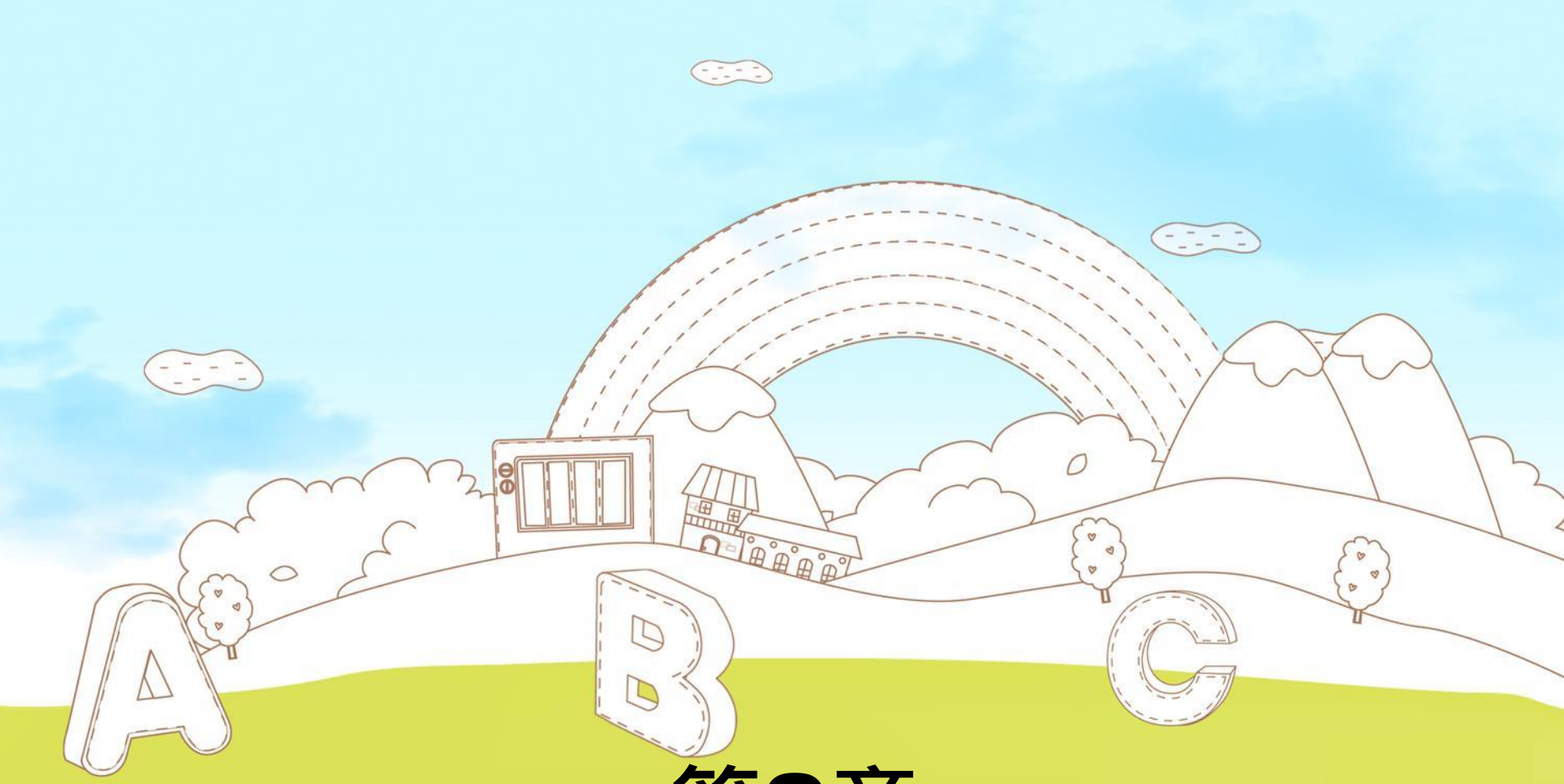
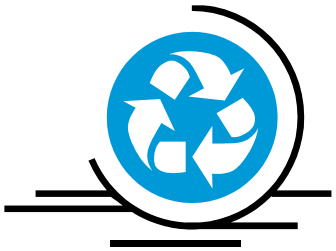


第2章
结构化和模块化设计

Cisco网络服务体系架构概述



设计模型

不分层结构

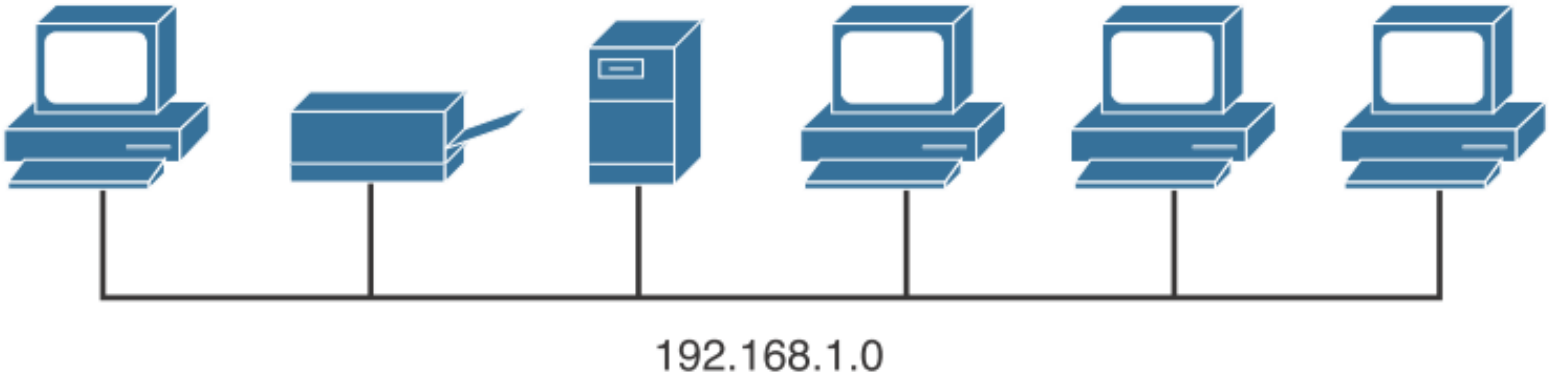
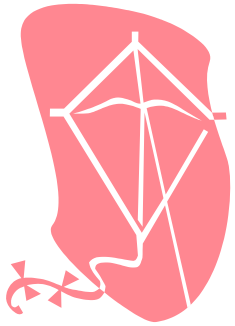


Figure 1-1 *Simple Shared Ethernet Network*



层次模型

网络分隔

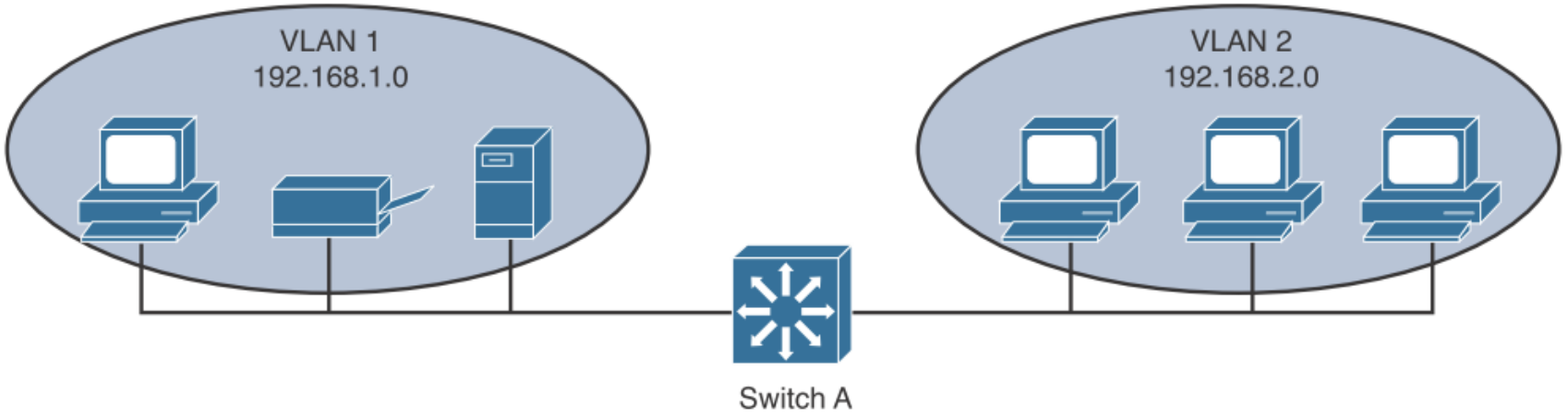


Figure 1-2 *Example of Network Segmentation*

VLAN子网

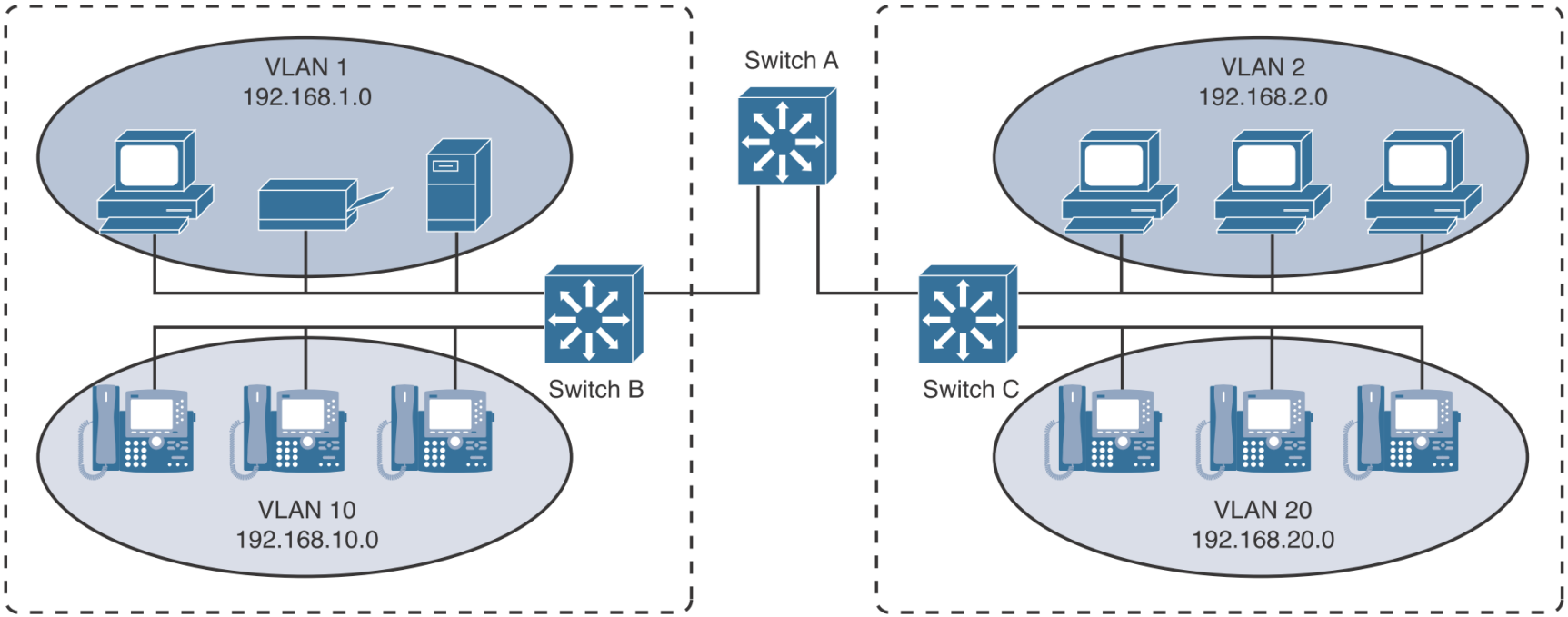


Figure 1-4 *Network Growth Through New VLANs*

二层结构

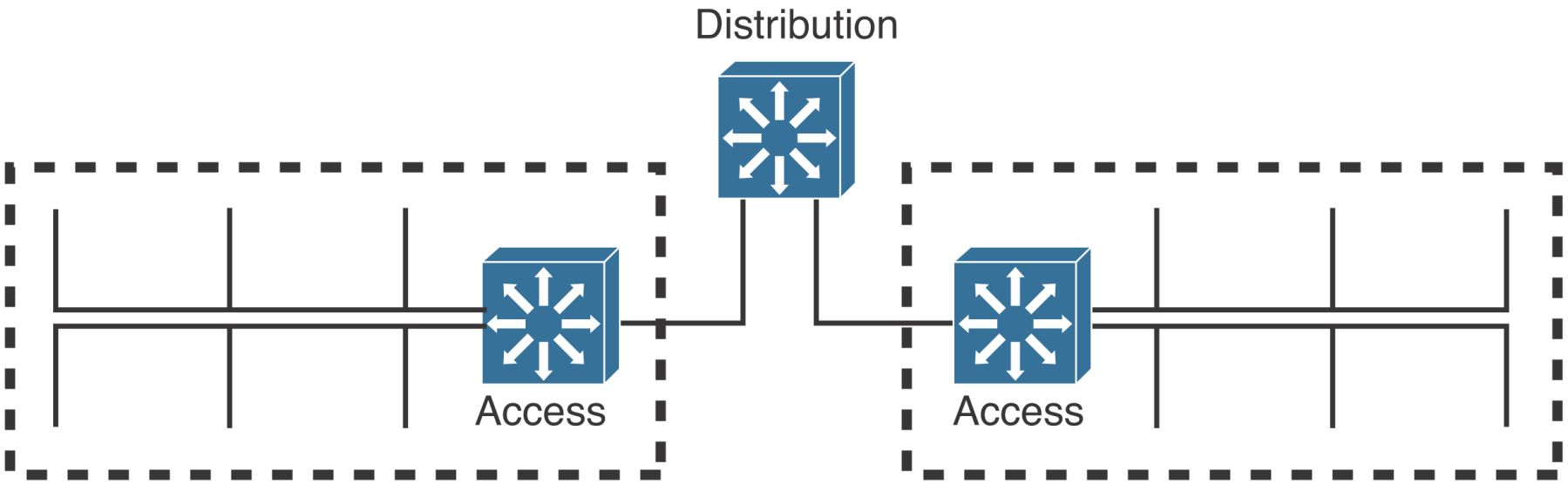


Figure 1-5 *Two-Layer Network Hierarchy Emerges*

三层结构

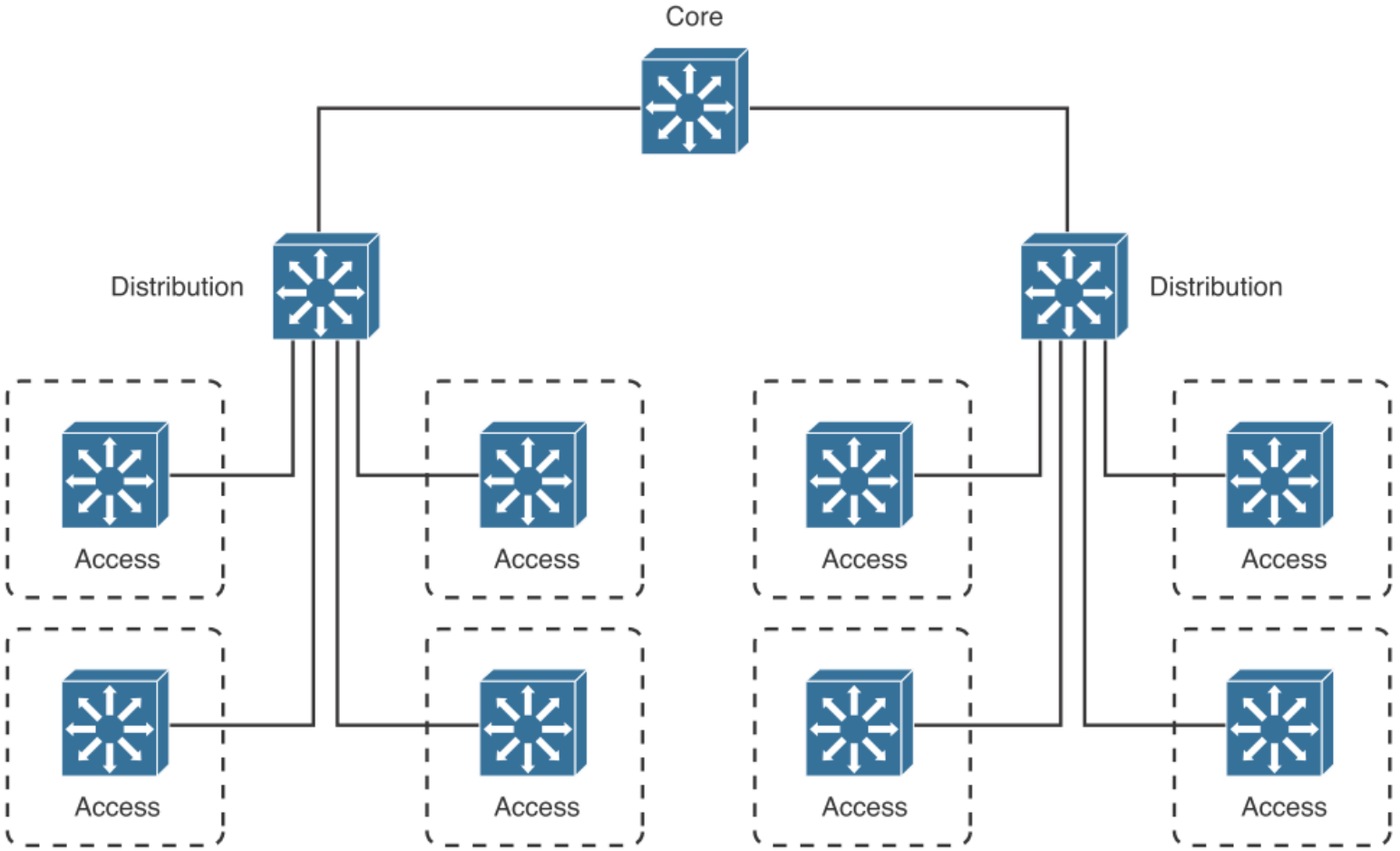
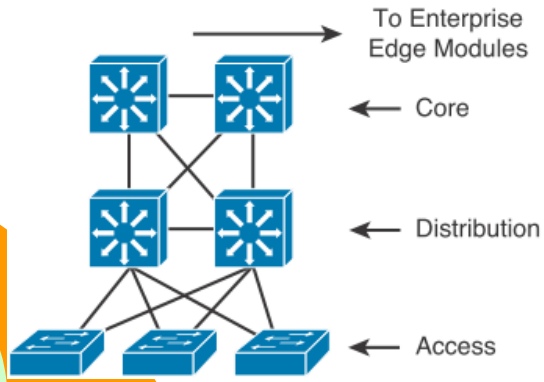


Figure 1-6 *Core Layer Emerges*

层次模型★



核心层core
高速转发.

分布层 distribution
基于策略的连接

接入层access
本地和远程工作组接入

aggregation layer (distribution layer)，汇聚层/分布层

Core Layer

Layer	Description
Core	• Fast transport • High reliability • Redundancy • Fault tolerance • Low latency and good manageability • Avoidance of slow packet manipulation caused by filters or other processes • Limited and consistent diameter • QoS

Distribution Layer

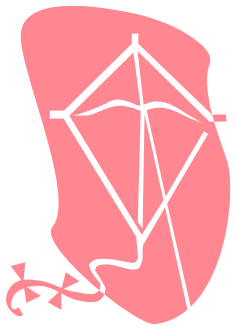
Layer	Description
Distribution	• Policy-based connectivity • Redundancy and load balancing • Aggregation of LAN wiring closets • Aggregation of WAN connections • QoS • Security filtering • Address or area aggregation or summarization • Departmental or workgroup access • Broadcast or multicast domain definition • Routing between VLANs • Media translations (for example, between Ethernet and Token Ring) • Redistribution between routing domains (for example, between two different routing protocols) • Demarcation between static and dynamic routing protocols

Access Layer

Layer	Description
Access	• Layer 2 switching • High availability • Port security • Broadcast suppression • QoS • Rate limiting • ARP inspection • VACLs • Spanning tree • Trust classification • Network Access Control (NAC) • PoE and auxiliary VLANs for VoIP

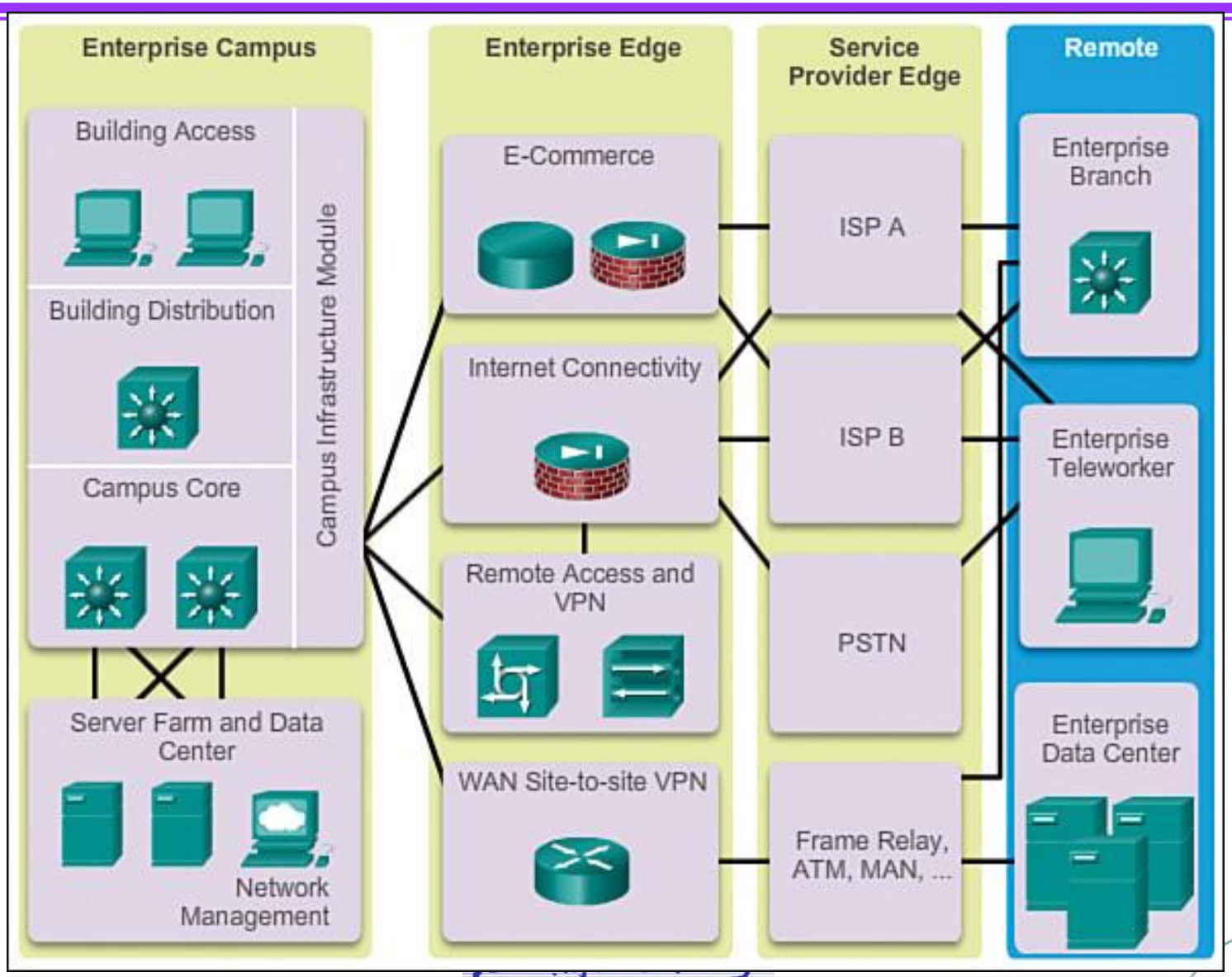
Benefits of the Hierarchical Model

- 层次结构的优点:★
  - Cost savings
  - Ease of understanding
  - Modular network growth
  - Improved fault isolation



CISCO企业架构

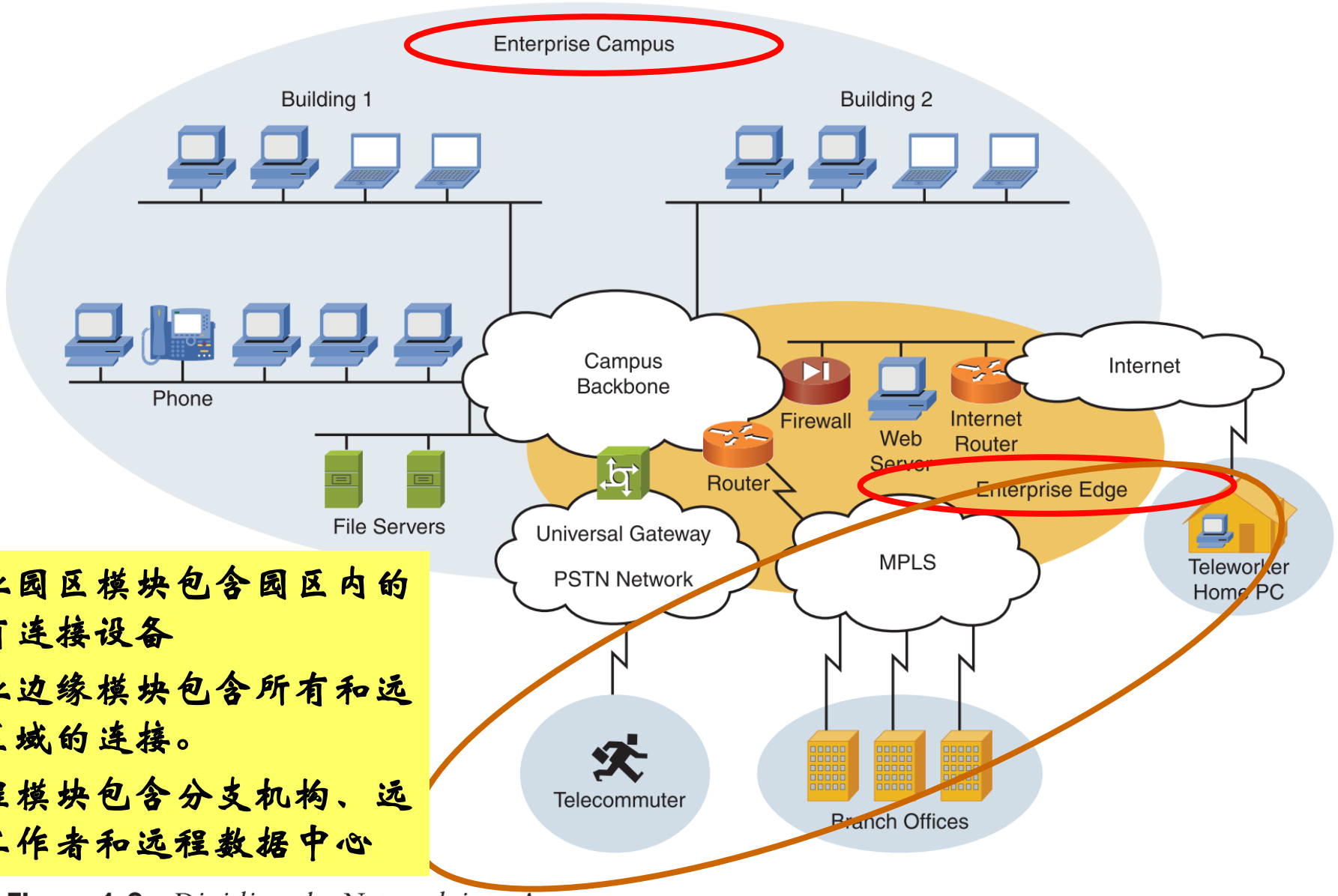
CISCO 企业网络架构★



子模块★

- CISCO 企业网络架构子模块
  - 企业园区：
    Enterprise Campus Modules
  - 企业边缘：
    Enterprise Edge Modules
  - 服务提供商：
    Service Provider Modules
  - 远程模块：
    Remote Enterprise Modules

区域划分



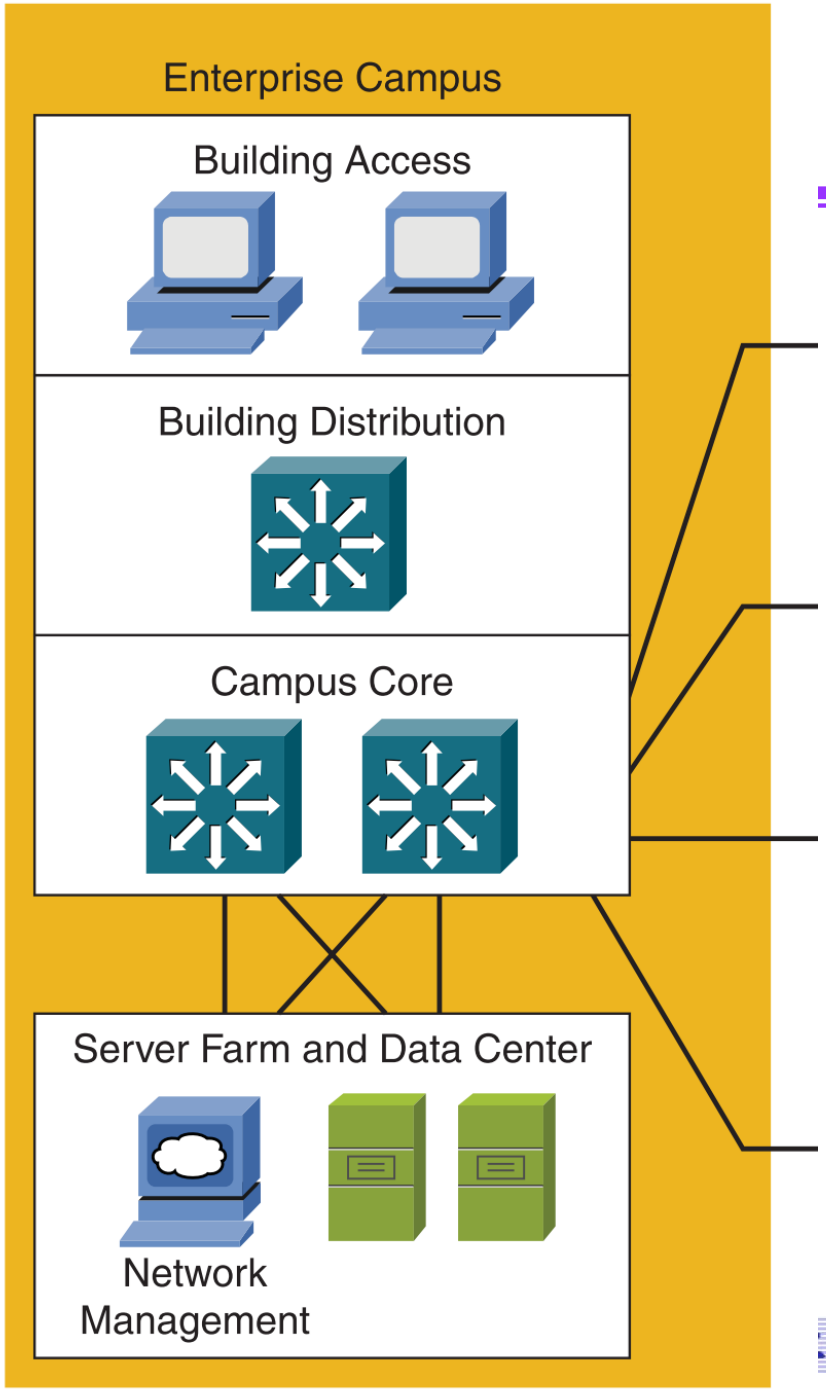
企业园区模块包含园区内的所有连接设备

企业边缘模块包含所有和远程区域的连接。

远程模块包含分支机构、远程工作者和远程数据中心

CISCO 企业架构

企业园区



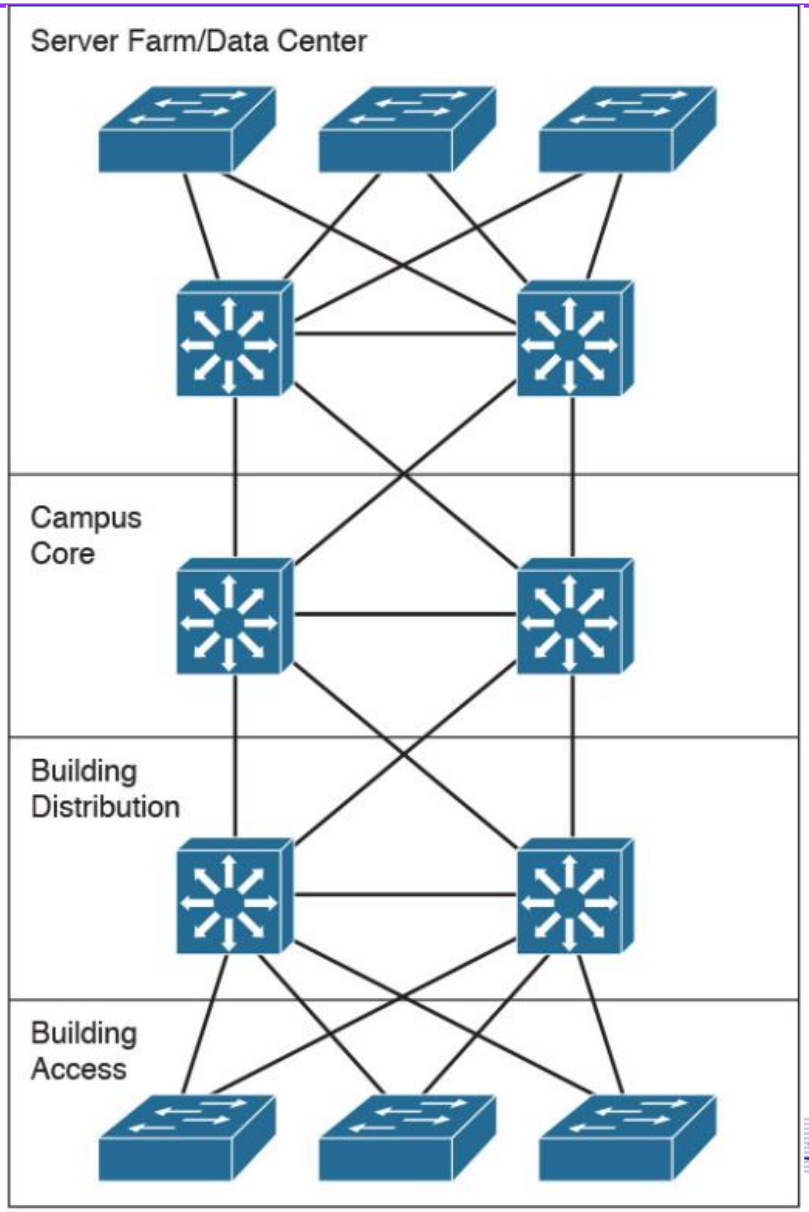
企业园区模块

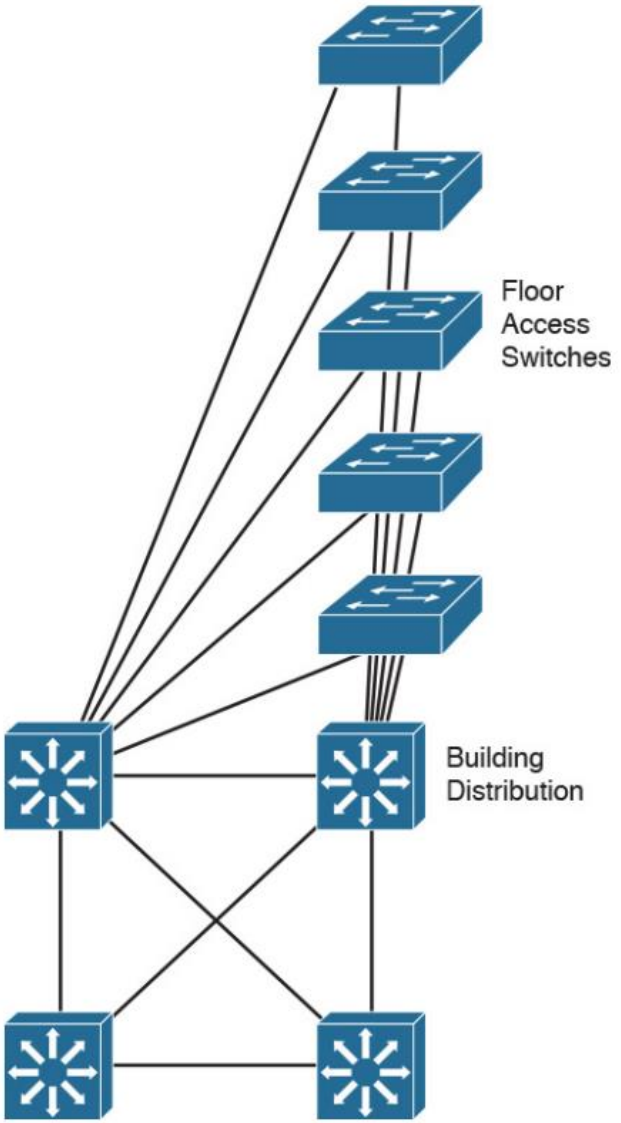
- 企业园区模块：★
  - 楼宇接入层：
    Building access
  - 楼宇汇聚层：
    Building distribution
  - 园区核心层：
    Campus core
  - 服务器群和数据中心：
    Server farm and data center

企业园区子模块划分

- 企业园区子模块划分
  1. 选择需要进行楼宇接入层和分布层设计的建筑。
  2. 确定接入层交换机的数目和位置。
  3. 确定分布层交换机（至少2台）。
  4. 每个接入层交换机使用两条上行链路分别连接到两台分布层交换机。
  5. 确定服务器位置，设计服务器群模块，使用至少两台分布层交换机连接各个服务器。使用带外连接连接所有网络关键设备，实行网络管理。
  6. 确定核心层交换机（至少2台），保证足够流量。
  7. 使用冗余链路将相关模块连接到园区核心模块。

多楼层连接


Server Farm/Data Center
Campus
Core
Building
Distribution
Building
Access


Floor
Access
Switches
Building
Distribution

服务集群

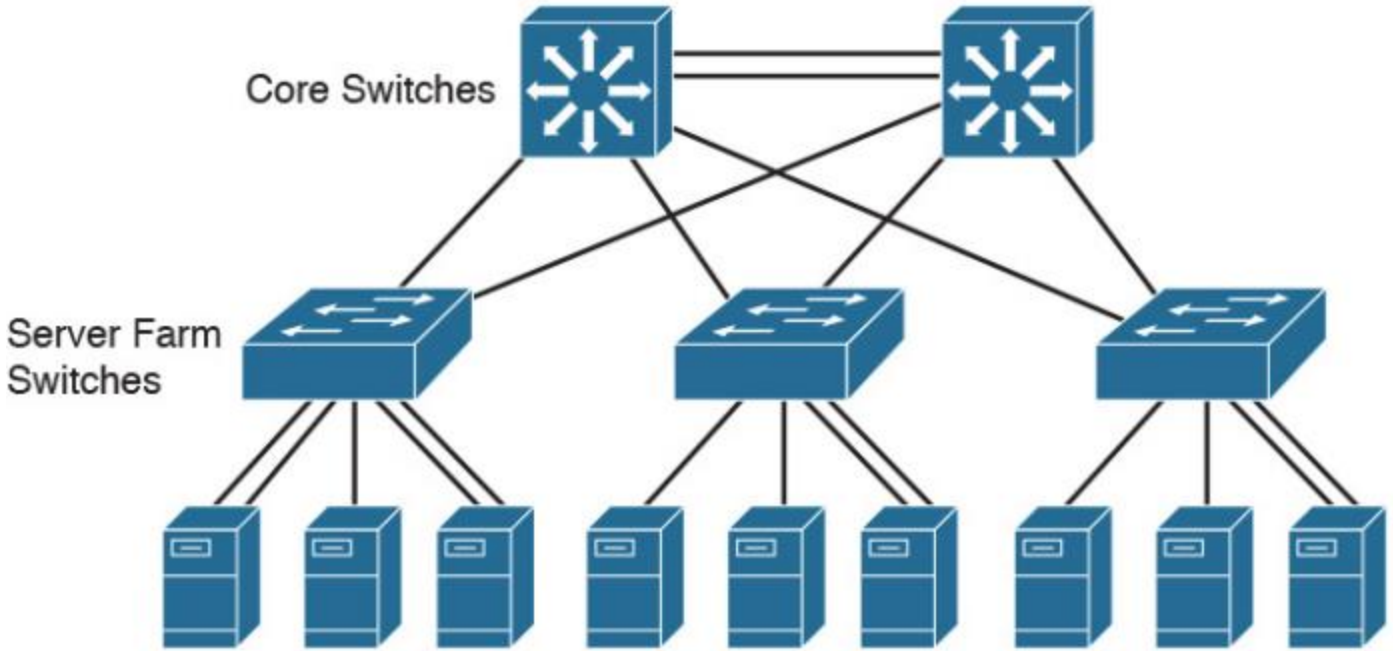
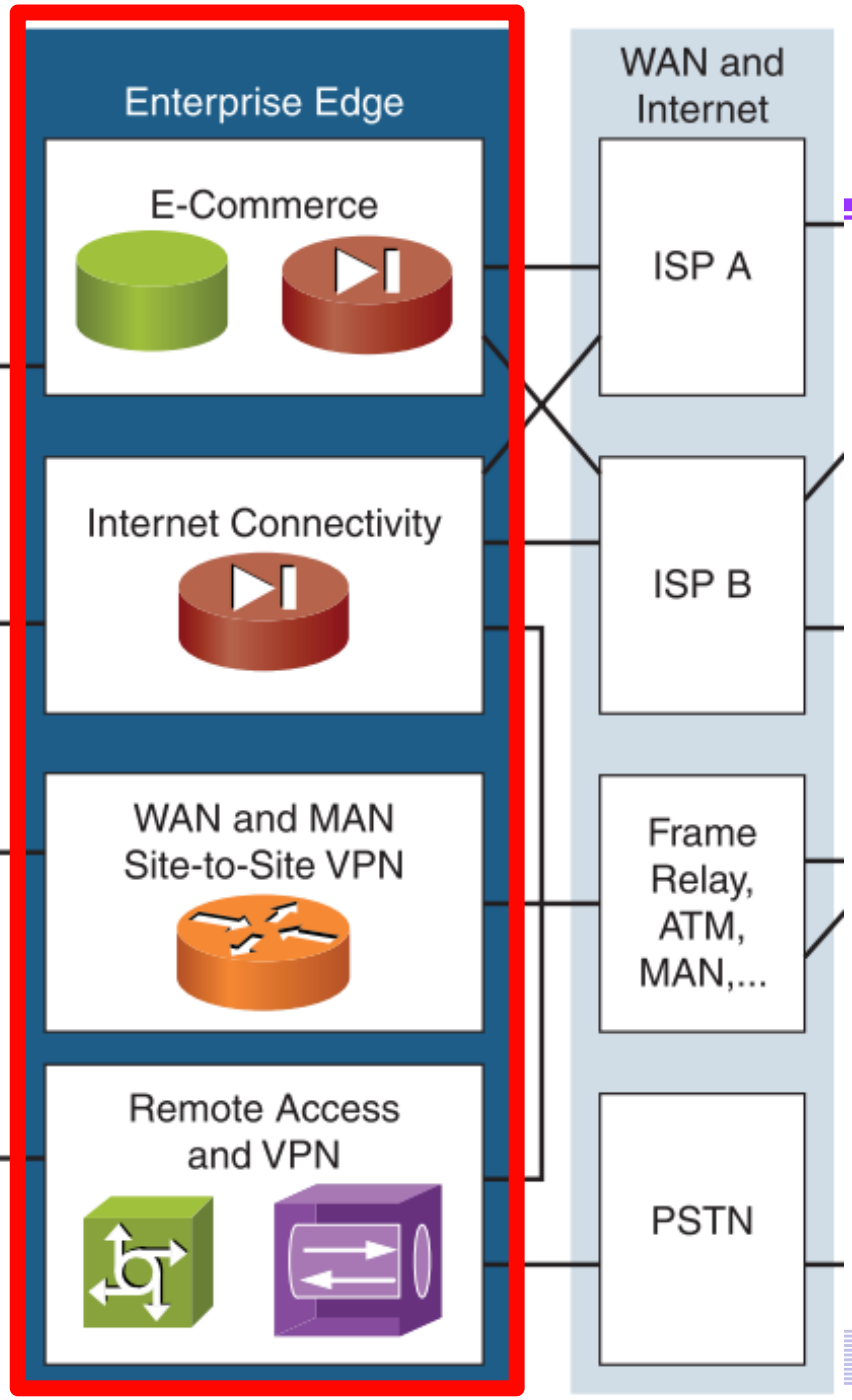


Figure 3-17 *Server farm*

CISCO 企业架构

企业边界

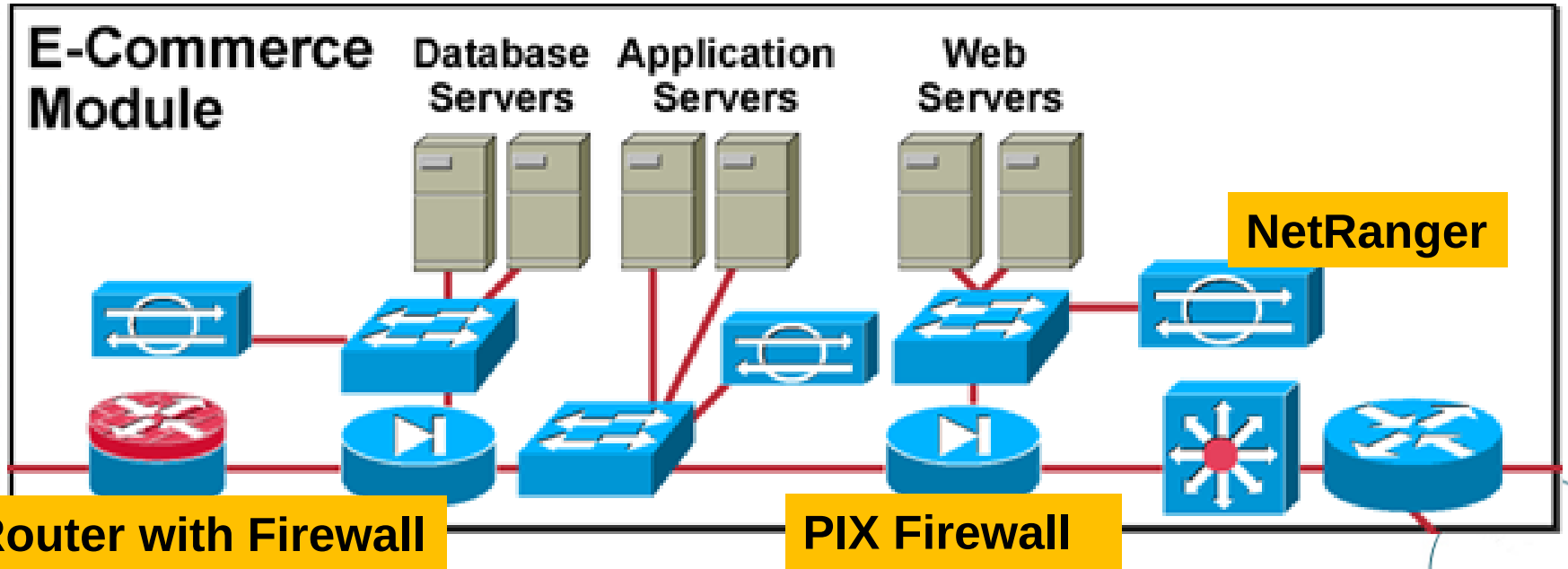


企业边界模块

- 企业边界模块★
  - 电子商务：E-commerce
  - 因特网接入：Internet connectivity
  - WAN、MAN和站点对站点的VPN：WAN and MAN and Site-to-site VPN
  - 远程访问和VPN：Remote access and VPN

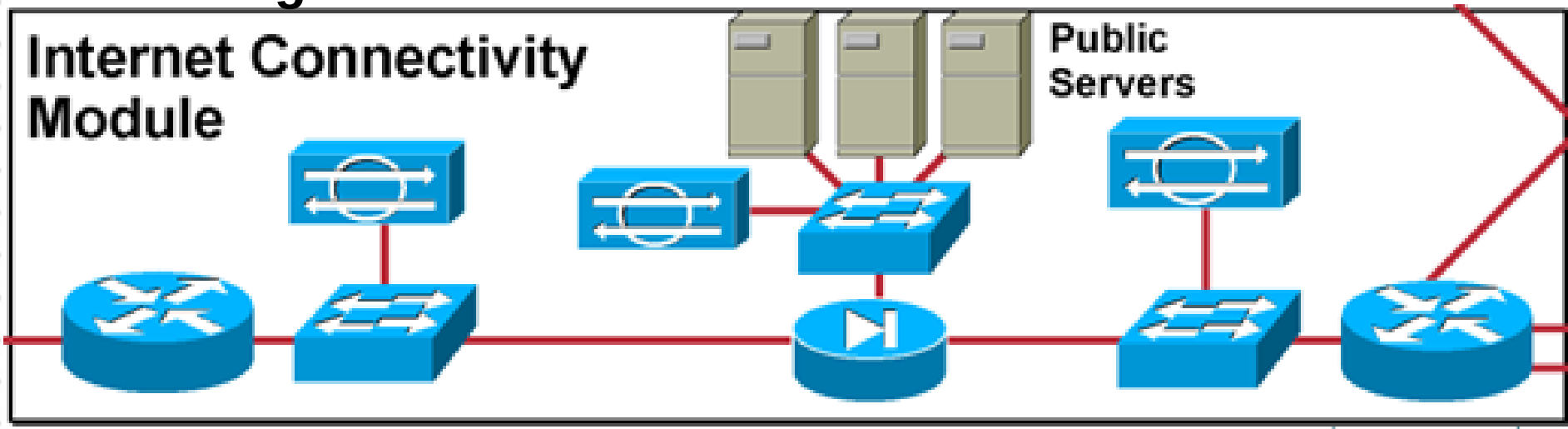
E-commerce

- 电子商务模块，包含以下组件：
  - Web servers
  - Application servers
  - Database servers
  - Firewall or firewall routes
  - Network intrusion prevention system (NIPS) appliances
  - Multilayer switch with IPS modules



Internet connectivity

- 因特网连接模块，提供因特网相关的服务
  - SMTP mail servers
  - Domain Name System (DNS) servers
  - Public servers(FTP and HTTP)
  - Firewall or firewall routers
  - Edge routers



WAN / MAN / site-to-site VPN

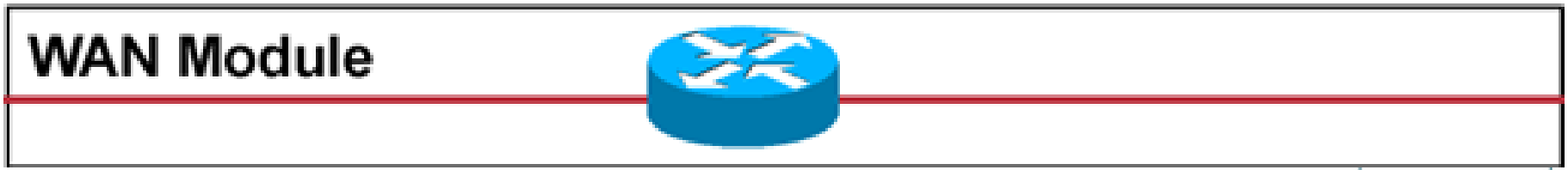
- **WAN/MAN/站点到站点VPN，实现总部和分支机构间的连接：**
  - **传统技术(leased lines and circuit-switched data link technologies, Frame Relay, and ATM)**
  - **新技术（SONET and SDH, cable, DSL, MPLS, Metro Ethernet, wireless, and service provider VPNs）**

SDH（Synchronous Digital Hierarchy，同步数字体系）

SONET （Synchronous Optical Network）同步光纤网络

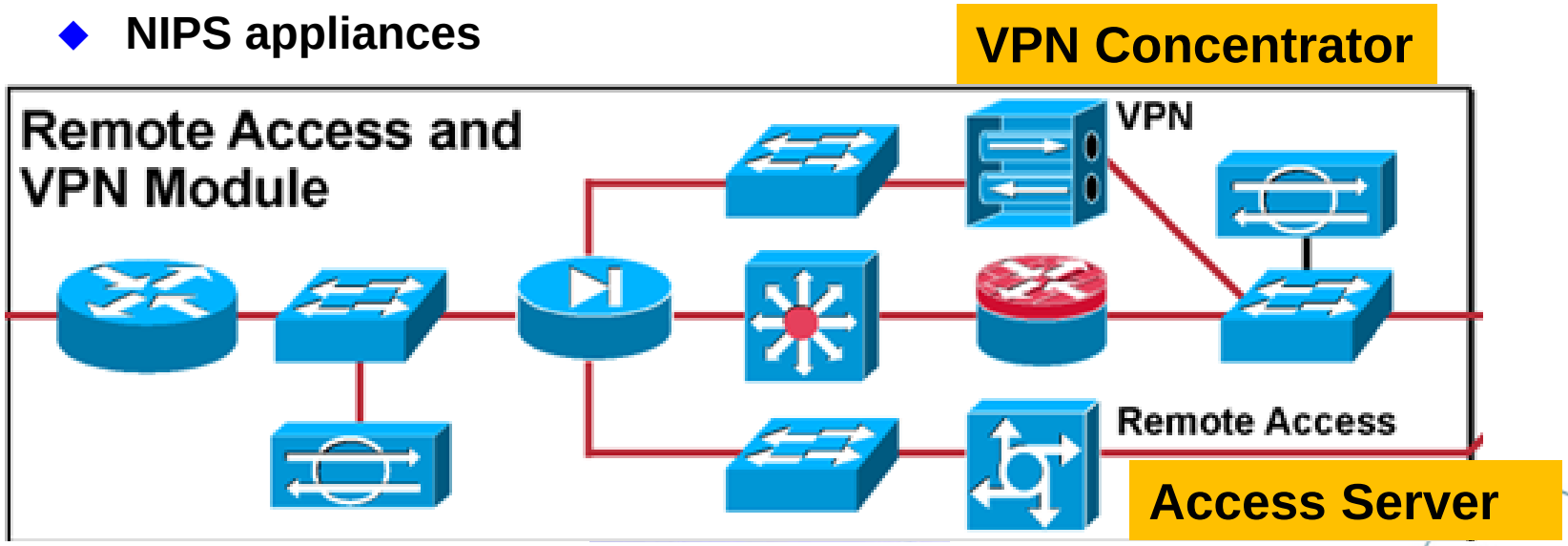
DSL(Digital Subscribe Line)数字用户线路

MPLS(Multi-Protocol Label Switching)多协议标签交换



Remote access and VPN

- 远程接入和远程VPN接入，实现远程工作人员的安全接入，
  - Dial-in access concentrators
  - VPN concentrators
  - Cisco Adaptive Security Appliances (ASA)
  - Firewalls or firewall routers
  - Intrusion detection system (IDS) appliances
  - NIPS appliances



企业边界模块的创建

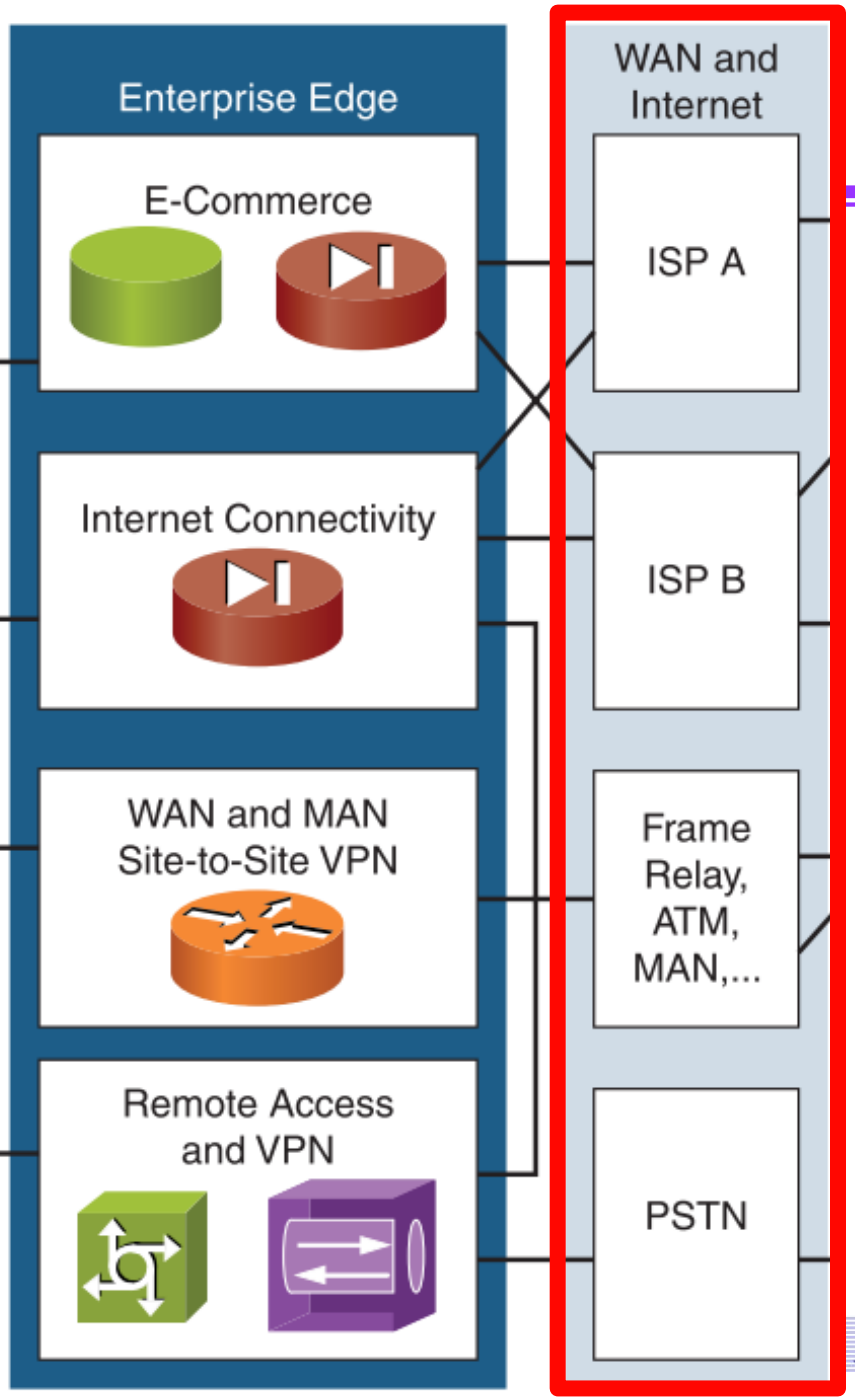
■企业边界模块的创建

- ◆创建电子商务模块，客户和合作伙伴可以通过因特网访问商务应用和数据服务器。
- ◆确定和因特网相连的连接，划分到因特网连接模块。（企业员工）
- ◆如果需要从外部使用VPN或拨号访问内部网络，则需要设计远程访问和VPN模块。（外出员工）
- ◆将需要使用永久的、专用的线路连接到企业远程区域的部分划分到WAN/MAN/站点到站点VPN模块。（分支机构）

公开的网页服务器可以放在因特网连接模块或电子商务模块。

CISCO 企业架构

服务提供模块



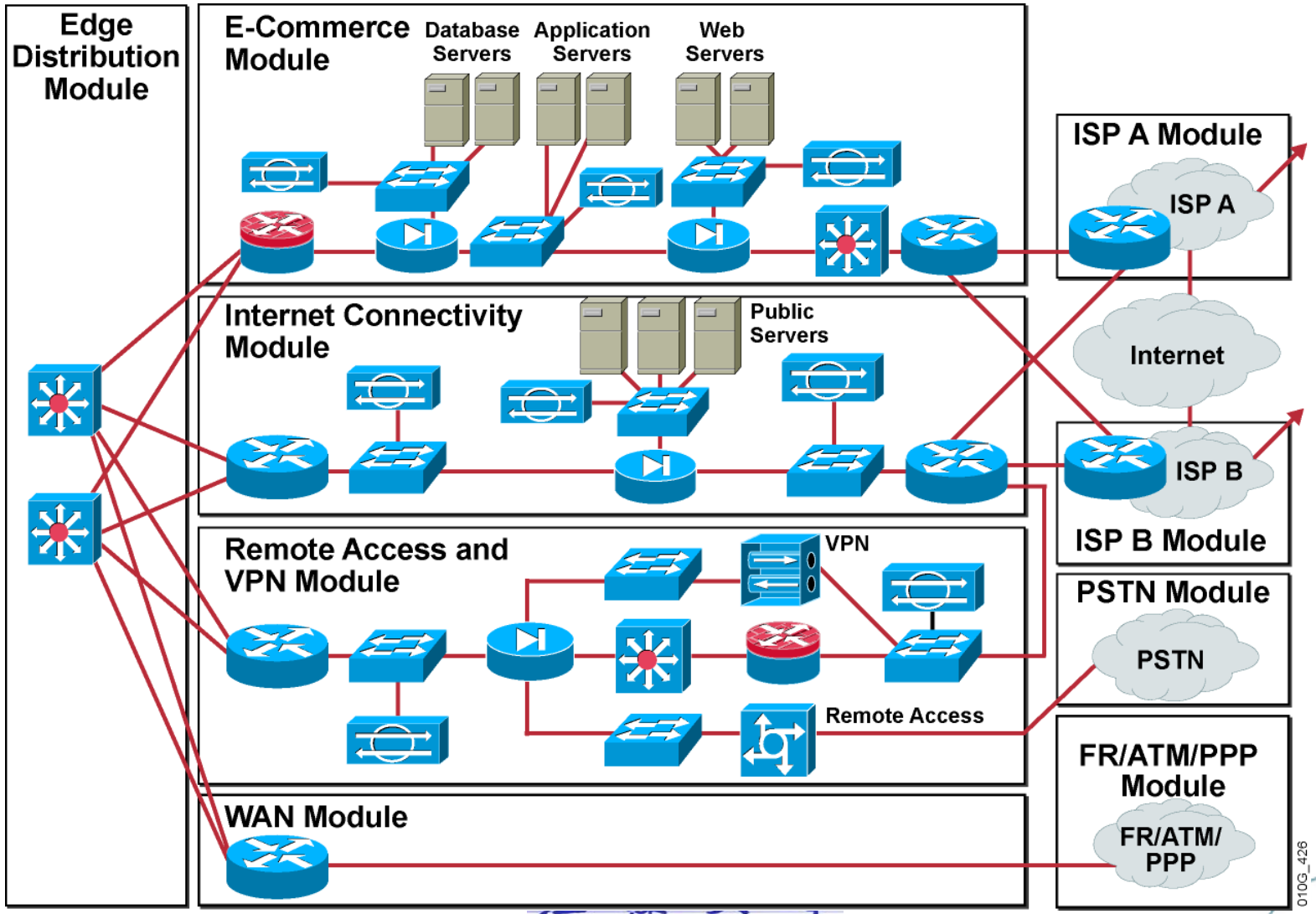
服务提供模块

- **服务提供模块★**
  - 由**服务提供商**设计，拥有，管理，运行。
    - **ISP Module**
    - **WAN Module**
    - **PSTN Module**

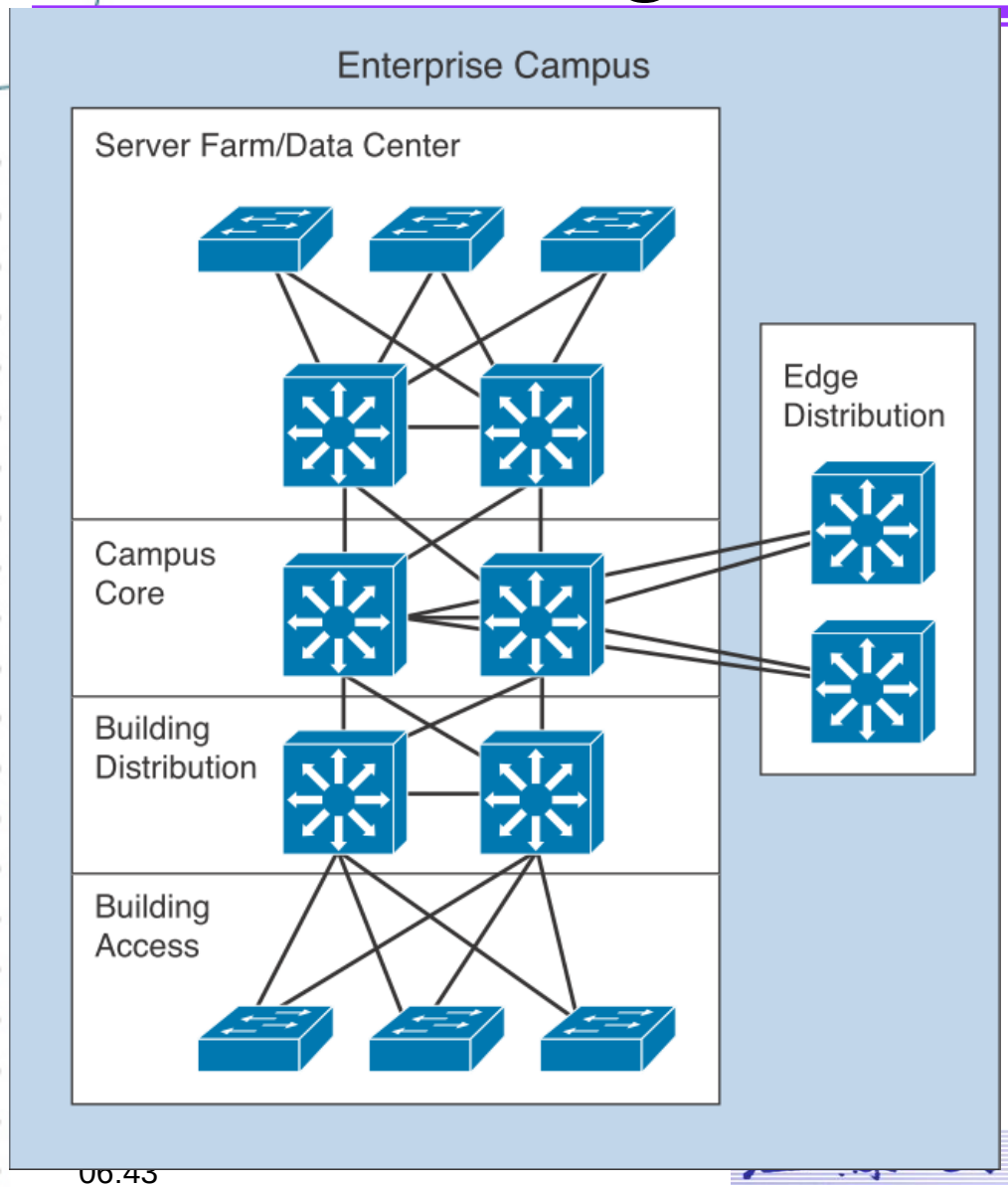
服务提供模块

- 服务提供模块
  - Internet Service Provider Module，ISP
    - ISP模块表示企业通过ISP网络进行因特网访问和企业边缘服务。可使用任意 WAN 技术。
  - Public Switched Telephone Network Module，PSTN
    - PSTN模块代表所有非永久WAN连接技术。PSTN使用拨号设备进行网络连接（ISDN, analog, and wireless telephony (cellular) technologies）.
  - Frame Relay/ATM Module，WAN
    - WAN模块代表所有永久连接到远端的WAN连接技术。

边界及服务提供模块


Edge Distribution Module
E-Commerce Module
Database Servers
Application Servers
Web Servers
Internet Connectivity Module
Public Servers
Remote Access and VPN Module
VPN
Remote Access
WAN Module
ISP A Module
ISP A
Internet
ISP B
ISP B Module
PSTN Module
PSTN
FR/ATM/PPP Module
FR/ATM/ PPP
010G_426

Edge distribution



边缘分布层可以为园区局域网和企业边界之间增加额外的安全保护：

- IP spoofing
- Unauthorized access
- Network reconnaissance
- Packet sniffers

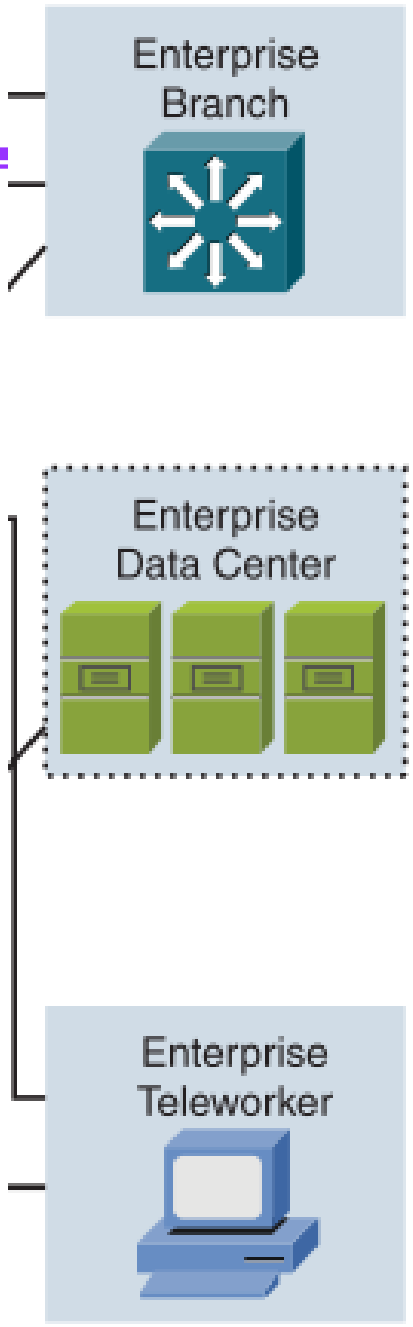
边缘分布层可以和园区核心层合并

CISCO 企业架构

企业远程模块

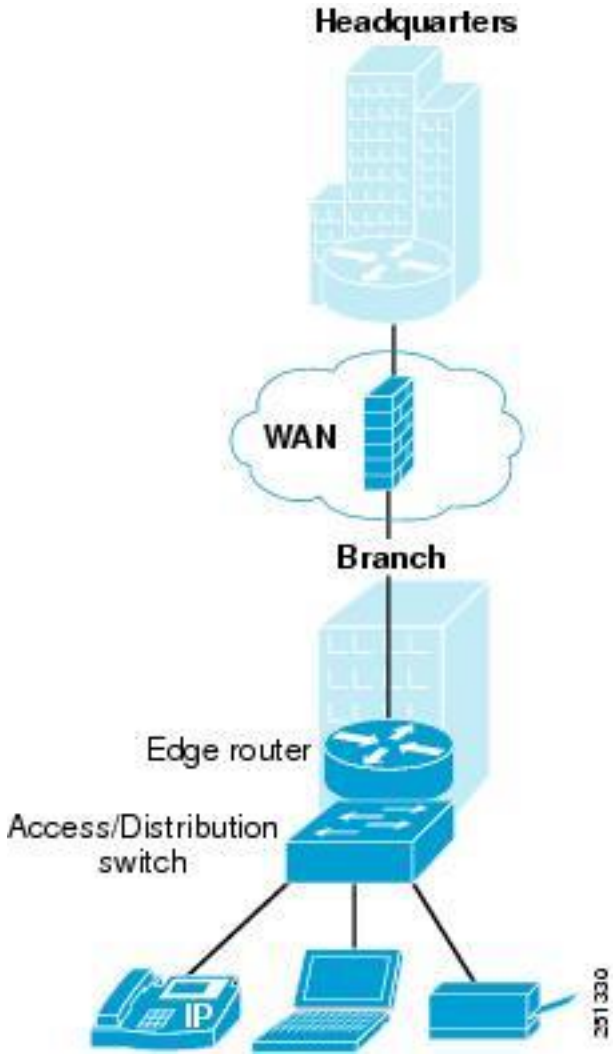
企业远程模块

- 企业远程模块包含：★
  - Enterprise branch
    企业分支机构
  - Enterprise data center
    企业远程数据中心
  - Enterprise teleworker
    企业远程工作者



Enterprise Branch Module

- 企业分支模块用来扩展企业网络的范围
  - 高速因特网访问
  - 合作伙伴的VPN接入
  - 居家办公人员的远程通讯功能
  - 视频会议功能
  - 基于IP网络的语音通话和传真功能



企业数据中心

- 远程企业数据中心，提高了安全性，降低了运营成本。可用于灾难恢复和企业的不间断服务。
  - **Networked infrastructure**: Gigabit or 10 Gigabit Ethernet switching, InfiniBand, and storage switching and optical transport
  - **Interactive services**: Storage fabric services, computer services, security services, and application optimization services
  - **Management**: Cisco Fabric Manager (element and network management) and Cisco VFrame (server and service provisioning)

Enterprise Teleworker Module

- 企业远程工作者模块提供了分散地理区域（家庭办公、旅馆等）到中央应用和网络服务的高安全性访问

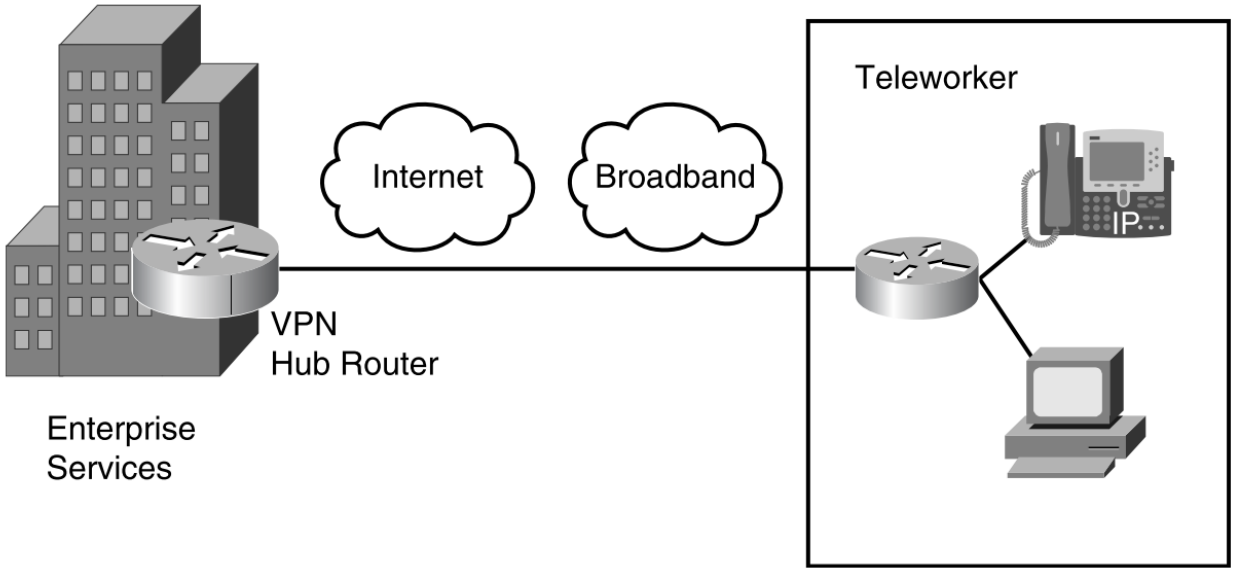


Figure 2-14 *Enterprise Teleworker Solution*

CISCO 企业架构

总结

CISCO 企业网络架构

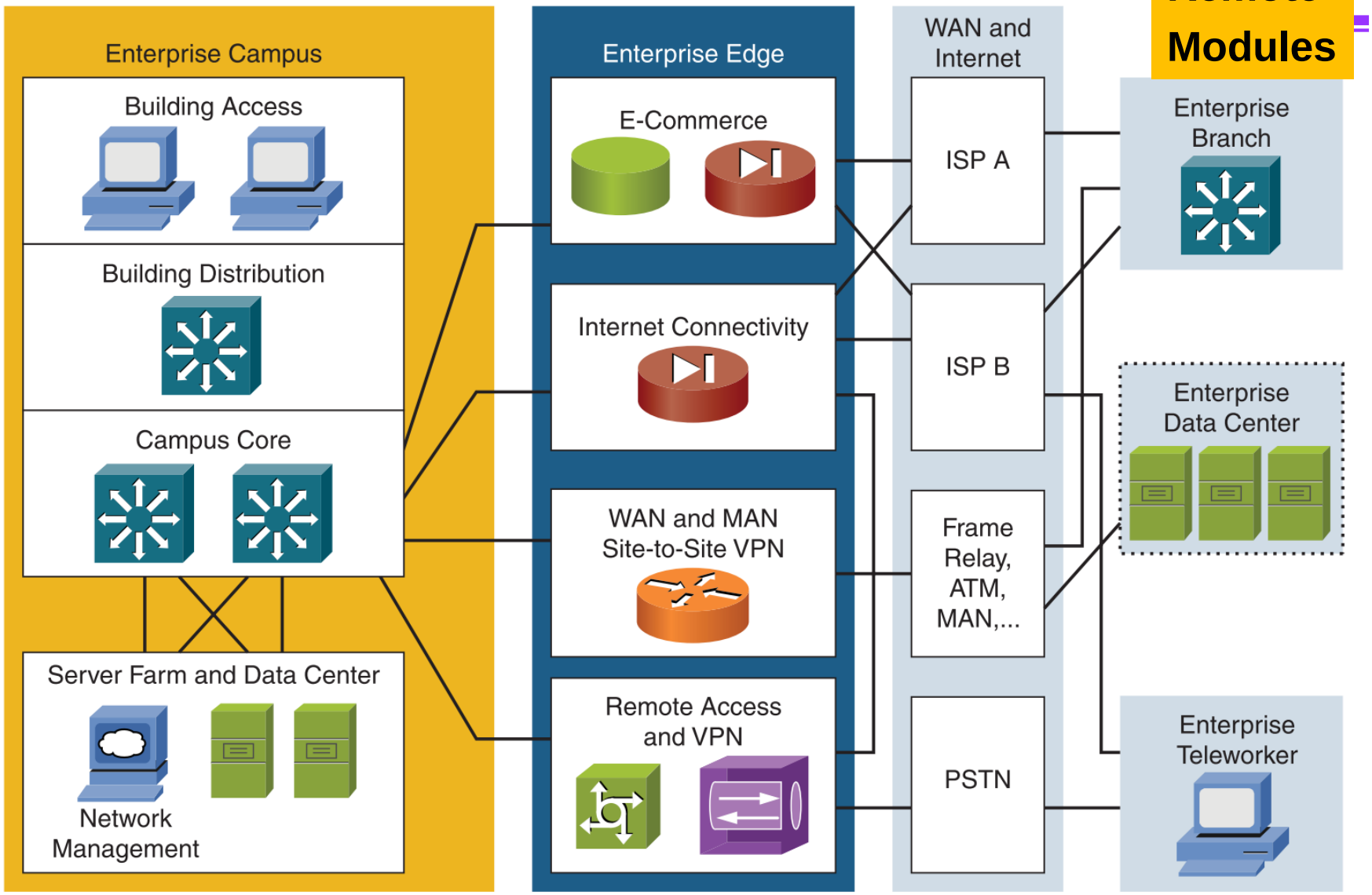
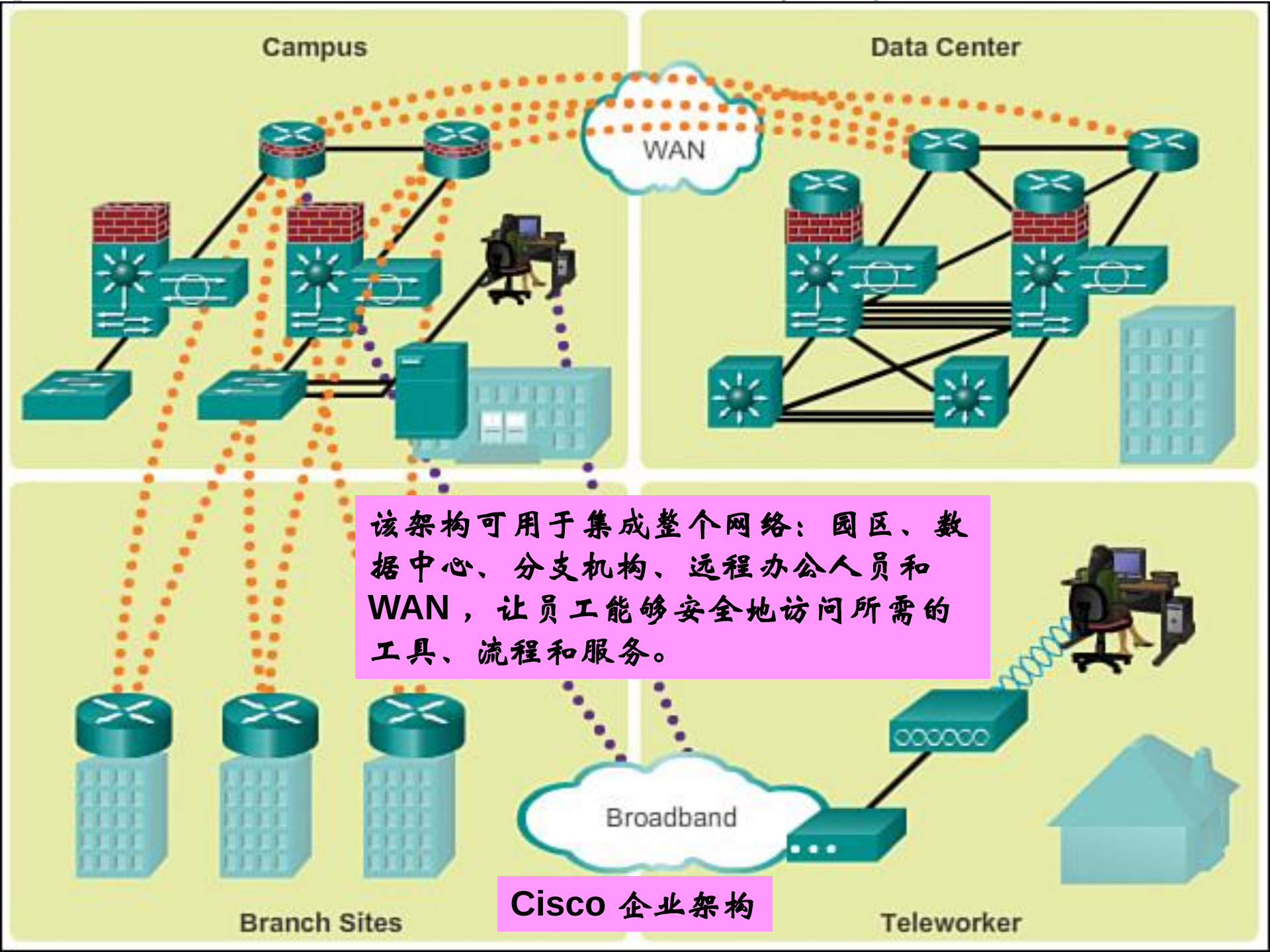
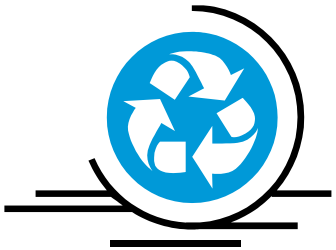


Figure 1-6 *Modular Network Design*



该架构可用于集成整个网络：园区、数据中心、分支机构、远程办公人员和 WAN，让员工能够安全地访问所需的工具、流程和服务。

Cisco 企业架构



企业网络设计方法

设计流程

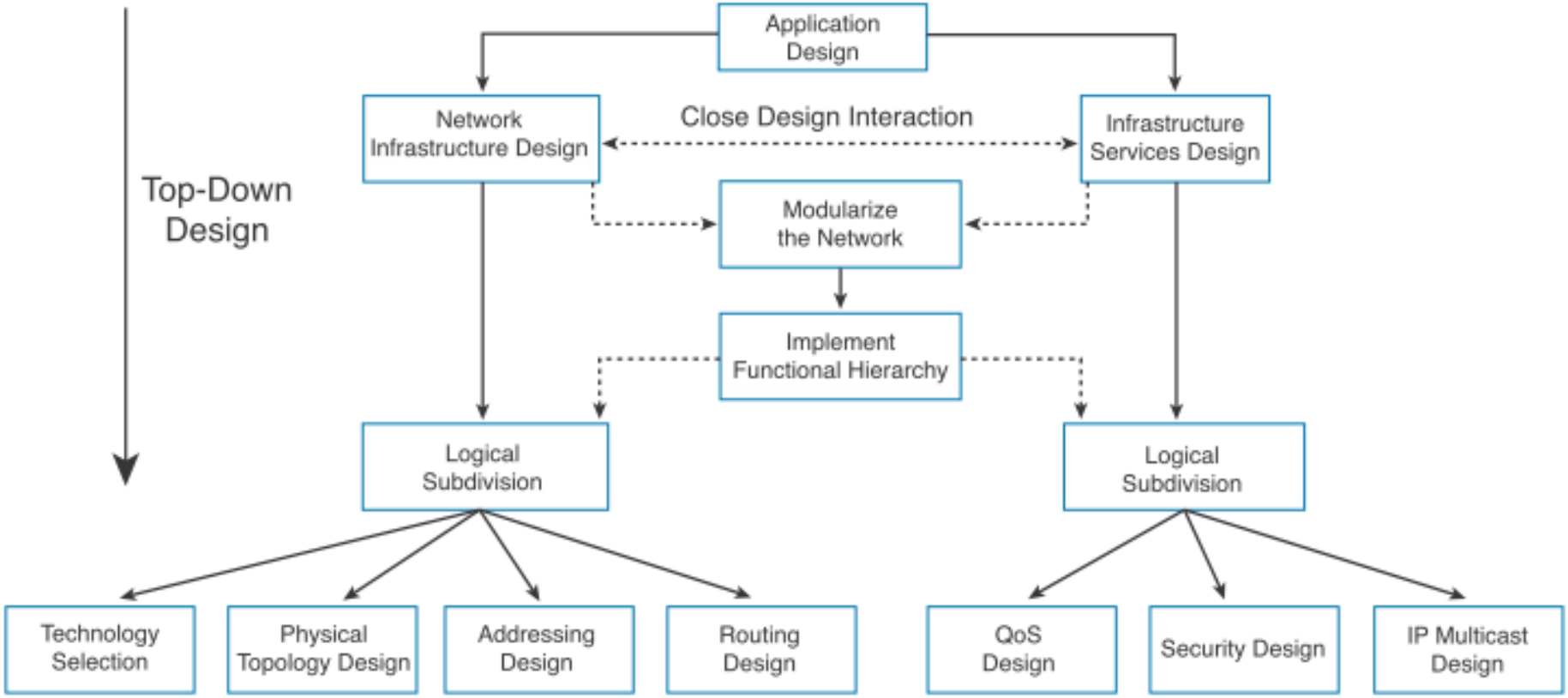
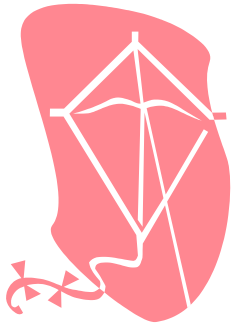


Figure 1-7 *Top-down design process*

企业园区网的设计流程★

- 企业园区网7步设计流程：
  - 第1步确定应用和数据传输需求。
  - 第2步设计逻辑网络。
  - 第3步设计物理网络。
  - 第4步选择网络设备，画出网络拓扑结构图，
  - 第5步选择合适的IP编址策略及编号方案。
  - 第6步选择路由协议。
  - 第7步设计边缘分发模块。

企业园区网的设计流程



第1步确定应用和数据传输需求

分析网络流量模型

- 园区单元的特性信息：
  - 活跃应用
  - 应用类型
  - 用户数量
  - 服务器数量
  - QoS需求
    - 如带宽、丢包率和时延容限等

Example: Characterizing Applications

Name of Application	Location	Type of Application	Number of Users	Number of Servers	Bandwidth/ Delay Tolerance/ Loss Characteristics
Marketing DSS	Building 1	Database (OLAP)	137	3	High bandwidth High delay tolerance Low loss
Corporate e-mail	Building 2	E-mail	65	2	Low bandwidth Low delay tolerance Low loss
File server	Building 3	File sharing (FTP)	48	1	Low bandwidth Medium delay tolerance Low loss

园区内信息流动

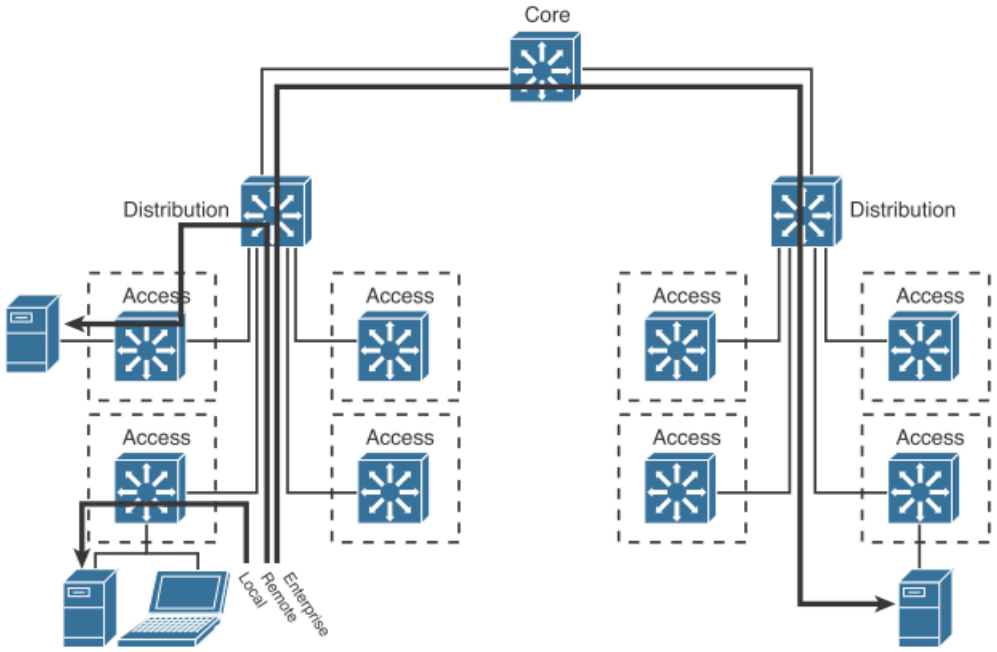


Figure 1-7 *Traffic Flow Paths Through a Network Hierarchy*

Table 1-2 *Types of Network Services*

Service Type	Location of Service	Extent of Traffic Flow
Local	Same segment/VLAN as user	Access layer only
Remote	Different segment/VLAN as user	Access to distribution layers
Enterprise	Central to all campus users	Access to distribution to core layers

网络应用类型★

- 常见有四种网络应用类型
  - Peer-peer
  - Client–local server
  - Client–data center
  - Client–enterprise edge server

对等应用

- Peer-Peer Applications

- 常见应用
  - 即时通讯，当用户建立连接后两者直接通讯。
  - IP 电话
  - 文件共享， 如WINDOWS系统
  - 视频会议

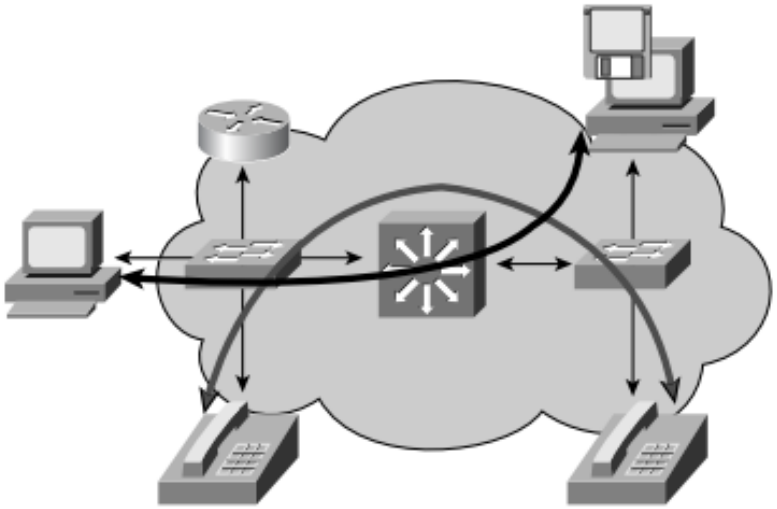


Figure 4-1 *Peer-Peer Applications*

客户-本地服务器方式

- Client–Local Server Applications

80/20规则

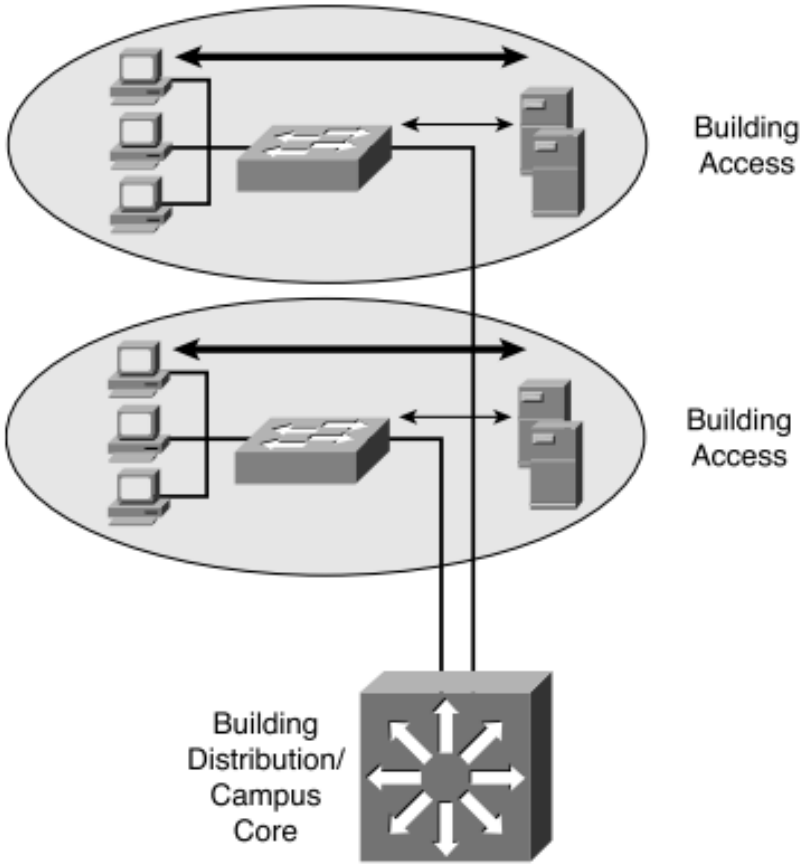


Figure 4-2 *Client–Local Server*

客户-数据中心方式

- Client–Data Center Applications

20/80规则

- 常见应用：
  - 企业（内部）邮件服务器
  - 通用文件服务器
  - 通用数据库服务器

高安全性
高可用性
高带宽
高可管理性

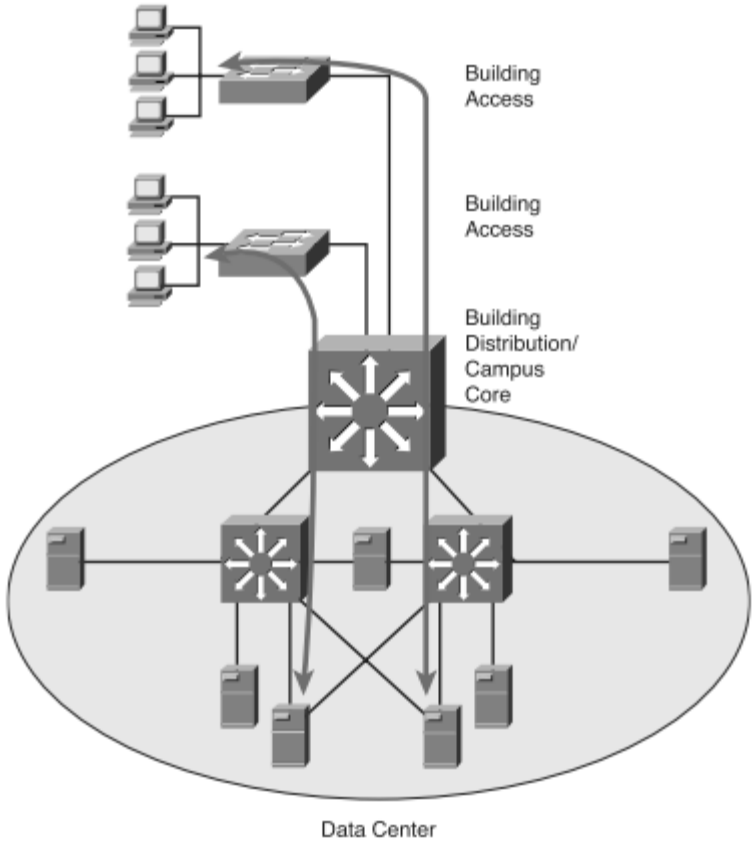


Figure 4-3 *Client–Data Center Application*

客户-企业边界应用

- Client–Enterprise Edge Applications

- 常见应用：
  - 外部邮件系统
  - DNS服务
  - 公开网站

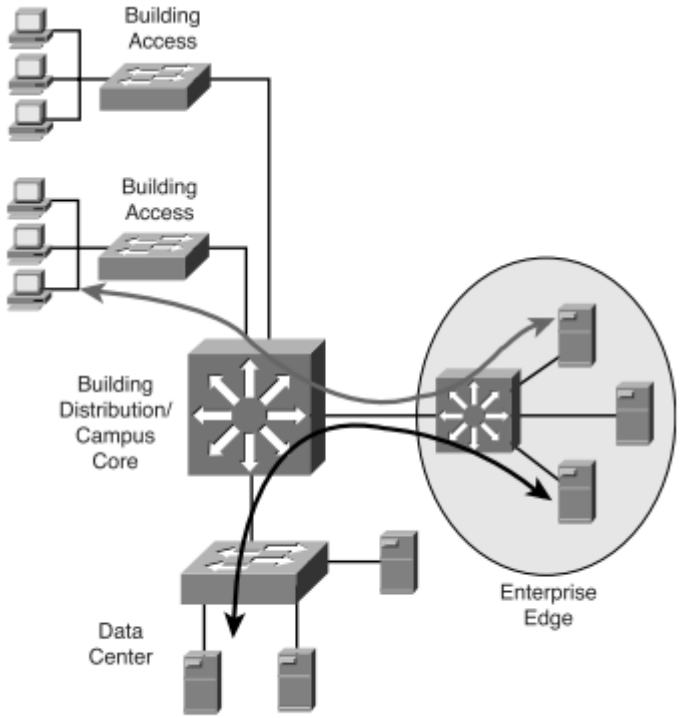
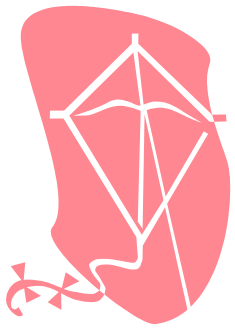


Figure 4-4 *Client–Enterprise Edge Application*

不同网络类型的特性比较

	Peer-Peer	Client–Local Servers	Client–Data Center	Client–Enterprise Edge Servers
Connectivity type	Switched	Switched	Switched	Switched
Total required throughput	Medium to high	Medium	High	Medium
High Availability	Low to high	Medium	High	High
Total network costs	Low to medium	Medium	High	Medium

企业园区网的设计流程



第2步设计逻辑网络

逻辑网段划分

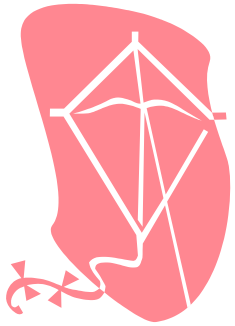
- 逻辑网段划分：
  - 在物理网络中划分VLAN
    - 根据部门和组织进行划分
    - 根据数据类型划分（数据，语音，视频）
  - 逻辑网络与物理网络一一对应
    - 仅用于小型网络

逻辑网段划分

- 推荐：
  - 不建议设计跨越整个园区的VLAN，因为配置过于复杂，无法对其它重要工作进行有效处理。
  - 将VLAN限制在单台数据链路层交换机之下，则可以避免产生环路，并降低网络配置的复杂度、提高网络的可管理性。

End-to-end VLAN
Local VLAN

企业园区网的设计流程



第3步设计物理网络

设计物理园区网

- 根据特定的网络互联需求，为园区网络基础设施模块选择：
  - 选择传输介质
  - 选择数据链路层协议
  - 选择物理网络分段策略
  - 选择生成树策略。

传输介质

	Copper Twisted-Pair	Multimode Fiber	Single-Mode Fiber	Wireless
Bandwidth	Up to 10 Gbps	Up to 10 Gbps	Up to 10 Gbps or higher	Up to 300 Mbps
Distance	Up to 100 m	Up to 2 km (FE) Up to 550 m (GE) Up to 300 m (10GE)	Up to 80 km (FE) Up to 100 km(GE) Up to 80 km (10GE) Up to 10 km (100GE)	Up to 500 m at 1Mbps
Price	Inexpensive	Moderate	Moderate to Expensive	Moderate

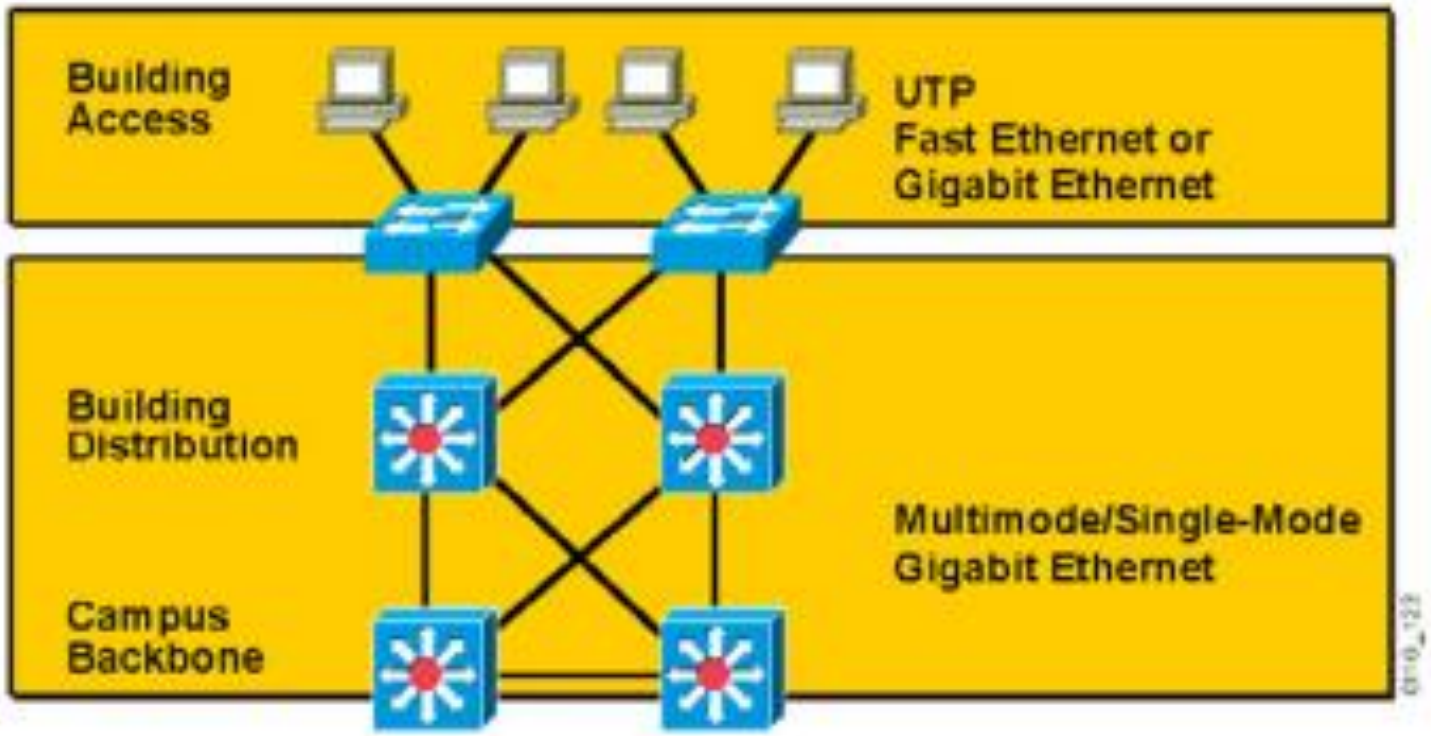
数据链路层

	速度	价格	适用
以太网	10Mbps	很低	大厦接入层
快速以太网	100Mbps	低	大厦接入层 大厦分布层
千兆以太网	1000Mbps	中等	大厦分布层 园区主干

现实条件的制约

- 现实条件影响网络拓扑设计
  - 网络节点的位置，节点间的距离。
    - **楼宇内部**：包含楼宇接入层和汇聚层，一般使用双绞线、光纤、无线连接
    - **楼宇之间**：距离在两公里之内，包含楼宇汇聚层和园区核心层，一般使用光纤
    - **远端建筑**： 间距超过两公里，可使用企业自有光纤或广域网连接，也可使用服务商提供的连接线路进行连接
  - 连接介质的成本。（预算，现有介质）
  - 信号衰减、EMI等技术因素也需考虑。

Transmission Media and Data Link Protocol Selection Example



物理网络分段策略

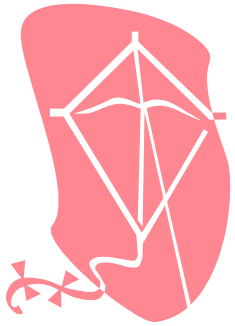
- 网络分段策略：
  - 广播域：Broadcast domain，可以利用多层交换技术来限制广播域的范围。
  - 故障域：Failure domain，由一组数据链路层交换机互联网络称为第2层交换域，即故障域。
  - 策略域：Policy domain，可以将一组具有相同策略（QoS、安全策略、DHCP网络服务等）的用户或服务器定义到同一个IP子网。

常见生成树协议

- 常见生成树协议
  - Spanning Tree Protocol (STP，802.1D)
  - Per-VLAN Spanning Tree Plus (PVST+)
  - Rapid Spanning Tree Protocol (RSTP，802.1w)
  - Multiple Spanning Tree (MST，802.1s)

协议	标准	占用资源	收敛速度	实例
STP	802.1D	低	慢	所有VLAN
PVST+	Cisco	高	慢	每VLAN
RSTP	802.1W	中	快	所有VLAN
PVRST+	Cisco	很高	快	每VLAN
MSTP	802.1S	中/高	快	VLAN列表

企业园区网的设计流程



第4步选择网络设备

总体原则

- 使用交换技术（SWITCH），不使用共享技术（HUB）。
  - 交换网络可支持网络基础服务，如：QoS、安全、管理等。
- 多层交换机集成交换和路由功能，在局域网设计时能有效替代路由器。
  - 数据包转发：
    - 2层交换机使用数据链路层地址进行
    - 3层交换机基于网络层地址。
    - 多层交换机还可基于高层协议

网络设备特性和考虑

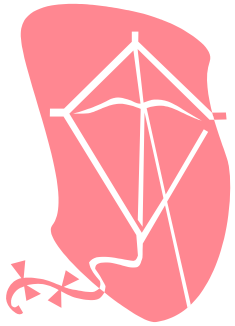
- 设备选择时应注意以下问题:
  - 基础服务能力
  - 网段的大小
  - 收敛时间
  - 费用

设备选择

- 1. 园区规模如何？ 小型/中型/大型园区
- 2. 端口（不包括上行链路端口）的传输速率？ 10M/100M/1000Mbps（铜线）/ GBIC接口
- 3. 交换机需要提供多少端口？ 1-24或以上
- 4. 上行链路的传输介质？ 铜线/光纤
- 5. 上行链路带宽是多少？ 100M/1000/10Gbps
- 6. 需要多少条上行链路？ 1条、2条或更多条
- 7. 是否需要配置冗余电源？
- 8. 交换机是否需要冗余交换引擎？
- 9. 交换机是否需要IP路由或多层交换功能？

设备选择（续）

- 10. 交换机是否需要IDS（Intrusion Detection System，入侵检测系统）、SLB（Server Load Balancing，服务器负载均衡）或NAM（Network Analysis Module，网络分析模块）？
- 11. 交换机是否需要为IP电话或无线接入点提供线内电源（Inline Power)?
- 12. 交换机需要运行CatOS还是NativeIOS,或是运行于混合模式下？
- 13. 交换机需要哪种版本的CatOS和/或IOS?
- 14. 需要在交换机中启用、配置并部署哪些智能网络服务？



第5步选择合适的IP编址策略

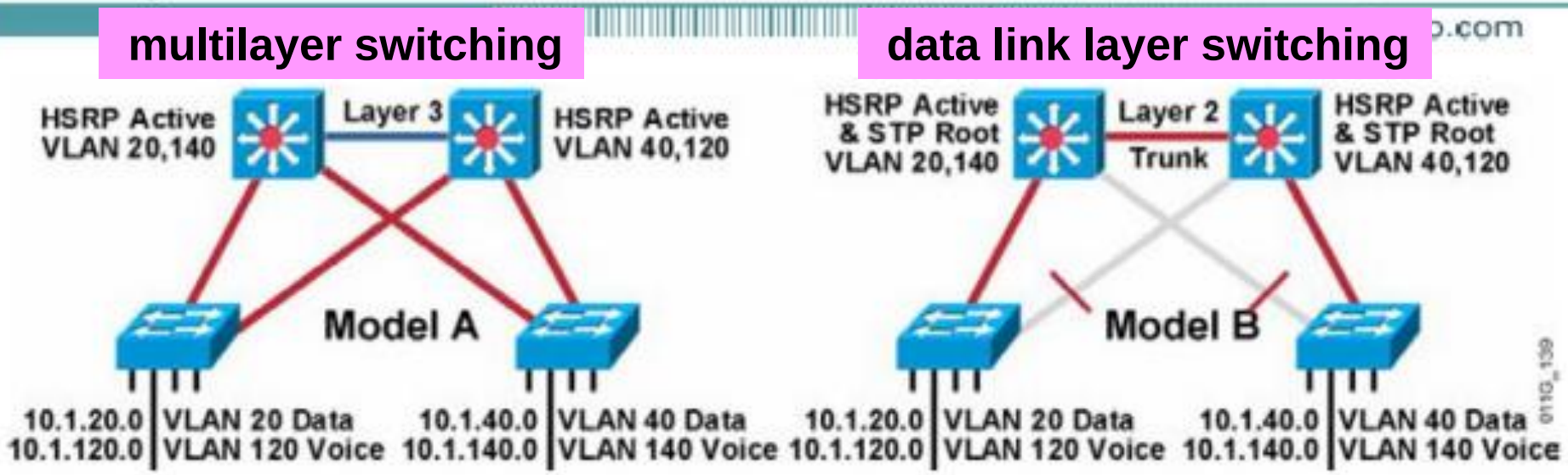
IP编址策略

- 第1步确定网络的规模和所需的IP地址数目。
  - 网络规模有多大?
  - 网络中有多少个网络单元，每个单元的规模如何?
- 第2步确定私有地址和公有地址需求
  - 有多少终端系统只需要访问公网（而无需对外公开）?
  - 有多少终端系统需要对公网公开?
  - 仅使用私有地址? 仅使用公有地址? 均使用?
  - 如何以及在何处实现公有IP地址与私有IP地址的转换?
  - 申请哪类IP地址? 需要的网络地址数又该为多少呢?
- 第3步确定分层IP编址方案实现
  - 需要分层的IP编址方案吗?
  - 将网络划分为多个路由汇总组的原则是什么?

私有地址/公有地址

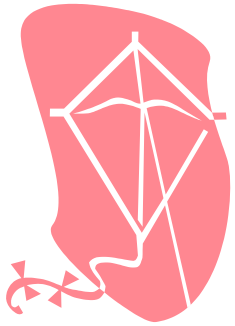
- 私有地址、公有地址选择：
  - 无Internet连接：此时网络属于完全隔离的私网，无需分配公有地址。
  - 有Internet连接，没有公开接入的服务器：由于网络已接到Internet上，因而至少需要分配一个公有IP地址。此时，需要在企业网内部分配私有IP地址。
  - 有Internet连接，有公开接入的服务器：需要为所有提供公开接入的服务器分配公有IP地址，以便将其接入Internet。
  - 所有终端系统都要提供公开接入：此时只能在全网都分配公有IP地址。

Mapping Layer 2 VLANs to Layer 3 Subnets



- Map Layer 2 domains to a Layer 3 subnet with an understandable VLAN to IP subnet numbering scheme.
- For example, data VLAN 20 and Voice VLAN 120 in Building 1 can correspond to 10.1.20.x/24 and 10.1.120.x/24.
- A good addressing scheme helps route summarization and eases troubleshooting.

企业园区网的设计流程



第6步选择路由协议

静态与动态路由协议选择

- 静态路由协议主要用于：
  - 末端网络（stub Network）
  - 预计不会有太大扩展可能的小型网络。
  - 支持DDR（Dial-on-Demand Routing，按需拨号路由）和ODR（On-Demand Routing，按需路由）等特殊功能。
  - 拨号环境下的拨号对等体指定路由。
- 动态路由主要用于：
  - 大型，可扩展网络

Routing Protocol Considerations

Cisco.com

	Summarization	Flat	Multiaccess (LAN)	Point-to-Point	Point-to-Multipoint (Frame Relay)
RIP		X	X	X	
IGRP		X	X	X	
EIGRP		X	X	X	X
OSPF	X		X	X	X
IS-IS	X		X	X	