IPv6 and Wireless Communication

陳孟彰

中央研究院資訊科學研究所

(mcc@iis.sinia.edu.tw)

Outline

- Wireless Network
- Internet Protocol version 6 (IPv6)

Wireless LAN and Cellular Phone

WLAN Current Status

- The 802.11 standards focus on the physical layer and data link layer.
  - 802.11: 2 Mbit/s, 2.4 GHz spread spectrum (or IR)
  - 802.11b: 11 Mbit/s, 2.4 GHz spread spectrum
  - 802.11a: 54 Mbit/s, 5 GHz OFDM
  - 802.11x: security, QoS, etc.
  - 802.15/SWAP/HomeRF simple 802.11

Blue Tooth

- Short range, low power, inexpensive wireless link
  - License exempted 2.4 GHz frequency hopping
  - Bandwidth 64 ... 721 kbit/s, range some meters
- Distributed mobile terminal
  - Replace Infrared between mobile terminal, PDA, hands free device, lap top, I/O device, screen, etc.

Blue Tooth (cont.)

- Connecting (Ad-Hoc) devices in a room
  - Jukebox, vending machine, home automation, locking, printer, health monitoring, & PDA/phone (UI+payment)
- Access solution (poor man's WLAN)
  - UMTS/BlueTooth dual mode terminal
- Other Wireless Personal Area Networks
  - 802.15/SWAP/HomeRF (simple 802.11)
- Refer to http://www.bluetooth.com

Mobile Telecommunication System

- First generation
  - Regional analog systems for speech service
- Second generation (today)
  - Digital circuit switched speech, slow data, and short message services
  - GSM (almost global), IS-95 CDMA, IS-136 TDMA. Very large business, soon 1 billion paying customers
  - WAP: independent third party service provision

Mobile Telecommunication System (cont.)

- **2G+, 2.5G (GPRS/PDC-P)**
  - packet switch data
- **Third generation (3G)**
  - Drivers: new terminals, capacity, internet boom, WAP,...
  - New services: m-commerce, location services, e-mail,...
- **Fourth generation:**
  - Telecom evolution
  - Wireless Local Area Networks

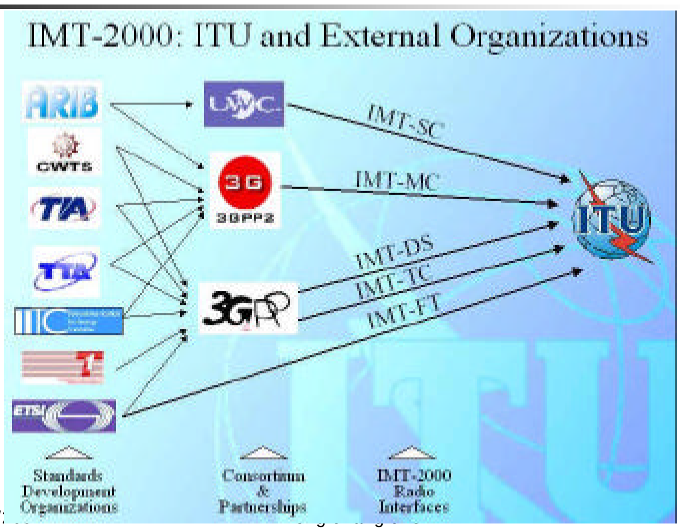
UMTS

New services and business model

- WAP, SIM toolkit, m-commerce security, ...

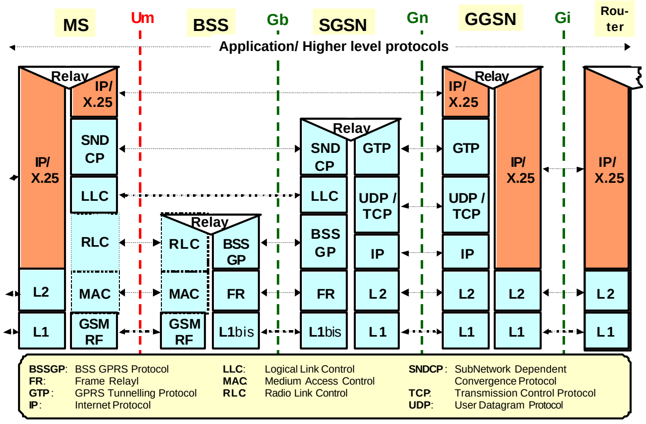
- **GPRS: up to 43 kbit/s**
  - IP packet switched
- **EDGE - enhanced data rates for GSM/global evolution**
  - triple capacity, an option for non-3G operators
  - frequency auctions have made EDGE more attractive
- **3GPP Release 99: WCDMA and 3G GPRS**
  - ca. 100 kbit/s, theoretically over 1 Mbit/s
- **3GPP Release 04: All-IP core-network**

3G Standards and Organizations (from C. Tsao)



3G Architecture and Technologies (from C. Tsao)

GPRS Transmission Planes



What IPv6 can do for Wireless?

- Address
  - More devices require larger address space
  - 4G adopts IP as addressing scheme
- Auto configuration
- Security

History of Internet Protocol Version 6 (IPv6)

- The Recommendation for the IP Next Generation Protocol, IETF RFC 1752, 1994.
- Internet Engineering Steering Group approved Proposed Standard, 1994.
- Core set of IPv6 protocols, IETF Draft Standard, 1998.
- For RFCs and status, refer to http://www.ipv6.org

Wireless boosting IPv6

- Proponents of IPv6, a controversial upgrade to the Internet's main communications protocol, say they have finally found their killer application: wireless.........CAROLYN DUFFY MARSAN, NetworkWorldDusion, 10/23/00

Difference between Ipv4 and IPv6 Formats

- Address size!
- Fixed format for headers
- No header checksum
- Different hop-by-hop segmentation procedure
  - IPv6 uses *path MTU discovery* to decide the max MTU size
- No TOS field

Ipv4 and IPv6—fields revised

- Different calculation for *payload length*
- *Protocol type* renamed to *next header*
- *Time-to-live* renamed to *hop limit*

Ipv4 and IPv6—new fields

- *Flow label*
  - For real-time traffic
- *Class*
  - 8 bits priority

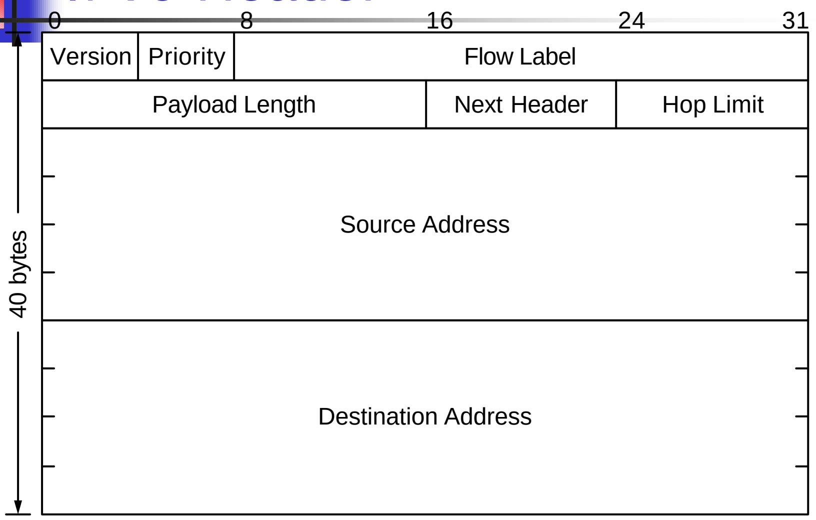
IPv4 Header

0 8 16 24 31

20 bytes

<table>
<tr><td>Version</td><td>Header Length</td><td>Type of Service</td><td colspan="2">Total Length (in bytes)</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source IP address</td></tr>
<tr><td colspan="5">Destination IP address</td></tr>
</table>

IPv6 Header



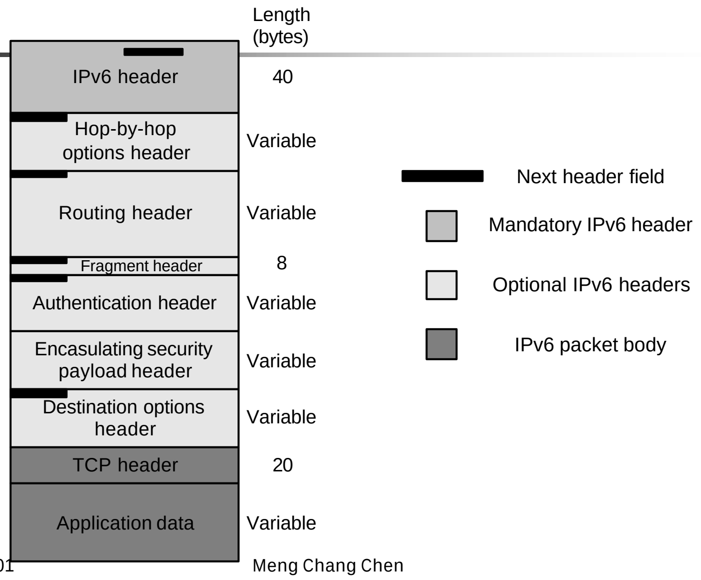
3/30/2001 Meng Chang Chen 19

IPv6 Addressing Architecture

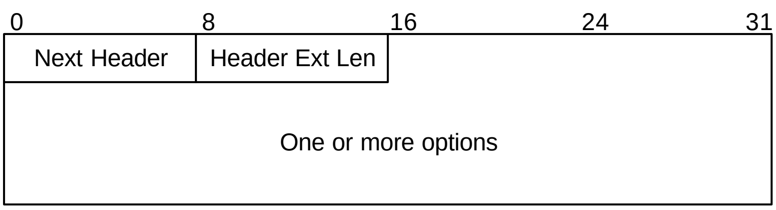
RFC 2373
R. Hinden, Nokia
S. Deering, Cisco
July 1998

3/30/2001 Meng Chang Chen 20

IPv6 Packet with All Extension Headers



Hop-by-Hop Options Header & Destination Options Header



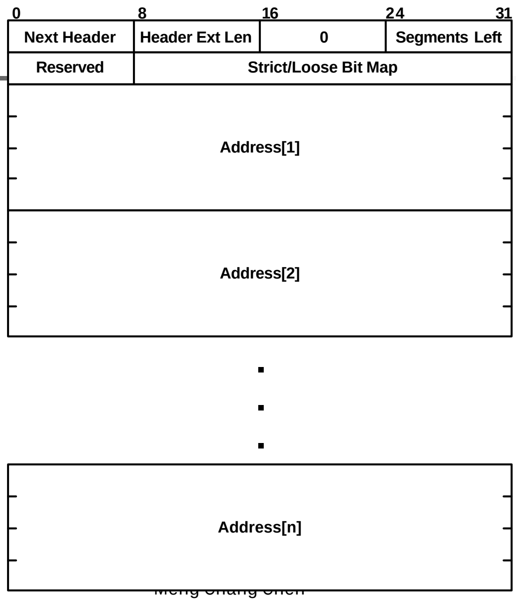
Fragment Header

0	8	16	29	31
Next Header	Reserved	Fragment Offset	Res	M
Identification				

Generic Routing Header

0	8	16	24	31
Next Header	Header Ext Len	Routing Type	Segments Left	
Type-Specific Data				

Type 0 Routing Header



What IPv6 can do for Wireless?

- Address
  - More devices require larger address space
  - 4G adopts IP as addressing scheme
- Auto configuration
- Security

IPv6 ADDRESSING

- IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces.
  - Unicast
  - Anycast
  - Multicast

Text Representation of Addresses

- There are three conventional forms for representing IPv6 addresses as text strings:
  - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
  - 1080:0:0:0:8:800:200C:417A

  - 1080::8:800:200C:417A
  - FF01::101

  - 0:0:0:0:0:0:13.1.68.3
  - 0:0:0:0:0:FFFF:129.144.52.38

Text Representation of Address Prefixes

- An IPv6 address prefix is represented by the notation:
  - ipv6-address/prefix-length
- For example, the following are legal representations of the 60-bit prefix 12AB00000000CD3 (hexadecimal):
  - 12AB:0000:0000:CD30:0000:0000:0000:0000/60
  - 12AB::CD30:0:0:0:0/60
  - 12AB:0:0:CD30::/60

Format Prefix (FP)

Allocation	Prefix (binary)	Fraction of Address Space
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP Allocation	0000 001	1/128
Reserved for IPX Allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Aggregatable Global Unicast Addresses	001	1/8
Unassigned	010	1/8
Unassigned	011	1/8
Unassigned	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link-Local Unicast Addresses	1111 1110 10	1/1024
Site-Local Unicast Addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

Interface Identifiers

- Interface identifiers in IPv6 unicast addresses are used to identify interfaces on a link. They are required to be unique on that link. They may also be unique over a broader scope. In many cases an interface's identifier will be the same as that interface's link-layer address.
- In a number of the format prefixes Interface IDs are required to be 64 bits long and to be constructed in IEEE EUI-64 format .

Unicast Addresses

- IPv6 unicast addresses are aggregatable with contiguous bit-wise masks similar to IPv4 addresses under Class-less Interdomain Routing

```
|                         n bits                         |   128-n bits   |
+--------------------------------------------------------+----------------+
|                     subnet prefix                      |  interface ID  |
+--------------------------------------------------------+----------------+
```

- The address 0:0:0:0:0:0:0:0 is called the unspecified address. It must never be assigned to any node. It indicates the absence of an address.
- The unicast address 0:0:0:0:0:0:0:1 is called the loopback address. It may be used by a node to send an IPv6 packet to itself.

Unicast Addresses

- IPv6 Addresses with Embedded IPv4 Addresses
  - IPv6 nodes that utilize this technique are assigned special IPv6 unicast addresses that carry an IPv4 address in the low-order 32-bits. This type of address is termed an "IPv4-

80 bits	16	32 bits
0000..............................0000	0000	IPv4 address

  - A second type of address is used to represent the addresses of IPv4-only nodes (those that *do not* support IPv6) as IPv6 addresses. This type of address is termed an "IPv4-mapped IPv6 address" and has the format:

80 bits	16	32 bits
0000..............................0000	FFFF	IPv4 address

Unicast Addresses

- Link-Local addresses have the following format:

10 bits	54 bits	64 bits
1111111010	0	interface ID

- Site-Local addresses have the following format:

10 bits	38 bits	16 bits	64 bits
1111111011	0	subnet ID	interface ID

Unicast Addresses

```
The IPv6 aggregatable global unicast address format is as follows:

| 3|  13 | 8 |   24   |   16   |          64 bits               |
+--+-----+---+--------+--------+--------------------------------+
|FP| TLA |RES|  NLA   |  SLA   |         Interface ID           |
|  | ID  |   |  ID    |  ID    |                                |
+--+-----+---+--------+--------+--------------------------------+

Where

   001          Format Prefix (3 bit) for Aggregatable Global
                Unicast Addresses
   TLA ID       Top-Level Aggregation Identifier
   RES          Reserved for future use
   NLA ID       Next-Level Aggregation Identifier
   SLA ID       Site-Level Aggregation Identifier
   INTERFACE ID Interface Identifier
```


Anycast Addresses

- Anycast addresses are allocated from the unicast address space, using any of the defined unicast address formats.
- When a unicast address is assigned to more than one interface, thus turning it into an anycast address, the nodes to which the address is assigned must be explicitly configured to know that it is an anycast address.

```
|                         n bits                 |   128-n bits   |
+------------------------------------------------+----------------+
|                     subnet prefix              | 00000000000000 |
+------------------------------------------------+----------------+
```

Multicast Addresses

- An IPv6 multicast address is an identifier for a group of nodes. A node may belong to any number of multicast groups. Multicast addresses have the following format:

Multicast Addresses

- flgs is a set of 4 flags: |0|0|0|T|
  - The high-order 3 flags are reserved, and must be initialized to 0.
  - T = 0 indicates a permanently-assigned ("well-known") multicast address, assigned by the global internet numbering authority.
  - T = 1 indicates a non-permanently-assigned ("transient") multicast address.
- scop is a 4-bit multicast scope value used to limit the scope of the multicast group.

```
|   8    |  4 |  4 |                  112 bits                   |
+------- -+----+----+---------------------------------------------+
|11111111|flgs|scop|                  group ID                   |
+--------+----+----+---------------------------------------------+
```

Multicast Addresses

- Scope
  - 1 , node-local scope
  - 2 , link-local scope
  - 5 , site-local scope
  - 8 , organization scope
  - E , global scope
- Solicited Multicast Prefix
  - FF01:0:0:0:0:1:FF00::/104
  - Append low-order 24bits from interface ID
    - Example: solicited node multicast address for node 4037::01:800:200E:8C6C is FF02::1:FF0E:8C6C

Index

Neighbor Discovery for IP Version 6

RFC 2461

T. Narten, IBM

E. Nordmark, Sun Microsystems

W. Simpson, Daydreamer

December 1998

Host Caches

- Host maintains for each interface
  - Neighbor Cache
    - IPv6 and media addresses
  - Destination Cache
    - IPv6 and neighbor addresses
  - Prefix List
    - Prefixes of networks learned from router advertisements
  - Router List
    - Link local addresses of interface of routers from RA.

States of Neighbor Cache

- INCOMPLETE
  - Address Resolution is in progress
- REACHABLE
  - Recently sent and still in Reachable time
- STALE
  - Recently sent but expire Reachable time
- DELAY
  - Recently fail , return fail to upper layer
- PROBE
  - Recently fail and verifying its reachability

Basic Packet Transmission Algorithm

- If the packet destination is in Destination Cache, transmit it to associated neighbor.
- Check Prefix list to see if cached prefix matches packet destination.
  - If yes, the destination is local.
  - If no, select a router to transmit the packet.

Basic Packet Transmission Algorithm (cont.)

- When next hop is selected, add to Destination Cache. Check Neighbor Cache.
  - If not exist, the host sends a *Neighbor Solicitation* message. The neighbor is added to Neighbor Cache with status *Incomplete*.
  - If exist and incomplete, wait for completion.
  - If exist and complete, transmit it using media address.
  - If the cache is not fresh, transmit the packet and send *Neighbor Solicitation.*

Neighbor Discovery

- Determine the link-layer addresses for neighbors reside on attached link
- Find neighbor routers
- Keep track of dynamic neighbor status (such as, reachable or not)
- Collect information for autoconfiguration

Neighbor Discovery protocol

- Based on ICMPv6 protocol with IP next header value of 58. (RFC 2463)
- Message types
  - Router Solicitation(RS)
  - Router Advertisement(RA)
  - Neighbor Solicitation(NS)
  - Neighbor Advertisement(NA)
  - Redirect

Neighbor Solicitation

- Issued by a host.
- Source link-layer address
  - Link-layer address for the sender
  - MUST NOT be included when the source IP address is unspecified

Neighbor Advertisement

- Target link-layer address
  - Link-layer address for the target => the sender of the advertisement
- ICMP fields description
  - R , whether sender is a router.
  - S , response to a NS.
  - O , override an existing cache entry.

Redirect

- To adjust error in packet forwarding.
- Target link-layer address
  - Should be include if known
- Redirected Header
  - Original IP packet (all or partial) < 1280 octets
- ICMP field
  - Target
    - Better “next-hop”
  - Destination
    - Origin Destination of packet redirected

Packet Sending Adjustment

- Check above information to determine appropriate “next hop” => “next-hop determination”
- Result of “next-hop determination” will be stored in Destination Cache
- Faults will result in “next-hop determination” being performed again
- If no router available, node will assume all destination are on the same link

Router Solicitation(RS)

- Issued by the host
- Source link-layer address
  - Link-layer address of the sender if known
  - MUST NOT be included if source IP unspecified
  - For unknown source, send multicast RA in response

Router Advertisement(RA)

- Replied by a router
- Possible Options (information for configuration)
  - Source link-layer address
  - MTU
  - Prefix information
    - All available prefixes except link-local prefix

ICMP fields description

- Cur Hop Limit
  - Default value for IP Hop limit field
- Router Lifetime
  - Indicate the life time of the router
  - In seconds , maximum to 18.2 hours
- Reachable Time
  - In milliseconds
  - Time period a node assume a neighbor is reachable after recent confirmation
- Retrans Timer
  - In milliseconds
  - Indicate the time period between NS

Router Advertisement Types

- Solicited
  - In response to RS
- Unsolicited
  - Periodically sent
- Both share a same timer limit the rate of sending RA
- A host MUST NOT send RA
- Router send consecutive RA when start up from the link

Router Advertisement consistency

- Routers inspect valid Router Advertisement sent by other routers
- If inconsistency found , log to system in order to do reconfiguration for system administrator
- Minimum set of information to check
  - M/O flags
  - Reachable Time
  - Retrans Time
  - MTU
  - Prefix associated information
  - Cur Hop Limit

Fields of Prefix Information

- Prefix length , 8-bit unsigned integer ,number of leading bits valid
- L, on-link flag,indicate that this prefix can be used for on-link determination
- A , autonomous flag,indicate that the prefix can be used for autonomous address configuration
- Valid Lifetime
  - In seconds
  - Time that the prefix is valid
  - Oxffffffff represents infinity
- Preferred Lifetime
  - In seconds
  - Time that the prefix is preferred
  - Oxffffffff represents infinity

Router and Prefix Discovery

- Router Discovery
  - To locate neighboring routers
  - Learn prefixes and configuration parameters
  - All messages must be validated before any processing

3/30/2001 Meng Chang Chen 57

Examples for message validation

- Check ICMP type and code
- Check the ICMP checksum
- Check ICMP length
- Check IP Hop Limit field has a value of 255 => the packet could not possibly have been forwarded by a router

3/30/2001 Meng Chang Chen 58

Processing Router Solicitations

- A host MUST ignore RS
- RA could be sent to unicast or multicast destination (response or advertise) , either way router shall reset its timer for sending RA

Processing Router Advertisements

- Update local variables with received information for existed router
- Unspecified not equal to default
  - Prevent nodes from changing variable values
- Create entry for router appear for the first time
- Purge router entry which has been timed out or expired

Default Router Selection

- Invoked during “next-hop determination” being performed or when communication fails
- Judging whether routers are reachable or probably reachable in default router list , and select a proper one
- If all router in default router list are unreachable, send packet to every router using round robin
- If no router response, node assume all destinations are on-link

Other Situations for Router Solicitations

- An interface becomes enabled
- Reinitialized
- A router become a host ,by have its IP forwarding capability turned off

Address Resolution and Neighbor Unreachability Detection

- Address resolution
  - Usually multicast NS with unicast NA
  - Receiver usually has no idea who sender is
- NUD (Neighbor unreachability detection)
  - Usually unicast NS with unicast NA
  - Receiver usually has the knowledge for sender
- DAD (duplicate address detection)
  - Usually multicast NS with multicast NA
  - Sender has no valid unicast IP

Unsolicited Neighbor Advertisements

- A node's link-layer address changed
- Set S=0 , for not confusing Neighbor
- Set Override
  - 0, Neighbor update state=STALE and probe on itself
  - 1, update Neighbor Cache with received NA

IPv6 Stateless Address Autoconfiguration

RFC 2462
S. Thompson, Bellcore
T. Narten, IBM
December 1998

AutoConfiguration

- Stateful (not included in RFC2462)
- Stateless
  - Address assignment
  - Information collection

Stateless AutoConfiguration Design Goals

- Manual configuration is not required
- A stateful server on the link is not required
- Configuration should facilitate the graceful renumbering
- System administrators need the ability to specify whether stateless, stateful or both be used

Stateless configuration for hosts

- Use neighbor discovery as base mechanism to achieve stateless autoconfiguration
- Creation of link local addresses
  - Whenever an interface becomes enabled
  - As described in RFC 2373
    - Prepending the link-local prefix FE80::0 to the interface identifier
    - Interface identifier is formed based on EUI64 format with minor change

Creation of Global and Site-local Addresses

- Prepending subnet prefix and interface identifier
- On receiving RA
  - Update link parameters
  - Update prefix information
    - Create new addresses
    - Expunge expire or invalid addresses
- Without router
  - Host determine that there is no router
  - Form link-local Address

Steps to get a unique address

- Form a link-local address (not assigned)
- Perform DAD
  - If DAD fails , log it and disable the interface. But user can still manually config it
- If DAD passed ,assign the link-local address to the interface
- Search for router
  - Receiving RA and config itself with information in RA

DAD

- Duplicate Address Detection
  - Use to examine whether a link-local address if unique
  - Implement with
    - Neighbor Solicitation
    - Neighbor Advertisement

Steps to perform DAD

- Sender : send NS Messages
- Receiver : receive NS
- Receiver : send NA if necessary
- Sender : receive NA (DAD fails)
  - If the address is a link-local address , disable the interface
  - Log the error

SITE RENUMBERING

- Time-out addresses assigned to interfaces in hosts
  - At present , upper layer protocols such as TCP provide no support for changing end-point addresses while a connection is open
  - even in UDP , addresses must generally remain the same during packet exchange

SITE RENUMBERING(cont.)

- Valid address
  - Preferred : When a new connection established ,use preferred address if possible
  - Deprecated : unless no preferred address available , don't use deprecated address in new connection

SITE RENUMBERING(cont.)

- IP layer is expected to provide a means for upper layer to select most appropriate source address
- If upper layer does not specify source address , IP layer should choose a suitable one on the application’s behalf

Considerations

- Stateless autoconfiguration imply unauthenticated node attached to network and work properly
- DAD opens up the possibility of DOS attack
  - Reply every DAD probing so no nodes can get a proper address

IEEE EUI-64

- The IEEE defined 64-bit extended unique identifier (EUI-64) is a concatenation of the 24-bit company_id value by the IEEE Registration Authority(IRA) and a 40-bit extension identifier assigned by the organization with that company_id assignment

Identifier applications

- MAC-48. A 48-bit identifier used to address hardware interfaces within 802 based networking applications.
- EUI-48. A 48-bit identifier used to identify a design instance, as opposed to an hardware instance. Examples include software interface standards (such as VGA) or the model number for a product.
- EUI-64. A 64-bit identifier used to identify each hardware instance of a product, regardless of application, such as wireless devices and computerized toasters.

Restricted encapsulated values

- To support encapsulation of EUI-48 and MAC-48 values within small subsets of the EUI-64 values, the first four digits of the manufacturer's extension identifier shall not be $FFFF_{16}$ or $FFFE_{16}$.
- Thus, the 64-bit values of the following form are never-assigned EUI-64 values:

$ccccccFFFEeeeeee_{16}$ (an EUI-48 extension)

$ccccccFFFFeeeeee_{16}$ (a MAC-48 extension)

Dilemma of Dynamic Host Configuration

- Situation 1: needs IPv6 to query servers and receive responses
- Situation 2: needs to locate and query DHCP server for IPv6 address
- Solution:
  - Link local address
  - multicast

Four steps DHCP Set-up

- Host: Solicitation
- DHCP server: Advertise
- Host: Request
- DHCP sever: Reply
- Other operation: release, reconfigure

DHCP Server Solicitation Procedure

- Host sends
  - *DHCP solicitation message* to *all DHCP servers and relay agents* address
    - Source address: host's link local address
    - Transport layer protocol: UDP port 546,547
- Relay agent sends (if receives from host)
  - DHCP solicit message to *all DHCP servers* addressServer replies
  - *Advertise message* to relay agent or host
    - Client's link local address
    - Extensions: configuration parameters for clients

DHCP Server Determination

- A host may receive several advertisement messages. Then it will select a DHCP server and maybe an agent.
- If not, it will repeat its solicitation.
- A host then sends a request message for requesting configuration parameters.

DHCP Server Extension Message

- Address: Client IPv6 address
- Preferred and Valid lifetimes (of address)
- Domain name
- Other server addresses:DNS, directory, etc.

What's wireless network related to IPv6?

- Implement neighbor discovery and autoconfiguration in IPv6 for wireless network.
- Optimize the implementation and operations.
- Make sure it works for all perspectives.
  - performance
  - Correctness
  - efficiency

The End.

陳孟彰
中央研究院資訊科學研究所
(mcc@iis.sinia.edu.tw)