v6ops

"opportunistic" and zero-configured tunneling

Pekka Savola
Jonne Soininen

"Opportunistic" vs zero-configured

The concepts

- ☐ "Opportunistic" in Internet domain
  - ○ Minimal or zero infrastructure
  - ○ Connectivity between peers set up in an "ad-hoc" fashion
  - ○ Required if assuming "vendor-driven" deployment
    - ▷ When the vendor requires IPv6 for enhancing its functions (e.g., peer-to-peer libraries)
    - ▷ In contrast to user installing a new shiny application which requires IPv6
  - ○ E.g., 6to4, Teredo
  - ○ Applicability: when the direct ISP doesn't offer service
    - ▷ Tunnel broker typically not available close by, or easy enough to set up

- ☐ "Zero-configured"
  - ○ "Configured tunnel" or similar but not configured manually
  - ○ Tunnel-end -point discovered automatically
    - ▷ E.g., STEP or ISATAP; TSP with some discovery mechanisms
  - ○ Applicability
    - ▷ 3GPP networks, direct ISP offering tunnel, enterprise -internal tunneling

"Opportunistic" vs zero-configured

What's so special about opportunistic?
- There was a long threat on the list
  - Not sure if it resolved much of anything..
  - Some (many?) see there is no purely "vendor-driven" approach
    - Or if there is, we should not be recommending it
  - If so, automatic tunneling maybe not be a strict requirement

- Critical point of opportunistic vs others
  - Whether infrastructureless, even partial, deployment is desirable
    - And how critical that infrastructure is
  - How much to weight in the favor of "less infrastructure"
  - Economics of deployment is also a factor - against both approaches
  - Anonymous services are better for 3rd party service providers
    - 6to4 relay with 192.88.99.1 vs Tunnel broker with native addresses

The different scenarios

The different scenarios
- ☐ Unmanaged user wants to do p2p with another
  - ○ Direct "short-cut" connectivity very important
  - ○ If no support from the direct ISP
    - ▷ Automatic tunneling works automatically: Teredo requires "Server" with low b/w reqs
    - ▷ Tunnel broker would help, if the users could find a free broker nearby
    - ▷ If there would be incentive for broker deployment, a "nearest broker discovery" process would also help
    - ▷ Unless the user is really determined, the user is lost without automatic tunneling
  - ○ If there is support from the direct ISP
    - ▷ Dual-stack or; tunnel broker or a simple configured tunneling system
    - ▷ If only one supports, still OK without infrastructure if "local" relays
- ☐ Enterprise internal network wants to deploy v6
  - ○ Zero-configured tunneling, configured tunneling, or dual-stack
- ☐ 3GPP user wants to use v6
  - ○ Zero-configured tunneling or dual-stack
    - ▷ The operator should provide a service, and if doesn't, similar to "unmanaged"

Opportunistic relay deployment

Relay deployment
- ☐ Native to 6to4
  - ○ All dual-stack sites could have a relay, just turn on 6to4 pseudo-i/f
    - ▷ But currently don't..
    - ▷ Would place the "burden" of deployment on native users
- ☐ 6to4 to Native
  - ○ Very difficult, but not worse than Tunnel Broker..?
- ☐ Native to Teredo
  - ○ All the sites could have a relay
    - ▷ But currently don't, and not sure if a good idea..
    - ▷ Would place the "burden" of deployment on native users
- ☐ Teredo to Native
  - ○ Very difficult, similar to 6to4..?
- ☐ 6to4 to Teredo
  - ○ Sites could have an internal Teredo relay
- ☐ Teredo to 6to4
  - ○ Nodes could have an internal 6to4 relay
    - ▷ But some NATs might block proto-41 at egress

"Zero-configured"

Teasing out "Zero-configured"

- Critical questions are at least
  - How important is 3rd party ISP tunneling? Are solutions required?
    - If yes, who would want to provide *production* service using their IPv6 addresses?
    - Would imply long tunnels, bad quality and bad IPv6 experience.. like today's 6bone
  - How much should we use existing tools/mechanisms, if available?
    - NAT traversal, authentication, prefix delegation, DNS discovery, etc.
    - Should be generic so that a node that is used in unmanaged or enterprise, with native or tunneling, doesn't have to multiple methods?
    - Implement from scratch ("short term fix"), develop good tools ("long term solution")?
  - How desirable is "opportunism" inside the ISP/3GPP or site?
    - The tradeoff: if the traffic grows too much, it's time to enable native IPv6?
    - Inside the ISP: (the neighbors wanting to talk p2p): probably not critical
    - Inside the 3GPP: depends on how much traffic between UEs; the IPv6 status?
    - Inside the enterprise: in larger sites, possibly desirable (e.g., p2p videoconferencing)

"Zero-configured" solutions

"Zero-configured" solution properties
- ☐ Direct connectivity between (some) peers
  - ○ ISATAP: yes
  - ○ Others: no
- ☐ Use of existing tools
  - ○ TSP: reinvents all discovery/config functions
  - ○ ISATAP: mostly new
  - ○ STEP: client - only little new; server - a bit
  - ○ L2TP architecture: uses only existing tools
- ☐ 3rd party tunneling (critical: authentication)
  - ○ TSP and L2TP: no problem if 3rd party ISPs exist ;-)
  - ○ STEP and ISATAP: out of scope or not applicable