

JANOG Softwire WG MAP-E相互接続試験 中間報告

sec-softwire@janog.gr.jp

Shishio Tsuchiya shtsuchi@cisco.com

Shuichi Ohkubo ohkubo@sakura.ad.jp

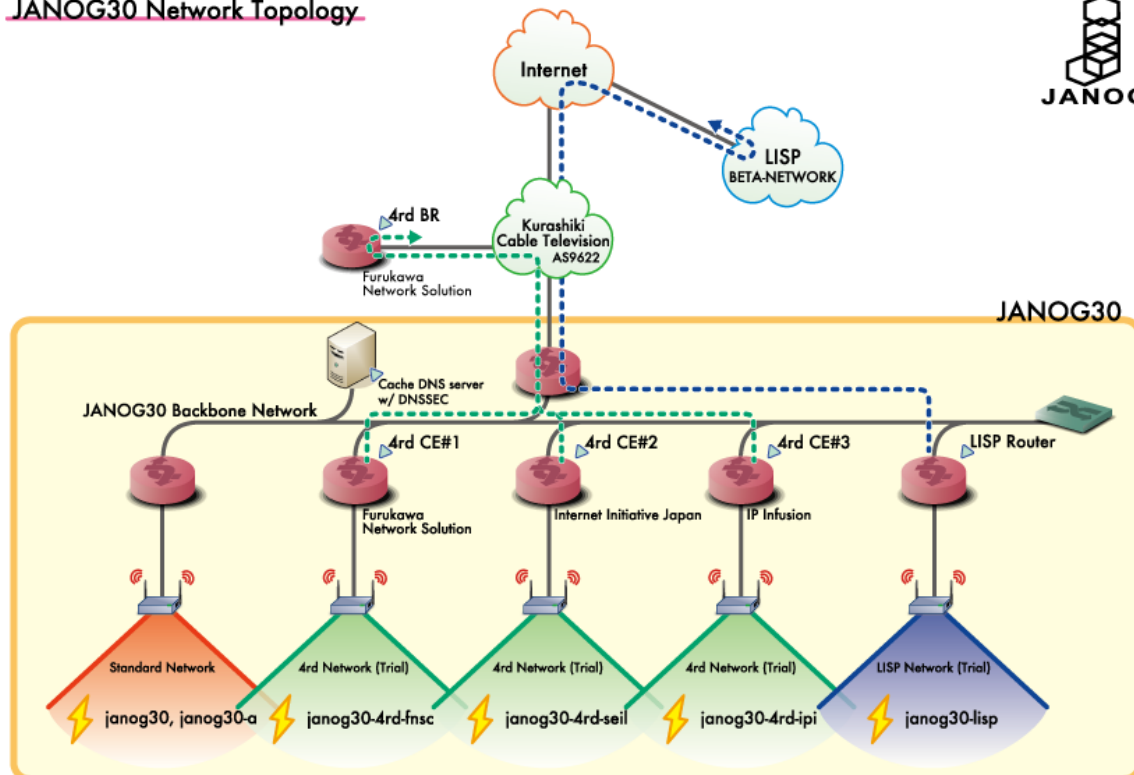
はじめに

- ありがとうございました！
- 会場およびネットワークを提供して頂いたNS
コンピュータサービス様、全般でサポート頂いた
長部さん、金子さん、ENOGの皆様
- 有意義に尚且つ楽しく過ごさせて顶けました。

JANOG30のお話

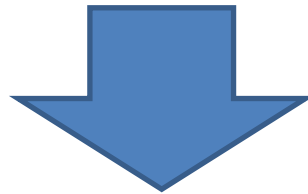
- JANOG30 では倉敷ケーブルテレビ様協力のもと、LAでネットワークを担当していた大久保さん、川上さん(IMF)を中心に4rd,LISPのネットワークを構築しました。

JANOG30 Network Topology



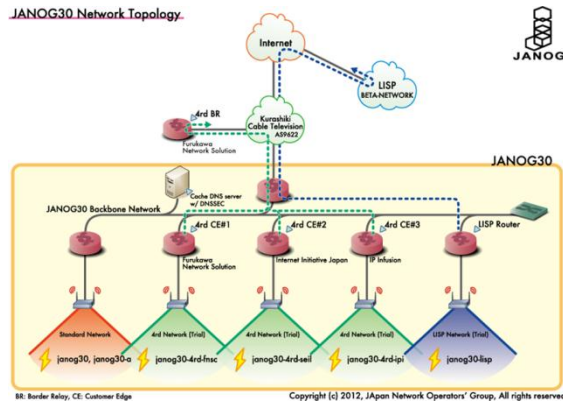
JANOG30のお話 *cont'd*

- 参加ベンダーはIPI,FNSC,IJJ(SEIL)
- 標準化プロトコルでも無い4rdの実装が3社！
- IETFでは標準化の議論がもめている。(MAP vs 4rd-u)
- 運用者＋提供者(ベンダー)の協力により出来た会場ネットワーク



ただネットワークを提供するだけでは勿体ない・・・

JANOG30のお話 *cont'd*



- 飯村くん投入
- 正確にテストを実施させる
- and JANOGerからのフィードバック
- レポートをまとめ I-D発行
- <http://tools.ietf.org/html/draft-janog-softwire-report-00>

ドラフトには

- インプリメンテーションレポート
- IPv6トンネル上のIPv4機能確認
 - ICMP,IPSec VPN,SSL VPN,PPTP,L2TP
 - インスタント・メッセンジャー/ビデオ
 - STUN, NAT-Analyzer
- 相互接続性

IETF84では



<https://www.facebook.com/photo.php?v=10150963959567666&set=vb.552692665&type=2&theater>

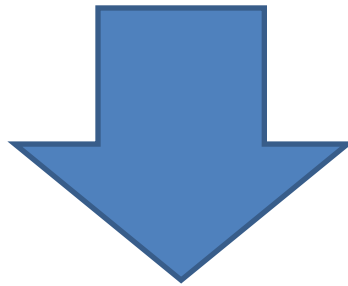
- コイントスの結果MAPはMAP-EとMAP-T
- 標準化プロトコルとしてMAP-Eが採用

Softwire WG発足の裏側

- WGの意義についてはJANOG30 のオープンマイクでも話題に。。。一方
- 4rd->MAP-Eに変わっていく中で・・・
- 折角早く実装した国産ベンダーの皆さんの優位性が見えなくなる・・・
- JANOGの意義はあくまで議論が中心
- 大久保さん、川上さんの活動もJANOGでないと制限される。
- 会場・インターネット接続の提供が制限される。
- ベンダーさんも協力してくれないかもしれない。。。。

Softwire WG発足の裏側

- JANOGの名前が欲しい。
- ネットワークの協力をお願いしたい。



- メンバーの一部によって構成される小さいグループで議論を行う方が、議論の収束性などの観点から好ましい場合がありますし、何らかの特定の目的を達成するためにそういった小さいグループを形成したい場合があります。
- JC5 JANOGワークキンググループ活動の手引き(Ver.2)

<http://www.janog.gr.jp/doc/janog-comment/jc5.txt>

ワーキンググループプロポーザル[softwire]

- [ワーキンググループ名称] それで良いのか4rd(仮)
- [メーリングリスト名称] softwire(仮)
- [チェア氏名, メールアドレス]
 - 土屋 師子生 shtsuchi@cisco.com
 - 大久保 修一 ohkubo@sakura.ad.jp
- [テーマ・目標]
 - IETF Softwire WGでWG documentとして議論されているMAP/4rdなどのプロトコルの実装促進
 - IPv6時代のIPv4運用に関するオペレーターからのフィードバックによる標準化促進
- [予定される成果物]
 - JANOGでの発表
 - IETFでのインプリメントレポートの提出
 - ベンダー実装の促進化(間接的)
 - Standard RFC発行の促進化(間接的)
- [希望期限]
 - 2012年7月20日より2013年1月30日
- [提案者氏名, メールアドレス]
 - 土屋 師子生 shtsuchi@cisco.com
- [提案日] 2012年7月10日

提案後・・・

- Committee・・・JC5初めて読んでない？？w
- 協力してくれる(ほしい)方々に事前に声掛け
- 会場・サポートに関して相談=>金子さん(ENOG)

JANOG Softwire WG相互接続試験のご案内

- (1) ベンダー
 - MAP-Eを実装した機器を提供
 - 相互接続試験に参加出来るベンダー
- (2) 試験協力者
 - MAP-Eを構築した環境で各種アプリケーション/プロトコルの試験を実施
 - 各種パブリックサーバーなどの提供が可能な方
 - 各種アプリケーション(P2Pを利用したアプリ、ゲームなど)の提供可能な方
- (3) 無線環境提供者
 - - 20名程度の会場で使用する為の無線LANのアクセスポイントなどを設定および提供可能な方

スケジュール

	10月24日	10月25日	10月26日
9:00	設置 準備	接続試験	接続試験
10:00			
11:00			
12:00			
13:00			
14:00	接続試験		片付け
15:00			ENOG17
16:00			
17:00			
18:00			
19:00			懇親会
20:00			
21:00			
22:00			
23:00			

参加ベンダー

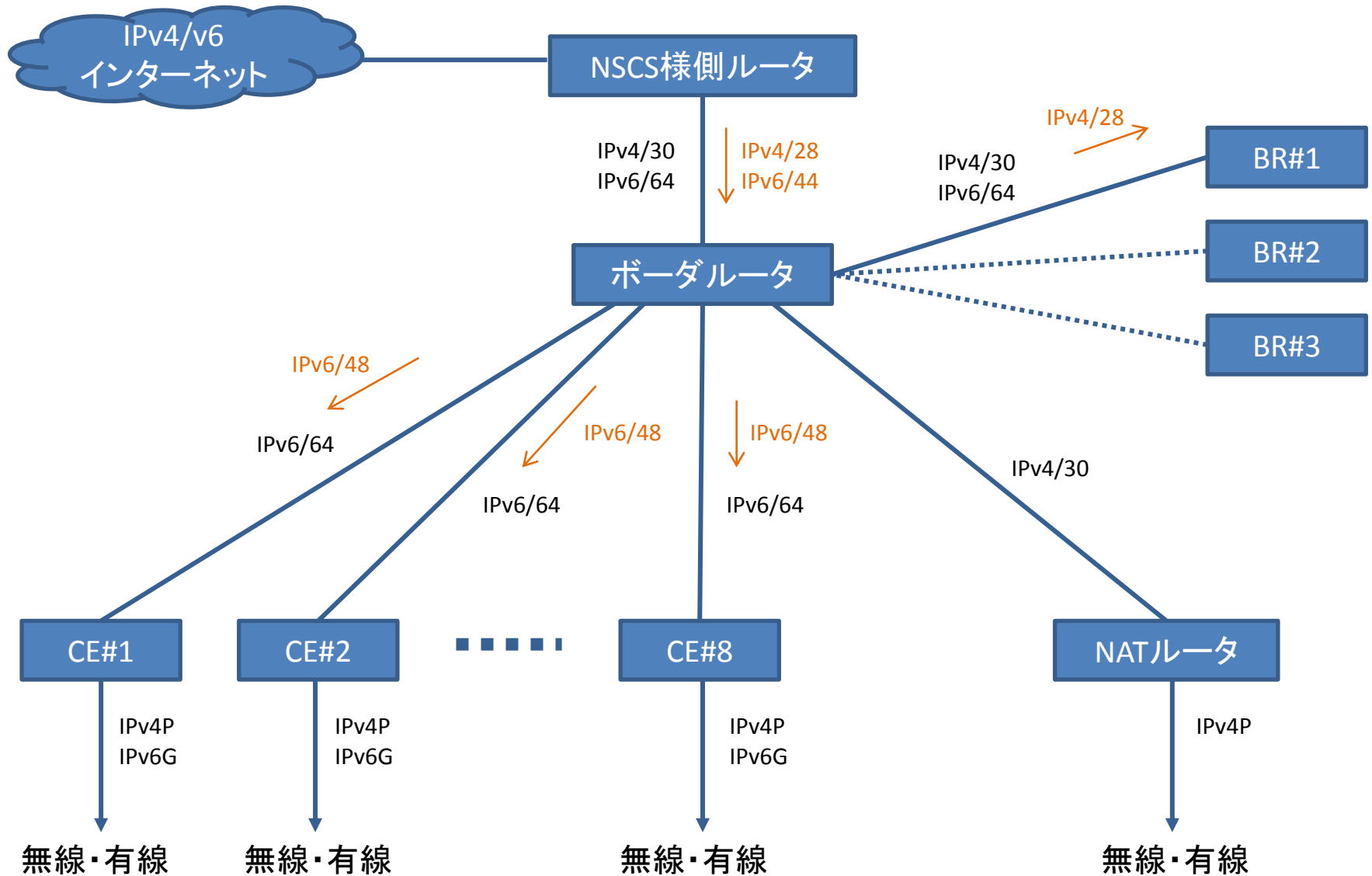
- A社 インプリ1 BR,CE
- A社 インプリ2 BR,CE
- B社 BR
- C社 BR,CE
- Dな人 BR,CE
- Eなインプリ CE
- F社 BR,CE
- G社 CE

相互接続表

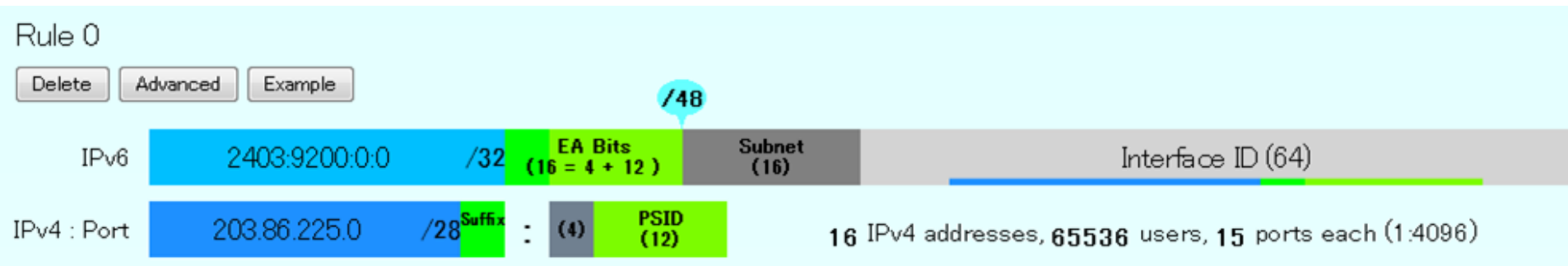
BR/CE	A	A	B	C	F
A					
A					
C					
D					
E					
F					
G					

BR/CEは確認必要
インターフェースも確認

論理ネットワーク構成



MAPパラメーター

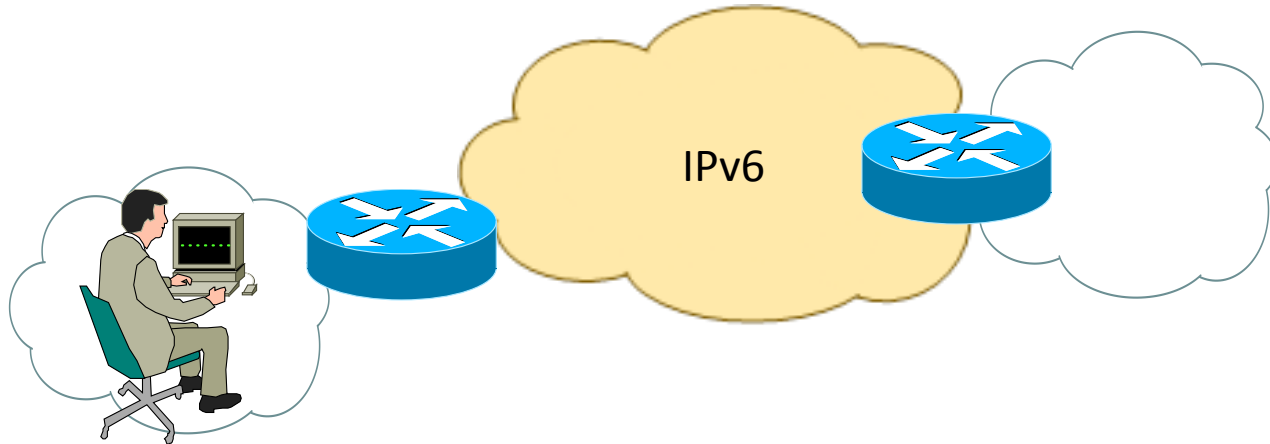


- 1つのIPv4アドレスを4096人で共有
- CEが使えるポート数は15個のみ

各ベンダー機能の確認

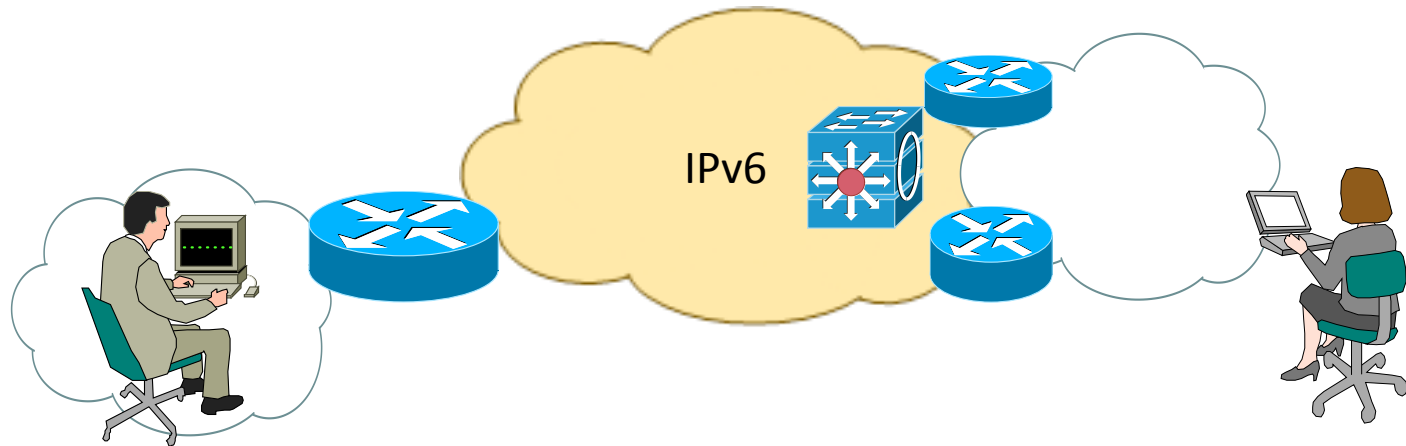
- 参考になっているインターネットドラフトは？
- BRアドレスがICMPに反応するかどうか？
- プロビジョニング方法は？
- セキュリティチェックの機能

IPv4機能性確認試験



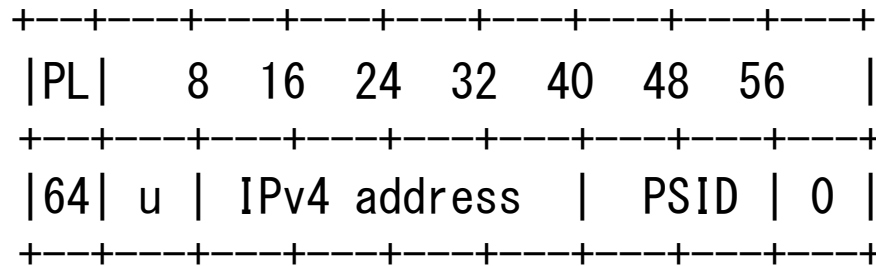
- VPN IPsec VPN,SSL VPN,PPTP,L2TP
- インスタント・メッセージャー/ビデオ(Skype,MSN,Facebookなど)
- BRのICMPエラーハンドル(time too exceed, host unreachable, fragment needed)
- NAT確認ツール Kさん提供STUNツール **TUN (NAT Analyzer)**

BR冗長性の確認



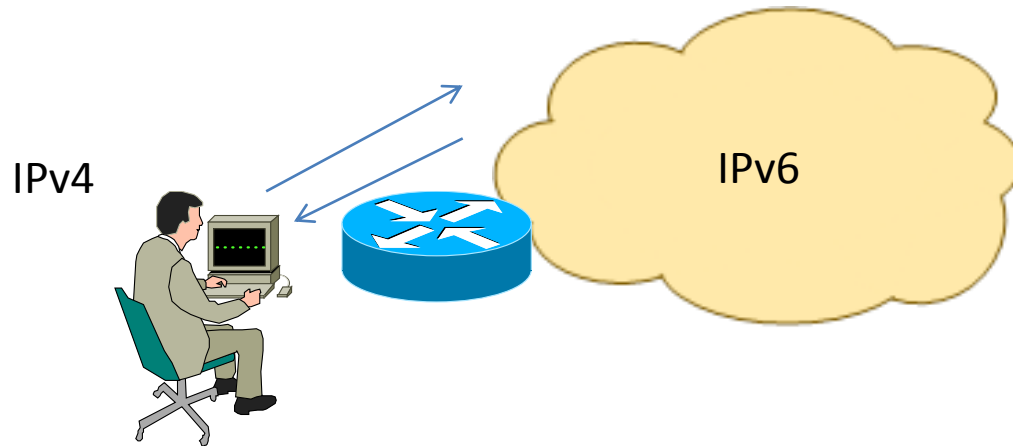
- BRの冗長性をマルチベンダー環境で確認
- ICMPとSkypeを実施し、ステートレストンネルテクノロジーであるため、セッションが切れない事を確認

IPv6 interface identifier



- PSIDが右寄せ(左側パディング)のところを 左寄せに(右側パディング)なってる為に、BRでパケットを破棄
- **ドラフトの解釈の違い**
- 即時修正

DNSでポートが枯渇



- DNS Queryだけでポートが枯渇
- AJAXでのポート消費よりもストレスフル
- CEでIPv4->IPv6 Proxyを実施
- DNS(UDP)は早めにtimeoutにする実装
- Proxyをベースに修正
- 本来はIPv6も提供される為、問題にならないかも。

コンフィグの問題

Rule IPv6 prefix:	2403:9200::/32
Rule IPv4 prefix:	203.86.225.0/28
EA bits:	16bit(48-32)
Port-Set ID:	12bit
PSID offset:	4
BR IPv6 address:	2403:9200:fff0:0::2



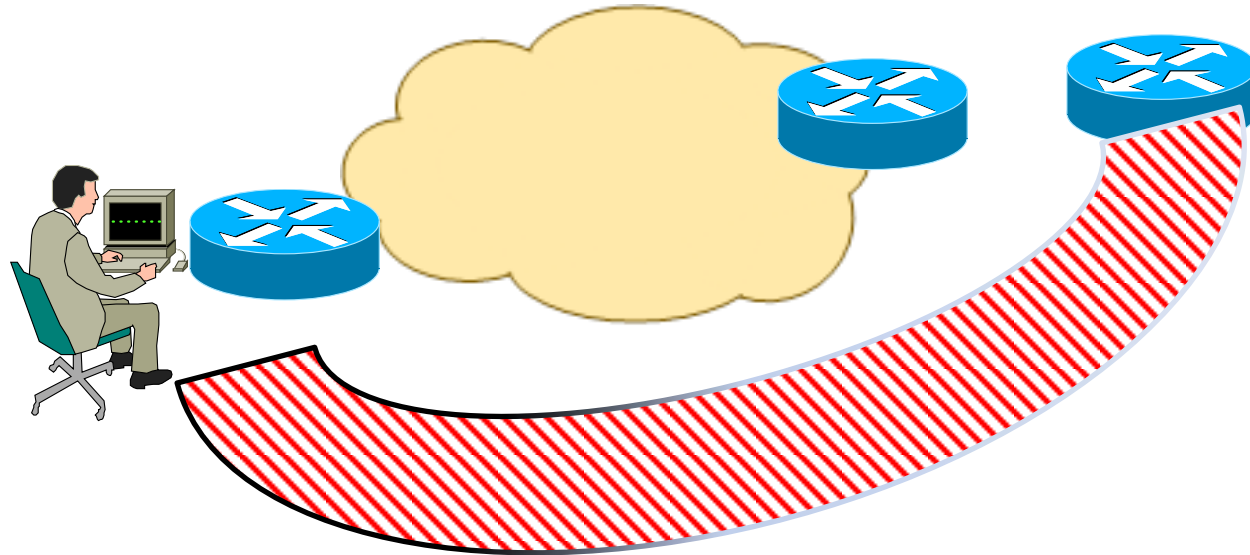
```
# set interfaces map map0 role br
# set interfaces map map0 br-address 2001:db8::1/64
# set interfaces map map0 default-forwarding-mode translation
# set interfaces map map0 default-forwarding-rule true
# set interfaces map map0 rule 1 ipv6-prefix 2001:db8:89ab::/48
# set interfaces map map0 rule 1 ipv4-prefix 192.0.2.0/24
# set interfaces map map0 rule 1 ea-length 16
```

フォーマットが想像しやすい

```
service cgn JANOG
service-location preferred-active 0/0/CPU0
service-type map-e Software
cpe-domain ipv4 prefix 203.86.225.0/28
cpe-domain ipv6 prefix 2403:9200::/32
sharing-ratio 12
aftr-endpoint-address 2403:9200:fff0::2
contiguous-ports 0
```

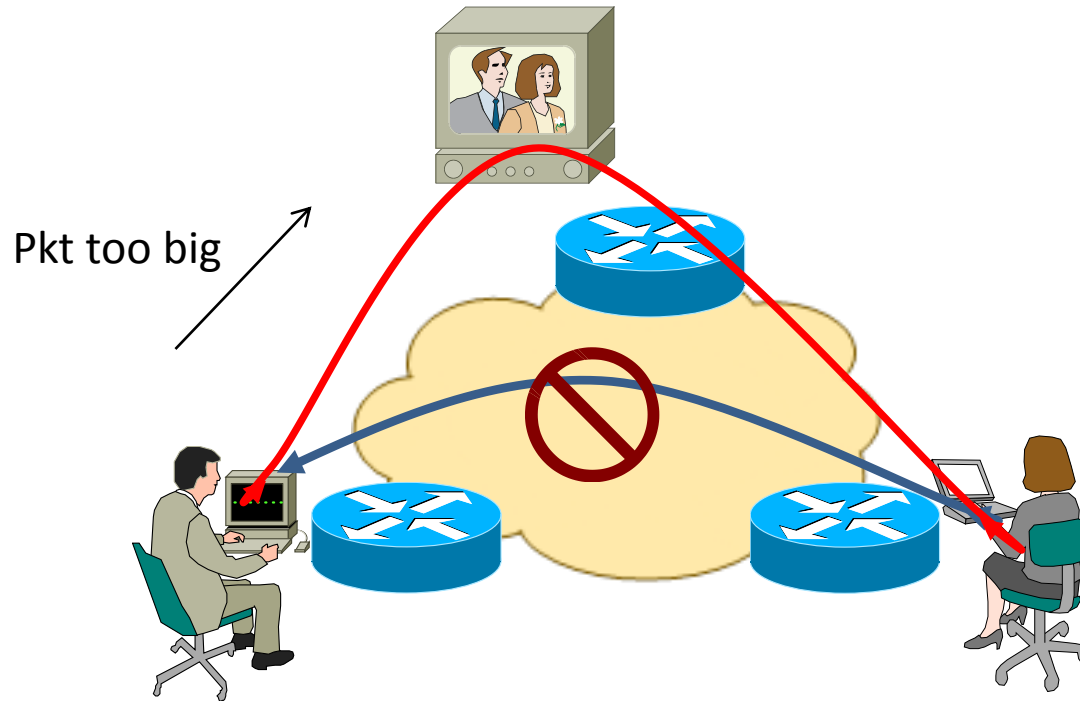
設計思想がわかりやすい

NATトラバーサルの際の問題



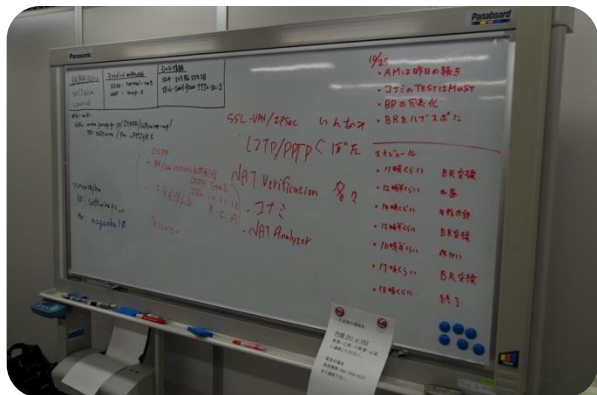
- NAT環境でIPSecを行う際に使用されるNATトラバーサルを実施すると起こる問題
- 即日修正

混在問題



- NATの特性によりHUB & Spokeの通信
- データ量が多い為 Pkt too bigメッセージ
- 上手く通信が繋がらない。。。
- Tunnel MTUはよく管理された状態で運用する

おもひで



まとめ

- 厳しい環境での試験をする事でデザイン上の懸念点や不具合が確認できた
- 相互接続試験によりドラフトの解釈の違いによるトラブルを未然に防げた
- インプリの違いによるパラメータの交渉の難しさを実感
- 短期間に集中して試験をやるためには合宿的な環境が良い
- ご飯も酒も旨い
- ありがとうございました。