本資料について

- 本資料は下記の論文を基にして作成されたものです．文章の内容の正確さは保障できないため，正確な知識を求める方は原文を参照して下さい．

- 著者：Shiang-Ming Huang,Quincy Wu,Yi-Bing Lin
- 論文名：Tunneling IPv6 through NAT with Teredo Mechanism
- 前半：Teredo概要，後半：Linuxに実装した評価から，前半だけを参照し，別の資料と合わせて作成しました．

Tunneling IPv6 through NAT with Teredo Mechanism

名城大学　理工学部　情報科学科

030432106

宮﨑　悠

Introduction

- インターネット技術における30年後の展開として、IETF (Internet Engineering Task Force)はIPv6 を次世代インターネットプロトコルとして開発している
- しかし、IPネットワークは未だにIPv4しかサポートしていない

IPv4ネットワークの中で、IPv6通信を可能にするために
トンネリング技術が利用できる
→Teredo

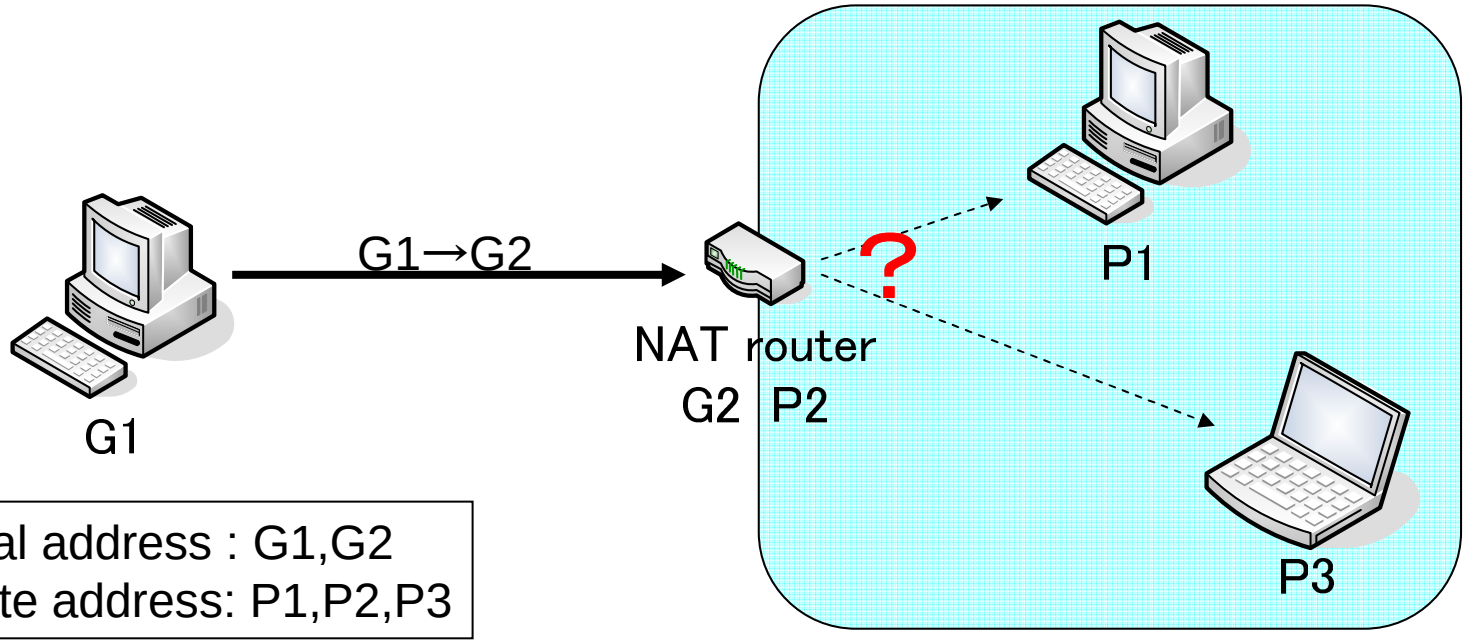
Teredo

- TeredoはIPv4環境でのIPv6ネットワークの透過的接続を実現
  - Microsoftを中心に進められている
- クライアントにはTeredoサーバからIPv6アドレスが与えられ、仮想ネットワーク端末として認識される

Teredoを利用したNAT越え

NAT越え問題

外部端末からすると、NATルータ内の構造が分からないため、
プライベートアドレス空間の端末と直接通信を行うことができない



Global address : G1,G2
Private address: P1,P2,P3

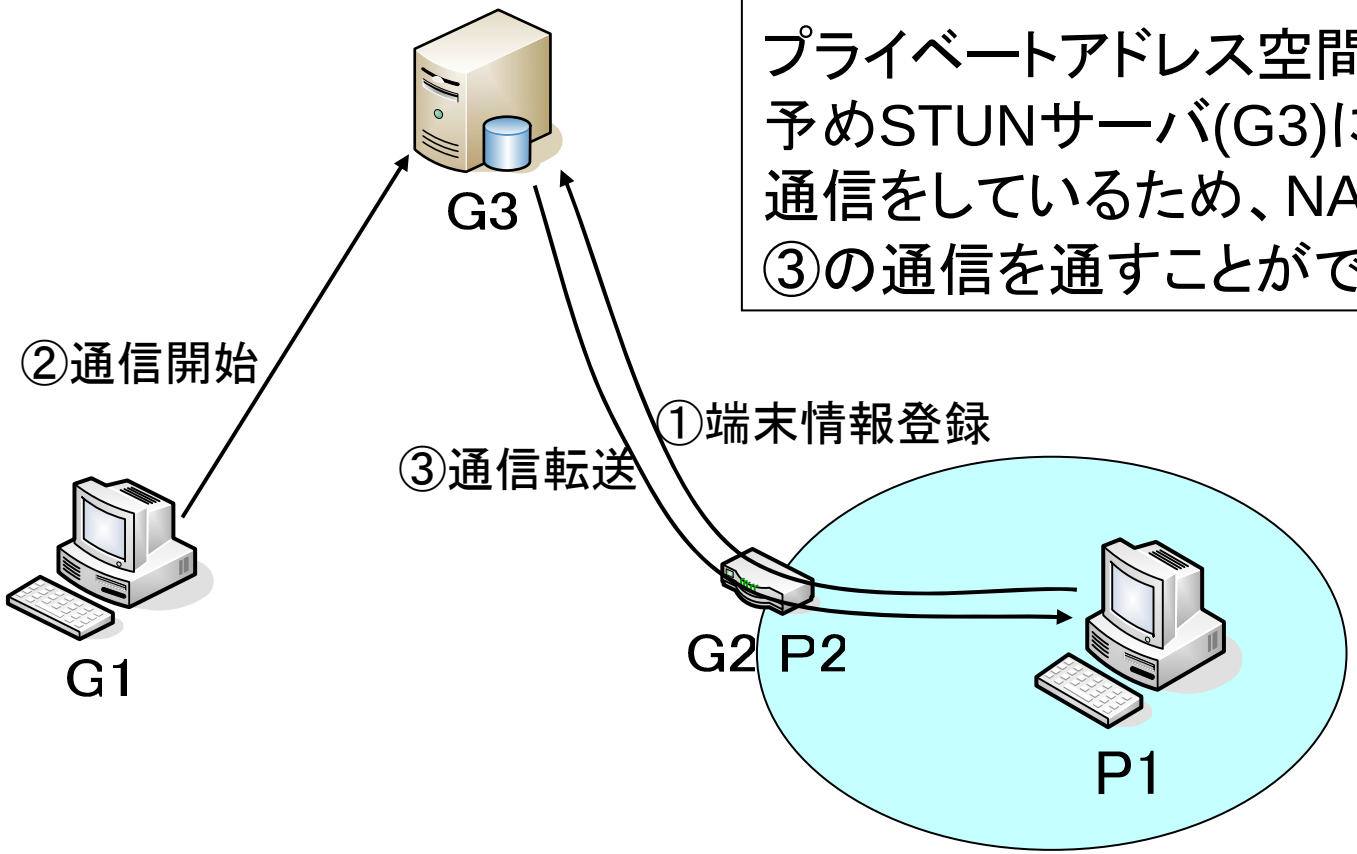
TeredoによるNAT越え

- TeredoはIPv6とIPv4との移行テクノロジであり、TeredoによるNAT越えは「IPv6のIPv4 NAT Traversal」とも呼ばれる
- IPv6-v4間はTeredo Relay Serverを中継して通信する
- IPv4間ではSTUNを利用
  →NATに制限有り

STUN
(Simple Traversal of UDP Through NATs)

UDP Hole Punchingの応用技術

プライベートアドレス空間の端末(P1)は
予めSTUNサーバ(G3)に情報登録時に
通信をしているため、NATルータ(G2)は
③の通信を通すことができる



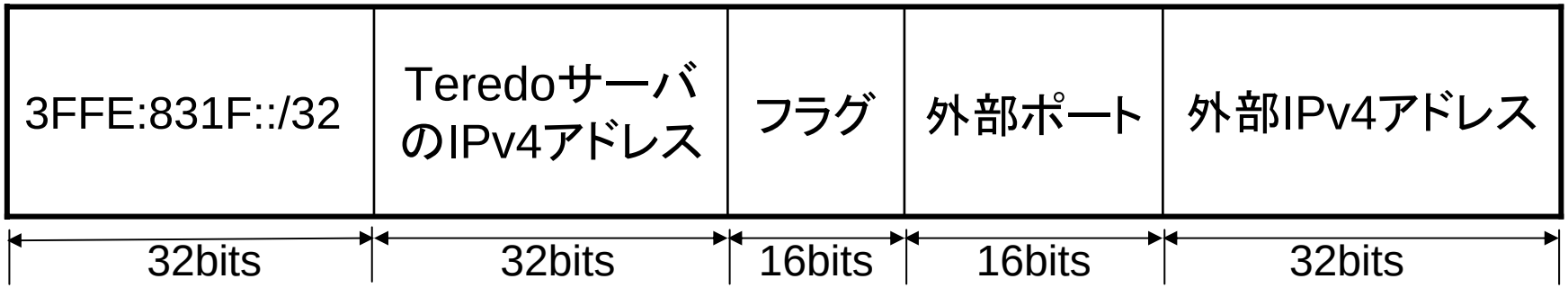
UDP Hole Punchingの必要条件

NATは一般的にアドレス・ポートペアの
マッピングの作成と管理の方法の違い
により以下の4種類に分類される

- Full Cone NAT
- Restricted cone NAT
- Port-restricted cone NAT
- Symmetric NAT

UDP Hole Punching
に対応

Teredo IPv6 address format



- 3FFE:831F::/32 (Teredoプレフィックス)

  Teredoアドレスだということを示す
- TeredoサーバのIPv4アドレス
- フラグ

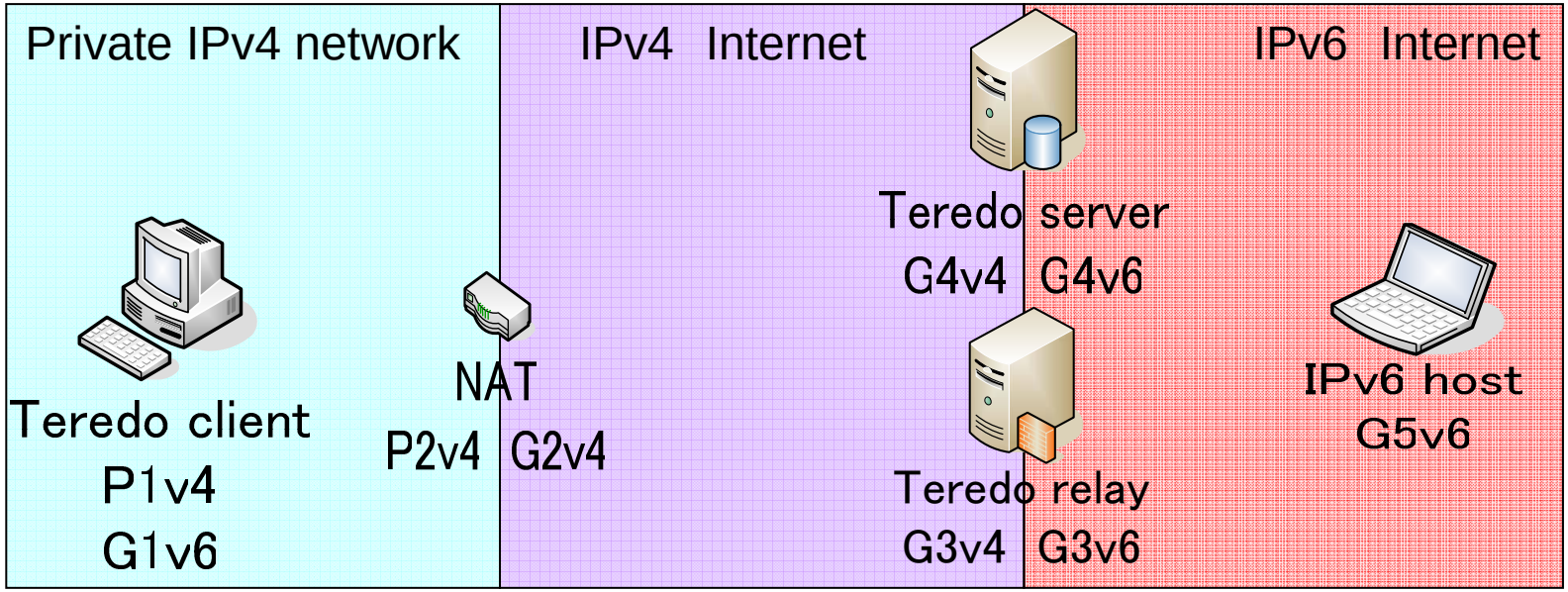
  クライアントのルータのタイプ(cone NATかどうか)

  cone NAT:0x8000,それ以外:0x0000
- 外部ポート・外部IPv4アドレス

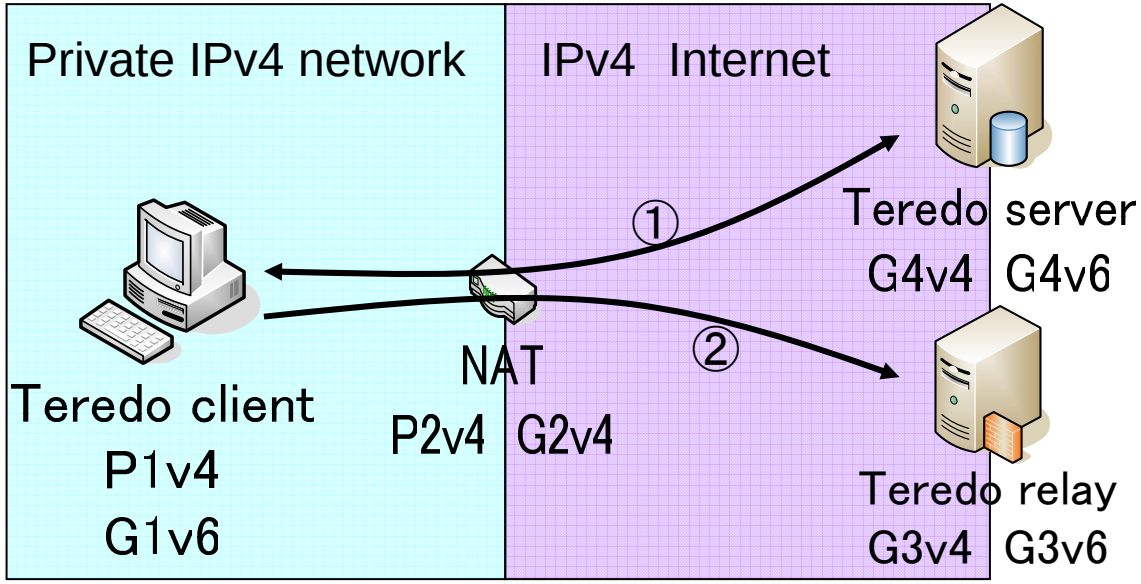
  TeredoサーバがTeredoクライアントにアクセスする為のUDPソケットアドレス

Teredo構成

- Teredo server：Teredo client管理装置
- Teredo relay・client：NAT越えを実現する装置
- IPv6 host：IPアドレスをv6とした端末
- NAT：無着手のNAT（cone NAT）



Teredo NAT Traversal　初期設定



①Teredoアドレス要求

→TeredoアドレスとTeredo relayのアドレスを返信

②Hole Punching

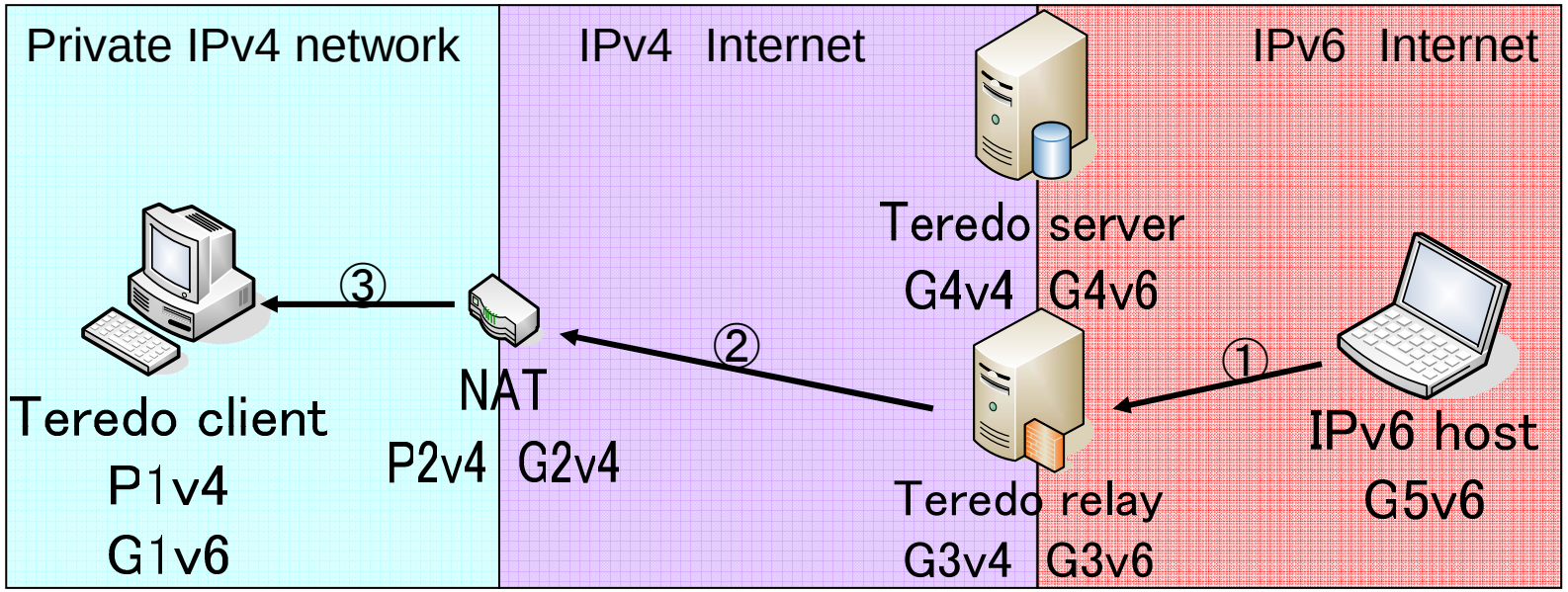
（NATテーブルの作成）

Teredo NAT Traversal

① IPv6 hostはIPv6パケットをTeredo relayに送信

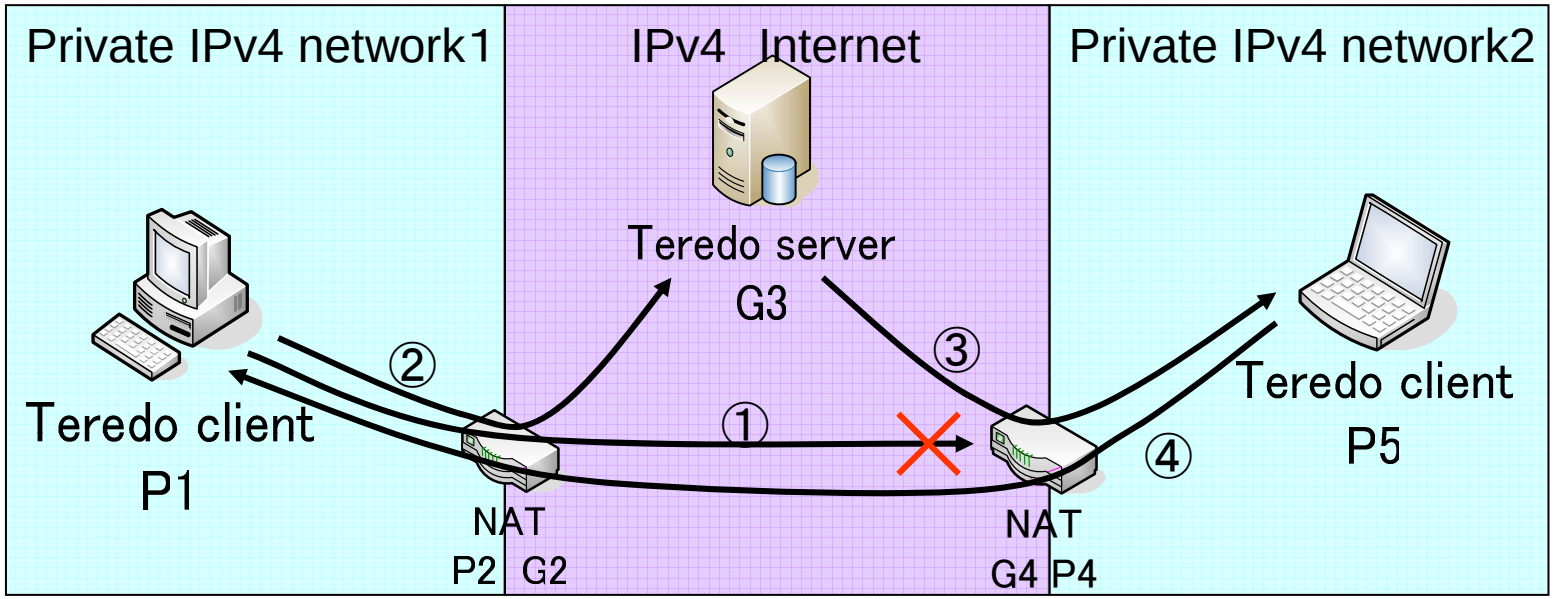
②Teredo relayは受け取ったパケットをIPv4 UDPでカプセル化し代理送信

③NATはUDPパケットを受信し、予め作成されているNATテーブルよりTeredo clientに転送



IPv4 Teredo NAT Traversal

①P1はP5宛に通信を開始するが、届かない
(この時P1→G4のNATテーブルが作成される)
②③P1はTeredo serverを通してP5に通信する
(登録時に各clientとserver間のNATテーブルは作成されている)
④通信を返して通信することができる(①があった為)

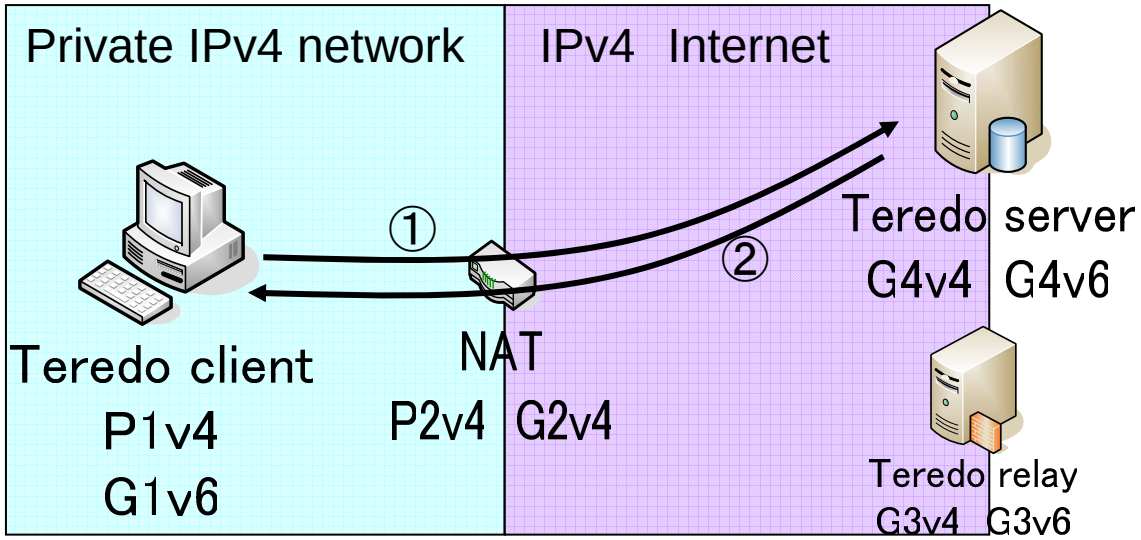


むすび

- Teredoについて説明
  - IPv4環境でのIPv6ネットワークの透過的接続を実現するためのプロトコル
- Teredoを利用したNAT越えを説明
  - Teredo serverを設置し、UDP hole punchingを応用して実現
  - そのためcone NATのみの対応

補足

補足：Teredoアドレスのフラグ判定法



ルータ要請メッセージ
(RS：Router Solicitation)

ルータ通知メッセージ
(RA：Router Advertisement)

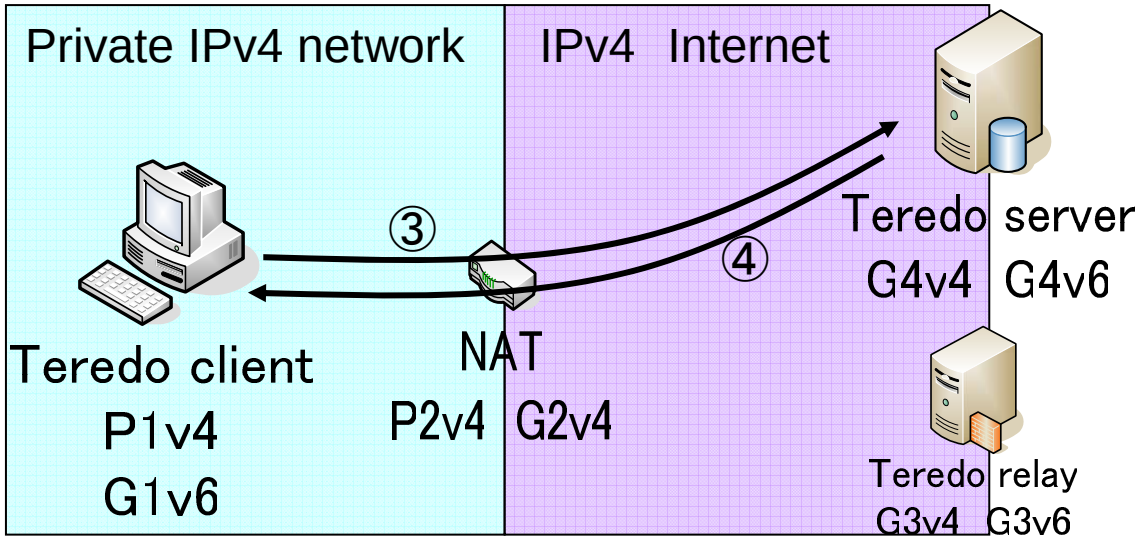
①Teredo clientから、予め設定されているTeredo serverにRSメッセージを送信

このRSメッセージのTeredoアドレスのフラグにはconeフラグ(0x8000)をセット

②Teredo serverからRAメッセージを返信 (この時送信元アドレスをG3v4とする)

Teredo clientが無事受信できた場合はTeredo clientがCone NATを介した接続であることが確定され、初期設定は完了

補足：Teredoアドレスのフラグ判定法



ルータ要請メッセージ
(RS：Router Solicitation)

ルータ通知メッセージ
(RA：Router Advertisement)

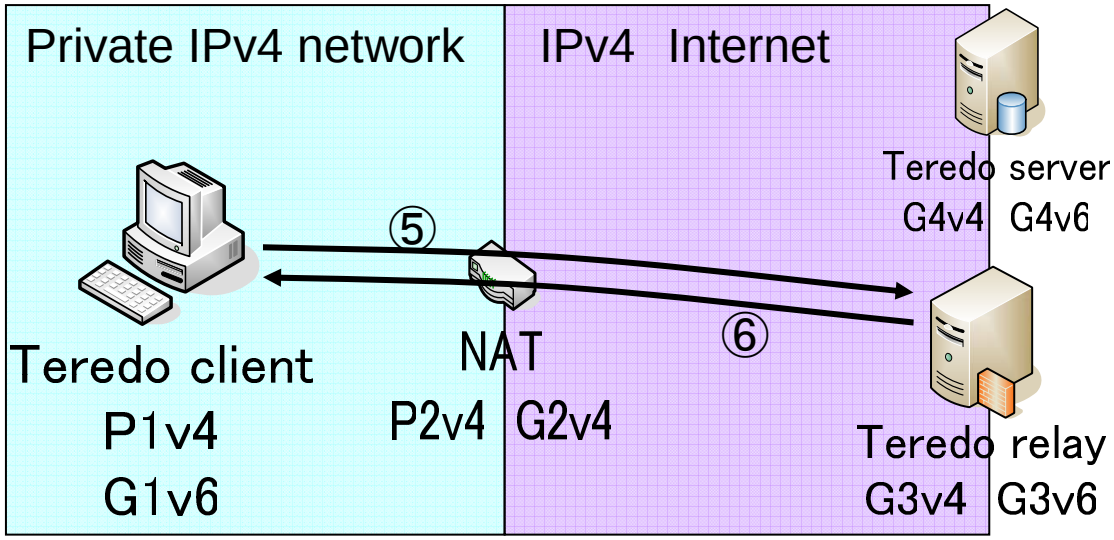
②を受信できなかった場合cone NATではないと判断

③Teredo clientはconeフラグをセットせずに(0x0000)再度メッセージを送る

④RAメッセージを返信する

clientが受信した場合はRestricted NATもしくはSymmetric NATであると判定される

補足：Teredoアドレスのフラグ判定法



ルータ要請メッセージ
(RS：Router Solicitation)

ルータ通知メッセージ
(RA：Router Advertisement)

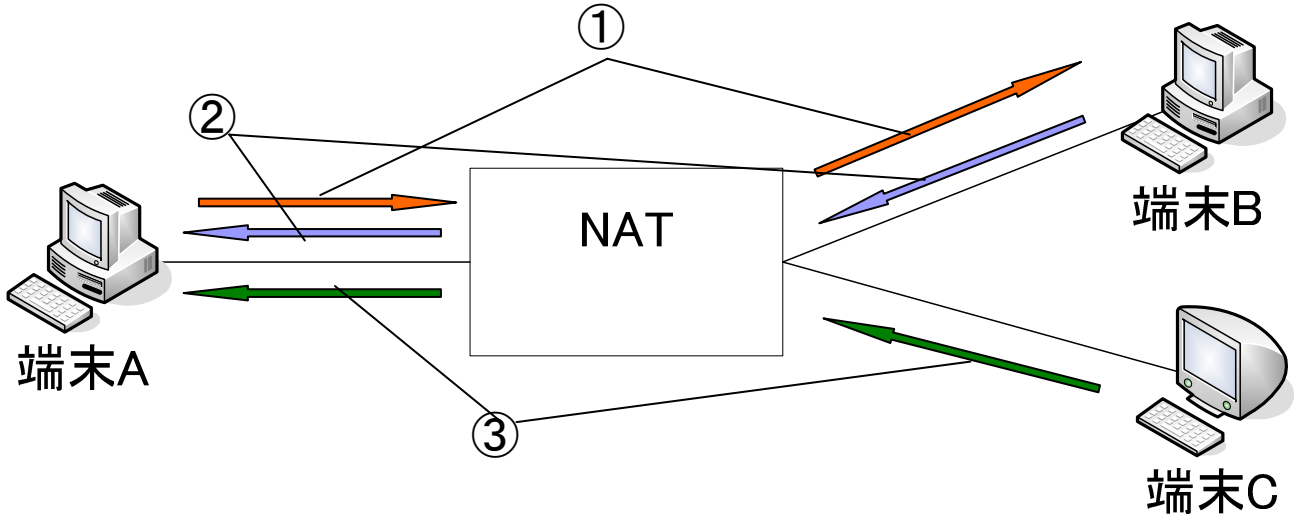
⑤Teredo clientはどちらのNATかの判定のために、Teredo relayにRSメッセージを送信

⑥Teredo relayはRSメッセージを返信し、clientはserverからのRSメッセージと比較し、外部ポートとして同一のUDPポートを使っていた場合はRestricted NATと確定され、初期設定は終了する

Cone NAT

- 内部アドレスおよびUDPポートと外部アドレスおよびUDPポートのマッピングを作成し、ポートがアクティブである限り、マッピングを有効に保持する。
- マッピングが有効の間は、NATのWAN側アドレスの該当UDPポートにて受信されたUDPパケットはNAT内部の対応するホストへと転送される。

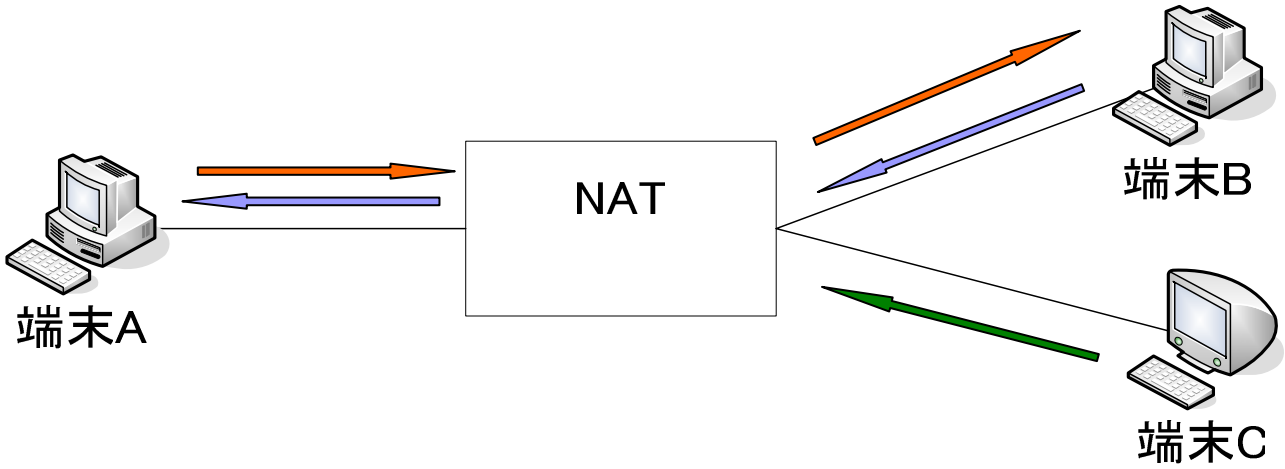
Cone NAT の動作



- 内部ホストAから送信された①のパケットによりマッピングテーブル中にエントリが作成される。
- Cone NATでは対象となる外部ホストの管理は行われないため、同一外部の端末Bからのパケット②だけでなく、異なる端末Cのパケット③もNATデバイスにより内部ホストAに転送される。

Restricted cone NAT

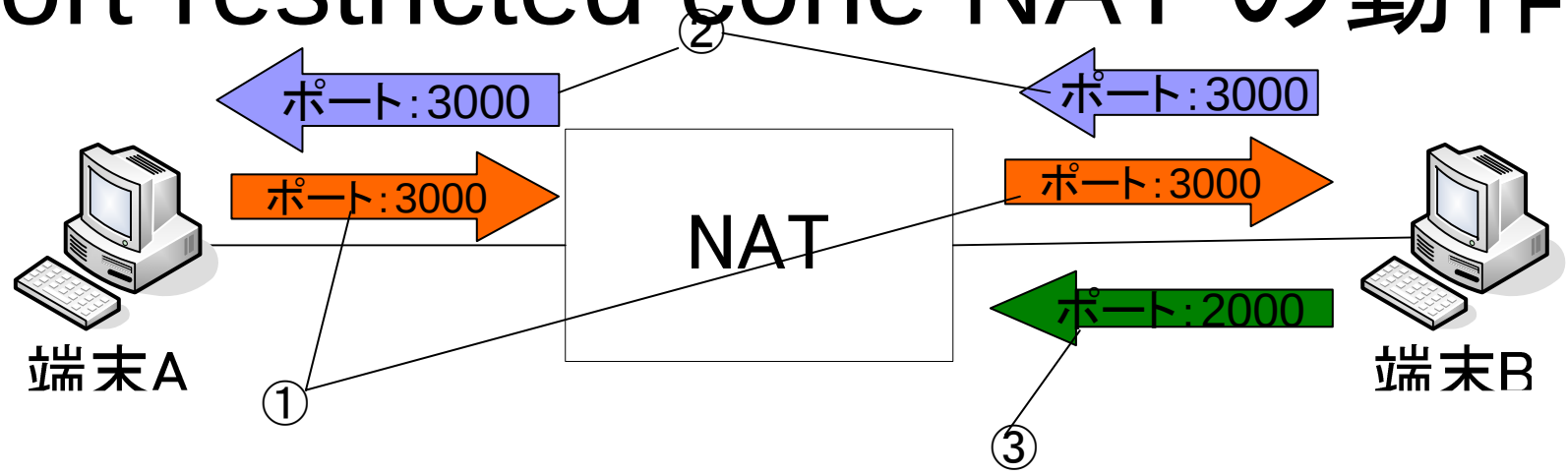
- 単にアドレスとUDPポートのマッピングを作成および維持するだけではなく、内部ホストからUDPパケットを送信した対象の外部ホストを管理している。
- これにより、内部ホストにより通信が開始された外部ホスト以外からのパケットの受信は拒否される。



Port-restricted cone NAT

- Port-restricted cone NATはRestricted cone NATによる外部からのパケットの受信の制限をさらに強化したNAT
- Restricted cone NATが承認された外部ホストだけを管理しているのに対し、Port-restricted cone NATは使用されているポートも管理対象とする。
- 外部からのパケットは内部ホストから通信が開始されたホストからであることとともに、そのときに利用されたポート宛であることが要求され、それ以外のパケットはすべて拒否される。

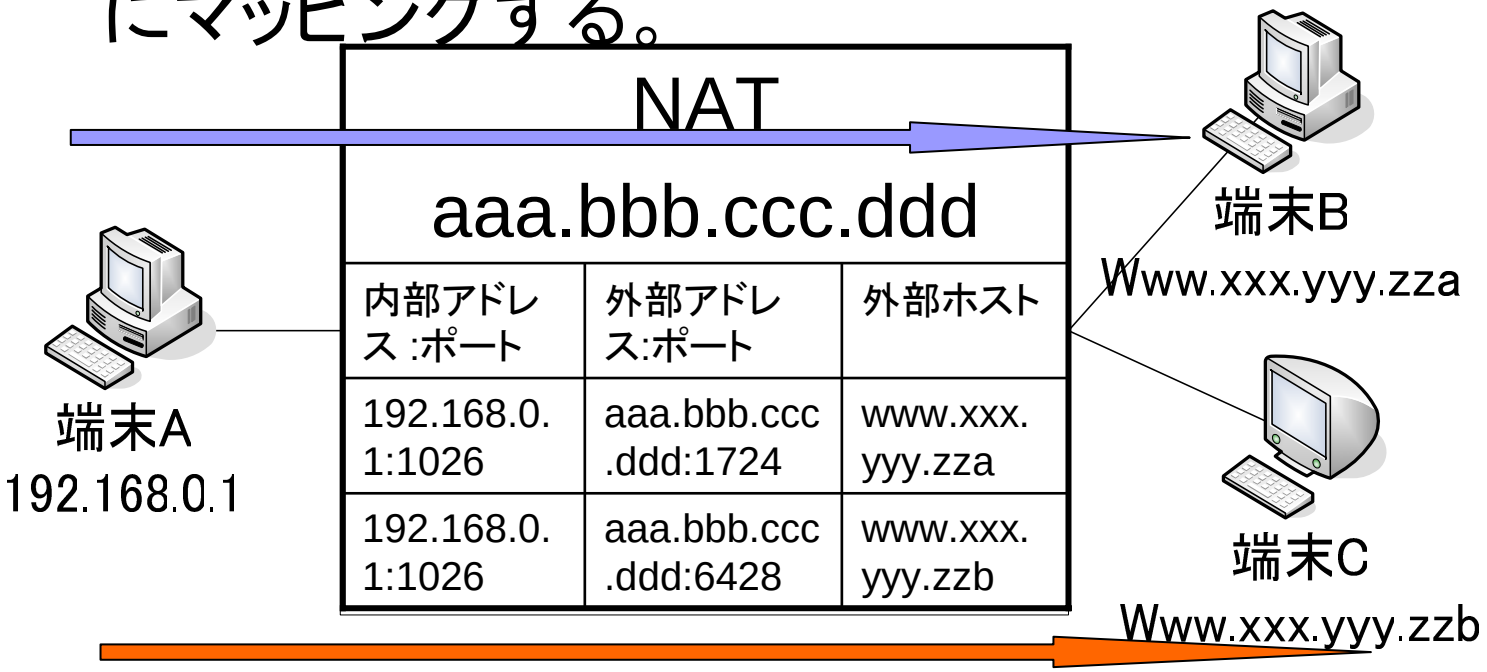
Port-restricted cone NAT の動作



パケット①と②の動作はRestricted cone NATと同様だが、たとえ同一のホストである外部ホスト端末Bあっても、異なるポートからのパケットである③はNAT内部に転送されない。

Symmetric NAT

- Symmetric NATは同一の内部アドレスとポートのペアを異なる外部アドレスとポートのペアにマッピングする。



※symmetric NATでは、内部ポートと外部ポートが違うため、hole punchingを対応させることができない。