NAT (NAPT)

- 世間一般には NAT（Network Address Translation）という用語は NAPT（Network Address Port Translation）を指している．NAPT は IP マスカレード，eNAT（拡張 NAT）などと呼ばれることもある．
  - 用語が混乱している．
- 元々は IP アドレス不足を補うためのもの．
  - 最近では Fire Wall として使用される．

- NAT はネットワーク層で働くが，NAPT はトランスポート層で働く．
- NAT（Network Address Translation）[本来の意味での NAT]
  - プライベートアドレスをグローバルアドレスに変換して使用．（通常は１対１）
- NAPT（IP マスカレード，eNAT）
  - NAPT はプライベートアドレスとグローバルアドレスおよびポート番号の変換を行う．
  - ポート番号ごとに通信を割り振る．（ポート番号の変換も行う）

実は NAT にはアドレスとポートの変換に関してタイプがある．

・コーン型

宛先に関わらず，ある NAT 内の”IP アドレス：ポート番号”は固定の”IP アドレス：ポート番号”に変換される．

1. Full cone 型

   一度も通信した事のないノードからの通信も受け入れる．

   相手の IP アドレス，ポート番号不問

2. Address-Restricted cone 型

   一度通信したノードからの通信を受け入れる．相手のポート番号は不問．

3. Port-Restricted cone 型

   一度通信したノードのポートからの通信（返信）のみを受け入れる．

・シンメトリック型

同じ NAT 内の”IP アドレス：ポート番号”でも，宛先毎に違うポート番号に変換される．

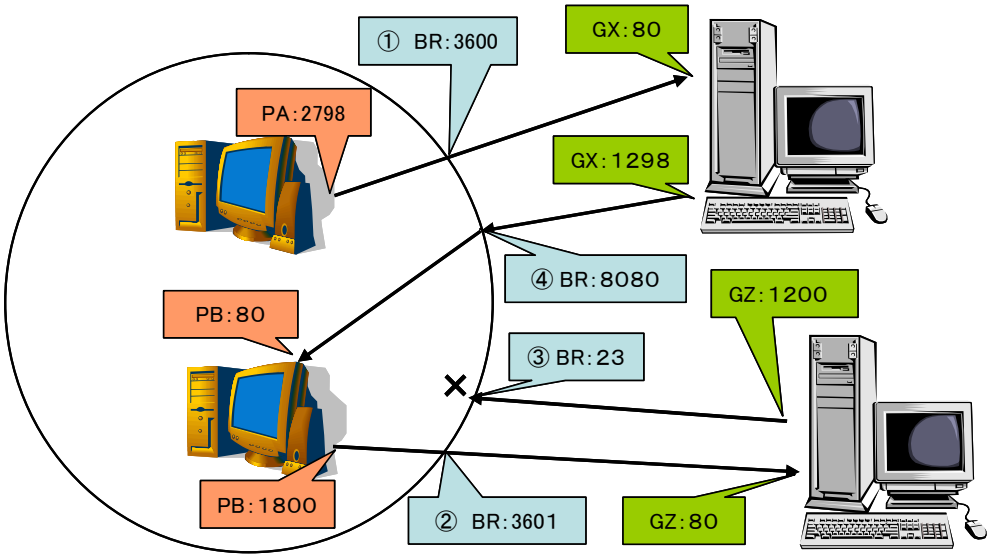
一度通信したノードのポートからの通信（返信）のみを受け入れる．

・NAPT によるアドレス・ポート番号変換

- Port-Restricted cone 型 または シンメトリック型の場合
  - 内部（プライベートアドレス空間）から外部（インターネット空間）へ行く場合，アドレスとポート変換表が作られる（①，②）．
  - 変換表が無い場合，外側からの信号は内部へ到達できない（③）．
  - 不特定の外部のアドレスに対して，アドレス変換を許す機能を，ポートフォワーディングと呼ぶ（④）．　内部サーバを外部に公開する場合に使用する．
  - DMZ（DeMilitarized Zone：非武装地帯）には，変換表に無い外部からの信号が全て転送される（本来の DMZ は違う意味）．

・ 最近の BB ルータはアプリケーションが自分の使用するポートに関して，ルータに変換テーブルの作成を指示する場合がある（UPnP）．

・ NAT(NAPT)超えの問題（SIP，Game）
  - UPNP，STUN サーバ，UDP ホールパンチング（Full または Address-Restricted cone の場合のみ）



変換表

	内部アドレス	ルータ	外部アドレス	
①	PA:2798	BR:3600	GX:80	自動作成
②	PB:1800	BR:3601	GZ:80	自動作成
④	PB:80	BR:8080	ー	ポートフォワード