

PRECHOD SIP CEZ NAT A FIREWALL (SIP TRAVERSAL OVER NAT)

Pavel Segeč

Pavel.Segec@fri.uniza.sk

Katedra informačných sietí FRI ŽU





PROBLÉM NAT A TYPY NAT

Prečo vznikol NAT - Problém IPv4 adresného priestoru

- Vďaka flexibilitnosti IP technológie nárast používania → každé IP zariadenie musí mať IP adresu
- Verejný adresný priestor
 - Problém → riadený a prideľovaný
 - V Európe prideľuje RIPE (Réseaux IP Européens)
 - Zákazník prenajíma od ISP



Public Internet addresses are regulated by five Regional Internet Registries (RIRs):

- ARIN
- RIPE NCC
- APNIC
- LACNIC
- AfriNIC

- Problém → Nedostatok voľných, prideliteľných verejných IP adries

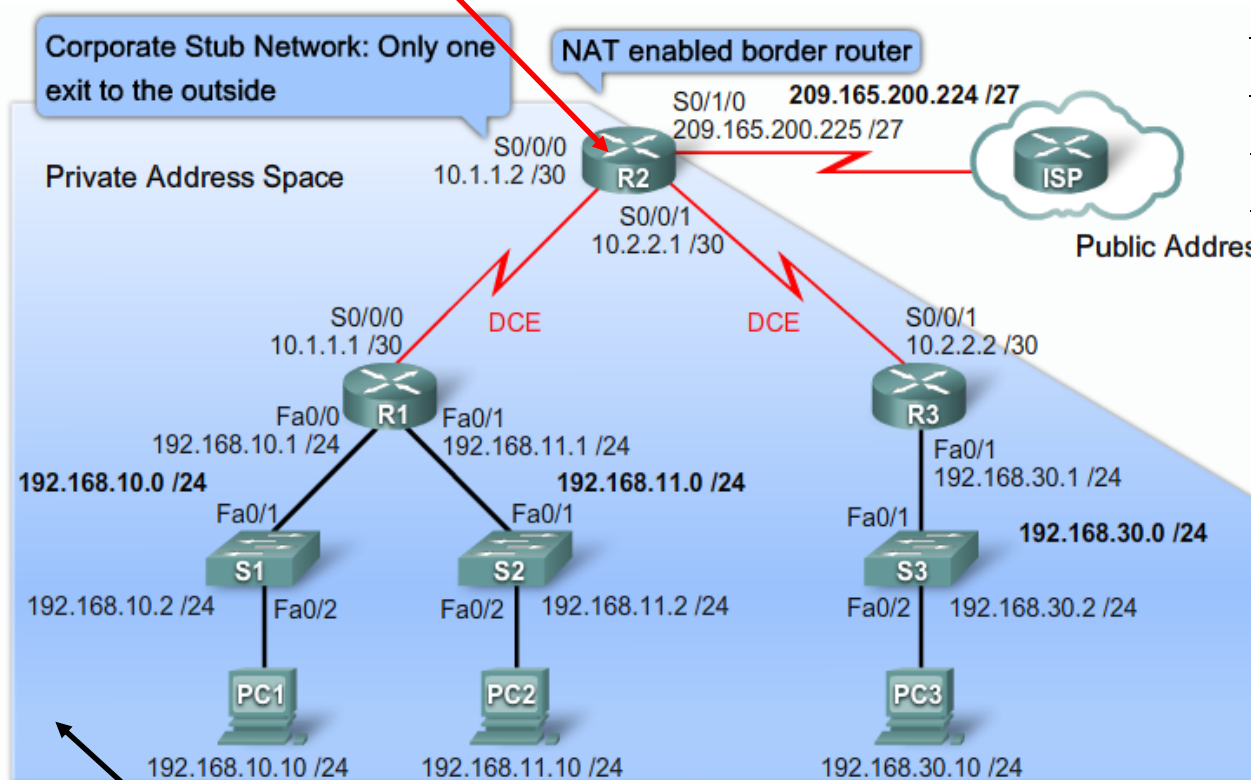
Riešenie - NAT

- Potreba nových metód riadenia adresných rozsahov v snahe riešenia adresnej krízy
- **Network Address Translation (NAT)**
 - Princíp:
 - Vo vnútri siete použitie neriadeného privátneho adresného priestoru na adresáciu IP zariadení
 - Pri prechode paketu cez okraj do verejného Internetu → preklad zdrojovej privátnej IP do verejného adresného IP priestoru
 - NAT musí byť stavový, kde si vedie zoznam prebiehajúcich komunikácií a použitých mapovaní
 - Avšak stále je potrebný verejný IP adresný priestor
 - Minimálne jedna adresa
- **Preklad adres a portov - NAPT**
- NAT ide proti end-to-end princípom Internetu
 - Nevkladať do vnútra siete zariadenia zaoberajúce sa stavom end-to-end spojenia (RFC1958)

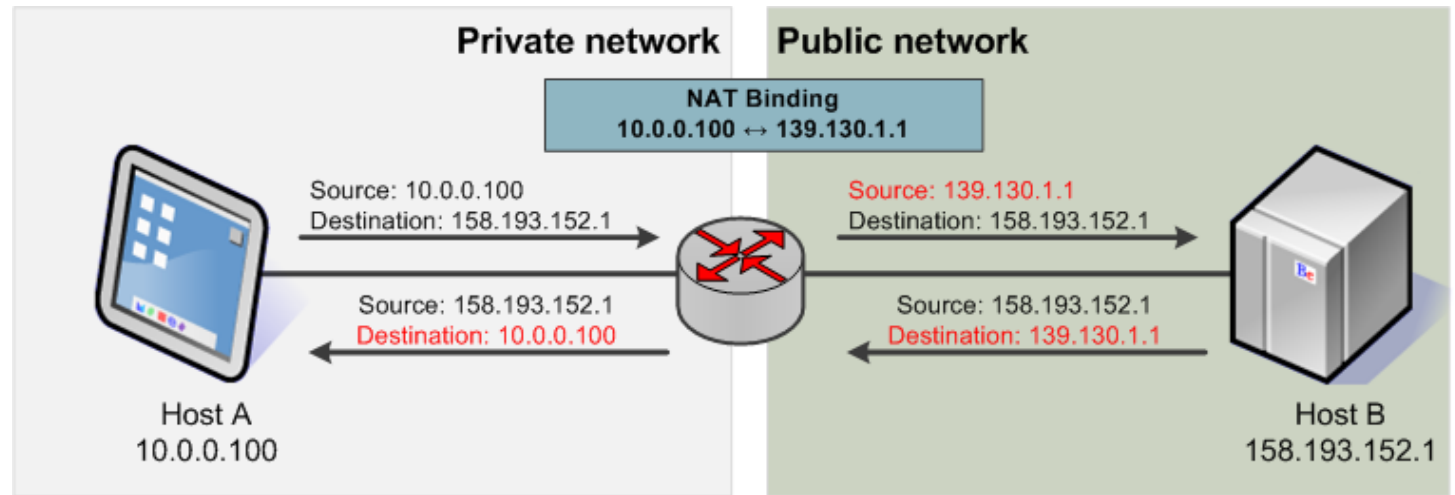
Zariadenia

- Border gateway router
- Pracuje typicky na hranici tzv. stub siete
 - Stub net = jeden vstup a výstup z/do siete

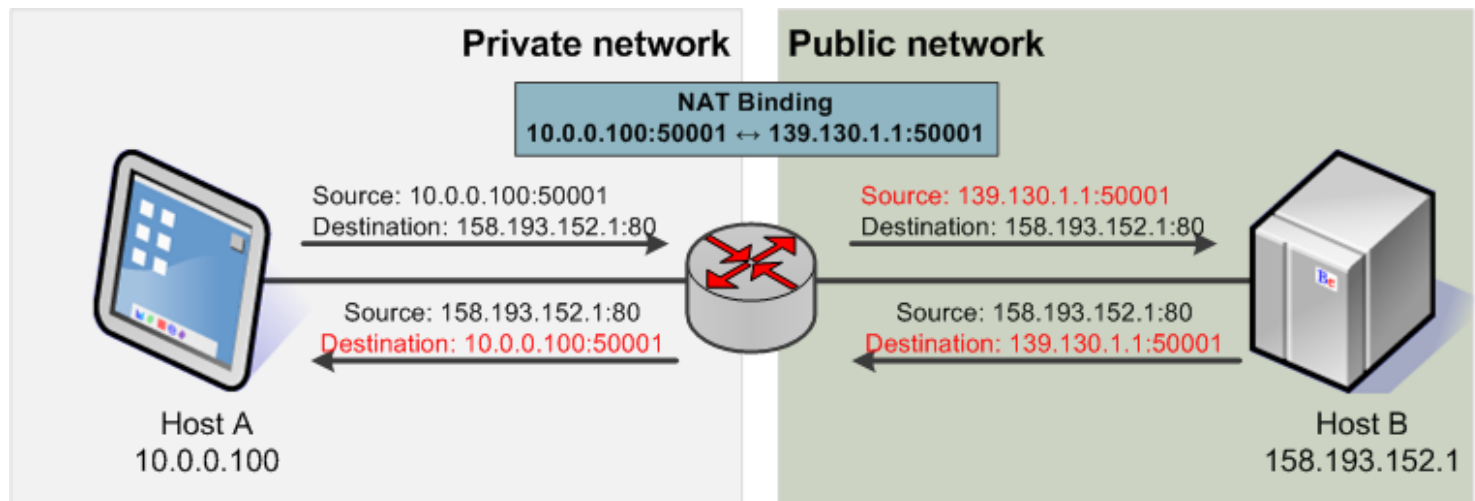
NAT princíp



NAT



NAPT




Vyčlenené privátne adresy pre NAT

- **Privátne IP adresy pre privátne siete**
 - Vyčlenené podľa RFC 1918
 - Môže použiť hocikto
 - Neriadený priestor
 - Routre nesmú smerovať vo verejnej IP sieti privátne adresy z dôvodu nedodržania jedinečnosti identifikácie (adresovania) IP uzla
 - ACL, Route policy a pod.

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0 / 8
B	172.16.0.0 - 172.31.255.255	172.16.0.0 /12
C	192.168.0.0 - 192.168.255.255	192.168.0.0 /16

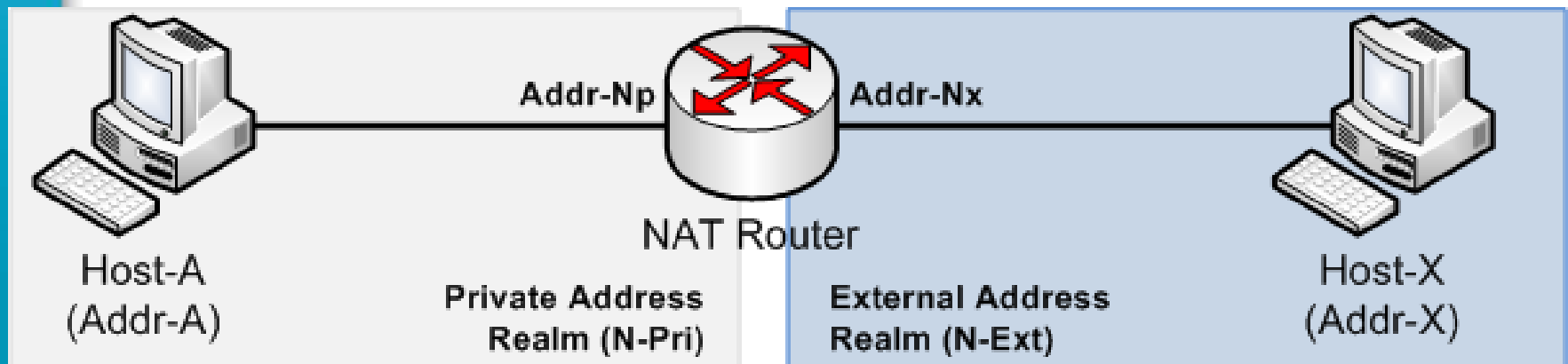
C	165.168.0.0 - 165.168.255.255	165.168.0.0 /16
---	-------------------------------	-----------------

Problémy ohľadne NAT


- **Z pohľadu end-to-end konektivity:**
 - NAT ohrozuje všeobecný princíp konektivity hostov na internete.
 - Host na Internete sa nemôže zvyčajne spojiť a komunikovať s hostom v privátnej sieti
 - Situácia je ešte komplikovanejšia ak sú oba hosty v privátnych sieťach a potrebujú spolu komunikovať
 - NAT mapovanie je udržiavané len na určitý čas 
- **Adresovanie v aplikačných správach**
 - Pri používaní apl. protokolov a aplikácii, ktoré nesú v aplikačnej správe IP adresu prechodom cez NAT vznikajú problémy
 - Niektoré NAT zariadenia skúmajú dátovú časť aplikačných správ a pri niektorých typoch protokolov prepisujú adresnú informáciu podľa existujúceho NAT mapovania.
- **Výkonnosť**
 - Modifikácia parametrov IP hlavičky = rekalkulácia CRC v IP hlavičke
 - Modifikácia transportného portu = rekalkulácia CRC v hlavičke transportného protokolu

Definiție NAT (RFC2663)

- RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations
- Traditional NAT
 - Basic NAT
 - NAPT
- Bi-directional NAT or Two way NAT
- Twice NAT
- Multi-Home NAT



Tradičný NAT (unidirectional or outbound)

- Umožňuje hostom v privátnej sieti transparentne pristupovať k hostom na externej sieti.
- Spojenie je **jednosmerné**, v **odchodzom** smere z privátnej siete 
- IP adresy externých hostov sú jedinečné v externej aj privátnej sieti.
- IP adresy privátnych hostov sú jedinečné len v privátnej sieti.
 - NAT nerozširuje info o adresných rozsahoch privátnej siete
 - Naopak však môže (externé rozsahy do privátnej siete)
- Ľubovoľná daná IP adresa je buď externá alebo privátna, ale nie aj aj
- NAT router umožňuje založiť spojenie z Host A na Host X **ale nie naopak!!**
- N-Ext je smerovateľné v N-Pri **ale nie naopak!!**

Basic NAT

- V *Basic NAT* variácií je zadefinovaný blok externých adries za účelom prekladu adries hostov z privátnej siete
 - Keď začnú spojenie smerom do externej siete.
 - $N\text{-Pri} \rightarrow \text{Addr}_i \in (N\text{-ext})$
- Pre pakety z privátnej siete idúce von sa prekladá
 - Zdrojová IP adresa, IP, TCP, UDP a ICMP checksum.
- Pre vstupujúce pakety sa prekladá cieľová IP adresa a dané checksums

Network Address Port Translation (NAPT)

- Rozšírenie NAT o identifikátor transportného protokolu (**PORT**) alebo typ ICMP dotazu (query)
- Umožňuje prekladať viaceré privátne identifikátory na jeden externý
 - A tým zdieľať viac privátnym hostom jednu externú adresu.
- Používa sa aj v kombinácii s *Basic NAT*
 - Na preklad používa pool externých IP spolu s prekladom portov.
- Pre pakety z privátnej siete idúce von sa prekladá
 - Zdrojová IP adresa, zdrojový port, IP, TCP, UDP a ICMP checksum.
- Pre vstupujúce pakety sa prekladá cieľová IP adresa, cieľový port a dané checksums

Bi-directional NAT or Two way NAT

- Spojenie môže byť iniciované z privátnej siete do externej ako aj **naopak**
 - Z Host A na host X
 - Z host X na host A
- Privátna adresa je napevno (staticky alebo dynamicky) spojená s globálne jedinečnou IP adresou.
 - Na NAT musí byť spravené mapovanie inside global adresy na inside local
- Na prístup z externých hostov na privátne sa odporúča použiť DNS (DNS ALG – rozšírenie DNS k NAT)
 - Ktoré vie korektné mapovanie podľa zdroja dotazu (N-ext or N-pri) a vie uviesť externé mapovanie k internému alebo naopak.
- N-Ext je smerovateľné v/z N-Pri, **ale nie naopak!!**

Twice NAT

- Sofistikovaný typ NAT, kedy sa prekladá aj zdrojová aj cieľová IP adresa naraz
 - Termín Once NAT-ed neexistuje
 - Umožňuje definovať v jednom pravidle preklad zdrojovej aj cieľovej adresy (cisco)
 - Alebo preklad podľa cieľa
 - Ak do X prelož ako ...
 - Ak do Y prelož ako ...
- Úzko využíva DNS (resp. DNS ALG)
- Nasadenie:
 - ak vnútorný uzol používa verejnú adresu niekoho iného (inej organizácie)
 - Napr. pri chybách, migráciach medzi ISP a pod.
 - Alebo ak je spojenie private to private network s tým istým rozsahom
 - Zlučovanie sietí

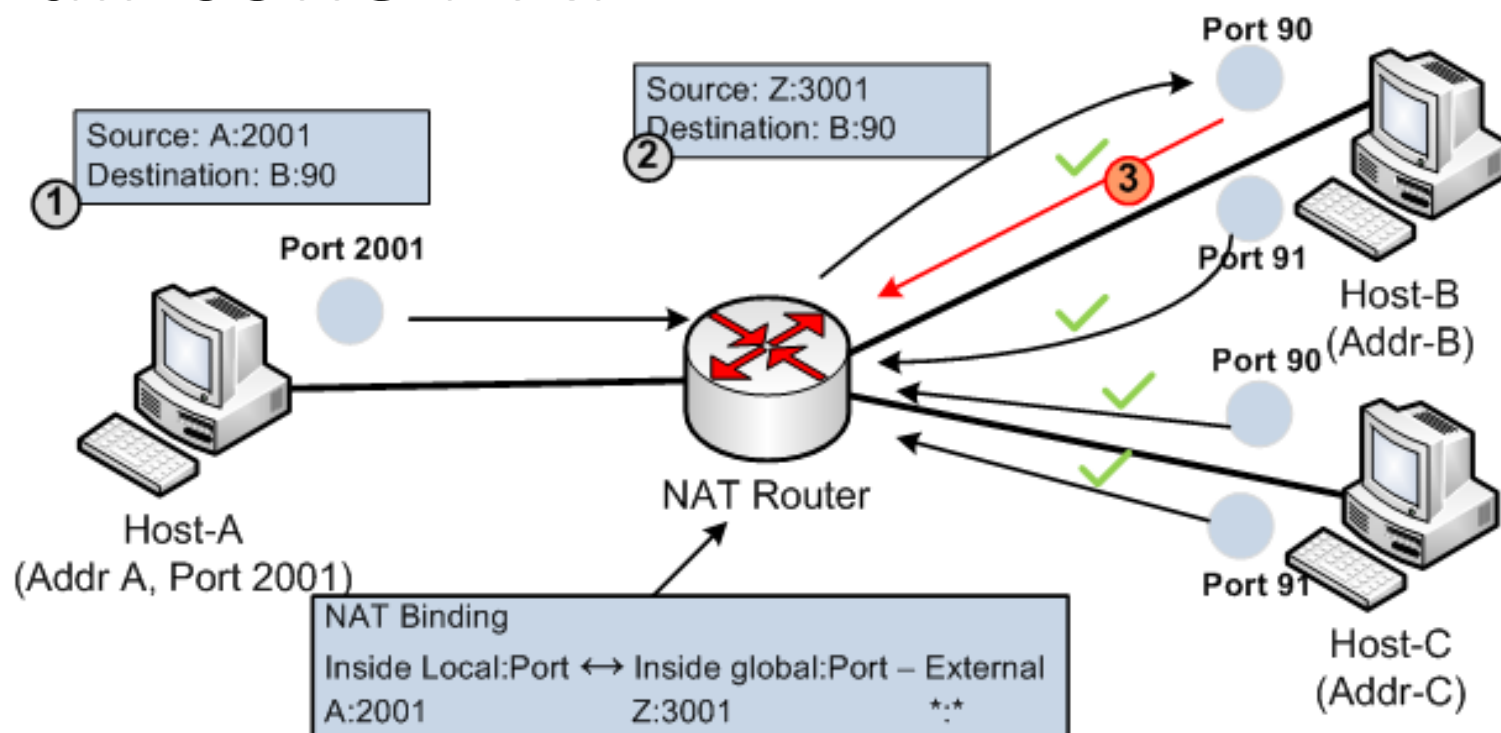
Multihomed NAT

- Typické nasadenie NAT je pre STUB siete
 - Tok pôjde dnu aj von cez to isté zariadenie (NAT si udržiava stavovú info o toku)
 - Centrálny bod chyby → problém s redundanciou pripojenia, ktorá je žiaduca.
- Multihomed NAT je riešenie umožňujúce viacnásobné NAT pripojenie
 - A tým napr. zálohovanie primárneho NAT routra záložným (-mi).
 - Ak primárny NAT zlyhá preberie jeho rolu záložný.
 - Aj s NAT-ovanými tokmi
 - Riešenie vyžaduje výmenu NAT stavových informácií.

Základné variácie implementácií NAT (RFC 3489)

- Pre UDP traversal
 - Full cone NAT
 - Address restricted cone NAT
 - Port restricted cone NAT
 - Symmetric NAT

Full-cone NAT



- Typ, kde všetky požiadavky z tej istej zdrojovej IP a portu sú mapované na tú istú externú IP adresu a port.
- Vytvorený NAT záznam môže použiť **ľubovoľný** externý host pre komunikáciu s interným hostom
 - Ak vie externú IP a port na NAT
- Najmenej reštriktívna forma NAT

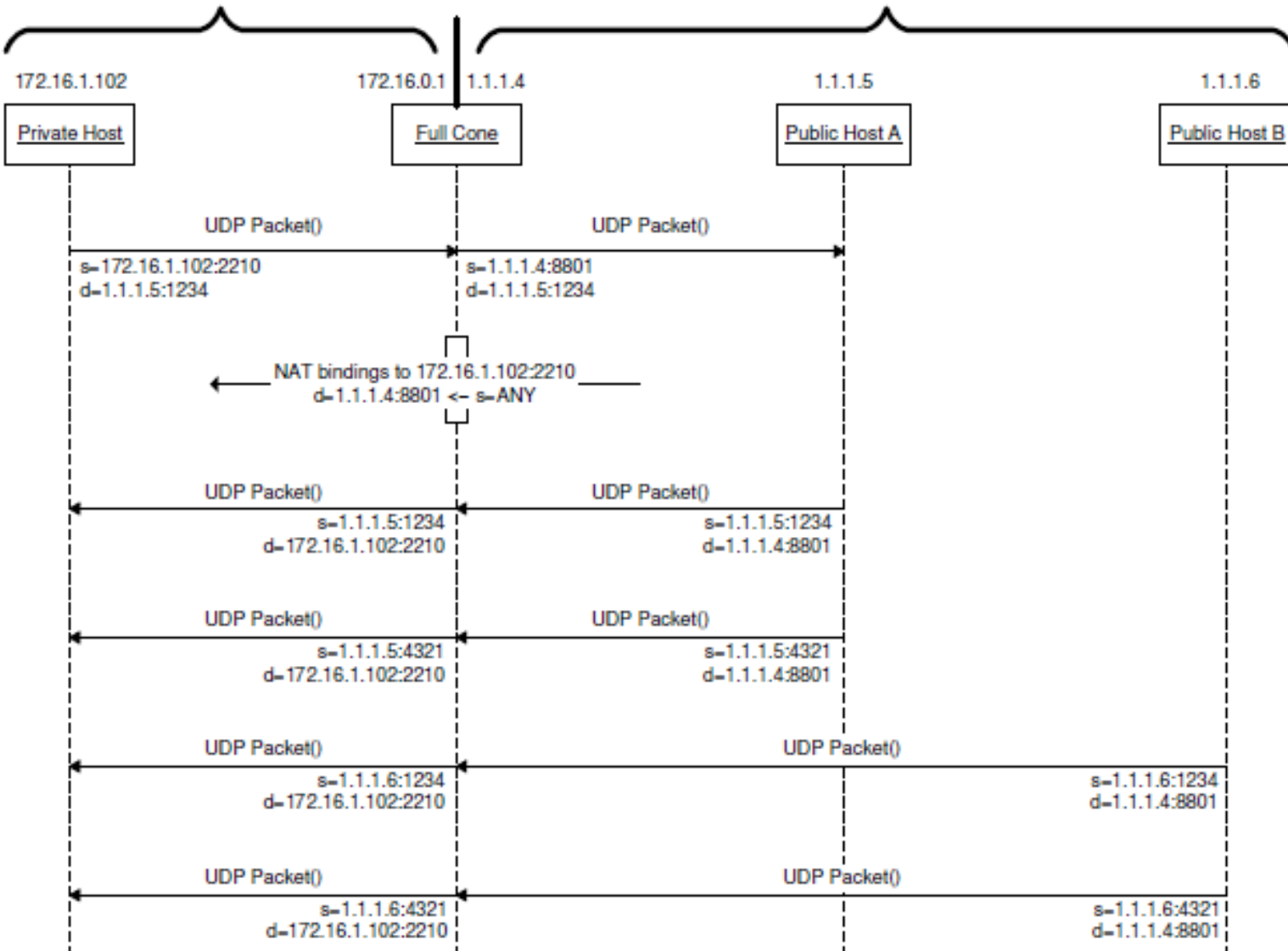
NAT Types: Full Cone NAT

Legend

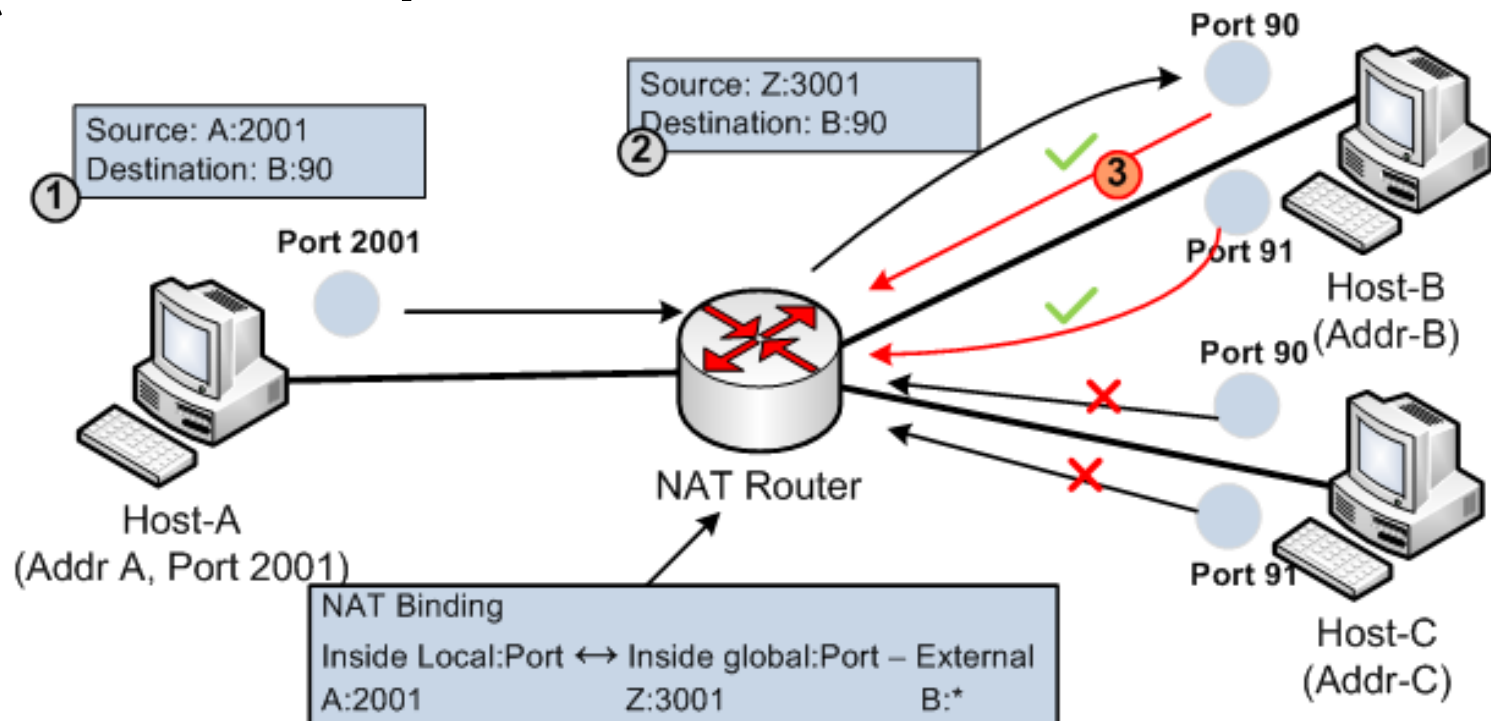
s=source address:port
d=destination address:port

Private
IP Address Realm
172.16.0.0/16

Public
IP Address Realm
Internet



(Address) Restricted-cone NAT

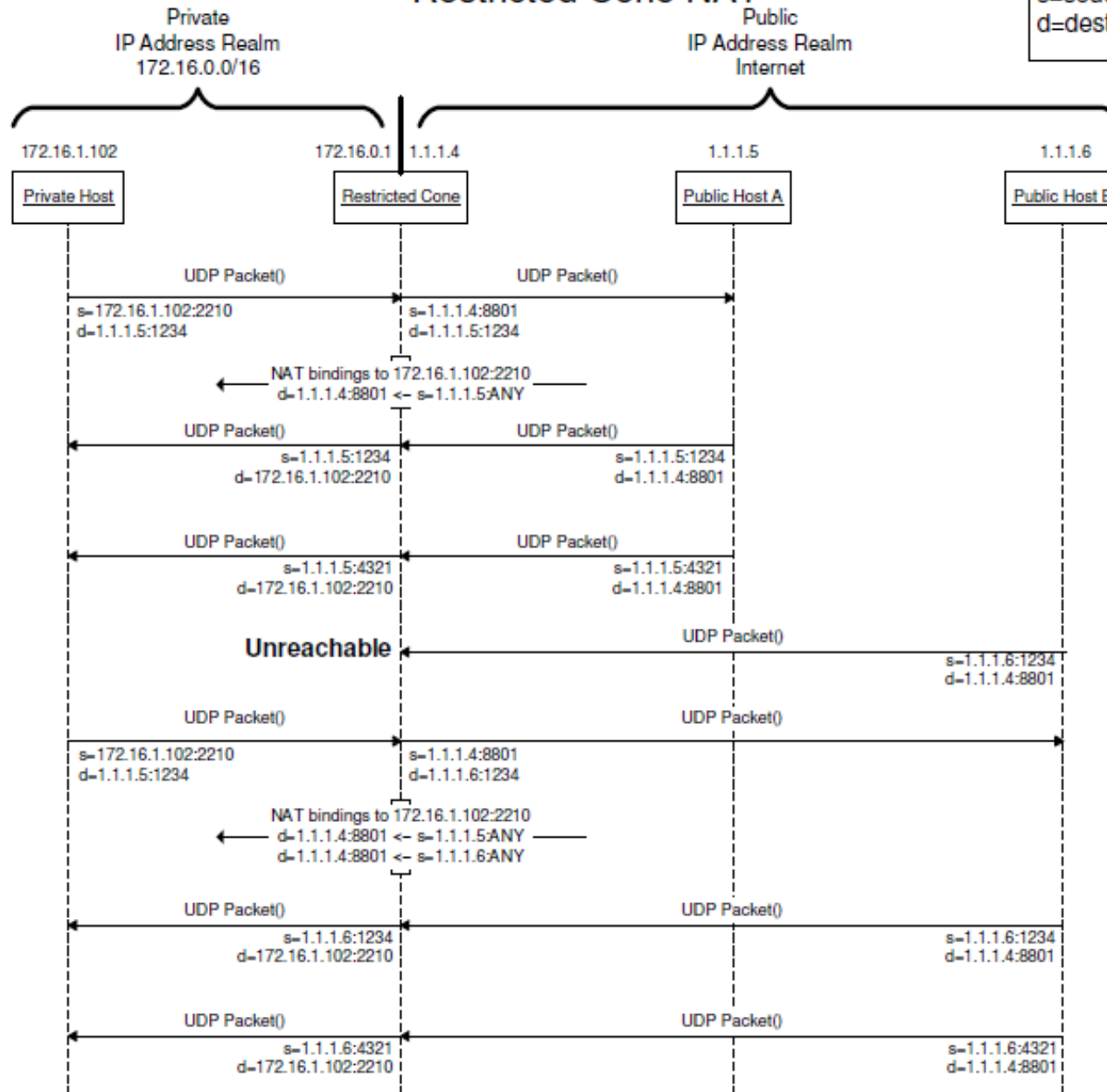


- Typ NAT, kde všetky požiadavky z internej IP adresy a portu sú mapované na rovnakú externú IP adresu a port.
- Na rozdiel od Full Cone NAT len externý host, ktorý prijal paket od interného hosta môže komunikovať späť
 - Port externého hosta nie je podstatný

NAT Types: Restricted Cone NAT

Legend

s=source address:port
d=destination address:port



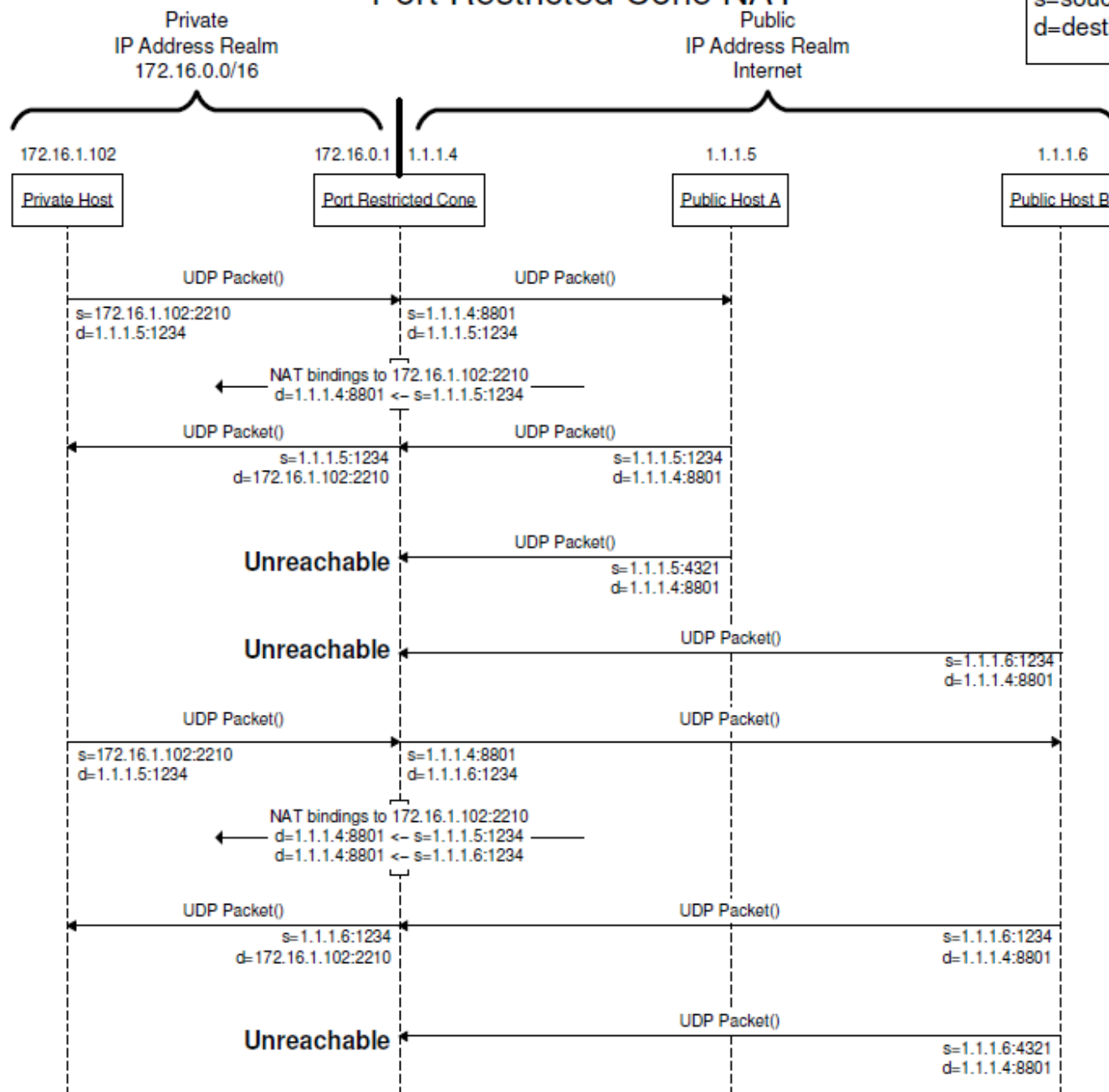
Port-restricted-cone NAT

- Ako restricted cone NAT, ale obmedzenia zahŕňajú aj číslo portu
 - Všetky požiadavky z internej IP adresy a portu sú mapované na rovnakú externú IP adresu a port.
- Externý host môže poslať paket, len ak predtým prijal paket od interného hosta
 - a musí ho poslať z čísla portu na ktorom predtým paket prijal

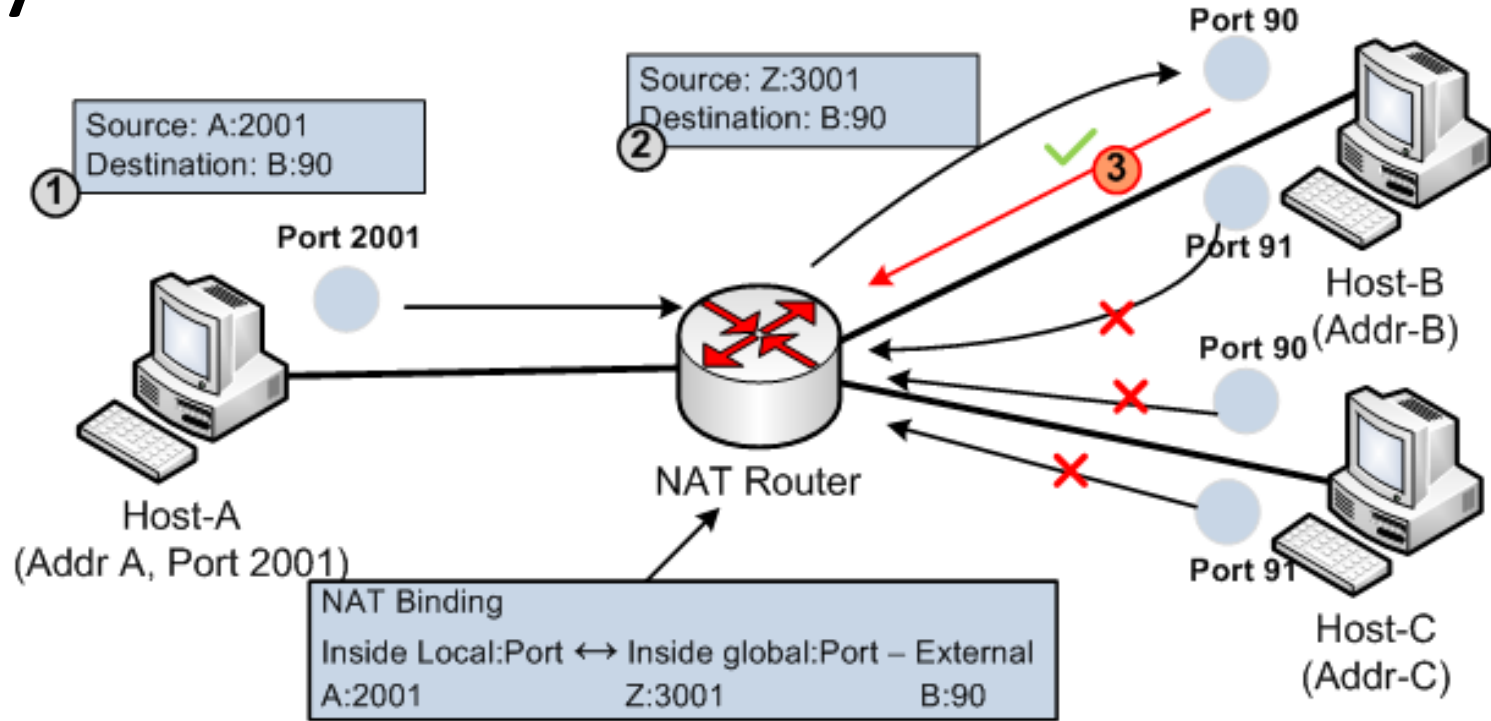
NAT Types: Port Restricted Cone NAT

Legend

s=source address:port
d=destination address:port



Symmetric NAT

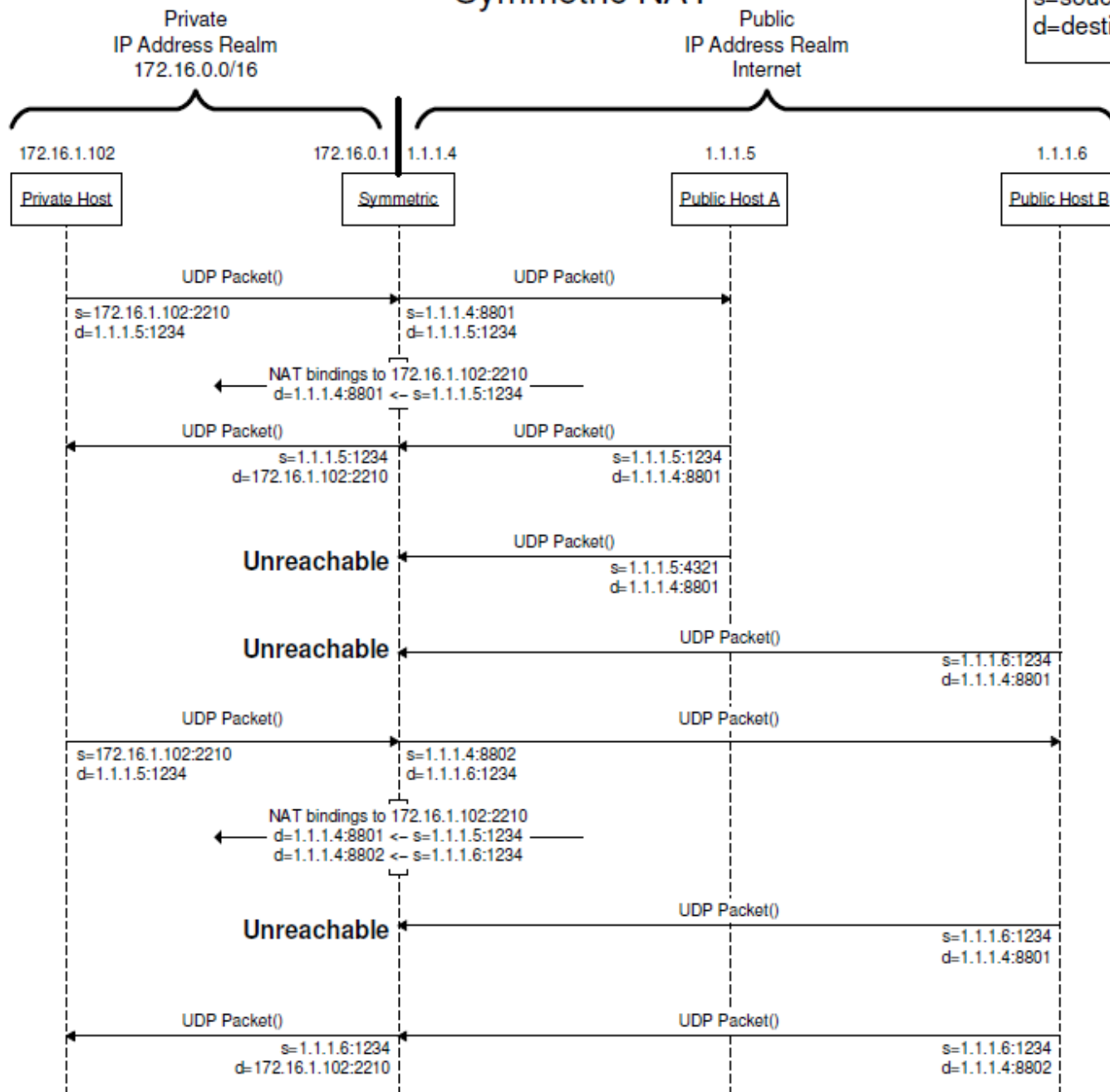


- Riešene, kde každá požiadavka z tej istej zdrojovej adresy a portu na špecifickú cieľovú adresu a port je mapovaná na tú istú externú adresu a port
- Ak ten istý interný host pošle paket s tou istou zdrojovou adresou a portom, ale inému cieľu, je použité nové mapovanie.
- Iba externý host, ktorý dostane paket z interného hosta môže poslať paket späť.
- Najreštriktívnejšia forma NAT

NAT Types: Symmetric NAT

Legend

s=source address:port
d=destination address:port





PROBLÉM SIP CEZ NAT

Zariadenia NAT a FW

- NATs (Network Address Translators)
 - “light” security device
 - Používané na *topology hiding*
 - Jednoduché firewall functionality
 - Počet NAT zariadení rastie
 - Znižuje potrebu po viac IPv4 adresách
 - Pri IPv6 nebude potreba NAT
 - Jedine ako jednoduchý bezpečnostný mechanizmus
- FWs (Firewalls)
 - Bezpečnostné zariadenie
 - Počet FW zariadení rastie
 - Pravidlá sú reštriktívnejšie

Problém SIP cez NAT/FW

- SIP svojim dizajnom porušuje odporúčania pre návrh protokolov priateľských voči NAT
 - Network Address Translator (NAT)-Friendly Application Design Guidelines (RFC3235)
 - V aplikačných správach nevkladať IP adresy

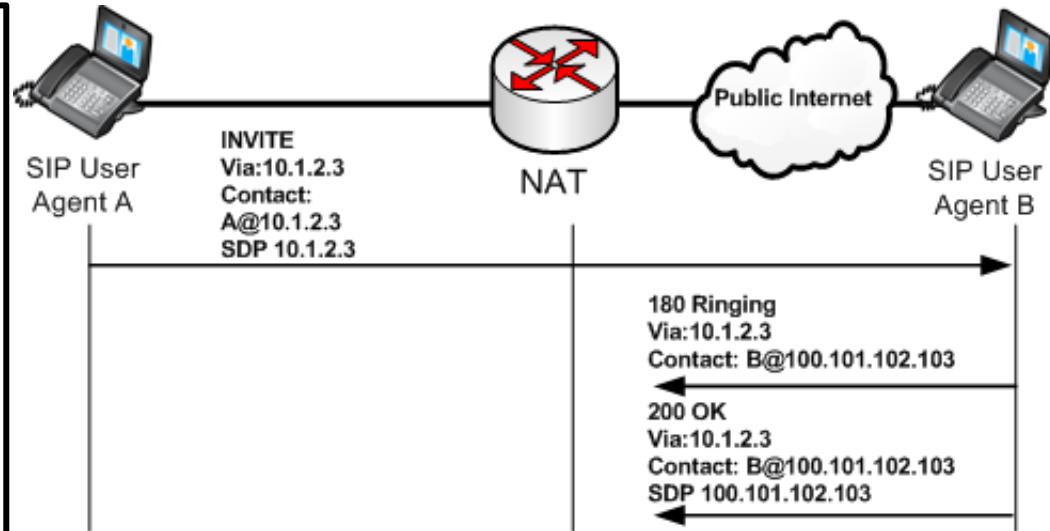
Okruhy problémov

- Pri prechode SIP cez NAT/FW sú dva okruhy problémov
 - So SIP signalizáciou
 - S RTP médiami
- SIP signalizácia prebieha medzi peerami (peer-to-peer)
- Media porty sú dohadované per hovor

Problém pri volaniach z privátnej siete

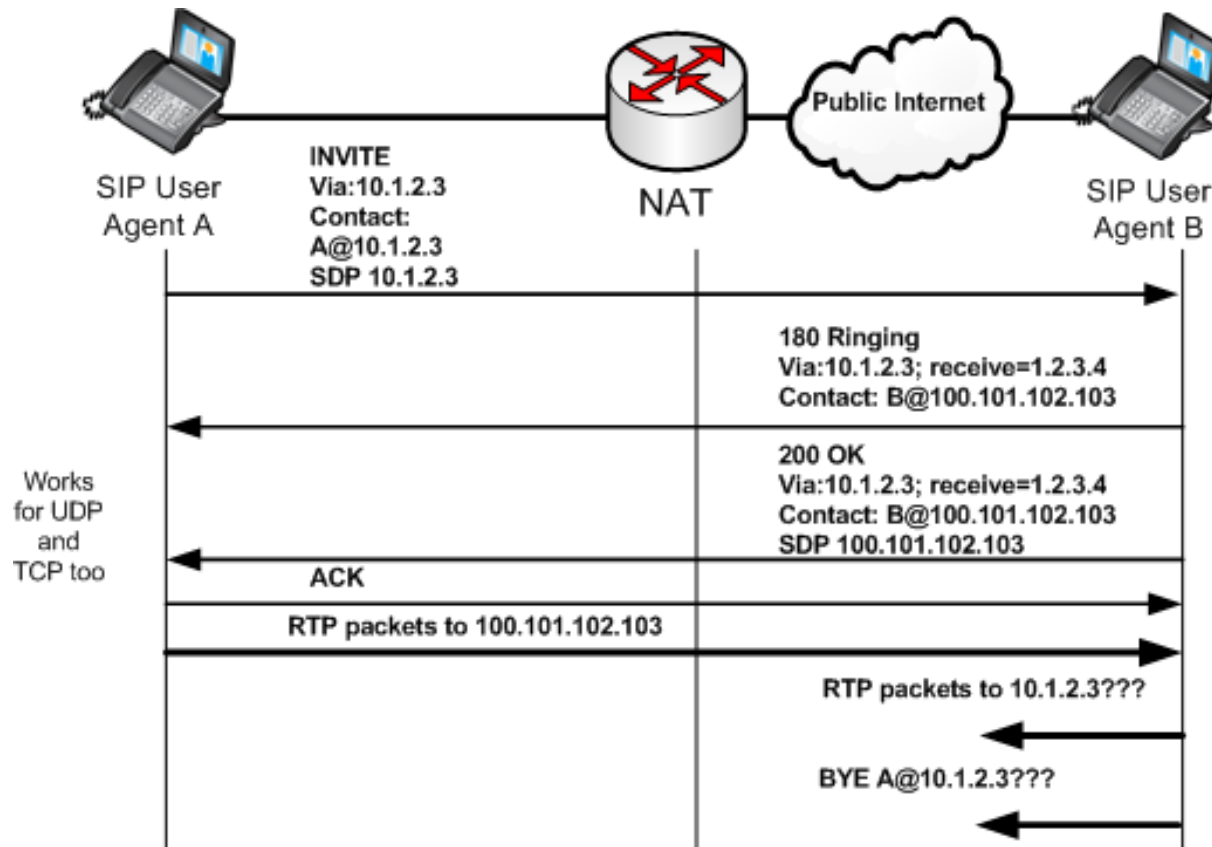
```
INVITE sip:UserB@there.com SIP/2.0
Via: SIP/2.0/UDP
10.1.2.3:5060;branch=z9hG4bKhjh
From: TheBigGuy
<sip:A@customer.com>;tag=343kdw2
To: TheLittleGuy <sip:UserB@there.com>
Max-Forwards: 70
Call-ID: 123456349fijoewr
CSeq: 1 INVITE
Subject: Wow! It Works...
Contact: <sip:A@10.1.2.3>
Content-Type: application/sdp
Content-Length: ...

v=0
o=UserA 2890844526 2890844526 IN IP4
UserA.customer.com
c=IN IP4 10.1.2.3
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```



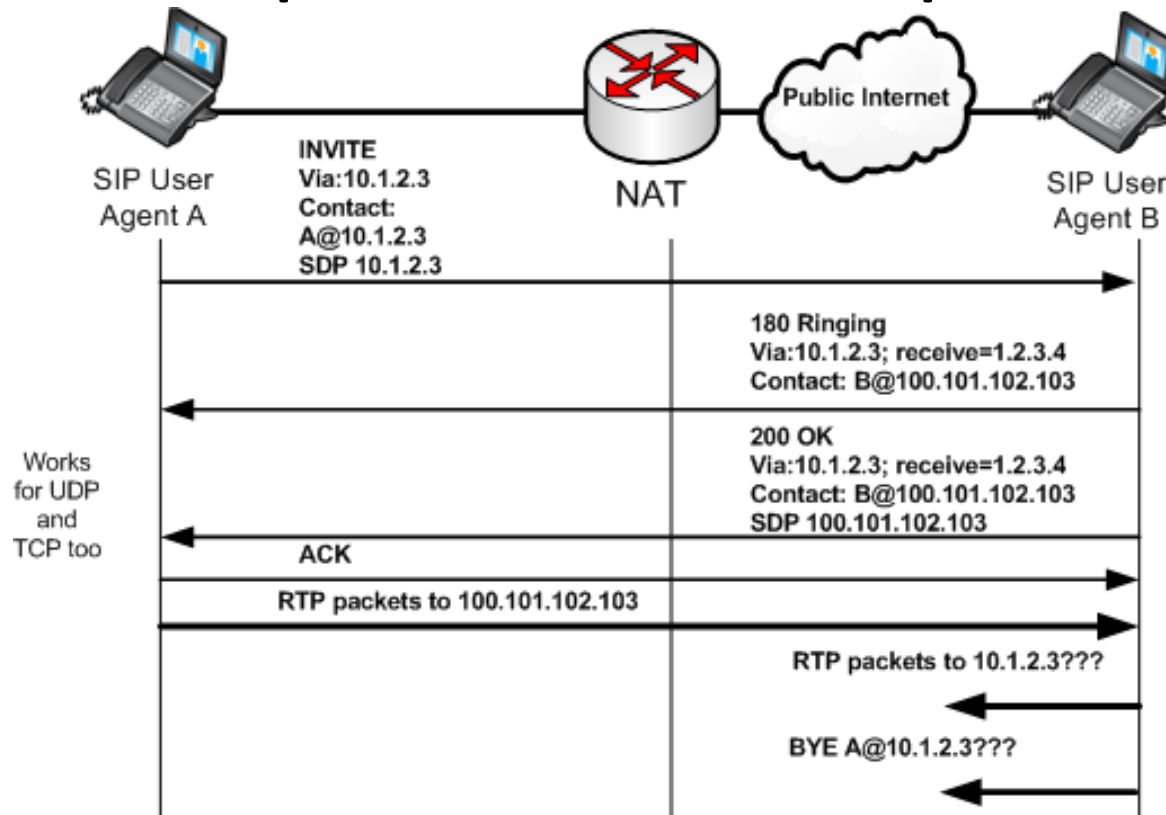
1. Smerovanie do privátnej siete nie je možné na základe Via hlavičky (*via header*)

Čiastkové riešenia



- Riešenie problému 1 – pomocou SIP
 - Najmä pri UDP, nie TCP ako transporte
 - SIP proxy kontroluje Source IP paketu s IP adresou uvedenou vo Via hlavičke
 - Ak je rozdiel (pri NAT áno), uvedenie v param. Received aktuálnu IP adresu za NAT
 - Received= parameter vo Via hlavičke

Problém pri volaniach z privátnej siete

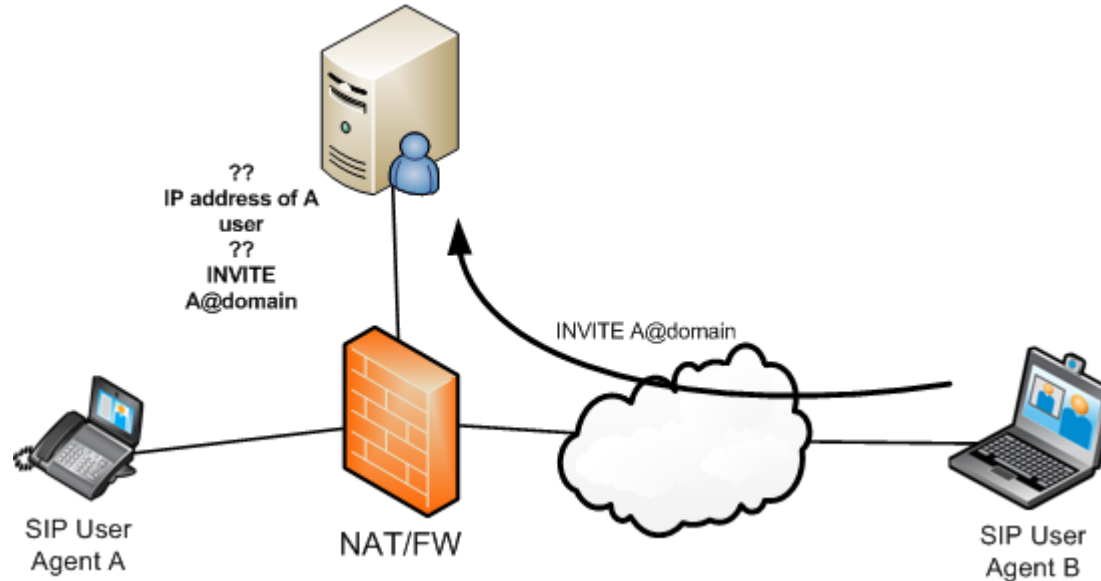


2. Nesprávna IP v Contact hlavičke
3. RTP stream pôjde len jednosmerne
4. Nie je možné smerovať ďalšie správy v rámci dialógu
5. Port čísla pre SIP a RTP sa tiež mohli zmeniť prechodom cez NAT

Čiastkové riešenia

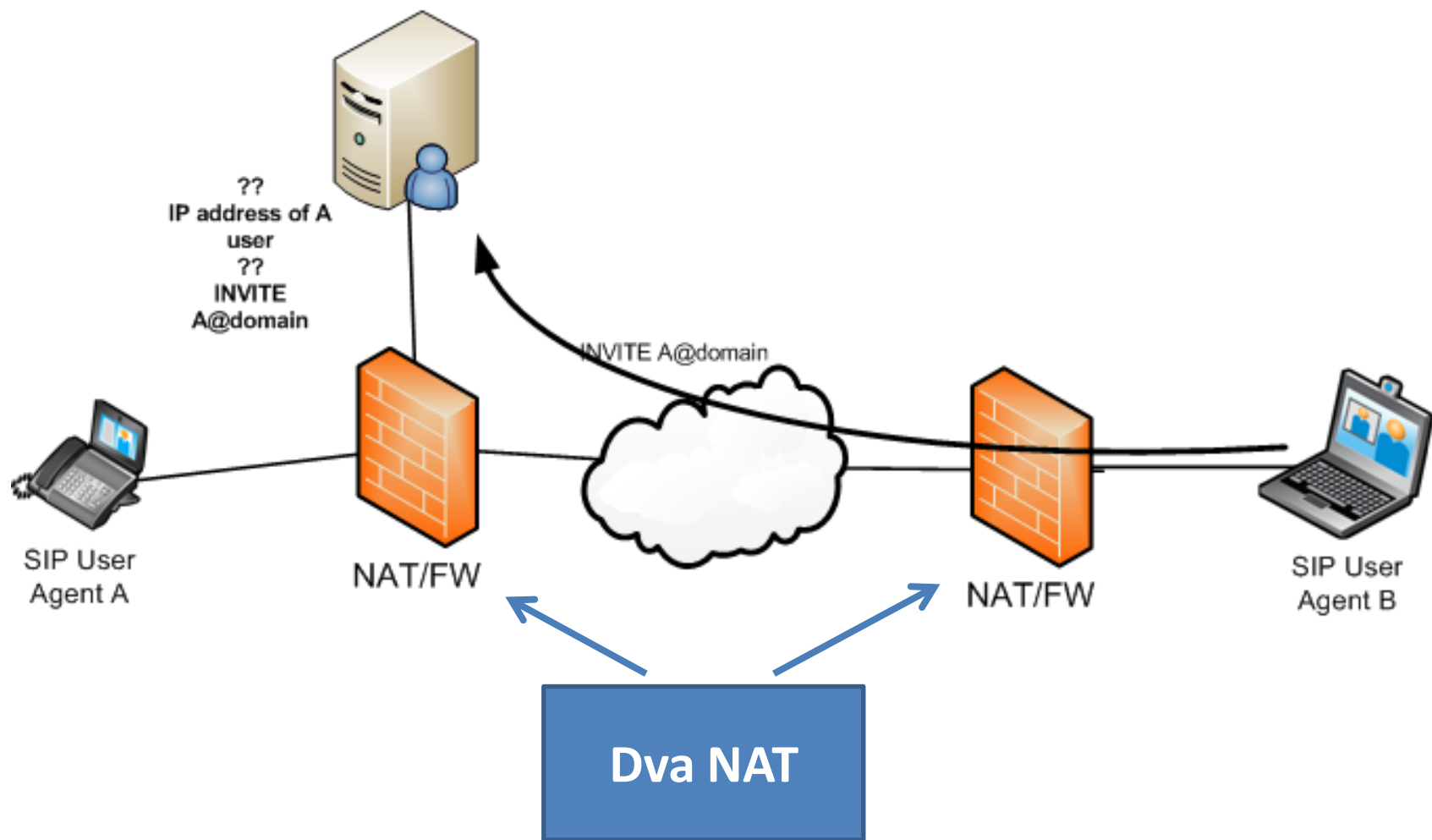
- Riešenie problému 2
 - Trvalo otvorené TCP spojenie namiesto UDP, potom sa `Contact` hlavička nepoužíva
- Riešenie ďalších
 - Nie je triviálne

Problém pri volaniach na hosta v privátnej sieti



- Po registrácii server vie verejnú IP adresu hosta, ktorá bola pridelené NAT-ovaním
- NAT binding je však dynamicky udržované
 - Po dobe neaktivity je vymazané
- Po čase teda SIP server stratí kontakt na klienta vo vnútri privátnej siete

A ešte jeden možný scenár





KOMPLEXNEJŠIE RIEŠENIA PRECHODU CEZ NAT

Riešenia prechodu cez NAT – strana UA

- STUN
 - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
 - Session Traversal Utilities for NAT
- TURN
 - Traversal Using Relay NAT
 - Po novom STUN Relay
- ICE
 - Interactive Connectivity Establishment (STUN + TURN)

Riešenia prechodu cez NAT – strana siete

- B2BUA
 - Back To Back User Agent
- RTP Relay
 - Media relaying
- ALG
 - Application Layer Gateway
 - Session Border Controller
- UPnP
 - Universal Plug and Play
- Statická konfigurácia
- Tunelovanie
 - Napr. VPN
- IPv6



STUN - SESSION TRAVERSAL UTILITIES FOR NAT

STUN

- **STUN** – Simple Traversal of User Datagram Protocol through Network Address Translators.
- Pôvodne definovaný v RFC 3489 pre UDP protokoly
- “*Po novom*” sa volá Session Traversal Utilities for NAT (RFC5389)

Čo STUN robí

- SIP UA použije STUN na zistenie, či leží za NAT/FW
 - A následne na „objavenie“ svojej verejnej IP adresy ako aj portového čísla pridelených v procese NAT-ovania
- STUN je „elegantné riešenie“, ktoré nevyžaduje žiadnu sieťovú konfiguráciu na strane SIP UA a NAT/FW
 - Funguje pomerne dobre
 - „objavený problém“ pri viacerých rozhraniach PC so SIP UA
 - <http://nil.uniza.sk/sip/openser/openser-voip-sip-so-sluzbami-prepojenim-na-cisco-call-managera#stun>

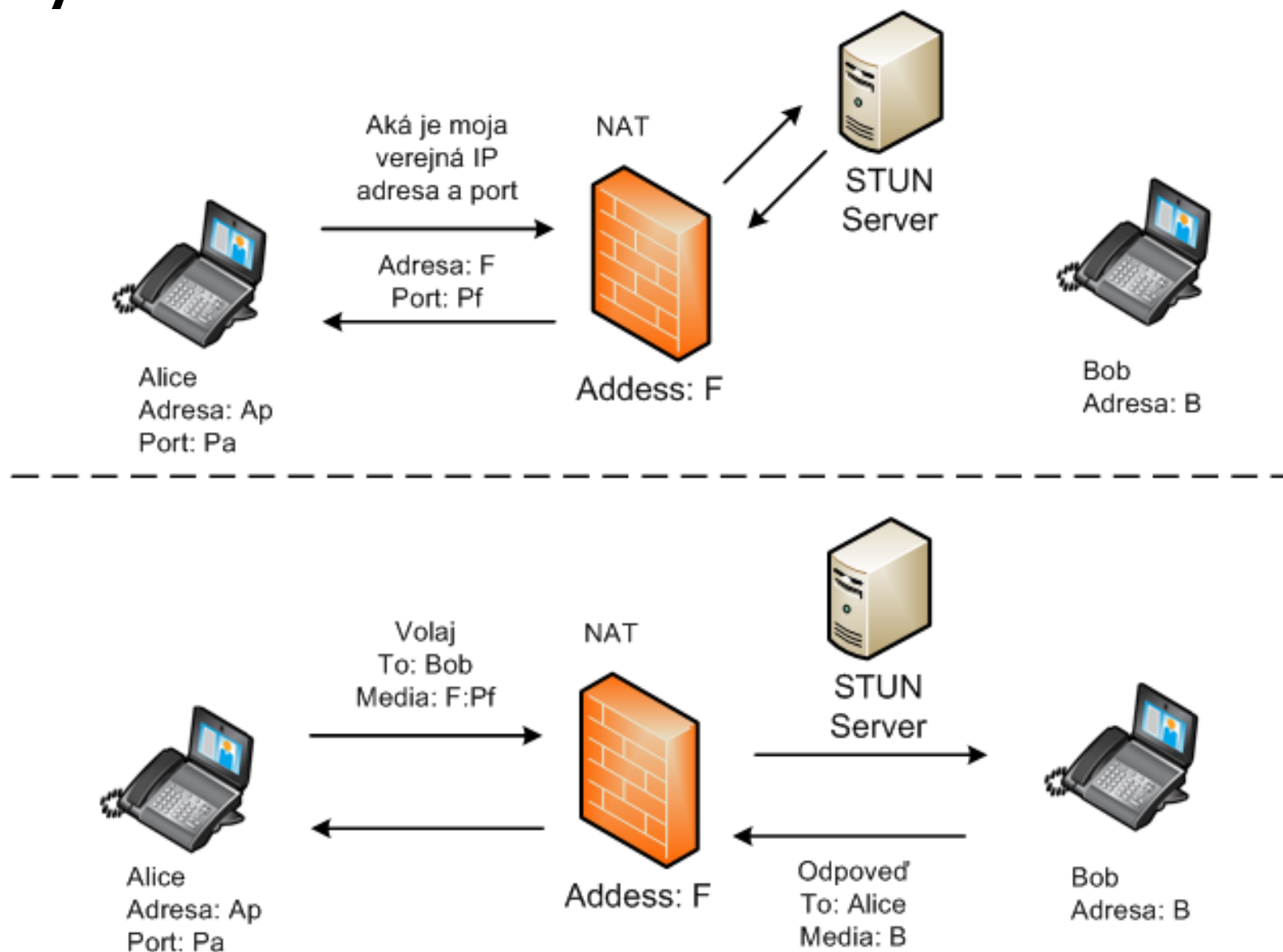
STUN vlastnosti

- STUN je klient/server
- STUN server
 - Je entita, ktorá odpovedá na STUN správy generované klientmi
 - Je umiestnený vo verejnom internete
 - V Linuxe STUN balíček (vyžaduje dve verejné IP adresy)
 - V internete je mnoho verejných STUN serverov
 - Zvyčajne má dve IP adresy
- STUN klient
 - Je entita ktorá generuje STUN správy
 - je zvyčajne zakomponovaná v SIP UA
 - Z odpovede servera si klient určí, či je v sieti NAT a akého je typu

STUN - princíp

- Klient pošle serveru Binding Request (BReq)
- Server odpovie Binding Response (BResp)
 - Pričom zdrojovú IP adresu z IP hlavičky uloží do tela odpovede
- Klient porovná svoju IP a IP v BResp a zistí typ NAT (ak sa adresa po ceste prekladá) a "svoju" verejnú IP adresu
 - Na základe získanej info „upraví“ odpovedajúce SIP a SDP hlavičky s IP adresami
- BReq a BResp sa posielajú ako UDP datagramy
- Pred úvodnou fázou môže ešte prebehnúť fáza TLS negociácie za účelom overenia dôvernosti STUN servera

Využitie STUN



STUN žiadosti - detailnejšie

- Server prijíma BReq na dvoch adresách a dvoch portoch (jeden z nich 3478)
- BReq obsahuje atribúty RESPONSE-ADDRESS a CHANGE-REQUEST
 - RESPONSE-ADDRESS
 - server odosiela odpoveď na túto adresu
 - CHANGE-REQUEST
 - klient môže vyžiadať od servera odpoveď z inej IP adresy/portu, ako z tej, na ktorú posielal BReq

STUN odpovede - detailnejšie

- BResp obsahuje **SOURCE-ADDRESS**, **CHANGED-ADDRESS**, a **MAPPED-ADDRESS**
 - do **SOURCE-ADDRESS** sa dosadí IP adresa/port, z ktorej sa BResp odosiela.
 - **CHANGED-ADDRESS** je adresa/port, na ktorú neprišla požiadavka (ak je pomocou **CHANGE-ADDRESS** vyžiadaná zmena IP aj portu, potom sa rovná **SOURCE-ADDRESS**)
 - t.j. druhá IP adresa STUN servera.
 - **MAPPED-ADDRESS** – do tohto atribútu sa dosadí zdrojová adresa IP paketu a číslo portu zo STUN BReq, .t.j. verejná IP adresa a port po NAT-ovaní.

STUN testy

- Vykonané klientom za účelom zistenia, či je UA za NAT a ak áno akého typu

NAT discovery (test 1)

- To determine if a NAT router/firewall is present, send a STUN request to the server. Wait for a response and analyze it.
- If the IP address and port number in the MAPPED-ADDRESS attribute of the payload in the STUN response equal the local IP address and port number that it bound to when sending the request:
 - Then the client is *NOT behind a NAT router*.
 - Otherwise, it is behind a NAT router.

NAT discovery – Full Cone (test 2)

- Full Cone NAT router – The client sets the IP address and port number flags in the CHANGE-REQUEST of the STUN request. This causes the server to send the response from the alternate IP and port number.
 - If the client *receives* the STUN response, then the client is behind *a full cone* router.
 - Otherwise, it is behind one of the other three NAT routers.

NAT discovery – Symmetric (test 3)

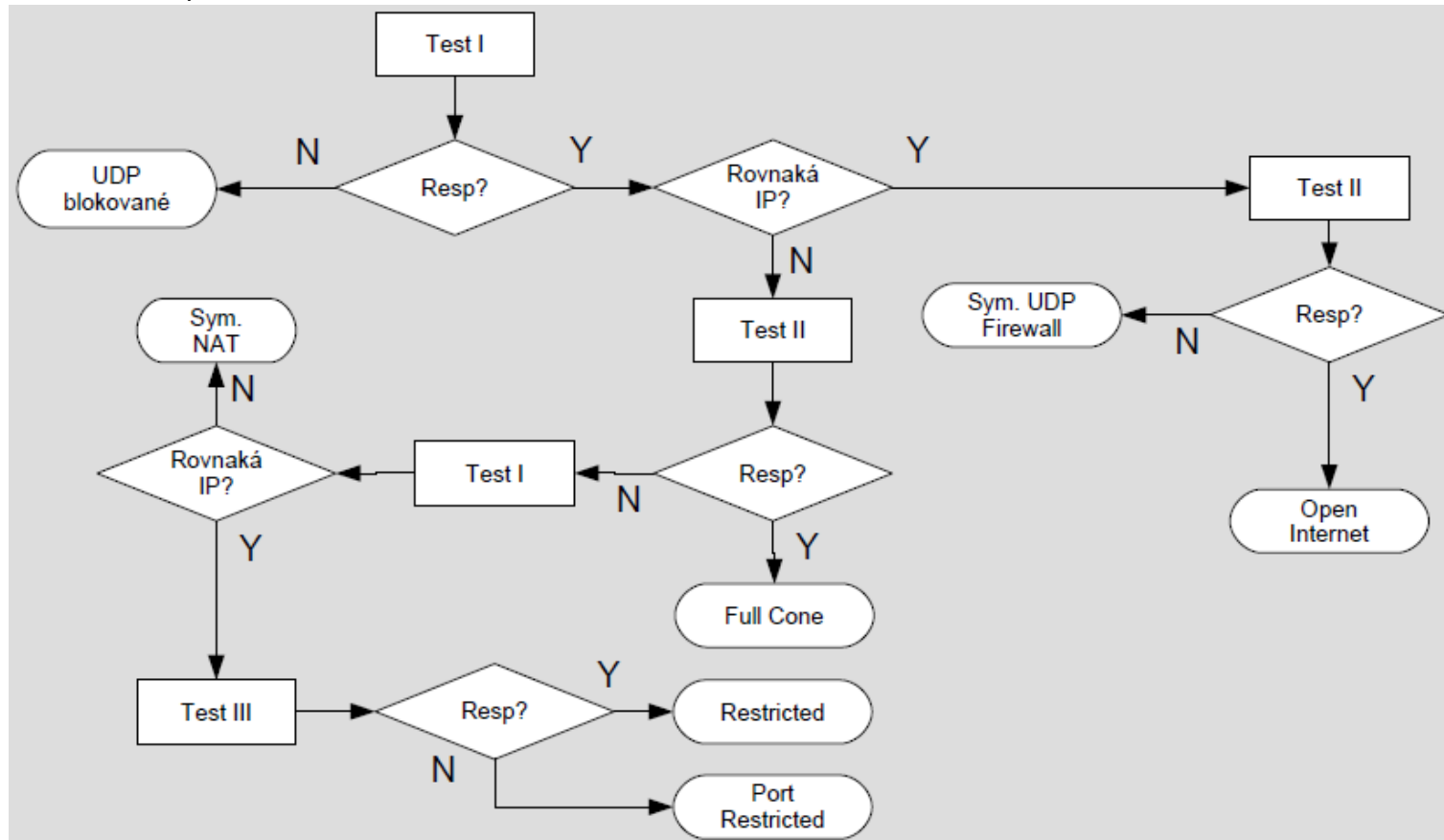
- Symmetric NAT – The client sends two STUN requests. One request is sent to a server at IP address X and port P, and another to a server at IP address Y and port P.
 - If the IP addresses and ports from the MAPPED-ADDRESS attributes in the two responses *do not match*, then it is behind a *Symmetric NAT* router.
 - If they do match, then it is behind one of the remaining two NAT routers.

NAT discovery – Restricted (test 4)

- Restricted NAT – The port flag in the CHANGE-REQUEST attribute of the request is set. This instructs the server to send a response from a different port.
 - If the response is *received*, it is behind a *restricted NAT* router.
 - If *no response* is received, it is behind a *port restricted* NAT router.

STUN flowchart

- I – BReq bez CHANGE-REQUEST a RESPONSE-ADDRESS
 - Som vôbec za NAT?
- II – BReq s vyžiadanou zmenou portu aj adresy v CHANGE-REQUEST
 - Som za Full cone NAT?
- III - BReq s vyžiadanou zmenou len portu v CHANGE-REQUEST
 - Za akým NAT teda som?



STUN na debiane

- `apt-get install stun`

Edituj súbor `/etc/default/stun`

```
# Defaults for stun initscript
# sourced by /etc/init.d/stun
# installed at /etc/default/stun by the maintainer scripts

#
# This is a POSIX shell fragment
#

# Uncomment the next line to allow the init.d script to start the stun daemon
START_DAEMON=true


# Additional options that are passed to the Daemon.
DAEMON_OPTS=""

PRIMARY_IP="158.193.152.1"
SECONDARY_IP="158.193.152.2"
PRIMARY_PORT=3478
SECONDARY_PORT=3479

# whom the daemons should run as
DAEMON_USER=nobody
```

Obmedzenia STUN

- Rieši hlavne príjem SIP volaní pre klientov za NAT
- Nepracuje s TCP
 - Riešenie cez STUNT (TCP NAT Traversal)
- Neumožňuje prechod prichádzajúcich spojení cez symetrický NAT
 - STUN nerieši všetky problémy s NAT dané NAT topológiami
- Takisto je problém s rôznymi implementáciami NAT
- Nepracuje ak **sú oba konce** za **tým istým** NAT
- Vyžaduje umiestnenie STUN servera na verejnej IP
- V prípade UDP spojení musia riešenia obsahovať nejaký KeepAlive mechanizmus!!



STUN RELAY (TURN)

Traversal Using Relay around NAT

- TURN je špecifikované v RFC5766
- Umožňuje klientom za NAT/FW prijať TCP or UDP spojenie
 - Dobre pracuje aj so symetrickým NAT
- Využíva medziľahlého hosta, ktorý slúži ako **relay** komunikačných spojení
 - TURN protokol umožňuje SIP UA získať IP adresu a port tohto relay hosta (TURN servera), od ktorého bude potom prijímať RTP média tok
 - Tým pádom sa nastaví v NAT (aj symetrickom) adekvátne mapovanie, vytvorené komunikáciou medzi SIP UA a TURN serverom
 - Celá RTP komunikácia na daného hosta, aj od viacerých peerov, ide cez TURN server (relay)
 - TURN protokol umožňuje kontrolu TURN relay servera klientom
- Navrhnutý ako súčasť väčšej ICE architektúry
 - A ako rozšírenie STUN

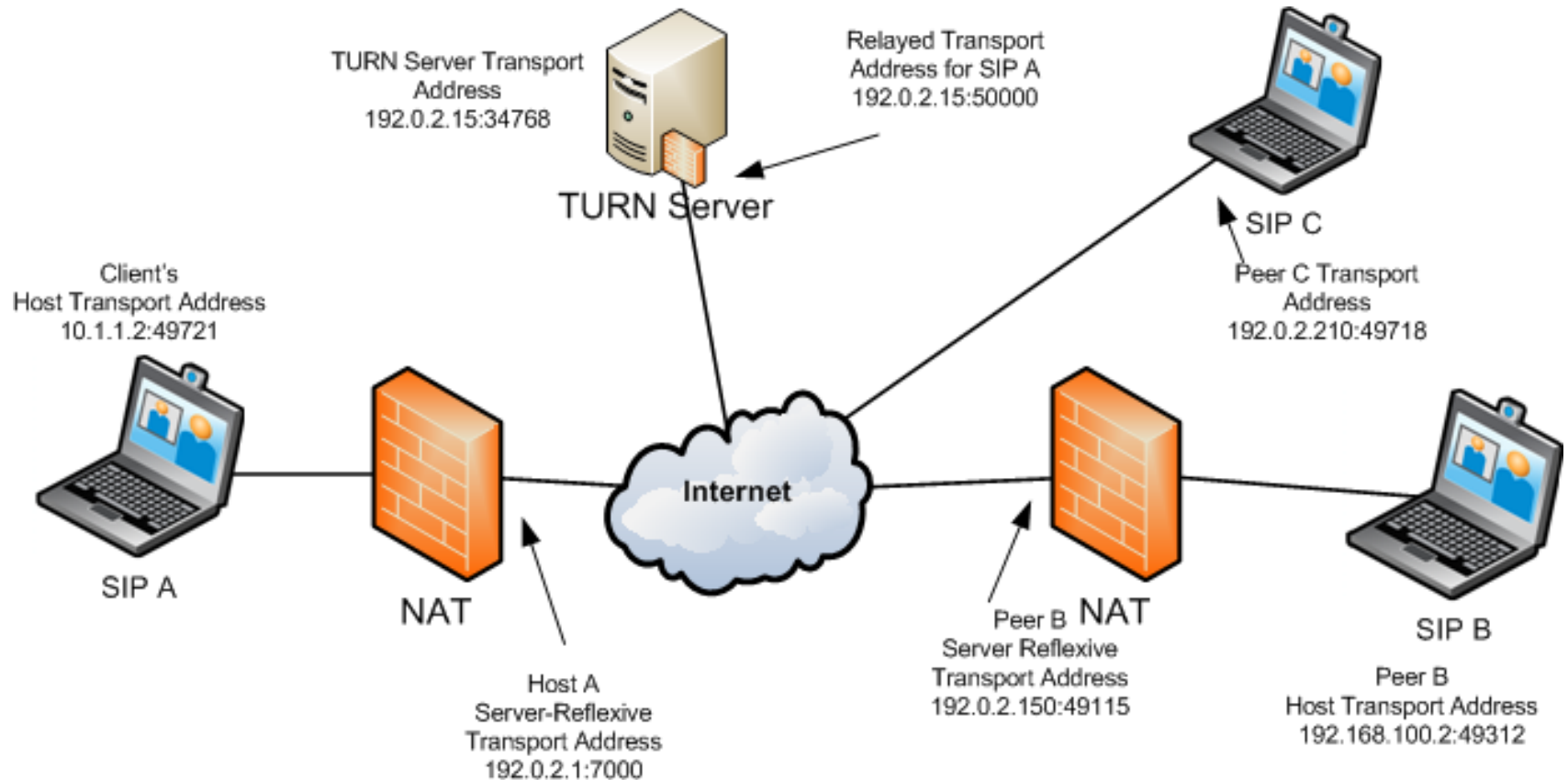
TURN vlastnosti

- TURN je klient/server
 - Komunikácia medzi klientom a serverom je enkapsulovaná v TURN správach
- TURN server (relay)
 - Slúži ako sprostredkovateľ
 - Umiestnený na verejnom Internet
- TURN klient
 - Je entita ktorá generuje TURN správy, ktorými žiada TURN server aby hral úlohu relay agenta
 - je zvyčajne zakomponovaná v SIP UA

TURN klient

- Žiada o pridelenie IP adresy a portu TURN servera
 - Volanú ***Relayed transport address***
- Ak SIP peer pošle správu na *Relayed transport address*, relay agent je prepošle na dané SIP UA, ktoré ju ma zarezervovanú
- Ak SIP klient pošle odpoveď na peera, TURN relay server použije *Relayed transport address* ako identifikátor zdroja
- Ako sa peer dozvie *Relayed transport address* TURN nedefinuje
 - Riešenia ako mail alebo cez tzv. Rendezvous protocol (RFC5128)
 - Môže ním byť SIP samotný
- Klient sa adresu servera musí nejako dozvedieť
- Klient udržiava svoje spojenie na server otvorené
 - keep alive mechanizmus

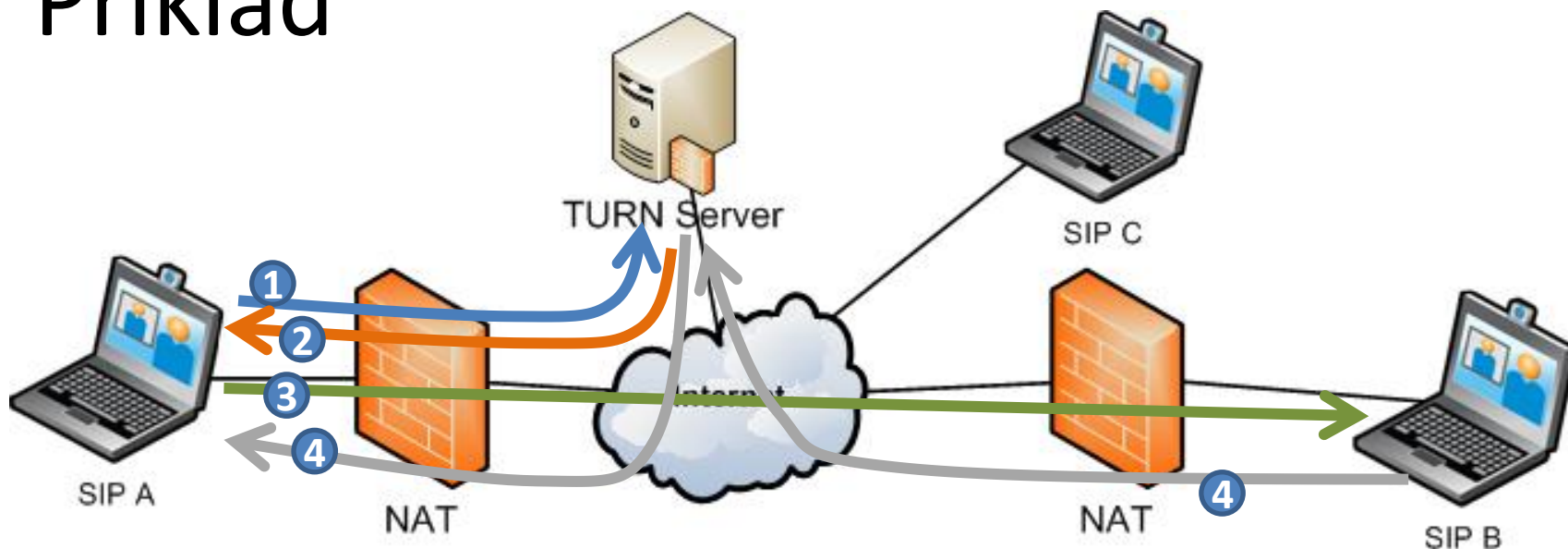
TURN - adresy



TURN adresy

- Server
 - Má pridelenú tzv. **TURN Server Transport Address** (IP adresa + port)
 - Klient sa ju musí nejako dozvedieť
 - DNS
 - Konfigurácia
- Klient
 - Má svoju Host Transport address
 - Privátna IP adresa
 - SERVER-REFLEXIVE transport address
 - Získaná natovaním ako ju vidí server pre žiadosti klienta
 - RELAYED TRANSPORT ADDRESS
 - Alokovaná TURN serverom pre relay

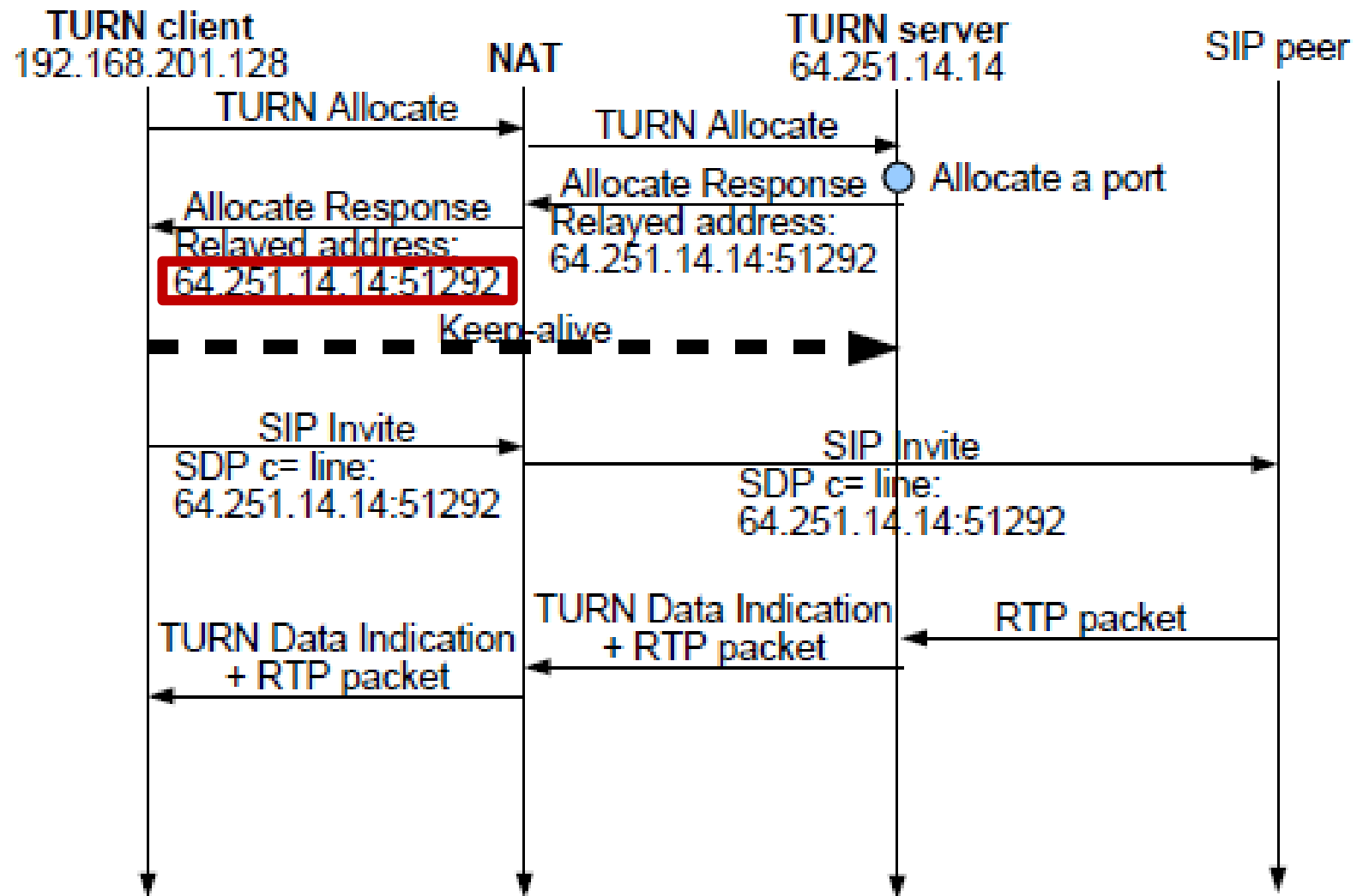
Príklad



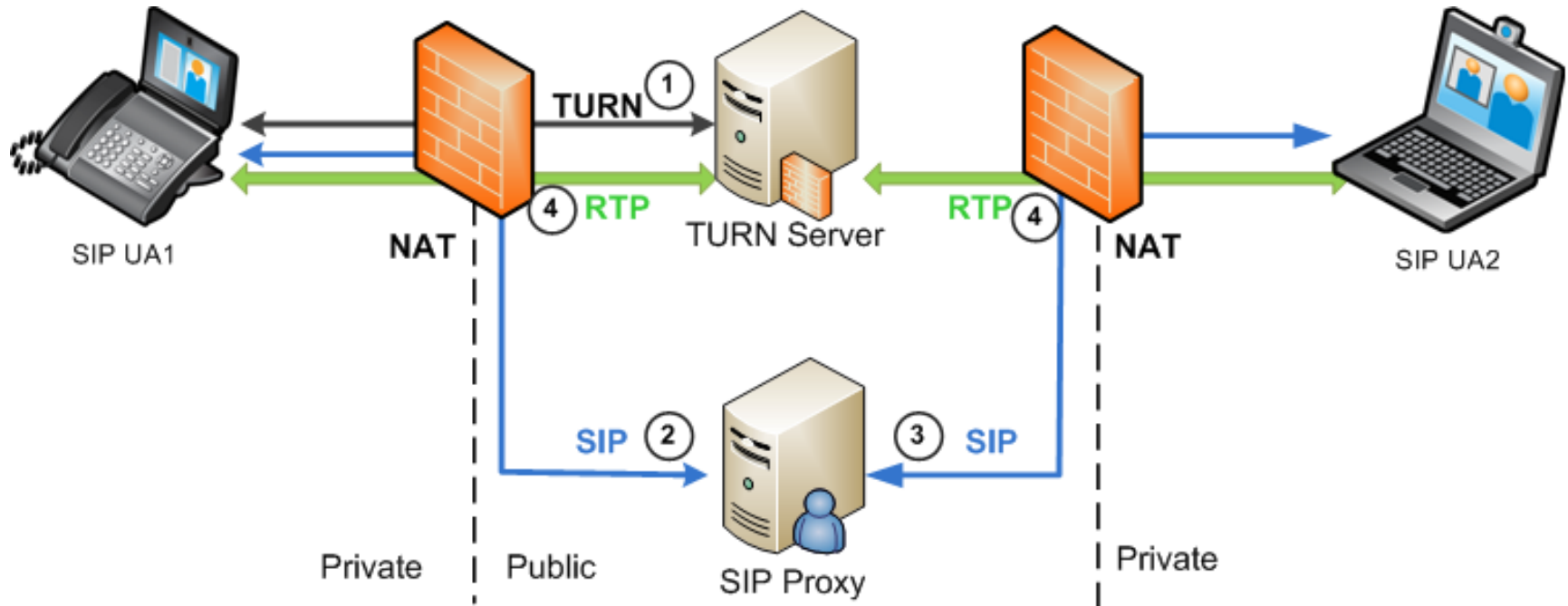
- 1) SIP A založí spojenie na TURN server
 - UDP or TCP (TLS)
- 2) SIP A prijme od TURN servera Relay Transport address, ktorú mu alokoval TURN server
- 3) SIP A musí nejakým spôsobom dať vedieť SIP B o získanej Transport relay adrese (SIP?)
- 4) SIP B založí spojenie na ponúkanú adresu (t.j. na TURN server) a ten spraví relay na SIP A

TURN server = STUN with relay capability

TURN Flow diagram



TURN



1. Na vyžiadanie TURN server vráti TURN klientovi globálnu IP adresu a port
 1. Relayed Transport Address (RTA)
2. SIP správa je modifikovaná s ohľadom na RTA a je odoslaná SIP Proxy
3. SIP je smerovaná na SIP UA2
 1. Musí byť otvorené a platné mapovanie v NAT
4. RTP je smerované cez TURN server

TURN záver

- Malo by to byť 100% riešenie na SIP NAT traversal
- Avšak
 - Je centrálnym prvkom
 - Problém s redundanciou a škálovateľnosťou
 - Ostáva v komunikačnej ceste
 - Riešiť zdroje
 - výkonnosť, šírku pásma
 - Implementácie nie sú veľmi rozšírené
 - Ani serverovské
 - Ani podpora v SIP UA
- Primárne je TURN pre UDP komunikáciu
- Pracuje sa na riešení TURN pre TCP

TURN riešenia

- Numb
 - <http://numb.viagenie.ca/>
- TurnServer
 - opensource
 - <http://turnserver.sourceforge.net/>
- Office SIP TURN server
 - Freeware
 - <http://www.officesip.com/>
- reTurn
 - Opensource
 - http://www.resiprocate.org/ReTurn_Overview
- Eyeball AnyFirewall

Odporúčanie

- Kde sa dá použiť STUN
 - Ak STUN nepracuje
- Použiť TURN
- **Riešenie známe ako**
ICE

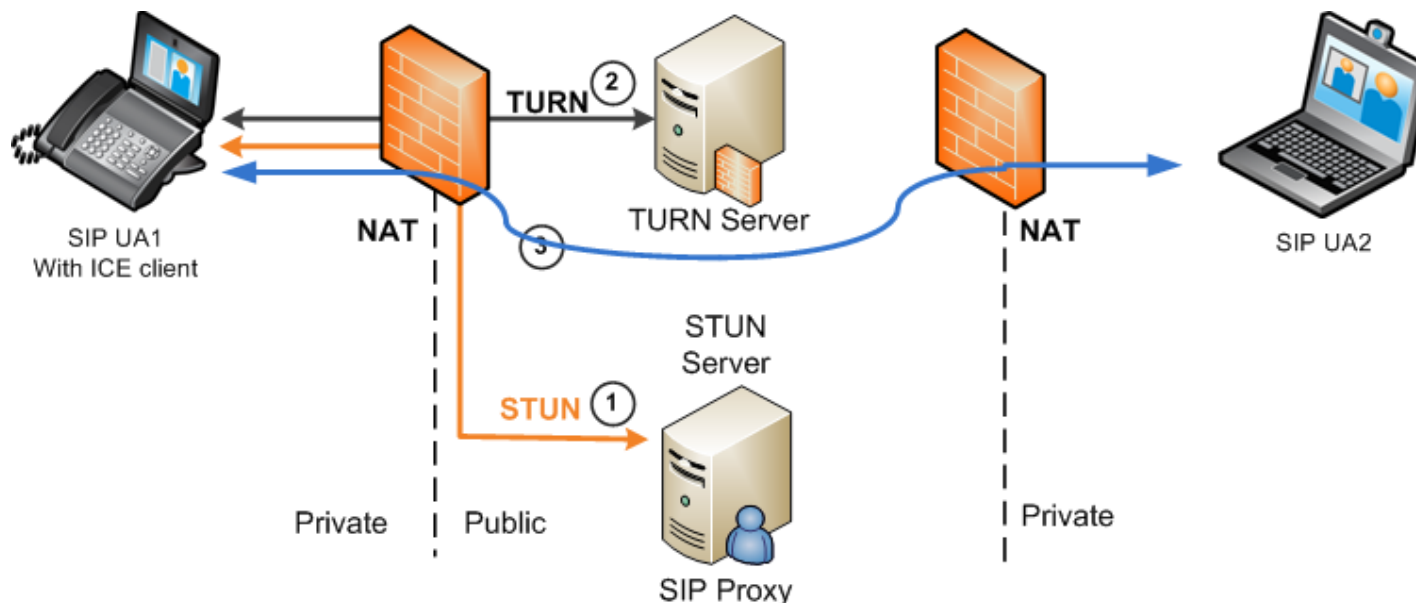


INTERACTIVE CONNECTIVITY ESTABLISHMENT (ICE)

Interactive Connectivity Establishment (ICE)

- RFC 5245 - Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- Konceptuálne jednoduché riešenie
- Spája súčasné riešenie STUN a TURN
 - Umožňuje nájsť vhodné riešenie komunikácie cez NAT/FW
- Pracuje so všetkými typmi NAT
- Umožňuje SIP peerom (ICE agentom) zistiť typ NAT a svoje možnosti komunikácie
 - Resp. vzájomnej dosažiteľnosti.
- Začína byť masívnejšie podporované výrobcami SIP UA
- Existuje rozšírenie SIP-u za účelom indikácie jeho využitia pri volaní na SIP UA
 - [RFC 5768](#) ICE Support

ICE call flow



1. UA 1 pomocou STUN servera zistí NAT a jeho typ
 - Plus akú verejnú IP a port NAT použil (Kandidát komunikácie 1)
2. Ako záložný plán si vyžiada od TURN servera relay transportnú adresu
 - (kandidát komunikácie 2)
3. SIP UA 1 pošle INVITE so zoznamom kandidátov komunikácie ako spôsobov jeho kontaktovania s preferovaným poradím
4. SIP UA 2 použije tento zoznam na kontaktovanie UA 1
 - Spôsob Pokus – omyl
 - A v správe 183 pošle zoznam svojich kandidátov komunikácie
5. Ak obaja majú vymenené svoje zoznamy vytvoria z nich kombináciami komunikačné páry a začnú si ich testovať
6. Testovanie je vykonávané posielaním STUN správ na komunikačného kandidáta suseda
7. Ak sa nájde cesta je poslaná 180 Ringing atď.

Kandidát komunikácie

- HOST CANDIDATE
 - A transport address on a directly attached network interface
- SERVER REFLEXIVE CANDIDATES
 - A translated transport address on the public side of a NAT (a "server reflexive" address)
 - Získané STUN
- RELAYED CANDIDATES
 - A transport address allocated from a TURN server (a "relayed address").



RTP (MEDIA) RELAY

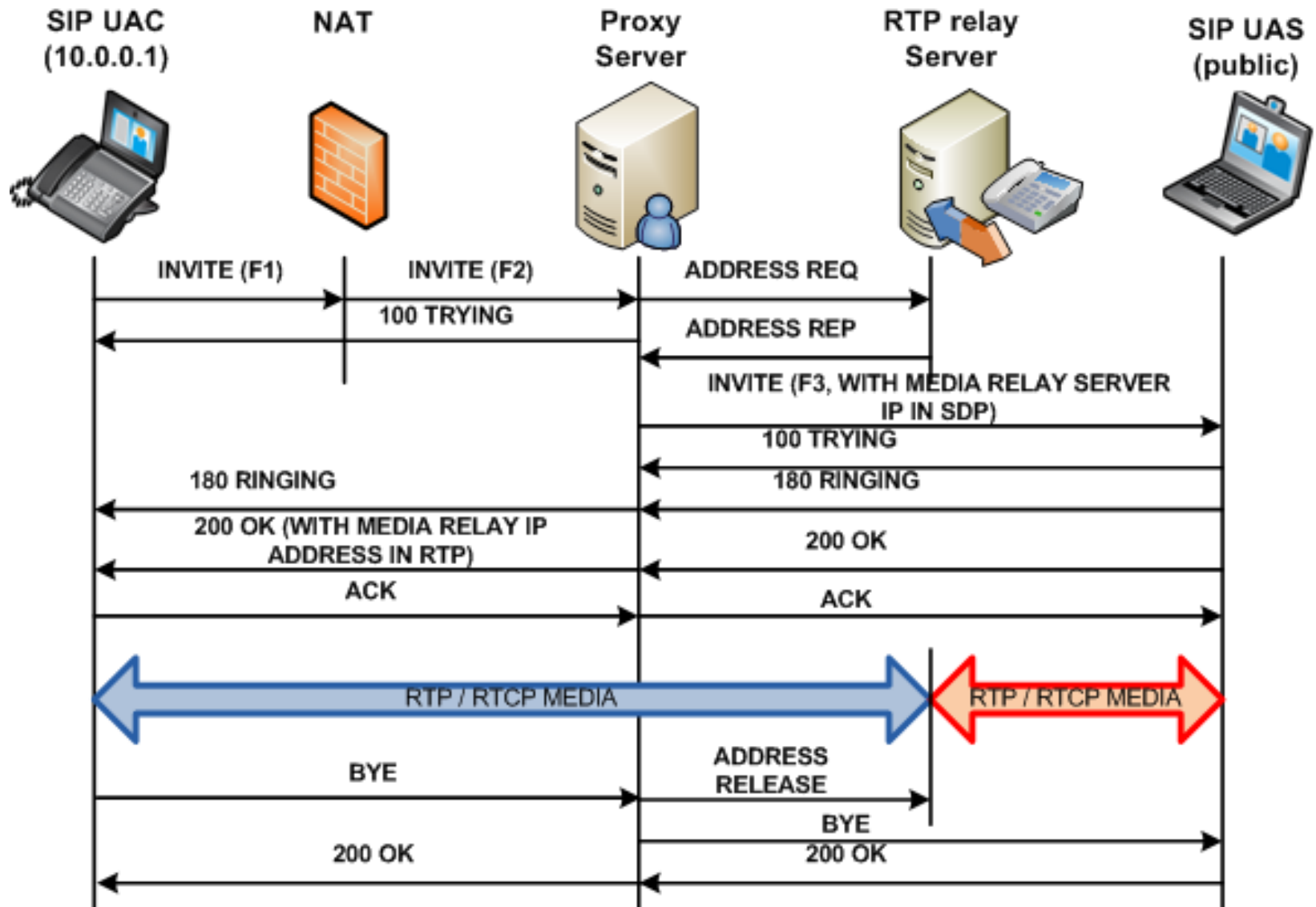
Riešenie Media relay

- Slúži ako prostredník pre RTP/RTCP a UDP prúdy dát
 - Vyžaduje podporu **Symetrického RTP**
 - Odosielanie aj príjem RTP médií z toho istého/na ten istý port
 - Vyžaduje zásah do konfigurácie SIP Proxy
 - Súčasné riešenia vhodné pre SER, OpenSER, Kamailio, OpenSIPS, SIP router, SIPPY B2BUA
- Zvýšená náročnosť na výkon
 - Nakoľko všetky RTP toky idú cez jeho prostriedky
 - Otázka škálovateľnosti

Súčasnú známe opensource riešenia

- Riešenie Sippy RTP Proxy
 - Sippy RTPproxy (známy aj ako NATHelper)
 - <http://www.rtpproxy.org/>
 - V repozitároch pre debian/ubuntu
- Media Proxy
 - <http://mediaproxy-ng.org>

Media Relay



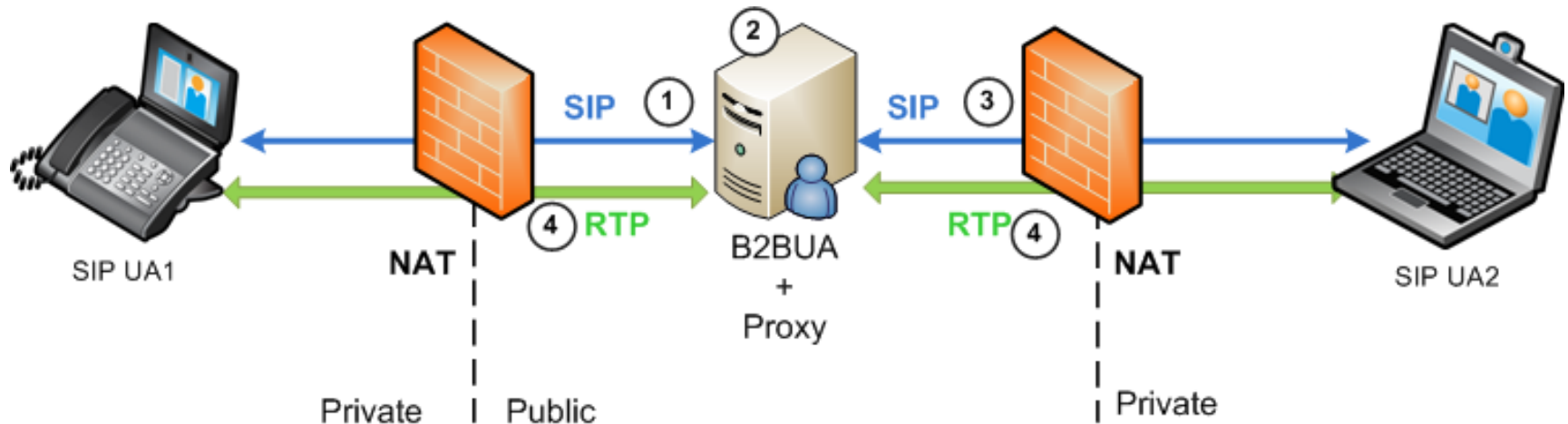



BACK 2 BACK USER AGENT


Back 2 Back User Agent

- Slúži ako (v spolupráci s) SIP gw pre signalizáciu a media proxy pre RTP
- Umiestnený na verejnom segmente
- Správa sa ako Man in the Middle
 - Bezpečnostná hrozba
 - Upravuje SIP signalizáciu aby ostal v ceste

B2BUA



1. UA pošle SIP INVITE na svoj Outbound Proxy (ktorý je aj B2BUA)
2. B2BUA modifikuje prechádzajúcu signalizáciu takým spôsobom aby ostal súčasťou tejto komunikácie (niečo ako Man in the Middle)
3. Modifikovaná SIP INVITE správa ide na SIP UA2 (musí byť v NAT/FW udržiavaná alebo otvorená „diera“) 
 1. 200OK ide späť cez B2BUA a ten ju modifikuje aby ostal v media ceste pre RTP od UA1
4. RTP ide medzi UAs cez B2BUA
 1. NAT je otvorený prvým RTP paketom



APPLICATION LAYER GATEWAY (ALG)

ALG

- Firewall, ktorý rozumie aplikačným protokolom
 - T.j. SIP signalizácii a SDP
 - Otvára „diery“ na požiadanie
 - Prechodom SIP cez FW plynule prepisuje odpovedajúce hlavičky správ podľa NAT mapovaní
 - Udržiava mapovanie (spojenie) otvorené.



UNIVERSAL PLUG AND PLAY

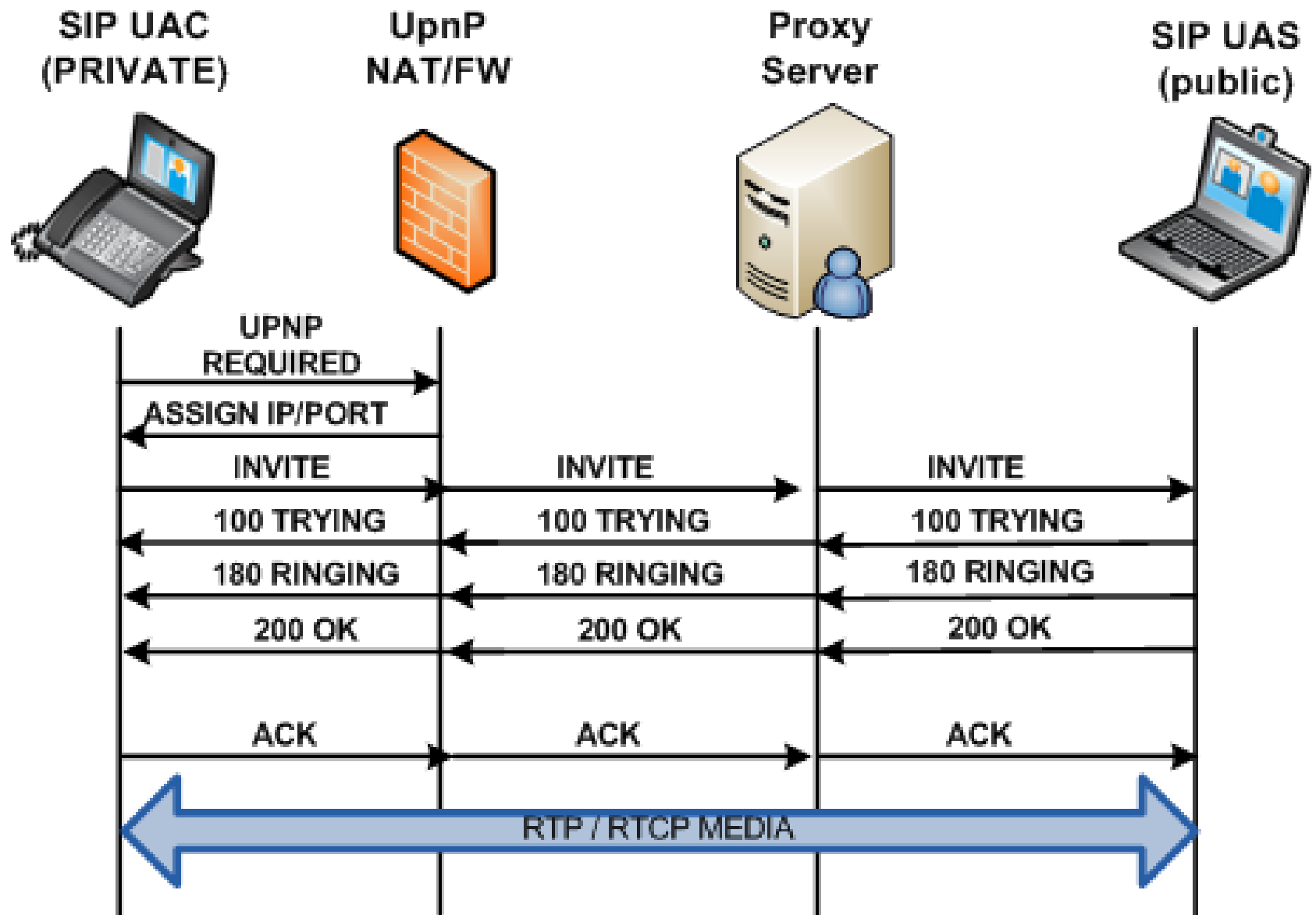
Čo je UPnP (www.upnp.org)

- Poskytuje prostriedky pre zjednodušené sieťové prostredie SOHO
 - domácnosti a malé firmy (*Small Office / Home Office*)
- Poskytuje framework pre auto konfiguráciu a auto popisovanie zariadení
 - Využíva existujúce internetové technológie
 - HTTP, XML
 - Umožňuje dynamické peer to peer prostredie
- Riešenie pre prepojenú, zosieťovanú domácnosť
 - Používateľský mainstream
 - Žiadne potrebné expertné zručnosti
- UPnP je zahrnuté v DLNA
 - *Digital Living Network Alliance*

UPnP

- Použitím UPnP požadujem od NAT aby „*otvoril dieru*„ pre komunikáciu a vrátil späť verejnú IP a port, ktorý bude pridelený
- Nasadenie v SOHO prostredí spolu s ATA (Analog Telephone Adapter)
- UPnP zariadenie očakáva, že aplikácia bude „hovoriť“ jazykom UPnP

UPnP



UPnP

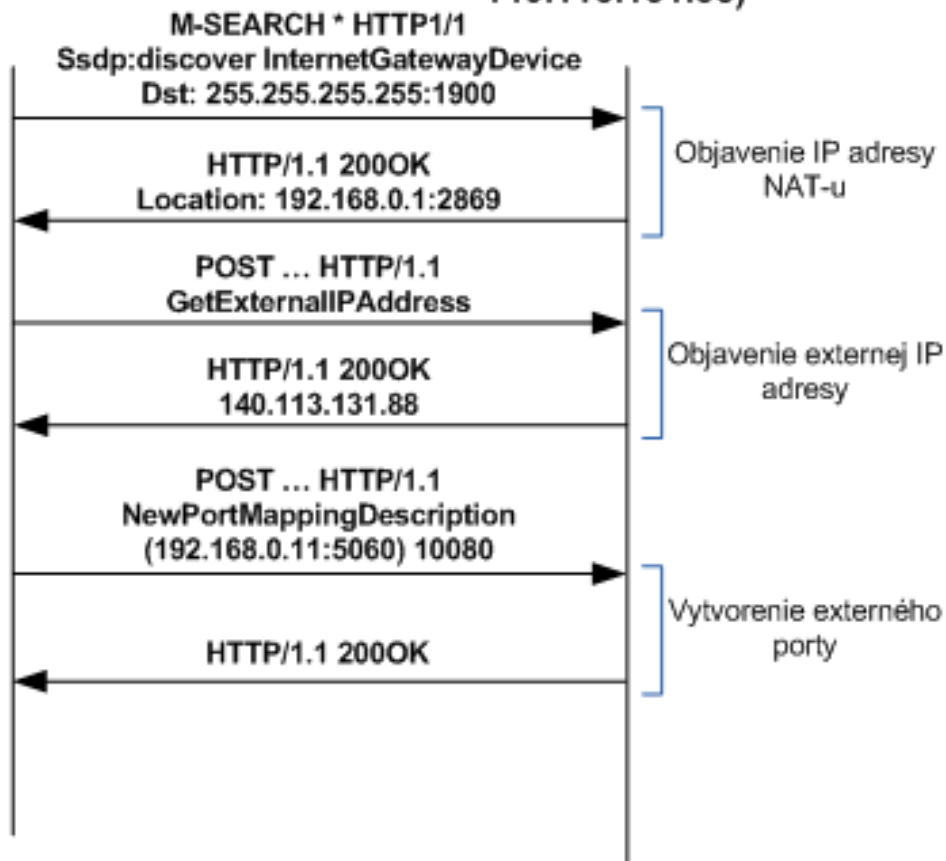


UPnP klient



NAT

(192.168.0.1/
140.113.131.88)





Final Solution

IPv6