エンドツーエンドNATを前提としたアドレス分配

太田昌孝（東京工業大学）
森岡仁志（ルート（株））
藤川賢治（NICT）

話の概要

- アドレス枯渇対策の現状
- エンドツーエンド原理とNAT
- エンドツーエンドNATの実際
  - 基本動作、スタティック／ダイナミック、ポート番号、アプリケーションリレー、ネスト、非対応端末、逆引き、マルチキャスト、モビリティ、、、
- 実装の紹介とデモ
- あるべきアドレスポリシー

IPアドレスが足りない！！

- それでもIETFなら、、、IETFならきっと何とかしてくれる！？
  - いまだに、何ともなっていない、なりそうもない
    - NATによるアドレス節約
      - エンドツーエンドインターネットを破壊
      - いろんなプログラムが、まともに動作しない
    - IPv6によるアドレス拡張
      - 実運用を考えない政治的妥協の産物
      - OH、PMD、AC、LLA等有害無益な機能を盛込み過ぎ
      - 本稿では、特に断らない限り、IPv4のみを仮定

SALTZER等の原論文でのエンドツーエンド論法

http://groups.csail.mit.edu/ana/Publications/PubPDFs/End-to-End%20Arguments%20in%20System%20Design.pdf

- The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)

今のNATはなぜエンドツーエンドでないのか？

- 途中でアドレスを書き換えたら、エンドツーエンドでなくなるのは、当たり前？
- 原論文によると
  - 網の機能（アドレス書き換え）は、端の知識と助けがないと不完全で不正確
  - 端の知識と助けがあれば？
    - 端が助けようにも、今のNATは、ほとんど見えない
      - エンドツーエンドでない原因
      - 端に隠しきれない不整合は見えるが、助けようがない

エンドツーエンドNAT
ー　NATの存在を端に積極的に見せる　ー

- プライベート網内の端末にNATGWの知る
  - 各端末で共有するパブリックアドレス
  - 各端末に割り当てたポートの範囲
  - NATGWとの通信方法（アドレス、ポート）

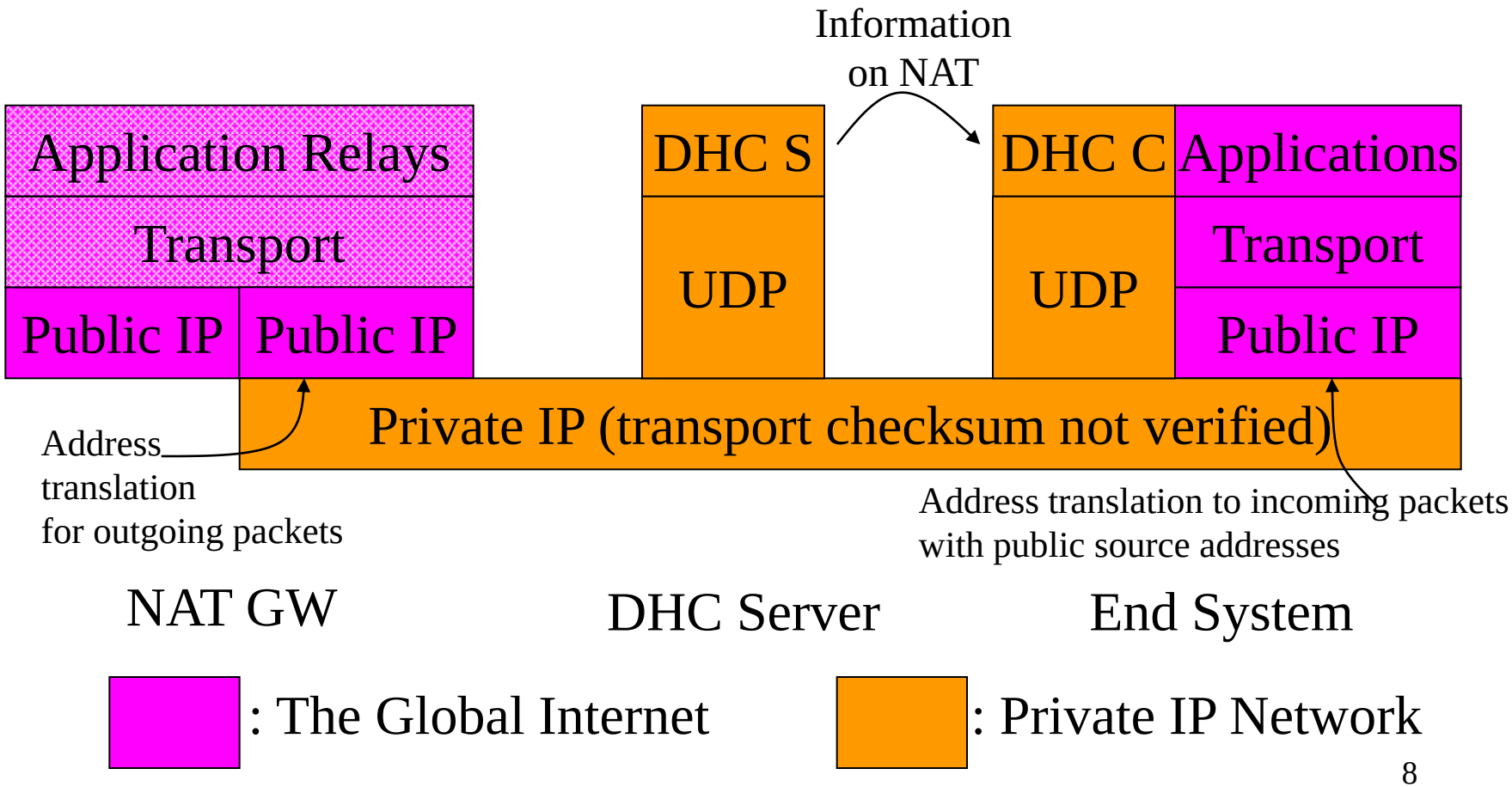
等の情報を、DHCPやPPP等で通知

- 各端末は
  - 自らの知識により、NAT動作が完全かつ正確なものになるように、補完する

エンドツーエンドNATの基本動作

- NATGWは
  - 外部からのパケットを、フラグメント解消後、ポート番号に応じ、受信者アドレス変換
    - トランスポート情報（ポート、チェックサム）は放置
    - 一部パケットは自分で受けてもよいが、、、
- プライベート網内の端末は
  - 受信者アドレスをパブリックアドレスに戻す
    - トランスポート情報との整合性も自ずから回復
  - 送信者ポートとして自分のものしか使わない

エンドツーエンドNATの レイヤー構造



スタティックNATと ダイナミックNAT

- スタティックNAT
  - 各端末に固定したポート範囲を割り当て
    - ポート数が多ければ（数百？）、これで十分
      - 端末は自己に割り当てられたポートのみをソースポートとして使う。返事が貰えないので、偽装は無理。
- ダイナミックNAT
  - 各端末は、ポート番号を随時NATGWに要求
    - NATGWのポート割当状態は、端末主導で更新
      - タイムアウト、複数GW間整合性等の問題は解消

固定ポートでのE2ENATとポートフォワーディングとの違い

- ポートフォワーディングでは
  - 一部のポートを特定の端末に固定割当
    - 旧来のNATが、トランスポート層で中継
    - スタティックNAT同様、端末はサーバ動作可能？
      - 実は透過性は無く、クライアントすらまともに動かない
- E2ENATでは
  - 端末の助けにより、完全なE2E透過性を実現
    - ftpクライアントのportコマンドも、動作

エンドツーエンドNATとポート番号

- 多くのアプリでは、デフォールト以外のポート番号をURLで陽に指定可
- E2ENATはほぼIP層だけで動作するが
  - 受信者ポート番号はIPヘッダの外にある
    - 純トランスポートプロトコルでは、IPヘッダ直後16ビットが送信者ポート、次16ビットが受信者ポート
    - ICMPの仕様から、ICMP以外は、送信者ポート番号は、IPヘッダ直後の8バイトに含まれるはず
      - ポート番号は、IPヘッダ直後8バイト内の2バイト境界間の16ビットと決め打ちしてもよさそう（IPSECも対応可）

エンドツーエンドNATとアプリケーションリレー

- DNS、SMTP、HTTP等は、NATGWのデフォールトポートでリクエストを受け、リクエスト中の情報（ドメイン名等）で、リクエストを端末に振り分け可
  - HTTP：のURLでのポート指定は不要に
  - DNSやSMTPのポートはNSとMXに内包され（URLで指定不可）、プライベート網内にサーバを置くには（置けなくても、ほとんど困らないが）、アプリケーションリレーは必須

エンドツーエンドNATと非対応端末

- NATGW背後のE2ENAT非対応端末は
  - DHCP等によるアドレス割り当ては受けても
    - NAT情報は理解できない
- 非対応端末が出したパケットに対して
  - NATGWは旧来のNATとして対応してもよい
    - UPnP機能等もあってもよい
- E2ENAT対応端末との区別は
  - 対応端末がNATGWに登録すれば可能

エンドツーエンドNATのネスト

- E2ENATGWはネスト可能
- ISPからスタティックNATで多数（数百？）のポート番号を割り当てられた顧客は
  - 一部をサーバで固定的に利用
  - 一部はダイナミックNATGWの外側に割当
    - ダイナミックNAT背後にネストしたプライベートネットワーク内の多数の端末で、ポート番号をダイナミックに共有

エンドツーエンドNATと逆引き

- 共有アドレスは普通に逆引き可能

  www.example.com A 208.77.188.166

  166.188.77.208.in-addr.arpa PTR www.example.com

- ポート別の逆引きは以下のように可能

  p1.example.org CNAME www.example.com

  1.0. 166.188.77.208.in-addr.arpa PTR p1.example.org

  p2.example.org CNAME www.example.com

  2.0. 166.188.77.208.in-addr.arpa PTR p2.example.org

  – PTRがCNAMEを指すことは、PTRから先の自動参照の懸念（RFC1034）はないので、問題ではない

エンドツーエンドNATと マルチキャスト

- マルチキャストアドレスは、内外で共通
- プライベート網内の端末が送信する場合
  - マルチキャスト経路制御にはソースアドレスへの経路が影響するので
    - マルチキャストパケットはNATGWが出すべき
    - 端末は、送信すべきパケットを、IP over IPで、NATGWへ転送
      - PIMの仕組みでも使えばよい

エンドツーエンドNATとモビリティ

- ホームアドレスがNAT背後にいる場合
  - NAT情報をMHに設定（静的設定で十分）
  - ホームNATGWとの通信は、HAが中継
- MHがNAT背後にいる場合
  - フォーリンアドレスとホームアドレスで、使えるポートは一般には一致しない
  - HA－＞MHのトンネルをIP over UDP over IPにすれば、解決
    - フォーリンポートは一個で十分（アドレス節約）

実装

- NetBSD5．0ベース
- 本質的改造は、
  - アドレス変換と逆変換のため
    - 端末のip__input．cへの数行の追加
    - GWのip__input．cの数十行の追加
  - ソースアドレスとソースポートの制限のため
    - 端末とGWのin__pcb．c等の数百行の追加
    - 端末とGWのip__output．cの数行の追加
      - NICにトランスポートチェックサム計算をやらせない

エンドツーエンドNATのデモ

- 時間とネットワーク環境の許す限り、、、

エンドツーエンドNATと アドレス分配ポリシー

- E2ENATは、現状のインターネット環境をエンドツーエンド透過性も含めほとんど全て保ちながら、アドレスを大幅に節約
- E2ENATをアドレス分配の前提にすべき
  - ISPの労力は？
    - どう考えても、IPv6とのデュアル運用より少ない
    - 特に、アドレスが暗記できるのは、非常に重要
- クラスEアドレスも利用すべき

エンドツーエンドNATへのISPの対応

- 旧割当はそのままに、新アドレスについて
  - スタティックNATGWを配備
    - 必用に応じて、アプリケーションGWを配備
  - 固定アドレスを渡していない場合
    - DHCPで（一般には毎回異なる）アドレスとポート番号範囲を顧客に渡す
  - 固定アドレスを渡している場合
    - DHCPや書面で、顧客に応じたアドレスとポート番号範囲を顧客に渡す

エンドツーエンドNATと クラスEアドレス

- クラスEアドレスは、長持ちしない！？
- E2ENATによるアドレス節約前提なら
  - 移行期間の後、クラスEアドレスをユニキャストに使う意味はある
    - E2ENAT対応には端末の改造が必須なので
      - 同時にクラスE対応にすればよい
    - ISPやルータや既存の端末が対応しないと相互接続性が、、、
      - IPv6対応よりは、はるかに簡単（特にISPやルータ）

エンドツーエンドNATとプリフィックス

- 大域経路表に／24より長いのが増える？
  - 1600万あれば十分（というか多すぎ）
- どのみち、IPv6では、大域経路表プリフィックス数の抑制の試みは崩壊
- IPで時間を稼いで
  - エンドツーエンドマルチホーミングを実現
  - 新世代IPに、乞う御期待
- ともかく、NICのビジネスではない

エンドツーエンドNATと エンドユーザー

- E2ENATの導入によりエンドユーザーは
  - サーバーもクライアントも今と同様に動作
  - IPv6対応は不要に
    - アドレス（とポート）は、普通の人でも暗記可能
  - httpのURLではポート指定不要
  - 既存ユーザーはそのままで、新規ユーザーは
    - （旧来のNAT環境が嫌なら）端末改造が必要
      - このまま旧来のNAT導入するより、遥かによい

エンドツーエンドNATとNIC

- エンドツーエンドNATを導入すると
  - 割振サイズは小さく
  - 割振速度は低下（／256で割振った場合）
  - IPv6対応は不要に

ポリシー提案

- 将来的（遅くとも、最終ブロックを使い始める時点）に、エンドツーエンドNATもしくは類似技術によるエンドツーエンド透過性を維持したアドレス節約を前提とし、利用者数に対するアドレス割当量を削減すること
- クラスEアドレスの将来的（エンドツーエンドNATもしくは類似技術が普及した後）なユニキャストでの利用

エンドツーエンドNATプロトコル詳細議論用のメイリングリスト

- 日本語(*=ja)、と英語(*=en)を用意
  - e2enat-*-admin at mobile-broadband.org
- 参加方法
  - e2enat-*-ctl at mobile-broadband.orgに、
  - subscribe Your-Last-Name Your-First-Name

まとめ

- E2ENATは、現状のインターネット環境をエンドツーエンド透過性も含めほとんど全て保ちながら、アドレスを大幅に節約
- E2ENAT前提のアドレス管理により、IPアドレス空間は（クラスEも使えばなおさら）当分持つ
- IPv6？なにそれ？

http://www.ictconsulting.ch/presentations/CHEP09-Final.ppt
より引用（赤字化は太田）

Where is the Internet heading to?

CHEP’2009 conference

Praha (24/3/09)

Olivier.Martin@ictconsulting.ch

Will IPv6 be deployed soon?

- Network World 20/3/09
  - *"Business incentives are completely lacking today for upgrading to IPv6, the next generation Internet protocol, according to a survey of network operators conducted by the Internet Society (ISOC)."*
  - http://www.isoc.org/pubs/2009-IPv6-OrgMember-Report.pdf
- Special Network World Issue 21/1/09 (sponsored by NTT)
  - IPv6: Not If, When?

Some statements on IPv6

- Are NATs for IPv6 a necessary evil?
  - Russ Housley (IETF Chair)
    - "They are necessary for a smooth migration from IPv4 to IPv6 so that the important properties of the Internet are preserved"
    - We need to be pragmatic!
- IVI draft X. Li
  - "The experience for the IPv6 deployment in the past 10 years strongly indicate that for a successful transition, the IPv6 hosts nee to communicate with the global IPv4 networks [JJI07]"

Large scale IPv6 deployment

- For sure, IPv6 migration will NOT happen as envisaged some 10 years ago, i.e. dual stack
  - May even never happen, even so this is rather unlikely!
- Changing paradigms
  - end2end no longer a dogma
  - NATs no longer evils
  - IPv4 only<-->IPv6 only, no longer a taboo
  - Translators needed (Many competing IETF drafts):
    - SIIIT (Stateless Ip/Icmp Translation, the basis)
    - IVI (CERNET)
    - NAT64 & DNS64
    - Dual-stack lite (Comcast)
    - 6rd (6to4 revisited) –free (France)
    - NAT6 IPv6 NAT (Cisco)
    - SNAT-PT (Simplified NAT-PT

Conclusions

- The IPv4 Internet is growing fast but cannot continue “as is” beyond 2011!
- IPv6 looks “almost” unavoidable but is by no means “guaranteed” to happen!
- Last major architecture change was the introduction of MPLS
- clean-slate solutions are unlikely to be viable before 7-15 years
  - the related work may be dangerous as it could create an even worse political delusion than the “IPv6 cures everything” delusion!
  - A gradual step-wise evolution appears to be much safer
- The instability of the Internet routing system is preoccupying as well as the increasing lack of “network neutrality”, copyright infringements, etc.