Internet Week 2001 チュートリアル

T15: IPv6 ユーザネットワークの移行

2001年12月6日

NEC
藤本幸一郎 <koichiro@ipv6.nec.co.jp>

NEC

Agenda

- 移行技術の分類：基礎
- 移行のフェーズ
- ISPの移行
- 大規模サイトの移行
- 小規模サイトの移行
- SOHO/個人サイトの移行
- アプリケーション
- セキュリティ
- 管理・監視系
- UNI
- 今後に向けて

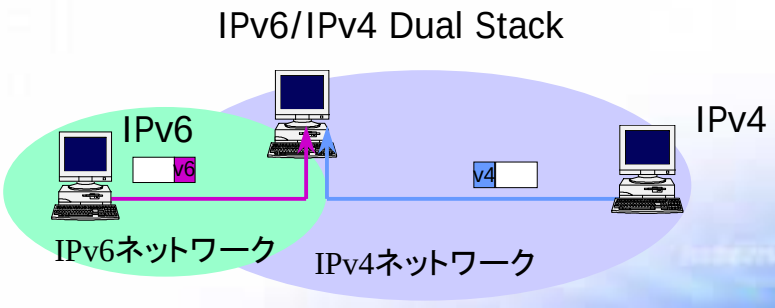
NEC

移行技術の分類：基礎

NEC

デュアルスタック

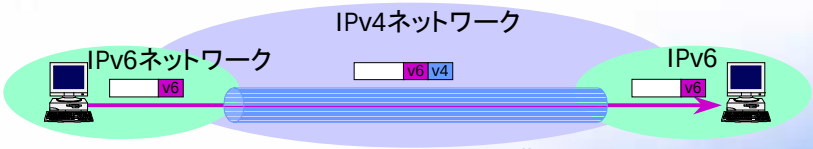
- デュアルスタック
  - サーバ等はIPv6とIPv4の両方と通信
  - IPv6への移行初期～IPv4端末が消滅するまで
  - ルータ等もデュアルスタックでパケットをフォワード



NEC

トンネリング

- トンネリング
  - IPv6のサイト（もしくはIPv4のサイト）同士がIPv4（もしくはIPv6）のネットワークを越えて通信
  - 移行初期には、IPv6 over IPv4にて手軽にIPv6網を拡大
  - 移行後期には、IPv4 over IPv6にて点在する残存IPv4網を接続



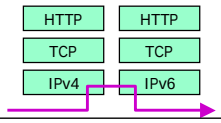
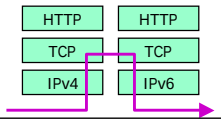
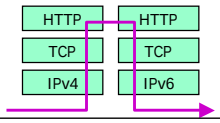
IPv6 over IPv4 Tunneling

IPv6/IPv4変換

- IPv6/IPv4変換
  - IPv6端末とIPv4端末同士が直接通信
  - IPv6 onlyの端末が出現し、IPv4 onlyの端末と通信する必要がある時点で用いられる
  - 複数の実現方法：
    - NAT
    - TCP Relay
    - Proxy

IPv6-IPv4 Translation

参考：IPv6/IPv4変換方式の比較

	ヘッダ変換（NAT）	TCPリレー	代理(Proxy)サーバ
階層図（例）			
処理	• IPレイヤでv4/v6のヘッダを付け替える	• TCPコネクションをトランスレータでリレーする	• APLレイヤでコネクションを終端し、トランスレータは代理(Proxy)サーバとなる
速度	速い ◀――――――――――――――――――――――――――――▶ 遅い		
長所	• IPレイヤに閉じており、ハードウェア化も可能で速い • クライアントに変更の必要なし	• DNSに変更不要 • APLのサービスを選ばない	• DNSに変更不要 • FTPも通る • APLに変更不要（SOCKS） • IPsecを実現しやすい（SOCKS） • 負荷分散しやすい
短所	• DNSに対して変更が必要 • APLでIPアドレスを意識するプロトコル（FTP等）は通らない • ICMPの変換が必要（ICMPv4をICMPv6に変換できない） • 負荷分散が困難（ボトルネックになりやすい）	• TCPしか使用できない • ハードウェア化は難しい • 負荷分散が困難（ボトルネックになりやすい）	• クライアントに変更が必要 -SOCKSクライアントを実装(SOCKS) -APLを変更(squid)

移行のフェーズ

フェーズ分け

- 初期（Phase-1）:
  - 新技術に積極的なISPがIPv6対応を進める
  - ごく一部の先進ユーザがIPv6を使い始める
  - ほとんどの企業ユーザは様子見
- 中期（Phase-2）:
  - ISPのほとんどはIPv6への対応を完了
  - 先進ユーザからIPv6利用が進む
  - 一部の企業ユーザが対外接続にIPv6採用を進める
- 後期（Phase-3）:
  - ほとんどのユーザに何らかの形でIPv6が浸透
  - 使うアプリによってIPv4は残るが一般にはIPv6を利用

NEC

ISPの移行

NEC

ISPにおける基本的事項

- ユーザニーズ
  - 欲しいと言われる前に準備しなければならない
    - IPv6による市場の獲得
  - 新たなアプリケーションの出現？
    - キラーアプリと言われて久しいが、出てきたら対応しないと・・・・
- 今のサービスを止めてはいけない
  - 新サービスへの投資という側面
  - かつ、既存のインフラを最大限利用したい
- 運用ツール・ポリシー
  - IPv4で作ったツールをそのまま使いたい
  - 常時接続によるユーザのセキュリティに関するクレーム
  - 安定性・運用性を高いレベルでサービス保証

NEC

IPv6網構築へのシナリオ

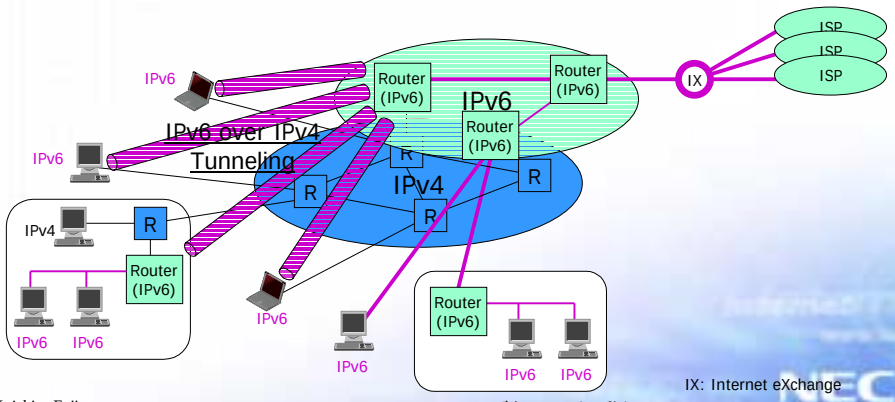
- 既存のIPv4網とどういう関係でIPv6網を構築するか？
  - Phase-1:
    - 新たにIPv6専用ネットワークを構築
    - ユーザへの提供部分のデュアル化
    - 対外接続のデュアル化
  - Phase-2:
    - IPv6とIPv4網のマイグレーション
    - ほとんどの部分でのデュアル化の完了
    - バックボーンもIPv6とIPv4を統合
  - Phase-3:
    - 不要な部分からIPv4サービスの巻き取り

NEC

IPv4→IPv6移行シナリオ(1)

トンネル vs. ネイティブ

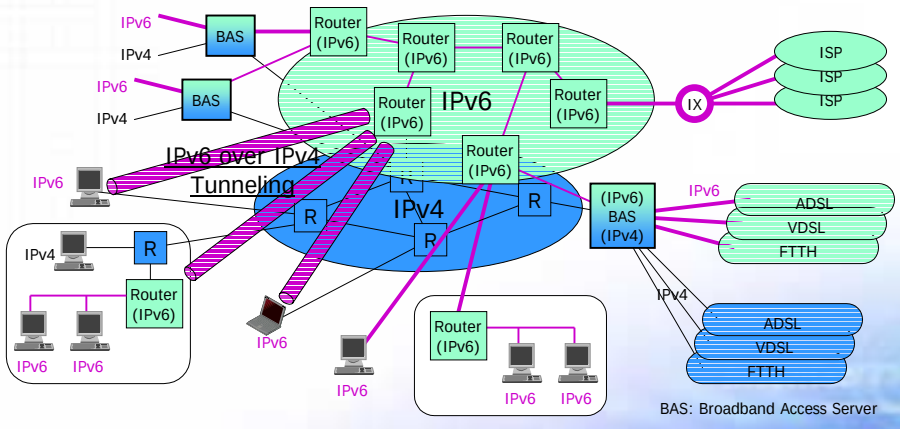
- IPv6 over IPv4 tunneling
  - ユーザネットワークのIPv6ルータとの間でトンネルを設定
- IPv6 native service
  - ユーザネットワークとIPv6で直接接続



IPv4→IPv6移行シナリオ(2)

IPv6-BASの導入

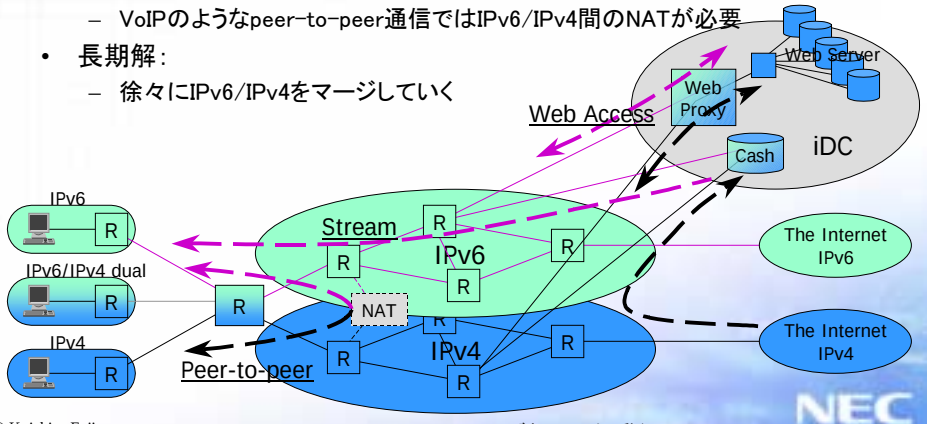
- Broadband AccessのIPv6/IPv4 dual化



IPv4→IPv6移行シナリオ(3)

IPv6とIPv4の共存

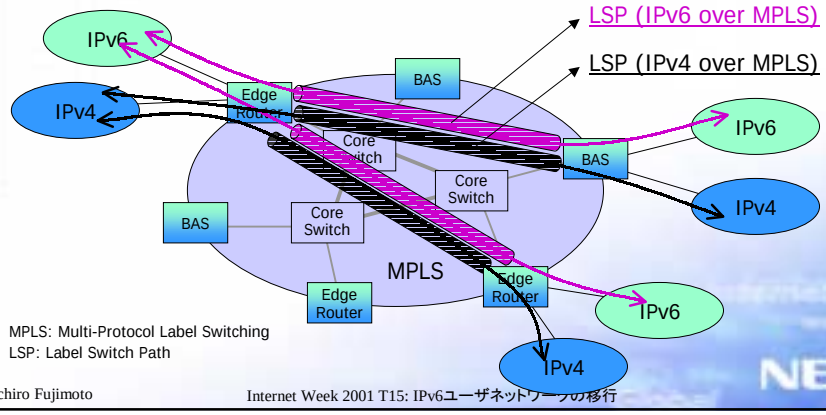
- 共存例:
  - コアネットワークはIPv6/IPv4を論理的に分離
  - エッジルータ/BASはIPv6/IPv4の両方を収容
  - Web AccessはWeb ProxyでIPv6/IPv4 dual化
  - ストリーム配信はキャッシュサーバのIPv6/IPv4 dual化で対処
  - VoIPのようなpeer-to-peer通信ではIPv6/IPv4間のNATが必要
- 長期解:
  - 徐々にIPv6/IPv4をマージしていく



IPv4→IPv6移行シナリオ(4)

MPLSによるBackboneの統合

- IPv4で構築したMPLS網にIPv6を統合
  - Edge(PE)ルータをIPv6/IPv4対応
  - IPv4のシグナリングでLSPを構築し、IPv6用Pathとして利用
  - Edge(PE)ルータ間で任意のRouting Protocol(IPv6)を利用
  - draft-ishii-ipv6-te-tunnel-00.txt



MPLS: Multi-Protocol Label Switching
LSP: Label Switch Path

大規模サイトの移行

NEC

大規模サイト(企業網)における基本的事項

- 今あるネットワークを移行する
  - ISPとは違い、新たに構築するわけにはいかない
  - 追加投資ではなく、既存設備の移行
    - 企業にとってはネットワークはツールであって、飯の種ではないから、追加投資は大変なこと
- 24H365日、業務を止めてはいけない
  - 既存のネットワーク構成、アプリケーションに依存
- 運用ポリシーの遵守
  - IPv4で作った運用ポリシーを引き継ぐ
  - セキュリティに関するポリシーも変えられない

NEC

運用ポリシーによる違い（典型的な例の場合）

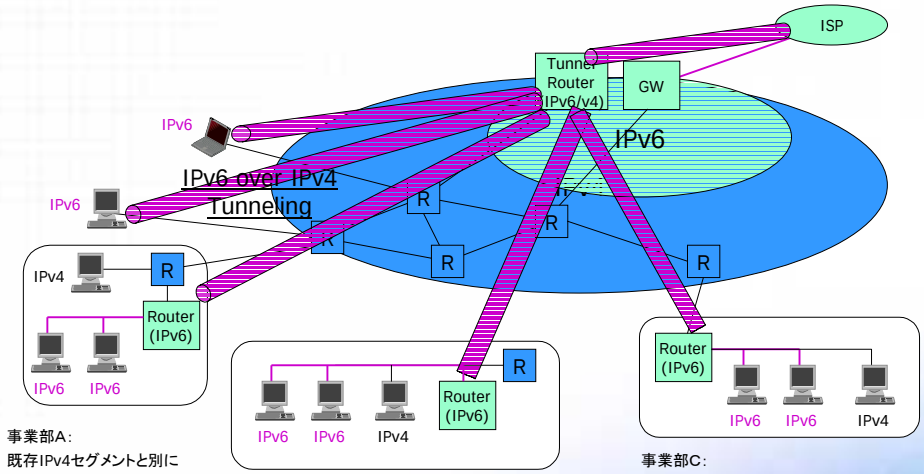
- ポリシー有り型
  - システム管理部門が各部門のネットワークを管理
  - システム管理部門のポリシーに従い、IPv6化
  - 予算が有るときに一気に導入 :-)
    - ただし、末端までIPv6対応の端末が普及している状態で
- ノンポリ型
  - 各部門が自立的にネットワークを管理
  - システム管理部門は外部への接続のみ請け負う
  - 各部門のIPv6ニーズが高まるにつれIPv6化
  - 予算は各部門持ちで徐々にIPv6化

運用ポリシーによる違い（典型的な例の場合）

ポリシー有り型	ノンポリ型
① トンネル →スター型 →トンネルトップはシステム管理部門（ここまでが長い^^;;;;） ② 基幹網のDual化 →主に予算的要因（買う or リース更新時にIPv6対応機器があれば・・・・） →一気にSIerが構築 ③ Gloal: 全てのネットワーク要素のDual化	① トンネル →横のつながりを求めて →外へは勝手に出る!? ② 基幹網のDual化 →システム管理部門が構築（ここまでが長い^^;;;;） →末端のRouter、L2/L3 SWは徐々に →長期的発展（ゆるやか） ③ Goal：全てのネットワーク要素のDual化

© Koichiro Fujimoto
Internet Week 2001 T15: IPv6ユーザネットワークの移行

各組織の移行形態例：ポリシー有り型

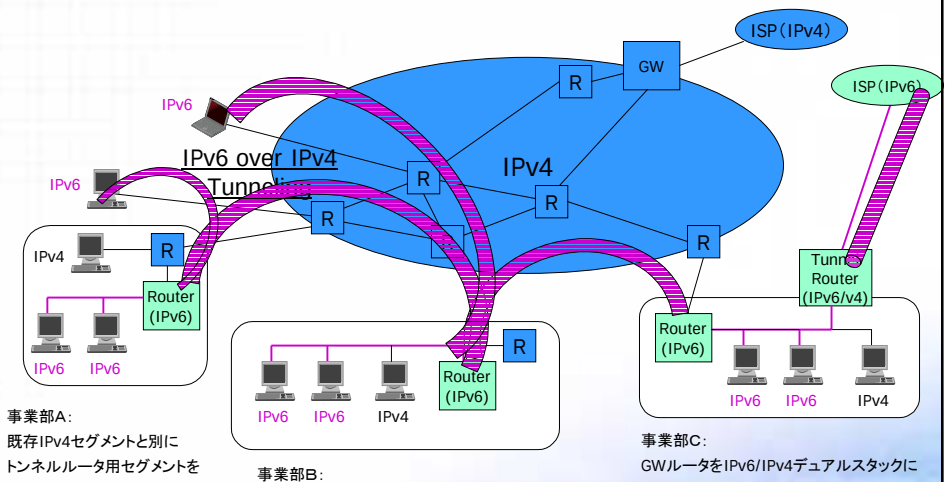


事業部A：
既存IPv4セグメントと別に
トンネルルータ用セグメントを
用意し、その配下にIPv6端末
を接続

事業部B：
既存IPv4セグメント上にトンネルルータを
接続し、事業部内LANをIPv6/IPv4 dual化

事業部C：
GWルータをIPv6/IPv4デュアルスタックに
置き換え、トンネルを終端し、事業部内
LANをIPv6/IPv4 dual化

各組織の移行形態例：ノンポリ型



事業部A：
既存IPv4セグメントと別に
トンネルルータ用セグメントを
用意し、その配下にIPv6端末
を接続

事業部B：
既存IPv4セグメント上にトンネルルータを
接続し、事業部内LANをIPv6/IPv4 dual化

事業部C：
GWルータをIPv6/IPv4デュアルスタックに
置き換え、トンネルを終端し、事業部内
LANをIPv6/IPv4 dual化

アドレッシング（1）

- 企業網の場合、基本的には/48を貰ってくる
  - これだけで約65,000サイトを構築できる
  - 各部門には/64を渡す
  - 大規模の場合：
    - 地理的なアグリゲート
    - 組織毎のアグリゲート

アドレッシング（2）

- /48の割り当て例
  - 前提：
    - 日本全国規模の企業
    - 全国に50組織
  - 各割当数：
    - /49　pool（先々のために予約）
    - 各組織に/56ずつ割り当て
      - 128個（7bit）の/56を各々の組織で分割利用
      - バックボーンにも一つの/56を割り当てて分割利用
    - 各組織が256個（8bit）の/64を利用可能

小規模サイトの移行

NEC

小規模網での基本的事項

- ISPサービスに左右される:-)
  - Tunnelサービス
  - IPv6 native+IPv4 native
  - IPv6/IPv4 dual
- お金はかけられない
  - 既存設備からのマイグレーション
- 運用ポリシー
  - IPv6導入の要求度合いによって運用ポリシーが変わる・・・・かもしれない:-)

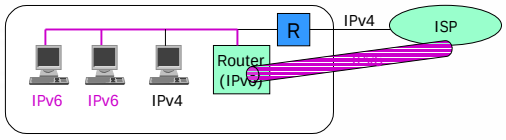
NEC

小規模網：ISP接続の移行例

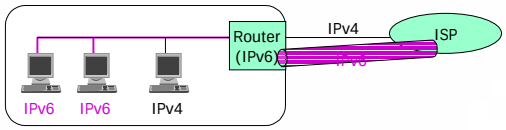
- Step 1:
  - 現在買っているISPのトンネルサービスを利用
  - 同一セグメントにトンネルルータを接続
- Step 2:
  - SOHO Routerのファームバージョンアップ or 買い換え
  - やっぱりトンネル
  - （Step 1 を飛ばしてここに来るサイトもあるだろう）
- Step 2’:
  - IPv6 NativeをEtherで提供を受ける場合
  - 既存IPv4ルータとIPv6ルータをパラレルに接続
  - （稀なケースかもしれない）
- Step 3 (Goal) :
  - IPv6/IPv4デュアルスタックルータで、IPv6/IPv4デュアルのNativeサービスを受ける

小規模網：ISP接続の移行例

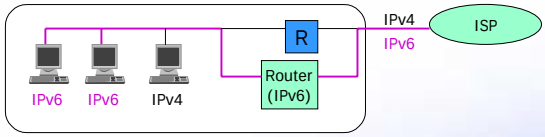
- Step 1:



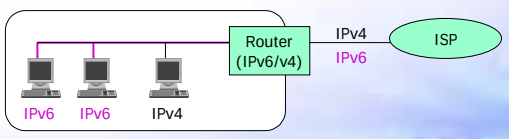
- Step 2:



- Step 2’:



- Step 3:



© Koichiro Fujimoto
Internet Week 2001 T15: IPv6ユーザネットワークの移行

アドレッシング

- 一つのLANしか存在しない場合：
  - /64で十分
    - /48を貰っても使い道がない :-)
    - ISPに/64を切りだして貰う
  - やっぱり/48
    - 将来の事業の伸びのために取る
    - ISPにとっては追加で/64をあげるよりも最初から/48を割り当て
- 複数のLANが存在する場合：
  - /48が基本
    - /48と/64の間で切り刻んで割り当てはしない
    - 複数になった時点で/48を割り当て
- （ISPの心境として現実的には）
  - /48だけの管理を考えたいという声も強い

SOHO/個人サイトの移行

SOHO/個人サイトでの基本的事項

- ユーザニーズ
  - IPv6を知らないで使う時代が来る
  - キラーアプリケーション
    - ポイント：常時接続、P2P、VoIP
  - コスト意識
    - キラーアプリ次第? :-)
- サービスの選択
  - 良いサービスへ乗り換え
  - キラーアプリによってはISPサービスを選択
    - 今のサービスで満足していれば、誰もIPv6には乗り換えない
- 運用ポリシー
  - 基本的に利用者のニーズそのまま
- セキュリティ
  - IPv4時代にはNAPTしていたユーザを守るためにISP側が考えないといけない

接続形態による違い

- ダイヤルアップ
  - IPv6になっても残るのは確実
    - IPv6ではIPアドレスはユーザ固定も一般的に?
  - 基本的にはIPv4でやっていたことがやれれば良い
- DSL、FTTH、等の常時接続型
  - IPアドレスがユーザ固定型の普及
  - 専用線的な利用においても設置時に自動設定をしたい
  - PPPを使う場合：
    - ダイヤルアップ同様にPPPで自動設定
  - PPPを使わない場合：
    - RAでアドレスを付与
- 課題：
  - IPアドレスの受け渡し、DNSサーバの通知などIPv4がPPP+DHCPに頼っていた部分が未解決
  - →後の「UNI」で詳しく

アプリケーション

NEC

利用アプリケーションの分類

- 企業独自系
  - DB系アプリ, EDI, ERP, CAD/CAM/CAE, スパコン :-)
- 一般
  - http, mail(smtp, pop3, IMAP4), ftp, telnet, ssh, smb, lpr, DNS, L2TP, NFS, ストリーム用アプリ, IRC, チャットツール, DB系アプリ, LDAP, etc.
- 管理系
  - Radius, TACACS, SNMP, NTP
- その他
  - Over IP系(DecNET, X.25, Netware, DLSW, etc.), CG, POS, 全銀NW, 証券, etc.

NEC

アプリケーションの移行

- 業務系:
  - 企業独自系等は5年, 10年というスパンで考える必要有り
    - 作り替えるという作業が必要
  - 業務系アプリでも置き換えには数年という単位
    - 使っているデータベース等との兼ね合いが大
- 一般的アプリケーション:
  - OSのIPv6対応と共にIPv6化が進行
  - 利用アプリによりIPv4を残さなければいけない端末の存在
  - IPv6とのDual化を進める事となる

→企業においてはIPv6 onlyは5～10年のスパンでは無理

NEC

セキュリティ

NEC

IPv6時代のセキュリティ

- ポイント
  - IPv6化により、常時接続や固定アドレスなどのメリットを享受できるようになる反面、下記のようなポイントを知っておくことが重要
    - NAT/Proxyが無くなる事による内部ネットワークへの直接攻撃の可能性（外部から内部への攻撃機会の増大）
    - グローバルIPアドレスの固定化による、特定アドレスへの継続的な攻撃可能性
    - グローバルIPアドレスでの常時接続による攻撃機会（時間的）の劇的な増大
    - NAPTなどが持っていたダイナミックフィルタ的効果の喪失

IPv6のIPSec

- IPv6の仕様
  - IPv6ではIPSecの実装が必須
- 現実
  - 必ずしも実装されていない
  - 実装されていても使うかどうかは利用者任せ
  - 情報家電に代表される組み込み機器では実装されない可能性も高い
- 相互接続性
  - IPv4で問題となる相互接続性は、IPv6では実装が進んでいない事もあり、IPv4よりは期待できる ;-)
  - 固定かつGlobal Addressが前提であるため、実装は進む可能性はある

End to Endのセキュリティと企業網

- 前提
  - IPv6では広大なアドレス空間によりEnd to Endのアプリケーション利用が期待されている
- End to End通信の必要性
  - 現在のWeb, Mailといったアプリケーションでは必要ない
  - 新しいアプリケーションの芽を育てる
    - VoIP, P2P, etc.
- セキュリティに対する考え方
  - 企業などの管理者にとって、外部からの直接到達性を認めるのは簡単ではない
  - End端末においてセキュリティの強化、機能面の見直しが必要
  - 業務での必要性によって「どのアプリケーションでEnd to Endの利用を認めるか？」の判断をしていく

ファイアウォール

- 目的
  - 外部からの直接通信を防ぐ
    - IPv6のグローバルな到達性と相反する要件
  - 通信される内容の制限、内容の監視
- IPSecとの関係
  - IPv6のIPSecで同等の目的を達成できるか？
    - 答え：No
  - 企業ではこれに全面的に移行はあり得ない
    - 通信内容をチェックしたいという企業ネットワーク管理者のニーズは高まる一方
- 必要なこと
  - Packet filteringなどが必要
    - 課題：現状では製品がほとんど無い

→やはり企業ではファイアウォールのようなモデルは残る

グローバルアドレスが産む問題

- 端末の特定
  - 特定のIPアドレスからのアクセスをトラッキング可能
    - 個人のプライバシー問題
    - EUI-64アドレスなら、端末ベンダーの特定
    - 利用アプリと端末の対応の特定
    - トラフィック解析による企業の活動内容の特定
  - →社内情報の遺漏につながる

→（IPv6業界では評判が悪いが）ProxyやNATを使うケースが残っていく

アプリケーションのセキュリティ

- 本質的にはIPv6とIPv4は何ら変わらない
- マイナス面：
  - 常時接続型のアプリケーションなど、IPv6よりも厳しい要求条件を突きつけられる
    - 冷蔵庫のクラック :-)
- プラス面：
  - これから作るアプリケーションは、IPv4での経験を活かして、新たな仕組みを盛り込んだり、IPv4での失敗を避けるためにプロトコルとしてセキュリティを考慮した作りにしていくことが必要
    - Eg. DHCPv6に認証を入れる, etc.

管理・監視系

NEC

管理・監視に求められること

- Traffic
  - SNMP（MIBサポート）
- Reachability
  - HW（ノード）
  - 回線
- 負荷
  - サーバ
  - ルータ
- 侵入検知（IDS）
- アプリケーションのAvailabilityとPerformance
  - 瞬間的値
  - 統計情報
- 対象のアプリケーション
  - DNS, Mail, Web, etc.
- 情報の可視化
  - Graph Tool 等

NEC

現在の対応状況と考察

- 既に製品として出始めたもの
  - Traffic監視ツール
  - ルータのMIBサポート
  - Ping6等のツール
  - Graph Tool 等
- 既存のものが使えるもの
  - 負荷（サーバ、ルータ）
  - アプリケーションのAvailabilityとPerformance（瞬間的値、統計情報）
  - 対象のアプリケーション（DNS, Mail, Web, etc.）
- 対応が未だのもの
  - IPv6 SNMP Trap：IPv4が存在する場所では特に問題ではない？
  - 侵入検知（IDS）：IPv6のセキュリティモデル問題

→ 企業網として必要とされるツール類はほぼ揃い始めている状況

NEC

UNI

NEC

PPPのIPv6化に関する問題点

- アドレスが渡せない
  - リンクの確立は出来るが、アドレスを渡す部分は未定義
- 接続する端末別の考察:
  - ホストの場合:
    - /128を渡すイメージでIPv4と同じ意味合いでアドレスを付与する仕組みは実装可能(現在非標準)
  - ルータの場合
    - ルータ配下に割り当てるアドレス(eg. /64)を通知する仕組みは未定義
- 接続形態別の考察:
  - アドレスが固定割り当ての場合
    - 現状、手で設定(つまり事前にオフラインで通知)すれば通信可能
  - アドレスが非固定割り当ての場合
    - 現状、アドレスを付与できない

アドレス割り当てに関する現在の議論

- PPPを使う場合:
  - Case1:
    - IPv4と同様に全てPPPの枠内(IPv6CP)でアドレスを渡す
    - → ユーザルータ配下のアドレスを渡す仕組みは検討が必要
  - Case2:
    - PPPでリンク確立後、Automatic Prefix Delegationによりアドレスを付与
      - Automatic Prefix Delegation: draft-haberman-ipngwg-auto-prefix-01.txt
  - Case3:
    - PPPでリンク確立後、RA+multi-link subnetによりアドレスを付与
      - Multi-link subnet: draft-thaler-ipngwg-multilink-subnets-01.txt
- PPPを使わない場合:
  - Case1:
    - DHCPv6で全ての端末に直接アドレスを付与
    - → ユーザ側にルータが居る場合はNG
  - Case2:
    - RAで全ての端末に直接アドレスを付与
    - ユーザ側にルータが居る場合はRA+multi-link subnetで付与も可能

DNS Serverの通知方法

- IPv4では:
  - PPPでユーザ端末(ルータ)にDNSを通知
  - ルータの場合DNS Proxyとして動作し、NAPTした配下の端末へDHCPを用いて自身のLAN側アドレスをDNSアドレスとして通知
- IPv6では:
  - Case1:
    - クライアントはSite-local anycastによってDNSが答えてくれるのを待つ
  - Case2:
    - RAと同様にService Advertisementを行う

    → 全く議論が不十分だし、ドキュメントも実装もない
  - Case3:
    - RAを拡張してDNSも通知

    → 一度IETFで却下されているが、簡便な接続には有効
  - その他:
    - RAでDNSのアドレスも通知:IETFでは却下
    - DHCPv6でDNSを通知:DNSだけのためにDHCPv6はやはり荷が重い

→ IETFでの議論を待たねばならない状況

NEC

今後の課題

NEC

現状の課題整理

- ネットワーク
  - コアの技術はほぼ完了
  - IPv4と同等以上に安定したネットワークの運用
- アプリケーション
  - 業務アプリケーション等のIPv6対応
- セキュリティ
  - IPv6におけるセキュリティモデルの確立
  - IPSecの実装
  - 企業向けのファイヤウォールの実装
  - NAPT等で守られてきたユーザのセキュリティ
  - IDSなどのツールの拡充
- UNI
  - ユーザへのアドレス自動割り当て方法
  - DNSサーバアドレスの通知方法
- Etc.

まとめ

- IPv6への移行は既に始まっている
  - 足りない技術はあるが、IPv4でも試行錯誤してきたことを忘れずに構築する努力は必要
  - ただし、気長にやる必要はあり
- IPv6はIPv4の置き換え
  - 基本的にはIPv4の枠を大きく飛び越えるものではない
  - 構築に関して大きな差異はなく、実装を頑張っていく側面が強い

  → 力業の側面も・・・・

- みんなでがんばりましょう

ご静聴ありがとうございました

T15: IPv6 ユーザネットワークの移行

Contact: koichiro@ipv6.nec.co.jp
（お気軽に・・・・）

NEC