perimeter-ident

ietf://homenet/84

ek@google.com

Disclaimers

- It's an annoying problem
  - IPoE is problematic—by design

- Needs smarter people thinking about it
  - Should be much simpler than it is now

- There are many distracting side-problems
  - multiple interior zones
  - what's the right policy to apply where
  - authenticated routing protocols
  - ...SQUIRREL!

Scope and Terminology

- Tried to limit the scope

- Terminology
  - "interior"
    approx. a single logical administrative domain
  - "exterior"
    everything else
  - "perimeter"
    the sum of (ephemeral) demarcations between

- Only going to deal with one of each

Signals we can use

- Product-defined interface purposes
- Routing adjacency
  - Security requirements/implications?
- Links requiring subscriber information
  - 3GPP ("valid SIM cards"), PPPoE with credentials
- Links requiring existing IP-layer connectivity
  - PPTP, L2TP, 6rd, 4rd, 6to4, Teredo
- Links that are point-to-point in nature
  - PPPo{A,E}, possible future link types

What to do with IPoE?

- DHCPv6-PD
  - If used in the interior then can't be a signal of the perimeter

- Other tricks?
  - If setting up rev DNS (vis. delegation drafts)
  - If DHCPv4 a non-RFC{1918,6598} address?
  - ...?

- Default: assume an **open** posture?

Additional considerations

- Physical vs. virtual interfaces
  - Recommendation: by default, if any interface has a perimeter they should all be classified as such
- Mixed zone next-hops on a single interface
  - Recommendation: by default, if forwarding to any next-hop on an interface transits a perimeter then all next-hops should be classified as such (and indeed the whole interface)
- IPv4 vs IPv6 perimeters
  - Keep them the same
    - Simple, and Principle of Least Surprise