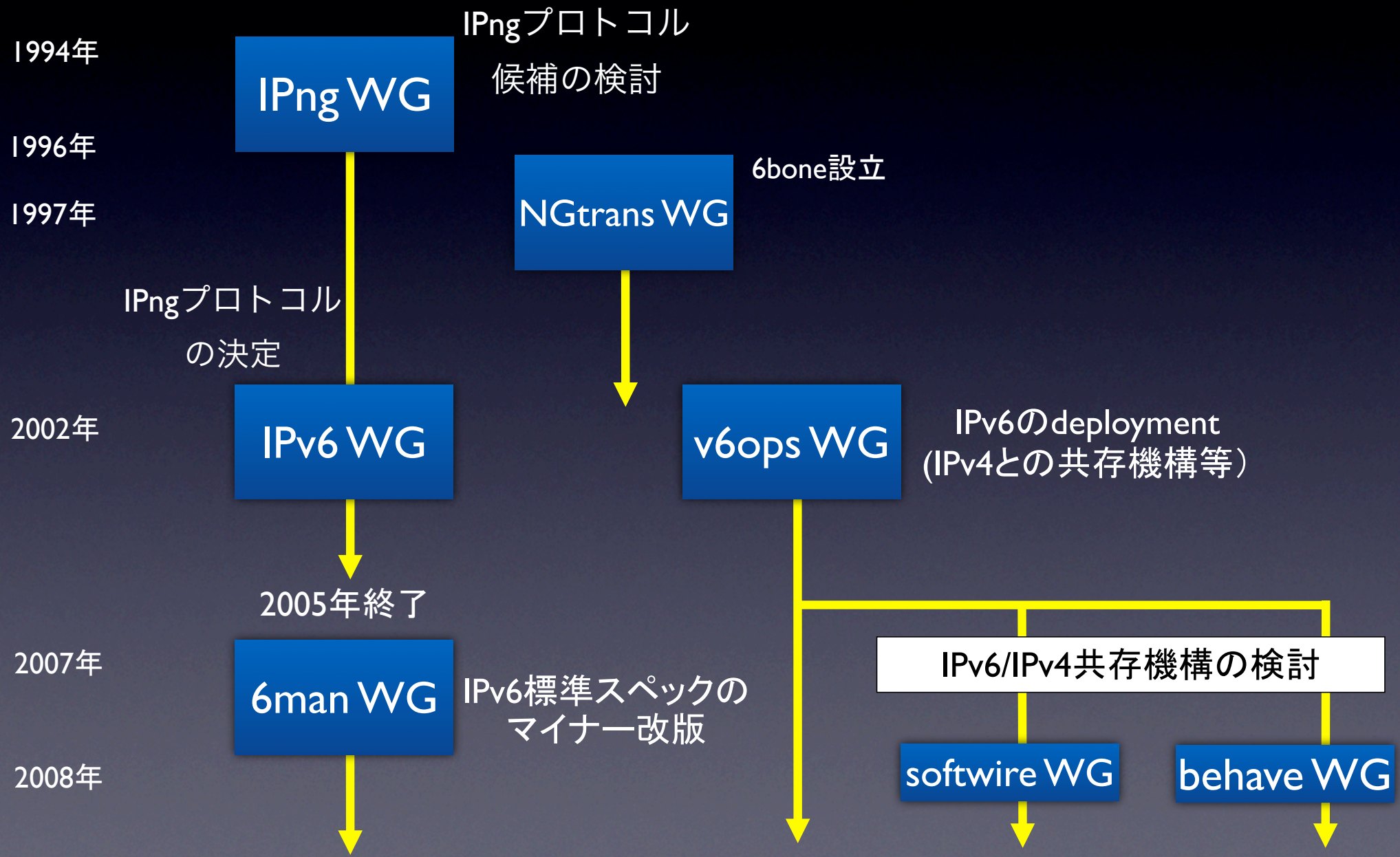
IPv6”再”入門
標準化最新動向

松本 存史
NTT 情報流通プラットフォーム研究所

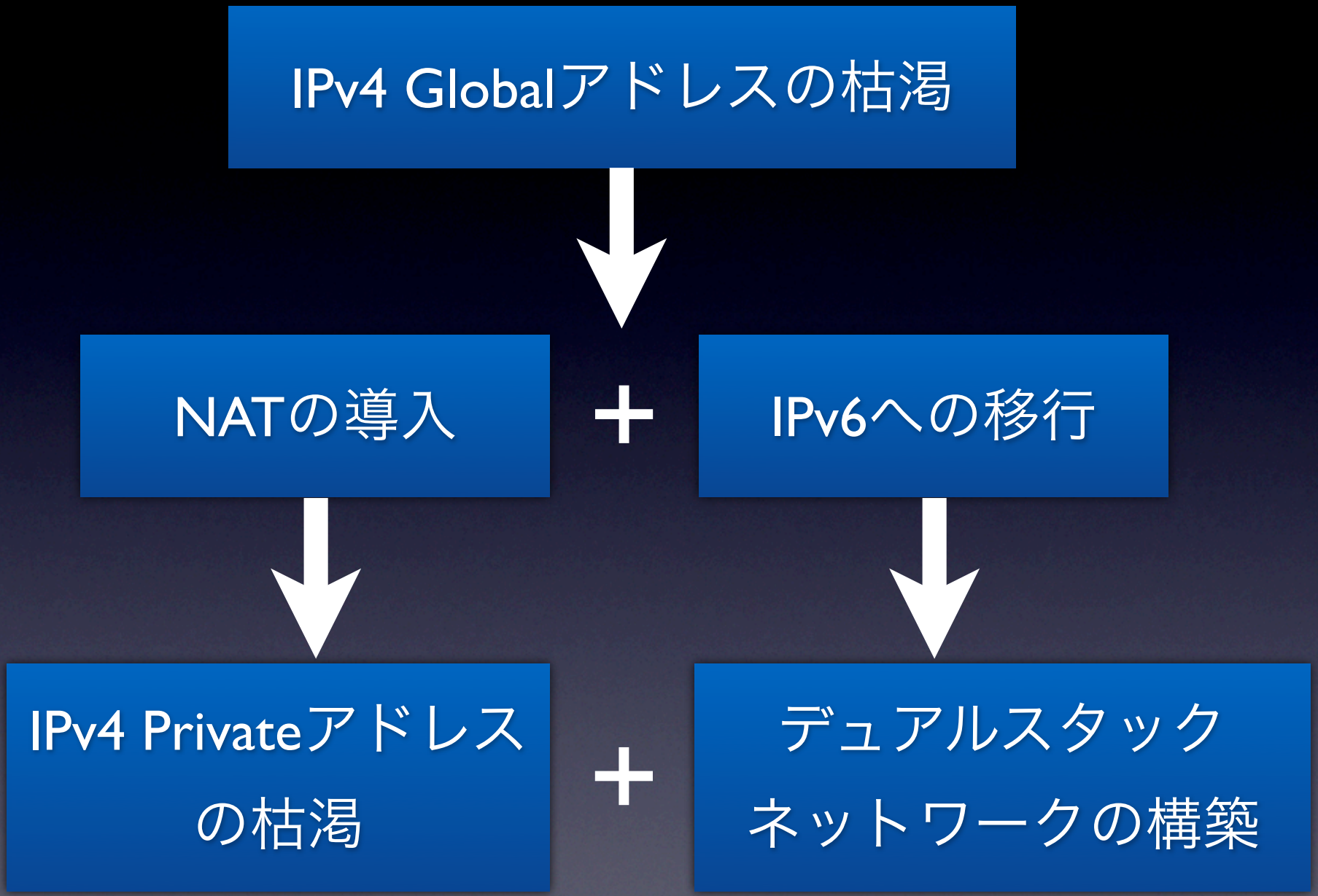
INDEX

- デュアルスタックネットワーク構成方式
  - CGN, A+P
  - DS-Lite, 6rd
- IPv4-IPv6トランスレーション方式
- IPv6-NAT
- アドレス選択技術
- IPv6のCPEセキュリティモデル

IPv6の標準化組織の変遷

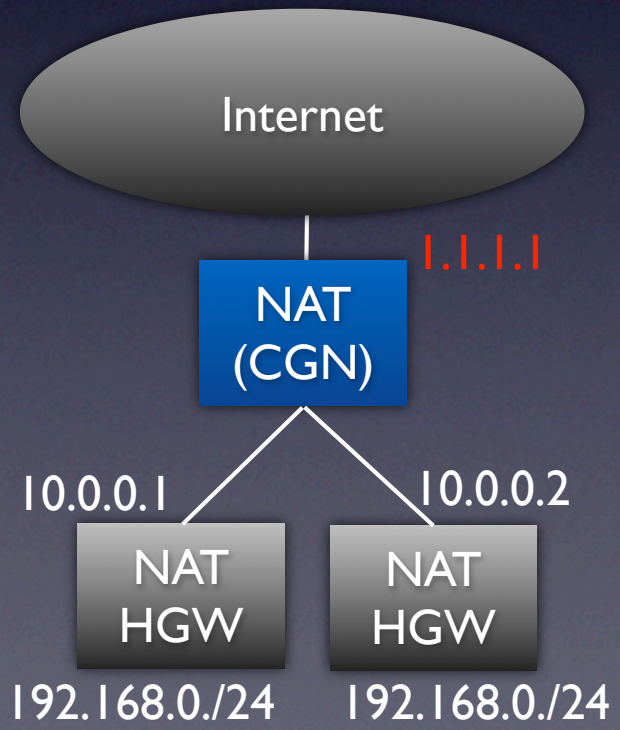


新たなデュアルスタック
ネットワーク構成方式

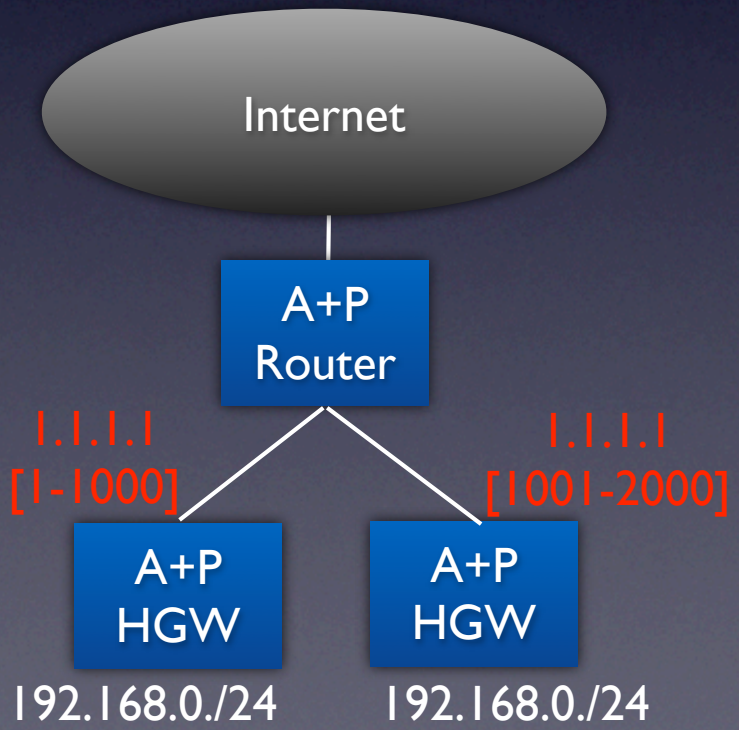

IPv4 Globalアドレスの枯渇
NATの導入
+
IPv6への移行
IPv4 Privateアドレスの枯渇
+
デュアルスタックネットワークの構築

IPv4 Globalアドレス枯渇対策

- Carrier Grade NAT
  - ユーザにPrivate
  - ISP網内でNAT



- A+P (Address+Port)
  - ポート範囲を制限したGlobal付与

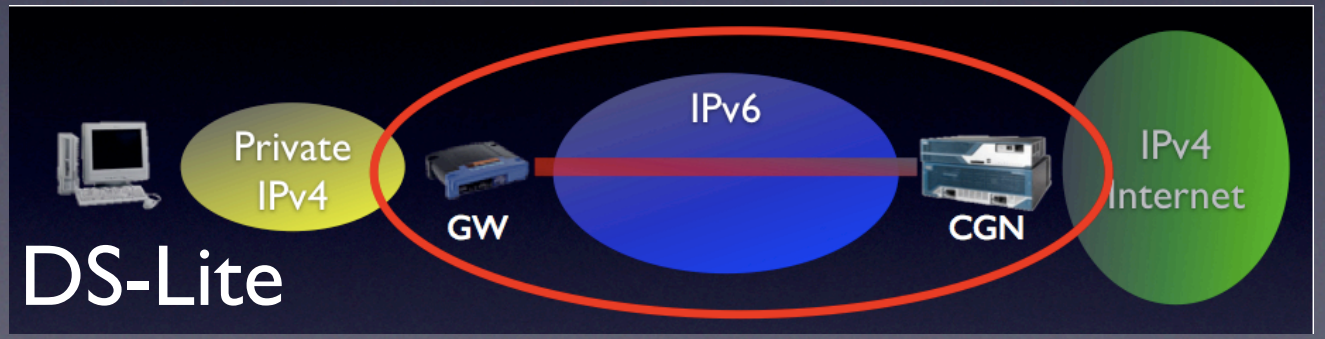


IPv4 Privateアドレス枯渇対策

- IPv4 Privateアドレス空間のおかわり
  - 新たな/8〜空間を定義しようという提案
    - draft-shirasaki-isp-shared-addr
  - 240/4の未使用空間をPrivateにする提案
- IPv6アドレスと紐付けてIPv4アドレスを管理
  - Dual Stack-Lite (次頁)
    - draft-ietf-softwire-dual-stack-lite

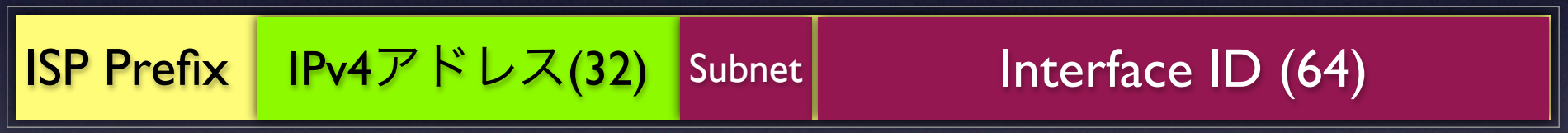
Dual-Stack Lite (DS-Lite)

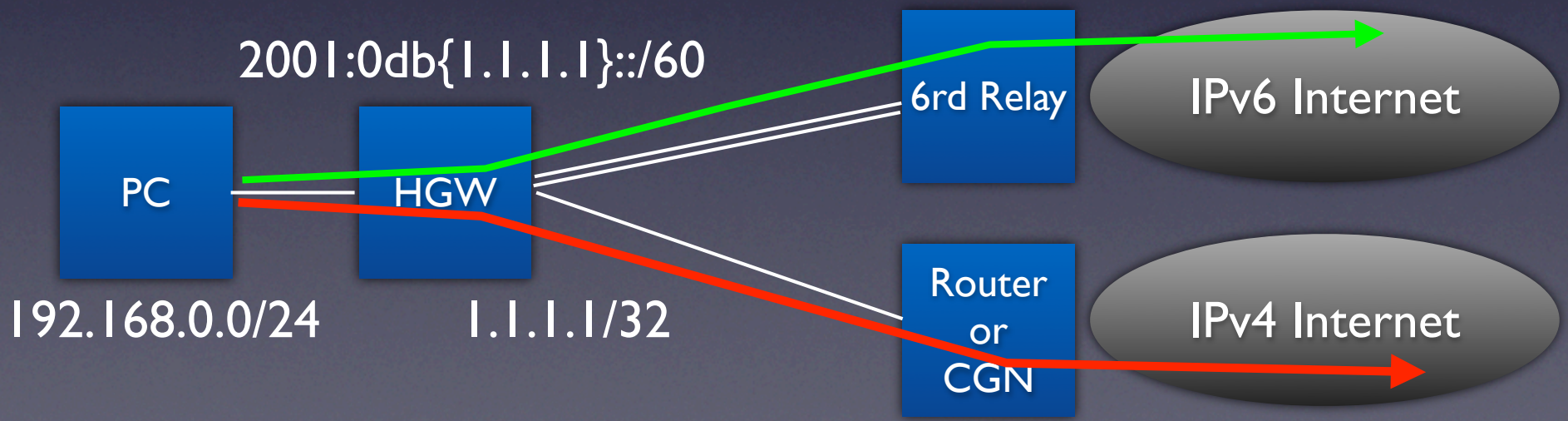
- IPv6アクセス網はIPv6-only、IPv4はトンネリング
  - HGWではNATせず、ISP側のみでNATを行う
  - IPv4はIPv6とのペアで管理。追加のPrivate不要
- HGW-CGN間のIPv4プライベートアドレスが不要
- アクセス網が単一プロトコルになり運用コスト減



IPv6 Rapid Deployment (6rd)

- draft-ietf-softwire-ipv6-6rd
- 既存のIPv4アクセス網上にトンネルでIPv6提供
  - ユーザに付与したIPv4を基にIPv6アドレスを自動設定





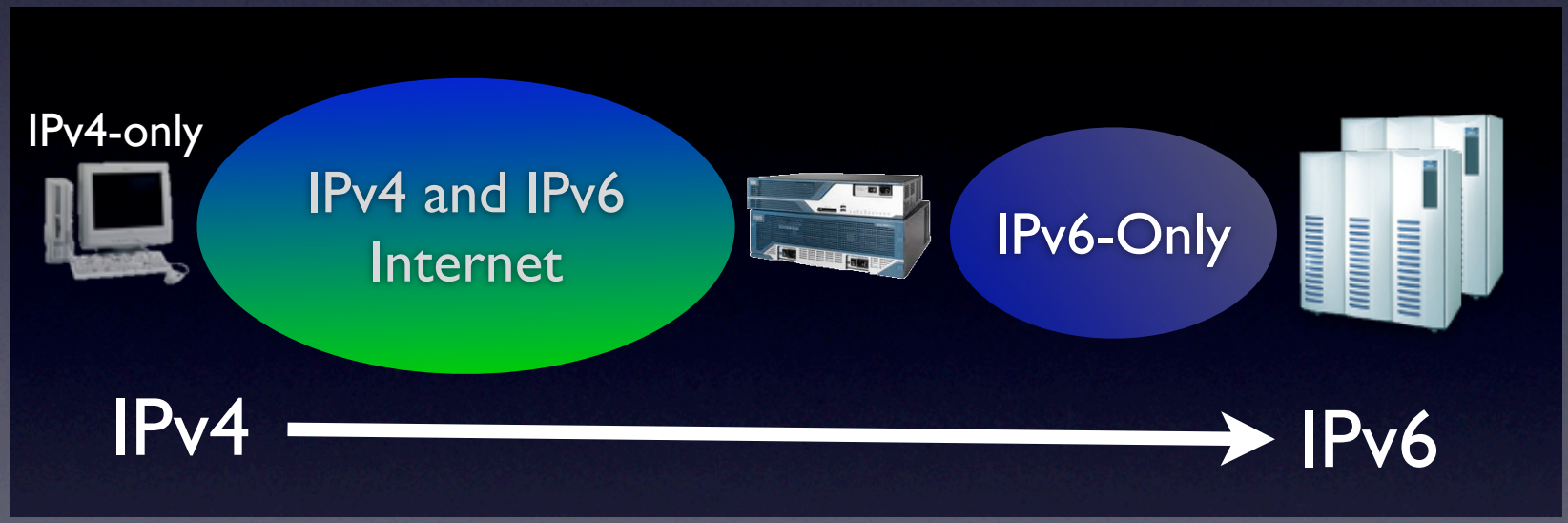
デュアルスタックネットワーク構成方法
今後の展望

- IPv4 Privateアドレスの拡張
  - 幾つかの案が並立しており、標準化の見通し立たず
- DS-Lite提案
  - 欧州を中心に採用を検討するISPがいくつか。OSSの実装も存在
  - 6rdと共に標準化がスムーズに完了する見込み
- 6rd提案
  - 既にFREE Telecom(仏)で採用実績あり、Ciscoなど北米で支持
  - IPv4 Privateアドレス枯渇の対策にはならず
  - 長期的にはネイティブIPv6アクセス網への移行が必要

IPv4-IPv6プロトコル変換方式

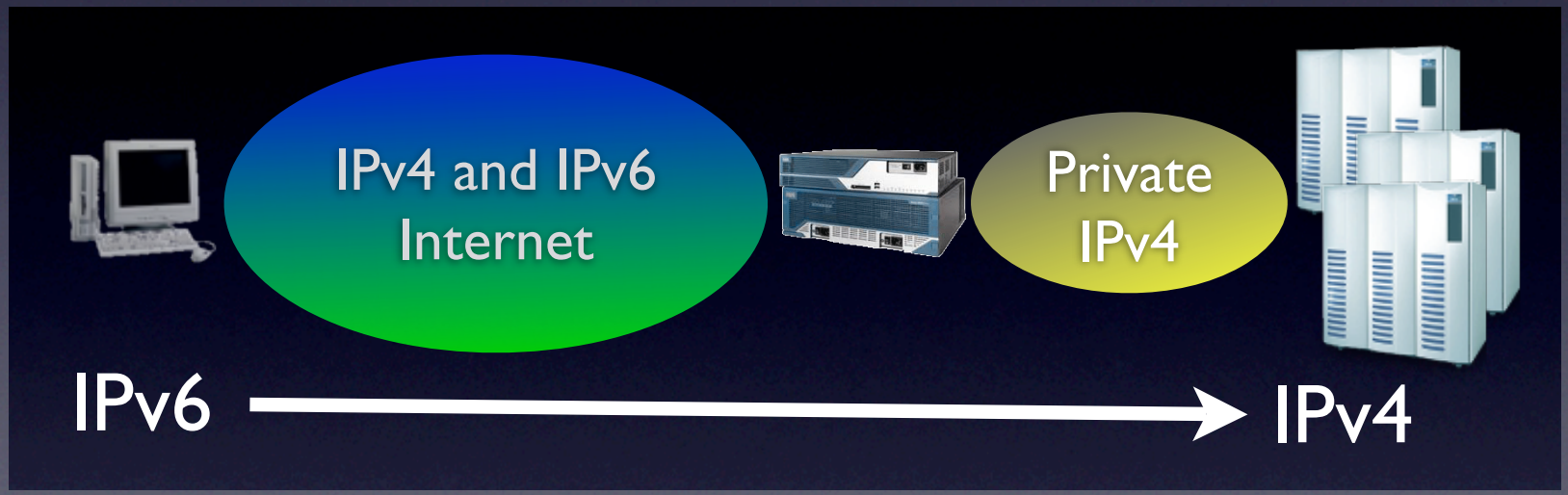
IPv4→IPv6変換は必要か？

- IPv4-only端末からIPv6サーバへの通信には必要
  - 組み込み端末など、IPv4-only端末は残り続ける
  - IPv4アドレス枯渇によりIPv6-onlyサーバが出現



IPv6→IPv4変換は必要か？

- IPv6端末からIPv4-onlyサーバへの通信には必要
  - サーバサイドのIPv6対応化は簡単ではない
  - 一時的なIPv6対応としてのプロトコル変換

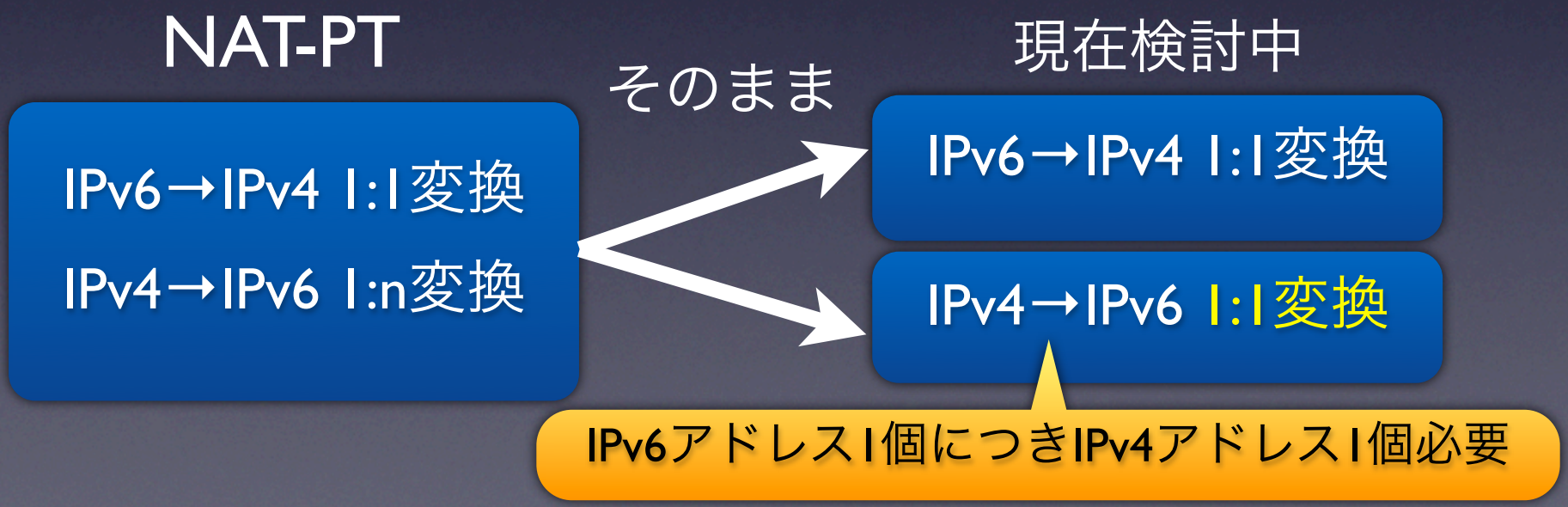


IPv4-IPv6変換方式の歴史

- 過去にRFC2766(NAT-PT)という変換方式が存在した 2000〜
  - DNS-ALGを利用し、IPv6→IPv4,IPv4→IPv6変換をサポート
- しかし、NAT-PTはHistoric(廃止)になった(RFC4966) 2007.夏
  - 理由は沢山ありすぎてどれが本質かは不明
    - ペイロードにIPアドレス情報を含むプロトコルに対応できない
    - IPv6/IPv4変換によるIP関連情報の欠落
    - パケットの断片化機構が煩雑になる
    - SCTPなど新規プロトコル、マルチキャストトラフィックを扱えない
    - DNSーALGを使ううことでネットワークトポロジの制限がでる、DNSSECが利用できなくなる.

しかしそうは言っても

- IPv6も普及してないし、色々なケースでIPv4-IPv6変換は必要、という意見が根強く
- 2008年秋、NAT-PT代替方式を検討する集中会合が開催
- 結果として、NAT-PTの機能限定版の標準化が進行中



IPv4-IPv6変換方式
今後の展望

- 現在の検討方式はNAT-PTの問題点を全て解決したわけではない
  - draft-ietf-behave-v6v4-xlate-stateful など
- しかし、IETFではトランスレーション技術の早期の必要性を認識している
- 標準化は粛々と進行しており、2009年中の仕様FIXを目指している

IPv6 NAT

IPv6 と NAT

- IPv6はEnd-to-End透過的な通信を実現し、NATの無いInternetを目指して設計された
- しかし、現在IETFにてIPv6-NATが検討されている
- 「IPv6でもNATが必要なケースがあり、NATの出現は不可避である」
- 「であるならば、標準仕様を定義して仕様の乱立を避けよう」

IPv6-NATが必要なケース

- 「企業のネットワークオペレータが必要だと言っていた」
- サイト内のトポロジーを隠蔽したい
- サイト内のホスト数を隠蔽したい
- サイト内のリナンバリングを避けたい
  - ISPを変更するとき等
- NATによるマルチホームを実現したい

NAT66

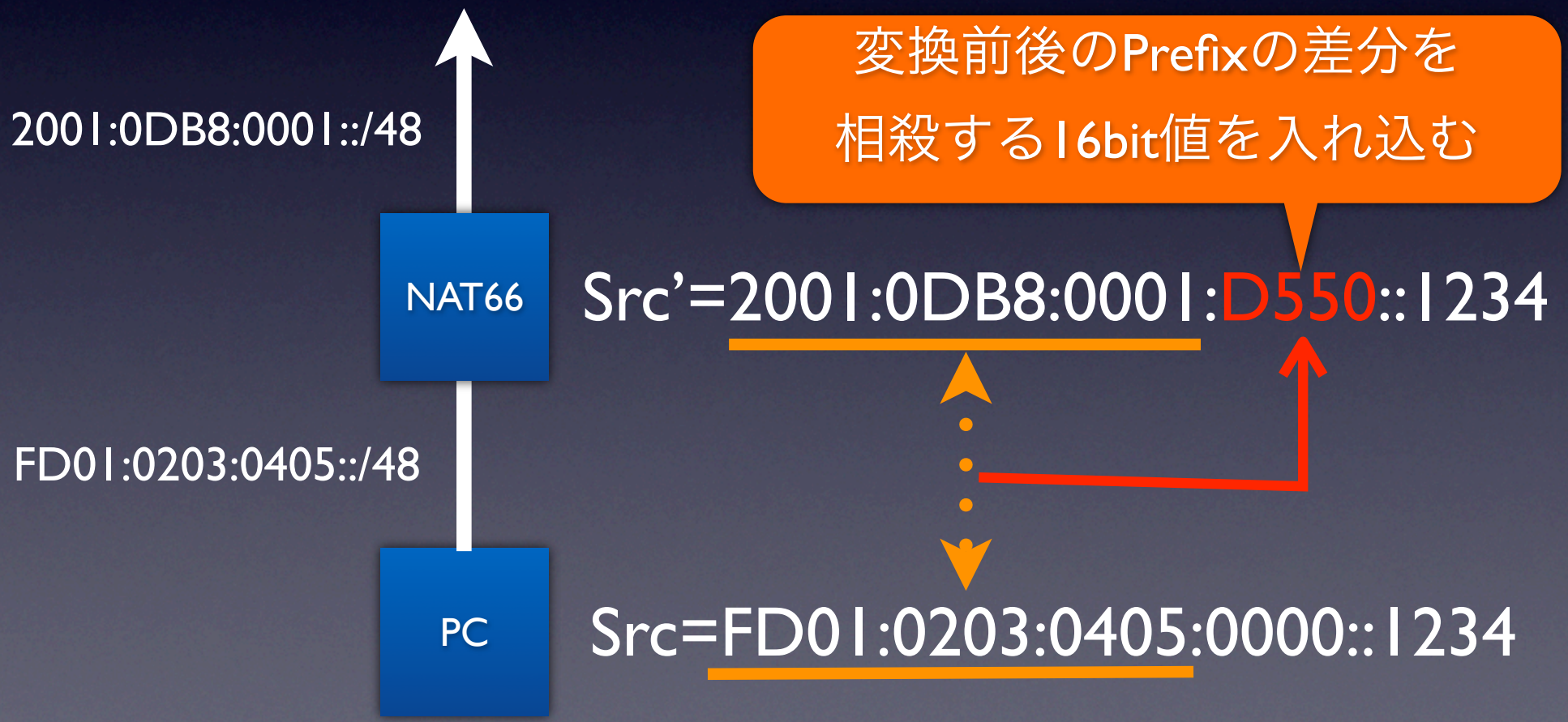
draft-mrw-behave-nat66

- 提案方式
  - ポート番号等、L4ヘッダーには変更を加えない
  - プレフィックスのみ書き換えを行う
  - チェックサム変更の不要なプレフィックスに変換する

NAT66

チェックサム透過なPrefix変換方式

チェックサムアルゴリズムは標準(RFC1071)のもの



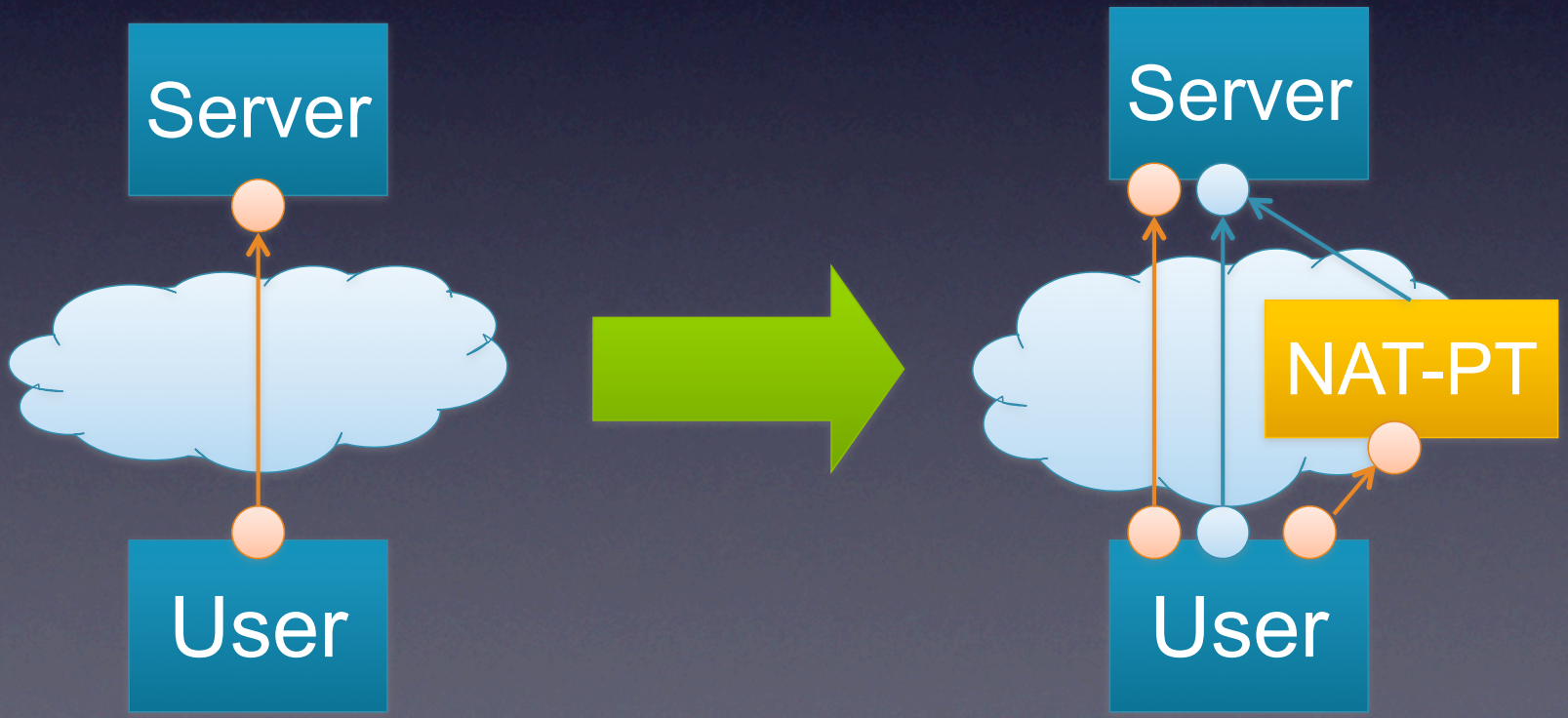
IPv6-NAT
今後の展望

- IETFでは未だスコープが絞り込めていない
  - やはりIPv6にNATを導入することへの抵抗は大きい
  - 目的がNAT以外の既存/新規技術で実現できないか？
  - NAT66がRFCになることで、NAT66の普及を促進してしまうのではないか？
- かたや、既にIPv6-NAT実装が出回り始めているのが現状
- ニーズに合う標準技術が無ければ、現場はアドホックに対処

IPv6アドレス選択技術

IPv6はマルチアドレス環境へ

- IPv6の普及は、ホストのマルチアドレス化を促す
- ユーザが、ネットワークをどの利用するか、に関する制御権限を取得することになる

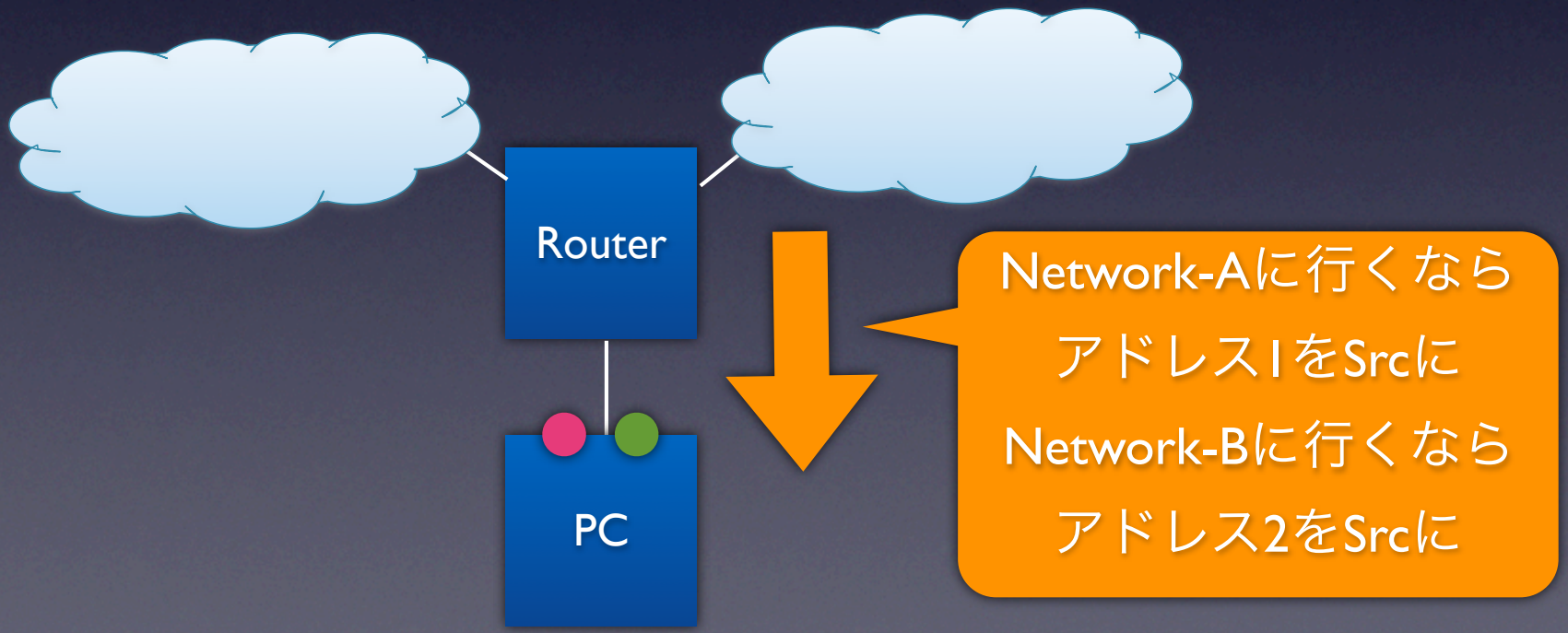


マルチアドレス化の例

- IPv4とIPv6のマルチアドレス
  - サーバ、クライアントともに
- マルチホームサイトのマルチアドレス
  - 各ISPから取得したIPv6 Prefixをサイト内に広告
- 複数種類のIPv6アドレスの利用
  - GlobalとULAの併用など

端末へのポリシー配布

- これまで中継装置で実現していたネットワーク利用ポリシーは、端末に実現させる
- Dst/Srcアドレス選択のポリシーを配布



CPEルータのIPv6セキュリティモデル

なぜ今CPEセキュリティの議論か？

- 加入者宅装置:CPE (Customer Premises Equipment)のIPv6セキュリティ機能について
- IPv6では長らくIPv6のセキュリティモデルについての決着がついていなかった
  - End-to-End透過性を保つには、全てのパケットをホストに転送するファイアウォール無しモデル
  - しかし、今更ファイアウォール無しの世界には戻れられないとするファイアウォール有りモデル

事の発端

- アップル社がIPv6対応AirMac Extremeを発売 2007/1
  - 6to4機能が乗っていて、自動でIPv6が利用可能だった
  - しかし、IPv6のフィルター機能は有効になっていなかった
- しかし、米国の国土安全保障省が当該製品をフィルターが無効であり脆弱であるとして、アドバイザリーを発表 2007/3
- アップル社エンジニアがIETFに対してIPv6のセキュリティモデルについて問い合わせ
- AirMac Extremeのフィルター機能がデフォルトで有効に 2007/4

参照: CVE-2007-1338

しかし、話は終わってはいなかった

- フィルターを有効にすると、P2Pアプリケーションや、FTP、IPsecなどが動作しない
- IETFでは、手動でのフィルター設定を提案
- アップル社エンジニアが堪りかねて、自動的にフィルターを制御するプロトコルNAT-PMPを提案
  - IPv4のUPnPでのGateway制御とほぼ同じ
- IPv6のCPEでのセキュリティモデルの議論へと発展

現在検討中の
セキュリティモデル

- draft-ietf-v6ops-cpe-simple-security-08
  - IKEパケットは通過させる
  - IPsecパケットはstatefulフィルターを使うべき
  - SCTP, DCCPのサポート
  - 自動フィルター制御方式は実装されるべき
    - しかし、具体的な方式はまだ決まっていない

おわりに

- IPv6の標準化に関するホットトピックをご紹介
  - IPv6移行技術
  - IPv6-NAT
  - IPv6アドレス選択技術
  - CPEルータでのセキュリティモデル
- IPv6の標準化は近年益々ホットに
  - 実利用者の声がIETFに届くこと等により、仕様変更/新方式の誕生に結びついている
  - これからIPv6の導入を考えているならば、IETFでの標準化動向も把握しておいて損は無い