

JANOG41

conference network

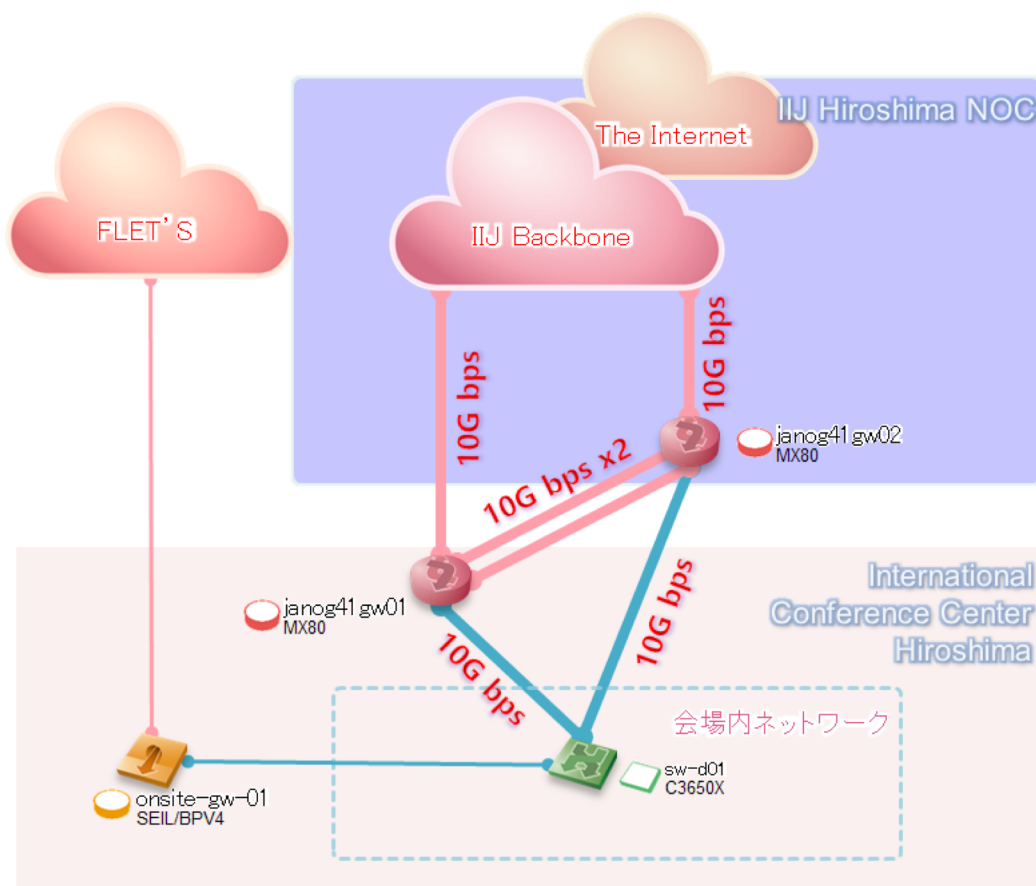
Matuzaki 'maz' Yoshinobu

<maz@ij.ad.jp>

やりたい事を考えた

- 会場にダークファイバを引き込む
 - グローバルIPアドレス配る
 - 無線区間ネットワーク品質の計測
 - 綺麗なモニタリング画面
-
- あと、おまけで洗濯バサミDHCP

10Gx2にしてみた



利用量は、ピークで165Mbps程度 :D

端末にIPv6/v4グローバルを配布

- IPv6は普通に接続サービスから割り当て
 - 利用者空間は普通に/64
- IPv4アドレスはJPNICの協力で /16 を確保
 - 利用者空間はドドンと /17
- NATしなくて良い
- 現地サーバを最小限にするため、参照用ネームサーバはIJJが顧客向けに提供してるのを流用
 - サーバ側で、今回使う新規IPv4空間からの名前解決を許可するようにACL更新

ネットワーク品質計測

- 無線フレームの再送率などを計測
- 学術方面で解析結果が共有されるはず

綺麗なモニタリング画面

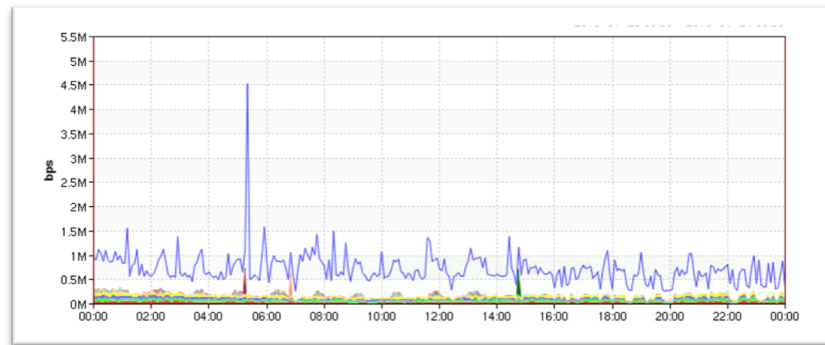


洗濯バサミ DHCP



想定していた問題

- ARP flooding
 - IPv4はスキャン等、様々なパケットが吹き荒れてる
 - /16向けで1Mbps程度を確認



- /17なんて使った日には、酷い状態になるはず
 - 実測で600arp/sec!
- 使われていないIPブロック宛の通信を破棄
 - 洗濯バサミDHCPがあるのでDHCP snoopingに頼れない

想定してなかった問題

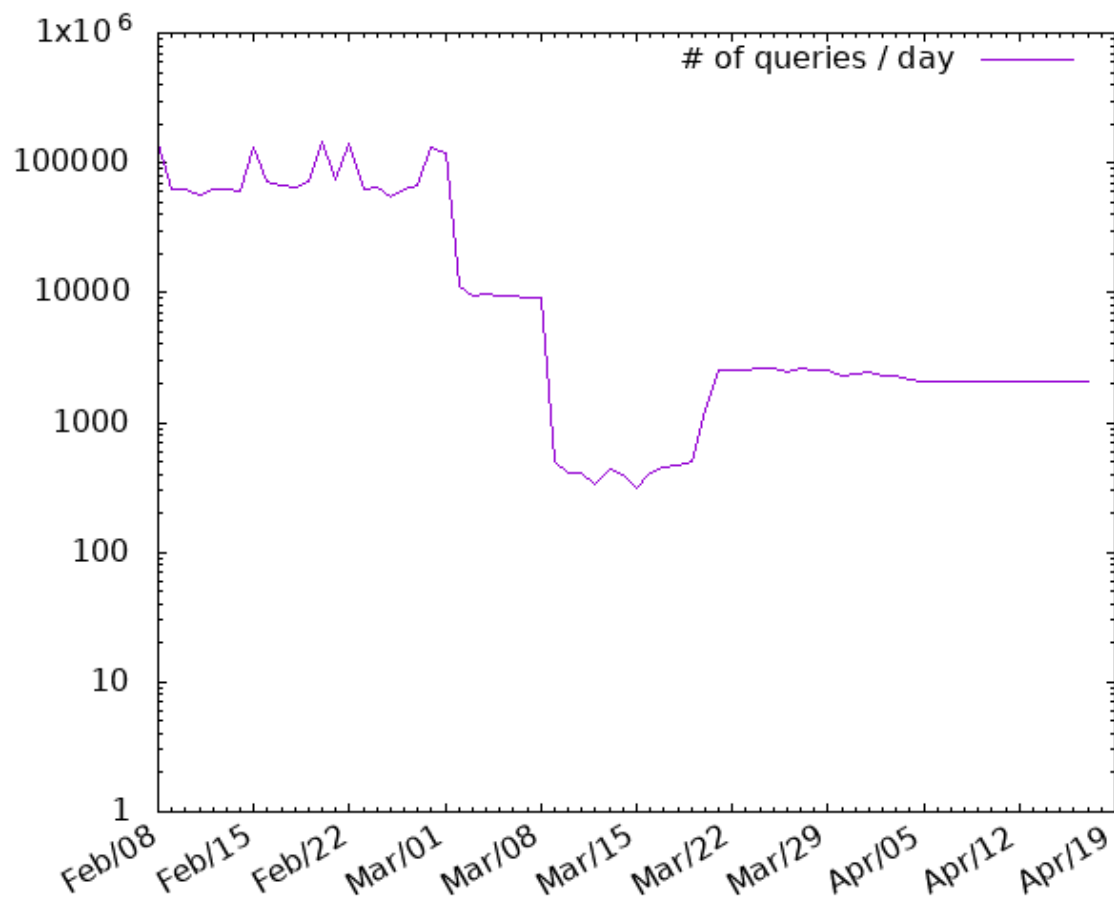
人多すぎ。

- 慌ててフェニックスホールでAP台数の増強
- 結果として想定より巨大なL2ネットワークが出来上がり、これまた無線区間の負荷が上昇

トラブル事例

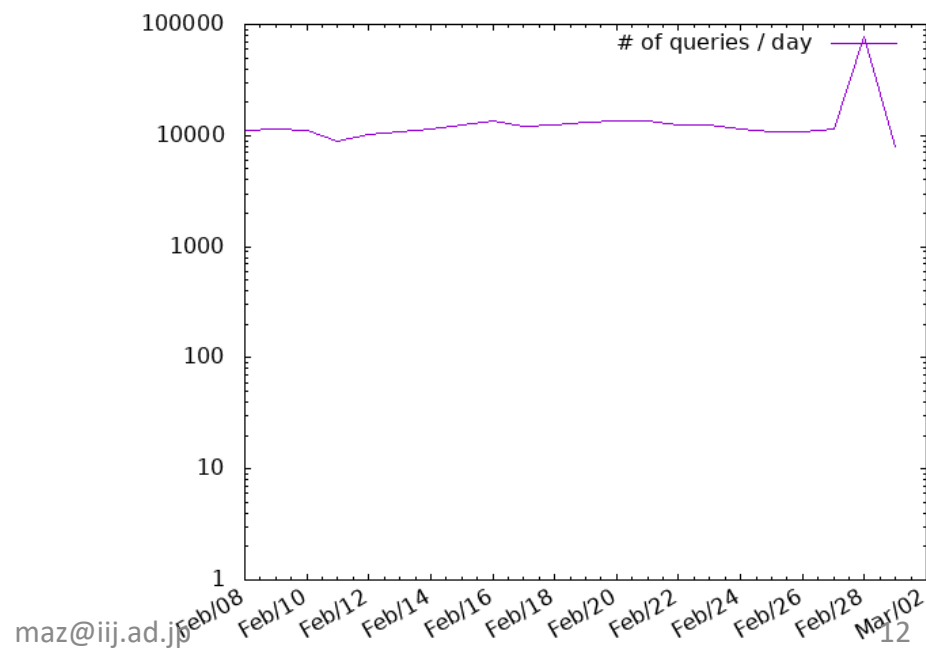
- 置いている筐体が熱い！
 - 手抜きで電源片系で運用していたら、実は稼働するファンも半分になっていた
 - 両系電源挿して万端
- 会場からIPsec VPNが繋がらない
 - VPNサーバ側ではNAT Traversal (UDP包み)だけを想定して、パケットフィルタしてた模様
 - クライアントはNAT越えをする必要がないので、UDP encap無しの素直なESPで通信を試みていた模様

JANOG41後の逆引き問合せ



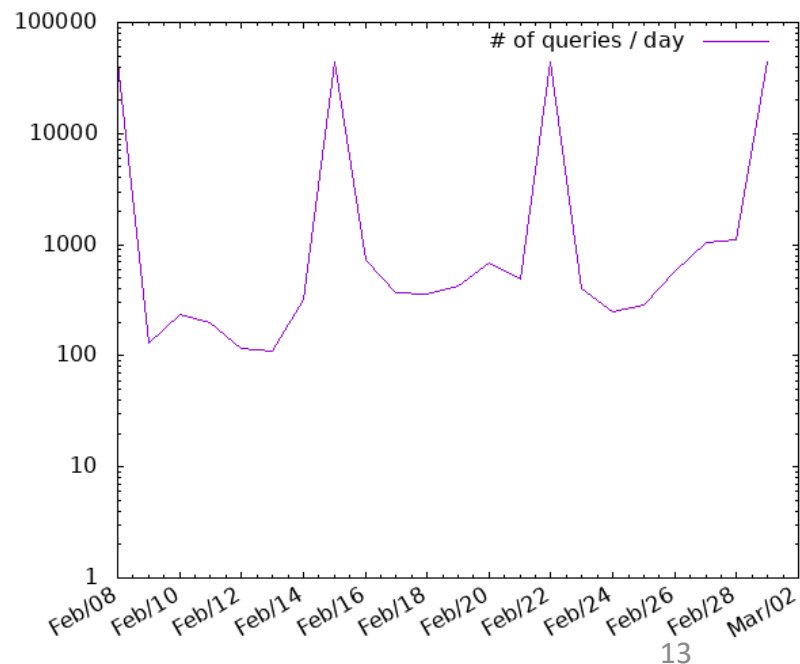
AS15169

- 2月28日に6qpsぐらいでゆっくり全PTR探索
 - 通常より + 65K増の問い合わせ
 - 37.71からインクリメンタル
 - Google Public DNSのdlsインスタンスから



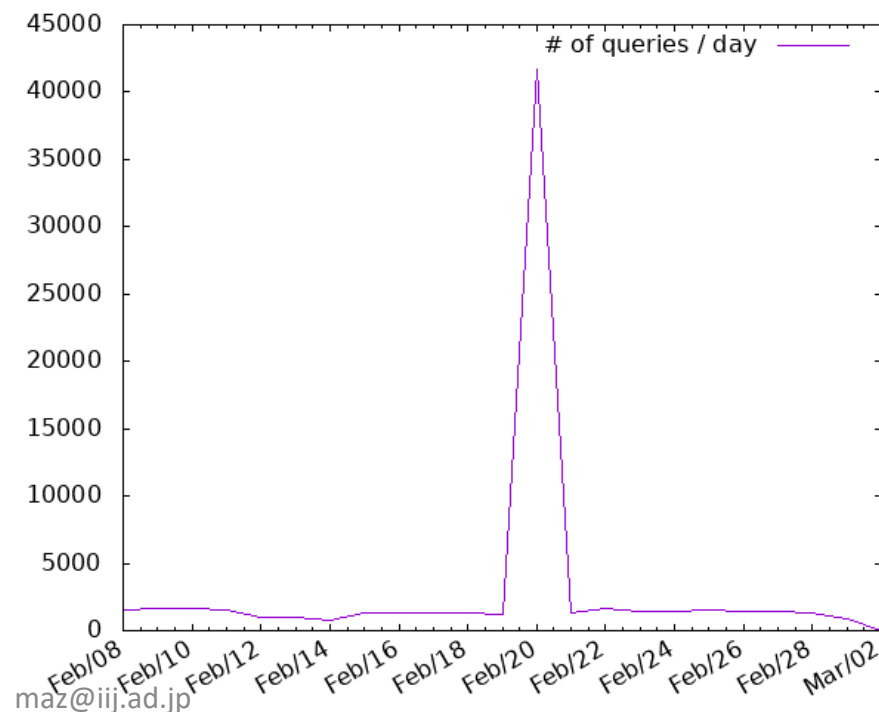
AS16509

- 毎週木曜日ぐらいに、ランダムな順序で1~1.5qpsぐらい
 - /24単位の委譲を想定してNSを問い合わせ
 - 何となく網羅的にPTR探索
 - 毎回44K問い合わせぐらい
 - 4回弱での網羅率は99%



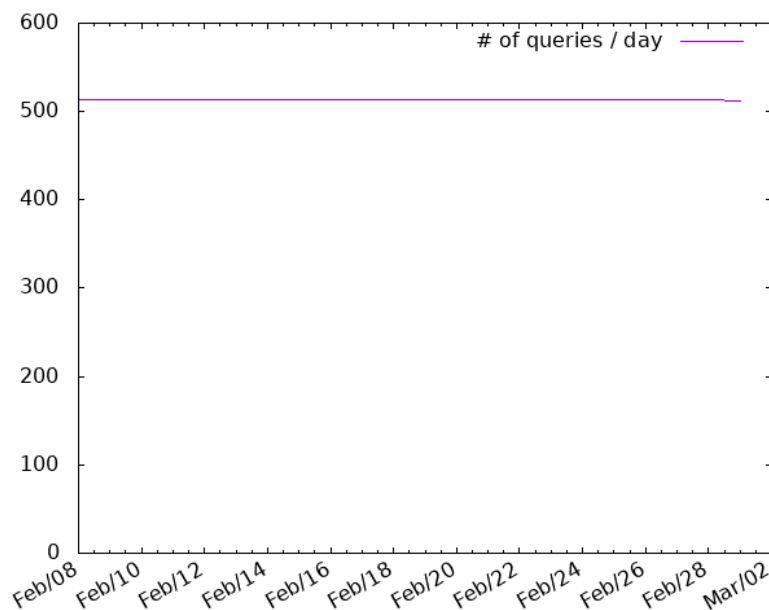
AS4134

- 2月20日に280qpsぐらいでなんとなく網羅的にPTR探索
 - 40K程度の探索、56%程度の網羅率



AS2515

- 2台からそれぞれ日次で200qpsぐらいの勢い
- /24単位でのNS委譲を仮定してSOAを聞く
- 問い合わせQNAMEを単にsortしてる模様
 - 119,12,120,121...



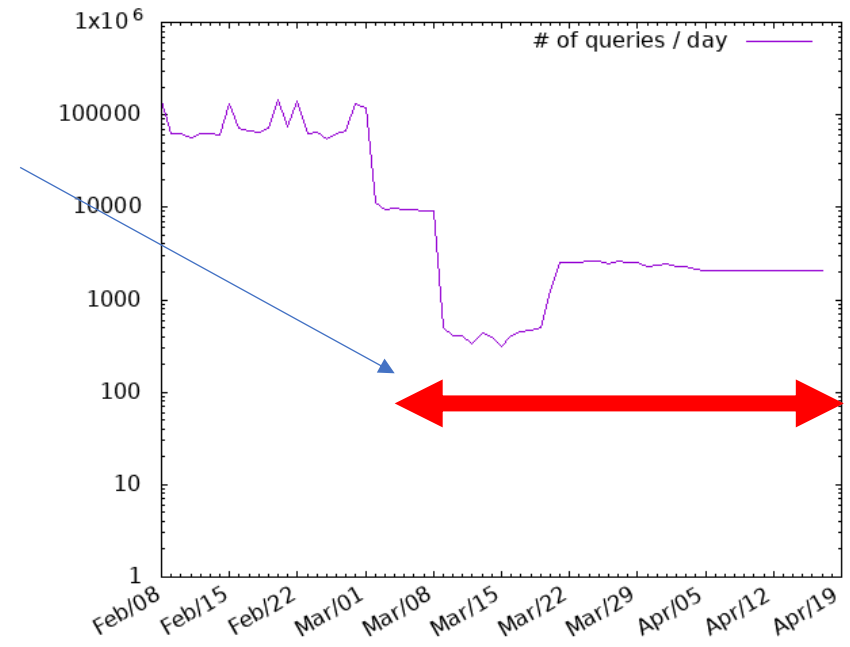
AS48285

- /24単位のドメイン名に対して
 - A
 - AAAA
 - NS
 - MX
 - TXT
 - SOA
 - NSEC
 - RRSIG
 - DNSKEY
 - SPF
- を5qpsぐらいで問い合わせで終了

該当ブロックは2/28返却
3/1午後には上位からNSも削除

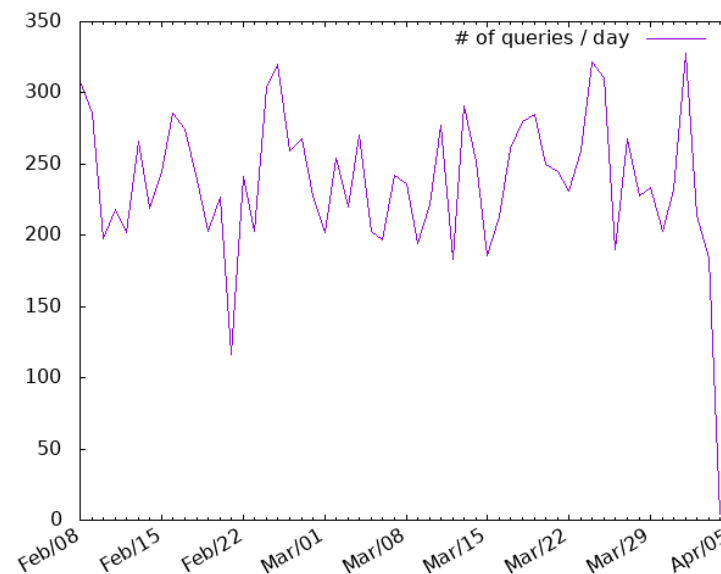
- 上位のNS TTLは86400 (1day)
- ゾーンのTTLは21600 (6hours)

- 何か執拗な人達がいる



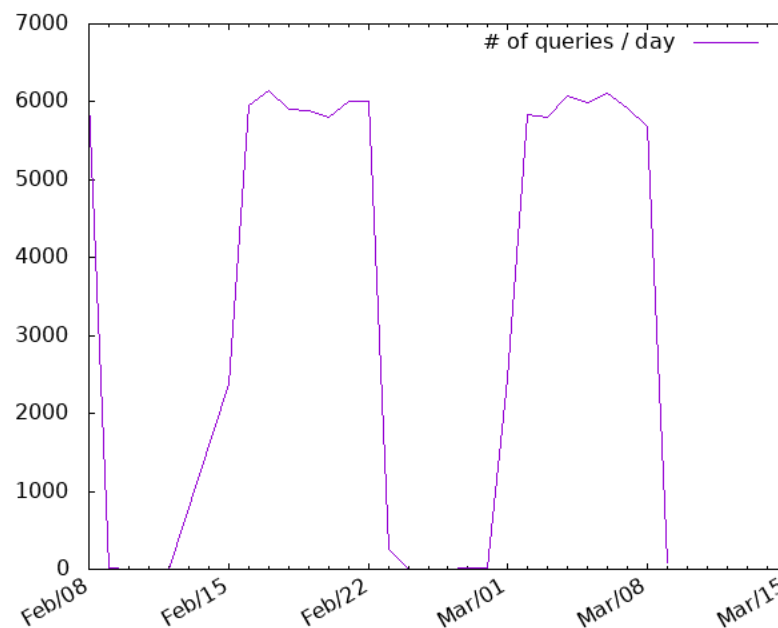
AS45021

- 不思議なパターン
 - 基本は固定ポートからのPTR問い合わせ
 - 概ね同じ問い合わせを同時に2回
 - 8秒後ぐらいに稀に同じ問い合わせをランダムなポートから問い合わせ
- 4月4日で終わり



AS20940 AS23454 AS24319 AS34164 AS35994

- ランダムな順序で0.07qps(13秒に1問合せ)程度
 - /24単位のドメイン名にANYを問い合わせ
 - 網羅的にPTR探索
 - 毎回44K問い合わせぐらい
 - 網羅率は2回で89%
- 3月9日で終わり



AS1280

- 3月17日までは/24単位の委譲を想定してNSを探索
- 3月22日からは0.025qps (40秒に1問合せ)程度で全PTR探索開始。現在も継続中で、あと数日で全探索が終わると思われる

