ヤマハ ルーター
NATディスクリプタ機能
～説明資料～

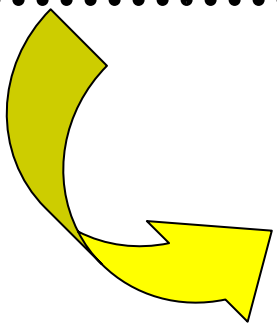
ヤマハ株式会社
AV･IT事業本部
マーケティング室
2002年3月

目次

- NATディスクリプタの特徴
- 応用例#1,#2
- IPマスカレードの処理選択
  - incoming/unconvertible/range
- IPマスカレードのアプリケーション対応
  - ping/traceroute/FTP/CU-SeeMe
  - NetMeeting 3.0対応
  - VPNパススルー機能
  - PPTPのマルチセッション対応
- 付録資料

アドレス変換機能(NAT) の要素

[必須]
- 動的NAT、静的NAT
- IPマスカレード
- 静的IPマスカレード
- DMZホスト機能
- WAN/LANへの適用



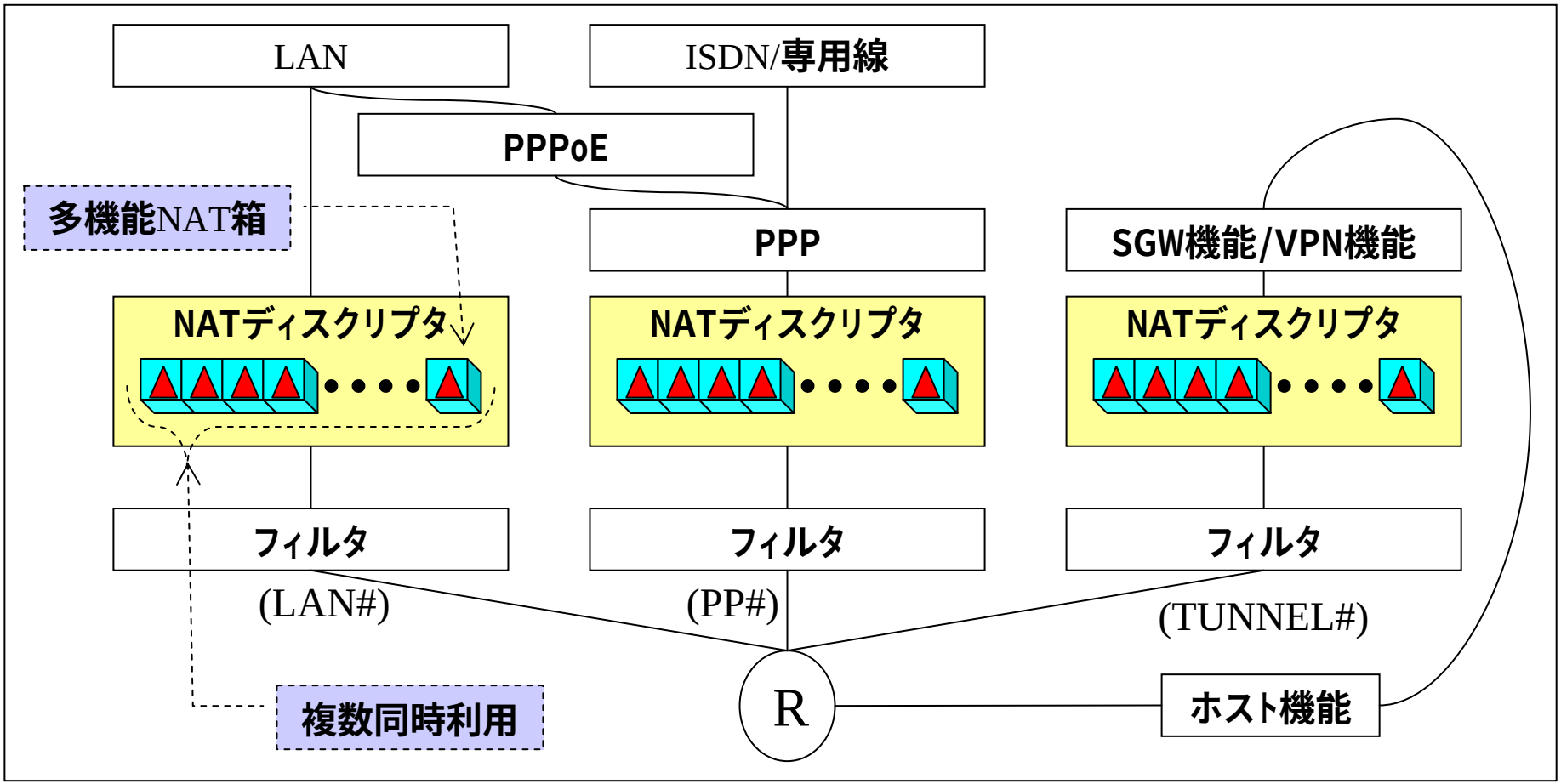
[ヤマハルータ]
- フレキシビリティ
- VPNへの適用
- IPマスカレード機能の選択
- アプリケーション対応
- VPNパススルー

アドレス変換機能の優位点

- フレキシビリティ
  - a) 多機能なNATモジュールを自在に並列利用可能
    ⇒最大16個のIPマスカレードを同時利用
  - b) ひとつのIPマスカレードは、4096個の接続を管理
  - c) 制約や制限が少なく(メモリの許す限り)
  - d) 動作仕様の細かい調整が可能
- アプリケーション対応
  - a) アドレス変換の苦手なアプリケーションへの対応
    FTP,CU-SeeMe,NetMeeting Version 3.0対応などで、安定した通信を可能とする。
    ※通信データの中身を監視し、コネクション管理やデータの書換えを必要とする。
  - b) 「ポート番号」の無いアプリケーション(通信手段)への対応
    ICMP(ping,tracert.exe)、IPv6トンネル、VPNパススルー(IPsec,PPTP,L2TP)
  - c) PPTPのマルチセッション対応

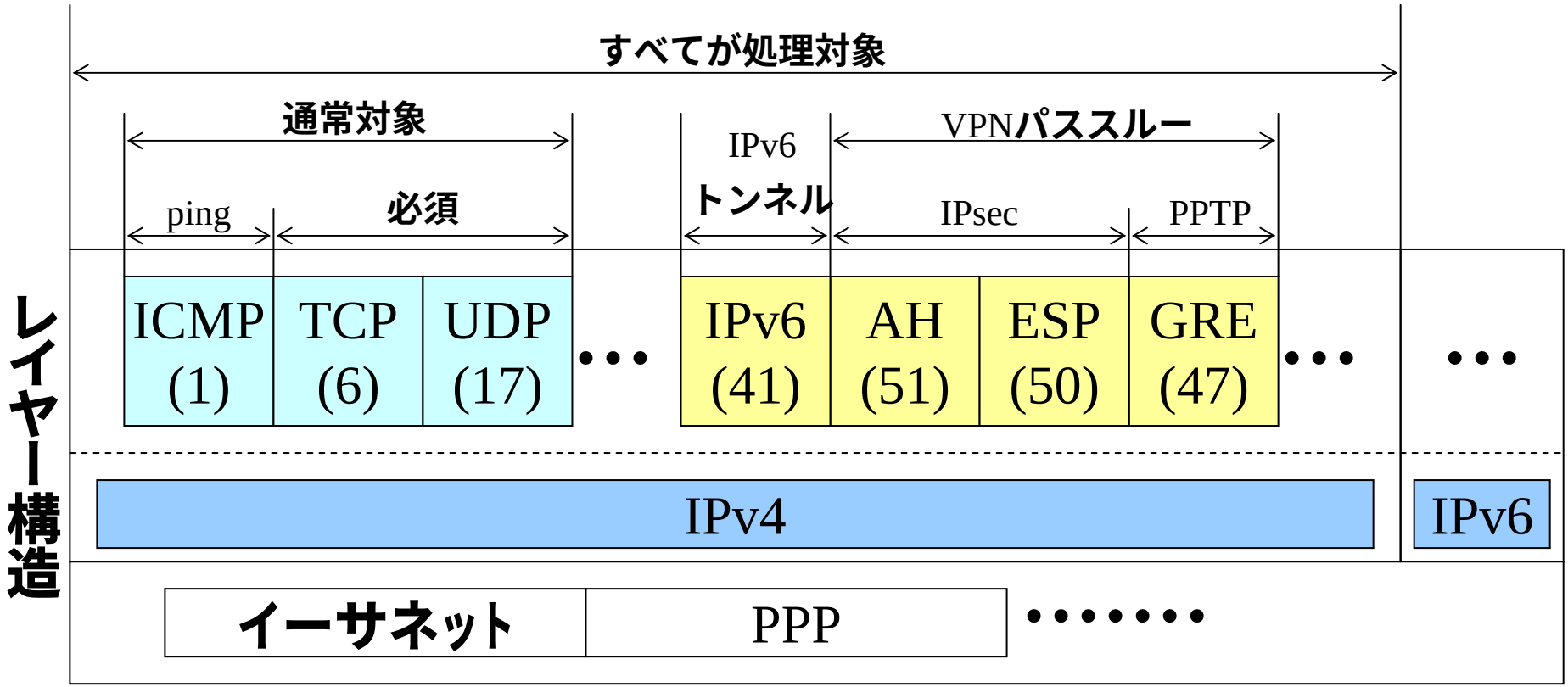
NATディスクリプタのフレキシビリティ

多機能なNAT箱を自由自在に複数同時利用できるしくみ



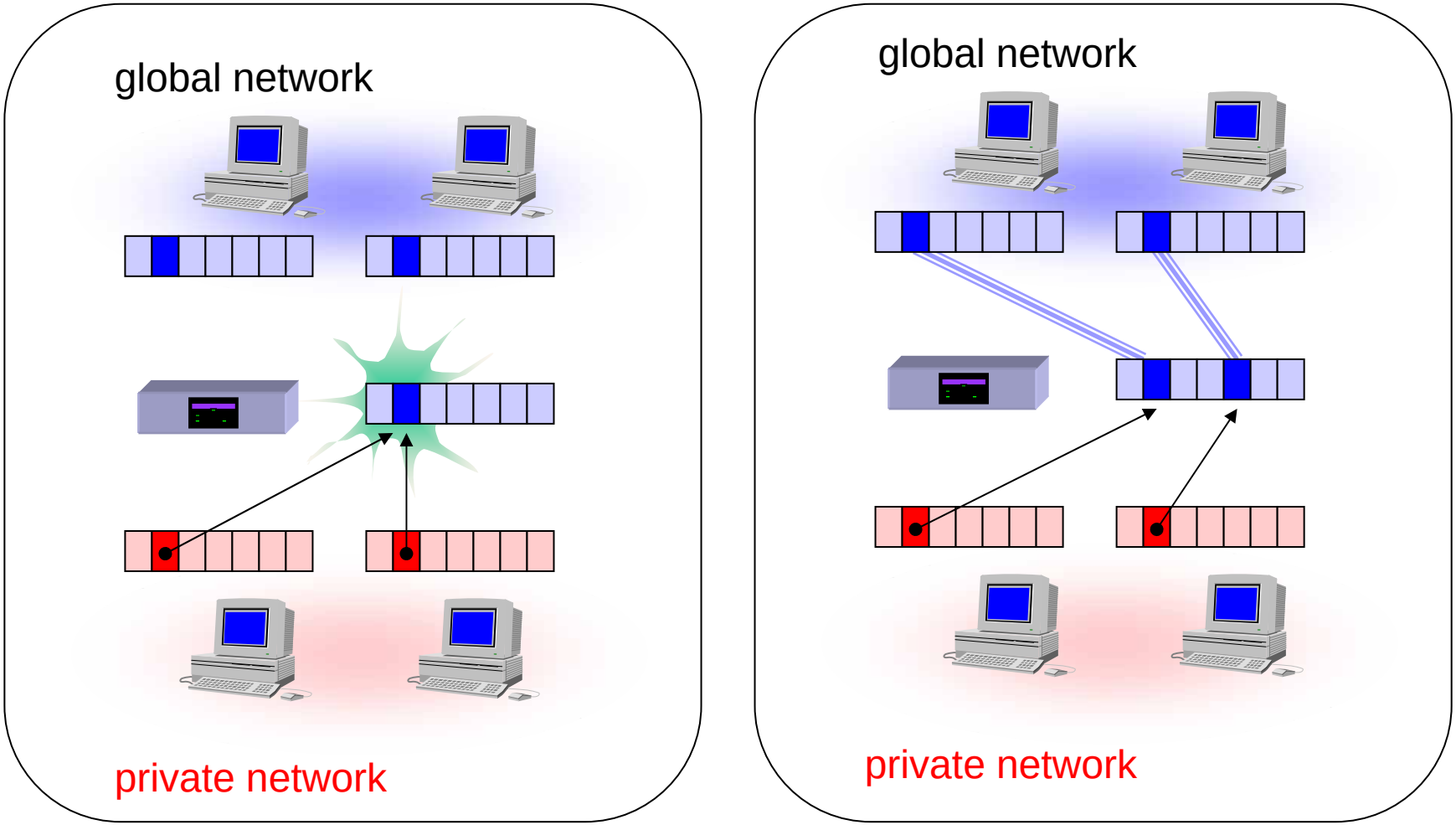
アドレス変換の処理対象

VPNやIPv6トンネルのためにICMP,TCP,UDPとは異なるプロトコルが利用される。IPマスカレードでも、これらのプロトコルに対してアドレス変換が行われる。



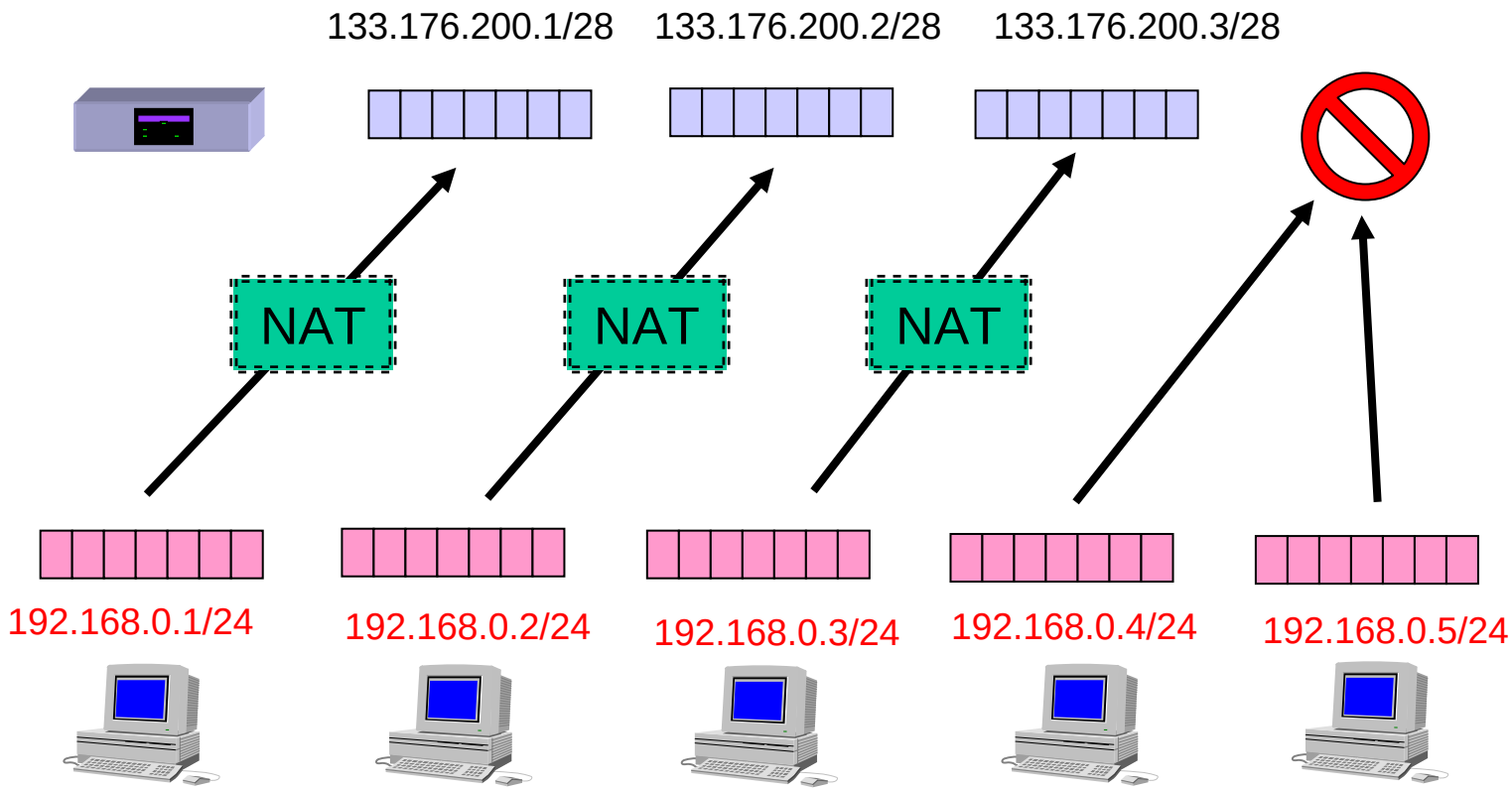
IPマスカレード(IP Masquerade)

nat descriptor type <NATディスクリプタ番号> masquerade



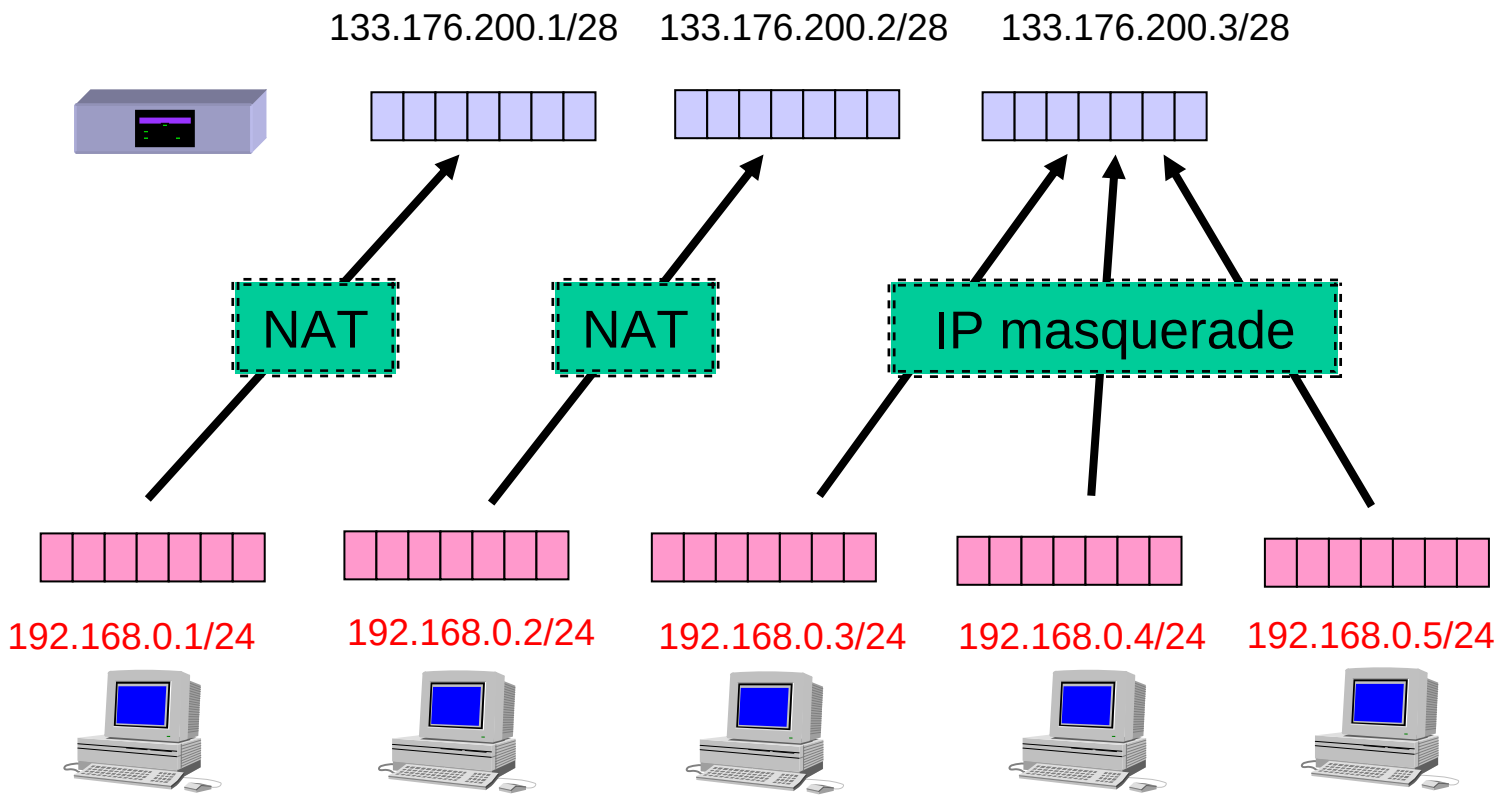
NAT (Network Address Translation)

nat descriptor type <NATディスクリプタ番号> nat

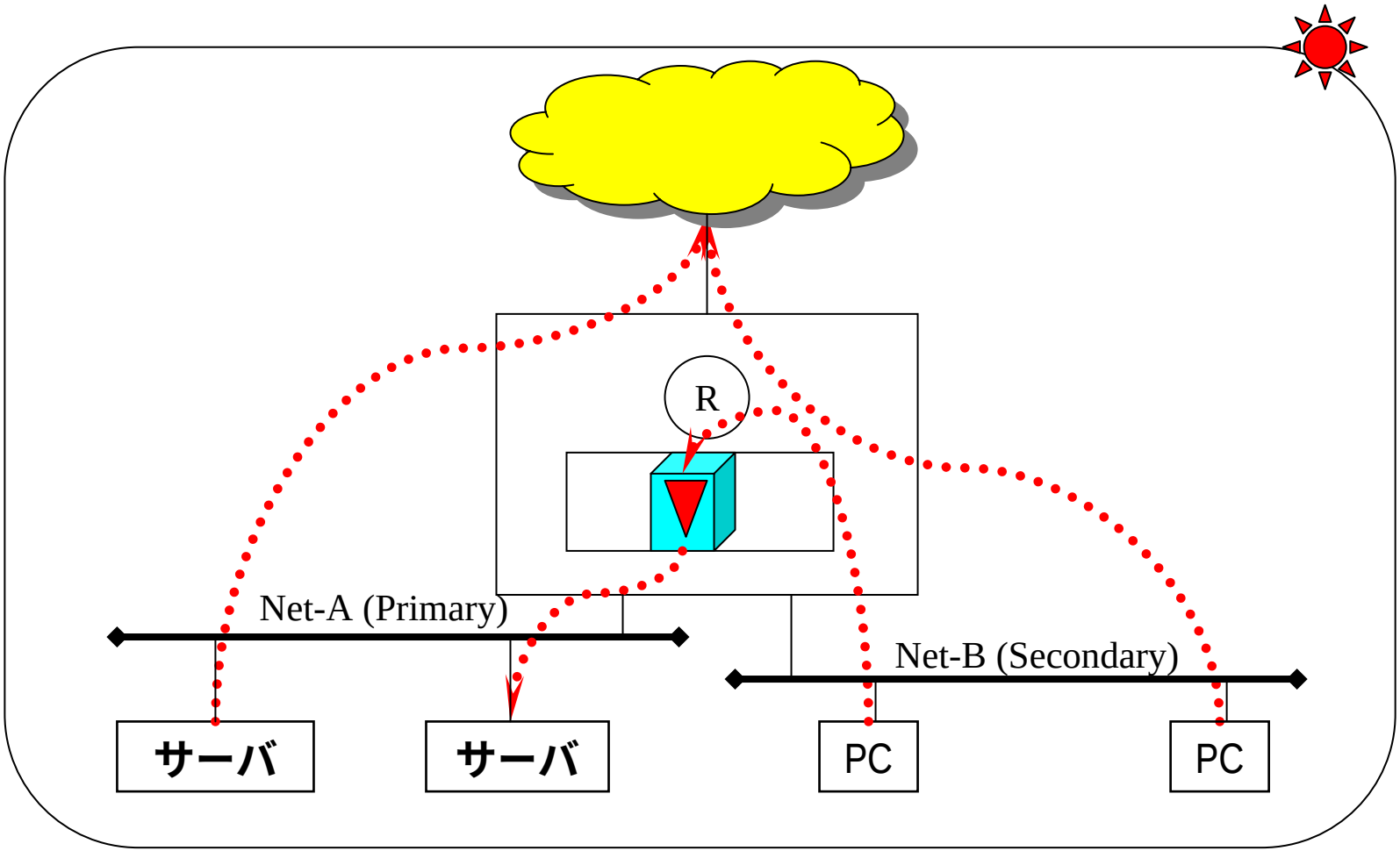


NAT + IPマスカレード形式

nat descriptor type <NATディスクリプタ番号> nat-masquerade

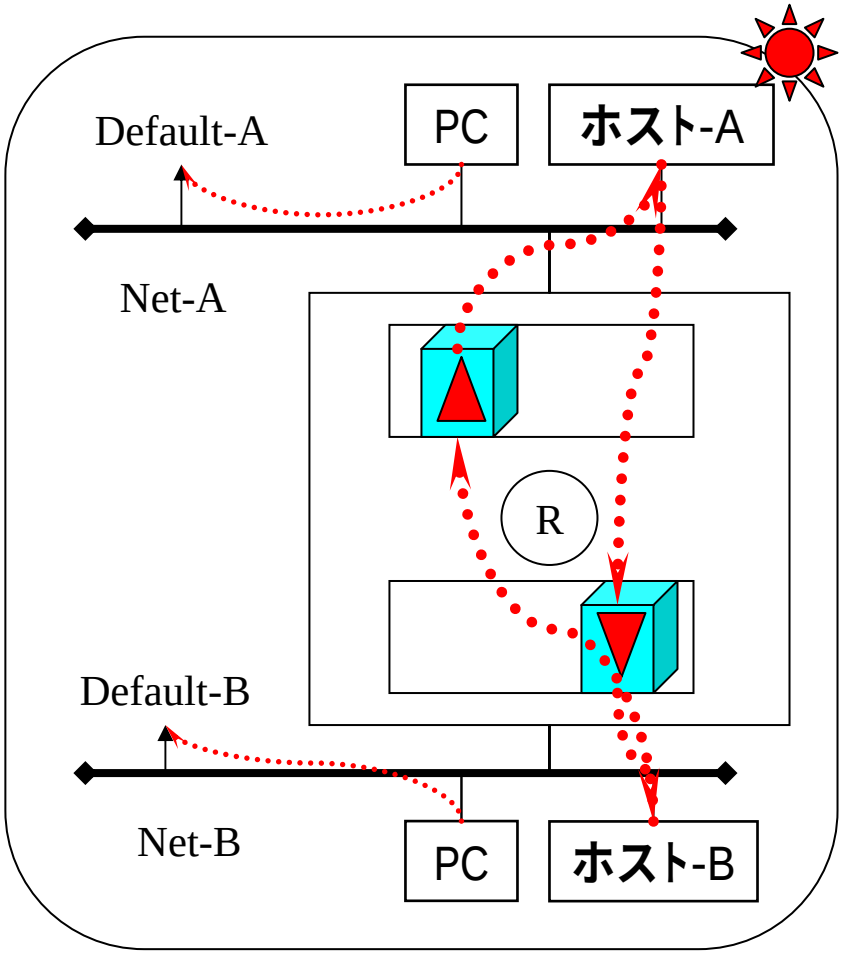


NATディスクリプタの応用例#1

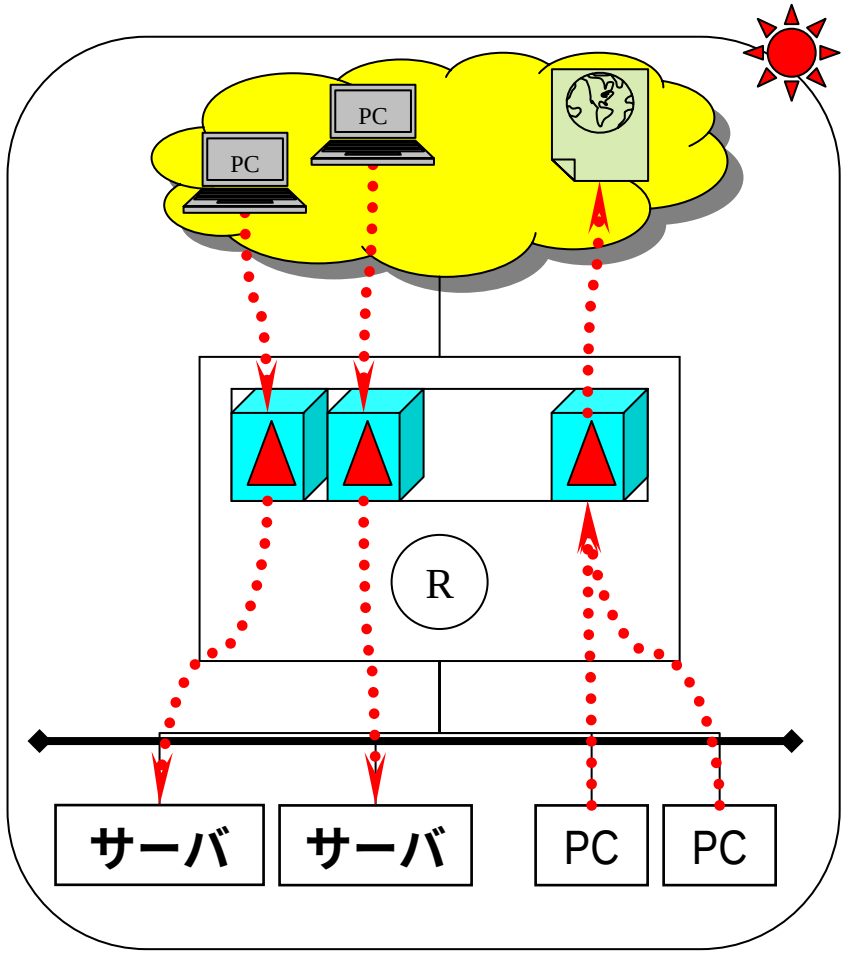


primary⇔secondary**間のIPマスカレード (逆マスカレード)**

NATディスクリプタの応用例#2



2つの隔離されたネット間での通信(hot line)

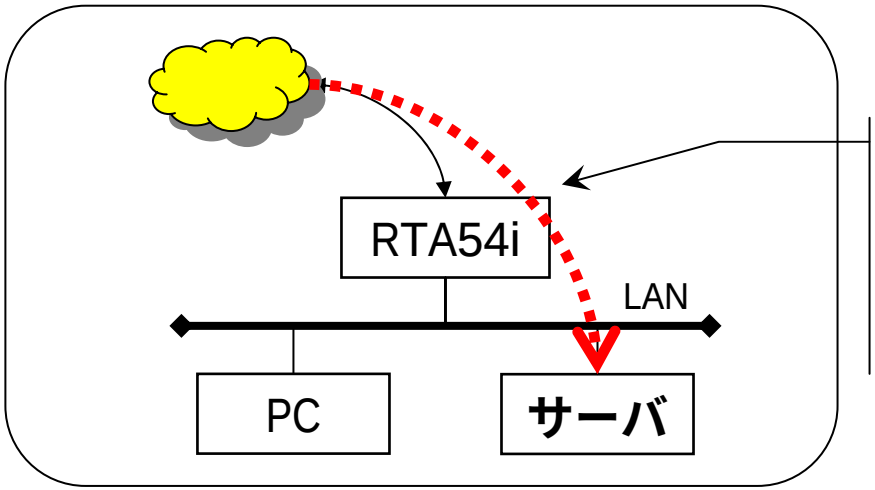


公開サーバにIPマスカレード適用

IPマスカレードの機能選択

- **外来パケット処理選択**(incoming)
  - **変換しないで、通過**(through)
  - **破棄** (reject,discard)
  - **特定のアドレスに変換** (forward…DMZ**ホスト機能**)
- **ポート割り当て方式の選択**(unconvertible port)
  - **必ずポート番号変換する処理**
  - **可能な限りポート番号変換しない処理**
- **ポート割り当て範囲の選択**(port range)
  - **ポート番号変換の割り当て範囲の変更**

DMZホスト機能



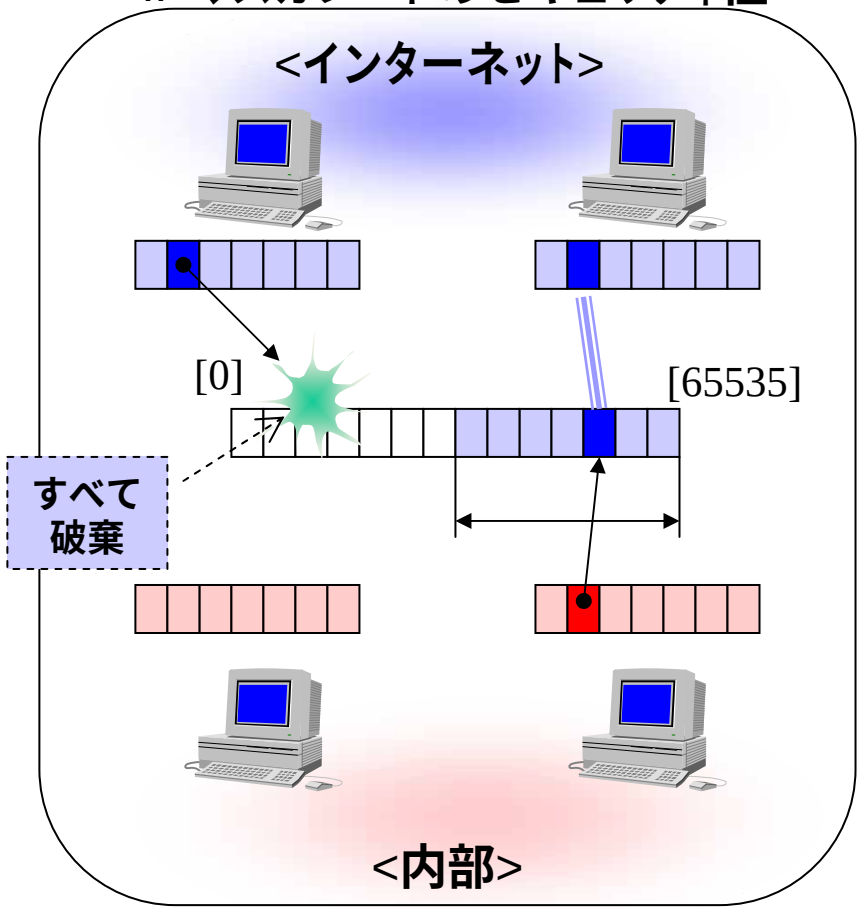
ISDN/ADSL/CATVプロバイダ接続(LAN)

[IPマスカレードの処理選択]
- through … 変換せずに通す
- reject …. 破棄して、TCPの場合はRSTを返す
- discard … 破棄して、何も返さない
- forward … 指定されたホストに転送する

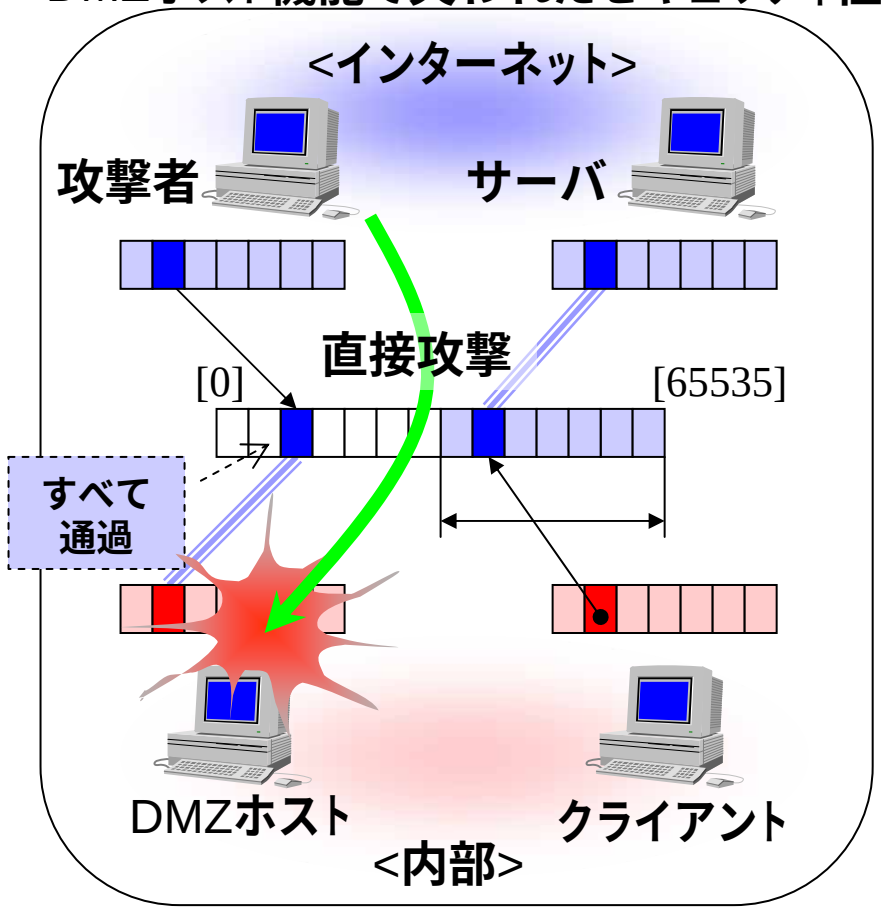
・ネットアプリ対応/ネットゲーム対応の機能
IPマスカレード機能を利用してインターネット接続を共有しているとき、インターネット側からの接続要求を特定のサーバ/ホストに転送する機能。
※セキュリティホールの側面

DMZホスト機能の脆弱性

IPマスカレードのセキュリティ性



DMZホスト機能で失われたセキュリティ性

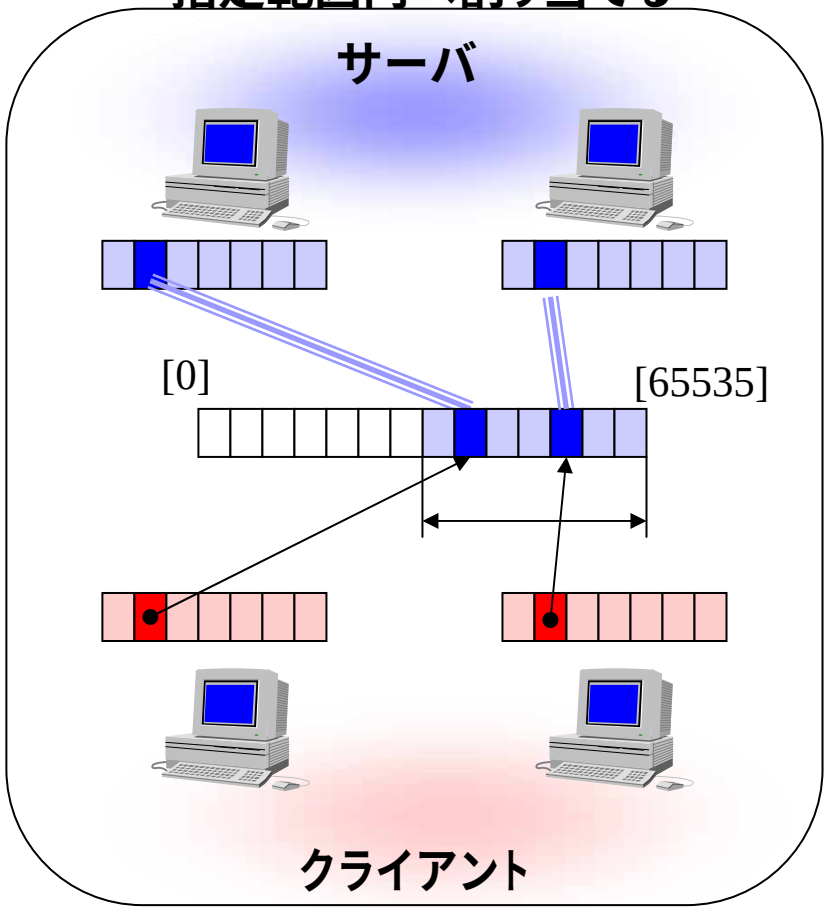


(利便性とセキュリティ性のトレードオフ)

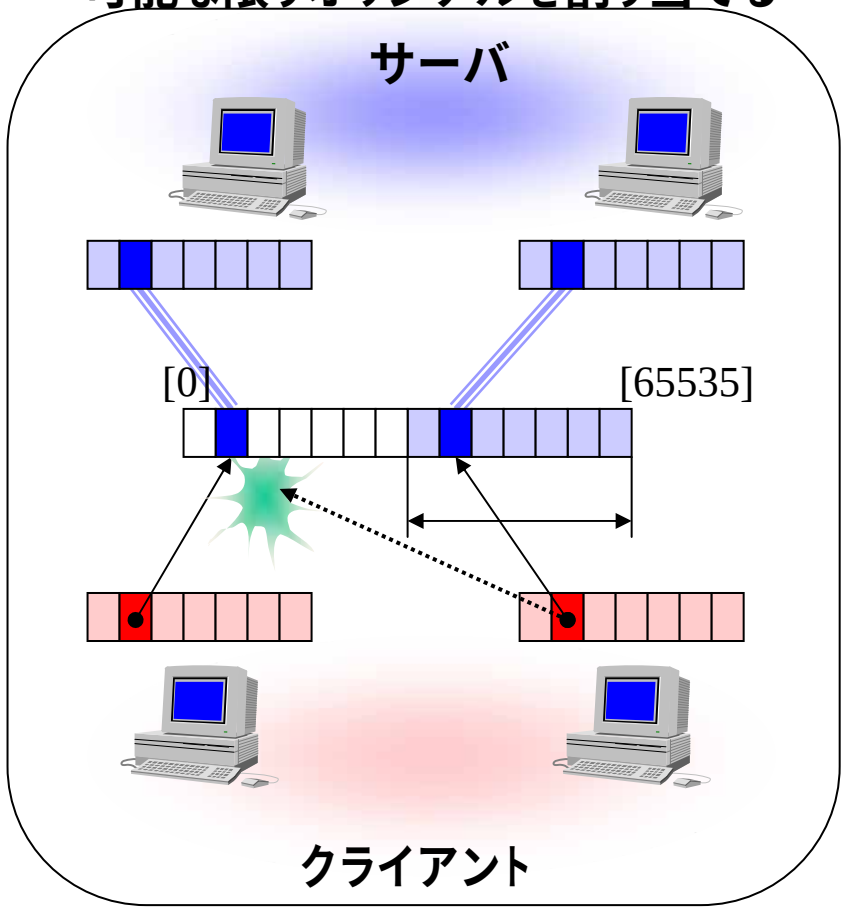
アドレス変換の苦手なアプリケーションが便利になるが、セキュリティ性は低下する。

ポート割当方式指定機能

指定範囲内へ割り当てる



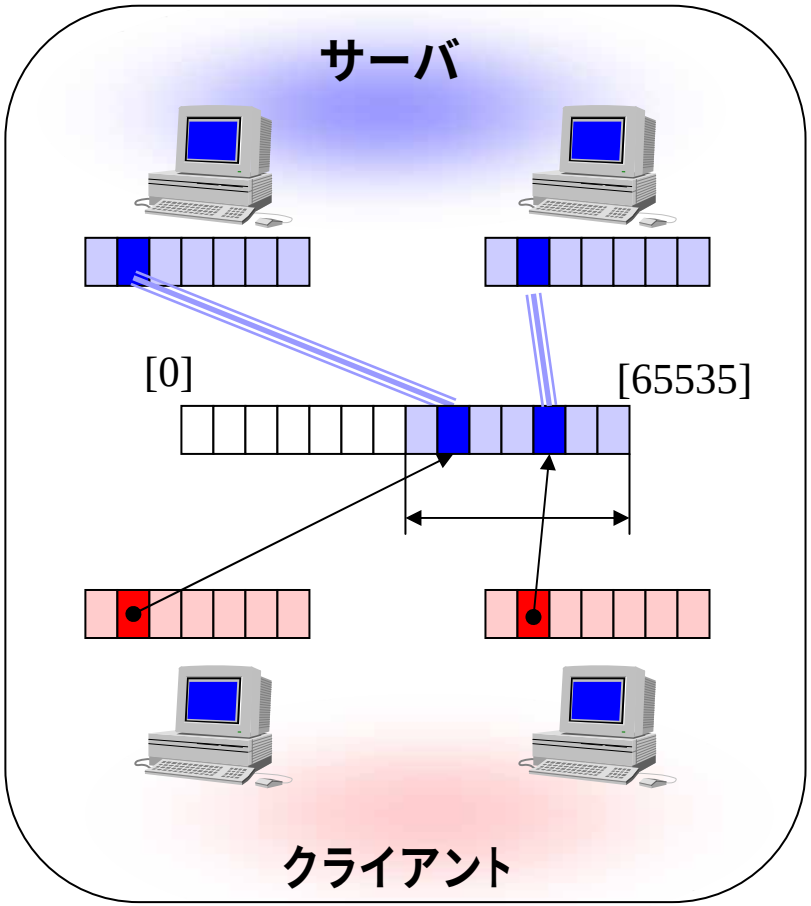
可能な限りオリジナルを割り当てる



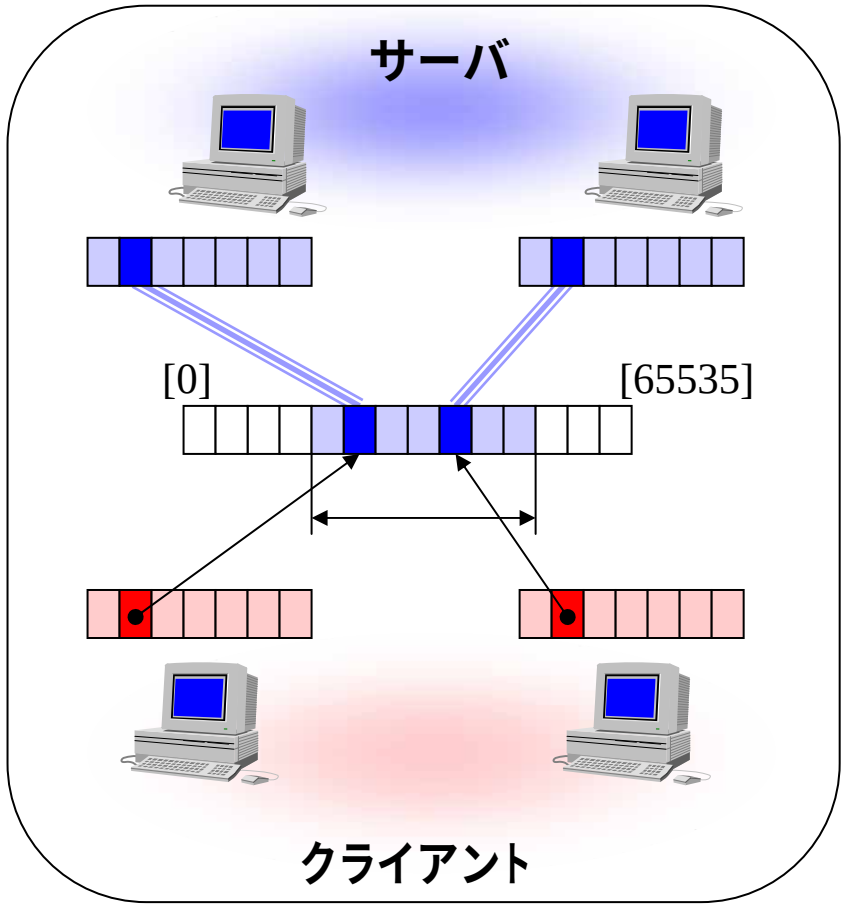
ポート番号変換を苦手とするアプリケーションの通信をできる限り救う。.

ポート割り当ての範囲指定機能

通常の割り当て範囲



割り当て範囲を変更

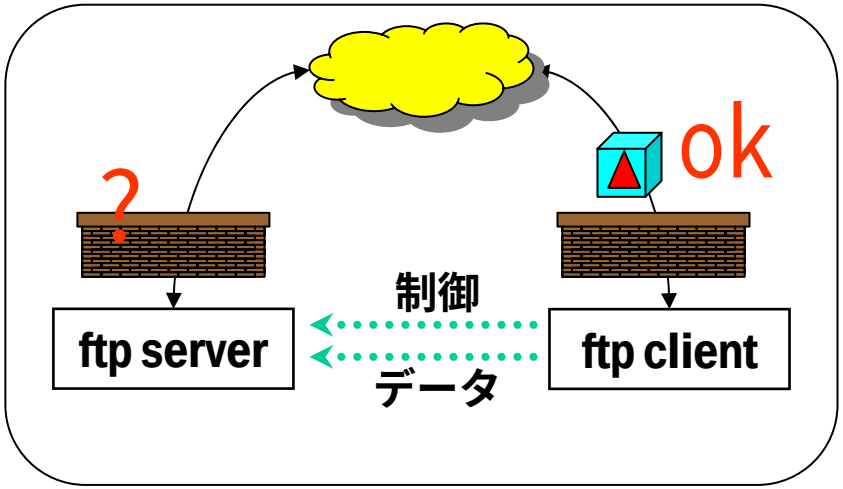


IPマスカレードで使用しているポート割り当て範囲(60000～64095)を他のアプリケーションで利用することができる。

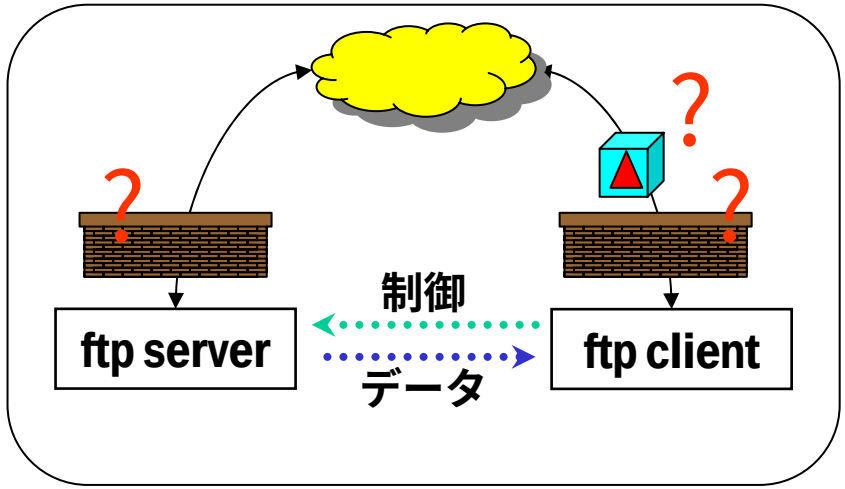
IPマスカレードのアプリケーション対応

- FTP対応
  - FTP/アプリケーション対応の必要性
  - FTPセッション保持機能
  - FTP監視ポート指定機能
- NetMeeting 3.0対応
  - 可能な限りポート番号変換しない処理
- VPNパススルー機能
  - 同時1セッション、静的IPマスカレードの制限緩和
- PPTPのマルチセッション対応

FTP/アプリケーション対応の必要性



ftpのパッシブ転送(PASVコマンド)



ftpのアクティブ転送(PORTコマンド)

[状況]

・アプリ/機能を実現するために複数のコネクションが必要

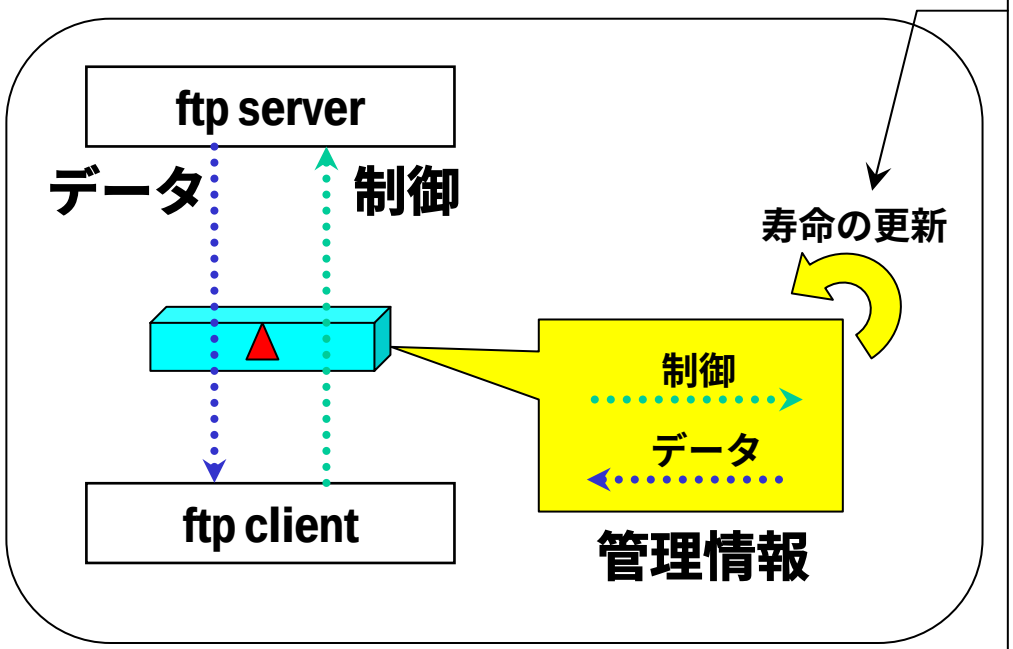
・双方向通信が必要なのに、片方向の通信環境での運用

[例外処理を必要とする通信]

・FTP,CU-SeeMe,NetMeeting Version 3.0, …

http://www.rtpro.yamaha.co.jp/RT/FAQ/TCPIP/ftp-passive-mode.html

FTPセッション保持機能



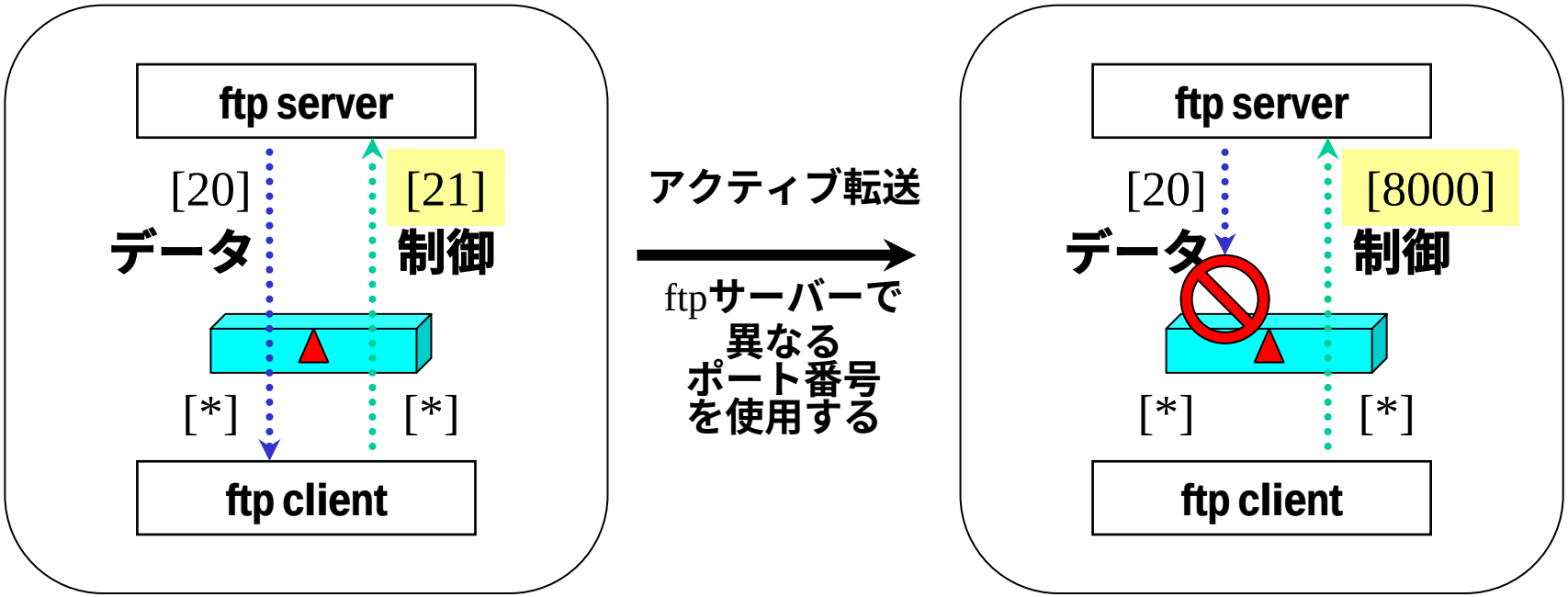
(通常の寿命更新)
　一定時間の寿命により管理情報から削除される。(接続が切れる)
(FTPセッション保持機能)
　ftpに連動したtcpの寿命延長

[FTPセッション保持機能の選択]
　FTPセッション保持機能における寿命延長対象の選択
- all … すべてのtcp
- ftp …. ftpの制御チャネルのみ

・大量のファイル転送が行われていると、通信に時間がかかり、制御チャネルのtcpコネクションが管理情報から削除されてしまう。
・ftp通信の制御チャネルを救うため、単純に寿命を長くすると、管理情報が溢れてしまう。

⇒効率的運用ノウハウ
　ftpの制御チャネルをtcpコネクションのみを寿命延長対象とする。

FTP監視ポート指定機能



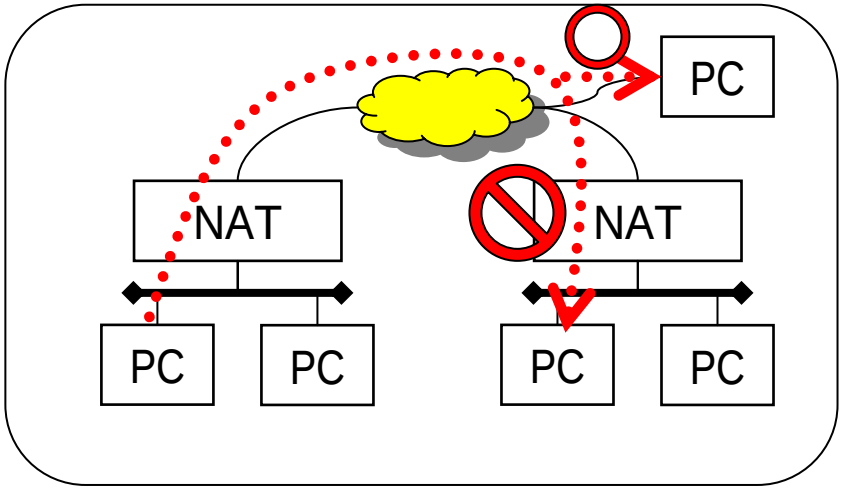
21番ポートで待ち受け⇒OK

8000番ポートで待ち受け⇒NG

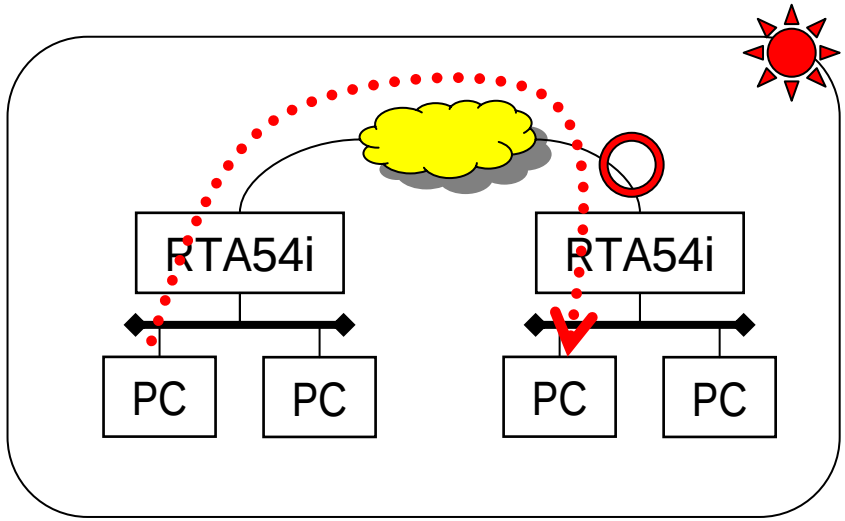
[悩み]

・ftpサーバーの待ち受けポート(LISTEN PORT)を21番以外に指定していると、NAT/IPマスカレードが越えられない。

NetMeeting Version 3.0対応



DMZホスト機能によるNetMeeting対応



NetMeetingの本格対応

- NetMeetingは、ブロードバンド時代のアプリケーション
  ビデオ会議、ホワイトボード、チャット、ファイル転送、
  プログラム共有、リモートデスクトップ共有
- 対応内容の違い
  DMZホスト機能による対応では、NATを使用していない通信相手に限られる。
  本格対応でNAT(IPマスカレード)越しでも通信可能

NetMeeting Version 3.0対応の仕様

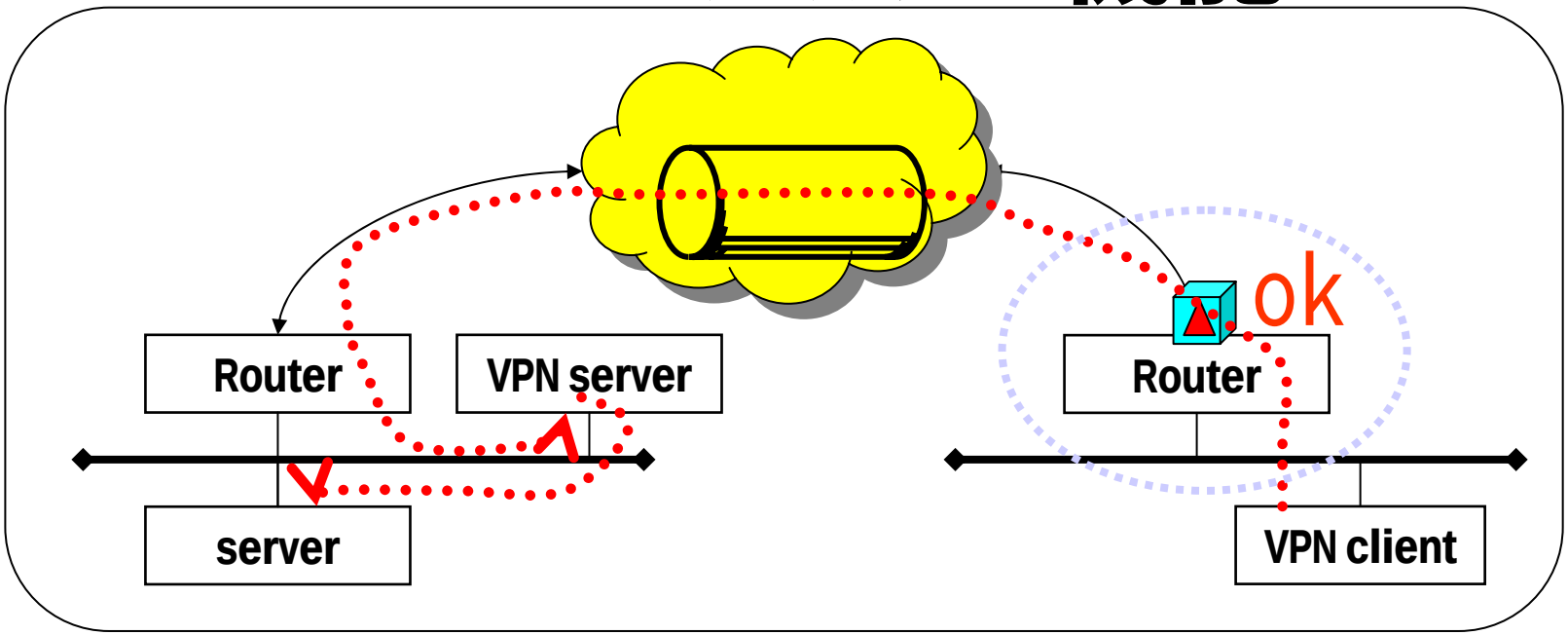
NATでNetMeetingに対応する処理を追加した。動作を確認している条件は 以下のとおりであるが、この条件を満たすときでも、ビデオや音声の片通 話などの問題が発生する可能性がある。なお、このような場合に、DMZホスト機能でNetMeetingを実施する端末を設定すると解決できることがある。

- NetMeeting Version 3.0
- ビデオ、音声、チャット、ホワイトボードの動作を確認済み
- ディレクトリサービスに対応しない
- 複数の端末がNATの外側へ同時に接続することはできない
- NATの外側から内側の端末へ接続するためには、下記のような静的 IPマスカレードの設定が必要

(例) NATの内側の端末のIPアドレスが192.168.0.2の場合

```
nat descriptor masquerade static 1 1 192.168.0.2 tcp 1720
nat descriptor masquerade static 1 2 192.168.0.2 tcp 1503
```

VPNパススルー機能

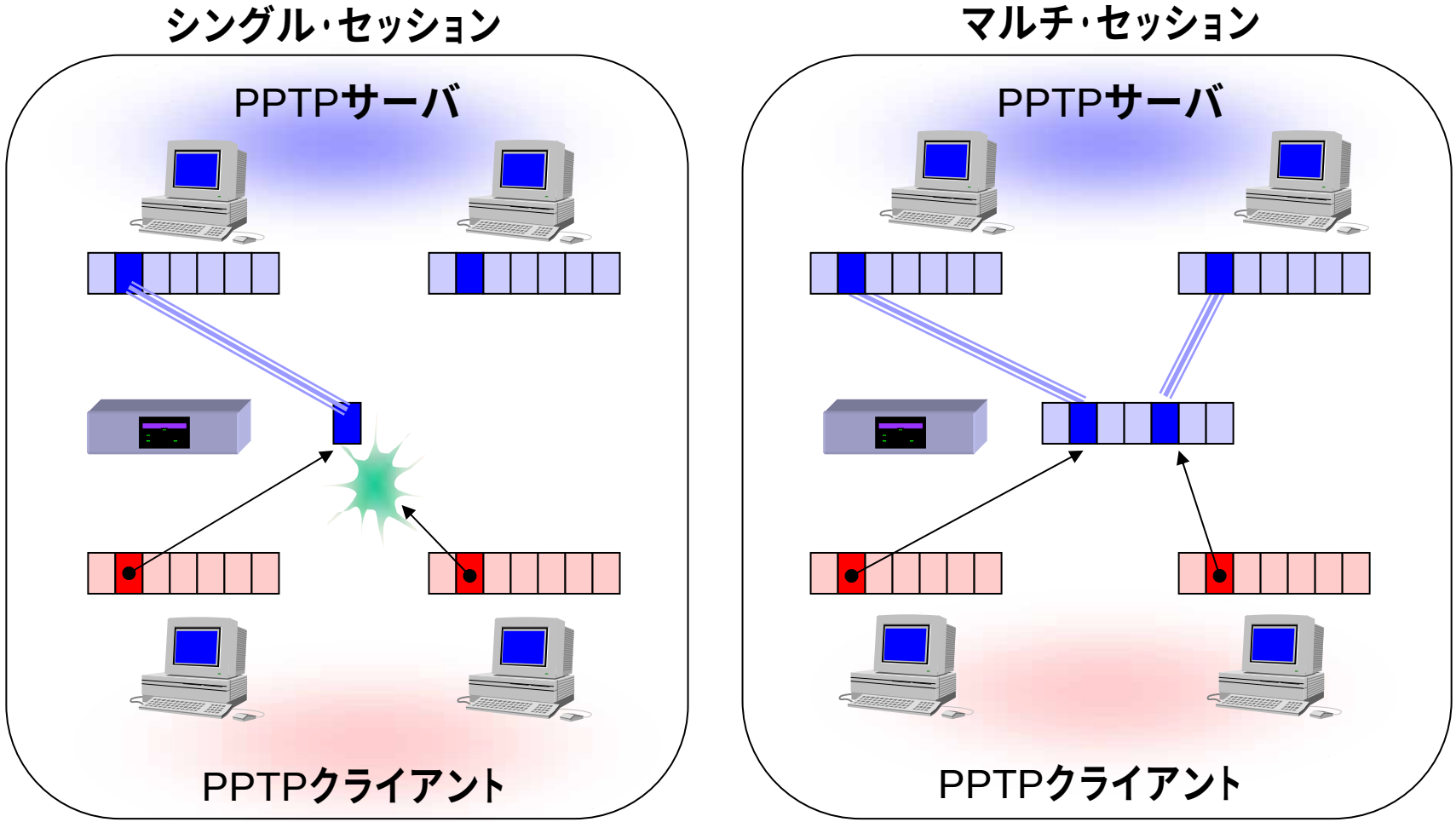


VPNやIPv6トンネルのためにICMP,TCP,UDPとは異なるプロトコルが利用される。これらのプロトコルに対しても、アドレス変換を行う機能。

⇒加えて、Rev.4.00.39より静的IPマスカレードによる固定を可能とした。

VPN種別	変換対象
PPTP L2TP	GRE(47)
IPsec	ESP(50) AH(51)

PPTPのマルチセッション対応



・同時に複数のMicrosoft VPN通信(PPTPによるVPN)が可能となる

PPTPのマルチセッション対応の仕様

IPマスカレードを動作させている時に、PPTPによるMicrosoft VPNを変換できるようにした。ルータ、Windows PC、Windows サーバのすべてで特別な設定は必要なく、IPマスカレードの内側(プライベートアドレス側)にあるPPTPクライアントである Windows PCから外側(グローバルアドレス側)にあるPPTP サーバであるWindows サーバとの間にPPTPによるVPNトンネルを通常の動作で設定できる。

同時に扱えるPPTPセッションの数に特に制限は設けていない。RTがIPマスカレードで扱える同時セッション数(最大4096)に制限を受ける。PPTPでは制御用と通信用で最低でも2つのセッションを必要とすることに注意。

Rev.6.02.18 リリースノートより

付録資料

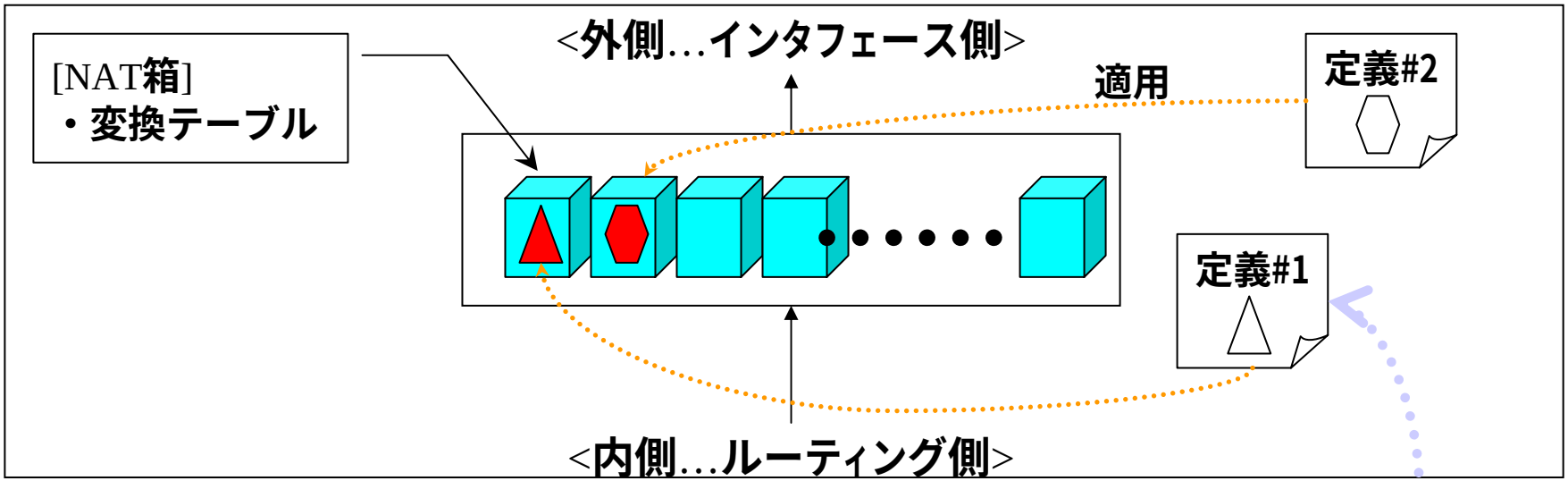
アドレス変換機能(NAT)への取り組み

日付	Revision	内容
1996年6月	Rev.1.06.08	・NAT機能
1996年11月	Rev.1.06.22	・IPマスカレード機能
1997年10月	Rev.2.02.15	・静的IPマスカレード機能
1999年 1月	Rev.4.00.02	・NATディスクリプタ機能(機能統合、多重適用、PP側適用、LAN側適用)
1999年4月	Rev.4.00.07	・TUNNELインタフェースへのNATディスクリプタ適用
1999年 8月	Rev.4.00.13	・ping./traceroute対応 ・IPマスカレード管理テーブルの仕様変更
2000年7月	Rev.4.00.39	・VPNパススルー(静的IPマスカレードの制限緩和)
2001年7月	Rev.6.02.07	・IPマスカレードにおける破棄パケットのログ
2002年1月	Rev.6.02.16	・DMZホスト機能 ・NetMeeting 3.0対応変換機能
2002年3月	Rev.6.02.18	・PPTPのマルチセッション対応処理 ・IPマスカレードのポート割り当て方式の指定 (常時変換、必要時変換) ・IPマスカレードのポーと割り当て範囲の指定 ・NAT/IPマスカレードのFTP監視ポートの指定

旧NAT機能(Rev.1系～Rev.3系)からの主な違い

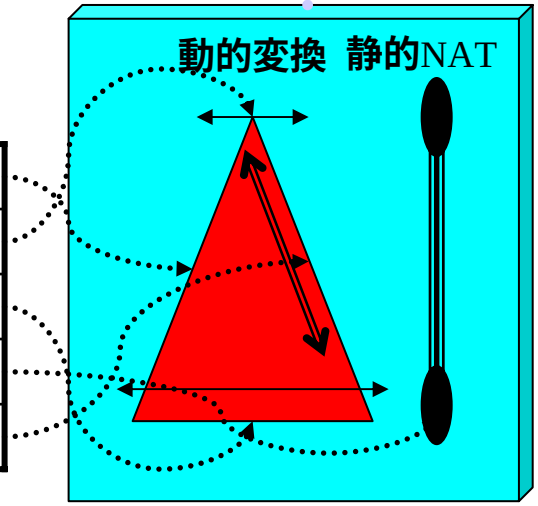
- LANインタフェースに対応
  - LANのprimary⇔secondaryの変換が可能
- TUNNELインタフェースに対応
  - VPNで変換が可能
- 3つの変換タイプ
  - NAT形式
  - IPマスカレード形式
  - NAT + IPマスカレード形式
- 機能統合、制限の緩和
  - 複数の変換規則を並列的に適用可能
    (ひとつのインタフェースに16組)

NATディスクリプタの構造



[定義→アドレス変換の設計図]

変換タイプ	動的なアドレス変換形式
外側アドレス範囲	動的アドレス変換に使用される範囲
内側アドレス範囲	動的アドレス変換の対象となる範囲
静的NAT	固定的なアドレス変換の組み合わせ
静的IPマスカレード	固定的なIPマスカレード変換



DMZホスト機能
～コマンド仕様～

IPマスカレードで、外側から受信したパケットに該当する変換テーブルが存在しないときに、そのパケットを特定のホストに転送できるようにした。このほかにも、破棄や通過などの動作を選択することができる。

○IPマスカレードで外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定

[入力形式] nat descriptor masquerade incoming DESC_ID ACTION [IP_ADDRESS]

[パラメータ] - DESC_ID ..... NATディスクリプタ番号
- ACTION ..... 動作
  - through ... 変換せずに通す
  - reject .... 破棄して、TCPの場合はRSTを返す
  - discard ... 破棄して、何も返さない
  - forward ... 指定されたホストに転送する
- IP_ADDRESS ... 転送先のIPアドレス

[説明] IPマスカレードで外側から受信したパケットに該当する変換テーブルが存在しないときの動作を設定する。ACTIONがforwardのときにはIP_ADDRESSを設定する必要がある。

[デフォルト値] reject

ポート割当方式指定機能
～コマンド仕様～

IPマスカレードで可能な限りポート番号変換を行わない方式を選択可能にした。これにより、アドレス変換を苦手とするアプリケーションを救えるようになる。

○IPマスカレードで、特定のポート番号は変換せずにそのまま外部に転送できる機能
を実装した。

[入力形式]

```
nat descriptor masquerade unconvertible port DESC if-possible
nat descriptor masquerade unconvertible port DESC PROTOCOL PORT
```

[パラメータ]

DESC ... ディスクリプタ番号
PROTOCOL ... プロトコル、'tcp'もしくは'udp'
PORT ... ポート番号の範囲

[説明]

IPマスカレードで変換しないポート番号の範囲を設定する。
if-possibleが指定されている時には、処理しようとするポート番号が他の通信で使われていない場合には値を変換せずそのまま利用する。

ポート割り当ての範囲指定機能
～コマンド仕様～

IPマスカレードで使用するポート割り当て範囲(60000～64095)を変更することができるようになった。これにより、この範囲を他のアプリケーションで利用することができるようになる。

○IPマスカレードで利用するポートの範囲を設定できるようにした。

[入力形式]

```
nat descriptor masquerade port range DESC START [NUM]
```

[パラメータ]

DESC ... ディスクリプタ番号
START ... 開始ポート番号、1024～65534
NUM ... ポート数、1～4096、省略時は4096

[説明]

IPマスカレードで利用するポート番号の範囲を設定する。STARTとNUMの和が65535以下(START + NUM ≦ 65535)でなくてはいけない。

[デフォルト]

60000 4096

FTPセッション保持機能の管理対象選択

～コマンド仕様～

このコマンドによってIPマスカレードテーブルのTTLの扱いを制御することができる。通常、テーブルのTTLは単調に減少するが、FTPのように制御チャネルとデータチャネルからなるアプリケーションでは、制御チャネルに対応するテーブルをデータ転送中に削除するべきではないため、制御チャネルとデータチャネルの両テーブルのTTLを同期させている。ただし、現有の機能では、制御チャネルとデータチャネルの対応を把握することが難しいため、同じホスト間の通信については、すべてのコネクションを関係づけ、TTLを同期させている。しかしながら、このような動作では、多くのテーブルのTTLが同期し、多くのテーブルが長く残留するという現象が起きる。さらに、状況に よっては、ルータのメモリが枯渇する可能性もある。そこで、この処理をFTPの制御チャネルに限定し、メモリの枯渇を予防する選択肢を提供する。

[入力形式]

```
nat descriptor masquerade ttl hold TYPE
```

[パラメータ]

TYPE ... TTLを同期させる方法

- ‘all’ ... すべてのコネクションを対象とする
- ‘ftp’ ... FTPの制御チャネルのみを対象とする

[説明]

TTLの同期をFTPの制御チャネルに限定するときには、パラメータに‘ftp’を設定する。FTPに限定せず、従来と同じように動作させるためには、パラメータに‘all’を設定する。

[デフォルト値]

all

FTP監視ポート指定機能

～コマンド仕様～

FTPサーバーの待ち受けを「任意のポート番号」でも、
FTP通信を適切に行えるようになる。

○NAT/IPマスカレードで、FTPとして認識するポート番号を設定できるようにした。

[入力形式]

```
nat descriptor ftp port DESC PORT [PORT...]
```

[パラメータ]

DESC ... ディスクリプタ番号、1～ 65535

PORT ... ポート番号、1～65535

[説明]

TCPで、このコマンドにより設定されたポート番号をFTPの
制御チャネルの通信だとみなして処理をする。

[デフォルト]

21