IPv4 と IPv6

●リンクローカル：ルータを越えない、つまり同一リンク内

※IPv4 においては、APIPA（Auto PIPA）に相当する。APIPA は DHCP サーバが不在の時、ホスト自身が 169.254.0.0~169.254.255.255 から IPA をランダムに設定する。

●ユニークローカル：ルータを越えるがインターネットには接続しない。

※IPv4 においては、通常の PIPA に相当する。

●グローバル：インターネットに接続する。

●リンクローカルユニキャストA（fe80::/10）

●ユニークローカルユニキャストA（fc00::/7）

●グローバルユニキャストA（2000::/3）

●マルチキャストA（ff00::/8）なお、マルチキャストA はリンクローカル、ユニークローカル、グローバルそれぞれにある。特に ICMPv6 に規定された近隣探索で利用するものはリンクローカルマルチキャストA（ff02）である。

●ループバック A は自分自身を表すので外部への通信は発生しない。つまり、外部からもアクセスできないため安全である。

①IPv4 のループバック A は 127/8 なので 127.0.0.1~127.255.255.254　**なは**

②IPv6 のループバック A は::1/128

●IP ヘッダは、ルータのルーティングに必要であり、IPv4 では可変長（20 バイト＋オプション）であるが、IPv6 は 40 バイトの固定長である。IPv4 のようなオプションに対しては、拡張ヘッダを追加して対応するが、拡張ヘッダの内容は、宛先ノードで処理し、ルータでは処理しない（例外として、ホップバイホップオプションヘッダだけはルータで処理）ので、ルータから見ると固定長

IGMP

●マルチキャストによる通信を管理するプロトコル

●マルチキャストグループに参加又は離脱したいホストは、受信したいマルチキャストアドレスと架空の MAC/A をサブネット内の最寄りの L2SW 等に IGMP で通知すると、サブネット内の最寄りのルータにも情報が転送される。

●当該ルータは、IGMP で他のルータにも情報を伝える。そして、PIM（Protocol-Independent Multicast）によって、ホストへのルーティングが可能となる。

●以上からルーティングは問題ないが、［ラストホップルータ　→　L2SW　→　ホスト］の際に L2SW によるフラッディング防止するために IGMP スヌーピングを実行しておく。

●IPv4 で使う IGMP は、IPv6 では **ICMPv6** の機能として MLD (Multicast Listener Discovery)があるので、IGMP は不要。

IGMP スヌーピング（スヌーピング：のぞき見する）

●L2SW 等の MAC/A テーブルは、受信ポートと送信元 MAC/A の対応表である。

●マルチキャスト MAC アドレス（正式名称）は、マルチキャスト IPA から生成した架空の MAC/A（架空 A）なので、ホストの NIC は、架空 A を受信するように対応するが、ホストの持つユニキャスト用のいつもの MAC/A とは当然異なるもの。

●よって、架空 A は MAC/A テーブルの送信元 MAC/A になり得ないため、L2SW 等は学習することができない。そのため、IGMP スヌーピングによって、架空 A を学習させる必要がある。

DHCP スヌーピング

●L2SW 等が DHCP サーバとクライアント間での DHCP メッセージを盗み見て、DHCP クライアントと繋がっている SW のポートを判別し、その情報に基づいて動的な IP フィルタリングを行う。つまり正当でない DHCP クライアントに繋がっているポートを遮断する。

●通常、L2SW はイーサネットヘッダのみを参照するため、IP フィルタリングは行わないが、DHCP スヌーピングを有効にすると、IP フィルタリングを行う。この時、DHCP メッセージをチェックしなければならないので CPU に負担がかかる。

「ス」で始まる類義語

●ＩＰスプーフィング（スプーフィング：だます）：ＩＰＡを偽装して攻撃すること。

●スニッフィング（においを嗅ぐ）：ＮＷに流れるデータを捕え、内容を解析して盗み見ること。

プレフィックス

●□.□.□.□/□