VPN Endpoint Discovery

draft-luciani-ppvpn-vpn-discovery-01.txt

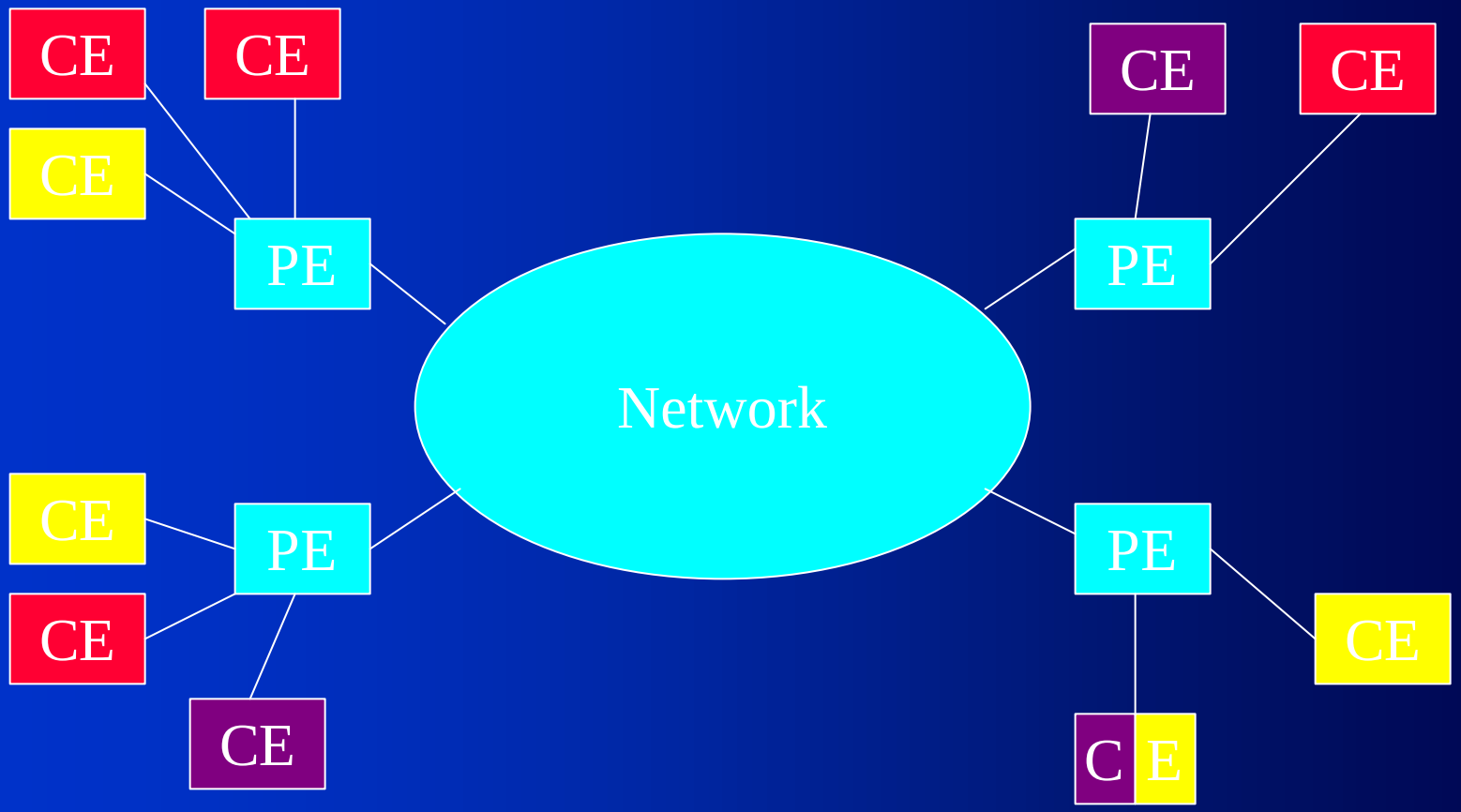
Matt Squire
Hatteras Networks
msquire@hatterasnetworks.com

IETF December, 2001

Many Authors

- Cedell Alexander - Extreme Networks
- Loa Andersson - Utfors
- Marty Borden - Atrica
- Ryan Brooks - Time Warner Telecom
- Juha Heinanen – Song Networks
- Giles Heron – Packet Exchange
- Pierre Lin - Yipes
- James Luciani – Crescent Networks
- Matt Squire - Hatteras Networks
- Olen Stokes – Extreme Networks

VPN Model



A Day in the Life of a VPN

- Discovery
  - Who do I talk to for this VPN?
  - Configuration, BGP, multicast
- Signaling
  - What do I need to know to I talk to them?
  - LDP, RSVP, BGP
- Data Transfer
  - How do I get data from PE1 to PE2?
  - MPLS, L2TP, GRE, IPSEC, etc.
- Membership Changes
  - How do I detect and adjust?
  - Configuration, BGP

Example: VPLS Proposals

- BGP
  - Include VPN IDs in BGP using multi-protocol extensions (RFC 2547) – discovery and signaling combined into advertisement
- Use discovery protocol plus signaling protocol
  - Signaling protocol depends on desired tunnel technology
    - LDP (draft-martini-l2circuit-trans-mpls-08.txt), RSVP (draft-cai-ppvpn-vc-rsvp-te-01.txt), L2TP, etc.
  - Discovery by
    - Multicast. Every VPN gets own multicast address in provider network (RFC 2917)
    - Directory/DNS. Perform lookup in well-known directory for VPN membership (*draft-luciani-ppvpn-vpn-discovery-01.txt*)

BGP Discovery Not For Everyone

- BGP is not (and should not be) everywhere
- Need not carry everything
- Increases size of routing table
- Hard to differentiate different peers
- Binds routing and VPN info

DNS Based Discovery

- Name configured in DNS with IP address of all PE equipment supporting that VPN

  DNS: companyX.serviceProviderY.net =

  { 63.64.65.1, 63.64.66.1, 63.64.67.1, 63.64.68.1}
- Each VPN configured with local port information, signaling method, and DNS name
- At startup, lookup all IPs associated with name and signal them individually (optionally use name in TLV while signaling)
- Membership changes made in DNS, not every PE
- Whenever DNS info expires or after configured t/o, PE's refresh
- Whenever you receive a signaling message from a "new" PE for a VPN, refresh DNS information
- Use DNS security mechanisms (DNSSEC, ACLs, etc.) to control access and provide authentication if desired

DNS Based Discovery Pros and Cons

- Pros
  - DNS is everywhere – no new protocol, ubiquity, easy
  - Character/string based IDs easier for people
  - Integrates easily and well into existing LDP/RSVP VPNs
- Cons
  - Requires a signaling protocol (LDP, L2TP, etc.)
  - Re-provision on DNS time scales
  - Can’t have mixed signaling types within a single VPN

DNS Based Discovery Not Yet Finished

- Signaling extensions in LDP and RSVP – signal DNS name instead of VC ID in FEC
- Issues of scale (oodles of PEs in VPN)
- More precise guidelines on synchronization performance
- Utility of dynamic DNS for PE registration?
- Zero TTLs to eliminate caching?
- Disposition of draft – WG, informative, etc.?