Radius Based VPN Discovery

Juha Heinanen
jh@song.fi

Motivation

- there is a need for BGP-free VPN discovery
  - BGP cost/operation cannot be justified in all PEs
- why Radius as directory based alternative:
  - wide support in routers and provisioning systems
  - built-in CE authentication function
  - easily extendable with new attributes
  - built-in multi-provider/multi-AS operation
  - scales to large, hierarchical VPNs

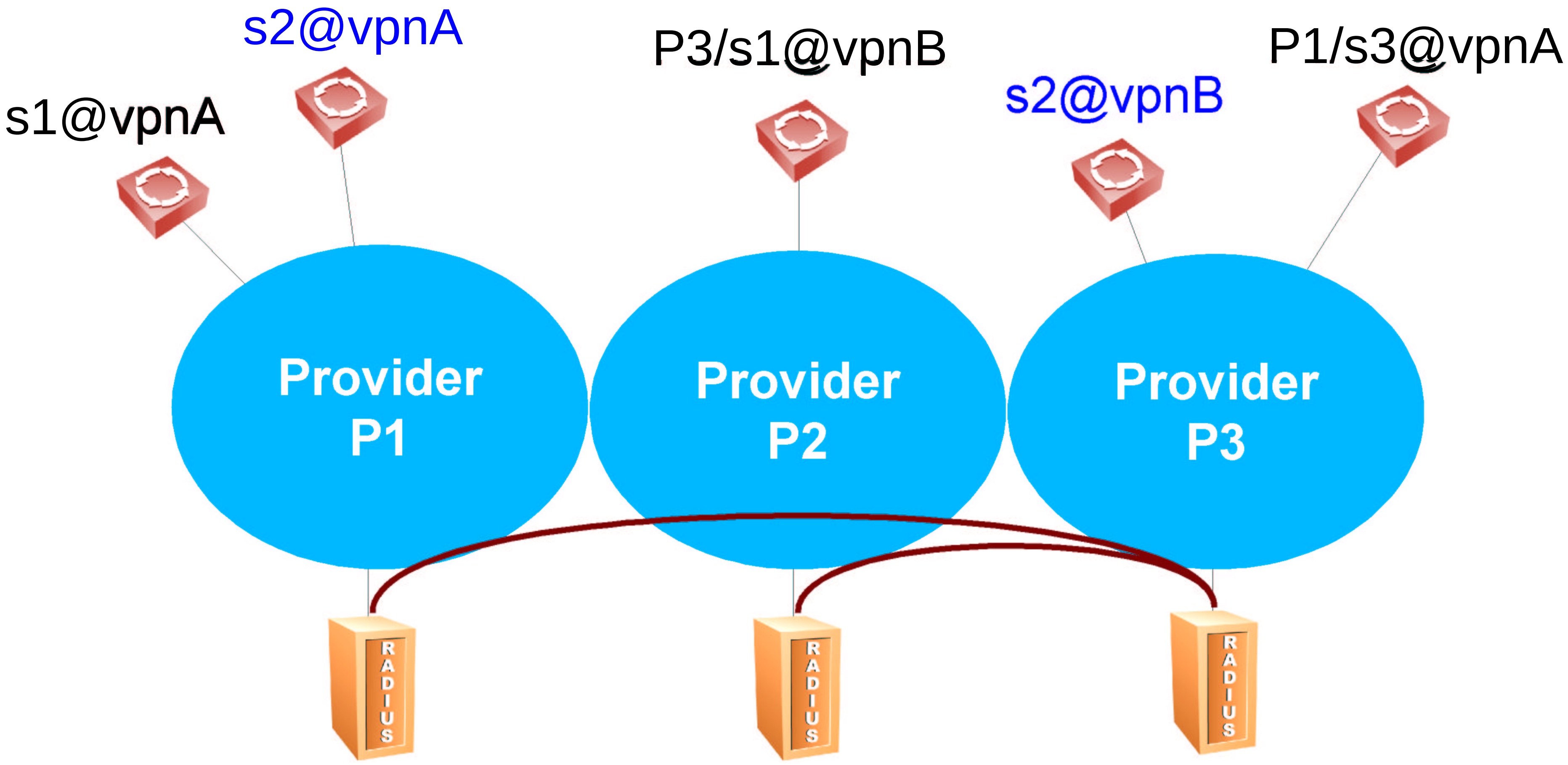
Using Radius for VPN Discovery

- Radius is used by PEs to
  - authenticate CEs and discover other PEs of a VPN
- in Radius terms
  - CEs are users and PEs are NASes (Radius clients)
- Radius servers are used to
  - process and proxy requests from PEs and foreign Radius servers

CE Identification

- each CE has a *user name* of the form
  - [provider/]site@vpn-id
- "provider/" is only needed if CE connects to a PE that doesn't belong to the VPN owner
- example:
  - ProviderX/atlanta@vpnY.domainZ.net

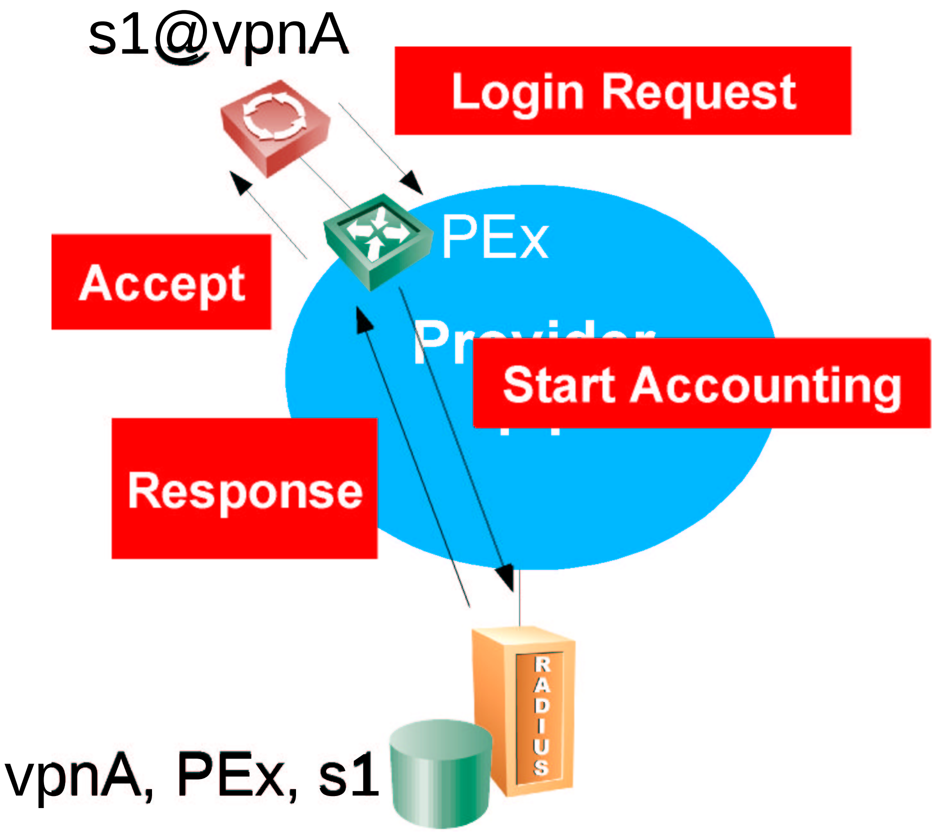
Radius Discovery Example



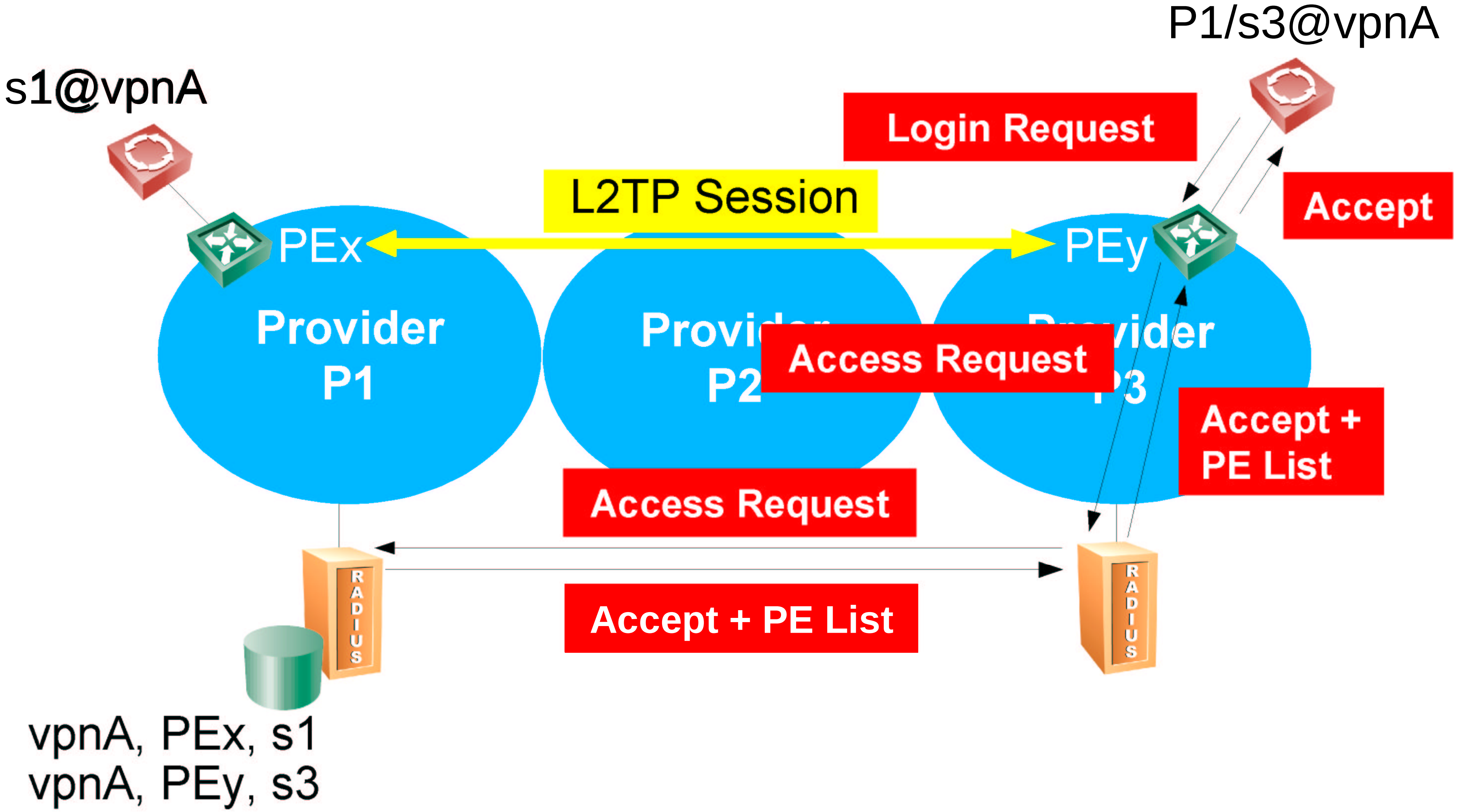
Radius Configuration

- Static CE/VPN membership information:
  - <CE user name, CE password, VPN id>
- Dynamic CE/PE attachment information:
  - <VPN id, PE IP address, CE user name>
- Dynamic PE liveness information:
  - <PE IP address, timestamp>
- Possible other information:
  - PE hub/key info, CE QoS, access lists, ...

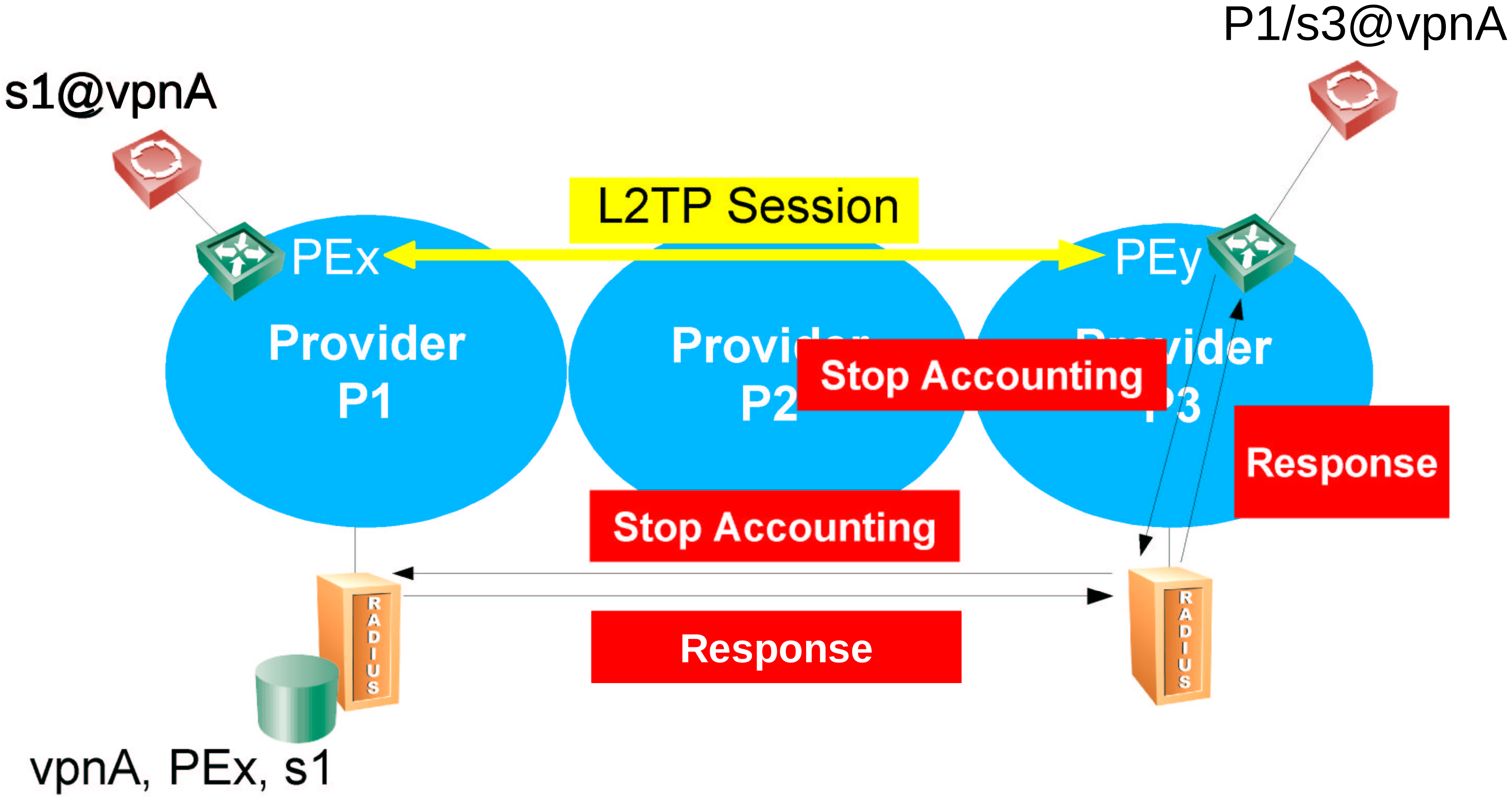
Connecting CEs to a VPN



Connecting CEs to a VPN ...



Disconnecting CEs from a VPN



Failure Detection

- a PE sends at least every N minutes a Radius requests for each realm its CEs belong to
- if Radius does not receive a request from a PE for M * N minutes, it removes all records related to that PE from its database

Next Steps

- find out if there is support for this
- detailed specification of required new Radius attributes (VPN id, PE list)
- implementations in Radius servers, PEs, and provisioning systems