HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA ATTT

BÀI GIẢNG PTTK AN TOÀN MẠNG

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

1. Thiết kế mô hình, địa chỉ, lựa chọn giao thức cho mạng
2. Xây dựng kế hoạch và chính sách an toàn
3. Thiết kế các cơ chế an toàn
4. Phân đoạn cụ thể giải pháp an toàn
5. Xây dựng quy trình quản lý mạng an toàn
6. Thiết kế vật lý mạng máy tính

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.1 Thiết kế mô hình, địa chỉ, lựa chọn giao thức cho mạng

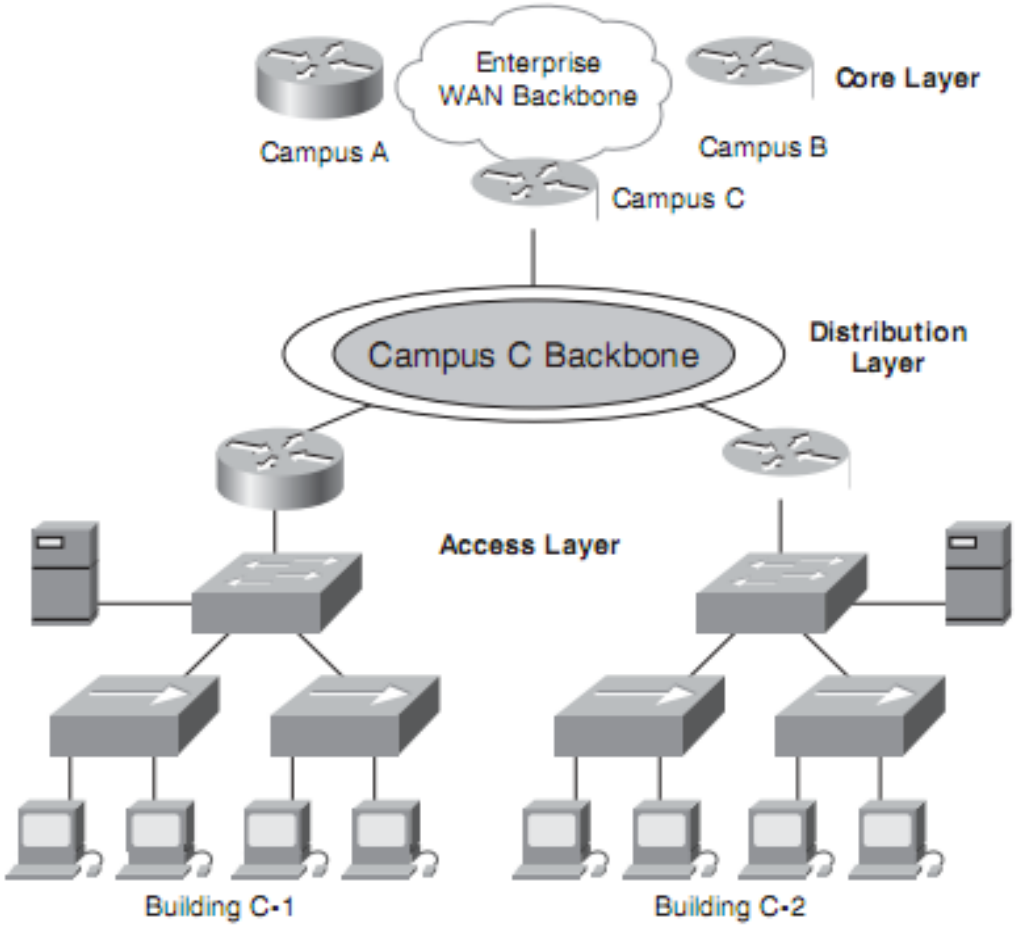
- Thiết kế Topology
- Thiết kế đánh địa chỉ mạng
- Lựa chọn giao thức chuyển mạch và định tuyến

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.1.1. Thiết kế Topology:

- *Topology* của mạng là cấu trúc hình học không gian mà thực chất là cách bố trí phần tử của mạng cũng như cách nối giữa chúng với nhau. Nó chỉ rõ các phân đoạn mạng, điểm liên kết và nhóm người dùng
- ***Mô hình thiết kế mạng phân cấp***
  - Mô hình này cho phép quản lý thiết bị tập trung, được đặt theo từng lớp riêng rẽ, tùy thuộc vào chức năng của từng lớp.
  - Mỗi lớp có thể được tập trung vào chức năng cụ thể cho phép ta chọn hệ thống phù hợp và các tính năng cho các lớp

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG



CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Đặc điểm của topo phân cấp gồm có 3 lớp:
  - Lớp core: bao gồm router và switch cao cấp tối ưu cho tính sẵn sàng và hiệu năng
  - Lớp distribution: bao gồm router và switch cài đặt các chính sách, trong các tổ chức nhỏ, thì lớp core và distribution có thể được gộp lại
  - Lớp access: kết nối người dùng cuối bằng switch hoặc các điểm truy cập không dây.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Lý do sử dụng mô hình thiết kế phân cấp:
  - Hỗ trợ dễ dàng cho việc sửa lỗi, nâng cấp và quản trị
  - Tối ưu hóa hiệu suất
  - Khả năng mở rộng, tính ổn định cao.
  - Giảm bớt yêu cầu tài nguyên mạng (CPU, bộ nhớ,băng thông…)

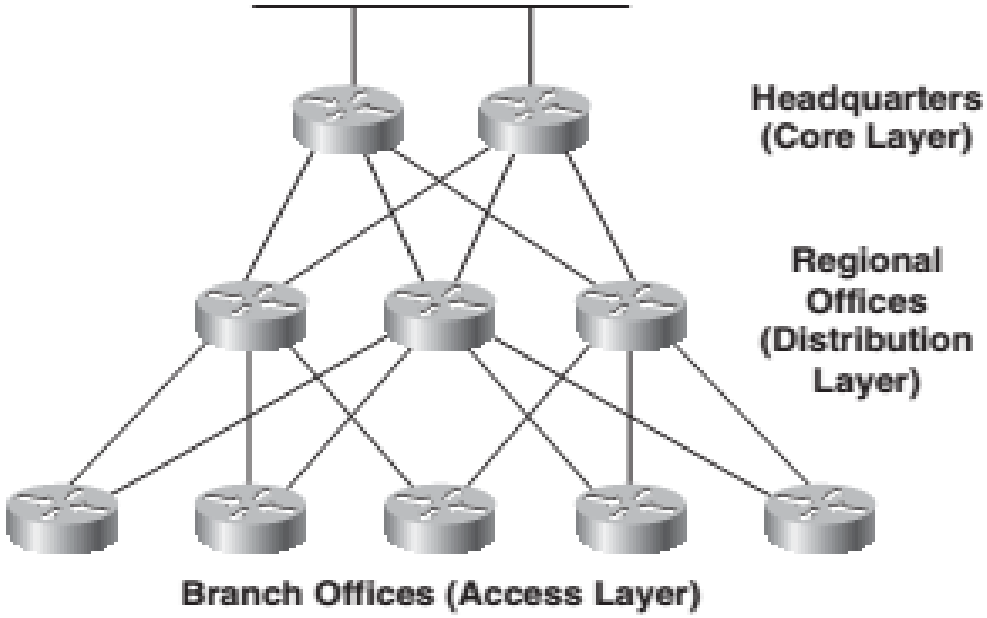
CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

Lưu ý khi thiết kế mạng theo mô hình phân cấp:

- Xác định kiến trúc và phạm vi mạng.
- Thực hiện kiểm soát kết nối mạng sẽ giúp được việc tính toán và giảm được độ trễ của mạng.
- Việc kiểm soát sẽ giúp việc dự đoán được định tuyến mạng, lưu lượng dữ liệu, các yêu cầu về khả năng đáp ứng.
- Một mạng được kiểm soát cũng làm cho xử lý sự cố và lập tài liệu mạng dễ dàng hơn.
- Cần thực hiện kiểm soát chặt chẽ liên kết mạng tại lớp truy cập vì đây là nơi dễ bị vi phạm nguyên tắc thiết kế mạng phân cấp.
- Thiết kế mạng phân cấp bắt đầu với thiết kế ở lớp Access đầu tiên, tiếp theo là lớp Distribution, và cuối cùng là lớp Core.

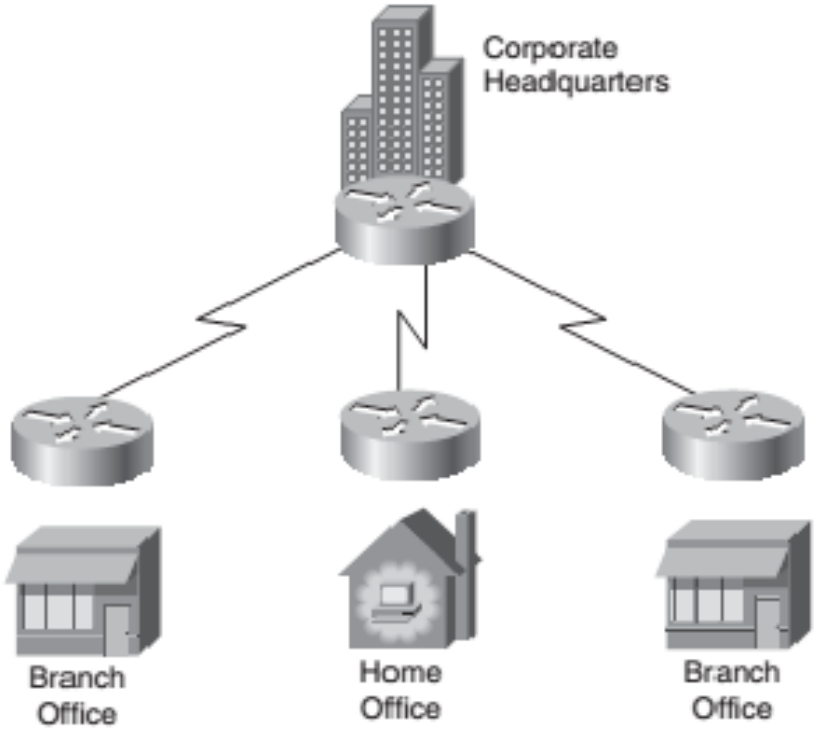
CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- ***Mạng doanh nghiệp***
  - Mạng doanh nghiệp được xây dựng theo dạng mô hình phân cấp, cũng gồm 3 lớp: Core, distribution, access



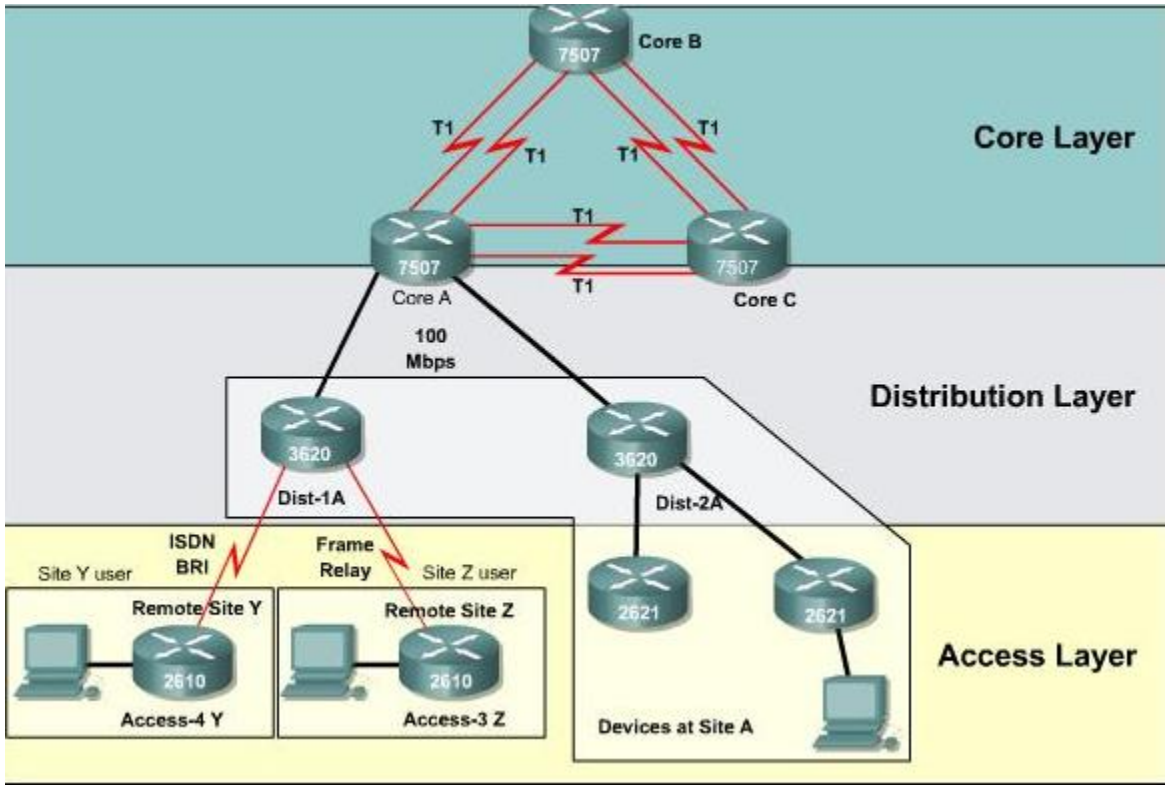
Partial-Mesh Hierarchical Design

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG



Hub-and-Spoke Hierarchical Topology for a Medium-Sized Business

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG



CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Lớp Core: cung cấp tối ưu hoá và độ tin cậy trong quá trình truyền tin với tốc độ rất cao (high speeds).
  - Lớp Core Layer không thể đáp ứng toàn bộ quá trình truyền thông tin trên mạng, nhưng nó có thể được coi như đường đại lộ liên kết các đường nhỏ với nhau, đôi khi các giao tiếp chỉ thực hiện ở một lớp duy nhất mà thôi.
  - Lớp Core Layer thực hiện các vai trò sau:
    - Kiểm tra Access-list
    - Mã hoá dữ liệu
    - Address translation

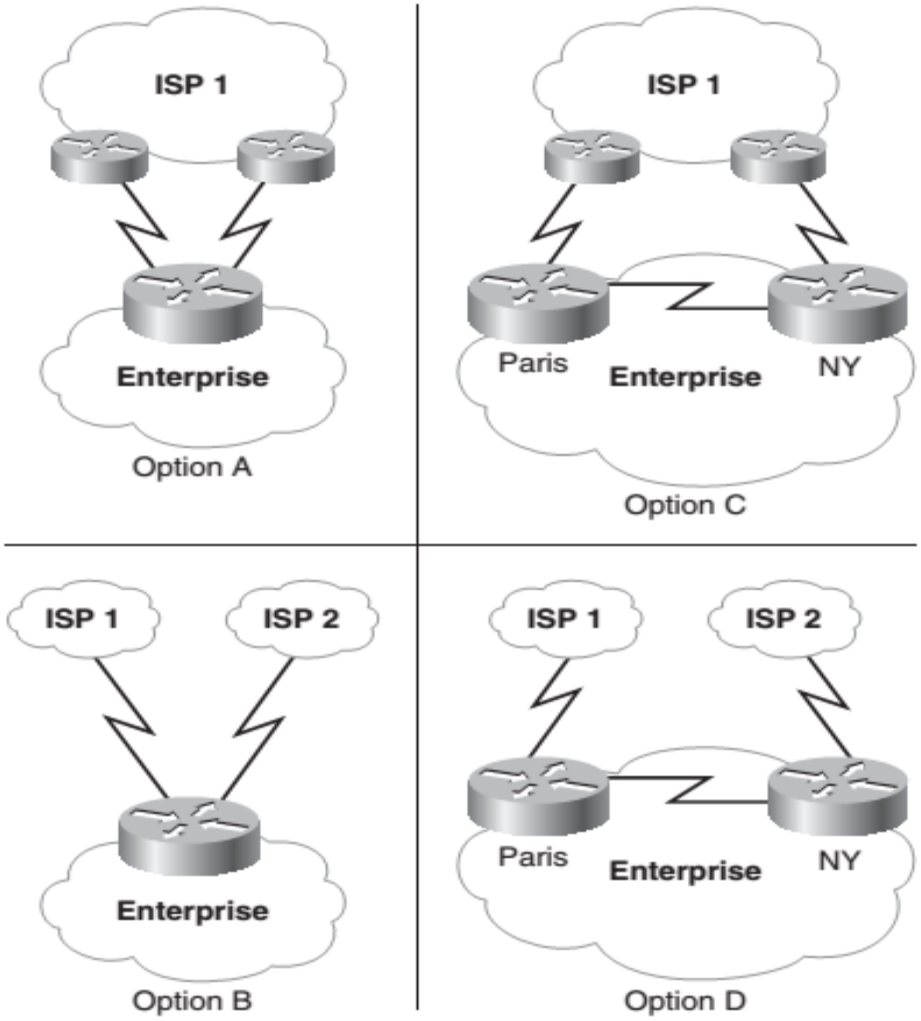
CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Lớp Distribution: làm việc ở giữa Core Layer và Access Layer, với vai trò đáp ứng một số giao tiếp giúp giảm tải cho lớp Core Layer trong quá trình truyền thông tin trong mạng.
  - Với tác dụng của lớp này cung cấp ranh giới cho việc sử dụng access lists và các tính năng lọc khác để khi cần thiết sẽ gửi lên lớp core layer.
  - Lớp này cũng là lớp định nghĩa các chính sách cho mạng. Một chính sách có thể áp dụng các dạng cụ thể sau:
    - Routing updates
    - Route summaries
    - VLAN
    - Sử dụng các chính sách để bảo mật mạng và chống các giao dịch không cần thiết.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

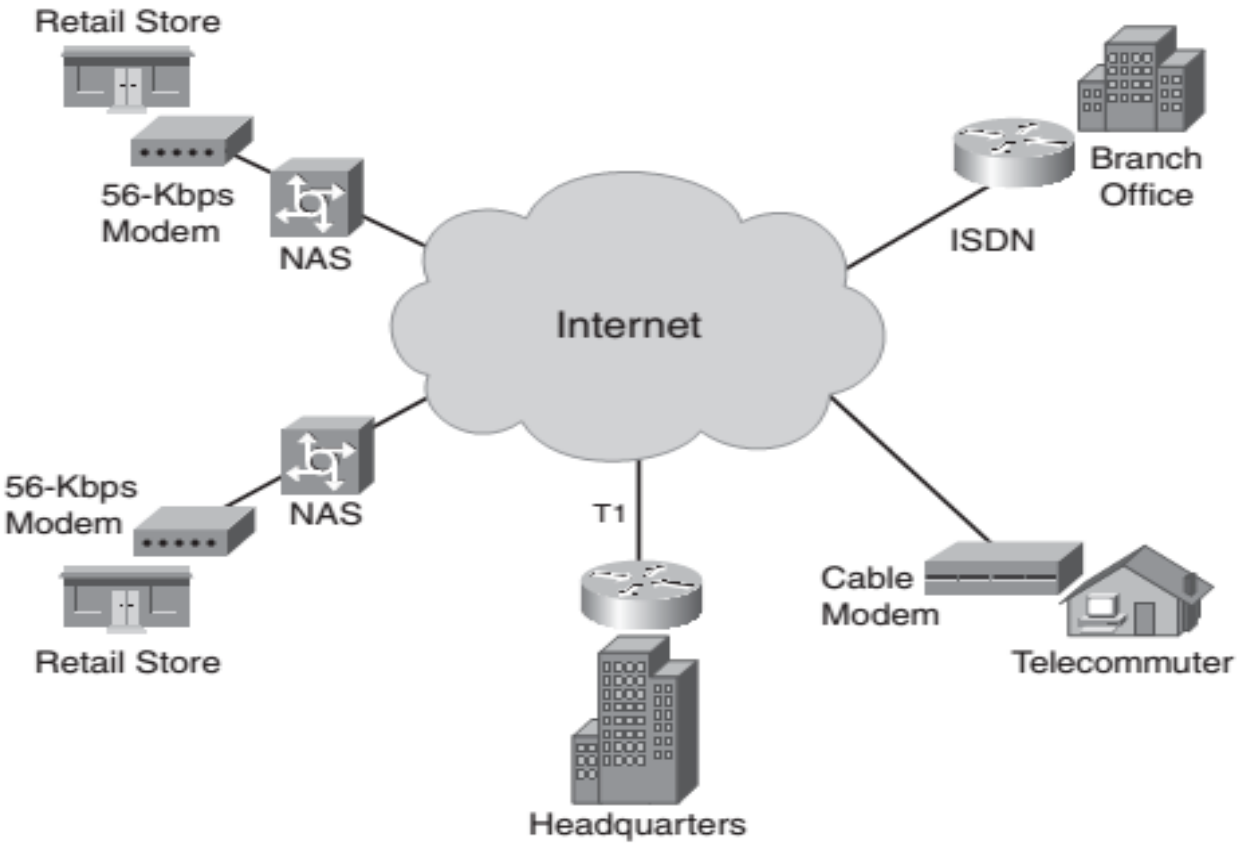
- Lớp Access: Kết nối người dùng với các tài nguyên trên mạng hoặc các giao tiếp với lớp Distribution. Access layer sử dụng Access lists quy định truy cập chống lại những xâm nhập bất hợp pháp

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG



Multihoming the Internet Connection

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG



Remote-Access VPN for a Retail Company

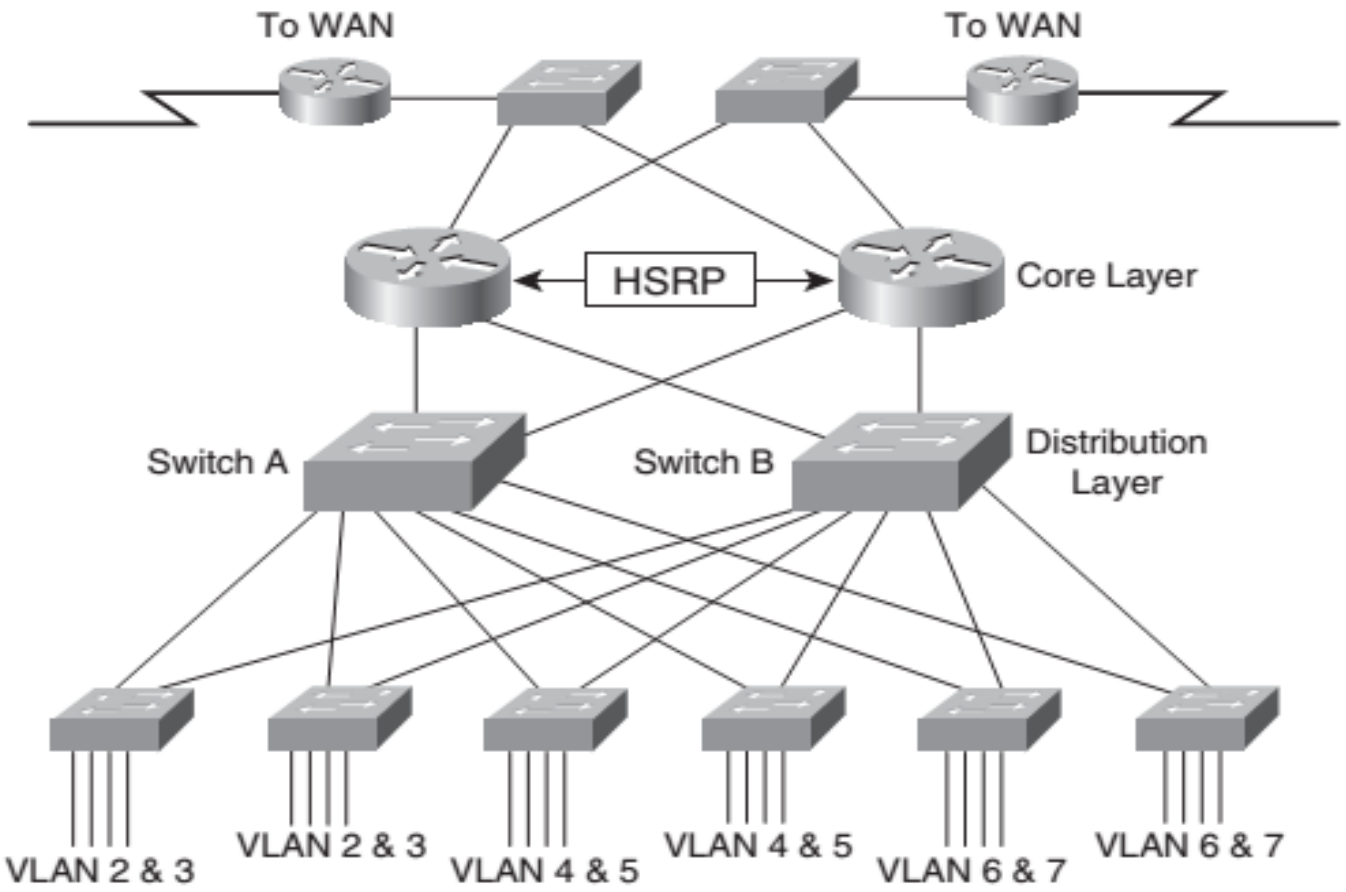
CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Mô hình thiết kế mạng Campus
  - Topo mạng Campus sẽ phải đáp ứng yêu cầu về tính sẵn sàng và hiệu năng bởi đặc tính băng thông miền nhỏ, vùng quảng bá nhỏ, dự phòng, server và nhiều đường từ máy trạm tới một router. Campus được thiết kế sử dụng mô hình phân cấp, mô-đun vì thế mạng sẽ có hiệu năng tốt, ổn định và có khả năng mở rộng.
- Mạng campus có thể gồm: accesss, distribution, core layers:
  - Access: mô-đun này chứa máy trạm và IP phone kết nôi với switch hoặc điểm truy cập không dây. Switch cao cấp sẽ cung cấp liên kết tới lớp distribution. Các dịch vụ được đưa ra bởi mô-đun này gồm: network access, broadcast control, packet filter

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Distribution: hợp nhất kết nối vào từ lớp access và cung cấp kết nối tới mạng core bằng router hoặc switch. Mô-đun này cung cấp định tuyến, QoS, kiểm soát truy cập. Dự phòng và chia sẻ tải cũng được khuyên dùng cho mô-đun này.
- Core: kết nối lớp access và distribution với trung tâm dữ liệu, mạng quản trị, edge mô-đun. Campus core cung cấp dự phòng và hội tụ nhanh.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG



Campus Hierarchical Redundant Topology

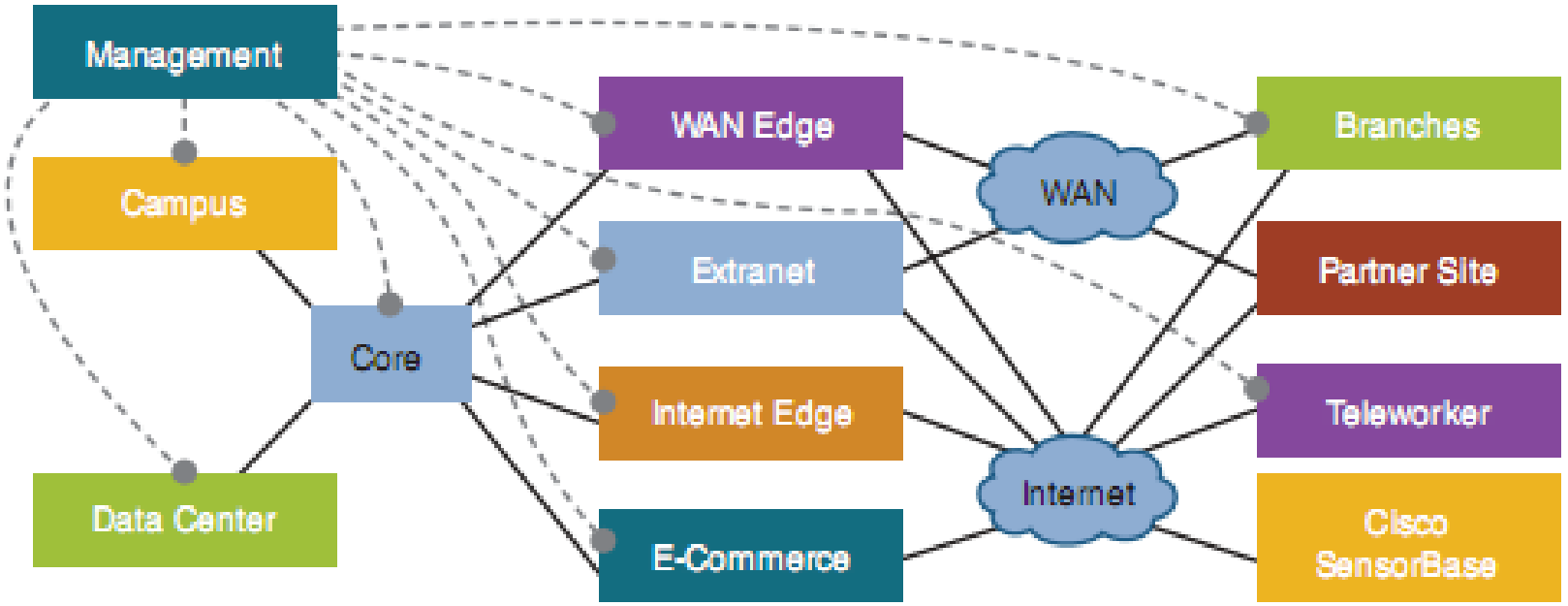
CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- **Thiết kế module mạng:**
  - Trong một dự án thiết kế, mạng lớn thường gồm những khu vực khác nhau hoặc những mô-đun khác nhau. Mỗi khu vực sẽ được thiết kế sử dụng một hệ thống, cách tiếp cận từ trên xuống dưới, áp dụng thiết kế phân cấp và dự phòng ở nơi tương ứng.
  - Giải pháp mạng và dịch vụ có thể được chọn trên một mô-đun cơ bản nhưng được đưa lên như một phần trên toàn bộ thiết kế mạng. Cisco phát triển kiến trúc tham chiếu SAFE miêu tả mỗi thành phần, mô-đun của mỗi loại mạng doanh nghiệp.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- *Kiến trúc an toàn tham chiếu Cisco SAFE*
  - SAFE là một kiến trúc tham chiếu cho người thiết kế mạng có thể sử dụng để đơn giản hóa sự phức tạp của một mạng lớn. Kiến trúc cho phép ta áp dụng các tiếp cận mô-đun tới thiết kế mạng. Với SAFE, ta có thể phân tích chức năng, lô-gic, và thành phần vật lý của một mạng, vì vậy sẽ đơn giản hóa quá trình thiết kế trên toàn mạng doanh nghiệp.
  - SAFE là kiến trúc đặc biệt liên quan tới an toàn, SAFE đưa ra phòng thủ theo chiều sâu, với nhiều lớp bảo vệ. Những lớp này bao gồm các phân đoạn mạng, thiết bị, dịch vụ mạng, điểm cuối, ứng dụng.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG



CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Hình trên gồm các mô-đun trong kiến trúc SAFE
  - Core: là một cơ sở hạ tầng tốc độ cao cung cấp tính tin cậy và khả năng mở rộng ở lớp 2, 3. Core được cài đặt với switch dự phòng hợp nhất kết nối tới campus, data center, WAN edge, Internet EDGE
  - Data center: là các host server, ứng dụng, thiết bị lưu trữ được sử dụng bởi người dùng bên trong. Trung tâm dữ liệu cũng kết nối cơ sở hạ tầng mạng, nó gồm router, switch, load balancer, thiết bị phân phối nội dung và thiết bị tăng tốc ứng dụng. Data center không thể truy cập trực tiếp từ internet.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Campus: Mạng campus cung cấp truy cập mạng tới người sử dụng cuối và thiết bị định tuyến trong cung một vị trí địa lý. Mạng campus có thể trên một vài tầng trong một tòa nhà hoặc nhiều tòa nhà cho một doanh nghiệp lớn. Campus cung cấp data, voice, video. Campus thiết kế sẽ cho phép người dùng campus có thể truy cập an toàn tới data center và Internet từ cơ sở hạ tầng campus.
- Management: mạng quản lý cung cấp quản trị, phân tích, xác thực và dịch vụ ghi nhật ký. Server quản trị hỗ trợ RADIUS, Kerberos, SNMP, syslog traffic.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- WAN edge: là một phần của mạng, nó hợp nhất traffic từ các chi nhánh về một site trung tâm, nó có thể được sở hữu bởi doanh nghiệp hoặc ISP.
- Internet edge: là cơ sở hạ tầng cung cấp kết nối internet và vai trò như một gateway cho doanh nghiệp. Dịch vụ internet edge bao gồm DMZ, VPN, đường truy cập Internet của công ty.
- Branches: cung cấp kết nối tới người dùng và thiết bị ở xa. Nó bao gồm một hoặc nhiều LAN kết nối tới site trung tâm bằng đường thuê riêng hoặc VPN. Branches có data, voice, video.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Extranet: cho phép thành viên, khách hàng, và nhà cung cấp truy cập vào một phần của mạng bằng giao thức an toàn. Dịch vụ extranet bao gồm VPN remote access.
- Partner site: là mạng được sở hữu bởi thành viên kinh doanh, khách hàng, nhà cung cấp. Truy cập dịch vụ trong extranet bằng WAN secure hoặc kết nối internet.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- E-commerce: Có chứa các ứng dụng, server và dữ liệu cho phép mua bán các sản phẩm, dịch vụ bao gồm từ lớp 2-7, traffic được lọc, và server được chạy cân bằng tải.
- Teleworker: là những người nhân viên làm việc full-time hoặc part-time, sử dụng VPN , desktop security và mạng không dây an toàn, IP telephony, IP video.
- Cisco SensorBase: gồm những nguy cơ cập nhật hàng hàng ngày từ sensor như botnets, darknet, malware, serial attacker. Sensor bồm IPS, email server, web security appliance

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.1.2 Thiết kế đánh địa chỉ mạng

- Một số nguyên tắc cơ bản cho việc địa chỉ :
  - Gán khối địa chỉ trên cơ sở mạng vật lý, không gán theo nhóm để tránh gặp phải vấn đề khi nhóm bị xóa.
  - Thiết kế mô hình đánh địa chỉ theo dạng phân cấp (sau này nâng cấp sẽ dễ dàng hơn.)
  - Để mềm dẻo và linh hoạt nên sử dụng cung cấp địa chỉ động cho các máy trạm
  - Sử dụng NAT để chuyển đổi địa chỉ riêng ra địa chỉ Public

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Sử dụng mô hình phân cấp cho việc đánh địa chỉ lớp mạng:
  - Mô hình phân cấp cho đánh địa chỉ nghĩa là địa chỉ phải có ý nghĩa, phân cấp và theo kế hoạch. Địa chỉ IP có cấu trúc bao gồm phần “tiền tố’ và “phần host”.
  - Việc sử dụng mô hình phân cấp giúp dễ dàng cho việc quản trị và sửa lỗi. Nó giúp dễ dàng hiểu sơ đồ mạng, hoạt động quản trị phần mềm, và nhận ra các thiết bị trong việc phân tích giao thức.
  - Việc phân cấp địa chỉ cũng làm dễ dàng hơn tối ưu mạng và bảo mật bởi vì chúng làm cho dễ dàng trong việc cài đặt lọc gói tin trên tường lửa, router, switch.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

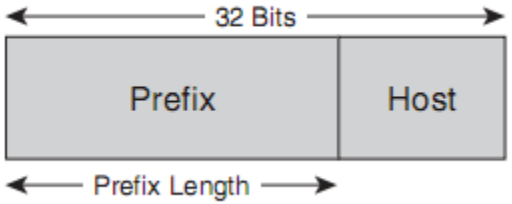
- Việc không phân cấp địa chỉ khi sử dụng sẽ dẫn tới một số vấn đề như: việc trùng lặp địa chỉ mạng, host, địa chỉ không hợp lệ không thể được định tuyến trên internet, địa chỉ không được sử dụng, dẫn tới lãng phí đại chỉ.
- Quản lý địa chỉ sẽ được thực hiện bởi trung tâm thẩm quyền, trung tâm sẽ thực hiện việc cấp phát địa chỉ tới các mạng, các host. Việc quản lý bởi trung tâm thẩm quyền này sẽ dễ dàng trong việc quản lý cũng như cấp phát địa chỉ IP

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Để dễ dàng trong quá trình cấp phát địa chỉ, ta cần trả lời các câu hỏi:
  - Sử dụng địa chỉ public, private hay cả hai loại?
  - Bao nhiêu máy trạm chỉ truy cập tới mạng riêng (cục bộ)?
  - Bao nhiêu máy trạm có thể truy cập ra ngoài (internet)?
  - Sẽ chuyển đổi địa chỉ private → public như thế nào?
  - Topo mạng sẽ được dùng ở biên giữa mạng private và public?

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Phân cấp địa chỉ là mô hình áp dụng cấu trúc tới đia chỉ gồm 2 phần đó là: tiền tố (phần mạng) và phần host. Phân cấp địa chỉ làm cho việc định tuyến dễ dàng hơn.
- Tại sao sử dụng hệ thống phân cấp địa chỉ?
  - Hỗ trợ dễ dàng cho việc sửa lỗi, nâng cấp và quản trị
  - Tối ưu hóa hiệu năng
  - Tốc độ hội tụ của giao thức định tuyến nhanh hơn
  - Khả năng mở rộng, tính ổn định cao.
  - Giảm bớt yêu cầu tài nguyên mạng (CPU, bộ nhớ,băng thông…)



CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

Class A	First bit = 0	Prefix is 8 bits
Class B	First bit = 10	Prefix is 16 bits
Class C	First bit = 110	Prefix is 24 bits

- Ta có thể chia mạng sao cho phù hợp với số host hiện có mà không phải phụ thuộc vào các lớp A, B, C.
- Ví dụ với một mạng có 22 host cho địa chỉ mạng là 192.168.1.0/24 ta có thể chia thành mạng con phù hợp với mạng của chúng ta. Địa chỉ mạng: 192.168.1.0/27

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.1.3 Lựa chọn giao thức chuyển mạch

- Việc lựa chọn giao thức định tuyến, chuyển mạch phụ thuộc vào mục tiêu kinh doanh và mục tiêu kỹ thuật.
- Một số giao thức chuyển mạch trong LAN:
  - VTP (VLAN Trunking Protocol):
  - STP (Spanning Tree Protocol):
  - Portfast:
  - DTP (Dynamic Trunk Protocol)

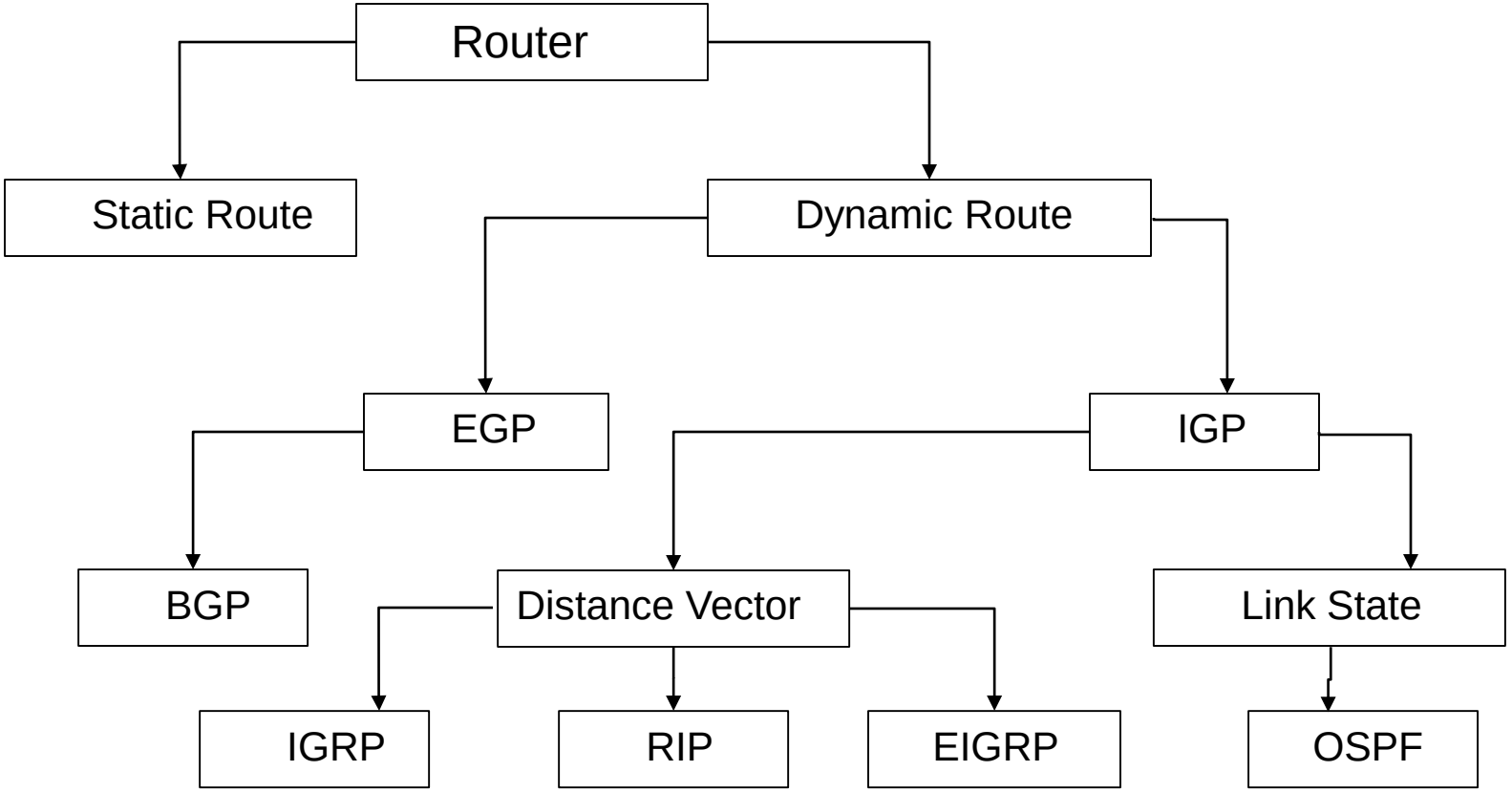
CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.1.4 Lựa chọn giao thức định tuyến

- Distance Vector: Sử dụng cho các mạng nhỏ, không thiết kế phân cấp, số lượng router hạn chế, không yêu cầu thời gian hội tụ nhanh.
- Link-state: Sử dụng cho các mạng lớn, có thiết kế phân cấp, yêu cầu thời gian hội tụ nhanh.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.1.4 Lựa chọn giao thức định tuyến



CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

1. Thiết kế mô hình, địa chỉ, lựa chọn giao thức cho mạng
2. **Xây dựng kế hoạch và chính sách an toàn**
3. Thiết kế các cơ chế an toàn
4. Phân đoạn cụ thể giải pháp an toàn
5. Xây dựng quy trình quản lý mạng an toàn
6. Thiết kế vật lý mạng máy tính

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.2 Xây dựng kế hoạch và chính sách an toàn

- Xây dựng kế hoạch đảm bảo an toàn
- Xây dựng chính sách an toàn
- Xây dựng thủ tục đảm bảo an toàn
- Duy trì an toàn

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.2.1 Xây dựng kế hoạch đảm bảo an toàn

- Kế hoạch này sẽ chỉ rõ thời gian, con người và những tài nguyên liên quan đến việc phát triển chính sách an toàn và sự bổ sung kỹ thuật cho chính sách
- Kế hoạch an toàn sẽ tham chiếu tới một mô hình mạng và bao gồm danh sách các dịch vụ sẽ được cung cấp (ví dụ: FTP, web, mail…). Danh sách này sẽ chỉ rõ việc cung cấp dịch vụ, ai sẽ được truy cập tới dịch vụ, dịch vụ được cung cấp sẽ được truy cập như thế nào, và ai sẽ là người quản trị dịch vụ đó

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.2.1 Xây dựng kế hoạch đảm bảo an toàn

- Một điều quan trọng trong việc phát triển chính sách an toàn phải chỉ rõ những ai sẽ được bao gồm trong xây dựng mạng an toàn:
  - Người quản trị an toàn
  - Người dùng cuối và người quản lý sẽ có thể gặp phải những vấn đề gì
  - Người dùng cuối, quản trị viên, nhân viên kỹ thuật sẽ được đào tạo dựa trên chính sách và thủ tục an toàn như thế nào
- Để cho chính sách được áp dụng, nó cần được triển khai tới tất cả các nhân viên trong tổ chức. Nó rất quan trọng với người quản trị của công ty.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.2.2 Xây dựng chính sách an toàn

- Chính sách an toàn là những quy tắc, nguyên tắc được đặt ra mà bắt buộc mọi người phải tuân theo.
- Một chính sách an toàn phải được thông báo tới người dùng, quản trị viên, nhân viên trong công ty, nó cũng chỉ rõ những nghĩa vụ mà người dùng phải đáp ứng

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Sau khi một chính sách được phát triển, nó phải được thông báo với nhân viên, người dùng, người quản lý.
- Phát triển một chính sách an toàn là công việc của quản lý cấp cao với sự giúp đỡ của quản trị mạng và quản trị an ninh. Các nhà quản trị có thông tin đầu vào từ các người dùng, người thiết kế và kỹ sư mạng, và các tư vấn về pháp lý.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.2.2 Xây dựng chính sách an toàn

- Người thiết kế mạng phải làm việc chặt chẽ với quản trị an ninh để xây dựng các chính sách an toàn phù hợp với thiết kế mạng
- Nhiều tổ chức yêu cầu nhân viên phải ký cam kết về việc đọc, hiểu và tuân theo chính sách
- Chính sách an toàn thường được cập nhật
- Xây dựng chính sách an toàn:
  - Chính sách mật khẩu
  - Chính sách an toàn máy trạm
  - Chính sách truy cập
  - vv…

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.2.3 Xây dựng thủ tục đảm bảo an toàn

- Thủ tục an toàn cài đặt chính sách an toàn
- Thủ tục an toàn định nghĩa việc cấu hình, đăng nhập, kiểm toán và duy trì
- Thủ tục an toàn sẽ được áp dụng cho người dùng cuối, người quản trị mạng, quản trị an toàn
- Thủ tục an toàn chỉ rõ việc khắc phục sự cố như thế nào khi sự cố xảy ra (ví dụ: Sẽ liên hệ với ai nếu phát hiện ra xâm nhập).

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.2.4 Duy trì an toàn

- Sự an toàn phải được duy trì bởi một chu kỳ lập lịch độc lập với kiểm toán, phân tích nhật ký kiểm toán, phản ứng khi có sự cố, sử dụng kiểm thử an toàn, đào tạo an toàn cho người quản trị và cập nhất các kế hoạch và chính sách an toàn.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

1. Thiết kế mô hình, địa chỉ, lựa chọn giao thức cho mạng
2. Xây dựng kế hoạch và chính sách an toàn
3. **Thiết kế các cơ chế an toàn**
4. Phân đoạn cụ thể giải pháp an toàn
5. Xây dựng quy trình quản lý mạng an toàn
6. Thiết kế vật lý mạng máy tính

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Thiết kế các cơ chế an toàn
  - Cơ chế an toàn vật lý
  - Cơ chế xác thực
  - Cơ chế cấp quyền
  - Cơ chế kiểm toán
  - Cơ chế mã hóa dữ liệu
  - Tường lửa
  - Hệ thống phát hiện xâm nhập trái phép.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

1. Thiết kế mô hình, địa chỉ, lựa chọn giao thức cho mạng
2. Xây dựng kế hoạch và chính sách an toàn
3. Thiết kế các cơ chế an toàn
4. **Phân đoạn cụ thể giải pháp an toàn**
5. Xây dựng quy trình quản lý mạng an toàn
6. Thiết kế vật lý mạng máy tính

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.4 Các giải pháp an toàn cho phân đoạn cụ thể

- Đảm bảo an toàn kết nối Internet
- Đảm bảo an toàn truy cập từ xa và mạng riêng ảo
- Đảm bảo an toàn cho các dịch vụ mạng và quản lý mạng
- Đảm bảo an toàn cho máy chủ nội bộ
- Đảm bảo an toàn cho dịch vụ người dùng
- Đảm bảo an toàn cho mạng không dây.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

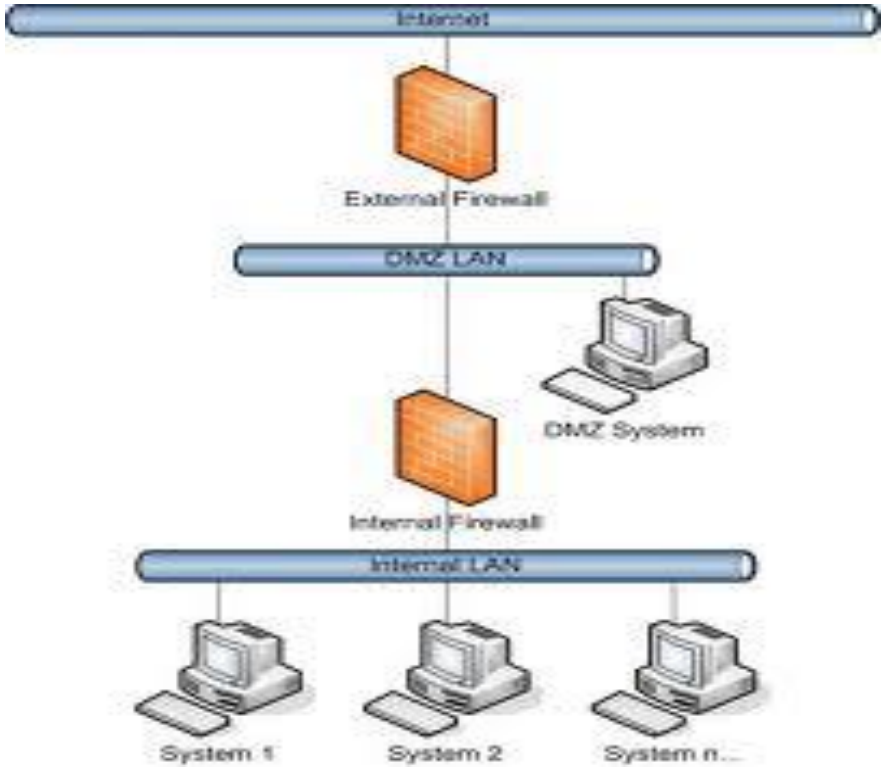
4.4 Các giải pháp an toàn cho phân đoạn cụ thể

- Đảm bảo an toàn kết nối Internet
  - An toàn kết nối: Kết nối internet sẽ an toàn với các cơ chế an toàn bao gồm tường lửa, bộ lọc gói tin, an toàn vật lý, kiểm toán, xác thực và cấp quyền
  - An toàn máy chủ dịch vụ Internet và thương mại điện tử
    - DMZ là một mạng tách biệt với mạng nội bộ vì DMZ sử dụng đường mạng (hoặc có subnet) khác với mạng nội bộ
    - Các máy chủ Web, Mail, FTP, VoIP… được đặt trong DMZ cung cấp các dịch vụ của tổ chức cho phép người dùng có thể truy cập và sử dụng từ mạng Internet
    - Các máy chủ phục vụ cho các mục đích nội bộ như DNS, DHCP, File/Print… vẫn được đặt trong vùng nội bộ
    - Giữa DMZ và mạng ngoài có thể đặt một firewall để cho phép các kết nối từ ngoài chỉ đến được DMZ
    - Giữa mạng nội bộ và DMZ có thể đặt thêm một firewall khác để kiểm soát các lưu lượng từ DMZ đi vào nội bộ

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.4 Các giải pháp an toàn cho phân đoạn cụ thể

- Đảm bảo an toàn kết nối Internet
  - An toàn máy chủ dịch vụ Internet và thương mại điện tử



CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.4 Các giải pháp an toàn cho phân đoạn cụ thể

- Đảm bảo an toàn kết nối Internet
  - An toàn máy chủ dịch vụ Internet và thương mại điện tử
    - Cấu hình và quản trị máy chủ an toàn

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.4 Các giải pháp an toàn cho phân đoạn cụ thể

Đảm bảo an toàn truy cập từ xa và mạng riêng ảo

- An toàn truy cập từ xa: người dùng từ xa dùng giao thức PPP nên sử dụng xác thực bằng CHAP hoặc RADIUS
- Mạng riêng ảo:
  - Cài các phần mềm diệt virus, tường lửa cá nhân trên các máy client
  - Mã hóa dữ liệu truyền đi (thường sử dụng IPSec)
  - Có thể triển khai VPN SSL để đảm bảo an toàn cho kết nối VPN.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.4 Các giải pháp an toàn cho phân đoạn cụ thể

- Đảm bảo an toàn cho các dịch vụ mạng và quản lý mạng
  - Để bảo vệ dịch vụ mạng bên trong, cần bảo vệ các thiết bị mạng như router, switch. Việc truy cập tới các thiết bị này được giới hạn theo địa chỉ IP, có cơ chế xác thực phù hợp. Khi truy cập tới switch, router thì phải sử dụng SSH
  - Để quản trị một lượng lớn các thiết bị như router và switch, có thể sử dụng TACACS, với ID và mật khẩu được quản trị trong cơ sở dữ liệu tập trung, đưa ra việc kiểm toán. Hoặc sử dụng SNMP thì nên sử dụng SNMPv3 vì nó hỗ trợ xác thực và mã hóa trên đường truyền
  - Để tối thiểu nguy cơ, hệ thống quản trị mạng nên được đặt ở DMZ, đằng sau tường lửa, với hệ điều hành thường xuyên được cập nhật đầy đủ các bản vá, các dịch vụ không cần thiết phải được vô hiệu hóa, đồng thời nên sử dụng xác thực hai nhân tố.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.4 Các giải pháp an toàn cho phân đoạn cụ thể

- Đảm bảo an toàn cho máy chủ nội bộ

  Cần phải phân biệt rõ ràng giữa các vùng mạng theo chức năng và thiết lập các chính sách an toàn thông tin riêng cho từng vùng mạng theo yêu cầu thực tế:

  - Phân vùng máy chủ (hay Server Farm): Đặt các máy chủ không trực tiếp cung cấp dịch vụ cho mạng Internet
  - Phân vùng mạng Internet (hay Untrusted Network): còn gọi là mạng ngoài
  - Phân vùng mạng DMZ: Đặt các máy chủ cung cấp dịch vụ trực tiếp ra mạng Internet như máy chủ web, máy chủ mail, máy chủ FTP, v.v...
  - Phân vùng mạng nội bộ: Đặt các thiết bị mạng, máy trạm và máy chủ thuộc mạng nội bộ của đơn vị

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.4 Các giải pháp an toàn cho phân đoạn cụ thể

- Đảm bảo an toàn cho máy chủ nội bộ
  - Một số chú ý khi tổ chức mô hình mạng
    - Nên đặt các máy chủ web, máy chủ thư điện tử v.v... cung cấp dịch vụ kết nối mạng Internet trong vùng mạng DMZ
    - Các máy chủ không trực tiếp cung cấp dịch vụ ra mạng ngoài như máy chủ ứng dụng, máy chủ cơ sở dữ liệu, máy chủ xác thực v.v... nên đặt trong vùng máy chủ nội bộ
    - Nên thiết lập các hệ thống phòng thủ như tường lửa và thiết bị IDS/IPS để bảo vệ hệ thống, chống tấn công và xâm nhập trái phép
    - Nên đặt một Router ngoài cùng (Router biên) trước khi kết nối đến nhà cung cấp dịch vụ internet để lọc một số lưu lượng không mong muốn và chặn những gói tin đến từ những địa chỉ IP không hợp lệ

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Giải pháp an toàn vật lý cho các phòng máy chủ
- Giải pháp an toàn kết nối
- Sử dụng phần mềm phòng chống virus cho máy trạm
- Giải pháp ngăn chặn mất mát dữ liệu
- Giải pháp về xác thực và cấp quyền cho tài khoản và nhóm người dùng.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.4 Các giải pháp an toàn cho phân đoạn cụ thể

- Đảm bảo an toàn cho dịch vụ người dùng
  - Một chính sách an toàn sẽ chỉ rõ ứng dụng được phép chạy trên mạng và hạn chế việc tải các ứng dụng từ Internet về
  - Máy tính cá nhân phải cài đặt tường lửa và phần mềm diệt virus, được cập nhật đầy đủ
  - Khuyến nghị người dùng đăng xuất khi không sử dụng phiên, tắt máy tính khi không sử dụng, khóa màn hình khi đi ra ngoài.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.4 Các giải pháp an toàn cho phân đoạn cụ thể

- Đảm bảo an toàn cho mạng không dây
  - Sử dụng các phương pháp lọc
  - Xác thực sử dụng 802.1x
  - Mã hóa dữ liệu truyền: WEP, WPA, WPA2

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

1. Thiết kế mô hình, địa chỉ, lựa chọn giao thức cho mạng
2. Xây dựng kế hoạch và chính sách an toàn
3. Thiết kế các cơ chế an toàn
4. Phân đoạn cụ thể giải pháp an toàn
5. **Xây dựng quy trình quản lý mạng an toàn**
6. Thiết kế vật lý mạng máy tính

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

4.5 Xây dựng quy trình quản lý mạng an toàn

- Tổ chức tiêu chuẩn quốc tế ISO định nghĩa 5 loại quy trình quản lý mạng (FCAPS):
  - Quản lý lỗi
  - Quản lý cấu hình
  - Quản lý kiểm toán
  - Quản lý hiệu năng
  - Quản lý an toàn

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Quản lý lỗi:
  - Phương pháp: Phát hiện, cách ly, chẩn đoán, khắc phục lỗi và sự cố
  - Tất cả các tài nguyên mạng nếu có thể phải cấu hình logging
  - Liên tục giám sát hoạt động của hệ thống để kịp thời phát hiện lỗi

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Quản lý cấu hình:
  - Phương pháp: Theo dõi, duy trì các thông tin đã được cấu hình trên hệ thống
  - Thông tin cấu hình Router
  - Thông tin cấu hình Firewall
  - Thông tin cấu hình máy chủ
  - Thông tin cấu hình máy trạm
  - V.v…

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Quản lý kiểm toán:
  - Là phương pháp thống kê – kiểm tra:
  - Bao gồm việc theo dõi sử dụng dịch vụ
  - Thẩm quyền sử dụng tài nguyên trên hệ thống
  - Hoạt động thêm người dùng, phân quyền
  - Hành động đăng nhập của các tài khoản người dùng

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Quản lý hiệu năng:
  - Bao gồm việc: **Thu thập, thống kê, đánh giá** lưu lượng sử dụng của mạng,
  - Việc sử dụng nguồn tài nguyên máy chủ, máy trạm của các tiến trình, ứng dụng.
  - Và các thiết bị mạng khác
  - Thực hiện bằng việc kiểm tra trực tiếp hoặc sử dụng công cụ gián tiếp

Nagios XI

Server Statistics

Metric	Value
Load	
1-min	0.53
5-min	0.85
15-min	1.33
CPU Stats	
User	3.70%
Nice	0.00%
System	9.39%
I/O Wait	5.59%
Steal	0.00%
Idle	81.32%
Memory	
Total	2017 MB
Used	1884 MB
Free	133 MB
Shared	0 MB
Buffers	203 MB
Cached	928 MB
Swap	
Total	5535 MB
Used	0 MB
Free	5535 MB

Last Updated: 2012-01-30 10:18:31

Monitoring Engine Performance

Metric	Value
Host Check Latency	
Min	0.00 sec
Max	3.35 sec
Avg	1.35 sec
Host Check Execution Time	
Min	0.01 sec
Max	10.11 sec
Avg	0.05 sec
Service Check Latency	
Min	0.00 sec
Max	1.12 sec
Avg	0.32 sec
Service Check Execution Time	
Min	0.01 sec
Max	10.19 sec
Avg	0.11 sec

Last Updated: 2012-01-30 10:18:01

Monitoring Engine Check Statistics

Metric	Value
Active Host Checks	
1-min	551
5-min	2135
15-min	2855
Passive Host Checks	
1-min	0
5-min	0
15-min	0
Active Service Checks	
1-min	2123
5-min	8239
15-min	12206
Passive Service Checks	
1-min	0
5-min	0
15-min	0

Last Updated: 2012-01-30 10:18:31

Monitoring Engine Event Queue

Scheduled Events Over Time

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
3683	1804	0	1892	0

Unhandled	Problems	All
	3696	7379

Last Updated: 2012-01-30 10:17:03

Host Status Summary

Up	Down	Unreachable	Pending
1816	7	0	0

Unhandled	Problems	All
	7	1823

Last Updated: 2012-01-30 10:17:00

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Quản lý an toàn:
  - Phương pháp: Điều khiển truy cập
  - Xác thực, thẩm quyền truy cập tới tài nguyên
  - Duy trì tính bí mật, toàn vẹn, kiểm toán

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

1. Thiết kế mô hình, địa chỉ, lựa chọn giao thức cho mạng
2. Xây dựng kế hoạch và chính sách an toàn
3. Thiết kế các cơ chế an toàn
4. Phân đoạn cụ thể giải pháp an toàn
5. Xây dựng quy trình quản lý mạng an toàn
6. **Thiết kế vật lý mạng máy tính**

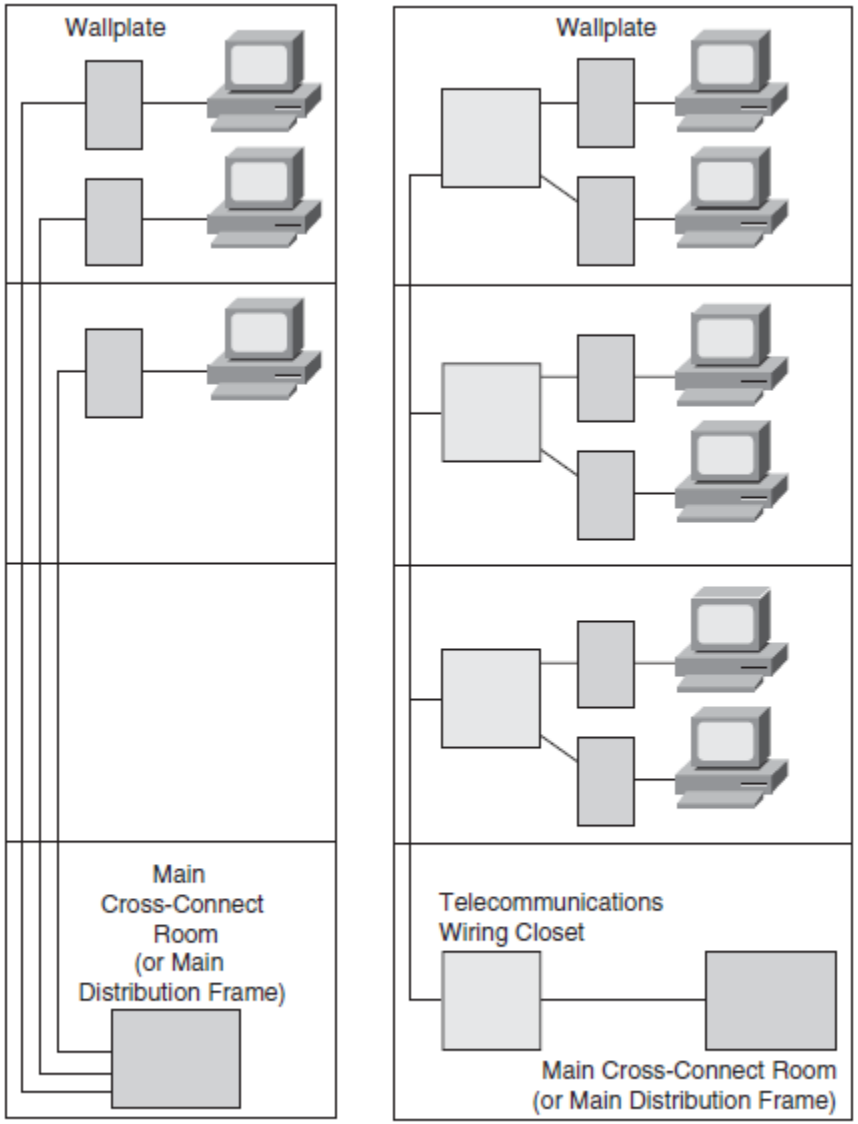
CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Thiết kế vật lý mạng máy tính
  - Lựa chọn công nghệ LAN và WAN như là Cáp, thiết bị kết nối mạng (switch, router, wireless access point), giao thức liên kết dữ liệu lớp 2
  - Lựa chọn công nghệ và thiết bị cho mạng vừa và nhỏ
  - Lựa chọn công nghệ và thiết bị cho mạng cỡ lớn
    - Công nghệ truy cập từ xa
    - Lựa chọn thiết bị truy cập từ xa khi thiết kế mạng doanh nghiệp
    - Lựa chọn router khi thiết kế WAN doanh nghiệp.

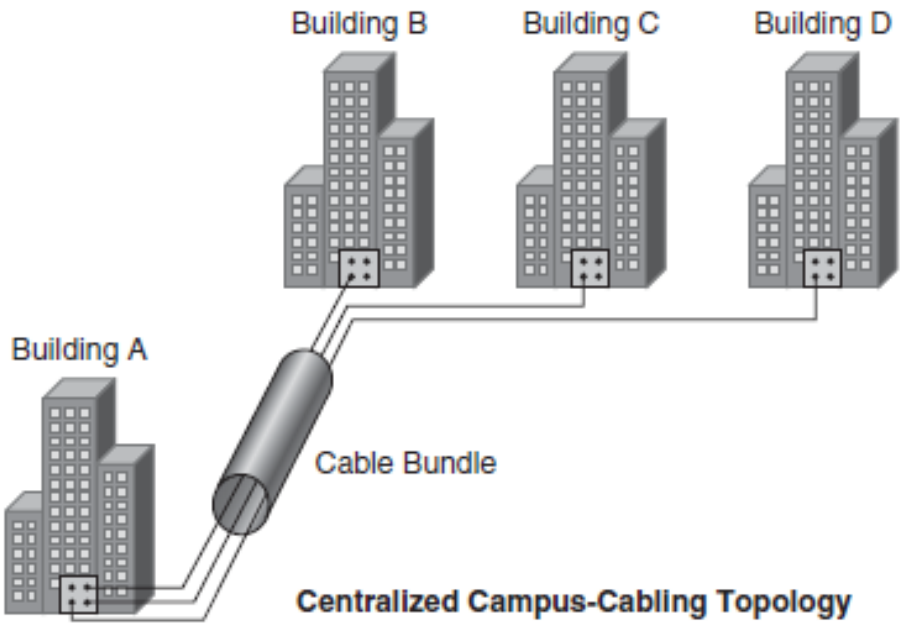
CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Thiết kế cáp cho mạng LAN
  - Mô hình cáp
    - Sơ đồ cáp tập trung: Tất cả các đường cáp đến các phòng đều kết nối trực tiếp với thiết bị chuyển mạch trung tâm. Sử dụng sơ đồ hình sao.
    - Sơ đồ cáp phân tán: Một đường trục chính kết nối từ trung tâm chuyển mạch phân phối vào các thiết bị chuyển mạch của các phòng.

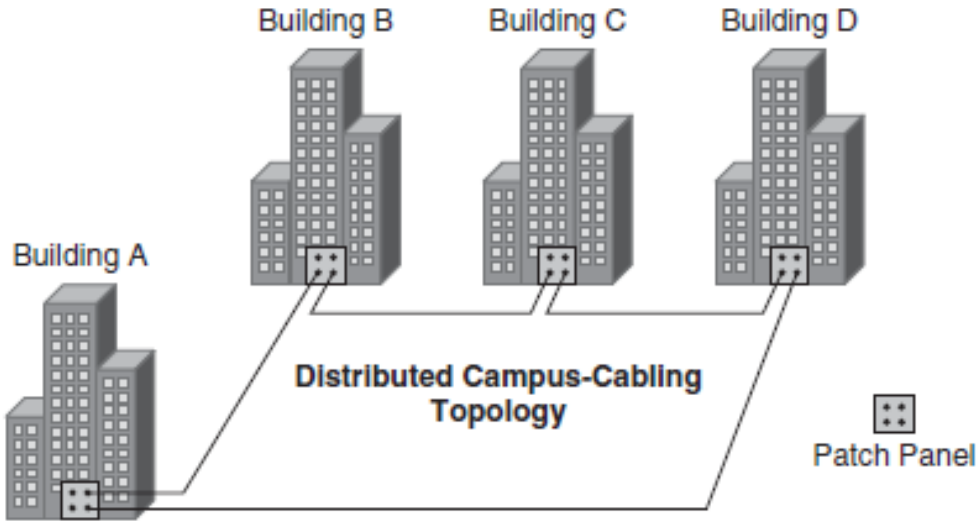
Mô hình sử dụng cáp



Mô hình sử dụng cáp Campus



Centralized Campus-Cabling Topology

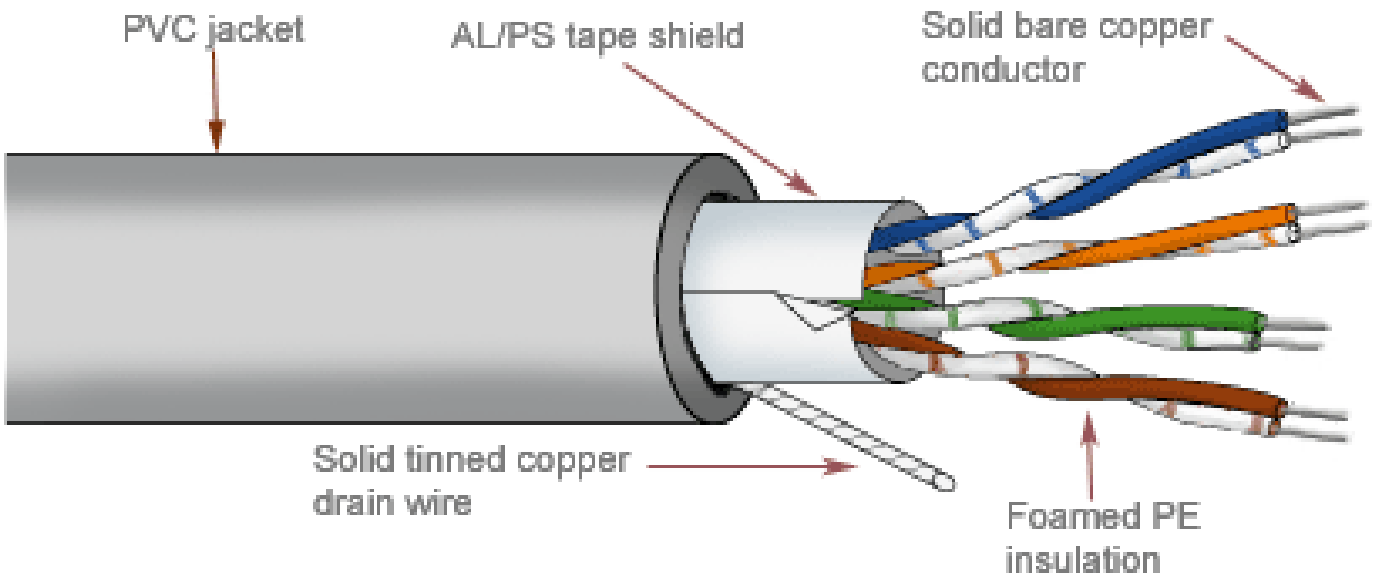


CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Thiết kế cáp cho mạng LAN
  - Các loại cáp
    - Cáp xoán đôi có vỏ bọc chống nhiễu:
    - Cáp xoán đôi có vỏ bọc không chống nhiễu
    - Cáp quang

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

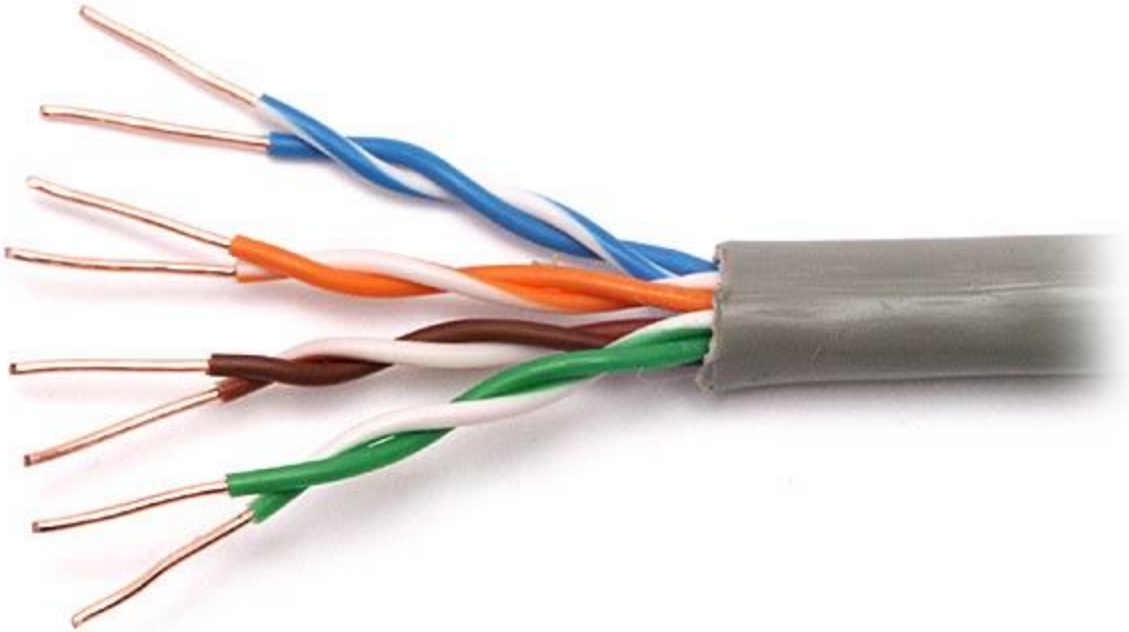
- Cáp xoán đôi có vỏ bọc chống nhiễu:



Cáp STP

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Cáp xoán đôi có vỏ bọc không chống nhiễu:



Cáp UTP

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Cáp quang:

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Cáp UTP thông thường hay sử dụng:
  - Cat 1 & 2: ko dùng truyền dữ liệu
  - Cat 3: dùng cho thoại, sử dụng truyền dữ liệu với chuẩn 10BASE-T Ethernet, tốc độ 4-Mbps
  - Cat 4: tốc độ truyền 16-Mpbs
  - Cat 5: tốc độ 100-Mbps, 4 cặp, hỗ trợ Gigabit
  - Cat 5e: tốc độ 100-Mbps, Gigabit.
  - Cat 6: tốc độ 100-Mpbs, Gigabit, phù hợp với băng thông tốc độ cao.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Lựa chọn thiết bị mạng:
  - Hub:
  - Bridge
  - Switch
  - Router

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Switch:

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Switch:

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Router:

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Lựa chọn công nghệ và thiết bị cho mạng cỡ lớn
  - Công nghệ truy cập từ xa
    - Giao thức PPP
    - Sử dụng modem hoạt động trên cáp đồng trục được cung cấp bởi dịch vụ truyền hình cáp
    - Sử dụng đường thuê bao số
    - Lựa chọn router khi thiết kế WAN doanh nghiệp.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Lựa chọn công nghệ và thiết bị cho mạng cỡ lớn
  - Lựa chọn thiết bị truy cập từ xa khi thiết kế mạng doanh nghiệp
    - Lựa chọn một router cho site ở xa
    - Lựa chọn Router và tường lửa ở site trung tâm
    - Lựa chọn công nghệ WAN

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Lựa chọn công nghệ và thiết bị cho mạng cỡ lớn
  - Lựa chọn thiết bị truy cập từ xa khi thiết kế mạng doanh nghiệp
    - Khi lựa chọn một router cho site ở xa cần chú ý những yêu cầu sau:
      - Đặc tính kỹ thuật đảm bảo an toàn VPN
      - Hỗ trợ NAT
      - Tính tin cậy
      - Chi phí
      - Dễ cấu hình và quản lý
      - Hỗ trợ một hoặc nhiều cổng kết nối ethernet
      - Tích hợp điểm truy cập không dây, hỗ trợ QoS, VoIP

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Lựa chọn công nghệ và thiết bị cho mạng cỡ lớn
  - Lựa chọn thiết bị truy cập từ xa khi thiết kế mạng doanh nghiệp
    - Lựa chọn Router và tường lửa ở site trung tâm cũng có vai trò là điểm đầu cuối của mạng VPN. Khi lựa chọn một VPN firewall, phải chắc chắn nó tương thích với các phần mềm VPN client, số kết nối đồng thời mà nó hỗ trợ, lượng lưu thông có thể chuyển tiếp, bộ xử lý, tốc độ RAM, hỗ trợ nguồn điện dự phòng, mã hóa sử dụng phần cứng, ngoài ra cần chú ý thêm các đặc điểm và thiết bị phải hỗ trợ đó là:
      - Giao thức IPSec, PPTP, L2TP
      - Thuật toán mã hóa: DES-56bit, 3DES 168bit, MPPE, 40, 128bit RC4, 128-192-256 bit AES
      - Xác thực bằng MD5, SHA-1, HMAC với MD5, HMAC với SHA-1
      - Giao thức hệ thống mạng như DNS, DHCP, RADIUS, Kerberos and LDAP
      - Giao thức định tuyến
      - Dịch vụ chứng thực
      - Giao thức an toàn: SSH, HTTP với SSL

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Lựa chọn công nghệ và thiết bị cho mạng cỡ lớn
  - Lựa chọn thiết bị truy cập từ xa khi thiết kế mạng doanh nghiệp
    - Lựa chọn công nghệ WAN
      - Đường thuể riêng
      - Mạng đồng bộ quang SONET
      - Frame Relay
      - ATM
      - Metro Ethernet

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG MẠNG

- Lựa chọn công nghệ và thiết bị cho mạng cỡ lớn
  - Lựa chọn router khi thiết kế WAN doanh nghiệp
    - Những tiêu chí khi lựa chọn router:
      - Phạm vi của dịch vụ và công nghệ được đưa ra bởi nhà cung cấp
      - Phạm vi địa lý, độ tin cậy và hiệu năng của nhà cung cấp
      - Mức an toàn, hỗ trợ được đưa ra bởi nhà cung cấp
    - Ngoài ra, cũng cần hiểu về đặc tính mạng bên trong của nhà cung cấp dịch vụ như tính dự phòng, tần số lỗi, cách thức bảo đảm an toàn của hệ thống mạng bên trong nhà cung cấp dịch vụ; một số vấn đề kỹ thuật như số port, tốc độ xử lý, môi trường và công nghệ được hỗ trợ.