IETF89報告会
6man/v6ops, opsawgの報告

浅井大史（東京大学）
panda@hongo.wide.ad.jp

IETF89報告会

2014年4月11日

報告内容

- 6man/v6ops UPDATE
  - SLAACプライバシー・セキュリティ関係
  - Efficient ND
- opsawg
  - Writable mib moduleについてのIESGの声明

6MAN/V6OPS

6man / Agenda

- Working Group Documents
  - Introduction, Agenda Bashing, Document Status, New Charter, Chairs, 15 min.
  - Packet loss resiliency for Router Solicitations draft-ietf-6man-resilient-rs , Suresh Krishnan, 10 min.
  - Recommendation on Stable IPv6 Interface Identifiers draft-ietf-6man-default-iids , Fernando Gont, 15 min.
  - **Privacy Considerations for IPv6 Address Generation Mechanisms** draft-ietf-6man-ipv6-address-generation-privacy , Alissia Cooper, 15 min.
  - Analysis of the 64-bit Boundary in IPv6 Addressing draft-carpenter-6man-why64 , Brian Carpenter, 30 min.
- **Efficient ND session** (45 minutes)
  - Problem statement draft-yourtchenko-colitti-nd-reduce-multicast draft-vyncke-6man-mcast-not-efficient draft-chakrabarti-nordmark-6man-efficient-nd , Erik Nordmark, Eric Vyncke, 13 min.
  - Solutions within existing protocol specifications , Andrew Yourtchenko, Lorenzo Colitti, 13 min.
  - Unresolved problems and larger changes required , Erik Nordmark, 13 min.
  - Summary , Chairs, 5 min.
- Speed Talks (5 Minutes, 3 slides)
  - Transmission of IPv6 Packets over IEEE 802.11p Networks draft-petrescu-ipv6-over-80211p , Alexandru Petrescu, 5 min.
  - Triggering ND Address Resolution on Receiving DAD-NS draft-halpern-6man-nd-pre-resolve-addr , Helen Chen and Joel Halpern, 5 min.
  - IPv6 Universal Extension Header draft-gont-6man-ipv6-universal-extension-header , Fernando Gont, 5 min.
  - Validation of Neighbor Discovery Source Link-Layer Address (SLLA) and Target draft-gont-6man-lla-opt-validation , Ron Bonica, 5 min.

v6ops / Agenda

- Wednesday March 5, 9:00-11:30
  - Agenda Bashing
  - Why Operators Filter Fragments and What It Implies, <draft-taylor-v6ops-fragdrop>
  - IPv6 Roaming Behavior Analysis, <draft-ietf-v6ops-ipv6-roaming-analysis>
  - IPv6 Transitional Technology IPv4 Prefix, <draft-byrne-v6ops-clatip>
  - **Why Network-Layer Multicast is Not Always Efficient At Datalink Layer**, <draft-vyncke-6man-mcast-not-efficient>
  - **Reducing Multicast in IPv6 Neighbor Discovery**, <draft-yourtchenko-colitti-nd-reduce-multicast>
- Thursday March 6, 13:00-15:00
  - IPv6 Operational Guidelines for Datacenters, <draft-ietf-v6ops-dc-ipv6>
  - Balanced Security for IPv6 Residential CPE, <draft-ietf-v6ops-balanced-ipv6-security>
  - Recommendations of Using Unique Local Addresses, <draft-ietf-v6ops-ula-usage-recommendations>
  - DHCPv6/SLAAC Address Configuration Interaction Problem Statement, <draft-ietf-v6ops-dhcpv6-slaac-problem>
  - DHCPv6/SLAAC Interaction Operational Guidance, <draft-liu-v6ops-dhcpv6-slaac-guidance>

PRIVACY CONSIDERATIONS FOR IPV6 ADDRESS GENERATION MECHANISMS (6MAN)

Privacy Considerations for IPv6 Address Generation Mechanisms (6man)

draft-ietf-6man-ipv6-address-generation-privacy

- 各IPv6アドレスの設定・生成方法に関するプライバシーおよびセキュリティ評価
  - 評価項目
    1. Network activity correlation
       - ネットワーク上でのアクティビティの関連付け可能性
    2. Location tracking
       - 位置情報のトラッキング
    3. Address scanning
       - 外部からのアドレススキャン攻撃
    4. Device-specific vulnerability exploitation
       - デバイス固有の脆弱性に対するエクスプロイト攻撃

Privacy Considerations for IPv6 Address Generation Mechanisms (6man)

- 評価対象のアドレス設定・生成方法
  - Static manual：手動設定
  - Stateless Address Autoconfiguration (SLAAC)による自動設定
    - IEEE identifier: IEEEインターフェイスID（MACアドレス）を基にしたアドレス[RFC2464]
    - CGA：暗号的に生成するアドレス[RFC3972]
    - Temporary: Privacy extensionアドレス[RFC4941]
    - Constant, semantically opaque: ランダム・マイクロソフト方式
    - Stable, semantically opaque: [draft-ietf-6man-stable-privacy-address]
  - DHCPv6: DHCPv6による自動設定[RFC3315]

Privacy Considerations for IPv6 Address Generation Mechanisms (6man)

Mechanism	Correlation	Location tracking	Address scanning	Device exploits
IEEE identifier	Possible for device lifetime	Possible for device lifetime	Possible	Possible
Static manual	Possible for address lifetime	For address lifetime	Depends on generation mechanism	Depends on generation mechanism
Constant, semantically opaque	For address lifetime	For address lifetime	No	No
CGA	For lifetime of (public key + modifier block)	No	No	No
DHCPv6	Possible for lease lifetime (typically hours)	No	Depends on generation mechanism	No
Stable, semantically opaque	Within single network	No	No	No
Temporary	Only possible for temp address lifetime	No	No	No

9

引用元：IETF88におけるCooperらの発表資料。IETF89におけるCooperらの資料を元に変更

Privacy Considerations for IPv6 Address Generation Mechanisms (6man)

- WGLC？

  → Link localに関する議論をメーリングリストで

EFFICIENT ND (6MAN/V6OPS)

Efficient ND (6man/v6ops)

http://www.ietf.org/proceedings/89/slides/slides-89-6man-9.pdf

- RFC1970の想定
  - Shared medium
    - マルチキャストはユニキャストと同様に信頼性がある
    - マルチキャストの転送コストがユニキャストと同じ（NICのコストは高い）
  - ノードは常に電源が入っている
    - ホストをオンにするために必要な手順が最適化されていない
    - Multicast DAD（常に聞いている必要がある）

Efficient ND (6man/v6ops)

http://www.ietf.org/proceedings/89/slides/slides-89-6man-9.pdf

- 背景
  - Sleeping nodes [RFC6574: IAB Workshop]
    - Small, low-cost, battery-poweredなノード
      - バッテリー消費量を減らすためにスリープする
    - 定期的に起きて処理を実行する
    - 送信前に
      - ユニキャストNSでDetect Network Attachment (DNA)をルータに
      - Sometimes: DADをlink-local, global addressに対して行い、MLDパケットを出す
        - » EUI-64で3パケット以上のマルチキャストパケット
        - » RFC4941に従った場合はそれ以上
  - Radio Efficient Nodes (IEEE802.11 Low Power Wi-Fi clients)
    - CPUがスリープでも電波はそのまま
    - APビーコン間は電波を停止（100ms）
    - WiFi APは以下を保存
      - スリープ中のLow powerノードへのユニキャストフレーム
      - 「全ての」マルチキャストフレーム
    - Low powerクライアントはAPビーコンを受信して復帰
      - Traffic Indicator Map (TIM)：フレームがあるかどうかのビットマップ
        - » これを見て自分宛のフレームがあれば起きる

Efficient ND (6man/v6ops)

http://www.ietf.org/proceedings/89/slides/slides-89-6man-9.pdf

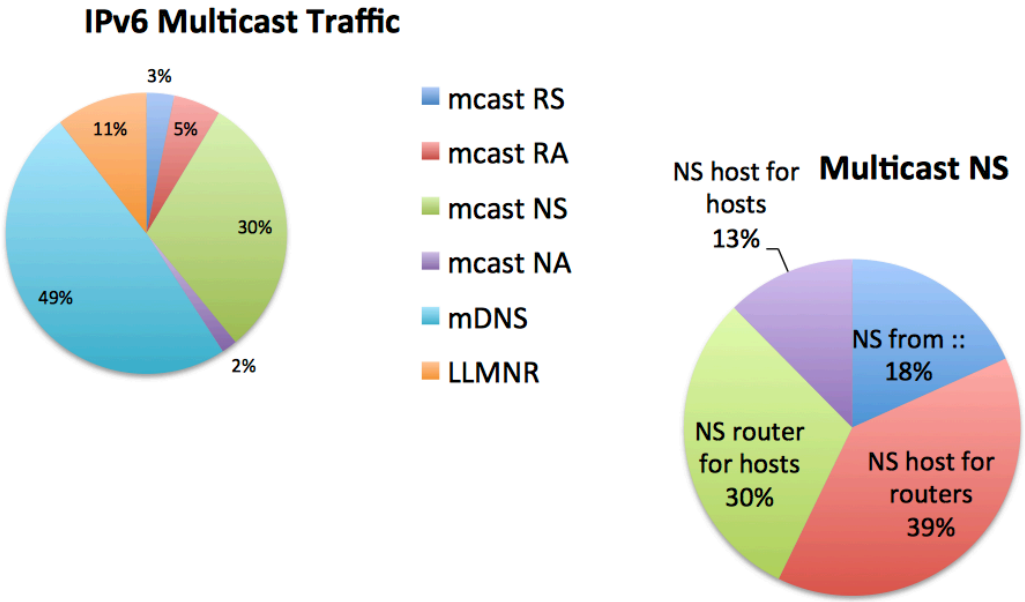
- 問題
  - マルチキャスト
    - 帯域の無駄遣い
      - ユニキャストの10倍以上の電波資源を使う(一番遅い送信速度を使うため)
      - RFC4541 MLD snoopingは？
        - » 一般にグローバルマルチキャストで実装
        - » EUI―64アドレスでないと動かない
    - スリープ中のノードの不必要な復帰
      - NICのフィルタ:ホストローカルな解法・帯域の無駄遣いは減らない
    - ND (RS, RA, DAD, address resolution)
  - DAD
    - 常にonでないとDADに反応できない
    - 1秒レスポンスを待つ必要がある
  - 他のDAD関係の問題
    - パケロスに対して弱い

Efficient ND (6man/v6ops)

http://www.ietf.org/proceedings/89/slides/slides-89-6man-9.pdf

Some data from IETF-hotel Wi-Fi

- Collected by a mostly silent node in promiscuous mode, 75% of IPv6 traffic was multicast



引用元：http://www.ietf.org/proceedings/89/slides/slides-89-6man-9.pdf

Efficient ND (6man/v6ops)

http://www.ietf.org/proceedings/89/slides/slides-89-6man-10.pdf

- NDの削減
  - ND multicast
    - DAD
      - 1 packet per IP address
    - RS
      - 1 packet per host
    - RA
      - Periodic: 1 packet every X seconds
      - Solicited: 1 packet for every host
    - NS
      - 1 packet for every new host

Efficient ND (6man/v6ops)

http://www.ietf.org/proceedings/89/slides/slides-89-6man-10.pdf

- NDの削減
  - ND multicast
    - DAD
      - 1 packet per IP address
    - RS
      - 1 packet per host
    - RA
      - Periodic: 1 packet every X seconds
      - Solicited: 1 packet for every host
    - NS
      - 1 packet for every new host

Efficient ND (6man/v6ops) : NDの削減

http://www.ietf.org/proceedings/89/slides/slides-89-6man-10.pdf

- Unicast solicited RAs
  - Solicited RAに対するRSをユニキャストにする
    - RFC的には問題なし
  - rate-limitをかけて、RSが多すぎる場合は multicast RAで送るべきだろう[SHOULD, probably]

Efficient ND (6man/v6ops) : NDの削減

http://www.ietf.org/proceedings/89/slides/slides-89-6man-10.pdf

- インフラ側でのマルチキャストフィルタリング
  - マルチキャストsnooping
    - SAVI [RFC6620]
  - マルチキャストをユニキャストに変換する
    - Pure 802.11
    - Unicast ethernet [RFC6085]
- Proxy ND
  - 802.11 infra modeではトラフィックは常にAPを通過する

Efficient ND (6man/v6ops) : NDの削減

http://www.ietf.org/proceedings/89/slides/slides-89-6man-10.pdf

- Periodic RAの送信間隔を長くする
  - 最大値
    - AdvDefaultLifeTime: 9000秒
    - MaxRtrAdvInterval: 1800秒
- Reachable Intervalを長くする
  - ルータが1つだけ or FHRP (VRRP, HSRP) ペアであれば問題無し

Efficient ND (6man/v6ops) : NDの削減

http://www.ietf.org/proceedings/89/slides/slides-89-6man-10.pdf

- Prefixのon-linkビットを0にする
  - link-local以外をoff-linkに
- ホストからのNSを削減
  - 注意
    - 1ホップ目のルータのリダイレクトを無効にする
      - » コントロールプレーンの高負荷防止
    - 全てのホストのトラフィックはルータへ

Efficient ND (6man/v6ops)：NDの削減

http://www.ietf.org/proceedings/89/slides/slides-89-6man-10.pdf

- DHCPv6の使用
  - ネットワーク上の全ステートを保存
    - DHCPv6のL3->L2マッピングを使用
    - ホスト間のNDを落とす
    - ホストへのNDに対してルータが代わりに答える
  - 問題：
    - DHCPv6をサポートしていないものがある
    - ネットワークがホストのアドレスをコントロールする
      - Privacy addressなどが使用できない

Efficient ND (6man/v6ops) : NDの削減

http://www.ietf.org/proceedings/89/slides/slides-89-6man-10.pdf

- スリープするときにインターフェイスを落とす
  - 問題 :
    - 復帰したときにさらに遅延が大きくなる
    - ネットワーク側から復帰出来ない
    - ユニキャストも落ちてしまう

OPSAWG / IESG : WRITABLE MIB

OPSAWG

- Writable MIB Module IESG Statement
  - March 2, 2014
  - http://www.ietf.org/iesg/statement/writable-mib-module.html

The IESG is aware of discussions in the OPS area and in a number of working groups about the current practice for standards-based approaches to configuration. The OPS area has shown strong support for the use of NETCONF/YANG while many working groups continue to specify MIB modules for this purpose. The IESG wishes to clarify this situation with this statement:

- IETF working groups are therefore encouraged to use the NETCONF/YANG standards for configuration, especially in new charters.
- SNMP MIB modules creating and modifying configuration state should only be produced by working groups in cases of clear utility and consensus to use SNMP write operations for configuration, and in consultation with the OPS ADs/MIB doctors.