Symmetric NAT における NAT 越え実現方式
A Realization method of NAT Traversal in Symmetric NATs

083430041　李慧
渡邊　晃研究室

1. はじめに

急速なインターネットの普及によって IPv4 グローバルアドレスが枯渇しつつある. この問題に対応するために, 組織のネットワークはプライベート IP アドレスで構築することが一般的となっている. しかしプライベート IP アドレスを用いると, NAT（Network Address Translator）越え問題と呼ぶ通信の制約が生じる. 近い将来, IPv6 へ移行すれば NAT が不要になるといわれているが, IPv6 は IPv4 との互換性がないことから普及が滞っている. 制約の度合は NAT のタイプによって異なる.

そこで本論文では, プロトコルを UDP に限定し, どのような NAT のタイプであっても NAT 越えを実現できる方式を提案する.

2. 既存技術とその課題

2.1 NAT 越え

NAT 越え問題とは,グローバルアドレス空間上のノードがプライベートアドレス空間上のノードを個別に識別できないため, グローバルアドレス側からプライベートアドレスに対して通信開始ができないという制約のことである.

NAT は大きく分類すると Symmetric 型 NAT と Cone 型 NAT がある.Symmetric 型 NAT は NAT テーブルを生成するときに,グローバル側の端末アドレスを記憶しておく.これをフィルタリングと呼ぶ.外部ネットワークからパケットを受信したとき,フィルタリングの内容からグローバル側の IP アドレスとポート番号が正しいかどうかをチェックするため,NAT 越えの制約が強い.Cone 型 NAT はフィルタリングのチェックを行わない NAT である.従って,フィルタリングには何も記述されない.Cone 型 NAT の場合,他の通信で生成した NAT テーブルを用いて,グローバルアドレス空間側からの通信の開始ができる.

2.2 STUN

既存の NAT 越え技術として様々な方式があるが,最も普及している方式として STUN（Simple Traversal of UDP through NATs）がある.グローバル側のネットワークに STUN サーバを設置し,あらかじめ内部端末と STUN サーバの間で通信を実行し,NAT テーブルを生成しておく.その NAT テーブルを使って外部端末から通信を開始することができる.しかし STUN は Symmetric NAT には対応できない.世の中の 7 割が Cone 型 NAT と言われているが,Symmetric NAT も多く存在するため,この問題は解決することが重要である。

3. 提案方式

本論文では Symmetric 型 NAT の場合においても,改良 STUN サーバを使うことによって,グローバルアドレス端末側から内部端末に通信を開始することができることを示す.図 1 に,改良 STUN サーバによる通信開始を示す.ノード B が Symmetric NAT 配下に存在するノード A に対して通信を開始する場合を想定する.ノード A はグローバルアドレス G5 を持つ NAT の配下に存在し,プライベートアドレス P1 を持つ.STUN サーバはグローバルアドレス G2 を持つ.ノード B はグローバルアドレス G3 を持つ.ノード B からノード A に通信を開始したい場合,事前の準備が必要である.ノード A は STUN サーバに向けて,送信元アドレスとポート番号 P1:s,宛先アドレスとポート番号 G2:d のパケットを送信する.このパケットは宛先がグローバルアドレスなので,必ず NAT に届く.NAT は NAT テーブル G5:m⇔P1:s を作る.さらにパケットの送信元アドレスとポート番号 P1:s を G5:m に変換して転送する.Symmetric 型 NAT では,グローバル側の IP アドレスをチェックするので,フィルタリングフィールドに IP アドレスとポート番号 G2:d を登録する.STUN サーバはこのパケットを受信すると,ノード A の名前と G5:m の関係を登録する.ここまでで事前の準備が終わる.

ノード B がノード A に通信を開始するためには,ノード A があらかじめノード B 宛にパケットを送信して NAT テーブルを作っておく必要がある.そこで,ノード B はまず改良 STUN サーバに対してノード A と通信をしたいことを伝える.改良 STUN サーバはこの通知を受けて,送信元アドレスとポート番号 G2:d,宛先アドレスとポート番号 G5:m のパケットを NAT に送信する.このパケットのメッセージフィールドにはノード B のアドレスとポート番号 G3:k が記載されている.このパケットは宛先が NAT であるため,Symmetric 型 NAT に届く.NAT は NAT テーブルに G5:m の情報があり,なおかつフィルタリングは G2:d なので,宛先アドレスとポート番号 G5:m を P1:s に変換して内部ネットワークに転送し,ノード A に届く.ノード B の情報 G3:k はそのままノード A に伝えられる.

次にノード A からノード B に送信元アドレスとポート番号 P1:s,宛先アドレスとポート番号 G3:k のパケットを送信する.

NAT は新しく NAT テーブル G5:n ⇔P1:s を作る.フィルタリングフィールドには IP アドレスとポート番号 G3:k を登録する.NAT はこのパケットの送信元アドレスとポート番号 P1:s を G5:n に変換して転送する.

ノード B はこのパケットを受信すると,NAT に正しい NAT テーブルが生成されたことを知り,通常の通信を開始する.次に通常の通信として送信元アドレスとポート番号 G3:k,宛先アドレスとポート番号 G5:n のパケットを送信する.これを受信した NAT は NAT テーブル G5:n があり,なおかつフィルタリングは G3:k なので,宛先アドレスとポート番号 G5:n を P1:s に変換してノード A に転送することができる.逆の方向のパケットはこれと逆の変換により,通信ができる.このようにして Symmetric 型 NAT であっても,ノード B からノード A に対して通信を開始することができる.

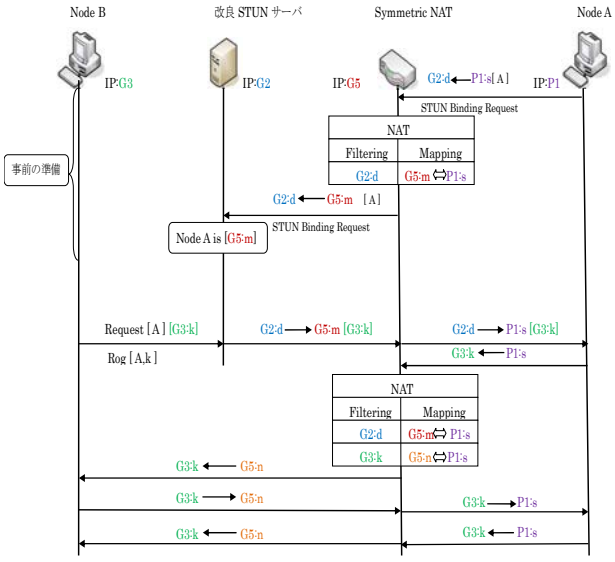


図 1　改良 STUN サーバによる通信開始

4. 評価

既存 STUN と提案方式を比較する.NAT の方式に関して比較すると,CONE 型 NAT の場合,既存 STUN と提案方式は両者ともグローバルアドレスからプライベートアドレスに通信を開始することができる.Symmetric 型 NAT の場合,既存 STUN では通信を開始することができないが,本提案方式では,改良 STUN サーバを使うことによって,グローバルアドレスからプライベートアドレスに通信を開始することができる.プロトコルに関して比較すると,UDP の場合,既存 STUN と提案方式はともに利用することが可能である.しかし,TCP に関しては両者とも利用できない.TCP の場合,NAT において TCP ヘッダ内のシーケンス番号のチェックなどを行っている場合があり,今回の方式だけでは対応できない.今後は,TCP の NAT 越えを検討する必要がある.

表 1 既存 STUN と提案方式の比較

		既存 STUN	提案方式
NAT 方式	CONE	○	○
	Symmetric	×	○
プロトコル	UDP	○	○
	TCP	×	×

5. まとめ

Symmetric 型 NAT では,STUN サーバを使っても,グローバルアドレスからプライベートアドレスに通信を開始することができない.そこで,この課題を解決するため,Symmetric NAT であっても NAT 越えができる手法ついて検討した.具体的には：まずグローバルアドレス側の端末は改良 STUN サーバに通信をしたいことを伝える.そのメッセージはプライベートアドレス側の端末に届けられる.次にプライベートアドレス端末からグローバルアドレス端末に直接通信を行い NAT テーブルを生成する.グローバルアドレス端末はここで生成した NAT テーブルを用いて,通信を開始することができる.今後は TCP における NAT 越えを検討する.

参考文献

[1] Egevang, K. and Francis, P.: The IP Network Address Translators (NAT), RFC1631, IETF (1994).

[2] 鈴木秀和，宇佐見庄五，渡邊　晃：外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装，情報処理学会論文誌， Vol.48, No.12, pp.3949-3961 (2007).

[3] UPnP Forum: Internet Gateway Device(IGD) Standardized Device Control Protocol V 1.0, http://www.upnp.org/standardizeddcps/igd.asp(2001).

[4] Rosenberg, J., Mahy, R. and Matthews, P.: Traversal Using Relays around NAT(TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), Internet-Draftdraft-ietf-behave-turn-16, IETF (2009).

[5] Rosenberg, J., Weinberger, J., Huitema, C., and Mahy, R., “STUN - Simple Traversal of User DatagramProtocol (UDP) Through Network Address Translators(NATs)”, RFC 3489, March 2003.

SYMMETRIC NATにおけるNAT越え実現方式

名城大学大学院理工学研究科
渡邊研究室
083430041　李慧

研究背景

- インターネットの普及に伴ない、ユビキタス社会化が進んでいる

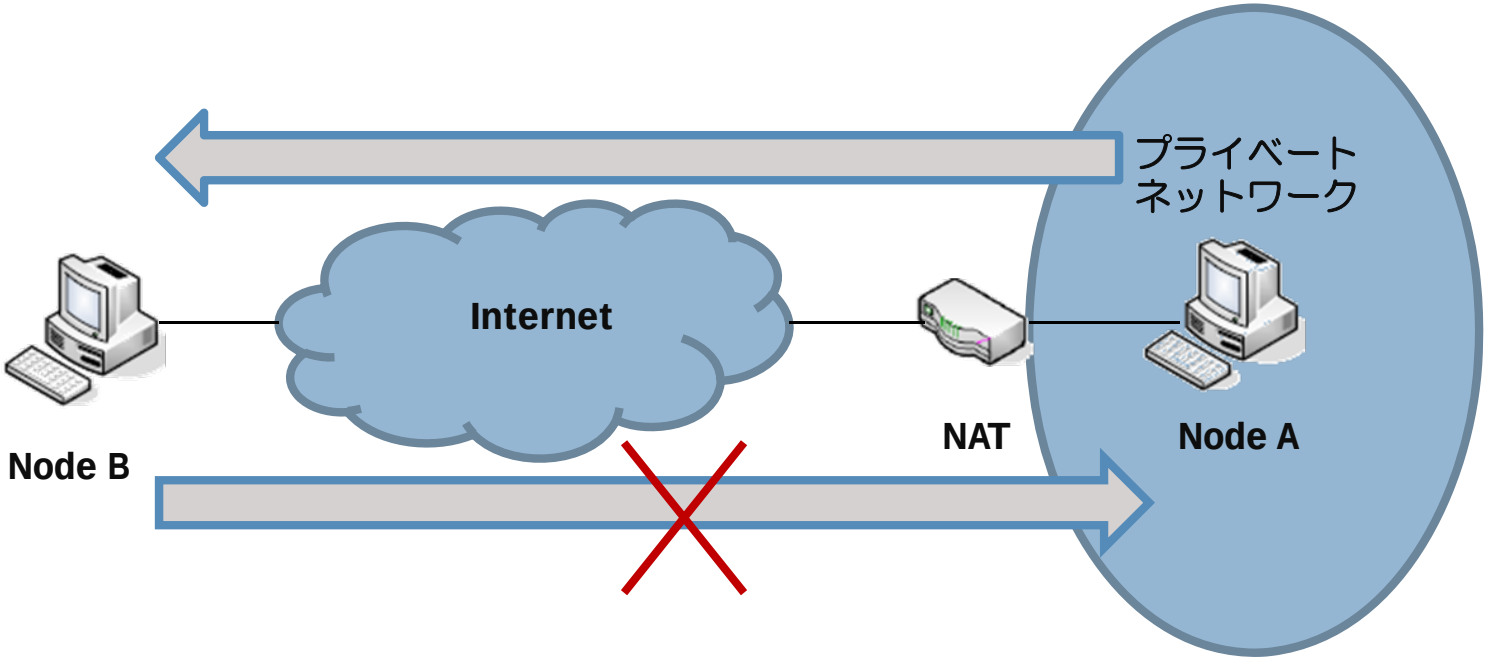
  →いつでもどこからでも通信したい

- グローバルアドレスが枯渇しているので、家庭内や企業内のネットワークはプライベートアドレスで構築される。そのために、アドレスを変換するNATが必要となる

  →**NAT(Network Address Translator)**が使用される

NAT越え問題

- インターネット側（グローバルアドレス側）からの通信開始ができない
- 外部からみると、グローバルアドレスは１つしか見えない

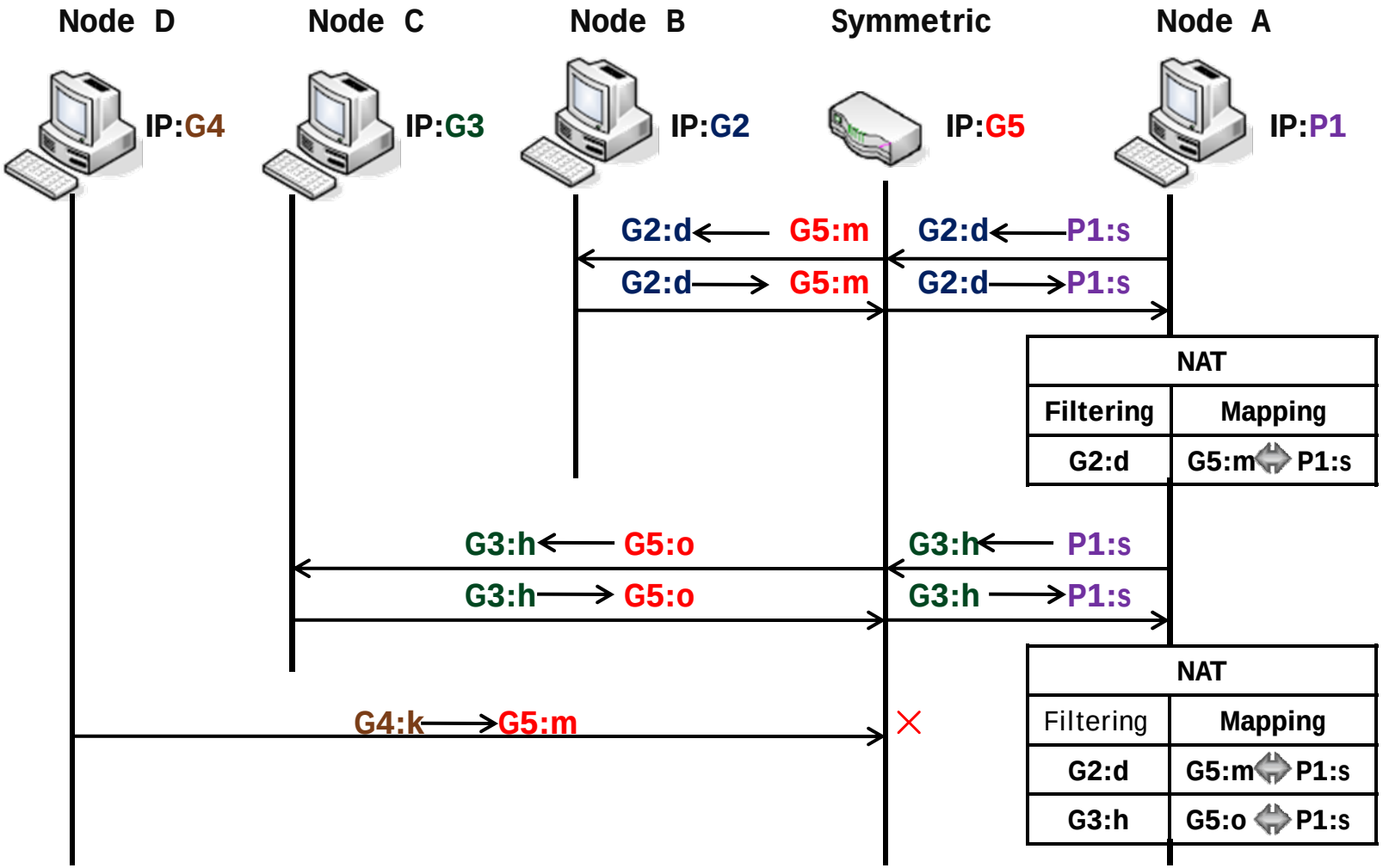


NATタイプ

- **Symmetric**
  - Symmetric型NATはNATテーブルを生成するときに、グローバル側の端末アドレスを記憶しておく。これをフィルタリングと呼ぶ。外部ネットワークからパケットを受信したとき、フィルタリングの内容からIPアドレスとポート番号が正しいかどうかをチェックするため,NAT越えの制約が強い
- **Cone**
  - Cone型NATはフィルタリングのチェックを行わないNATである。従って、フィルタリングには何も記述されない。Cone型NATの場合,他の通信で生成したNATテーブルを用いて、グローバルアドレス空間側からの通信の開始ができる

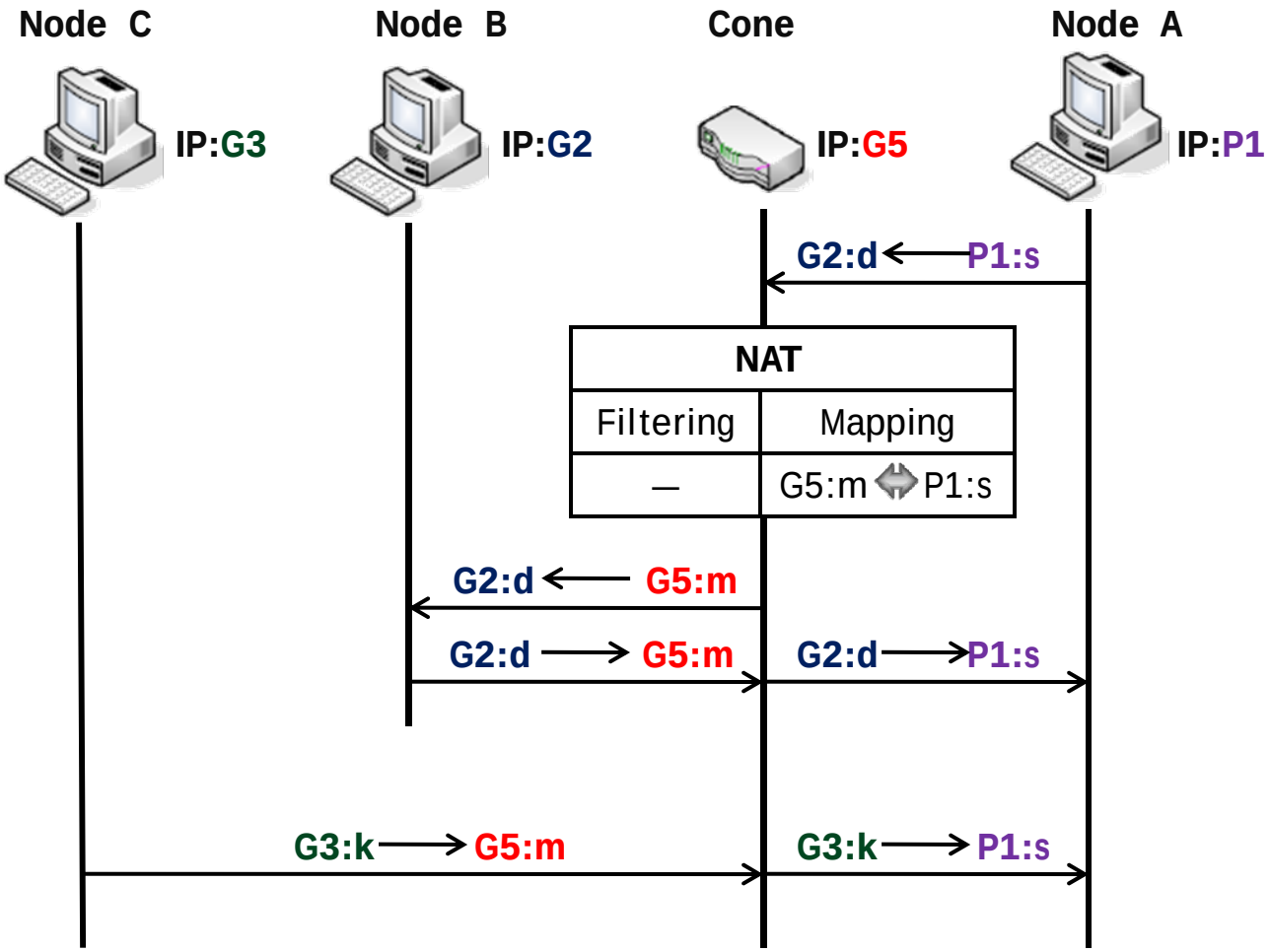
NATの原理とその種類

- Symmetric型NATの動作原理



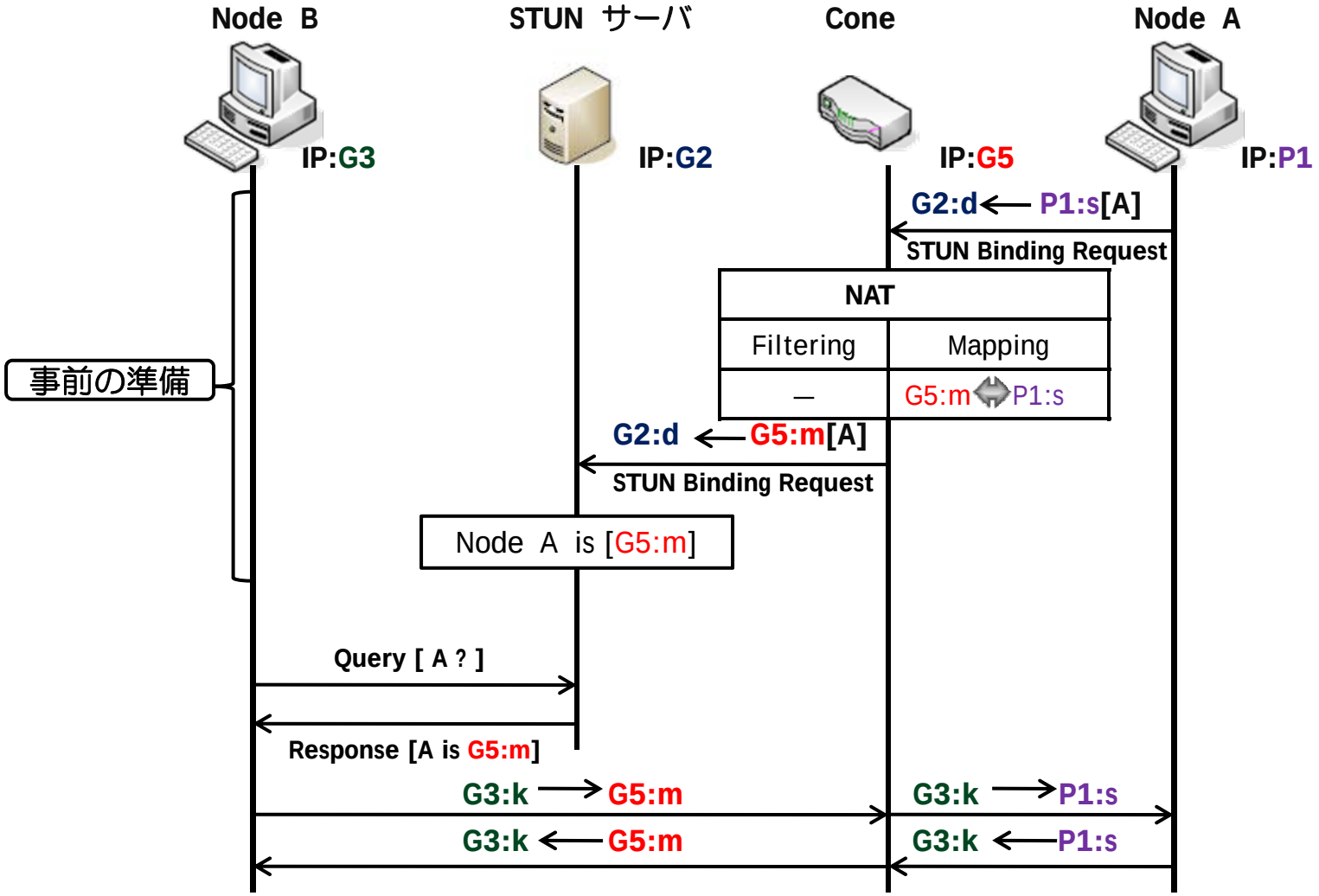
NATの原理とその種類

- CONE型 NATの動作原理

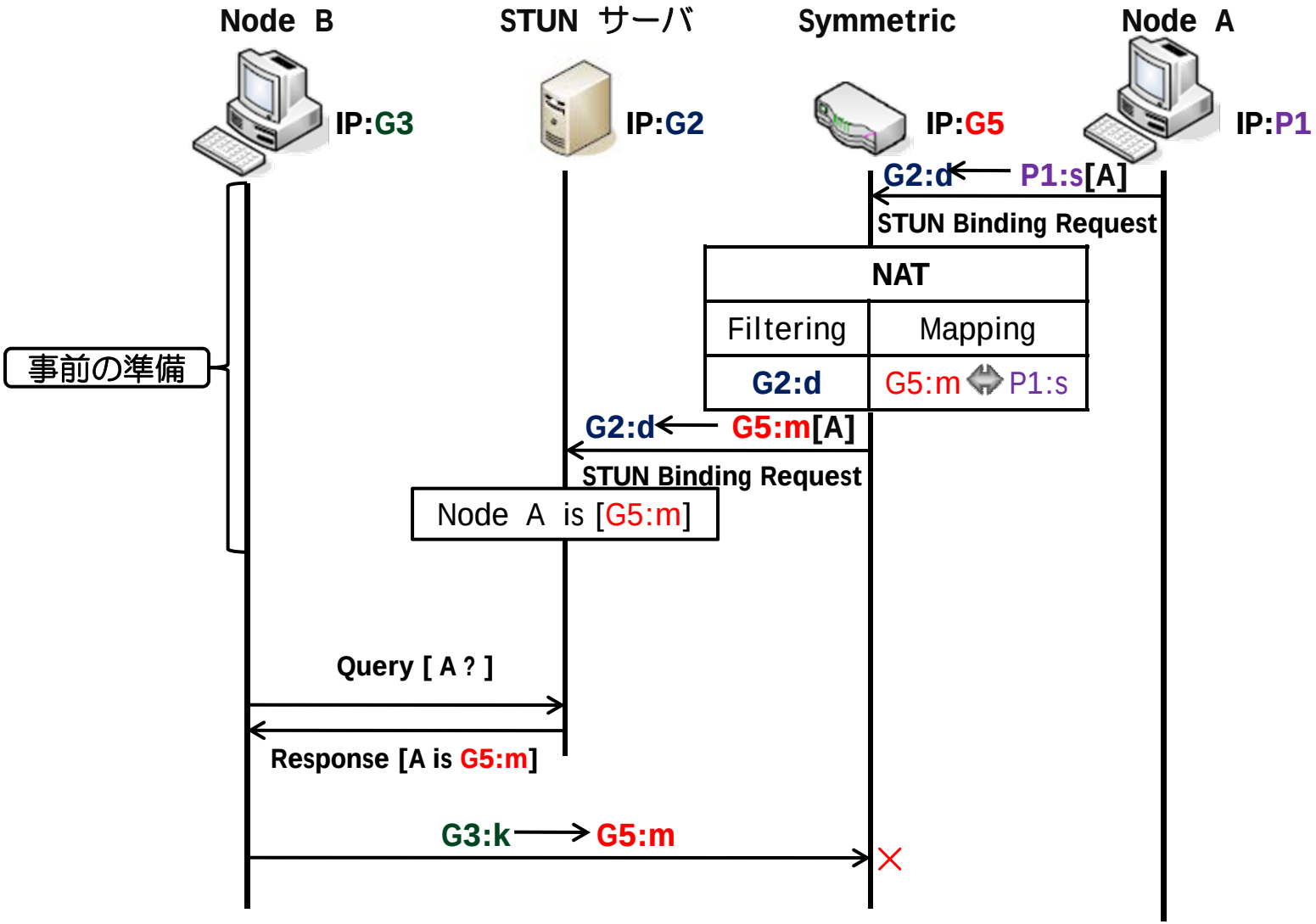


STUN（SIMPLE TRAVERSAL OF UDP THROUGH NATS）

- NAT越え通信の代表的な技術
- Cone型NATにのみ適用が可能



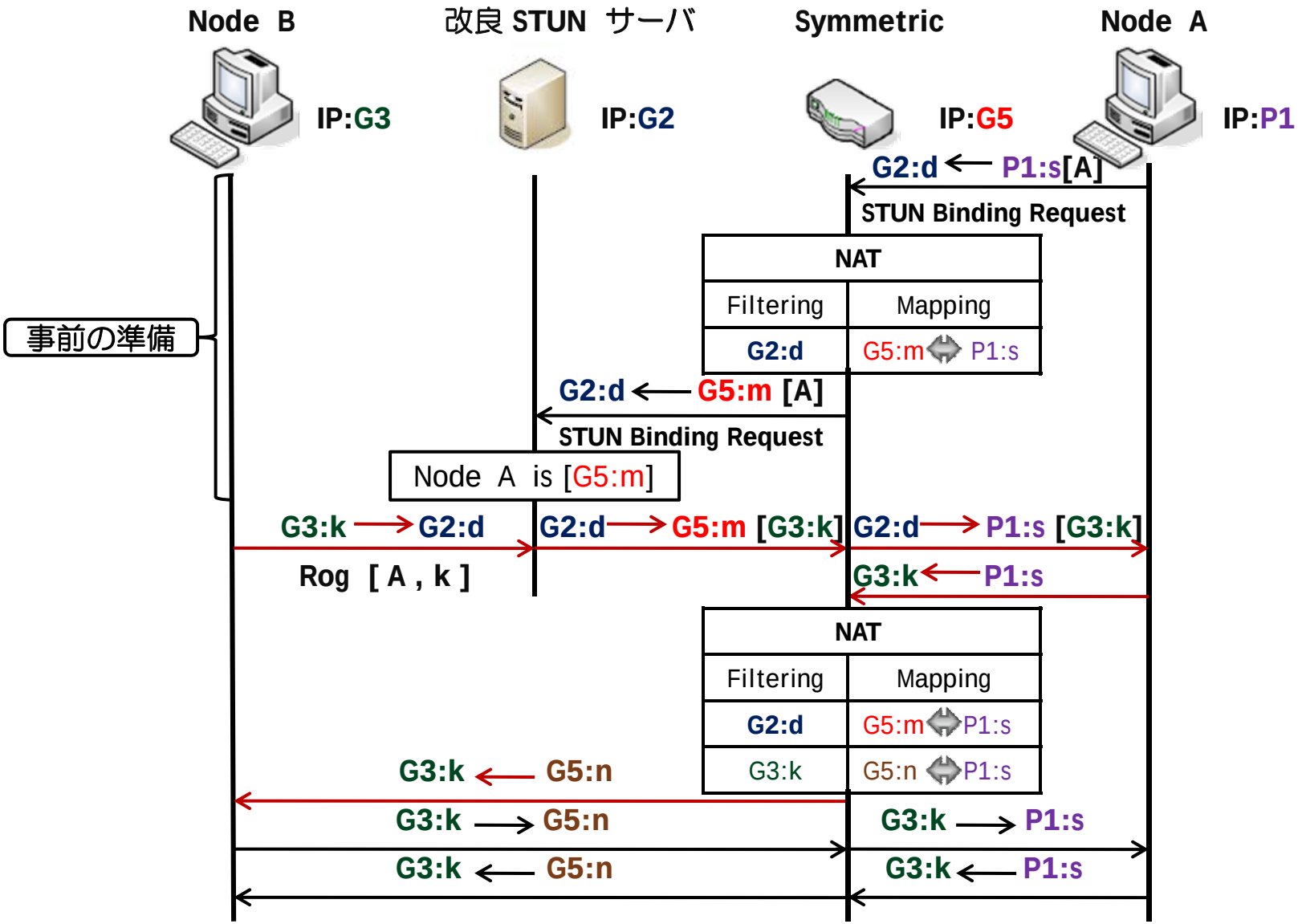
STUN


Node B
STUN サーバ
Symmetric
Node A
IP:G3
IP:G2
IP:G5
IP:P1
G2:d ← P1:s[A]
STUN Binding Request
NAT
Filtering
Mapping
G2:d
G5:m ⇔ P1:s
事前の準備
G2:d ← G5:m[A]
STUN Binding Request
Node A is [G5:m]
Query [A ?]
Response [A is G5:m]
G3:k → G5:m

提案方式概要

- Symmetric NATであってもNAT越えができる手法について検討した
- 具体的にはグローバルアドレス側の端末は改良STUNサーバに通信をしたいことを伝える
- そのメッセージはプライベートアドレス側の端末に届けられる
- 次にプライベートアドレス端末からグローバルアドレス端末に直接通信を行いNATテーブルを生成する
- グローバルアドレス端末はここで生成したNATテーブルを用いて、通信を開始することができる

提案方式


Node B
改良 STUN サーバ
Symmetric
Node A
IP:G3
IP:G2
IP:G5
IP:P1
G2:d ← P1:s[A]
STUN Binding Request
NAT
Filtering
Mapping
G2:d
G5:m P1:s
事前の準備
G2:d ← G5:m [A]
STUN Binding Request
Node A is [G5:m]
G3:k → G2:d
G2:d → G5:m [G3:k]
G2:d → P1:s [G3:k]
Rog [A , k]
G3:k ← P1:s
NAT
Filtering
Mapping
G2:d
G5:m P1:s
G3:k
G5:n P1:s
G3:k ← G5:n
G3:k → G5:n
G3:k → P1:s
G3:k ← G5:n
G3:k ← P1:s

評価

- 表１　既存**STUN**と提案方式の比較

		既存STUN	提案方式
NAT方式	CONE	○	○
	Symmetric	×	○
プロトコル	UDP	○	○
	TCP	×	×

まとめ

- Symmetric型NATの場合、STUNサーバを使っても、グローバルアドレスからプライベートアドレスに通信を開始することができない
- この課題を解決するため、改良STUNサーバを使うことにより、外側から内部に通信を開始することができることを示した
- 今後はTCPにおいてもNAT越えができる方式を検討する必要がある

補足説明

- **TCP**ができない理由
- **TCP**パケットでないと**TCP**の**NAT**テーブルは生成できない
- **TCP**の開始は必ずコネクション確立である
- **3 way handshake**に合わせたシーケンスにする必要がある

補足説明

- ノードBからのリクエストは通常のクエリと同じと考えてよいか
- リクエストの中にこれから通信に使うポート番号の情報を含んでいる必要がある
- 従って、通常のクエリとは異なる

補足説明

- **K**をあらかじめ決めることはできるのか
- できるけど、方法については今後検討の必要がある