



SIPのNAT越え

渡邊研究室

030432047

葛谷章一

目次

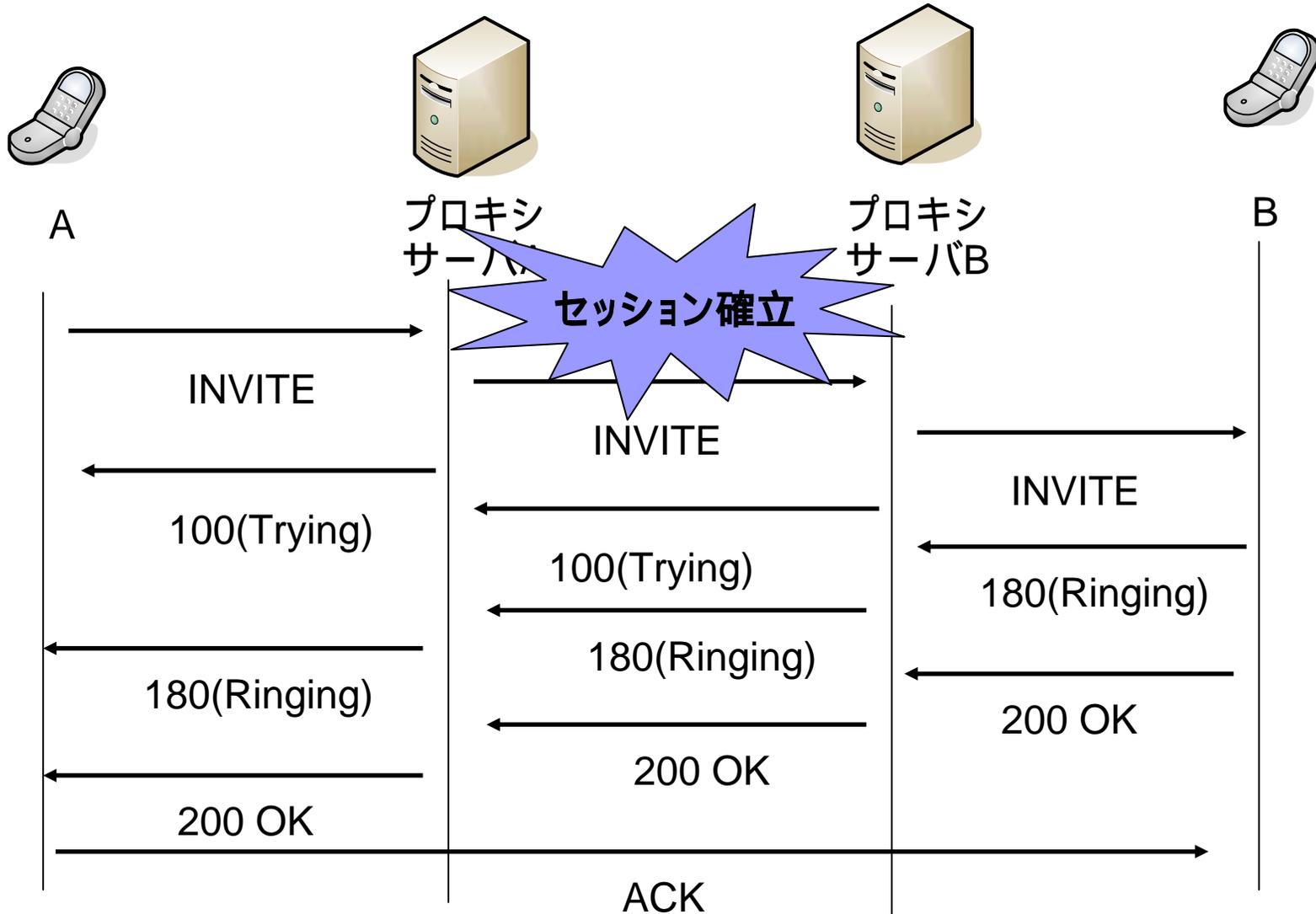
- 1章 SIPとNAT
- 2章 ICE
- 3章 STUNとTURNの処理
- 4章 使用事例の代表例

1章 SIPとNAT

SIPとは

- Session Initiation Protocolの略
- アプリケーション層で使用する。
- 2つ以上のクライアントに対して、音声や映像などの交換などを行うために必要なセッションの生成・変更・切断を行うプロトコルです。

SIPの動作

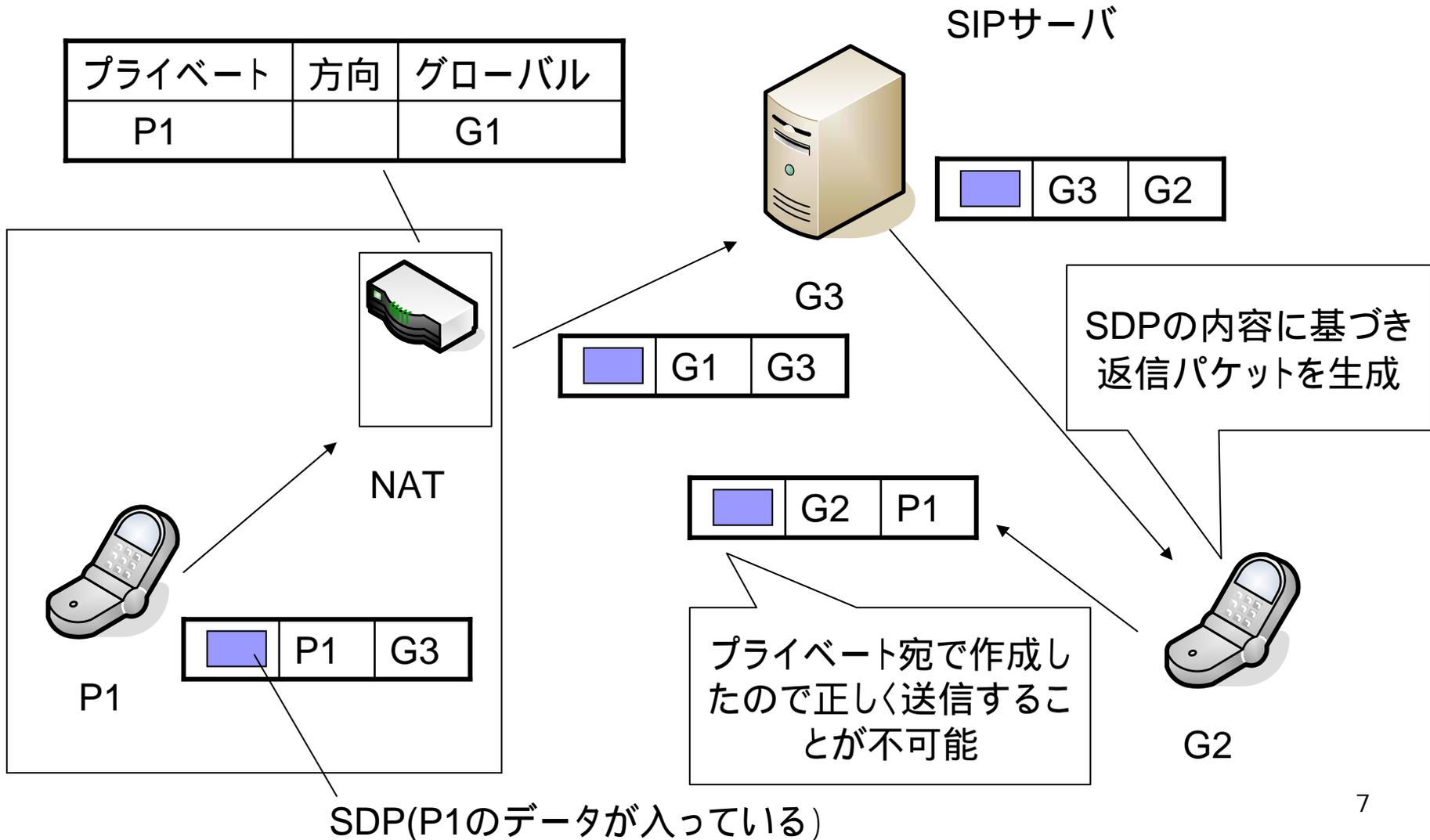


NAT

- NATとは

LAN内で使われるプライベート・アドレスとインターネットで使われるグローバル・アドレスを変換する技術を指す。

SIPのNAT越え問題



2章 ICE

ICEとは

- Interactive Connectivity Establishmentの略
- 特徴
 - ・新しいプロトコルではない
 - ・既存のプロトコルであるSTUNやTURNなど拡張せずに使用

STUN (Simple Traversal of UDP through NAT)
TURN (Traversal Using Relay NAT)

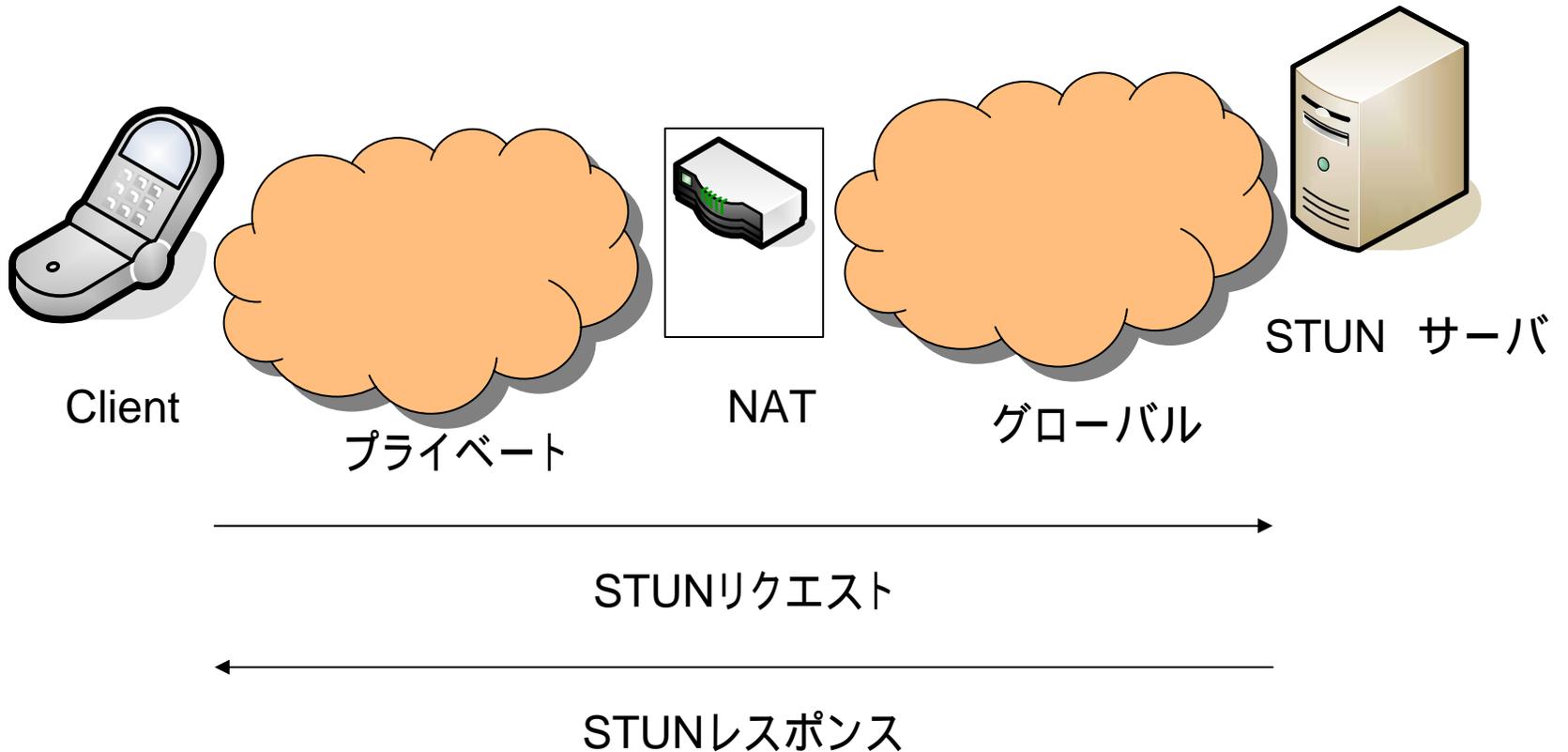
STUNとは

- Simple Traversal of UDP through NATの略

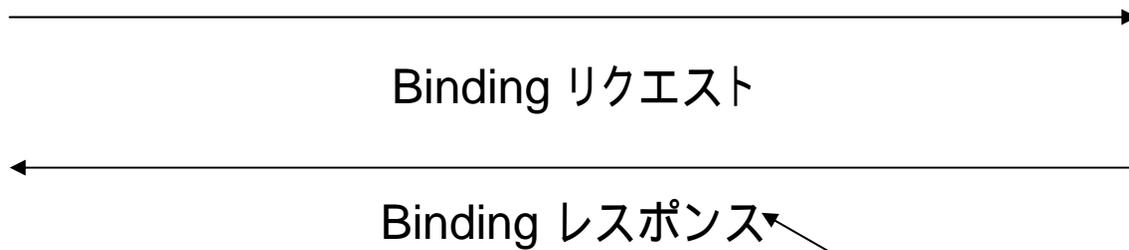
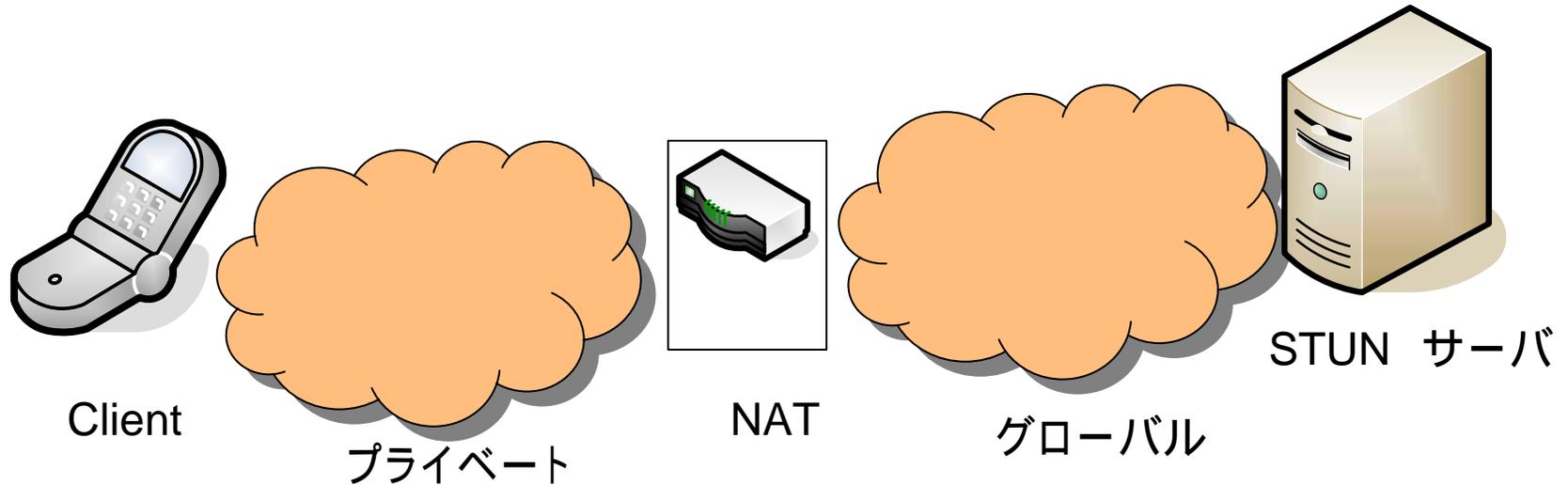
- 目的

グローバル側からプライベート側へのパケット
通過を可能にするためにNATのグローバル
側のアドレスとポートを検出すること

STUN (サーバー認証)



STUN (アドレス判定)



NATのグローバル側のアドレス (MAPPED-ADDRESS)
STUNサーバのアドレス (SOURCE-ADDRESS)
をクライアントに通知

TURNとは

- Traversal Using Relay NATの略
- TCPまたはUDPの接続上に入って来るデータを受け取れることをNATかファイアウォールの後ろの要素のために可能にする単純なプロトコルです。

ICEアルゴリズムとは

■ ICEアルゴリズム

2つの実体が接続しようとして互いのアドレスを交換することを反復するプロセス

■ 概要

- ・SIPは使える可能性のあるアドレスを調べて集める
- ・IPアドレスの優先順位をつける
- ・優先順位をつけたIPアドレスを順番に使用して、パケットを送受信をテストする
- ・成功したらメディアストリームを確立する



A



B



集めたTransportアドレスを送信する



集めたTransportアドレスを送信する

接続性チェック

接続性チェック

メディアストリームを確立

アドレスとポートを集める処理

- 集めるアドレス (Transportアドレス)
 - Local Transport Addresses
 - Derived Transport Addresses
- Local Transport Addresses
 - ホストのOSから割り当てられたアドレス
- Derived Transport Addresses
 - STUNやTURNを使用して得られるアドレス

■ Derived Transport Addresses

事前にDerived Transport Addressesの1つをTURNやSTUNサーバから最低1つは受信する必要があります。

■ Local Transport Addresses

インターフェース上で一時的なポート結合することにより得ることができる。

優先Transportアドレスを決める

■ 優先順位の高い

IPv6アドレス

IPv4アドレス

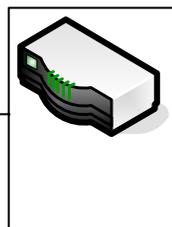
STUNから割り当てられたNAT上のIPアドレス

TURNとVPNなどプロトコルを通して割り当てられたアドレス

3章 STUNとTURNの処理



Client A
10.0.1.1:8866

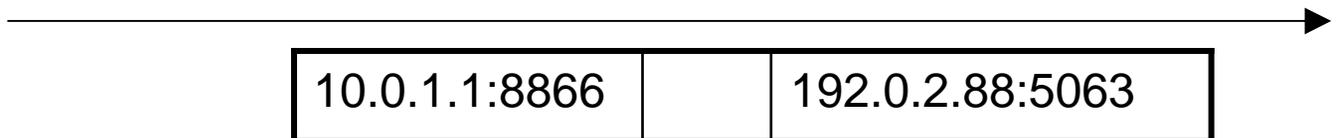


NAT



TURNサーバー
192.0.2.1:7764

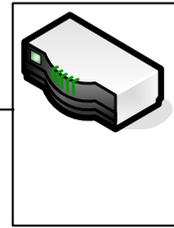
TURNサーバーにTURNリクエストを送信



192.0.2.1:26524を割り当て、TURNレスポンスを送信

これにより、TURNサーバーからクライアントAに送られる全てのデータを192.0.2.1から10.0.1.1に送られることを念頭におくようになる

Client A
10.0.1.1:8866



NAT

TURNサーバー
192.0.2.1:7764

クライアントAは
10.0.1.1上でSTUN
サーバーを動かします。

STUN
サーバー

STUNサーバーが
192.0.2.1:26524 上で動くと
広告する

Client B
192.0.2.77:1296

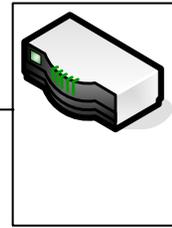


STUNリクエスト

192.0.2.88 10.0.1.1

ソースアドレス	終点アドレス
192.0.2.1:7762	192.0.2.88:

Client A
10.0.1.1:8866



NAT

TURNサーバー
192.0.2.1:7764

クライアントAは
10.0.1.1上でSTUN
サーバーを動かします。

STUN
サーバー

STUNサーバーが
192.0.2.1:26524 上で動く
と広告する

Client B
192.0.2.77:1296



STUNレスポンス

ソースアドレス	終点アドレス
10.0.1.1:8866	192.0.2.1:7764

STUNレスポンス

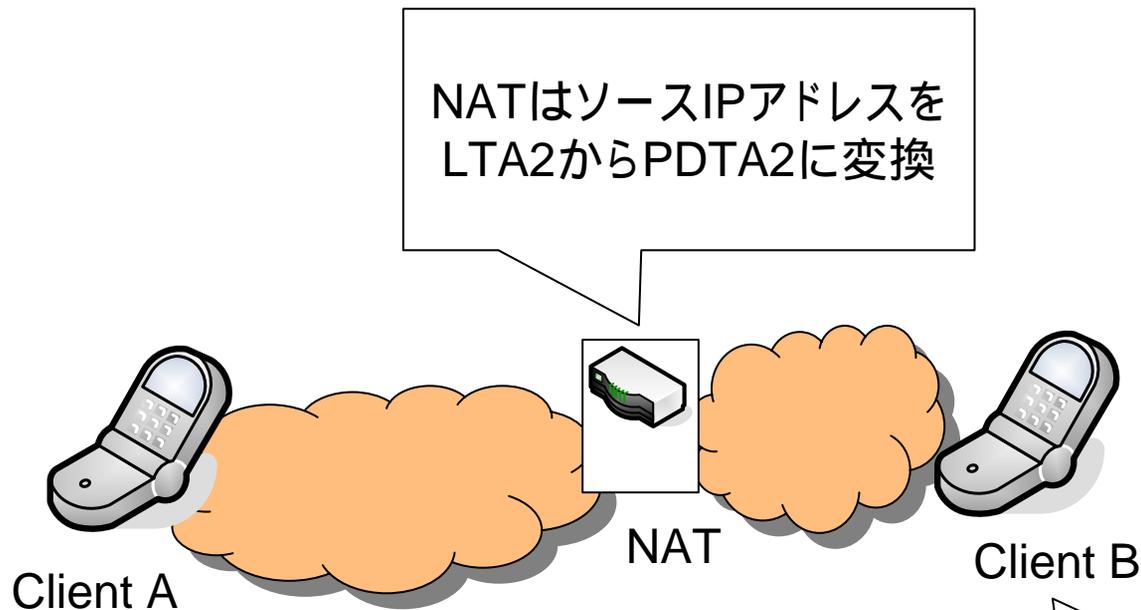


ソースアドレス	終点アドレス
192.0.2.1:8866	192.0.2.77:1296

4章 使用事例の代表例

用語

- Local Transport Address: ホストのOSから割り当てられたアドレス (LTA)
- Derived Transport Address: STUNやTURNを使用して得られるアドレス (DTA)
- Peer Derived Transport Address : 広告されたSTUNサーバから学んだDerived Transport Address である。(PDTA)

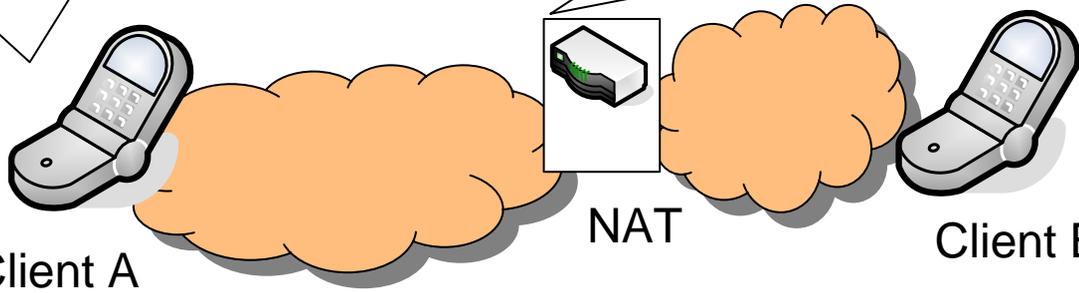


Aに接続性を持っていること
もう1つのアドレス(PDPA2)を
持つこと学びます。

ユーザ名とパスワードを
供給

AはBに対して接続性があるか確認するため

NATは終点アドレスをPDTA2からLTA2に変換



STUNリクエストをPDTA2に送る

NATのグローバル側のMAPPED-ADDRESSを含む

STUNレスポンスをLTA1に送る

AはBに接続性があること
Aが提供するDTAがないことを学習する

UPDATEリクエストを送信

BはすべてのTransportアドレスを所有していないので

200 OK

おわり

SDP

- SDP (Session Description Protocol) の略
- SDPの中に入っている情報

セッション記述

(セッション名、セッション生成者)

時間記述

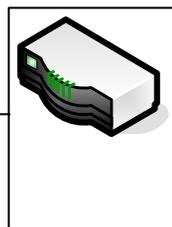
(セッションの有効期間)

メディア記述

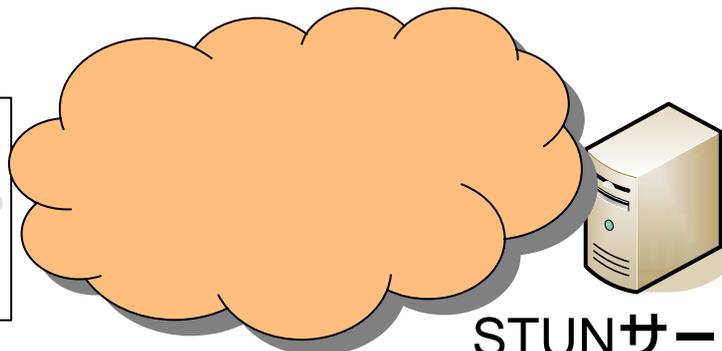
(音声や動画を受信するのに必要な情報)



Client A
(LTA)10.0.1.1:8866



NAT



STUNサーバー
192.0.2.1:3478



STUNリクエスト

10.0.1.1		192.0.2.88
----------	--	------------



STUNサーバー
(LTA)10.0.1.1:8866

STUNレスポンス

STUNサーバーが192.0.2.88:5063
上で動くと広告します。

