



IPv6 Transition and Co-existent with IPv4

Internet Week 2014
November 19th, 2014

Tetsuya Innami
Japan Technology and Research Center
Cisco Systems G.K.

Agenda

1. IPv6とインターネット
2. IPv6の普及とその尺度
3. IPv6導入の指針
4. 構成モデルと移行のステップ
5. 必要な技術と標準化
6. IPv6におけるセキュリティー
7. 移行・共存のためのデザイン

自己紹介 +α

- 1992年「AT&T Jems」入社
 - 当初はUNIX System上でCodingの業務にあたる。その後、まだ一般的でなかった商用UUCPやISPの業務を担当。

1993年頃 JPNIC CIDRパイロットプロジェクト開始
1995年頃 BGP4への移行

PCの低価格化
コンシューマーインターネットサービスの一般化

1998年頃 IPv6の標準化作業がほぼ完了
2000年頃 IPv6対応機器が出荷開始

- 2004年「SoftBank BB」入社
 - コンシューマー向けインターネットサービスやIPv6を担当。
- 2011年「Cisco Systems」入社

ブロードバンドインターネットの爆発的普及とIPv4アドレス消費の加速

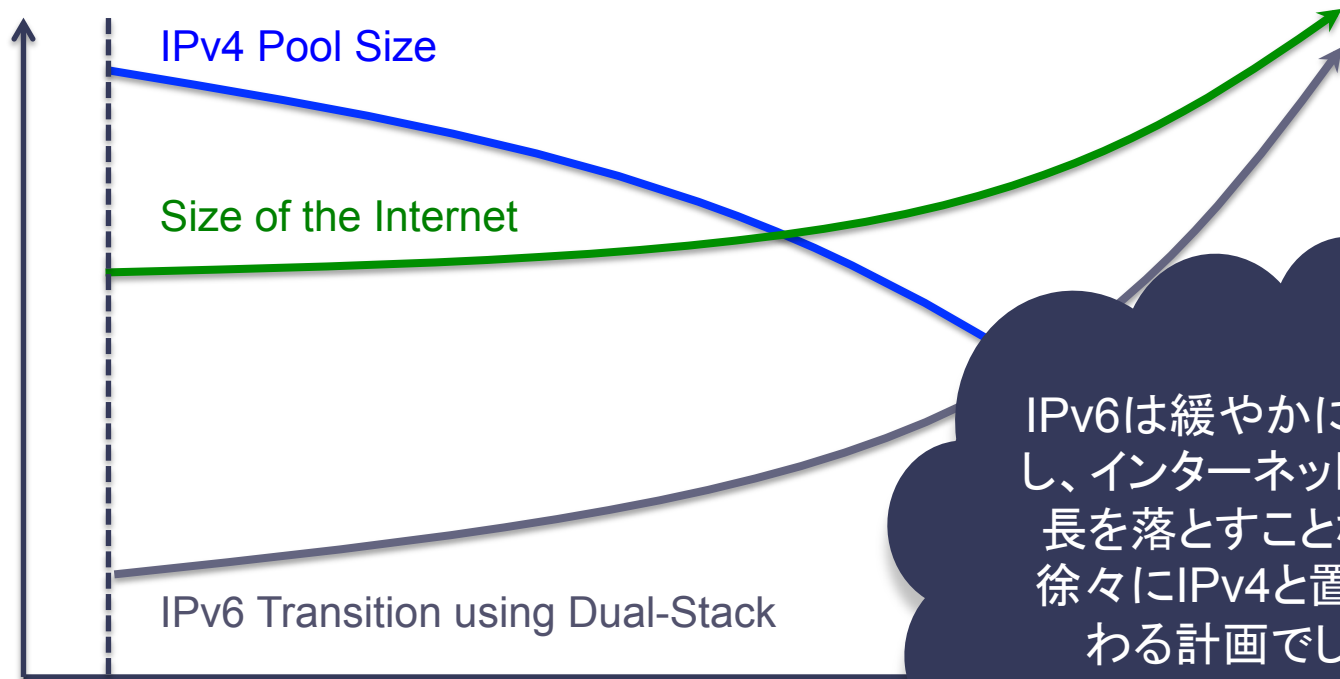
2011年
IANAのIPv4 Poolが枯渇
NTT東西 フレッツネクストでIPv6インターネット接続サービスを開始

- IPv6 はなぜ作られたか？
- IPv4 addressの枯渇とは
 - World IPv6 Launch

IPv6とインターネット

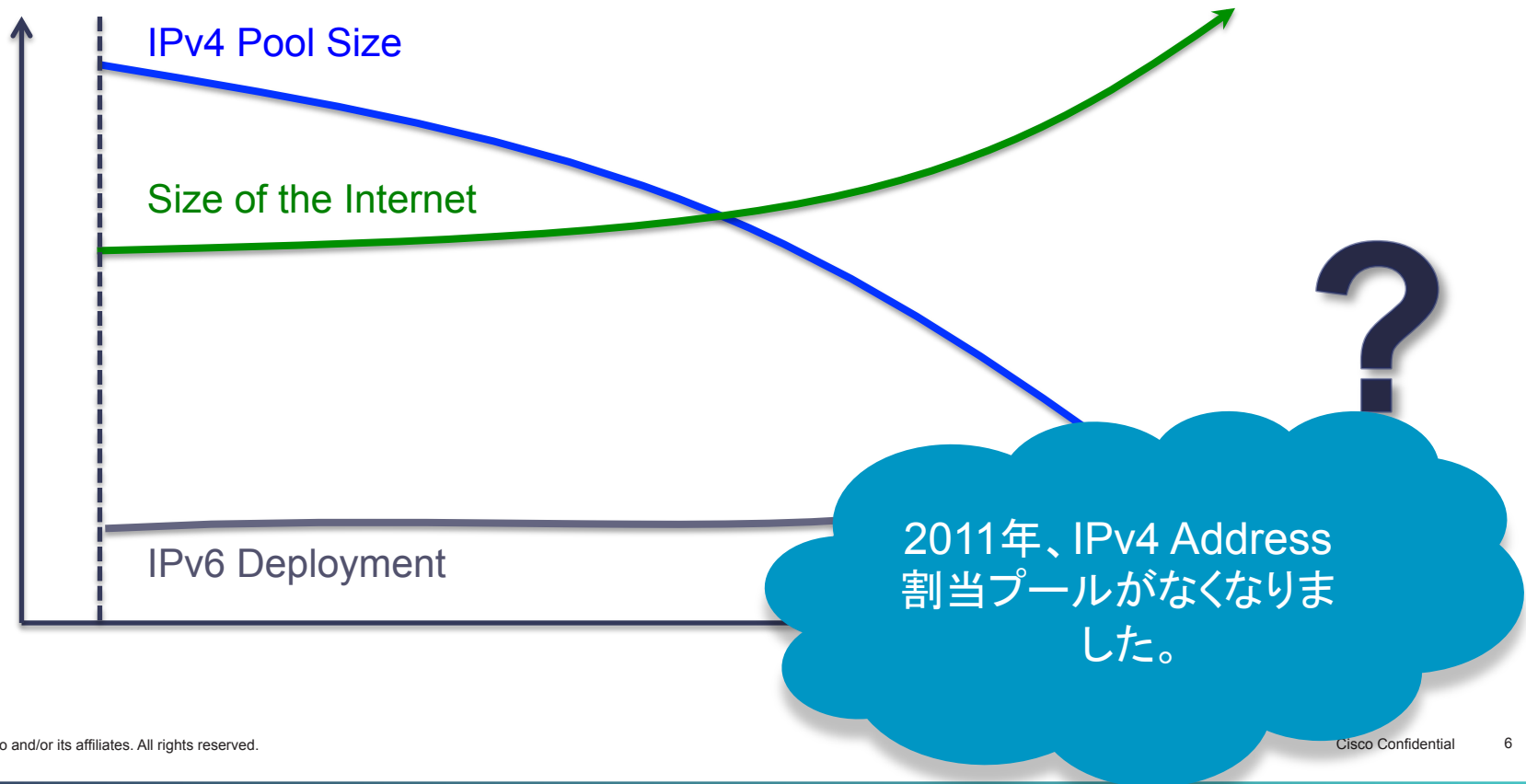
IPv6 はなぜ作られたか？

- 標準化されたのは1995～1998年頃
- 当時既にIPv4 Addressの”枯渇”が予想されていた

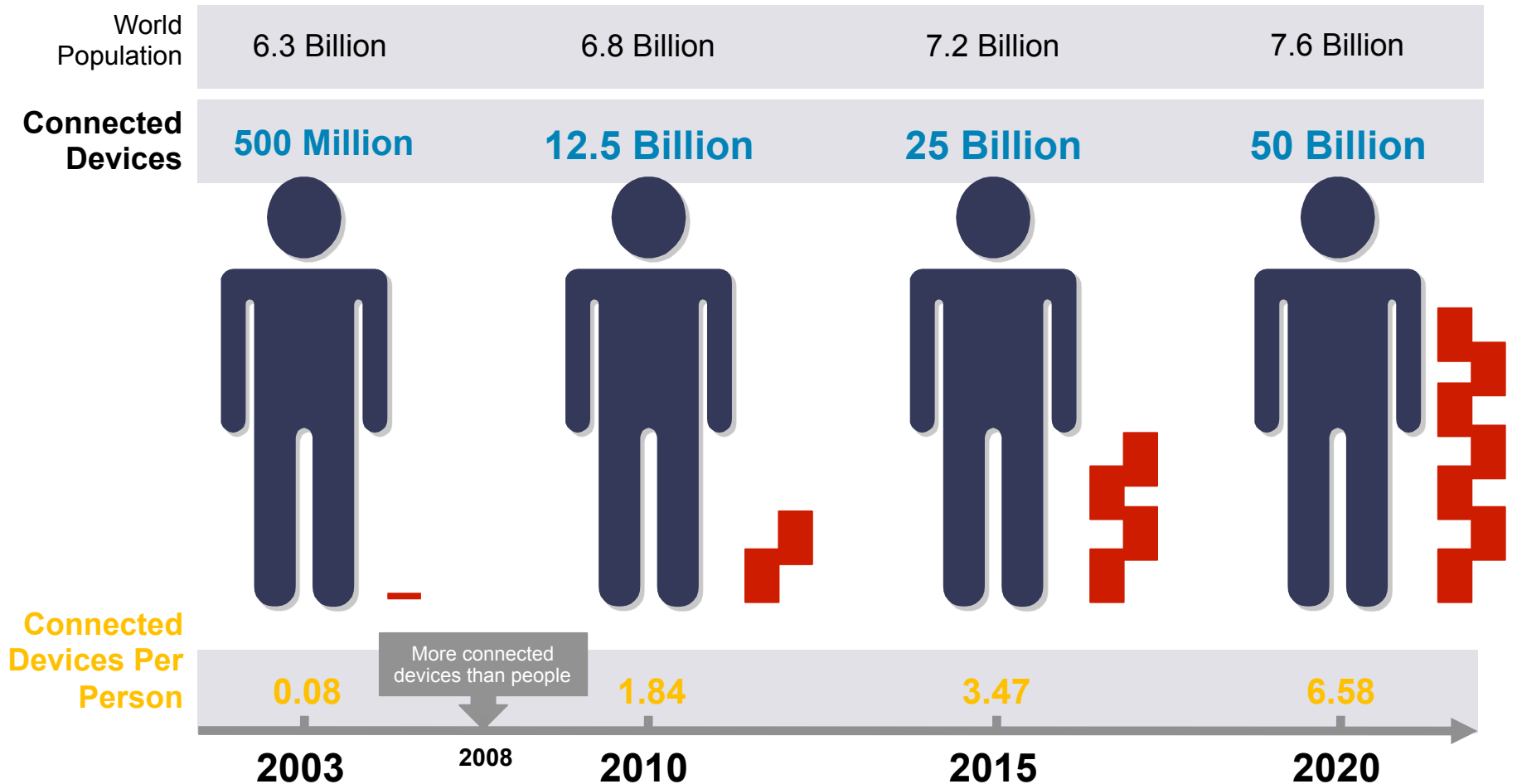


実際には...

- IPv4は、本当になくなるのか？
 - IPv6は普及してきているのか...？！



ネットワーク利用者の増加傾向は変わっていない



Source: Cisco IBSG, 2010

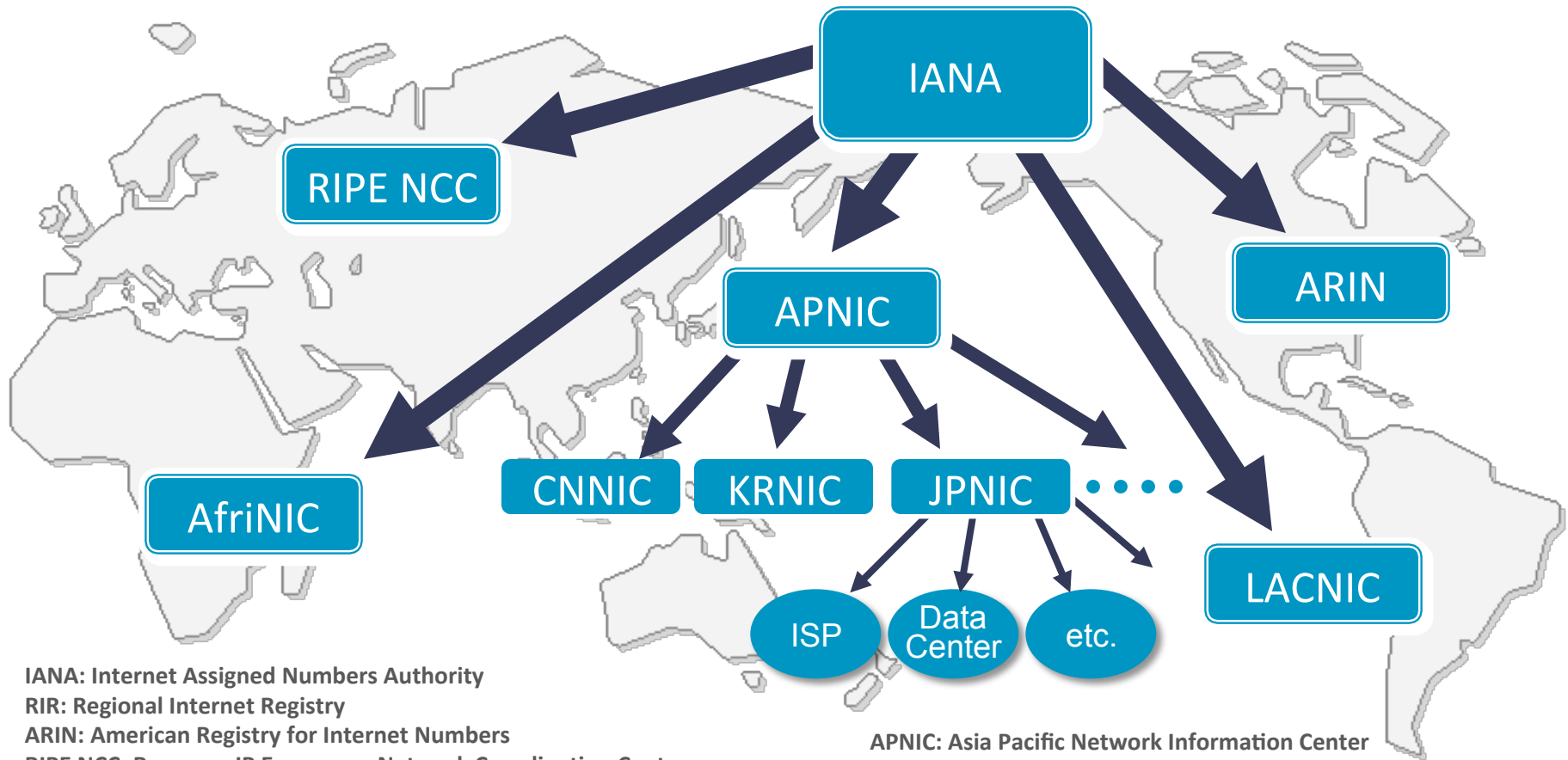
42.8億 = IPv4 addressでは不十分です

IPv4 Addressの枯渇とは？！

- 現在使われているIPv4 Addressがなくなってしまう訳ではない
 - IP Addressの管理機関は、新しいIPv4 Addressを割り当てるための”在庫”を管理している
 - この”在庫”が一定レベルを下回った段階で、今までとは異なる新規割当てルールが適用されることになる
- 今までの割当てルールとは、
 - 既に割り当てられているaddressを一定レベル以上使用済みで、今後一定期間内で一定レベル以上のaddressを使用する予定がある場合、必要な大きさのaddressの割り振りを(複数回)受けることができる

ところで、”IP Address 管理
機関”とはなんでしょう？！

IPアドレス管理の階層構造



IANA: Internet Assigned Numbers Authority

RIR: Regional Internet Registry

ARIN: American Registry for Internet Numbers

RIPE NCC: Resource IP Europeans Network Coordination Centre

LACNIC: Latin American and Caribbean Internet Address Registry

AfriNIC: African Network Information Centre

APNIC: Asia Pacific Network Information Center

JPNIC: Japan Network Information Center

KRNIC: Korea Network Information Center

CNNIC: China Internet Network Information Center

IPv4 Address 枯渇予想

(generated at 04-Nov-2014 08:09 ZURU)

IANA Unallocated Address Pool Exhaustion:

~~03 Feb 2011~~

割当てblockが残り5個になった時点でそれらを1つつつ、5つのRIRに割り振りました。

Projected RIR Address Pool Exhaustion Dates:

APNIC:	10 Apr 2011
RIPE/NCC:	14 Sep 2012
LACNIC:	10 Jun 2014
ARIN:	30-Mar-2015
AfriNIC:	07-Jul-2019

残り割当てblockが1つだけになったAPNICとRIPEは、最終割当て方式に移行しました。

Source: <http://www.potaroo.net/tools/ipv4/>

枯渇後は、どうなってしまうのでしょうか？

- 既に割り当てられているIPv4 Addressは、今後もそのまま使い続けることができる
 - 枯渇後ルールが適応されるのは、これから割当てを受けるときのみ
 - このルールは、1組織につき1回かぎり/22 block(=host数で約1,000)の割り振りを受けることができる
- 新しいネットワークを作るにはどうしたらいいのか？
 1. 既に取得済みのIPv4 Addressを節約して使う
 - Private Addressを有効に活用し、Global AddressはNATなどを介して複数のユーザーが共同で使うなどの方法が考えられる
 2. 他の組織からIPv4 Addressを移転してもらう
 - 2011年8月から、日本国内では他の組織が割り振りを受けたIPv4 Addressの移転(名義変更)ができるようになった
 3. IPv6を導入する

World IPv6 Launchとは？！

- 2012年6月6日12:00(UTC)から、IPv6対応を一斉に開始するkick-offイベント
 - 昨年実施された、“World IPv6 Day”は24hの時間限定のテストイベント
 - 今回は、永続的にIPv6を使用する前提であり終了しない
- ISOCが運営を行った
- 3種類の参加カテゴリが用意された(W6DはWeb Siteのみ)
 - Website Operator
 - Network Operator
 - Home Router Vendor



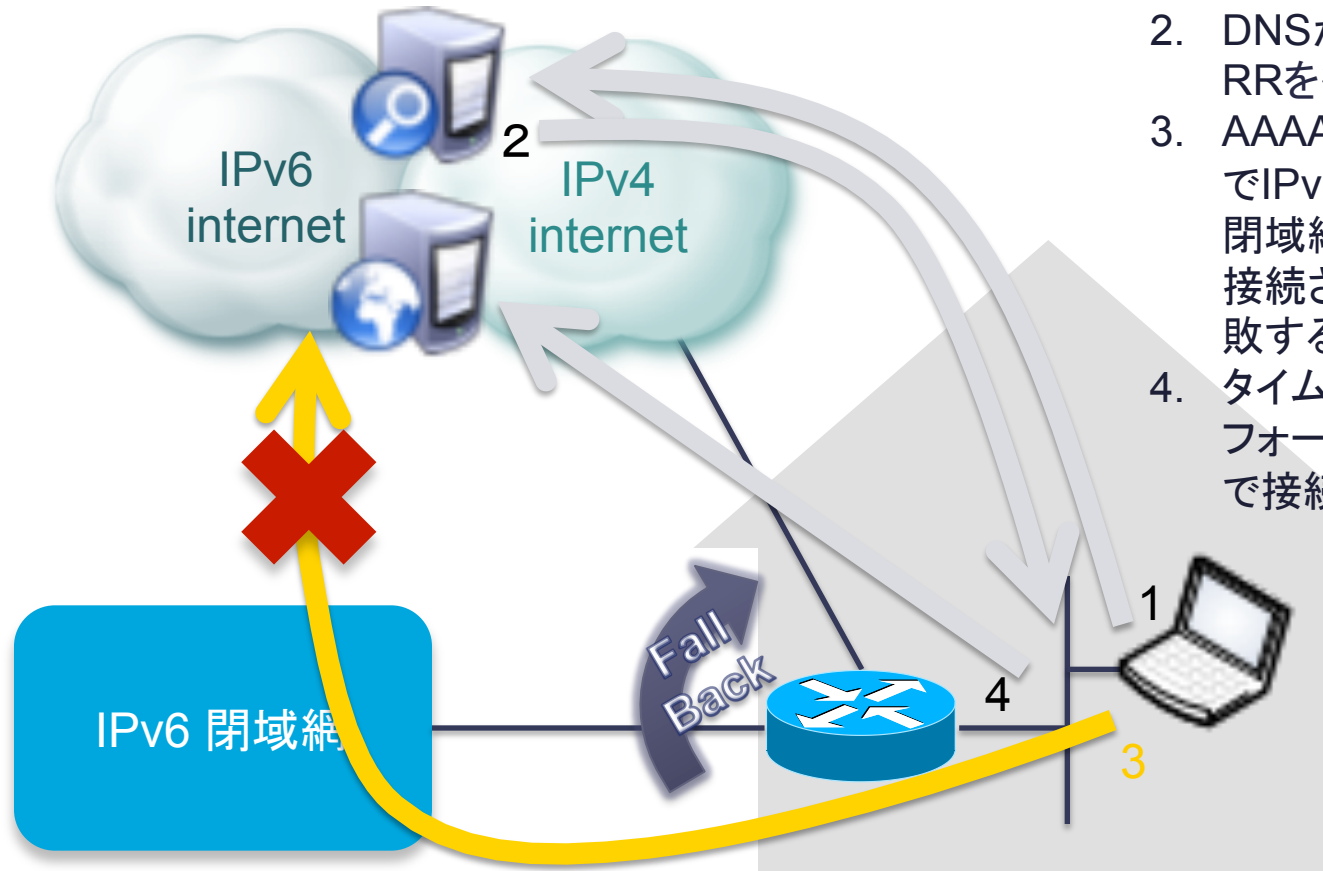
World IPv6 Launchへの参加条件

- Web Site Operator
 - メインとなるWeb SiteにAAAA RRが付加されてIPv6によるアクセスが可能であることが必要です。ipv6専用siteなどは不可とされている
- Network Operator
 - 全ての新規ユーザーにIPv6が標準的に提供され、既存ユーザーを含む全体の1%以上のユーザーがIPv6 Web Siteにアクセス可能である必要がある
- Home Router Vendor
 - コンシューマー向けCPE製品が、IPv6に固有の設定をエンドユーザーが行うことなく標準的にIPv6を使用可能で、かつUNH-IOLの相互運用テストシナリオを完了したことを示すリストにあげられていることが必要

Network OperatorにとってのW6L

- 「全体の1%以上のユーザーがIPv6 Web Siteにアクセス」とは？
 - World IPv6 Launchに参加しているWeb Siteの一部に対するIPv6とIPv4のTraffic比率が1%を超えることが求められている
 - ただし、これらのWeb Siteの中には、IPv6によるアクセスがIPv4と比較して遅延が大きい場合などに、IPv6によるアクセスを制限している場合が存在している
 - ✓ 日本国内では、フォールバック問題の存在などにより、この問題の影響を受けているNetwork Operatorが多く存在していると言われている
 - ✓ いろいろな問題が、克服されつつあると言われるが、IPv6の本格的な導入を行うために、周囲の状況を把握することが重要であると考えられる

(For Your Reference) Fallback問題とは



1. wwwサーバーのアドレスをDNSに問い合わせる
2. DNSからAAAA RRとA RRを得る
3. AAAA RRが存在するのでIPv6で接続を試みるが、閉域網でインターネットに接続されていないので失敗する
4. タイムアウトを待ち、フォールバックして、IPv4で接続を試みる

- IPv6 普及度の統計
 - IPv6対応状況
 - IPv6 利用者数統計
- 国内 IPv6 普及の現状

IPv6の普及とその尺度

IPv6 普及度の統計 - 必要性

Internet事業のビジネス判断

商用インターネット

現在のインターネットは、その多くが“商用=ビジネス”で提供されている。

- ✓ 商用ISP
- ✓ コンテンツサービス
- ✓ 携帯電話

投資の合理性

投資を行うためには、合理的な理由が必要。

- ✓ IPv4アドレスの枯渇と事業継続性
- ✓ 市場・競合他社の状況
- ✓ 行政の規制方針
- ✓ 技術的な優位性による差別化

判断基準

IPv6 サービスの事業化判断のための情報を収集

- ✓ だれがサービスを提供しているか？
- ✓ 誰がサービスを利用しているか？
- ✓ 収益性と投資の回収

サービス事業者は IPv6 事業化の判断を行うために、普及度の統計情報が必要

IPv6 普及度の統計 – 統計の対象

サービス事業者の統計

- ▶ サービス用ネットワークのIPv6対応
- ▶ コンテンツ・アプリケーションのIPv6対応
- ▶ IPv4とIPv6の利用比率

地理・ルーティング的統計

- ▶ 国及び地域ごとの統計
- ▶ AS毎の統計

利用者数の統計

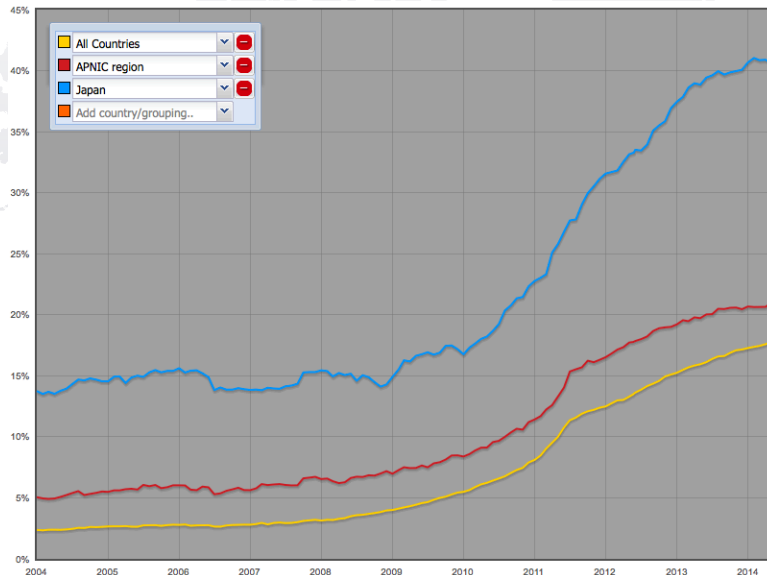
- ▶ 特定のアクセスサービスにおけるIPv6利用者数
- ▶ 特定のコンテンツに対するIPv6利用者数

必要な統計値の選択が必要



IPv6対応状況 - サービスネットワーク

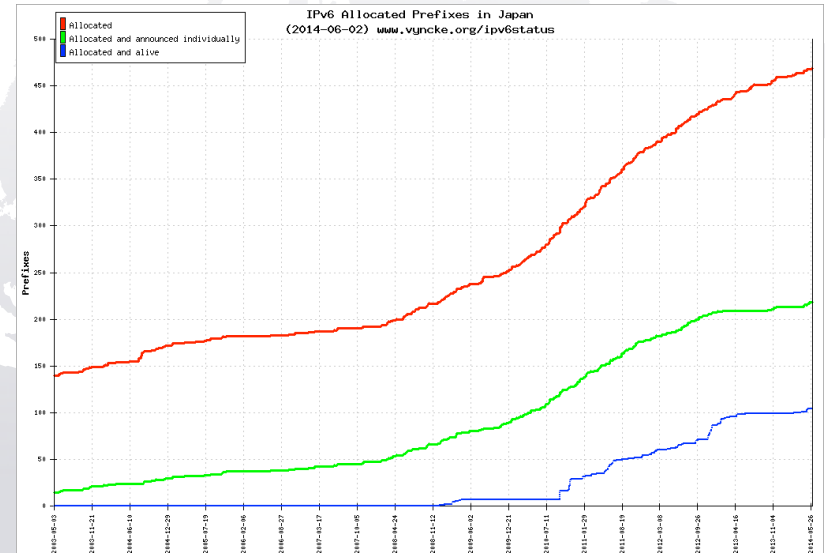
国及び地域別・AS別



RIPE/NCCによるASの統計

ルーティングテーブル上のASのうち、IPv6 Prefixを広告しているASの比率の統計。

<http://v6asns.ripe.net/v/6?s= ALL;s= RIR APNIC;s=JP>



Eric Vyncke の統計

割り当て済み・広告済み・IPv6到達可能なIPv6 Prefixの数の統計。国単位で参照可能。

<https://www.vyncke.org/ipv6status/plotbgp.php?country=jp>

IPv6対応状況 - アプリケーション 国及び地域別・サイト単位

IPv6 Deployment Status

For country: [Japan] For type: [All categories] [Filter]

Japan is scanned since 2010-06-17 and the last information is dated 2014-06-01. Return to [Aggregated Results](#). Jump to the [IPv6 allocated prefixes](#). Leave the cursor over a green/orange box to have more information (MSS, MTU). Hover the mouse over a red box to display the AS of the web site (this is usually a good indication of the web hoster). Click on any graphs or maps to zoom on it. You can add a widget on your own web site with your country IPv6 status or get more geographical maps, click [here](#) to see how ->

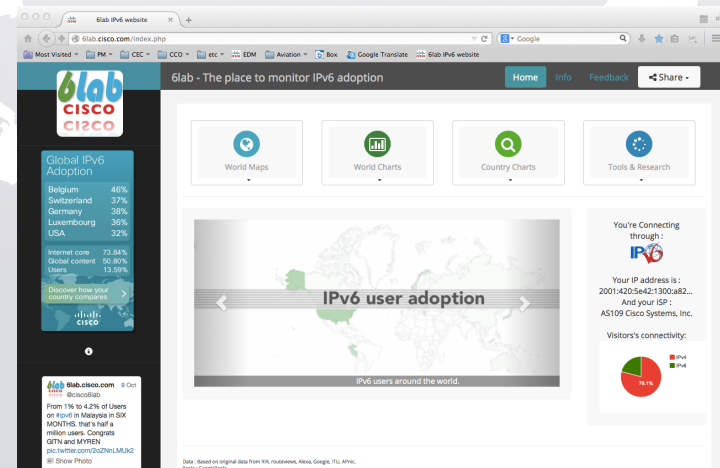
this site participated at the World IPv6 Day in 2011.
 this site has removed the IPv6 access after the World IPv6 Day (fear!).

Name	Alexa	Web	Mail	DNS
Search Yahoo	1/21	FAILED	FAILED	FAILED
Search Google	2/34	FAILED	FAILED	FAILED
R2C Amazon	3/52	FAILED	FAILED	FAILED
fc2.com	4/60	FAILED	FAILED	FAILED
rakuten.co.jp	5/96	FAILED	FAILED	FAILED
ameblo.jp	6/121	FAILED	FAILED	FAILED
livedoor.com	7/157	FAILED	FAILED	FAILED
nicovideo.jp	8/218	FAILED	FAILED	FAILED
naver.jp	9/235	FAILED	FAILED	FAILED
goo.ne.jp	10/245	FAILED	FAILED	FAILED
stam.co.jp	11/255	FAILED	FAILED	FAILED
ameba.jp	12/375	FAILED	FAILED	FAILED
kakaku.com	13/400	FAILED	FAILED	FAILED
ck101.com	14/465	FAILED CDV	ASP0X4 GOOGLEMAIL.com	ASP0X4 GOOGLEMAIL.com
decoy.jp	15/508	FAILED	FAILED	FAILED
seesaa.net	16/514	FAILED	FAILED	FAILED
hateba.jp	17/537	FAILED	FAILED	FAILED
pixiv.net	18/541	FAILED	FAILED	FAILED
blogspot.jp	19/588	FAILED	FAILED	FAILED
sakura.ne.jp	20/628	FAILED	FAILED	FAILED
nifty.com	21/830	FAILED	FAILED	FAILED
mixi.jp	22/853	FAILED	FAILED	FAILED
biglobe.ne.jp	23/923	FAILED	FAILED	FAILED
weblio.jp	24/996	FAILED	FAILED	FAILED
japanpost.jp	25/1013	FAILED	FAILED	FAILED
so-net.ne.jp	26/1020	FAILED	FAILED	FAILED
exblip.jp	27/1028	FAILED	FAILED	FAILED
livedoor.biz	28/1031	FAILED	FAILED	FAILED
geocities.jp	29/1096	FAILED	FAILED	FAILED
exblip.jp	30/1130	FAILED	FAILED	FAILED
rakuten.ne.jp	31/1154	FAILED	FAILED	FAILED

Eric Vyncke の統計

Alexa Top 500のドメインに対し、HTTP/SMTP/DNSの各プロトコルをIPv6で定期的に試行する。この結果の統計情報を国毎に表示する。

<https://www.vyncke.org/ipv6status/>



Cisco 6Labの統計

国毎のIPv6対応サイト統計や、APNIC Lab, RIPE/NCCなど他のサイトの統計情報を一括して提供している。

<http://6lab.cisco.com/>

IPv6利用者数統計 - IPv6 普及・高度化推進協議会

フレッツ光ネクスト等の利用者数

- IPv6インターネット接続を利用可能な、NTT東西が提供する、“フレッツ光ネクスト”の加入者のうち、有効と思われるIPv6利用者の加入者の全体に対する指標値

IPoE方式及びPPPoE方式それぞれにおける、フレッツ光ネクスト全体に対するIPv6利用者数を推定し、合算する。

- ✓ IPoE VNE事業者から提供されるIPoE方式加入者数から、全体に対する加入者の割合を算出する
- ✓ 統計に協力しているPPPoE ISPが、利用実績のあるPPP アカウント数を集計し、全体加入者に対するシェアを考慮した、全体に対する加入者の割合を算出する

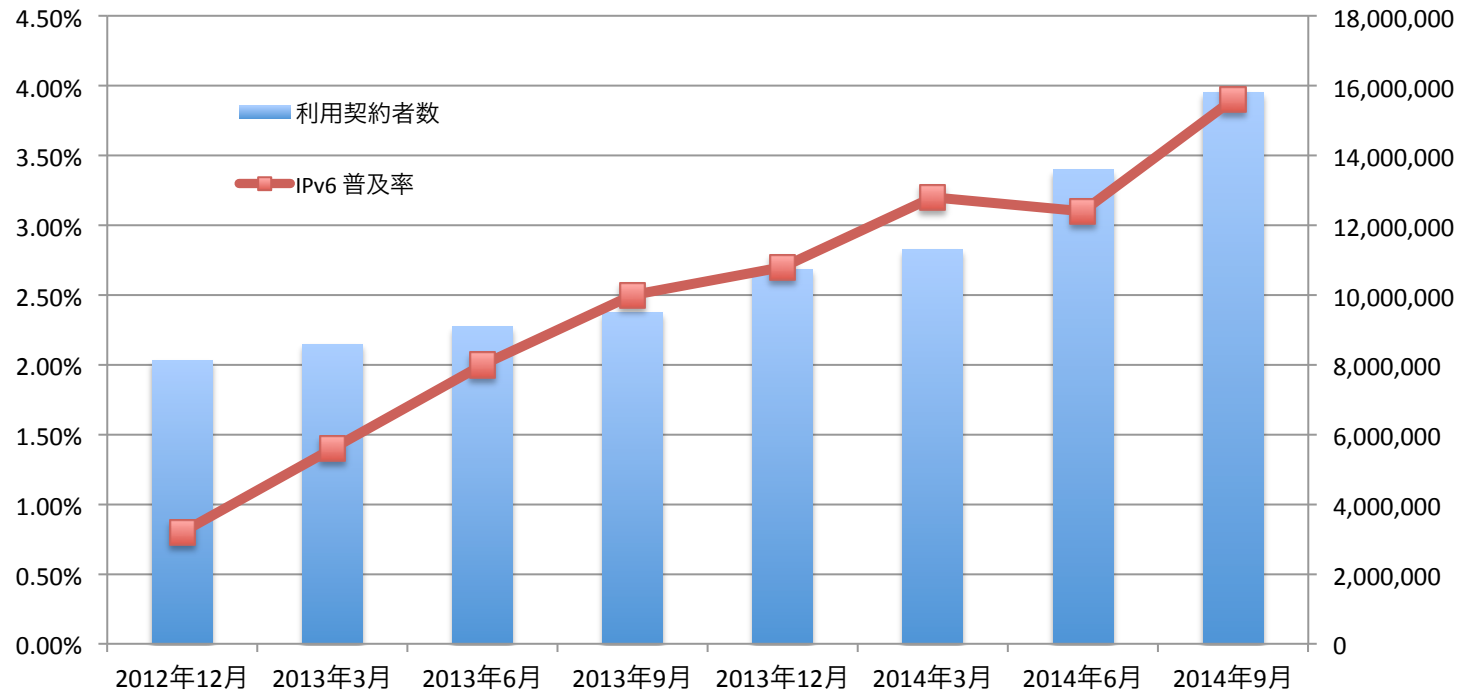
4半期毎に集計を行い、IPv6高度化・普及推進協議会のWebサイトにて公表する



<http://v6pc.jp/jp/spread/ipv6spread.phtml>

IPv6 高度化・普及推進協議会によるIPv6利用者数統計 – Cont'd

フレッツ光ネクスト IPv6普及率指標値

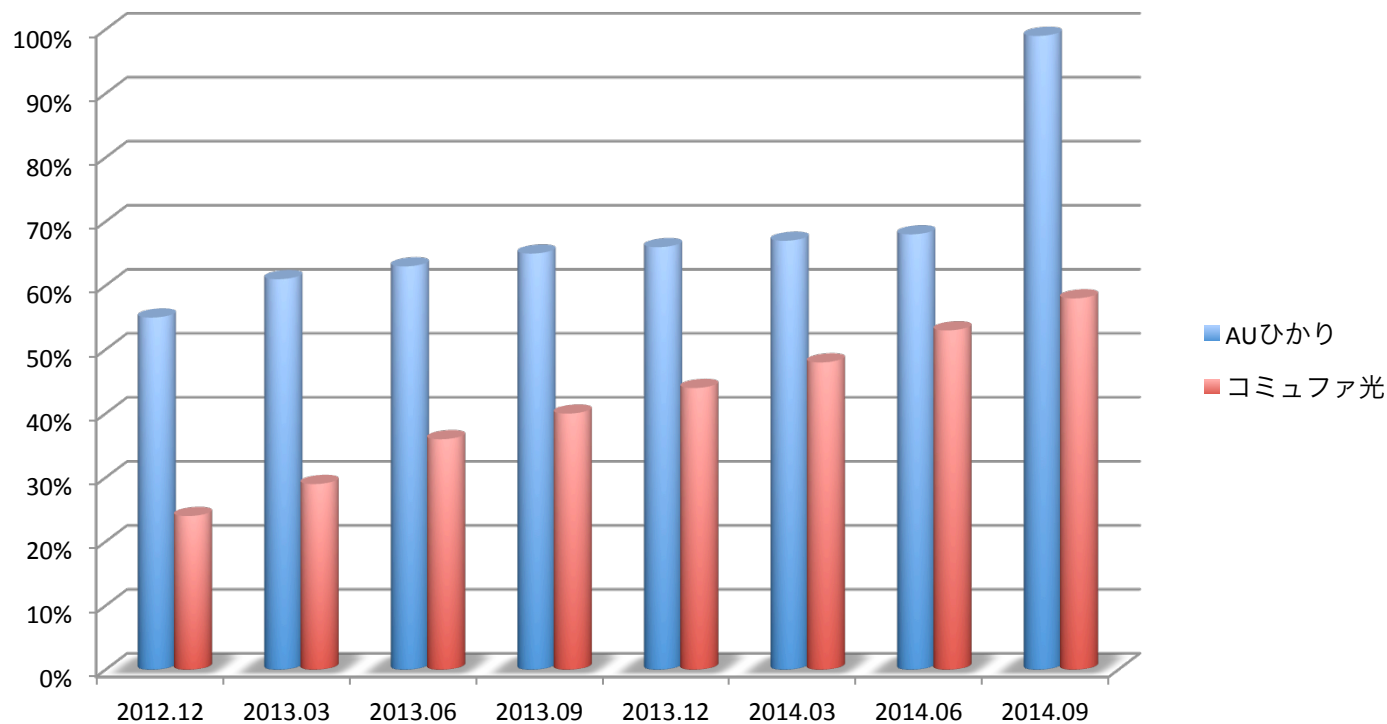


数値自体は十分なレベルでないが、上昇傾向にある

協力会社 - 東日本電信電話株式会社、西日本電信電話株式会社、BBIX株式会社、日本ネットワークイネイブラー株式会社、インターネットマルチフィード株式会社、エヌ・ティ・ティ・コミュニケーションズ株式会社、株式会社インターネットイニシアティブ、ソネットエンタテインメント株式会社、KDDI株式会社、中部テレコミュニケーション株式会社

IPv6 高度化・普及推進協議会によるIPv6利用者数統計 – Cont'd

KDDI・CTC IPv6普及率



順調に普及がすすんでいる。

国内 IPv6 の普及の現状

通信事業者

大手を中心に通信事業者の多くは IPv6対応の準備を行っている

- ✓ 中小規模の事業者には未だ課題が残っている
- ✓ 携帯通信事業者の本格対応はこれから

コンテンツ事業者

コンテンツ事業者のIPv6対応はこれから

- ✓ 通信事業者とは考え方・立場が違う
- ✓ 課題の整理が必要

エンドユーザー

着実に増加している

- ✓ エンドユーザーが直接IPv6を必要とする動機は未だ少ない
- ✓ ユーザー数の増加は間接的なもので、絶対数もまだ小さい

継続的な統計の実施がIPv6の普及を促進する

(参考) 統計サイト



<http://www.google.com/ipv6/statistics.html>
<http://www.yynche.org/ipv6status/>
<http://6lab.cisco.com/stats/>
<http://www.worldipv6launch.org/measurements/>
<http://v6asns.ripe.net/v/6>

- IPv6移行の動機と前提条件
 - Dual-Stack環境
- NAT - IPv4 addressの節約

IPv6 導入の指針

IPv6移行の動機と前提条件

- 基本的な動機
 - IPv4 addressの枯渇をネットワーク拡張の制限にしない
 - 外部のIPv6サイトへの接続性を担保する
- 前提条件
 - 既存の機器を有効に活用する
 - 既存の環境に与える影響を最小限に抑える
 - IPv6の広大なアドレス空間を使用可能にするだけでなく、IPv4アドレスの節約を同時に行う

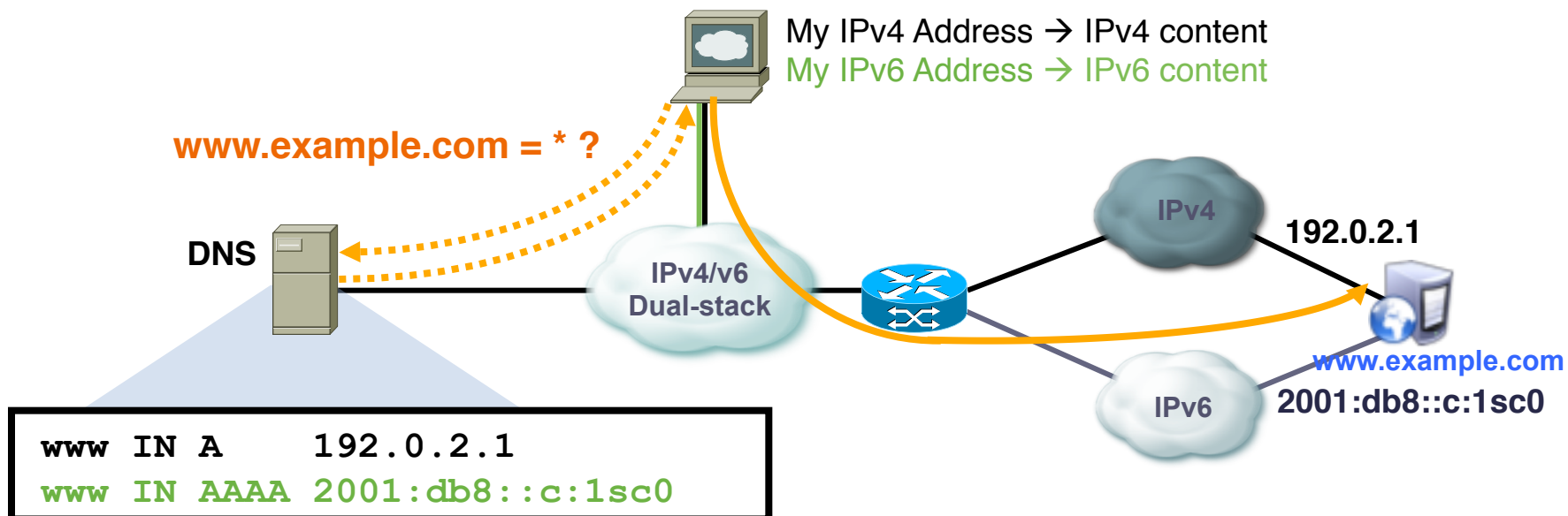
Dual-StackとIPv4 Address

- 当面IPv4 Internetは使われ続けると思われるため、可能であればエンドユーザーの環境としては、Dual-Stack環境が必要
 - 基幹ネットワークは、必ずしもDual-Stackである必要はなく、IPv6ネットワーク上に、IPv4を重畳させたり、その逆を行うような移行技術も存在している
- IPv4 Address資源は、既に枯渇しており、潤沢に使用することは難しい
 - 一つのIPv4 Addressを複数のユーザーで、“共用”する技術を組み合わせて使用することが求められる

Dual-Stack環境

- IPv6の直接のMotivationは、IPv4をなくすことではない
 - 当面は、既存のIPv4環境に影響を与えず、共存することを考慮すべき
- アプリケーションの両端はDual-Stack
 - エンドユーザーおよびアプリケーション・プロトコルのサーバーは、基本的にIPv4/IPv6両方で同等なサービスを利用・提供可能であるべき
- 基本的にエンドユーザーとサーバーの間のネットワーク・機器がすべてdual-stackである必要はない
- 将来的にIPv4を全く使う必要がなくなった時点で、IPv6 single stackとなる

Dual-StackとDNS

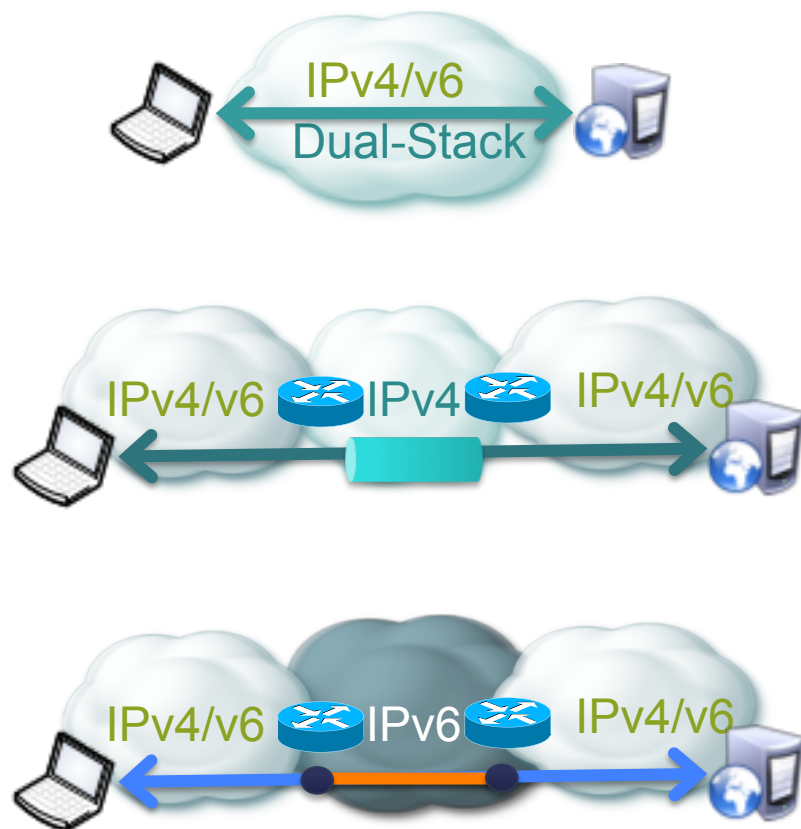


• DNS (Domain Name System)のDual-Stack対応

- DNSのデータ(RR)はIPv4 records (A) and/or IPv6 (AAAA) recordsに対応している
- DNSの問い合わせ/返答protocol自体は、IPv4/IPv6から独立している
- エンドユーザーは、任意のTransport(v4 or v6)で、必要な資源レコード(A and/or AAAA RR)を問い合わせできる

基幹ネットワークへのDual-stack導入の手法

- 完全Dual-Stack
 - エンドユーザーとサーバーの間のすべての区間がIPv4/IPv6双方をroutingする
- Tunneling
 - 例えばIPv6のパケットを転送する場合、IPv4でカプセル化することにより、IPv4インフラ上でもIPv6の転送を可能とする
- Double Translation
 - 例えばIPv4のパケットを転送する場合、一度IPv6に変換してからIPv4に戻すことにより、IPv6インフラ上でもIPv4の転送を可能とする



IPv4 addressの節約

一般的なIPv4接続サービスは、

“加入者一人” = “IPv4アドレス一個”

これを更に節約するには、

“加入者一人” < “IPv4アドレス一個”

すなわち、

一つのIPv4アドレスを複数の加入者で共有する

必要がある

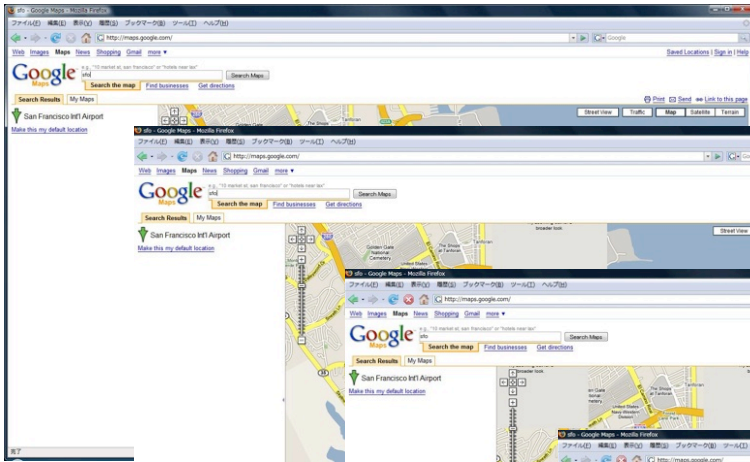
IPv4 addressの共有

- 複数の加入者が”同じ”IPv4 addressを使用する
 - 加入者を区別するためには、トランスポートプロトコル(TCP4/UDP4)のポート番号を使用する
 - 加入者間でのポート番号の重複を避けるためNATと同時にポート番号も変換する(NAPT: Network Address and Port Translation)
- NAPTの利用
 - RFC3022
- NAPTの使用に関する課題
 - 利用可能なポート数の制限
 - 常に”内側”からのコネクション・TCP/UDP/ICMPのみ
 - NAPTの設置場所・トポロジー

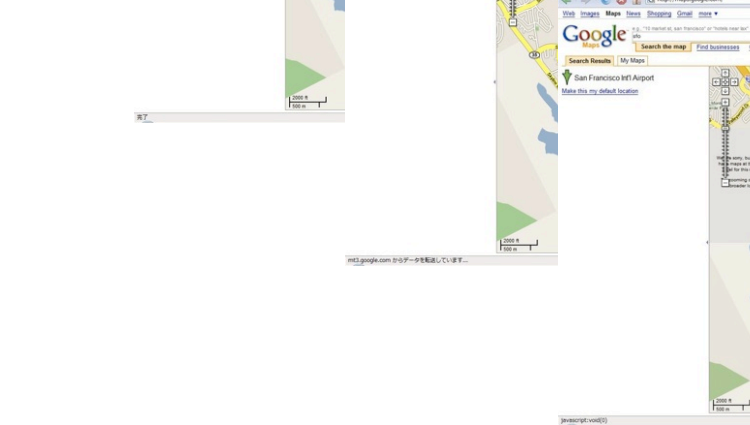
NAPTにおけるポート数の制限

- 同時に多くのポートを使用するアプリケーションは、ポート数の制限により機能が限定される場合が存在する
 - ポート数制限環境における(ちょっと前の)Google Mapsの例
 - - AJAXアプリケーション, etc
 - Reference:
Hiroshi Esaki, Ph.D: www2.jp.apan.net/meetings/kaohsiung2009/presentations/ipv6/esaki.ppt

Max Numbers of Connections



30 Connections



20 Connections



15 Connections



10 Connections

5 Connections....

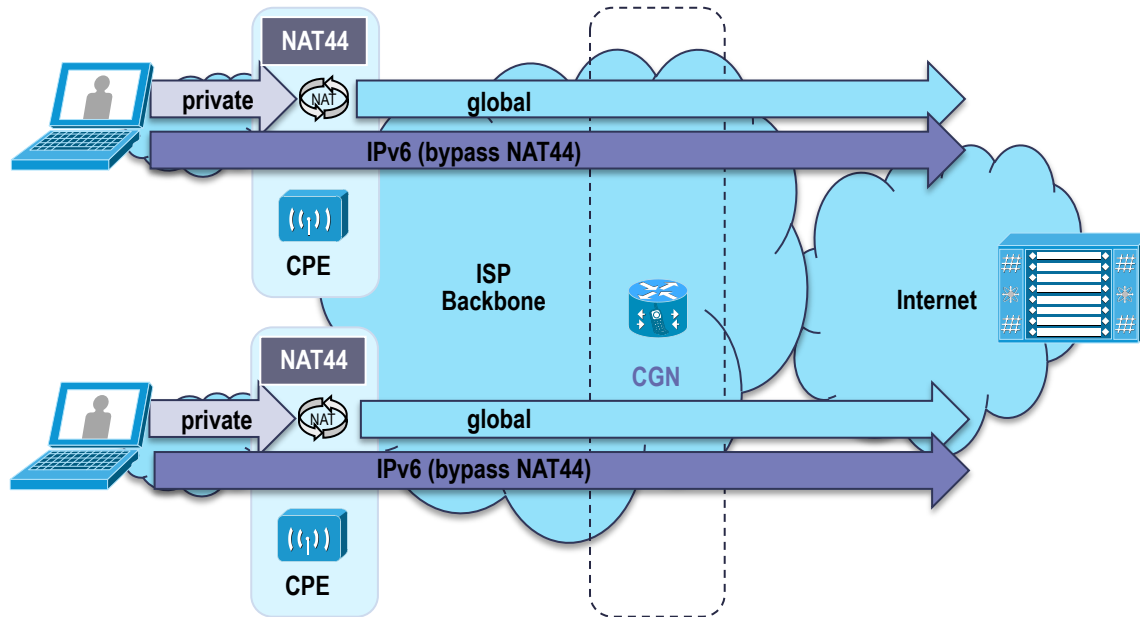


サーバが見つかりませんでした
maps.google.com という名前のサーバが見つかりませんでした。
• www.example.com を変更して www.example.com と入力するなど、アドレスを修正して入力していないご確認ください。
• 本サイトは本番環境であるため、コンピュータネットワーク接続を確認してください。
• ファイアウォールやプロキシソフトウェアが保護されている場合は、Fireboxによる Web アクセスが許可されているか確認してください。

NATの位置

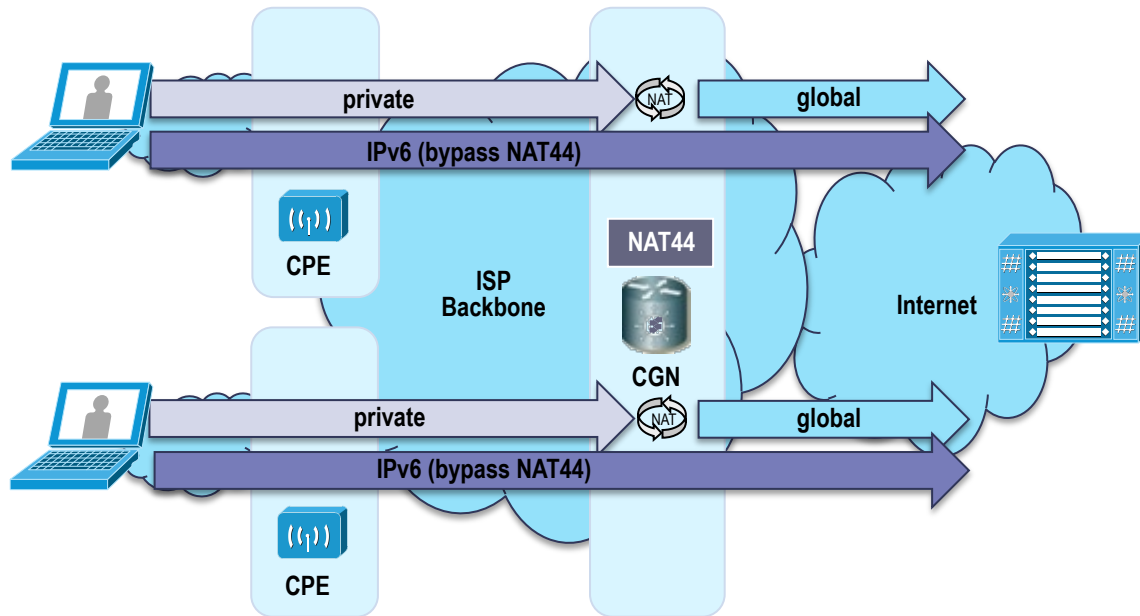
- NAT装置の設置位置によりIPv4アドレスの共有形態に差異が存在する
 - 理論的には、より集中させるほど共有効率は向上する
 - 同一のIPv4アドレスを異なるNAT装置で使用する場合はポート番号の割り振りメカニズムが必要

CPEにおけるNAT



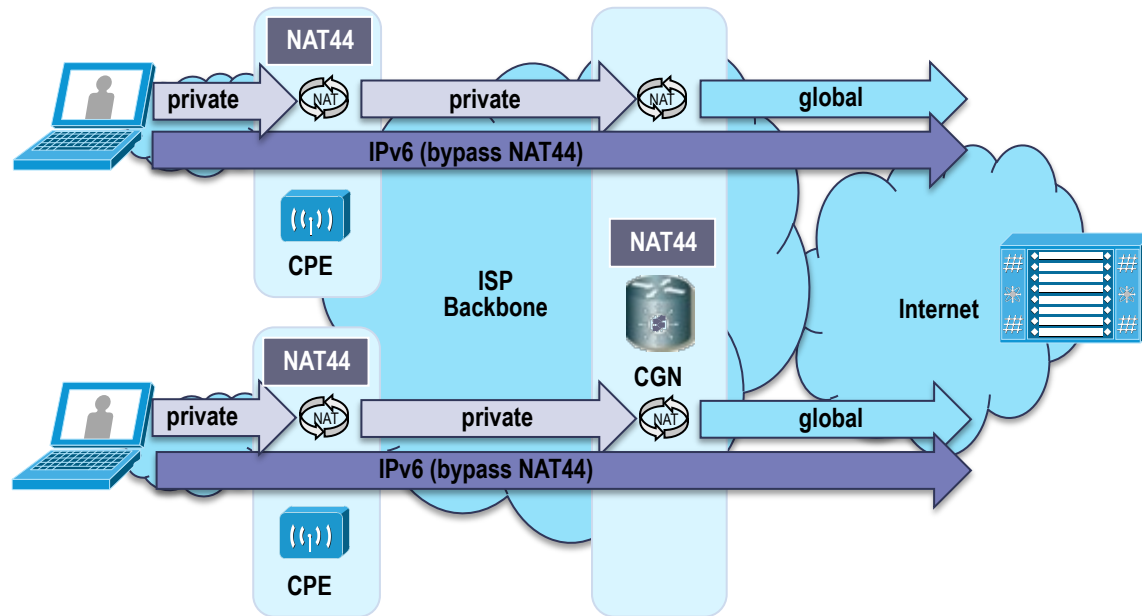
- CPE(宅内設置ルーター)にNAT機能を実装する
- 今日最も一般的な形態
- 各加入者の自由度が高いが、IPv4アドレスの共有効率は低い
 - 共有効率をあげるために、CPE毎のポート番号に制限を付加し、複数のCPEで共通のIPv4 addressを使用する場合も存在する – Port Restricted NAT

CGN (Carrier Grade NAT)



- ISPの基幹設備内に設置し、複数の加入者が利用する
 - ISPの設備内に、加入者毎の状態を保存しなければならないため運用負荷が高い
- 容易に複数の加入者が一つのIPv4アドレスを共有できるため、その効率が高い
- 加入者からGlobal Addressを操作不可

Double NAT (CPE NAT+CGN, a.k.a. NAT444)



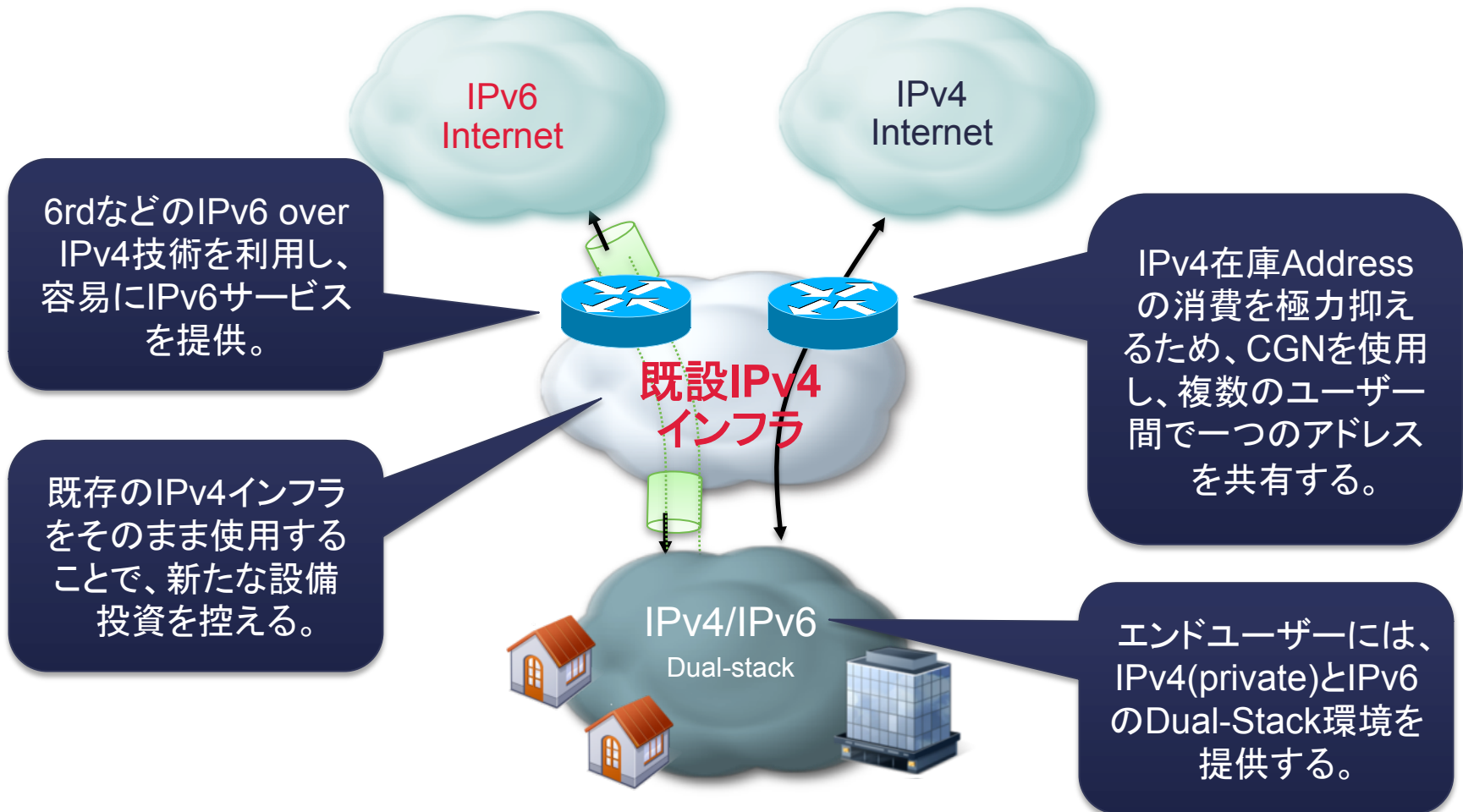
- CPEによるNATとCGNの併用
 - CPE NATは非常に一般化しているため、CGNの導入は、実質的にDouble NAT環境となる
- 加入者からGlobal Addressを操作不可で、特にUPnPなどへの対応も困難となりうる
 - 現在この問題を解決するために新Protocolの検討作業も進められている

- 構成モデル – 既設IPv4インフラの活用
 - 構成モデル - IPv6 onlyインフラ
 - 移行のステップ

構成モデルと移行のステップ

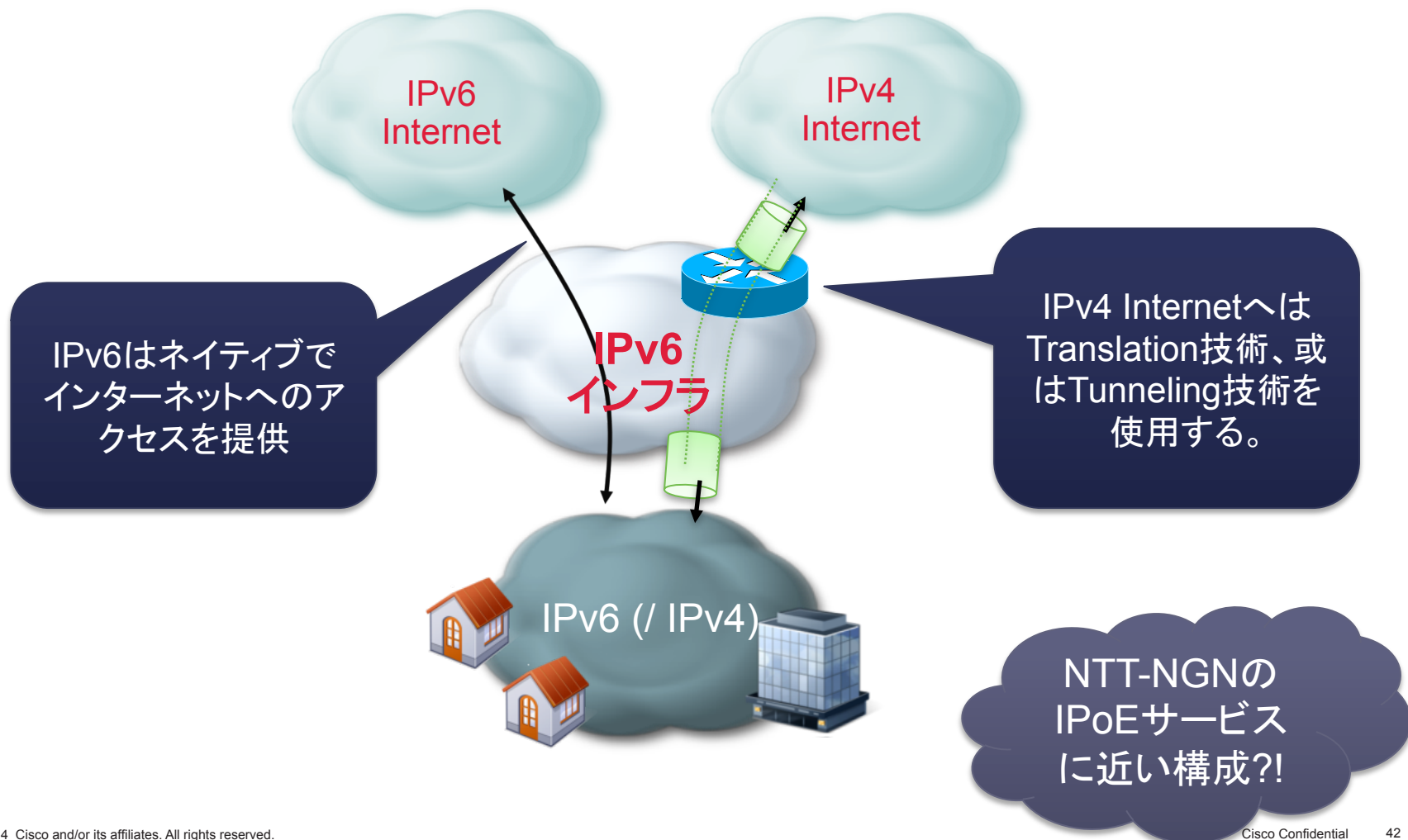
構成モデル – 既設IPv4インフラの活用

- IPv6 over IPv4 Tunneling + Carrier Grade NAT

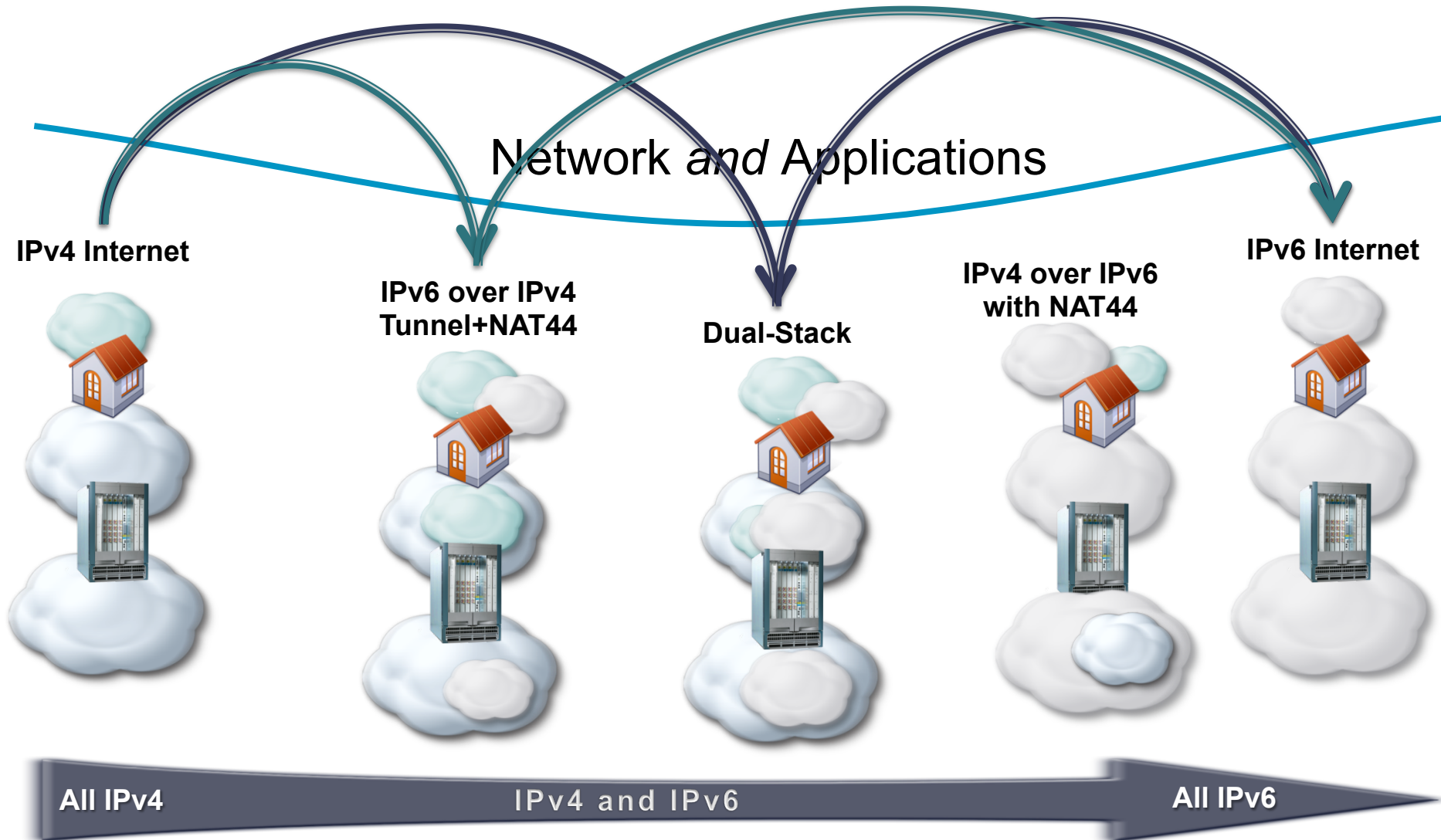


構成モデル - IPv6 onlyインフラ

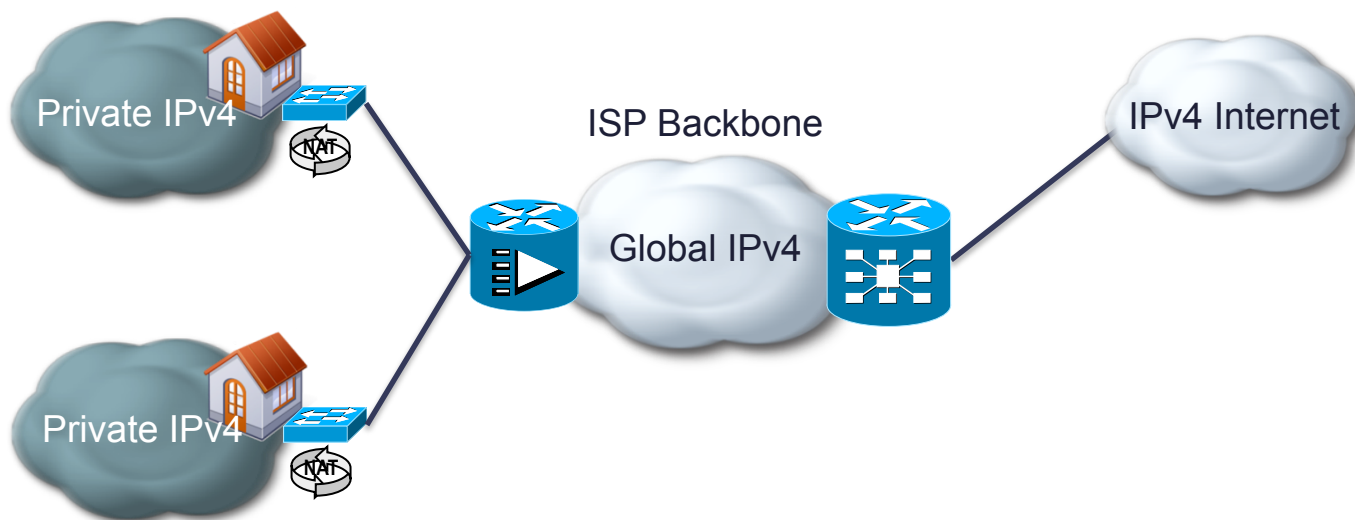
- Native IPv6 + IPv4 overlay → 前項の逆パターン



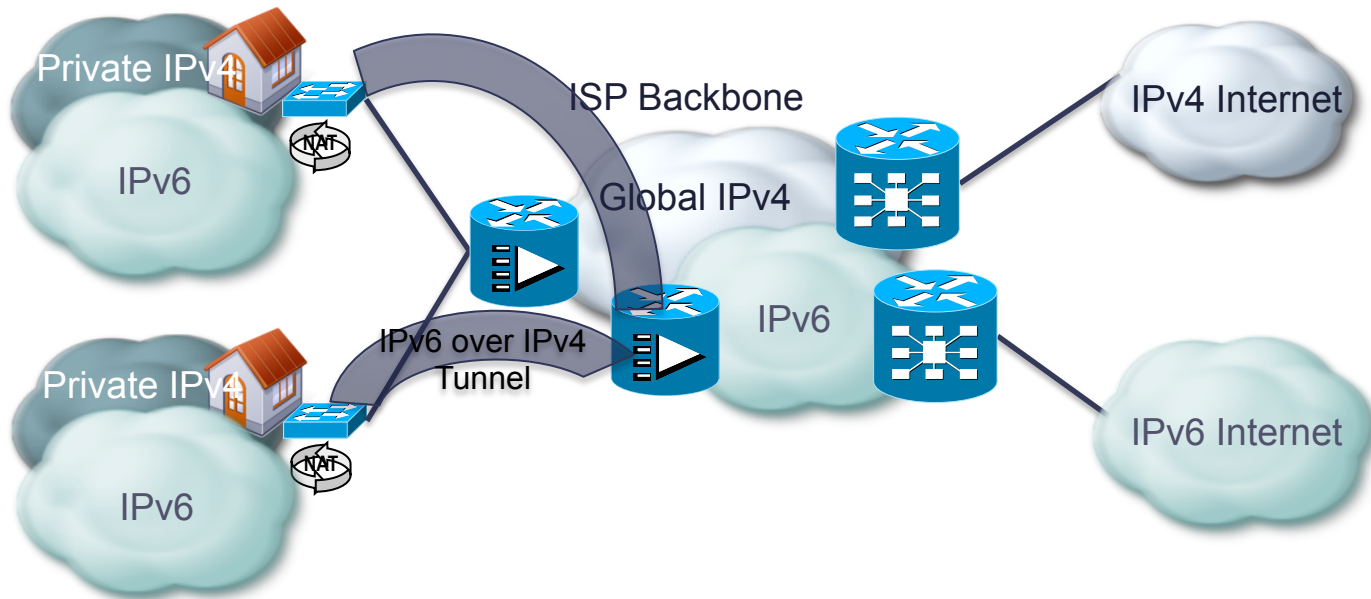
移行のステップ



Step.0 今日のインターネット

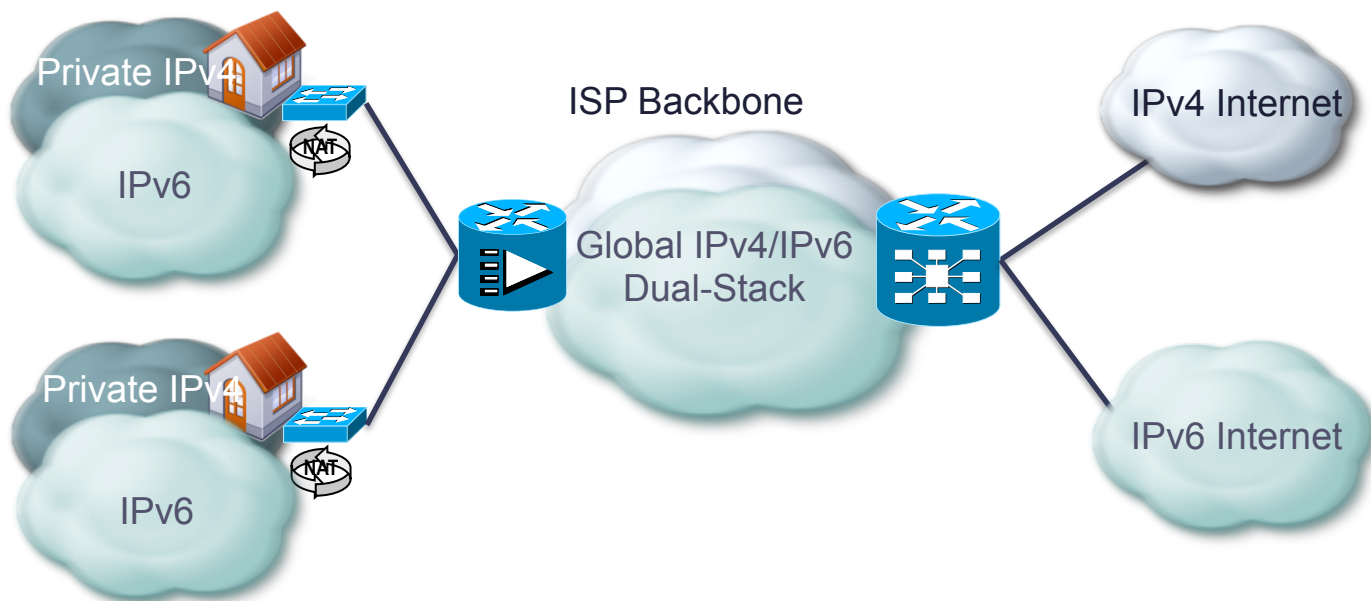


Step.1 TunnelingによるIPv6接続



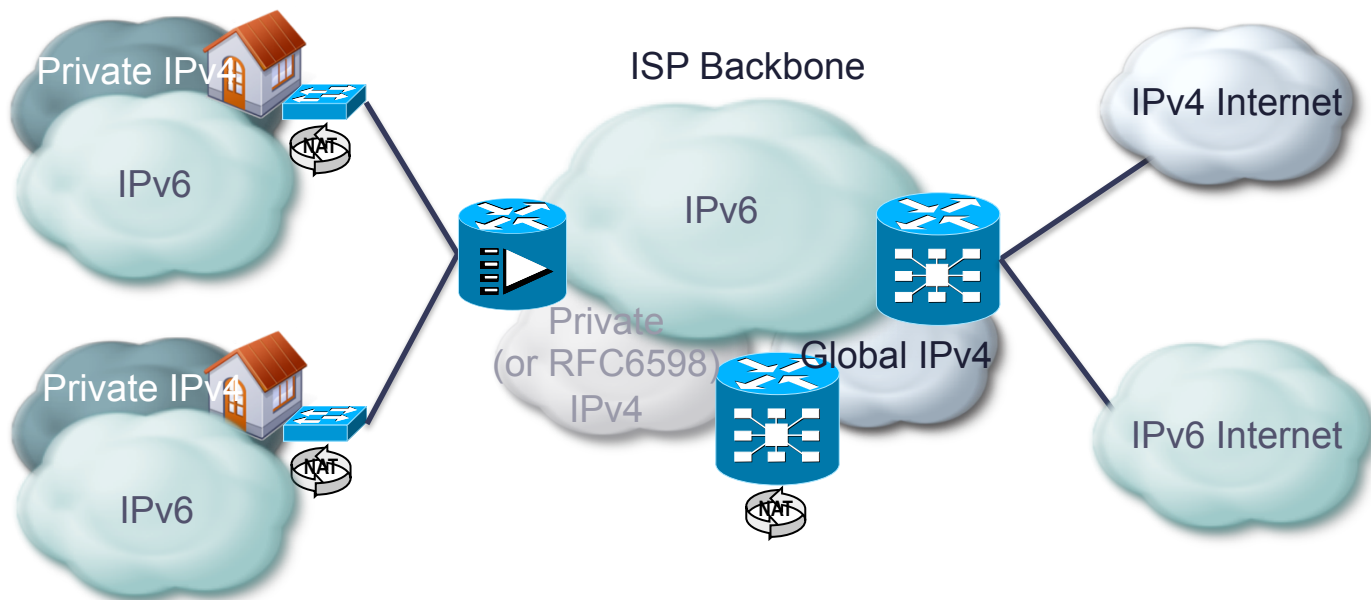
CPEとISPのTunnel Concentratorの間はIPv6 over IPv4 Tunnelで接続

Step.2 BackboneのDual-Stack化



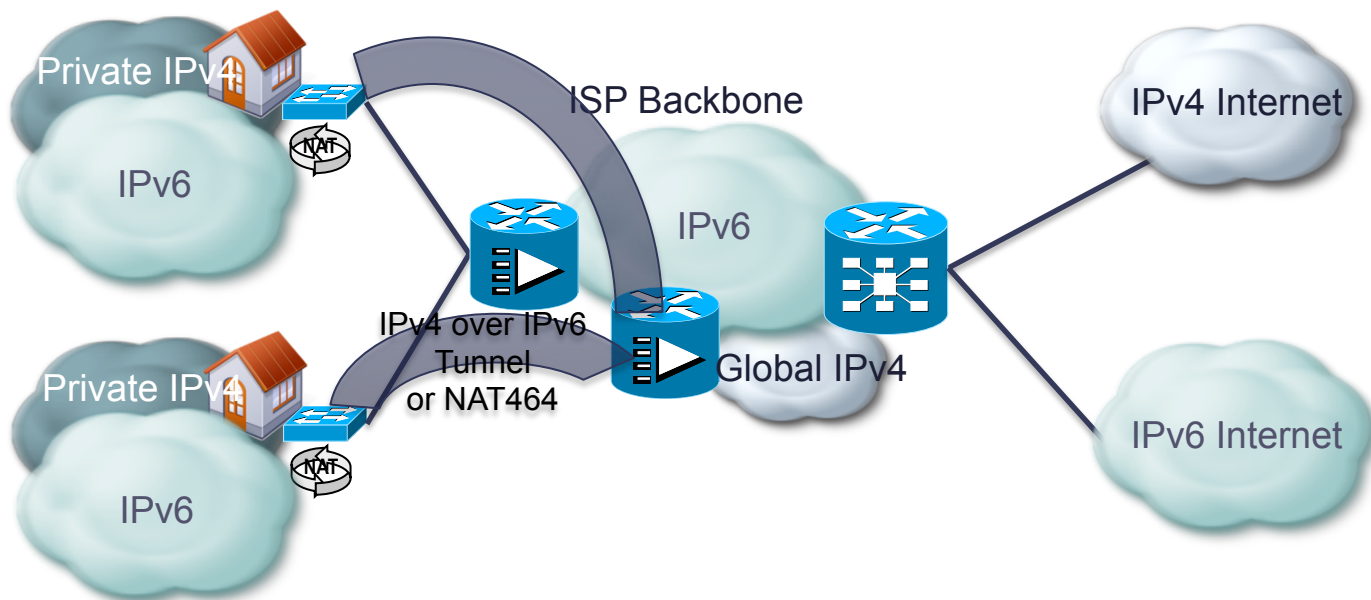
Native IPv6接続

Step.2+ CGNの導入



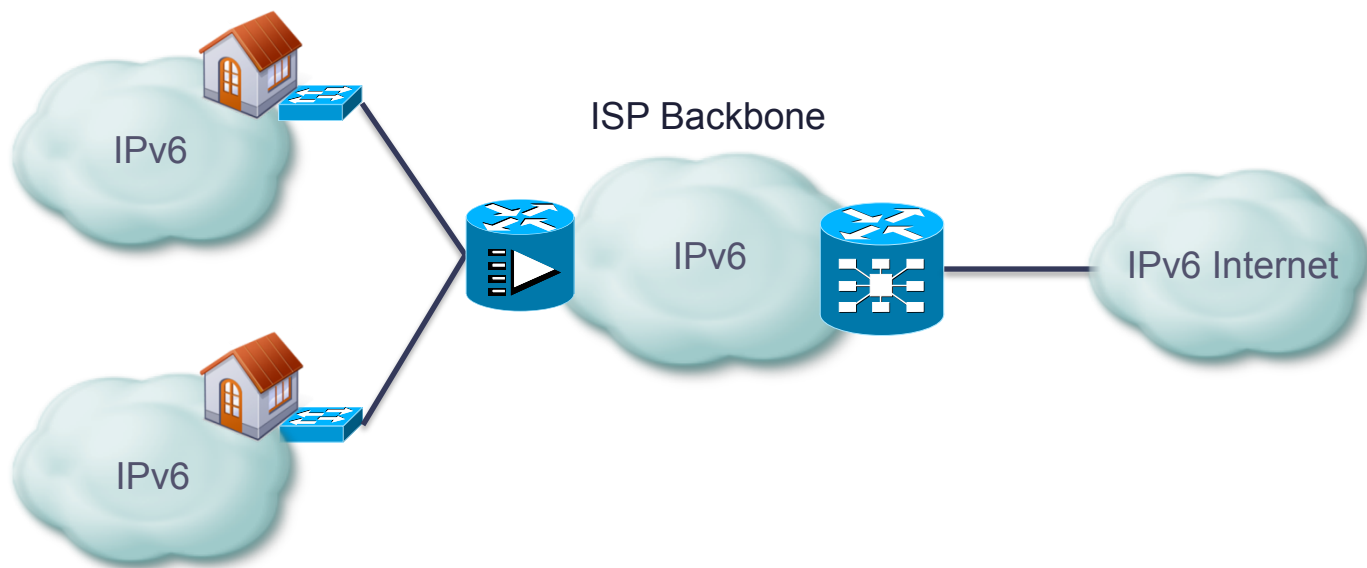
CGNの使用による
IPv4 Dual NAT接続

Step.3 IPv4接続をOverlayに移行



IPv4 Backboneを極小化し、IPv6インフラ上でIPv4接続
CGNを併用することもあり

Step.4 IPv6に移行

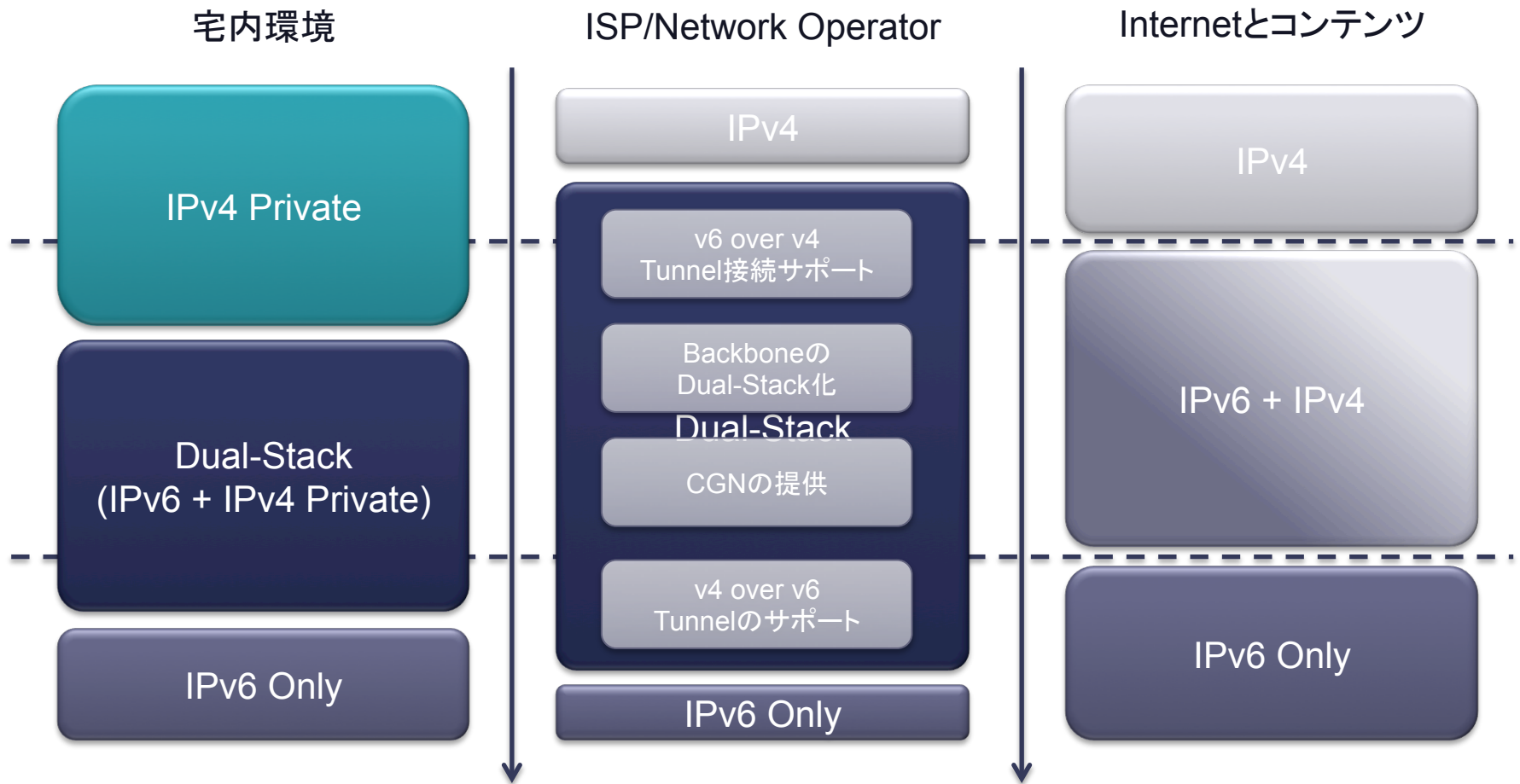


すべてのアプリケーション
がIPv6を使用する

- アクセス環境の変遷
- 移行のための要素技術
 - StatefulとStateless
- 各種移行技術の紹介

必要な技術と標準化

アクセス環境の変遷



移行のための要素技術

- すべてのrouting nodeをDual-Stack化すると、運用コストが上昇する
 - Tunneling/Translation技術とNATを組み合わせて、効率化をはかる
 - MPLSなどの基幹ネットワーク技術を併用することも可能
- 基幹ネットワークにおける加入者の状態保存
 - インターネットでは、中継ノードで利用者の状態を保持しないことが基本とされているが、NAT等の導入により状態保持の必要性が発生した
 - 状態を保持することで加入者単位の管理を行うことも可能
 - 一方で、状態を保持することで、加入単価の上昇、スケータビリティの低下を招く恐れがある

中継ノードが状態を、

保持する方式 → Stateful方式

保持しない方式 → Stateless方式

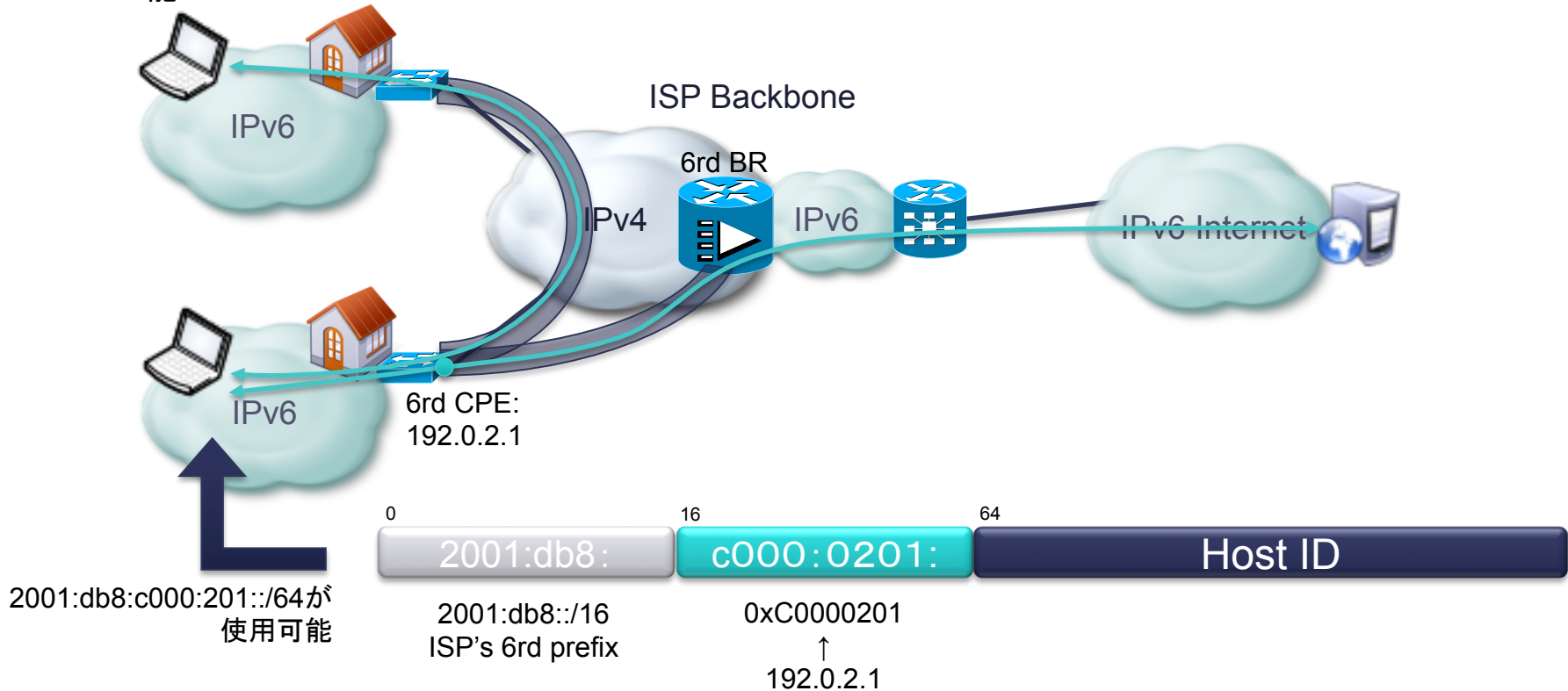
StatefulとStateless

	IPv6 over IPv4	IPv4 over IPv6
Stateful	IP in IP configured Tunnel GRE PPPoE + L2TP Etc....	DS-Lite (RFC6333) 464XLAT
Stateless	6to4 / 6rd	MAP-E/T 4rd Etc...

一般的には、Statefulの方がより管理しやすく、Statelessの方がよりスケーラブルなソリューションになる

6rd – IPv6 Rapid Deployment (RFC5969)

- 6to4(RFC3050)をベースに、任意のprefixを使用可能にしたstateless tunnel
- 6rd CPE間で直接通信することが可能
- IPv4 addressをIPv6 address中に埋め込むことにより実現するが、一部を”省略”することも可能

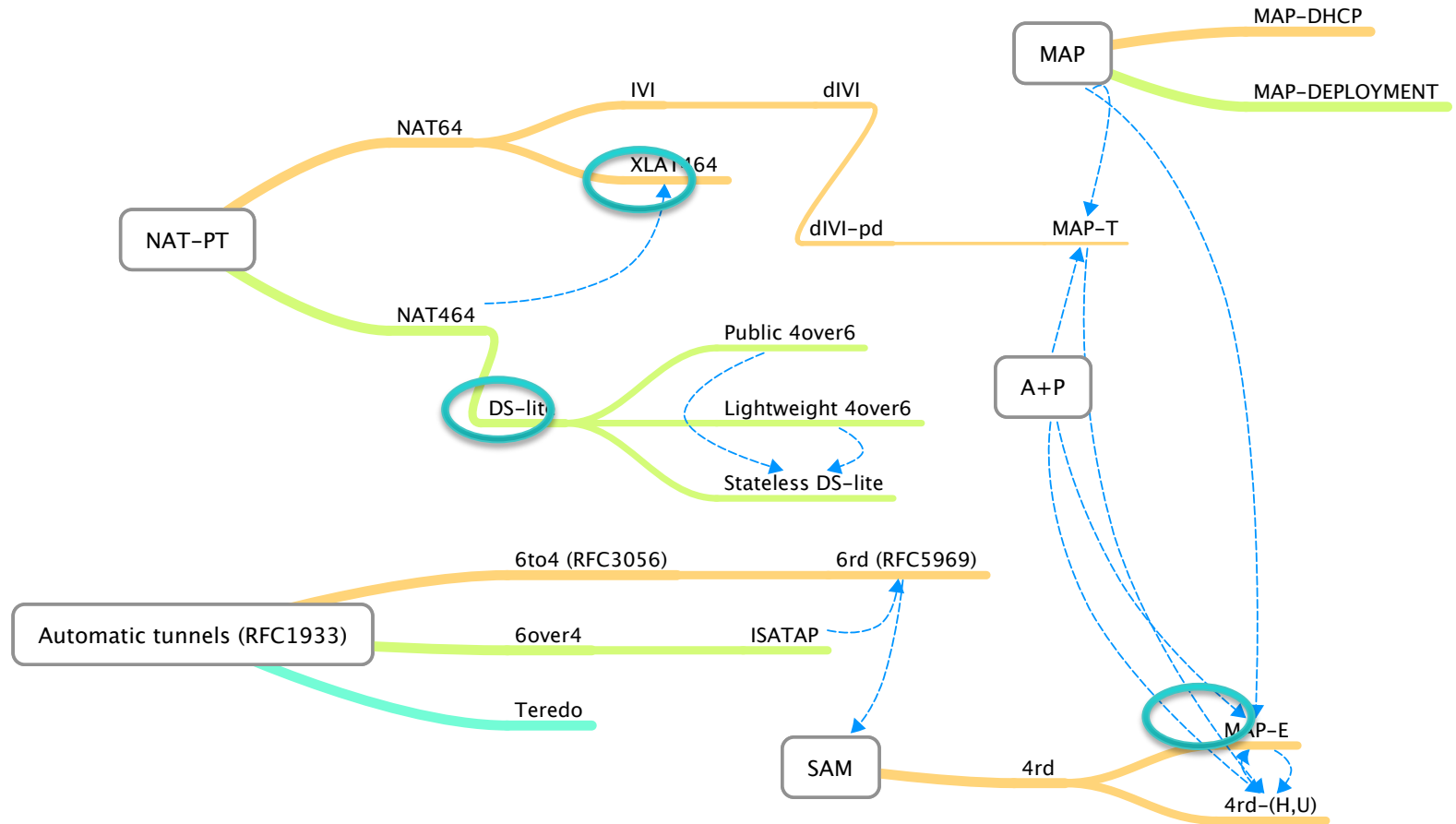


IPv4 over IPv6 – Protocolのカテゴリ

	Stateless	Stateful
Encapsulation	MAP-E	DS-Lite / LW 4 over 6
Translation	MAP-T	464XLAT

IPv4 over IPv6 – 標準化の変遷

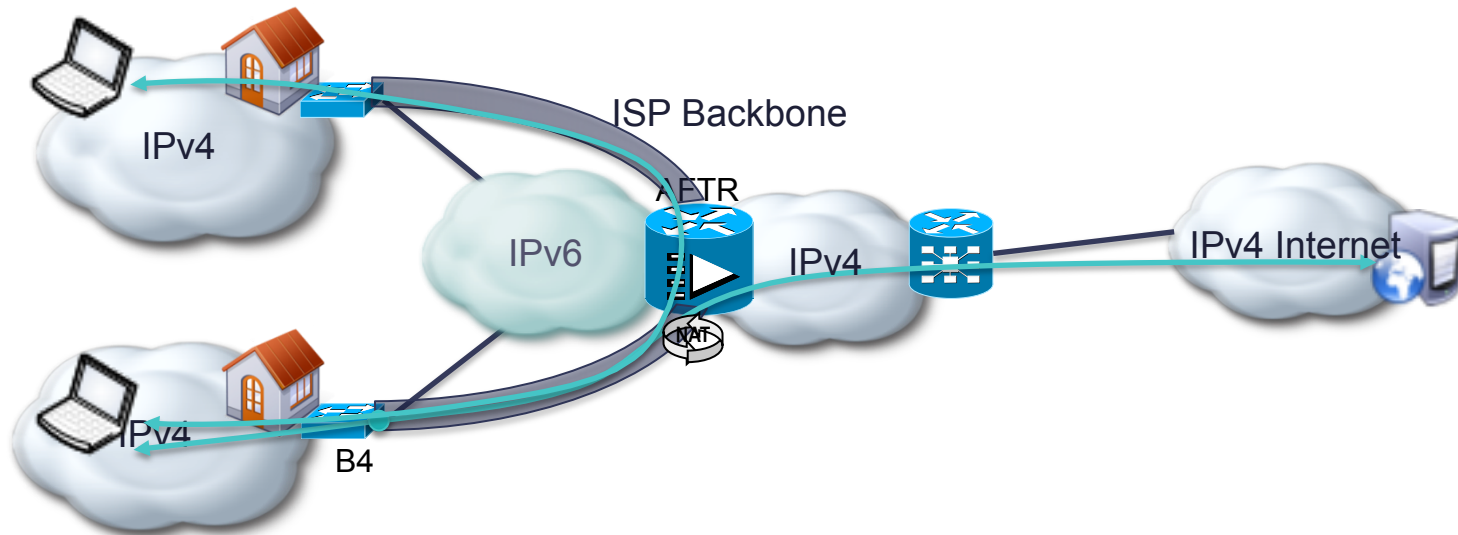
by Ole Troan, Cisco Systems, Softwire WG, IETF



Source: <http://tools.ietf.org/agenda/83/slides/slides-83-softwire-10.pdf>

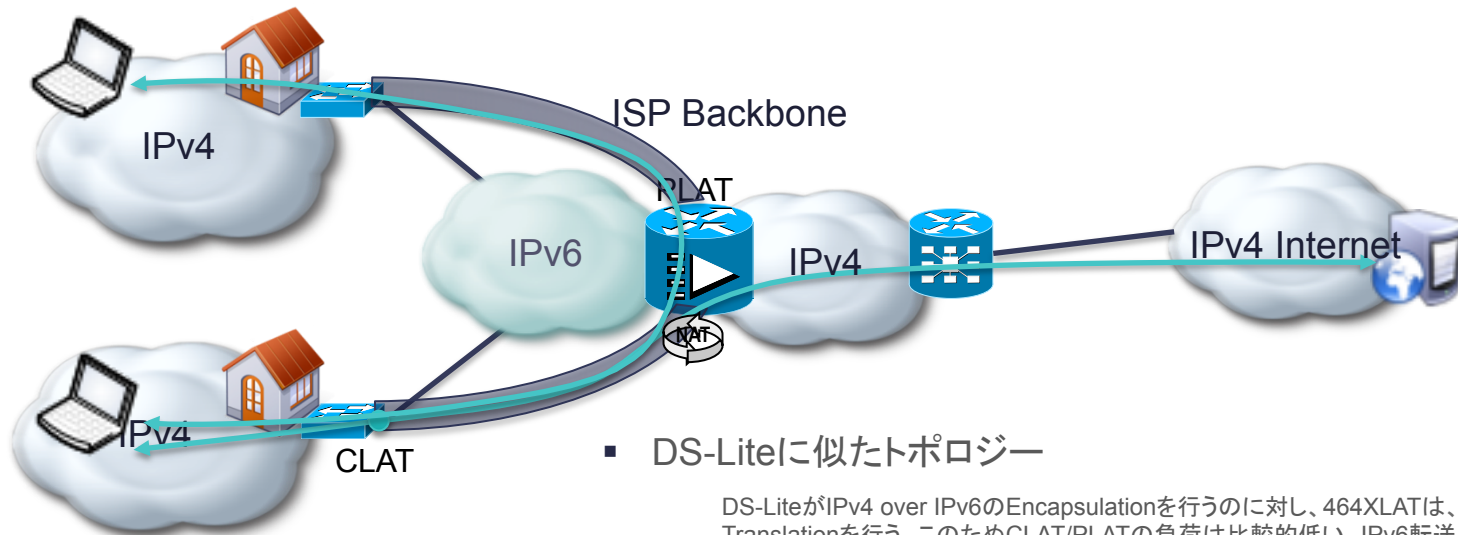
DS-Lite – Dual Stack Lite (RFC6333)

- ISPが設置したトンネル終端装置は、CGNも実装し、トンネルの端点(CPE)のIPv6 Addressで加入者を識別する
 - DS-LiteのCPEは”B4”、トンネル終端装置は”AFTR”と呼ばれる
 - Statefulだが、比較的状态保持の負荷は低い



464XLAT – Stateless + Stateful XLAT

- CPE側でStateless XLAT(RFC6145)、ISP内でAddress共有型Stateful XLAT(RFC6146)を行うことでIPv6上でIPv4 Trafficを転送する
 - 既に標準化作業が完了している2つの技術を組み合わせて実現している
 - この組み合わせでの利用法も”Best Current Practice”としてRFCされる見込み
 - (XLAT: Translation)



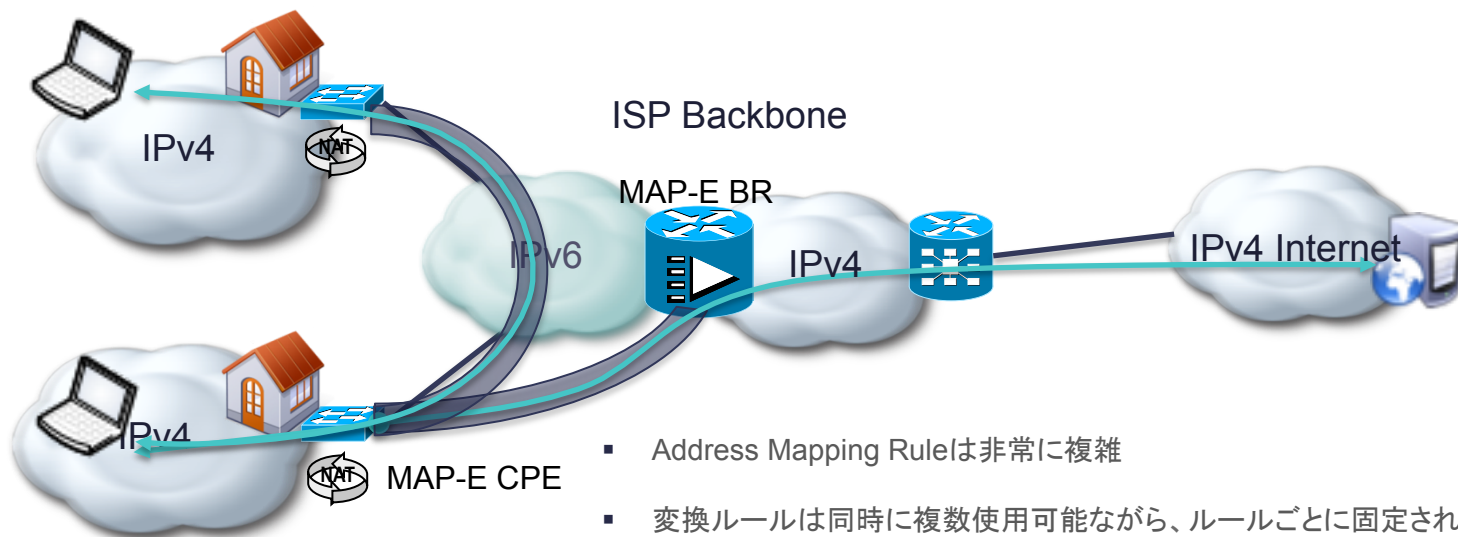
■ DS-Liteに似たトポロジー

DS-LiteがIPv4 over IPv6のEncapsulationを行うのに対し、464XLATは、v4/v6 Translationを行う。このためCLAT/PLATの負荷は比較的低い。IPv6転送区間のペイロードも小さく、シンプルな転送が可能。

- CLAT/PLATはそれぞれ単独でNAT64のTranslatorとしても動作可能

MAP-E – Mapping Address and Port

- IPv4アドレスの一部と使用可能なポート番号レンジをIPv6アドレスに埋め込むことで状態を保持することなくIPv6インフラ上でIPv4トラフィックの転送を行う。
 - CPE単位で使用できるポート範囲が固定されているため、NATは常にCPEで行う(ただしPort Restricted NAT)
 - CPE間で直接通信が可能
- MAP-Eはトンネリング(Encapsulation)を行うが、同様の仕組みをTranslationで行うMAP-Tも存在する。



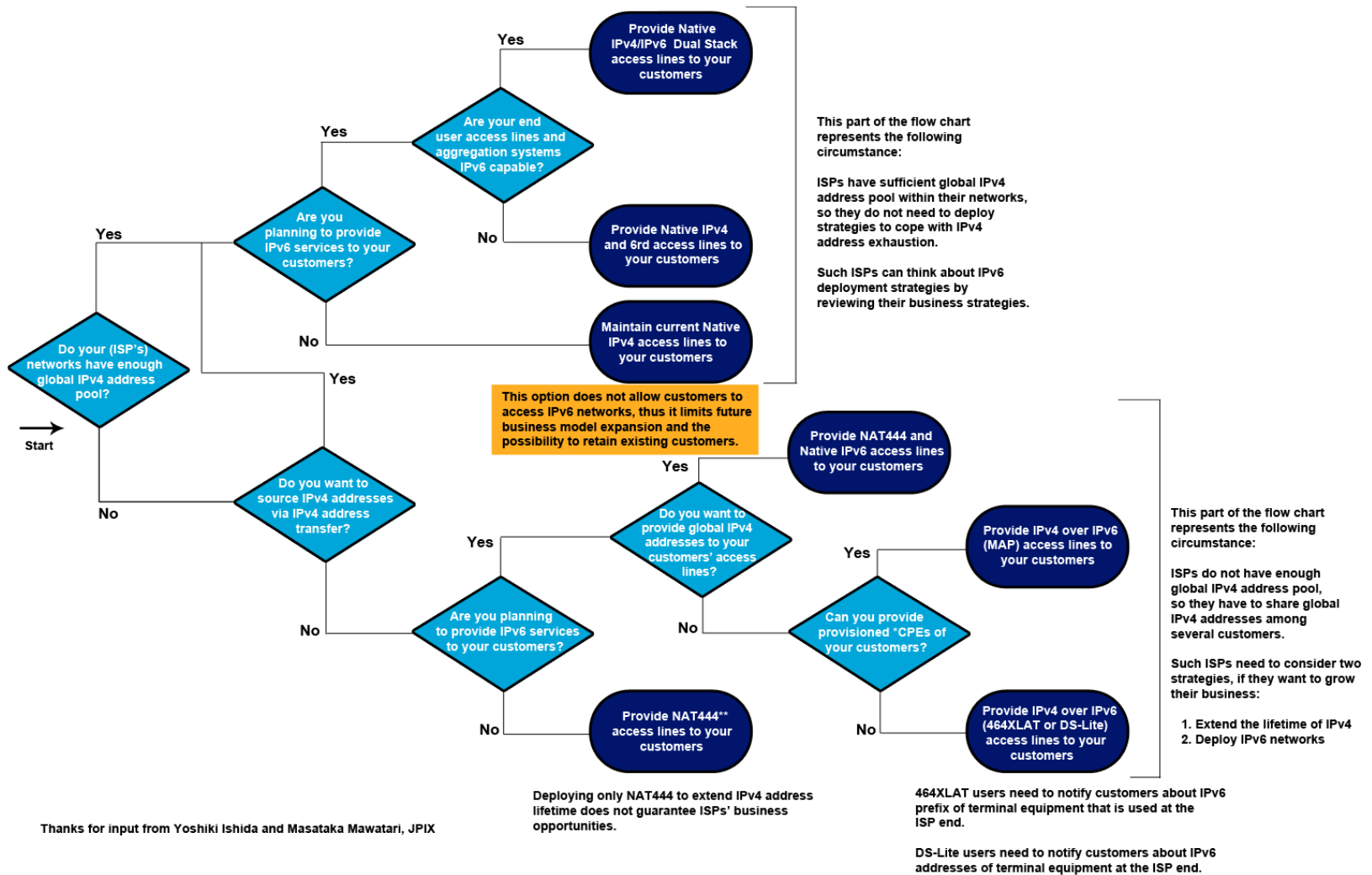
- Address Mapping Ruleは非常に複雑
- 変換ルールは同時に複数使用可能ながら、ルールごとに固定されているためIPv4アドレスの使用効率はやや低い
- IETFにおける標準化作業が進められているが、非常に多くのバリエーションが存在し、現在はMAP-EがStandard Trackとされている

MAP-T, 4rd(-U)はExperimental

まとめ – 移行技術の選択

- 移行技術はDual-Stackの実現方法とNATの配置がポイントになる
- Dual-Stackを実現するために、オーバーレイ技術等を活用して柔軟な構成を検討する
 - 非常に多くの方式が存在するため、それぞれの環境への適合性や、標準化動向を十分考慮する
- NATの配置は慎重に検討する
 - 将来的になくなるべきもの
 - 設置箇所によりネットワーク構成に影響

参考 – IPv6 decision flowchart



Source: http://www.apnic.net/community/ipv6-program/ipv6-cto/IPv6_decision_flowchart.png

- IPv4との違い
- IPv6に固有の課題
- IPv6とセキュリティー

IPv6におけるセキュリティー

IPv4との違い

- 根本的には同じもの
 - アドレス空間の大きさや、Protocolの構造に起因する差異は存在しますが、IPv4とIPv6には根本的なセキュリティーの性質の差はそれほど大きくありません。
 - (例) L2アドレスの解決・Spoofing・Source Routing・Routing Protocol・Application・DoS
- IPsecの幻想
 - IPv6の標準的な実装ではIPsecが必須ですが、これはセキュリティーが担保されていることを意味するわけではありません。IPsecを使用することが有効でないケースも多数存在します。またIPsecはIPv4でも使用可能です。

多くの場合IPv6でもIPv4と同じ手法で対策をとることが可能です。

IPv6に固有の課題 – アドレス空間

- IPv4と比較して非常に大きなアドレス空間を持つIPv6は、大きさ自体に起因するいくつかの違いがあります。また、明確なアドレス・スコープの区別が存在することも大きな差異の一つです。
 - ✓ 攻撃対象の選定
 - 例えば、攻撃者がその対象をしらみつぶしに見つける様なタイプの攻撃を行うためには、より多くの労力が必要となります。
 - 逆に、空間の大きさに余裕があるため、常に同じアドレスを使用することが多いと考えられます。この問題への対応として、プライベート拡張機能も利用可能ですが、安全性が高まる反面、管理が大変になってしまうデメリットもあります。
 - ✓ Link-Local アドレス
 - Link-LocalアドレスはOn-Linkのみで使用できます。この特性を利用することで外部との通信を制御することも可能です。

IPv6に固有の課題 - Protocol

- ICMP, NDP, ARP
 - IPv4のARPに相当する機能は、整理統合されておりARP単体では存在しません。
 - Plug-and-Playを実現するための機能が追加されており、セキュリティーとして考慮すべきIPv6とIPv4が大きく異なっている箇所と言えます。
- 拡張ヘッダとフラグメント
 - 拡張ヘッダのチェーンに制限がないため、チェックする機構のスケーラビリティに影響を与えます。またフラグメントが発生していると、さらに複雑なチェックメカニズムが必要になります。

IPv6に固有の課題 – 運用性

- 現実的な運用としてIPv4と違いを認識すべきものが存在します。
 - ✓ 運用データベース
 - Spam DatabaseなどIPv6では未整備のものが存在します。
 - ✓ Path MTU Discovery
 - PMTUdは、ICMPを使用して実現されています。一部IPv4で行われている様な、セキュリティーを目的として全てのICMPを通過させない様な運用は接続性に影響を与えます。
 - ✓ Dual-Stack/Tunnel over IPv4
 - IPv4/IPv6それぞれのセキュリティーを考えなくてはいけないのは、もちろんのこと、移行手段としてのTunnel技術は管理が複雑になりがちで、セキュリティーの低下が懸念されます。
 - ✓ ノウハウとトレーニング
 - 運用自体の経験の少なさから生じる問題は最も大きな課題といえるでしょう。同様にトレーニングの不足もこれを助長します。
- Topologyの隠蔽
 - IPv4ではNAT/NAPTの使用が一般的であるため、Topologyが隠蔽されていることが前提とされた運用が行われていることがあり、注意が必要です。

IPv6とセキュリティ

- IPv6は多くの面で、アドレス空間の大きなIPv4と捉えることができます。そしてセキュリティの観点では両者にそれほど著しい差異はありません。
 - Link-Local Addressのように、大きくセキュリティが向上しているものや、拡張ヘッダのように取り扱いが難しいものも存在します。
 - すべてでIPsecを使用するといったような、誤った認識も改める必要があります。
- 最も危険なのは、運用経験やトレーニングの不足が不足していることが根本的なセキュリティ脅威の原因になってしまうことです。

まとめ - 移行・共存のためのデザイン

IPv6対応と事業継続性への影響

IPv6導入のMotivation

企業ネットワークにおけるIPv6の導入

移行のステップ

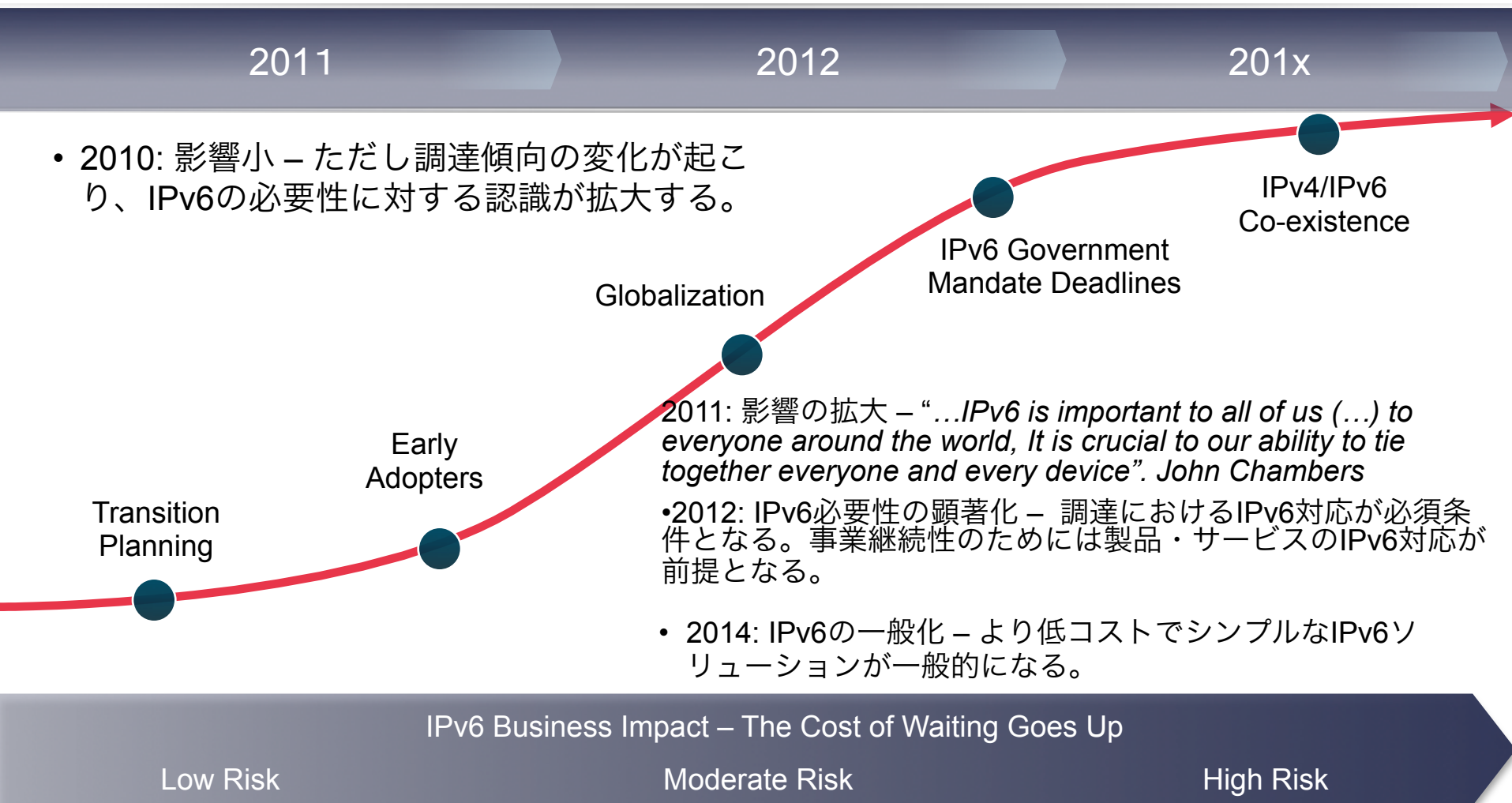
IPv6の実ネットワークへの導入

いつIPv6を導入すべきなのか？

- IPv6対応と事業継続性への影響
 - IPv6導入のMotivation
- 企業ネットワークにおけるIPv6の導入
 - 移行のステップ
 - IPv6の実ネットワークへの導入
 - いつIPv6を導入すべきなのか？

移行・共存のためのデザイン

IPv6対応と事業継続性への影響予測



IPv6導入のMotivation

外的要因

成長/投資保護

- IPv4 addressが枯渇してもInternetの成長傾向は継続する。
- エンタープライズには市場の維持・拡大が必要。

パートナー

- パートナー或は競合のIPv6導入
- 政府機関・業務提携先によるIPv6の要件

OS

- ほとんどのOSが標準的にIPv6をサポート
- OSサポートの一部のProtocolがIPv6専用の物も登場

旧来の問題

- 企業買収・統合によるネットワーク拡大
- NATによる技術的制限

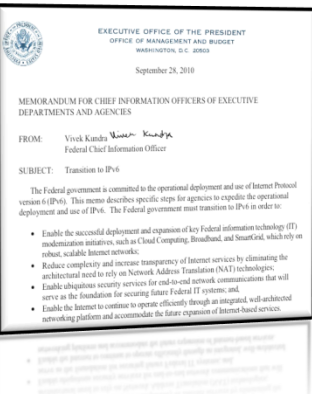
新テクノロジー

- サーバーの仮想化
- IoT / Sensor Network

内的要因

IPv6普及の流れ

US Federal, OMB Mandate



主要なコンテンツ
プロバイダが
1日IPv6でサービ
スを提供!
業界全体の大き
な自信に

ISP:
1%の加入者がIPv6加入
新規ユーザーはIPv6サービ
スがdefault
主要コンテンツプロバイダ:
IPv6 in production.

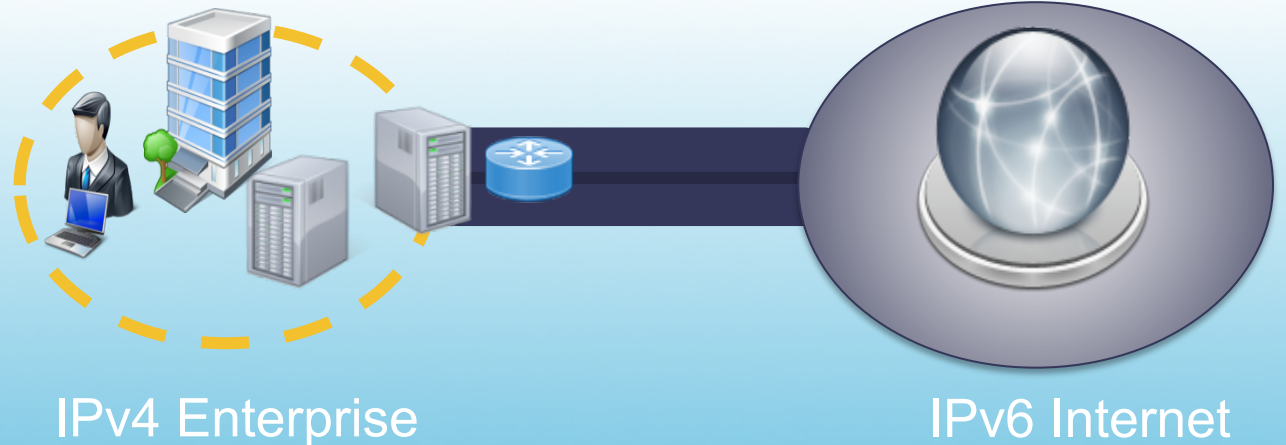
2014年。日本国内でも本
格的な普及期が訪れる!
か?



企業ネットワークにおけるIPv6の導入

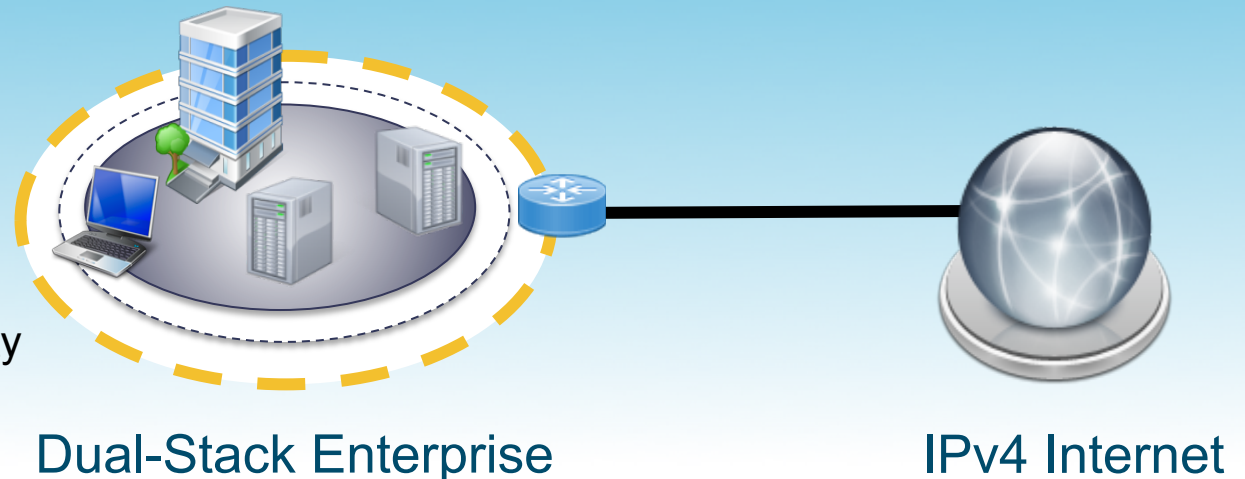
Outside – In

- インターネットの革新
- ビジネス持続性
- B2C, B2B



Inside – Out

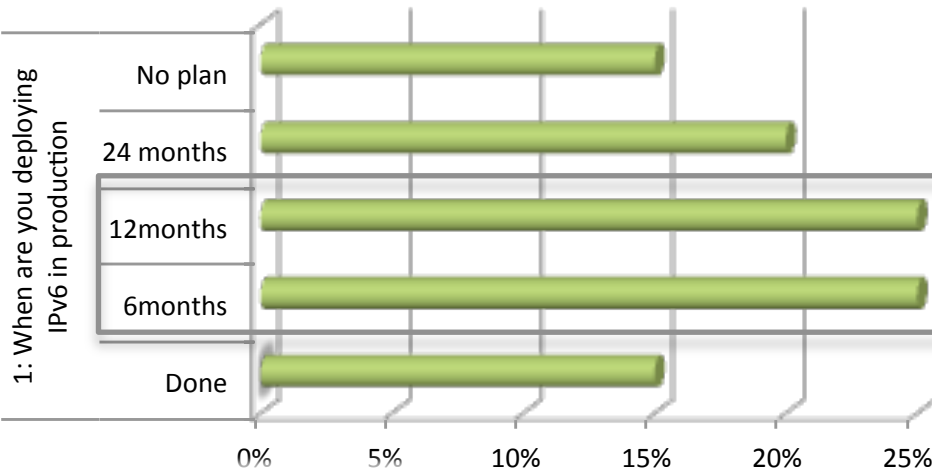
- 国際化
- 技術的優位性
- 業界によっては必須
- BYOD-Security-Visibility



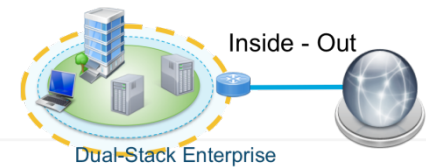
http://www.cisco.com/en/US/netsol/ns817/networking_solutions_program_home.html

IPv6の実ネットワークへの導入 - アンケート結果

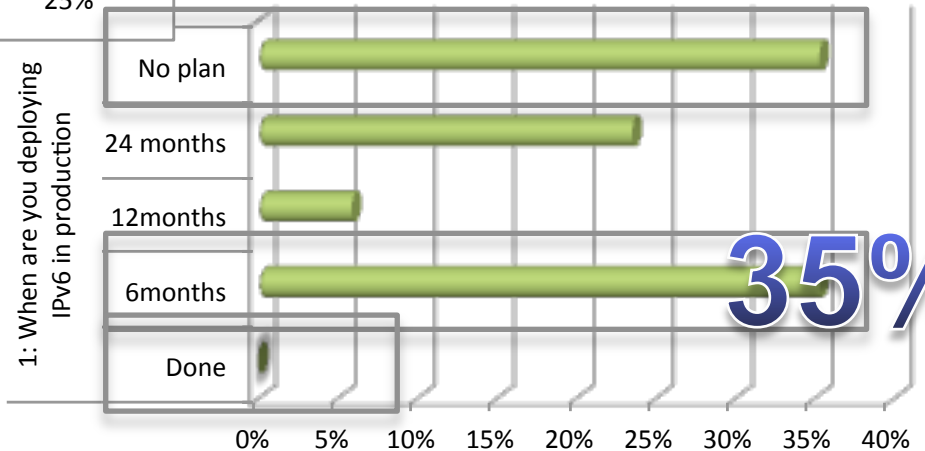
Internet Presence



50%



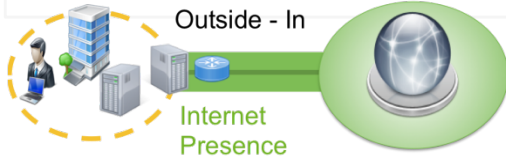
Internal Network



35%

Outside - In

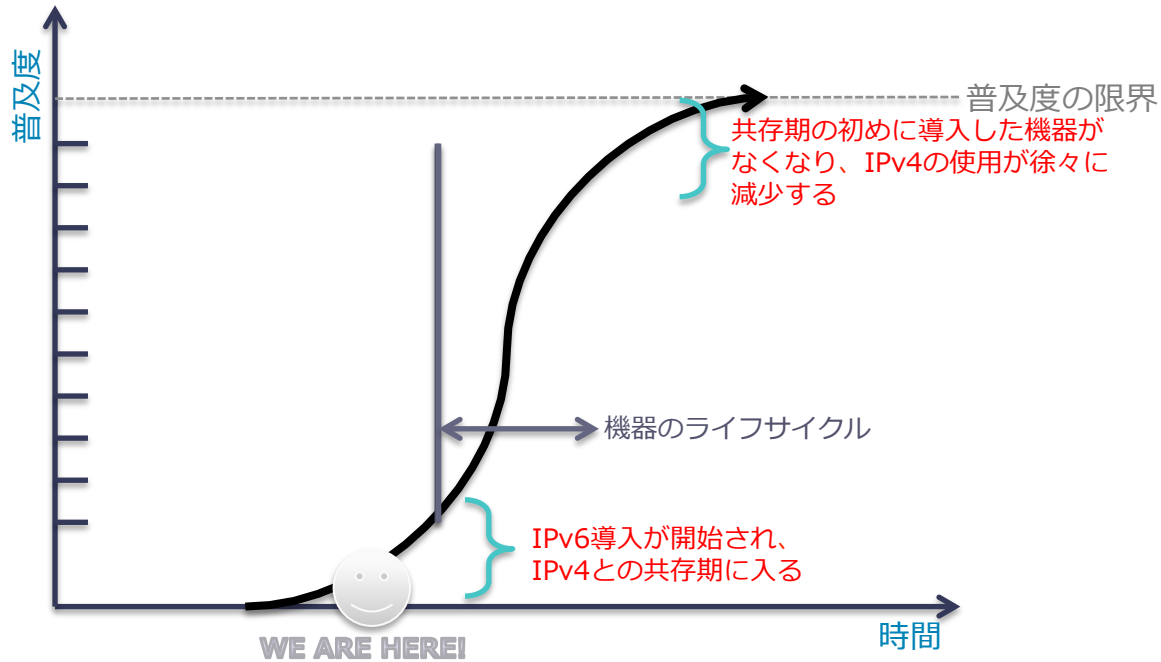
Internet Presence



いつIPv6を導入すべきなのか？！

“Adoption follows an S curve”

より多くのユーザーが利用することで、普及が加速される。



全世界での普及度12~13%

Thank you.

