Home Network Evolution

Laurent Toutain – ENST Bretagne

In this talk, we forecast network and protocols evolution related to IPv6 and explore new functionalities made available by this new version of the IP protocol. We will take some conservative hypothesis concerning network evolution: we still consider a network composed of infrastructure (with routers and hosts) and we consider that IP hierarchical addressing scheme is not modified. Core network is not logically impacted by the introduction of IPv6, since current IPv6 addressing plan derive from CIDR mainly used in IPv4. Provider network will have to allocate IPv6 prefixes (i.e. only one part of the address) instead of a full IPv4 addresses. The main impact of IPv6 will be found on small stub sites such as Home or SME networks, where the plug and play (with security) will be an accelerating deployment factor. One goal of this talk is to study evolution of routing protocols, which should include new features (auto-configuration, multi-homing, new routing strategies). The interaction with service discovery protocols may be used to select the best provider or to configure automatically firewall. The combination of these protocols may help to establish a link between the providers and the users.

Nowadays home or SME Networks are very simple and are composed of a single link where Ethernet and Wi-Fi are bridged. Auto-configuration for IPv4 is obvious; a DHCP server located in the CPEv4 can allocated private IPv4 addresses to equipments requesting it. If other routers are introduced in that network either the user must have some network knowledge or the topology must be a star centred on the access gateway. Even if the size of the network is limited to a house or small company, the network could evolve to a more complex topology due to the different layer 2 technologies used to transport information. The topology of the network may also change frequently when the user plug or unplug equipments. Bridging these different medias could lead to a very inefficient network. Protocols like spanning tree can avoid loops, but without a careful configuration, the use of available bandwidth will not be optimised. Routing is more adapted to traffic engineering but implies routers configuration. Hosts' auto-configuration in IPv6 network is presented as a major feature, but it supposes that routers have been previously manually configured. In a first approach, router auto-configuration can be done using a hierarchical DHCPv6 Prefix Delegation mechanism, but this solution does not handle easily network topology changing or multi-homing. Router auto-configuration can be included in the routing protocol leading to a more flexible and distributed approach as shown in [AINA2005]. Some prototypes have proved the feasibility concept [Globecom2005] in terms of responsiveness and efficiency.

Multi-homing will be more and more common feature, not only for reliability reasons as it is defined nowadays, but because the connectivity offer will be *de facto* larger (3G, ADSL,…) . IPv6 approach consists in allocating to every host an address per provider to limit the expansion of core routing table. Currently this approach does not work in stub site networks since packet forwarding is based only on the destination address. If packets reach a provider with a source address different from the one assigned by this provider, the packet will be discarded for security reasons. A routing protocol for stub sites should take into account the source address in their forwarding decisions. In the future, this can be viewed as a generalization of the Always Best Connected concepts; where a host is not directly connected to several access networks, but the source address selection allows the network provider choice. Access routers may announce the network characteristics, combined with multiple addresses management as defined by the shim6 working group, this will allow application to adapt to the access provider characteristics, by reducing bandwidth or stopping transmission when some criteria are not reached.

IPv6 in this king of stub network will have an impact on firewall. In IPv4, firewall combined with a NAT, are configured with a limited number of parameters. IPv6 firewall can block incoming session to reach the same level of security, but this limits the benefits of global addresses. A dialog must be established between applications and firewalls to allow incoming sessions. The number of parameters to define an IPv6 session is more important than in IPv4: extension parameters have to be described (especially if multi-homing or mobility is allowed), extensions order may also have an impact, hosts addresses may change from time to time to guaranty privacy. This remote firewall configuration can be compared to UPnP functionalities, but they must be done securely. Pre-established security links can be a way to simplify user configuration and allow equipments certified by the provider or the gateway manufacturer.

Finally, bandwidth may become a scare resource in such environment, current IGP trends to aggregate traffic to high capacity links. In home network, such links will probably not exist. In that case routing protocol should be adapted to spread the traffic among available links and take into account some flow characteristics.

Bibliography

[AINA2005] G. Chelius, E Fleury, and L. Toutain, No admistration protocol (nap) for ipv6 router autoconfiguration, Int. J. Internet Protocol Technology, vol. 1 (2005), no. 2, p. 101-108.

[GlobeCom] J. Mangues-Bafalluy, G. Martinez-Perez, and G. Chelius, Evaluation of router autoconfiguration time during network initialization for centralized and distributed schemes, Globecom 2005 (Saint Louis, USA), IEEE, November 2005.