Scalable Connectionless Tunneling Architecture and Protocols for VPNs

<draft-kuwahara-cl-tunneling-vpn-00.txt>

July 16, 2002 The 54th IETF PPVPN WG

T.Kuwahara, J. Murayama, N. Yoshida, M. Tanikawa
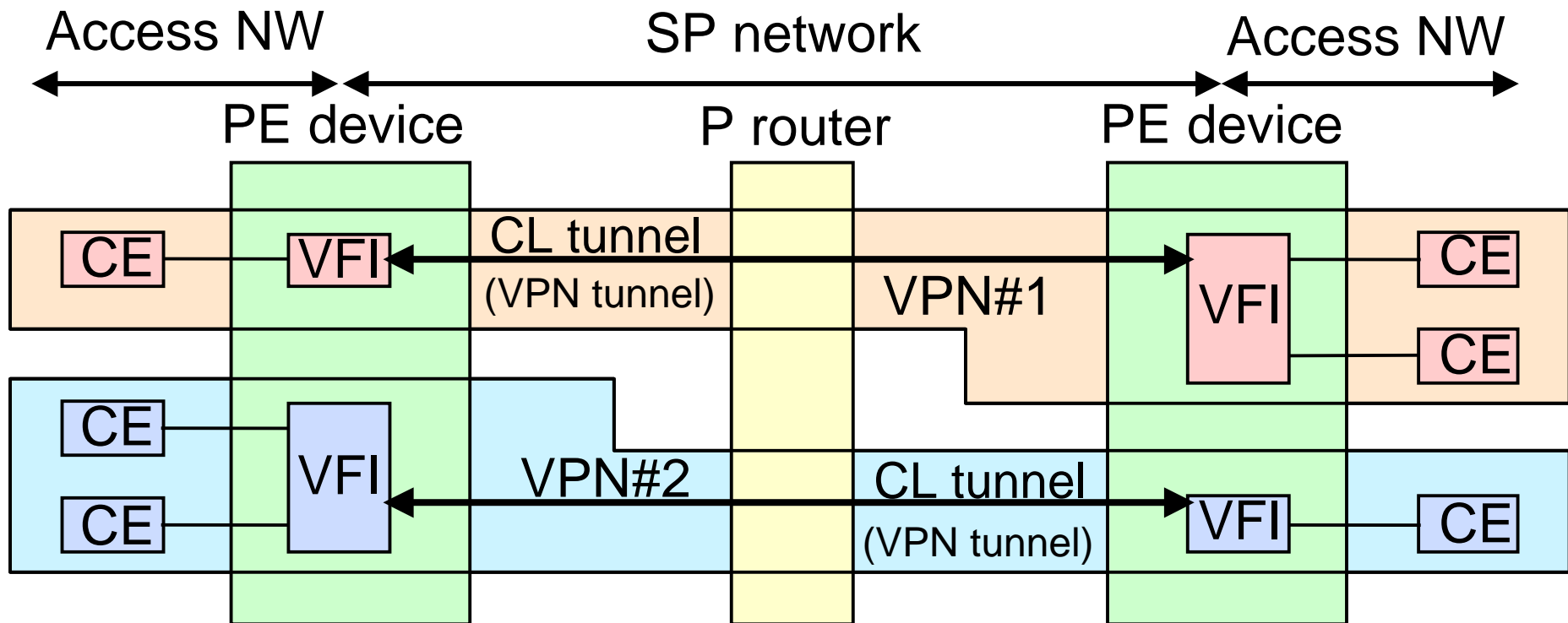Presented by M. Suzuki

NTT

Overview of the draft

- Objectives
  - To define a CL tunneling architecture
  - To specify protocols for the architecture
- Architecture conforms to ref. model for L3 PE-based VPNs
  - VPN tunnels based on CL tunneling protocol (e.g., IP-in-IP)
- CL tunneling architecture supports:
  - Full mesh and hub & spoke CL tunnel topologies
  - Static default tunnels based on routing information
  - Dynamic cut-through tunnel setup for hub & spoke topology
- Connection-less tunneling control protocol (CTCP)
  - Stateless and light weight control protocol
  - Enable dynamic cut-through tunnel establishment

Connectionless Tunneling Architecture (Mesh topology)

- Architecture conforms to ref. model for L3 PE-based VPNs
- VPN tunnels based on CL tunneling protocol (e.g., IP-in-IP)

Access NW | SP network | Access NW

PE device | P router | PE device

CE — VFI ← CL tunnel (VPN tunnel) → VFI — CE
VPN#1
CE

CE — VFI ← VPN#2 — CL tunnel (VPN tunnel) → VFI — CE
CE

- CL tunneling architecture supports full mesh and hub & spoke CL tunnel topologies

Connectionless Tunneling Architecture
(Hub and spoke topology)

- CL tunneling architecture supports:
  - Static default tunnels based on routing information
  - Dynamic cut-through tunnel setup for hub & spoke topology
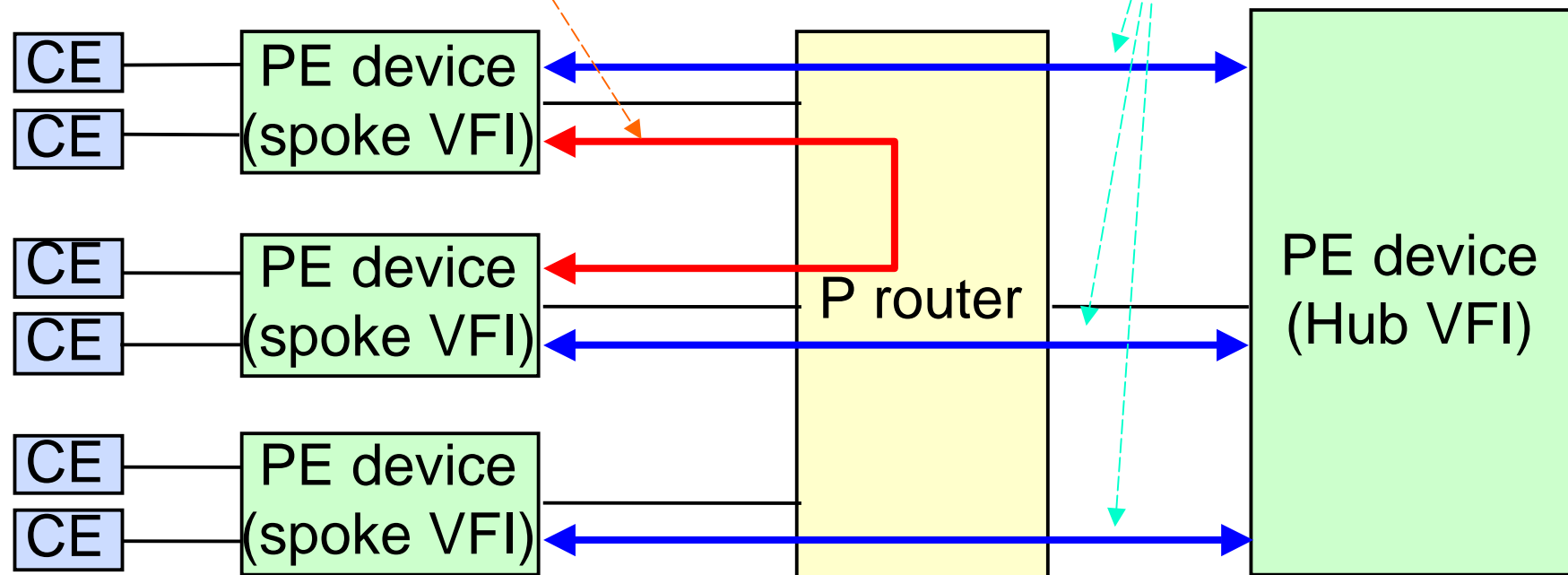
- Connection-less tunneling control protocol (CTCP)
  - Stateless and light weight control protocol
  - Enable dynamic cut-through tunnel establishment

Dscussion 1: Scope of the architecture

- Q: Specifications for VPN membership discovery and routing protocol for SP network are not described in the draft
- A: Out of scope of "tunneling architecture"
  - No restriction for these protocols
  - VPN membership configuration schemes (e.g., manual, SNMP, LDAP, DNS, BGP-4) may be used with it
  - CTCP doesn't impact on routing protocol behavior
- The architecture specifies minimum protocols for tunneling
  - IP-in-IPv6 for SP network and tunneling protocols
  - ICMPv6 for SP network control
  - CTCP is proposed for tunnel control
- Clarify scope of tunneling architecture in the next version

Protocols for the architecture
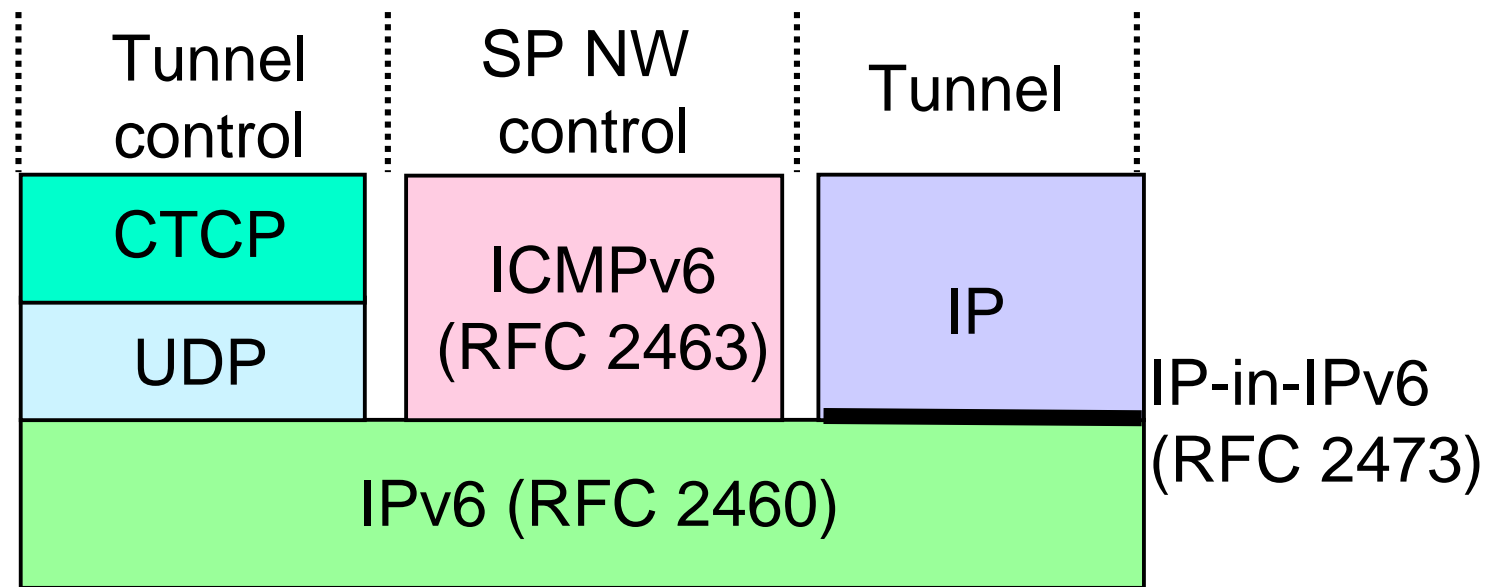
Tunnel control	SP NW control	Tunnel
CTCP	ICMPv6 (RFC 2463)	IP
UDP		

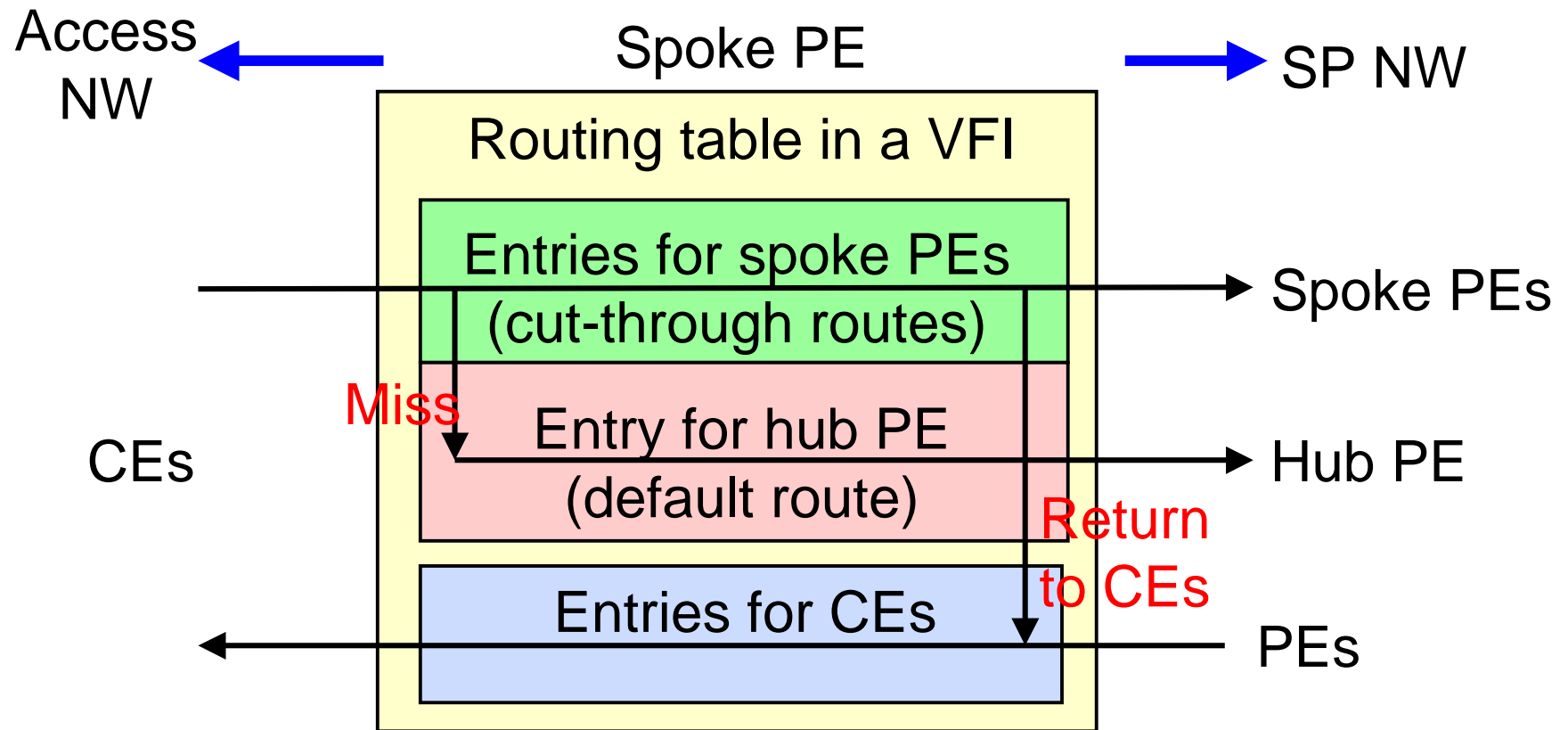IP-in-IPv6 (RFC 2473)

IPv6 (RFC 2460)

- The architecture specifies minimum protocols for tunneling
  - IP-in-IPv6 for SP network and tunneling protocols
  - ICMPv6 for SP network control
  - CTCP is proposed for tunnel control
- Clarify scope of tunneling architecture in the next version

Discussion 2: Loop free routing

- Q: CTCP may trigger off routing loop
- A: Implementation dependence
  - Routing table separation ensures loop free routing
  - A routing table in a VFI of a spoke PE should consist of:
    - Entries for cut-through routes (created by CTCP)
    - Entry for default route (created by routing protocol)
    - Entries for CEs (created by routing protocol)
  - When spoke PE receives a packet from a CE, first it searches for cut-through routes. If it misses, it further searches for default route
  - When spoke PE receives a packet from a PE, it searches for entries for CEs, never forward to a PE.
- Clarify routing table implementation in the next version

Routing table separation

Access NW ←   Spoke PE   → SP NW

Routing table in a VFI

Entries for spoke PEs
(cut-through routes) → Spoke PEs

CEs

Miss

Entry for hub PE
(default route) → Hub PE

Return to CEs

Entries for CEs → PEs

Further issues and next steps

- Further issues
  - UDP port number assignment for CTCP
  - Terminology update to coordinate with the latest version of the layer 3 PPVPN framework document
  - References section update to align with the new RFC editorial policy
- Next steps
  - Submit revised version until the coming September, then solicit WG last call
  - Request UDP port number assignment to the IANA after the IESG review
  - Publish as a proposed standard RFC