TRƯỜNG ĐẠI HỌC THỦY LỢI

KHOA CÔNG NGHỆ THÔNG TIN

Bộ môn: Mạng và an toàn thông tin

QUẢN TRỊ MẠNG

Giảng viên: Trần Văn Hội

Email: hoitv@tlu.edu.vn

Điện thoại: 0944.736.007

NỘI DUNG MÔN HỌC

- Chương 1: Tổng quan về mạng
- Chương 2: Các kỹ thuật định tuyến
- Chương 3: Chuyển mạch trong mạng LAN
- Chương 4: Công nghệ mạng WAN
- Chương 5: Bảo mật mạng

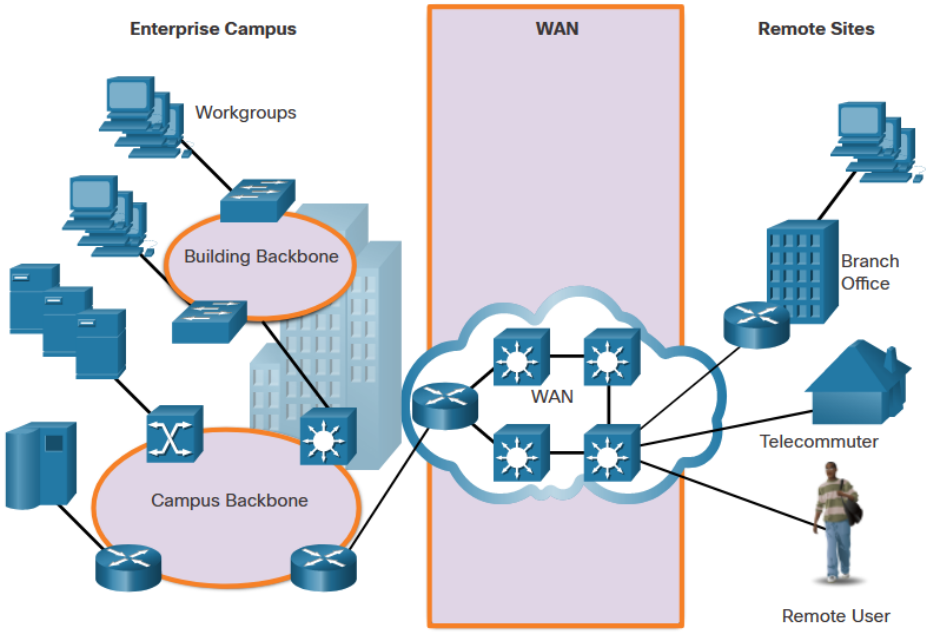
CHƯƠNG 4: CÔNG NGHỆ MẠNG WAN

- 1. Mục đích mạng WAN
- 2. Hoạt động của mạng WAN
- 3. Công nghệ mạng riêng ảo VPN

MỤC ĐÍCH CỦA MẠNG WANs

Mạng WAN là một mạng viễn thông trải rộng trên một khu vực địa lý rộng lớn như một quốc gia, một khu vực, trên toàn cầu.

Local Area Networks (LANs)	Wide Area Networks (WANs)
Mạng LAN cung cấp các dịch vụ mạng trong một khu vực địa lý nhỏ.	Mạng WAN cung cấp các dịch vụ mạng trong một khu vực địa lý rộng lớn
Mạng LAN được sử dụng để kết nối các máy tính, thiết bị ngoại vi và các thiết bị khác trong một đơn vị, tổ chức.	Mạng WAN được sử dụng để kết nối người dùng từ xa, kết nối các mạng và site của các tổ chức với nhau.
Mạng LAN được sở hữu và quản lý bởi một cơ quan, tổ chức hoặc người dùng gia đình.	Mạng WAN được sở hữu và quản lý bởi các nhà cung cấp dịch vụ internet, điện thoại, cáp và vệ tinh.
Ngoài chi phí đầu tư cơ sở hạ tầng mạng, sử dụng mạng LAN không mất phí.	Sử dịch vụ WAN có tính phí.
Mạng LAN cung cấp tốc độ băng thông cao sử dụng dịch vụ Ethernet và Wi-Fi có dây.	Các nhà cung cấp mạng WAN cung cấp tốc độ băng thông từ thấp đến cao, trên khoảng cách xa.



PRIVATE AND PUBLIC WANS

- Mạng WAN riêng là kết nối dành riêng cho một khách hàng.
- Mạng WAN riêng cung cấp những điều sau:
  - Đảm bảo chất lượng dịch vụ
  - Băng thông được đảm bảo
  - Đảm bảo tính bảo mật
- Kết nối WAN công cộng thường được cung cấp bởi ISP hoặc nhà cung cấp dịch vụ viễn thông sử dụng internet. Trong trường hợp này, các chất lượng dịch vụ và băng thông có thể thay đổi, các kết nối được chia sẻ và không đảm bảo tính bảo mật.

WAN TOPOLOGIES

Mạng WAN được triển khai sử dụng các thiết kế cấu trúc (Topology) logic sau:

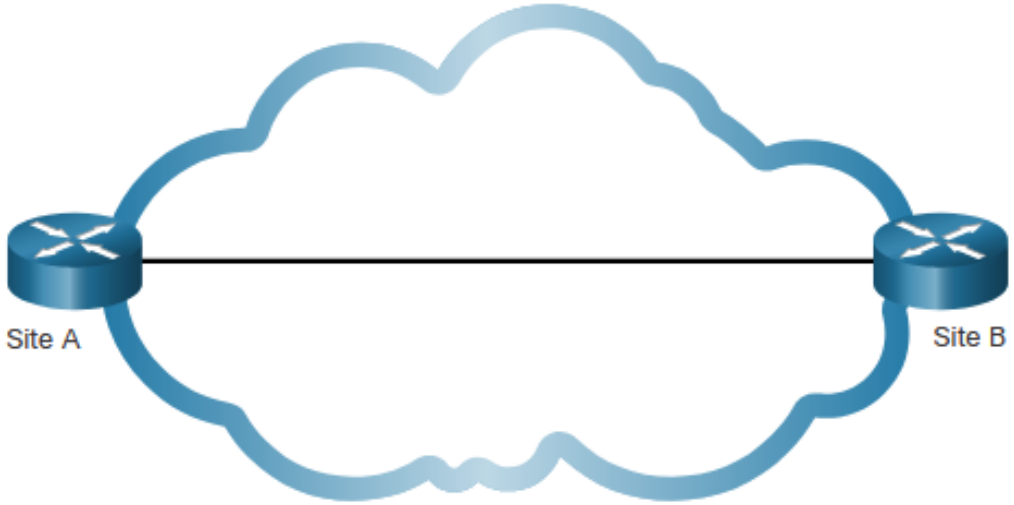
- Point-to-Point Topology
- Hub-and-Spoke Topology
- Dual-homed Topology
- Fully Meshed Topology
- Partially Meshed Topology

Các mạng lớn thường triển khai kết hợp các cấu trúc liên kết này.

WAN TOPOLOGIES (CONT.)

Cấu trúc liên kết điểm-điểm

- Sử dụng một mạch điểm-điểm giữa hai điểm cuối.
- Liên quan đến dịch vụ vận chuyển Lớp 2 thông qua mạng của nhà cung cấp dịch vụ.
- Kết nối điểm-điểm là trong suốt đối với mạng khách hàng.

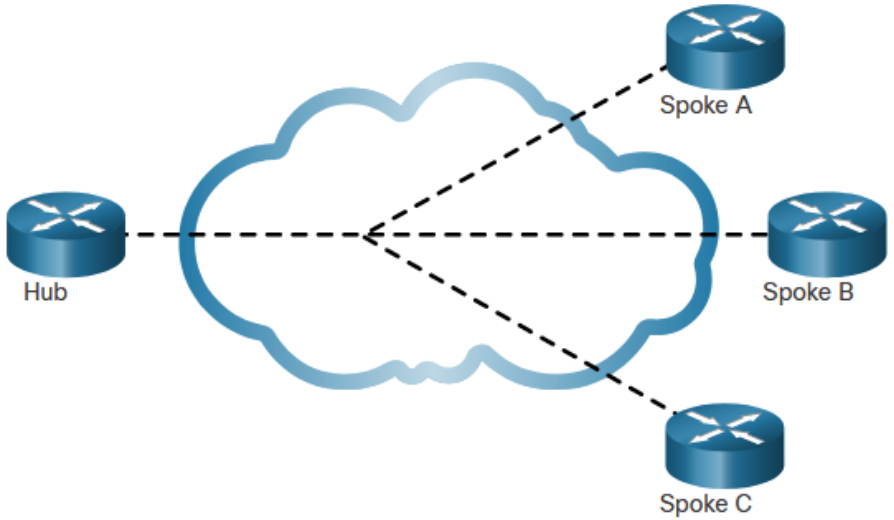


Nếu cần nhiều kết nối điểm-điểm giá thành của hệ thống trở nên đắt đỏ.

WAN TOPOLOGIES (CONT.)

Cấu trúc liên kết Hub-and-Spoke

- Cho phép một giao diện bộ định tuyến hub chia sẻ các mạch tới các spoke.
- Các bộ định tuyến Spoke có thể được kết nối với nhau thông qua bộ định tuyến trung tâm hub bằng cách sử dụng các mạch ảo và các giao diện con được định tuyến.
- Các bộ định tuyến Spoke chỉ có thể giao tiếp với nhau thông qua bộ định tuyến trung tâm Hub.

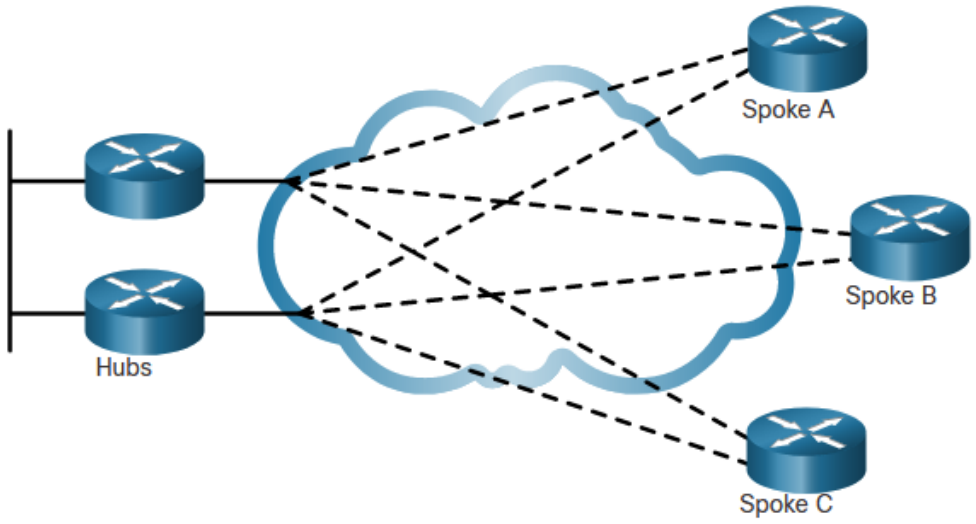


Chú ý: Khi bbộ định tuyến trung tâm hub bị lỗi. Việc kết nối giữa các spoke cũng không thành công.

WAN TOPOLOGIES (CONT.)

Dual-homed Topology

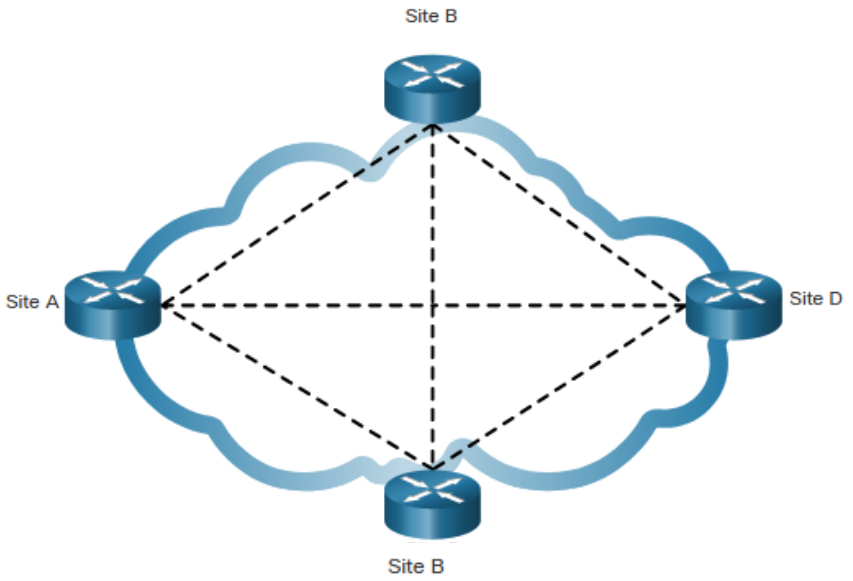
- Cung cấp khả năng dự phòng mạng nâng cao, cân bằng tải, tính toán và xử lý phân tán cũng như khả năng thực hiện các kết nối dự phòng đến nhà cung cấp dịch vụ.
- Giá thành sẽ đắt hơn so với cấu trúc single-homed. Điều này là do chúng yêu cầu phần cứng mạng, như bộ định tuyến và bộ chuyển mạch.
- Khó thực hiện hơn vì chúng yêu cầu các cấu hình bổ sung và phức tạp hơn



WAN TOPOLOGIES (CONT.)

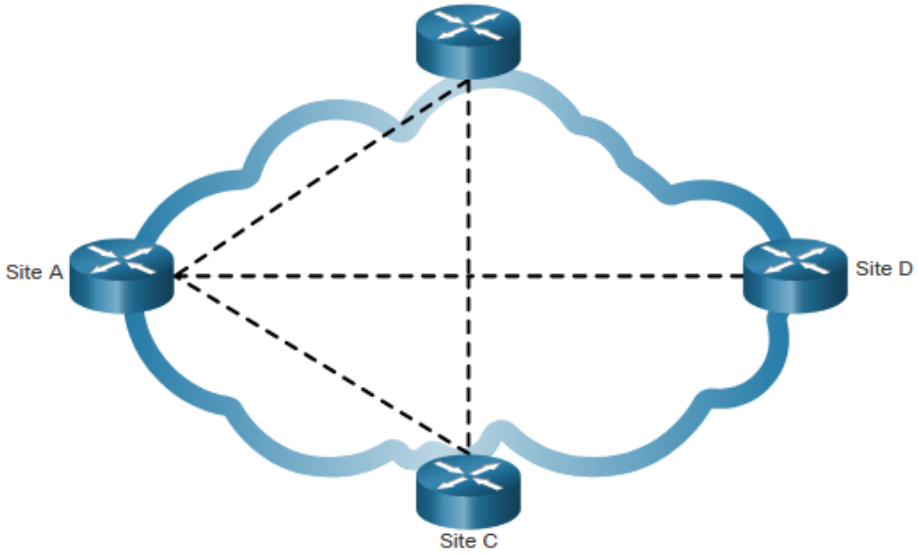
Fully Meshed Topology

- Sử dụng nhiều mạch ảo để kết nối tất cả các site với nhau.
- Cấu trúc này có khả năng chịu lỗi cao nhất.



Partially Meshed Topology

- Sử dụng các kết nối nhưng không đến tất cả các site

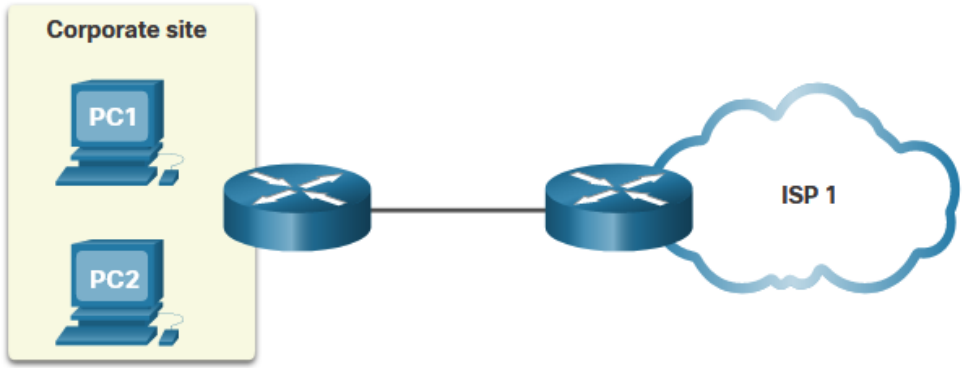


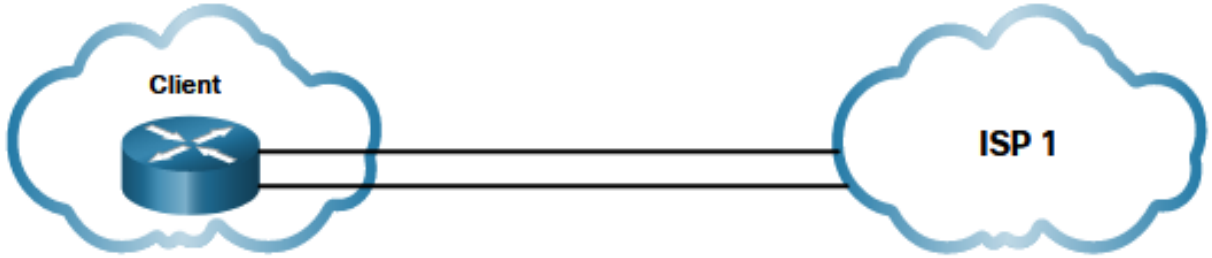
KẾT NỐI VỚI ISP

- Một khía cạnh khác của thiết kế mạng WAN là cách một cơ quan, tổ chức kết nối với internet. Một tổ chức thường ký thỏa thuận cấp độ dịch vụ (SLA) với nhà cung cấp dịch vụ. SLA phác thảo các dịch vụ dự kiến liên quan đến độ tin cậy và tính khả dụng của kết nối.
- Một nhà cung cấp dịch vụ sở hữu và đảm bảo duy trì kết nối vật lý và thiết bị giữa nhà cung cấp và khách hàng.
- Thông thường, một tổ chức sẽ chọn một kết nối WAN:
  - Single-homed, dual-homed, Multihomed, Dual-multihomed

KẾT NỐI VỚI ISP

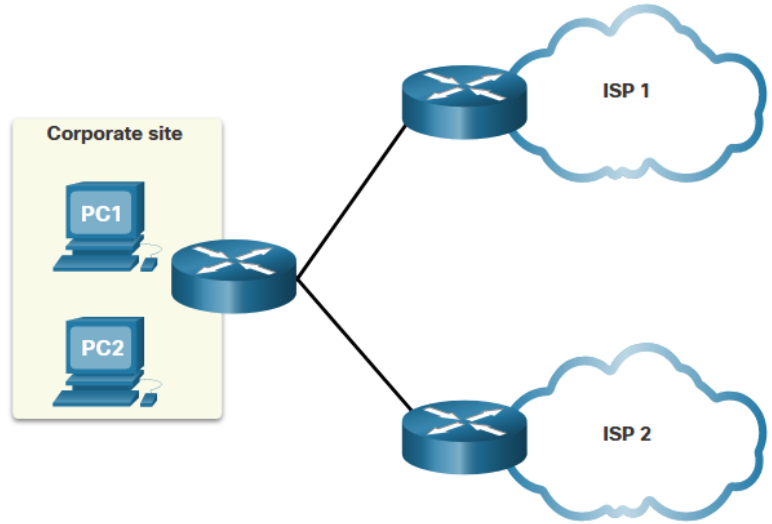
- Single-homed - Kết nối dơn với một nhà cung cấp dịch vụ ISP. Không cung cấp dự phòng và là giải pháp ít tốn kém nhất.
- Dual-homed - Kết nối với cùng một ISP bằng hai liên kết. Cung cấp cả dự phòng và cân bằng tải. Tuy nhiên, tổ chức sẽ mất kết nối internet nếu ISP gặp sự cố ngừng hoạt động.

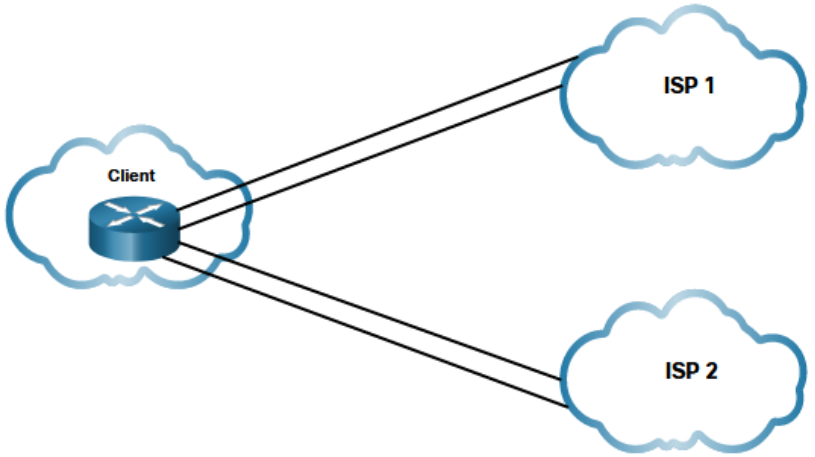




KẾT NỐI VỚI ISP

- Multihomed - Máy khách kết nối với hai ISP khác nhau. Thiết kế này cung cấp khả năng dự phòng tăng lên và cho phép cân bằng tải, nhưng nó có thể tốn kém.
- Dual-multihomed - là cấu trúc liên kết có khả năng phục hồi tốt nhất trong số bốn mô hình được hiển thị. Máy khách kết nối với các liên kết dự phòng tới nhiều ISP. Cấu trúc liên kết này cung cấp dự phòng nhiều nhất có thể. Đó là lựa chọn đắt nhất trong bốn.





CHƯƠNG 4: CÔNG NGHỆ MẠNG WAN

- 1. Mục đích mạng WAN
- 2. Hoạt động của mạng WAN
- 3. Công nghệ mạng riêng ảo VPN

HOẠT ĐỘNG CỦA MẠNG WAN
WAN STANDARDS

Các tiêu chuẩn mạng WAN được xác định và quản lý bởi một số cơ quan tổ chức, bao gồm:

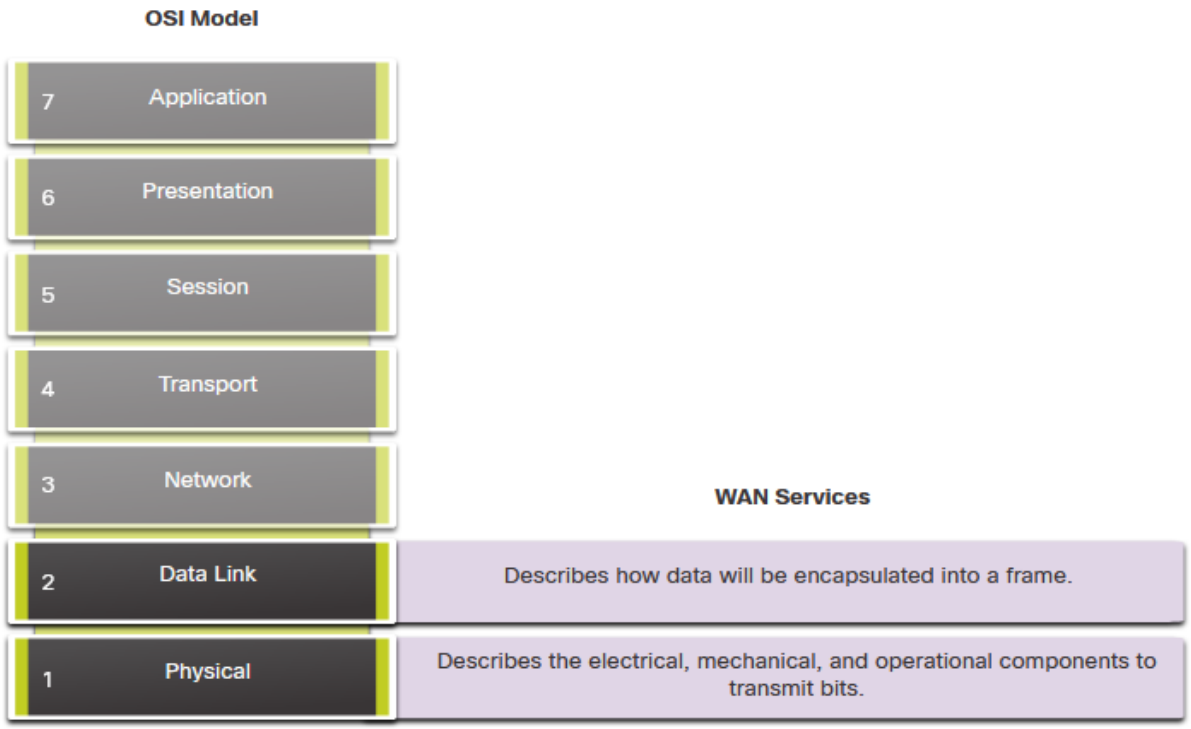
- TIA/EIA (Telecommunications Industry Association and Electronic Industries Alliance) - Hiệp hội Công nghiệp Viễn thông và Liên minh Công nghiệp Điện tử
- ISO (International Organization for Standardization) - Tổ chức tiêu chuẩn hóa quốc tế
- IEEE (Institute of Electrical and Electronics Engineers) - Viện Kỹ sư Điện và Điện tử

WANS IN THE OSI MODEL

Hầu hết các tiêu chuẩn WAN đều tập trung vào lớp vật lý và lớp liên kết dữ liệu.

Giao thức lớp 1:

- SDH (Synchronous Digital Hierarchy) - Hệ thống truyền dẫn số đồng bộ.
- SONET (Synchronous Optical Networking) - Mạng quang đồng bộ.
- DWDM (Dense Wavelength Division Multiplexing) - Ghép kênh phân chia theo bước sóng.



SDH, SONET, and DWDM

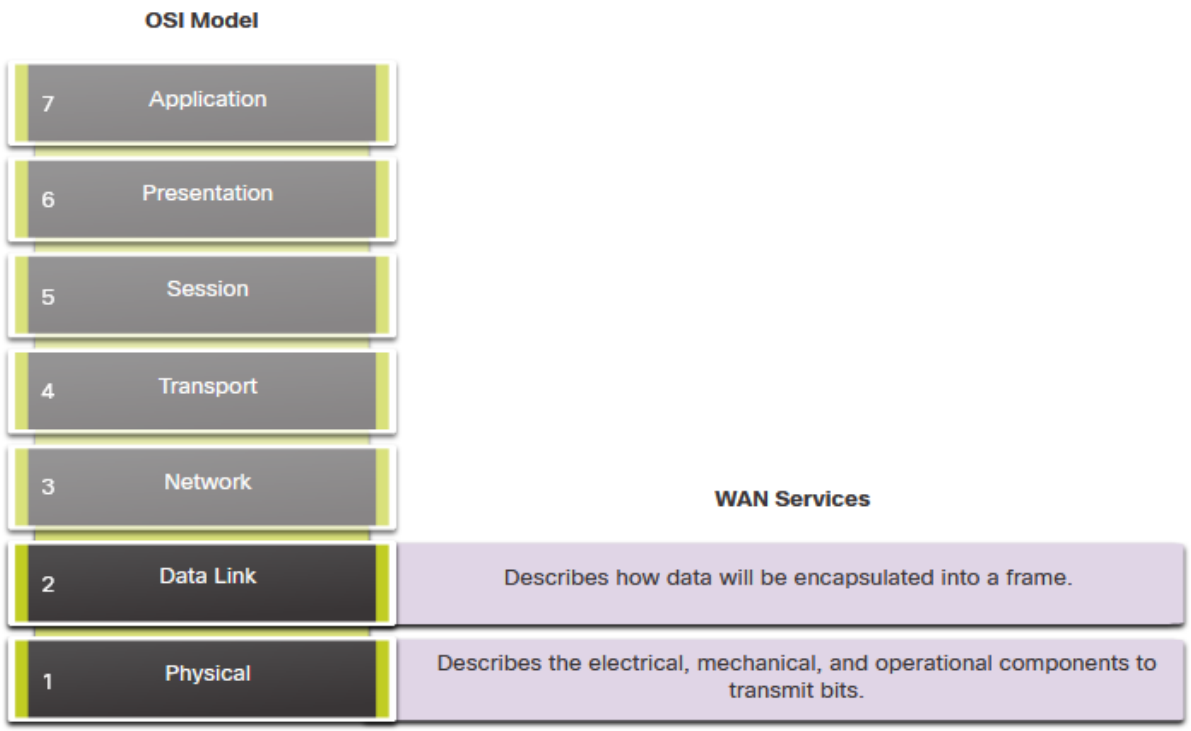
Sử dụng đường truyền cáp quang theo kết nối điểm điểm để truyền dữ liệu. Có hai tiêu chuẩn sợi quang OSI lớp 1 dành cho các nhà cung cấp dịch vụ:

- SDH - Hệ thống phân cấp kỹ thuật số đồng bộ (SDH) là tiêu chuẩn toàn cầu để truyền dữ liệu qua cáp quang.
- SONET - Mạng quang đồng bộ (SONET) là tiêu chuẩn Bắc Mỹ cung cấp các dịch vụ giống như SDH.
- SDH/SONET xác định cách truyền nhiều thông tin liên lạc dữ liệu, thoại và video qua sợi quang sử dụng điốt laze hoặc điốt phát quang (LED) ở khoảng cách xa.
- Ghép kênh phân chia theo bước sóng dày đặc (DWDM) là một công nghệ mới hơn giúp tăng khả năng mang dữ liệu của SDH và SONET bằng cách gửi đồng thời nhiều luồng dữ liệu (ghép kênh) sử dụng các bước sóng ánh sáng khác nhau.

WANS IN THE OSI MODEL

Giao thức lớp 2

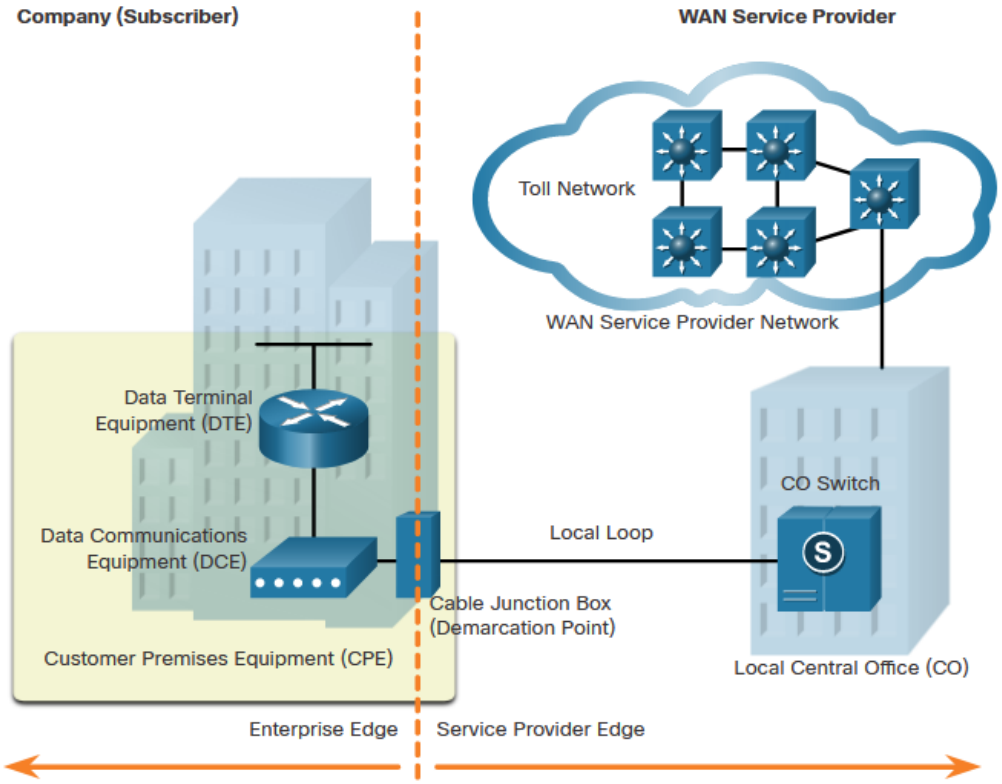
- Băng thông rộng (DSL và Cáp)
- Không dây (Wireless)
- Ethernet WAN (Metro Ethernet)
- Chuyển mạch nhãn đa giao thức (MPLS - Multiprotocol Label Switching)
- Giao thức PPP (Point-to-Point) (ít sử dụng)
- Giao thức HDLC (High-Level Data Link Control) (ít sử dụng)
- Chuyển tiếp khung Frame Relay (cũ)
- Chuyển mạch tế bào ATM (Asynchronous Transfer Mode) (cũ)



COMMON WAN TERMINOLOGY

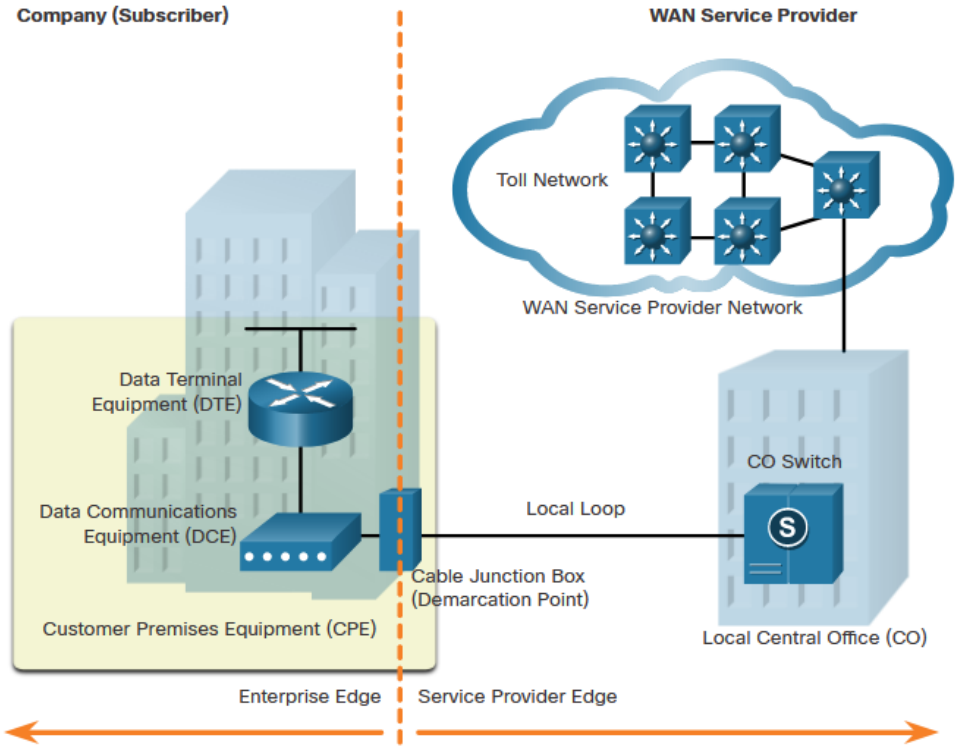
Có các thuật ngữ cụ thể được sử dụng để mô tả các kết nối WAN giữa người đăng ký (tức là công ty/khách hàng) và nhà cung cấp dịch vụ WAN.

WAN Term	Description
Data Terminal Equipment (DTE)	Thiết bị kết nối mạng LAN của thuê bao với thiết bị liên lạc WAN
Data Communications Equipment (DCE)	Thiết bị dùng để giao tiếp với nhà cung cấp
Customer Premises Equipment (CPE)	Đây là thiết bị DTE và DCE nằm ở phía doanh nghiệp
Point-of-Presence (POP)	Điểm mà thuê bao kết nối với mạng của nhà cung cấp dịch vụ
Demarcation Point (DP)	Vị trí thực tế trong tòa nhà hoặc khu phức hợp chính thức ngăn cách CPE khỏi thiết bị của nhà cung cấp dịch vụ.



COMMON WAN TERMINOLOGY (CONT.)

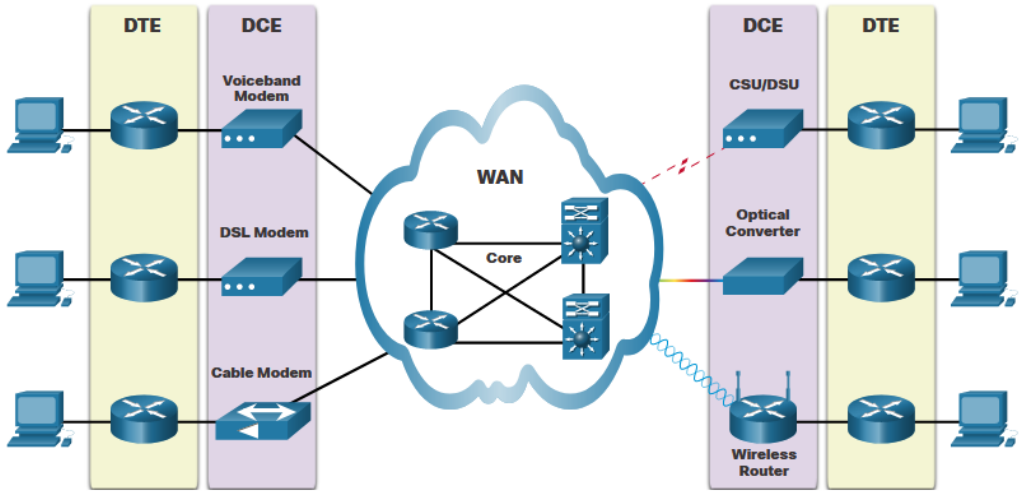
WAN Term	Description
Local Loop (last mile)	Cáp đồng hoặc cáp quang kết nối CPE với CO của nhà cung cấp dịch vụ
Central office (CO)	Cơ sở hoặc tòa nhà của nhà cung cấp dịch vụ địa phương kết nối CPE với mạng của nhà cung cấp
Toll network	Bao gồm các đường truyền thông tin liên lạc kỹ thuật số, và các thiết bị mạng có chức năng chuyển tiếp dữ liệu từ khách hang đến mạng Backhaul.
Backhaul network	Mạng trung chuyển, kết nối nhiều nút mạng Toll đến mạng Backbone.
Backbone network	Các mạng lớn, dung lượng cao được sử dụng để kết nối các mạng của nhà cung cấp dịch vụ và để tạo một mạng dự phòng



WAN DEVICES

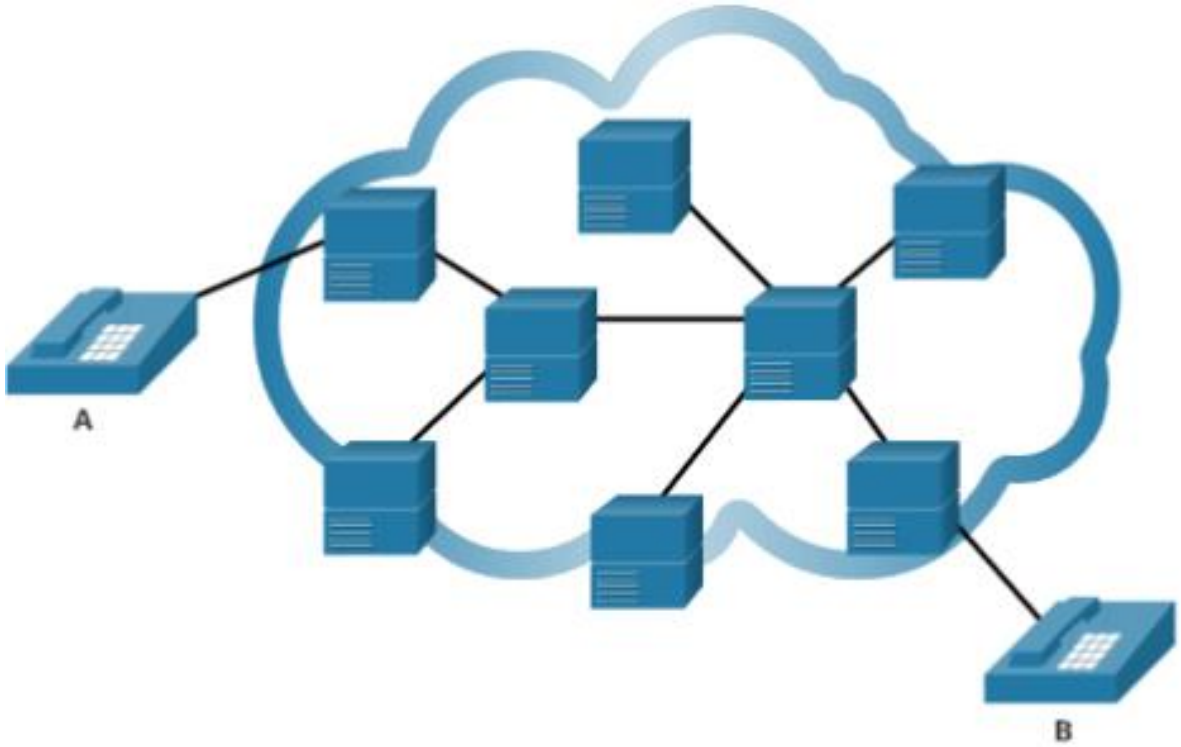
Có nhiều loại thiết bị dành riêng cho môi trường WAN.

WAN Device	Description
Voiceband Modem	Dial-up modem – sử dụng đường dây điện thoại (thiết bị cũ)
DSL Modem / Cable Modem	Được gọi chung là modem băng thông rộng, những modem kỹ thuật số tốc độ cao này kết nối với bộ định tuyến DTE bằng Ethernet.
CSU/DSU (Channel Service Unit/Data Service Unit)	Kênh thuê riêng kỹ thuật số yêu cầu CSU và DSU. Nó kết nối một thiết bị kỹ thuật số với một đường dây kỹ thuật số..
Optical Converter	Kết nối sợi quang với cáp đồng và chuyển đổi tín hiệu quang thành xung điện.
Wireless Router / Access Point	Các thiết bị được sử dụng để kết nối không dây với nhà cung cấp mạng WAN.
WAN Core devices	Đường trục WAN bao gồm nhiều bộ định tuyến tốc độ cao và bộ chuyển mạch lớp 3.



CIRCUIT-SWITCHED COMMUNICATION

- Mạng chuyển mạch kênh thiết lập một mạch (hoặc kênh) chuyên dụng giữa các điểm cuối trước khi người dùng có thể truyền thông.
- Thiết lập kết nối ảo chuyên dụng thông qua mạng của nhà cung cấp dịch vụ trước khi có thể bắt đầu liên lạc.
- Tất cả các giao tiếp sử dụng cùng một đường dẫn. Hai loại công nghệ WAN chuyển mạch kênh phổ biến nhất là mạng điện thoại chuyển mạch công cộng (PSTN) và Mạng kỹ thuật số dịch vụ tích hợp kế thừa (ISDN).

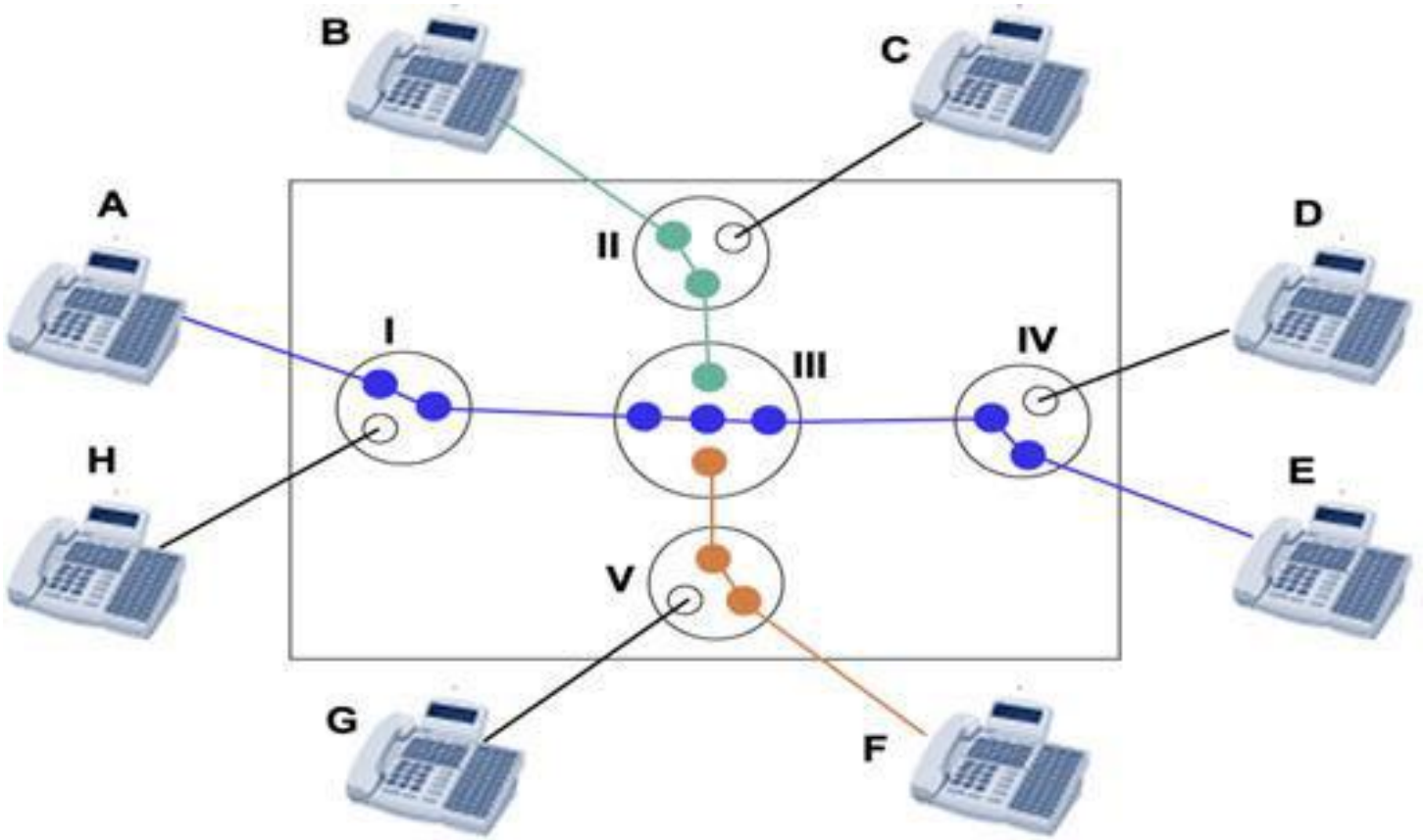


KỸ THUẬT CHUYỂN MẠCH KÊNH

Có hai tùy chọn chuyển mạch kênh truyền thống:

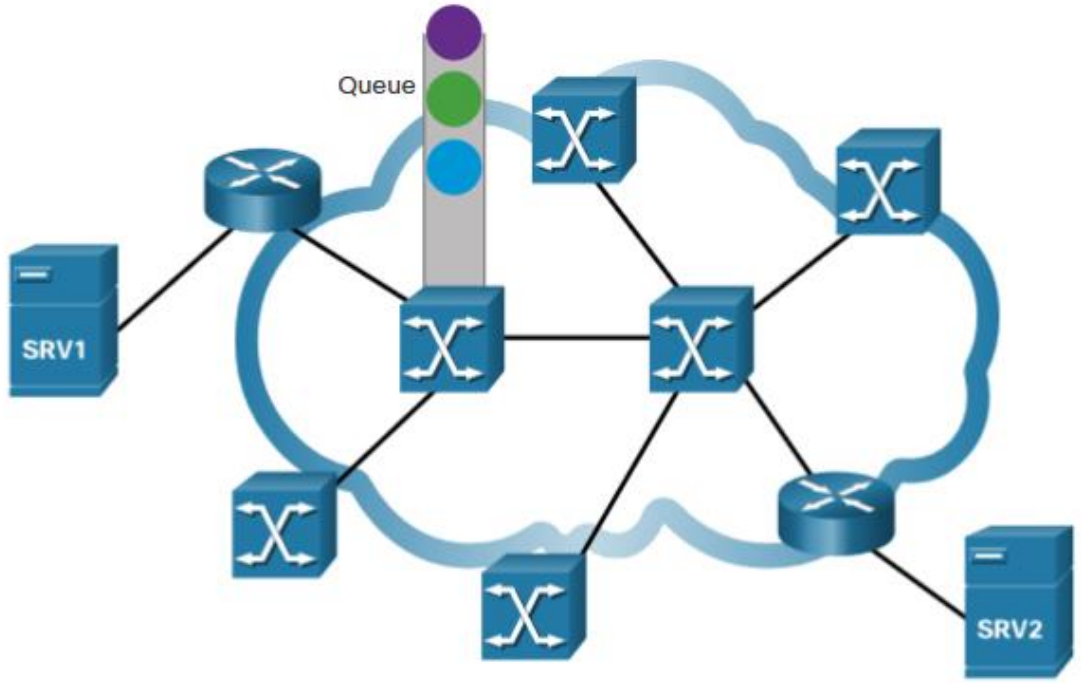
- Mạng điện thoại dịch vụ công cộng (PSTN): Truy cập WAN quay số sử dụng PSTN làm kết nối WAN của nó. Các vòng lặp cục bộ truyền thống có thể vận chuyển dữ liệu máy tính nhị phân qua mạng điện thoại thoại bằng modem băng tần thoại. Các đặc điểm vật lý của vòng lặp cục bộ và kết nối của nó với PSTN giới hạn tốc độ của tín hiệu dưới 56 kbps.
- Mạng kỹ thuật số dịch vụ tích hợp (ISDN) ISDN là công nghệ chuyển mạch cho phép vòng lặp cục bộ PSTN mang tín hiệu kỹ thuật số. Điều này cung cấp các kết nối chuyển đổi dung lượng cao hơn so với truy cập quay số. ISDN cung cấp tốc độ dữ liệu từ 45 Kbps đến 2,048 Mbps.

KỸ THUẬT CHUYỂN MẠCH KÊNH



PACKET-SWITCHED COMMUNICATION

- ❖ Truyền dữ liệu qua mạng được thực hiện phổ biến nhất bằng cách sử dụng kỹ thuật chuyển mạch gói.
- ➢ Phân đoạn dữ liệu lưu lượng thành các gói được định tuyến qua mạng chia sẻ.
- ➢ Ít tốn kém hơn và linh hoạt hơn nhiều so với chuyển mạch kênh.
- ❖ Các loại công nghệ WAN chuyển mạch gói phổ biến là:
- ➢ Chuyển mạch Ethernet WAN (Metro Ethernet),
- ➢ Chuyển mạch nhãn đa giao thức (MPLS)
- ➢ Chuyển mạch khung Frame Relay
- ➢ Chuyển mạch không đồng bộ (ATM).



KỸ THUẬT CHUYỂN MẠCH GÓI

Có hai tùy chọn chuyển mạch kênh:

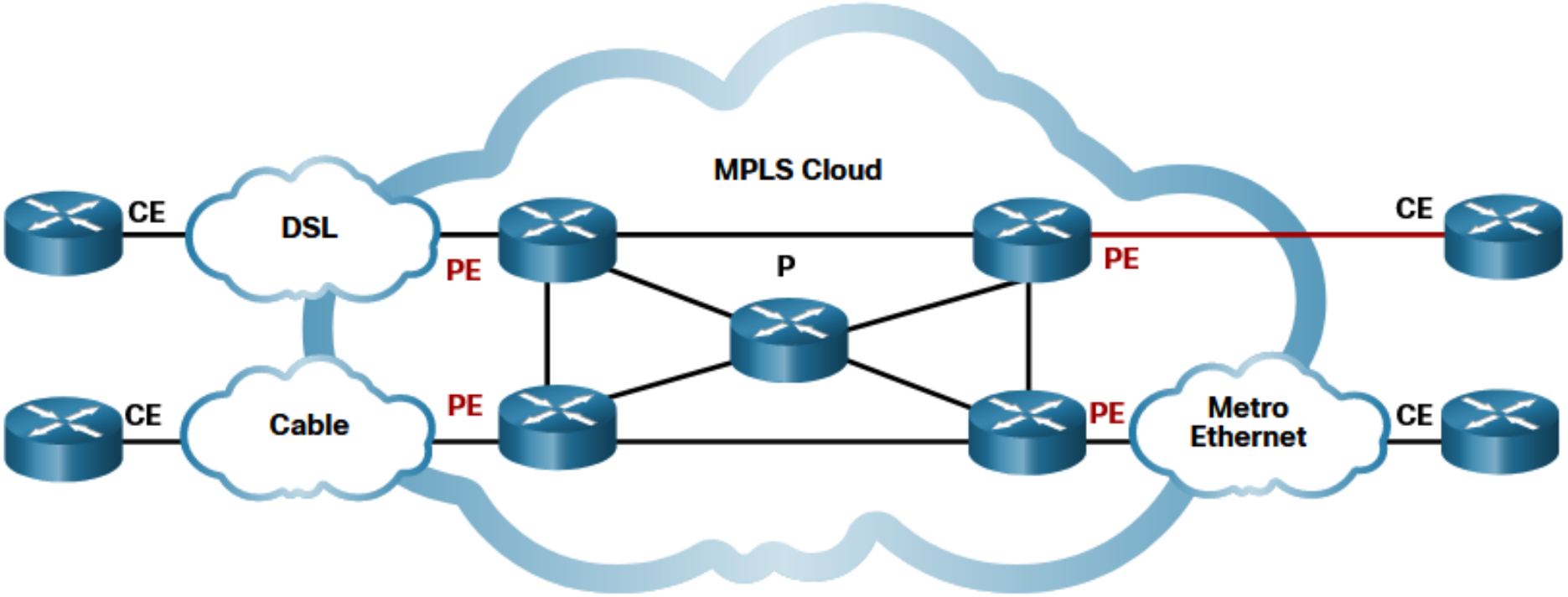
- Chuyển mạch khung Frame Relay: là công nghệ WAN đa truy cập lớp 2 đơn giản được sử dụng để kết nối các mạng LAN doanh nghiệp. Frame Relay tạo ra các PVC được xác định duy nhất bằng mã định danh kết nối liên kết dữ liệu (DLCI).
- Chế độ truyền không đồng bộ (ATM): Công nghệ Chế độ truyền không đồng bộ (ATM) có khả năng truyền giọng nói, video và dữ liệu qua các mạng riêng và mạng công cộng. ATM được xây dựng trên kiến trúc dựa trên tế bào hơn là kiến trúc dựa trên khung. Tế bào ATM luôn có độ dài cố định là 53 byte.

CHUYỂN MẠCH NHÃN ĐA GIAO THỨC MPLS

- Chuyển mạch nhãn đa giao thức (MPLS) là công nghệ định chuyển mạch WAN của nhà cung cấp dịch vụ hiệu suất cao để kết nối các máy khách mà không cần quan tâm đến phương thức truy cập hoặc tải trọng.
- MPLS hỗ trợ nhiều phương thức truy cập máy khách (ví dụ: Ethernet, DSL, Cáp, Frame Relay).
- MPLS có thể đóng gói tất cả các loại giao thức bao gồm lưu lượng IPv4 và IPv6.
- Bộ định tuyến MPLS có thể là bộ định tuyến biên khách hàng (CE), bộ định tuyến biên nhà cung cấp (PE) hoặc bộ định tuyến nhà cung cấp nội bộ (P).
- Các bộ định tuyến MPLS là các bộ định tuyến chuyển mạch nhãn (LSR).

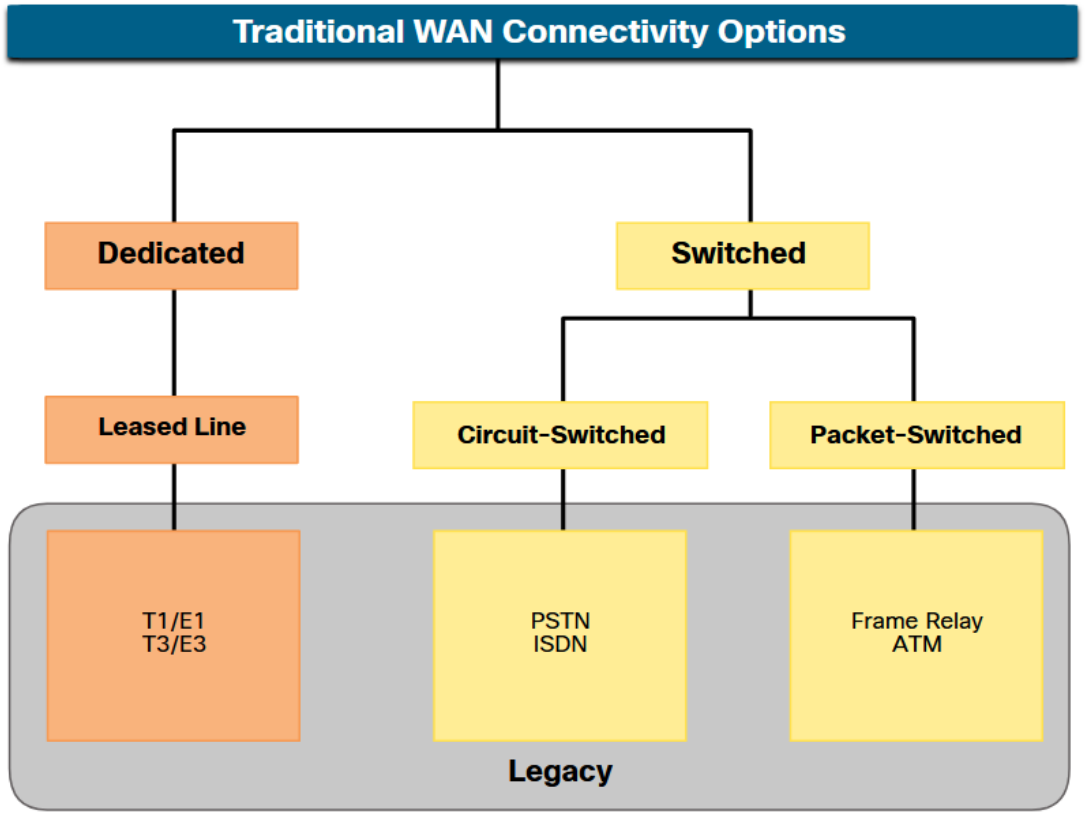
CHUYỂN MẠCH NHÃN ĐA GIAO THỨC MPLS

- Chúng gắn nhãn vào các gói mà sau đó được sử dụng bởi các bộ định tuyến MPLS khác để chuyển tiếp lưu lượng.
- MPLS cũng cung cấp các dịch vụ hỗ trợ QoS, kỹ thuật lưu lượng, dự phòng và VPN.



CÁC KẾT NỐI TRONG MẠNG WAN

- Để hiểu các mạng WAN ngày nay, cần biết chúng bắt đầu từ đâu.
- Khi mạng LAN xuất hiện vào những năm 1980, các tổ chức bắt đầu nhận thấy nhu cầu kết nối với các địa điểm khác.
- Để làm như vậy, họ cần mạng của họ kết nối với mạng vòng cục bộ của nhà cung cấp dịch vụ.
- Điều này được thực hiện bằng cách sử dụng các đường dây chuyên dụng hoặc bằng cách sử dụng các dịch vụ chuyển đổi từ nhà cung cấp dịch vụ.

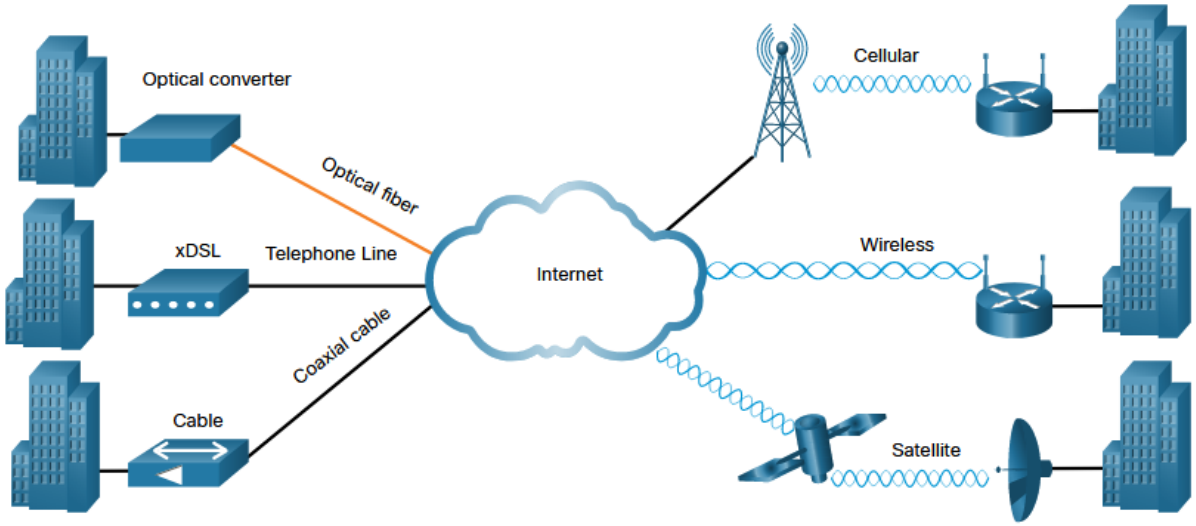


CÁC KẾT NỐI TRONG MẠNG WAN

- Đường truyền điểm-điểm (point to point) có thể được thuê từ nhà cung cấp dịch vụ và được gọi là "đường thuê riêng".
- Đường dây thuê riêng có các dung lượng cố định khác nhau và thường được định giá dựa trên băng thông cần thiết và khoảng cách giữa hai điểm kết nối.
- Có hai hệ thống được sử dụng để xác định dung lượng kỹ thuật số của liên kết nối tiếp phương tiện truyền thông đồng:
- T-carrier - Được sử dụng ở Bắc Mỹ, T-carrier cung cấp các liên kết T1 hỗ trợ băng thông lên tới 1,544 Mbps và các liên kết T3 hỗ trợ băng thông lên tới 43,7 Mbps.
- E-carrier – Được sử dụng ở Châu Âu, E-carrier cung cấp liên kết E1 hỗ trợ băng thông lên tới 2,048 Mbps và liên kết E3 hỗ trợ băng thông lên tới 34,368 Mbps.

KẾT NỐI WAN HIỆN ĐẠI

- Mạng WAN hiện đại có nhiều tùy chọn kết nối hơn mạng WAN truyền thống.
- Các doanh nghiệp hiện yêu cầu các tùy chọn kết nối mạng WAN nhanh hơn và linh hoạt hơn.
- Các tùy chọn kết nối WAN truyền thống đã nhanh chóng bị từ chối sử dụng vì chúng không còn khả dụng, quá đắt hoặc có bang thông giới hạn.

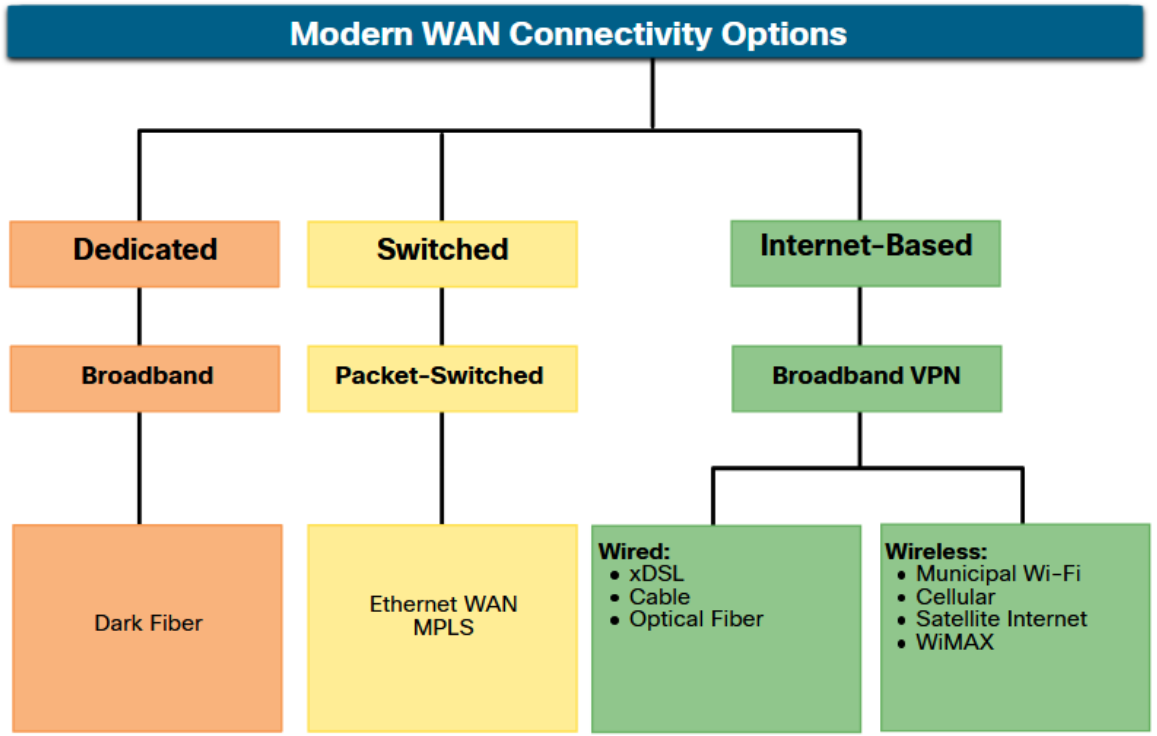


Hình này hiển thị các kết nối vòng lặp cục bộ hiện nay.

KẾT NỐI WAN HIỆN ĐẠI

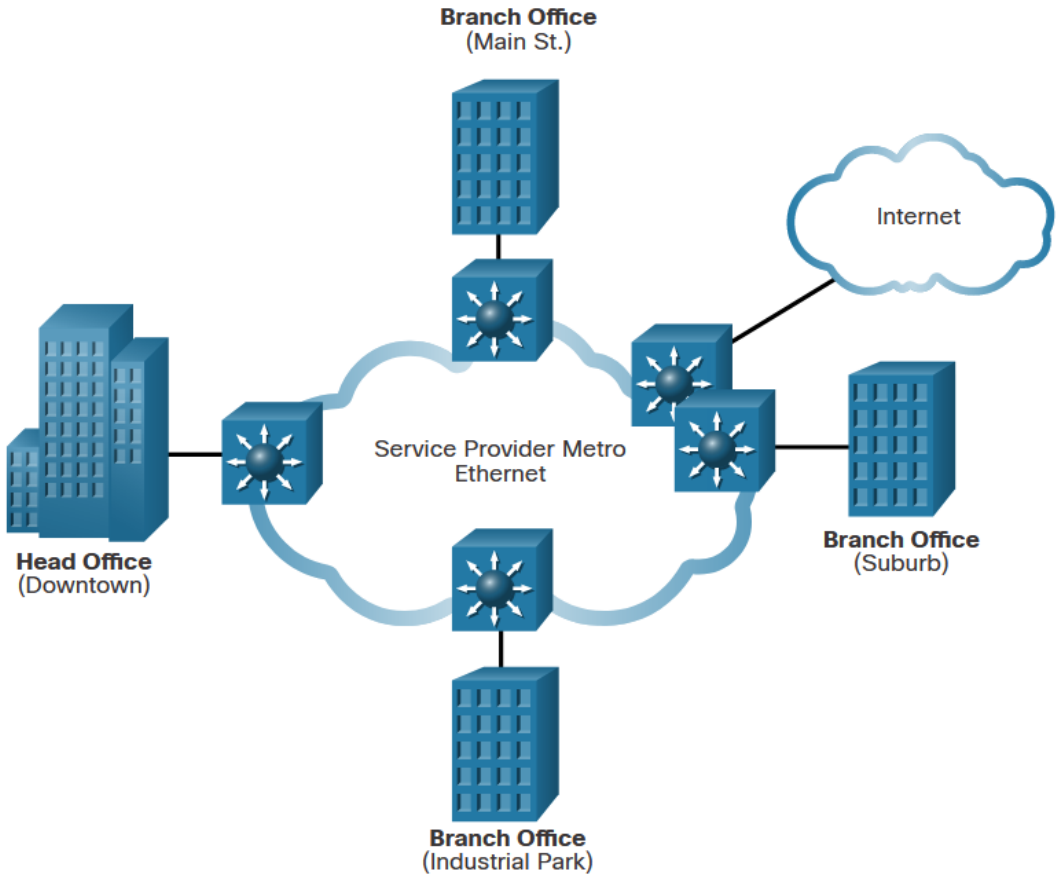
Các kế nối hiện đại sử dụng dịch vụ băng thông rộng dùng cáp quang từ nhà cung cấp ISP để kết nối trực tiếp các địa điểm từ xa với nhau.

- ❖ Có thể thuê đường truyền từ nhà cung cấp.
- ❖ Chuyển mạch gói Metro Ethernet – Thay thế nhiều tùy chọn WAN truyền thống. MPLS – Cho phép các trang web kết nối với nhà cung cấp bất kể công nghệ truy cập của nó.
- ❖ Băng thông rộng dựa trên Internet: Các tổ chức hiện đang sử dụng phổ biến cơ sở hạ tầng internet toàn cầu để kết nối mạng WAN.



KẾT NỐI WAN HIỆN ĐẠI - Ethernet WAN

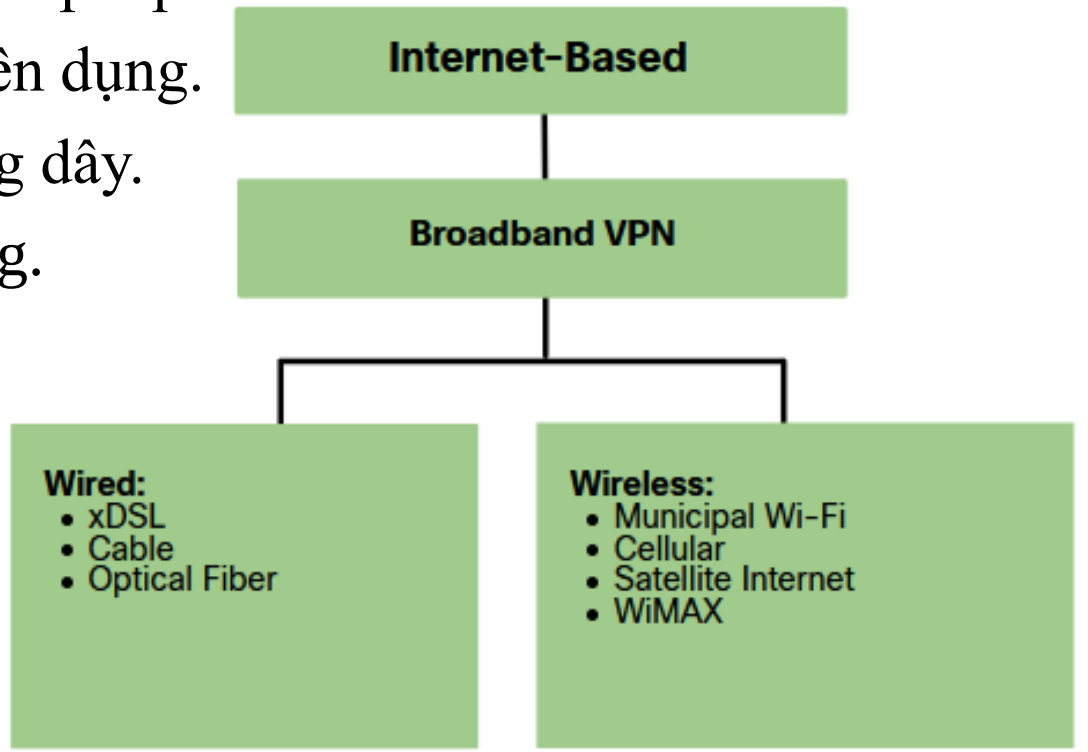
- Các nhà cung cấp dịch vụ hiện cung cấp dịch vụ Ethernet WAN sử dụng cáp quang.
- Dịch vụ Ethernet WAN có thể có nhiều tên như:
  - Ethernet đô thị (Metro E)
  - Ethernet qua MPLS (EoMPLS)
  - Dịch vụ LAN riêng ảo (VPLS)
- Có một số lợi ích đối với Ethernet WAN:
  - Giảm chi phí và quản lý
  - Dễ dàng tích hợp với các mạng hiện có
  - Năng suất kinh doanh được nâng cao



Lưu ý: Ethernet WAN đã trở nên phổ biến và hiện đang được sử dụng phổ biến để thay thế các liên kết nối tiếp truyền thống point-to-point, Frame Relay và ATM WAN.

INTERNET-BASED CONNECTIVITY

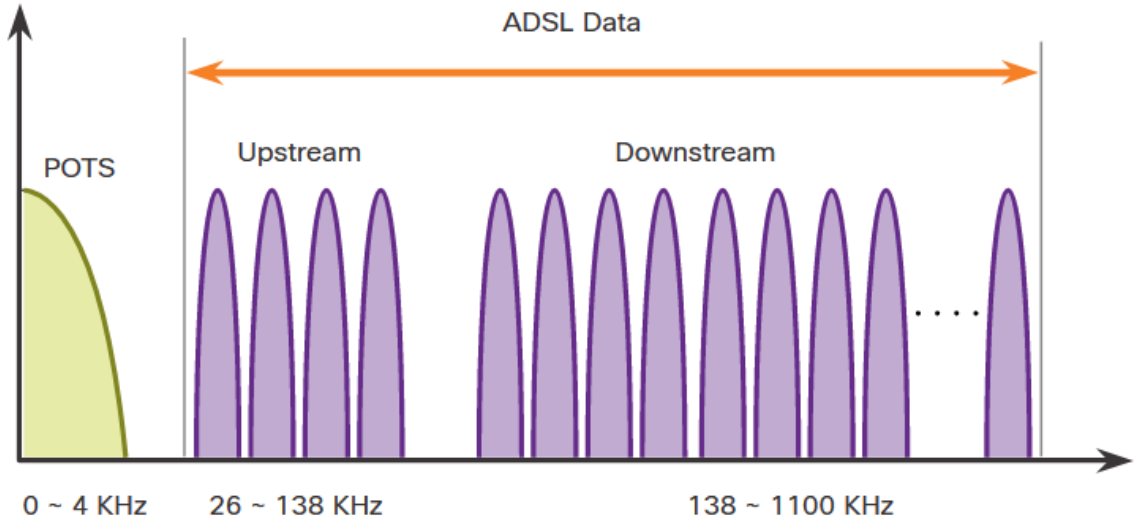
- ❖ Kết nối băng thông rộng dựa trên Internet là một giải pháp thay thế cho việc sử dụng các tùy chọn WAN chuyên dụng.
- ❖ Kết nối dựa trên Internet được chia có dây và không dây.
  - ➢ Tùy chọn có dây: Sử dụng cáp đồng hoặc cáp quang.



- ❖ Tùy chọn không dây
  - ➢ Các tùy chọn không dây ít tốn kém hơn khi triển khai so với các tùy chọn kết nối WAN khác vì chúng sử dụng sóng vô tuyến thay vì phương tiện có dây để truyền dữ liệu. Ví dụ: dịch vụ internet di động 3G/4G/5G hoặc vệ tinh.
  - ➢ Tín hiệu không dây có thể bị ảnh hưởng tiêu cực bởi các yếu tố như khoảng cách từ tháp radio, nhiễu từ các nguồn khác và thời

INTERNET-BASED CONNECTIVITY - DSL TECHNOLOGY

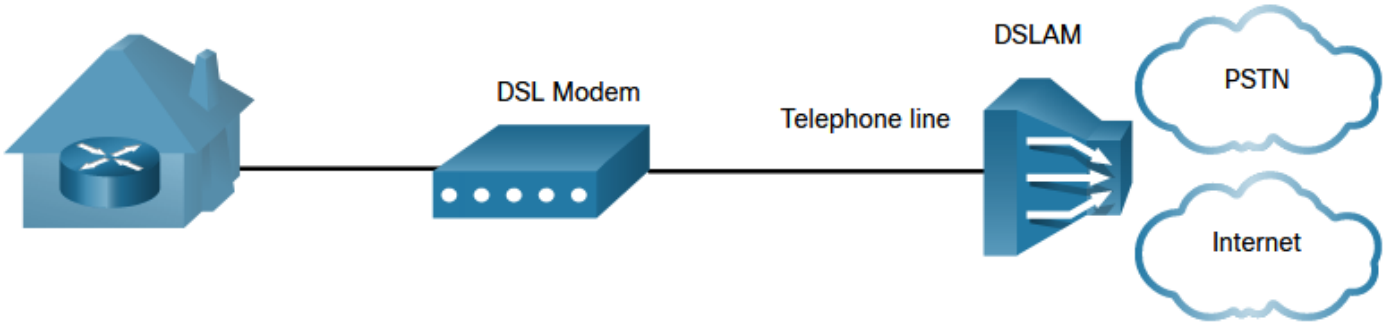
- Đường dây thuê bao kỹ thuật số (DSL) là công nghệ kết nối tốc độ cao, sử dụng các đường dây điện thoại xoắn đôi hiện có để cung cấp dịch vụ IP cho người dùng.
- DSL được phân loại thành DSL bất đối xứng (ADSL) hoặc DSL đối xứng (SDSL).
- ADSL và ADSL2+ cung cấp cho người dùng băng thông tải xuống cao hơn băng thông tải lên.
- SDSL cung cấp dung lượng như nhau theo cả hai hướng.Tốc độ truyền DSL phụ thuộc vào độ dài thực tế của vòng lặp cục bộ, loại và tình trạng của cáp.



DSL Connections

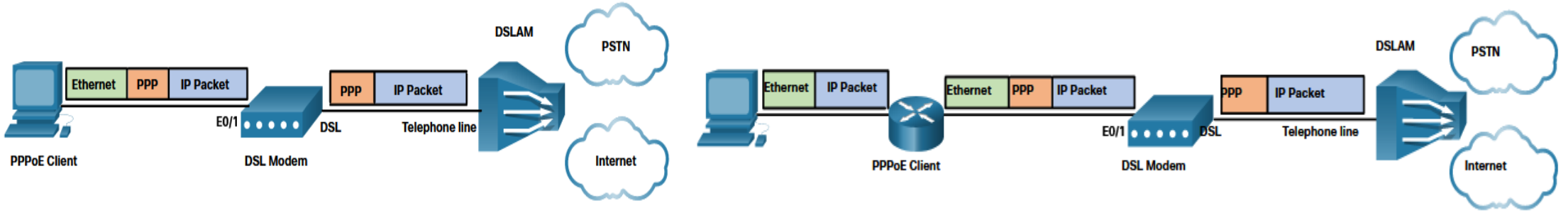
Các nhà cung cấp dịch vụ triển khai các kết nối DSL trong mạng vòng cục bộ (Local Loop). Kết nối được thiết lập giữa modem DSL và bộ ghép kênh truy cập DSL (DSLAM).

- Modem DSL chuyển đổi tín hiệu Ethernet từ thiết bị làm việc từ xa thành tín hiệu DSL, tín hiệu này được truyền tới bộ ghép kênh truy cập DSL (DSLAM) tại địa điểm của nhà cung cấp.
- DSLAM được đặt tại Văn phòng Trung tâm (CO) của nhà cung cấp và tập trung các kết nối từ nhiều thuê bao DSL.
- DSL không phải là một phương tiện chia sẻ. Mỗi người dùng có một kết nối trực tiếp riêng biệt với DSLAM. Thêm người dùng không cản trở hiệu suất.



Internet-Based Connectivity
DSL and PPP

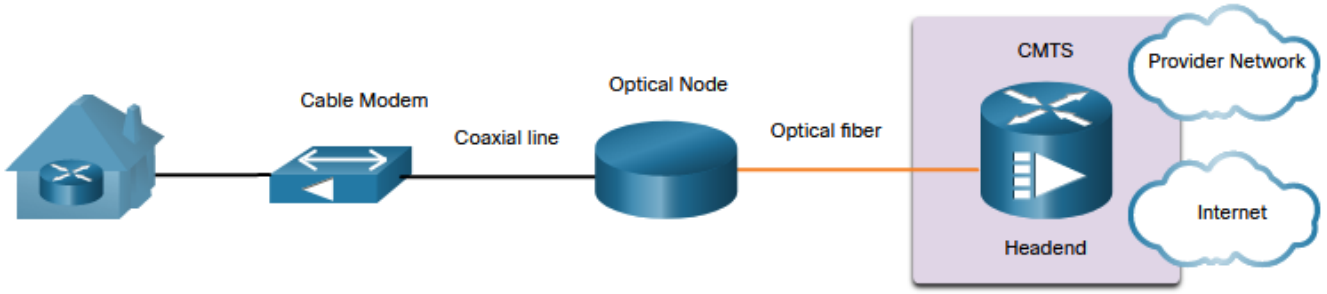
- ❖ Các ISP sử dụng PPP làm giao thức Lớp 2 cho các kết nối DSL băng thông rộng.
- ❖ PPP có thể được sử dụng để xác thực thuê bao.
- ❖ PPP có thể gán địa chỉ IPv4 public cho người dùng.
- ❖ PPP cung cấp các tính năng quản lý chất lượng liên kết.
- ❖ Có hai cách có thể triển khai PPP qua Ethernet (PPPoE):
  - ➢ Host với PPoE client - Phần mềm máy khách PPPoE giao tiếp với modem DSL sử dụng PPPoE và modem giao tiếp với ISP bằng PPP.
  - ➢ Router PPPoE client – Router là PPPoE client và nhận cấu hình từ nhà cung cấp.



Internet-Based Connectivity
Cable Technology

Công nghệ cáp là công nghệ kết nối luôn bật tốc độ cao, sử dụng cáp đồng trục của công ty truyền hình cáp để cung cấp dịch vụ IP cho người dùng.

- Thông số kỹ thuật giao diện dịch vụ dữ liệu qua cáp (DOCSIS) là tiêu chuẩn quốc tế để truyền dữ liệu băng thông cao trên hệ thống cáp hiện có.
- Nút quang chuyển đổi tín hiệu RF thành xung ánh sáng qua cáp quang.
- Phương tiện sợi quang cho phép các tín hiệu truyền đi trên một khoảng cách dài đến đầu cuối của nhà cung cấp nơi đặt Hệ thống đầu cuối modem cáp (CMTS).
- Headend chứa cơ sở dữ liệu cần thiết để cung cấp truy cập internet trong khi CMTS chịu trách nhiệm liên lạc với modem cáp.



Internet-Based Connectivity
Optical Fiber

Nhiều đô thị, thành phố và nhà cung cấp lắp đặt cáp quang đến địa điểm người dùng. Điều này thường được gọi là Fiber to the x (FTTx) và bao gồm những điều sau:

- Fiber to the Home (FTTH) - Sợi quang vươn tới ranh giới của nơi ở.
- Fiber to the Building (FTTB) - Fiber đến ranh giới của tòa nhà với kết nối cuối cùng đến không gian sống cá nhân được thực hiện thông qua các phương tiện thay thế.
- Fiber to the Node/Neighborhood (FTTN) – Cáp quang đến một nút quang giúp chuyển đổi tín hiệu quang sang định dạng chấp nhận được đối với cáp xoắn đôi hoặc cáp đồng trục đến tiền đề

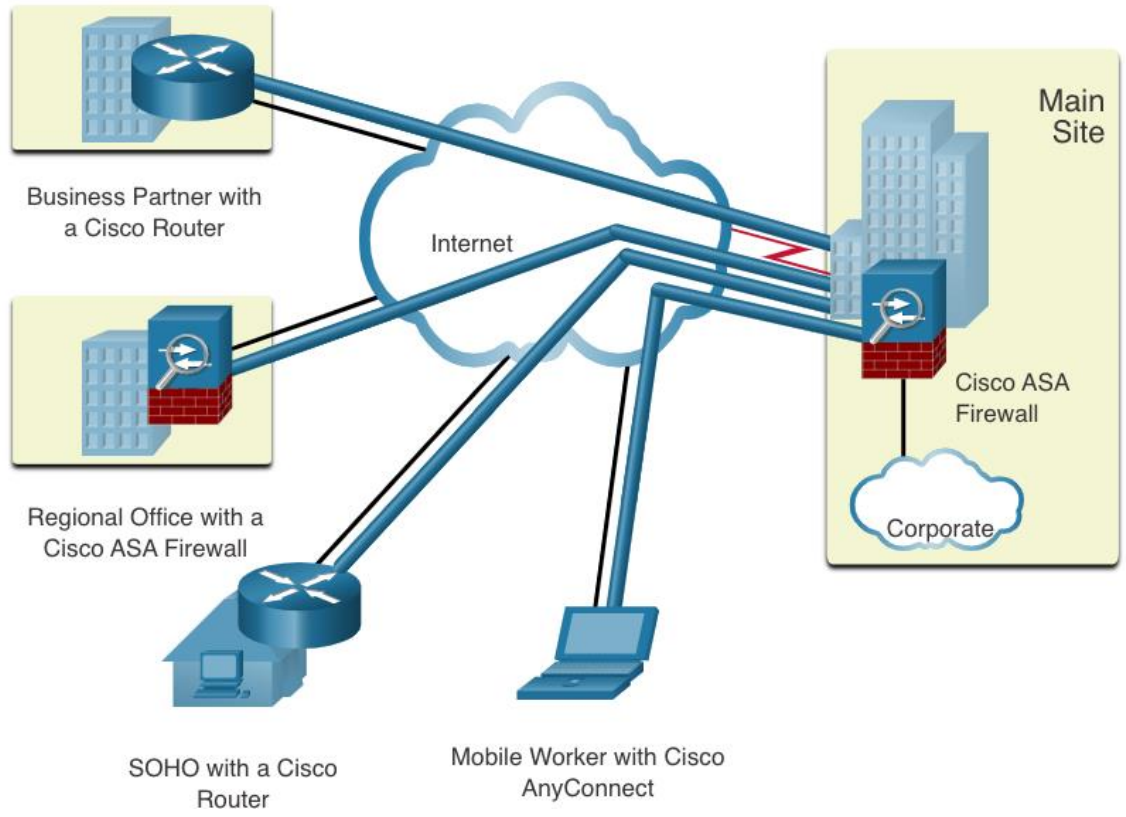
Lưu ý: FTTx có thể cung cấp băng thông cao nhất trong tất cả các tùy chọn băng thông rộng.

CHƯƠNG 4: CÔNG NGHỆ MẠNG WAN

- 1. Mục đích mạng WAN
- 2. Hoạt động của mạng WAN
- 3. Công nghệ mạng riêng ảo VPN

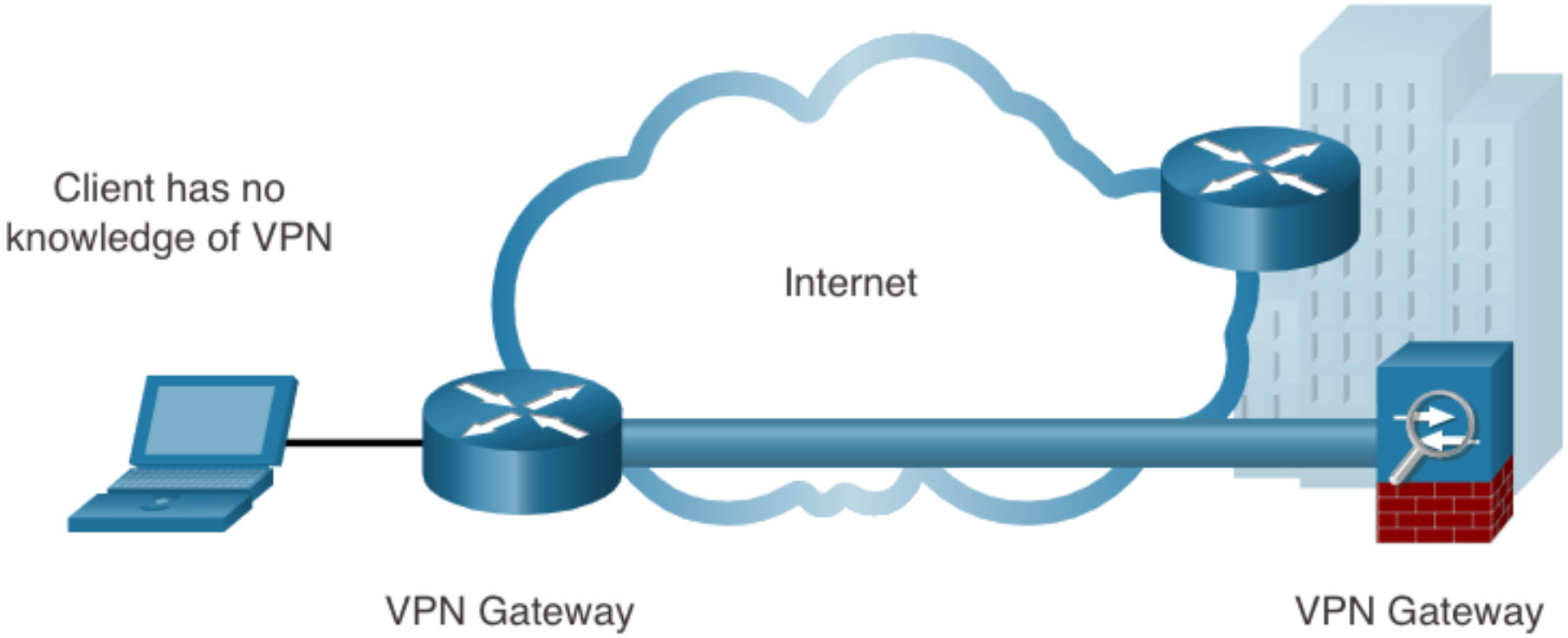
Virtual Private Networks

- Mạng riêng ảo (VPN) tạo kết nối mạng riêng thông qua mạng WAN.
- VPN là ảo ở chỗ nó mang thông tin trong mạng riêng, nhưng thông tin đó thực sự được truyền qua mạng công cộng.
- VPN là mạng riêng nhưng lưu lượng được mã hóa để giữ bí mật dữ liệu trong khi dữ liệu được truyền qua mạng công cộng.



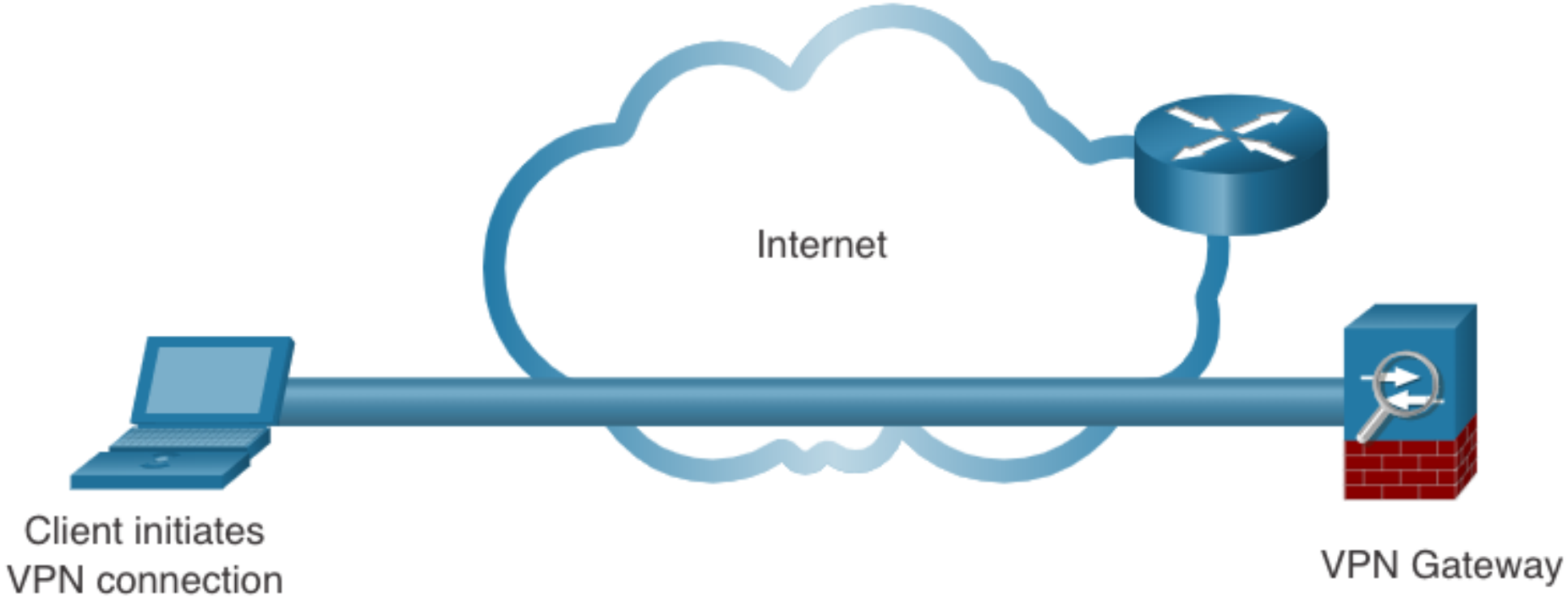
Site-to-Site and Remote Access VPNs

A site-to-site VPN là mạng riêng ảo kết nối các site ở xa (các mạng LAN) với nhau thông qua các đầu cuối VPN gateways. Luồng dữ liệu VPN chỉ được mã hoá bảo mật giữa các gateways. Các host nội bộ bên trong mạng LAN không quan tâm và không biết đang sử dụng VPN.



Site-to-Site and Remote Access VPNs (Cont.)

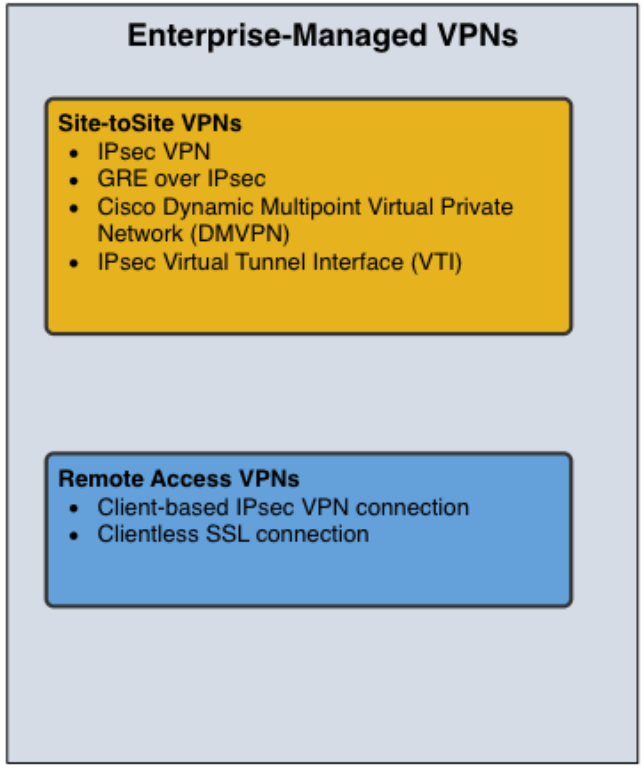
A remote-access VPN được tạo động để thiết lập kết nối an toàn giữa máy khách từ xa và thiết bị đầu cuối VPN.

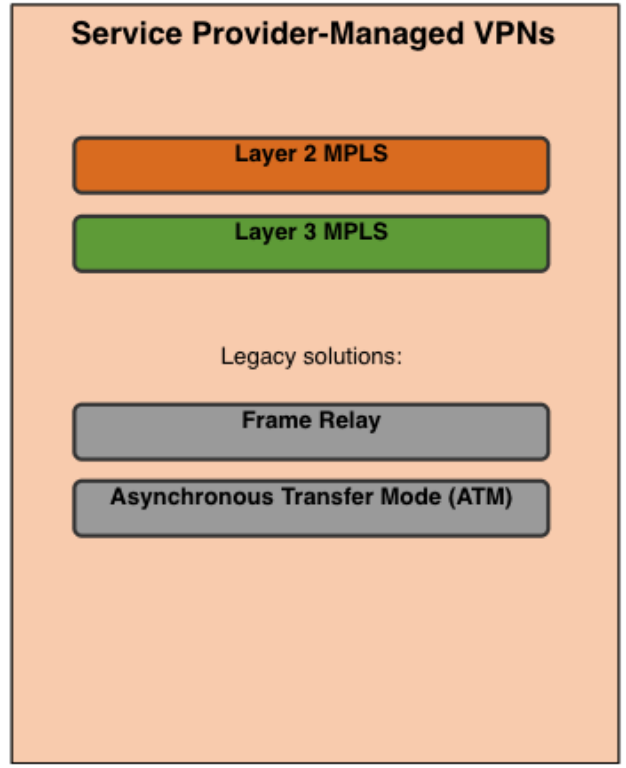


Enterprise and Service Provider VPNs

VPN có thể được quản lý và triển khai như:

- VPN doanh nghiệp - giải pháp phổ biến để bảo mật lưu lượng doanh nghiệp trên internet. VPN truy cập từ xa và site-to-site được tạo và quản lý bởi doanh nghiệp bằng IPsec và SSL VPN.
- VPN của SP - được tạo và quản lý bởi mạng của nhà cung cấp. Nhà cung sử dụng (MPLS) ở Lớp 2 hoặc Lớp 3 để tạo các kênh an toàn giữa các site của doanh nghiệp, tách biệt hiệu quả lưu lượng truy cập khỏi lưu lượng khách hàng khác.

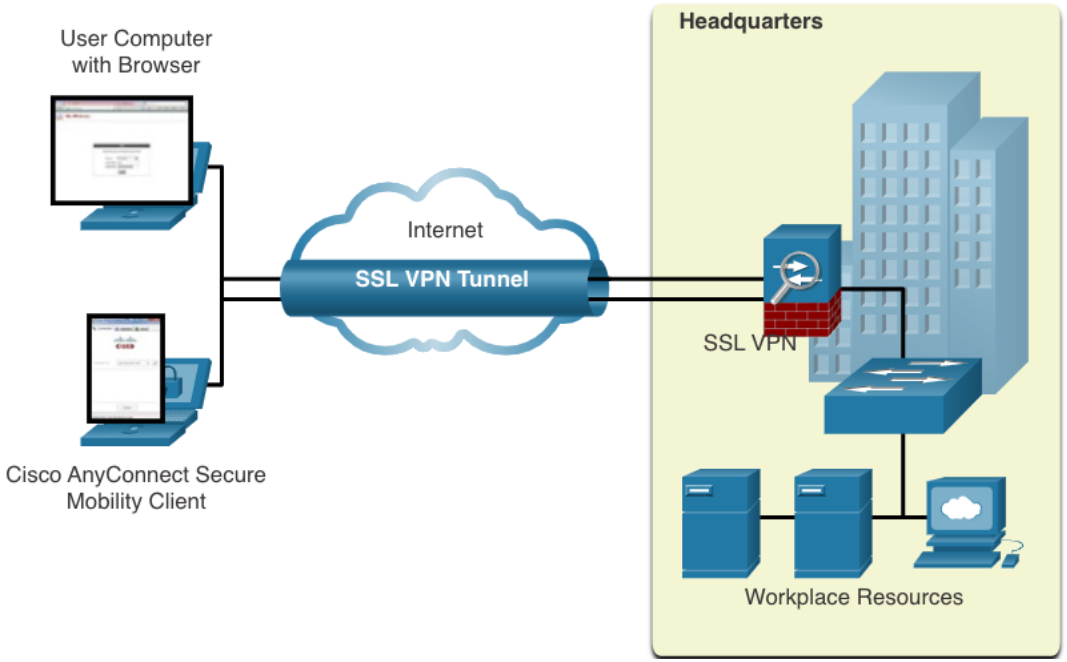




Types of VPNs

Remote-Access VPNs

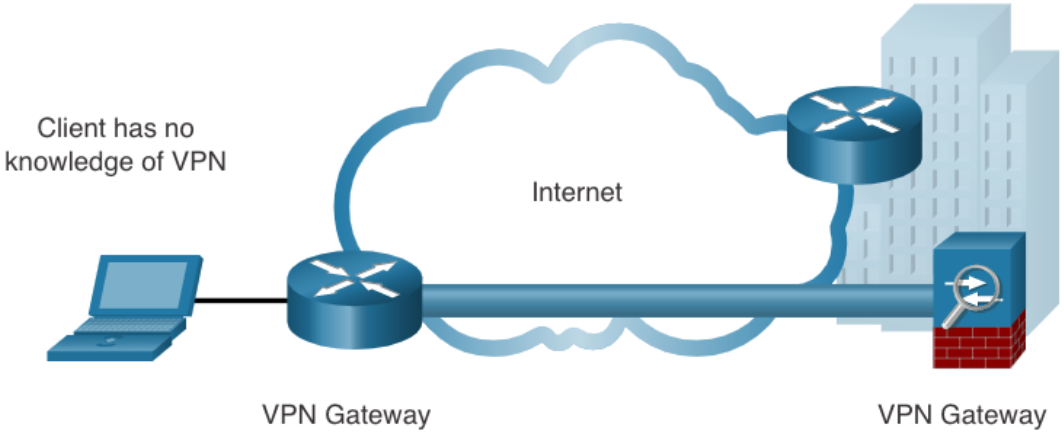
- Remote-access VPN cho phép người dùng di động và từ xa kết nối an toàn với doanh nghiệp.
- Remote-access VPN thường được người dùng kích hoạt tự động khi có yêu cầu và có thể được tạo bằng cách sử dụng IPsec hoặc SSL.
- Kết nối VPN Clientless - Kết nối được bảo mật bằng kết nối SSL của trình duyệt web.
- Kết nối VPN Client-based - Phần mềm máy khách VPN như Cisco AnyConnect phải được cài đặt trên thiết bị đầu cuối của người dùng từ xa.



Types of VPNs

Site-to-Site IPsec VPNs

- VPN site-to-site kết nối các mạng trên một mạng không đáng tin cậy như internet.
- Máy host gửi và nhận lưu lượng TCP/IP không được mã hóa bình thường thông qua cổng VPN.
- Cổng VPN đóng gói và mã hóa lưu lượng gửi đi từ một trang web và gửi lưu lượng qua đường hầm VPN đến cổng VPN tại trang đích. Cổng VPN nhận loại bỏ các tiêu đề, giải mã nội dung và chuyển tiếp gói tới máy chủ đích bên trong mạng riêng của nó.



GRE over IPsec

- Generic Routing Encapsulation (GRE) là một giao thức đường hầm VPN site-to-site không an toàn.
- Một đường hầm GRE có thể đóng gói các giao thức lớp mạng khác nhau cũng như lưu lượng multicast và lưu lượng quảng bá (broadcast).
- GRE không hỗ trợ mã hóa theo mặc định; và do đó, nó không cung cấp đường hầm VPN an toàn.
- Một gói GRE có thể được gói gọn trong một gói IPsec để chuyển tiếp nó một cách an toàn đến cổng VPN đích.
- VPN IPsec tiêu chuẩn (non-GRE) chỉ có thể tạo đường hầm an toàn cho lưu lượng truy cập unicast.
- Đóng gói GRE vào IPsec cho phép cập nhật giao thức định tuyến multicast được bảo mật thông qua VPN.

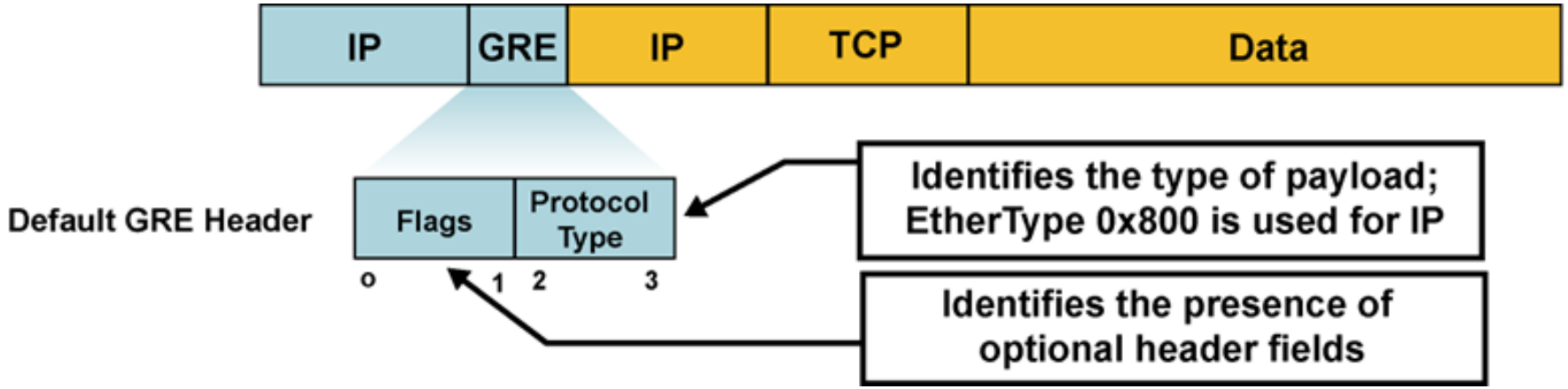
GRE over IPsec (Cont.)

Các thuật ngữ được sử dụng để mô tả việc đóng gói GRE qua đường hầm IPsec là passenger protocol, carrier protocol, and transport protocol.

Passenger protocol - Đây là gói ban đầu sẽ được GRE đóng gói. Đó có thể là gói IPv4 hoặc IPv6, bản cập nhật định tuyến, v.v.

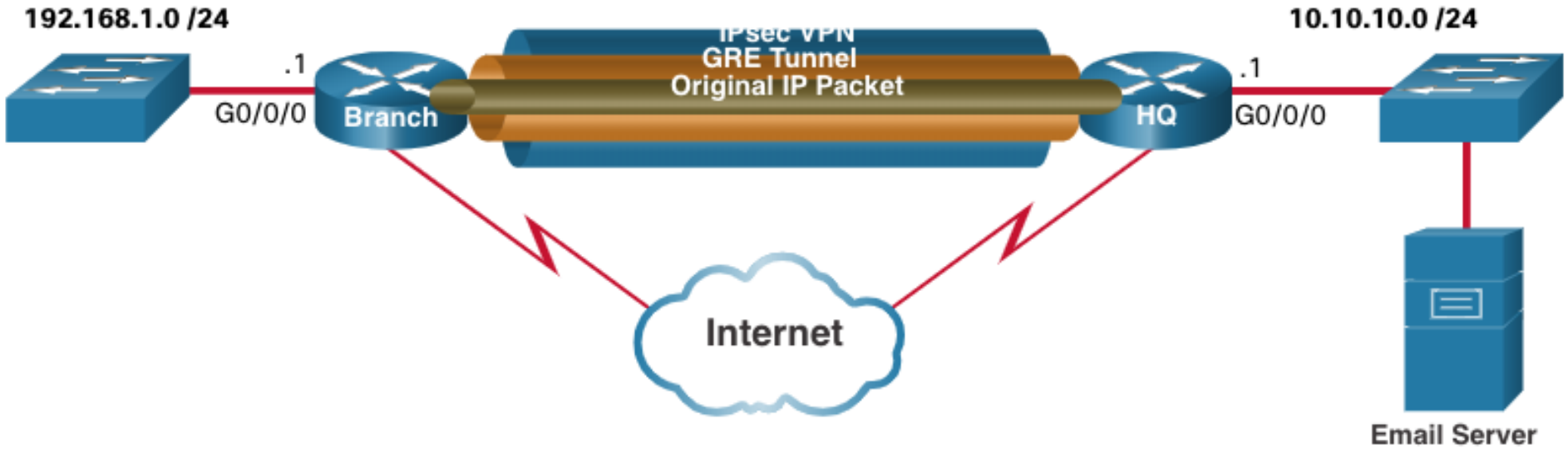
Carrier protocol – GRE là giao thức thực hiện đóng gói gói tin passenger ban đầu để vận chuyển qua đường hầm.

Transport protocol – Đây là giao thức sẽ thực sự được sử dụng để chuyển tiếp gói tin. Đây có thể là IPv4 hoặc IPv6.

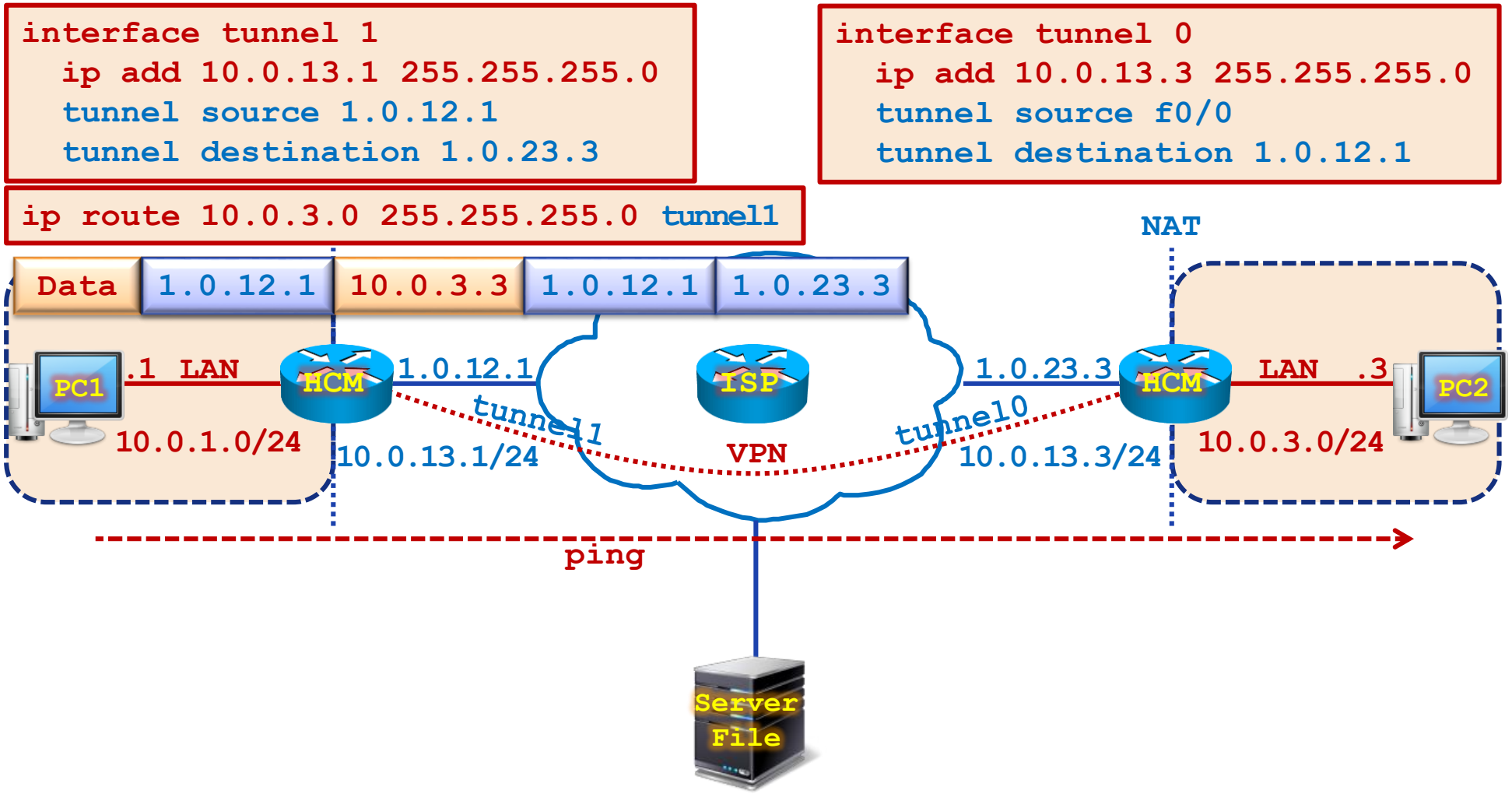


GRE over IPsec (Cont.)

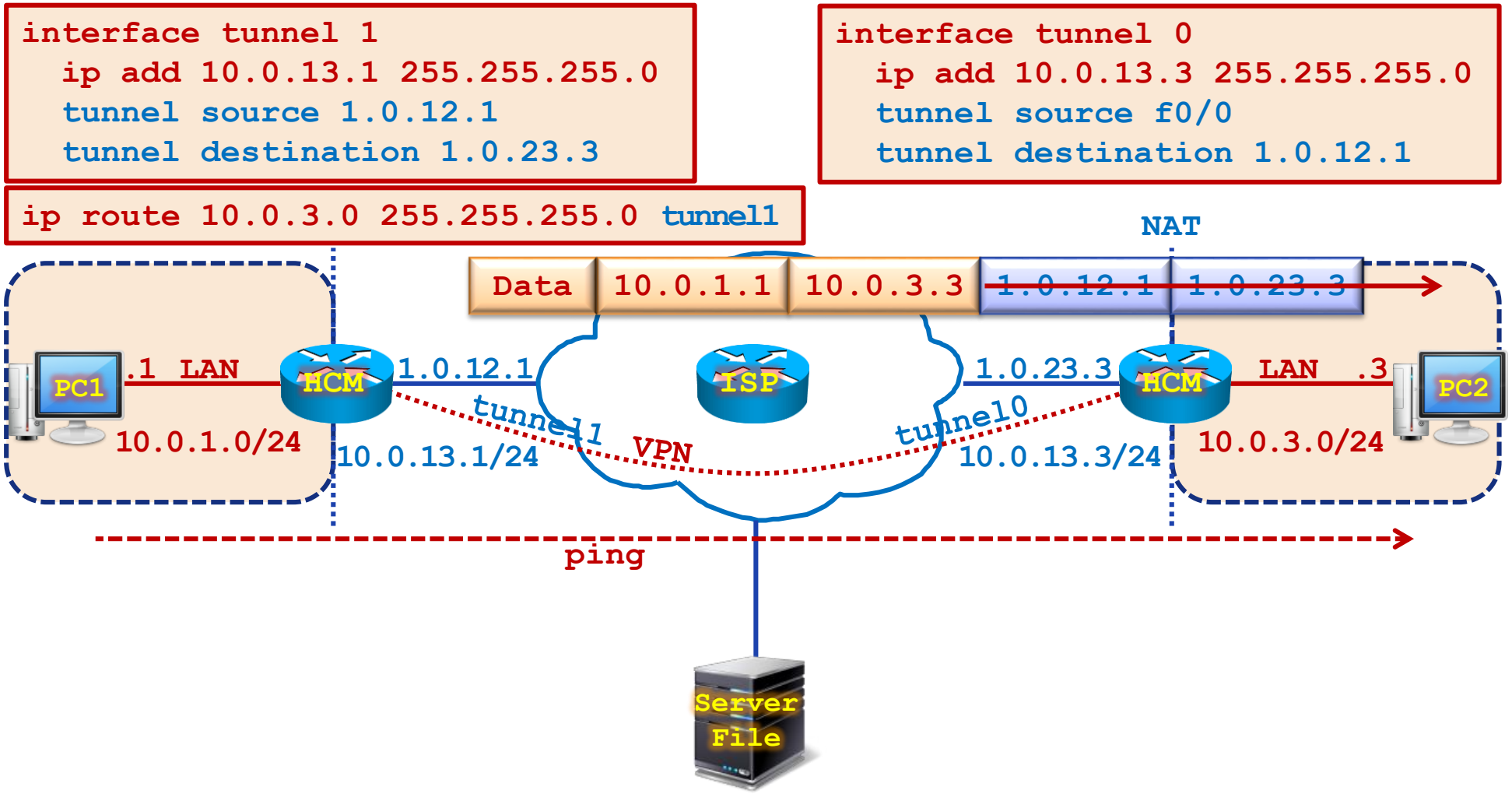
Ví dụ, Branch và HQ cần trao đổi thông tin định tuyến OSPF qua IPsec VPN. GRE over IPsec được sử dụng để hỗ trợ lưu lượng giao thức định tuyến qua IPsec VPN. Cụ thể, các gói OSPF (nghĩa là giao thức passenger) sẽ được đóng gói bởi GRE (tức là giao thức carrier) và sau đó được đóng gói trong đường hầm IPsec VPN.



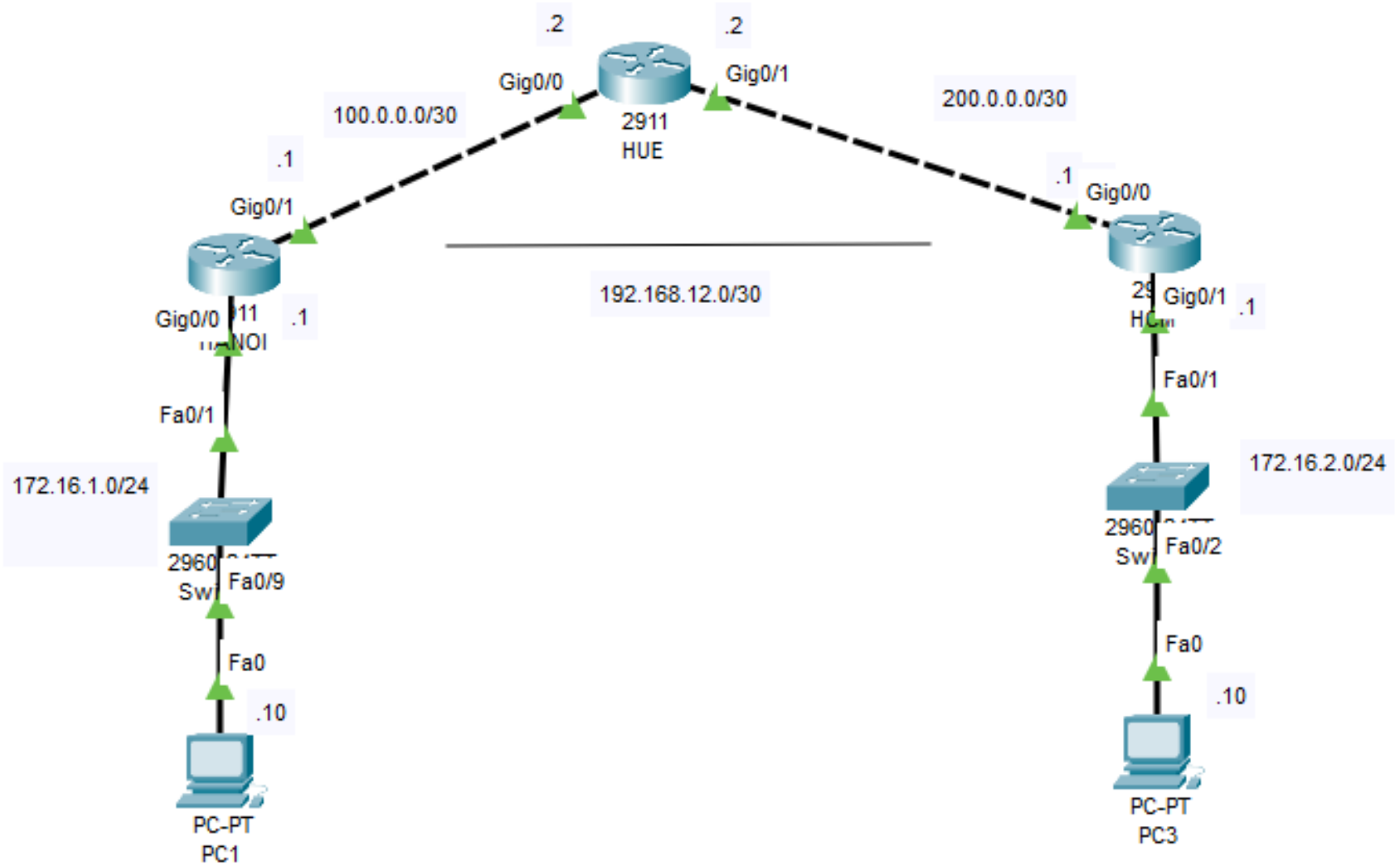
GRE VPN: Site-to-Site VPN



GRE VPN: Site-to-Site VPN



CẤU HÌNH GRE VPN



CÁC BƯỚC THỰC HIỆN

- Cấu hình cơ bản các Router
- Cấu hình định tuyến trên các router
  - R1(config)# ip route 0.0.0.0 0.0.0.0 100.0.0.2
  - R2(config)# ip route 0.0.0.0 0.0.0.0 200.0.0.2
  - ISP(config)# ip route 172.16.1..0 255.255.25.5.0 100.0.0.1
  - ISP(config)# ip route 172.16.2..0 255.255.25.5.0 200.0.0.1
- Cấu hình Tunnel
  - R1(config)#interface tunnel 0
  - R1(config-if)#tunnel soure 100.0.0.1
  - R1(config-if)#tunnel destination 200.0.0.1
  - R1(config-if)#tunnel mode gre

CÁC BƯỚC THỰC HIỆN

- R1(config-if)#tunnel mode gre ip
- R1(config-if)#ip ađ 192.168.12.1 255.255.255.252
- Trên R2
- R2(config)#interface tunnel 0
- R2(config-if)#tunnel soure 200.0.0.1
- R2(config-if)#tunnel destination 100.0.0.1
- R2(config-if)#tunnel mode gre
- R2(config-if)#tunnel mode gre ip
- R2(config-if)#ip ađ 192.168.12.2 255.255.255.252
- Cấu hình định tuyến tĩnh qua đường hầm.
- R1(configf)#ip route 172.16.2.0 255.255.255.252 192.168.12.2
- R2(config)#ip route 172.16.1.0 255.255.255.252 192.168.12.1

Dynamic Multipoint VPNs

VPN IPsec site-to-site và GRE over IPsec là không đủ khi doanh nghiệp thêm nhiều site nữa. Dynamic Multipoint VPN (DMVPN) là một giải pháp phần mềm của Cisco để xây dựng nhiều VPN một cách dễ dàng, nó mang tính động và có thể mở rộng.

- DMVPN đơn giản hóa cấu hình đường hầm VPN và cung cấp tùy chọn linh hoạt để kết nối một site trung tâm với các site chi nhánh.
- Nó sử dụng cấu hình hub-and-spoke để thiết lập cấu trúc liên kết lưới đầy đủ (full mesh).
- Các site Spoke thiết lập các đường hầm VPN an toàn với site hub.
- Mỗi site được định cấu hình bằng cách sử dụng Muiltipoint GRE (mGRE). Giao diện đường hầm mGRE cho phép một giao diện GRE duy nhất hỗ trợ động nhiều đường hầm IPsec.
- Các Spoke site cũng có thể thu thập thông tin về nhau và xây dựng các đường hầm trực tiếp giữa chúng (đường hầm speak-to-spoke).

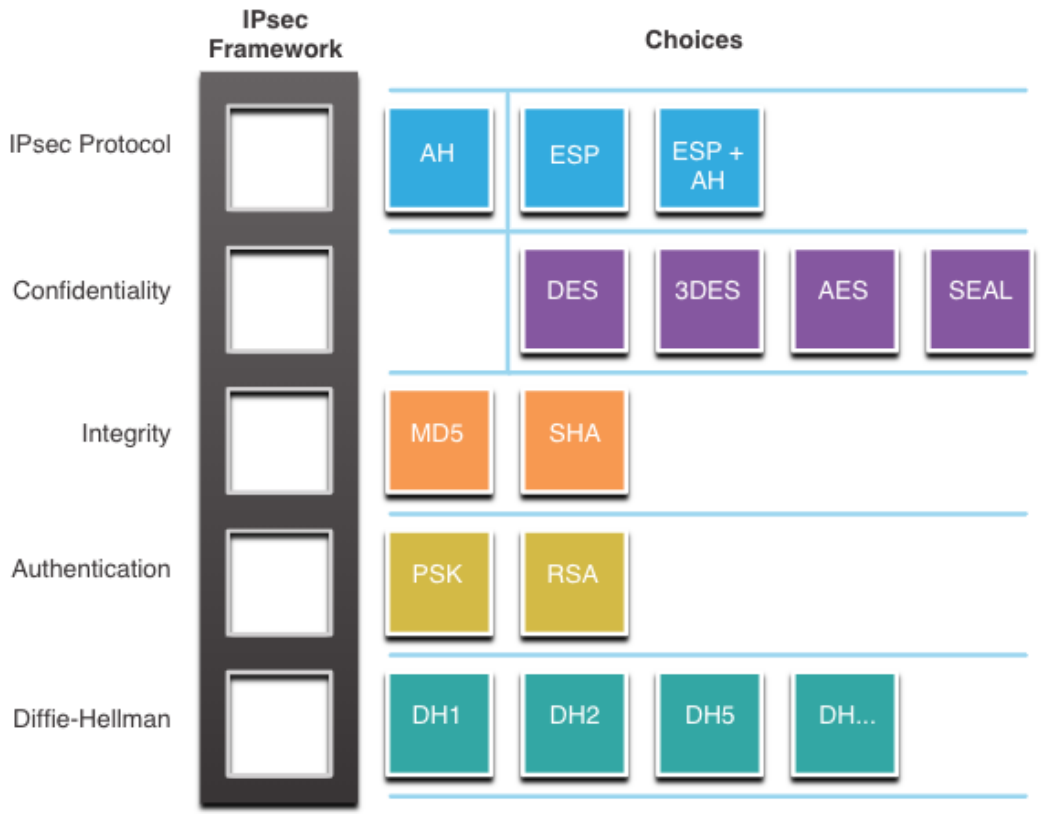
IPsec Technologies

IPsec là một tiêu chuẩn IETF xác định cách VPN có thể được bảo mật trên các mạng IP. IPsec bảo vệ và xác thực các gói IP giữa nguồn và đích và cung cấp các chức năng bảo mật thiết yếu sau:

- Bảo mật (**Confidentiality**)- Sử dụng thuật toán mã hóa để ngăn chặn tội phạm mạng đọc nội dung gói tin.
- Tính toàn vẹn (**Integrity)** - Sử dụng thuật toán băm để đảm bảo rằng các gói không bị thay đổi giữa nguồn và đích.
- Xác thực nguồn gốc (**Origin authentication)** - Sử dụng giao thức trao đổi khóa Internet (IKE) để xác thực nguồn và đích.
- **Diffie-Hellman** – Được sử dụng để đảm bảo trao đổi khóa.

IPsec Technologies (Cont.)

- IPsec không bị ràng buộc với bất kỳ quy tắc cụ thể nào để liên lạc an toàn.
- IPsec có thể dễ dàng tích hợp các công nghệ bảo mật mới mà không cần cập nhật các tiêu chuẩn IPsec hiện có.
- Các vị trí mở trong khung IPsec được hiển thị trong hình có thể được lấp đầy bằng bất kỳ lựa chọn nào có sẵn cho chức năng IPsec đó để tạo một liên kết bảo mật duy nhất (SA).

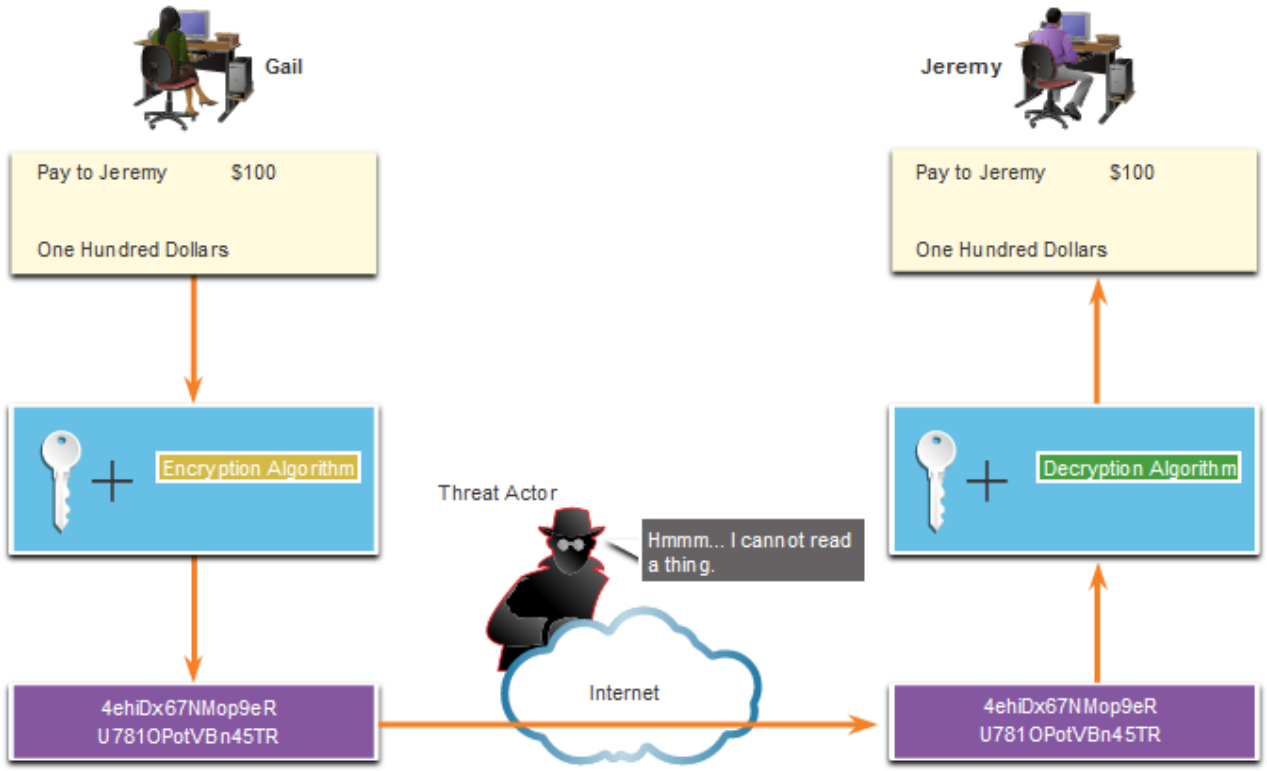


IPsec Protocol Encapsulation

- Chọn giao thức đóng gói IPsec là khối xây dựng đầu tiên của khung.
- IPsec đóng gói các gói bằng Tiêu đề xác thực (AH - Authentication Header) hoặc Giao thức bảo mật đóng gói (ESP- Encapsulation Security Protocol).
- AH chỉ phù hợp khi không yêu cầu hoặc không cho phép bảo mật.
- ESP cung cấp cả bảo mật và xác thực.

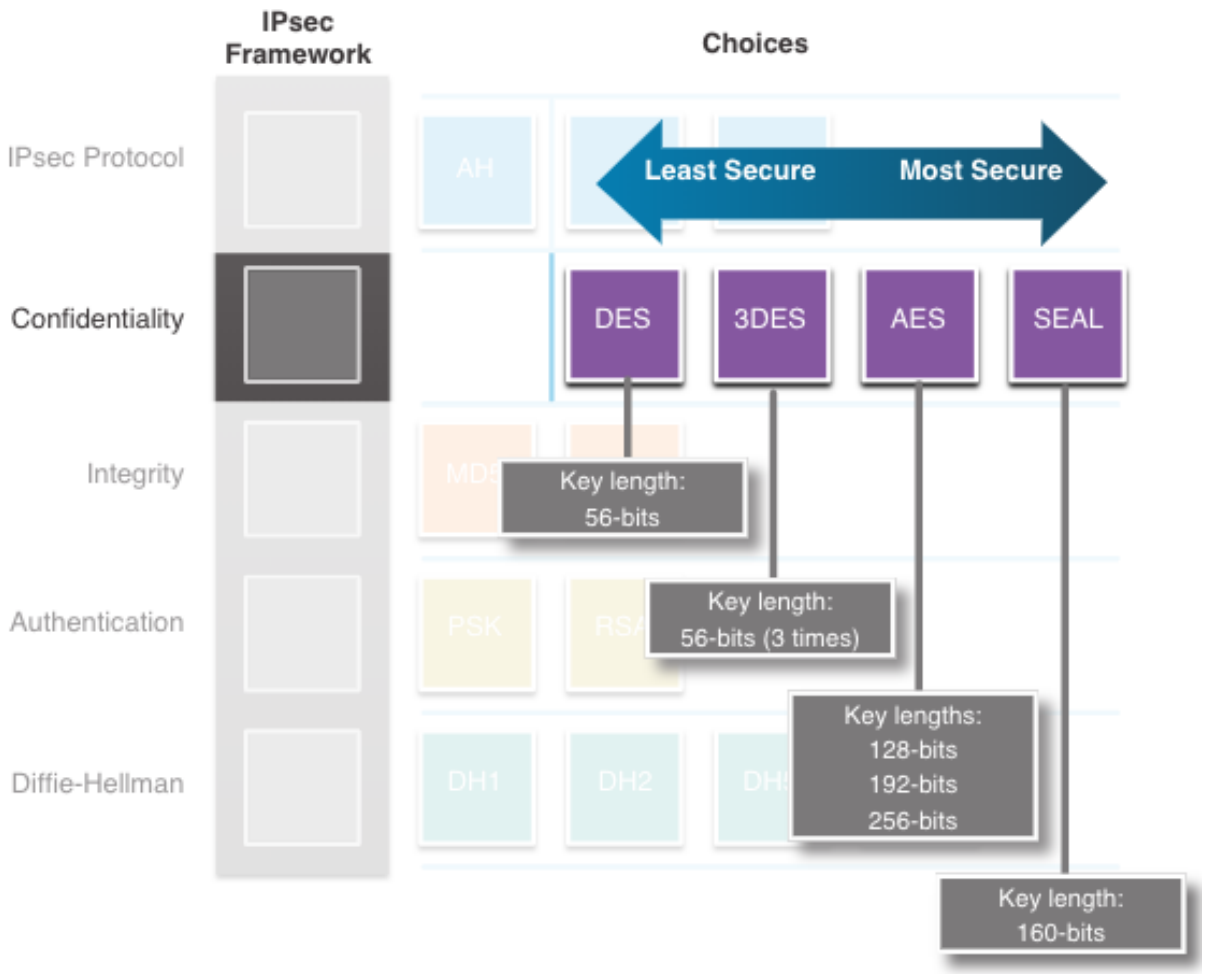
Confidentiality

- Mức độ bảo mật phụ thuộc vào thuật toán mã hóa và độ dài của khóa được sử dụng trong thuật toán mã hóa.
- Số lượng khả năng hack khóa là một chức năng của độ dài của khóa - khóa càng ngắn thì càng dễ bị hack.



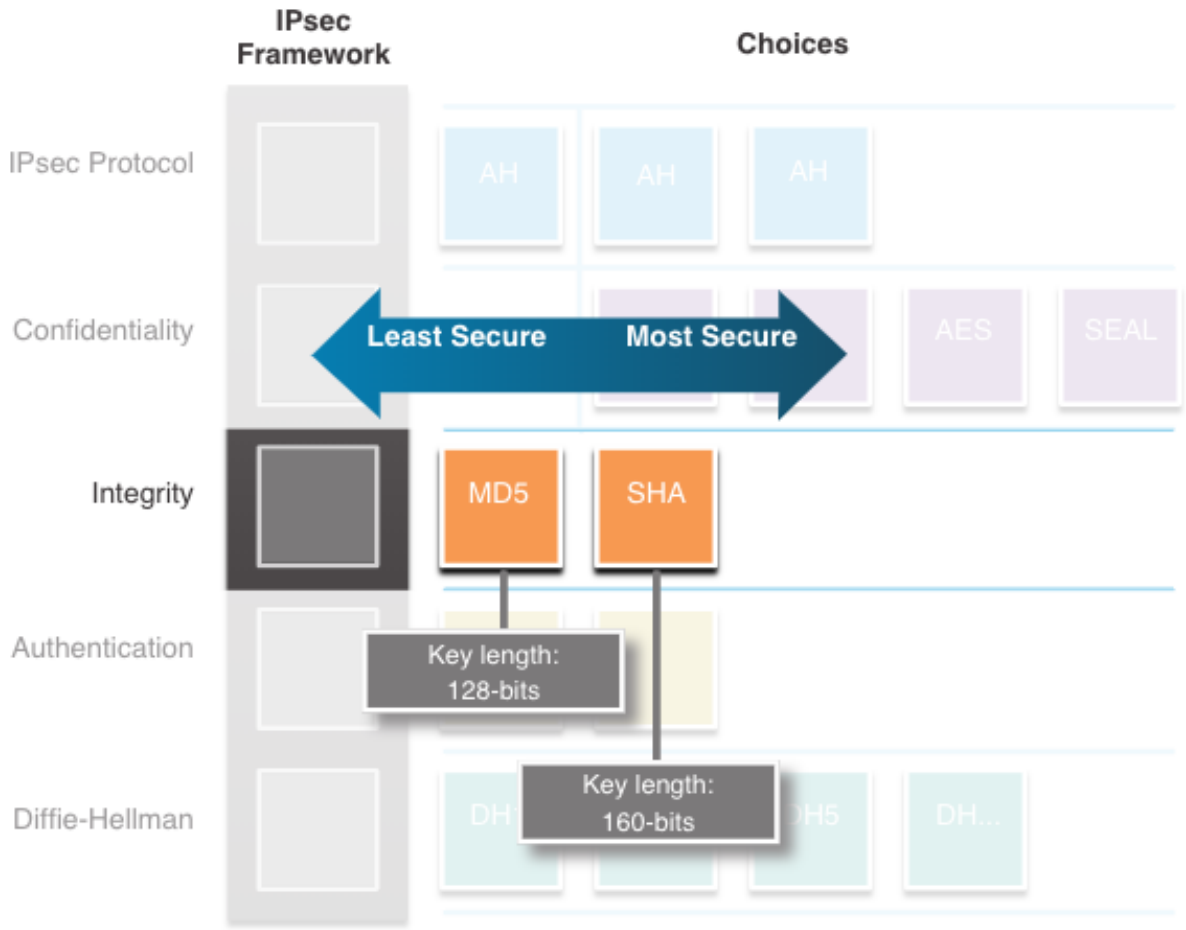
Confidentiality (Cont.)

- Các thuật toán mã hóa được đánh dấu trong hình đều là các hệ thống mật mã khóa đối xứng:
- DES sử dụng khóa 56 bit.
- 3DES sử dụng ba khóa mã hóa 56-bit độc lập cho mỗi khối 64-bit.
- AES cung cấp ba độ dài khóa khác nhau: 128 bit, 192 bit và 256 bit.
- SEAL là một mật mã dòng, có nghĩa là nó mã hóa dữ liệu liên tục thay vì mã hóa các khối dữ liệu. SEAL sử dụng khóa 160 bit.



IPSec
Integrity

- Toàn vẹn dữ liệu có nghĩa là dữ liệu không thay đổi trong quá trình truyền.
- Một phương pháp đảm bảo tính toàn vẹn của dữ liệu là bắt buộc.
- Mã xác thực thư đã băm (HMAC) là một thuật toán toàn vẹn dữ liệu đảm bảo tính toàn vẹn của thông báo bằng cách sử dụng giá trị băm.
- Message-Digest 5 (MD5) sử dụng khóa bí mật dùng chung 128 bit.
- Thuật toán băm an toàn (SHA) sử dụng khóa bí mật 160 bit.



- Data integrity means that the data has not changed in transit

IPSec
Authentication

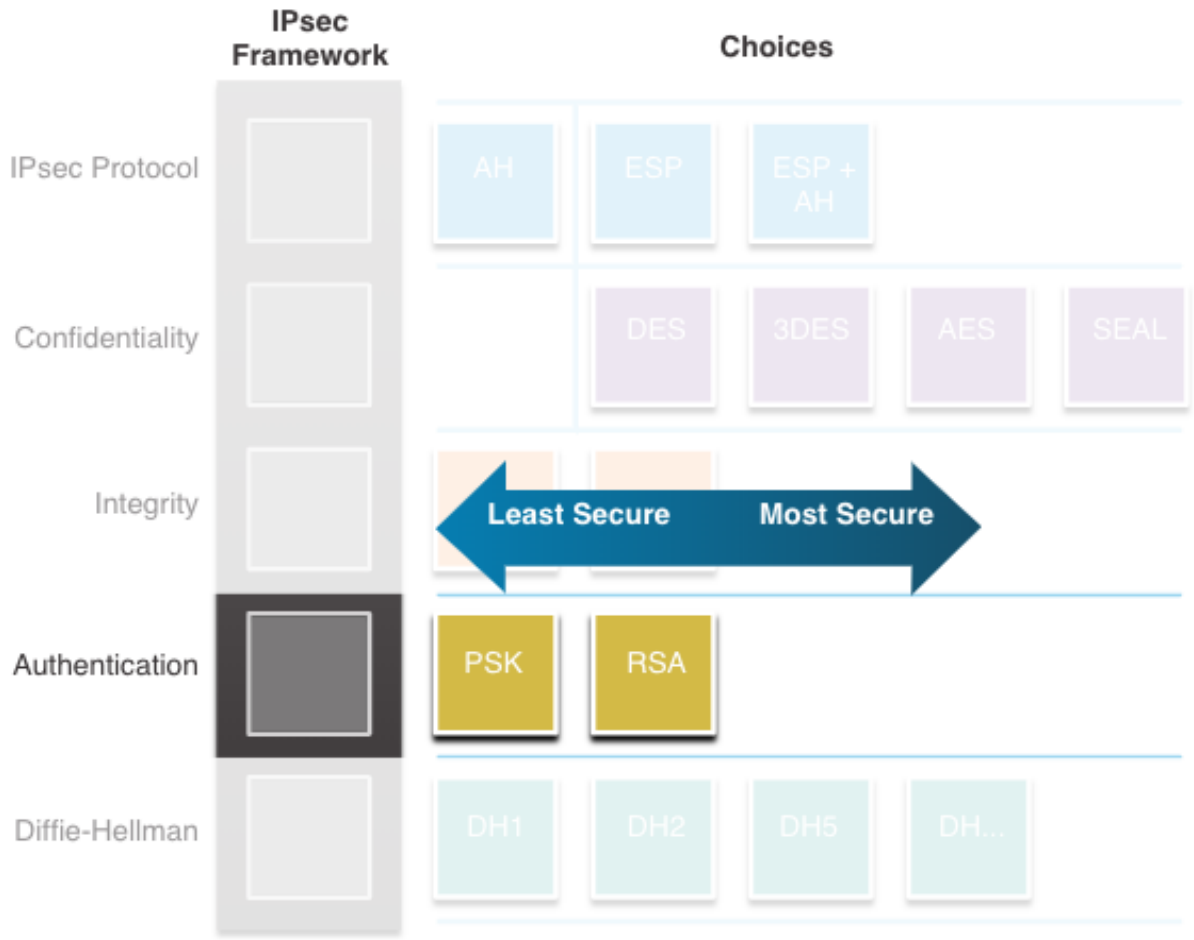
Có hai phương thức xác thực ngang hàng IPsec:

Giá trị khóa chia sẻ trước (PSK) - (PSK) được nhập vào từng thiết bị ngang hàng theo cách thủ công.

Dễ dàng cấu hình thủ côngKhông mở rộng quy mô tốtPhải được cấu hình trên mọi thiết bị ngang hàng

Rivest, Shamir và Adleman (RSA) - xác thực sử dụng chứng chỉ kỹ thuật số để xác thực các đồng nghiệp.

Mỗi máy ngang hàng phải xác thực máy ngang hàng đối diện của nó trước khi đường hầm được coi là an toàn.



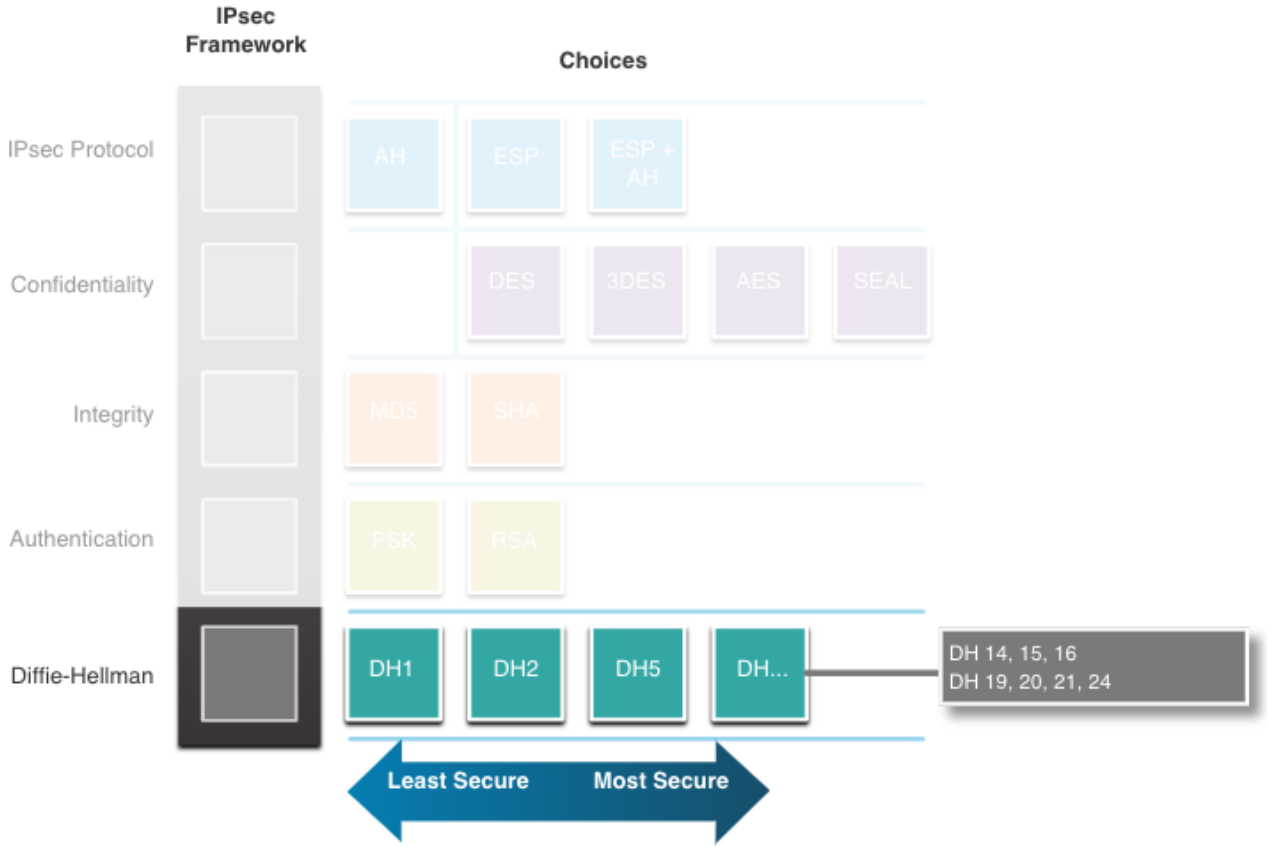
There are two IPsec peer authentication

Secure Key Exchange with Diffie - Hellman

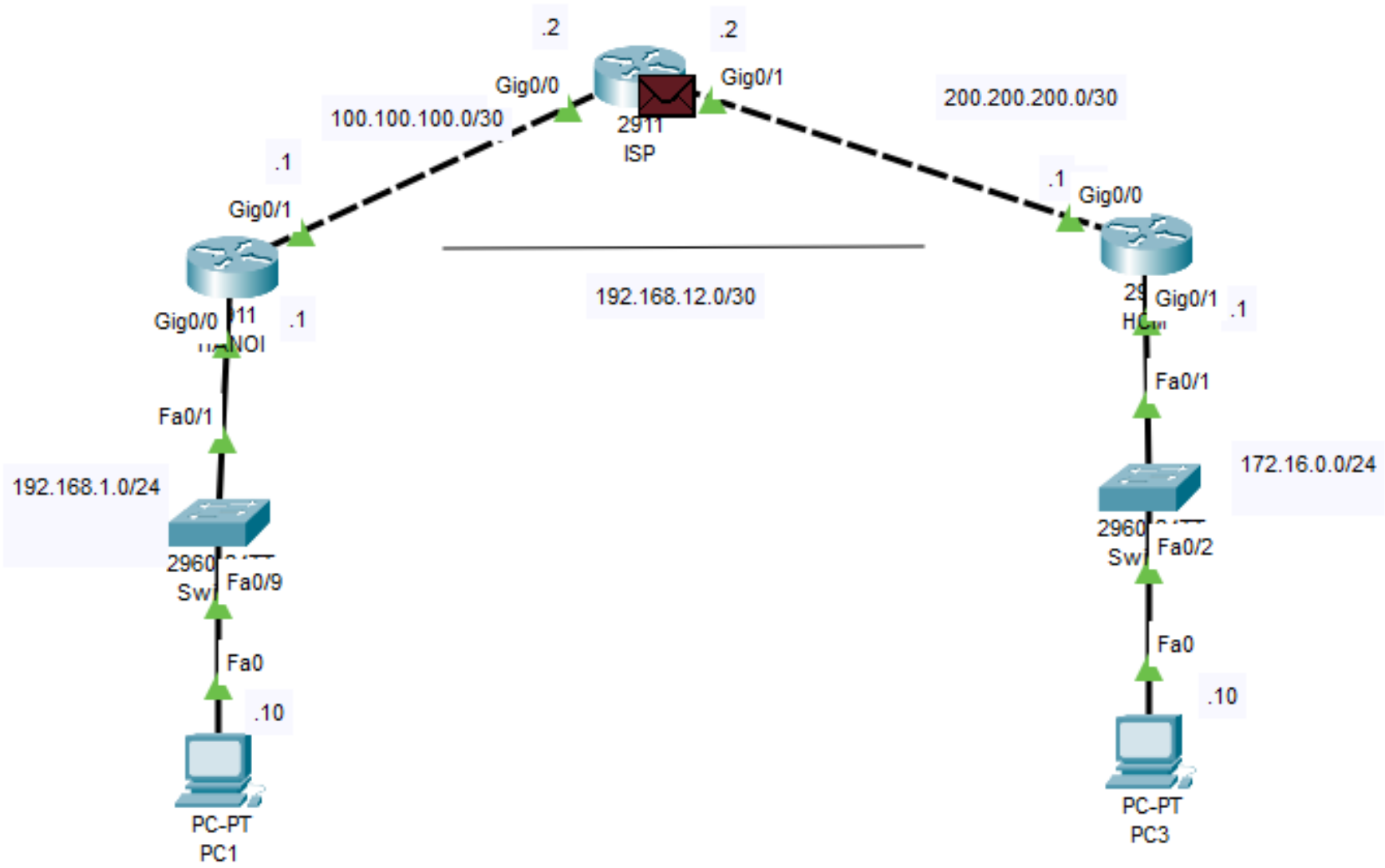
DH provides allows two peers to establish a shared secret key over an insecure channel.

Variations of the DH key exchange are specified as DH groups:

- DH groups 1, 2, and 5 should no longer be used.
- DH groups 14, 15, and 16 use larger key sizes with 2048 bits, 3072 bits, and 4096 bits, respectively
- DH groups 19, 20, 21 and 24 with respective key sizes of 256 bits, 384 bits, 521 bits, and 2048 bits support Elliptical Curve Cryptography (ECC), which reduces the time needed to generate keys.



IPSEC VPN


.2
.2
Gig0/0
Gig0/1
100.100.100.0/30
200.200.200.0/30
2911
ISP
.1
.1
Gig0/1
Gig0/0
192.168.12.0/30
Gig0/0
.1
Gig0/1
.1
Fa0/1
Fa0/1
192.168.1.0/24
172.16.0.0/24
Fa0/9
Fa0/2
Fa0
Fa0
.10
.10
PC-PT
PC1
PC-PT
PC3

CÁC BƯỚC THỰC HIỆN

Cấu hình 2 Lan trên 2 site liên lạc đực với nhau thồng qua VPN

Các bước cấu hình VPN site to site

Bước 1. Cấu hình chính sách ISAKMP/KE phase 1

Bước 2. Cấu hình IPSec Transform-set (ISAKMP/KE phase 2)

Bước 3. Tạo Access control list ACL

Bước 4. Cấu hình Crypto Map

Bước 5. Đưaa Crypto Map lên interface