IPv6 and home networking

Laurent Toutain
Laurent.Toutain@enst-bretagne.fr

Triple play architecture

- Provider services have a public address
  - They can be managed directly
- User is behind a NAT so:
  - He cannot be joined directly
  - He does not know the public address
  - Security feeling
- Is NAT the provider way to impose its own value added services and block the others?
NAT: Fortified castle?

- UP&P allows applications to modify NAT context to publish port numbers
  - Big security issue
- NAT traversal exists:
  - Skype uses it:
    - Locate a relay with a public address
    - Use this relay to communicate with private equipments
  - Microsoft TEREDO generalized this approach
    - An IPv6 address is constructed based of public IPv4 address
    - Even behind a NAT an application will have an IPv6 public address.
- Routing is inefficient, but who cares if it works

Model evolution

- Going back to end-to-end principle
  - I know my identity on the network
  - I can be joined directly
- Introduce security and trust to services
  - I cannot be joined directly if I have not registered my service
- Introduce more flexibility
  - In terms of architecture
  - In terms of services deployment
- Very smooth evolution from existing architecture to the new one
- Adapted to large audience without any network knowledge
IPv6

- IPv4 prefixes are more and more difficult to obtain
  - End forecasted in 2008-2010
- IPv6 offers almost unlimited addressing space
  - But every equipment (host, router) and application have to be modified
  - Most of content is only accessible in v4
  - Dual Stack approach (private IPv4 and public IPv6)
- If IPv6 packet format is different, administrative process and network architecture remain the same
  - IPv4 : one address is allocated to site
  - IPv6 : one prefix (part of the address) is allocated to site

Adding IPv6

- IPv4 and IPv6 prefixes are managed the same way
- Adapt equipment to IPv6 (routing protocol and forwarding plan)
  - If not possible with core network elements : use MPLS or 6PE
- We already have some IPv6 core networks
• V6fication can be a question of investment

• But last mile syndrome… may stay IPv4 until new IPv6 based services are developed in home network.

• Transition is possible
  • IETF’s Softwires working group

---

• During first phase : L2TP
  • L2TP uses UDP => NAT Traversal
  • PPP is encapsulated in L2TP :
    • User authentication
    • Keep alive messages to maintain NAT contexts
    • Link Local addresses configuration

• Study prefix delegation
  • Interaction with DHCPv6 PD
  • Interaction with AAA
Softwires’ tunnels

Home Network

Access Network

• Three possibilities in Home Network:
  • CPE on hosts: One IPv6 address per host
  • CPE on special devices:
    • Prefiguration of IPv6 service: always-on, not computer centric
    • Point6box experimentation
  • CPE on Home Gateway
    • Last step before dual stack Access Network

• Challenge:
  • Low cost CPE
  • PE architecture

Home Network Architecture

Home Network

Applis

NAT

H
G
W

• Have some dedicated applications outside of the gateway
  • Managed by the provider?
  • Security is a key element
Laurent Toutain

Home Network Security

- In IPv4: NAT gives a security feeling
- In IPv6: Firewall can do the same
  - Address scanning is more difficult
  - Ingress connection filtering can be done
- Benefits: Application knows their addresses
- But we need to go forward to accept some incoming sessions:
  - With extensions: protocol stack is complex and order is important
  - Addresses may change from time to time (privacy issues)
- Need for a formal language to specify rules
- Need dialog between applications and routers
  - Based on a service discovery protocol

Laurent Toutain

Home Network Architecture

- Better security than UPnP NAT context setting
- Authentication is a way to maintain links between providers HGW and applications
  - Standard protocols or pre-registered keys?
• **User can build complex architecture**
  - If Bridging is used: loops must be detected
  - Spanning Tree is not efficient for Traffic Engineering
  - Traffic will converge on some links

• **Routing will allow more control:**
  - Routers have to be configured

| GP = provider | SID = ? | I-ID = autoconf |
**DHCPv6 Prefix Delegation**

- **Main idea:** The edge router
  - become the DHCPv6 server for prefixes (/64) for the home network.
  - Get a global prefix for the provider.
  - Create a pool of GP:SiD to reach the /64 boundary
  - Allocate these prefixes to routers

- **When a router starts:**
  - Periodically broadcast requests until receiving an answer from a DHCPv6 server
  - When configured act as a DHCPv6 relay.

- **More studies on multi-homing and network stability are needed**

---

**No Administration Protocol**

- **draft-chelius-router-autoconf-00.txt**

- **Main idea:**
  - IPv6 address is divided in 3 parts
    - GP is given by the ISP (DHCPv6,...)
    - IID is obtained through auto-configuration
    - SID is currently configured manually in routers
  - To allow a full auto-configuration, SID must be assigned automatically.

- **Solution:**
  - Use extension to OSPF to obtain a consensus on SID value in a domain.

- **Next Step:**
  - Better integration with routing protocols
**IPv4 Multi-homing**

- Private addresses for hosts
- Packets are routed to the closest exit router
- Exit router will change the source address to the provider's address
- Applications are not multi-home aware

**IPv6 Multi-homing**

- Host will have one per provider
  - Rules to select source address are very simple
- Routing is based mainly on default route
  - Packet may lead to the wrong provider and discarded
- Modify IGP to handle source address in default routing?
ABC Extension

- Improve IGP to handle source address properly
- When an equipment selects a provider by selecting the source address

Edge routers using service discovery protocol gives information concerning providers network (cost, bandwidth, error rate, prefix…)

Application selects source address regarding edge router information

If one access fails, application decides the appropriate behavior
  - Wait until network recover
  - Change addresses (source or destination)

Compatible with shim6 multi-homing approach
**ABCD example**

- **Home Network**
  - UMTS: Expensive, low bandwidth
  - ADSL: Free, high bandwidth

- **α**
- **β**

- **Peer to peer application:**
  - Use β prefix - if β fail, wait
- **VoIP application:**
  - Use β prefix - if β fail use α (a multi-homing mechanism will manage address change)
- **Monitoring application:**
  - Use β prefix - if β fail use α and reduce quality

**Routing strategy**

- **Current IGP:**
  - Scalable
  - Traffic converge to high speed links
- **Home network:**
  - Relatively low bandwidth
  - No scalability problems
  - Spread as much as possible traffic to use available bandwidth
Conclusions: Time line

- Tunneling to IPv6 core networks
- Simple Firewalls
- End-to-end applications
- Simple registration protocol
- Multi-homing
- Source address selection
- Adaptive applications + shim6
- Router auto-configuration
- Multi-homing Routing protocol
- Complex network topology
- QoS aware routing

Conclusions

- To go from interface to interconnection:
  - Guaranty security
    - Trust in providers, in equipments
  - Guaranty simplicity
    - For users: plug and play
    - For providers: not all services in one box
    - Keep IPv6 simple to allow interconnection
  - Guaranty quality
    - For user: “intuitive” cabling
  - Guaranty incomes
    - Based on service discovery and security