
■ IRS Workshop 16

日時 : 2008/04/22 (Tue) 15:00 - 18:00
場所 : Cisco Systems, G.K. 会議室

---

(1)「4octet-AS 実装(予定)最新状況と運用方法の検討」
発表者: NTT Communications 吉田さん、Cisco Systems 兼松さん、
Force10 Networks 宗像さん、Juniper Networks 河野さん、
物産ネットワークス 天田さん、Alaxala Networks 鈴木さん (発表順)

- AS allocation
  - 50000を越えている
  - 2007年に割り振りが上昇している原因は 4octet の割り振りが開始された為
  - いまは 40000番台の後半くらい

- ルール
  - 2007/03/06 まで : 2octet の AS番号を割り振りする
  - 2007/03/07 - 2008/12 : 原則として 2octet を割り振るが、希望がある場合には 4octet を割り振る
  - 2008/1 - 2008/12 : 基本的には 4octet を割り振る

- AS number format
  - asdot : <higher 16bit>.lower 16bit
  - asdot+ : higher 16bit.lower 16bit
    0. と表記をする必要がある
  - asplain : 32bit で表記をする
  - asip : いまは無い表記の方法。全部を 8bit で区切る

- AS Path Update
  - ^(200_)+(23456_)+$: これだけでは 4octet が分からない
  - ^(200_)+(2.10_)+$: 必須
  - ^(200_)+(131172_)+$: 相手が asdot 表記ではない場合にはこの記述になる
    しかし、asdot と asplain が混在して煩雑になる

- os version up 時には path の扱いに注意

- 議論をしたい事
  - AS_PATH UPDATE を続けるなら...?
    - 記述方式
    - asdot or asplain or both
  - ¥ の扱い
    - 記述して update を出すか?
  - AS_TRANS (AS23456) の扱い

  - 各社の記述方法の実装状況:

Cisco	Force10	Juniper	Foundry	Alaxala
asdot	asplain, asdot	asplain, asdot	N/A	N/A

- 他の方式？
  - IRR の AS-Set を参照し、origin based filter + prefix でフィルタをする？
    - IRR AS-SET Based Filter + prefix

◇ Cisco Systems - 4 byte ASN / シスコシステムズ 兼松さん

- 対応状況
  - IOS XR 3.4 CRS1 GSR
  - IOS 12.0S 2008 End (変更の可能性もあり)
    12.0SR 2008 End
    12.0SB 2008 End
    12.0SX 2008 End
    12.5T 2009 Q2
- 実装
  - RFC 4893
  - 表記方法: XX.YY
- 運用での変更点

  ・configuration (IOS XR)
  # router bgp ?
  - <1-65535>   AS $ for our autonomous system
  - <1-65535>.   AS $ for our autonomous system (xx.yy format)

  - router bgp 0.? とやると怒られる

  # router bgp 10.?
  - <0-65535>   second half of xx.yy.as number

  - 相手の AS 番号が 2octet の時は、これまでどおりの表記なり、0.? とは書かない
    - 自AS が 2-byte の時はこれまで通り
  - capability の箇所に 4-byte capable と表示される
  - 4octet に対応していない OS の場合には、23456 と表示される
- その他の注意事項など
  - capability の箇所に 4-byte capable と表示される
  - neighbor に 4byte ASN capable な人と not capable な人がいると update group は別になる
  - as-path filter
    - まだ、兼松さんは確認をする事が出来ていない
  - aggregate
    - 2-byte な人が 4-byte の経路を集約したらどうなる?

◇ FTOS AS4 サポート状況 / フォーステン・ネットワークス 宗像さん

- 対応状況
  - FTOS 7.7.1 からサポートされる予定
    - 5月中旬 GA リリース
  - extended community の同時サポート
  - FTOS 7.6.1 では未サポートとなっている
    - unknown/opt-trans として処理
  - E シリーズ、C シリーズで対応
- 実装方式
  - asplain 方式による configuration
  - FTOS 7.8.1 にて asdot 方式のサポートを予定
    - asdot+ のサポート予定は無い

    - デフォルトの振る舞いに変更は無し
    - コマンドライン (show debug) 出力は、asdot での表記
    - AS4 サポートに伴う、特別な CLI 追加 (show) は無し
    - 現状のコマンドからの追加は無し
  - ポリシー
    - dot の扱い
      - "." : any single character
      - "¥." : exact match

◇ JUNOS 4byte ASN support / Juniper Networks 河野さん

- JUNOS 9.1 (May 2008)
  - Notation -- asplain only
    - 正規表現 (regexp) との干渉が無い
    - シンプル
    - 本来階層概念はなかった
    - パースが早い
    - duplication check が早い
- JUNOS 9.2 (Aug 2008)
  - Notation -- asplain asdot
- asdot notation (R9.2 or later)
  - デフォルトは asplain 表記
  - 下記コマンドにより asdot 表記を行う
    - set routing-options autonomous-system asdot-notation
- parse の際...
  - 上記のコマンドの設定にかかわらず "." があれば asdot 表記とみなして解釈をする
  - "." を "." としてみたい場合にには "¥" をつける

◇ 4 octets ASN / Foundry Networks(物産ネットワークス) 天田さん

- 現状はどの機器も未サポート
- 対応予定機器は XMR/MLX シリーズ
  - XMR4000/8000/16000/32000
  - MLX4/8/16/32
  - 2008/12 - 2009/01 くらいをターゲット
  - IronWare 4.1 でサポートを予定 (現行は 3.8)
- 実装方式はまだ未確定
  - ユーザ要求や他社インプリを収集中

◇ 4byte-AS への対応方針・懸念事項 / Alaxala Networks 鈴木さん

- 現在は未対応
- 2008年度中のどこかで対応を検討中
- 実装方式
  - asdot で対応をしたい
    - asplain : 可読性が低い
    - asdot+ : 非現実的
- 運用上の変更点
  - ¥(4713_)+(2¥.0_)+$ と記述をする
  - "." の前後に 0 があってもかまわない
  - "¥." も 1文字 として勘定される
    - e.g.) 任意の 2/4byte-AS 1つ ([0-9.]+_)
- 推奨する正規表現の書き方
  - 正規表現の dot は別の表現に変えませんか？
    - 機械は困りませんが、人間が誤読します
      - e.g.) ^4713 2.10$ -> ^4713 2[0-9]10_$

^4713 .*_$ -> ^4713 [0-9.]*_$
- メイルで asdot を書く時は、常に ¥. で表記しませんか？
  - 人間は理解をする事が出来ますが、機械が誤読します
    - e.g.) ^47.3 を copy&paste すると、47.3 のみならず、47[0-9]3 もマッチする
  - asplain 実装も考えると、(asdot|asplain|astrans) という表記にせざるをえないか？
    - e.g.) AS47.3 -> (47¥.3|3080195|23456)
- 他に気になっていること
  - community をどうするか？
    - IPv4 address specific extended community で IPv4 アドレスの代わりに 4byte-AS を使用
    - local administrator field が 2byte に挟まるが、運用は可能か？
    - その場合の community 表示書式は？
  - sFlow や NetFlow v9
    - プロトコル的には 4byte-ready だが、実装は？

◇ 質疑応答

C: （ネットワーク管理つながりで）AS 番号の MIB はどうなるんだろう
- MIB
  - AS番号 MIB : snmp syntax = integer32 (0..65535)
  - 65536以上を「異常扱い」する SNMP Manager があることを危惧。
  - 当面は 23456 を返すしかない？

C: 4byte ASをAS番号MIBで返す時の挙動は以下の通り
- SNMP Manager 不明
- Juniper 不明
- Force10 不明

C: Flow Collector 側が対応していない。AS情報を無視する、経路自体を無視するといった可能性が考えられるため、下手に 4byte ASN を広告するのは危険。

A: (Flow Collector の) genie ATM とかは対応している。

C: show と config の regexp は同じノリで入れていいのか。ちょっと show で出てきたものを試して config したい

C: asplain がいいというが、AS番号はどこまでいくと考えているか。10年後、上の桁が100ぐらいまでいったとき、内部の実装はともかくとして、表現としてはわかりやすそう。

C: 長い番号が羅列しても、人間は区切って覚える。昔は携帯電話の番号は区切り方が違ったが、3桁4桁4桁になった。ドットがあろうとなかろうと、人間が覚えていく。機械の confusion よりは問題が少ないのではないか。

C: APNIC の配り方は confusing。表記に頼っているが、それとは無関係に割り当てたのが混乱することをしている。

C: いまは 1023 まで。単に量が出る予定がないのでそうしていると思う。(AS番号の増加は) 一年間で 3000 ぐらい。日本は 100 ぐらい。アジア全体でも数百個なのでそのぐらい reserve したのかと思う。

C: ちなみに電話番号のハイフンになったかどうかは、番号にハイフンはなく、人間が勝手に決めている。入力にハイフンはあっても、

ハイフンなしで記録する。内部の処理の問題と表現の問題は区別して考えるべき。

C: plain の方が regexp の問題はないので、back slash をケアする必要はない。チェックをするといっても難しい。ドットの方が文字として覚えやすいのではないか。IRR とかもドットになっている。あの辺はそもそも 4byte-as で入るのか。

C: show route の後に expression を書くが、その表現によって得られる結果と、config の as path 表現によって書く結果、as-path regular expression の書き方をしたときに、同じ挙動が期待したい。もし違うところがあればオペレータ的に罠ではないかと思う。

Q: OS を上げると直ぐ動くのか? config を入れる必要があるのか？

A: IOS XR 3.4 は 23456 は見えない?
見えないのではないか
A: Force-10 は default で disable, config を入れる必要がある
A: Juniper は default で 4 octet を動くか
A: Foundry はこれから考える
A: Alaxala はこれから考える

C: 容易に上げると、意図していない状態でも動いてしまう。準備していないとそういう状況が来るのが恐いので、すぐ動かない方が嬉しい。

---

(2)「ICMPv6とパケットフィルタの微妙な関係」
発表者: WIDE/JPIX 石田慶樹さん

- 前提
  - BCP38/IPv6 が当然の事となっている
  - 技術として uRPF が広く使われている
- 疑問
  - 中間ノードが ICMP エラーメッセージを返す場合に、その source アドレスは何か？
  - その source アドレスはアナウンスされているか？
  - ICMPv6 とソースアドレスフィルタリングはどちらを優先するか？
    - BCP38 vs RFC4890
- 思考実験
  - IX は IXP 用の IPv6 アドレスを利用している
  - その IPv6 アドレスはグローバルにアナウンスされていない
  - ISP はバックボーンでジャンボフレームを利用している
  - オリジナルサイズを利用
- 解決方法
  - みんなで MTU をジャンボフレームにする
  - みんなで MTU をオリジナルサイズにする
  - IX を含め全ての経路をアナウンスする
  - uRPF を利用しない
  - uRPF を適用する前に ICMPv6 (特に Type=2、Packet Too Big) は必ず通す

- 聞きたい事
  - ベンダ向け
    - ルータが返す ICMPv6 の source address は RFC 2463 -> RFC 3484 に従うとともに静的にも設定可能か？
      (traceroute などの reply は reachable な IP アドレスにしたほうが良い)
    - uRPF を適用する前に特定のパケットフィルタ (ICMPv6 のみ accept とか) のルールを適用する事は出来ますか？
  - xSP のオペレータ向け
    - IPv6 でも uRPF は使いますか？
    - IX の IPv6 prefix の経路情報は流れていたほうが良いですか？

C: net-hop self と connected の IP アドレス の話は IGP の話

C: 中間ノードの IP アドレスを隠蔽したい場合は、どのアドレスを source address にするのかどうか？

C: IPv6 の場合はリンクローカルアドレスを使用してプライベートピアをする場合も一緒の問題

Q: 途中のネットワーク上でフィルタされたら意味がないのではないか？
A: 皆でこうしようということ

Q: 1500 をまもっているから動いている
A: IPv4の世界では落とされている。だからこそ IPv6 では通せと書いてある

Q: firewall があって uRPF があるという順序
firewall を通って uRPF をスキップしないといけないという事か？
A: yes,

Q: DoS につかえないか？
A: ICMPv6 を reject はしてはダメだが、rate-limit はしても良い

C: ICMPv6 は ping-pong issue とかいやないことがある

C: IPv6 で uRPF は普通に動くし、パケットがどれぐらい来ているかみている

Q: TTL hack は？
A: BGP のセッションを守るのには有効だが、IX そのものに対する攻撃を防げない

Q: traceroute で見えるアドレスで、到達性のないアドレス空間にリナンバする作業をしている外部から traceroute すると * になって、上位の uRPF でフィルタしているのではないかと推測

Q: IX のプレフィックスは可能であれば流さないでほしい

C: IX 上で利用する IPv6 アドレスを広告するかどうかは IX が選べるように変わった

- やるべき事
  - I-D を書く
  - IETF/NANOG でプレゼンする？
  - ICMPv6 の RFC をアップデートする？

C: IX のアドレスのスコープの話ではなく、IX があってもアナウンスしたくない、ブラックボックス化したいが、source アドレスを何を選ぶかが本質
ISP がバックボーンのアドレスを隠蔽して、/128 をブラックホールに流すとか

C: IPv4 でもますます増えていく環境？

C: JANOG Comment では、source アドレスがプライベートアドレスなパケットはエッジで落とすことが推奨

---

(3)「JPIRRユーザへ経路ハイジャック通知実験開始します!」
発表者: JPNIC 岡田雅之さん

- IRR とは
  - whois のデータベースとは別
  - ルーティングに必要な情報を登録
  - 利用例
    - フィルタ作成
    - 連絡先のデータベース
  - 世界の IRR
    - RADB
    - RIR の IRR
    - ISP の IRR
  - どの IRR に登録をすれば良いのか？

- JPIRR
  - 経緯
    - 2002年 - 2006年 : 試験サービス
    - 2006/08 : 正式サービス
  - JPNIC が運営する IRR
    - ミラー先
    - RADB、NTTCOM、TELECOM-ISAC、APNIC、RIPE NCC

- JPIRR の利用方法
  - JPIRR への登録条件
    - IP 指定事業者
    - AS を JPNIC から割り当て
    - 特殊用途 PI アドレスを JPNIC から割り当て
    - 歴史的 PI アドレスを JPNIC から割り当て
  - IRRToolSet など
  - Route object
    - less specific
    - more specific
  - Aut-num object
    - AS 番号
  - AS-Set object

- 正式サービス化後のオブジェクト数推移
  - 2006/8 2006/3 順調に増えている
  - JPNIC 割り当て分の 3割 ぐらいの AS が登録

- 今回の実験の位置づけ
  - 経路制御品質維持手法の一つとして JPIRR を用いた経路ハイジャック検知手法の有効性を検証

- 実験をひとことで説明をすると？
  - Telecom-ISAC Japan の経路奉行で検知をした経路ハイジャックの情報を JPIRR ユーザへ通知する

- 経路ハイジャックが疑われる状態とは？
  - JPIRR へ登録された route object と異なる origin の経路が観測された状態
  - multiple origin など
  - Origin AS が違う

- 記述方法
  - Route object の descr: へ X-Keiro: と言う接頭語の後にメイルアドレスを記述する
    - X-keiro: hogehoge@example.com
  - Maintainer object の descr: に X-Keiro: を記述した場合は、Maintainer 配下の全ての route に X-keiro: を記述した事と同じになる

- 注意事項
  - いまのところ source:JPIRR のオブジェクトのみが検知対象となっている
  - ただ登録していると何も起きない

Q: 実験用のアドレスを流す等はない？
A: 一度使うと色がついてしまうのではないか
　RIPE の RIS では似た事をやっているので、出来なくはない

C: IRRd のバグが多い
近藤さんが修正したりする
RIPE のミラーが大変; 1GB 近くあるので立ち上げるのが大変

C: 普段はクエリが少ない
ただし時々たくさんアクセスが来る...

◇ 次回の IRS

・IRS17 2008/8/8 (金)
  - Cisco さん、いつもありがとうございます。
  - オリンピックの開幕日のようです