セッション P12

IBM eServer iSeries

iHOPE
iSeries Hands-On Professional Education

TCP/IP IPv6 入門

特記事項

当資料で解説される項目の更に詳細な説明は、製品から提供されるマニュアル、オンライン・ヘルプ、Web上の情報を参照してください。

当資料は、2003年4月現在のIBMその他の製品情報に基づいて作成されております。この資料に含まれる情報は可能な限り正確を期しておりますが、日本アイ・ビー・エム株式会社による正式なレビューは受けておらず、当資料に記載された内容に関して日本アイ・ビー・エム株式会社および日本アイ・ビー・エム　システムズ・エンジニアリング株式会社が何ら保証をするものではありません。したがって、この情報の利用またはこれらの技法の実施はひとえに使用者の責任においてなされるものであり、当資料の内容によって受けたいかなる被害に関しても一切の保証をするものではありませんのでご了承ください。

商標

以下の用語は、アメリカ合衆国、あるいは他国、あるいは両国でのIBM Corporationの商標です:

- AS/400
- AS/400e
- DB2
- IBM
- MQSeries
- Operating System/400
- OS/400
- SanFrancisco
- stylized 
- WebSphere
- 400
- iSeries
- eServer

以下の用語は、アメリカ合衆国、あるいは他国、あるいは両国でのLotus Development社の商標です:

- Domino
- Domino.Doc
- LearningSpace
- Lotus
- QuickPlace
- Sametime

JavaとすべてのJavaをベースとする商標およびロゴは、アメリカ合衆国、他国、あるいは両国のサン・マイクロシステムズ社の商標または登録商標です。

Microsoft Windows, Windows NT, およびWindowsのロゴは、アメリカ合衆国、他国、あるいは両国のマイクロソフト社の商標です。

他の会社、製品、およびサービス名は、その会社の商標あるいはサービスマークかもしれません。

このプレゼンテーションに含まれるサードパーティーに関連する題材は、これらのサードパーティーから得られた情報に基づいています。これらの情報の正確さの確認のための、いかなる努力もなされていません。このプレゼンテーションは、いかなるサードパーティー製品またはサービスの、IBMによる推薦あるいは指示を表したり、ほのめかすものではありません。

Notes:

このページはブランクです。

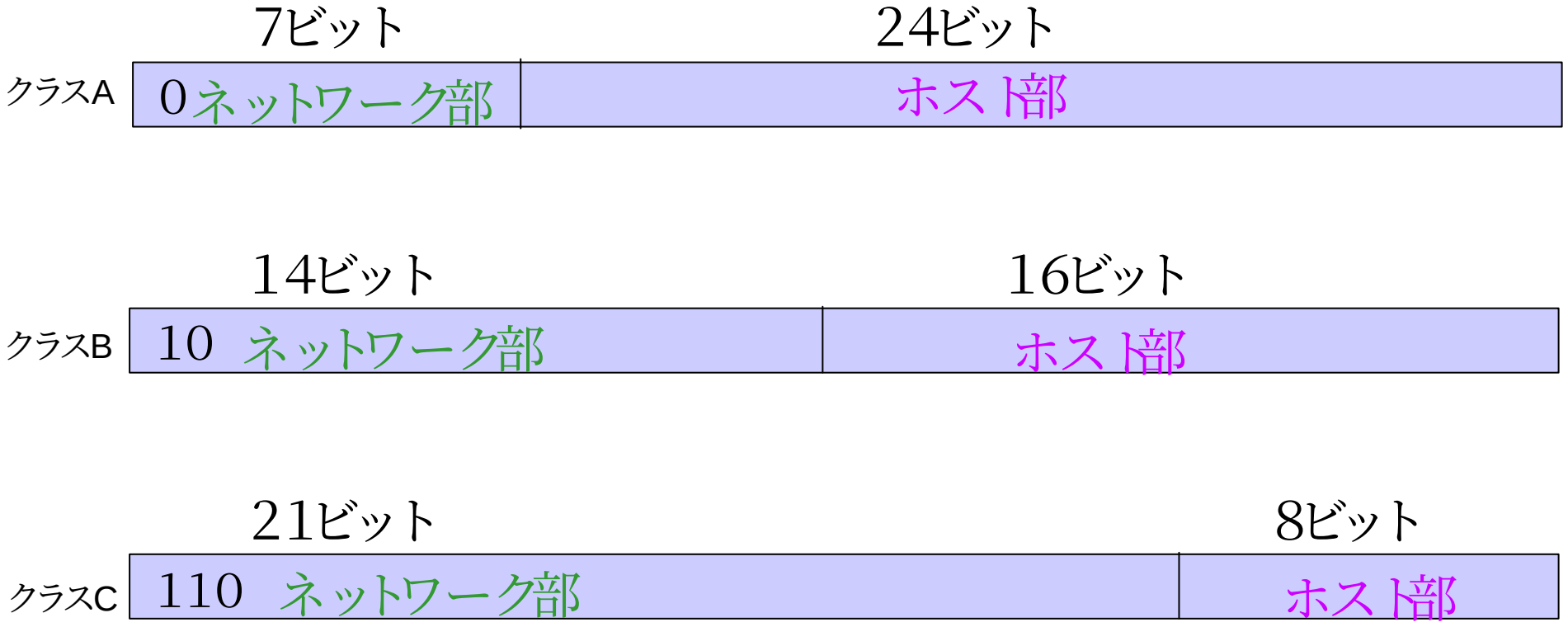
第1章
IPv4の問題点

IPv4の問題点

- IPアドレスの割り当て
- 経路指定

IPアドレスの割り当て

- IPアドレスの割り当てとIPアドレスの枯渇



Notes:

IPアドレスの割り当て
インターネット（Internet)の割り当ては、IANA（Internet Assigned Number Authority)で割り当てます。
しかし、爆発的に増加したネットワークでは、IPの枯渇の問題があげられます。
現在、次のようにクラスを分けていますが、現在クラスAを新たに取得することはできません。

クラスA
先頭ビットが'0'で、ネットワーク部は7ビットからなり、ホスト部は、２４ビットからなります。
大規模ネットワークの構成ができます。最大で16，777，214のホストを接続できます。
インターネット全体で、１２８の組織に割り当てできます。

クラスB
先頭ビットが' 10'で、ネットワーク部は１４ビットからなり、ホスト部は、１６ビットからなります。
中規模ネットワークの構成ができます。最大で65、534のホストを接続できます。
インターネット全体で、１６、３８４の組織に割り当てできます。

クラスC
先頭ビットが'110'で、ネットワーク部は２１ビットからなり、ホスト部は、８ビットからなります。
小規模ネットワークの構成ができます。最大で２５４５のホストを接続できます。
インターネット全体で、2，097，152の組織に割り当てできます。

経路指定

- 経路表の情報
  - ネットワーク・アドレス
    - ホスト部の全てのビットを0にしたアドレス
  - ネットワーク・マスス
    - ネットワークアドレスと、上位何ビットまでがネットワーク部なのかを示す
  - 次の宛先インターフェースのアドレス
    - ネットワークアドレスで示すグループに到達するための次のインターフェースのアドレス

Notes:

- 経路表の情報
  経路表は次の情報を含み、送信したいIPが指定のネットワーク上のホストに到達できるようにします。
  この方法で管理した場合に、経路表は膨大になり、中継での性能が低下します。

  - ネットワーク・アドレス
    - ホスト部の全てのビットを0にしたアドレス
  - ネットワーク・マスク
    - ネットワークアドレスと、上位何ビットまでがネットワーク部なのかを示す
  - 次の宛先インターフェースのアドレス
    - ネットワークアドレスで示すグループに到達するための次のインターフェースのアドレス

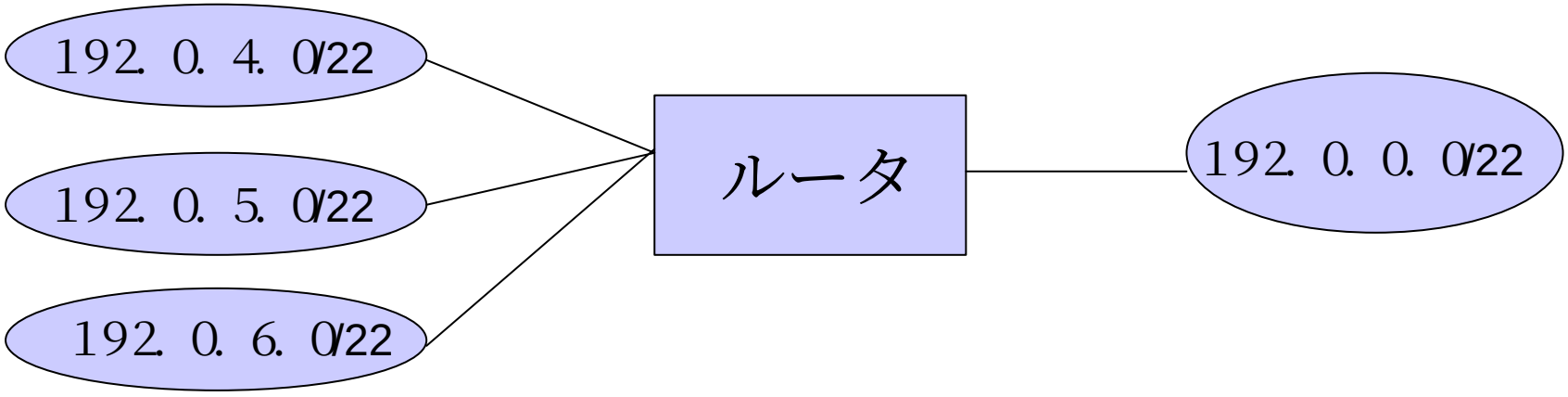
第2章
IPv4での対応

現在の問題への対応と次期IPの検討

- IPv4の問題とCIDRの導入
- NAT機能

IPv4の問題とCIDRの導入

- IPv4の問題
  - 300のホストでクラスBを割り当てると
  - 65、000以上のIPアドレスが無駄になる。
- 中規模ネットワークが増大し続けている
  - ルータの経路表が増大している
- CIDR（Classless Inter-Domain Routing)の導入
  - IPアドレスの無駄をなくす
  - 経路表を小さく維持する

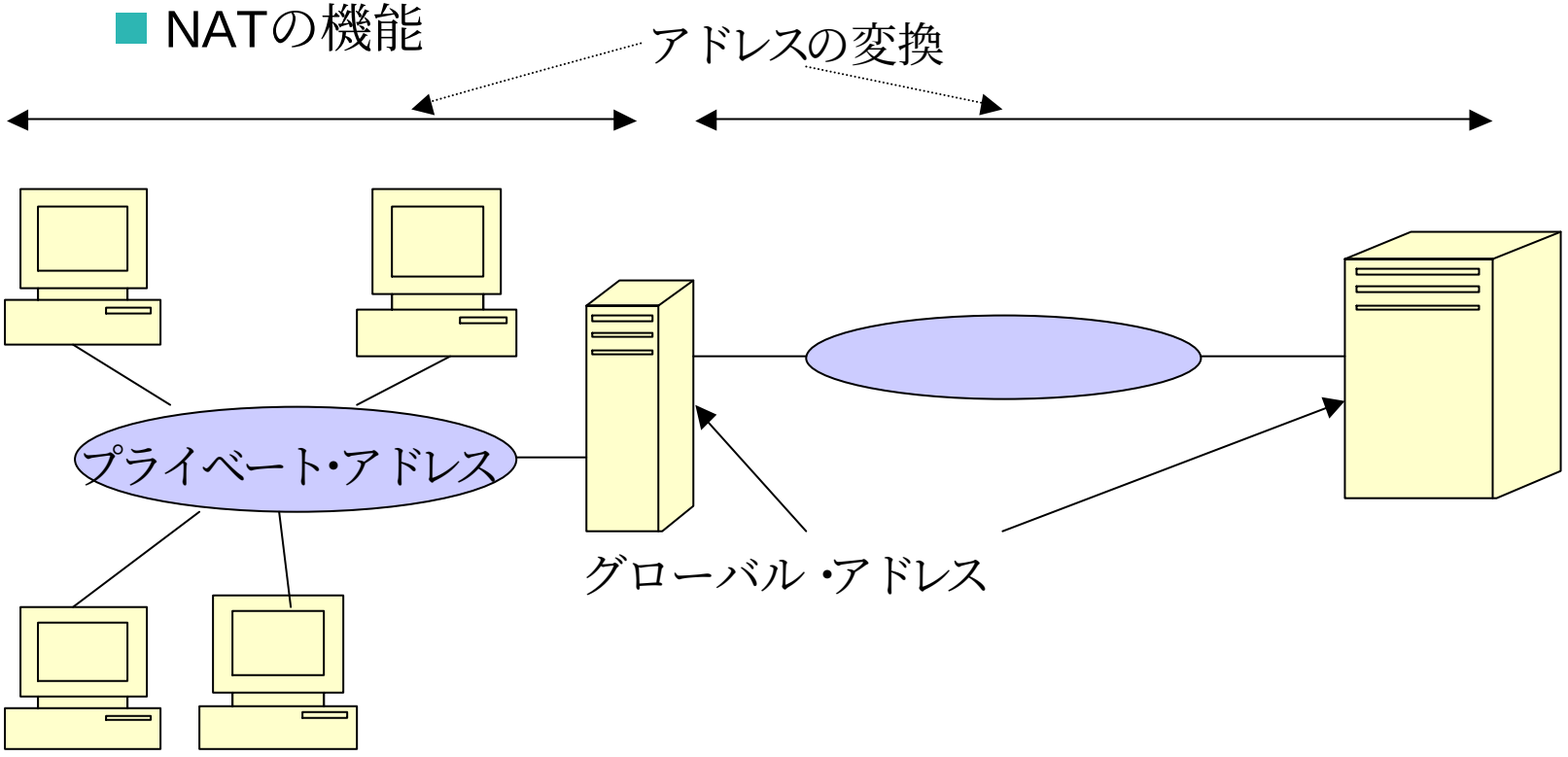


Notes:

- IPv4の問題
  - 300のホストを必要としている場合に、クラスBを割り当てると、65、000以上のIPアドレスが使用されないため無駄になります。
- 中規模ネットワークが増大し続けている
  - 全てのノードは、インターネット全体に関する経路表を持つ必要がありあます。接続されるネットワークの増大に伴い経路表が大きくなっています。経路表がおおきくなると中継機能の性能が低下するという問題が発生します。
- CIDR (Classless Inter-Domain Routing)の導入
  - IP v4のクラスA, クラスB, クラスCというクラス分けで生じるIPアドレスの無駄をなくす方法および、且つ経路表を小さくする方法としてCIDR(Classless Inter－Domain Routing)という概念が採用されました。
  - CIDRは、ネットワーク部のビット数を可変にして、必要なホスト数を割り当てられるようにしました。
  - 上図のように、192.0.4 , 192.0.5 , 192.0.6 は、上位22ビットは同じです。この場合、ルータの右側にあるノードの経路表は、ルータの左側の３つのノードの宛先とするエントリーは同じホップになります。従って、これらを１つのエントリーにまとめることにより経路表を小さくできます。
  - できるだけ、このようにネットワークのエントリーをまとめるようにするには、割り当てるにあたり、世界中を各地域にまとめて割り当てる方法を採用しました。
  - 次の３つの地域に分けて割り当てます。
    - アメリカ大陸
    - アジア太平洋地域
    - ヨーロッパおよびアフリカ

NAT(Network Address Translation)

- NATの機能



Notes:

- NATの導入
- 組織の出入り口に該当するゲートウェイにだけグローバルIPアドレスを与える。
- プライベート･ネットワークは、企業ないに割り当て、外部と通信する必要が発生したらゲートウェイを経由して通信をおこなう。
- ネットワーク内のホストは、ゲートウェイを通して実現される。

第3章
IPv6のメリット

Notes:

この章ではIPv6のメリットについて述べていきます。

IPv6のメリット

- アドレス空間の拡大
  - 32 ビットから128 ビットへ
  - 3.4×10^{38} 個のアドレス
- アドレス自動設定
  - ネットワークの Plug and Play の実現
  - 携帯端末など広範囲のデバイスで利用可能
- 既存技術の集約
  - IPSec やQoS などの技術を標準装備
  - 標準への対応が容易

Notes:

インターネットは急速な勢いで成長してきました。2000年1月のインターネット・ドメイン・サーベイでは約1億1千万ものホストがインターネットへ接続されています。32ビットのアドレス空間を持つIPv4は、40億以上のアドレスを定義することができます。これは一見まだ40倍のアドレス数を定義することができるように見えます。しかし、実際はプライベート・アドレスやネットワーク・クラスの概念によりすべてをインターネット接続に利用することはできません。

このような背景の中でIPv6は次世代IP（IP Next Generation:IPng）としてIETF（Internet Engineering Task Force）で1991年頃から検討が開始され、1995年頃に今のIPv6の元になる128ビットのアドレス空間を持つものができ、改定を繰り返し、1998年にRFC2460として定義されました。

その特徴として、

■128ビットのアドレス空間

これにより、アドレス不足の心配がなくなり、

■アドレスの自動設定機能

長くなったアドレスの複雑さを隠蔽することができ、

■セキュリティーや暗号化の機能の標準装備

IPv4でオプションとして利用されているIPSecやMD5などのセキュリティー・アルゴリズムが実装されている

ことなどがあげられます。

IPv6のメリット-アドレス空間の拡大-

- アドレス空間の飛躍的な拡大
  - IPv4 (アドレス長 :32bit=4byte)
    - 2^{32} = 4,294,967,296
  - IPv6 (アドレス長 :128bit=16byte)
    - 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456
    - 1人当たり 18,000,000,000,000,000,000 個のアドレス
    - 地球上 1m^2 当たり 665,570,793,348,866,943,898,599

Notes:

IPv4でのアドレス不足を克服するためにIPv6ではアドレス空間を32ビットから128ビットへ拡張しています。
その数は、2^{128}個のアドレスを定義することができます。これにより事実上無限の固有 IP アドレスを使用可能にすることできます。その数は、1人1人が個人のネットワークを構築したと仮定するとそのネットワークで 18,000,000,000,000,000,000,000 個のアドレスを使用することができ、地球上1m2当たり665,570,793,348,866,943,898,599 を割り当てることができます。（海、山、氷河を含みます。）

拡張された IPv6 のアドレッシング機能は、アドレス不足問題の解決策を提供します。これは、より多くの人々が携帯電話や携帯用コンピューターなどのモバイル・コンピューターを使用するようになっているので特に重要です。ワイヤレス・ユーザーの需要の増大は、IPv4 アドレス不足に拍車をかけることが予想されます。拡張された IPv6 の IP アドレス機能は、増大するワイヤレス装置の数に見合うIP アドレスを供給することによってこの問題を解決します。

IPv6のメリット-アドレス自動設定-

- アドレス自動設定
  - 2つの自動アドレス設定機能
    - Stateless Address Autoconfiguration（RFC2462）
      - ネットワーク上のルーターからアドレスを取得
    - Stateful Address Autoconfiguration
      - DHCPサーバーからアドレスを取得
      - DHCPv6
  - ホスト部（インターフェースを識別する部分）は自動生成
    - MACアドレスから自動生成
      - EUI-64 による生成（RFC2373）
      - MAC アドレスに FFFE を挿入

        00-D0-59-83-EB-2C ⇒00:D0:59:FF:FE:83:EB:2C

Notes:

このアドレッシング機能に加えて、IPv6はネットワーク上のアドレスの構成および管理タスクを単純化する新しい機能を提供しています。ネットワークの構成と保守は、非常に労力を要する作業です。IPv6は、いくつかのネットワーク管理者のタスクを自動化することによって、作業負荷を軽減しています。

IPv6 の自動構成機能は、ユーザーに代わって自動的にインターフェースとルーターのアドレスを構成します。Stateless Autoconfigurationでは、IPv6はホストのMACアドレスと、ルーターによって提供されるネットワーク接頭部を取り、それら2つのアドレスを結合してIPv6 アドレスを生成します。この機能によって管理者の時間と会社の経費が節減されます。この機能は、RFC2462で定義されています。
また、従来どおりDHCPサーバーによってアドレスを自動的に設定することもできます。この機能はDHCPv6と呼ばれ、現在、Internet Draftとして検討されています。

より簡単にネットワーク上で固有のアドレスを生成するためにIPv6では、ホスト･インターフェースを識別するためにホスト部をMACアドレスより生成することを基本としています。これは元々MACアドレスが固有であることに着目し、48ビットのMACアドレスをEUI-64に従ってインターフェースIDを生成するものです。
MACアドレスは、

- ■カンパニーID（上位24ビット）
- ■ベンダ供給ID（下位24ビット）

で構成されています。
この間に0xFFFEを挿入することにより64ビットのインターフェースIDを生成するものです。

IPv6のメリット-アドレス自動設定 続き-

- Neighbor discovery
  - IPv6 ノードがリンク上の他のIPv6 のノードを検索
    - ルーター
    - 他ノード
  - 自分のリンクレイヤ・アドレスが他と重複しないかを検査
  - ネットワーク・プレフィクスの取得
  - ICMPv6 により実装
  - 5つのメッセージ
    - Router Solicitation
    - Router Advertisement
    - Neighbor Solicitation
    - Neighbor Advertisement
    - Redirect

Notes:

Neighbor Discovery機能を使用することにより、IPv6 ノードはリンク内の他のIPv6 ノードの存在（ルーター、他ノード）を検索し、自分の使用可能なリンクレイヤ・アドレスの決定とルーターへの登録を行います。
IPv6 ノードはICMPv6 プロトコルを使用して他ノードと通信を行います。ICMPv6 プロトコルには5つのメッセージが存在します。

■Router Solicitation
IPv6 ノードはルーターへこのメッセージを送ることによってルーターの情報（Router Advertisement）のリクエストを送信します。

■Router Advertisement
Router Solicitationメッセージを受け取ったルーターはこのメッセージを生成し、回答として要求元ノードに転送します。この情報を元にノードはサイト・ローカル・アドレスやグローバル・アドレスを生成します。

■Neighbor Solicitation
ノードはこのメッセージを送信することにより隣のノードのリンクアドレスを取得しようとします。

■Neighbor Advertisement
Neighbor Solicitationメッセージの回答として要求元ノードへ送られます。

■Redirect
ルーターはこのメッセージでそのノードの宛先への最初のホップとなるホスト（ルーター）を連絡します。

Neighbor Discoveryに関する詳細はRFC2461を参照してください。

IPv6のメリット-アドレス自動設定 続き-

- Stateless autoconfiguration
  - IPv6 の自動アドレス設定の手法
  - アドレスの前半部分をルーターから取得
  - 後半部分は自分で生成
  - 5つのステップで実行
    - インターフェースID（ホスト部）の生成
    - リンク・ローカル・アドレスを生成
    - 重複アドレスの検出
    - ルーターからネットワーク・プレフィックス情報を取得
    - グローバル・ユニキャスト・アドレスを生成

Notes:

Stateless autoconfigurationはIPv6 ノードがIPv6アドレスを生成するための手法で以下の手順で実行されます。

■インターフェースIDの生成
IPv6 ノードは自分のMACアドレスを元に64ビットのインターフェースID（多くの場合この部分がホスト部になります。）を生成します。

■リンク・ローカル・アドレスの生成
IPv6 ノードは単一リンク内でのみ使用可能なアドレスを生成します。このアドレスを使用してリンク内の他のノードとの通信を行います。リンク・ローカル・アドレスについては後述します。

■重複アドレスの検出
IPv6 ノードは、Neighbor Discovery機能を使用して、リンク内に重複アドレスがないかどうか検索を行います。ノードはNeighbor Solicitationパケットを送信し回答を待ちます。Neighbor Advertisementパケットを受け取った場合はそのアドレスがすでに使用されていることを示しています。

■ルーターからネットワーク・プレフィクス情報を取得
ルーターはリンク内のノードのためにRouter Advertisementパケットを定期的に送信しています。ノードはそのパケットを受け取り、IPアドレスの前半部分を認識します。

■グローバル・ユニキャスト・アドレスを生成
ルーターから取得したネットワーク・プレフィクスとインターフェースIDを組み合わせてIPv6アドレスを生成します。

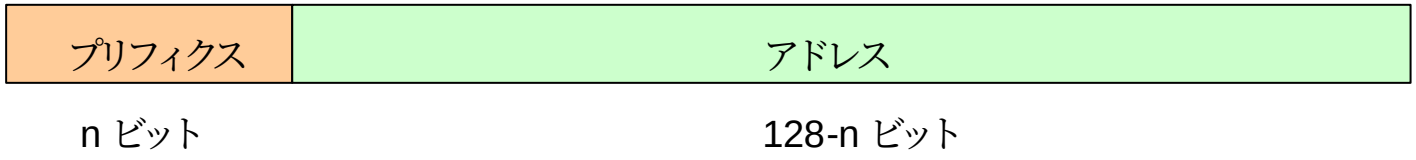
第4章
IPv6アドレス体系

Notes:

この章ではIPv6のアドレス体系について簡単に解説していきます。

IPv6アドレス体系 -表記法-

- IP アドレス表記
  - 128バイトを4桁の16進数ごとにコロン(:)で区切って表記
    - 1234:0567:0089:0000:0000:0000:ABCD:0001
    - 各セクションの先頭の’0’は省略可
      - 1234:567:89:0:0:0:ABCD:1
    - 連続する‘0000’は二重コロン(::)で省略可
      - 使用は1回のみ
      - 1234:567:89::ABCD:1
- プリフィクス
  - IPv6 アドレスの種類を指定
  - 表記方法はアドレス/プリフィクス長
    - fedc:ba98:4321::/48 最初の48ビットがプリフィクスとなる）



Notes:

IPv6アドレス・サイズは128ビットです。推奨されているIPv6アドレスの表記は、
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
と表わされ、各xは4ビットの16進数で示されます。
IPv6のアドレスの範囲は、
0000:0000:0000:0000:0000:0000:0000:0000 からffff:ffffffff:ffff:ffff:ffff:ffff:ffff:ffff
です。
IPv6アドレスをより見やすくするために以下のような規定がされています。

■先行'0'の消去

16ビットのまとまりが16進数の1000より小さい値を持つ場合、頭の0は表記する必要はありません。ただし、最低1つの数字は必要となります。これを使用することにより、

1234:0567:0089:0000:0000:0000:ABCD:0001 を
1234:567:89:0:0:0:ABCD:1
と表記することができます。

■連続する値の省略

さらにIPv6のアドレス表記を簡潔にする方法として、複数の16ビットのまとまりを2つのコロン（::）で省略することを許しています。これにより、

1234:567:89:0:0:0:ABCD:1
1234:567:89::ABCD:1
と表記することができます。ただし、'::'による省略は1つのアドレス中に1度しか使用してはなりません。

また、IPv6アドレスはプリフィクスによって階層化されています。これは、電話番号の国コードと市外局番に似ています。これによりアドレス中のルーティングに使用するための情報とその長さを知ることができます。表記法は、通常と同じように16進数で表現するが、意味を持つビット部分を示すためにアドレスに続けてスラッシュ（/）で区切りビット長を記述します。

IPv6アドレス体系 –その他-

- IPv4 のための2つの代替フォーマット
  - IPv4-mapped IPv6 address
    - ::ffff:<IPv4 address>
    - IPv4 ノードを IPv6 アドレスで表わす
    - IPv6 アプリケーションが IPv4 アプリケーションと直接通信可能
  - IPv4-compatible IPv6 address
    - ::<IPv4 address>
    - 既存の IPv4 ネットワークに IPv6 トラフィックをトンネリングする際に使用
    - 最初の 96ビットはすべて0で表わす

Notes:

IPv6アドレス体系では、既存のIPv4ネットワークと互換性を保つために以下の2つのアドレス・フォーマットをもっています。

■IPv4-mapped IPv6 address
■IPv4-compatible IPv6 address

■IPv4-mapped IPv6 address
このタイプのアドレスはIPv4 ノードをIPv6アドレスを使用して表わすために使用されます。これにより、IPv6アプリケーションが直接IPv4アプリケーションとやり取りを行うことができます。
例えば、192.1.56.10というIPv4アドレスは、0:0:0:0:0:ffff:192.1.56.10 (::ffff:192.1.56.10/96) と表わすことができます。

■IPv4-compatible IPv6 address
このタイプのアドレスは既存のIPv4ネットワーク上でIPv6 ノード同士が通信を行う場合に使用されます。
IPv4-compatible IPv6 addressは、先行する96ビットをすべて0で定義します。例えば、192.1.56.10というIPv4アドレスは、0:0:0:0:0:0:192.1.56.10 (::192.1.56.10/96) と表わすことができます。

IPv6アドレス体系 -アドレスタイプ-

- アドレスタイプ
  - ユニキャスト･アドレス
    - 通常の通信に使用
    - グローバル ･アドレス
    - サイト･ローカル ･アドレス
    - リンク ･ローカル ･アドレス
  - マルチキャスト･アドレス
    - 1対多の通信に使用
    - ビデオ配信
  - エニイキャスト･アドレス
    - 1対多の通信に使用
    - ルーター間の経路探索など

Notes:

IPv6アドレスは基本的に3つに分けられます。

- ■ユニキャスト・アドレス
- ■マルチキャスト・アドレス
- ■エニイキャスト・アドレス

ユニキャスト・アドレスは、単一のインターフェースを示すもので、ユニキャスト・アドレスを持つホストへのパケット転送は、1台の発信元ホストから宛先ホストへ送り届けられます。ユニキャスト・アドレスには次の3つのタイプがあります。

- ■グローバル・アドレス
- ■サイトローカル・アドレス
- ■リンクローカル・アドレス

これらに関しては後述します。

マルチキャスト・アドレスは、1対nで同時配信を行うような場合に使用するアドレスです。このアドレスはビデオ配信のようなアプリケーションに利用することができます。

エニイキャスト・アドレスは、1対nという意味ではマルチキャスト・アドレスと同じですが、異なる点としてはグループのいずれか1台に届けばよいというところが異なります。エニイキャスト・アドレスはルーター間の最短経路探索などに利用されます。

IPv6アドレス体系 -アドレスタイプ 続き-

- ユニキャスト・アドレス
  - グローバル ・アドレス
    - 従来のグローバル ・アドレスに相当
  - サイト・ローカル ・アドレス
    - 従来のプライベート・アドレスに相当
    - 上位 48ビットは 「fec0:0:0」に固定
  - リンク ・ローカル ・アドレス
    - 同一リンク内のみで使用できるアドレス
    - 128ビットをコンピューター自身が生成
    - 上位 48ビットは 「fe80:0:0」で固定
  - 特別なアドレス
    - 未定義アドレス (0:0:0:0:0:0:0:0)
    - ループバック ・アドレス (0:0:0:0:0:0:0:1)

Notes:

ユニキャスト・アドレスは、単一のインターフェースを示すもので、ユニキャスト・アドレスを持つホストへのパケット転送は、1台の発信元ホストから宛先ホストへ送り届けられます。ユニキャスト・アドレスには次の3つのタイプがあります。

■グローバル・アドレス

グローバル・アドレスは、IPv4のグローバル・アドレスに相当するアドレスでインターネットをはじめとする様々なネットワークで利用することが可能です。グローバル・アドレスを示すプリフィクスは0x2(001)になります。

■サイトローカル・アドレス

サイトローカル・アドレスはIPv4のプライベート・アドレスに相当するものである組織やサイト内で自由に使用することができるアドレスです。サイトローカル・アドレスのプリフィクスはfec0::/10です。ルーターは発信元アドレスにサイトローカル・アドレスが指定されているパケットに関しては、そのサイトの外には転送しません。

■リンクローカル・アドレス

リンクローカル・アドレスは単一のローカルリンク（ex.ローカルLAN）内で利用可能なアドレスです。リンクローカル・アドレスはすべてのインターフェースで自動的に生成されます。プリフィクスはfe80::/10です。このアドレスを含むパケットはルーターによって転送されません。

ユニキャスト・アドレスには2つの特別なアドレスがあります。

■未定義アドレス

未定義アドレスは、0:0:0:0:0:0:0:0または2つのコロン（::）で表記されます。使用できるアドレスがない場合に使用されます。それは本来使用すべきアドレスがまだ割り振られない場合など発信元アドレスとして使用できるものが何もない場合に使用されます。このアドレスが宛先アドレスに使用されることはあってはなりません。

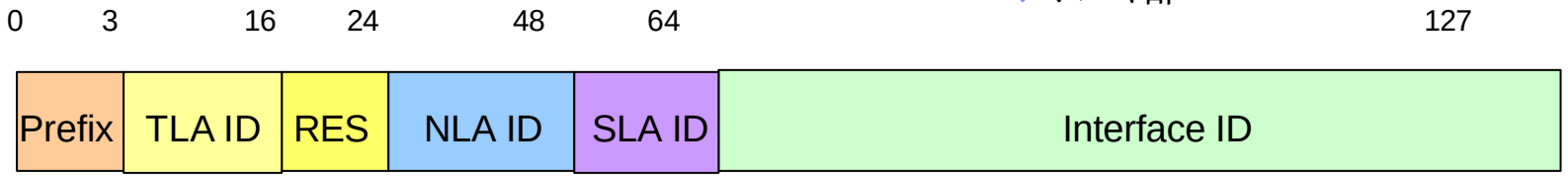
■ループバック・アドレス

ループバック・アドレスは、0:0:0:0:0:0:0:1または::1で表現されます。従来のループバック・アドレスと同じように単一ホストのインターフェースの検査などに用いられます。

IPv6アドレス体系 -グローバル・アドレス-

- グローバル・アドレス
  - インターネットに接続可能なアドレス
  - RFC2374 で規定
  - プレフィックス 200::/3
  - 3つの階層で構成されている
    - Public Topology
    - Site Topology
    - Interface ID

- Prefix
  - 02
- TLA ID（Top-Level Aggregation ID）
  - 最上位階層識別子
- Reservation
- NLA ID（Next-Level Aggregation ID）
  - 次階層識別子
- SLA ID（Site-Level Aggregation ID）
  - サイト識別子
- Interface ID
  - インターフェース識別子
  - ホスト部

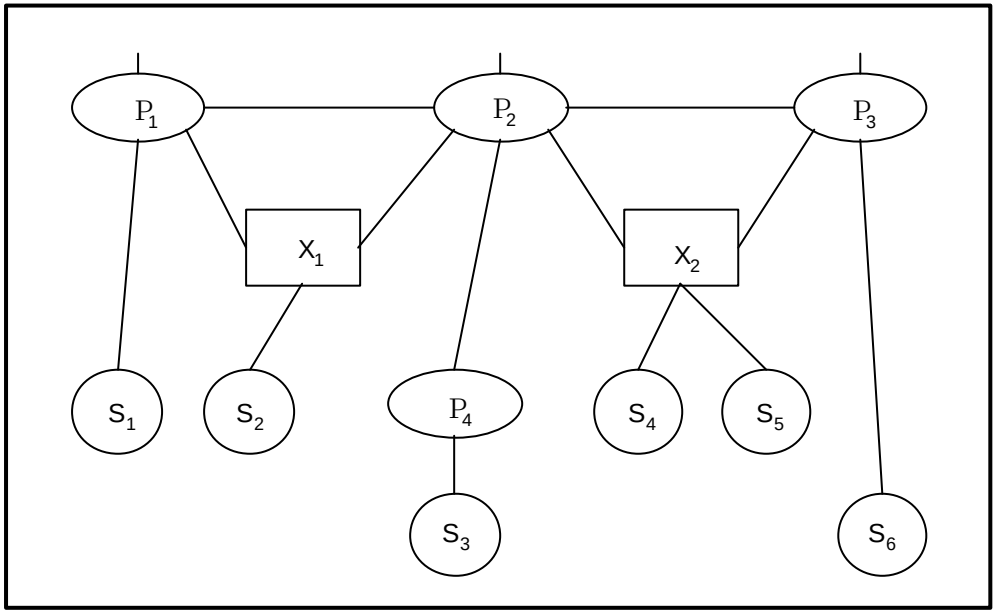


Notes:

グローバル・アドレス（グローバル・ユニキャスト・アドレス）はRFC2374- An IPv6 Aggregatable Global Unicast Address Format（IPv6の集約可能グローバルユニキャストアドレス形式）-で定義されていて、ホストがインターネットへ接続する際に使用するアドレス形式として有力です。集約可能なアドレスは以下の3階層構成になっている。

- パブリックトポロジー
- サイトトポロジー
- インターフェイス識別子

パブリックトポロジーは、公共的なインターネット配送サービスを提供するプロバイダおよびIXの集合です。サイトトポロジーは、サイト外のノードへは配送サービスを提供しない組織および特定のサイトのみを指します。インターフェイス識別子はリンク上にあるインターフェイスを識別します。



グローバル・アドレスは左の図のようなネットワークに対応するようにデザインされています。P1、P2、P3はバックボーンプロバイダーを表わしています。P4はP2よりサービスを受けている小規模プロバイダーです。X1、X2はIXであり、S1～S6は利用者を表わしています。IPv6のグローバル・アドレスはこのようなインターネットの階層に基づいて構成されているので、プロバイダーやIXを変更した場合でもアドレスの変更に対して意識する必要はありません。グローバル・アドレスの構成については次ページで説明します。

Notes:

グローバル・アドレスは、6つのセクションから構成されています。

■プリフィクス
グローバル・アドレスのプリフィクスは0x2です。

■TLA ID (Top-Level Aggregation ID)
TLA IDは経路制御における階層の最上位に位置します。デフォルト経路の設定されていないルータでは、すべての有効なTLA IDに対するエントリーがルーティング・テーブル内になければなりません。TLA IDは8,192個サポートされています。

■Reserve
将来のための予約域でゼロに設定されなければなりません。

■NLA ID (Next-Level Aggregation ID)
NLA IDは、TLA IDを割り当てられている組織において、下部のアドレス階層の作成やサイトの識別のために利用されます。組織のネットワークに合ったアドレス階層を作成するために、NLA IDの最上位部分を割り当てることができる。NLA IDフィールドの残りのビットは、その組織内のサイトの識別に利用できる。

■SLA ID (Site-Level Aggregation ID)
SLA IDは、個々の組織において自組織内のアドレス階層を作り、サブネットを識別するために利用されます。これは、各組織がずっと多くのサブネットを持つことを除いては、IPv4におけるサブネットに類似しています。16ビットのSLA IDフィールドは65,535個のサブネットをサポートしています。

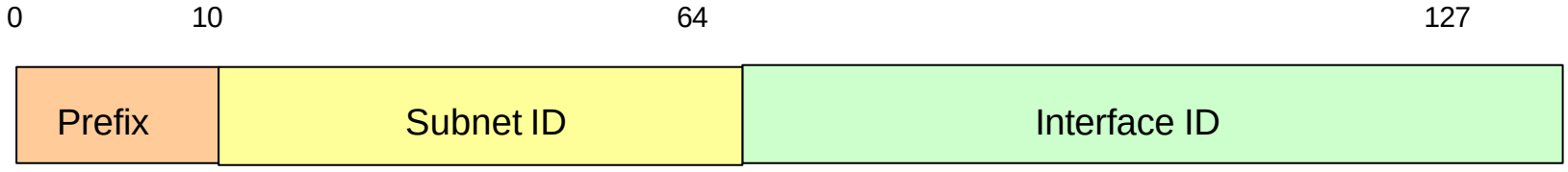
■Interface ID
Interface IDは、リンク上のインターフェイスを識別するために利用されます。インターフェイス識別子はリンク上で固有でなければなりません。Interface IDは当該インターフェイスのMACアドレス自体もしくはそのアドレスから生成される値が用いられます。

Notes:

このページはブランクです。

IPv6アドレス体系 -サイト・ローカル ・アドレス-

- サイト・ローカル ・アドレス
  - サイト（組織）内でユニークなアドレス
  - サイト内の通信に利用
  - プレフィックス fec0::/10
    - 1111:1110:11
- Prefix
  - fec0
- Subnet ID
  - サイト固有の識別子
- Interface ID
  - インターフェース識別子
  - ホスト部



Notes:

サイトローカル・アドレスは、そのサイト内で有効なIPアドレスで、IPv4でのプライベート・アドレス（10.0.0.0、176.16.0.0-176.31.0.0、192.168.0.0-192.168.255.0）に相当します。このアドレスをもったパケットをルーターはインターネットへ転送することはできません。
フォーマットは以下のとおりです。

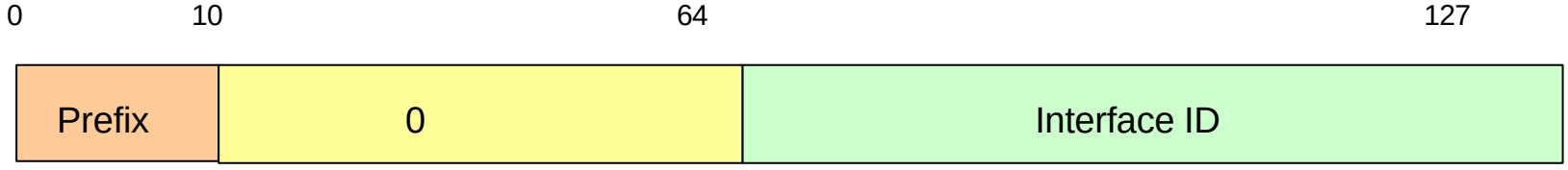
■プリフィックス
プリフィクスは、fec0::/10です。

■Subnet ID
組織内でのサブネットを識別するためのIDを付与することができます。通常、最後の16ビットを使用することになっています。

■Interface ID
Interface IDは、リンク上のインターフェイスを識別するために利用されます。インターフェイス識別子はリンク上で固有でなければなりません。Interface IDは当該インターフェイスのMACアドレス自体もしくはそのアドレスから生成される値が用いられます。

IPv6アドレス体系 -リンク・ローカル・アドレス-

- リンク・ローカル・アドレス
  - リンク内でユニークなアドレス
  - 起動時等に使用
    - アドレス未割当時」
  - プレフィックス fe80::/10
    - 1111:1110:10
- Prefix
  - fe80
- Interface ID
  - インターフェース識別子
  - ホスト部



Notes:

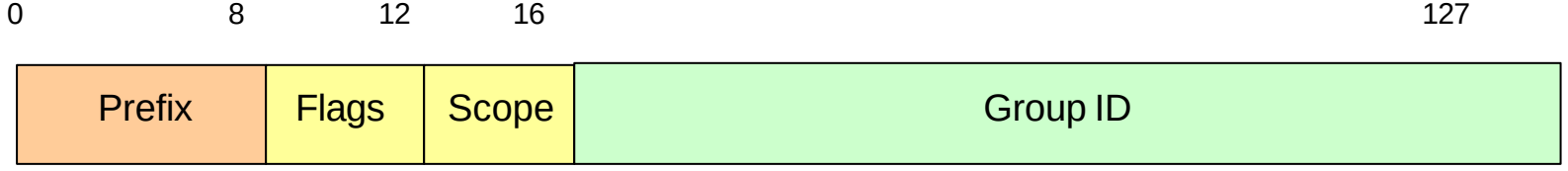
リンクローカル・アドレスは、そのインターフェースが接続されているローカル・ネットワークのみで利用可能なユニキャスト・アドレスです。主にグローバル・アドレスを取得をルーターに要求するときのアドレスとして利用されます。
フォーマットは以下のとおりです。

■プリフィックス
プリフィックスは、fe80::/10です。

■Interface ID
Interface IDは、リンク上のインターフェイスを識別するために利用されます。インターフェイス識別子はリンク上で固有でなければなりません。Interface IDは当該インターフェイスのMACアドレス自体もしくはそのアドレスから生成される値が用いられます。

IPv6アドレス体系 -マルチキャスト・アドレス-

- マルチキャスト・アドレス
  - 同報通信や1対nの通信に使用
  - プレフィックス ff00::/8(1111:1111:0000:0000)
  - 定義済みマルチキャスト・アドレス
    - ff01::1 （全システム/ノードローカル）
    - ff02::1 （全システム/リンクローカル）
    - ff01::2 （全ルーター/ノードローカル）
    - ff02::2 （全ルーター/リンクローカル）
    - ff05::2 （全ルーター/サイトローカル）
    - ff02::b （モバイル・エージェント/リンクローカル）
    - ff02::1:2 （DHCPエージェント/リンクローカル）
    - ff05::1:3 （DHCPサーバー/サイトローカル）



Notes:

マルチキャスト･アドレスは複数のホストのグループを識別するためのアドレスです。ホストは複数のグループに属してよいことになっています。
フォーマットは以下のとおりです。

■プリフィクス
プリフィクスはFFです。

■フラグ
フラグは4ビットで構成されていますが実際には最下位の1ビットのみ使用されています。
'0000 'はアドレス割り当ての権限を持つ機関から割り当てられた永続的なアドレスです。
'0001 'は一時的に割り当てられたアドレスであることを示します。

■スコープ
マルチキャストを行う範囲（スコープ）を示します。その値は、
0 予約
1 ノードローカルスコープ
2 リンクローカルスコープ
5 サイトローカルスコープ
8 組織ローカルスコープ
E グローバルスコープ
F 予約
となります。

■グループID
マルチキャスト･グループを指定します。

マルチキャスト･アドレスには定義済みのものがいくつかあります。これらのアドレスは、各ホストやルーターであらかじめ実装される必要があります。

IPv6アドレス体系 -エニーキャスト･アドレス-

- エニーキャスト･アドレス
  - 経路探索（最短経路などの検索）に使用
  - ユニキャスト･アドレスと文法的には同じ構成
  - ルーターのみ設定可能

Notes:

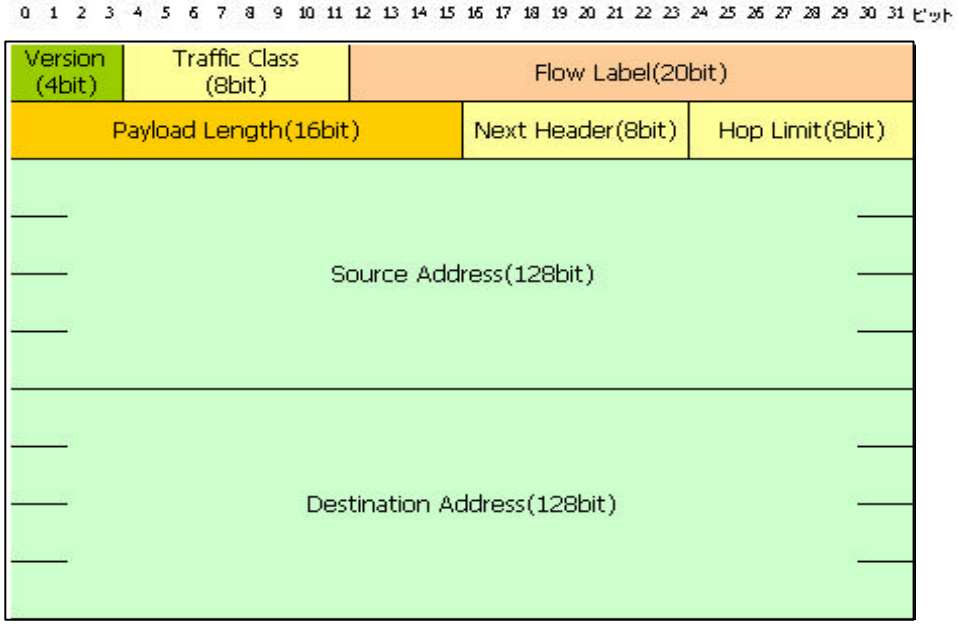
IPv6 エニイキャスト・アドレスは、1つ以上のインタフェース (通常異なるノードに属する) に割り当てられるアドレスであり、エニイキャスト・アドレスに送信されたパケットは、ルーティングプロトコルの距離計測に従って、そのアドレスを持つ「最も近い」インタフェースに振り分けられるという特性を持ちます。

エニイキャスト・アドレスは、定義されたユニキャストアドレス形式のどれかを使用して、ユニキャストアドレス空間から割り当てられます。従って、エニイキャスト・アドレスは文法的にユニキャスト・アドレスと識別できません。ユニキャスト・アドレスが1つ以上のインタフェースに割り当てられるためにエニイキャスト・アドレスに変わる時、そのアドレスが割り当てられたノードは、それがエニイキャスト・アドレスであることを認識できるよう明示的に設定する必要があります。

エニイキャストアドレスの期待された使用方法の1つにインターネットサービスを提供している組織に属するルーターの集合を識別することがあげられます。そのようなアドレスは、IPv6 ルーティングヘッダの中間アドレスで使用でき、特定の集約あるいは一連の集約を経由してパケットを転送することができます。他の使用方法としては、特定のサブネットに接続されたルーターの集合や、特定のルーティングドメインへのエントリーを提供しているルーターの集合を識別することがあげられます。

IPv6アドレス体系 -基本ヘッダー-

- IPv6ヘッダーフォーマット
  - ヘッダーサイズの固定
  - フォーマットの単純化
  - ルーター処理の高速化
- 基本ヘッダー
  - Version ⇒ ‘6’
  - Traffic Class
  - Flow Label
  - Payload Length
  - Next Header
  - Hop Limit
  - Source Address
  - Destination Address



Notes:

IPv6ヘッダー・フォーマットは、IPv4に比べ簡素化されています。IPヘッダーの長さはIPv4の20バイトよりも長い40バイトになっています。この中に2つの16バイトのIPアドレス（発信元および宛先）やそれに先行する形で8バイトの制御フィールドが存在します。

IPv4では2つの4バイトのIPアドレスと12バイトの制御フィールドやオプション・データで構成されていましたが、IPv6では制御情報を減らし、オプション・データを制限することにより、基本ヘッダーを40バイトの固定長にしています。これによりルーターでのパケット当りの処理を効率化を実現しています。オプション部分に関しては、拡張ヘッダーという形で基本ヘッダーに付加する形をとっています。

IPv6基本ヘッダーのフォーマットは以下のとおりです。

■Version

4ビットでIPのバージョンを示します。IPv6では6が指定されます。

■Traffic Class

8ビットでIPパケットの優先度を示します。このフィールドによって輻輳時に廃棄されるかどうかの2つの種類のパケットに区別されます。それぞれの中でさらに優先度が設定されます。このフィールドの使用法については現在も検討が続けられています。

■Flow Label

IPv6ヘッダの20 ビットのフローラベルフィールドは、例えば、デフォルトでないサービス品質や「リアルタイム」サービスといった、IPv6ルータで特殊な操作を実行することを要求するパケットを判別するために、使用されることを目的に定義されています。

■Payload Length

IPv6ペイロードのオクテット単位の長さ、すなわちIPv6ヘッダに続く残りのパケットの長さを表わします。

■Next Header

基本ヘッダーのすぐ後に続くデータの種別を表わします。

■Hop Limit

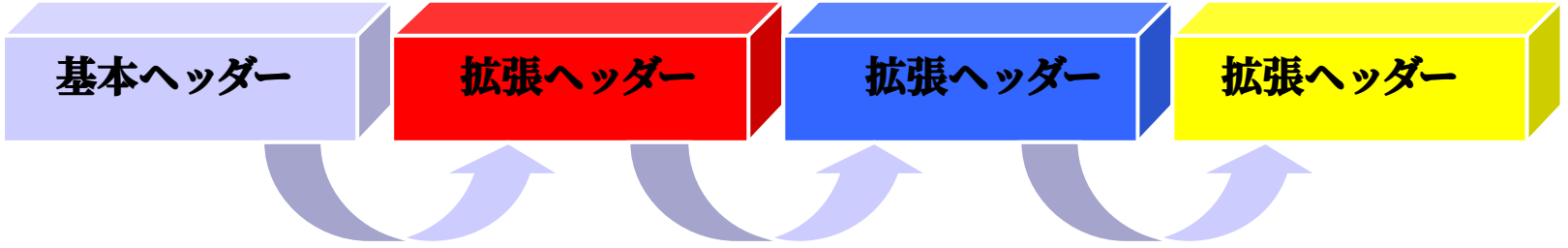
このIPパケットをどれくらい遠くまで転送することができるかを決定します。この値はルーターを通る毎に1づつ減らされ、0になると廃棄されます。

■Source Address、Destination Address

128ビットの送信元、宛先アドレスを表わします。

IPv6アドレス体系 -拡張ヘッダー-

- 拡張ヘッダー
  - 基本ヘッダーをシンプルにするためオプションは拡張ヘッダーで対応
  - 基本ヘッダー/拡張ヘッダーの Next Header 部に次にくるヘッダーを指定
    - Hop-by-Hop Options Header（0）
    - IPv6 Routing Header（43）
    - IPv6 Fragment Header（44）
    - Encapsulating Security Payload（50）
    - IPv6 Authentication Header（51）
    - No Next Header（59）
    - Destination Options Header（60）
    - TCP（6）



Notes:

IPv6では、オプションのインターネット層情報は、IPv6ヘッダーとパケット中の上位層ヘッダーとの間に置いてもよい別個のヘッダーで符号化されます。このような拡張ヘッダーはいくつか存在し、各々異なるNext Header フィールドの値によって識別されます。IPv6パケットは、1つあるいは複数の拡張ヘッダーを運んでもよく、先行するヘッダーのNext Header フィールドによって識別されます。基本ヘッダーに続くヘッダーには以下のようなものがあります。

■Hop-by-Hop Options Header
パケットの配送パスに属する全てのノードがチェックしなければならないオプション情報を運ぶために使用されます。

■IPv6 Routing Header
送信元ホストが送信するパケットの経路を制御したい場合にこのヘッダーを用います。

■IPv6 Fragment Header
1つのパケットに入りきれないような大きなデータを転送する場合にこのヘッダーを使用します。

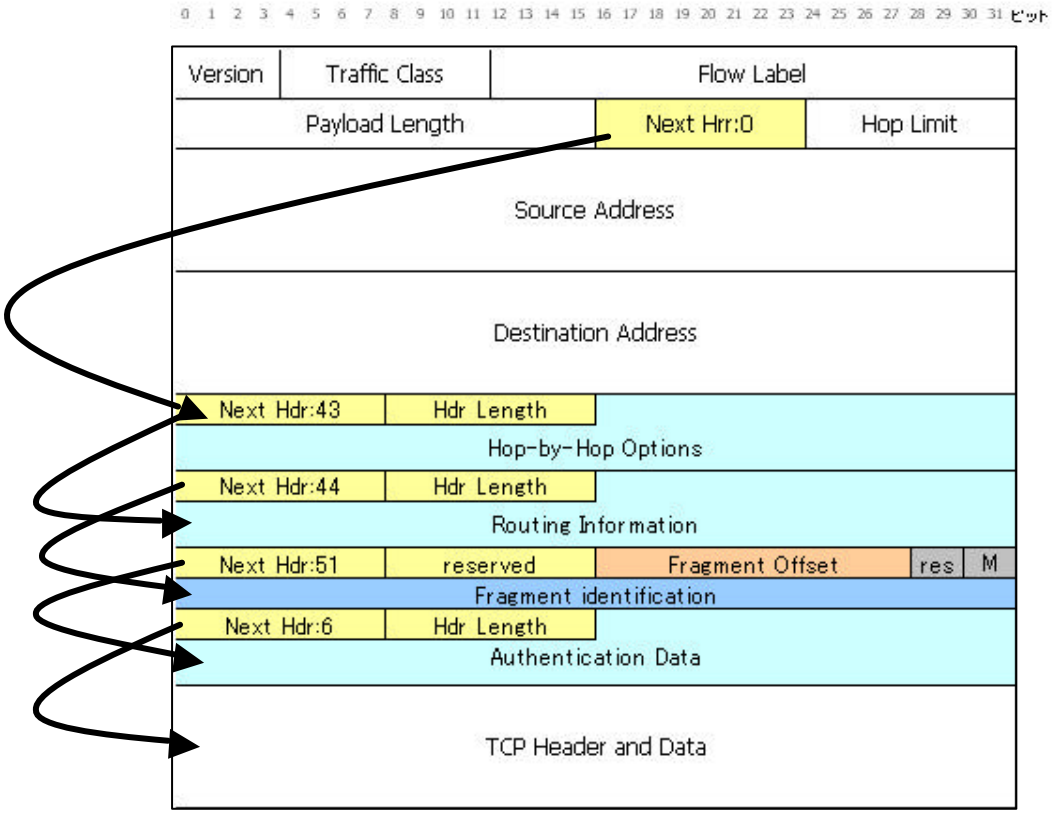
■Encapsulating Security Payload

■IPv6 Authentication Header
データの信頼性を表わすための送信者からの認証データが含まれています。

■No Next Header
次ヘッダーがないことを表わします。

■Destination Options Header
宛先ホストでこのパケットに対して実行してほしいオプションを指定することができます。

IPv6アドレス体系 -拡張ヘッダー続き-



- 拡張ヘッダーの例
  - 基本ヘッダー
  - Hop-Hop Header
  - Routing Information
  - Fragment Identification
  - Authentication Data
  - TCP Header and Data

Notes:

ここでは、拡張ヘッダーの例を示しています。この例では、

1.基本ヘッダー
↓
2.ホップバイホップ・オプション
↓
3.ルーティング・インフォメーション
↓
4.フラグメント・ヘッダー
↓
5.認証ヘッダー
↓
6.TCPヘッダーおよびデータ

の順にヘッダーが連なっています。

IPv6アドレス体系 -IPSec-

- IPSec（IP Security）
  - IPSecを標準で実装
  - Authentication Header：51
    - データの送信元の認証、データの完全性、リプレイからの保護
    - HMAC（Hashed Message Authentication Code）で認証
    - データの暗号化は行わない
  - ESP（Encapsulating Security Payload）：50
    - データの機密性を提供
    - 暗号用キーを使用してIPパケットの暗号化を行う
    - データの送信元の認証、データの完全性、リプレイからの保護機能を提供

Notes:

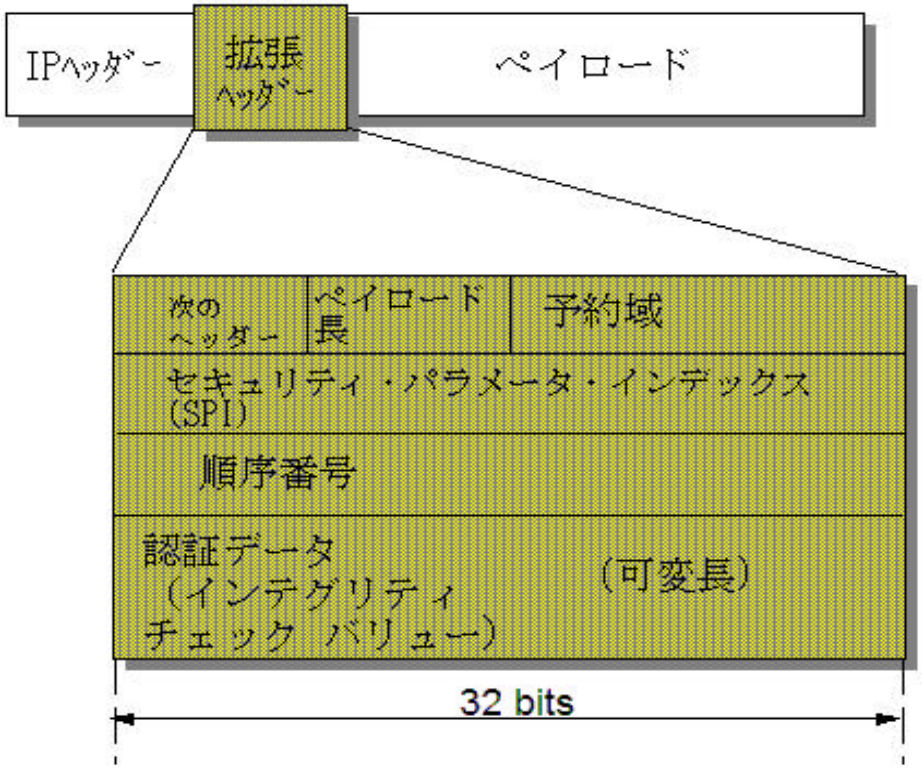
IPSecは元々IPv6のために設計されたものでしたが、すでにIPv4でも実装されています。IPv6ではIPSecを拡張ヘッダーによって実装しています。

■Authentication Header
Authentication Headerは受信したパケットが途中で変更されていないことを保証し、また確実に送信元からのパケットであることを認証します。基本的には認証アルゴリズムとしてMD5が使用されます。Authentication HeaderはNext Headerが51のヘッダーになります。

■ESP（Encapsulating Security Payload）
ESP（Encapsulating Security Payload）はデータの暗号化を提供します。これによってデータの盗聴を防ぎ、データの機密性を提供します。ESPは拡張ヘッダー50で提供されます。

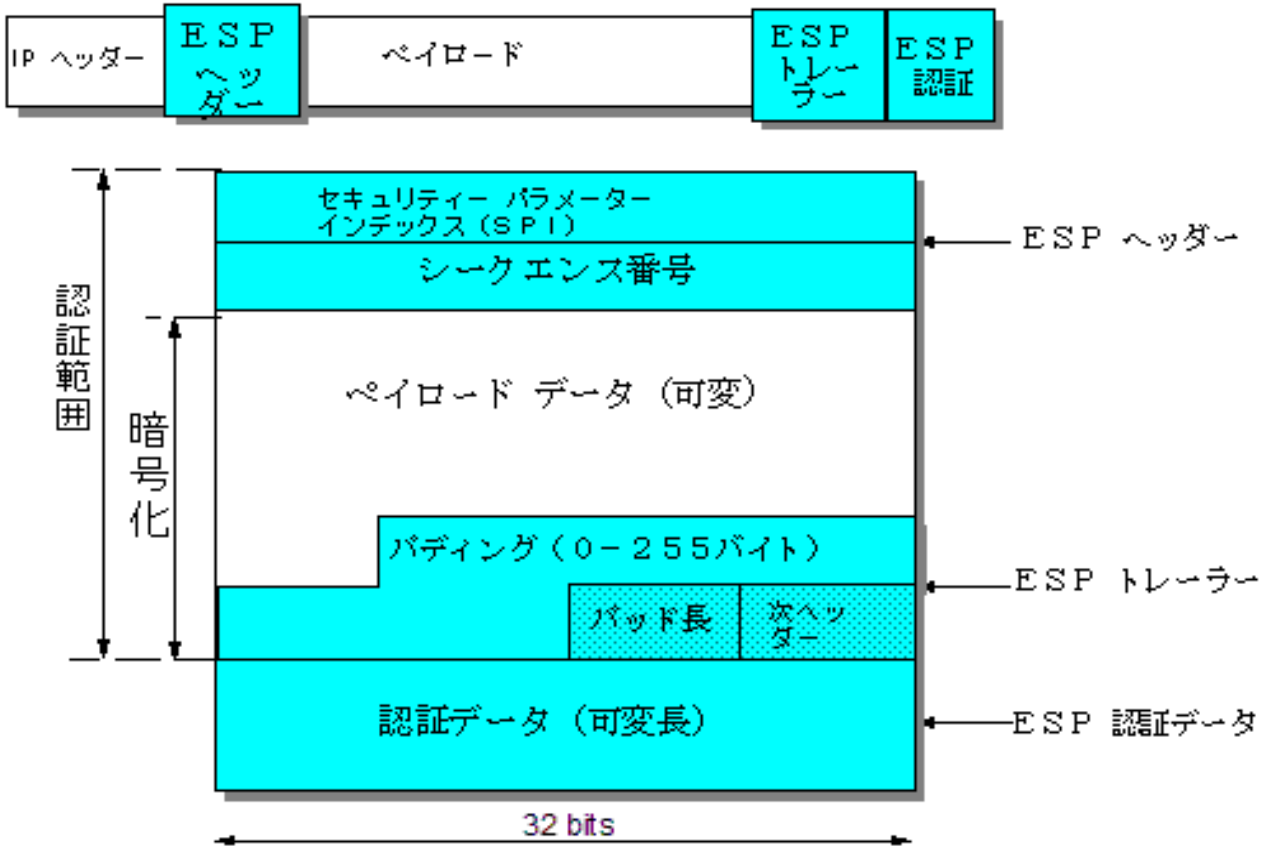
IPv6アドレス体系 –付録 :AHヘッダー-

- AHヘッダー・フォーマット



IPv6アドレス体系 -付録 :ESPフォーマット

- ESP（Encapsulating Security Payload）フォーマット



第5章
IPv6の現状

Notes:

この章では、IPv6についての
- 現在の状況
- 各国の対応状況
- ベンダーの対応状況

について述べていきます。

IPv6の現状

- 基本機能に関する仕様はほぼ決定
  - RFC2460　Internet Protocol Version 6 (IPv6)
  - RFC2373　IP Version 6 Addressing Architecture
  - RFC2374　An IPv6 Aggregatable Global Unicast Address Format
  - etc
- キラーアプリケーション不足
  - IPv6 の普及を加速するようなアプリケーションがない
  - IPv4 はインターネット自体がキラーアプリケーションだった？

Notes:

IPv6は1992年に次世代IP（IPng）としてIETFによって調査を開始されて以来、約10年間にわたり標準化活動が行われてきました。これまでに発表されてきたRFCには以下のようなものがあります。

- RFC2373 :IPv6 Addressing Architecture
- RFC2374 :An IPv6 Aggregatable Global Unicast Address Format
- RFC2401 :Security Architecture for the Internet Protocol
- RFC2460 :IP v6 Specification
- RFC2461 :Neighbor Directory for IPv6
- RFC2462 :IPv6 Stateless Address Autoconfiguration
- RFC2463 :ICMP for IPv6

このほかにも多数のRFCが起草されIETFのコメントを待っています。また、メーカーからも数々のドラフトが提出されています。

一方、IPv6のプロトコルとしての成熟とは別に市場への浸透に関しては、遅々としたものがあるということができます。この理由の1つとしてIPv6でなければならないという理由付けがまだ少ないことがあげられます。第3世代携帯電話に代表されるようなIPv6の技術を利用したアプリケーションの出現が待たれるところです。

IPv6の現状 -各国の対応-

- 日本
  - e-Japan 構想の1つの目玉として政府主導で推進
  - 各国内ベンダーも基礎技術として製品に組み込みつつある
- アメリカ
  - 今まではあまり積極的ではなかった
    - 不透明なビジネスモデル
  - 今後急速に進む可能性
    - 政府機関の調達仕様にIPv6対応を明記
      - DoD
- ヨーロッパ
  - 政府レベルでの積極的な推進
- アジア
  - 対応は様々
    - 積極派 :台湾、中国
    - 消極派 :韓国、インド

Notes:

IPv6に対する各国の対応は以下のとおりです。

・日本

日本では2000年に森前首相により打ち出されたe-Japan構想のキーワードの1つにIPv6が含まれたこともあり、国家的プロジェクトとして各メーカーやプロバイダーによって様々な実証実験が展開されています。代表的な実験の1つとして情報家電インターネット実証実験などがあります。

・アメリカ

アメリカでは、他の国に比べIPv4アドレスを豊富に持っていることやIPv6に関するビジネスモデルが不透明なこともあり今まではあまりIPv6には積極的ではなかったといえます。ただし、技術的にはCISCOを初めとするルーター・メーカーやIBM、Microsoftなどのメーカー/ベンダーで積極的に取り入れられています。最近注目をされているのは、政府機関（特に国防省）の調達仕様にIPv6対応の必要が明記されたことです。

・ヨーロッパ

EU各国はIPv6による次世代インターネットの推進に積極的です。特にヨーロッパではモバイルや携帯電話に関する技術が進んでいることもあり、この分野からのIPv6化に積極的です。

・アジア

アジア各国に関しては、国よりIPv6に対する取り組みには温度差がありますが、積極的な姿勢を見せているのは中国や台湾などの国々です。中国は特に人口の多さもあり、政府でも最近IPv6への興味を示しているようです。消極的な姿勢を見せているのは韓国です。韓国では98年からの国家プロジェクトによるブロードバンド（ADSL）の普及によりアドレス不足によるIPv6への移行という意識は低い状態です。ただし、最近では日本と同様、国家プロジェクトとして次世代インターネット推進が明言され、それに伴いIPv6への取り組みも始まっています。

IP v6の現状 -各ベンダーの対応-

- IBM
  - AIX V4.3 以降
  - z/OS V1R4
  - OS/400 V5R2
- CISCO
  - ルーター製品：IOS 12.2(2) 以降
- Microsoft
  - Windows2000（Developer's Workbench）
  - Windows XP（not-for-production support）
  - CE.NET
- Linux
  - Kernel 2.2 以降
  - 本格的な実装は 2.4 以降
- SUN
  - Solaris 8
- HP
  - HP-UX 11i

Notes:

IPv6へ主なハードウェア/ソフトウェア・メーカー/ベンダーの対応は以下のとおりです。

IBM
AIX V4.3 以降
z/OS V1R4
OS/400 V5R2

CISCO
ルーター製品 IOS 12.2(2) 以降

Microsoft
Windows2000、XP、CE.NET

Linux
Kernel 2.2 以降
本格的な実装は 2.4 以降

SUN
Solaris 8

HP
HP-UX 11i

第6章
OS/400 V5R2 IPv6 サポート

Notes:

この章では、iSeriesでのIPv6のサポートについて解説します。

V5R2 IPv6 サポート

- IPv6 アプリケーション開発 / テストのための機能を提供
  - iSeries ナビゲーター ウィザードによる構成
    - ループバック
    - IPv6 用イーサネット定義の作成
    - IPv6 用トンネル定義の作成
  - ソケットの拡張
    - IPv4 と IPv6 をサポートするアプリケーションを開発可能
    - AF_INET6 アドレス・ファミリーのサポート
  - TCP/IP ツールの拡張
    - DNS AAAA レコードのサポート
    - Ping のサポート
    - 経路トレースのサポート
    - netstat コマンドのサポート
    - 通信トレースのサポート

Notes:

OS/400 V5R2では、IPv6はIPv6対応アプリケーションを構築するための開発/テスト用のプラットフォームとしての機能を提供します。OS/400によって提供されるツールのいくつかはIPv6対応になっています。

V5R2によって提供される機能は以下のとおりです。

■iSeries ナビゲーターによる構成

IPv6を構成するためには、iSeriesナビゲーターを使用しなければなりません。iSeriesナビゲーターはIPv6を構成するためのウィザードを提供します。iSeries上で構成できるIPv6インターフェースは以下のとおりです。

- ループバック
- IPv6 用イーサネット定義
- IPv6 用トンネル定義

■ソケットの拡張

ソケットAPIの拡張により、IPv6に対応したアプリケーションを開発することができます。この拡張は、既存のIPv4アプリケーションに影響をおよぼしません。この新しいAF_INET6アドレス・ファミリーをサポートすることによりソケット・アプリケーションでIPv6アドレスを扱いうことができます。

■TCP/IPツールの拡張

・DNSの拡張

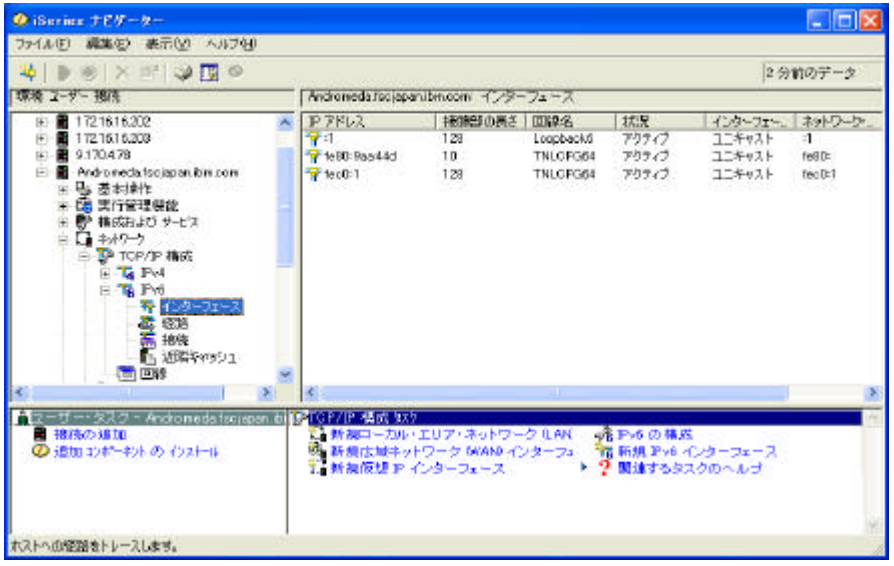
DNSは、AAAAアドレスと逆探索用の新しいドメインIP6.ARPA をサポートしています。これによりIPv6アドレスに対する名前解決をiSeriesで提供することができます。

・問題解決およびテストツールの拡張

PINGコマンド、経路トレース、通信トレース、netstatコマンドがIPv6に対応しました。これによりIPv6アプリケーションの開発/テストをより協力にサポートします。

IPv6構成

- 3つの構成を iSeries に構成可能
  - ループバック
    - イーサネット回線や他のノードを必要としない
    - 自ノードへの PING やアプリケーションの開発に利用
  - IPv6 用イーサネット回線
    - IPv6 専用のイーサネットカードが必要
      - #2838
      - #2349
    - IPv6 機能を利用可能
      - Stateless automatic configuration ....
  - IPv6 用トンネル回線
    - 既存の IPv4 ネットワーク上でIPv6を利用
    - 仮想回線上に構成可能
    - Point to Point で構成可能



Notes:

iSeriesで利用可能なIPv6構成は以下の3つです。

■ループバック
■IPv6用イーサネット回線
■IPv6用トンネル回線

IPv6を構成するためには、必ずIPv4が構成されていなければなりません。これはIPv6を構成するためには必ず、iSeriesナビゲーターを使用する必要があるからです。IPv6の構成に5250インターフェースを利用することはできません。

■ループバック

ループバック・インターフェースは、もっとも簡単にiSeries上にIPv6を構成することができる方法です。この構成に関してはイーサネットカードのような物理回線は必要ありません。iSeries上でIPv6のアプリケーションの開発/テストを行うときに有効な手段になります。

■IPv6用イーサネット回線

iSeriesのイーサネット回線上にIPv6を構成することができます。構成方法はIPv4と異なります。構成可能なイーサネットカードは#2838または#2849のみです。この方法でIPv6を構成することによりIPv6のアドレス自動構成の機能などIPv6の機能をフルに利用することができます。

■IPv6用トンネル回線

この方法は、仮想回線上にIPv6を構成することができます。この構成にはIPv6専用の回線は必要ありません。既存のIPv4ネットワーク上にIPv6を構成することができます。それぞれのトンネルの定義はポイント-ポイントになります。つまり必ず1つの相手先を定義する必要があります。

ソケットの拡張

- IPv4 とIPv6 をサポートするアプリケーションを開発可能
- AF_INET6 アドレス・ファミリーのサポート
  - アドレス構造を指定するための API
  - IPv6 のみ
  - IPv4 のみ
  - IPv6,IPv4 両方

Notes:

AF_INET6 ソケットは、IPv6の128ビットアドレス構造をサポートします。プログラマーはAF_INET6アドレス・ファミリーを使用してアプリケーションを作成し、IPv4 ノードまたはIPv6 ノードのどちらかから、 あるいはIPv6 ノードのみから、クライアント要求を受け入れることができます。

AF_INETソケット同様、AF_INET6 ソケットにも、コネクション型 (タイプ SOCK_STREAM) とコネクションレス型 (タイプ SOCK_DGRAM) があります。コネクション型AF_INET6 ソケットは、TCPをトランスポート・プロトコルとして使用します。

コネクションレス型 AF_INET6 ソケットは、UDP をトランスポート・プロトコルとして使用します。AF_INET6 ドメイン・ソケットの作成時に、 ソケット・プログラムのアドレス・ファミリーに AF_INET6 を指定します。AF_INET6 ソケットもタイプ SOCK_RAW を使用することができます。このタイプを設定すると、アプリケーションは IP 層に直接接続し、TCP または UDP トランスポートのいずれも使用しません。

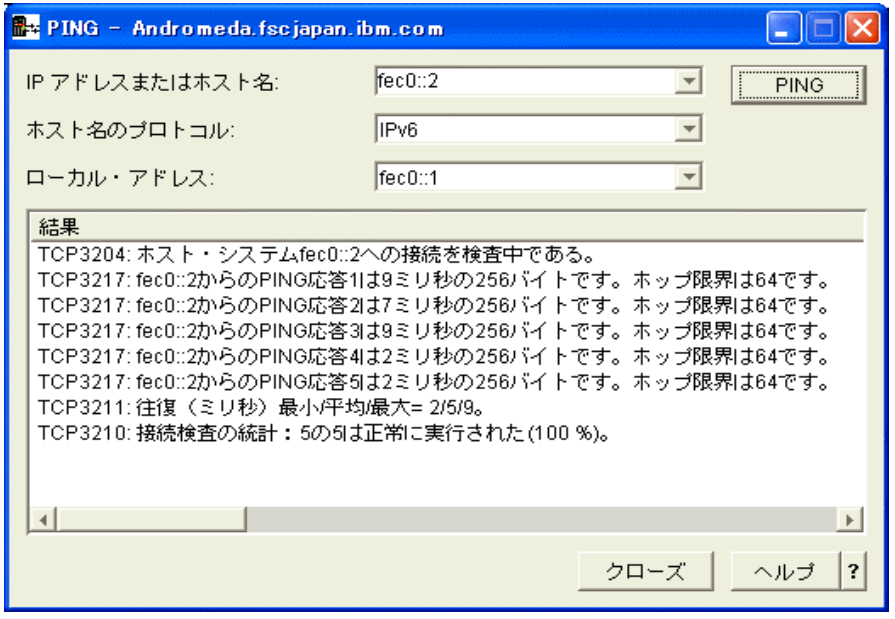
AF_INET6 アドレス・ファミリーを使ってソケット・アプリケーションを作成すれば、IPv6アプリケーションは、IPv4 アプリケーション (AF_INET アドレス・ファミリーを使用するアプリケーション) と一緒に機能できるようになります。この機能により、 ソケット・プログラマーは IPv4 マップ IPv6 アドレス形式を使用できます。このアドレス形式は、IPv4 ノードの IPv4 アドレスを IPv6 アドレスとして表します。IPv4 アドレスは IPv6 アドレスの下位 32 ビットにエンコードされ、高位 96 ビットは 0:0:0:0:0:FFFF という接頭部で固定されます。IPv4 マップ・アドレスの一例を挙げます。

::FFFF:192.1.1.1

IPv6 ソケット・プログラミングに関する詳細は、インフォメーション・センターを参照ください。

DNS および TCP/IP ツールの拡張

- DNS の拡張
  - AAAA レコードのサポート
- TCP/IP ツールの拡張
  - Ping のサポート
  - 経路トレースのサポート
  - netstat コマンドのサポート
  - 通信トレースのサポート



Notes:

IPv6は、アドレス・スペースの問題を解決しますが、その128ビットという長いアドレス体系のため、アドレスを覚えることが以前にも増して難しくなりました。IPv6の世界においてDNSの役割はユーザーにとってさらに重要なものになると思われます。

iSeriesのDNSは、BIND（Berkeley Internet Name Domain）のバージョン8.2.5をサポートし、IPv6アドレスのためのAAAAレコードを提供します。そのフォーマットは、

‘オーナー’‘クラス’‘TTL’AAAA‘IPv6 アドレス’

の形式をとります。例を以下のとおりです。

host1.itsoroch.ibm.com IN AAAA 1234::206:29ff:feec:c4b

リバース・ルックアップ（逆引き）を行う場合には、IPv6アドレスを16進数で記述し、ドット（.）で区切ります。この場合のPTRレコードは以下のようになります。

b.4.c.c.e.e.f.f..f.9.2.6.0.2.4.3.2.1.ip6.arpa. IN PTR host1.itsoroch.ibm.com

BIND 8.2.5はAAAAレコードをサポートしますが、IPv6による通信をサポートしません。BIND 8のサーバーに対してDNSの探索を行う場合には、IPv4で通信を行わなければなりません。BIND 9.xではIPv6による通信がサポートされ、さらに多くのIPv6に関連する機能が実装される予定です。

IPv6ではPING、netstat、経路トレース、およびIPv6ネットワークとトンネル用の通信トレースなどのOS/400標準のトラブルシューティング・ツールを使用することができます。これらのツールは、IPv6アドレス・フォーマットをサポートしています。

IPv6関連資料

- Redbook
  - http://www.redbooks.ibm.com/
    - iSeries IP Networks :Dynamic!(SG24-6718-00)
    - TCP/IP Tutorial and Technical Overview(GG24-3376-06)
- www
  - http://www.rfc-editor.org/
    - RFC の検索
  - http://www.ietf.org/
    - IETF のホームページ