CE Auto-Configuration for Provider Provisioned CE-based VPN

<draft-lee-ppvpn-ce-auto-config-00.txt>

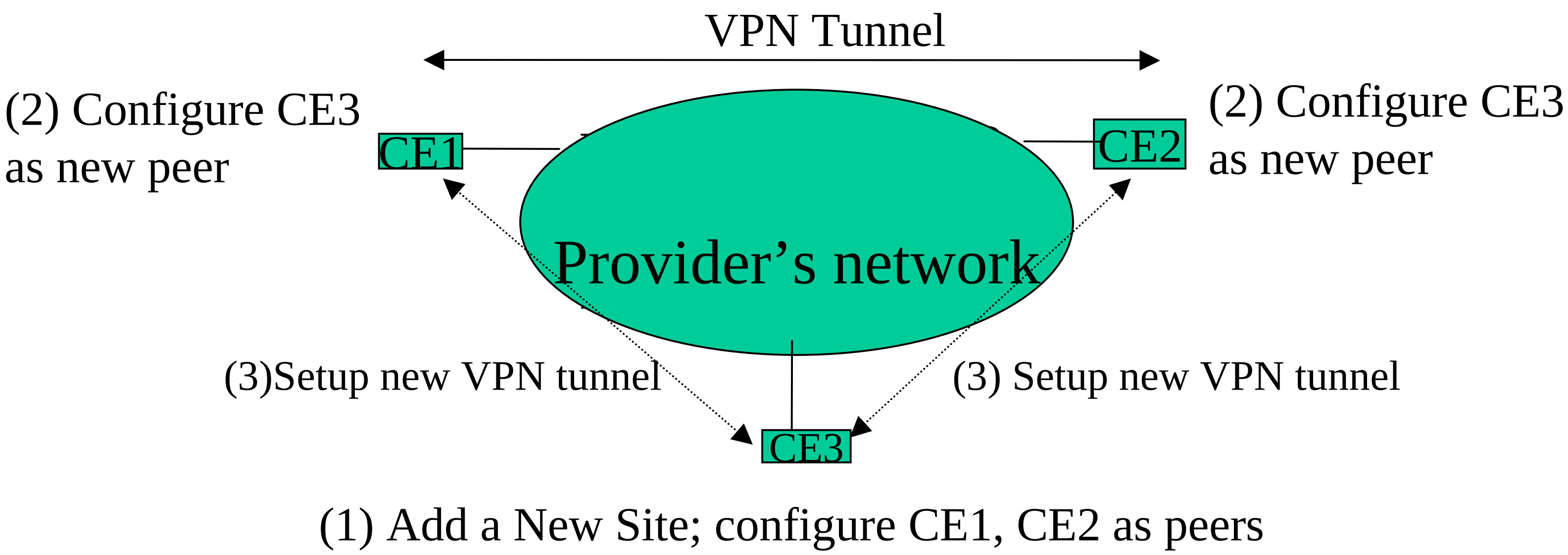
53rd IETF, PPVPN WG

Cheng-Yin Lee
Jeremy deClercq

Why CE auto-configuration?

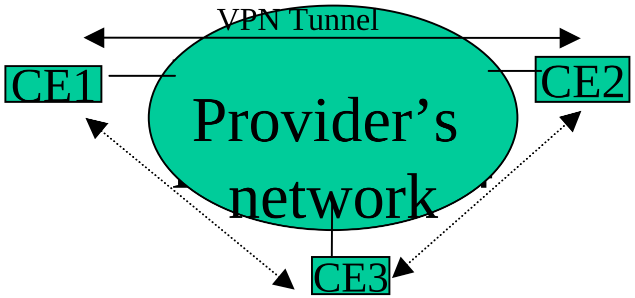
- Every time a site of a VPN is added or removed, other sites of the VPN must be informed:
  - error prone if each CE must be manually updated
  - not cost efficient if to provision all affected CEs (Customer Edge (Equipment)), require "truck-rolls"

CE Provisioning Issues


VPN Tunnel
(2) Configure CE3 as new peer
CE1
CE2
(2) Configure CE3 as new peer
Provider's network
(3)Setup new VPN tunnel
(3) Setup new VPN tunnel
CE3
(1) Add a New Site; configure CE1, CE2 as peers

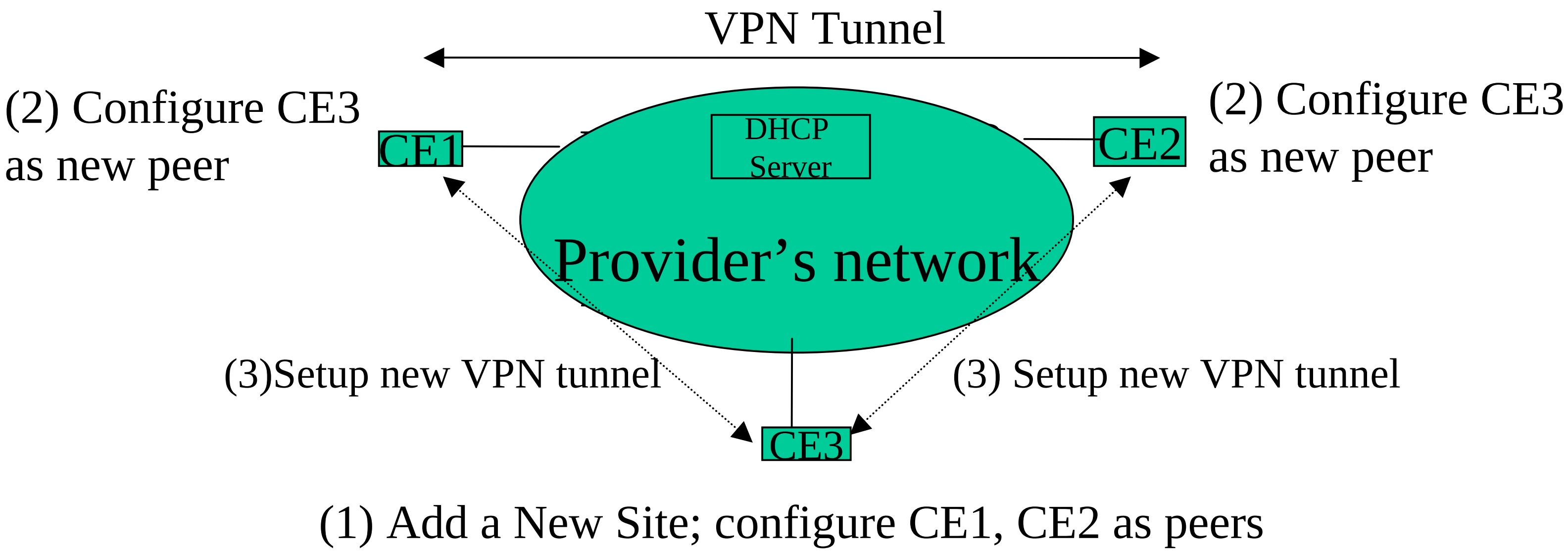
- CE3 must learn about CE1 & CE2
- CE1 & CE2 must be informed of the new site, CE3

CE Provisioning Issues (cont)



- CE3 must learn about CE1 & CE2
  - *could pre-configure CE3 with CE1 & CE2 address or*
  - *(more flexible if) CE3 could dynamically learn of CE1 & CE2 [e.g. use DNS/LDAP, a routing protocol (may not scale), or use DHCP]*
- CE1 & CE2 must be informed of the new site
  - *CE1 & CE2 could poll a server (e.g. DNS, LDAP) for VPN sites update (how frequent?) OR*
  - *when CE3 attempts to setup tunnel to CE1 & CE2, CE1 &CE2 implicitly being informed of CE3 (implies network operator is not able to explicitly setup or teardown tunnel to new/old sites) OR*
  - *could dynamically update CE1 & CE2 [e.g. use DHCP (lightweight) or a policy server or a routing protocol] OR*
  - *could use YAP ?*

Brief Overview (using DHCP)


VPN Tunnel
(2) Configure CE3 as new peer
CE1
DHCP Server
Provider's network
CE2
(2) Configure CE3 as new peer
(3)Setup new VPN tunnel
(3) Setup new VPN tunnel
CE3
(1) Add a New Site; configure CE1, CE2 as peers

- CE3 requests VPN sites info via DHCP (using RFC2131 DHCP INFORM)
- CE1 & CE2 are informed (using RFC3203 FORCERENEW) of new VPN sites via DHCP
- Note: DHCP messages are authenticated

Next steps

- Get WG consensus on the VPN parameters to be configured (as described in FW doc) on CE
  - Feed requirements to the appropriate WG (e.g. to DHC WG to add DHCP option for VPN peers)
- Consider case for different (business) scenarios
- Compare different approaches and select suitable approaches for auto-configuration and/or remote manual provisioning
  - DHCP, http, polling a (DNS, LDAP) server for update, SNMP, modify LDAP?, COPS, IKE?, etc
- input to CE-based VPN framework/solution document

Q & A

Q: Can DHCP be used beyond a LAN?

A The DHCP Relay Agent (RFC 1542), relays DHCP messages between DHCP clients and DHCP servers on different LAN.

Q: How to configure CEs on multiple DHCP servers?

A: How DHCP servers are configured and managed is out of scope of this draft, but there are already products which allows multiple DHCP servers to be configured from one management station. CE configuration could be added to these management tools.

Note: RFC3118 allows DHCP messages to be authenticated, RFC3046 addresses several security issues with DHCP use in public networks