CE Auto-Configuration for Provider Provisioned CE-based VPN

<draft-lee-ppvpn-ce-auto-config-02.txt>

55th IETF, PPVPN WG

Cheng-Yin Lee
Jeremy deClercq

Context of proposal

- This proposal identifies some of the mechanisms that may be used to automatically configure a Customer Edge (CE) Equipment to support a VPN service offered by a provider.
- automatic mechanisms for membership discovery/distribution is identified as a requirement in draft-ietf-ppvpn-ce-based-02.txt:
  - "Manual configuration of the information related to the new site into every existing CE in the particular VPN is not a scalable option. An automatic mechanism for membership discovery/distribution is therefore required."

Types of mechanisms (from mailing list discussions)

i) "pull" method

e.g. query a RADIUS/LDAP/http server for VPN site addresses. The server does not push VPN information updates to CEs. The CE may poll the server periodically

ii) "pull" and "push" method

e.g. using something like DHCP which allows a CE to pull/query and DHCP server(s) to push/update CE sites with new VPN information)

iii) receive-trigger-then-pull method

e.g. send "alarms/alerts" to a CE or receive tunnel setup attempt

this will trigger the CE to query a server for new VPN information. If using SNMP messaging to send alarms/alerts, may have to do a "get" from the CE to confirm alarm/alert message is received.

iv) Polling and receive-trigger-then-pull combo (i & iii)

Issues

- Is being able to update/push necessary?
  - No excessive polling messages, but require additional push mechanisms at server
- Is polling sufficient?
  - How frequent to poll? Is it scalable for large number of CEs?
  - If only polling is used, need to trade off timeliness of VPN info with scalability
- Combining polling with receive-trigger-then-pull or push approach may be a good compromise (may then reduce polling interval)?

Next steps

- input to CE-based VPN framework/solution document