Real-time Communication Protocols
Real-time Communication Applications
Protocols

sip & xmpp
The basics of IP telephony
Registration

- Authentication uses http-style digest MD5 challenges
- Content can be protected with TLS but ...
  - SIP often uses plain UDP
  - XMPP almost always OK

Bob
Address: B
Port: Pb

Alice
Address: A
Port: Pa

network core
(registrars, proxies, ...)

REGISTRATION
Inter-Server Communication

SIP: SMTP-like (no real limitation)

XMPP: Requires TLS and use of certificates

end-to-end encryption for IM uses OTR

(Off The Record messaging)
The basics of IP telephony
A sample call

Bob
Address: B
Port: Pb

Alice
Address: A
Port: Pa

network core
(registrars, proxies, ...)

Call:
To: A
Media: B:Pb
The basics of IP telephony
A sample call

Bob
Address: B
Port: Pb

Alice
Address: A
Port: Pa

network core
(registrars, proxies, ...)

Answer:
To: B
Media: A:Pa
The basics of IP telephony.

**Alice**
Address: A
Port: Pa

**Bob**
Address: B
Port: Pb

**network core**
(registrars, proxies, ...)

... MEDIA over (S)RTP ...

OSSIR, November 2010 emil.ivov@sip-communicator.org 8/45
 Encrypting RTP

- SRTP provides tools for encrypting RTP flows
- Key management was commonly based on PKIs until
- ZRTP arrived with an alternative
Reality check!

Are we forgetting something?
Standard NAT use
Less standard NAT usage: End – to – end services
Session initialization with SIP and XMPP

INVITE sip:barbara@b.com SIP/2.0
Via: SIP/2.0/UDP 10.43.122.3;branch=cl39ge
From: sip:alice@a.com;tag=4ad340f
To: sip:barbara@b.com
Contact: <sip:alice@10.43.122.3>
Call-ID: 1874630@10.43.122.3
Cseq: 12442 INVITE

v=0
o=alice 14341433 14341433 IP4 10.43.122.3
s=.
t=0 0
c=IN IP4 10.43.122.3
m=audio 13222 RTP/AVP 0
a=rtpmap:0 PCMU/8000

<iq from='juliet@capulet.lit/balcony'
id='hs81w639'
to='romeo@montague.lit/orchard'
type='set'>
</iq>

<jingle xmlns='urn:xmpp:jingle:1'
action='session-accept'
initiator='romeo@montague.lit/orchard'
responder='juliet@capulet.lit/balcony'
sid='a73sjjvkla37jfea'>
<content creator='initiator' name='voice'>
<description xmlns='urn:xmpp:jingle:apps:rtp:1' media='audio'>
<payload-type id='18' name='G729'/>
</description>
<transport xmlns='urn:xmpp:jingle:transports:raw-udp:1'>
<candidate component='1'
generation='0'
id='z7adjb01hf'
ip='208.68.163.214'
port='9876'/>
<candidate component='2'
generation='0'
id='hg92ls910b'
ip='208.68.163.214'
port='9877'/>
</transport>
</content>
</jingle>
</iq>
And then NATs were born …
How do NATs work …

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12 : 2368</td>
<td>8632</td>
</tr>
</tbody>
</table>

Alice
192.168.0.12

**MSG:**
- **Dst:** 130.79.200.22 : 80
- **Src:** 192.168.0.12 : 2368

Internal Address: 192.168.0.254

NAT

**MSG:**
- **Dst:** 130.79.200.22 : 80
- **Src:** 212.50.2.18 : 8632

Public Address: 212.50.4.18

Server
Address: 130.79.200.22
How do NATs work ...

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12 : 2368</td>
<td>8632</td>
</tr>
</tbody>
</table>

**Alice**

- Internal Address: 192.168.0.12
- MSG: Dst: 192.168.0.12 : 2368
  - Src: 130.79.200.22 : 80

**NAT**

- Internal Address: 192.168.0.254
- Public Address: 212.50.4.18

**Server**

- Address: 130.79.200.22
- MSG: Dst: 212.50.4.18 : 8632
  - Src: 130.79.200.22 : 80
How do NATs work …

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12 : 2368</td>
<td>8632</td>
</tr>
</tbody>
</table>

**Endpoint-Independent Mapping**

**Endpoint-Independent Filtering**

Alice

192.168.0.12

NAT Internal Address: 192.168.0.254

MSG: Dst: 192.168.0.12 : 2368
Src: 60.55.68.53 : 9595

NAT Public Address: 212.50.4.18

Server Address: 130.79.200.22

Bob

Address: 60.55.68.53

MSG: Dst: 212.50.4.18 : 8632
Src: 60.55.68.53 : 9595
Basic Firewall and NAT Traversal

STUN

What are my address and port?

Address: F
Port: Pf

STUN Server

Alice
Address: Ap
Port: Pa

Bob
Address: B

Call:
To: B
Media: F:Pf

STUN Server

Answer:
To: A
Media: B

Alice
Address: Ap
Port: Pa

Bob
Address: B
How do NATs work …
Address (and port) dependent filtering

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
<th>Active connections host:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12 : 2368</td>
<td>8632</td>
<td>130.79.200.22 (: 80)</td>
</tr>
</tbody>
</table>

MSG: Dst: 130.79.200.22 : 80
Src: 192.168.0.12 : 2368

Alice
192.168.0.12

NAT
Internal Address: 192.168.0.254

NAT
Public Address: 212.50.4.18

STUN Server
Address: 130.79.200.22
How do NATs work …
Address (and port) dependent filtering

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
<th>Active connections host:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12 : 2368</td>
<td>8632</td>
<td>130.79.200.22 (: 80)</td>
</tr>
</tbody>
</table>

**Alice**
Internal Address: 192.168.0.12

**MSG:**
Dst: 192.168.0.12 : 2368
Src: 130.79.200.22 : 80

**NAT**
Internal Address: 192.168.0.254

**MSG:**
Dst: 212.50.4.18 : 8632
Src: 130.79.200.22 : 80

**NAT**
Public Address: 212.50.4.18

**STUN Server**
Address: 130.79.200.22
How do NATs work …
Address (and port) dependent filtering

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
<th>Active connections host:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12 : 2368</td>
<td>8632</td>
<td>130.79.200.22 (: 80)</td>
</tr>
</tbody>
</table>

**Endpoint-Independent Mapping**

**Endpoint-Dependent Filtering**

Alice
192.168.0.12

NAT
Internal Address: 192.168.0.254

NAT
Public Address: 212.50.4.18

STUN Server
Address: 130.79.200.22

MSG: Dst: 212.50.4.18 : 8632
Src: 60.55.68.53 : 9595

Bob
Address: 60.55.68.53
How do NATs work …
Address (and port) dependent filtering

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
<th>Active connections host:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12 : 2368</td>
<td>8632</td>
<td>130.79.200.22 (: 80)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>60.55.68.53 (: 80)</td>
</tr>
</tbody>
</table>

Alice
192.168.0.12

NAT
Internal Address: 192.168.0.254

NAT
Public Address: 212.50.4.18

STUN Server
Address: 130.79.200.22

Bob
Address: 60.55.68.53

MSG:
Dst: 60.55.68.53 : 80
Src: 192.168.0.12 : 2368

MSG:
Dst: 60.55.68.53 : 80
Src: 212.50.4.18 : 8632
How do NATs work …
Address (and port) dependent filtering

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
<th>Active connections host:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12 : 2368</td>
<td>8632</td>
<td>130.79.200.22 (: 80)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>60.55.68.53 (: 80)</td>
</tr>
</tbody>
</table>

Endpoint-Independent Mapping
Endpoint-Dependent Filtering

MSG: Dst: 192.168.0.12 : 2368
Src: 60.55.68.53 : 80

Alice
192.168.0.12

Internal Address: 192.168.0.254

NAT

STUN Server
Address: 130.79.200.22

Address: 60.55.68.53

Bob

MSG: Dst: 212.50.4.18 : 8632
Src: 60.55.68.53 : 80

192.168.0.12 : 2368
60.55.68.53 : 80
How do NATs work …
Endpoint dependent mapping

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
<th>Active connections host:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12 : 2368</td>
<td>8632</td>
<td>130.79.200.22 (: 80)</td>
</tr>
</tbody>
</table>

**Diagram:**
- **Alice** with Internal Address: 192.168.0.12
  - Sends message to **NAT** with Internal Address: 192.168.0.254, Port: 2368
  - **NAT** maps to **STUN Server** with Public Address: 212.50.4.18, Port: 8632
- **NAT** sends response to **STUN Server** with Public Address: 130.79.200.22, Port: 80
  - STUN Server then sends message to **Alice**

**Messages:**
- **MSG:** Dst: 130.79.200.22 : 80
  - Src: 192.168.0.12 : 2368
- **MSG:** Dst: 130.79.200.22 : 80
  - Src: 212.50.4.18 : 8632
How do NATs work …
Endpoint dependent mapping

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
<th>Active connections host:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12:2368</td>
<td>8632</td>
<td>130.79.200.22 (: 80)</td>
</tr>
</tbody>
</table>

MSG:
Dst: 192.168.0.12:2368
Src: 130.79.200.22:80

MSG:
Dst: 212.50.4.18:8632
Src: 130.79.200.22:80

NAT Internal Address: 192.168.0.254

NAT Public Address: 212.50.4.18

STUN Server Address: 130.79.200.22
How do NATs work …

Endpoint dependent mapping

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
<th>Active connections host:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12 : 2368</td>
<td>8632</td>
<td>130.79.200.22 (: 80)</td>
</tr>
<tr>
<td>192.168.0.12 : 2368</td>
<td>9391</td>
<td>60.55.68.53 (: 80)</td>
</tr>
</tbody>
</table>

Alice
192.168.0.12

STUN Server
Address: 130.79.200.22
Public Address: 212.50.4.18

NAT
Internal Address: 192.168.0.254

NAT
Public Address: 212.50.4.18

MSG:
Dst: 60.55.68.53 : 80
Src: 192.168.0.12 : 2368

Bob
Address: 60.55.68.53

MSG:
Dst: 60.55.68.53 : 80
Src: 212.50.4.18 : 9391
How do NATs work …
Endpoint dependent mapping

<table>
<thead>
<tr>
<th>Internal host:port</th>
<th>NAT port</th>
<th>Active connections host:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.12 : 2368</td>
<td>8632</td>
<td>130.79.200.22 (: 80)</td>
</tr>
<tr>
<td>192.168.0.12 : 2368</td>
<td>9391</td>
<td>60.55.68.53 (: 80)</td>
</tr>
</tbody>
</table>

Endpoint-Dependent Mapping
Endpoint-Dependent Filtering

Alice
192.168.0.12

NAT
Internal Address: 192.168.0.254

NAT
Public Address: 212.50.4.18

MSG:
Dst: 192.168.0.12 : 2368
Src: 60.55.68.53 : 80

Bob
Address: 60.55.68.53

MSG:
Dst: 212.50.4.18 : 8632
Src: 60.55.68.53 : 80

STUN Server
Address: 130.79.200.22
Universal Plug and Play (UPnP)

Designed for zero-configuration networking and to allow devices to:

- dynamically join a network and obtain an IP address
- announce its name
- advertise capabilities
- discover other devices and their capabilities

Makes it easy to:

- Learn the external (public) address of an internet gateway
- Enumerate existing port mappings
- Add and remove port mappings
- Assign lease times to mappings

www.upnp.org
Relaying Media

Symmetric NAT/Firewall $F1:p1$

TURN Server
Address: $T$
Port: $Pt$

Reserve port

Call:
To: $B$
Media: $T:Pt$

Bob
Address: $B$

Alice
Address: $Ap$
Port: $Pa$

Symmetric NAT/Firewall $F1:p2$

Call:
To: $B$
Media: $T:Pt$

Reply: $T:Pt$
**Relaying Media**

Symmetric NAT/Firewall $F1:p1$

**TURN Server**
- Address: $T$
- Port: $Pt$

**Alice**
- Address: $Ap$
- Port: $Pa$

**Bob**
- Address: $B$

Symmetric NAT/Firewall $F1:p2$
Relaying Media The SIP Way

Latching
Relaying Media The SIP Way
Latching

NAT/Firewall

SIP Server
Address: T
Port: Pt

Alice
Address: Ap
Port: Pa

Bob
Address: B
Relaying Media

SIP clients behind a symmetric NAT/firewall

non-scalable expensive complex

SIP clients behind a symmetric NAT/firewall

Relay Server

symmetric firewall

symmetric NAT/firewall
Using P2P networks for NAT Traversal

- Skype – among the first to implement the technique
- P2PSIP – set off to imitate Skype. No conclusive results after four years
- Jingle Nodes – an interesting alternative that is worth keeping an eye on
Could we please have IPv6 now?

... ok, it’s probably high time we moved to IPv6 ...
Could we please have IPv6 now?

… this should simplify VoIP

… shouldn’t it?
VoIP and IPv6 – demo version

Call:
To: 2001:660::1
Media: 2001:660::1

network core
(registrars, proxies, ...)

Bob
2001:660::1

Alice
2001:660::2
VoIP and IPv6 – demo version

network core
(registrars, proxies, ...)

Alice
2001:660::2

Answer:
To: 2001:660::1
Media: 2001:660::2

Bob
2001:660::1
VoIP and IPv6 – demo version

Bob
2001:660::1

Alice
2001:660::2

network core
(registrars, proxies, ...)

... MEDIA ...

OSSIR, November 2010
emil.ivov@sip-communicator.org
Reality check!

Reality check!
Reality check!

Alice’s list of addresses:
2001:660::2
192.168.0.6
172.16.0.9
130.79.12.64
64.233.187.99
212.50.4.12
How to avoid relaying?

Interactive Connectivity Establishment (ICE)

An IETF RFC brought to you by Cisco’s Jonathan Rosenberg
Address management with ICE

Alice’s list of addresses:
- 2001:660::2
- 192.168.0.6
- 172.16.0.9
- 130.79.12.64
- 64.233.187.99
- 212.50.4.12

Please try me on any of the following:
- 2001:660::2
- 192.168.0.6
- 172.16.0.9
- 130.79.12.64
- 64.233.187.99
- 212.50.4.12
Address management with ICE

Alice's list of addresses:
- 2001:660::2
- 192.168.0.6
- 172.16.0.9
- 130.79.12.64
- 64.233.187.99
- 212.50.4.12

Bob
- 216.109.112.135
- 192.168.0.6
- 2001:660::2

SIP network

Stun Relay Server
- 212.50.4.12

VPN
- Priv: 172.16.0.0
- Pub: 64.233.187.99

NAT
- 192.168.0.6
- 172.16.0.9
- 2001:660::2

ERROR
- 192.168.0.6
- 172.16.0.9
- 2001:660::2
Real-time Communication 101

NAT and Firewall Traversal