Auto-Transition
IPv6 SIG
Hanoi, APNIC20 Sept. 2005

Jordi Palet (jordi.palet@consulintel.es)
Miguel A. Díaz (miguelangel.diaz@consulintel.es)

Framework and Objectives

- This work seek to ensure that any device can obtain IPv6 connectivity at any time and whatever network is attached to, even if such network is connected to Internet only with IPv4
  - Or already has IPv6 but with poor performance
- Deal with aspects regarding
  - Evaluation of the possible IPv6 transition mechanisms
  - How to overcome IPv4 network barriers like NAT and Firewalls
  - Definition of an algorithm to choose the best mechanism according to performance criteria

Why ?

- Lots of devices and applications around us will benefit obtaining IPv6 connectivity everywhere:
  - home automation, wearable devices, cars, PDAs, mobile phones, peer-to-peer applications, remote control applications, etc.
- The main goal of the “auto-transition” concept is to facilitate the IPv6 deployment in a seamless way for such devices and applications:
  - native IPv6 connectivity is not always possible
  - users need to use an IPv6 transition mechanism in a seamless way

Motivation (I)

- There are well known methods for IPv6 autoconfiguration
  - Stateless and statefull IPv6 autoconfiguration (RFC2461)
- There are also transition mechanism for getting IPv6 connectivity through IPv4 networks
  - Tunnel-based (6to4, TB, ISATAP, Teredo, …)
  - Most of them aren't automatic
- There is a contradiction:
  - While IPv6 tries to help the users by means of autoconfiguration, it only can be used if native IPv6 connectivity is available.
- Users and appliances require complete PnP, even when only IPv4 is available, so it is required a method that deals with this problem

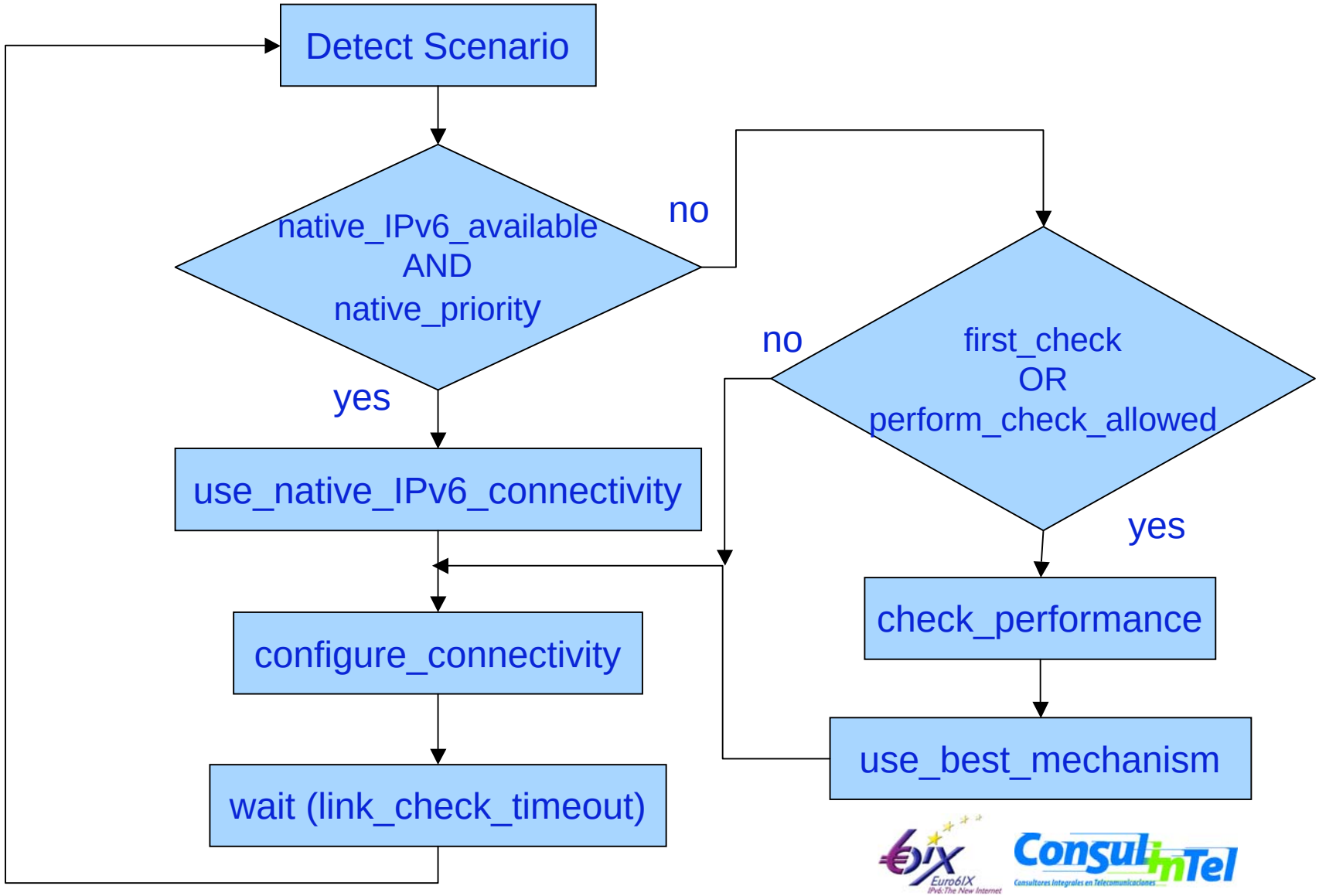
Motivation (II)

- The algorithm is defined to be possibly integrated into the IPv6 stack-set or as a kind of wizard
- Applicable to nodes and middle-boxes (CPEs)
  - Hosts, consumer electronics, appliances, alarms, home-automation devices, …
- Users don’t need to know anything about how to get IPv6 connectivity

Algorithm behavior (I)

- Native IPv6 is preferred, but users could decide to use a transition mechanism if it offers better performance
- The selection criteria is based on connection performance
  - To simplify actual implementation only delay and losses are considered

Algorithm behavior (II)



Modularity Approach

- A possible list of mechanisms to be checked, ordered by preference could be:
  - Native IPv6 Connectivity
  - TS with proto-41
  - TS with UDP
  - ISATAP
  - STEP
  - 6to4
  - Teredo
- But it should be open to others or possibly new mechanisms

Transition Mechanism to overcome IPv4 network barriers

- NAT boxes, proxies or firewalls do not allow tunnel-based transition mechanisms to work properly
- It is required that the auto-transition mechanisms uses a method that cannot be rejected by the middle box. The following solutions could be considered:
  - Layer II tunnels (L2TP, PPTP, PPPoE)
  - Layer III tunnels (L3 VPNs)
  - Layer IV tunnels (TLS/SSH, HTTP, SSH)

Discovery of the TEP

- Devices running the auto-transition algorithm need to know where to find the IPv6 Tunnel End Point (TEP), which provides the IPv6 connectivity, just in case native IPv6 connectivity is not available.
- Users want plug-and-play devices/services and that most of them do not have any knowledge about how the transition mechanisms works or where the nearest TEP is located.
- It is required to consider the auto-discovery of the IPv6 TEP (which could also include the tunnel setup handshake).

Auto-Discovery Proposal

- Usage of existing infrastructure and protocols.
  1. DNS server with SRV RR support. The service name for the auto-discovery purpose should be standardized for each transition mechanism in the following form:
     - _transition-mechanism_srv._protocol.ispname.com

       One important advantage of this method is that load balancing can be done easily and efficiently by means of priority and weight parameters defined in SRV RR.
  2. A/CNAME RR for Unicast. A standardized A/CNAME RR for each supported transition mechanisms within the domain of the ISP. According to the same nomenclature, the DNS entries would follow the form:
     - transition-mechanism_srv.ispname.com
  3. Anycast (Shared Unicast) Addresses. Each transition mechanism would have an assigned anycast (shared unicast) address, such as in the case of the 6to4 transition mechanism. The anycast prefix/address for each transition mechanism would be specified by IANA

Network Managed Transition

- The process used for getting IPv6 connectivity can be improved by using new functionalities provided by the Network
- The new approach is based on PBNs
- The network stores transition mechanism policies
  - Interaction with other policies is allowed: QoS, Security, Routing, etc.
- The transition mechanism would work better, but it must work even if the network support is not present
- The ISP has control over the transition process

Conclusions

- There is a need for a method to provide plug-and-play features to IPv6 transition mechanisms in the same way that the IPv6 protocol does in the local network.
- With this philosophy users do not have to know any technical knowledge to choose the more adequate transition mechanisms, nor to make any setup of it, nor to find out where the nearest TEP is located.
- They just plug their devices and they automatically become IPv6 capable whether they are in a native IPv6 environment or not, even if they are in a private IPv4 environment behind a NAT box.
- Some research to achieve these goals is being done and some preliminary work is presented in this paper.

Thanks !

Questions ?