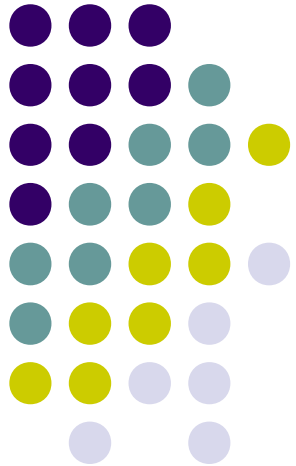
Mạng riêng ảo VPN
(Virtual Private Networks)

Võ Viết Minh Nhật
Nguyễn Ngọc Thủy
Khoa CNTT – ĐHKH Huế



Nội dung trình bày

- Giới thiệu mạng riêng ảo
- Các loại mạng riêng ảo
  - VPN truy cập từ xa (remote access)
  - VPN qua từng site (site-to-site)
  - VPN dựa vào tường lửa (firewall-based)
- Các mô hình mạng riêng ảo
  - VPN xếp chồng (overlay)
  - VPN ngang hàng (peer-to-peer)
- So sánh và Kết luận

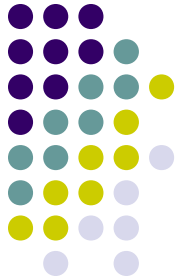
Giới thiệu mạng riêng ảo

- Nhu cầu truy cập và trao đổi thông tin
  => Vấn đề chia xẻ thông tin
- Cạnh tranh giữa các dịch vụ cung cấp thông tin: kịp thời, chính xác, …
  => Vấn đề hệ nền chia sẻ cho các dịch vụ
- Giải pháp cho hệ nền chia xẻ hiện nay: sử dụng các loại mạng public như Internet
  - ưu: mạng lưới kết nối rộng, chi phí thấp, …
  - khuyết: bị xâm nhập, an toàn thông tin thấp, …

Giới thiệu mạng riêng ảo

- Mạng riêng ảo:
  - triển khai trên một hệ nền mạng public
  - sử dụng chung các chính sách an toàn, quản lý và chất lượng dịch vụ
  - dể mở rộng
  - dể thiết lập và bảo trì
  - chi phí thấp
  - khả năng cung cấp dịch vụ cao
  - thuận tiện cho khách hàng và nhà cung cấp

Giới thiệu mạng riêng ảo



- Có 2 cách cài đặt và quản lý VPNs:
  - tự cài đặt và quản lý mạng VPN
  - chuyển giao quyền đó cho nhà cung cấp dịch vụ
- VPNs có thể được cung cấp theo kiểu từng gói và khách hàng chỉ việc yêu cầu theo nhu cầu sử dụng của mình.

Các loại mạng riêng ảo

- VPN truy cập từ xa (remote access)
- VPN qua từng site (site-to-site)
- VPN dựa vào tường lửa (firewall-based)
- Lưu ý: cho dù la loại mạng VPN nào, đặc điểm chung của chúng là đều bao gồm 2 nút đầu-cuối (routers, firewalls, client workstations, servers.)

VPN truy cập từ xa

- Được triển khai cho những người dùng ở xa (mobile users)
- Là một hình thức mở rộng của mạng dialup truyền thống
- Thực hiện kết nối từ PC của người dùng qua ISP để truy cập đến các mạng công ty
- Phần mềm trên PC của người dùng sẽ đảm bảo việc thiết lập tunnel an toàn

VPN qua từng site

- Được triển khai để kết nối các corporate sites
- Là một hình thức mở rộng của mạng WAN truyền thống
- Được phân thành 2 loại: intranet VPN và extranet VPN
  - intranet VPN: các sites thuộc về cùng một tổ chức
  - extranet VPN: các sites thuộc về các tổ chức khác nhau

VPN dựa vào tường lửa

- Là một hình thức khác của VPN qua từng site, trong đó tường lửa được sử dụng cho vấn đề an toàn thông tin
- Được triển khai để tăng cường an toàn thông tin qua VPN

Một vài thuật ngữ thông dụng

- Mạng nhà cung cấp (P-network): hệ nền của nhà cung cấp được sử dụng để cung cấp dịch vụ VPN
- Mạng khách hàng (C-network): phần mạng chịu sự điều khiển của khách hàng
- Site khách hàng: một phần tiếp giáp của mạng khách hàng (về vị trí vật lý)
- Router bên trong của nhà cung cấp (P-router): thiết bị bên trong mạng nhà cung cấp mà không kết nối trực tiếp với mạng khách hàng.

Một vài thuật ngữ thông dụng

- Router biên của nhà cung cấp (PE-router): thiết bị biên của mạng nhà cung cấp có kết nối trực tiếp với mạng khách hàng.
- Router biên của khách hàng (CE-router): thiết bị biên của mạng khách hàng có kết nối trực tiếp với mạng nhà cung cấp.
- Liên kết ảo (VC): liên kết logic điểm-điểm được thực hiện ở tầng 2 của hệ nền.

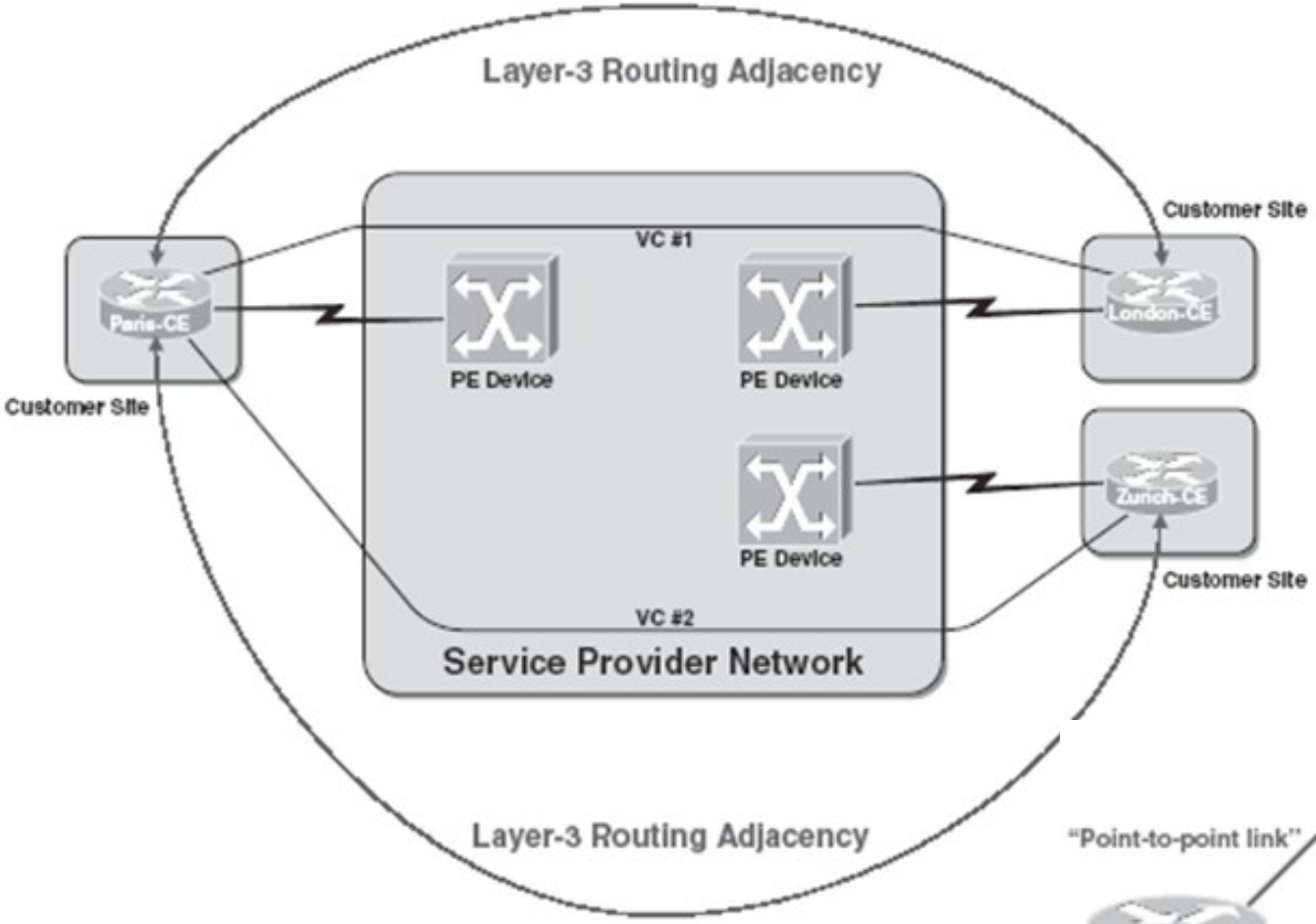
Các mô hình mạng riêng ảo

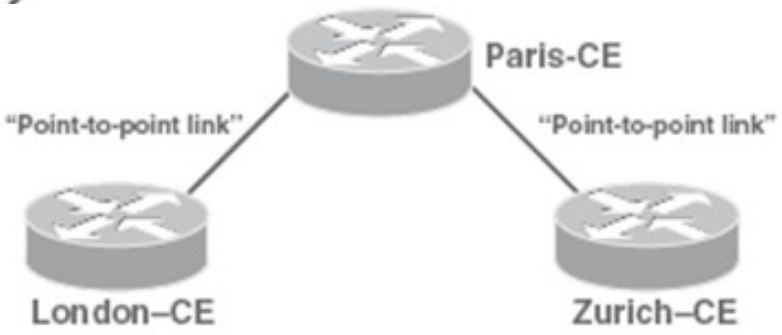
- VPN xếp chồng (overlay): trong đó các liên kết ảo điểm-điểm giữa các sites khách hàng được cấp phát bởi nhà cung cấp
- VPN ngang hàng (peer-to-peer): trong đó nhà cung cấp tham gia vào việc định tuyến (routing) với khách hàng

VPN xếp chồng

- Được triển khai qua hệ nền của nhà cung cấp, có thể ở tầng L1, L2 hoặc L3.
- Routing thực hiện trực tiếp giữa các router khách hàng và trong suốt đối với mạng nhà cung cấp
- Nhà cung cấp chỉ thiết lập các VCs giữa các site khách hàng
- Khó mở rộng (scalability)
- Không thể triển khai full mesh các VCs

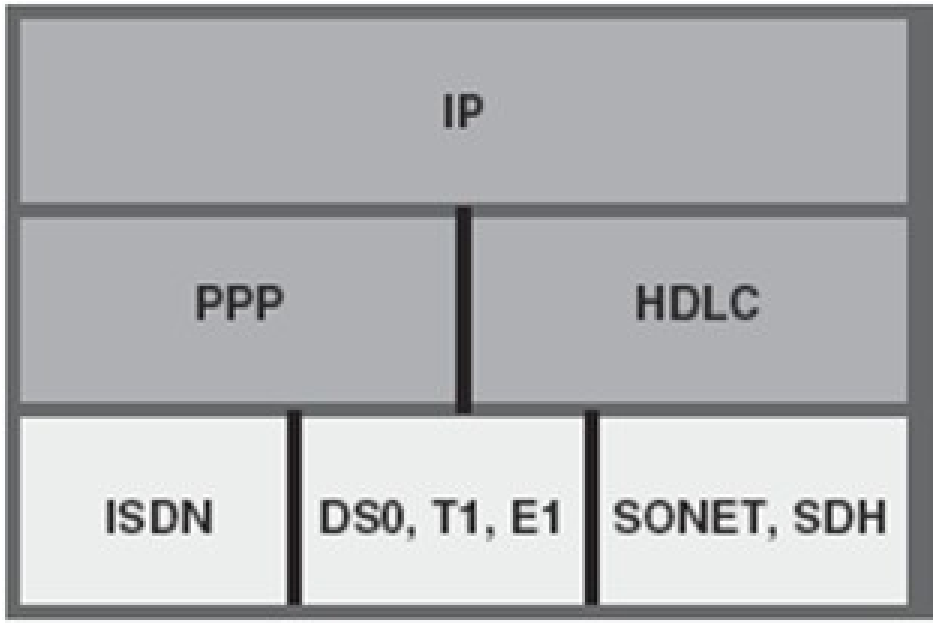
VPN xếp chồng (2)





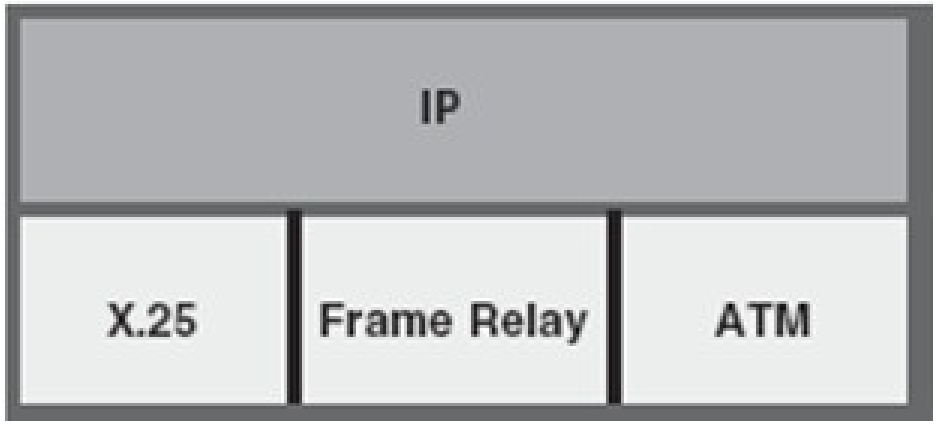
VPN xếp chồng L1

- Sử dụng kỹ thuật TDM truyền thống
- Nhà cung cấp thiết lập các kết nối tầng vật lý (L1) qua ISDN, DS0, T1, E1, SONET hoặc SDH
- Khách hàng sẽ thực hiện các cài đặt ở các tầng cao hơn như PPP, HDLC và IP



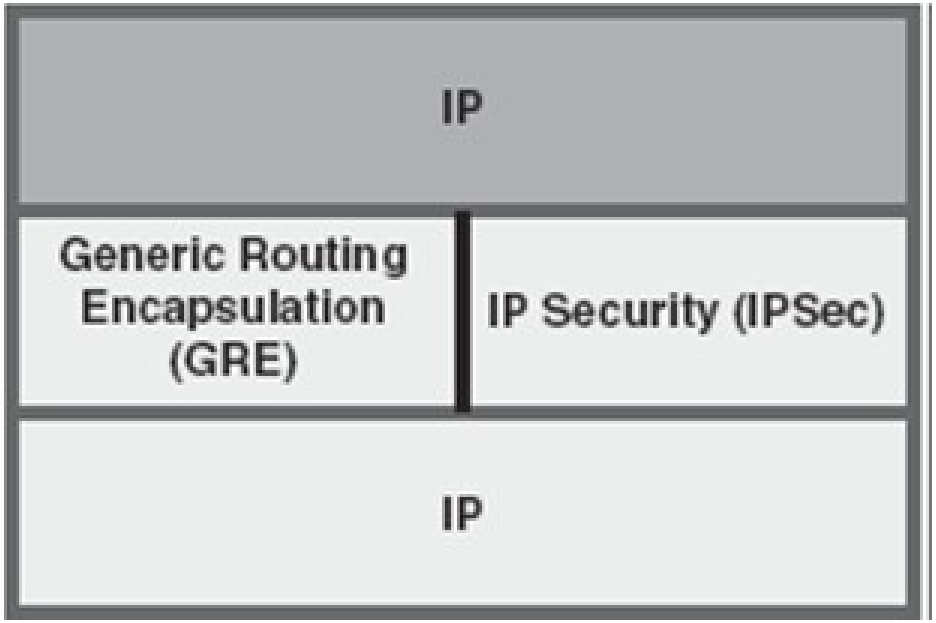
VPN xếp chồng L2

- Sử dụng kỹ thuật chuyển mạch WAN truyền thống
- Nhà cung cấp thiết lập các VCs (L2) qua X.25, Frame Relay hay ATM
- Khách hàng sẽ thực hiện các cài đặt ở tầng IP



VPN xếp chồng L3

- IP-over-IP tunnel điểm-điểm
- Không cần đổi địa chỉ khi đi qua mạng nhà cung cấp
- Tunnels có thể được thực hiện bởi
  - GRE
  - IPSec



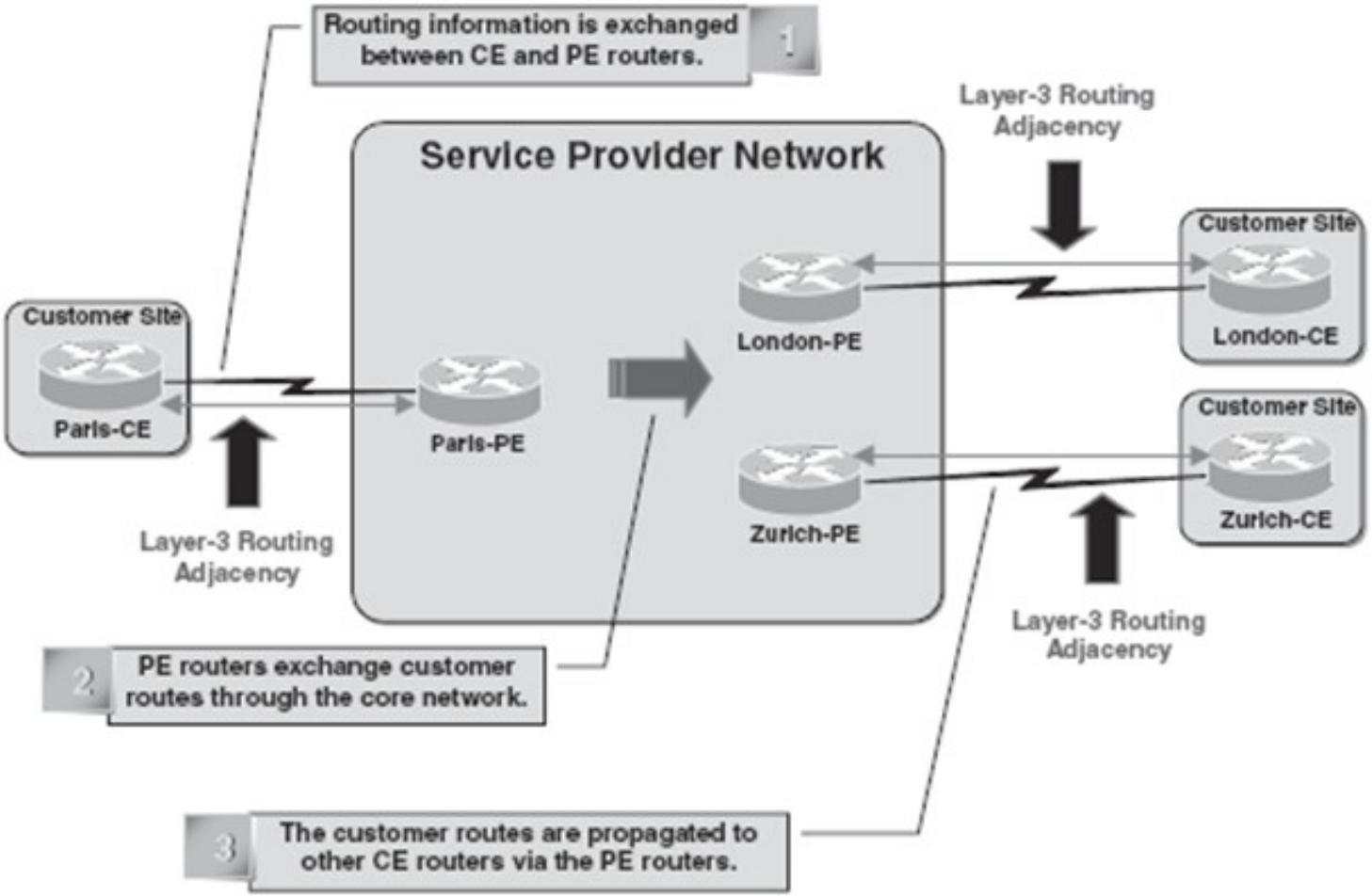
VPN xếp chồng L3 (2)

- GRE (generic routing encapsulation)
  - Gói dữ liệu với header mới => tunnel đầu-cuối
  - Không cung cấp công cụ bảo mật
  - Thường được kết hợp với IPSec
- IPSec (IP security)
  - Một chuẩn của IETF về mã hóa
  - Được cài đặt trong suốt đối với hệ nền
  - Tăng cường tính an toàn cho mạng
  - Kết hợp với GRE để thực hiện multicast

VPN ngang hàng

- Nhà cung cấp và khách hàng sử dụng chung giao thức
- PE routers và CE routers trao đổi thông tin để thiết lập routes giữa chúng
- Việc triển khai full mesh các VCs là không cấn thiết
- Việc bổ sung hay loại bỏ sites là dễ dàng => dể mở rộng (scalability)
- Địa chỉ hóa và quản lý không gian địa chỉ được thực hiện ở mạng khách hàng.

VPN ngang hàng (2)

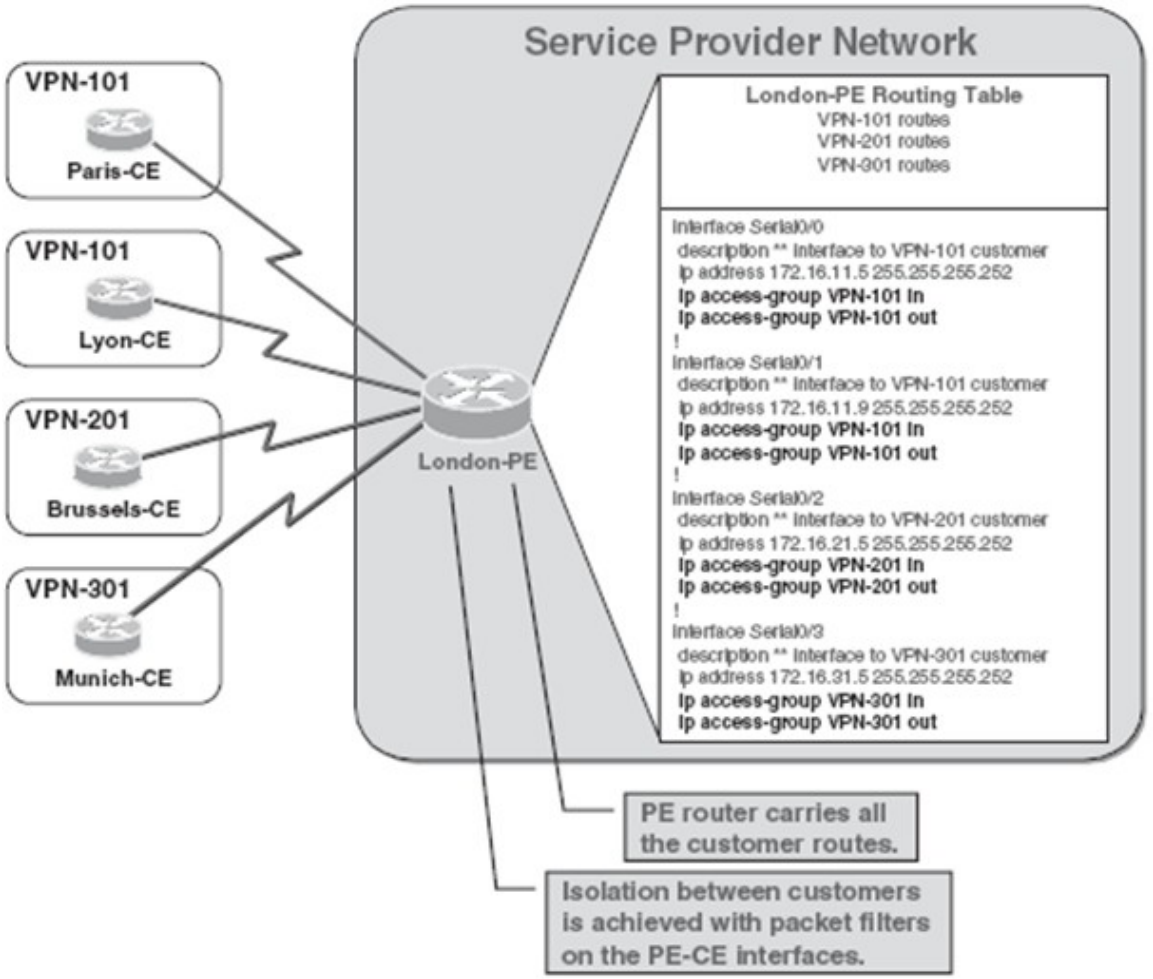


VPN ngang hàng (3)

- VPN ngang hàng bao gồm 3 mô hình
  - Mô hình dựa trên PE router chia sẻ
  - Mô hình dựa trên PE router dành riêng
  - Mô hình dựa trên MPLS

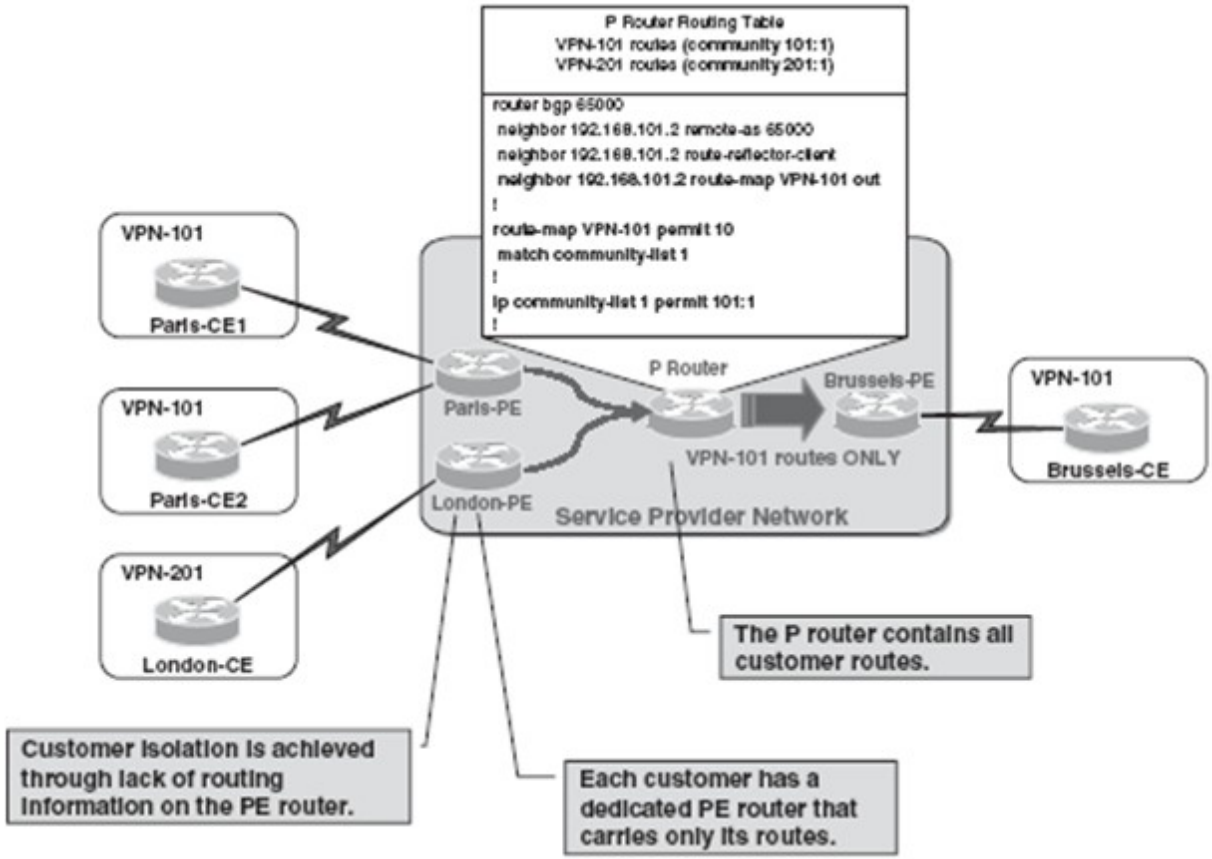
VPN ngang hàng dựa trên PE router chia sẻ

- Một PE router được sử dụng chung cho việc mang các routes khách hàng
- PE-CE interfaces trên PE router này phân loại các routes khách hành khác nhau



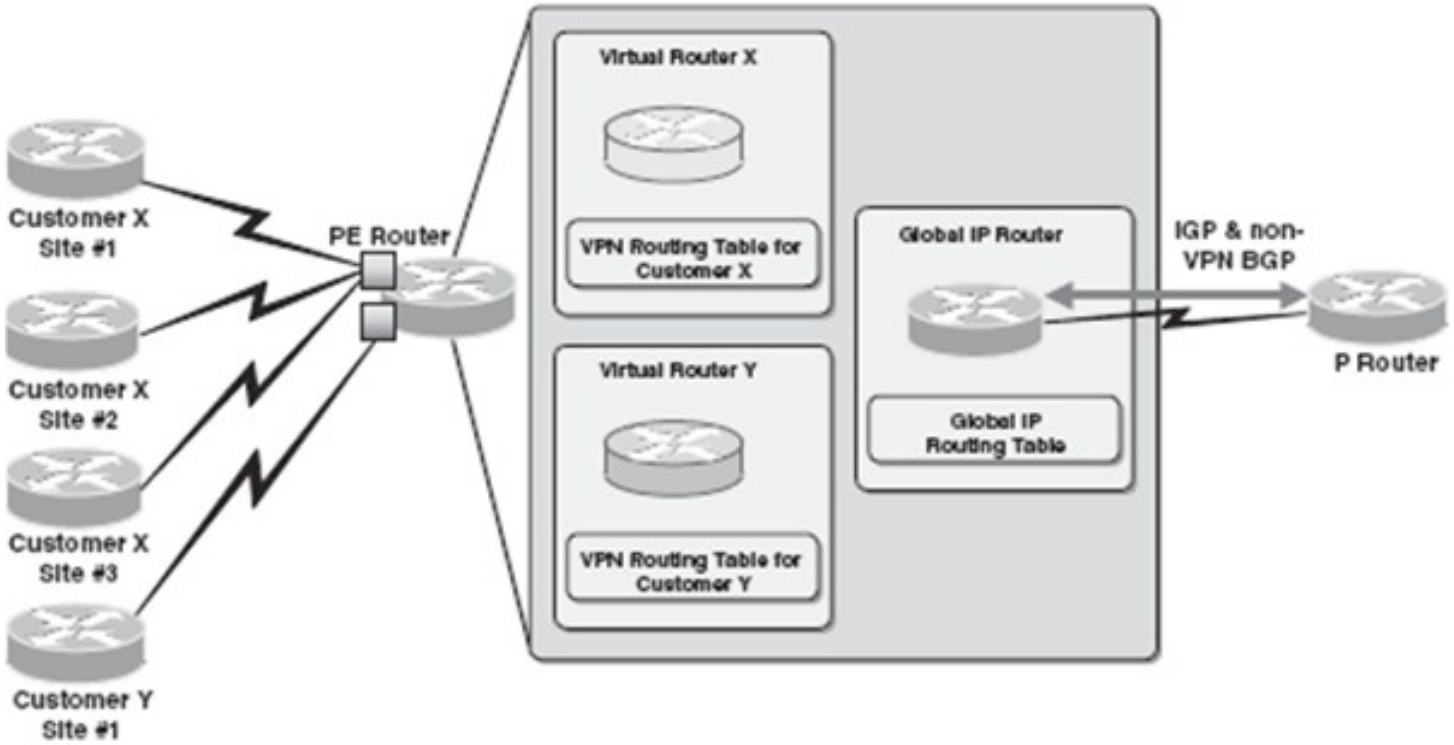
VPN ngang hàng dựa trên PE router dành riêng

- Mỗi khách hàng có môt PE router dành riêng
- P routers thực hiện phân loại các routes khách hàng bằng cách sử dụng PGP Communities
- Chi phí cao



VPN ngang hàng dựa trên MPLS

- Tương tự như VPN ngang hàng dựa trên PE router dành riêng, nhưng thay vì sử dụng các PE routers dành riêng, nó cài đặt các bảng routing ảo (VRF) trên PE router.



So sánh và kết luận

Overlay VPN		P2P VPN	
Ưu	Khuyết	Ưu	Khuyết
Cho phép tái tạo địa chỉ IP	Khó mở rộng	Dể mở rộng	Không cho phép tái tạo địa chỉ IP
Tách rời rõ giữa các khách hàng	Yêu cầu full mesh để routing tối ưu	Cấu hình routing đơn giản hơn đối với khách hàng	Tất cả các routes được mang bên trong mạng nhà cung cấp
Dịch vụ VPN an toàn	L3-CE thực hiện routing giữa các sites liền kề	Routing tối ưu giữa các sites	Các PE dành riêng phức tạp

So sánh và kết luận

IPSec VPN (overlay)	MPLS VPN (p2p)
• Cài đặt ở tầng mạng • Được quản lý bởi khách hàng • Tunnels đầu-cuối • An toàn dữ liệu do khách hàng chịu trách nhiệm • Khó mở rộng	• Cài đặt ở tầng mạng • Được quản lý bởi nhà cung cấp • Cung cấp các liên kết IP cho khách hàng • Dễ mở rộng