Virtual Private Networks

Juha Heinänen

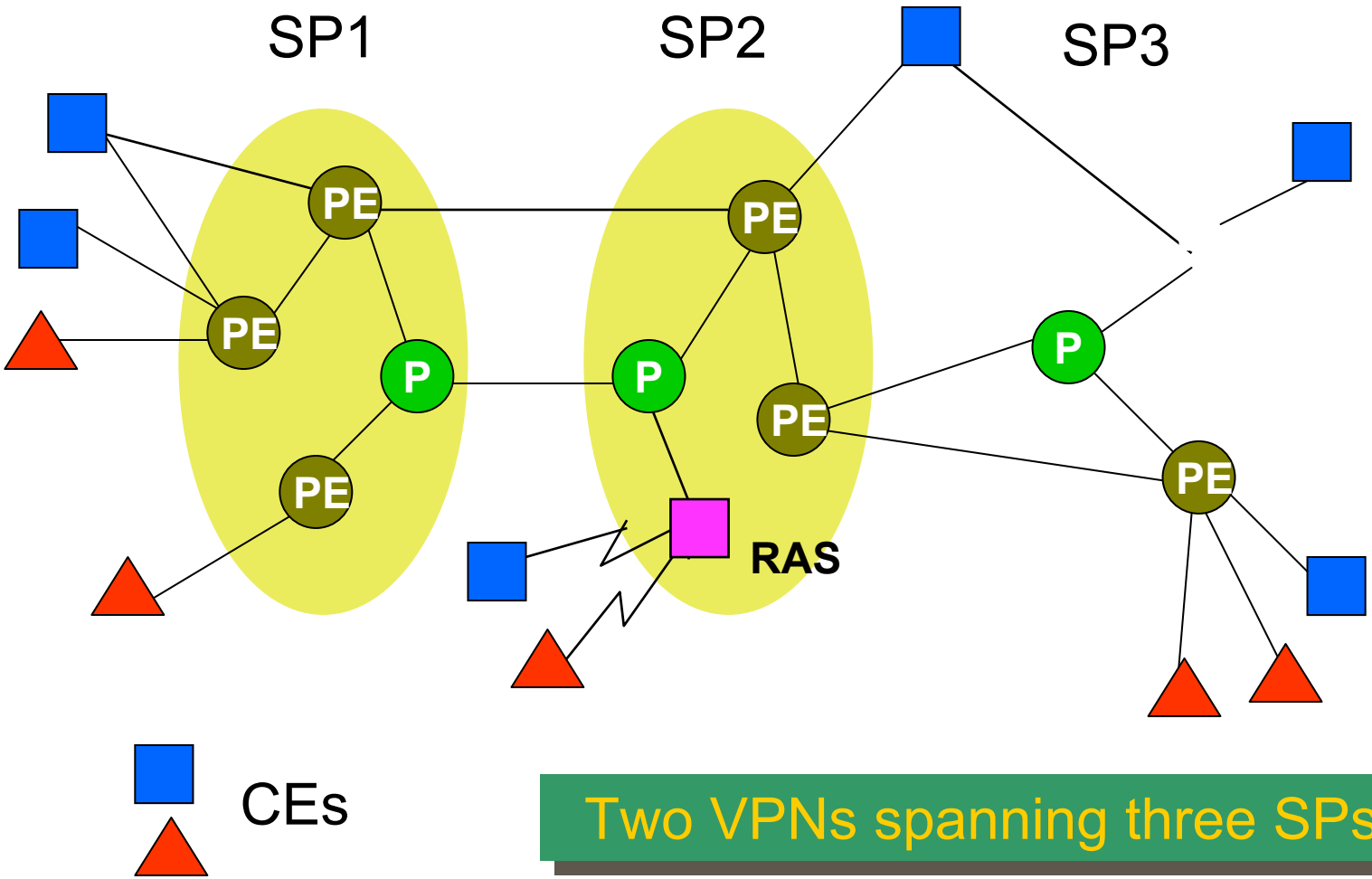
jh@song.fi

Song Networks

What is an IP VPN?

- an emulation of private (wide area) network facility using provider IP facilities
- provides permanent connectivity between multiple customer sites
- implementation can be either customer or provider based
- can span multiple providers

VPN Example



Two VPNs spanning three SPs

VPN Requirements

- support for customer addressing
  - non-unique, overlapping address spaces
- support for data security
  - authenticity, privacy, integrity
- support for QoS assurances
  - bandwidth, latency

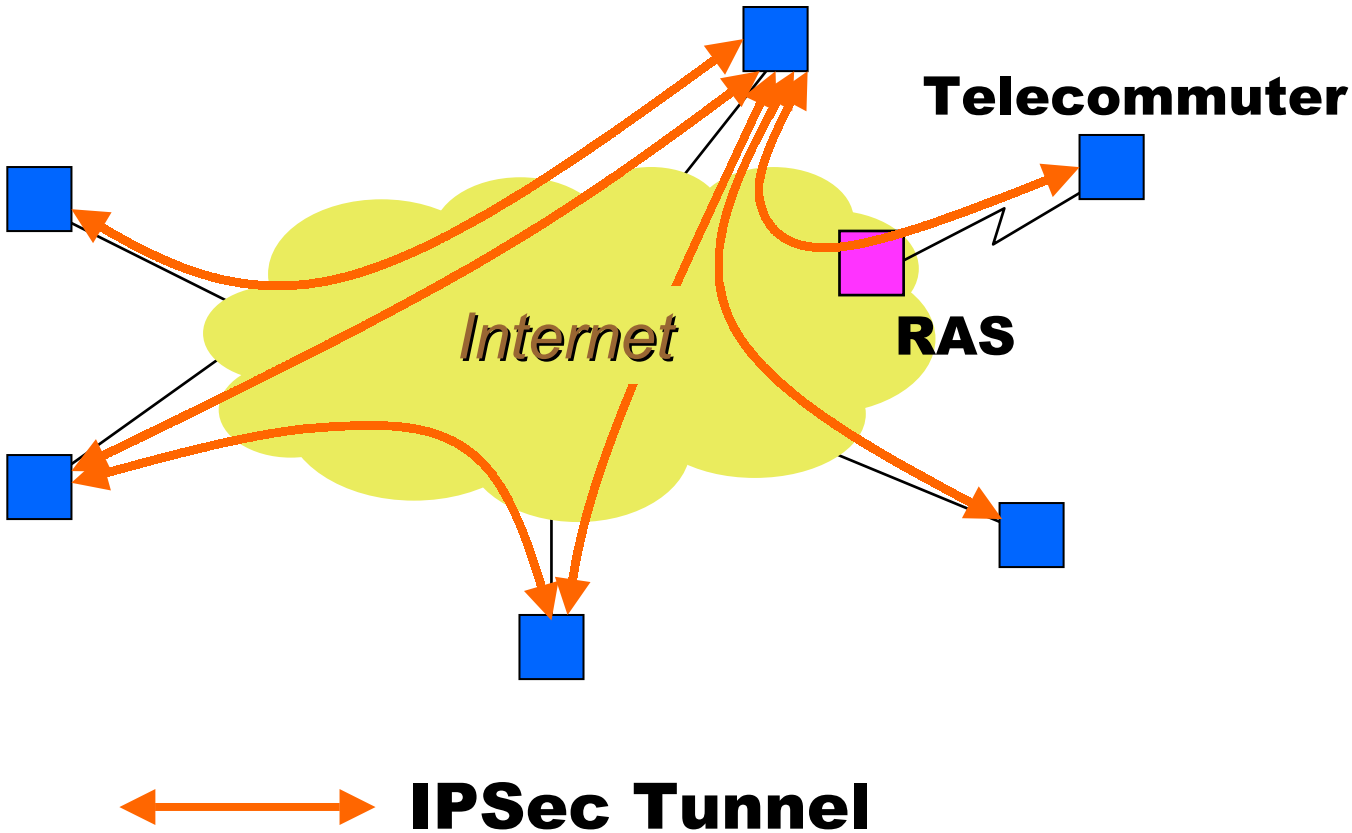
VPN Classification

- Who implements the VPN
  - CE or PE based
- at which layer the VPN operates
  - Layer 2 or Layer 3
- how the VPN is implemented
  - membership discovery, signaling, tunneling protocol, ...

CE Based VPNs

- integrate VPN capabilities in CE devices
  - CEs are connected via IPSec tunnels over the Internet (available everywhere)
  - provide site-to-site security
  - require networking skills and a key management system
- the only choice if security of the VPN service is a concern

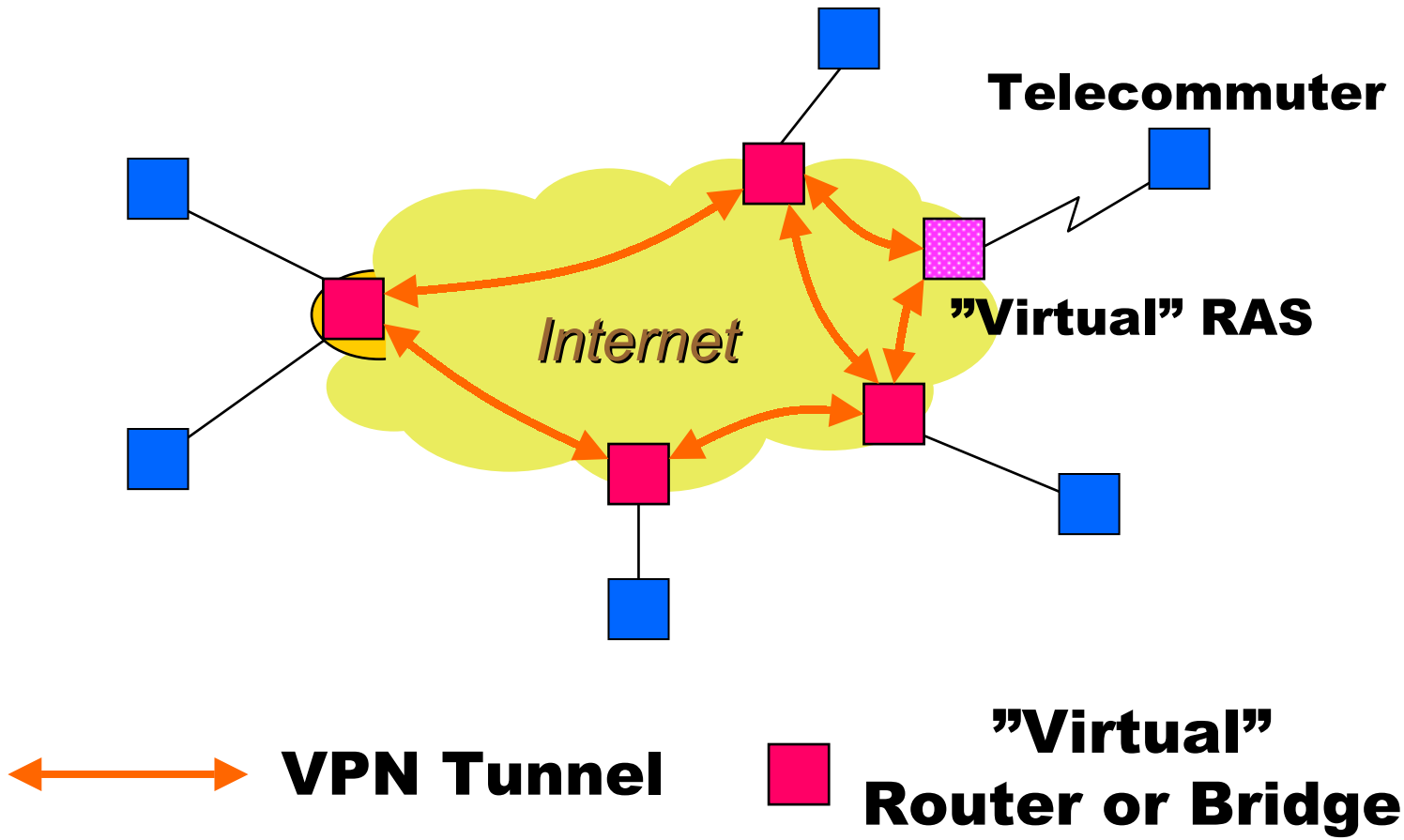
A CE Based VPN



PE Based VPNs

- Outsource the VPN operation to SPs
  - PEs appear as router peers or bridges to CEs
  - works with conventional access routers
  - simplified CE operation
  - brings new revenue sources to SPs
- suitable when the SPs and local loops can be trusted

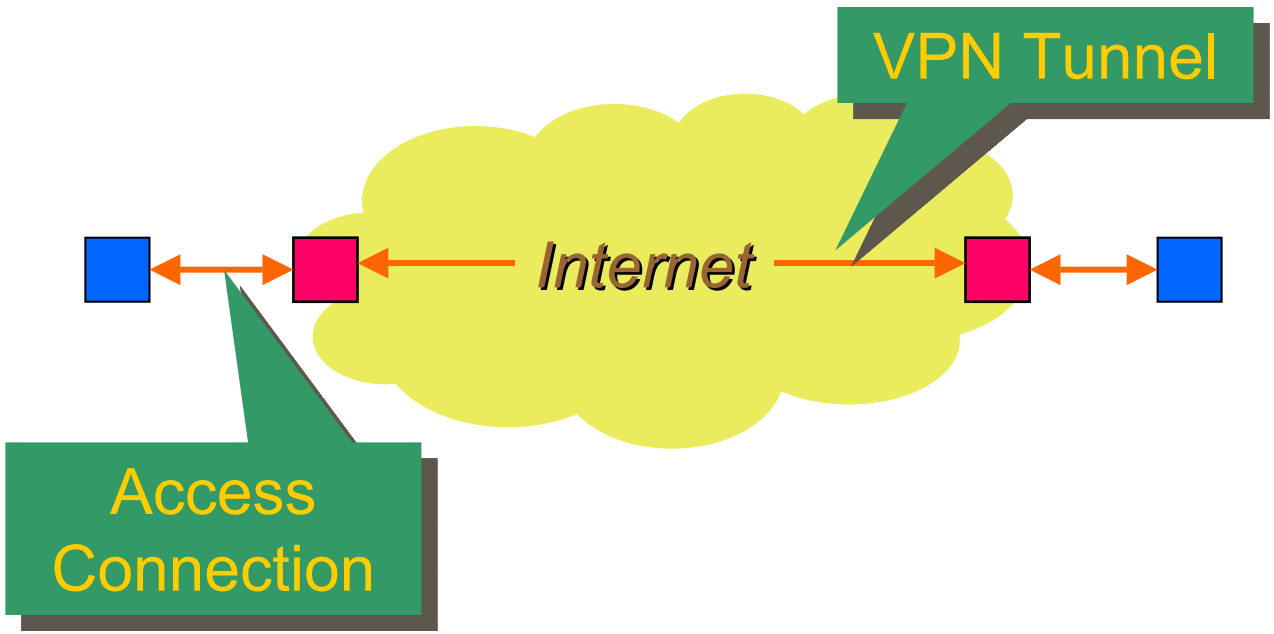
A Network Based VPN



Layer 2 vs. Layer 3 VPNs

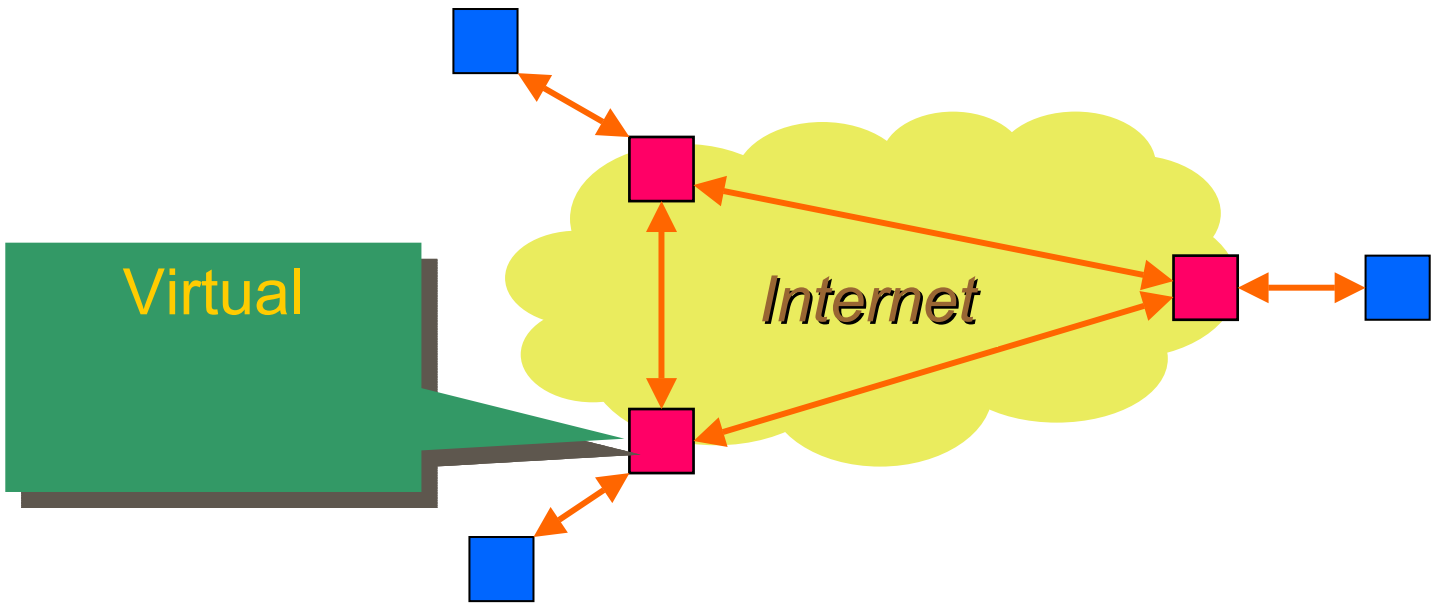
- Layer 2 VPNs
  - provide Virtual Private Wire Service (VPWS) or Virtual Private LAN Service (VPLS)
  - PEs not aware of customer's Layer 3 protocols, addresses, or routing
- Layer 3 VPNs
  - provide Virtual Routing Service
  - PEs participate as routing peers in customers' Layer 3 protocols

Virtual Private Wire Service



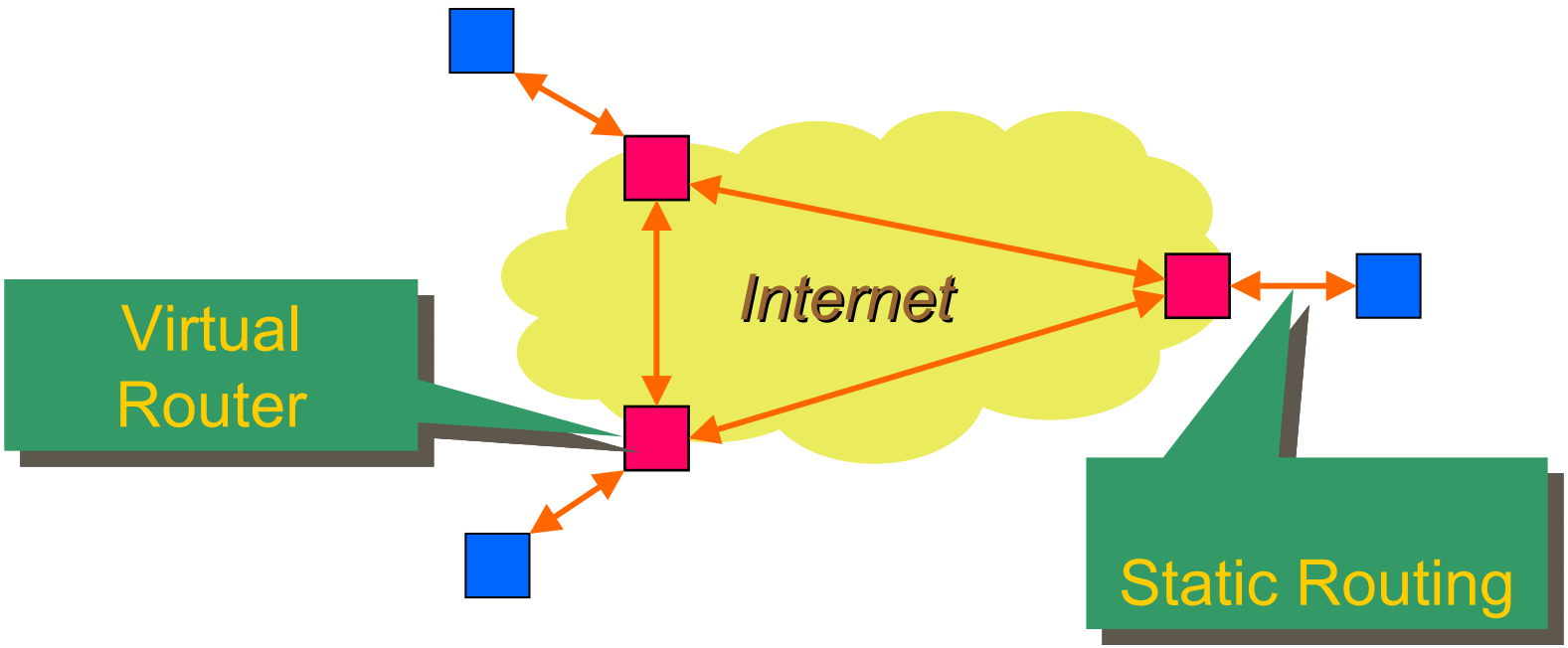
AC can be physical PPP or Ethernet link,
FR or ATM VC, VLAN, MPLS LSP, etc.

Virtual Private LAN Service



AC can be physical Ethernet link or VLAN

Layer 3 VPN



AC can be physical PPP or Ethernet link,
FR or ATM VC, VLAN, MPLS LSP, etc.

Generic VPN Problems

- how to *discover* which other CEs or PEs belong to the same VPN
- how to *setup* VPN tunnels and which tunneling protocols to use
- how to *advertise* end-point reachability within a VPN

VPN Membership Discovery

- a CE or a PE port is configured to belong to a given VPN
- CE or PE learns about other members via
  - configuration (CEs)
  - BGP piggy packing (PEs)
  - DNS (CEs and PEs)
- DNS vs. BGP for discovery is currently a hot issue

VPN Tunneling

- choices for VPN tunneling protocols
  - MPLS (over MPLS or GRE), L2TPv3, IPSec
- choices for tunnel setup protocols
  - LDP, BGP piggy packing, L2TPv3, IPSec
- tunneling protocol can be chosen independently of discovery protocol

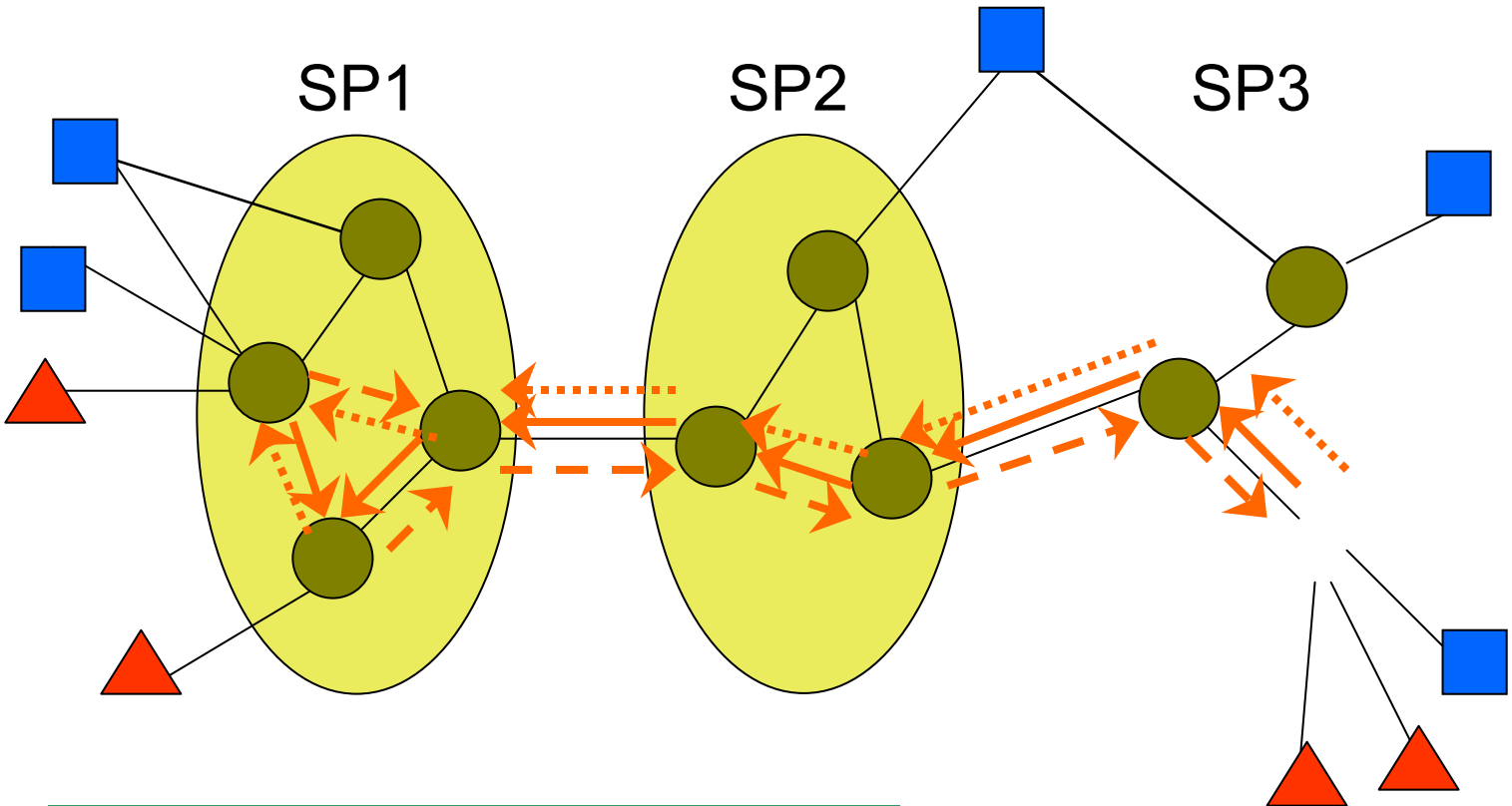
Advertising Reachability

- Layer 2 VPNs
  - VPLS has no need to advertise reachability
  - VPWS can piggy pack Layer 3 reachability into tunnel setup
- Layer 3 VPNs
  - via IGP over VPN tunnels between VRs
  - via BGP extended with VPN addresses

BGP Piggy Packing

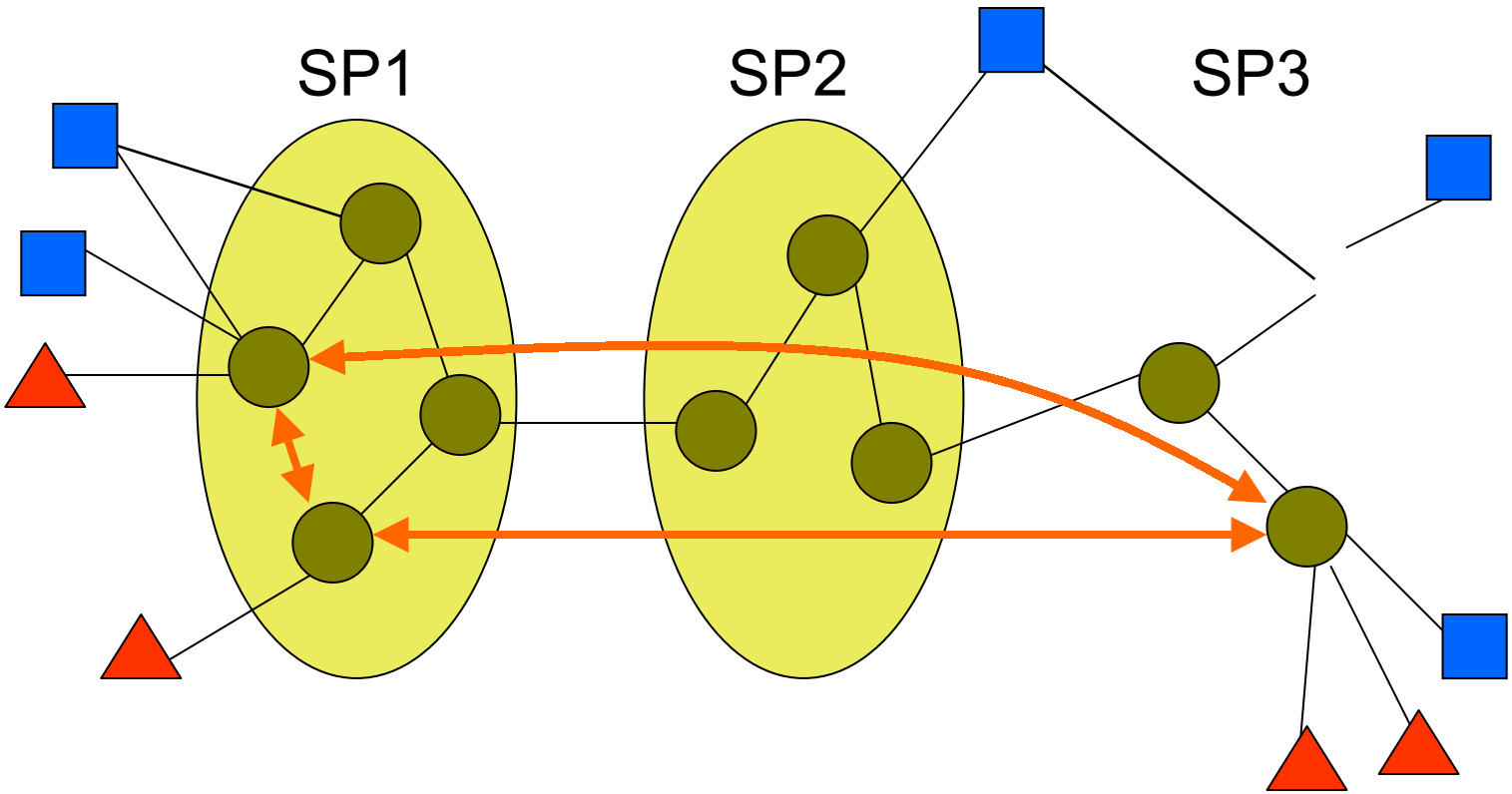
- Assumes that each PE runs (extended) BGP
- difficulties with multiprovider VPNs
  - all transit SPs need to be trusted
  - VPN information visible at boarder routers
  - advertisement scope is difficult to control
- OK for single SP VPNs where customer sites can be backhauled to BGP speaking PEs

BGP/MPLS Model



MPLS LSPs for the ▲ VPN

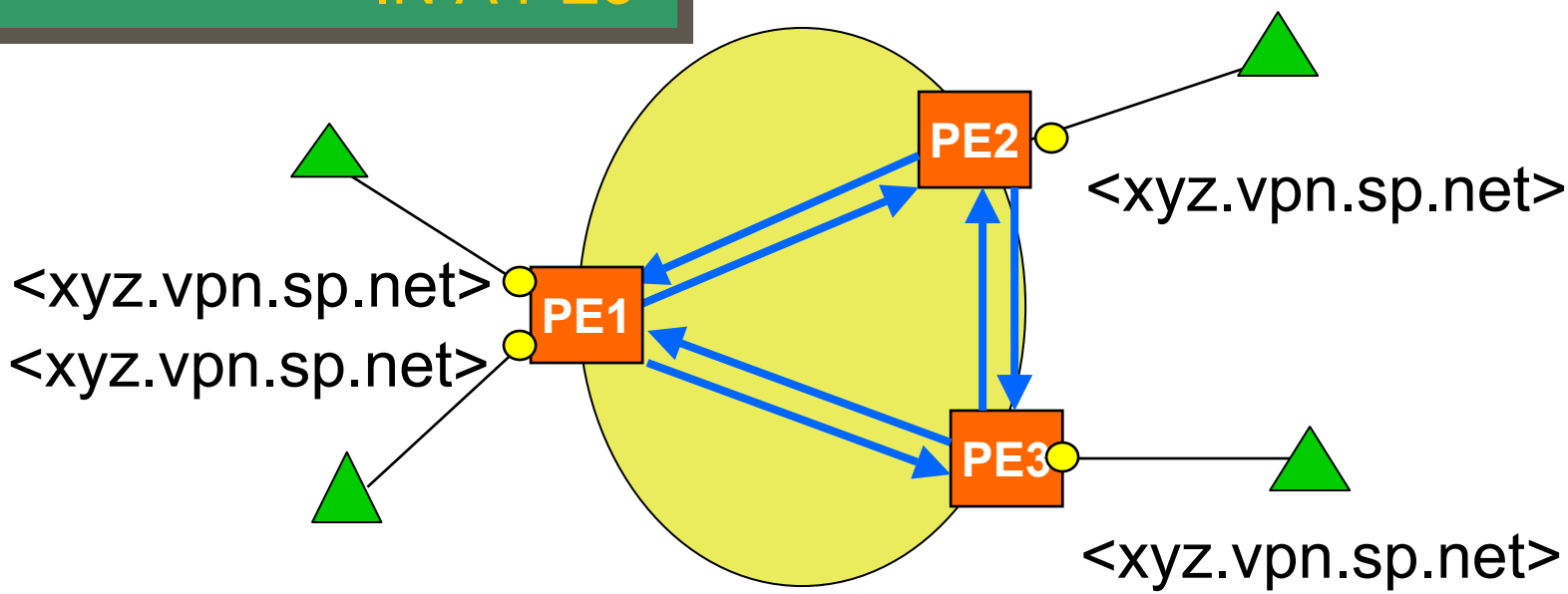
DNS/GRE/MPLS Model



IP tunnels for the ▲ VPN

DNS Based VPLS Example

xyz.vpn.sp.net IN A PE1
IN A PE2
IN A PE3



Summary

- Frame Relay and ATM based VPNs are migrating to IP based VPNs
- a secure VPN can only be implementing using IPSec between CEs
- Layer 2 VPNs (especially VPLS) is becoming an alternative to Layer 3 VPNs
- jury is still out regarding the discovery and tunneling protocols