Bài 2

MẠNG DOANH NGHIỆP VÀ THIẾT KẾ AN NINH

TS. Nguyễn Hồng Sơn

NỘI DUNG

- THIẾT KẾ MẠNG DOANH NGHIỆP
- THIẾT KẾ AN NINH MẠNG

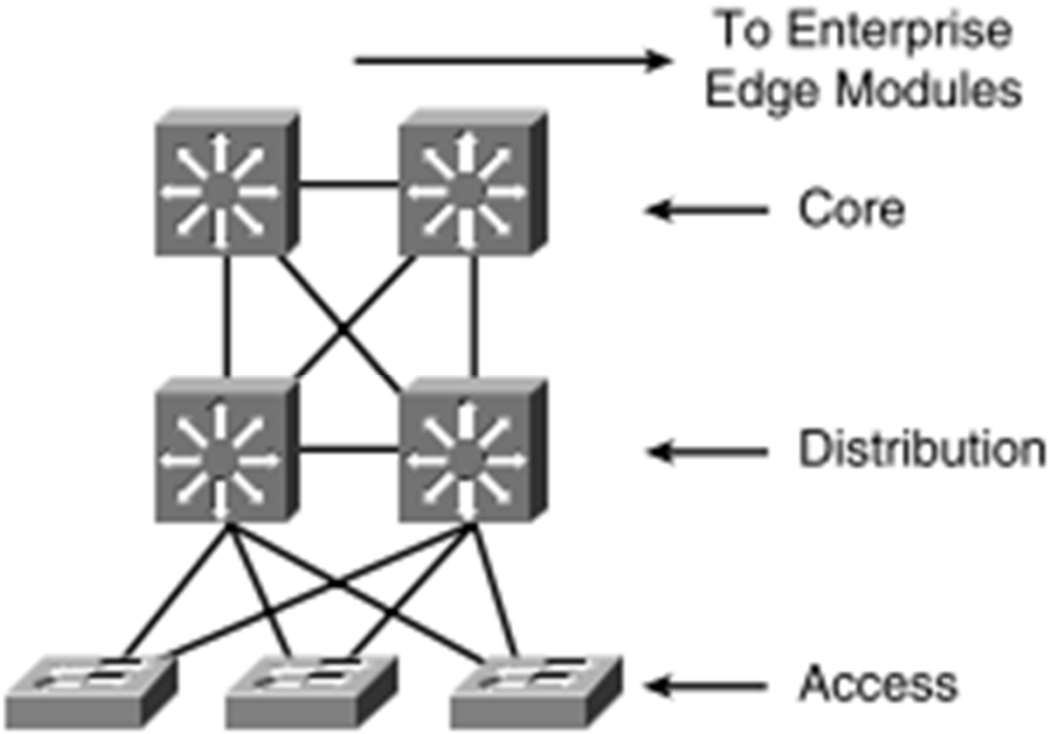
THIẾT KẾ MẠNG DOANH NGHIỆP

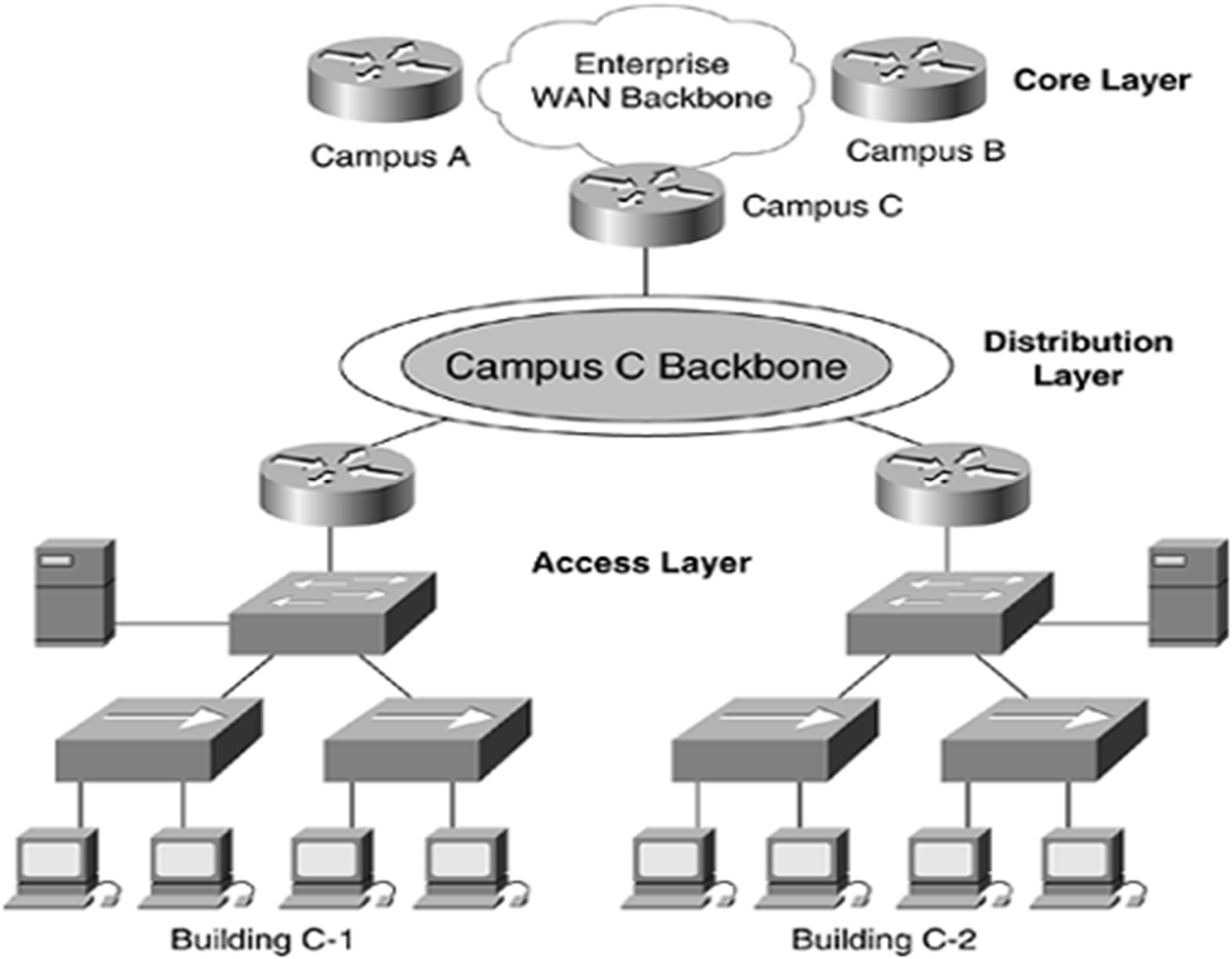
NỘI DUNG

- THIẾT KẾ MẠNG PHÂN CẤP
- TOPO MẠNG CÓ DỰ PHÒNG
- THIẾT KẾ MẠNG MODULE
- THIẾT KẾ TOPO MẠNG CAMPUS
- THIẾT KẾ TOPO CHO ENTERPRISE EDGE

THIẾT KẾ MẠNG PHÂN CẤP (Hierarchical Network)

- Theo mô hình thiết kế mạng phân cấp: phát triển topo dưới dạng các lớp rời rạc
  - Core layer
  - Dstribution layer
  - Access layer
- Mỗi lớp tập trung vào các chức năng đặc biệt, cho phép chọn ra các hệ thống và đặc tính phù hợp


To Enterprise
Edge Modules
Core
Distribution
Access


Enterprise
WAN Backbone
Core Layer
Campus A
Campus B
Campus C
Campus C Backbone
Distribution
Layer
Access Layer
Building C-1
Building C-2

Flat network Topology

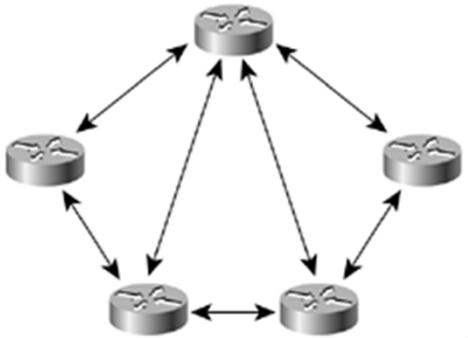
- Phù hợp cho mạng rất nhỏ
- Mỗi thiết bị liên mạng có nhiệm vụ như nhau
- Khi có sự cố phải kiểm tra toàn mạng
- Topo mạng Flat WAN
  - Gồm nhiều điểm kết nối thành vòng
  - Mỗi điểm là một router kết nối với hai router kế qua một P2P link
  - Các giao thức định tuyến hội tụ nhanh
  - Thông tin có thể phục hồi khi một link bị hỏng

Các Flat LAN topology

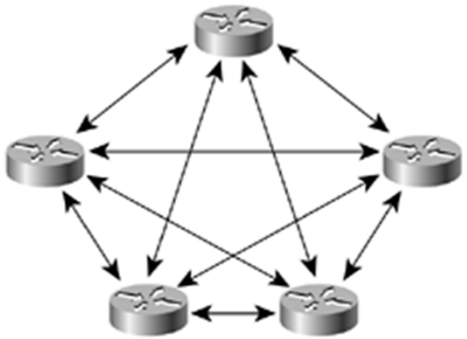
- Đầu thập niên 1990 các thiết kế tiêu biểu cho LAN là các PC và Server nối vào một hay nhiều Hub theo một flat topology
- Ngày nay thay Hub bằng Switch (lớp 2)
- Mesh topology ~ nhu cầu khả dụng (availability)
  - Full-mesh topology
  - Partial-mesh topology

Các Flat LAN topoogy (2)

- Số link trong full-mesh: n*(n-1)/2
- Chi phí cao, khó bảo trì sửa chữa hay nâng cấp
- Lưu lượng quảng bá cho định tuyến tăng



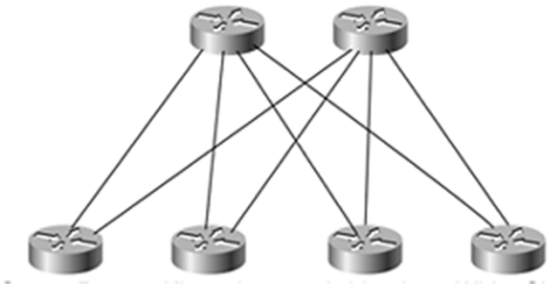
Partial-Mesh Topology



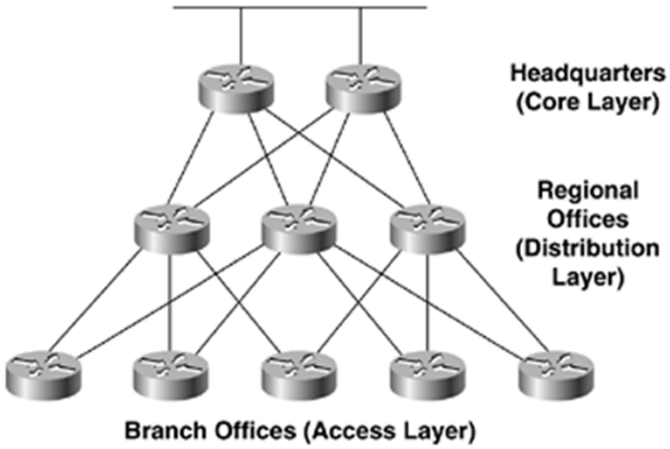
Full-Mesh Topology

Dùng hierarchical topology

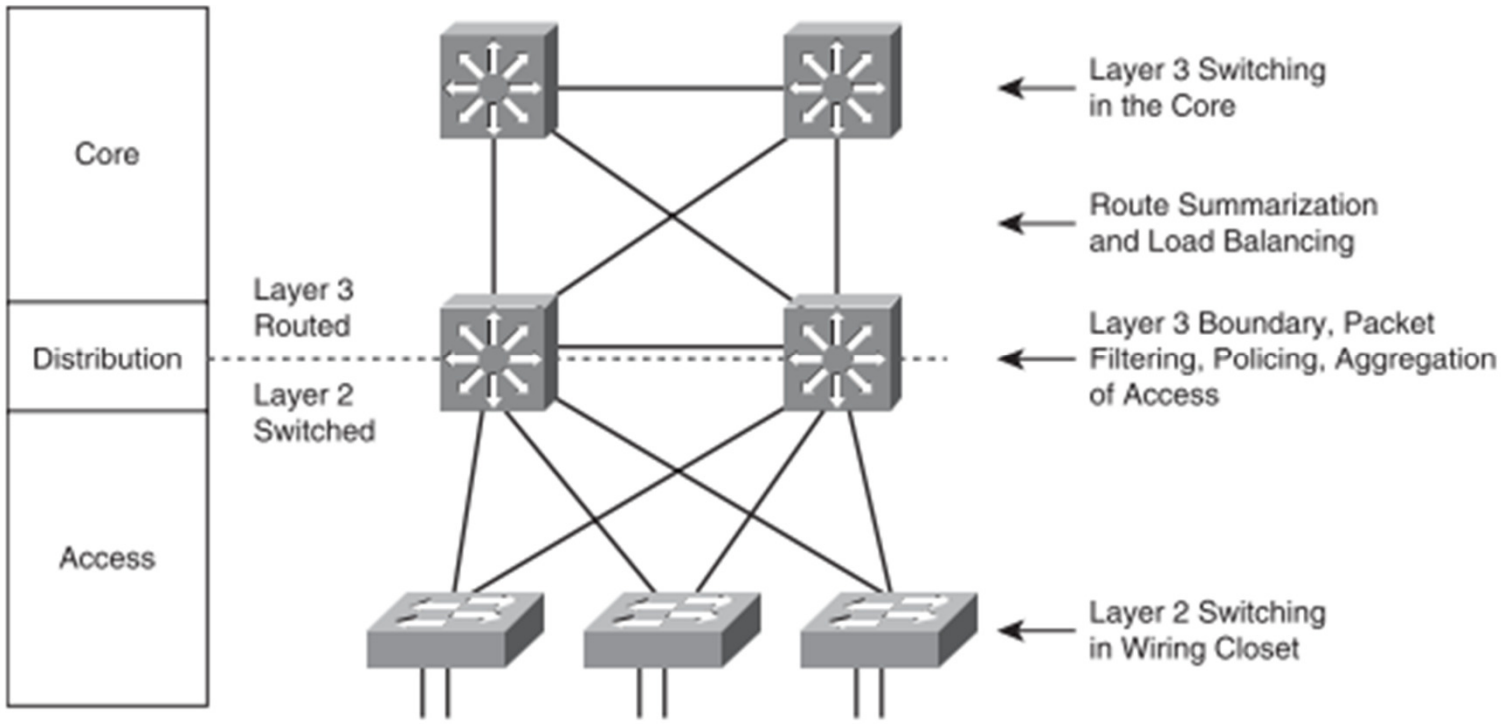
- Hierarchical Redundant topology



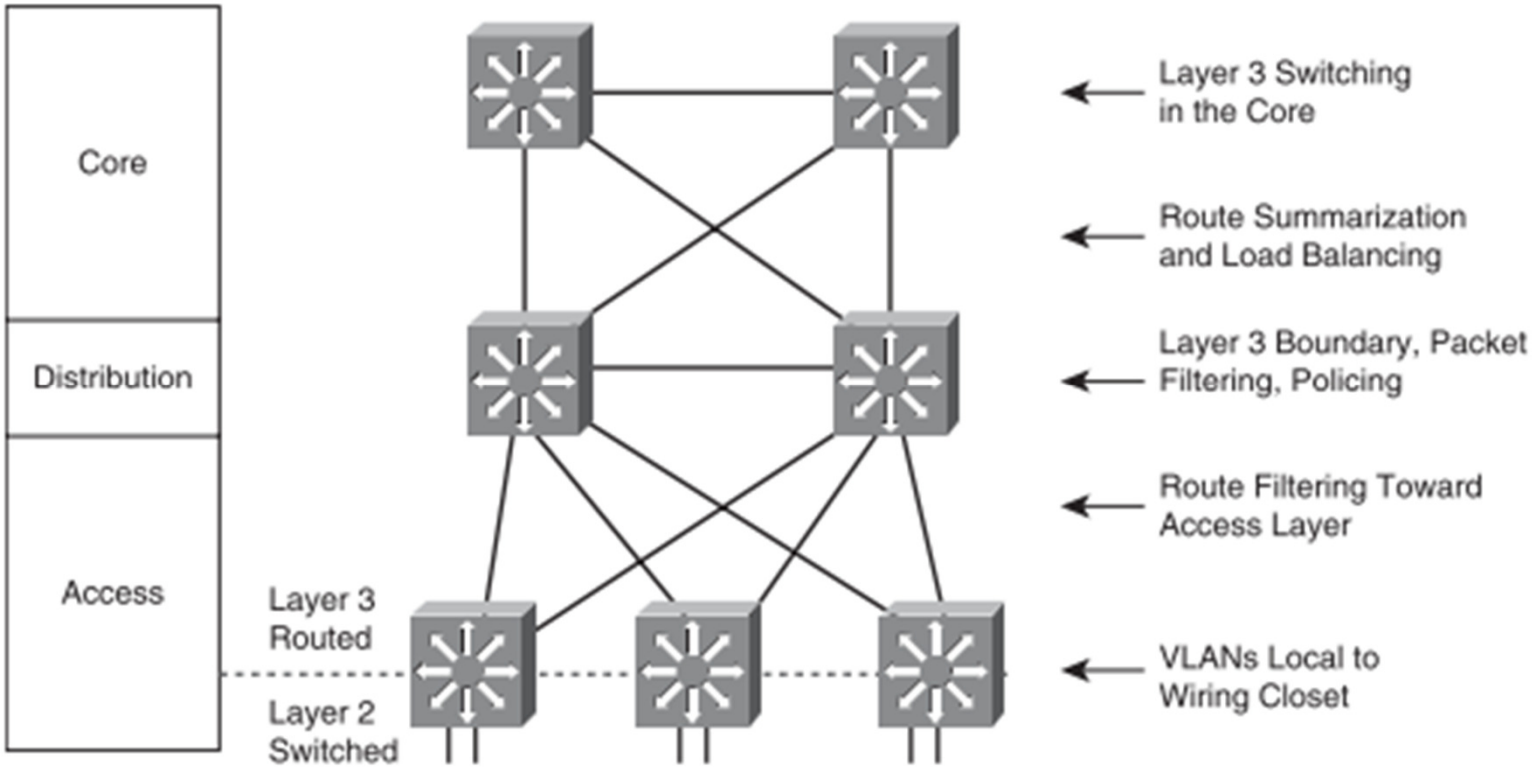
- Partial-Mesh Hierarchical topology



Switched Hierarchical Design

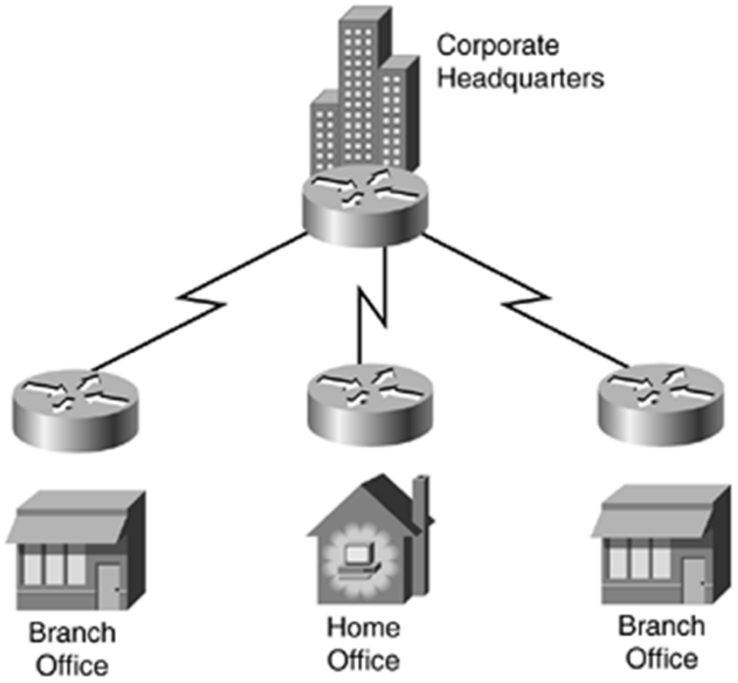


Routed Hierarchical Design



Mô hình mạng cho công ty vừa và nhỏ

- Hub-and-Spoke Hierarchical Topology



Đặc trưng của core layer

- Backbone tốc độ cao, tin cậy, dự phòng và thích ứng tốt
- Độ trễ nhỏ
- Có kích thước giới hạn

Đặc trưng của Distribution layer (1/2)

- Kiểm soát truy xuất tài nguyên vì lý do an ninh
- Kiểm soát lưu lượng mạng
- Xác định các miền quảng bá
- Định tuyến giữa các VLAN
- Cho phép core kết nối các điểm chạy các giao thức khác nhau
- Tái phân bố giữa các giao thức định tuyến ở lớp access và giao thức định tuyến lớp core

Đặc trưng của Distribution layer (2/2)

- Tóm tắt đường đi từ lớp access
- Trong một số trường hợp có thể cung cấp default route cho các router lớp access và chỉ chạy giao thức định tuyến động khi giao tiếp với core router
- Ẩn các thông tin về topo của access layer đối với core layer và ngược lại

Đặc trưng access layer

- Tạo điều kiện cho các user trên các phân đoạn cục bộ truy nhập vào internetwork
- Bao gồm router, switch, bridge, hub và access point.
- Switch thường được dùng để triển khai access layer trong các campus net nhằm phân chia các miền băng thông phù hợp với các ứng dụng cần nhiều băng thông
- Dùng các công nghệ như ISDN, Frame Relay, leased line và analog dialup để hỗ trợ các chi nhánh hay văn phòng nhỏ truy nhập vào internetwork.

Topo mạng có dự phòng

- Nhân đôi các thành phần mạng, loại trừ những điểm mà khi lỗi làm tê liệt mạng.
- Các thành phần có thể là core router, switch, link giữa hai switch, CSU, nguồn điện, WAN trunk, kết nối Internet...
- Xây dựng các data center dự phòng hoàn chỉnh
- Có thể thực hiện dự phòng trong mạng campus, giữa các lớp trong mô hình phân cấp, trên edge net của enterprise net

Đường đi dự phòng (backup path)

- Backup path bao gồm các router và switch và các link dự phòng riêng giữa các router và switch, là bản sao của đường đi chính
- Xem xét hai khía cạnh của backup path:
  - Băng thông là bao nhiêu
  - Tốc độ chuyển dụng nhanh cỡ nào
- Nên dùng công cụ mô phỏng để đánh giá hiệu quả

Load sharing (load balancing)

- Cho phép hai hay nhiều giao tiếp hay đường dẫn chia sẻ tải với nhau
- Mục tiêu chính của dự phòng là đáp ứng tính khả dụng, mục tiêu phụ là nhằm cải thiện performance của mạng bằng cách chia tải qua các liên kết song song
- Load sharing phải được qui hoạch và cấu hình

Thiết kế mạng module

- Một dự án thiết kế mạng lớn và các mạng lớn bao gồm nhiều phần khác nhau
- Mỗi phần nên được thiết kế theo giải pháp top-down có hệ thống, áp dụng nguyên lý phân cấp và dự phòng.
- Các giải pháp mạng và dịch vụ có thể được chọn trên căn bản module nhưng phải là một thành phần của mạng toàn cục
- Cisco system dùng mô hình Enterprise Composite Network Model để mô tả các thành phần khác nhau hay module của một mạng doanh nghiệp

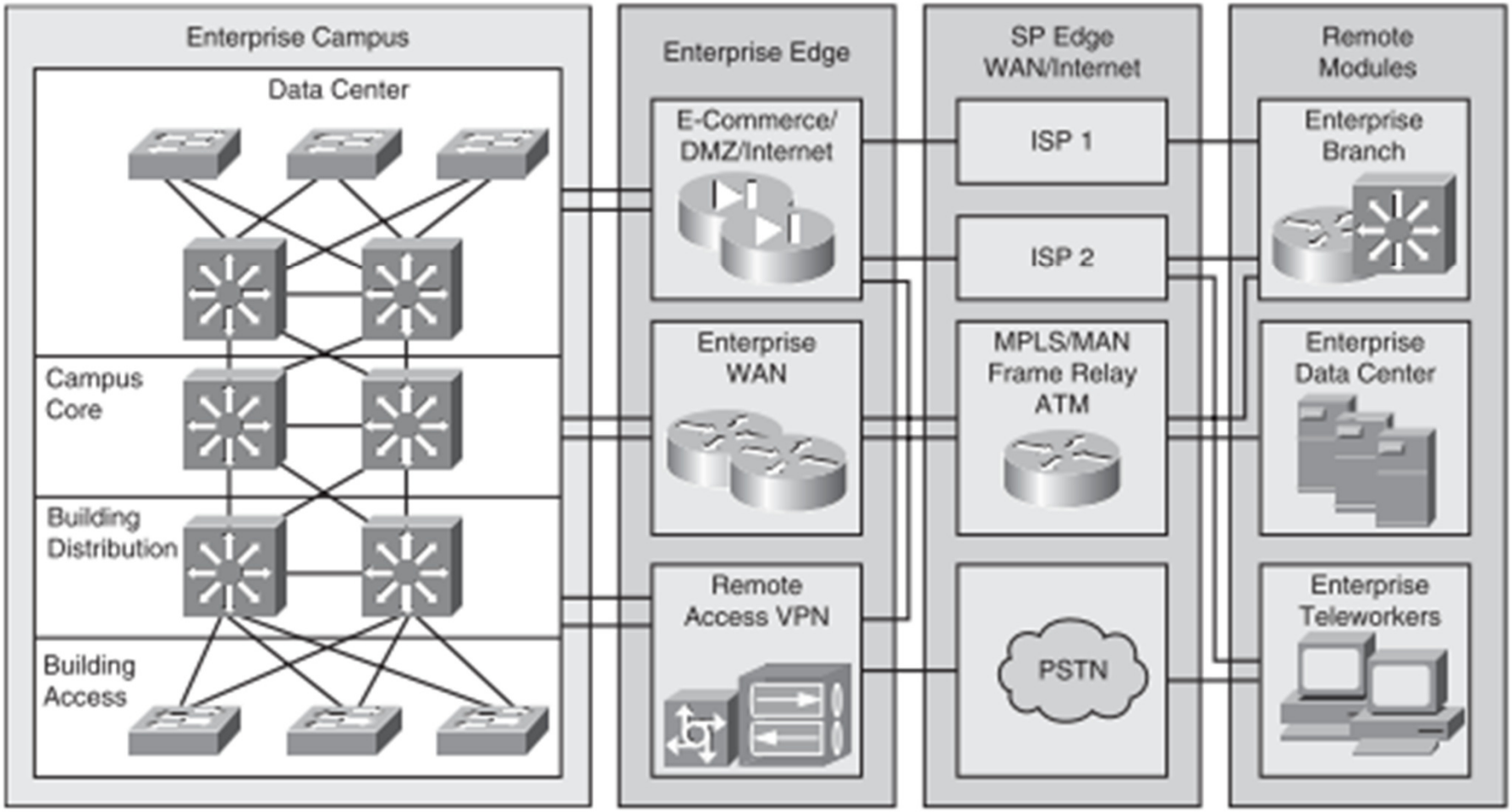
Enterprise Composite Network Model (1/4)

- ECNM gồm 3 vùng chính, mỗi vùng có thể tạo ra các module nhỏ hơn:
  - Enterprise campus: gồm các module để xây dựng mạng campus vững chắc. Chứa tất cả các thành phần cho sự hoạt động độc lập bên trong campus.
  - Enterprise edge: tập hợp tất cả các kết nối từ các phần tử khác nhau tại biên của mạng enterprise. Chứa tất cả các phần tử để truyền thông hiệu quả và an toàn giữa các campus, vị trí ở xa, đối tác, user di động và Internet.
  - Service provider edge: cho phép truyền thông với các mạng khác dùng các công nghệ WAN khác nhau và hỗ trợ bởi các ISP

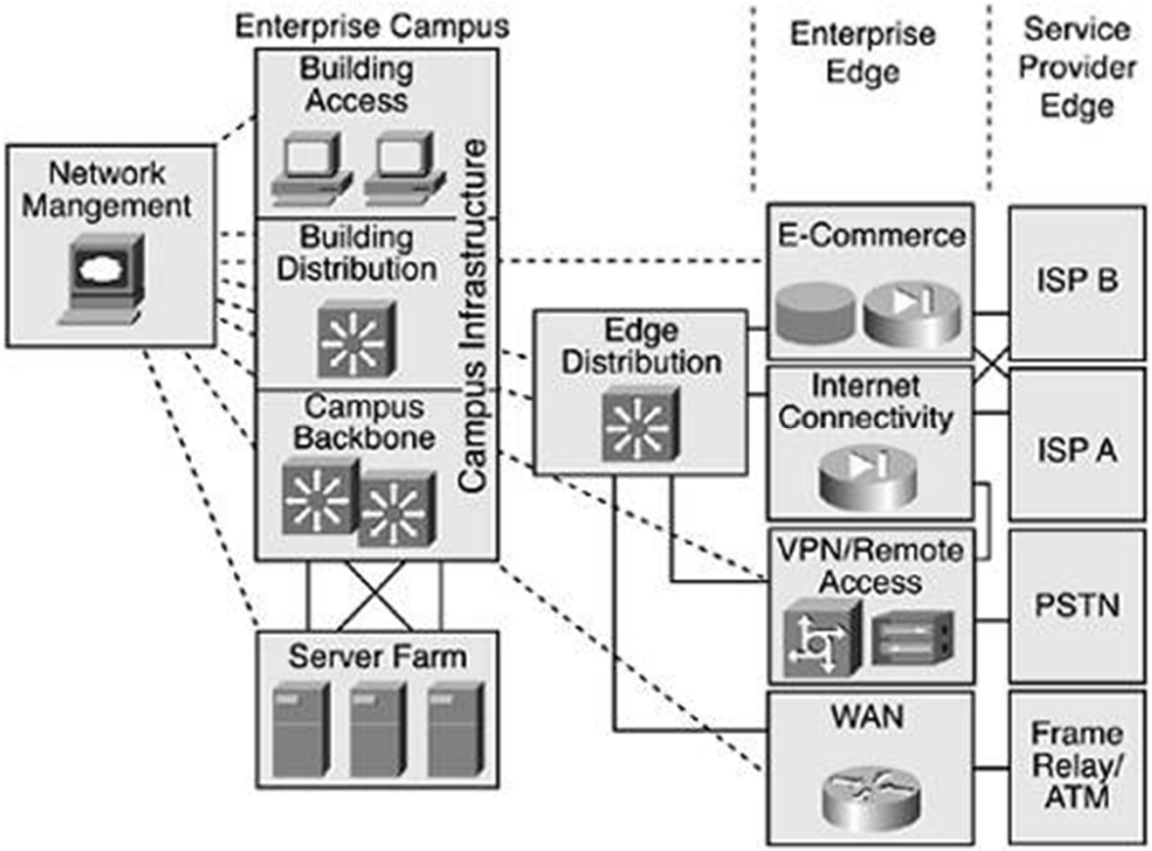
Enterprise Composite Network Model (2/4)

- Mỗi vùng có thể chia thành các module nhỏ hơn
- Ví dụ campus có thể gồm campus backbone, server farm, building access và distribution module, network management module. Enterprise edge có thể gồm WAN, VPN, Internet access, và e-commerce module
- Có thể bổ sung module nếu cần

Enterprise Composite Network Model (3/4)



Enterprise Composite Network Model (4/4)



Thiết kế topo mạng campus

- Theo ECNM, một campus bao gồm campus infrastructure module, server farm, network management module và một edge distribution module
- Infrastructure module có 3 module con:
  - Building access submodule
  - Building distribution submodule
  - Campus backbone

Building access submodule

- Chứa các đầu cuối kết nối đến switch hay access point.
- Các switch cung cấp các liên kết đến building distribution module
- Các dịch vụ gồm network access, broadcast control, protocol filtering, packet marking

Building distribution submodule

- Tập hợp các tủ nối dây trong tòa nhà và cung cấp kết nối đến campus backbone qua các router (hay switch lớp 3).
- Thực hiện định tuyến, QoS và các phương thức điều khiển truy xuất phù hợp với nhu cầu an ninh và performance.
- Backup path và Load sharing

Campus backbone

- Là core layer của campus infrastructure module nối building access và building distribution với server farm, network management và edge distribution module
- Redundancy và fast converging
- Dùng router (hay switch lớp 3) tốc độ cao
- Cung cấp tính năng QoS và security

Spanning Tree Protocol

- IEEE 802.1D và IEEE 802.1w
- Topo của mỗi module và submodule được xác định từng phần bởi STP
- Nên chọn gốc (root bridge) bằng cách dùng lệnh cấu hình để tránh trường hợp giao thức tự động chọn gốc không thích hợp

Virtual LAN (1/3)

- Bandwidth domain
- Broadcast domain
- Switch chia mạng thành những bandwidth domain nhỏ (mỗi port + thiết bị kết nối đến = bandwidth domain)
- Mặc định switch không chia broadcast domain, nhưng trong building access module dùng switch sẽ kiểm soát broadcast bằng VLAN

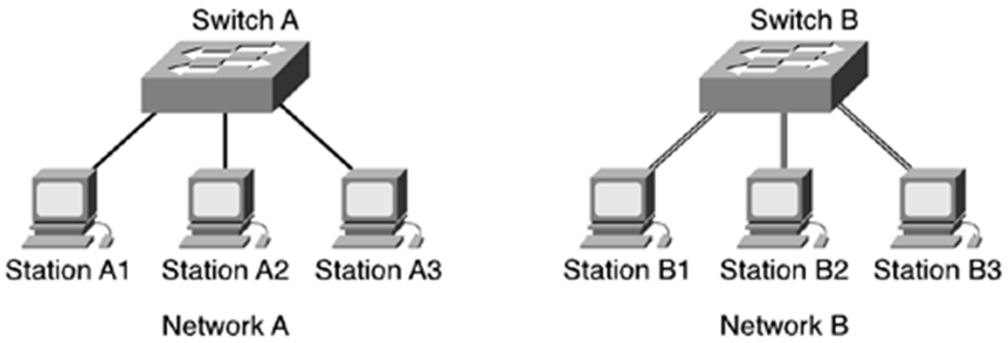
Virtual LAN (2/3)

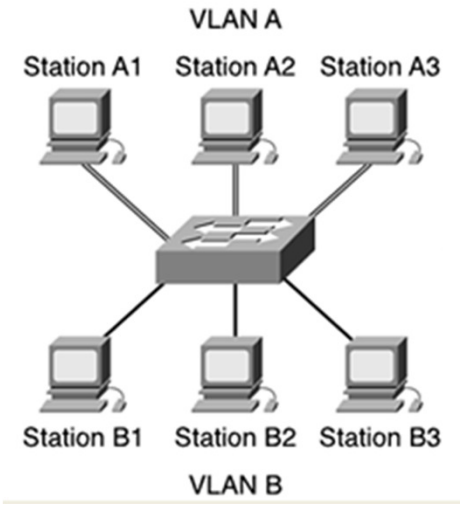
- VLAN là giải pháp truyền data theo chuẩn LAN nhưng không bị hạn chế bởi các ràng buộc vật lý truyền thống
- Bất chấp vị trí vật lý của một user ở đâu, người quản trị đều có thể gán user vào một VLAN bất kỳ
- Việc gán VLAN dựa trên các ứng dụng, giao thức, các nhu cầu về performance, nhu cầu về security, đặc tính tải và lưu lượng, hay các yếu tố nào đó theo đặc thù mạng

Virtual LAN (3/3)

- VLAN xuyên qua nhiều physical LAN
- Nhiều VLAN trên một physical LAN
- Trong mạng IP, một VLAN được thực hiện như là một mạng con (IP subnet) (bởi ARP)

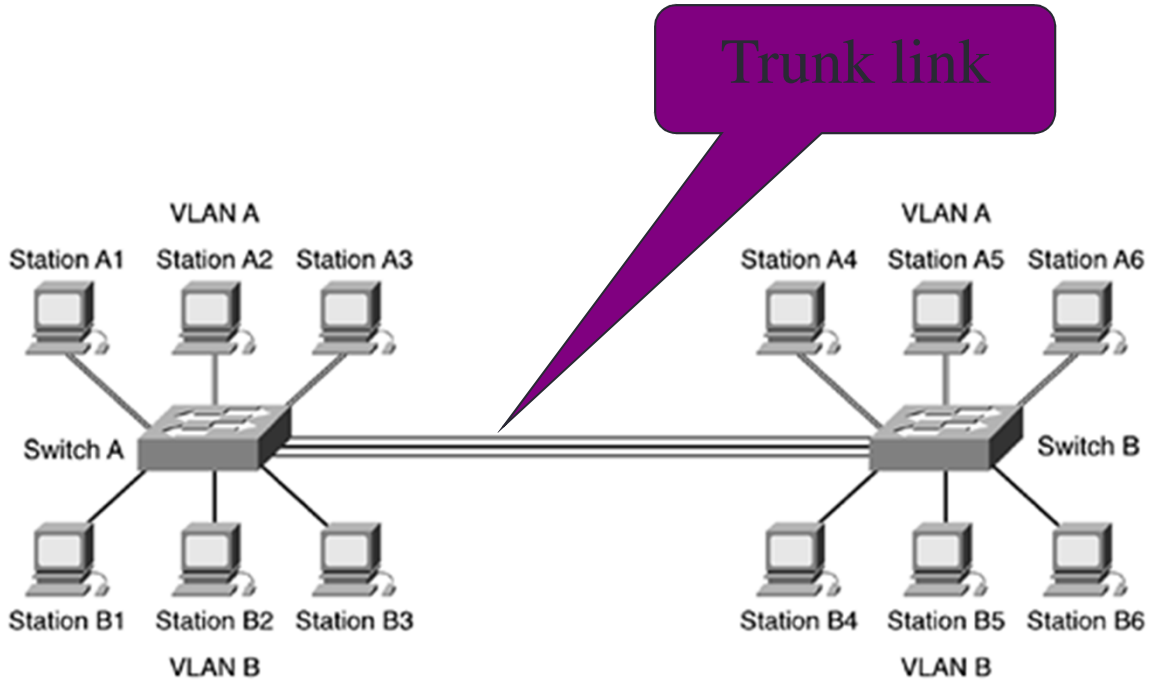
Thiết kế VLAN cơ bản (1/3)





Thiết kế VLAN cơ bản (2/3)

- VLAN qua nhiều switch
- IEEE 802.1Q
- Cisco ISL protocol



Thiết kế VLAN cơ bản (3/3)

- Cần xác định phạm vi của mỗi VLAN
- Mỗi VLAN sẽ trãi ra trên bao nhiêu switch
- Xác định dung lượng của trunk link, dùng các phương pháp trong chương 4
- Đối với mạng phòng lab thì thường dùng 10Mbps Ethernet trunk

Wireless LAN (1/3)

- Access point (AP), wireless cell
- Xác định tầm phủ của một wireless cell và cần bao nhiêu wireless cell
- Các yếu tố ảnh hưởng gồm: data rate, công suất, anten và vị trí đặt

Wireless LAN (2/3)

- Nguyên lý anten là đẳng hướng
- Tín hiệu mạnh với các hướng trực giao với trục anten
- Chú ý không để AP tại các mặt phản xạ hướng ra ngoài vị trí cần
- Bức tường có thể làm suy giảm tín hiệu nhưng không ngăn chặn hoàn toàn

Wireless LAN (3/3)

- Kích thước cell càng lớn bandwidth domain càng lớn, performance càng thấp
- Có thể dùng nhiều AP để mở rộng tầm phủ hỗ trợ truy xuất không gián đoạn khi user chuyển chỗ, cách làm là đặt các user di động trong cùng một IP subnet hay VLAN
- Tách biệt subnet cũng giúp cải thiện khả năng quản lý và security

Dự phòng cho wireless LAN

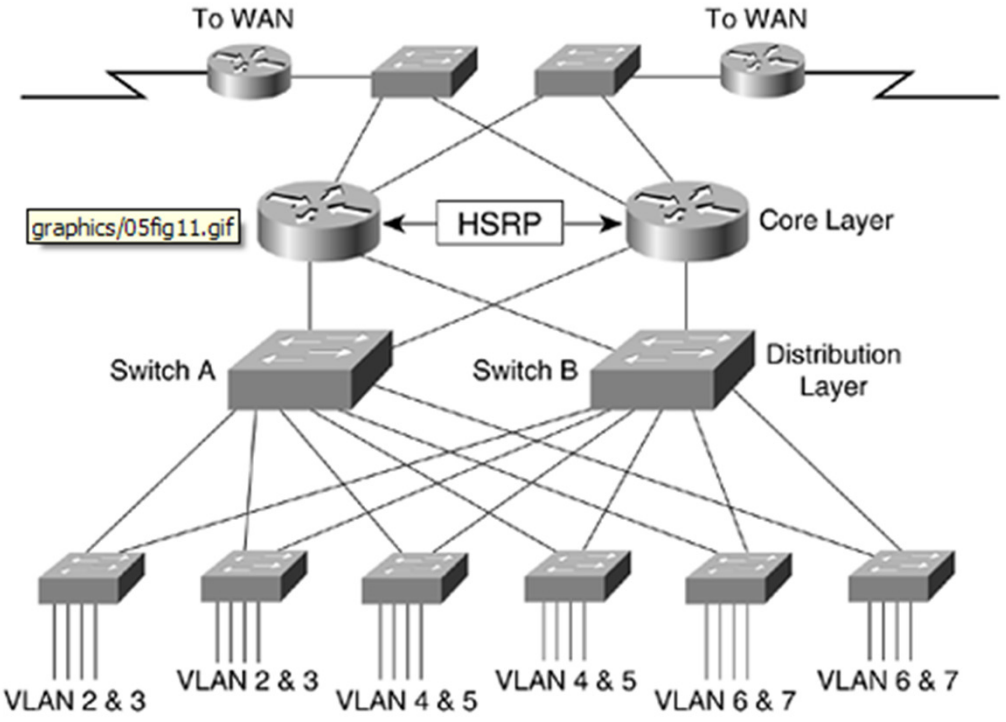
- Access point hot standby: Cho phép 2 AP được cấu hình dùng cùng kênh trong trong một vùng phủ. Chỉ một AP được active và AP kia dự phòng
- Đặt 2 AP gần nhau
- Khi đưa AP chính trở lại làm việc cần reset AP dự phòng bằng tay

PVST+ và MISTP (1/2)

- Per VLAN Spanning Tree + là giải pháp tạo một spanning tree cho mỗi VLAN để tạo khả năng dự phòng
- PVST+ cho phép load sharing nhờ có nhiều đường chuyển khác nhau trên mỗi VLAN
- MISTP (Multi-Instance Spanning Tree Protocol) cho phép nhiều VLAN được nhóm lại trong một spanning tree
- IEEE 802.1s (Multiple Spanning Tree)

PVST+ và MISTP (2/2)

- Nếu dùng VLAN trong thiết kế campus dùng switch có hỗ trợ 802.1s, PVST+ hay MISTP có thể dùng là link dự phòng cho load sharing

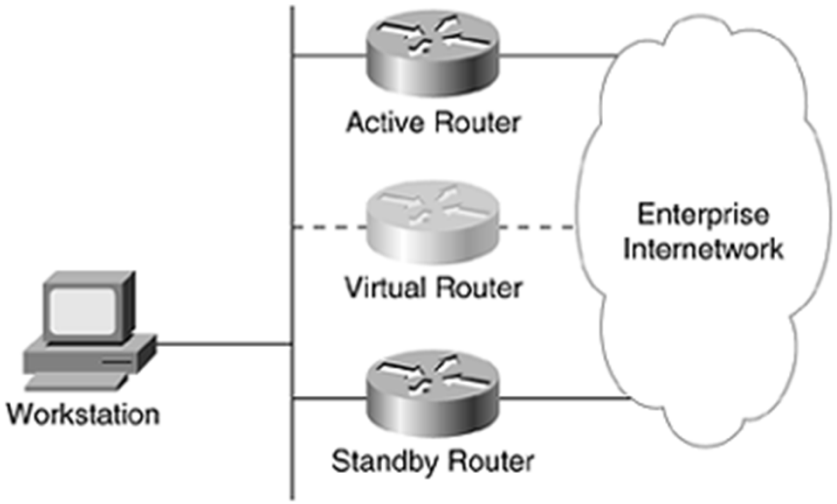


HSRP hay VRRP (1/2)

- Hot Standby Router Protocol (HSRP) giúp máy trạm vẫn giữ liên lạc với internetwork ngay cả khi gateway mặc định bị hỏng
- Trong RFC 2338 gọi là VRRP
- Tạo virtual router (phantom router) với IP và MAC address, mỗi máy trạm đều được cấu hình dùng virtual router như default gateway

HSRP hay VRRP (2/2)

- Các HSRP router trên LAN trao đổi với nhau để chỉ định active hay standby router
- HSRP cũng có thể đóng vai trò proxy ARP

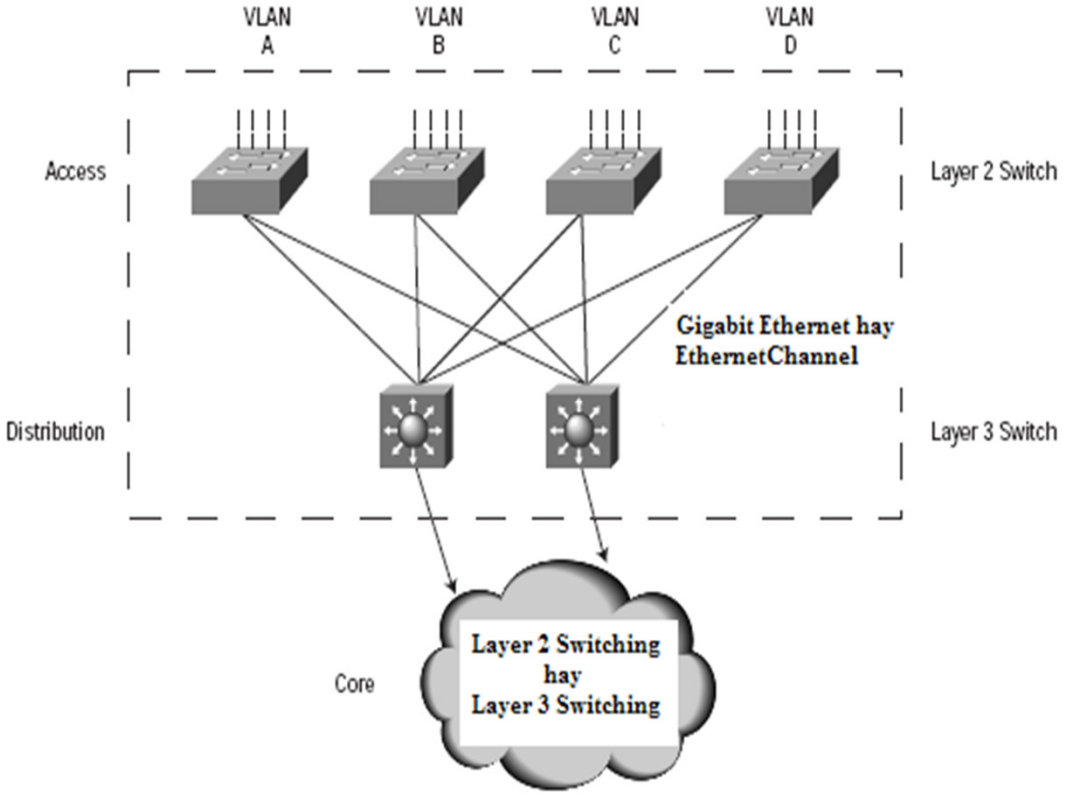


Gateway Load Balancing Protocol

- GLBP cho phép cân bằng tải qua nhiều router dùng một địa chỉ IP ảo và nhiều địa chỉ MAC ảo.
- Mỗi host được cấu hình cùng địa chỉ IP ảo và tất cả các router trong nhóm router ảo cùng tham gia chuyển gói
- Các thành viên trong nhóm GLBP bầu một router là active virtual gateway (AVG)
- AVG gán cho mỗi thành viên dự phòng còn lại một địa chỉ MAC ảo

Thiết kế building network: building block không mở rộng VLAN (1/2)

- Gigabit Ethernet trunk kết nối Layer 2 switch đến cặp Layer 3 switch trong distribution layer
- Mỗi module là thành phần cơ bản tạo nên building network

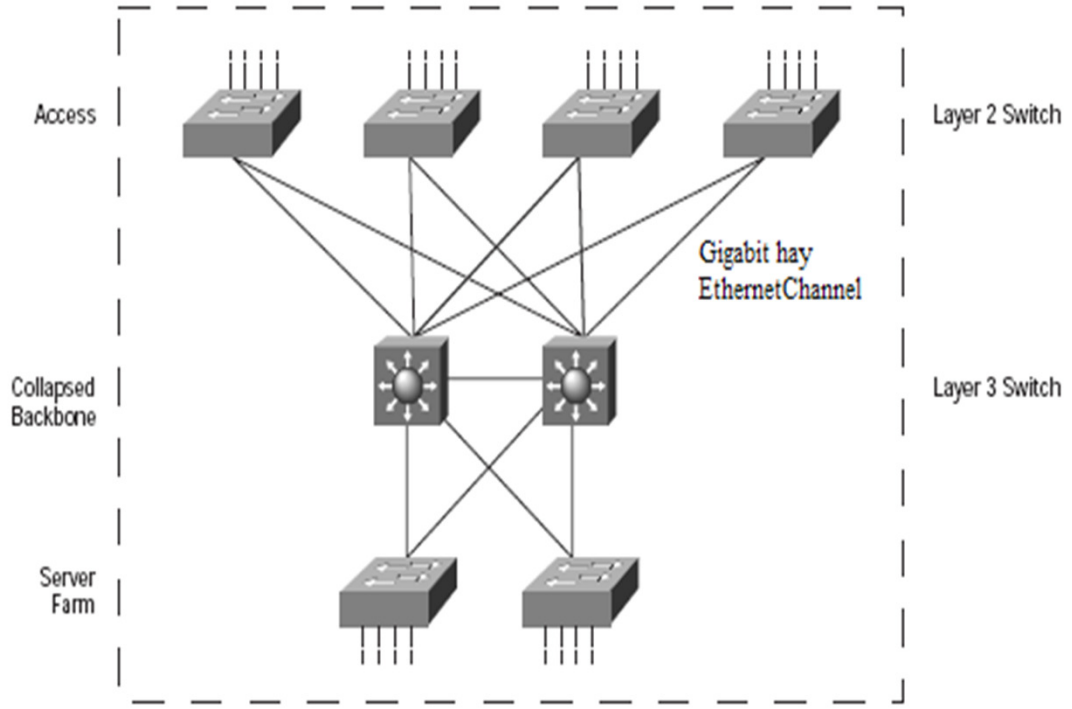


Thiết kế building network: building block không mở rộng VLAN (2/2)

- IP subnet giới hạn trong một switch (một wiring-closet)
- Không có vòng lặp (loop) và không có VLAN trunking giữa các layer 2 switch.
- Mỗi Gigabit uplink là giao tiếp được định tuyến trên các Layer 3 switch trong distribution layer.

Thiết kế building network: building block không mở rộng VLAN, dự phòng (1/2)

- Building block có dự phòng
- Hai Layer 3 switch tạo thành một building backbone giản lược

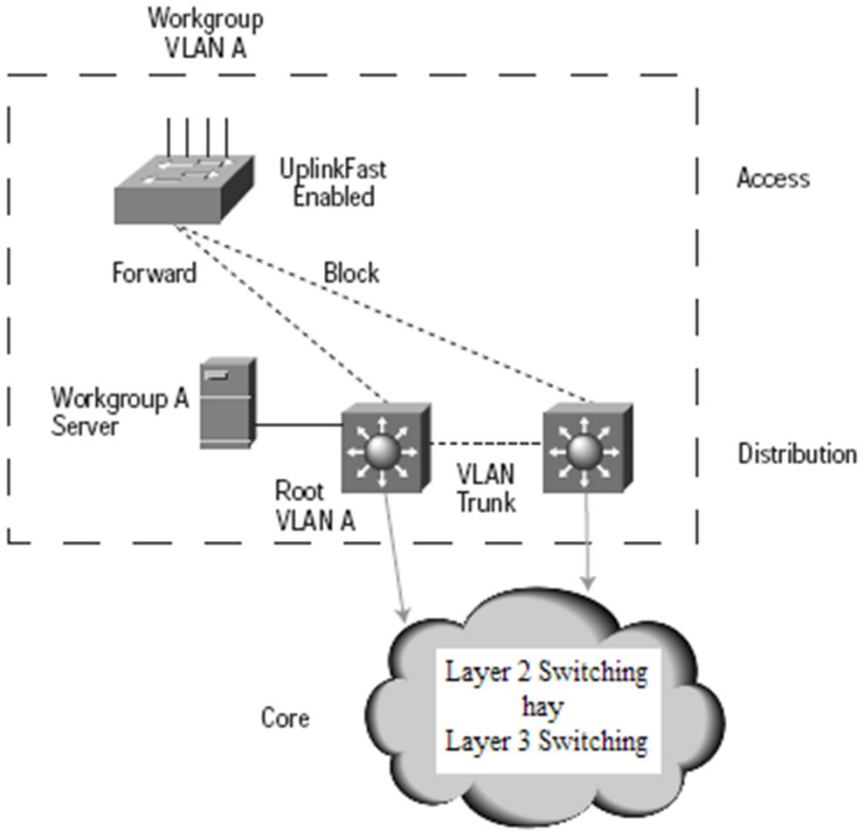


Thiết kế building network: building block không mở rộng VLAN, dự phòng (2/2)

- Tối ưu cho thiết kế building: tắt chức năng trao đổi định tuyến giữa các subnet (một subnet được giới hạn trong một tủ nối dây)
- Để thực hiện dùng passive interface command trên distribution-layer switch.
- Distribution-layer switch chỉ trao đổi định tuyến với core switch

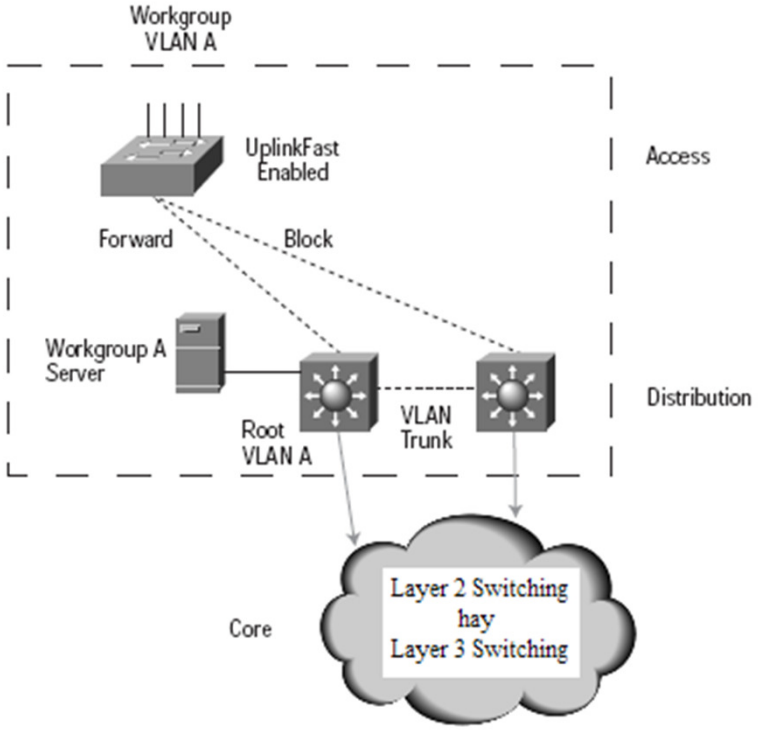
Thiết kế building network: building block mở rộng VLAN (1/3)

- Khi muốn server của nhóm A ở trong cùng subnet và VLAN như các client vì lý do liên quan đến chính sách.
- Đặt VLAN trunk giữa các distribution-layer switch



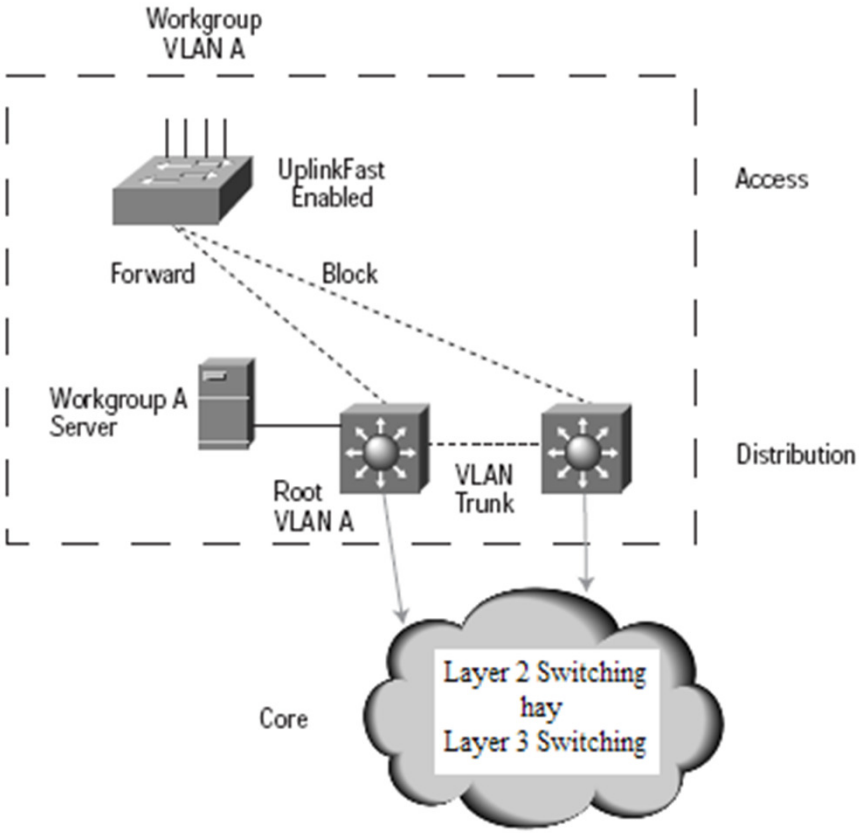
Thiết kế building network: building block mở rộng VLAN (2/3)

- VLAN cho nhóm A hình thành tam giác --> dùng STP đặt một link vào chế độ block.
- Topo tam giác phòng trường hợp một uplink bị hỏng, VLAN vẫn hoạt động bình thường nhờ VLAN trunk làm đường dẫn dự phòng tại layer 2.
- Một distribution-layer switch làm ST root cho các VLAN mang số chẵn và switch kia làm ST root cho VALN mang số lẻ.



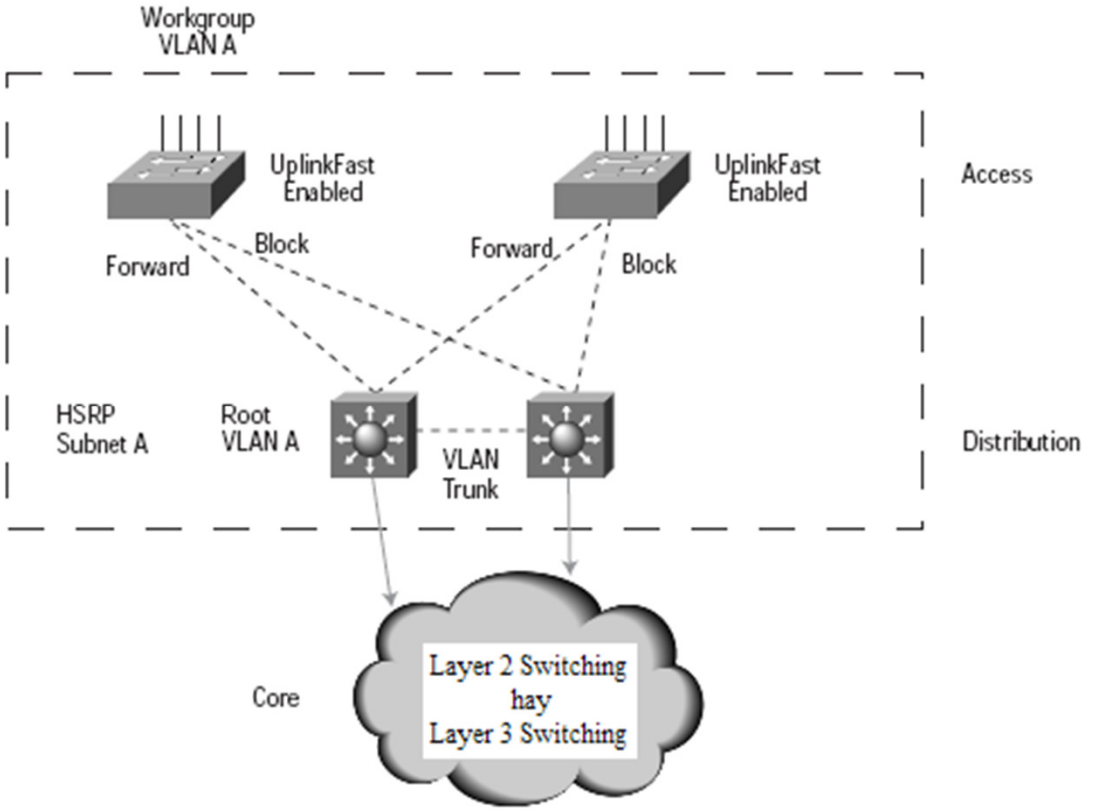
Thiết kế building network: building block mở rộng VLAN (3/3)

- Distribution-layer switch cũng làm HSRP cho các VLAN để đảm bảo cân xứng giữa lớp 2 và lớp 3
- Cho phép đặc tính UplinkFast trên mỗi switch lớp access để khôi phục nhanh ST ở lớp 2 (khi forwarding uplink bị hỏng, chỉ trong 2 giây blocking uplink sẽ chuyển sang forwarding mode)

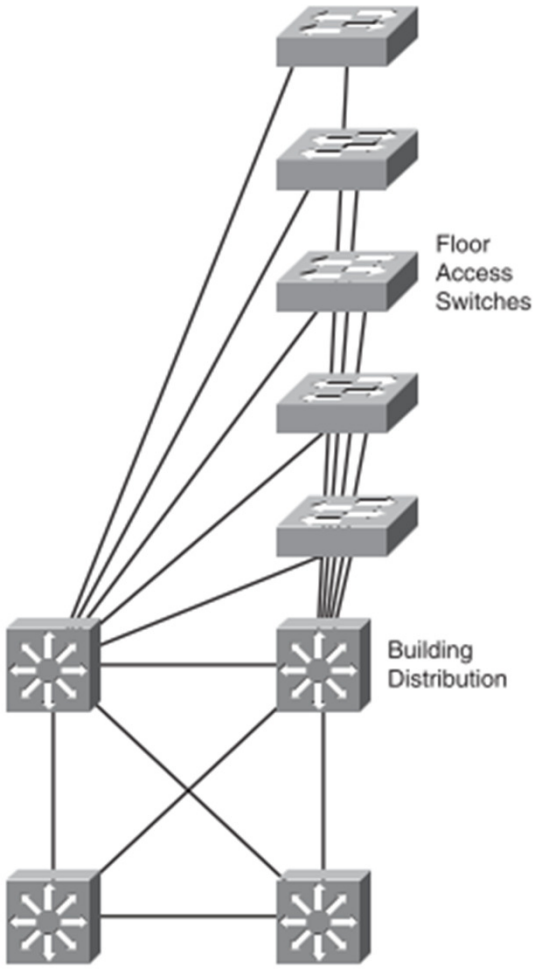


Thiết kế building network: building block mở rộng VLAN

- Tổng quát hơn với VLAN A trải ra nhiều switch

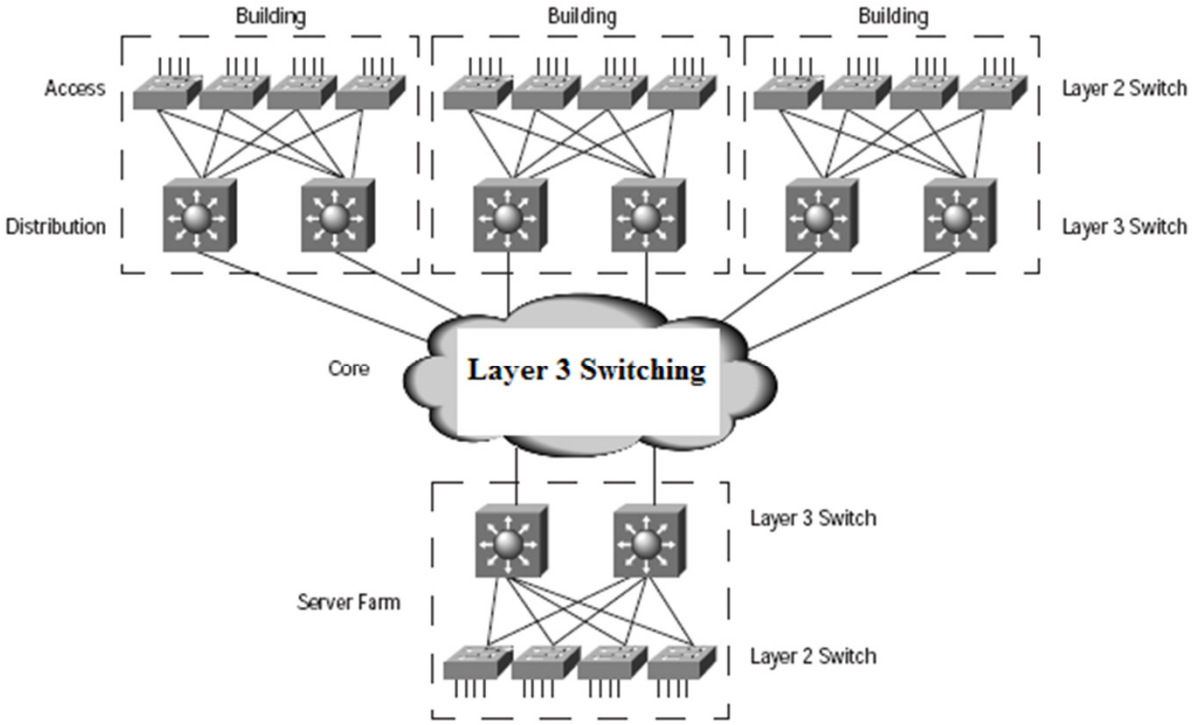


Sơ đồ cho Building LAN lớn



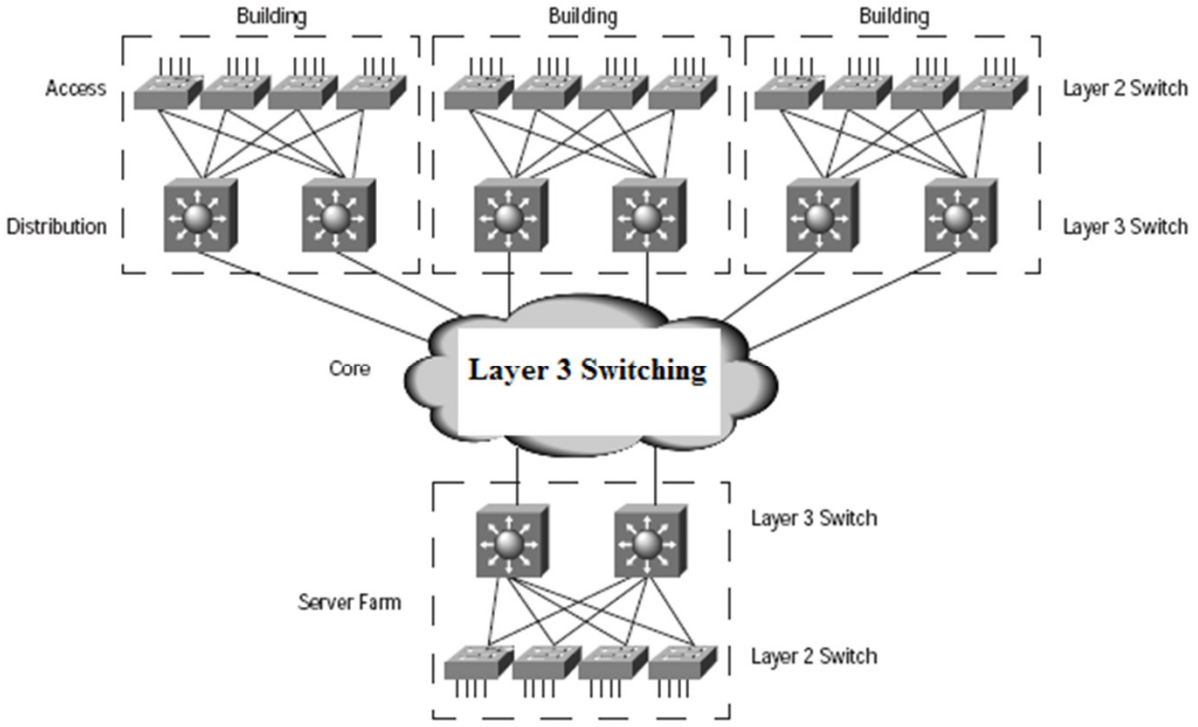
Thiết kế Campus đa lớp (1/3)

- Nhiều khối building kết nối qua campus backbone (--> Thiết kế backbone)
- Có tính khả triển
- Dự phòng building block được tăng cường từ dự phòng ở backbone
- Một backbone layer gồm ít nhất hai swicth, đặt ở các building khác nhau



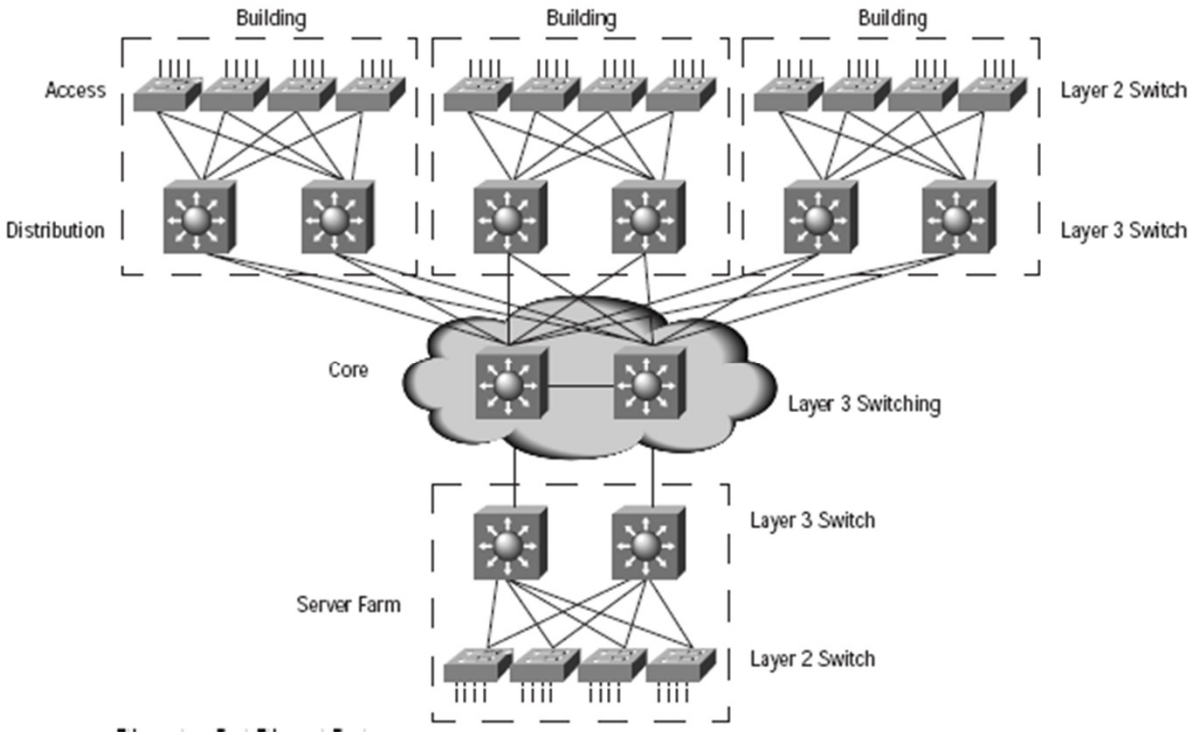
Thiết kế Campus đa lớp (2/3)

- Thiết kế campus đa lớp cần tối đa các ưu thế của các dịch vụ lớp 3 gồm: segmentation, load balancing, and failure recovery
- Định tuyến PIM kiểm soát lưu lượng IP multicast trong tất cả các Layer 3 switch.
- Hạn chế broadcast qua backbone (broadcast--> unicast)



Thiết kế Campus đa lớp (3/3)

- Dùng cặp đường dẫn để khôi phục nhanh
- Có thể dùng EtherChannel để tăng cường tính khả dụng
- Đặc tính hỗ trợ IP-based load balancing qua EtherChannel

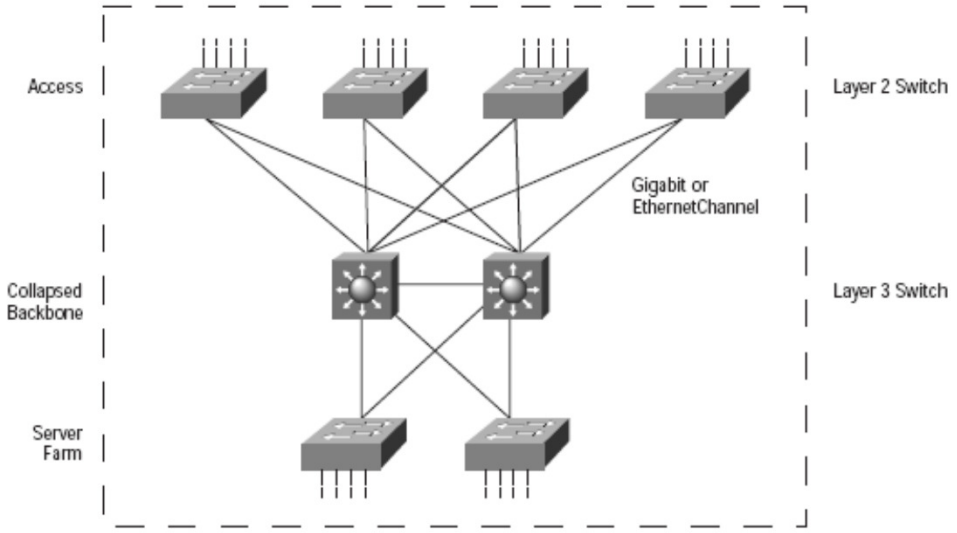


Thiết kế campus backbone nhỏ (1/3)

- **Backbone giản lược**. Gồm hai hay nhiều layer 3 switch như mạng building.
- Các layer 3 switch phải duy trì các mục ARP cho các thiết bị hoạt động trong campus.

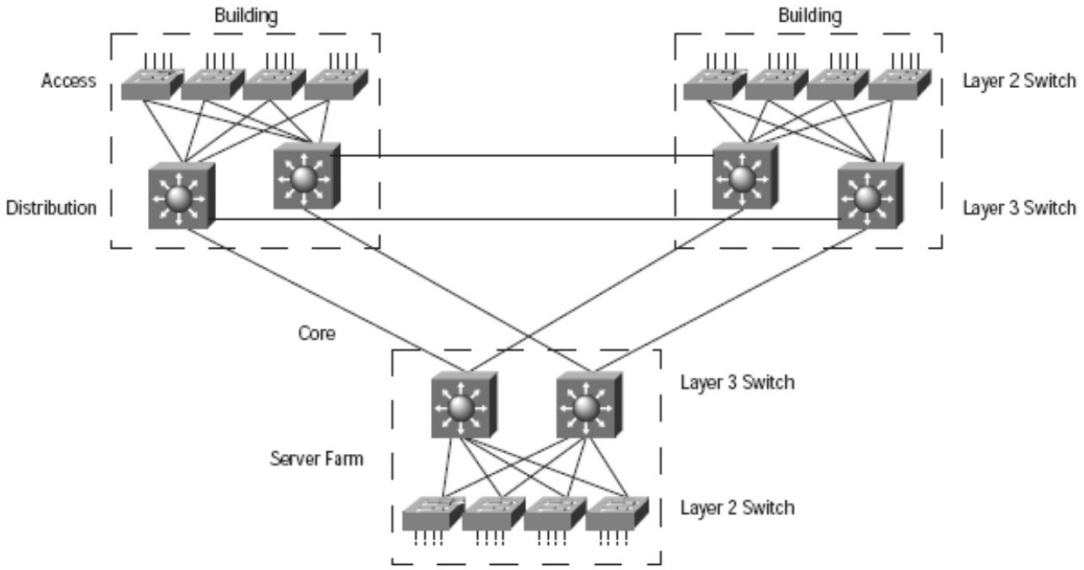
Hoạt động ARP quá mức--> CPU-->backbone performance

Giải pháp



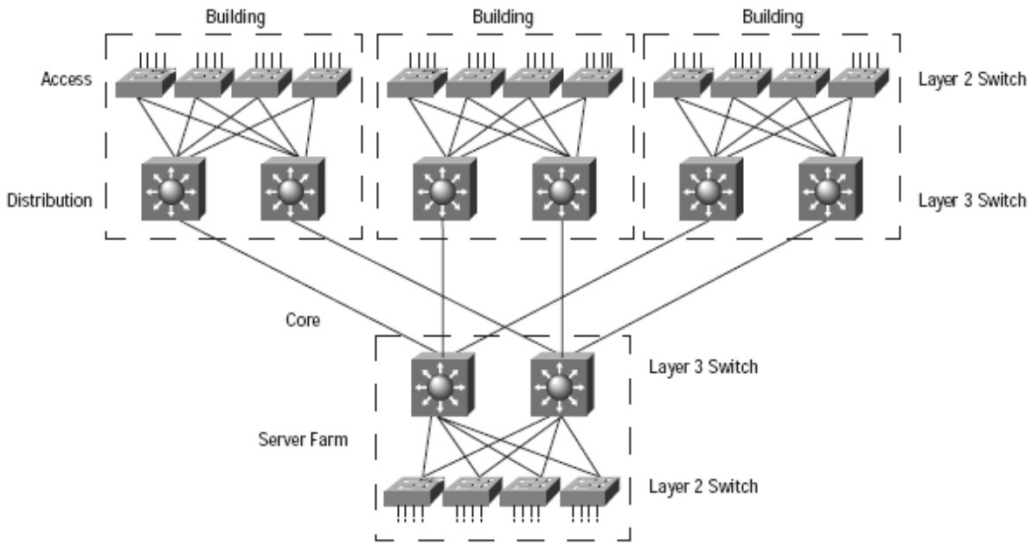
Thiết kế campus backbone nhỏ (2/3)

- **Full-mesh backbone** gồm ba module với các Layer 3 switch được liên kết trực tiếp thành một full mesh.
- Tăng module---> tăng phức tạp
- Nâng cấp băng thông cũng khó



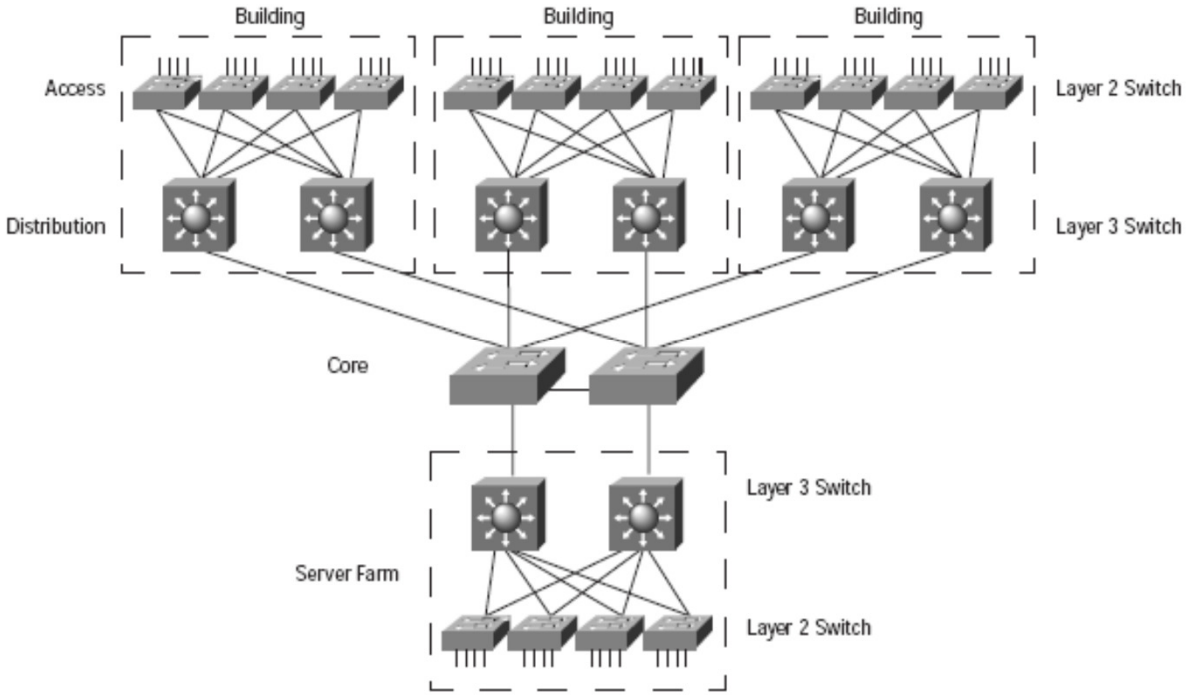
Thiết kế campus backbone nhỏ (3/3)

- **Partial mesh backbone**.
- Thích hợp cho campus nhỏ, lưu lượng chủ yếu hướng vào server farm.
- Dùng trunk dung lượng lớn từ các layer 3 switch của các building đến server farm
- Các layer 3 switch của server farm trở thành backbone giản lược cho lưu lượng giữa hai module



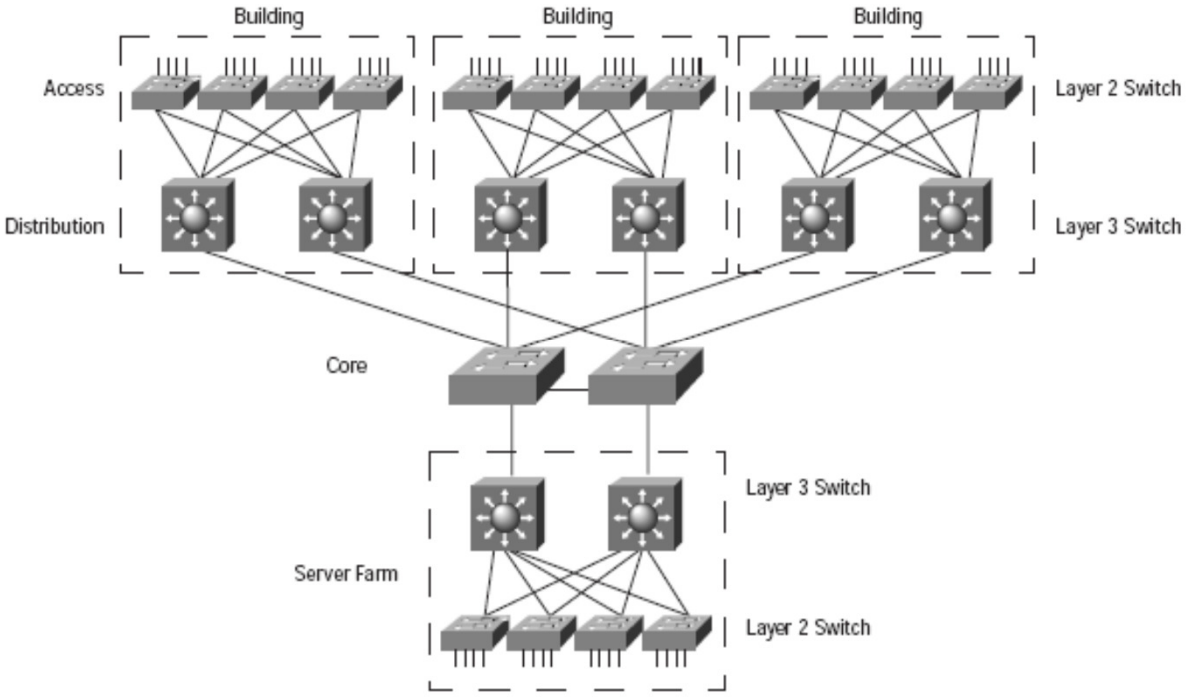
Thiết kế campus backbone lớn: Layer 2 switched backbone (1/2)

- **Layer 2 switched backbone,** thích hợp cho campus có từ ba tòa nhà trở lên.
- Bổ sung các switch vào backbone làm giảm số kết nối và dễ bổ sung module.
- Backbone thực sự là layer 2 switched domain có dạng star



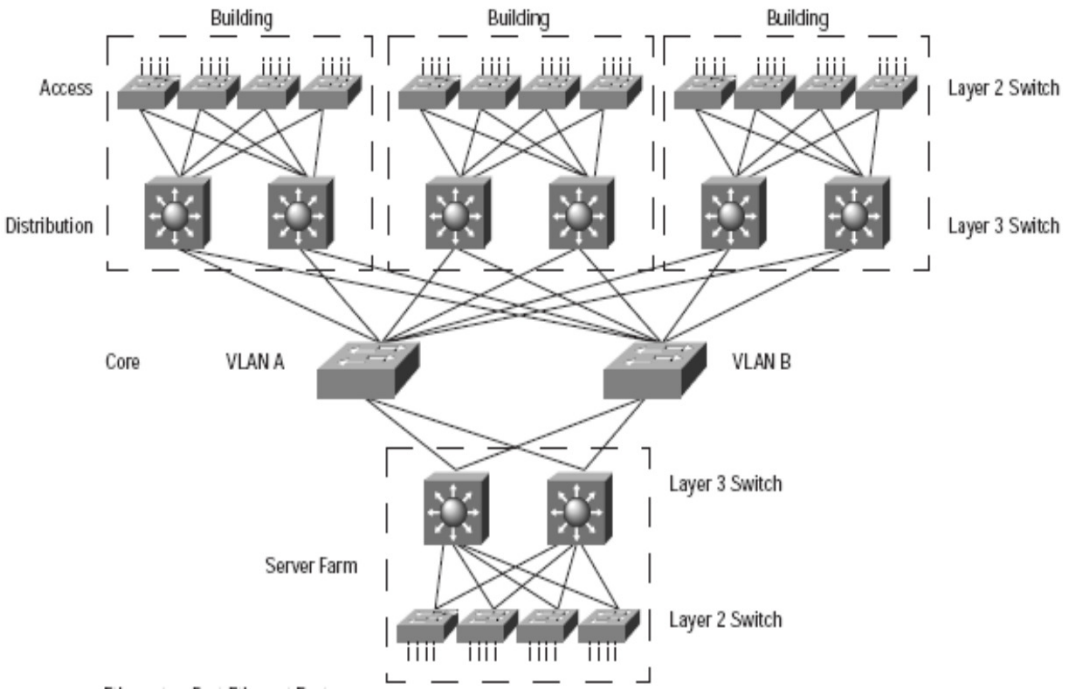
Thiết kế campus backbone lớn: Layer 2 switched backbone (1/2)

- Dùng một IP subnet cho backbone
- Mỗi switch lớp distribution định tuyến lưu lượng qua backbone subnet
- Cấu hình các liên kết nối đến backbone thành các giao tiếp được định tuyến, không phải là VLAN trunk (<>spanning tree protocol loop)



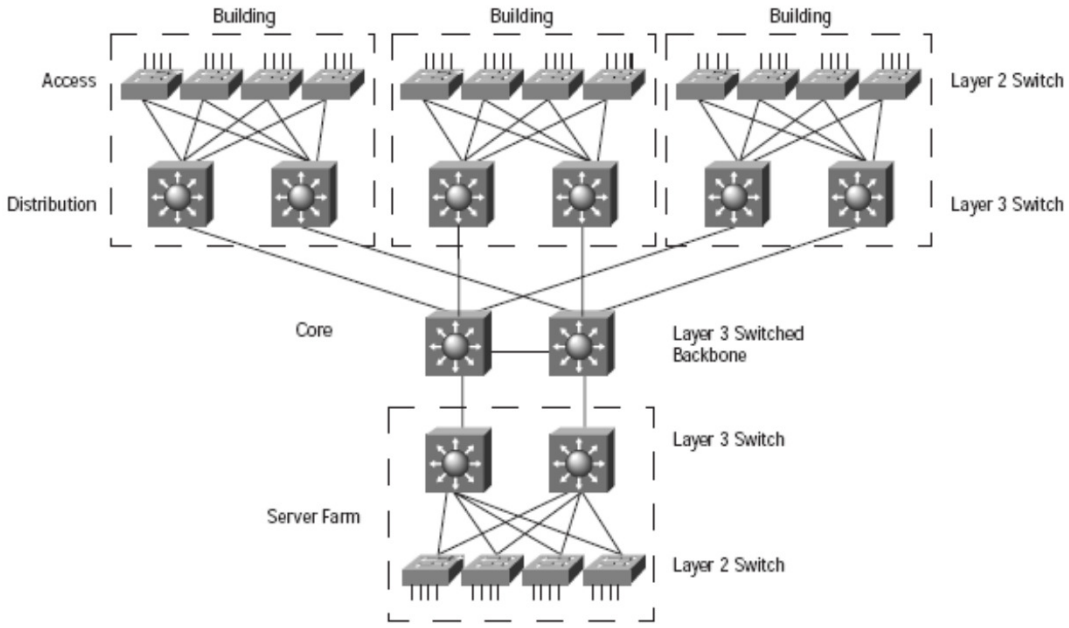
Thiết kế campus backbone lớn: Layer 2 switched backbone (2/2)

- **Split layer 2 backbone**
- Tăng tính khả dụng và dung lượng.
- Hình thành hai backbone riêng biệt dự phòng cho nhau.



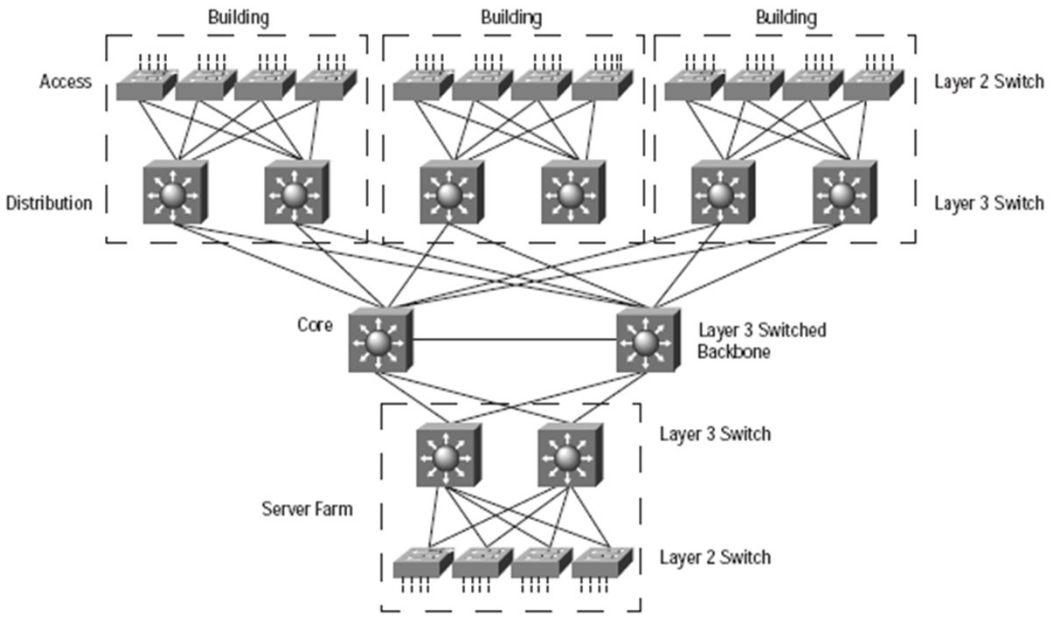
Thiết kế campus backbone lớn: Layer 3 switched backbone (1/3)

- **Layer 3 switched backbone**
- Backbone linh hoạt và khả triển nhất dùng các chuyển mạch lớp 3. Các chuyển mạch được kết nối bởi các Gigabit Ethernet hay EtherChannel được định tuyến.



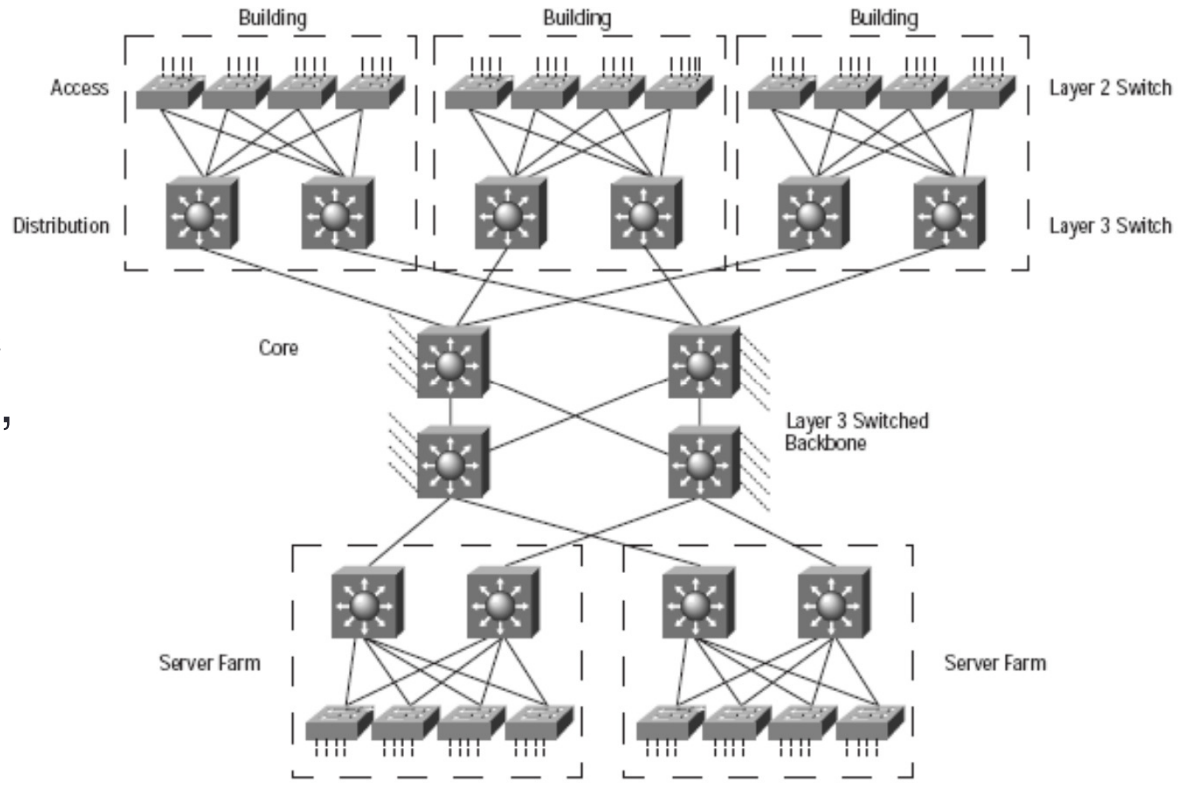
Thiết kế campus backbone lớn: Layer 3 switched backbone (2/3)

- Dự phòng đường đi để khôi phục nhanh.
- Cũng gấp đôi dung lượng cho trunk



Thiết kế campus backbone lớn: Layer 3 switched backbone (3/3)

- Large-Scale Layer 3 Switched Campus Backbone
- Backbone có 4 switch lớp 3 nối nhau bằng các liên kết Gigabit Ethernet, đều được định tuyến, không có ST loop

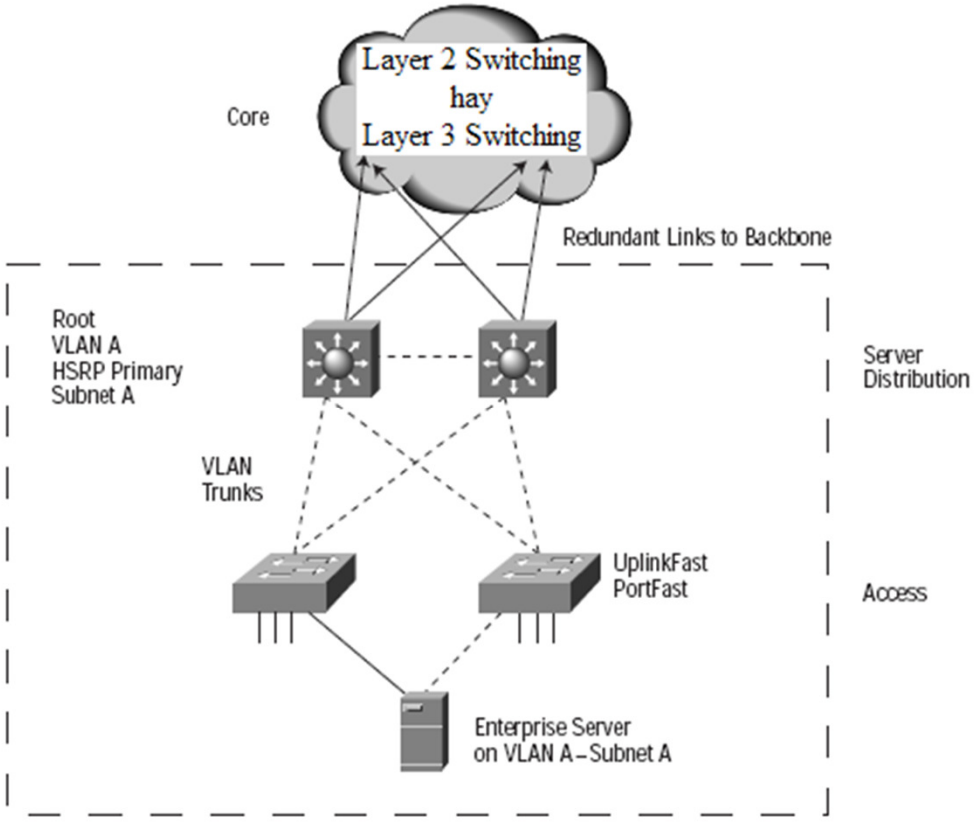


Thiết kế Server Farm

- Một building block tốc độ cao nối vào backbone.
- Nơi host các ứng dụng mạng của doanh nghiệp, mức độ tranh chấp phải thấp
- Hạn chế oversubscription

Thiết kế Server Farm

- Kết nối server có nhiều cách: có thể dùng một hay hai Fast Ethernet. Nếu có 2 kết nối thì một ở chế độ dự phòng.
- Dual-homing cho phép tăng tính khả dụng, dùng Layer 2 dual homing hay Layer 3 dulal-homing (phức tạp ~ NOS)
- Hai yếu tố chính: dạng lưu lượng, số user (Tốc độ trung bình phát gói và kích thước gói trung bình)



Dự phòng server (1/3)

- Các server: file, web,DHCP, DNS, Database
- Cân nhắc nhu cầu và dự phòng, ví dụ server làm nhiệm vụ ánh xạ số điện thoại và địa chỉ IP trong VoIP
- DHCP server có thể được đặt ở access hay distribution layer
- Trong mạng nhỏ DHCP dự phòng đặt tại distribution layer, trong mạng lớn DHCP luôn đặt tại access layer?

Dự phòng server (2/3)

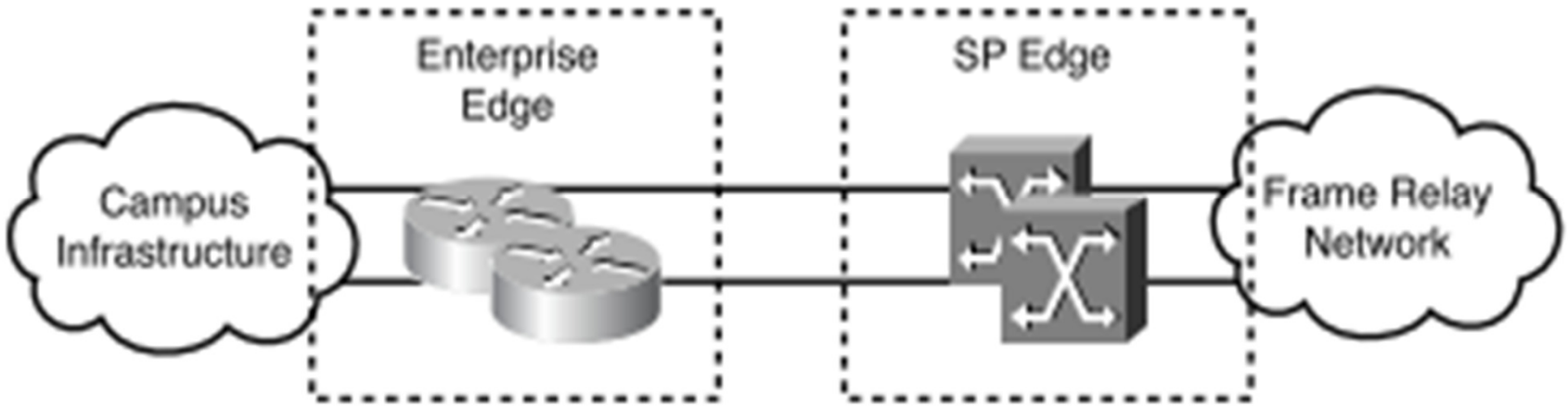
- Nếu DHCP được đặt về phía bên kia của router, cần cấu hình router để chuyển các DHCP broadcast từ các host.
- DNS server có thể được đặt tại access hay distribution layer
- Trong các ứng dụng mà thời gian ngưng trệ file server là lỗi nghiêm trọng thì phải thực hiện các bản sao y cho các file server.

Dự phòng server (3/3)

- Bố trí các file server trên các mạng khác nhau nhưng phải có kỹ thuật đồng bộ để đồng nhất (dùng duplexing, SAN)
- Dự phòng server cũng có thể cho phép các server chia sẻ tải với nhau, dùng CDN (content delivery network) hay các thiết bị dịch vụ nội dung

Thiết kế topo cho enterprise edge

- Tùy vào nhu cầu performance cần thiết kế dự phòng segment WAN trong intranet, nhiều path đến extranet và Internet.
- Dùng VPN kết nối các cơ sở của doanh nghiệp thông qua mạng WAN công cộng hay Internet

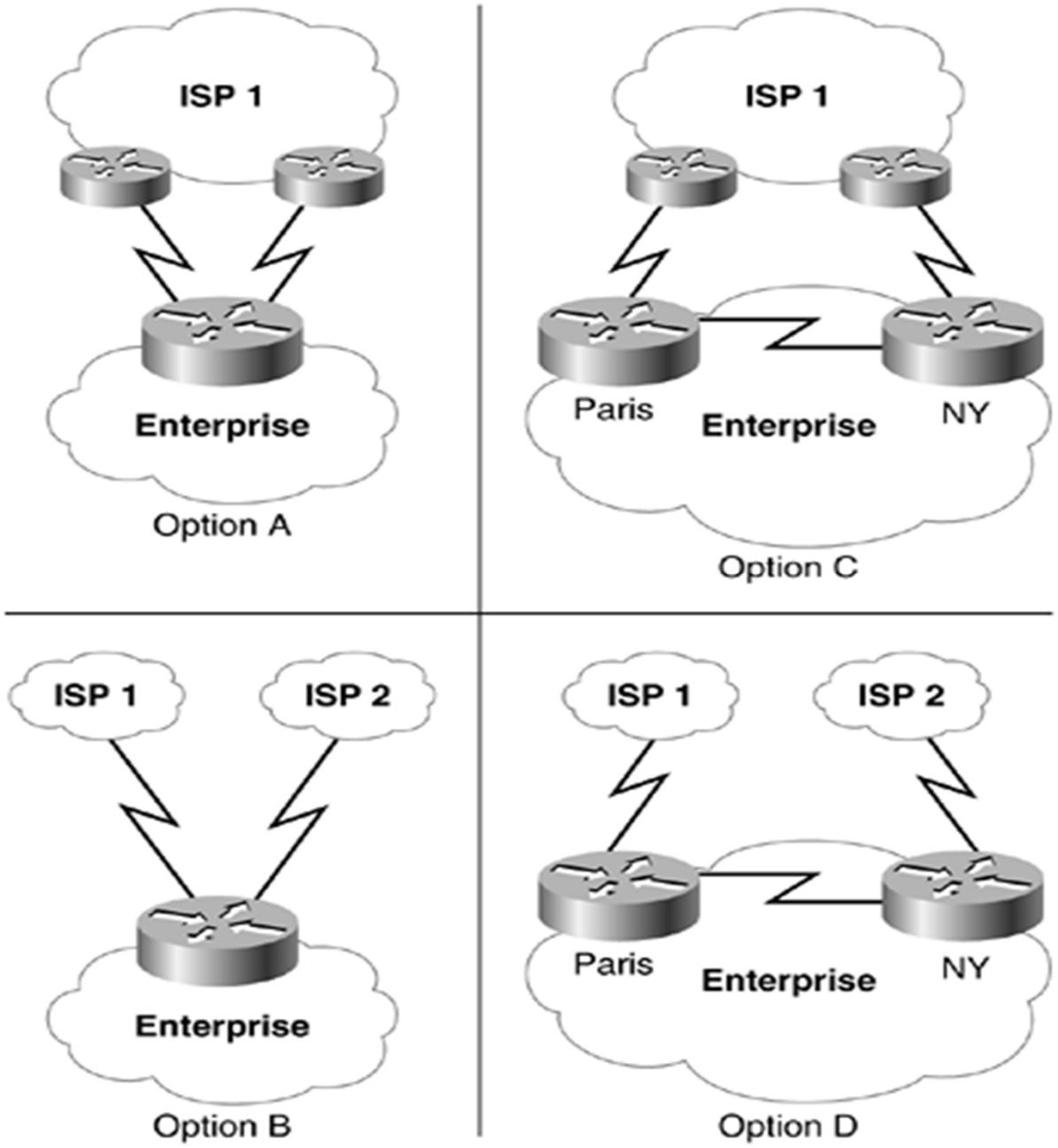

Enterprise
Edge
SP Edge
Campus
Infrastructure
Frame Relay
Network

Dự phòng WAN segment

- WAN có thể được thiết kế theo dạng partial mesh
- Nên khảo sát kỷ mạch vật lý, để đảm bảo đường dự phòng là dự phòng thực sự (circuit diversity) <-- các carrier thuê dung lượng lẫn nhau
- Khi phân tích circuit diversity phải chú trọng vào đường cáp cục bộ và dịch vụ của nhà cung cấp đường truyền
- Ghi rõ cam kết về circuit divesity vào hợp đồng

Dự phòng nhiều kết nối Internet

- Thuật ngữ multihome
- Có thể multihome đến Internet cho Enterprise theo nhiều cách tùy vào nhu cầu.
- Xem hình mô tả 4 lựa chọn


ISP 1
Enterprise
Option A
ISP 1
Paris
Enterprise
NY
Option C
ISP 1
ISP 2
Enterprise
Option B
ISP 1
ISP 2
Paris
Enterprise
NY
Option D

VPN (1/2)

- VPN là phương pháp dùng encryption tiên tiến và tunneling để kết nối qua một third-party network
- Tunneling protocol
- Giao thức đường hầm ở lớp 2: Point -to-Point Tunneling Protocol (PPTP), Layer 2 Forwarding (L2F), MPLS VPN, Layer 2 Tunneling (L2TP_ RFC 2661), L2TPv3
- Giao thức đường hầm lớp 3: IPSec, Cisco Generic Routing (GRE)

VPN (2/2)

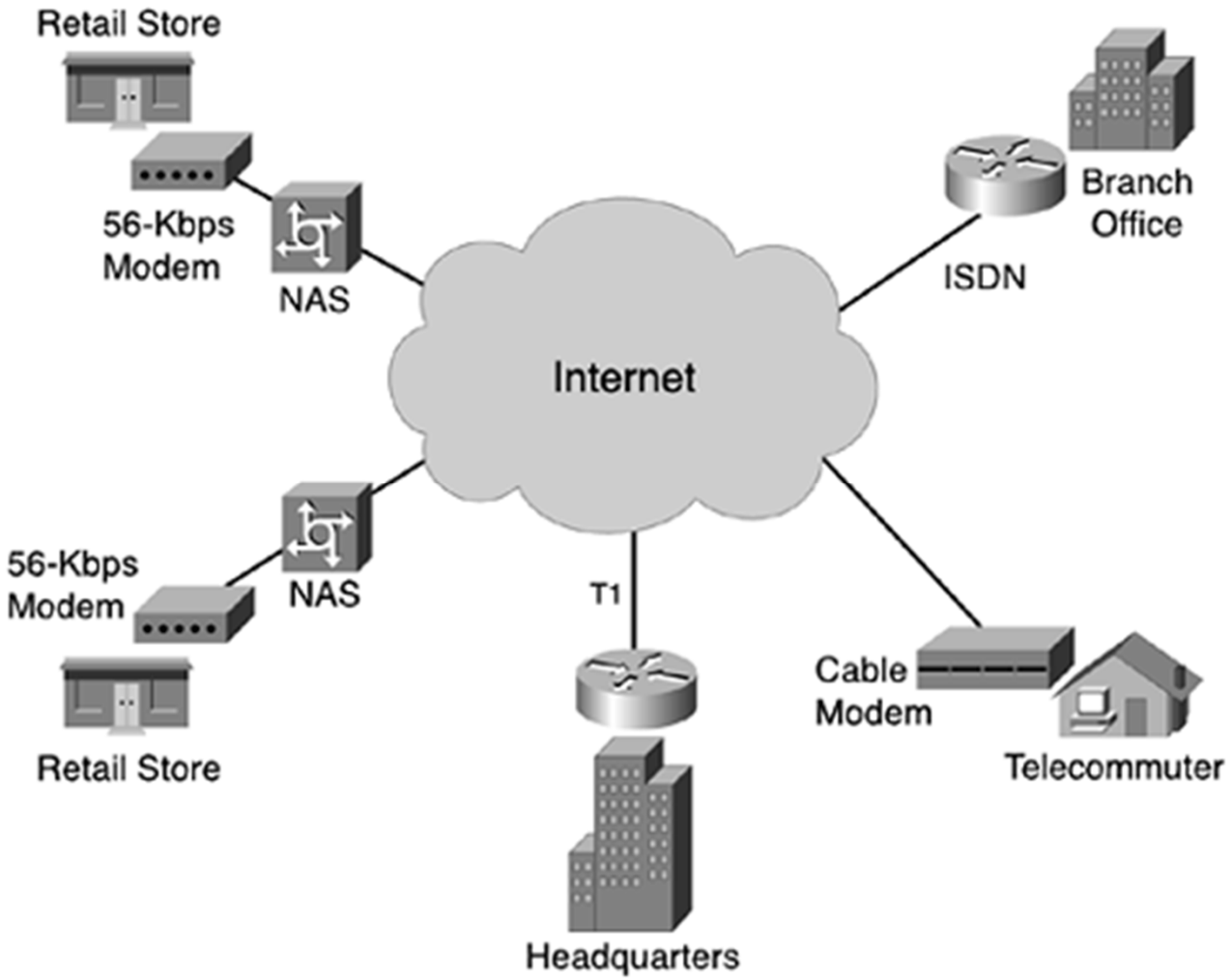
- IPSec cho IP unicast, GRE cho multicast, broadcast và non-IP cần tunneling
- VPN áp dụng cho Enterprise được chia thành 2 loại:
  - Site-to-site VPN: kết nối trải ra trên nhiều cơ sở, nhiều tổ chức
  - Remote Access: kết nối các user ở xa và các đối tác kinh doanh

Site-to-site VPN

- Thay cho PDN (private data network)
- Trước đây thường dùng T1 để kết nối các cơ sở, chi phí cao
- Các topo phổ biến nhất cho site-to-site network là:
  - Hub-and-spoke: 1 headquarter và nhiều chi nhánh
  - Mesh: kết nối nhiều khu vực tập trung với lưu lượng lớn trao đổi giữa các cơ sở.
  - Hiearachical: nhiều headquarter và nhiều vùng với lưu lương rất lớn. Topo gồm full hay partial mesh core với các cơ sở ngoại vi nối với core dùng hub-and-spoke

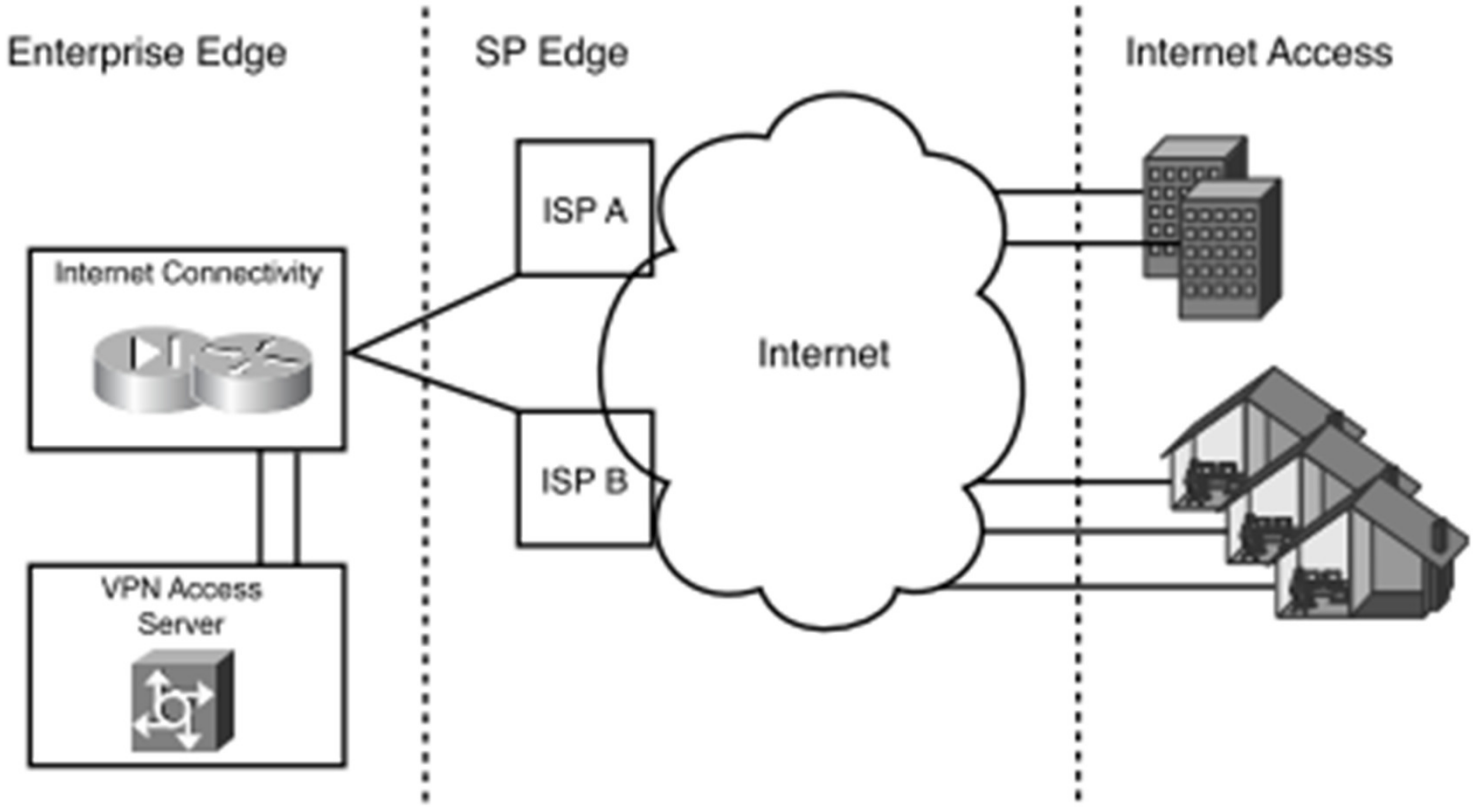
Remote Access VPN

- Cho phép truy xuất theo nhu cầu qua kết nối được mật mã.
- Xác định nơi tiến hành tunneling và encryption, trên client hay network access server
- Nếu khởi động phía client thì một tunnel bảo mật được thiết lập bởi client software dùng IPSec, L2TP hay PPTP, ưu điểm là bảo mật cả đoạn "last mile" từ client đến POP (point of presence của nhà cung cấp dịch vụ

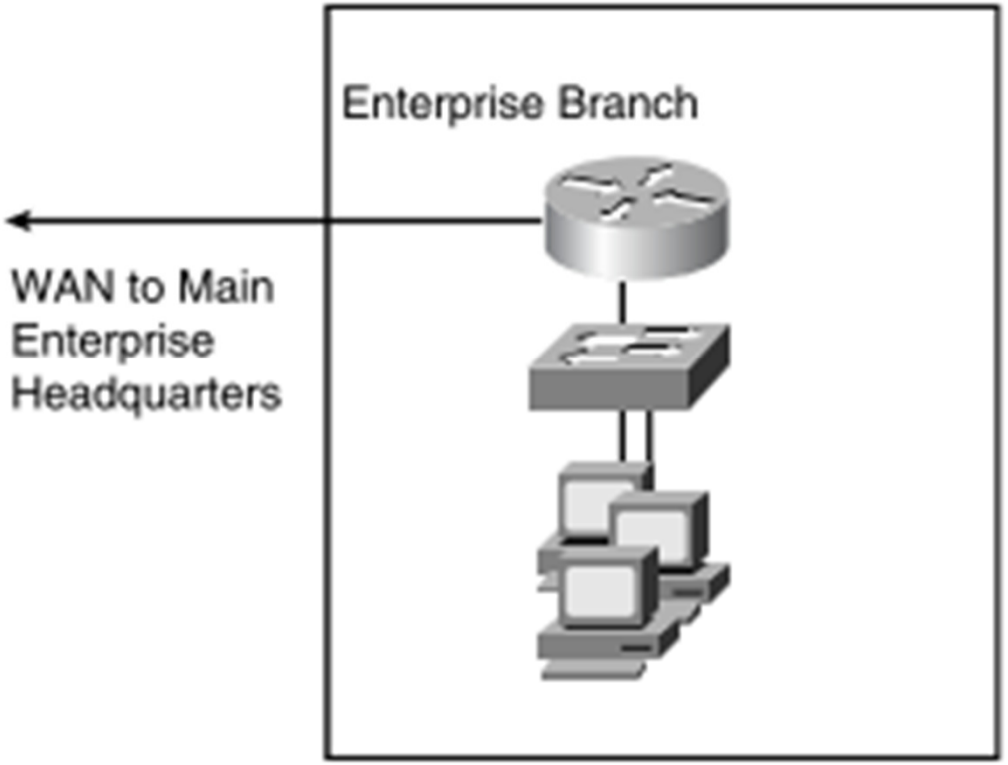


Ví dụ về Remote Access VPN cho một công ty bán lẻ

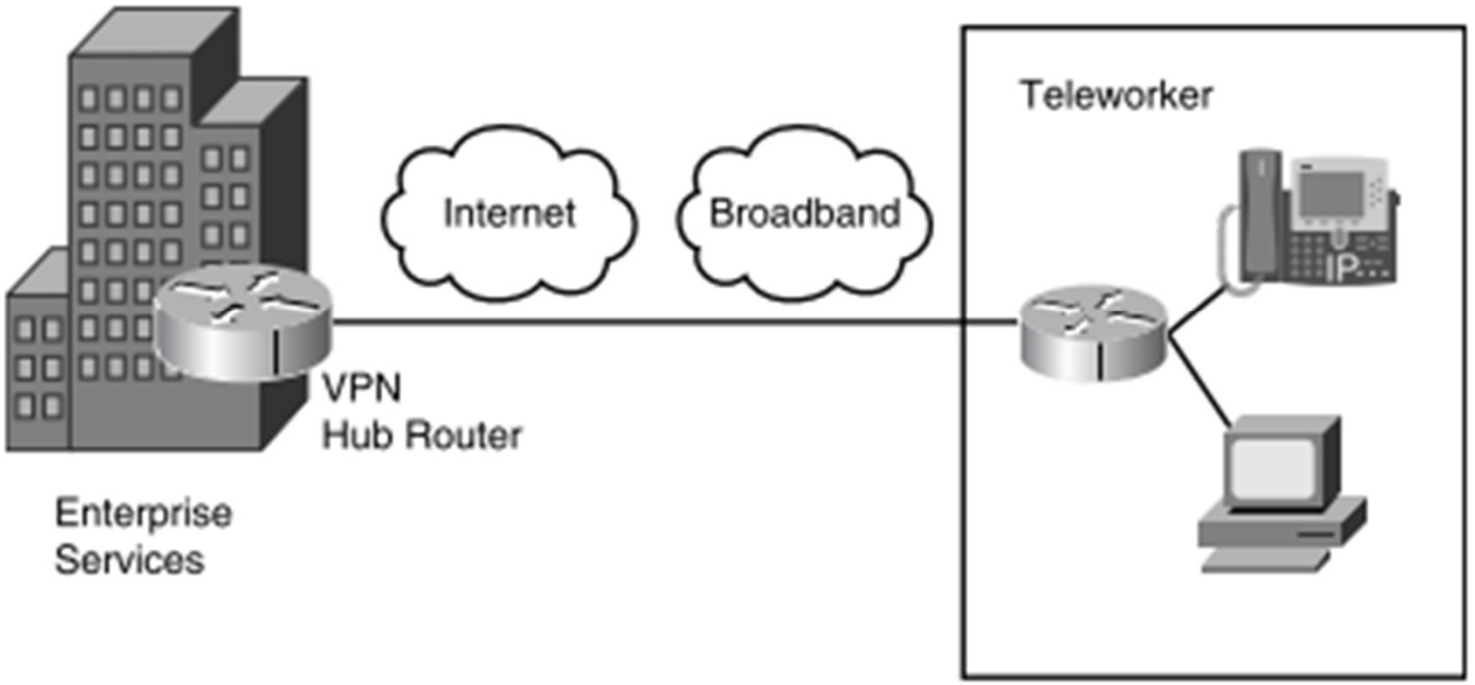
VPN Architecture



Enterprise Branch Module



Enterprise Teleworker Module



THIẾT KẾ AN NINH MẠNG

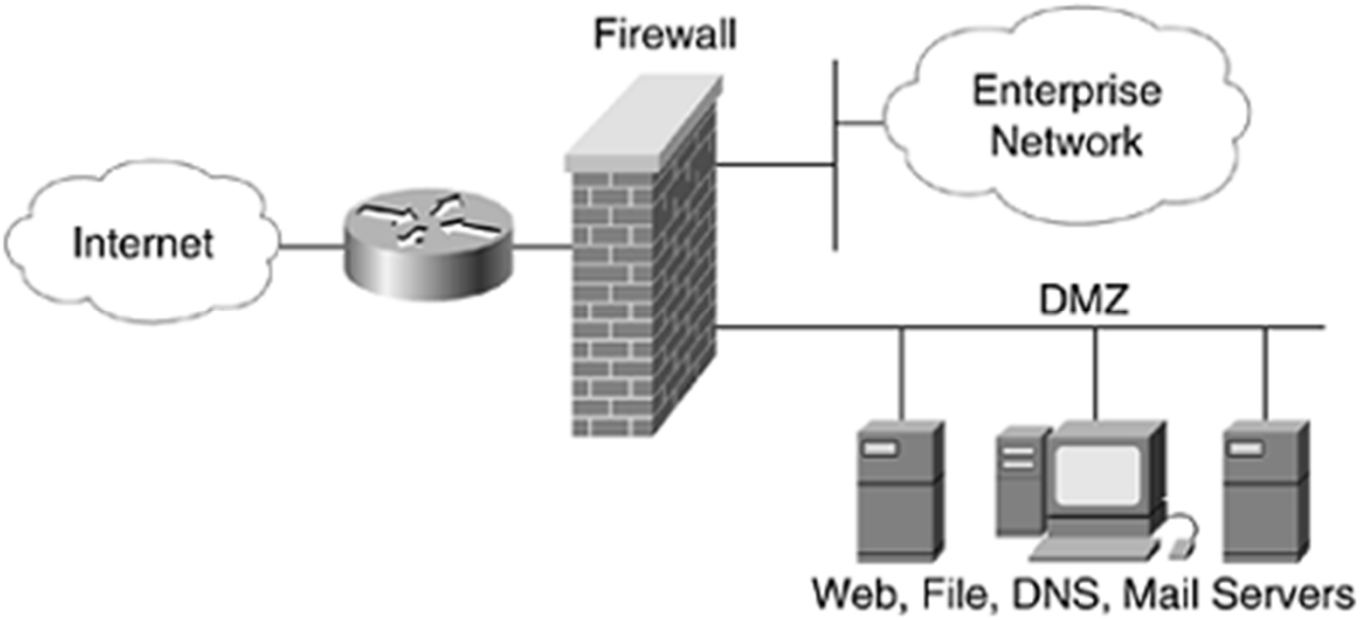
Tổng quan thiết kế an ninh mạng

- Đảm bảo an ninh mạng là quá trình liên tục
- Chu kỳ: thi công, giám sát, kiểm thử và cải tiến
- Cập nhật liên tục các cơ chế an ninh để chống lại các kiểu tấn công mới nhất
- Xác định tài nguyên cần bảo vệ
- Phân tích các nguy cơ
- Phân tích các yêu cầu an ninh và cân nhắc lợi hại
- Xây dựng kế hoạch an ninh
- Xây dựng chính sách an ninh
- Xây dựng thủ tục và qui trình an ninh

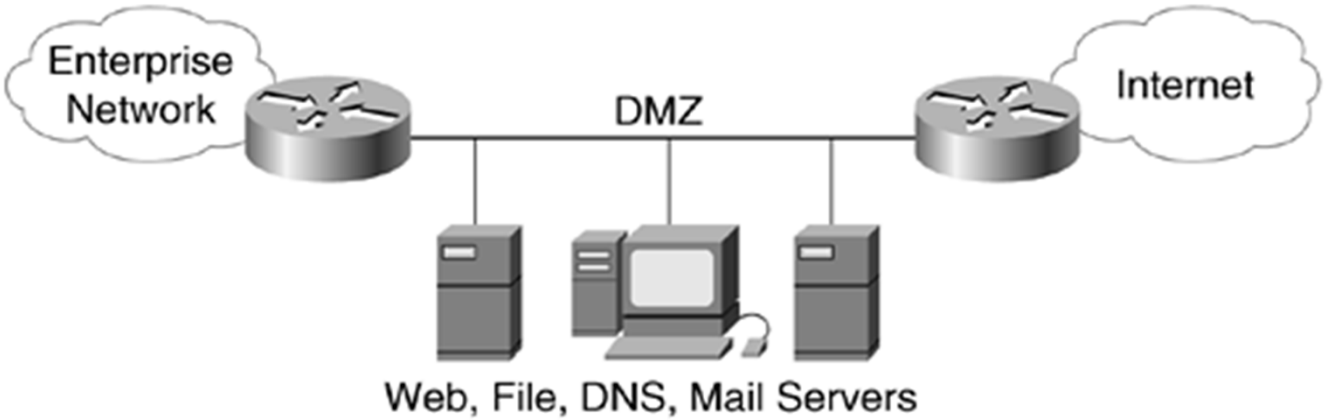
Firewall

- Là nơi thi hành phần lớn các security policy tại biên giới mạng
- Chứa tập luật chi phối lên traffic
- Static packet-filter firewall
- Statefull firewall
- Proxy firewall

Firewall (DMZ) topology



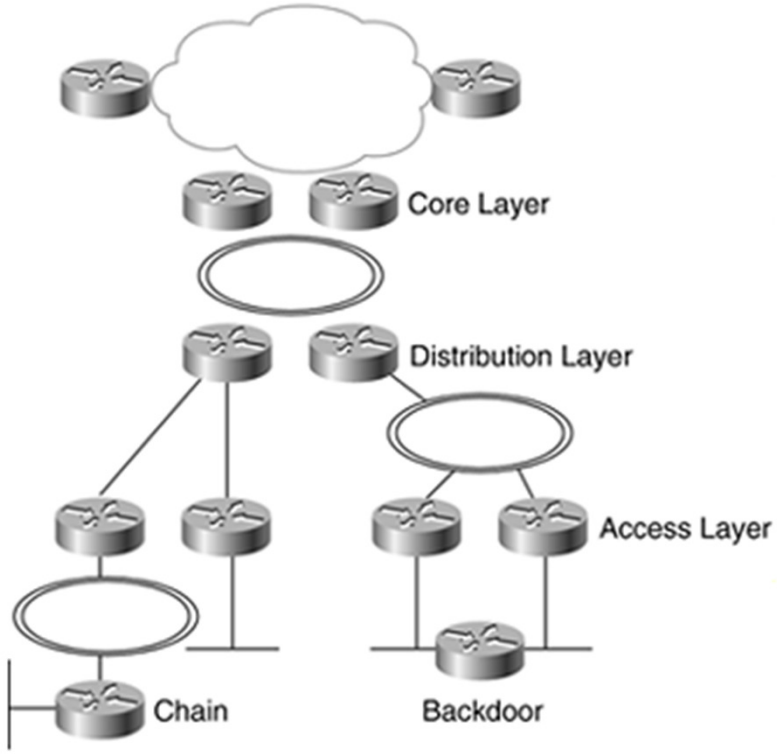
Three-Part firewall topology



- Cấu hình phức tạp
- Traffic của Enterprise chạy qua DMZ , DMZ có thể bị thỏa hiệp làm bàn đạp tấn công Enterprise.
- Giải pháp: dùng các ACL tại các router, dùng firewall với cấu hình nhiều ACL hơn, chạy phần mềm firewall trên các host trong DMZ và cấu hình dịch vụ giới hạn.

Lưu ý an ninh mạng phân cấp

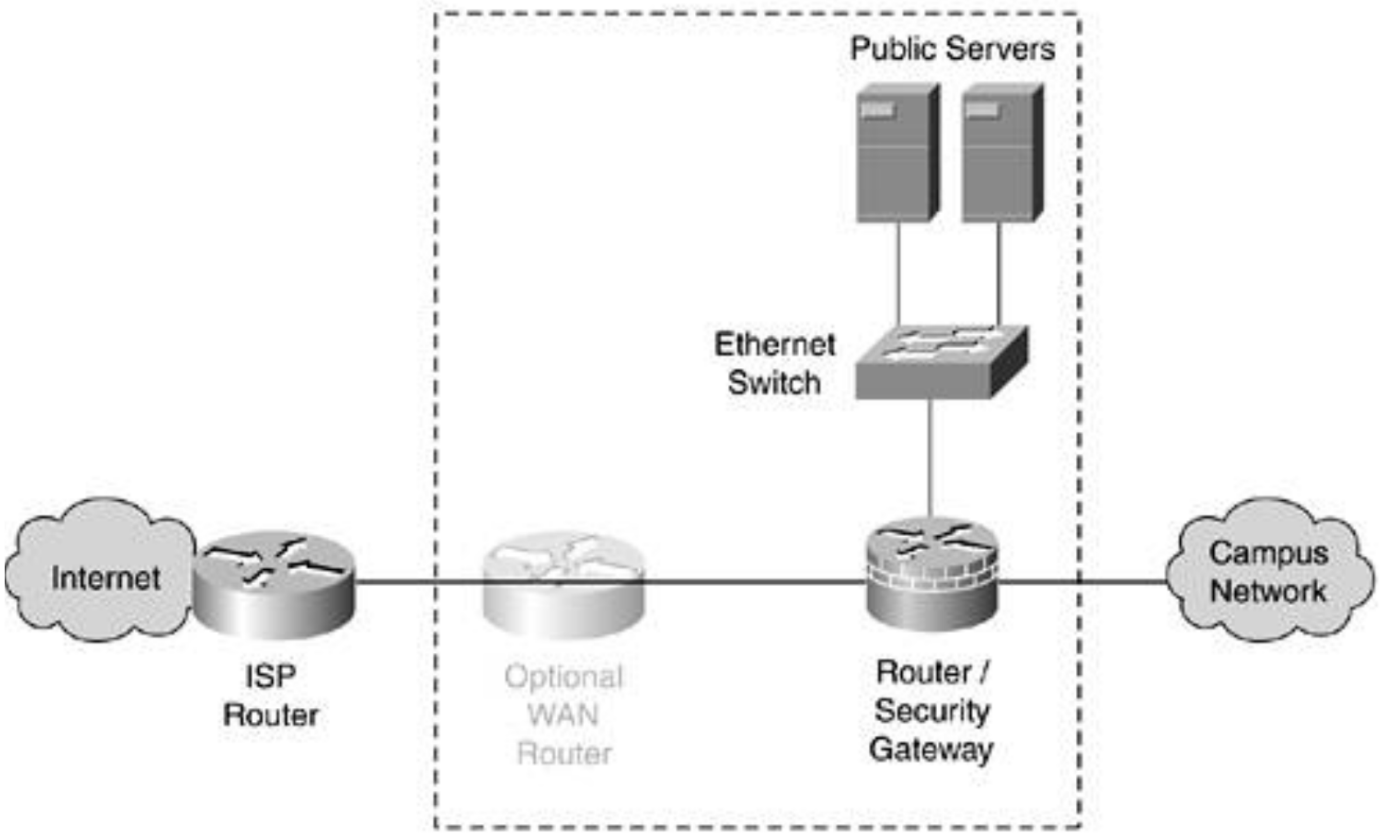
- Kiểm soát chặt chẽ topo mạng tại access layer
- Chú ý các lỗi:
  - Adding a chain
  - Backdoor



An ninh mạng vành đai

- Mạng vành đai cỡ nhỏ
- Thiết kế tiêu biểu
- Phân tích các nguy cơ an ninh
- Đề xuất áp dụng giải pháp an ninh cho từng bộ phận

Thiết kế tiêu biểu



Các nguy cơ an ninh

- Buffer overflow
- Virus/worm/Trojan horse
- Direct access
- Probe/scan
- Application flooding
- Rootkit
- Remote control software
- Identity spoofing
- Web application

Đề xuất áp dụng giải pháp an ninh cho từng bộ phận

- Gateway
- WAN router
- Ethernet switch
- Public server
- Kết nối Internet

Gateway

- Cài đặt lọc stateful và stateless .
- Áp đặt Signature-based NIDS
- Củng cố bản thân thiết bị
- Cài đặt các bộ lọc theo RFC 2827, RFC 1918, và bogon filtering
- Cài đặt lọc ICMP
- Nên cài đặt CAR (committed access rate)
- Áp dụng TCP intercept để tối thiểu ảnh hưởng của TCP SYN flood trên host

WAN router

- Cài đặt các bộ lọc vào/ra theo RFC 2827, RFC 1918, và bogon filtering
- Có thể bổ sung uRPF
- Cài đặt lọc ICMP
- Có thể sử dụng xác thực giao thức định tuyến
- Cài đặt CAR để chống DDoS

Ethernet Switch

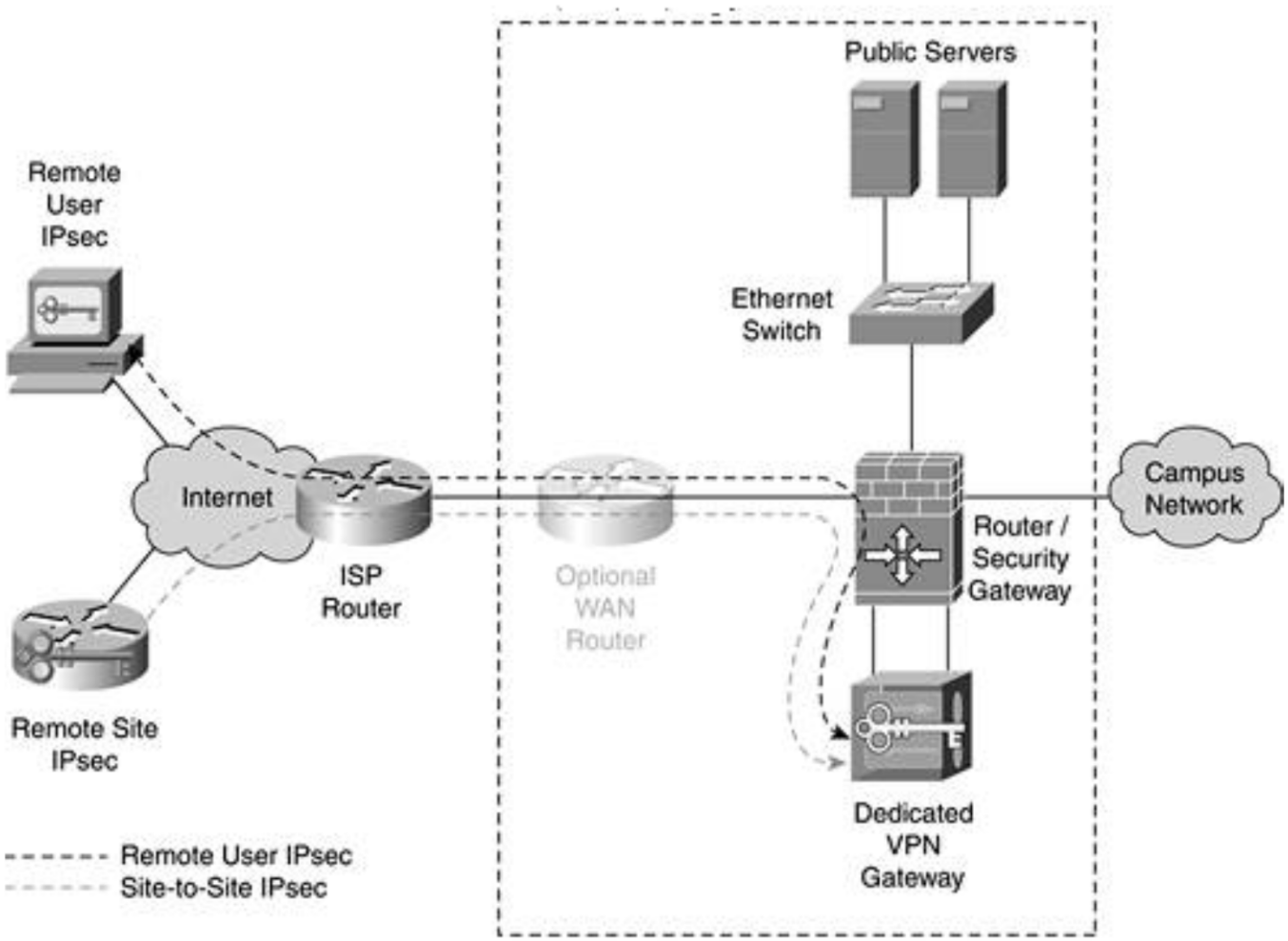
- Tất cả các switch nên thực hiện theo thủ tục an toàn cho giao thức điều khiển lớp 2.
  - Luôn dùng một VLAN ID cho tất cả các trunk ports.
  - Tránh dùng VLAN 1.
  - Cài đặt tất cả user ports thành nontrunking.
  - Triển khai port security khi có thể cho các user ports.
  - Chọn một hay nhiều tùy chọn an ninh ARP.
  - Mở tính năng giảm nhẹ tấn công STP (BPDU Guard, Root Guard).
  - Dùng PVLAN ở những chỗ thích hợp.
  - Dùng MD5 authentication cho VTP khi cần dùng VTP.
  - Với thiết bị Cisco thì cấm CDP khi không cần đến.
  - Cấm tất cả các port không dùng và nhóm chúng trên một VLAN không dùng.
  - Ngăn chặn tấn công DHCP.
- Cấu hình port security trên public server switch
- Dùng VLAN để hỗ trợ quản lý an ninh của thiết bị này.
- Nếu ARP inspection có sẵn trên switch được dùng trên mạng chứa public server thì nên cho phép tính năng này.
- Cấu hình Private VLAN trên public server switch để tách biệt các public server không cần thông tin trực tiếp với nhau.

Public server

- Xác thực đăng nhập bằng mật khẩu (dùng lại)
- Dùng PKI/sessionapp crypto: Nếu các public servers đều cung cấp các kết nối HTTPS, cần có chứng nhận từ một nguồn tin cậy trên Internet.
- Củng cố hệ điều hành và các ứng dụng
- Kiểm tra tính toàn vẹn của file system
- Dùng host antivirus/host IDS

Kết nối Internet

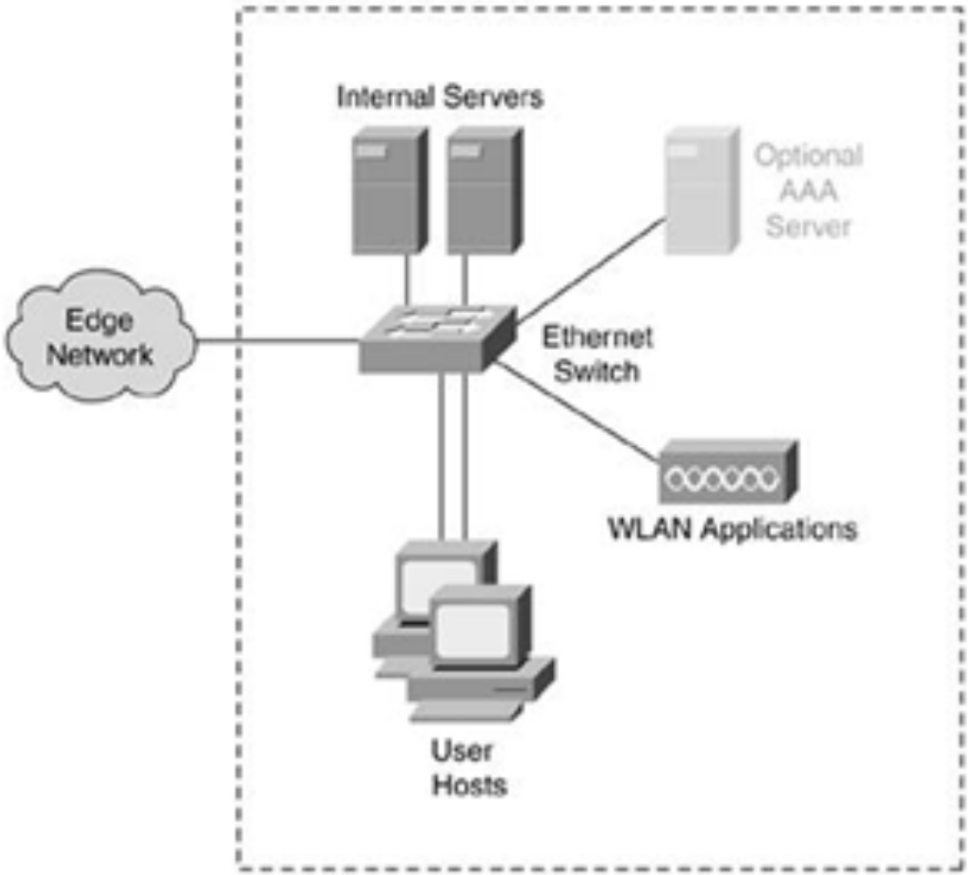
- Khi có nhu cầu kết nối từ xa qua mạng Internet, dùng VPN
- Với mạng vành đai nhỏ thì trong kết nối site-to-site có thể chỉ dùng preshared key là đủ, không cần tạo hầm GRE (generic route encapsulation tunnel).
- Với remote user có thể dùng các preshared key nhóm, nếu muốn mở rộng có thể dùng OTP
- Direct access và identity spoofing là các mối đe dọa đối với VPN. Có thể ngăn chặn cả hai mối đe dọa này bằng sự kết hợp network crypto và các cơ cấu OTP


Public Servers
Remote
User
IPsec
Ethernet
Switch
Internet
ISP
Router
Optional
WAN
Router
Router /
Security
Gateway
Campus
Network
Remote Site
IPsec
Dedicated
VPN
Gateway
Remote User IPsec
Site-to-Site IPsec

An ninh mạng campus

- Mạng campus cỡ nhỏ
- Thiết kế tiêu biểu
- Phân tích các nguy cơ an ninh
- Đề xuất áp dụng giải pháp an ninh cho từng bộ phận

Thiết kế tiêu biểu



Các nguy cơ an ninh

- Identity spoofing
- Virus/worm/Trojan horse
- Rogue devices
- Sniffer
- Man-in-the-middle
- War dialing/driving
- Direct access
- ARP redirection/spoofing
- Remote control software
- Buffer overflow

Đề xuất áp dụng giải pháp an ninh cho từng bộ phận

- Ethernet Switch
- Internal Servers
- User Hosts
- WLAN AP
- AAA Server

Ethernet Switch

- Cài đặt STP BPDU Guard trên tất cả các PC port để ngăn chặn các sự cố spanning tree vô tình hay cố ý.
- Hạn chế số địa chỉ MAC trên từng port của switch. Dùng port security.
- Dùng VLAN để hỗ trợ quản lý an ninh
- Cho phép chức năng kiểm duyệt ARP nếu được hỗ trợ. Có thể dùng công cụ như ARPwatch.
- Có thể dùng private VLAN để tách biệt các hệ thống
- Nếu có thể, triển khai DHCP snooping hay VLAN ACL để ngăn chặn hầu hết các tấn công DHCP.

Internal Servers

- Xác thực với cặp username/password
- Sử dụng mật mã cho các phiên ứng dụng nhạy cảm
- Củng cố bản thân OS/application.
- Sử dụng công cụ kiểm tra hệ thống file
- Sử dụng host antivirus, triển khai trên mỗi hệ thống (server hay client)

User Hosts

- Dùng xác thực đăng nhập với username/password
- Củng cố bản thân OS/appplication, tận dụng cơ chế tự động vá lỗ hổng của các OS và ứng dụng
- Sử dụng host antivirus

WLAN AP

- Dùng VLAN để tách biệt lưu lượng không dây
- Củng cố thiết bị

AAA server

- Bất cứ sự triển khai AAA server nào đều tuân theo các đề nghị an ninh cho server như internal server.
- Kỹ thuật an ninh bổ sung thêm trên AAA server là RADIUS/TACACS+

HẾT BÀI 2