NATのご利用は計画的に

■ ISPにおけるLSN導入に関する技術的課題

JANOG24 Meeting in TOKYO

2009/07/10(Fri)

イッツ・コミュニケーションズ株式会社

芦田宏之

Agenda

- 自社紹介
- IPv4アドレス枯渇とLarge Scale NAT (背景)
- LSNと技術的課題
  - ポート数制限
  - 他
- LSNを投入するタイミング
- まとめ
- 議論

自社紹介

勤務先

イッツ・コミュニケーションズ株式会社

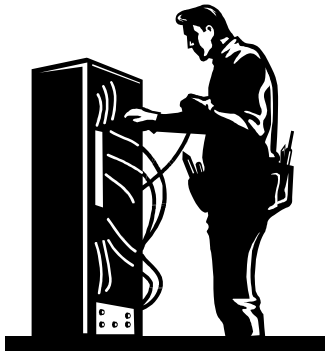
its communications Inc.

旧社名 = (株)東急ケーブルテレビジョン

- 事業エリア = 東急電鉄沿線
  - 渋谷区、世田谷区、目黒区、大田区、町田市
  - 川崎市(高津区/中原区/宮前区)
  - 横浜市(港北区/都築区/青葉区/緑区)
- (都市型)ケーブルテレビ事業者
  - 有線テレビジョン放送事業
  - 電気通信事業(ブローバンドアクセスISP)

何でNATの話?

- 自社にNATedサービス
  - 商用のNAT設備を構築・運用する立場
  - 過去の商品と互換性維持のため継続

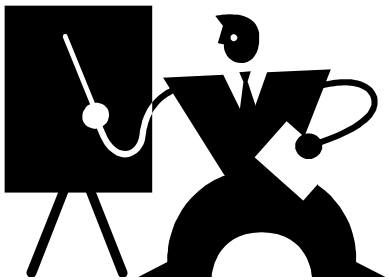


- LSN, NAT444に関わる各種提案活動
  - JPOPM13, APNIC25

    AP地域LIR共同利用IPv4アドレス空間の新設
  - IETF

    draft-shirasaki-isp-shared-addr

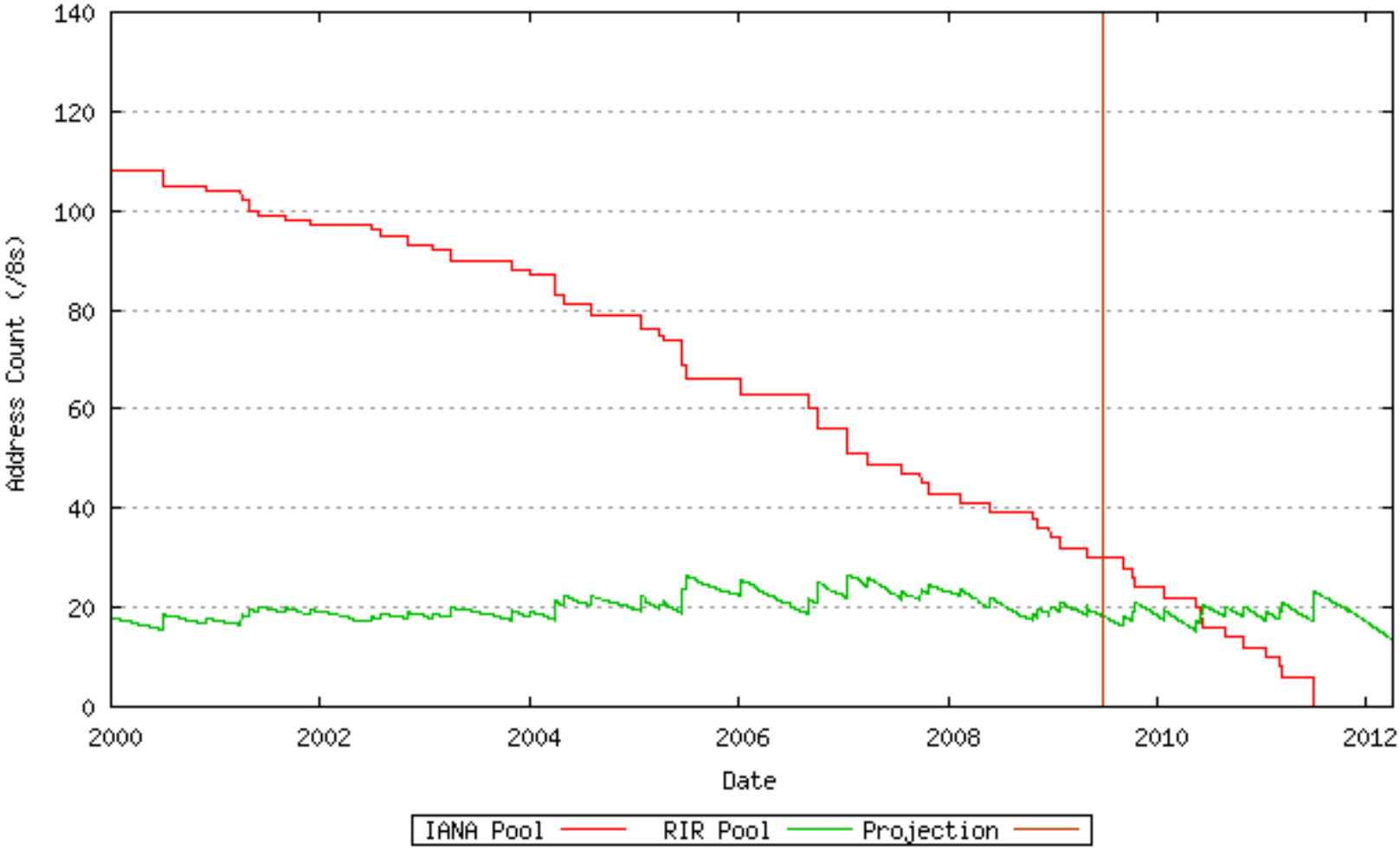
    draft-shirasaki-nat444-isp-shared-addr



IPv4アドレス枯渇と Large Scale NAT (背景)

背景(1) IPv4アドレス枯渇

Geoff Huston 氏による枯渇予測グラフ



※ http://www.potaroo.net/tools/ipv4/ より

背景(2) 総務省報告より

インターネットの円滑なIPv6移行に関する調査研究会 報告書（総務省、2008/6/17）

3. アドレス枯渇対策への対応方策

表 3－1 対応方策の比較

	NAT/NAPT の利用	割り振り済みの IPv4 アドレスの再配分	IPv6 への移行
期限内での方策実現可能性	○	疑問	極めて困難
サービスの継続性	制限が生じる	○	○
効果の永続性	疑問	×	○

※http://www.soumu.go.jp/menu_news/s-news/2008/080617_2.html より

背景(3) IPv4アドレス枯渇対応TFアンケート

IPv4 EXHAUSTION

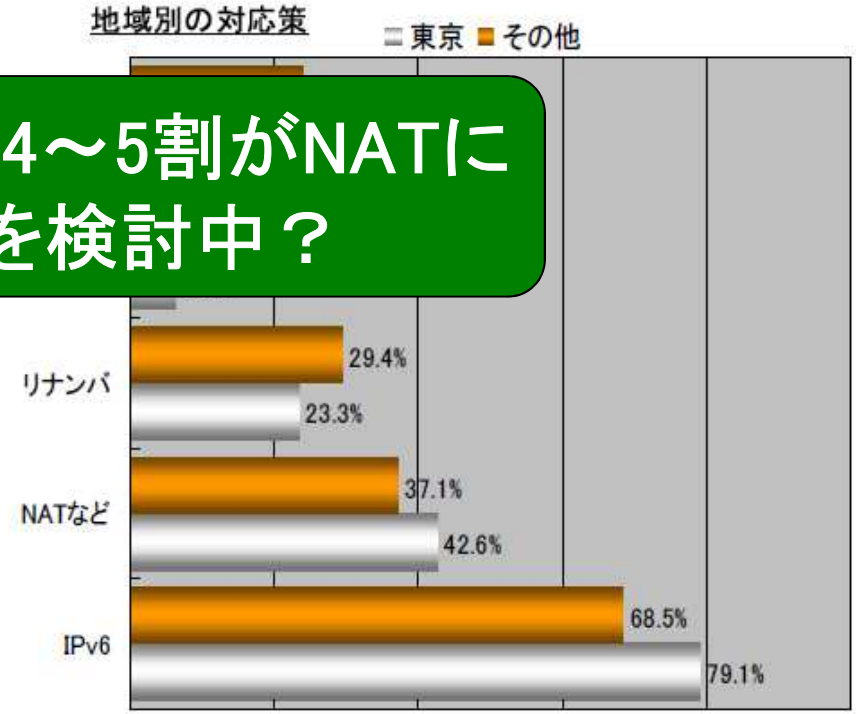
検討中の対応策

サービス事業者と製造、SIerで
IPv6導入に差があり(*)
地域別でも対応策に若干の差

Q:現在IPv4アドレス在庫枯渇への具体的な対応策として現在検討、あるいは検討予定のものがあれば選んでください。(複数回答可)

	IPv6導入	NATなどv4アドレスの効率利用	リナンバなど既存NWから	その他	対応策未検討
通信事業	81.5%	48.1%	3		
ISP	86.6%	43.3%			
ASP・CSP	66.7%	40.0%	2		
iDC事業者	78.3%	47.8%	39.1%	8.7%	17.4%
放送事業(CATV)	81.5%	51.9%	25.9%	3.7%	14.8%
ソフトウェア製品	62.5%	12.5%	0.0%	0.0%	37.5%
通信機器製造業	56.7%	23.3%	6.7%	0.0%	36.7%
その他製造業	70.0%	50.0%	20.0%	0.0%	10.0%
SIer	55.0%	30.0%	15.0%	5.0%	35.0%
	72.7%	39.3%	26.2%	4.4%	19.6%

事業者の4～5割がNATによる対応を検討中？



枯渇対策進捗アンケート報告(2009/05/18)

※http://www.kokatsu.jp/blog/ipv4/data/kokatsu-research-200904.pdf

2001:db8:1256:a4da::9

背景(4) JANOG22での議論

IPv4アドレス販売終了のお知らせ?

宍倉さん(NTT.com)、西谷さん(NTT.com)、佐藤さん(コナミ)

- ISPによるNAT検討状況
- ISPのNATによる影響
  - パケットを改変するために起こる問題 = 利用不能なアプリ
  - IPアドレスをユーザ識別子として使えない
    - POP before SMTP破綻
    - アクセスフィルタの影響(アドレスを共有するユーザ巻き添え)
- LSN(旧称Carrier Grade NATの要件
- NATの分類: フルコーン、制限付きコーン、シンメトリック
- NAT越えの技術

http://www.janog.gr.jp/meeting/janog22/program/day1/day1-5.html

本当にLSN導入しますか?

- 本音: できることなら避けたい、本質解はIPv6
- 実際: 必要に迫られて導入を検討

- IPv4を無効にできない = IPv6 onlyでは生活できない
  - 大多数の対地はIPv4のまま
  - IPv4アドレス枯渇後も加入は続く
  - Windows XP (DNSトランスポートがIPv4のみ) 問題

導入して本当に大丈夫なのか?

ネットワークオペレータは何を準備すべきなのか?

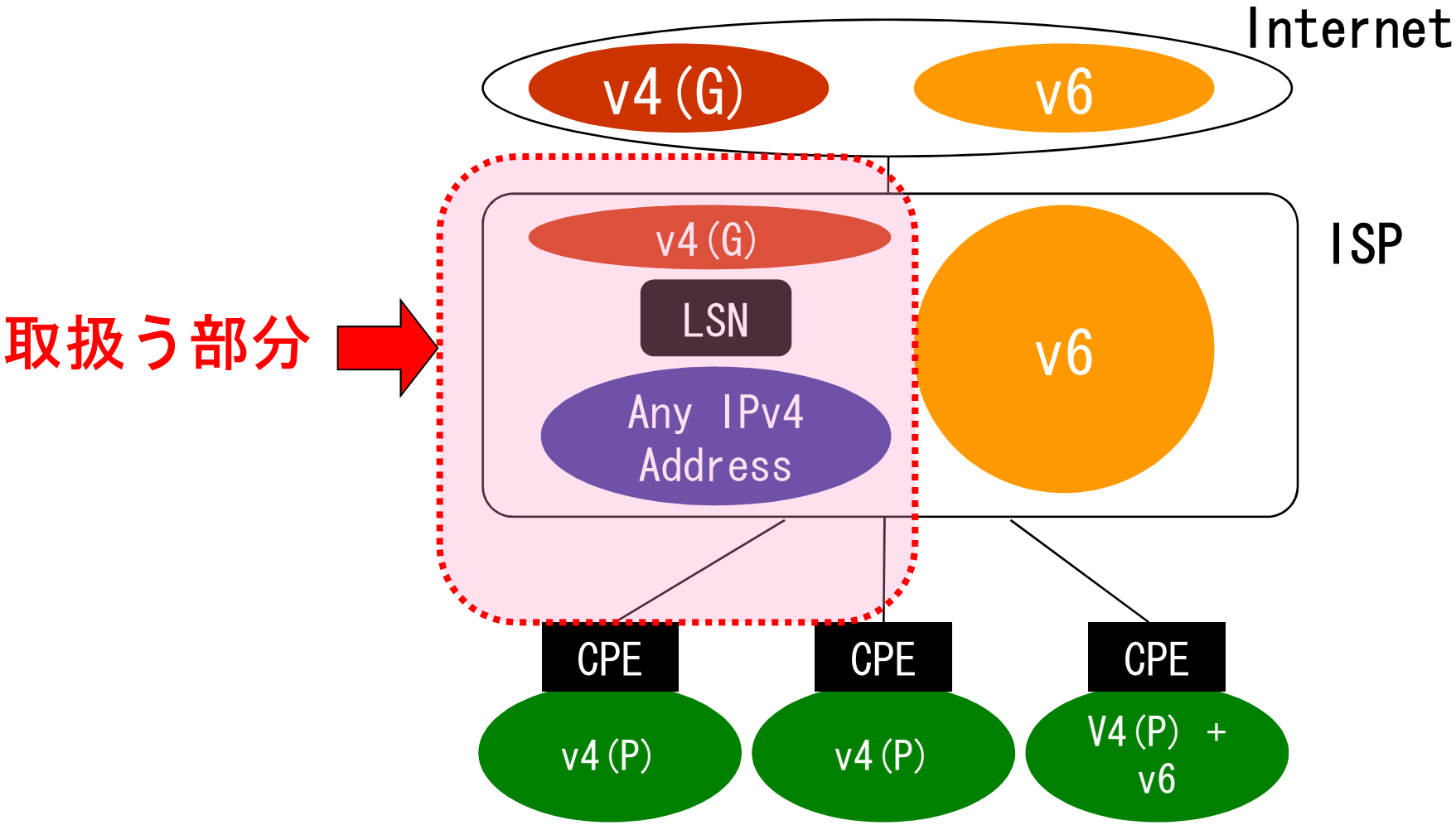
LSNと技術的課題

LSNと技術的課題

- ポート数制限（欠けるGoogleマップ）
- 利用者特定
  - ログ用ストレージ
- ルーティング
- IPアドレス
- 冗長、HA

前提とするネットワークモデル: NAT444

IETF74 OpsArea KDDI中川さん提案資料より



http://www.ietf.org/proceedings/09mar/slides/opsarea-2/opsarea-2_files/v3_document.htm

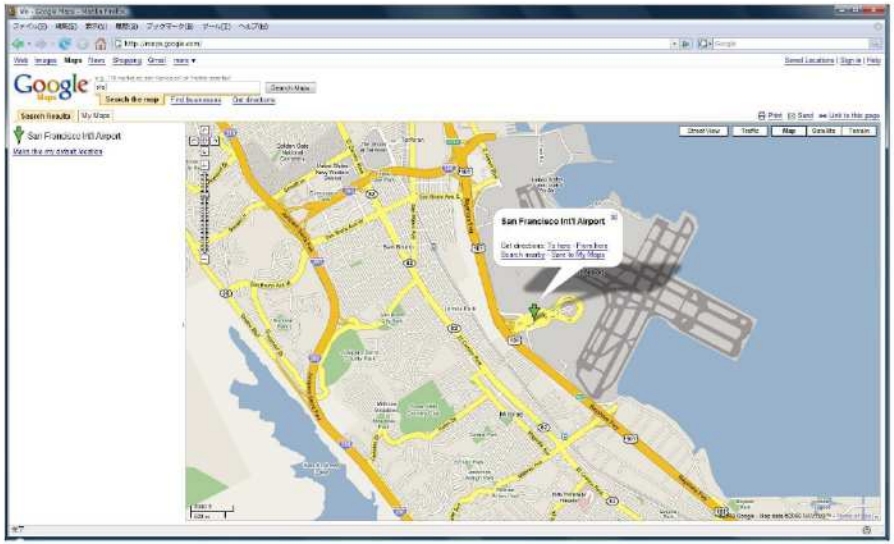
LSNと技術的課題

- ポート数制限（欠けるGoogleマップ）
- 利用者特定
  - ログ用ストレージ
- ルーティング
- IPアドレス
- 冗長、HA

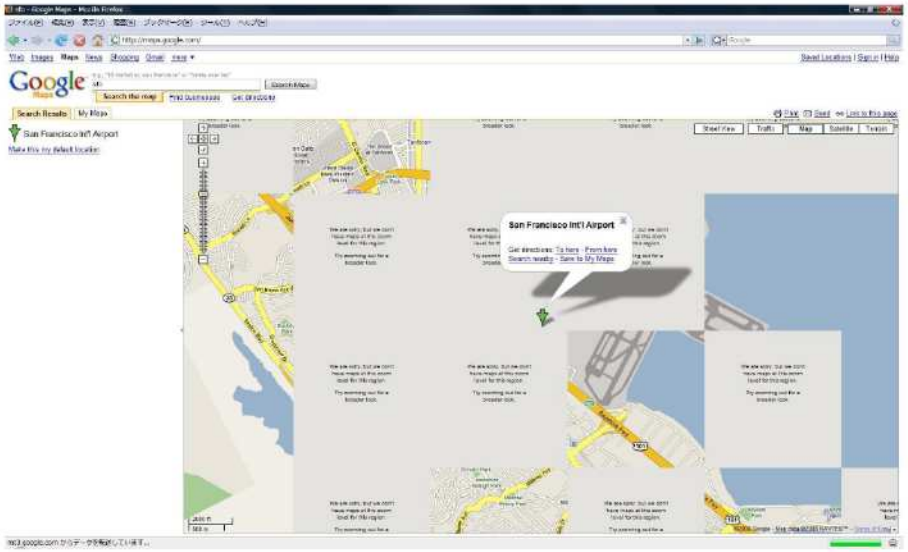
ポート数制限: 欠けるGoogleマップ

- NTT.com宮川氏による発表(IETF72 PLENARY)
- INTEROP Tokyo 2009 枯渇TFブースにてデモ

Max 30 Connections



Max 15 Connections

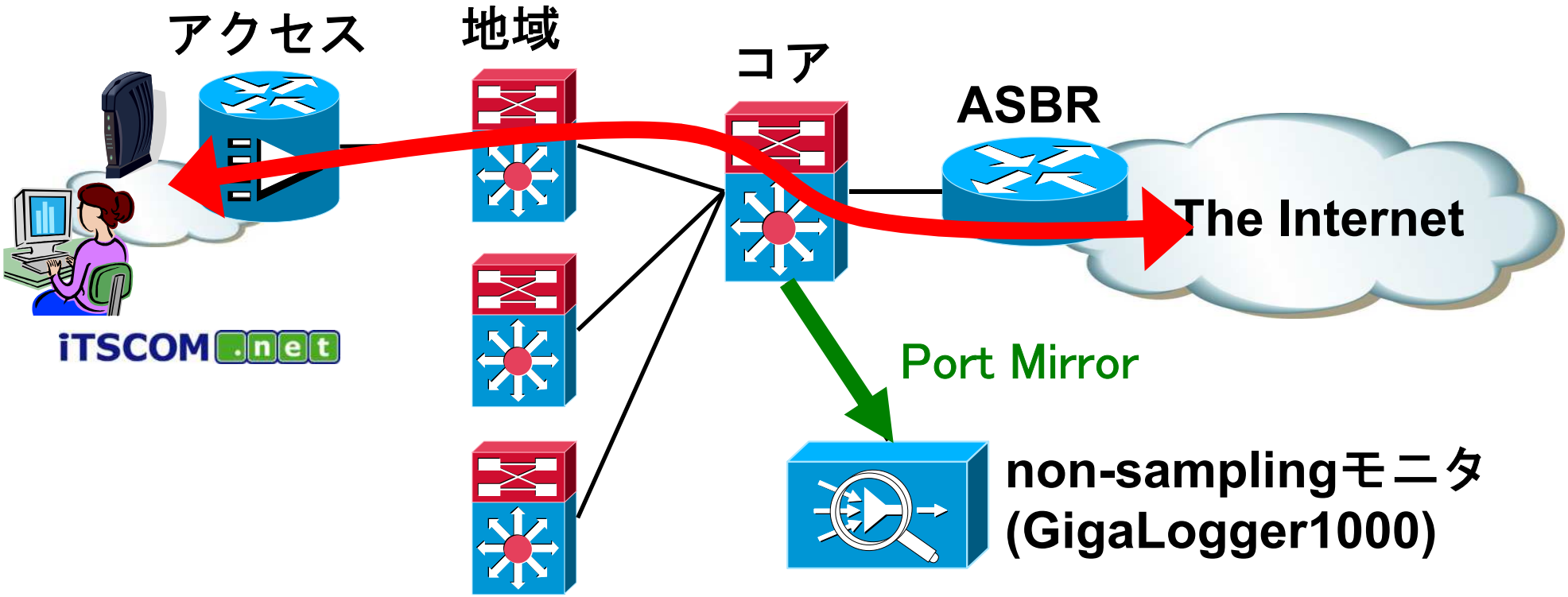


※ http://www.nttv6.jp/~miyakawa/IETF72/IETF-IAB-TECH-PLENARY-NTT-miyakawa-extended.pdf より

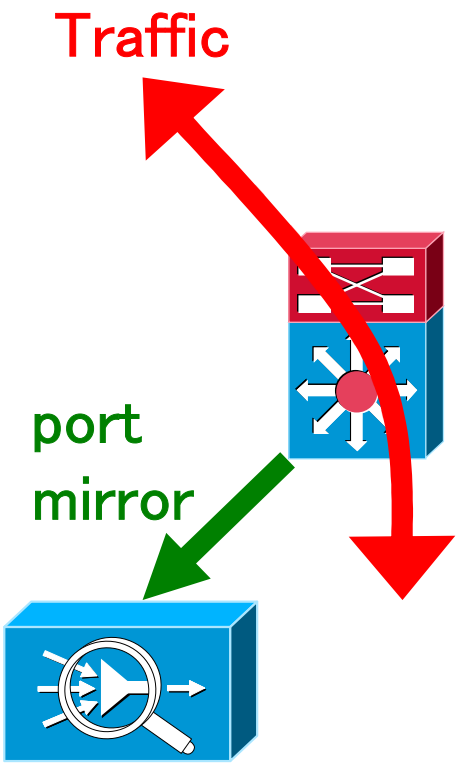
ポート数制限: 本当に起こるのか?

- 現用のNAT装置から得られるデータで大丈夫?
  - 低速商品限定、旧サービスからの移行が主
- 今ドキのブロードバンドアクセスの傾向は?

⇒ 実トラフィックをノンサンプリングフロー分析



セッション数カウントの前提条件



- TCP
  - セッションopen: SYNをカウント
  - セッションclose: FINをカウント
    未使用のまま10分経過
- UDP
  - セッションopen: パケット通過
  - セッションclose: 未使用のまま1分経過
- ICMP, 他プロトコル
  - ノーカウント

現実のLSNの実装を模倣したものではなく、
参考値をカウントするための割り切り仕様

ポート数について考察

- 1ユーザあたり平均50～300セッション程度
  ⇒条件によりかなりバラツキがある

- 母数が少ないと1ユーザあたりの数が多くなる(統計多重?)
- 地域(ユーザ層)による違いが顕著
- 商品/アクセス速度との相関は見られない
  ※今回の比較対象は全て個人向けブロードバンドアクセス

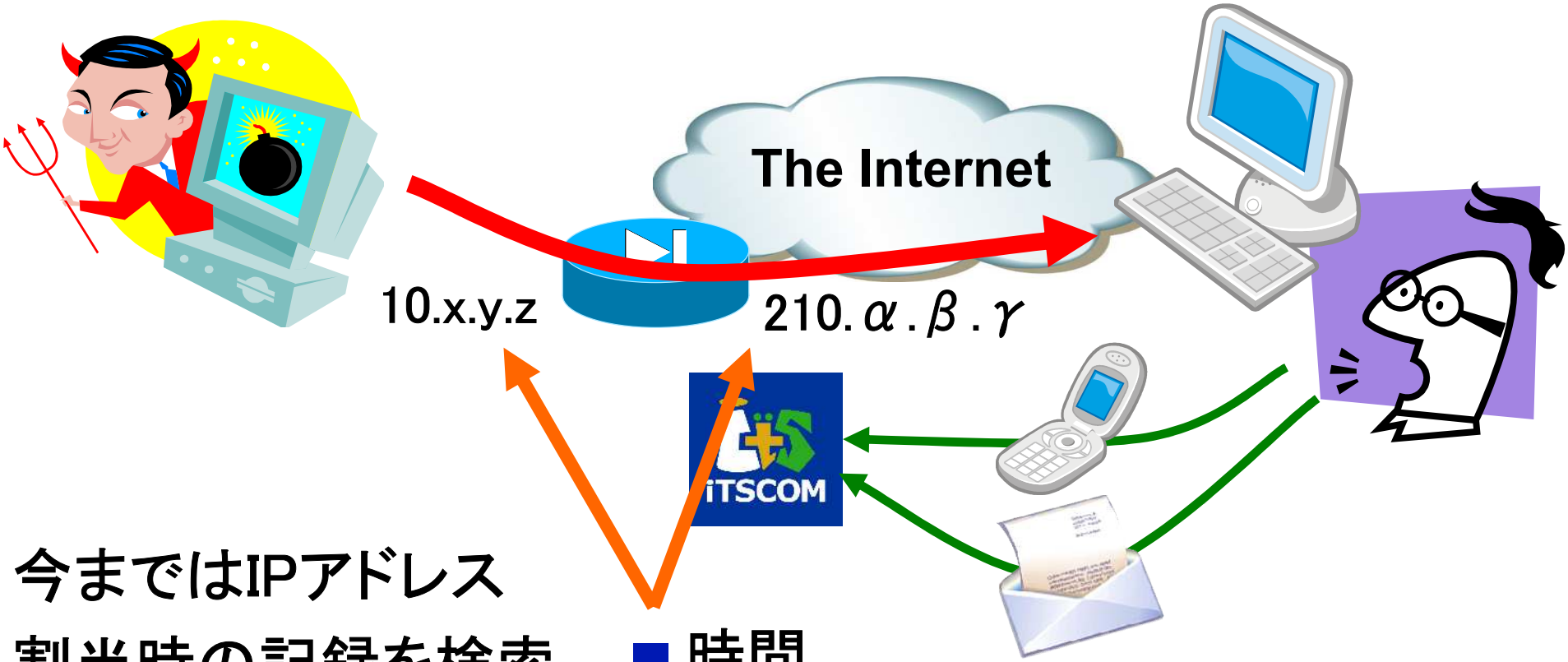
- NetBIOSをdenyすれば半減?

- トラフィックと同様の傾向 = 2:8の法則、1:9の法則

LSNと技術的課題

- ポート数制限（欠けるGoogleマップ）
- 利用者特定
  - ログ用ストレージ
- ルーティング
- IPアドレス
- 冗長、HA

利用者特定とNAT



今まではIPアドレス
割当時の記録を検索

NATを経由
した場合

- 時間
- ソースアドレス:ポート
- 宛先アドレス:ポート
- アドレス変換記録

から検索

2001:db8:1256:a4da::21

ログストレージに必要な容量(見積)

- レコードあたりの情報量: およそ48byte
  - Source IP Address + Port : 48bit
  - Destination IP Address + Port : 48bit
  - Translated IP Address + Port : 48bit
  - タイムスタンプ: 64bit
  - 他付加情報(ステータス情報、NAT箱の情報など)

- ポート数集計時に観測されたフローから推測

  ⇒ 1日あたり 約40GB?

  ⇒ 1年間保存すると … 約14TB??

ストレージに要求される要件

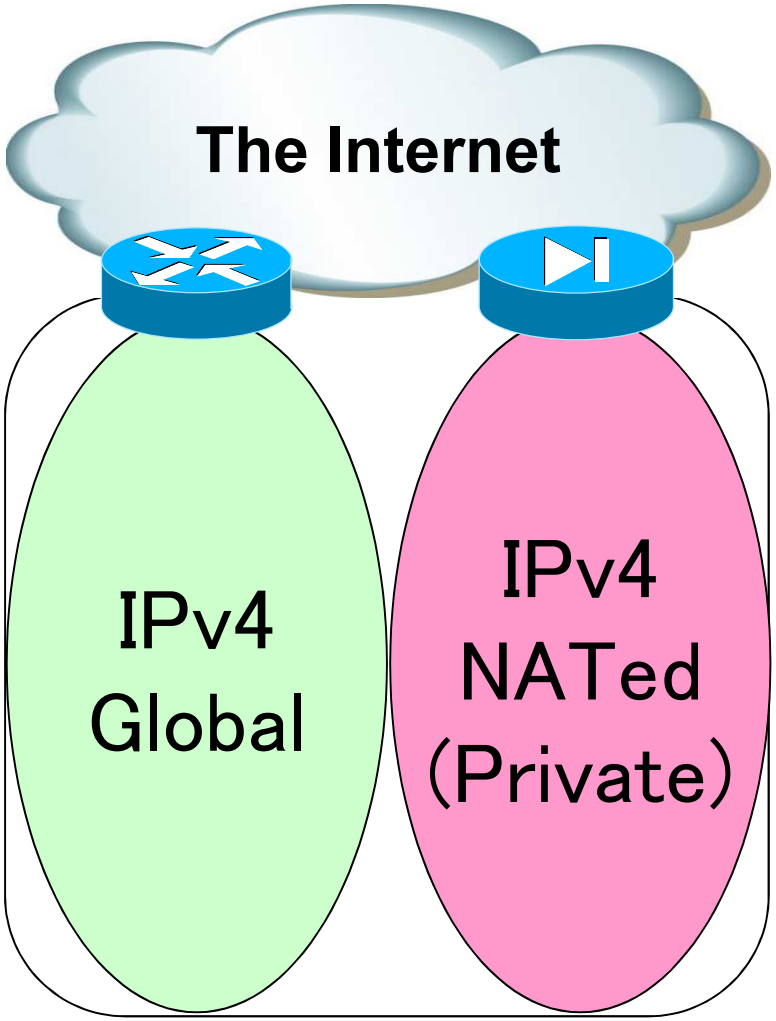
- 容量：何TB必要なんですか?
  - タマだけなら最近安いけど…
- パフォーマンス
  - 実トラフィックフローに追従できる書き込み速度?
  - サーチに堪えるアクセス速度?
- 消えちゃいけません！

LSN BOXより高ぇ?

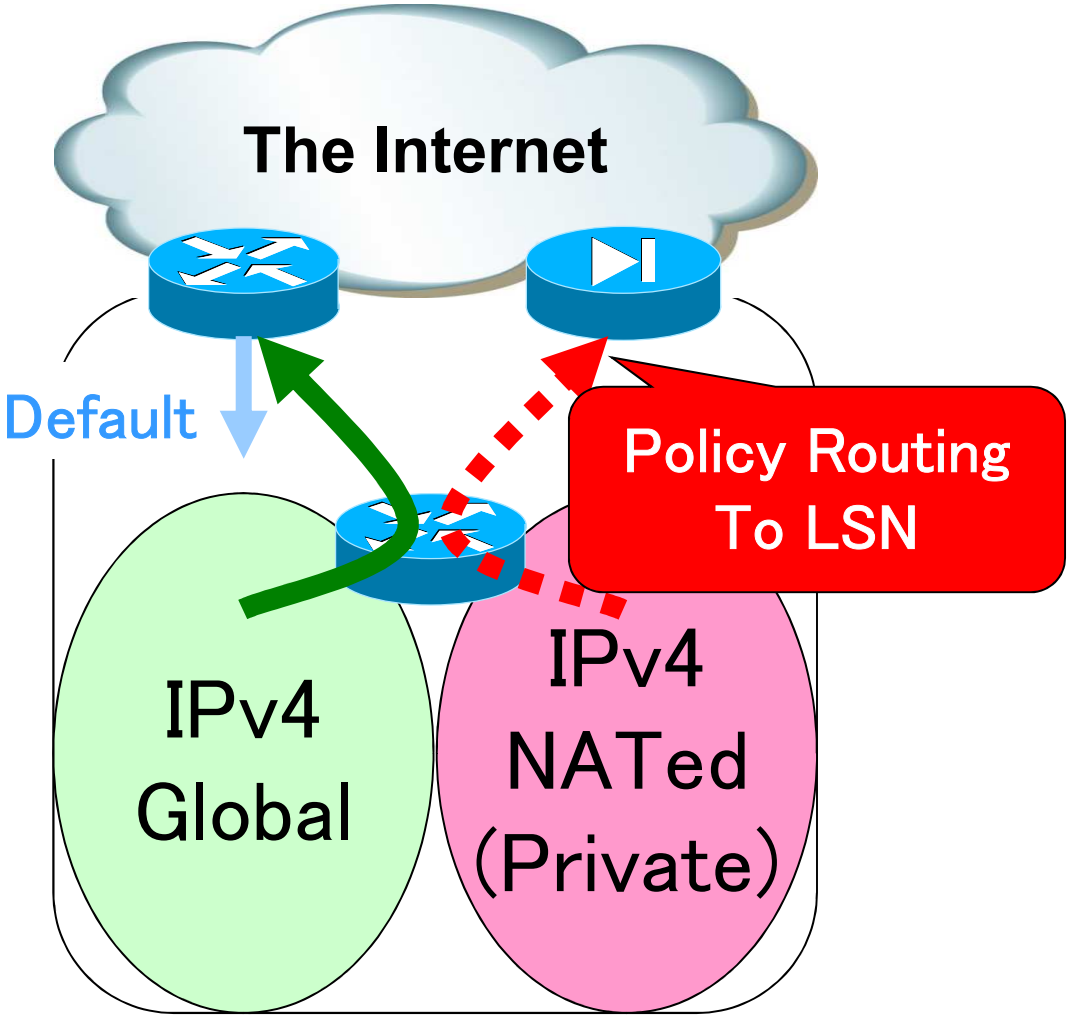
LSNと技術的課題

- ポート数制限（欠けるGoogleマップ）
- 利用者特定
  - ログ用ストレージ
- ルーティング
- IPアドレス
- 冗長、HA

LSNの配置(1/2)

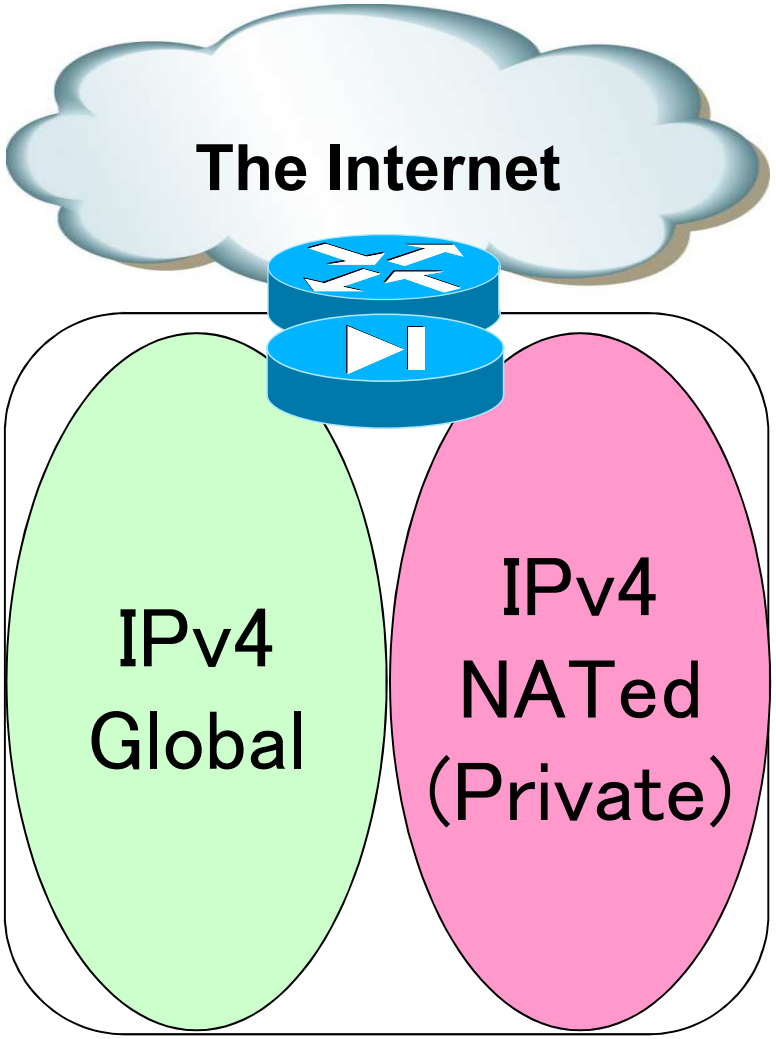


分割収容パターン



混在収容パターン

LSNの配置(2/2)



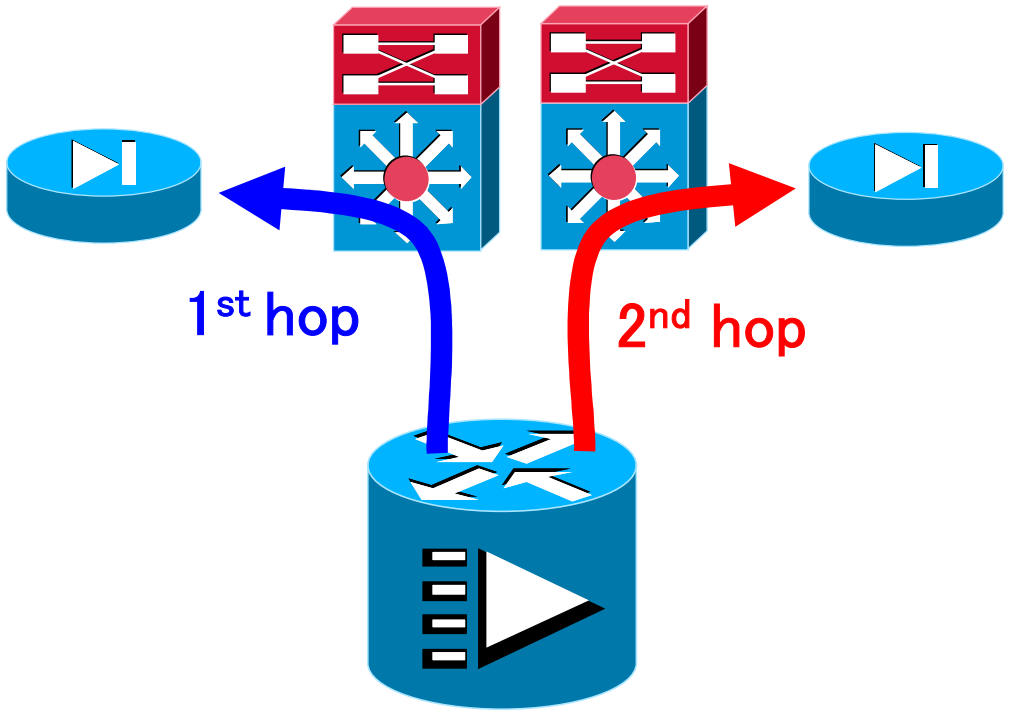
ルータモジュールに
組み込んで一体化
パターン

混在収容した場合

- NATedなアドレス空間のパケットをLSNまで運ぶ

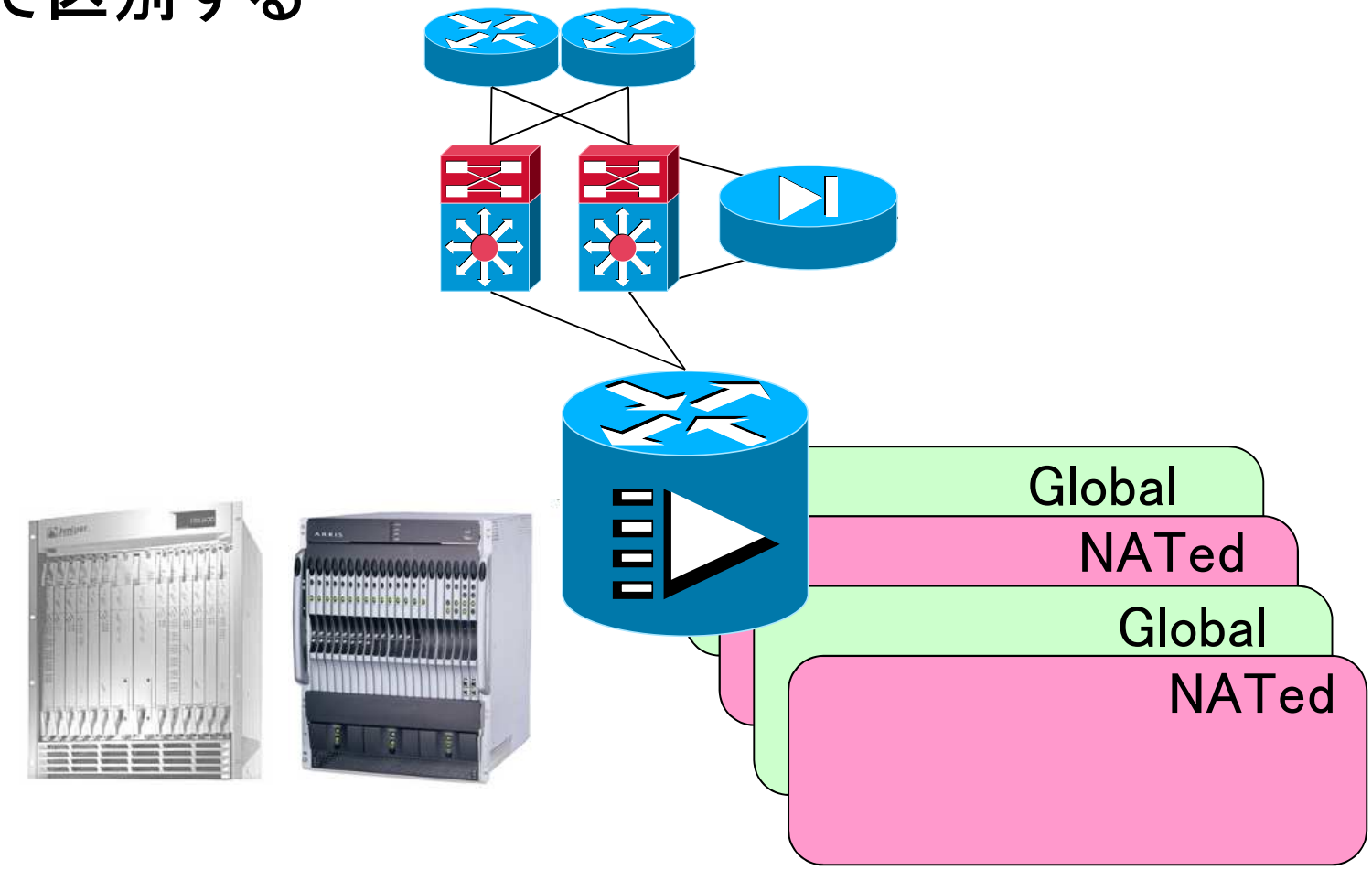
⇒ ポリシルーティング書きまくり

- 最初から最後までスタティックルーティング？
- デスティネーションベースのルーティングは崩壊

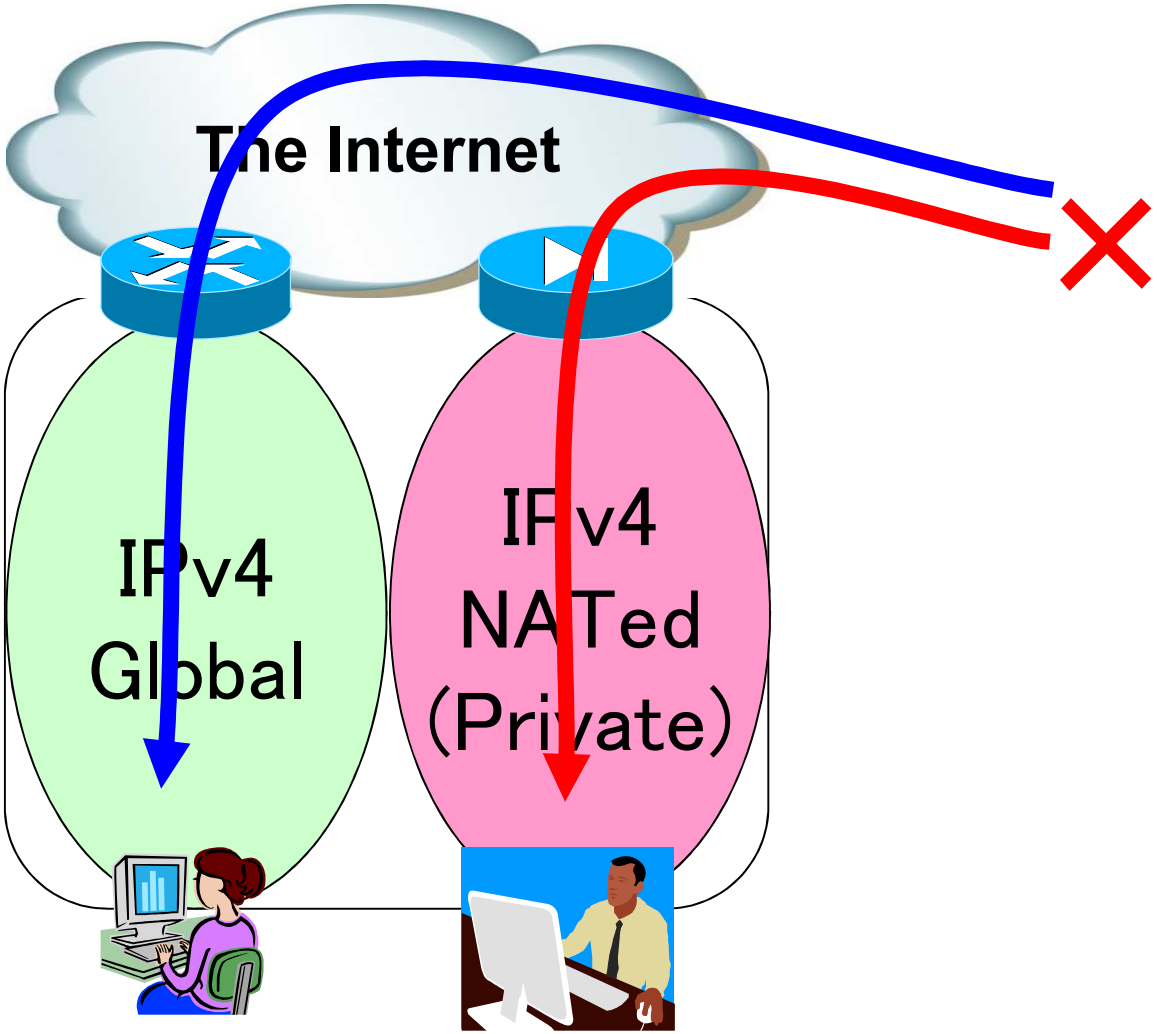


混在収容になるときって?

- アクセスコンセントレータ(CMTS,BRASなど)を共有
- 同一インフラで割り当てるアドレスをプロビジョニングで区別する



分割収容したらしたで …



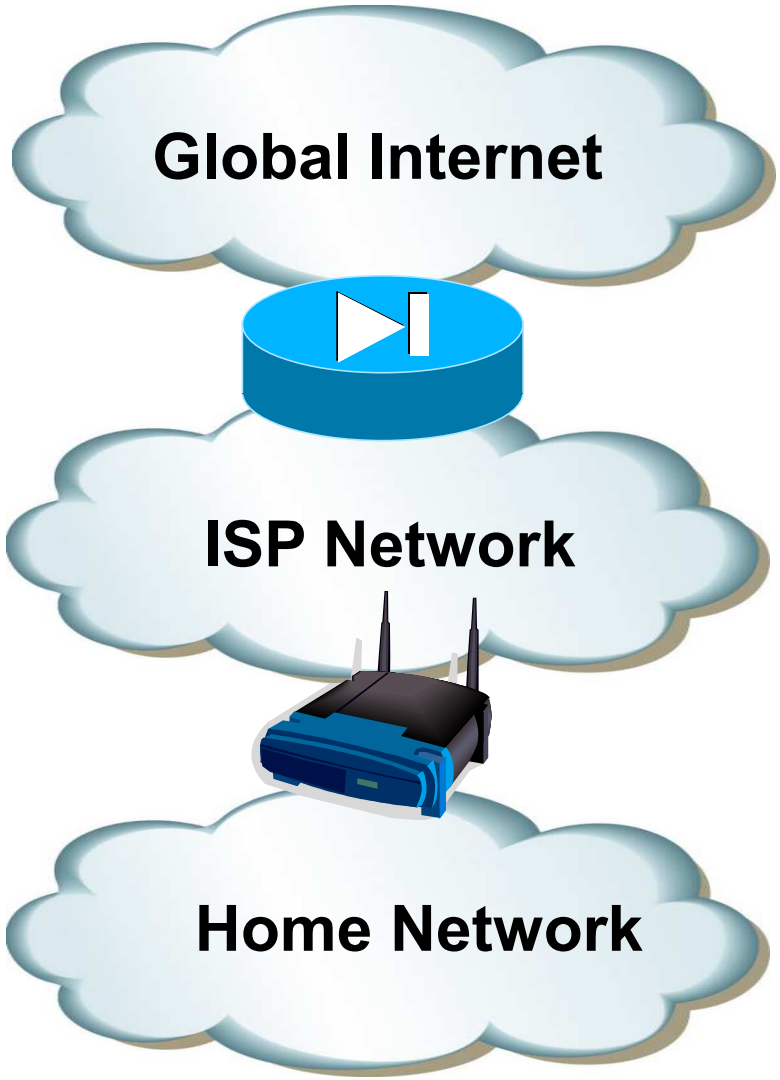
2001:db8:1256:a4da::29

LSNと技術的課題

- ポート数制限（欠けるGoogleマップ）
- 利用者特定
  - ログ用ストレージ
- ルーティング
- IPアドレス
- 冗長、HA

2001:db8:1256:a4da::30

IPアドレス問題(1): NAT前後で重複



ISPで使う空間を宣言する

個人向けルータのLAN側アドレスのデフォルトはほとんど192.168.x.x

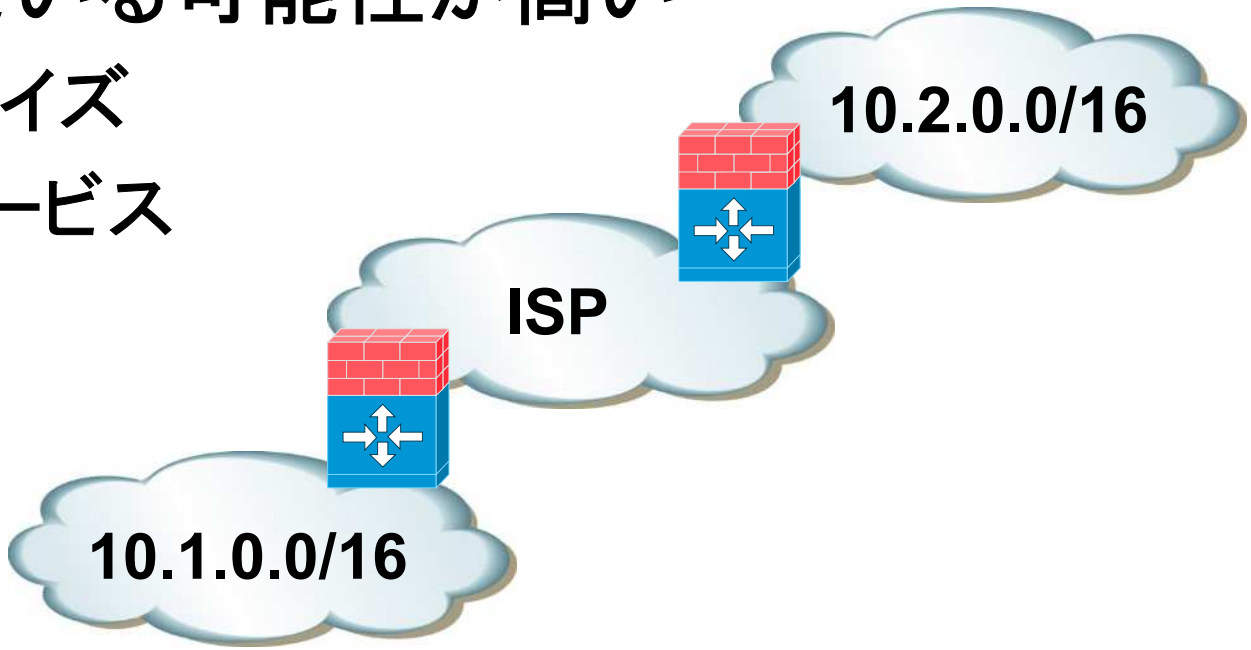
10.x.x.x　　10.x.x.x

192.168.x.x　　10.x.x.x

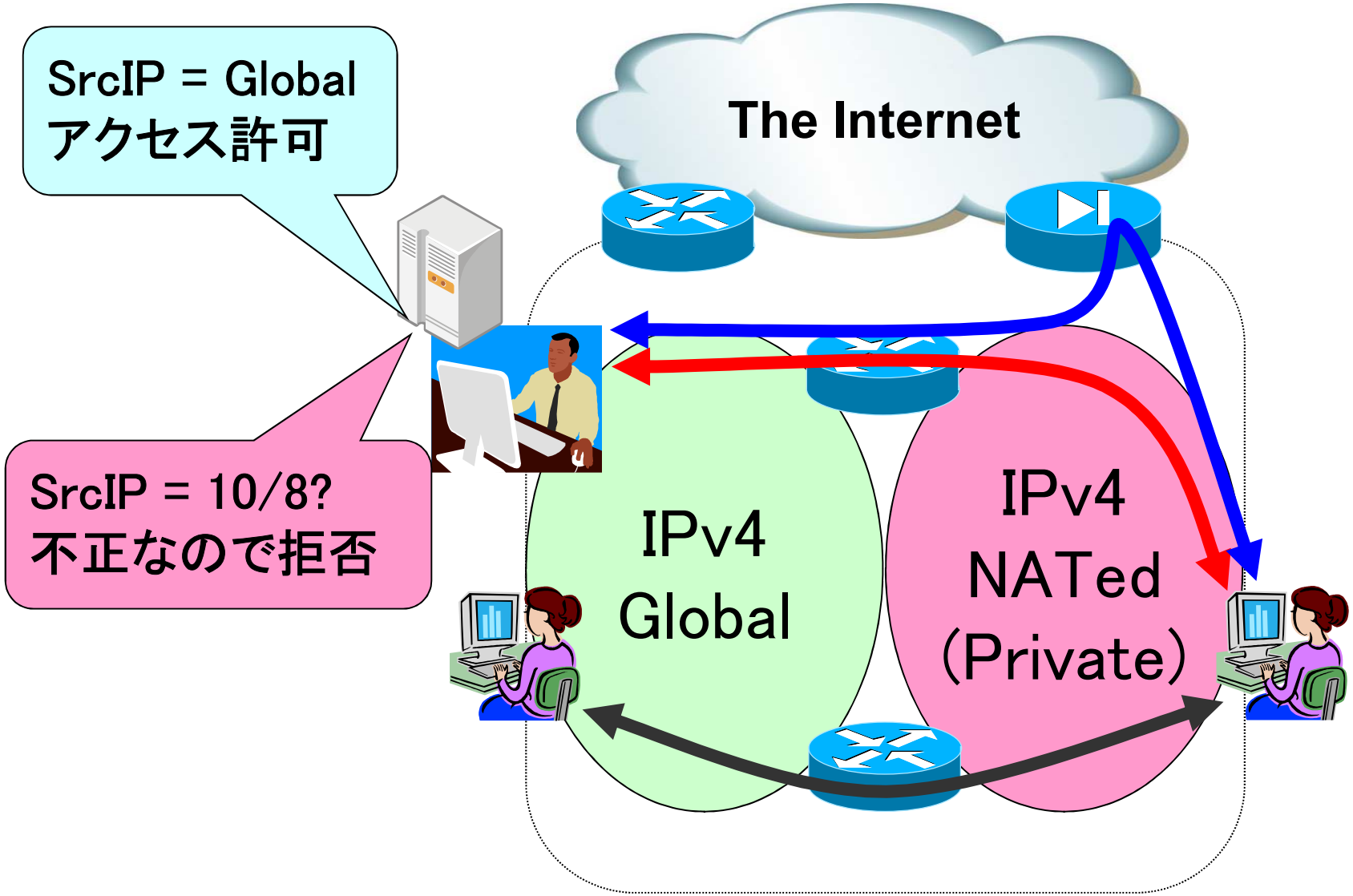
IPアドレス問題(2): 10/8使えない

- 既にインフラで使っている
  - DOCSISケーブルモデム
  - 電話サービス用TA
  - etc

- 顧客が使っている可能性が高い
  - エンタープライズ
  - 特にVPNサービス



IPアドレス問題(3): 顧客間通信



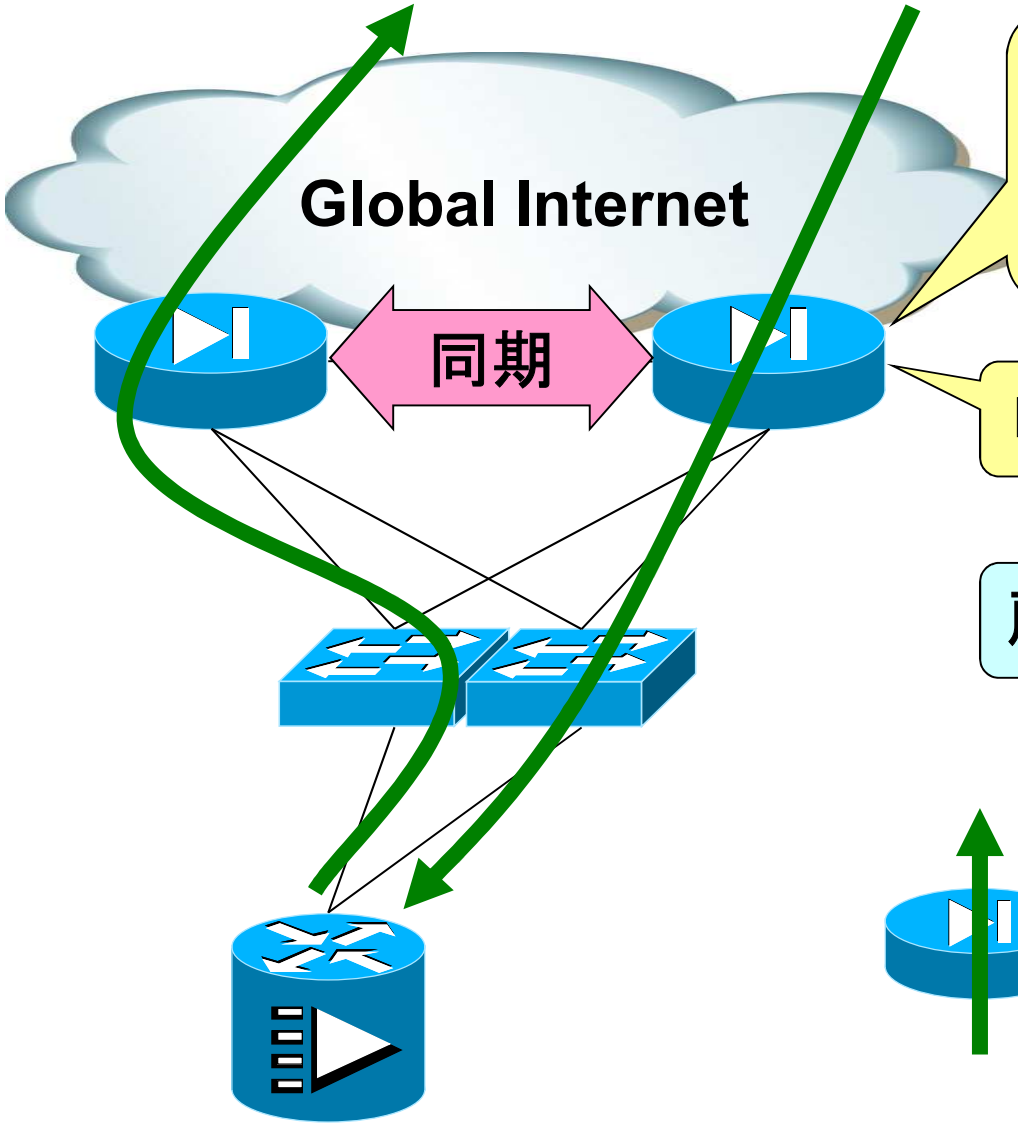
IPv4アドレス空間の選択肢

- Global IPv4 Address
- RFC1918 Private IPv4 Address: 10/8
  - 既に使われている(モデム、一部サービス)
  - 顧客間通信時の問題
- Class-E IPv4 Address: 240/4
  - 現行デバイスでほとんど動かない
  - draft-wilson-class-e はexpire?
- Shared ISP Address

LSNと技術的課題

- ポート数制限（欠けるGoogleマップ）
- 利用者特定
  - ログ用ストレージ
- ルーティング
- IPアドレス
- 冗長、HA

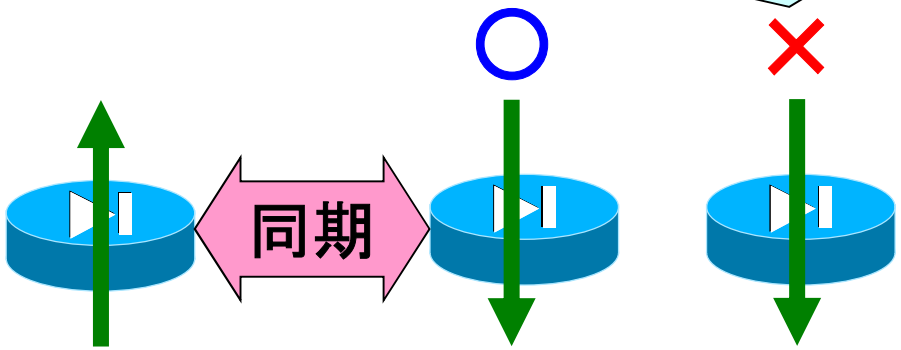
NATステートの維持 = 筐体間で同期



複数筐体間でステートフルになるようセッション情報を同期して保持

ログの整合性に注意

戻りの経路にも気を付ける

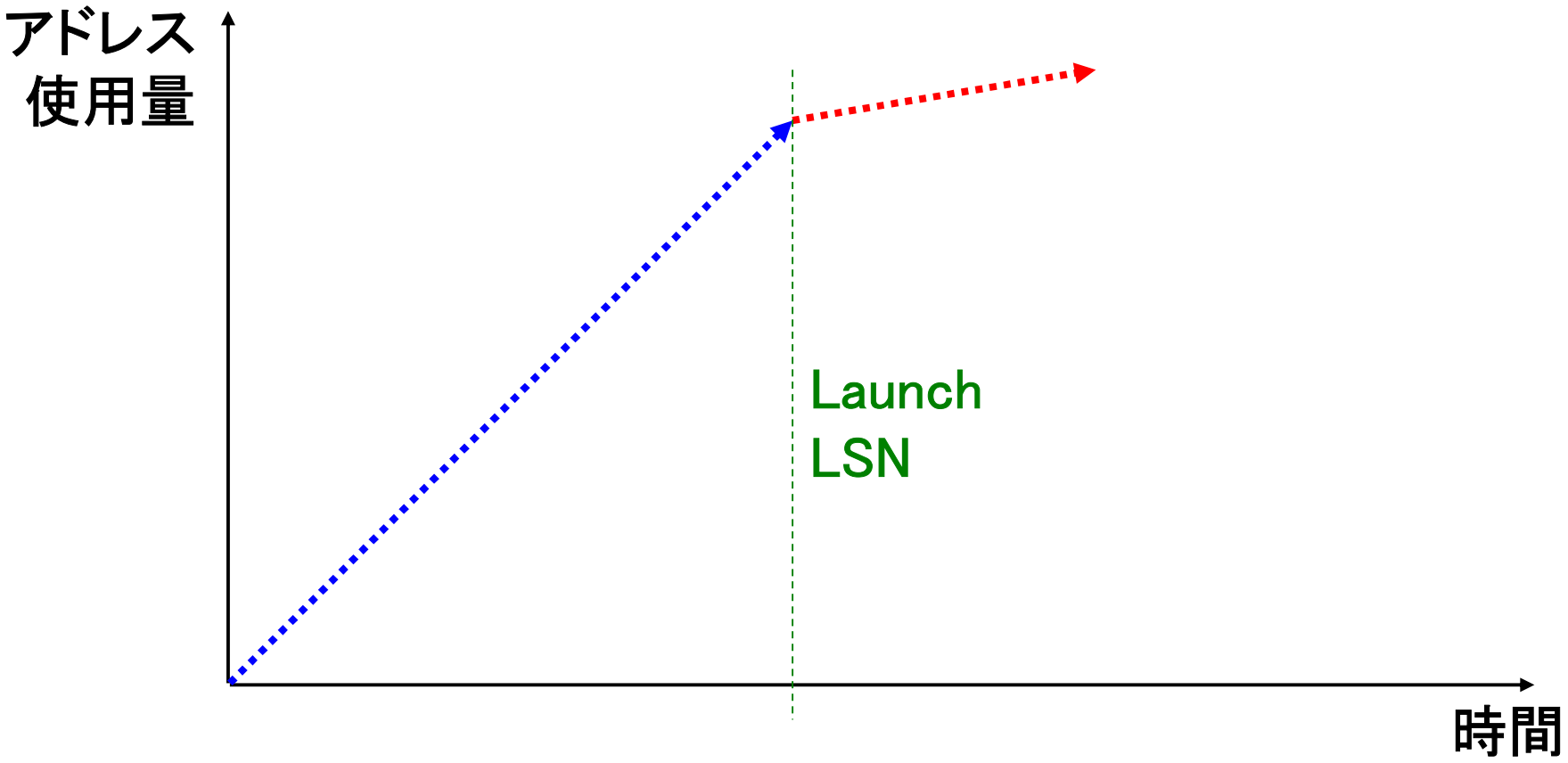


LSNを投入するタイミング

LSNを導入することによる効果

LSNで一つのGlobal IPv4アドレスをN人のユーザで共有

⇒ アドレス消費ペースが 1/N に減速するだけ



自社アドレス在庫と投入タイミング

※全て自社のアドレスプールで賄う前提

■アドレス消費ペース = 1,000アドレス/月

■LSNで1アドレスを50ユーザで共有

⇒ 20アドレス/月に減速

残りアドレス /24 で投入: 約12ヶ月でNATプール枯渇

/22 で投入: 約50ヶ月?

/21 で投入: 約100ヶ月?

IPv4アドレス共有プールの確保

- Last /8 割り振り: 一事業者あたり /22
- LSNを維持する期間を見越してリザーブ

- やりたくない方法
  - 既存ネットワークをGlobalアドレスからNATedアドレスにリナンバして捻出
  - 他社から移転(購入)

まとめ

まとめ: LSNに関する実証と議論から

- ポート数問題、Googleマップ欠落
  - 本当に発生したら立派な障害
    - 最近のホテルのNETってよく落ちませんか?
    - NATテーブルが溢れてるような挙動
  - トラフィックよりも使われ方
    - 地域性、顧客層、アプリケーション・サービス
  - プールアドレス設計、運用時のモニタリング
- 設計上のポイント(ルーティング、ストレージ)
- 投入タイミング … 枯渇直前では遅い！

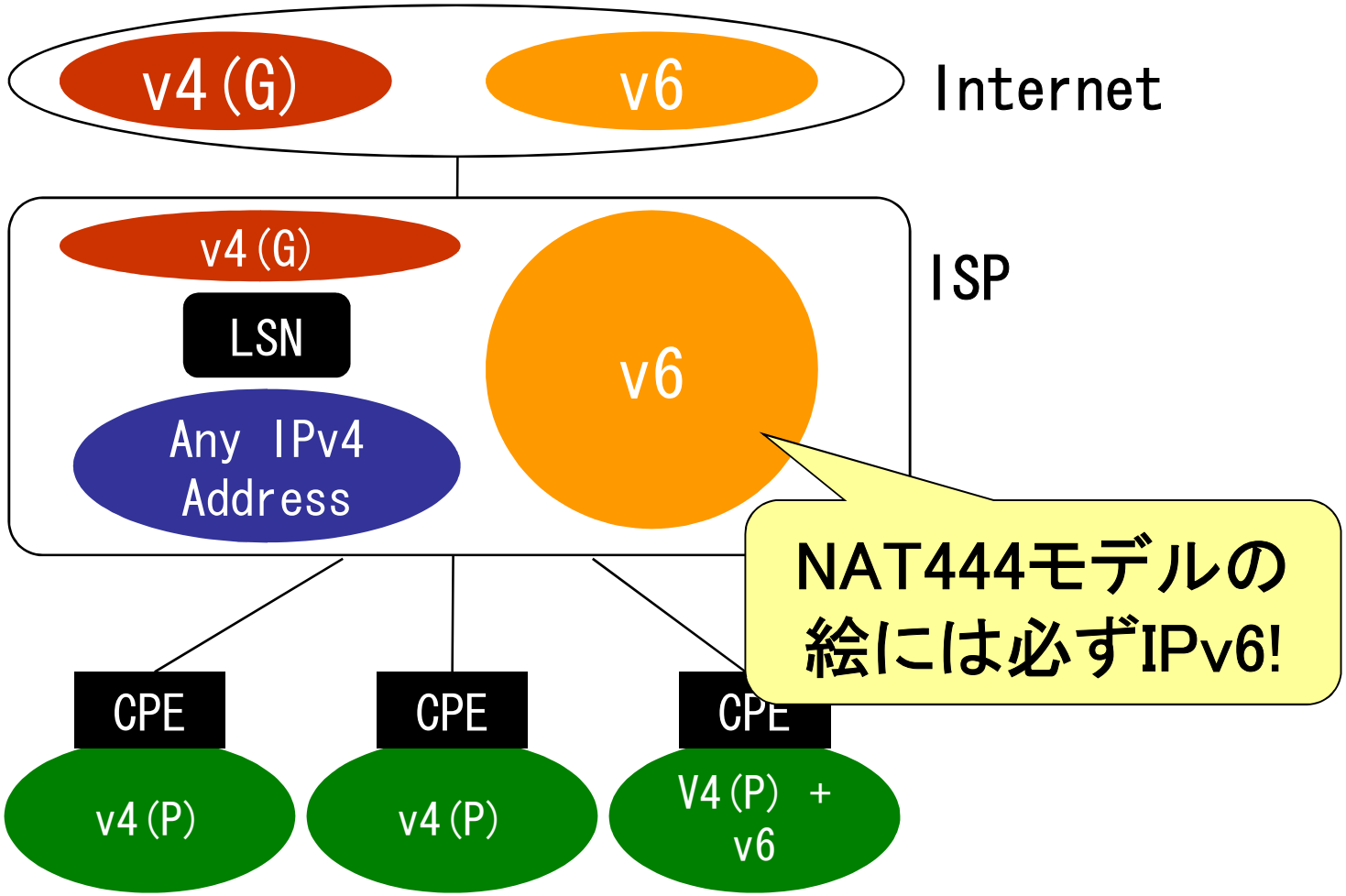
⇒ 逆線表引いて冷静に考えてみよう

NATはあくまで救済策

- 箱以外にかかるコスト
- 枯渇期以後のLSNはIPv4 onlyサイトへの接続性維持のために設けられるもの
- NAT越えによる制約、運用負荷は避けられない
- NAT変換後Global IPv4アドレスの確保
  - 4to4 NAT、4⇔6 変換
  - どんなモデルでも、接続先がIPv4である以上必要

提案中のNAT444モデル

IETF74 OpsArea KDDI中川さん提案資料より



http://www.ietf.org/proceedings/09mar/slides/opsarea-2/opsarea-2_files/v3_document.htm

議論

・IPv4アドレス共有の否定
・NATの分類(フルコーン,etc)
※JANOG22で紹介済み

■オペレータ視点

- ホントにLSNやりますか?
- NATしなきゃいけないほど困ってますか?
- NATをIPv6とセットで提供しますか?

■コンテンツプロバイダ視点

- ISPがLSNを使い始めたらIPv4のままでいいですか?
- IPv6で提供していこうと思いますか?

■エンドユーザ視点

- NATされても許容できますか?
  - ポート数リミッタは?
- (サービス側が対応している前提で)IPv6を積極的に使っていこうと思いますか?