非PC系デジタル機器のIPv6最小仕様

(tiny@tahi.org活動紹介)

㈱東芝　研究開発センター
井上　淳
inoue@isl.rdc.toshiba.co.jp

Outlines

- TAHI Projectの経緯
- tiny@tahi.orgグループ設立の経緯
- 仕様検討とドラフト化
- IETF発表とその結果
- その他の活動

TAHI Projectの経緯

TAHI Projectと関わりの深い、国内のIPv6研究／開発活動

- KAME Project
  - 1998/4に活動開始
  - IPv6 参照コードの提供と標準化への貢献
  - 富士通(株)、(株)日立製作所、(株)インターネットイニシアティブ、日本電気(株)、(株)東芝、横河電機(株)
  - http://www.kame.net/

- USAGI Project
  - 2000/1に活動開始
  - LinuxのためのIPv6開発
  - (株)日立製作所、NTTソフトウェア(株)、(株)東芝、横河電機(株)、東京大学、慶応大学
  - http://www.linux-ipv6.org/

- TAHI Project
  - 1998/10活動開始
  - IPv6検証技術の開発とテストイベントの主催
  - 東京大学、横河電機(株)
  - http://www.tahi.org/

TAHI Project の経緯

- 1998/10/1 活動開始
  - KAME Project との連携
  - IPv6テストツールの開発、公開
  - IPv6テストイベントの主催
  - 他テストイベントの支援
- 2000/4/1 USAGI Projectとの連携開始
  - Linux IPv6カーネルの品質向上

TAHI Projectの経緯

- 2001/3/1「IPv6最小仕様」の活動開始
  - Low Cost Network Applianceをターゲットとし
    - IPv6最小仕様の検討
    - テストツールの開発、公開
- 2001/11/19 ETSI、IRISAとの連携開始
  - Mobile IPv6を中心としたテストツールの共同開発
  - テストイベントのCooperation

テスト・イベント

- **主催：**
  - 1999/09/26-10/01: 1st TAHI IPv6 Interoperability test event @ Tokyo
  - 2000/07/15-18: 2nd TAHI IPv6 Interoperability Test Event @ Yokohama
  - 2002/01/23-26: 3rd TAHI IPv6 Interoperability Test Event @ Yokohama (**予定**)
- **他テストイベントの支援：**
  - 2000/03/02-09: Connnectathon @ San Jose
  - 2001/03/01-08: Connnectathon @ San Jose
  - 2001/11/19-23: ETSI 2nd IPv6 Plugtests @ Cannes, France

2nd TAHI IPv6 Interoperability Test Eventの風景




tiny@tahi.orgグループの経緯

グループの位置付け

- H13年度IPAプロジェクト「情報家電の相互接続安全性技術仕様策定と検証に関する研究開発」の一環
  - 仕様策定（tiny@tahi.org）
  - 検証・参照ソフト開発（横河さん@TAHI）
- 本グループが最小仕様の素案を作る
  - IPv6関係者として
  - 個別機器の実装者の立場で
- INTAP情報家電安全性技術委員会
  - 上位組織・オープンコンソーシアム(netha@intap.or.jp)
  - 仕様の確認

実施体制

ネット家電のセキュリティ仕様と、検証及び相互接続性技術の研究開発プロジェクト

リーダ ：東大 江崎浩助教授
事務局： INTAP

WIDEプロジェクト

TAHI
プロジェクト

- 東京大学
- 横河電機
- YDC

現在のメンバー

- 検討メンバーとして以下のベンダ、組織の研究者、実装者が参加：

(株)ACCESS
(株)創夢
東京大学
(株)東芝
横河電機(株)
IP infusion Inc.
セイコーエプソン(株)
Dallas Semiconductor
(株)日立製作所
松下電器産業(株)
松下伝送システム(株)

- １１組織、２０名以上

仕様策定

最小仕様検討の目的

- 家電などの一般消費財にふさわしいIPv6実装のガイドラインを作成すること:
  - 低コスト
  - 限られたROM、RAM容量
  - 物理的サイズの制約
  - 非力なCPU
  - ネットワークを知らない人が使う
  - 使用目的が限定されている

仕様策定の方法

- 既に製品を持っている人がコミットしている
  - http://www.i-node.co.jp/
  - http://www.access.co.jp/
- 実装担当者がコミットしている

→実製品を意識し、リソース制約、実際の利用モデルを考慮して、IPv6フル仕様の実装妥当性を検討し、「ベースライン仕様」を策定する

→特定利用形態のオプション仕様については、それを実装することのインパクトを明示する

LCNA example (IP sensor)

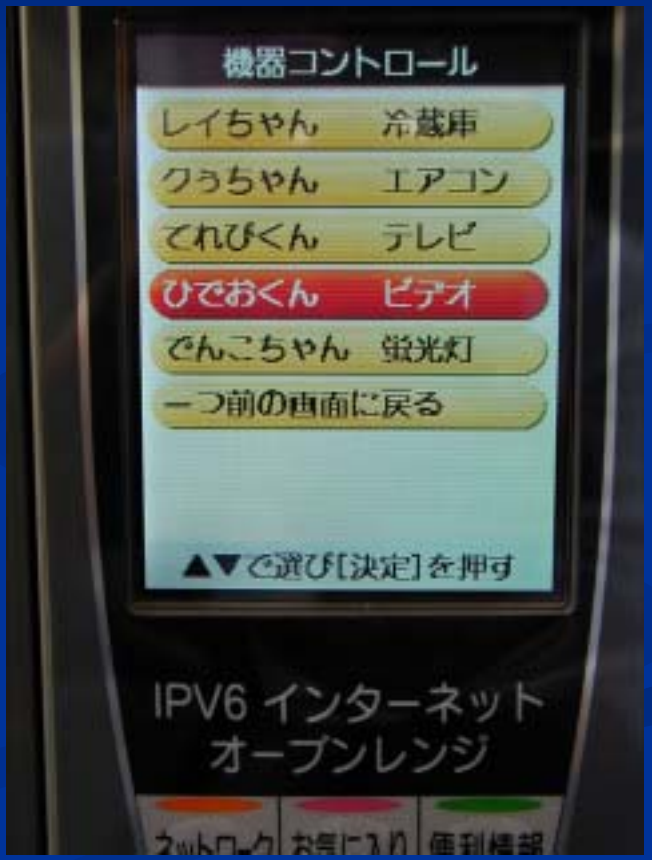
- SIMM size
- 1MROM
- 1MRAM
- 8bits,40MHz
- IPv4: 7KB
- IPv6:21KB
- JVM
- HTTPD, Telnet, Ftp

LCNA example (Home appliances)

Toshiba Internet Refrigerator

LCNA example (Home appliances)

Panasonic Internet Microwave Oven



大量のInternet-drafts

- Internet-Drafts:
  - IPv6 Node Information Queries (33418 bytes)
  - A flexible method for managing the assignment of bites of an IPv6 address block (15862 bytes)
  - Advanced Sockets API for IPv6 (172229 bytes)
  - Internet Control Message Protocol (ICMPv6)for the Internet Protocol Version 6 (IPv6) Specification (36802 bytes)
  - Default Address Selection for IPv6 (53023 bytes)
  - IP Version 6 Addressing Architecture (52282 bytes)
  - IP Version 6 Scoped Address Architecture (48889 bytes)
  - Basic Socket Interface Extensions for IPv6 (78930 bytes)
  - Unicast-Prefix-based IPv6 Multicast Addresses (13623 bytes)
  - IPv6 Stateless DNS Discovery (19866 bytes)
  - Default Router Preferences and More-Specific Routes (28847 bytes)
  - Avoiding ping-pong packets on point-to-point links (10038 bytes)
  - An analysis of IPv6 anycast (22718 bytes)
  - Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (50091 bytes)
  - Analysis of DNS Server Discovery Mechanisms for IPv6 (76678 bytes)
  - Management Information Base for the Internet Protocol (IP) (111232 bytes)
  - Management Information Base for the Transmission Control Protocol (TCP) (46599 bytes)
  - IP Forwarding Table MIB (57237 bytes)
  - Management Information Base for the User Datagram Protocol (UDP) (37964 bytes)

大量のRFCs

- RFCs
  - An Architecture for IPv6 Unicast Address Allocation (RFC 1887) (66066 bytes)
  - DNS Extensions to support IP version 6 (RFC 1886) (6424 bytes)
  - Path MTU Discovery for IP version 6 (RFC 1981) (34088 bytes)
  - OSI NSAPs and IPv6 (RFC 1888) (36469 bytes)
  - TCP and UDP over IPv6 Jumbograms (RFC 2147) (6383 bytes)
  - Advanced Sockets API for IPv6 (RFC 2292) (152077 bytes)
  - IPv6 Multicast Address Assignments (RFC 2375) (14356 bytes)
  - An IPv6 Aggregatable Global Unicast Address Format (RFC 2374) (25068 bytes)
  - IP Version 6 Addressing Architecture (RFC 2373) (52547 bytes)
  - Neighbor Discovery for IP Version 6 (IPv6) (RFC 2461) (222516 bytes)
  - IPv6 Stateless Address Autoconfiguration (RFC 2462) (61210 bytes)
  - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (RFC 2463) (34190 bytes)
  - Transmission of IPv6 Packets over Ethernet Networks (RFC 2464) (12725 bytes)
  - Transmission of IPv6 Packets over FDDI Networks (RFC 2467) (16028 bytes)
  - Transmission of IPv6 Packets over Token Ring Networks (RFC 2470) (21677 bytes)
  - IPv6 Testing Address Allocation (RFC 2471) (7991 bytes)
  - Internet Protocol, Version 6 (IPv6) Specification (RFC 2460) (85890 bytes)
  - IP Version 6 Management Information Base for the Transmission Control Protocol (RFC 2452) (19070 bytes)
  - IP Version 6 Management Information Base for the User Datagram Protocol (RFC 2454) (15858 bytes)
  - Management Information Base for IP Version 6: Textual Conventions and General Group (RFC 2465) (77339 bytes)
  - Management Information Base for IP Version 6: ICMPv6 Group (RFC 2466) (27547 bytes)
  - Proposed TLA and NLA Assignment Rules (RFC 2450) (24484 bytes)
  - IP Version 6 over PPP (RFC 2472) (29696 bytes)
  - Generic Packet Tunneling in IPv6 Specification (RFC 2473) (77956 bytes)
  - Transmission of IPv6 Packets over ARCnet Networks (RFC 2497) (10304 bytes)
  - IP Header Compression (RFC 2507) (106292 bytes)
  - Reserved IPv6 Subnet Anycast Addresses (RFC 2526) (14555 bytes)
  - Transmission of IPv6 over IPv4 Domains without Explicit Tunnels (RFC 2529) (21049 bytes)
  - Basic Socket Interface Extensions for IPv6 (RFC 2553) (89215 bytes)
  - IPv6 Jumbograms (RFC 2675) (17320 bytes)
  - Multicast Listener Discovery (MLD) for IPv6 (RFC 2710) (46838 bytes)
  - IPv6 Router Alert Option (RFC 2711) (11973 bytes)
  - Format for Literal IPv6 Addresses in URL's (RFC 2732) (7984 bytes)
  - DNS Extensions to Support IPv6 Address Aggregation and Renumbering (RFC 2874) (44204 bytes)
  - Router Renumbering for IPv6 (RFC 2894) (69135 bytes)
  - Initial IPv6 Sub-TLA ID Assignments (RFC 2928) (11882 bytes)
  - Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (RFC 3041) (44446 bytes)
  - IP Version 6 Management Information Base for the Multicast Listener Discovery Protocol (RFC 3019) (28293 bytes)
  - Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification (RFC 3122) (40416 bytes)
  - IPv6 multihoming support at site exit routers (RFC 3178) (24453 bytes)
  - Transmission of IPv6 Packets over IEEE 1394 Networks (RFC 3146) (16569 bytes)

最小ホストの前提

- ホストであり、ルータでない
- IPv6のExtension headerは送信しない
  - 現時点の仕様ではMobile IPv6機能以外にはホストがextension headerを出す必要はない
- ネットワークI/Fを１つのみ持つ（複数あると以下が要検討になって面倒！）
  - Source address selectionが煩雑になる
  - Routing informationの管理が必要
  - ND関連のキャッシュエントリが増える（近隣キャッシュ、デフォルトルータリスト、プレフィックスリストなど）

検討対象外の機能

- 明らかに最小ホストでは不要と思われる機能
  - アドレス割り当て関連
  - Jumbogram関連
  - Multicast, anycast関連
  - MIB、ヘッダ圧縮、PPP/Ether以外のL2対応

  →あまり深く考えていない、多分に直感的
- IPv4からの移行技術も検討対象外
  - 純粋なIPv6ネットワークの通信のみを対象とする
  - 正直言うと、IPsecのNAT対応が厄介
  - 実際には、接続試験の対応など要検討だが……

検討のポイント(RFC2460)

- 最小ホストなので、extension headerつきパケットは送信しない
  →受信したときの最低限の動作を規定する
  - 未サポートのヘッダ……ICMP param problemを相手に返す
  - 未サポートのオプション…オプション毎のエラー処理
- Extension headerの機能が不要なら、順序チェックは省略可能

Extension headerの処理(RFC2460)

- Hop-by-Hop option header
  - headerとして認識し、オプションに沿って処理
- Routing header, Destination header
  - Mobile IP（と経路最適化）する場合、このヘッダを使用
- Fragment header
  - Fragment処理はバッファメモリを浪費するのでできれば避けたい
  - 例えばTCPでMSS(Max Segment Size)を絞って、パケットサイズを制限するとか（UDPは？）
  - これによりPMTU発見もサボる

検討のポイント(RFC2461-2463他)

- ND(RFC2461):ルータ用機能を省略できる
  - RAの送信、RSの受信、redirectの受信
- アドレス重複検出(DAD)はNDが実装されていれば実装できるので原則として実装すべき
  - ネットワークブートされるホストは別途要検討
- ICMPv6：ルータでのみ使用のICMPは省略
- DNS:AAAAは必須、A6は様子見

検討のポイント(IPsec)

- ホスト同士のTransport modeのみに限定
  - Security Gatewayが関与する通信は検討外
- ノード同士が最低1回は安全に通信できると仮定
  - CAなどの特別な認証インフラは仮定しない
- 標準化が未決なものは対象外
  - マルチキャスト、IPsec MIB、IPsec固有なICMP

検討のポイント(IPsec)

- プロトコルはESPのみ実装必須
  - 暗号化NGな場合はNULLアルゴリズム
  - AHは最小仕様から省く
- SAパラメータの最小構成
  - Src/Dst IPv6 addr, SPI, Protocol, ESP(alg,key,IV),
  - HMAC(alg, key), seq-counter, replay protection
- アルゴリズム
  - AES（鍵長128ビット）は実装必須
  - 認証はHMAC-SHA2-256を実装必須

検討のポイント(IPsec)

- 手動鍵管理は実装必須
  - 自動鍵管理は実装必須としない
  - 実装した場合、SAパラメータとして生存時間が加わる
- 鍵交換アルゴリズム→IKEは不適当
  - 処理が煩雑、例外処理が不明確
  - IPアドレス固定を仮定
  - より軽量なアルゴリズム、IKEの改良版が望まれる
  - 鍵配布センターモデル（KDC）も利用モデルによっては使えそう

ドラフト化とIETF発表

00版ドラフト化

- IPv6最小要求仕様 (3章) はほぼ同じ
- セキュリティ仕様 (4章) を大幅に変更
  - 手動・自動鍵交換の定義を明確化
  - そもそもIPSECがLCNAできちんと使われるかの懸念を表明(4.1)
- Security Considerationを追加

00版ドラフトの検討課題

- Mobile IPv6
- セキュリティ
- ドラフトの落とし所
- 今後の動向を見守るべき標準化案

00版ドラフト検討課題：Mobile IPv6

- Mobile IPv6に関しては、オプション扱いだった。
  - 「すべてのIPv6ノードは、移動ノードと通信できねばならない」という強い要求があった：
    - Home Address Option の解釈
    - Binding Cache　の扱い

00版ドラフトの検討課題：Mobile IPv6

- 課題：
  - Home Address Option
    - 「すべてのIPv6ノードで解釈は必須」となっている。
    - しかし、潜在的なセキュリティ問題が指摘されている。
  - Binding Cache
    - 実装は必須とされていないので、ICMPエラーを返すのも可能。
    - Binding Updateのセキュリティ議論が収束していない。
- そこで、
  - 当面、Mobileip WGの議論を見守る。

00版ドラフト検討課題：セキュリティ

- 課題：
  - 家庭のネットワークであってもセキュリティは重要。
  - しかし、LCNAは資源とコストが厳しいので、IPsecやSSLの実装が困難な場合がある。
  - IPv6が普及したら、ネットワーク構成が変化しないか？
    - 複数アドレス、マルチホーム、モーバイル、、、
  - 家庭のネットワーク構成はどうなるか？
    - ホームルータで一極管理、無線でマルチホーム、、、
  - などなど、、、
- そこで、
  - 議論と検討は継続する；
  - 上述した課題を洗い出し、整理する。
  - IPv6普及・高度化推進協議会（http://www.v6pc.jp）セキュリティWGとのリエゾン。

00版ドラフト検討課題：ドラフトの落とし所

- 本ドラフトの狙い：
  - われわれの議論と経験を、他の開発者を共有する。
  - LCNA実装者のIPv6開発を支援する。
  - LCNAに適したIPv6のガイドラインを、ドキュメントとして残す。
- そこで、
  - 標準化 (Standard track) でなくてよい。
  - InformationalやBCP (Best Current Practice)でも十分。

00版ドラフトの検討課題：今後の動向を見守るべき標準化案

- Mobileip
  - draft-ietf-mobileip-ipv6-XX
- Default Address Selection
  - draft-ietf-ipngwg-default-addr-selection-XX
- Stateless DNS Discovery
  - draft-ietf-ipngwg-dns-discovery-XX
- **他のIPv6最小仕様**
  - draft-manyfolks-ipv6-cellular-host-XX

IETF52～懸念と実際

- LCNAのイメージが欧米人に理解しもらえるか？
  - I-nodeを例として引いて補足
  - コストが重要という点が若干弱かった
- Nokiaグループ（セルラホスト最小仕様）との関連
  - Co-chairのSteve Deeringは、2件を“Node Requirement”とまとめたカテゴリで扱った
  - が、実際は、Nokia組は今回はもう1件の3GPPドキュメントとセットでIETFとのリエゾンを図る意味の参加であった
- 特に質疑応答なし
  - この時点ではWGとして、Node requirementをどう扱うかのwillが不明確だった
  - IDを今後どうしたいのかを明確にすべきだった？

01版ドラフトへの更新

- IETF52以降のMLでの議論を反映
  - Multicastの規定（MLDなし）
  - Mobile IPv6関係の記述を明確化
    - 2.8節、5章を追加
    - 関連拡張ヘッダの記述を変更
  - Default Address Selection for IPv6の章を新設
  - その他editorialな誤りを修正
- セキュリティの章を大改定
  - IPsec必須をなくし、必要なレイヤでアプリに応じた適切なセキュリティ機構を保持すること、と変更
  - その代わり、従来のIPsecを仕様の削減例として、付録に掲載

IETF53直前の状況

- Nokia組Cellular最小仕様が更新ドラフトを出した
  - IPsecはOptional？
  - DADもOptional？
  - NDだって必須じゃない
  - ……..
- IPv6WGのML上で大議論！！
  - 原理主義者の怒りに触れた
  - 我々も、さりげなくIPsecは必須じゃないと書いたのだが

01ドラフトの課題

- IPsecの扱い
  - 一旦、optionalとしたが、WGの世論に負け、02でゆり戻し
    - 実装仕様を削るのはVendorがat its own responsibilityで
- LCNAの場合、ネットワークモデル、利用モデルの暗黙の了解がない
  - 家電機器 LCNA＋ホームゲートウェイのモデル
  - センサ型LCNAと情報収集サーバのモデル
- セキュリティソリューションの客観的評価データがない
  - ただ重いというのではなく、データに裏打ちされた主張を！
- Standard trackはNodereqに任せ、Informational or BCPを目指す

IETF53後の状況

- NokiaのJohn Loughneyをリーダにして Generic Node requirement検討チームが発足
- tiny@tahi.orgから4名（岡部、井上、石山、坂根）が参加
- 現在、ML上で仕様策定に向け議論中

Node requirement検討Team

- John Loughney
- Marc Blanchet
- OKABE Nobuo
- Jari Arkko
- Ito-jun
- Samita Chakrabarti
- Alain Durdand
- Dave Thaler
- Margaret Wasserman
- Inoue-san
- Rajiv Raraghun
- Masahiro-san
- Juha Wiljakka
- Joseph T. Klein
- Bob Hinden
- Steve Deering

検討プロセス

- 3 Types (from 2580)
  - Unconditionally Mandatory
    - i.e. - 2460
  - Conditionally Mandatory
    - I.e. – IPv6 over Ethernet
  - Unconditionally Optional
    - All the rest …
- Will need to go into details of the standards.
- Focus on Standards Track documents.
- Shoot for a Standards Track document.
- Any corrections, clarifications, etc. need to be done in the original specifications.

その他の活動

- ドキュメント、最新仕様→TAHIページで公開
  http://www.tahi.org/minspec/
- IPSJ学会誌9月号解説記事
- Global IPv6 Summit in Japan2001で発表
- IPv6 Journal冬号
- 日経バイト1月号（？）
- v6start.net(2002/2/12)

関連活動、他組織との連携

- IPv6普及・高度化推進協議会（http://www.v6pc.jp/）セキュリティWG
  - IPv6を普及させるに必須なセキュリティ課題を議論する。情報家電も議論の範囲。
  - LCNAのセキュリティ標準化という点で、協調する必要がある。
- Nokia (http://www.nokia.com/)
  Ericsson (http://www.ericsson.com/)
  - セルラ向けIPv6最小仕様を検討（draft-manyfolks-ipv6-cellular-host-02.txt）
  - 広義でのホスト要求というカテゴリで協調する必要あり。
  - 2001/8/13にヘルシンキでミーティング開催
- ETSI(http://www.etsi.org/)、
  IRISA (http://www.irisa.fr/)
  - Mobile IPv6を中心としたConformance Test Suitesの共同開発。
  - IPv6テストイベントの共同開催（日本、EU）

連絡先

- tiny@tahi.org
- http://www.tahi.org/

謝辞

- 本活動を含めTAHI Projectのすべての活動は、WIDE Project (http://www.wide.ad.jp/) の支援なしにはできませんでした。
- 現在のTAHI Projectの活動は、INTAP (http://www.intap.or.jp/)の支援により運営されています。