Například INVITE, REGISTER atd. |
| Request-URI | Indikuje další skok, kam má být požadavek směrován. Tato hodnota se mění v každé proxy na cestě. |
| Protocol version | Version of SIP protocol. SIP/2.0 |
| Via | Každé proxy na cestě požadavku je do tohoto pole zaznamenáno a tak je možné tuto cestu opakovat. Pole *Via* lze rovněž použít pro detekci smyček. |
| From | Identifikuje iniciátora volání (volající). Pole *From* obsahuje parametr *tag*, který slouží jako identifikátor dialogu. |
| To | identifikuje příjemce (volaného). |
| Contact | Obsahuje IP adresu a port, na kterém odesílatel očekává další žádosti odesílané volaným. |
| Call-ID | Identifikátor relace (volání). Jeho cílem je identifikovat zprávy náležející jednomu volání. Takovéto zprávy mají stejný identifikátor *Call-ID*. |
| CSeq | Command Sequence – skládá se ze dvou částí – čísla a názvu metody. Číslo odlišuje požadavky v rámci relace. Metoda je použita k rozlišení mezi odpovědmi na zprávy CANCEL a INVITE. Protože žádosti mohou být odeslány nespolehlivým přenosem, příjemce musí rozpoznat opakování přenosu a selektovat žádosti. |
| Max-Forwards | Obdoba TTL u IP paketů. Slouží k vyřazení cyklujících zpráv. Každé proxy snižuje tuto hodnotu, v případě poklesu hodnoty na nulu je zpráva vyřazena. |
| Content-Length | Délka těla zprávy odděleného od záhlaví jednoduchým CRLF. |

# Přenos parametrů hovoru

```
INVITE sip:darda@sip.domainB.cz SIP/2.0
Via: SIP/2.0/UDP
195.122.198.236:5065;rport;branch=z9hG4bK1441F37B74154C09BD150D68AD
8B83F7
From: markl <sip:jarda@sip.domainA.cz:5065>;tag=1603324369
To: <sip:darda@sip.domainB.cz>
Contact: <sip:jarda@195.122.198.236:5065>
Call-ID: 650ADF5C-0EB4-499A-9744-2B2561B30C94@192.168.2.111
CSeq: 9126 INVITE
Max-Forwards: 70
Content-Type: application/sdp …typ těla zprávy
User-Agent: SIPphone Lite release 1104v
Content-Length: 321 …délka těla
v=0
o=markl 212548077 212548116 IN IP4 195.122.198.236
s=SIPphone Lite
c=IN IP4 195.122.198.236
t=0 0
m=audio 8000 RTP/AVP 0 8 3 98 97 101
a=rtpmap:0 pcmu/8000
a=rtpmap:8 pcma/8000
a=rtpmap:3 gsm/8000
a=rtpmap:98 iLBC/8000
a=rtpmap:97 speex/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

# Pole protokolu SDP
## (Session Description Protocol)

| Pole | Popis |
|---|---|
| V | Verze protokolu SDP. Platná verze je 0. |
| O | Origin – Není použito protokolem SIP. |
| S | Subject – Není použito protokolem SIP. |
| C | Connection – síť (IN pro Internet), typ addresy (IP4 pro IPv4) a adresa, kam směrovat proud RTP paketů. |
| T | Time – není použito protokolem SIP |
| M | Media – media type (audio, video), číslo portu (8000) atd. |
| A | Attribute – podporované kodeky, frekvence vzorkování atd. |

# Metoda REGISTER

```
Via:SIP/2.0/UDP 195.122.198.236:5065; rport;
branch=z9hG4bK4CA55835E62B4946BF92115DE0603D53
From: Jarda <sip:jarda@sip.domain.cz>;tag=4292754936
To: markl <sip:jarda@sip.domain.cz>
Contact: „jarda" <sip:markl@195.122.198.236:5065>
Call-ID: 575AA2FBE68944D48AD5FAEC66C71855@sip.domain.cz
CSeq: 1893 REGISTER
Expires: 1800
Max-Forwards: 70
User-Agent: SIPphone Lite release 1104v
Content-Length: 0
```

- Metoda REGISTER informuje register server o aktuální pozici (IP adresa) telefonu.
- Uživatel může mít zaregistrováno více lokací (několik IP adres přístrojů) přičemž preference pro výběr kontaktní lokace se nastavují pomocí tzv. q-hodnot.
- Při nastavení většího množství kontaktních lokací pak může být kontaktováno více telefonů najednou (pomocí forking mechanizmu) popřípadě mohou být adresy zkoušeny postupně.

# Nejdůležitější pole metody REGISTER

| Záhlaví | Popis |
| --- | --- |
| Contact | Obsahuje URL, které může být použito pro zpřístupnění uživatele. Může rovněž obsahovat PSTN telefonní číslo nebo URL uživatelových webových stránek. |
| Expires | Indikuje dobu platnosti registrované adresy. |

# Kategorie návratových kódů

- Protokol SIP používá číselné kódy pro předání informace o průběhu zpracování požadavku. Některé kódy jsou přímo převzaty z protokolu HTTP,  jiné jsou specifické pro protokol SIP.
- Návratové kódy jsou rozděleny do šesti kategorií:
  - požadavek je zpracováván
  - požadavek byl úspěšně zpracován
  - požadavek je třeba směrovat jinam
  - chyba klienta
  - chyba na serveru
  - globální chyba

# Šest kategorií návratových kódů

| Třída | Popis |
|---|---|
| 1xx | Požadavek je zpracováván (např. „100 Trying“, “180 Ringing”). |
| 2xx | Požadavek byl úspěšně zpracován (např. “200 OK”). |
| 3xx | Přesměrování: Požadavek je třeba směrovat jinam (např. “305 Use proxy”). |
| 4xx | Chyba klienta: Dotaz by se neměl ve stejné podobě opakovat (např. "403 Forbidden"). |
| 5xx | Chyba na serveru (např. "500 Server Internal Error", "501 Not Implemented"). |
| 6xx | Globální chyba ("606 Not Acceptable"). |

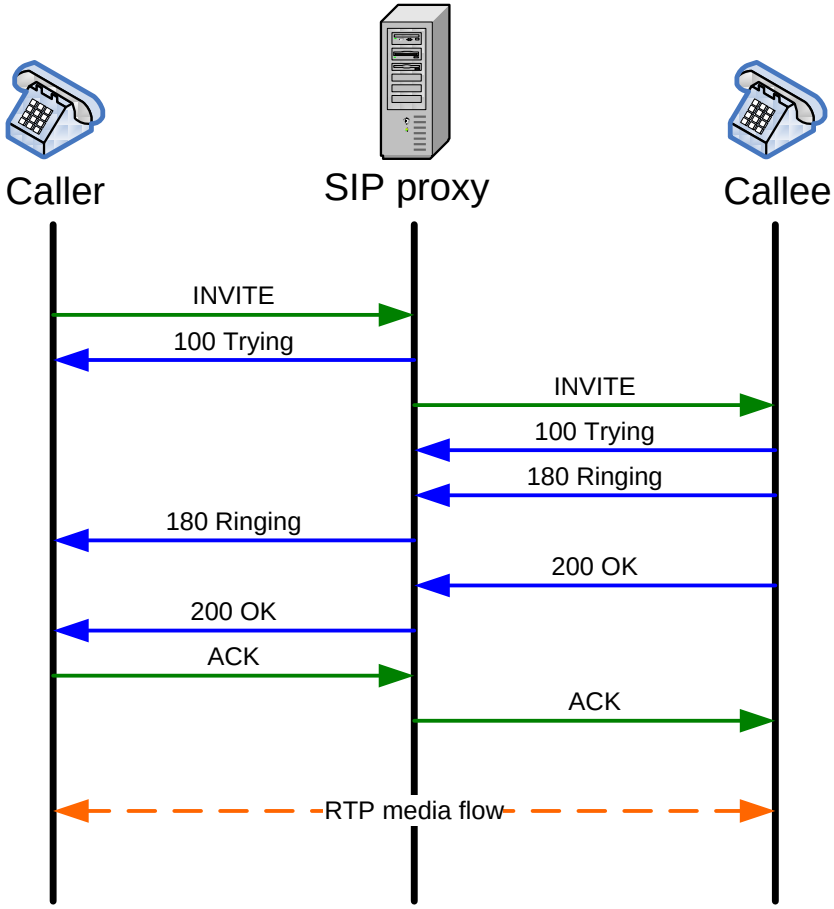
# Základní typy výměn zpráv

- INVITE
- INVITE s proxy autentizací
- BYE
- CANCEL
- REGISTER

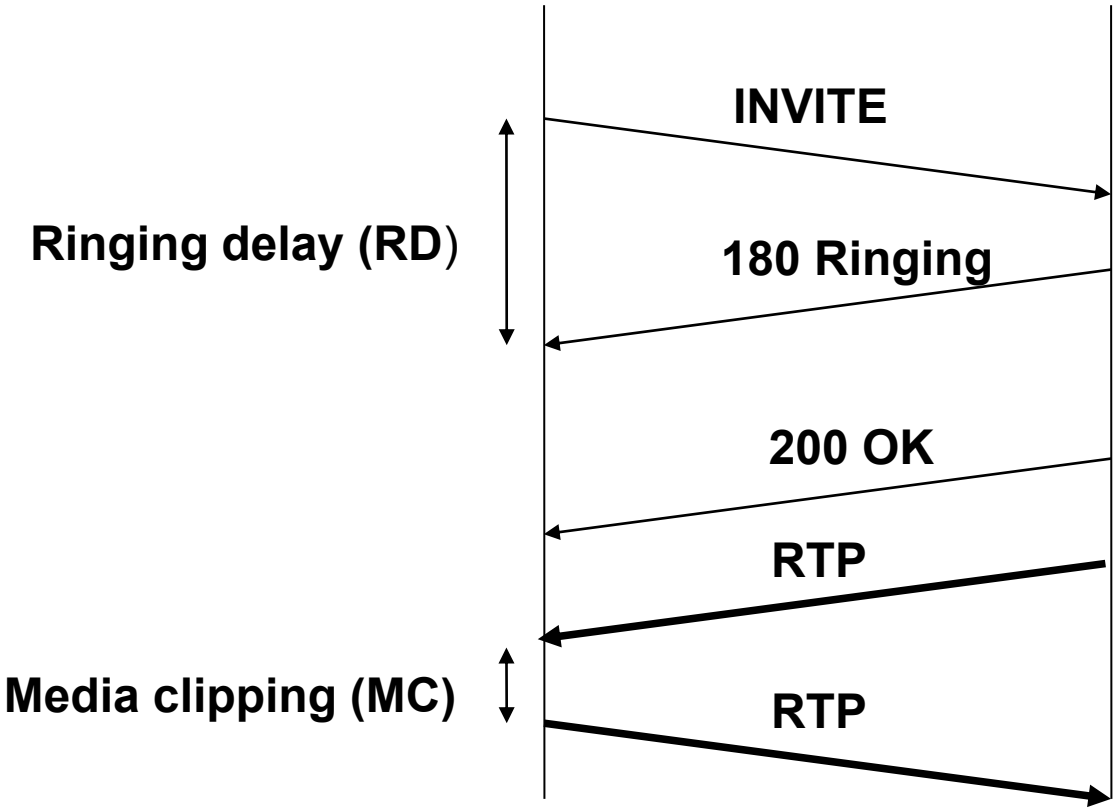
# Sestavení spojení pomocí zprávy INVITE

- Když volající chce uskutečnit hovor, jeho telefon posílá zprávu INVITE na SIP proxy volaného (v dalším textu budeme pro zjednodušení vždy uvažovat jednoduchou variantu, kdy jsou oba účastnící ze stejné domény, popřípadě kdy účastník nepoužívá odchozí SIP proxy, hovor je tak směřován pouze přes jednu SIP proxy).
- SIP proxy odpoví volajícímu provizorní odpovědí 100 Trying, která znamená, že se SIP proxy snaží kontaktovat telefon volaného.
- SIP proxy pak provede vyhledání kontaktní IP adresy volaného v lokální databází a odešle zprávu INVITE na telefon volaného.
- Telefon po přijetí zprávy INVITE začne zvonit a informuje o tom volajícího zprávou 180 Ringing.
- Když potom volaný přijme hovor, odezva 200 OK je poslána volajícímu.
- Telefon volajícího potvrdí úspěšné sestavení spojení zprávou ACK.
- Spojení je nyní sestaveno a přenos RTP může začít.

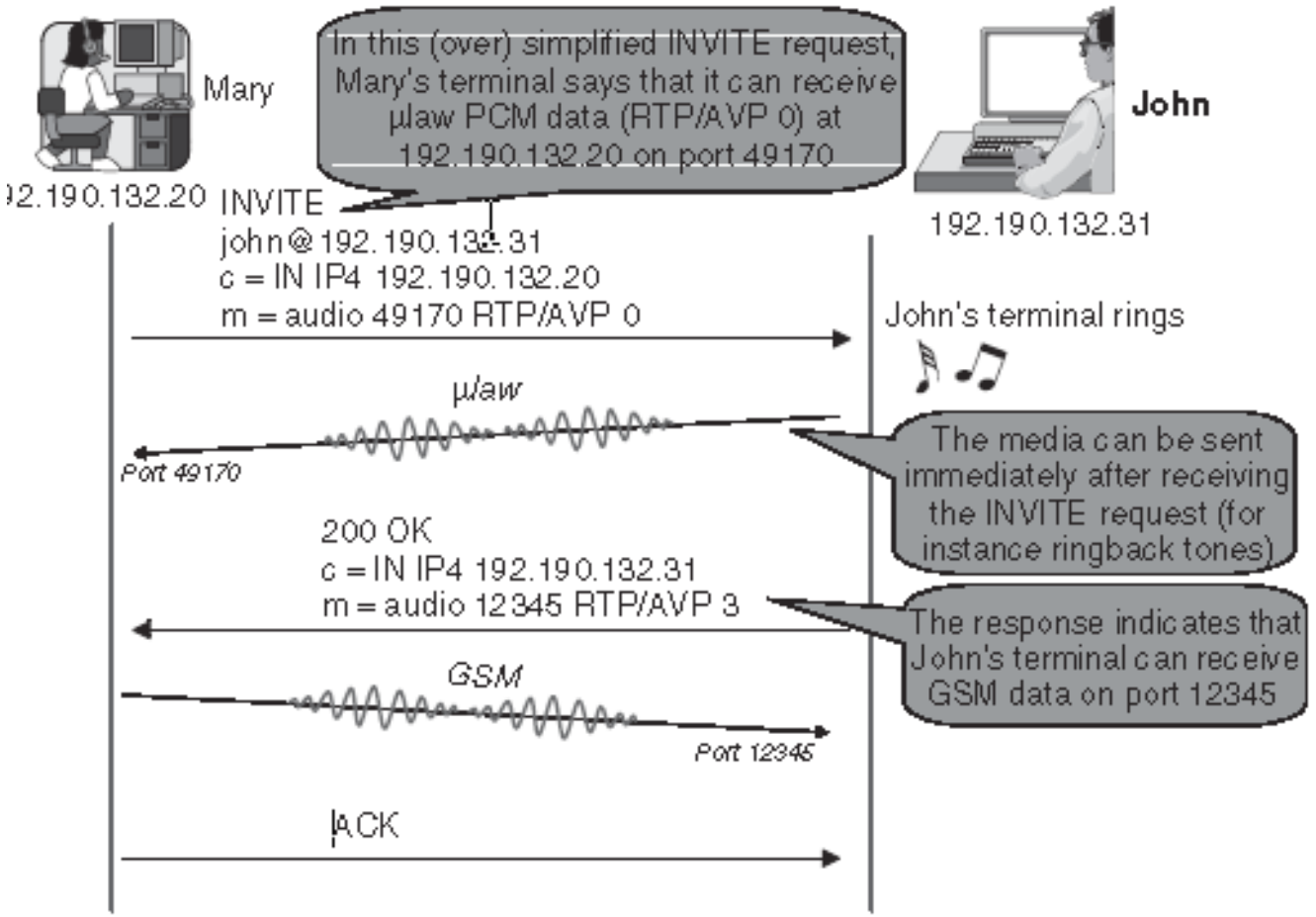
# INVITE


Caller
SIP proxy
Callee
INVITE
100 Trying
INVITE
100 Trying
180 Ringing
180 Ringing
200 OK
200 OK
ACK
ACK
RTP media flow

# Co vlastně měříme?
## Poznámka k výkonnostním metrikám



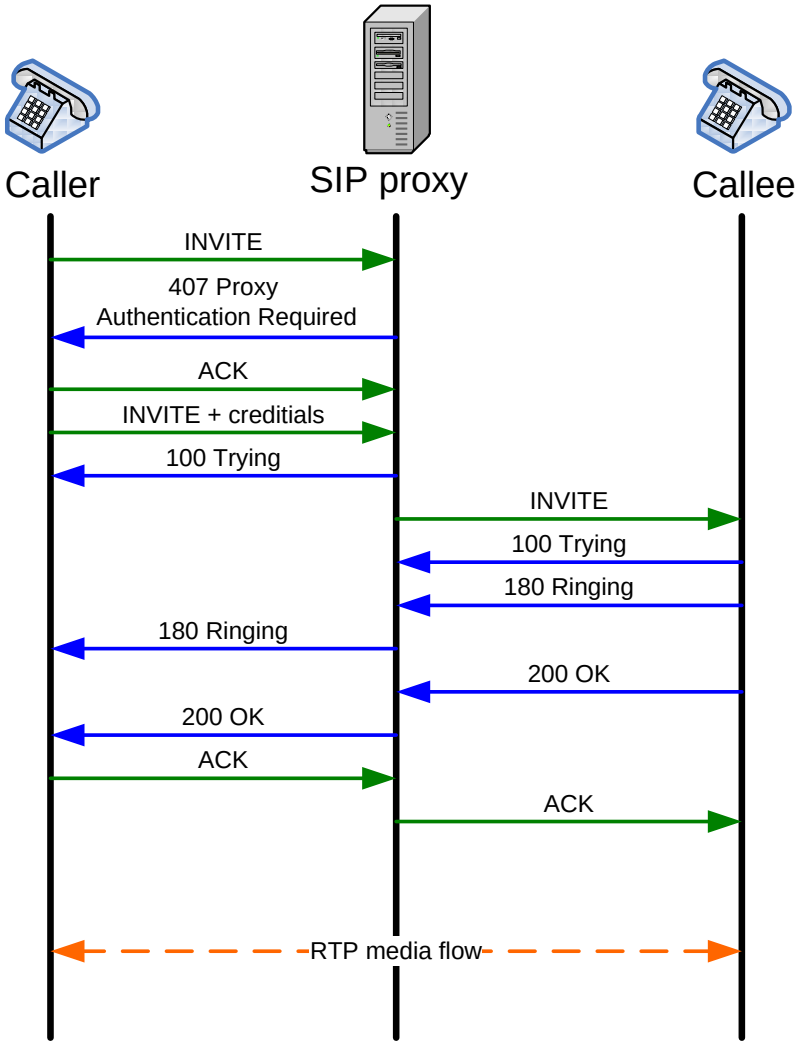
# Příklad


Mary
2.190.132.20
In this (over) simplified INVITE request, Mary's terminal says that it can receive µlaw PCM data (RTP/AVP 0) at 192.190.132.20 on port 49170
John
192.190.132.31
INVITE
john@192.190.132.31
c = IN IP4 192.190.132.20
m = audio 49170 RTP/AVP 0
John's terminal rings
µlaw
Port 49170
The media can be sent immediately after receiving the INVITE request (for instance ringback tones)
200 OK
c = IN IP4 192.190.132.31
m = audio 12345 RTP/AVP 3
The response indicates that John's terminal can receive GSM data on port 12345
GSM
Port 12345
ACK

# Sestavení spojení pomocí zprávy INVITE s autentizací

- V případě, kdy SIP proxy vyžaduje autentizaci, je první zpráva INVITE poslána stejným způsobem, jako v předchozím případě.
- Proxy reaguje na přijatou INVITE zprávu odezvou 407 Proxy Authentication Required, kde proxy umístí Proxy-authenticate výzvu s nastavenými poli realm a nonce.
- Telefon volajícího potvrdí odpověď SIP proxy zprávou ACK a použije získaná pole realm a nonce k vytvoření hodnoty pole Response v nové INVITE zprávě.
- Nová zpráva INVITE s Proxy-Authentication záhlavím, obsahující uživatelské jméno, realm, nonce a vygenerované pole Response, je poslána znovu na SIP proxy.
- SIP proxy ověří zadané hodnoty a když proxy odpovídají, pokračuje ve zpracování požadavku stejně jako v předchozím scénáři bez proxy autentizace.

# INVITE s proxy autentizací

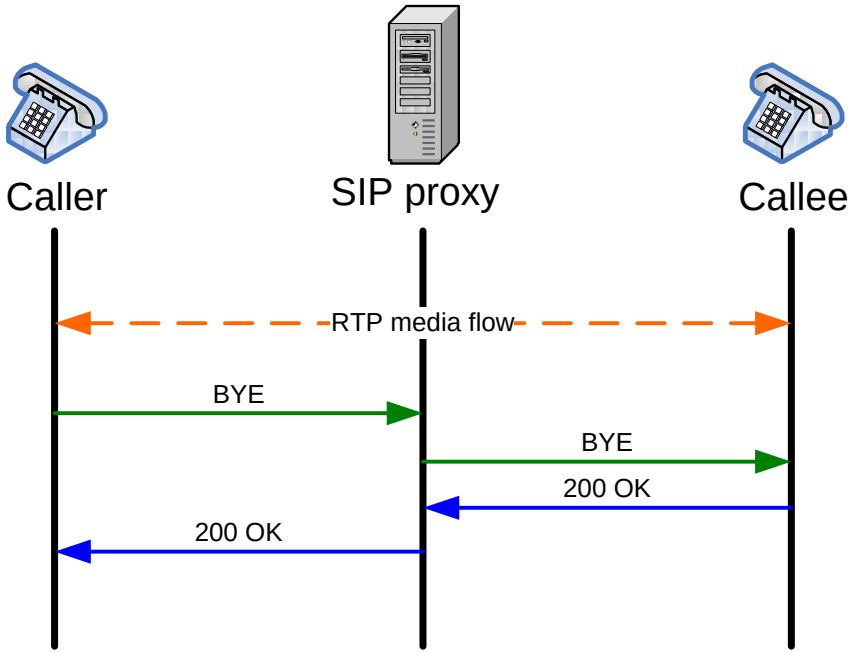


**describes the timer, and the meaning of the timer.**

# Časovače podle RFC3261

| Časovač | Defaultní hodnota | Význam |
|---|---|---|
| T1 | 500 ms | Round-trip time (RTT) – odhad |
| T2 | 4 s. | Maximální interval retransmise |
| T4 | 5 s. | Maximální doba setrvání zprávy v síti |
| Timer A | původní T1 | Interval retransmise žádosti INVITE (UDP) |
| Timer B | 64*T1 | Vypršení transakce INVITE |
| Timer D | > 32 s. pro UDP | Čekání na odpověď retransmisí |
| | 0 s. pro TCP a SCTP | |
| Timer E | původní T1 | Interval retransmise žádostí non-INVITE (UDP) |
| Timer F | 64*T1 | Vypršení transakce non-INVITE |
| Timer G | původní T1 | Interval retransmise odpovědi na INVITE |
| Timer H | 64*T1 | Čekání na příjem ACK |
| Timer I | T4 pro UDP | Čekání na retransmise ACK |
| | 0 s. pro TCP a SCTP | |
| Timer J | 64*T1 pro UDP | Čekání na retransmise non-INVITE žádostí |
| | 0 s. pro TCP a SCTP | |
| Timer K | T4 pro UDP | Čekání na odpověď retransmisí |
| | 0 s. pro TCP a SCTP | |

# Ukončení hovoru pomocí zprávy BYE




- Když chce jeden z uživatelů ukončit hovor, pošle jeho telefon zprávu BYE telefonu druhého uživatele.
- Telefon druhého uživatele potvrzuje ukončení hovoru zprávou 200 OK. Zde připadají v úvahu dvě varianty závisející na tom, zda je či není používán tzv. record-routing mechanizmus.

# Pole Record-route

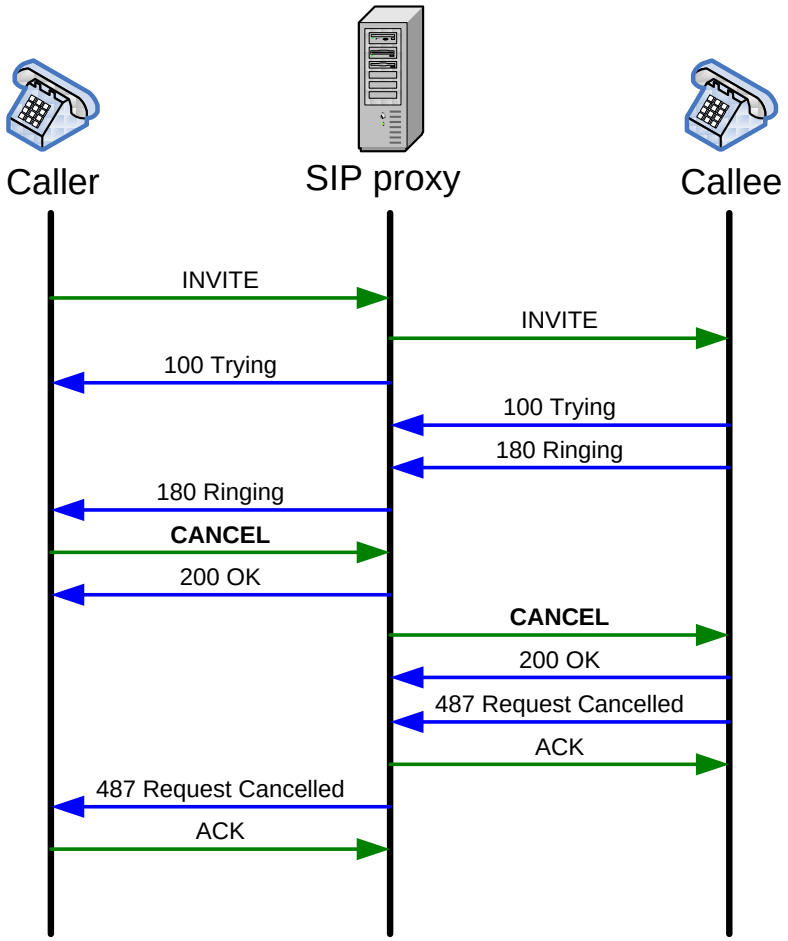
Na předchozím slajdu je zobrazena varianta, kdy zpráva BYE je posílána druhému telefonu opět přes SIP proxy. Toho může být docíleno jednak nastavením telefonu tak, že je vynuceno užití odchozí proxy pro všechny zprávy, popřípadě použitím vnitřního mechanizmu SIP protokolu zvaného record-routing. Ten se používá zejména v případech, kdy potřebujeme zajistit plnou informovanost SIP proxy o stavu volání (plně stavová proxy), což je důležité například pro získání délky doby hovoru (doba mezi průchodem zprávy INVITE a zprávy BYE) pro účely účtování hovorů. Pole Record-route jsou přidávána každou SIP proxy, kterou zpráva INVITE prochází na cestě k telefonu volaného. Záhlaví record-route jsou poté zkopírovány telefonem volaného do odpovědi 200 OK a tato zpráva je zaslána volajícímu. Telefon volajícího transformuje obdržená record-route záhlaví z přijaté zprávy 200 OK na záhlaví Route, která jsou poté umístěna do další zprávy zasílané telefonem volajícího (to může být například právě zpráva BYE).

Při zpracování následujících zpráv, ve kterých jsou nastavena pole Route, SIP proxy používá tato pole pro určení následující SIP proxy, kam mají být zprávy směrovány. Tak je zajištěno, že všechny následné zprávy procházejí stejnou cestou jako původní zpráva INVITE.

# Zrušení hovoru pomocí zprávy CANCEL

- Zpráva CANCEL se používá pro zrušení právě probíhající transakce. Například když volající chce zrušit právě probíhající transakci INVITE (uživatel „vytočil telefonní číslo“, zpráva INVITE již byla odeslána, ale před tím než došlo ke spojení, uživatel se rozhodl hovor zrušit a zavěsil). Telefon v tomto případě pošle zprávu CANCEL se stejnou hodnotou pole Cseq, jaká byla v předchozí zprávě INVITE.
- Transakce INVITE je nyní zrušena.
- Celá situace je zachycena na dalším slajdu.

# CANCEL


Caller
SIP proxy
Callee
INVITE
INVITE
100 Trying
100 Trying
180 Ringing
180 Ringing
CANCEL
200 OK
CANCEL
200 OK
487 Request Cancelled
ACK
487 Request Cancelled
ACK

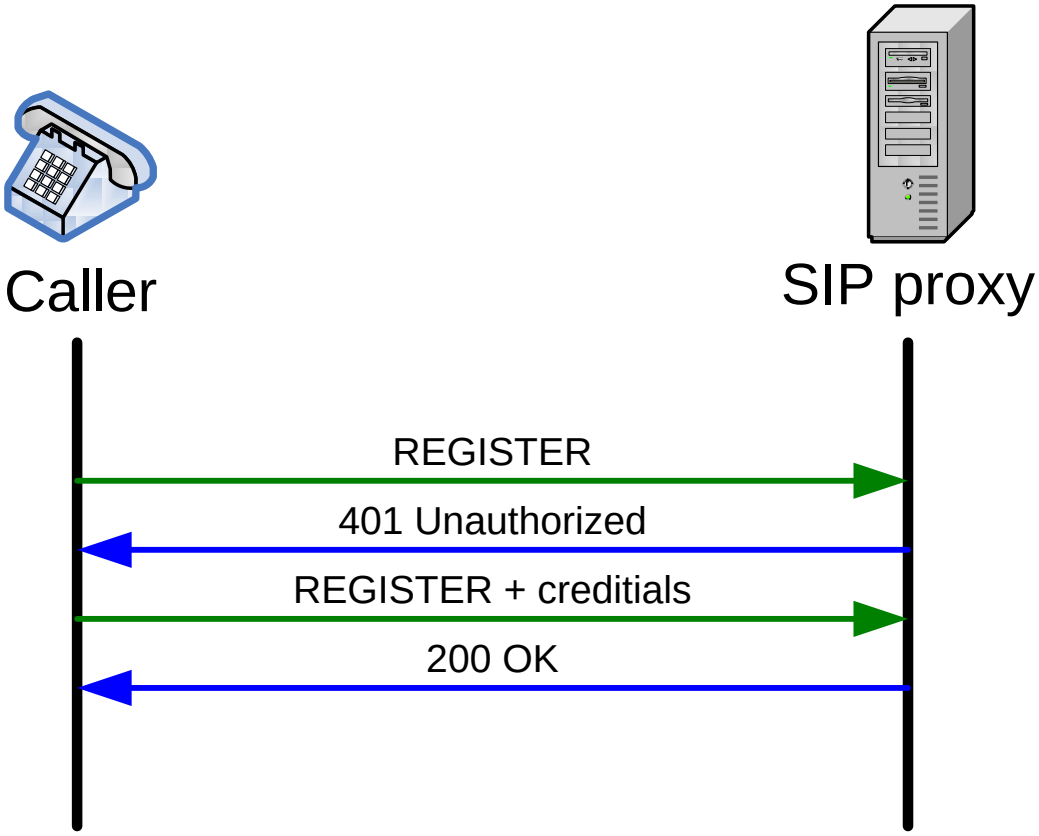
# Zpráva CANCEL s hodnotou pole CSeq

- Na začátku pošle přístroj volajícího zprávu INVITE a tak započne transakci a procedura kontaktování volaného je spuštěna. Nyní volaný chce ukončit probíhající transakci, a proto pošle zprávu CANCEL s hodnotou pole CSeq nastavenou stejně jako v předchozí INVITE zprávě.
- První SIP proxy v cestě odpoví zprávou 200 OK okamžitě poté, co obdrží zprávu CANCEL. Zpráva CANCEL je poté přeposlána volanému.
- Přístroj volaného rovněž odpoví okamžitým odesláním zprávy 200 OK a následně pošle také zprávu 487 Request Cancelled na SIP proxy.
- Proxy potvrdí přijetí zprávy zprávou ACK a přepošle zprávu 487 Request Cancelled volajícímu.
- Přístroj volajícího potvrdí SIP proxy přijetí zprávy zprávou ACK.

# Scénář registrace v případě vyžadované autentizace

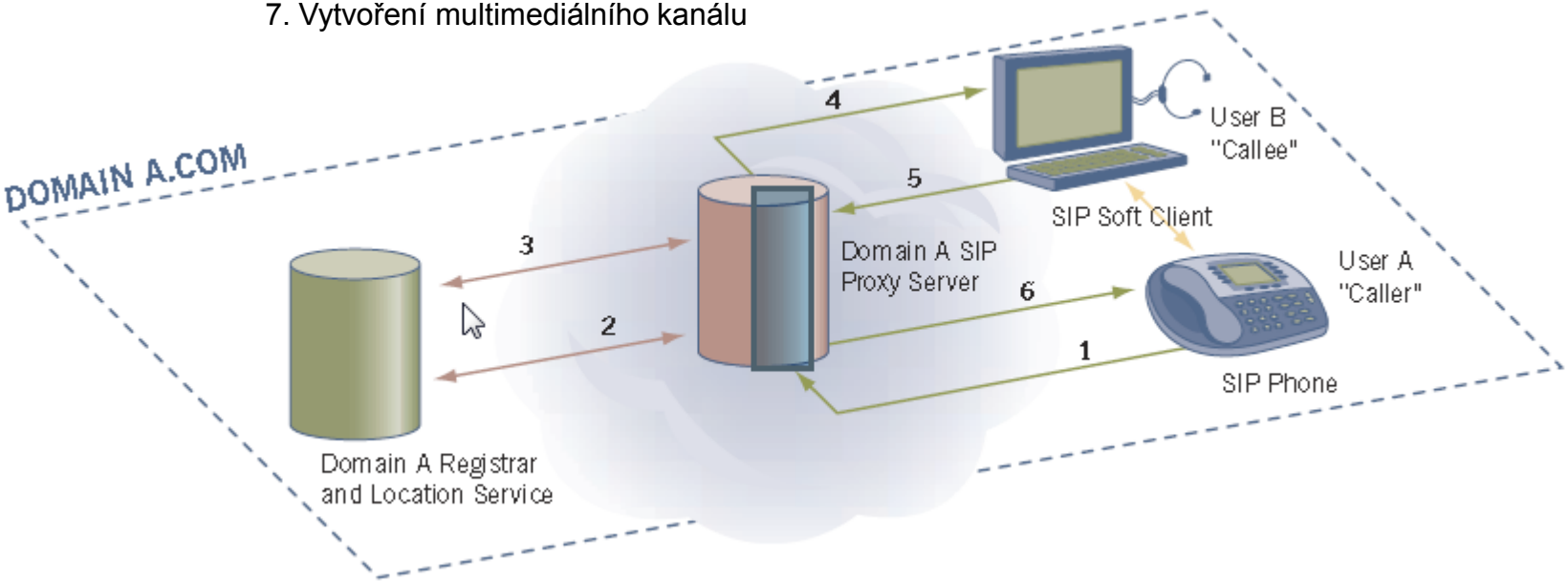
- Nejprve je zaslána zpráva REGISTER se záhlavím Contact a bez jakéhokoliv autentizačního záhlaví.
- Proxy na tuto zprávu reaguje odesláním odpovědi 401 Unauthorized, do níž proxy vloží záhlaví WWW-authenticate s nastavenými hodnotami polí realm a nonce.
- Telefonní přístroj použije přijaté hodnoty polí nonce a realm k vygenerování hodnoty pole Response.
- Poté je na SIP proxy znovu poslána zpráva REGISTER obsahující záhlaví Authorization s poli username, realm, nonce a vygenerovaným polem Response.
- SIP proxy ověří přijaté hodnoty a v případě, že jsou správné, uloží získané kontaktní údaje (pole Contact) do location databáze a odpoví zprávou 200 OK registrovanému přístroji.

# REGISTER

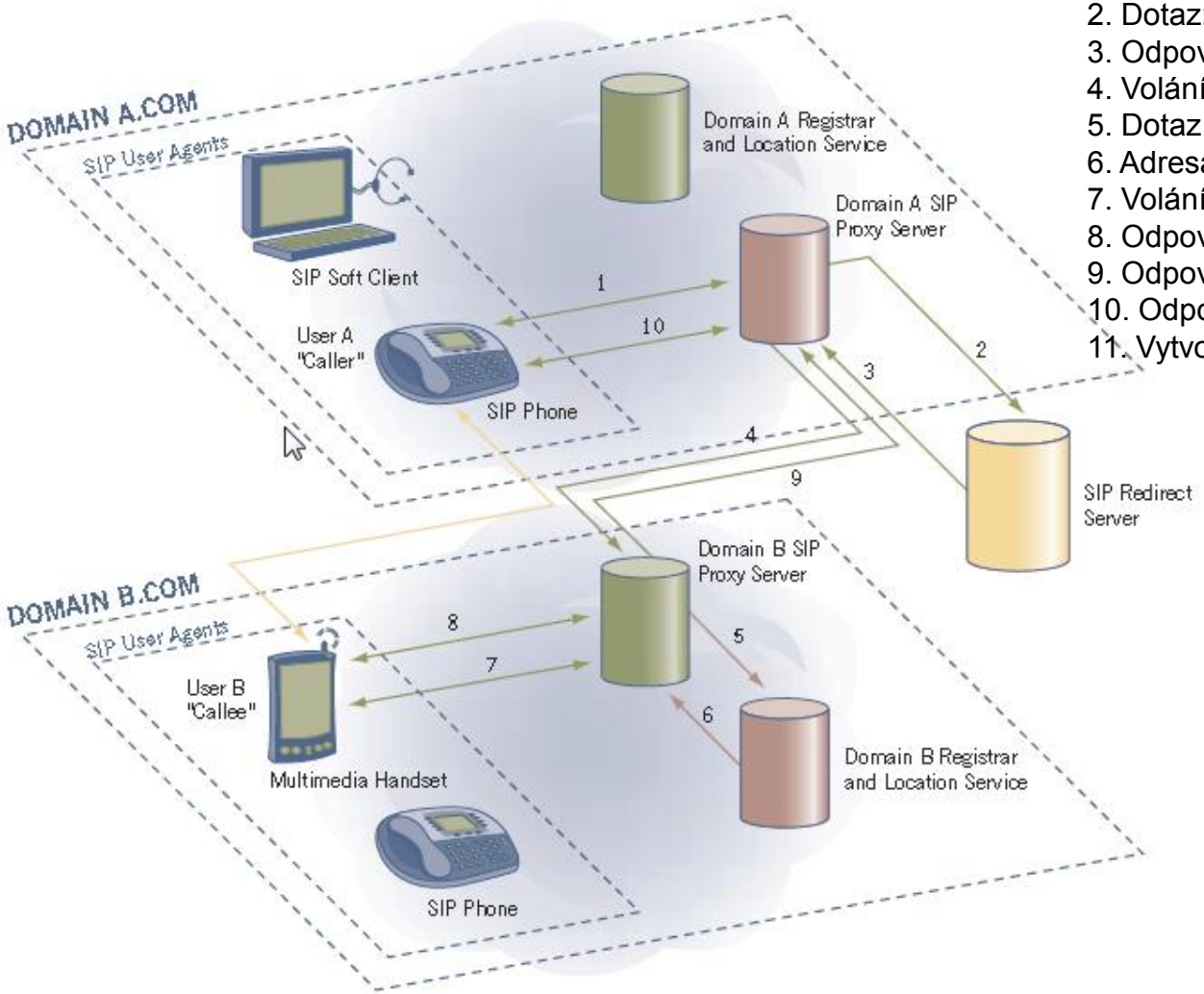

Caller
SIP proxy
REGISTER
401 Unauthorized
REGISTER + creditials
200 OK

# Volání v rámci jedné domény

1. Volání uživatele B
2. Dotaz “Kde je uživatel B?”
3. Odpověď “SIP adresa uživatele B”
4. Volání přes proxy
5. Odpověď
6. Odpověď
7. Vytvoření multimediálního kanálu



# Volání mezi doménami




1. Volání uživatele B
2. Dotaz: Jak se dostanu  k uživateli B v doméně B?“
3. Odpověď „Adresa řadiče proxy domény“
4. Volání přes proxy na proxy domény B
5. Dotaz „Kde je uživatel B?“?”
6. Adresa uživatele B
7. Volání zprostředkované přes proxy
8. Odpověď
9. Odpověď
10. Odpověď
11. Vytvoření multimediálního kanálu

# 3. Bezpečnostní otázky

# Bezpečnostní mechanismy protokolu SIP

- HTTP Digest
- S/MIME
- TLS
- IPSec s ručně nastavenými klíči
- IPSec s IKE
- MIKEY

# SIP HTTP autentizace

- Vychází z RFC 2617. Jde o jednoduchou autentizaci typu dotaz-odpověď, kde odpověď tvoří:
  - kontrolní suma uživatelova jména (defaultně MD5)
  - heslo
  - hodnota nonce
  - http metoda a požadované URI (Uniform Resource Identifier).
- Heslo je přenášeno v zašifrované podobě, přesto tato metoda autentizace není v současnosti doporučovaná.

# S/MIME

- Další autentizační metodou použitou v SIPu je S/MIME
- Již samotný MIME (Multipurpose Internet Mail Extensions) používá metody pro kontrolu integrity a šifrování
- S/MIME je doplňuje o takové mechanismy jako je distribuce veřejných klíčů a autentizace
- V RFC 3261 je doporučeno pro UA

# TLS

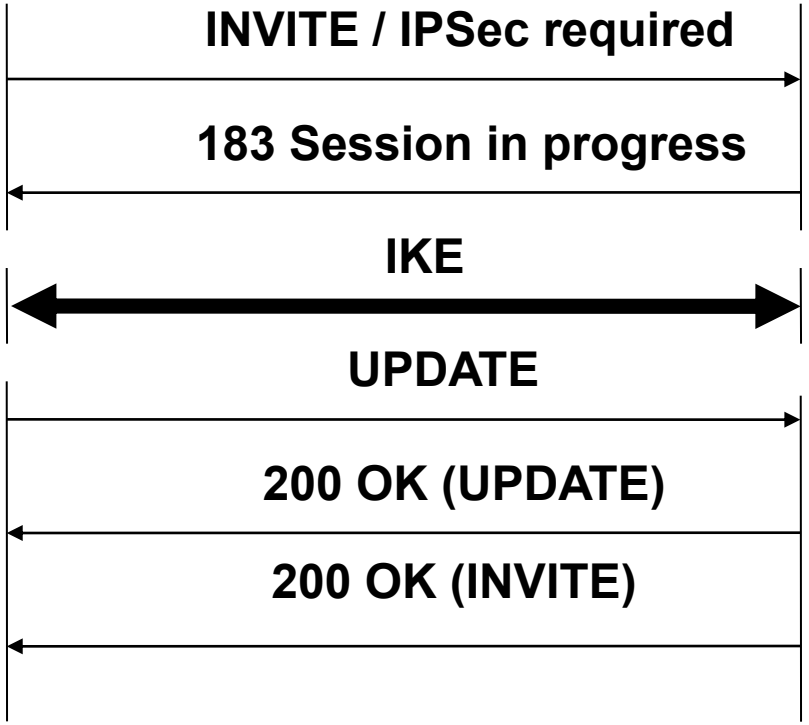
- Pro ochranu SIP signalizace mezi UA a proxy, redirect serverem a register serverem je v RFC 3261 doporučen protokol TLS. Tento protokol umožňuje
  - kontrolu integrity
  - zajištění důvěrnosti
  - ochranu proti přehrávání
  - integrovaný management klíčů se vzájemnou autentizací a jejich bezpečnou distribucí
- Předpokládá se použití metodou skoku (hop-by-hop) mezi UA a proxy resp. mezi dvěma proxy
- Stinnou stránkou použití TLS je nutnost použít spolehlivý transportní mechanismus (SIP signalizaci na bázi TCP), UDP použít nelze

# IPSec s ručně nastavenými klíči

- Na síťové vrstvě lze využít mechanismu IPSec, který slouží k zajištění
  - autenticity
  - integrity
  - důvěrnosti
  - proti přehrávání
- Scénáře mohou být typu hop-by-hop i end-to-end.
- IPSec zatím nemá definovanou kryptosadu pro SIP.

# IPSec s IKE integrovaným do SDP

Internet Key Exchange (IKE nebo IKEv2) vytváří bezpečnostní asociace

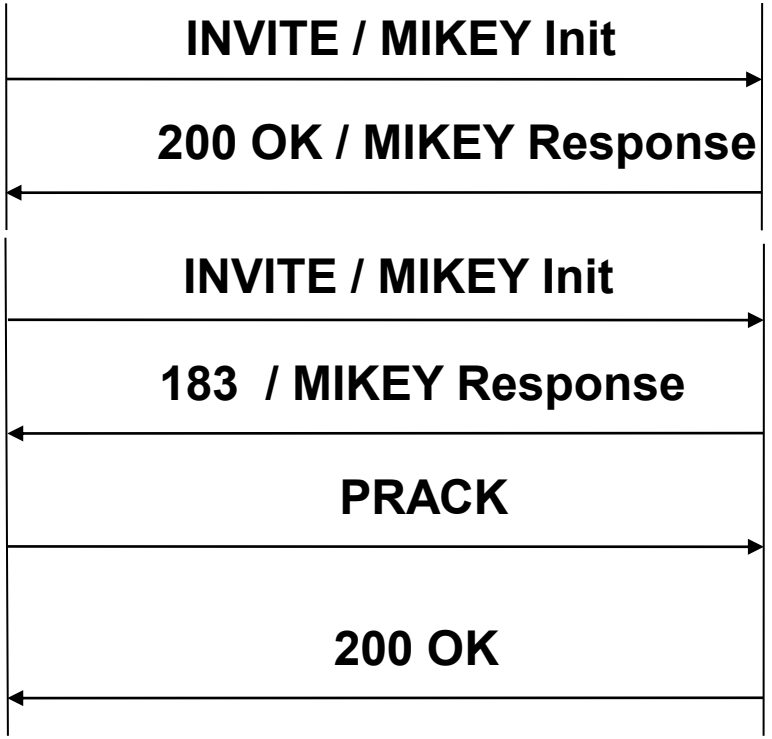


# MIKEY

Může být

- v MIME
- v SDP

```
a=crypto:<tag> <cryptosuite>
<keyparams>[<sessionparams>]
```




PRACK – Provisional ACK

# Problém s NAT

Problémy jsou zde obdobné jako u protokolu H.323 vyjma toho, že navázání spojení a analýza záhlaví jsou zde mnohem jednodušší.

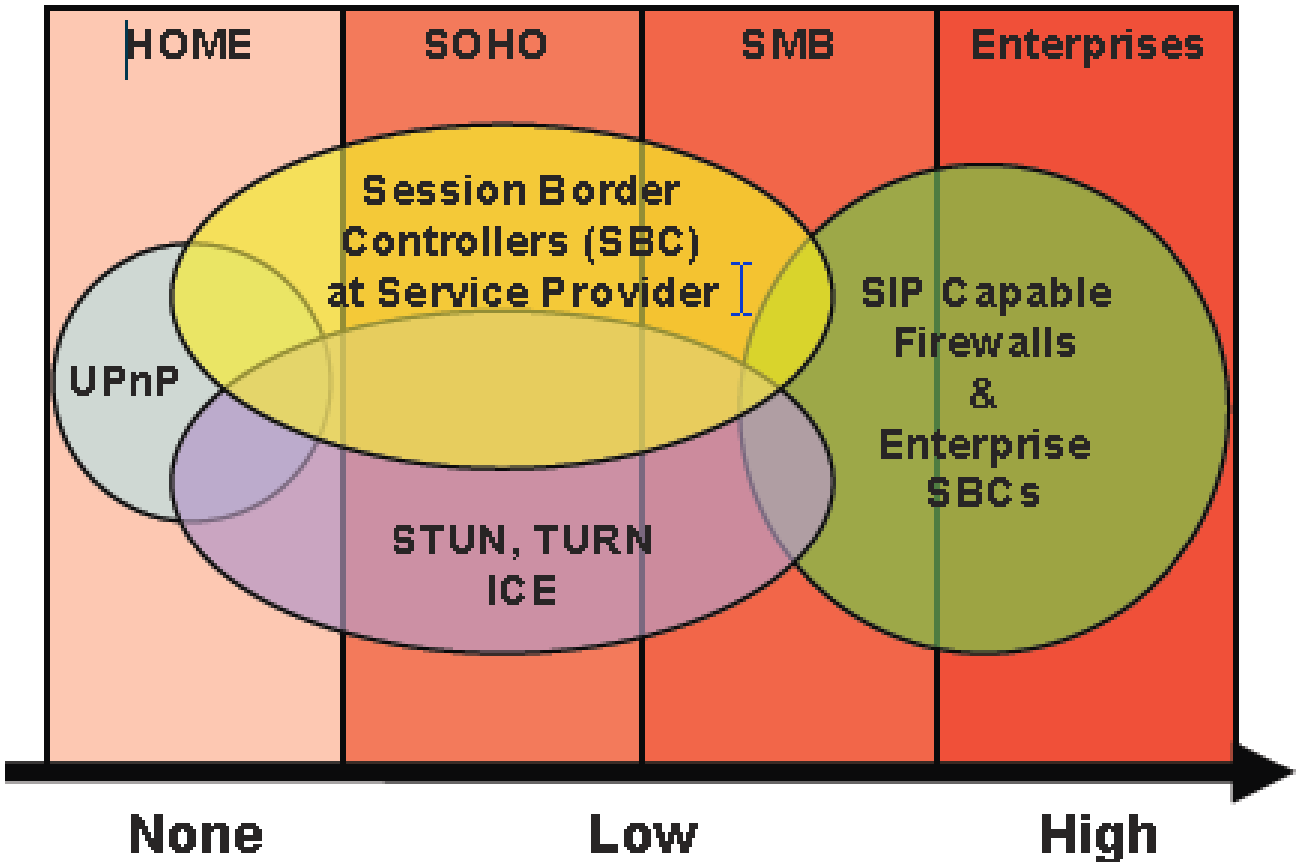
Velký problém je právě s NAT. Otázkou je, kde je umístěno proxy:

- uvnitř vnitřní sítě (v rámci lokální LAN);
- v rámci vnější sítě a z vnitřní sítě se je třeba k němu přihlašovat;
- dvě administrativní domény jsou spolu propojeny, každá má vlastní proxy.

Nejnepříjemnější situace je ta druhá uvedená, kdy se uživatel přihlašuje z vnitřní sítě k proxy ve vnější síti. Jeho privátní IP adresa je z privátní sítě (např. 10.1.1.100) a přichází k proxy v příkazu INVITE spolu s jeho SIP adresou (např. pepa@unob.cz). Odpověď OK pak nenalezne příjemce. Možným řešením je použití transportního protokolu TCP anebo protokolu STUN. A nejlepším řešením je NAT vůbec pokud možno nepoužívat – což je i jeden z argumentů pro přechod na IPv6.

# Kdy STUN a kdy firewall?

STUN – Simple traversal of UDP through NATs



# RFC3489

Obsoleted by: 5389 PROPOSED STANDARD

Network Working Group
Request for Comments: 3489
Category: Standards Track

J. Rosenberg
J. Weinberger
dynamicsoft
C. Huitema
Microsoft
R. Mahy
Cisco
March 2003

**STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)**

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN) is a lightweight protocol that allows applications to discover the presence and types of NATs and firewalls between them and the public Internet. It also provides the ability for applications to determine the public Internet Protocol

# RFC5389

Network Working Group
Request for Comments: 5389
Obsoletes: 3489
Category: Standards Track

J. Rosenberg
Cisco
R. Mahy
P. Matthews
Unaffiliated
D. Wing
Cisco
October 2008

**Session Traversal Utilities for NAT (STUN)**

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

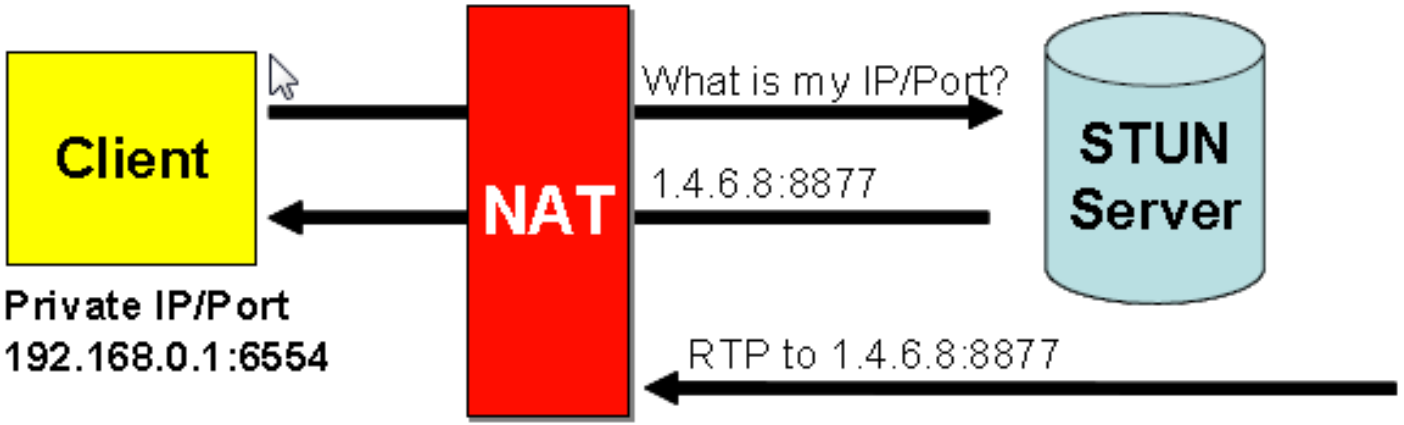
Abstract

Session Traversal Utilities for NAT (STUN) is a protocol that serves as a tool for other protocols in dealing with Network Address Translator (NAT) traversal. It can be used by an endpoint to determine the IP address and port allocated to it by a NAT. It can also be used to check connectivity between two endpoints, and as a keep-alive protocol to maintain NAT bindings. STUN works with many existing NATs, and does not require any special behavior from them.

STUN is not a NAT traversal solution by itself. Rather, it is a tool to be used in the context of a NAT traversal solution. This is an important change from the previous version of this specification (RFC 3489), which presented STUN as a complete solution.

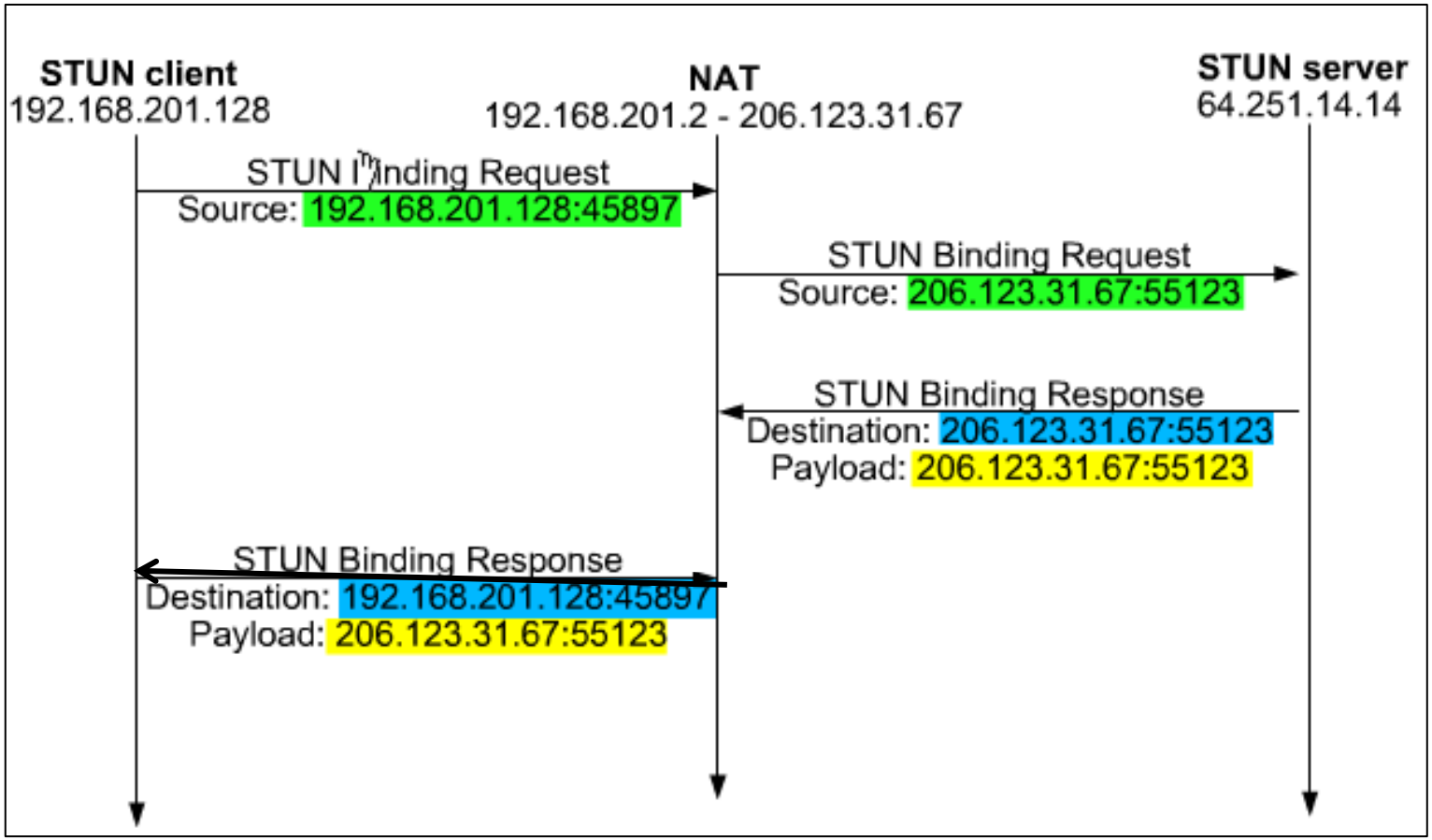
# *STUN*
## *(Simple/Session Traversal of UDP through NATs)*

- Dvojice adres „server-reflexivní“
- Obvykle u ISP jako služba
- STUN2 xoruje k adrese nonce
- Klient je cloněn pouze nepříliš bezpečným NAT a je vystaven útokům kohokoliv, kdo odchytá STUN provoz
- Nezajišťuje symetrický NAT, kdy mezi unikátními IP adresami a porty odesilatele a příjemce misí být unikátní i dvojice na NATu (jen pro ně).



# Příklad

**Klient: Jako co mě vidíš? Server: Vidím tě jako 206.123.31.67:55123**



# draft-rosenberg-midcom-turn-08

MIDCOM
Internet-Draft
Expires: March 13, 2006

J. Rosenberg
Cisco Systems
R. Mahy
Airspace
C. Huitema
Microsoft
September 9, 2005

**Traversal Using Relay NAT (TURN)**
**draft-rosenberg-midcom-turn-08**

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

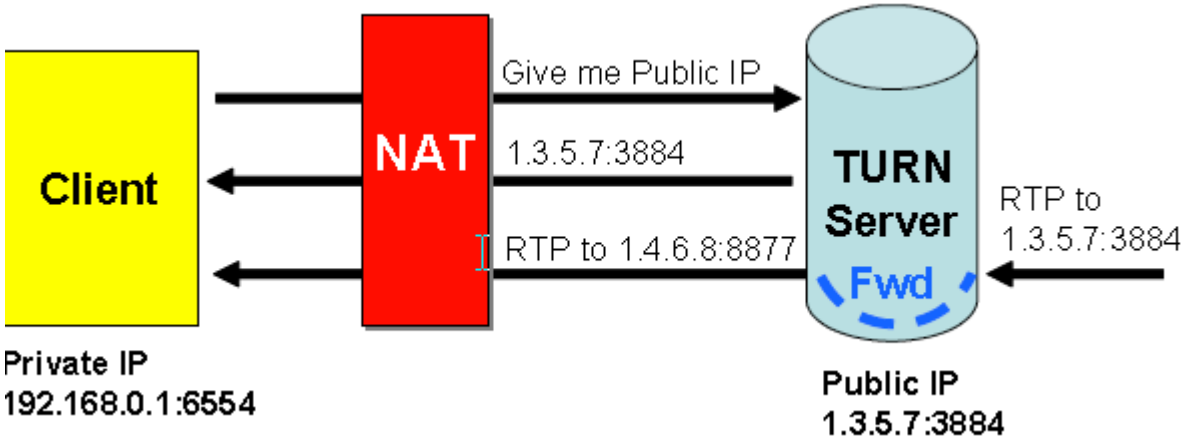
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

# TURN
## *(Traversal Using Relay NAT)*

- Metoda náročná na šířku pásma
- Server musí být blízko NATu a k dispozici po celou dobu komunikace
- Zajišťuje symetrický NAT

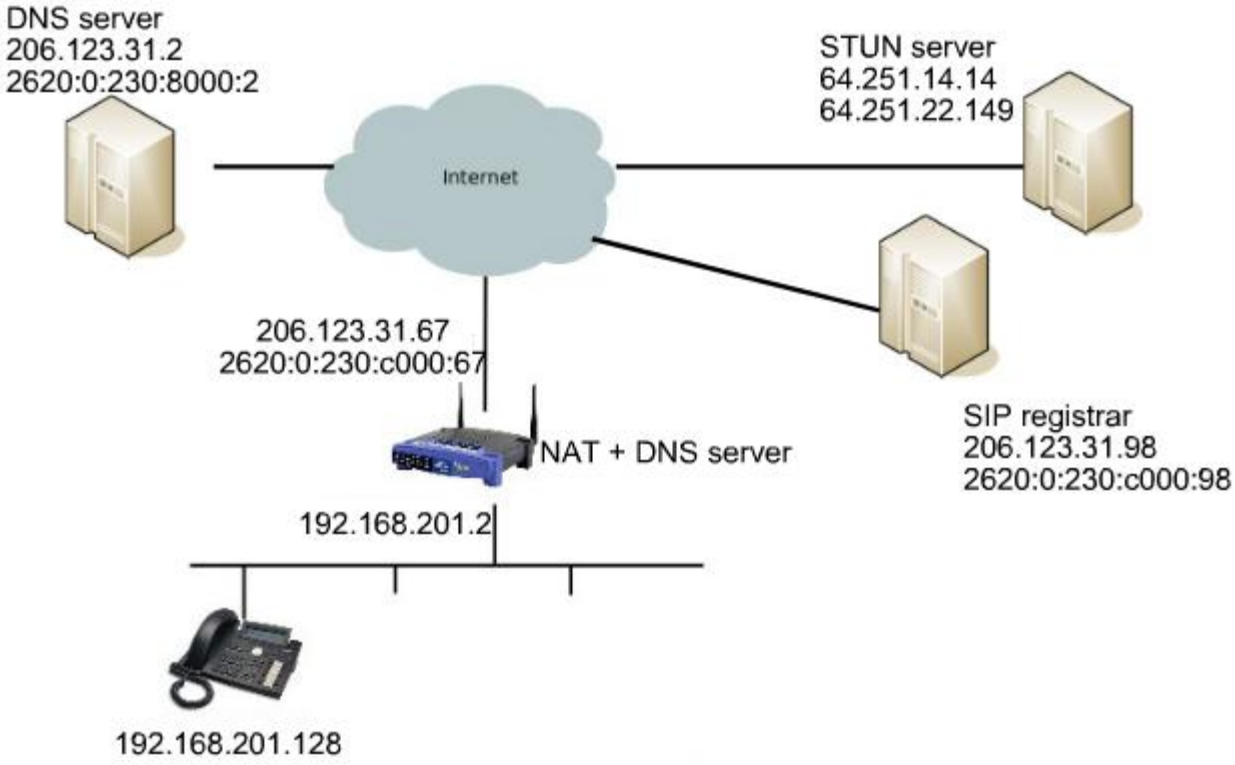


# TURN je součást migrace do IPv6

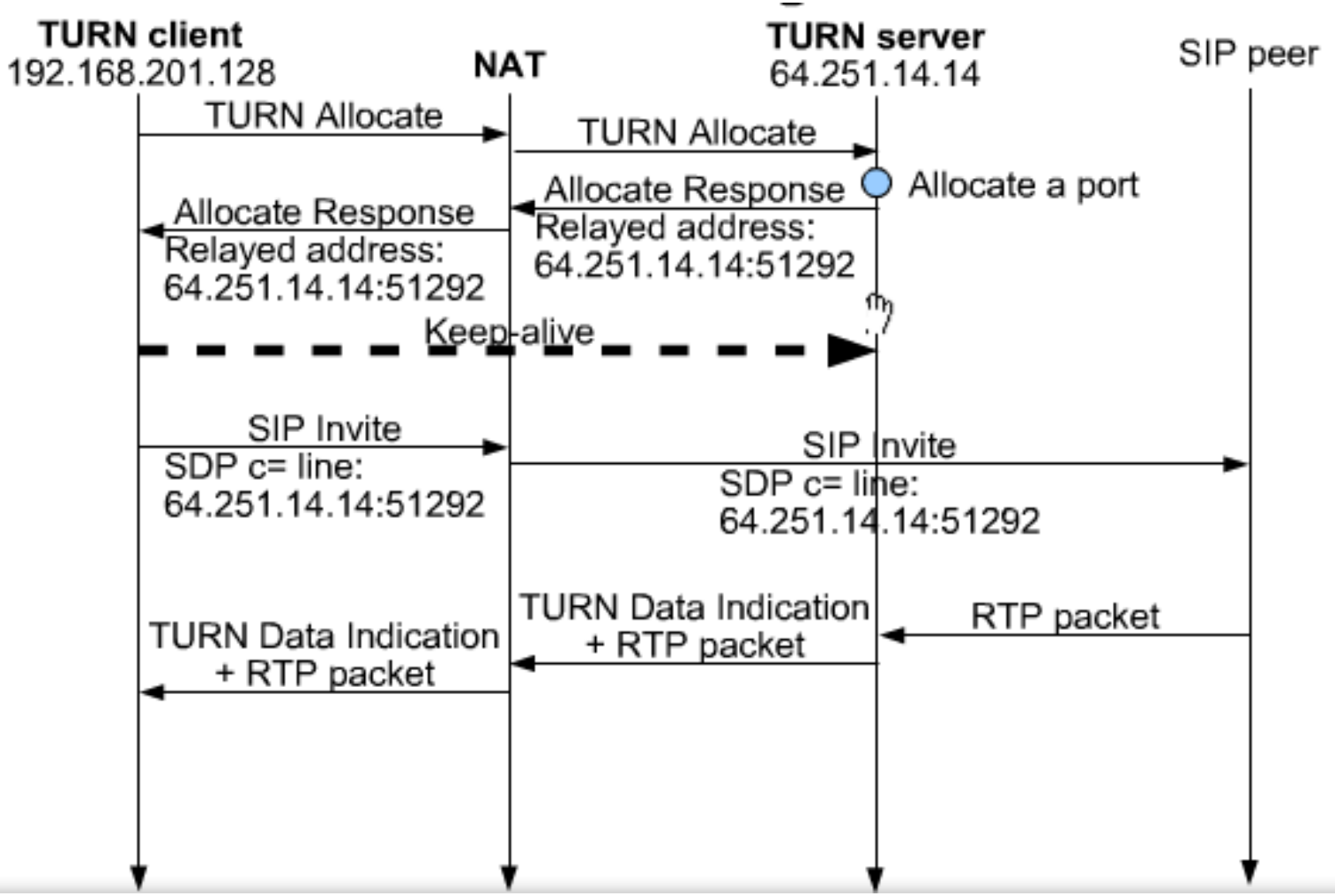
BEHAVE
Internet-Draft
Intended status: Standards Track
Expires: January 9, 2011

G. Camarillo
O. Novo
Ericsson
S. Perreault, Ed.
Viagenie
July 8, 2010

**Traversal Using Relays around NAT (TURN) Extension for IPv6**
**draft-ietf-behave-turn-ipv6-11**



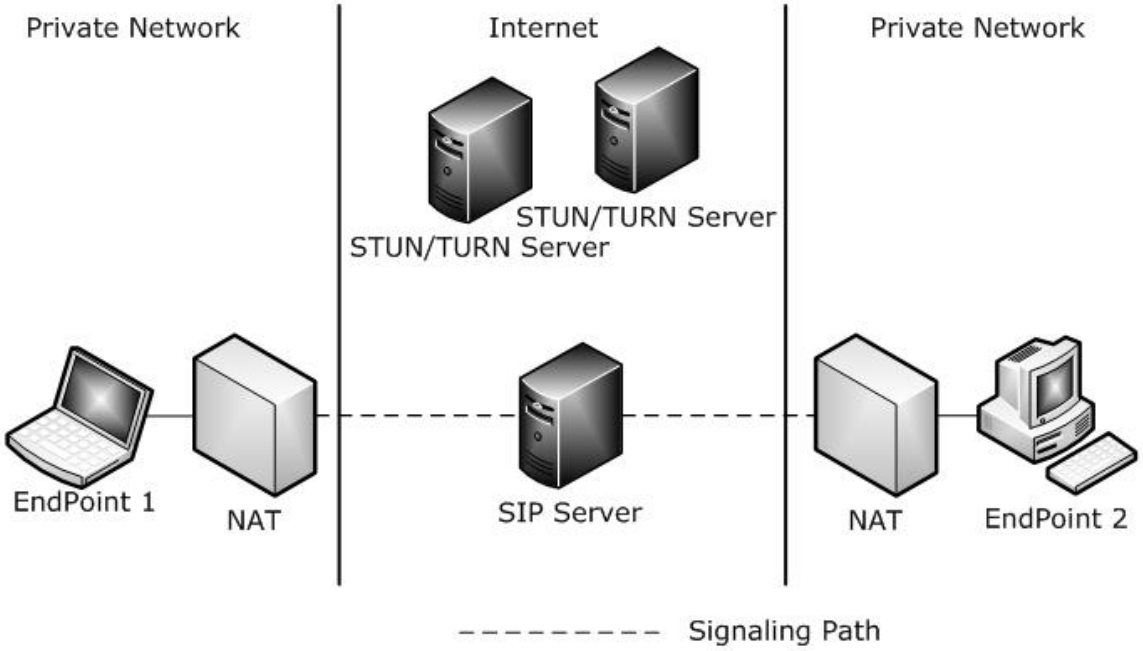
# Příklad


TURN client
192.168.201.128
NAT
TURN server
64.251.14.14
SIP peer
TURN Allocate
TURN Allocate
Allocate Response
Allocate a port
Allocate Response
Relayed address:
64.251.14.14:51292
Relayed address:
64.251.14.14:51292
Keep-alive
SIP Invite
SDP c= line:
64.251.14.14:51292
SIP Invite
SDP c= line:
64.251.14.14:51292
TURN Data Indication
+ RTP packet
RTP packet
TURN Data Indication
+ RTP packet

# ICE
# (Interactive Connectivity Establishment)

- Využívá STUN i TURN podle nastavené priority
- Zprostředkovává je volanému prostřednictvím CDP
- Po navázání spojení zastaví jejich použití

Microsoft Office Communications Server 2007 R2, A/V Edge Server
je rozšířen o STUN/TURN, blíže Mike Atkins v „Troubleshoot STUN with TURN
in Office Communications Server 2007 R2“ v http://blogs.technet.com z prosince 2010



# Microsoft ICE z roku 2008 – 1. krok

## *Klient posílá požadavek na STUN/TURN server*

Klient STUN posílá *TURN Allocation request* na A/V Edge Server

```
Frame: Number = 473, Captured Frame Length = 138, MediaType = ETHERNET
+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-02-B3-DC-7D-7E],SourceAddress:[00-25-64-05-2D-
AD]
+ Ipv4:Src = 65.53.10.25, Dest = 65.53.10.100, Next Protocol = UDP, Packet ID = 7768, Total IP Length = 124
+ Udp: SrcPort = 62826, DstPort = 3478, Length = 104
- TURN: TURN:Allocate Request
  + MessageHeader: TURN:Allocate Request, TransactionID = 0x2112a4425ccd0c8a916db536d408efa1
  - MagicCookie: 0x72c64bc6
    AttributeType: Magic Cookie
    AttributeLength: 4 (0x4)
    MagicCookie: 1925598150 (0x72C64BC6)
  + UndefineAttribute:
  - UserName: Username
    AttributeType: Username
    AttributeLength: 56 (0x38)
    UserName: Binary Large Object (56 Bytes)
```

Záznam: Microsoft Network Monitor 3.4

# 2. krok

## *Odpověď STUN/TURN serveru*

```
Frame: Number = 475, Captured Frame Length = 185, MediaType = ETHERNET
+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-25-64-05-2D-AD],SourceAddress:[00-02-B3-DC-7D-7E]
+ Ipv4:Src = 65.53.10.100, Dest = 65.53.10.25, Next Protocol = UDP, Packet ID = 968, Total IP Length = 171
+ Udp: SrcPort = 3478, DstPort = 62826, Length = 151
- TURN: TURN:Allocate Error Response
 + MessageHeader: TURN:Allocate Error Response, TransactionID = 0x2112a4425ccd0c8a916db536d408efa1
 - MagicCookie: 0x72c64bc6
   AttributeType: Magic Cookie
   AttributeLength: 4 (0x4)
   MagicCookie: 1925598150 (0x72C64BC6)
 - ErrorCode: Number = 1, The request did not contain a Message-Integrity attribute
   AttributeType: Error Code
   AttributeLength: 61 (0x3D)
   Reserved: 0 (0x0)
   Class: 4 (0x4)
   Number: 1 (0x1)
   ReasonPhrase: The request did not contain a Message-Integrity attribute
 - AlternateServer: 65.53.10.100:3478
   AttributeType: Alternate Server
   AttributeLength: 8 (0x8)
   Reserved: 0 (0x0)
   Family: IP (IP version 4)
   Port: 3478 (0xD96)
   IPV4Address: 65.53.10.100
 - Nonce: 0xb537075f2b21005b2330f4846ccde6b189e89a83
   AttributeType: Nonce
   AttributeLength: 20 (0x14)
   Nonce: Binary Large Object (20 Bytes)
 - Realm: 0x227274636d6564696122
   AttributeType: Realm
   AttributeLength: 10 (0xA)
   Realm: Binary Large Object (10 Bytes)
```

# 3. krok

## *Výpočet MI a její odeslání na STUN/TURN server*


Message-Integrity = MD5(username ":" realm ":" SASLPrep(password))

kde SASL (Simple Authentication and Security Layer) je obecná metoda ověřování v protokolech klient/server
SASLprep – reprezentace jmen a hesel pro SASL - viz RFC 4013

# 4. krok

## Server STUN/TURN odpovídá vzdálenému klientu

- Server STUN/TURN odesílá paket Allocate Response, v ní hodnotu časovače, šířky pásma…
- XORMappedAddress je počítána XORem z MagicCookie z 1. kroku

```
Frame: Number = 489, Captured Frame Length = 162, MediaType = ETHERNET
+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-25-64-05-2D-AD],SourceAddress:[00-02-B3-DC-7D-
7E]
+ Ipv4:Src = 65.53.10.100, Dest = 65.53.10.25, Next Protocol = UDP, Packet ID = 975, Total IP Length = 148
+ Udp: SrcPort = 3478, DstPort = 62825, Length = 128
- TURN: TURN:Allocate Response
 + MessageHeader: TURN:Allocate Response, TransactionID = 0x2112a4428e070a2a03ba024faac51e83
 - MagicCookie: 0x72c64bc6
   AttributeType: Magic Cookie
   AttributeLength: 4 (0x4)
   MagicCookie: 1925598150 (0x72C64BC6)
 + Lifetime: 60
 + Bandwidth: 750
 - MappedAddress: 65.53.10.100:58688
   AttributeType: Mapped Address
   AttributeLength: 8 (0x8)
   Reserved: 0 (0x0)
   Family: IP (IP version 4)
   Port: 58688 (0xE540)
   IPV4Address: 65.53.10.100
 - XORMappedAddress: 96.39.174.91:54395
   AttributeType: XOR Mapped Address
   AttributeLength: 8 (0x8)
   Reserved: 0 (0x0)
   Family: IP (IP version 4)
   XPort: 54395 (0xD47B)
   IPV4XAddress: 96.39.174.91
 + UndefineAttribute:
 + MessageIntegrity: HMACSHA1Hash = 0x3976cdb6d5d551f7bfbd9524e61fb21ac0ff447c
```

# Rok 2010: Cisco s RFC5898

PROPOSED STANDARD

Internet Engineering Task Force (IETF)
Request for Comments: 5898
Category: Standards Track
ISSN: 2070-1721

F. Andreasen
Cisco Systems
G. Camarillo
Ericsson
D. Oran
D. Wing
Cisco Systems

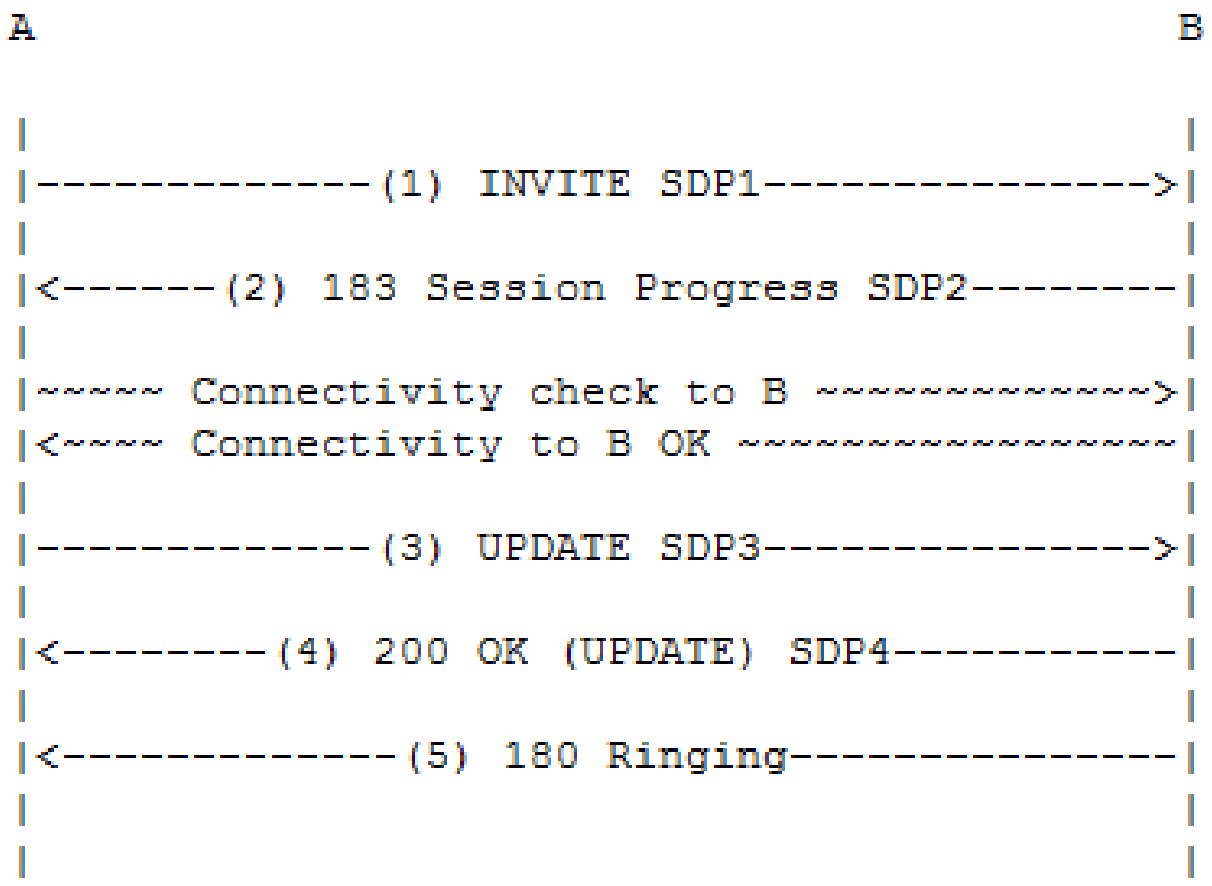
July 2010

**Connectivity Preconditions for Session Description Protocol (SDP) Media Streams**

Abstract

This document defines a new connectivity precondition for the Session Description Protocol (SDP) precondition framework. A connectivity precondition can be used to delay session establishment or modification until media stream connectivity has been successfully verified. The method of verification may vary depending on the type of transport used for the media. For unreliable datagram transports such as UDP, verification involves probing the stream with data or control packets. For reliable connection-oriented transports such as TCP, verification can be achieved simply by successful connection establishment or by probing the connection with data or control packets, depending on the situation.

# Navazování spojení s kontrolou na použití ICE



# INVITE SDP1

Pohled stanice A

| Direction | Current | Desired Strength | Confirm |
|---|---|---|---|
| send | no | mandatory | no |
| recv | no | mandatory | no |

```
a=ice-pwd:asd88fgpdd777uzjYhagZg
a=ice-ufrag:8hhY
m=audio 20000 RTP/AVP 0
c=IN IP4 192.0.2.1
a=rtcp:20001
a=curr:conn e2e none
a=des:conn mandatory e2e sendrecv (nabídka)
a=candidate:1 1 UDP 2130706431 192.0.2.1 20000 typ host
```

# Session Progress SDP2

Pohled stanice B

| Direction | Current | Desired Strength | Confirm |
|---|---|---|---|
| send | no | mandatory | no |
| recv | no | mandatory | no |

```
a=ice-lite
a=ice-pwd:qrCA8800133321zF9AIj98
a=ice-ufrag:H92p m=audio 30000 RTP/AVP 0
c=IN IP4 192.0.2.4
a=rtcp:30001
a=curr:conn e2e none
a=des:conn mandatory e2e sendrecv
a=conf:conn e2e send (chce potvrzení ve směru send)
a=candidate:1 1 UDP 2130706431 192.0.2.4 30000 typ host
```

# UPDATE SDP3

Pohled stanice A po kontrole konektivity

Zkontroloval konektivitu ICE k B v obou směrech

| Direction | Current | Desired Strength | Confirm |
|---|---|---|---|
| send | yes | mandatory | no |
| recv | yes | mandatory | yes |

Pohled stanice B po kontrole konektivity

| Direction | Current | Desired Strength | Confirm |
|---|---|---|---|
| send | no | mandatory | no |
| recv | yes | mandatory | no |

```
a=ice-pwd:asd88fgpdd777uzjYhagZg
a=ice-ufrag:8hhY
m=audio 20000 RTP/AVP 0
c=IN IP4 192.0.2.1
a=rtcp:20001
a=curr:conn e2e sendrecv
a=des:conn mandatory e2e sendrecv
a=candidate:1 1 UDP 2130706431 192.0.2.1 20000 typ host
```

Pohled stanice B po UPDATE

| Direction | Current | Desired Strength | Confirm |
|---|---|---|---|
| send | yes | mandatory | no |
| recv | yes | mandatory | no |

# Útoky na SIP proxies

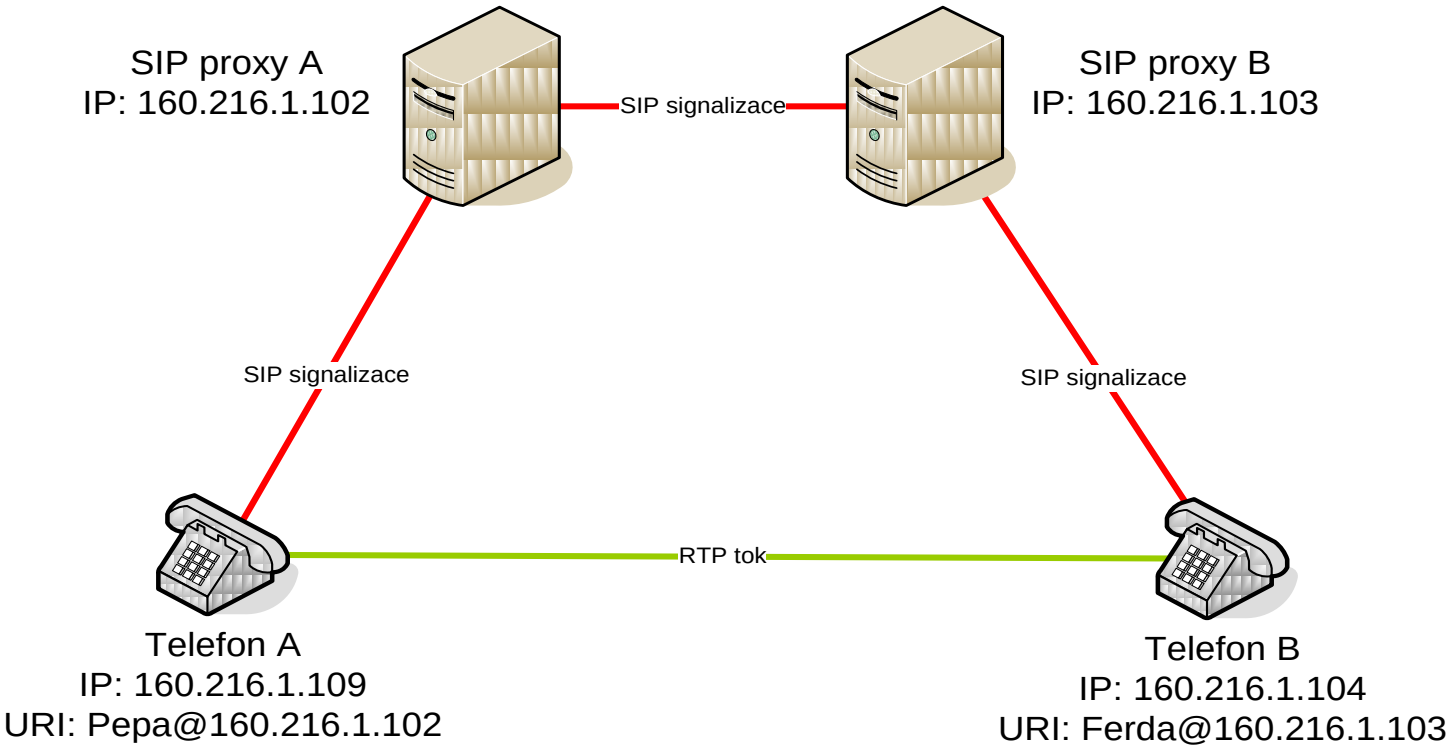
Útoky na protokolovou sadu TCP/IP

Např. Ping of Death, SYN Flood, Smurf…

Útoky využívající specifické slabiny protokolu SIP

Např. přerušením relací…

# Testování možnosti registrovat útoky



# Test v SNORT na útok SYN Flood

```
alert tcp any any -> $SIP_PROXY_IP any \
(msg: "TCP SYN packet flooding from single source"; \
threshold: type both, track by_src, count 200, seconds 20; \
flow:stateless; flags:S,12; sid:5000100; rev:1;)
```

# SNORT log

```
[1:5000001:1] TCP SYN packet flooding from single source [**]
[Priority: 0] {TCP} 160.216.1.102:1653 -> 160.216.1.103:506011/10-17:22:18.980228  [**]
[1:5000002:1] TCP SYN packet flooding (simple or distributed) [**]
[Priority: 0] {TCP} 143.110.215.175:3957 -> 160.216.1.103:506011/10-17:23:18.000308  [**]
[1:5000002:1] TCP SYN packet flooding (simple or distributed) [**]
[Priority: 0] {TCP} 151.170.194.143:11334 -> 160.216.1.103:506011/10-17:23:32.253141  [**]
[1:5000004:1] INVITE message flooding [**]
[Priority: 0] {UDP} 160.216.1.102:3069 -> 160.216.1.103:506011/10-17:23:35.037319  [**]
[1:5000005:1] REGISTER message flooding [**]
[Priority: 0] {UDP} 160.216.1.102:2002 -> 160.216.1.103:506011/10-17:24:14.483933  [**]
[1:5000007:1] TCP/IP message flooding directed to SIP proxy [**]
[Priority: 0] {UDP} 160.216.1.102:7777 -> 160.216.1.103:506011/10-17:24:40.652745  [**]
[1:5000008:1] DNS No such name threshold. Abnormaly high count of No such name responses.[**
[Priority: 0] {UDP} 160.216.40.10:53 -> 160.216.1.103:105411/10-17:24:54.120039  [**]
[1:5000011:1] SQL Injection. Injection of DROP statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:55.220988  [**]
[1:5000012:1] SQL Injection. Injection of DELETE statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:56.265353  [**]
[1:5000013:1] SQL Injection. Injection of SELECT statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:57.390944  [**]
[1:5000014:1] SQL Injection. Injection of INSERT statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:58.397378  [**]
[1:5000015:1] SQL Injection. Injection of UPDATE statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:58.994778  [**]
[1:5000016:1] SQL Injection. Injection of UNION statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:5060
```

# Zpráva INVITE

```
RECEIVE TIME: 10913072
RECEIVE << 160.216.1.102:5060
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 160.216.223.122:5060;rport=5060;
branch=z9hG4bKE0BCCD41AF0648378E3200A1924B454D
From: Pepa <sip:pepa@160.216.1.102>;tag=2110609961
To: <sip:ferda@160.216.1.103>;tag=1461585288
Contact: <sip:ferda@160.216.1.103:5060>
Record-Route: <sip:160.216.1.103;ftag=2110609961;lr=on>
Call-ID: 2F56AA96-23FD-4F06-8706-BF2866B97772@160.216.1.103
CSeq: 18188 INVITE
Server: SIPphone Lite release 1104v
Content-Length: 0
```

# Test na útok INVITE Flood

```
alert ip any any -> $SIP_PROXY_IP $SIP_PROXY_PORTS \
(msg:"INVITE message flooding"; content:"INVITE"; depth:6; \
threshold: type both, track by_src, count 200, seconds 60; \
sid:1000100; rev:1;)

#Suppresion of alerting for known proxy 160.216.1.102
suppress gen_id 1, sig_id 1000100, track by_src, ip
160.216.1.103
```

# SNORT log podruhé

```
[1:5000001:1] TCP SYN packet flooding from single source [**]
[Priority: 0] {TCP} 160.216.1.102:1653 -> 160.216.1.103:506011/10-17:22:18.980228  [**]
[1:5000002:1] TCP SYN packet flooding (simple or distributed) [**]
[Priority: 0] {TCP} 143.110.215.175:3957 -> 160.216.1.103:506011/10-17:23:18.000308  [**]
[1:5000002:1] TCP SYN packet flooding (simple or distributed) [**]
[Priority: 0] {TCP} 151.170.194.143:11334 -> 160.216.1.103:506011/10-17:23:32.253141  [**]
[1:5000004:1] INVITE message flooding [**]
[Priority: 0] {UDP} 160.216.1.102:3069 -> 160.216.1.103:506011/10-17:23:35.037319  [**]
[1:5000005:1] REGISTER message flooding [**]
[Priority: 0] {UDP} 160.216.1.102:2002 -> 160.216.1.103:506011/10-17:24:14.483933  [**]
[1:5000007:1] TCP/IP message flooding directed to SIP proxy [**]
[Priority: 0] {UDP} 160.216.1.102:7777 -> 160.216.1.103:506011/10-17:24:40.652745  [**]
[1:5000008:1] DNS No such name threshold. Abnormaly high count of No such name responses.
[Priority: 0] {UDP} 160.216.40.10:53 -> 160.216.1.103:105411/10-17:24:54.120039  [**]
[1:5000011:1] SQL Injection. Injection of DROP statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:55.220988  [**]
[1:5000012:1] SQL Injection. Injection of DELETE statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:56.265353  [**]
[1:5000013:1] SQL Injection. Injection of SELECT statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:57.390944  [**]
[1:5000014:1] SQL Injection. Injection of INSERT statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:58.397378  [**]
[1:5000015:1] SQL Injection. Injection of UPDATE statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:58.994778  [**]
[1:5000016:1] SQL Injection. Injection of UNION statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:5060
```

# Test na útok Register Flood

```
alert ip any any -> $SIP_PROXY_IP $SIP_PROXY_PORTS \
(msg:"REGISTER message flooding"; content:"REGISTER"; depth:8;\
threshold: type both , track by_src, count 100, seconds 60; \
sid:1000200; rev:1;)
```

# SNORT log potřetí

```
[1:5000001:1] TCP SYN packet flooding from single source [**]
[Priority: 0] {TCP} 160.216.1.102:1653 -> 160.216.1.103:506011/10-17:22:18.980228  [**]
[1:5000002:1] TCP SYN packet flooding (simple or distributed) [**]
[Priority: 0] {TCP} 143.110.215.175:3957 -> 160.216.1.103:506011/10-17:23:18.000308  [**]
[1:5000002:1] TCP SYN packet flooding (simple or distributed) [**]
[Priority: 0] {TCP} 151.170.194.143:11334 -> 160.216.1.103:506011/10-17:23:32.253141  [**]
[1:5000004:1] INVITE message flooding [**]
[Priority: 0] {UDP} 160.216.1.102:3069 -> 160.216.1.103:506011/10-17:23:35.037319  [**]
[1:5000005:1] REGISTER message flooding [**]
[Priority: 0] {UDP} 160.216.1.102:2002 -> 160.216.1.103:506011/10-17:24:14.483933  [**]
[1:5000007:1] TCP/IP message flooding directed to SIP proxy [**]
[Priority: 0] {UDP} 160.216.1.102:7777 -> 160.216.1.103:506011/10-17:24:40.652745  [**]
[1:5000008:1] DNS No such name threshold. Abnormaly high count of No such name responses.
[Priority: 0] {UDP} 160.216.40.10:53 -> 160.216.1.103:105411/10-17:24:54.120039  [**]
[1:5000011:1] SQL Injection. Injection of DROP statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:55.220988  [**]
[1:5000012:1] SQL Injection. Injection of DELETE statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:56.265353  [**]
[1:5000013:1] SQL Injection. Injection of SELECT statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:57.390944  [**]
[1:5000014:1] SQL Injection. Injection of INSERT statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:58.397378  [**]
[1:5000015:1] SQL Injection. Injection of UPDATE statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:58.994778  [**]
[1:5000016:1] SQL Injection. Injection of UNION statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:5060
```

# Útok SQL Injection

```
Select password from subscriber
where username='myname'; and
realm='160.216.1.102'
```

```
Select password from subscriber
where username='myname;
DROP table Subscriber -- ' and
realm='160.216.1.102'
```

# Test na útok SQL Injection

```
alert ip any any -> $SIP_PROXY_IP $SIP_PROXY_PORTS \
(msg:"SQL Injection - Injection of DROP statement"; \
pcre:"/\'drop/ix"; \
sid: 1000510; rev:1;)
alert ip any any -> $SIP_PROXY_IP $SIP_PROXY_PORTS \
(msg:"SQL Injection - Injection of DELETE statement"; \
pcre:"/\'delete/ix"; \
sid: 1000520; rev:1;)
alert ip any any -> $SIP_PROXY_IP $SIP_PROXY_PORTS \
(msg:"SQL Injection - Injection of SELECT statement"; \
pcre:"/\'select/ix"; \
sid: 1000530; rev:1;)
alert ip any any -> $SIP_PROXY_IP $SIP_PROXY_PORTS \
(msg:"SQL Injection - Injection of INSERT statement"; \
pcre:"/\'insert/ix"; \
sid: 1000530; rev:1;)
```

.....

# SNORT log naposledy

```
[1:5000001:1] TCP SYN packet flooding from single source [**]
[Priority: 0] {TCP} 160.216.1.102:1653 -> 160.216.1.103:506011/10-17:22:18.980228  [**]
[1:5000002:1] TCP SYN packet flooding (simple or distributed) [**]
[Priority: 0] {TCP} 143.110.215.175:3957 -> 160.216.1.103:506011/10-17:23:18.000308  [**]
[1:5000002:1] TCP SYN packet flooding (simple or distributed) [**]
[Priority: 0] {TCP} 151.170.194.143:11334 -> 160.216.1.103:506011/10-17:23:32.253141  [**]
[1:5000004:1] INVITE message flooding [**]
[Priority: 0] {UDP} 160.216.1.102:3069 -> 160.216.1.103:506011/10-17:23:35.037319  [**]
[1:5000005:1] REGISTER message flooding [**]
[Priority: 0] {UDP} 160.216.1.102:2002 -> 160.216.1.103:506011/10-17:24:14.483933  [**]
[1:5000007:1] TCP/IP message flooding directed to SIP proxy [**]
[Priority: 0] {UDP} 160.216.1.102:7777 -> 160.216.1.103:506011/10-17:24:40.652745  [**]
[1:5000008:1] DNS No such name threshold. Abnormaly high count of No such name responses.
[Priority: 0] {UDP} 160.216.40.10:53 -> 160.216.1.103:105411/10-17:24:54.120039  [**]
[1:5000011:1] SQL Injection. Injection of DROP statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:55.220988  [**]
[1:5000012:1] SQL Injection. Injection of DELETE statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:56.265353  [**]
[1:5000013:1] SQL Injection. Injection of SELECT statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:57.390944  [**]
[1:5000014:1] SQL Injection. Injection of INSERT statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:58.397378  [**]
[1:5000015:1] SQL Injection. Injection of UPDATE statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:506011/10-17:24:58.994778  [**]
[1:5000016:1] SQL Injection. Injection of UNION statement [**]
[Priority: 0] {UDP} 160.216.1.102:1049 -> 160.216.1.103:5060
```

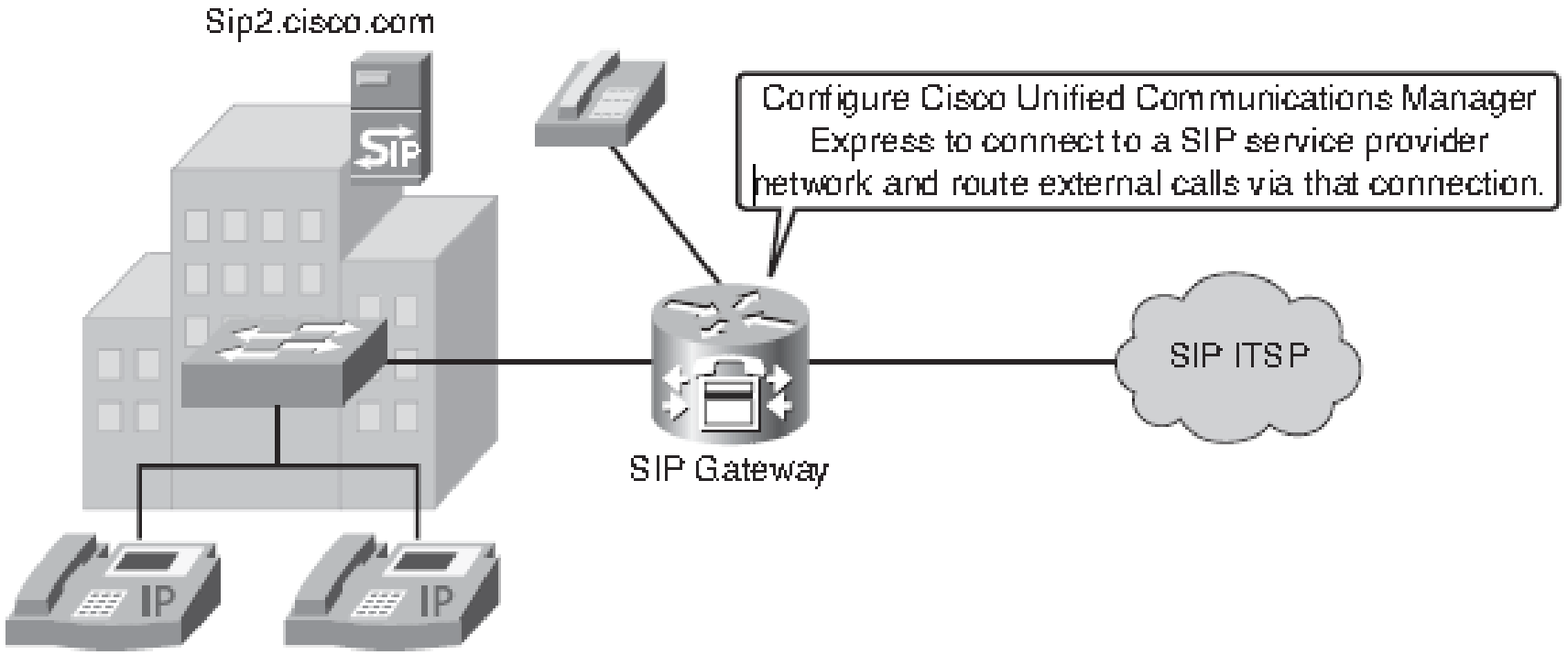
# 4. Konfigurace SIP na Cisco směrovačích

# Scénář konfigurace brány SIP

Jako síťový administrátor máte nakonfigurovat hlasovou bránu tak, abyste integrovali konektivitu Vaší firmy s poskytovatelem Vašich hlasových služeb. Konkrétně:

- Použít SIP jako signalizační protokol
- Nastavit transportní protokol na UDP
- Použít rozhraní Loopback 0 jako zdrojové rozhraní pro SIP
- Změnit UA takto:
  - Zapnout místní ověřování
  - Aktivovat registraci adresy E.164 přímo připojených analog. Telefonů
  - Nastavit server SIP
  - Změnit počet opakování INVITE, RESPONSE, BYE A CANCEL na 2

# Topologie bran IOS a ITSP
## *(Internet Telephony Service Provider)*



# Integrace bran IOS s ITSP SIP s poznámkami 1/2

```
Router(config)#voice service voip
! Zadání VoIP jako typ zapouzdření hlasu (může být i POTS, VoFR, VoATM
Router(conf-voi-serv)#sip
! Vstup do režimu konfigurace SIP
Router(conf-serv-sip)#session transport udp
! Volba transportního protokolu
Router(conf-serv-sip)#bind control source-interface Loopback 0
! Svázání zdrojové adresy pro signalizaci s adresou IP rozhraní
Router(conf-serv-sip)#bind media source-interface Loopback 0
! Svázání zdrojové adresy pro přenos paketů hlasu s adresou IP rozhraní
Router(conf-serv-sip)#exit
Router(conf-voi-serv)#no shutdown
! Aktivace hlasové služby
Router(config-sip-ua)#retry bye 2
Router(config-sip-ua)#retry cancel 2
```

# Integrace bran IOS s ITSP SIP s poznámkami 2/2

```
Router(config)#sip-ua
! Vstup do režimu konfigurace UA SIP
Router(config-sip-ua)#authentication username JD password secret
! Nakonfigurování ověřování typu Digest
Router(config-sip-ua)#registrar dns:sip2.cisco.com expires 3600
! Je umožněno registrovat čísla E.164 (číslovací plán používaný pro
! telef.) hlasových portů (FXS) analogových telefonů a IP telefonů
! u externího proxy SIP nebo registračního serveru SIP
Router(config-sip-ua)#sip-server dns:sip2.cisco.com
! Zadání adresy hostitele
Router(config-sip-ua)#retry invite 2
Router(config-sip-ua)#retry response 2
Router(config-sip-ua)#retry bye 2
Router(config-sip-ua)#retry cancel 2
! Přizpůsobení parametrů podmínkám sítě
```

# Integrace bran IOS s ITSP SIP

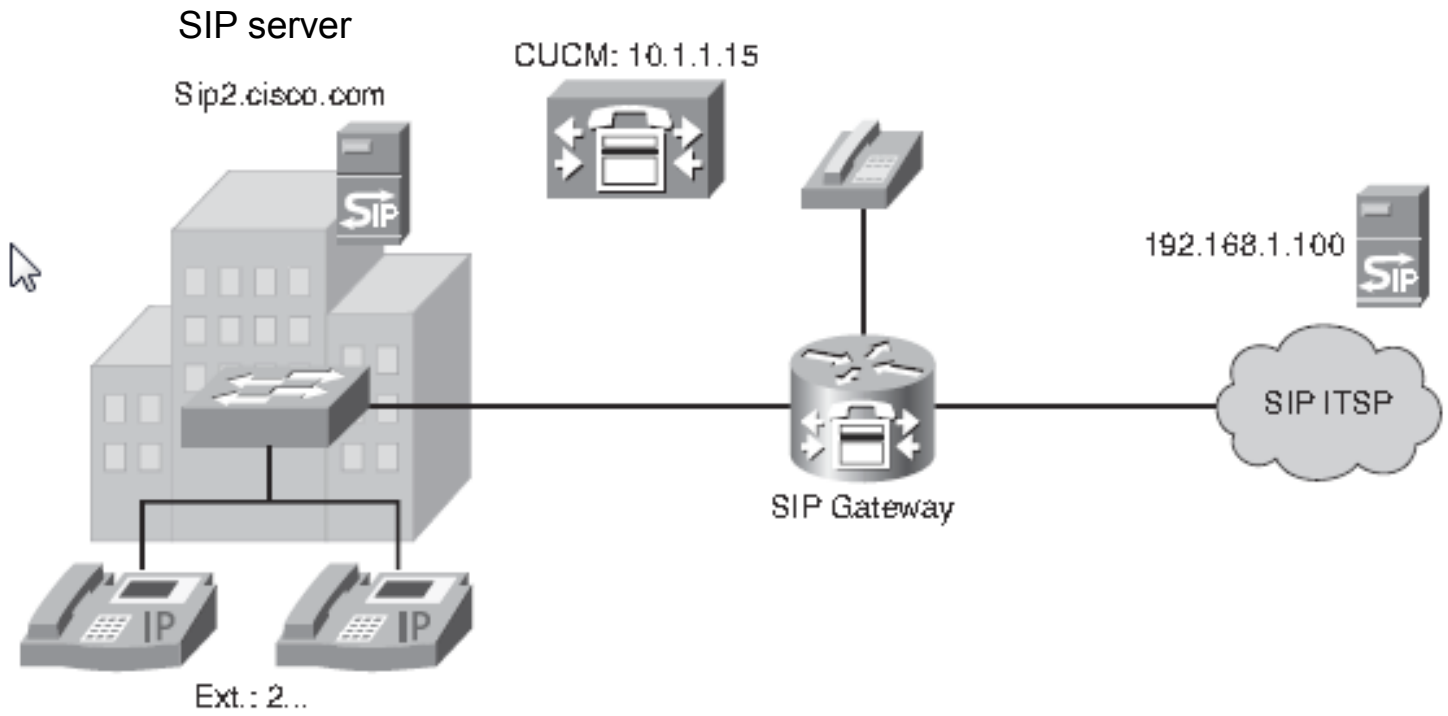
```
Router(config)#voice service voip
Router(conf-voi-serv)#sip
Router(conf-serv-sip)#session transport udp
Router(conf-serv-sip)#bind control source-interface Loopback 0
Router(conf-serv-sip)#bind media source-interface Loopback 0
Router(conf-serv-sip)#exit
Router(conf-voi-serv)#no shutdown
Router(config)#sip-ua
Router(config-sip-ua)#authentication username JDoe password secret
Router(config-sip-ua)#registrar dns:sip2.cisco.com expires 3600
Router(config-sip-ua)#sip-server dns:sip2.cisco.com
Router(config-sip-ua)#retry invite 2
Router(config-sip-ua)#retry response 2
Router(config-sip-ua)#retry bye 2
Router(config-sip-ua)#retry cancel 2
```

# Dial peer

- Dial peer je adresovatelný koncový bod volání
- Příslušná adresa se označuje za vzor cíle (destination patern) a konfiguruje se v každém dial peeru.
- Vzory cíle mohou využívat přímo zadané číslice i zástupné proměnné
- Dial peery definují parametry hovorů, kterým odpovídají
- Hlasové brány Cisco podporují pět typů dial peerů: POTS, VoIP, VoFR, VoATM a MMoIP (Multimedia Mail over IP).

  - Dial peery POTS poskytují tel. Číslo a ukazují na konkrétní hlasový port
  - Dial peery VoIP zajišťují cílovou adresu (tel. Číslo) okrajového zařízení na druhé straně, přiřazují cílovou adresu ke směrovači

# Příklad topologie dial peeru SIP



# Konfigurace dial peeru SIP

```
Router(config)#dial-peer voice 2000 pots
Router(config-dial-peer)#destination-pattern 2...
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target sip-server
Router(config-dial-peer)#dtmf-relay rtp-nte
Router(config)#dial-peer voice 2001 pots
Router(config-dial-peer)#destination-pattern 2...
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target ipv4:10.1.1.15
Router(config-dial-peer)#dtmf-relay sip-notify
Router(config-dial-peer)#preference 1
Router(config)#dial-peer voice 90 voip
Router(config-dial-peer)#destination-pattern 9T
Router(config-dial-peer)#session target ipv4:192.168.1.100
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#dtmf-relay rtp-nte
```

# Konfigurace dial peeru SIP

```
Router(config)#dial-peer voice 2000 pots
Router(config-dial-peer)#destination-pattern 2...
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target sip-server
Router(config-dial-peer)#dtmf-relay rtp-nte
!DTMF tóny jsou zakódovány v nte (named telephone events)
!formátu a přenášeny stejným RTP kanálem jako hlas
!nte jsou vyhrazená čísla z rozsahu 96 až 127
Router(config)#dial-peer voice 2001 pots
Router(config-dial-peer)#destination-pattern 2...
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target ipv4:10.1.1.15
Router(config-dial-peer)#dtmf-relay sip-notify
! Zajistí upozornění na události telefonu zprávami NOTIFY
Router(config-dial-peer)#preference 1
Router(config)#dial-peer voice 90 voip
Router(config-dial-peer)#destination-pattern 9T
Router(config-dial-peer)#session target ipv4:192.168.1.100
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#dtmf-relay rtp-nte
```

# Ověřování stavu brány

```
Router#show sip service
SIP Service is up
Router#
Router#show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP max-forwards : 6
SIP DNS SRV version: 1 (rfc 2052)
Redirection (3xx) message handling: ENABLED
Router#
Router#show sip-ua timers
SIP UA Timer Values (millisecs)
trying 500, expires 180000, connect 500, disconnect 500
comet 500, prack 500, rel1xx 500, notify 500
refer 500, register 500
```

# Ověřování stavu brány

```
Router#show sip-ua register status
Line peer expires(sec) registered
4001 20001 596 no
4002 20002 596 no
5100 1 596 no
9998 2 596 no
router#show sip-ua calls
SIP UAC CALL INFO
Number of SIP User Agent Client(UAC) calls: 0
SIP UAS CALL INFO
Call 1
SIP Call ID : D215F304-7B5A11DC-8005EA1A-6A8F4AD@10.10.10.2
State of the call : STATE_ACTIVE (7)
Substate of the call : SUBSTATE_NONE (0)
Calling Number : 2818902001
Called Number : 1003
Bit Flags : 0x1212003A 0x100000 0x488
CC Call ID : 1
Source IP Address (Sig ): 10.10.10.1
Destn SIP Req Addr:Port : 10.10.10.2:5060
Destn SIP Resp Addr:Port: 10.10.10.2:56884
Destination Name : 10.10.10.2
```

# Zpráva INVITE

```
router#debug ccsip messages
SIP Call messages tracing is enabled
router#
*Mar 6 14:19:14: Sent:
INVITE sip:3660210@166.34.245.231;user=phone;phone-context=unknown SIP/2.0
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Sat, 06 Mar 1993 19:19:14 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Cisco-Guid: 2881152943-2184249568-0-483551624
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Max-Forwards: 6
Timestamp: 731427554
Contact: <sip:3660110@166.34.245.230:5060;user=phone>
Expires: 180
Content-Type: application/sdp
Content-Length: 138
```

# Zpráva OK

```
*Mar 6 14:19:16: Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;
tag=27DBC6D8-1357
Date: Mon, 08 Mar 1993 22:45:12 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Timestamp: 731427554
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Contact: <sip:3660210@166.34.245.231:5060;user=phone>
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 138
v=0
o=CiscoSystemsSIP-GW-UserAgent 1193 7927 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20224 RTP/AVP 0
```

# Zpráva Bye

```
*Mar 6 14:19:19: Received:
BYE sip:3660110@166.34.245.230:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 166.34.245.231:53600
From: <sip:3660210@166.34.245.231;user=phone;phone-
context=unknown>;tag=27DBC6D8-1357
To: “3660110” <sip:3660110@166.34.245.230>
Date: Mon, 08 Mar 1993 22:45:14 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Max-Forwards: 6
Timestamp: 731612717
CSeq: 101 BYE
Content-Length: 0
```

# Konfigurace dial peeru SIP

```
Router(config)#dial-peer voice 2000 pots
Router(config-dial-peer)#destination-pattern 2...
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target sip-server
Router(config-dial-peer)#dtmf-relay rtp-nte
Router(config)#dial-peer voice 2001 pots
Router(config-dial-peer)#destination-pattern 2...
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target ipv4:10.1.1.15
Router(config-dial-peer)#dtmf-relay sip-notify
Router(config-dial-peer)#preference 1
Router(config)#dial-peer voice 90 voip
Router(config-dial-peer)#destination-pattern 9T
Router(config-dial-peer)#session target ipv4:192.168.1.100
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#dtmf-relay rtp-nte
```