Agilent Technologies

Virtual Private Networks:

The Hot Revenue Source for Service Providers

December 11, 2001

presented by:

Akram Ashamalla

Agenda

- Why are we talking about VPNs?
- What is a VPN - Layer 2/Layer 3/IP VPN & what is the problem?
- What are the network concerns?
- What are the necessary types of testing (the common part)?
- What are the steps of setting up a VPN?
- What are some test scenarios specific to the different VPN protocols?
- What can Agilent’s Tools do to meet the testing needs?

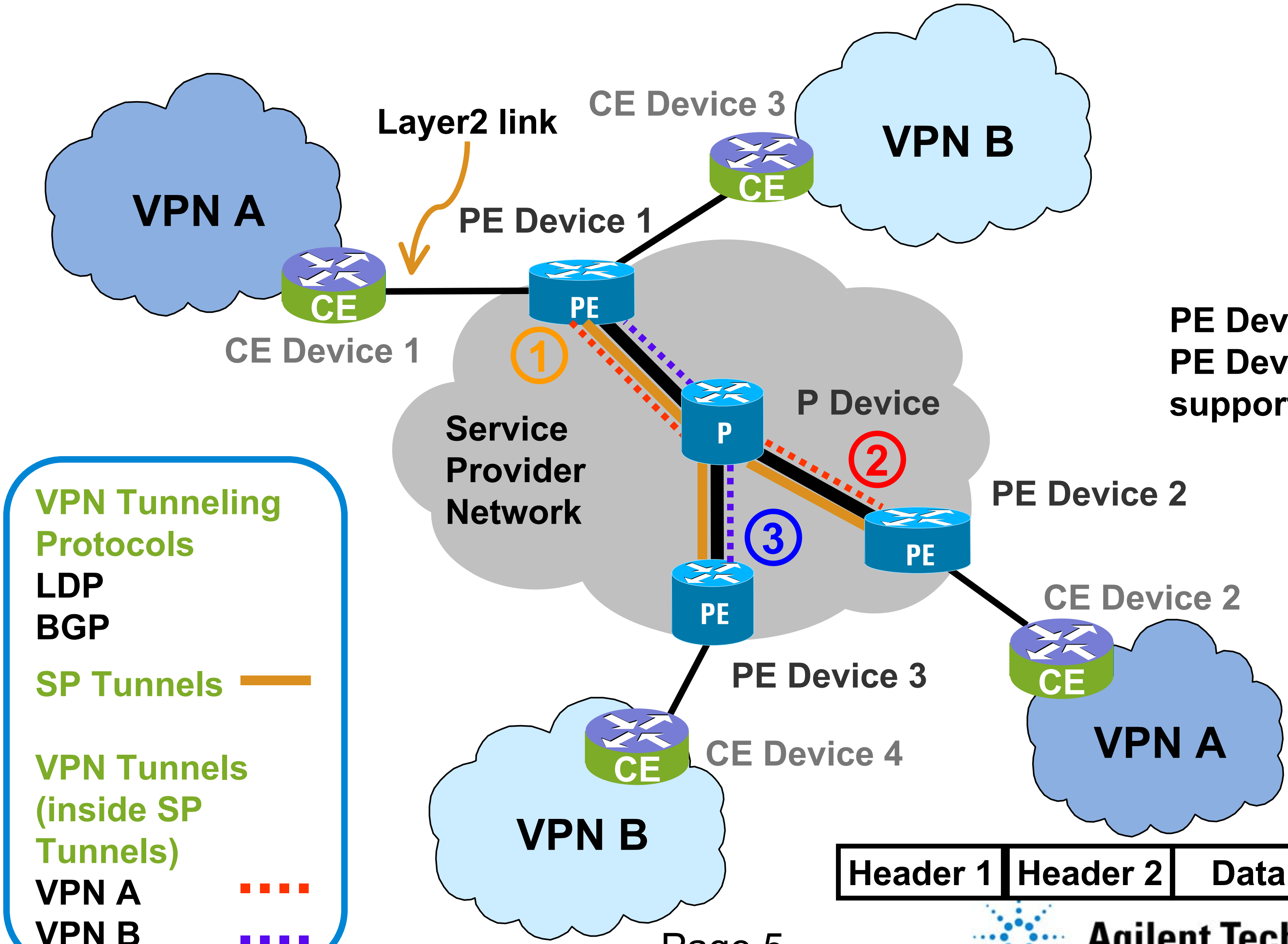
What is a Virtual Private Network?

- VPN (Virtual Private Network) is simply a way of using a public network for private communications, among a set of users and/or sites
- Remote Access: Most common form of VPN is dial-up remote access to corporate database - for example, road warriors connecting from laptops
- Site-to-Site: Connecting two local networks (may be with authentication and encryption) - for example, a Service Provider connecting two sites of the same company over its shared network

What are Layer 2, Layer 3 & IP VPNs?

- VPNs based on a layer 2 (Data Link Layer) technology and managed at that layer are defined as layer 2 VPNs (MPLS, ATM, Frame Relay) - ref. OSI Layer model
- VPNs based on tunneling above layer 3 (Transport Layer) are Layer 3 VPNs, (L2TP, IPSec, BGP/MPLS)
- IP-VPNs are a type of Layer 3 VPNs, which are managed purely as an IP network (L2TP, IPSec)

Visually - Layer 2 VPN



PE Device 1 &
PE Device 2
support VPN

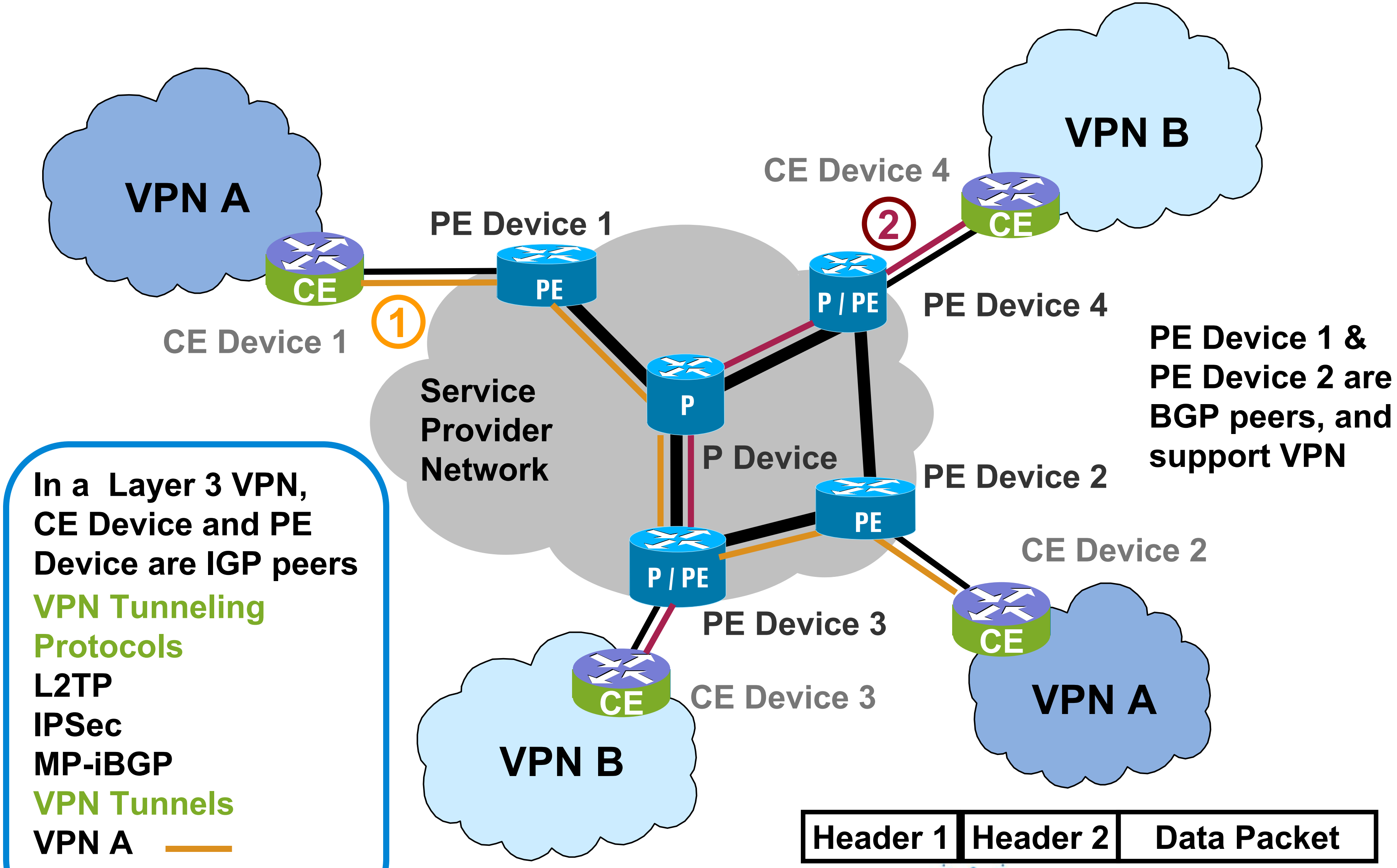
VPN Tunneling Protocols
LDP
BGP

SP Tunnels ━━

VPN Tunnels (inside SP Tunnels)
VPN A ▪▪▪▪
VPN B ▪▪▪▪

Header 1	Header 2	Data Packet

Visually - Layer 3 VPN



PE Device 1 & PE Device 2 are BGP peers, and support VPN

In a Layer 3 VPN, CE Device and PE Device are IGP peers

VPN Tunneling Protocols

L2TP
IPSec
MP-iBGP

VPN Tunnels

VPN A ━
VPN B ━

Header 1	Header 2	Data Packet

Delivering VPN Services requires:

- Setting up the VPN tunnels/sessions
  - tunnel set up protocol exchange
  - authentication procedure (if applicable)
  - security procedure (if applicable)
- Sending traffic through the tunnels
  - sending with the right tunnel encapsulation
  - sending to the right recipient
  - ensuring promised service quality

And these capabilities must SCALE!

Scaling needs for VPN Services

Site-to-Site

- PPVPN Requirements Document (draft-ietf-ppvpn-requirements, August 2001) states that a major Service Provider will be required to support on the order of 10,000 VPNs within four years, with interfaces per site ranging from just a few to over 50,000 per VPN

Remote Access

- A service provider offering Remote Access VPN services could easily provision for thousands of tunnels and sessions
- NEMs are reacting to this need by offering equipment that can sustain 250, 000 tunnels and more. The latest L2TP draft has increased tunnel ID values from 16 to 32 bits

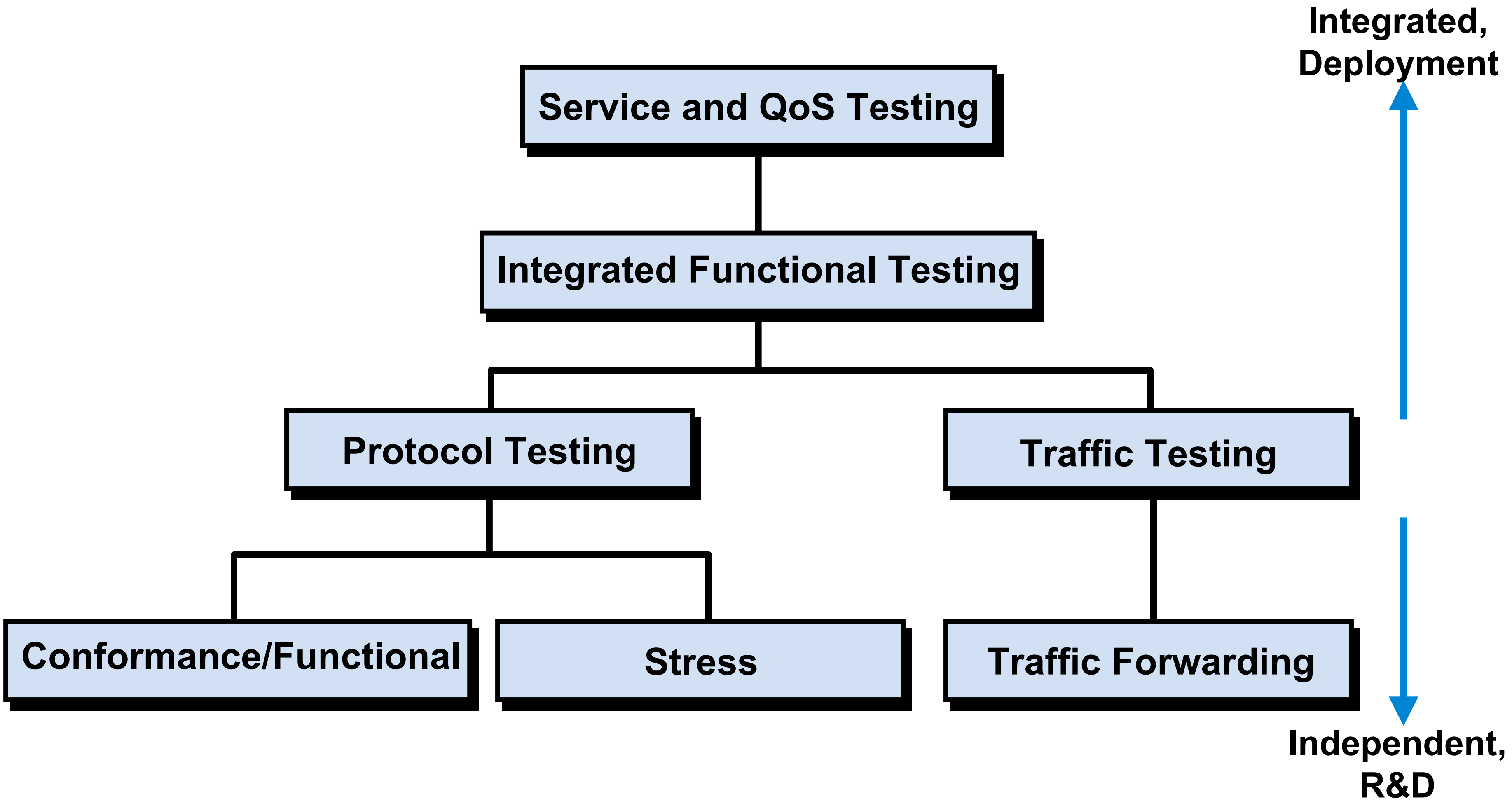
VPN service delivery and scalability requirements bring a number of test challenges to light….

What are the network concerns?

- Correct VPN protocol exchange - protocol functionality issues
- Handle incorrect protocol behaviour - protocol robustness issues
- Traffic flow over the VPN - integrated functionality and QoS issues
- Make VPN work with equipment from multiple vendors - interoperability issues
- Manage large number of tunnels - performance and scalability issues
- Manage network changes/failures - restoration issues

What is Testing in this Context?

Types of Testing

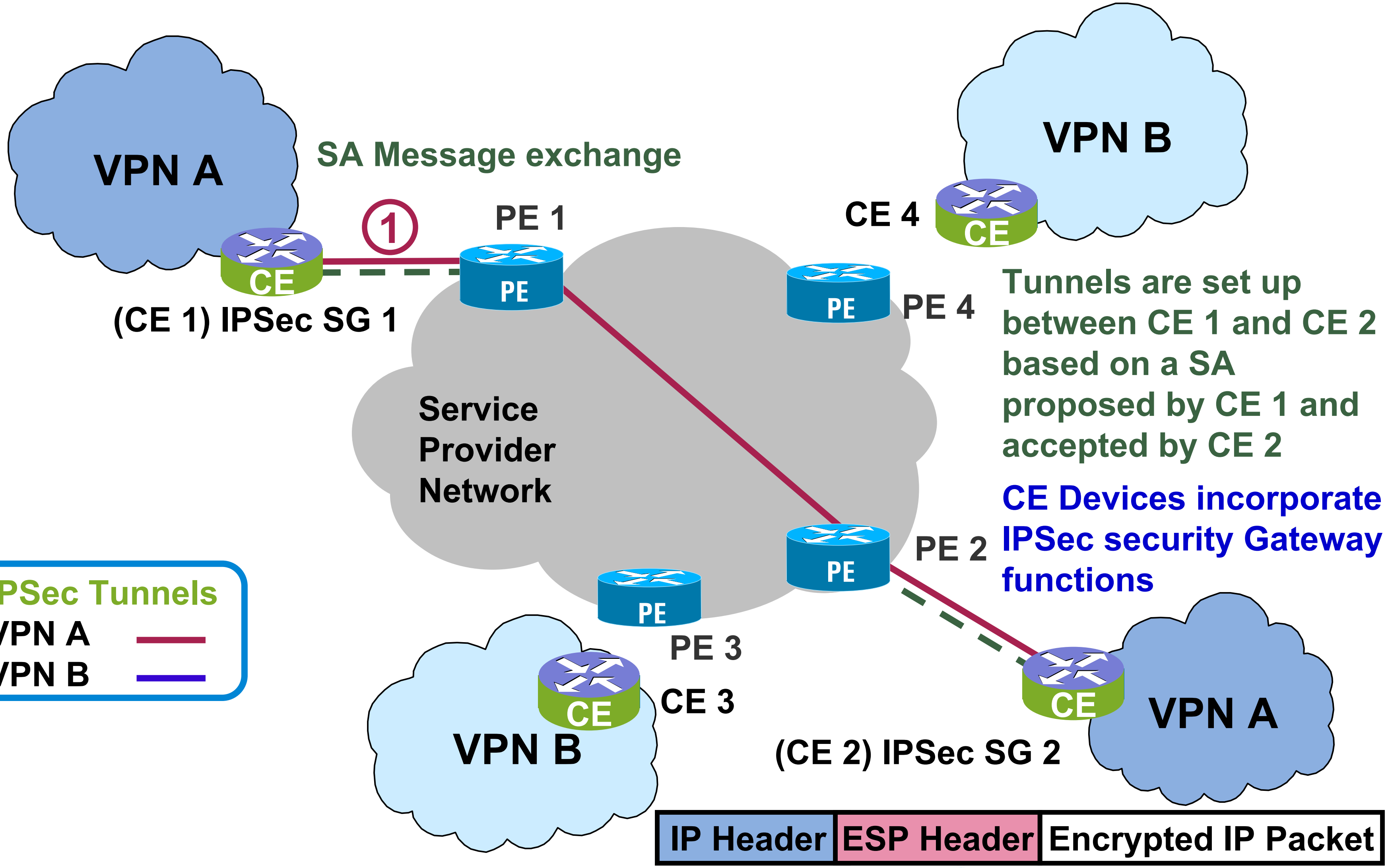


VPN Test Scenarios

We will cover the following:

- Layer 3 Test Scenarios
  - IP VPNs
  - IPSec
  - L2TP
  - BGP/MPLS
- Layer 2 Test Scenarios
  - L2 over MPLS

IPSec - IP Security Network Scenario (1)



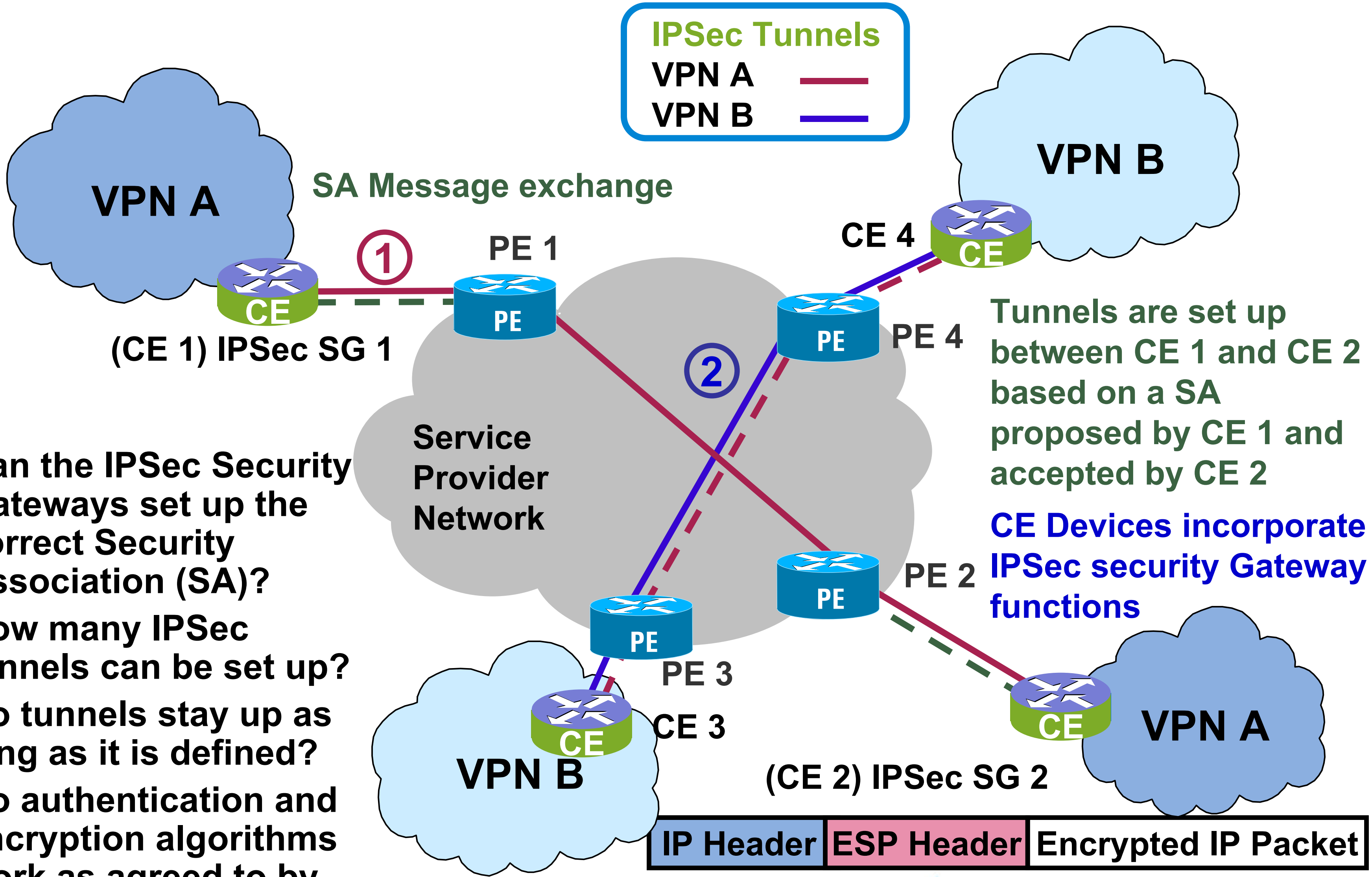
Tunnels are set up between CE 1 and CE 2 based on a SA proposed by CE 1 and accepted by CE 2

CE Devices incorporate IPSec security Gateway functions

IPSec Tunnels

VPN A	🟥
VPN B	🟦

IPSec - IP Security Network Scenario (2)



IP Header	ESP Header	Encrypted IP Packet

Tunnels are set up between CE 1 and CE 2 based on a SA proposed by CE 1 and accepted by CE 2

CE Devices incorporate IPSec security Gateway functions

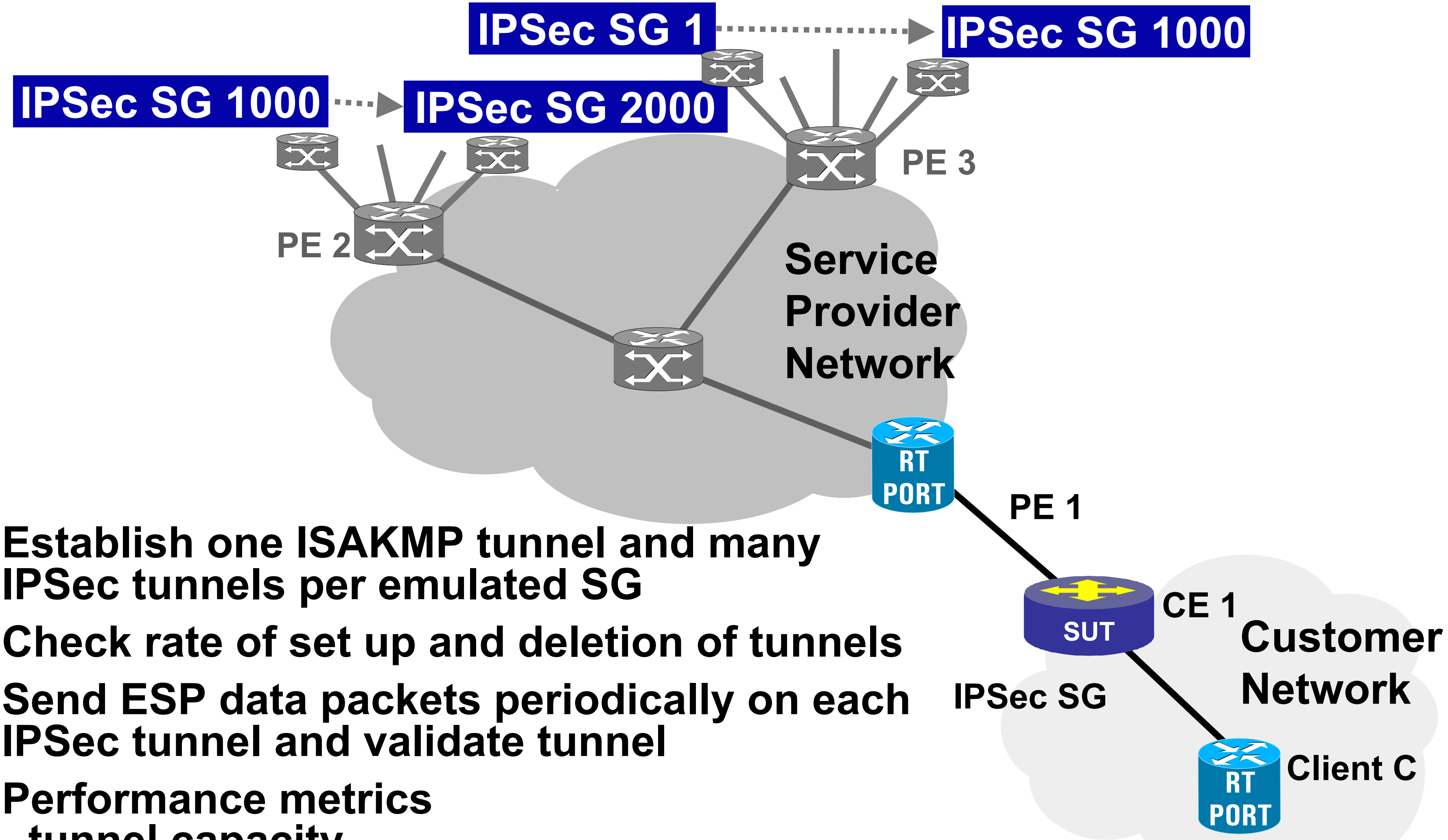
- Can the IPSec Security Gateways set up the correct Security Association (SA)?
- How many IPSec tunnels can be set up?
- Do tunnels stay up as long as it is defined?
- Do authentication and encryption algorithms work as agreed to by the SG's on both ends?

How to set up an IPSec VPN

- Setting up a VPN
  - Initiating Security Gateway (SG1) proposes a ISAKMP Security Association (SA) which is accepted by destination SG (SG2)
  - SG1 exchanges “keying information” with SG2 through “Diffie-Hellman exchange”
  - Both SG1 and SG2 are authenticated using encrypted exchanges and completes ISAKMP Tunnel set up
  - SG1 proposes IPSec Security Association (SA) and accepted by SG2 and an IPSec tunnel is established
- Reachability information may be statically configured or available through a database lookup
- Security is provided through a) authentication of the parties involved through secure exchanges, and b) encryption of every IP datagram

(ISAKMP=Internet Security Association and Key Management Protocol)

Scalability & Performance Test Scenario

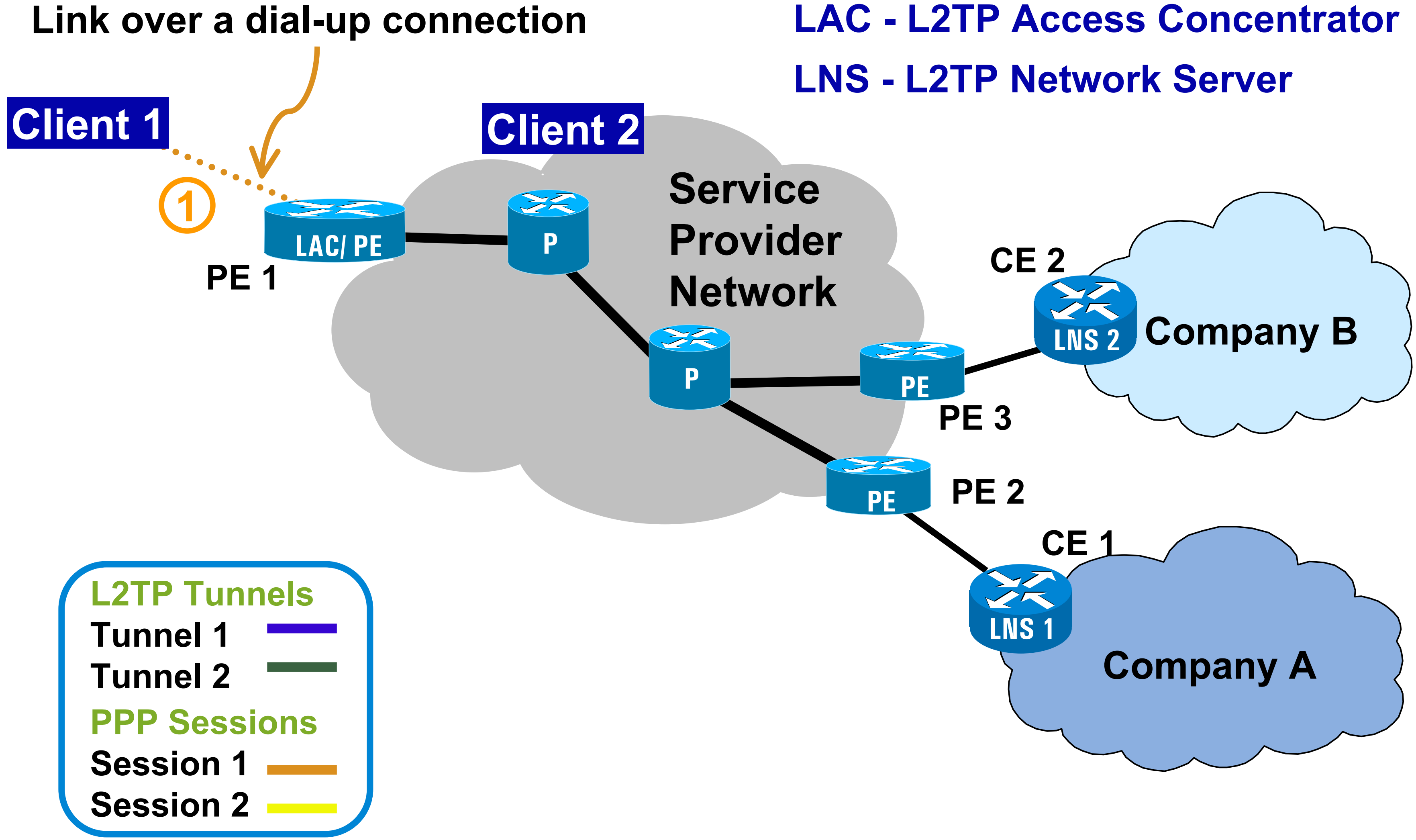


- Establish one ISAKMP tunnel and many IPSec tunnels per emulated SG
- Check rate of set up and deletion of tunnels
- Send ESP data packets periodically on each IPSec tunnel and validate tunnel
- Performance metrics
  - tunnel capacity
  - steady state tunnel creation rate
  - tunnel deletion rate

Layer 2 Tunneling Protocol Scenario (1)

LAC - L2TP Access Concentrator

LNS - L2TP Network Server



L2TP Tunnels

- Tunnel 1
- Tunnel 2

PPP Sessions

- Session 1
- Session 2

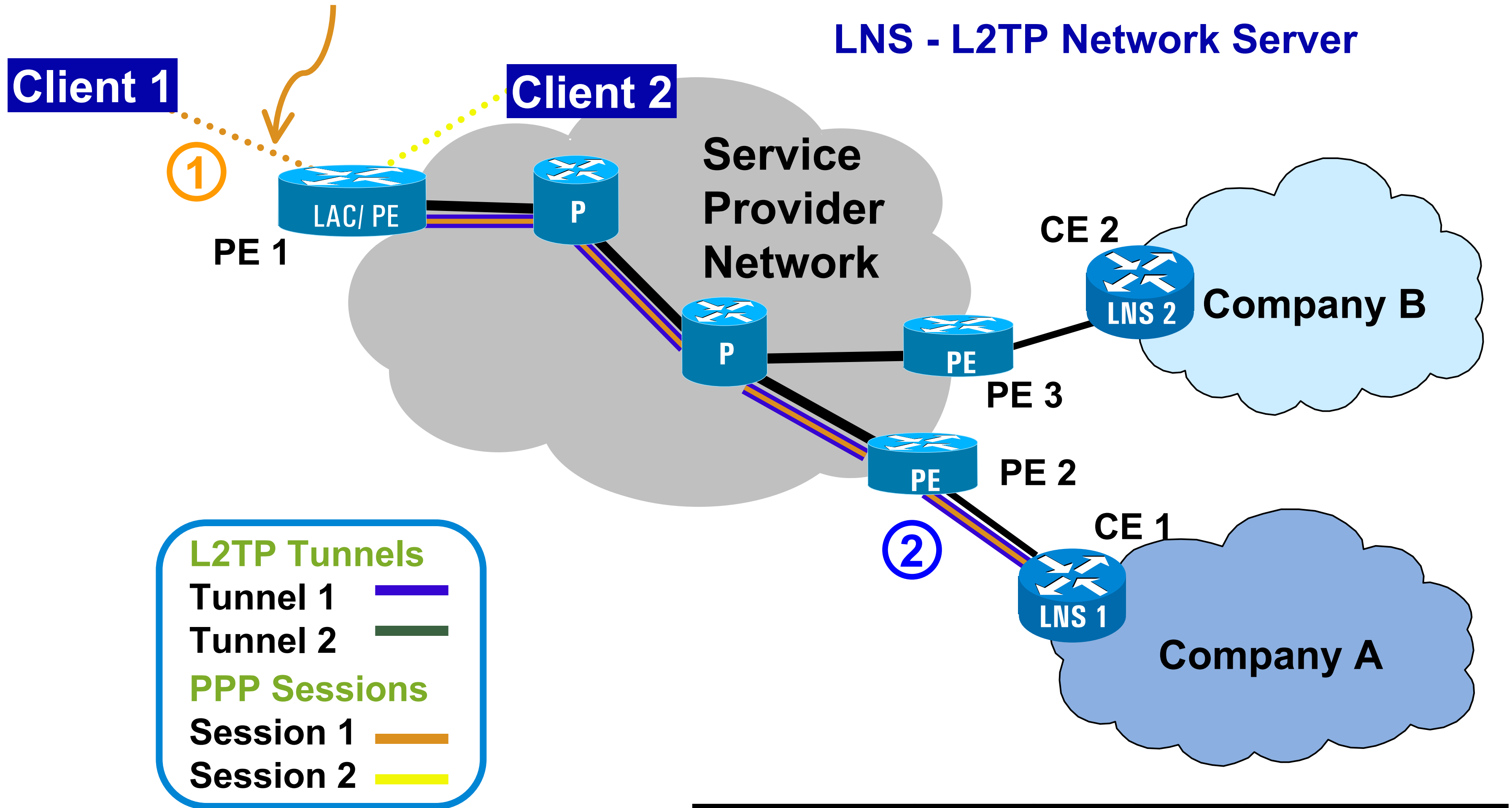
Agilent Technologies

Layer 2 Tunneling Protocol Scenario (2)

Link over a dial-up connection

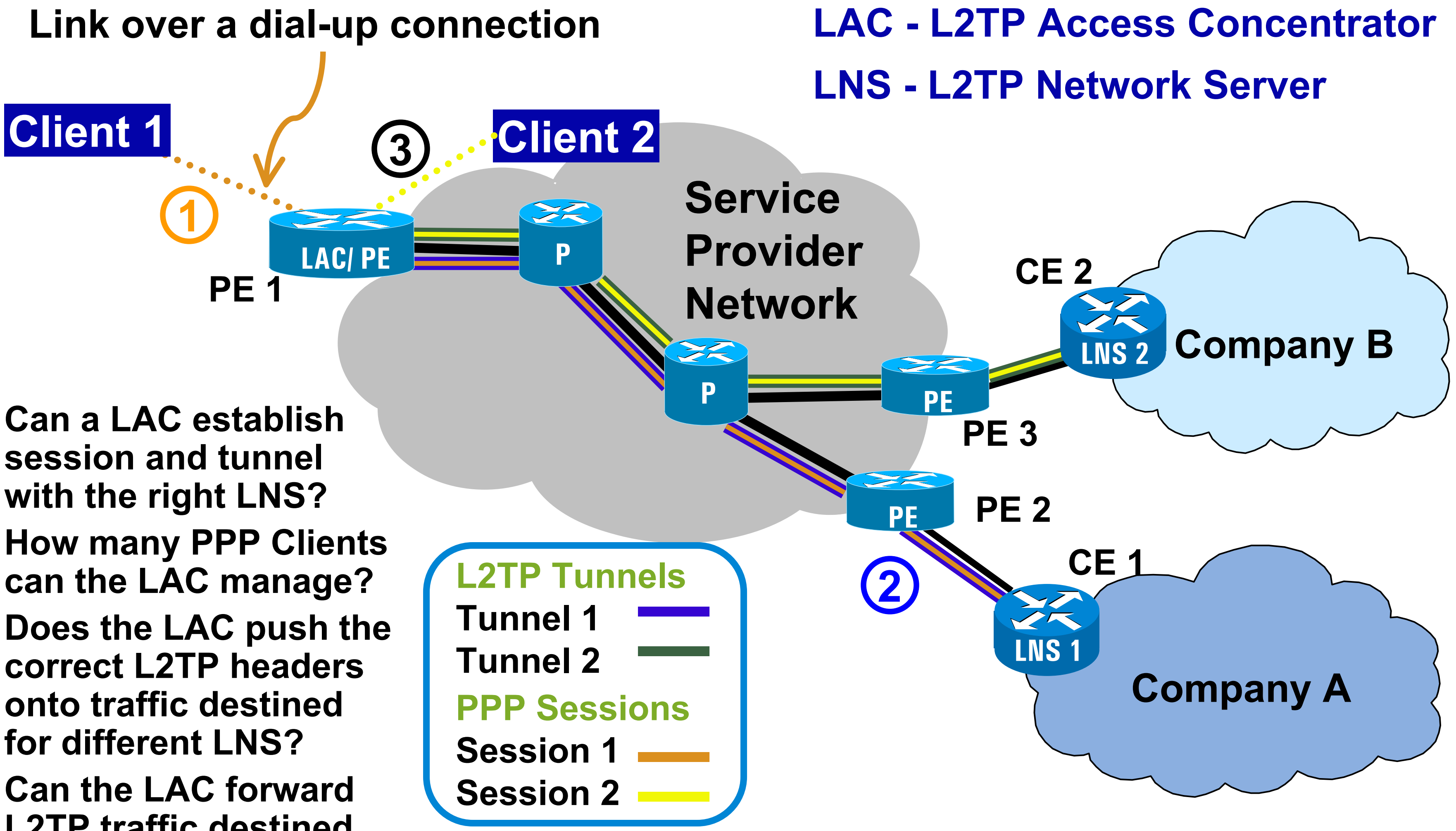
LAC - L2TP Access Concentrator

LNS - L2TP Network Server



IP Header	UDP	L2TP	PPP	IP Packet

Layer 2 Tunneling Protocol Scenario (3)



- Can a LAC establish session and tunnel with the right LNS?
- How many PPP Clients can the LAC manage?
- Does the LAC push the correct L2TP headers onto traffic destined for different LNS?
- Can the LAC forward L2TP traffic destined for customer sites (LNS) at required rates?

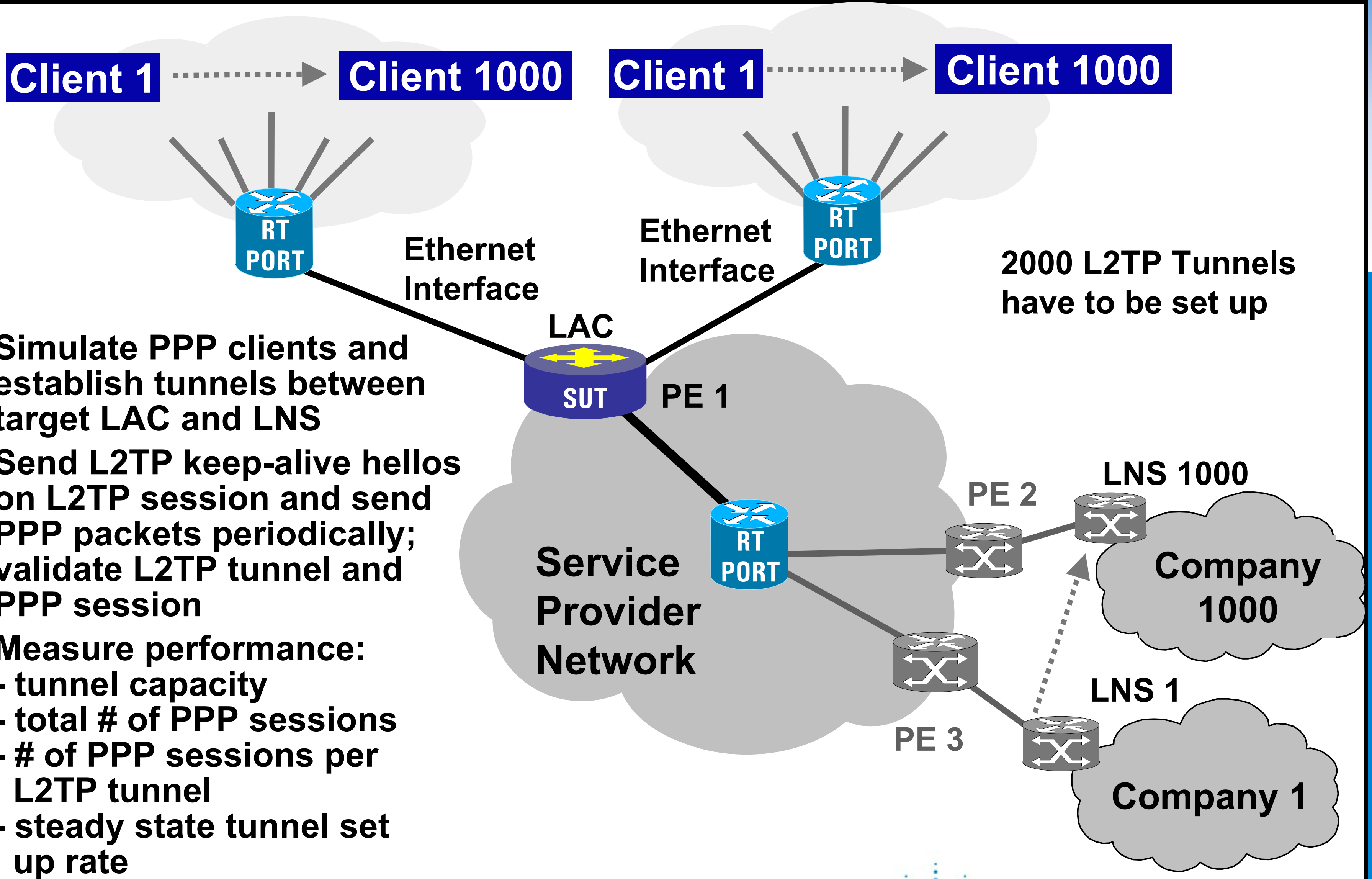
IP Header	UDP	L2TP	PPP	IP Packet

How to set up an L2TP VPN

- Setting up VPN
  - Remote user initiates a PPP session over a layer two connection with a L2TP Access Concentrator (LAC)
  - LAC can optionally authenticate remote user or directly establish a L2TP Tunnel with appropriate L2TP Network Server (LNS)
  - LAC sets up an L2TP session with the LNS
  - LAC forwards PPP traffic to LNS
  - LNS establishes PPP session with Remote Client
- Reachability information may be statically configured or available through a database lookup
- Security in the form of authentication (PAP/CHAP) is available in PPP

  (PAP=Password Authentication Protocol, CHAP=Challenge Handshake Authentication Protocol)

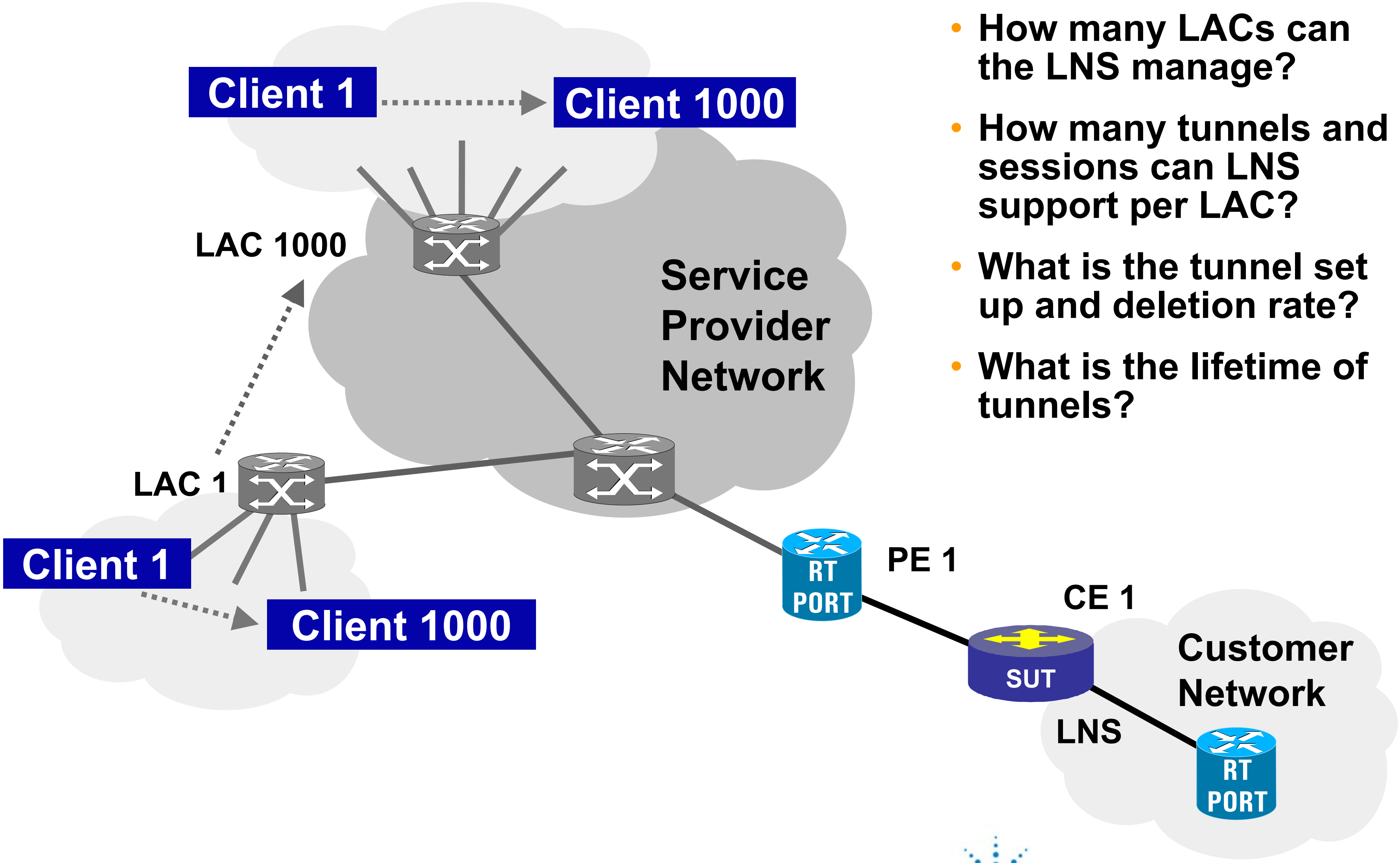
Scalability Test Scenario for LAC



2000 L2TP Tunnels have to be set up

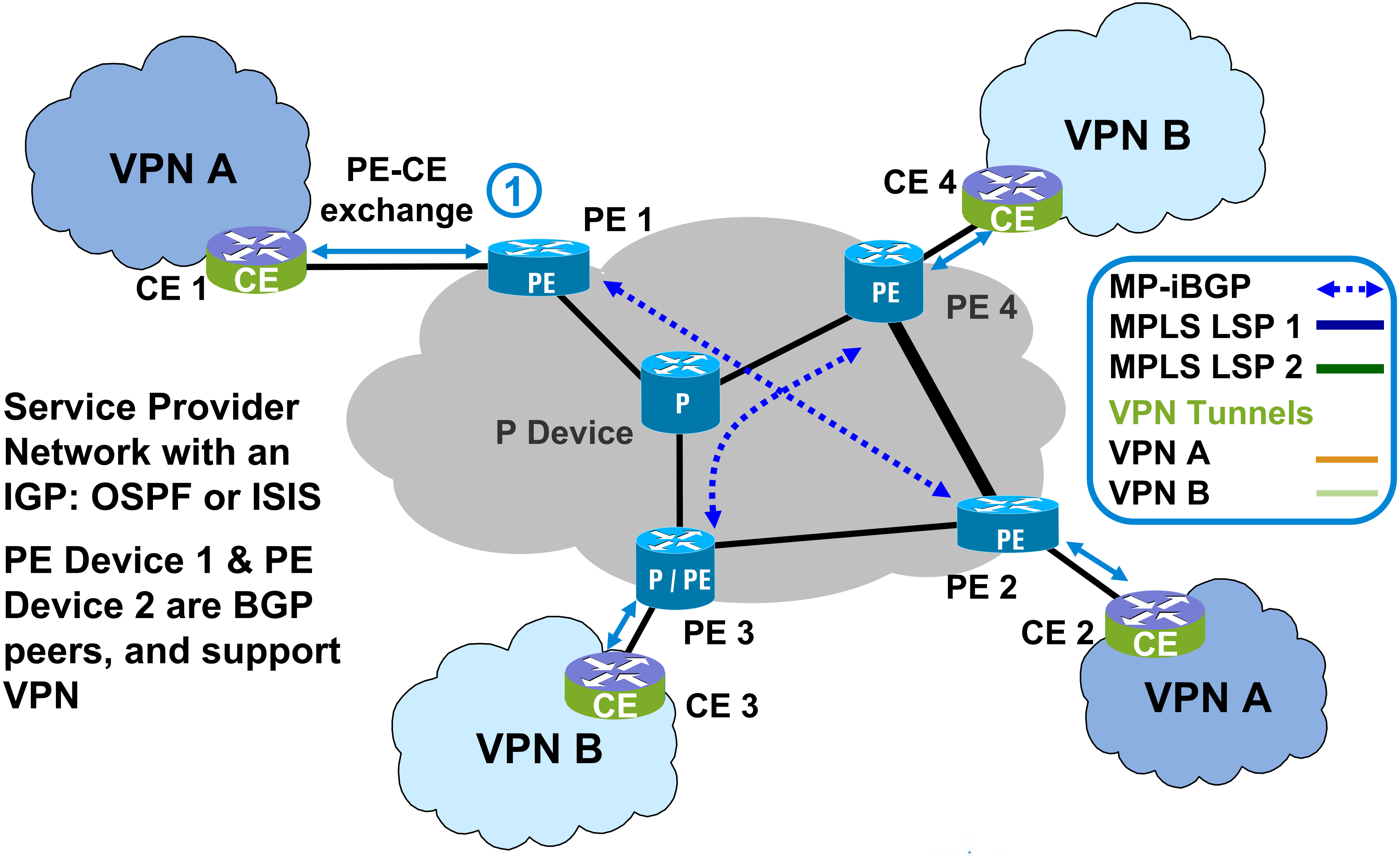
- Simulate PPP clients and establish tunnels between target LAC and LNS
- Send L2TP keep-alive hellos on L2TP session and send PPP packets periodically; validate L2TP tunnel and PPP session
- Measure performance:
  - tunnel capacity
  - total # of PPP sessions
  - # of PPP sessions per L2TP tunnel
  - steady state tunnel set up rate
  - tunnel deletion rate

Scalability Test Scenario for LNS



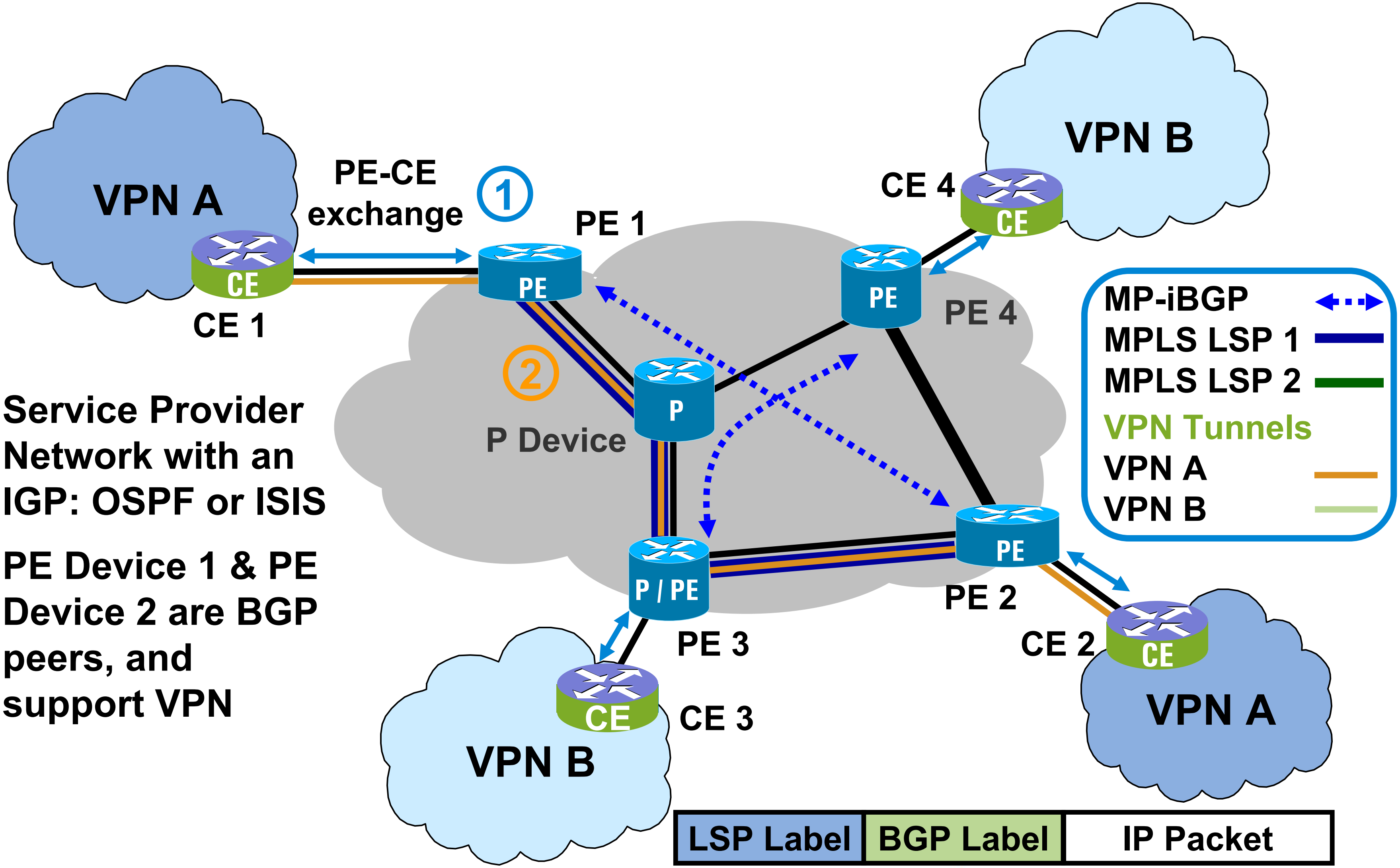
- How many LACs can the LNS manage?
- How many tunnels and sessions can LNS support per LAC?
- What is the tunnel set up and deletion rate?
- What is the lifetime of tunnels?

BGP/MPLS VPN Network Scenario (1)



- Service Provider Network with an IGP: OSPF or ISIS
- PE Device 1 & PE Device 2 are BGP peers, and support VPN

BGP/MPLS VPN Network Scenario (2)

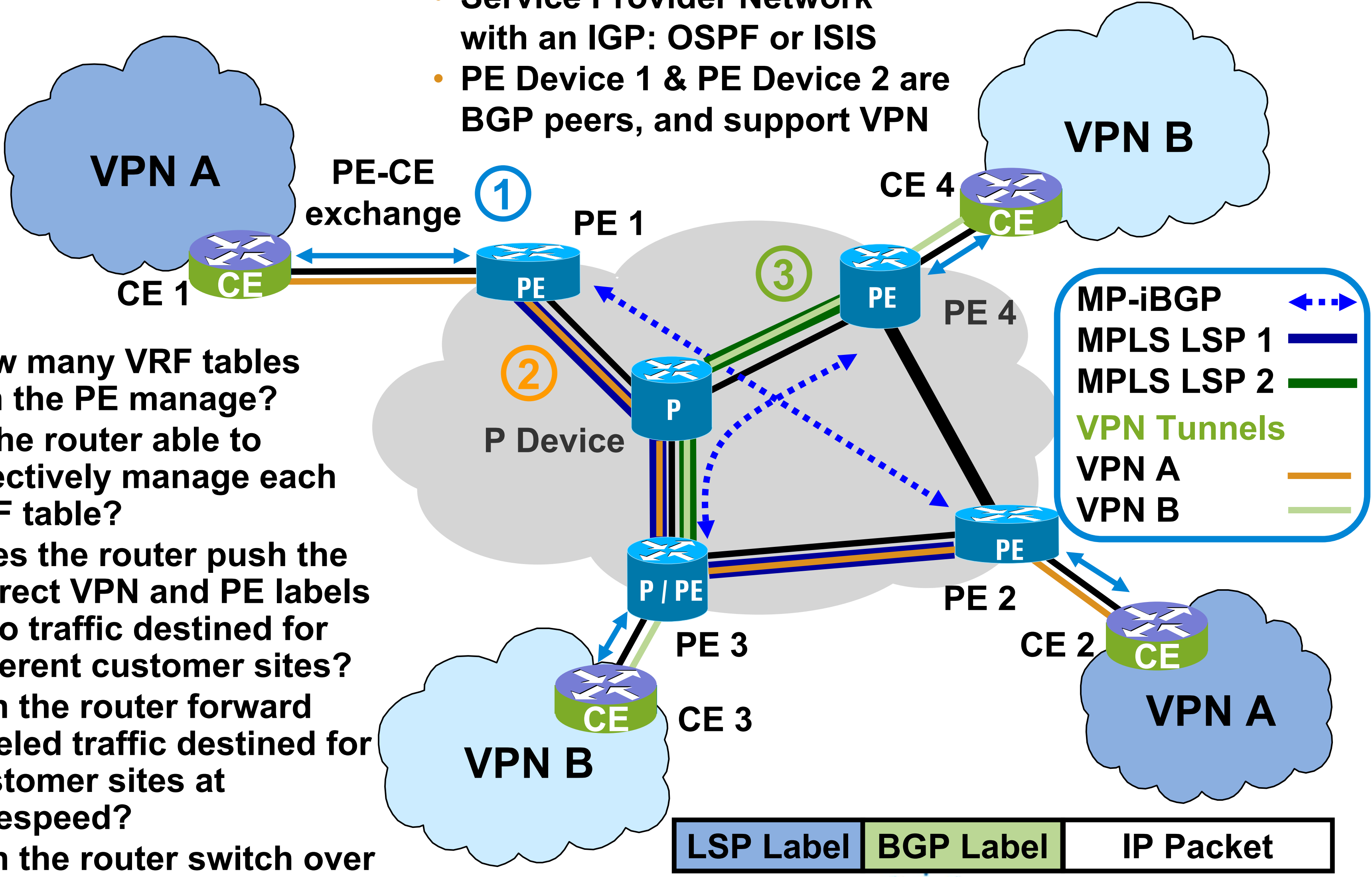


- Service Provider Network with an IGP: OSPF or ISIS
- PE Device 1 & PE Device 2 are BGP peers, and support VPN

LSP Label	BGP Label	IP Packet

BGP/MPLS VPN Network Scenario (3)

- Service Provider Network with an IGP: OSPF or ISIS
- PE Device 1 & PE Device 2 are BGP peers, and support VPN

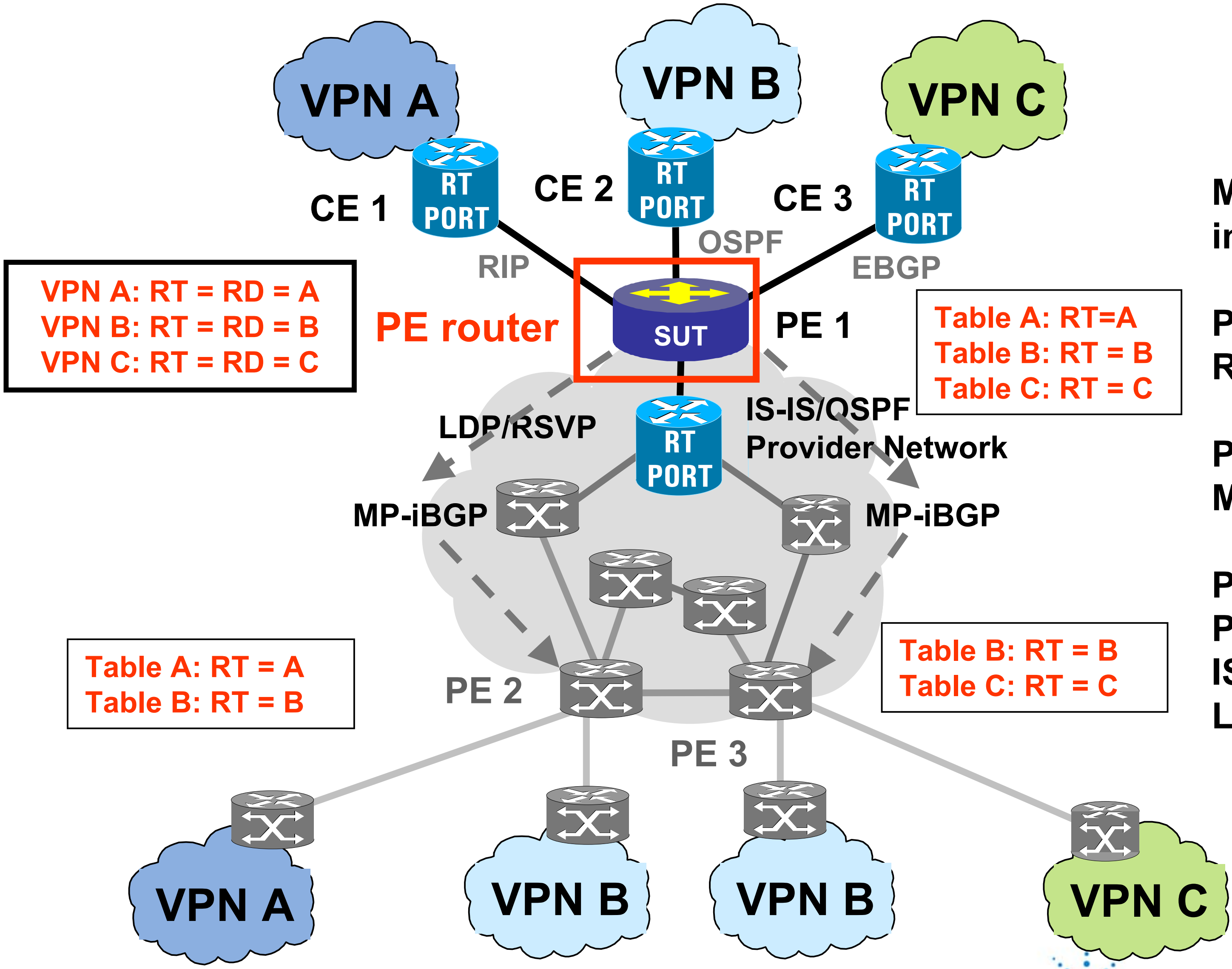


- How many VRF tables can the PE manage?
- Is the router able to effectively manage each VRF table?
- Does the router push the correct VPN and PE labels onto traffic destined for different customer sites?
- Can the router forward labeled traffic destined for customer sites at wirespeed?
- Can the router switch over VPN traffic to back up tunnels effectively?

How to set up a BGP/MPLS VPN

- Runs over an MPLS Label Switched Path
- Setting up VPN
  - iBGP protocol with multiprotocol extensions exchanges VPN information between PE routers
  - A BGP label is used to identify the VPN
  - New scheme to handle overlapping address space: “VPN-IPv4 Address” = [“Route Distinguisher” + IPV4 Address]
  - Every PE maintains VPN Routing & Forwarding (VRF) tables, one VRF table per “site” (CE router) attached to the PE
- Reachability information for a given VPN is propagated only to members of that VPN using BGP multi-protocol extensions
- No special security except inherent security due to the BGP label & unique VRF table, and the LSP between the PE routers

Functionality Test Scenario



VPN A: RT = RD = A
VPN B: RT = RD = B
VPN C: RT = RD = C

Table A: RT=A
Table B: RT = B
Table C: RT = C

Table A: RT = A
Table B: RT = B

Table B: RT = B
Table C: RT = C

Multiple Protocols involved:

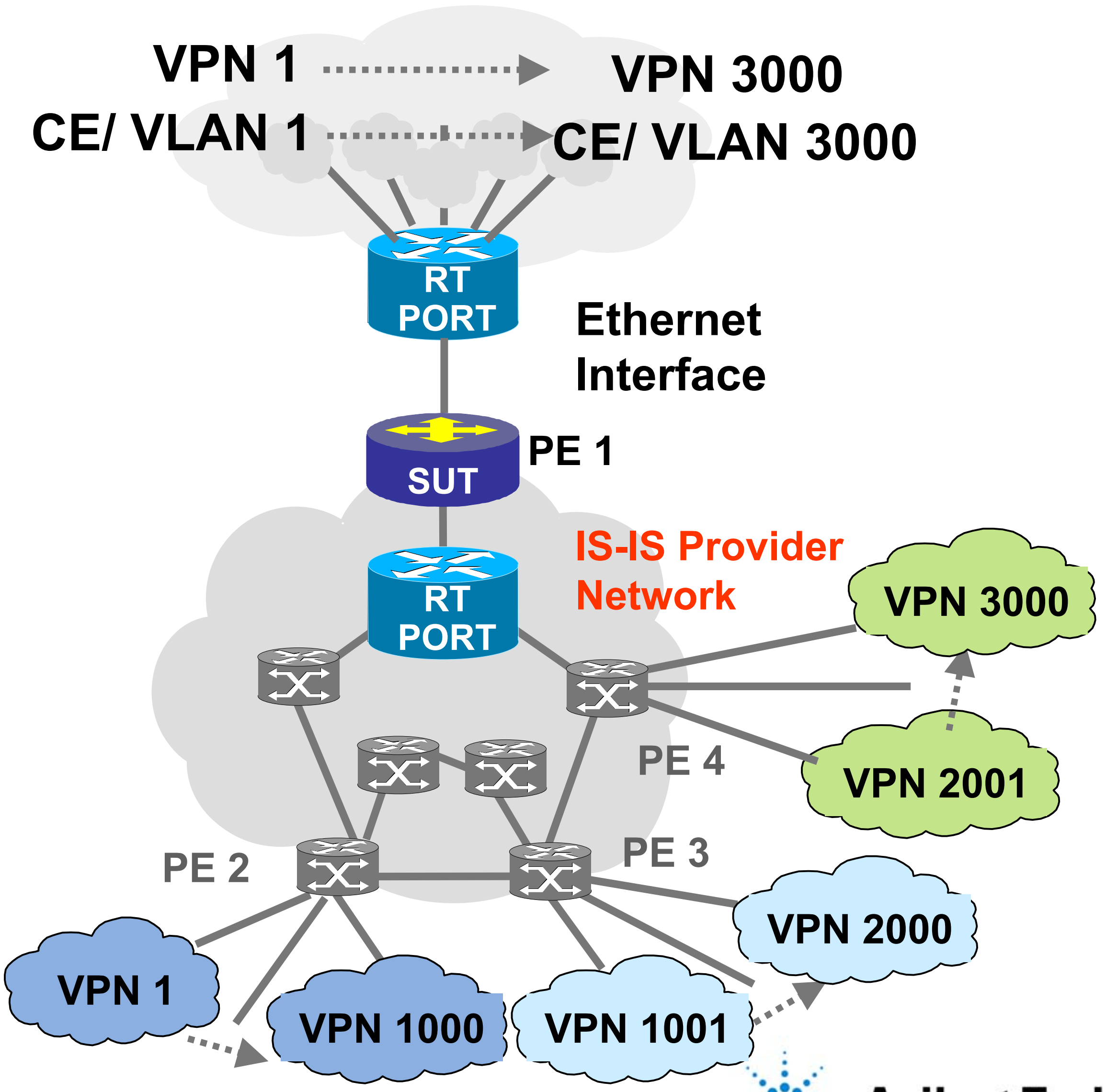
PE-CE Protocols:
RIP, OSPF, EBGP

PE-PE Protocols:
MP-iBGP

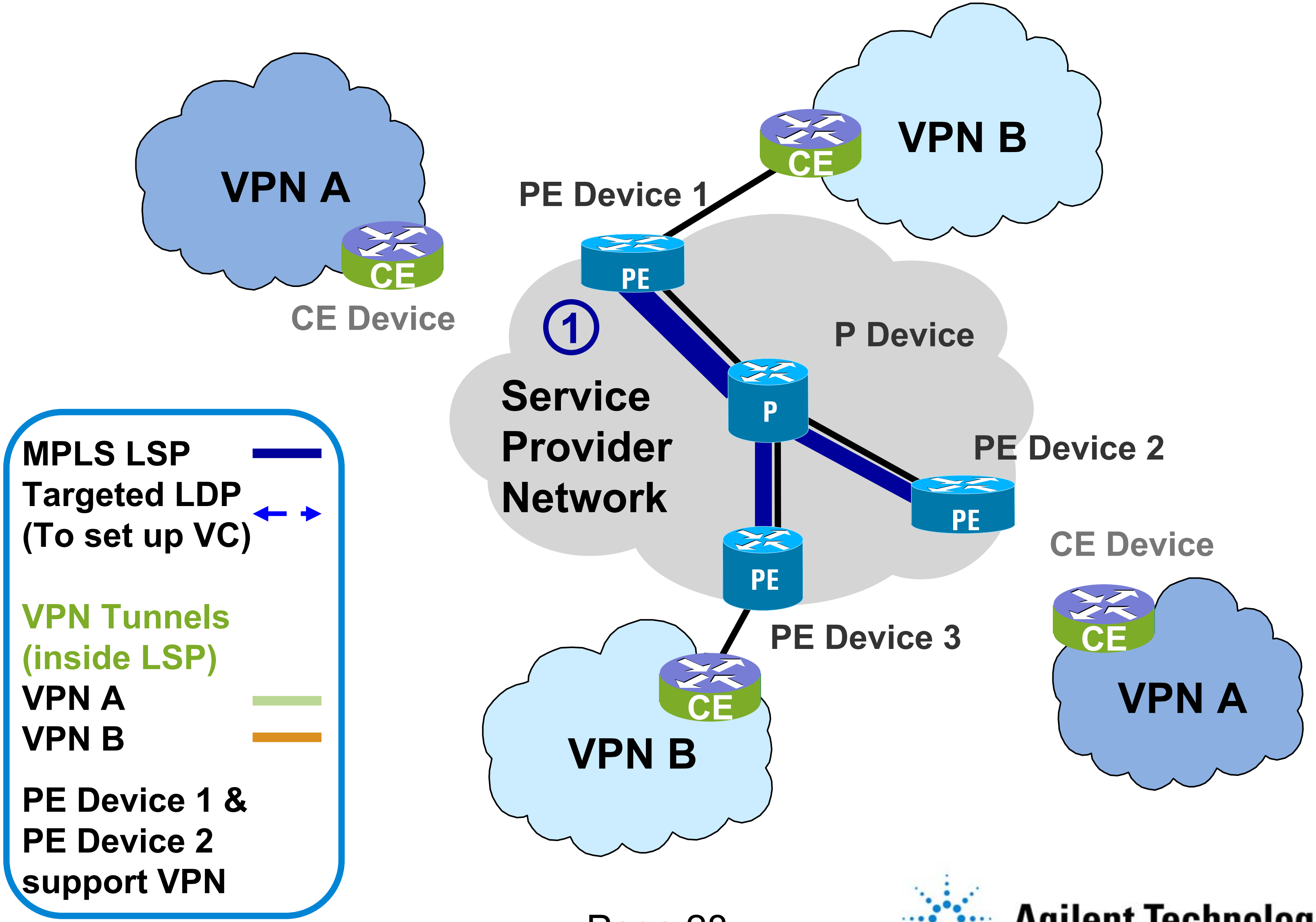
Provider Network Protocols:
IS-IS, OSPF-TE, LDP/CR-LDP, RSVP

Scalability Test Scenario

- SUT needs to maintain 3,000 VRF tables



Layer 2 over MPLS Network Scenario (1)



MPLS LSP 🟦

Targeted LDP (To set up VC) ← →

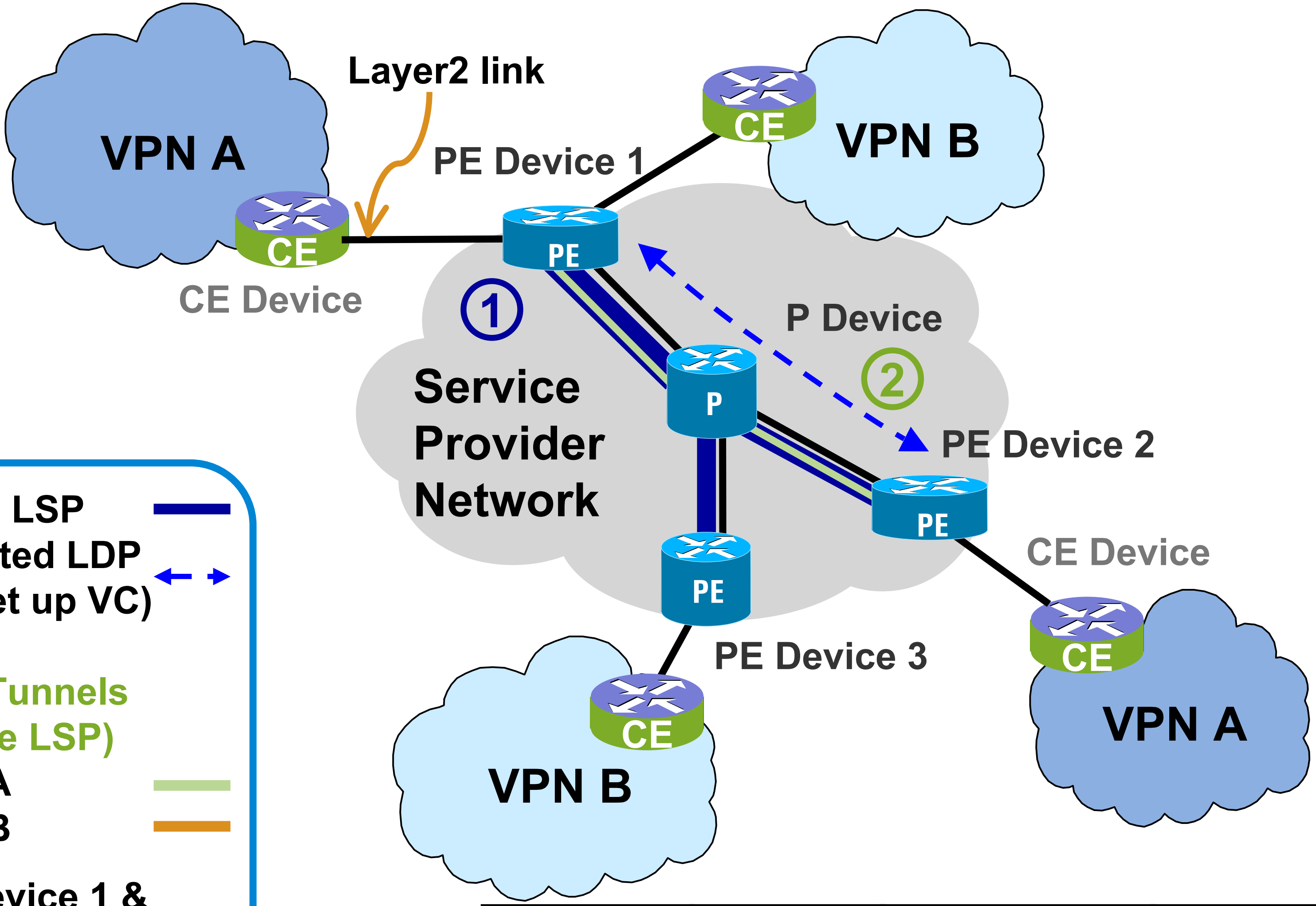
VPN Tunnels (inside LSP)

VPN A 🟩

VPN B 🟧

PE Device 1 & PE Device 2 support VPN

Layer 2 over MPLS Network Scenario (2)



MPLS LSP ━━

Targeted LDP (To set up VC) ← - →

VPN Tunnels (inside LSP)

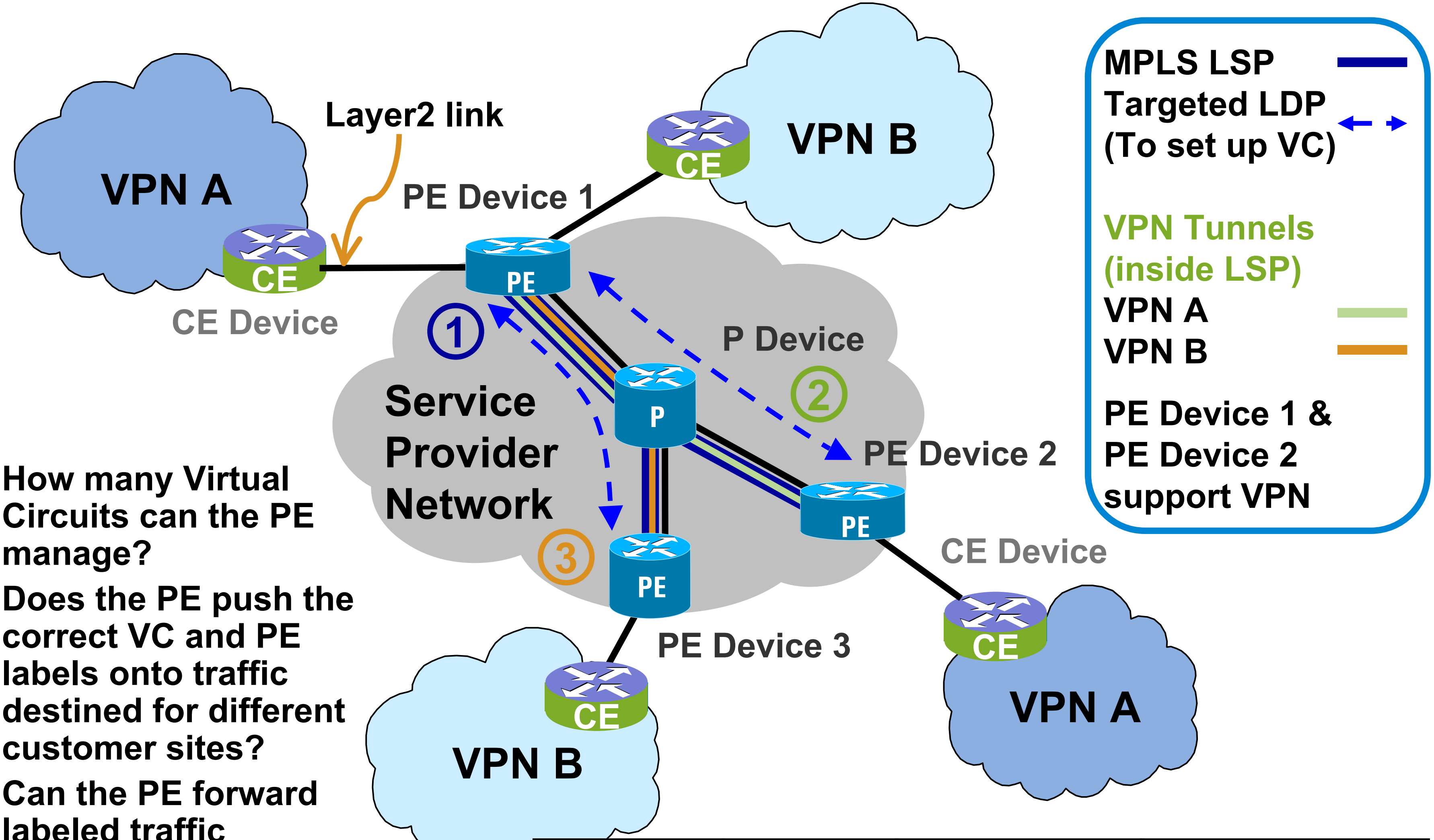
VPN A 🟩

VPN B 🟧

PE Device 1 & PE Device 2 support VPN

LSP Label	VC Label	Control Word	Layer 2 Payload

Layer 2 over MPLS Network Scenario (3)



MPLS LSP
Targeted LDP (To set up VC)

VPN Tunnels (inside LSP)
VPN A
VPN B

PE Device 1 & PE Device 2 support VPN

- How many Virtual Circuits can the PE manage?
- Does the PE push the correct VC and PE labels onto traffic destined for different customer sites?
- Can the PE forward labeled traffic destined for customer sites at wire-speed?

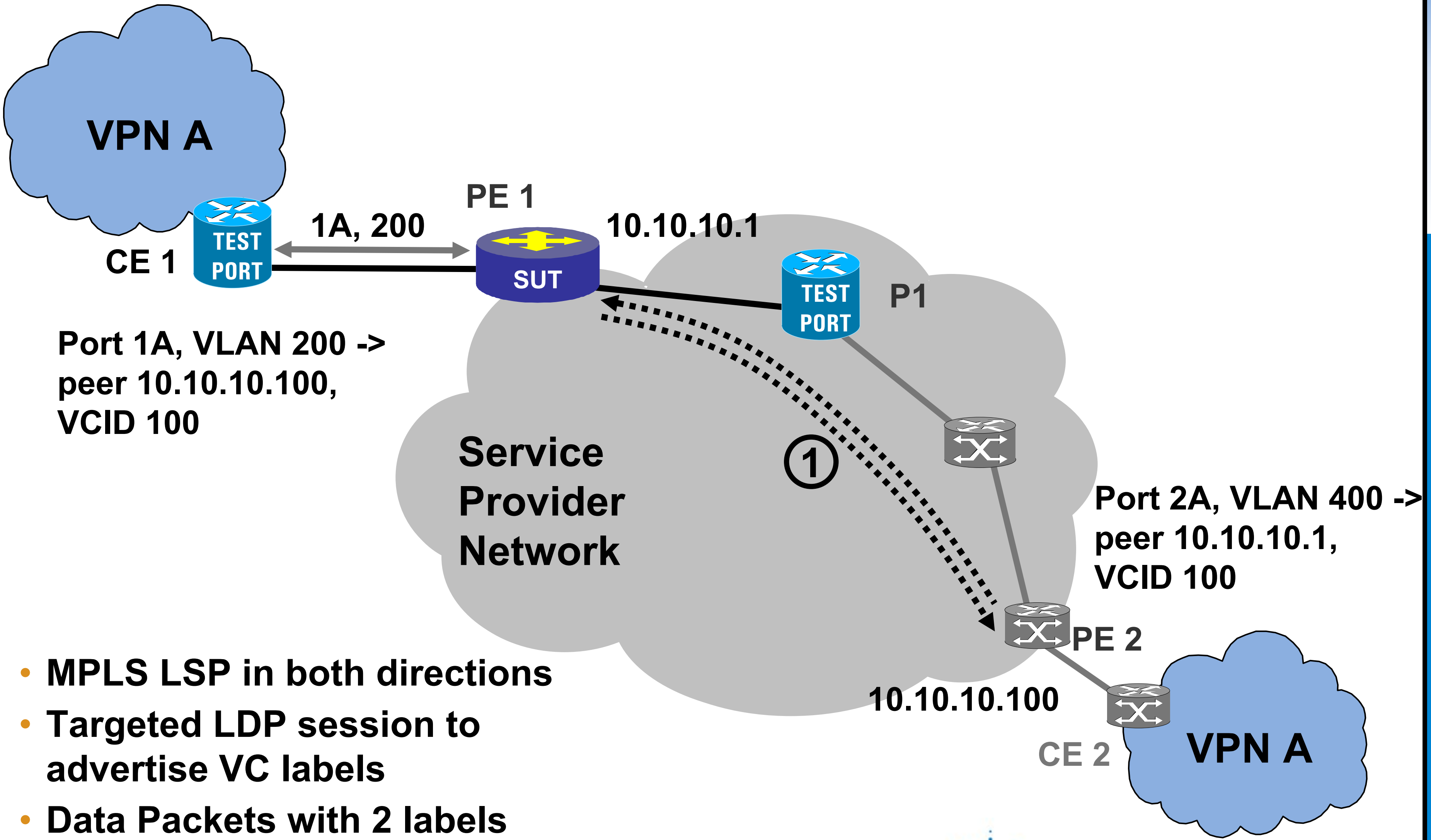
LSP Label	VC Label	Control Word	Layer 2 Payload

Agilent Technologies

How to set up a Layer 2 MPLS VPN

- Runs over an MPLS Label Switched Path
- Setting up the Point-to-Point Layer 2 VPN
  - LDP protocol with extensions exchanges VPN information between PE routers
  - A special Virtual Circuit (VC) label is used to identify the VPN
  - A “Control Word” encapsulation may be used to replace the Layer 2 packet header
  - VC’s are set up only between PE routers which have an LSP set up between them
- Reachability information for a VC to a target CE is propagated to the source PE from the destination PE using a “targeted” LDP session
- No special security except inherent security due to the VC label and the LSP between the PE routers

Functionality Test Scenario (1)

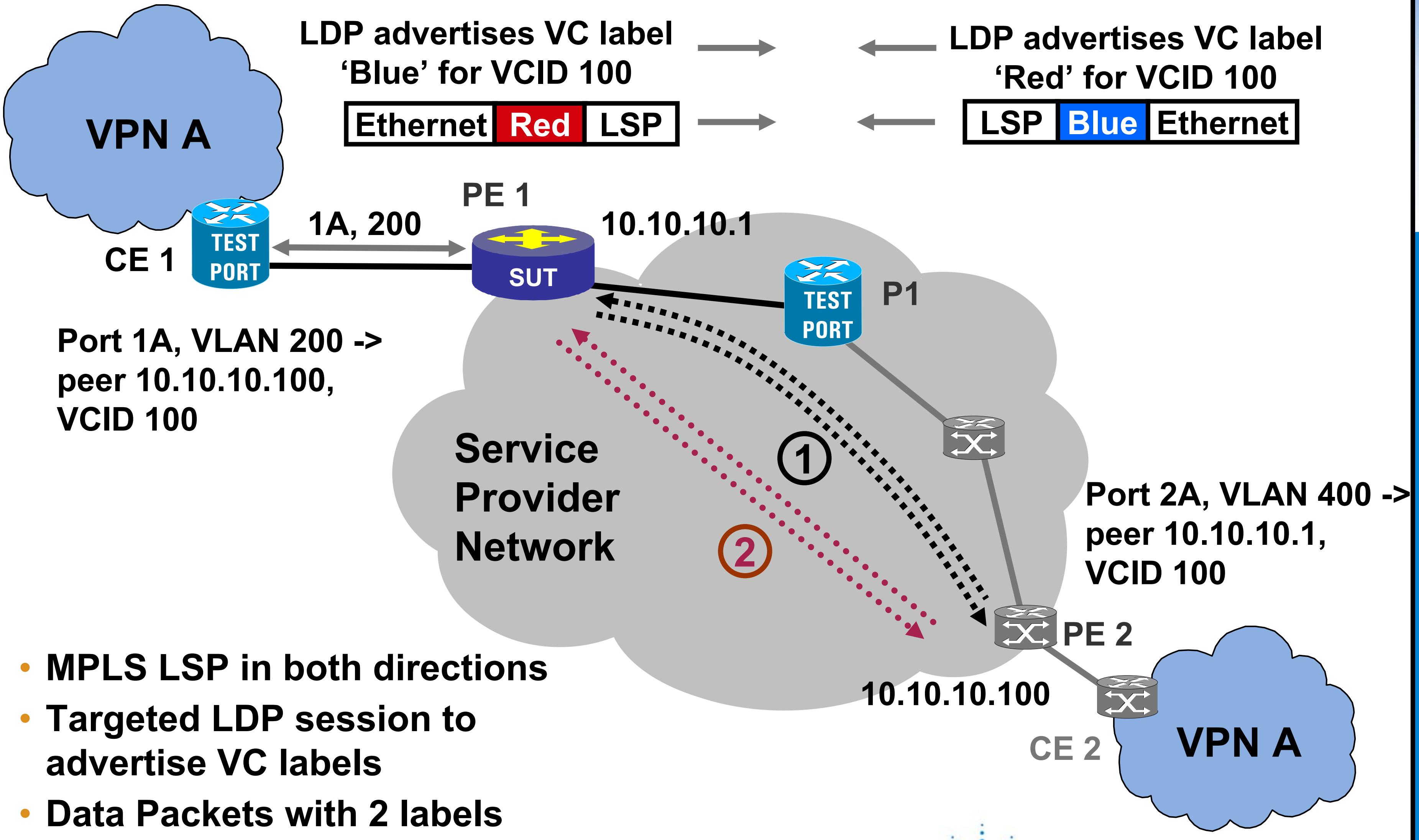


Port 1A, VLAN 200 -> peer 10.10.10.100, VCID 100

Port 2A, VLAN 400 -> peer 10.10.10.1, VCID 100

- MPLS LSP in both directions
- Targeted LDP session to advertise VC labels
- Data Packets with 2 labels exchanged

Functionality Test Scenario (2)



LDP advertises VC label 'Blue' for VCID 100

Ethernet	Red	LSP

LDP advertises VC label 'Red' for VCID 100

LSP	Blue	Ethernet

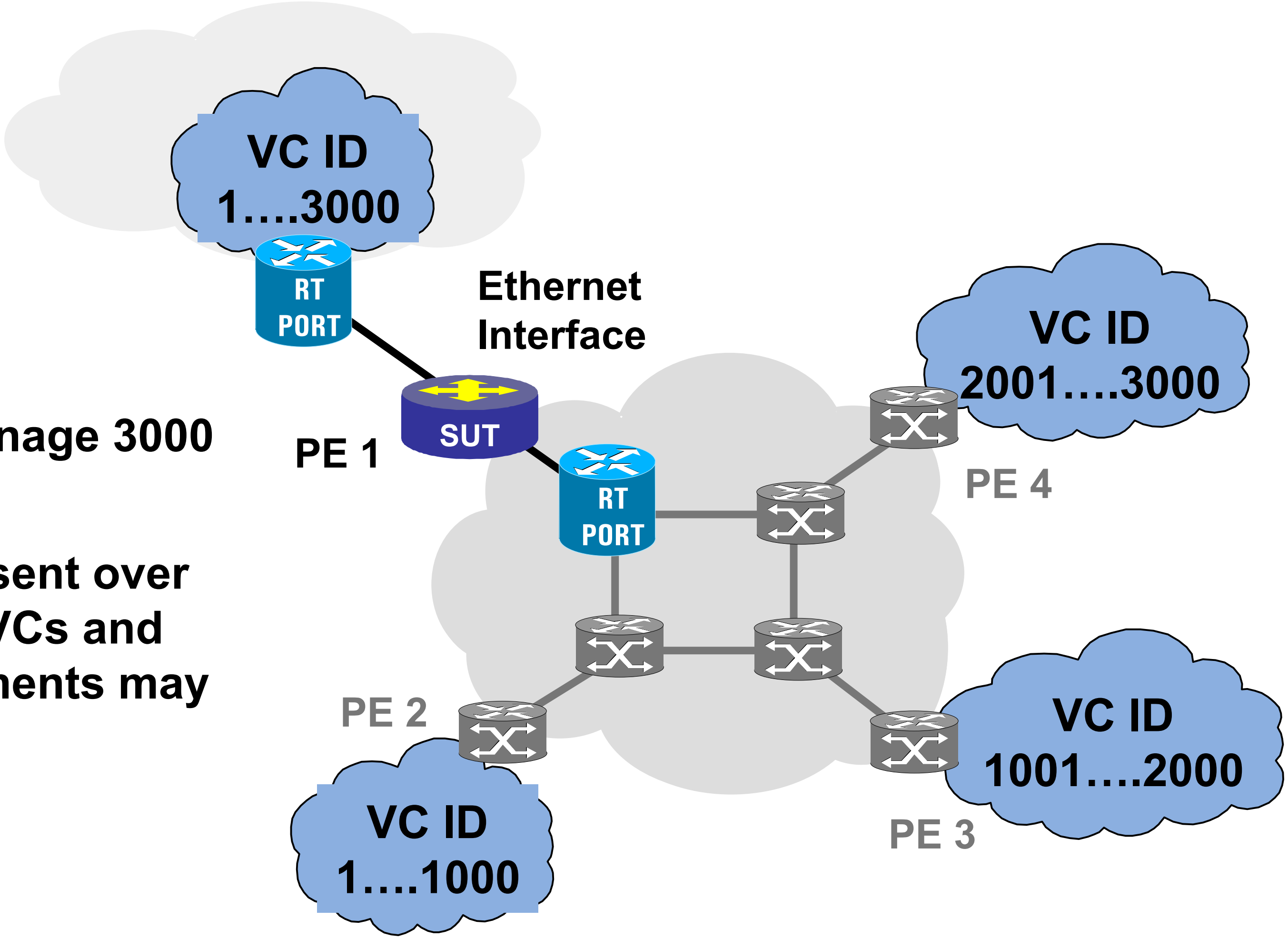
Port 1A, VLAN 200 -> peer 10.10.10.100, VCID 100

Port 2A, VLAN 400 -> peer 10.10.10.1, VCID 100

- MPLS LSP in both directions
- Targeted LDP session to advertise VC labels
- Data Packets with 2 labels exchanged

Scalability & Performance Test Scenario

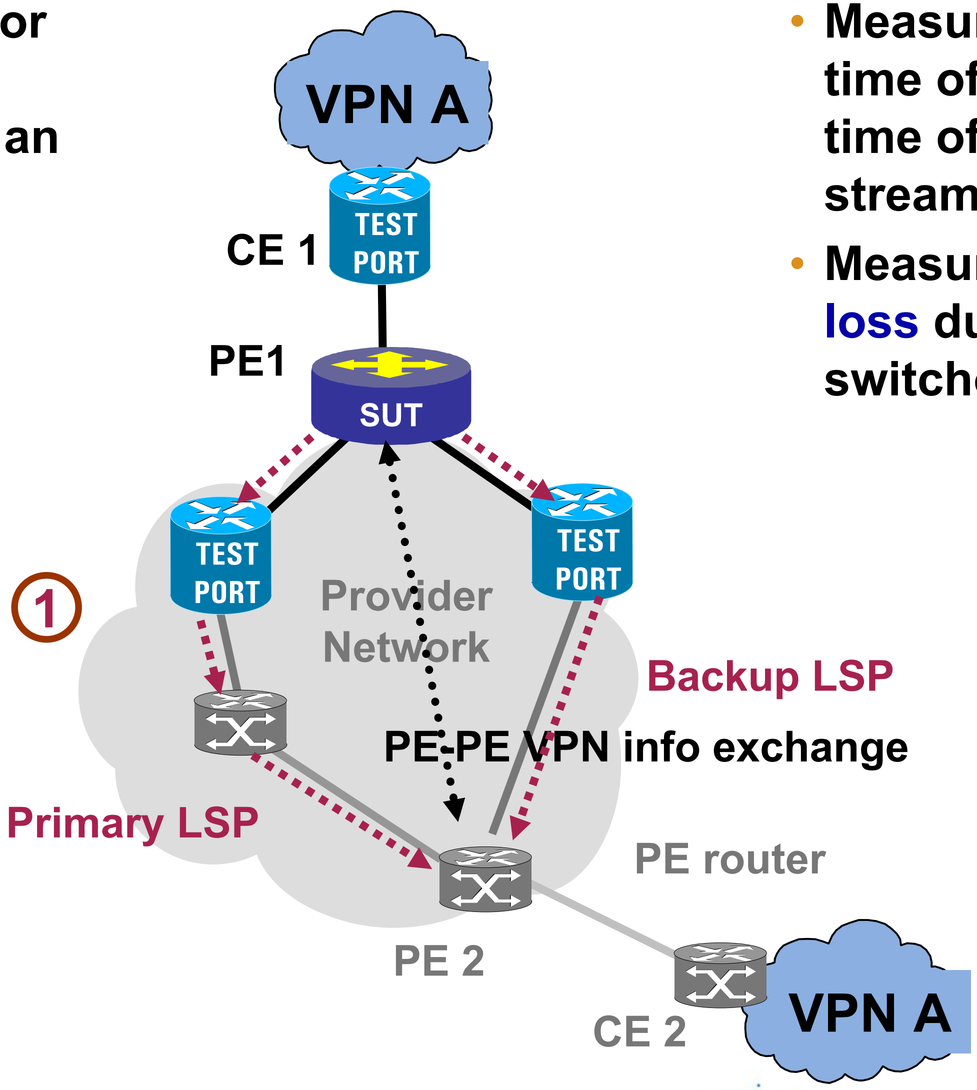
- SUT has to manage 3000 VCs
- Traffic can be sent over each of these VCs and QoS measurements may be made



Service Restoration/QoS Test Scenario 1

The QoS guarantees for the VPN needs to be maintained in case of an LSP failure.

This figure discusses the a typical VPN scenario.

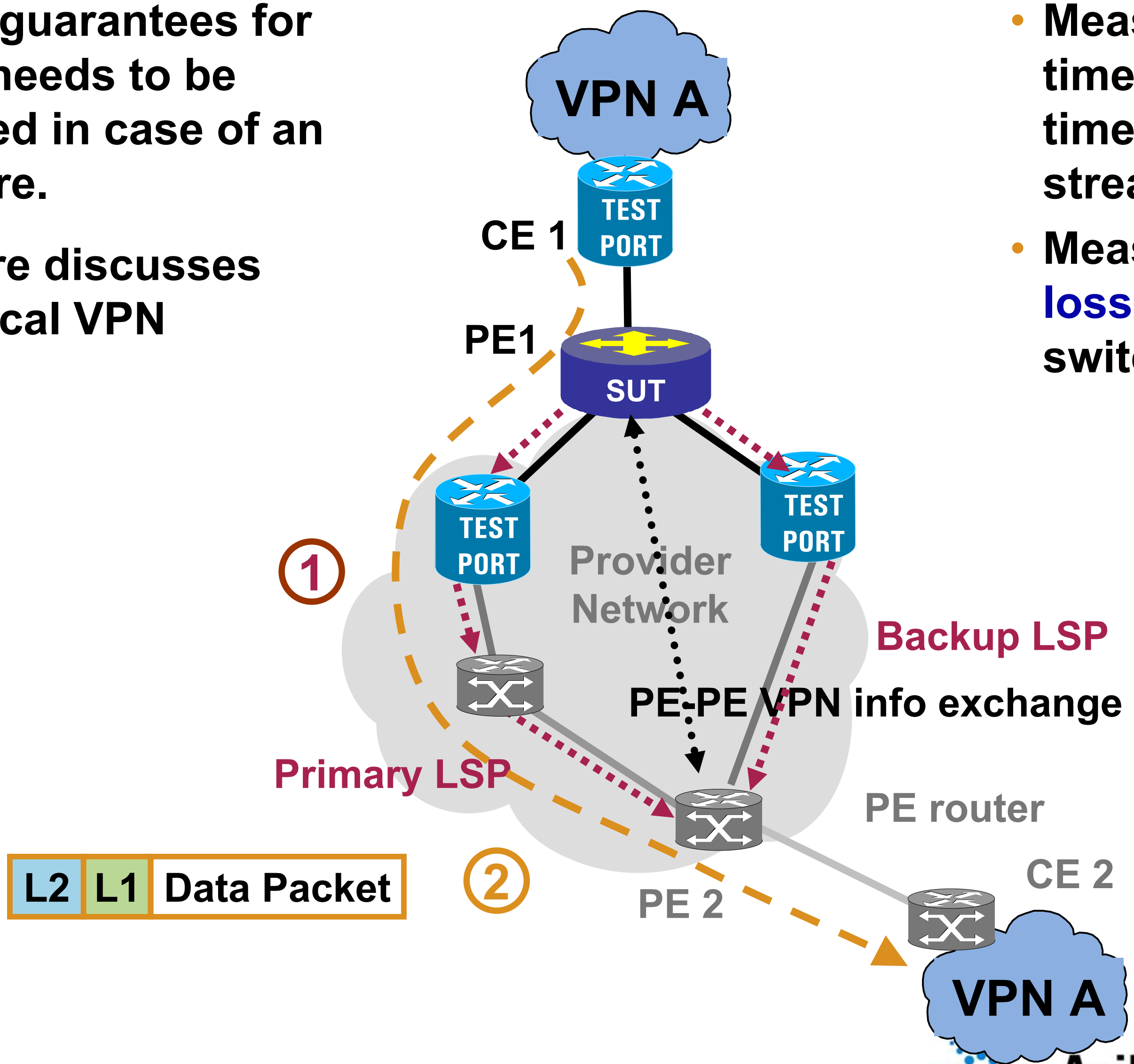


- Measure delay from time of failure to time of arrival of stream on new port
- Measure packet loss during this switchover

Service Restoration/QoS Test Scenario 2

The QoS guarantees for the VPN needs to be maintained in case of an LSP failure.

This figure discusses the a typical VPN scenario.



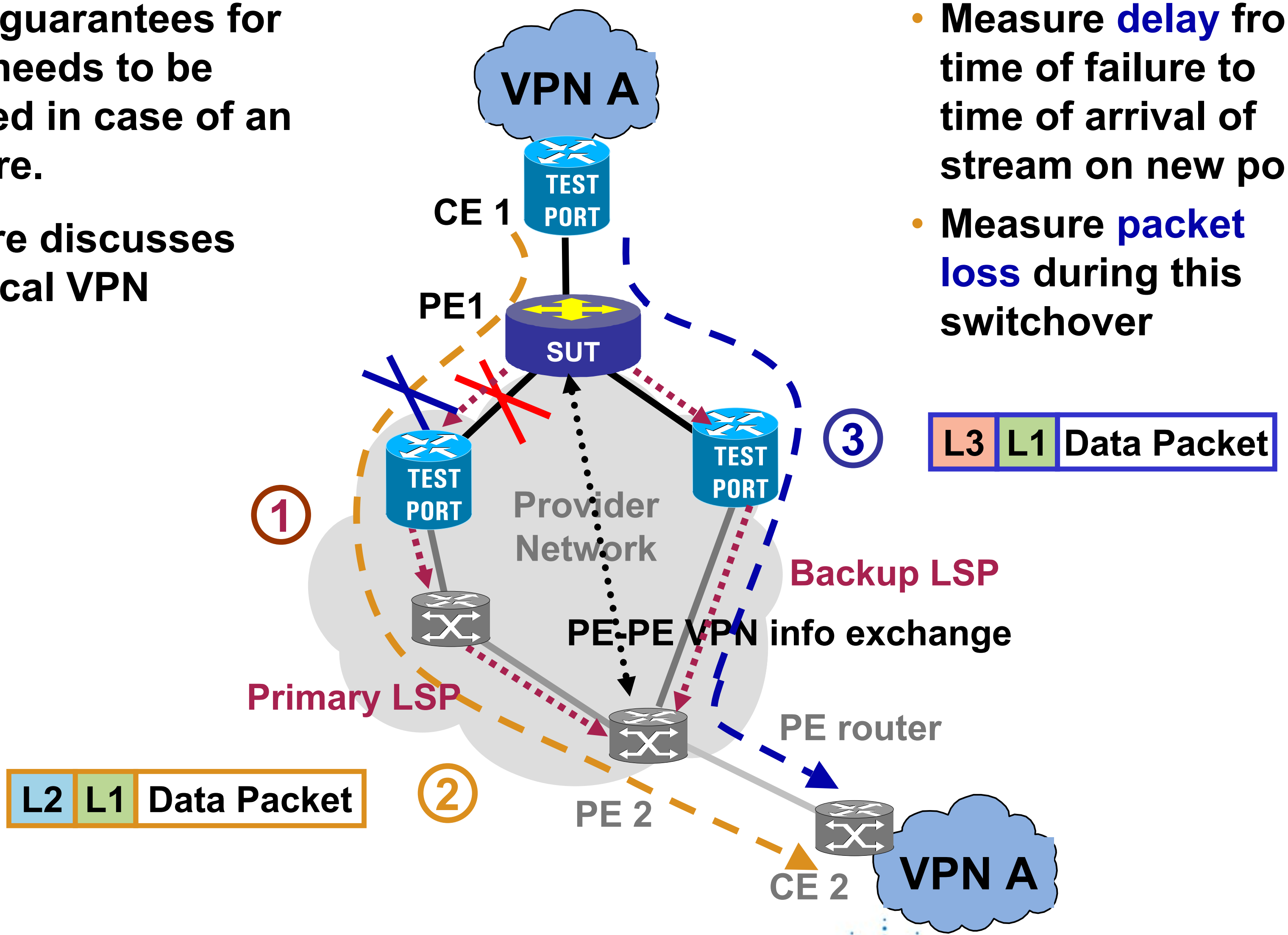
- Measure delay from time of failure to time of arrival of stream on new port
- Measure packet loss during this switchover

Service Restoration/QoS Test Scenario 3

The QoS guarantees for the VPN needs to be maintained in case of an LSP failure.

This figure discusses the a typical VPN scenario.

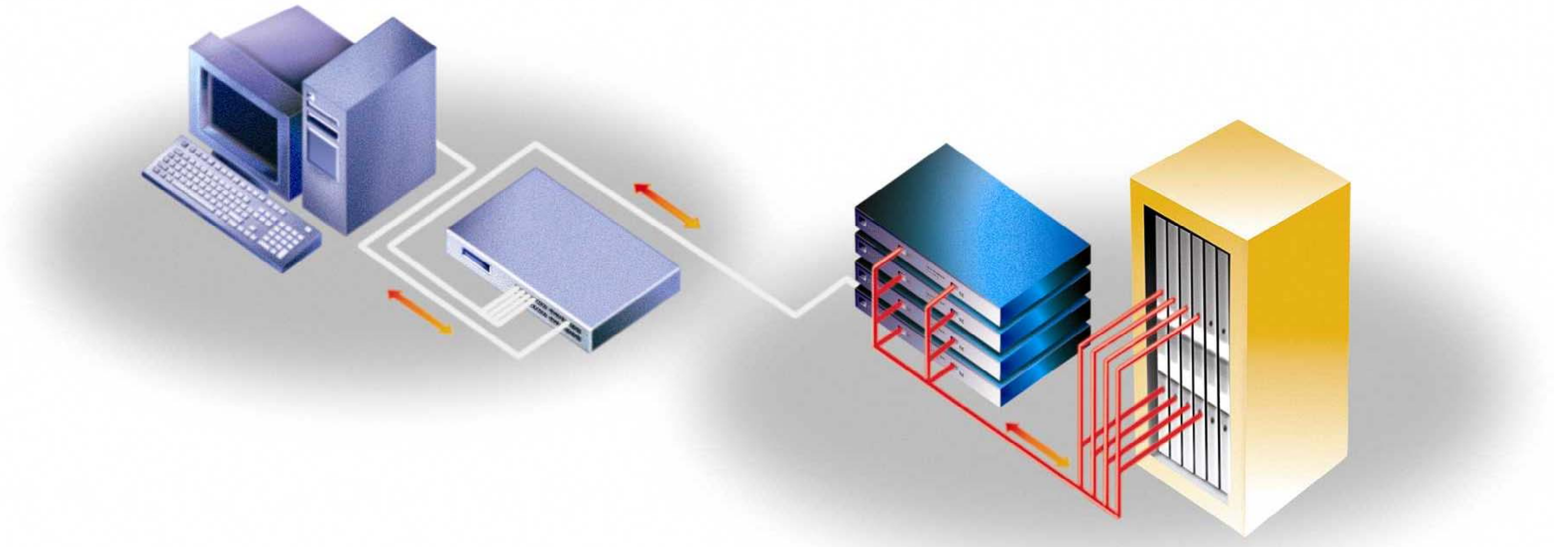
- Measure delay from time of failure to time of arrival of stream on new port
- Measure packet loss during this switchover



Agilent Technologies

What does Agilent offer?

- We know what it takes to test these VPN protocols and services!
- We have all the tools to test these VPN protocols and services!



Agilent Technologies' VPN Test Tools

- RouterTester platform with protocol and data stress capability
- Multiple interfaces:
  - POS (OC-3, OC-12, OC-48, OC-192)
  - ATM (OC-3, OC-12)
  - 10/100
  - Gigabit Ethernet
- Wire-speed traffic testing
  - Fully synchronized QoS measurements

RouterTester

Agilent Technologies’ VPN Test Tools

- Protocol Testing:

	Protocol Conformance Test	Protocol Emulation
L2TP	x	x
IPSec	x	x
LDP	x	x
RSVP-TE	x	x
OSPF	x	x
RIP		x
ISIS	x	x
BGP	x	
E-BGP		x
MP-iBGP		x

- For more information, see Resource Page at end of presentation