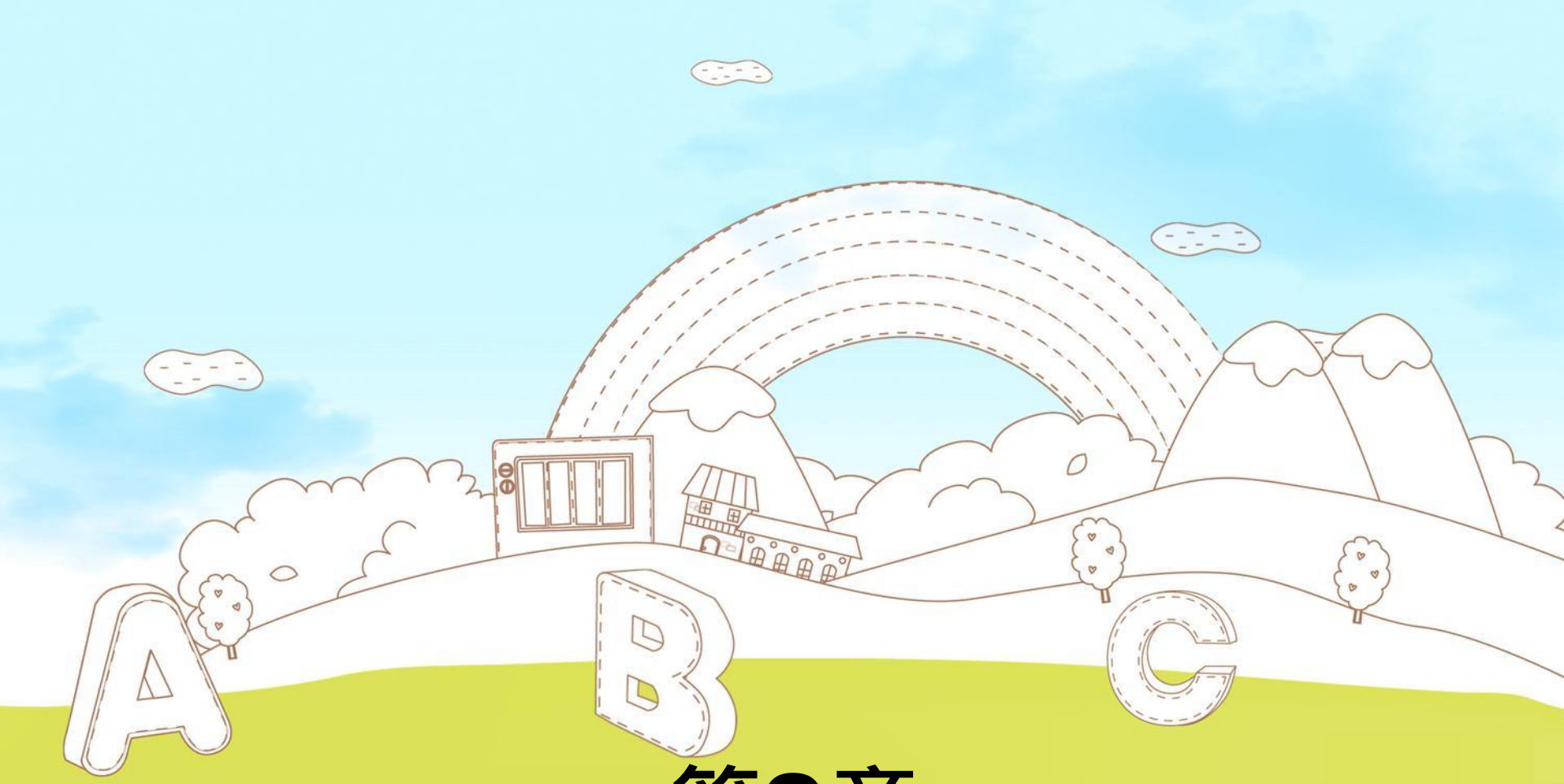
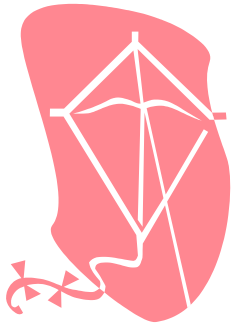


第9章
无边界网络服务

无边界网络服务

- 无边界网络服务关键功能：
  - 移动性 Mobility
  - 安全性 Security
  - 高性能 Performance
  - IP 通讯 IP communication



移动性支持（Mobility）

移动性服务

- **移动性服务**将移动客户连接到企业网络。
- 无线局域网有特殊问题：
  - 存在由覆盖问题，射频传输的多径失真，和其他无线服务/网络的相互干扰引起连接问题。
  - 由射频信号泄漏引起的私密性问题。

思科统一无线网络(UWN)

- **Cisco Unified Wireless Network**

思科统一无线网络构成

⑩有线网络：

无线局域网控制器：
WLAN controller

⑩无线接入点：
Wireless Aps

⑩用户设备：
⑩End-user devices

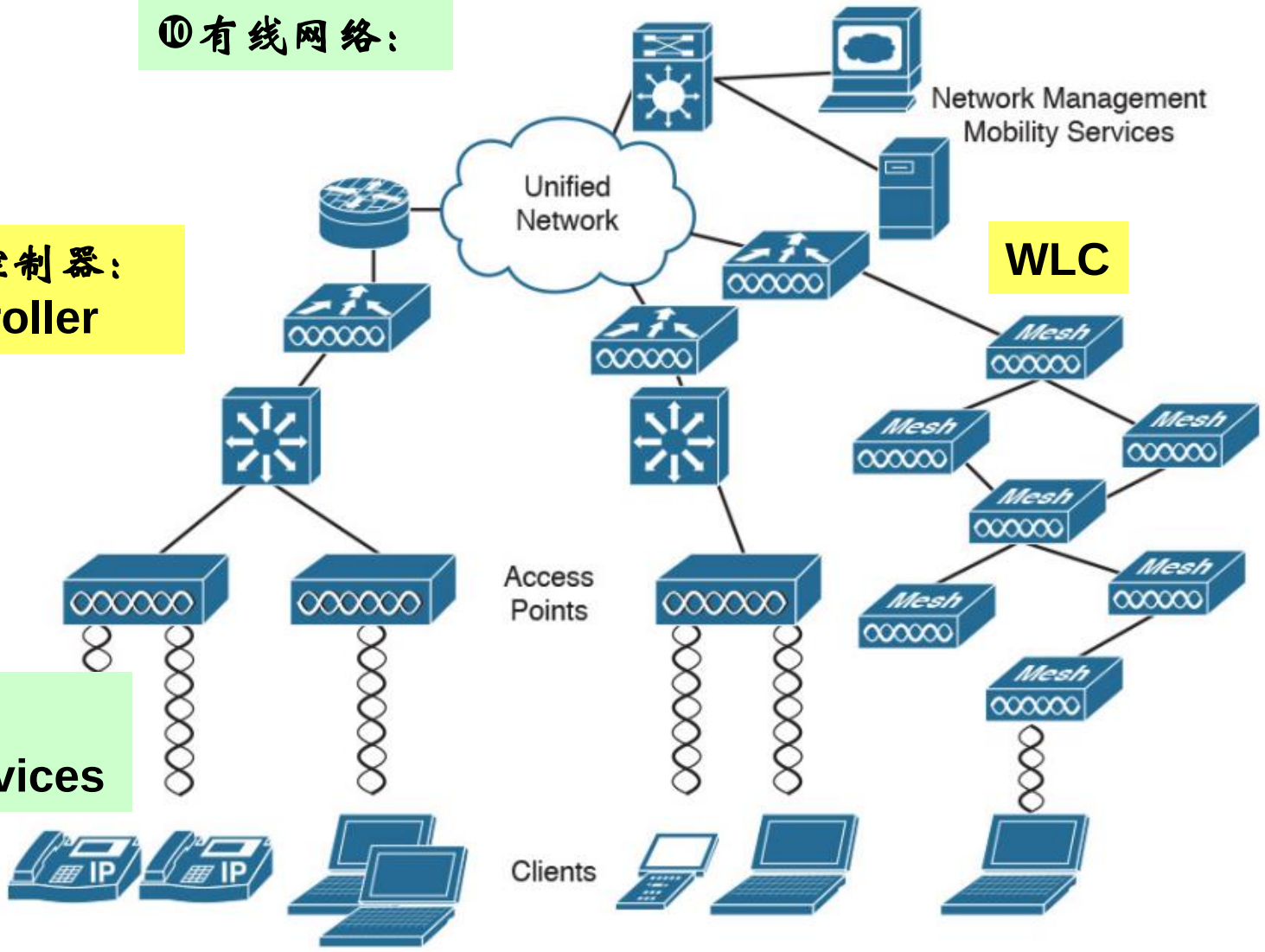


Figure 5-2 *Cisco UWN architecture*

胖AP和瘦AP 的区别

Lightweight	Autonomous
Thin	Thick
LWAPP/CAPWAP	IOS
Controller Based	Standalone
Airespace	Aironet

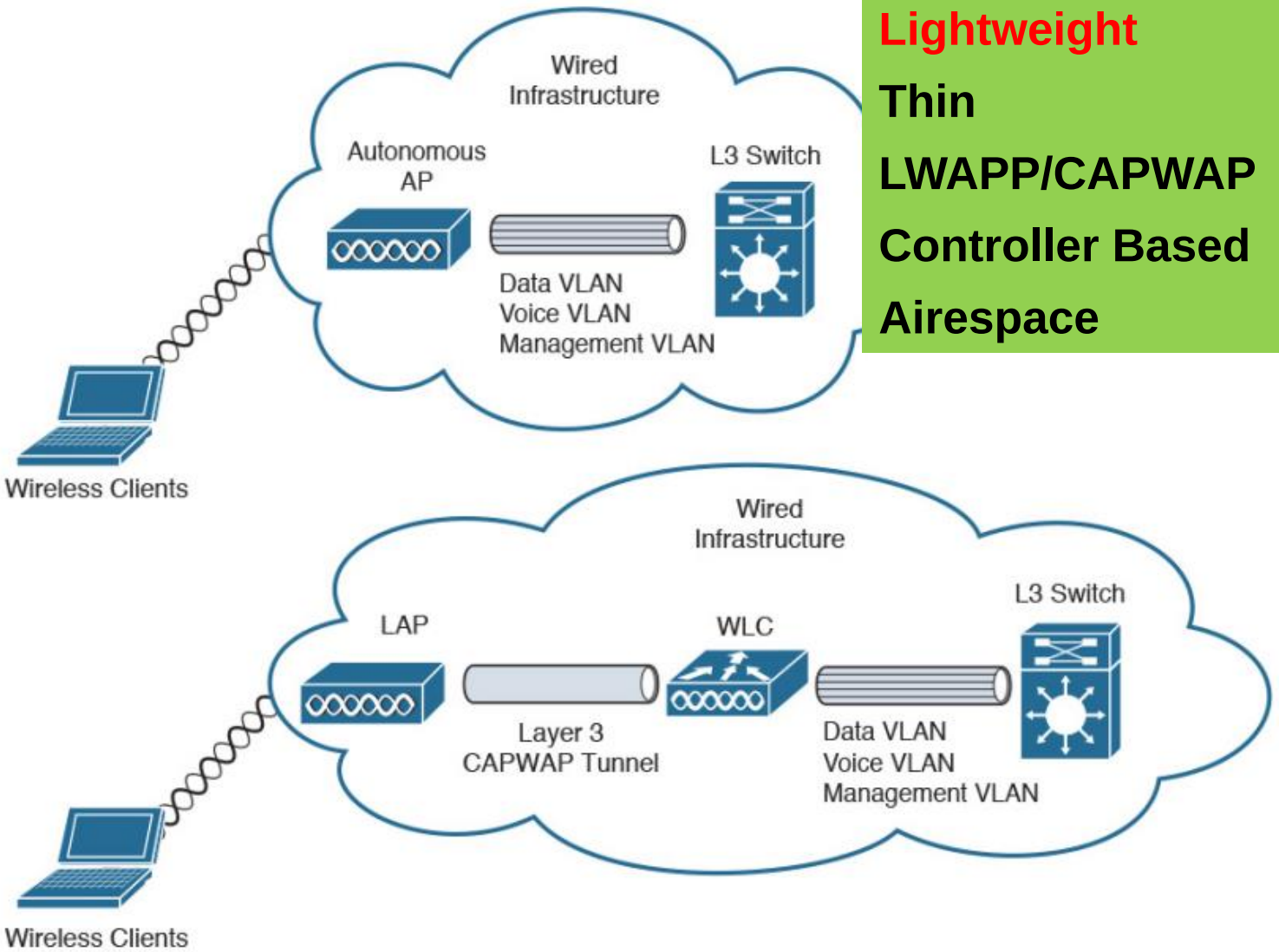


Figure 5-6 *Autonomous AP versus CAPWAP AP with WLC*

集中控制无线局域网

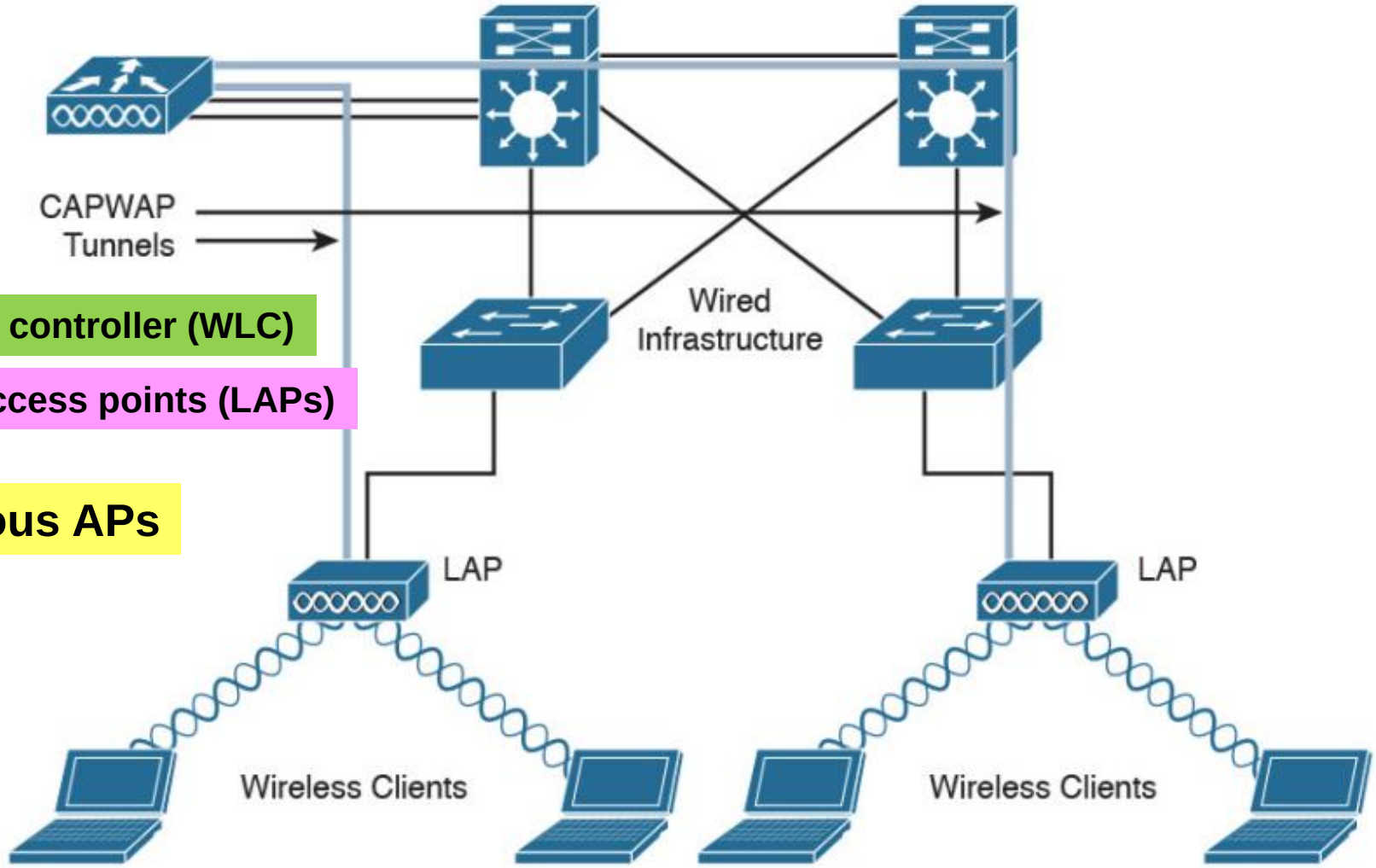


Figure 5-3 *Centralized WLAN architecture using WLC*

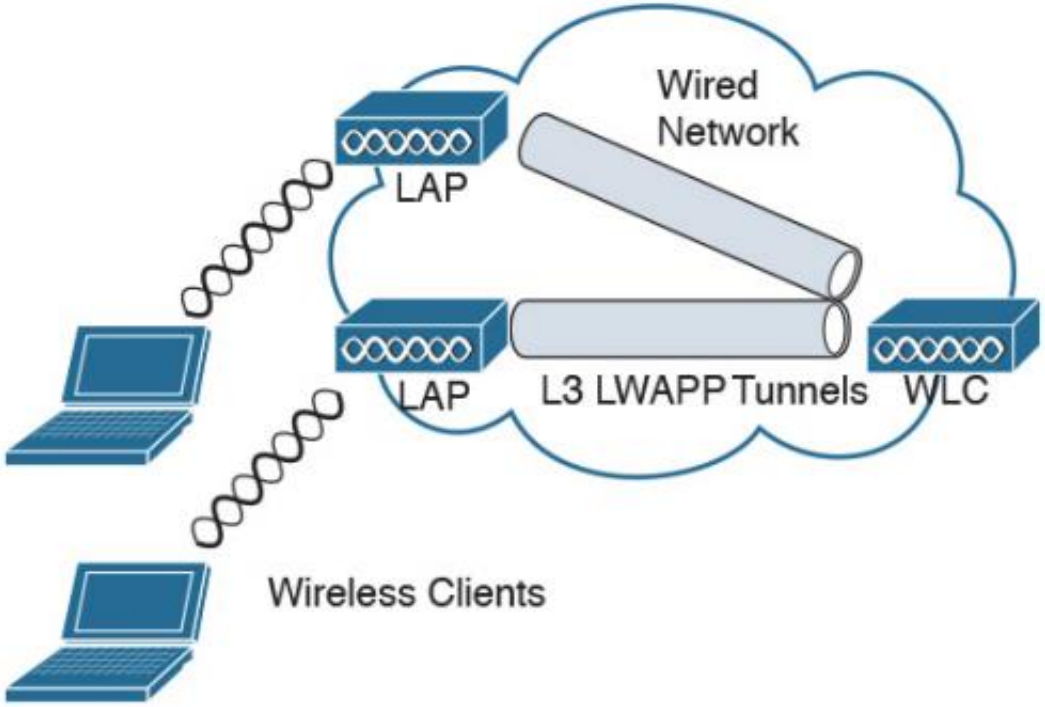
wireless LAN controller (WLC)

lightweight access points (LAPs)

autonomous APs

Control and Provisioning for Wireless Access Point (CAPWAP)

通信协议--（过时）LWAPP



⑩Lightweight Access Point Protocol (LWAPP)

通信协议--CAPWAP

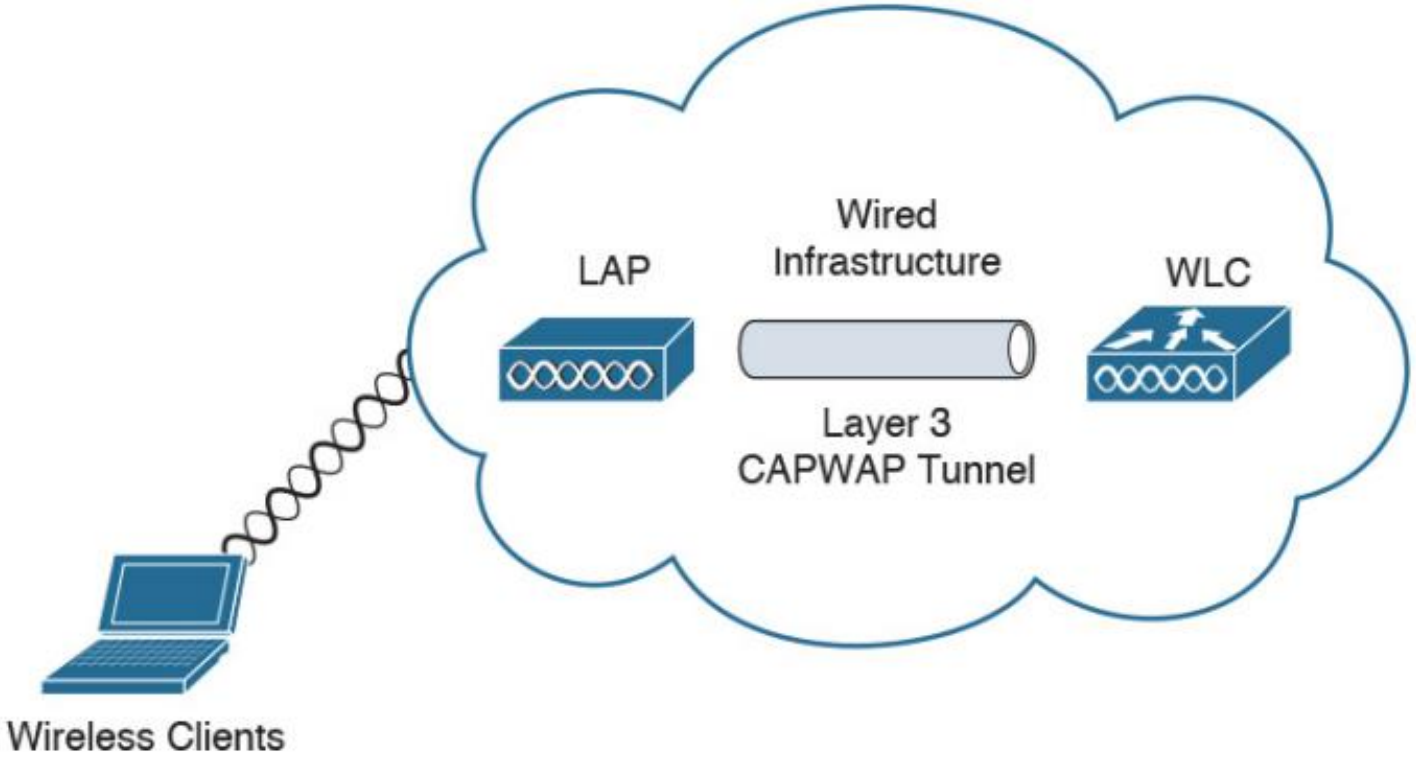


Figure 5-5 *CAPWAP tunnel*

Control and Provisioning for Wireless Access Point (CAPWAP)

安全认证

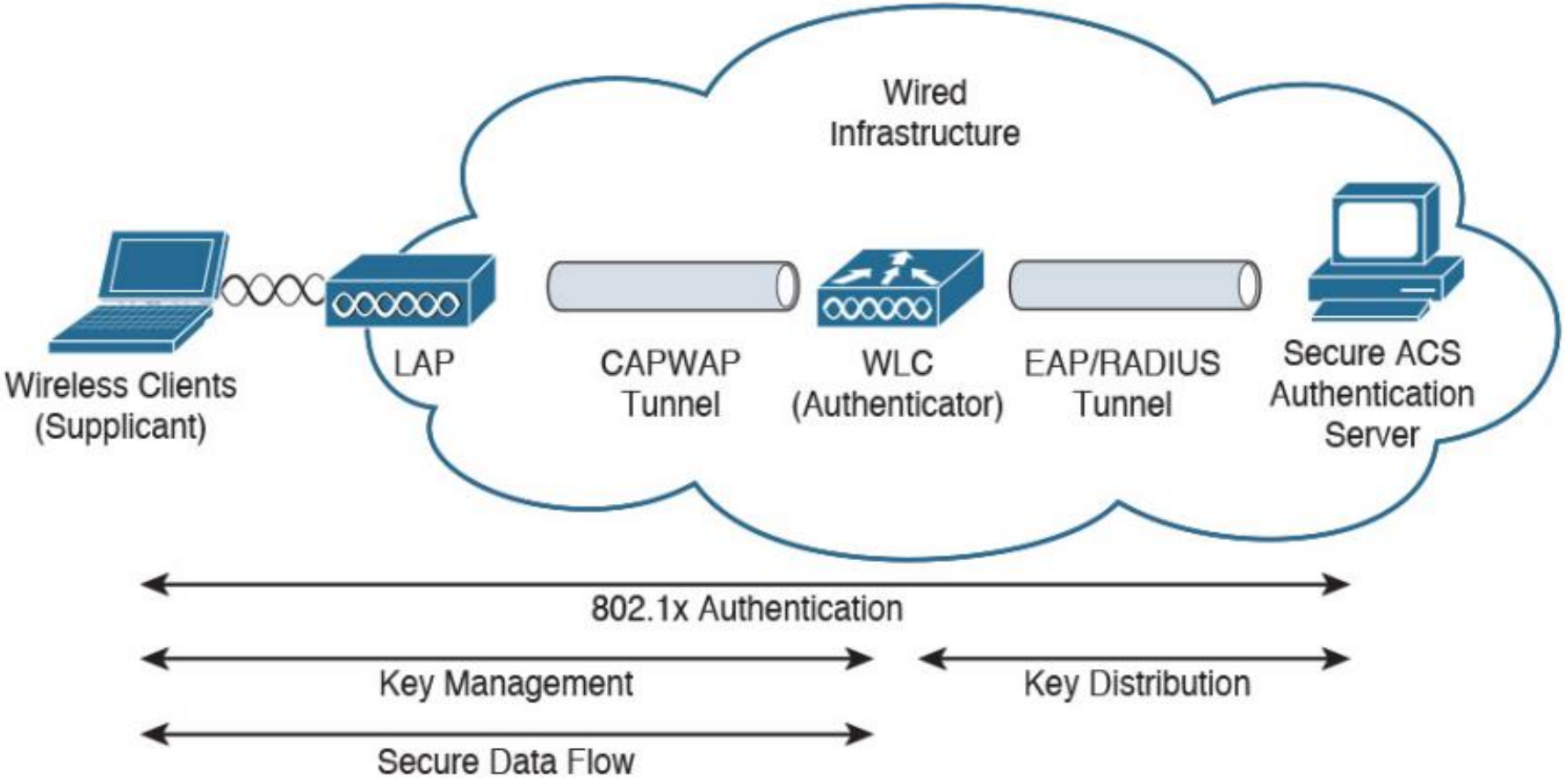


Figure 5-7 *WLAN authentication*

移动性支持

漫游

Roaming

同个WLC，不同LAP

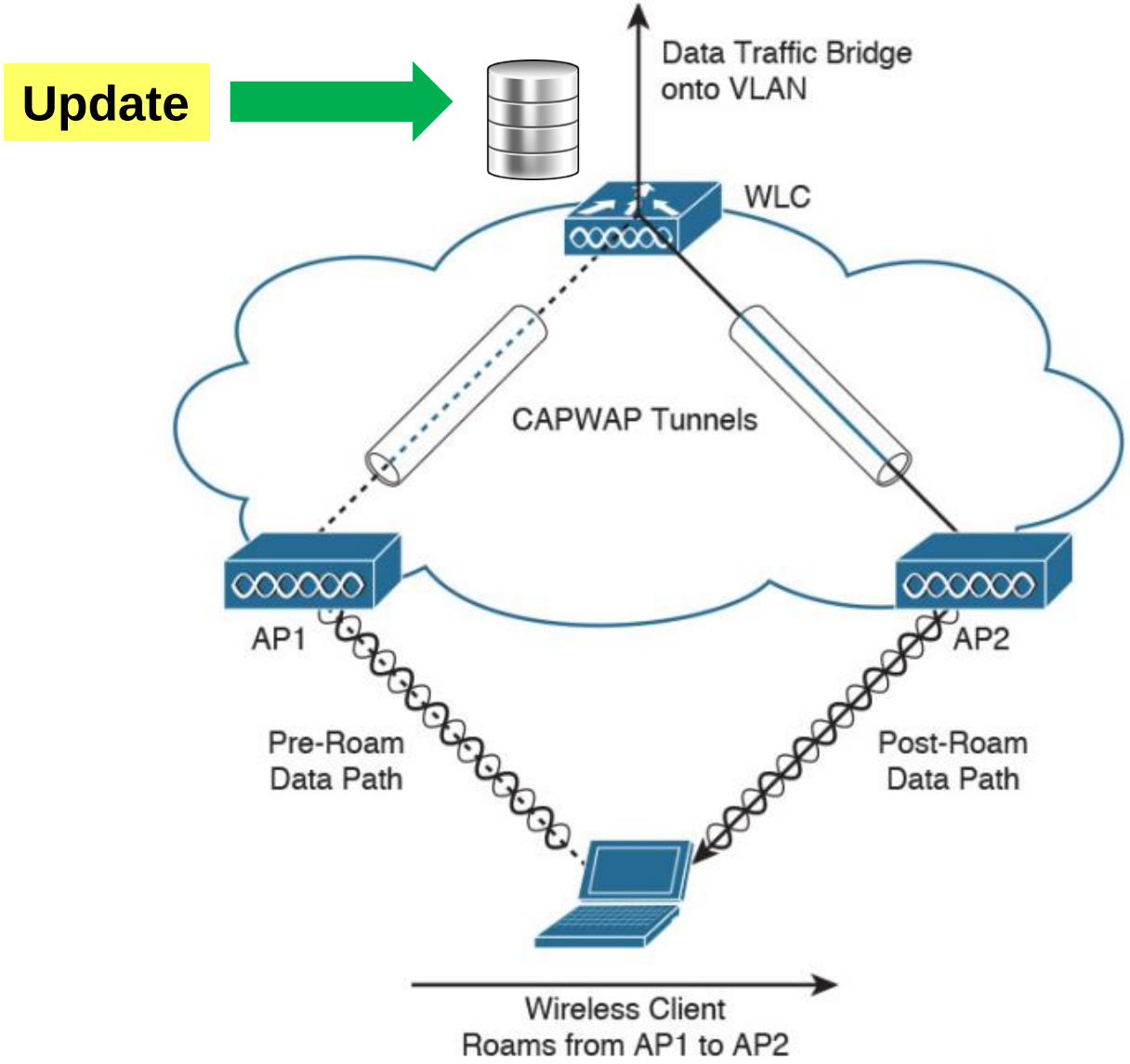


Figure 5-10 *Intracontroller roaming*

同个子网，不同WLC

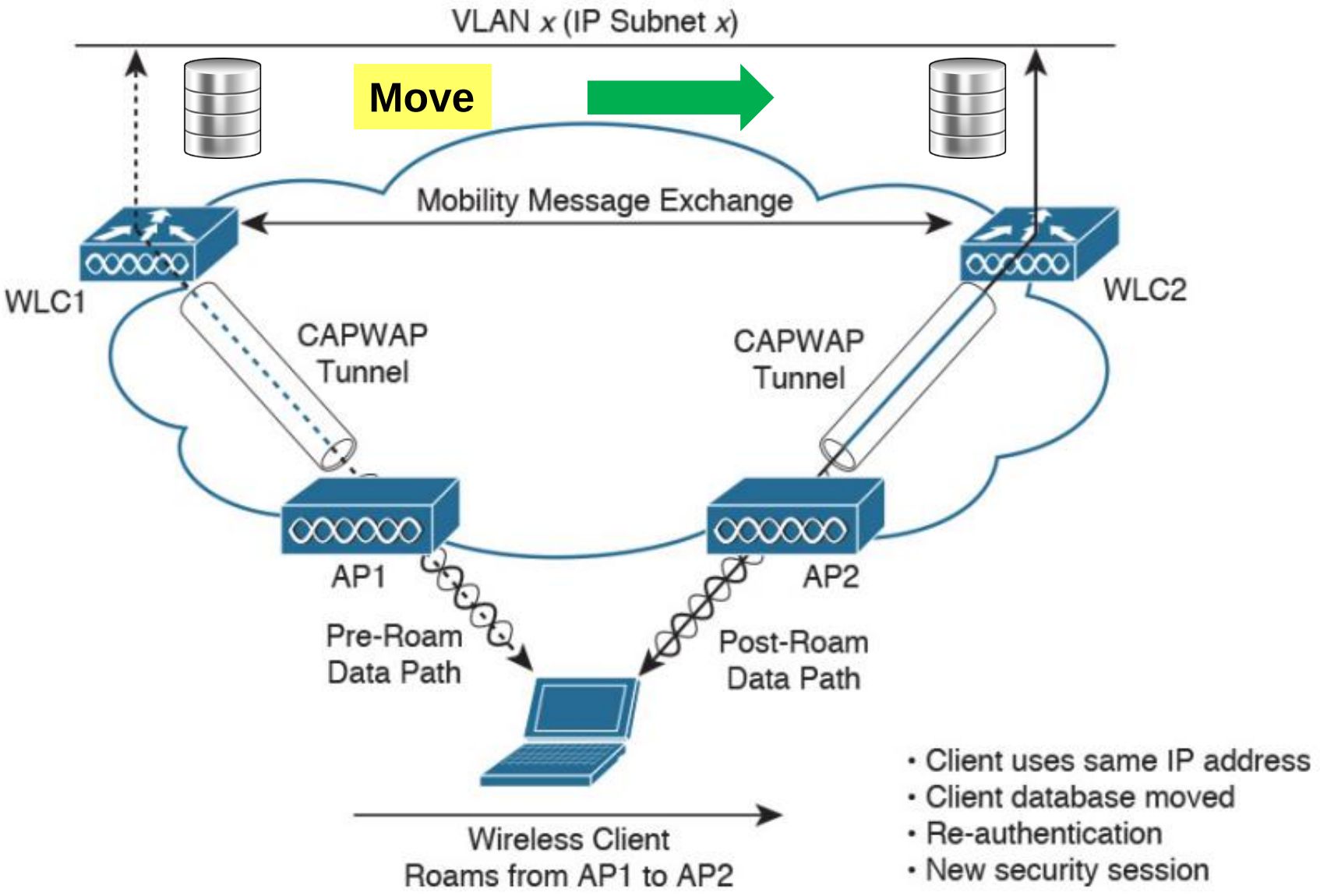


Figure 5-11 *Layer 2 intercontroller roaming*

不同子网，不同WLC

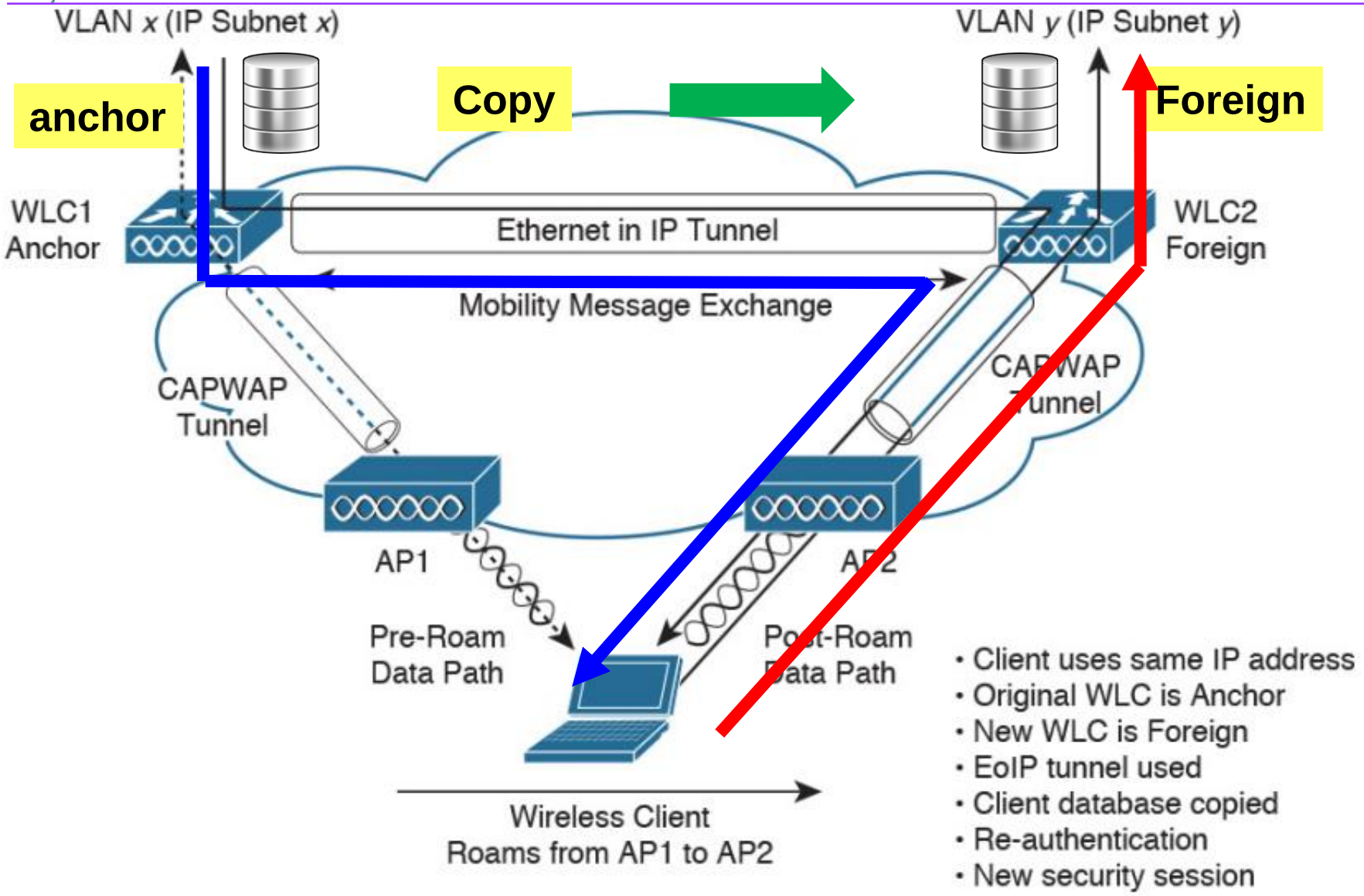


Figure 5-12 *Layer 3 intercontroller roaming*

WLC 冗余设计
Controller Redundancy Design

WLC冗余方案

- WLC冗余方案
  - 动态冗余
    - 使用CAPWAP实现
  - 确定性冗余
    - 在AP上配置：主、次、第三个WLC

N+1

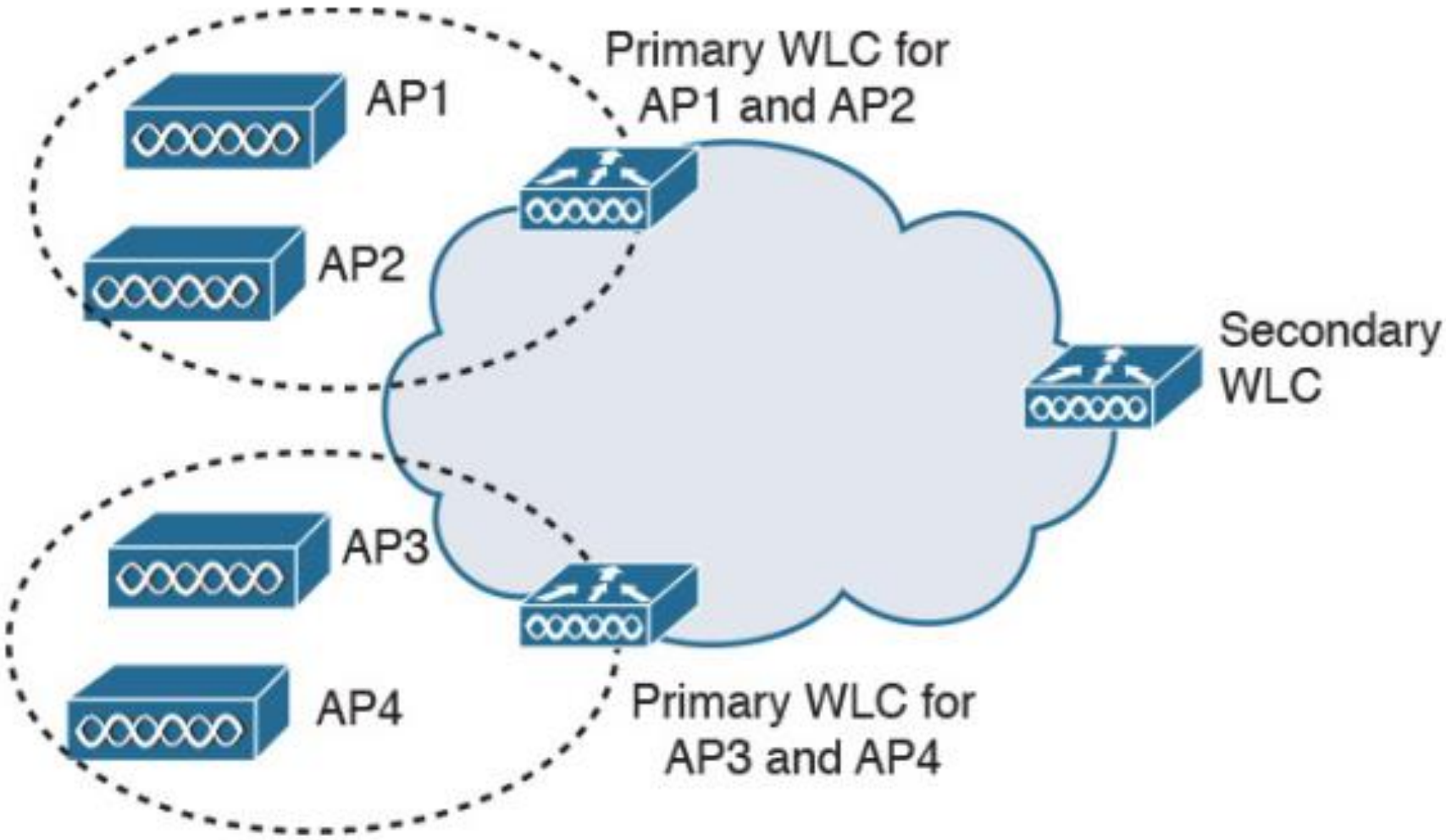


Figure 5-13 *N+1 controller redundancy*

N+N

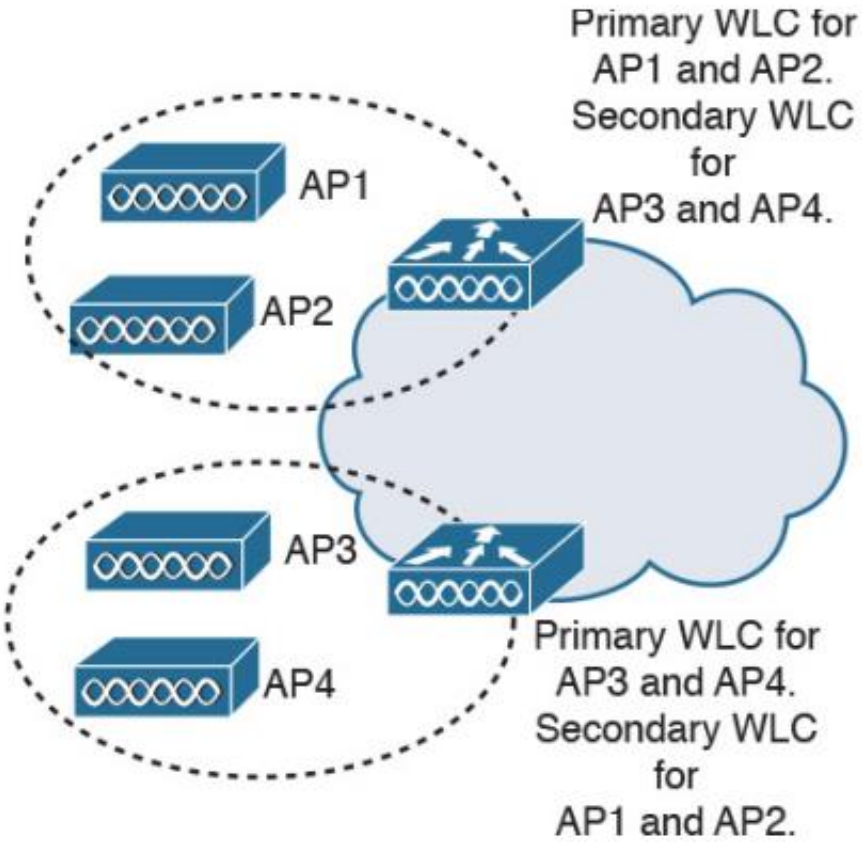


Figure 5-14 *N+N controller redundancy*

N+N+1

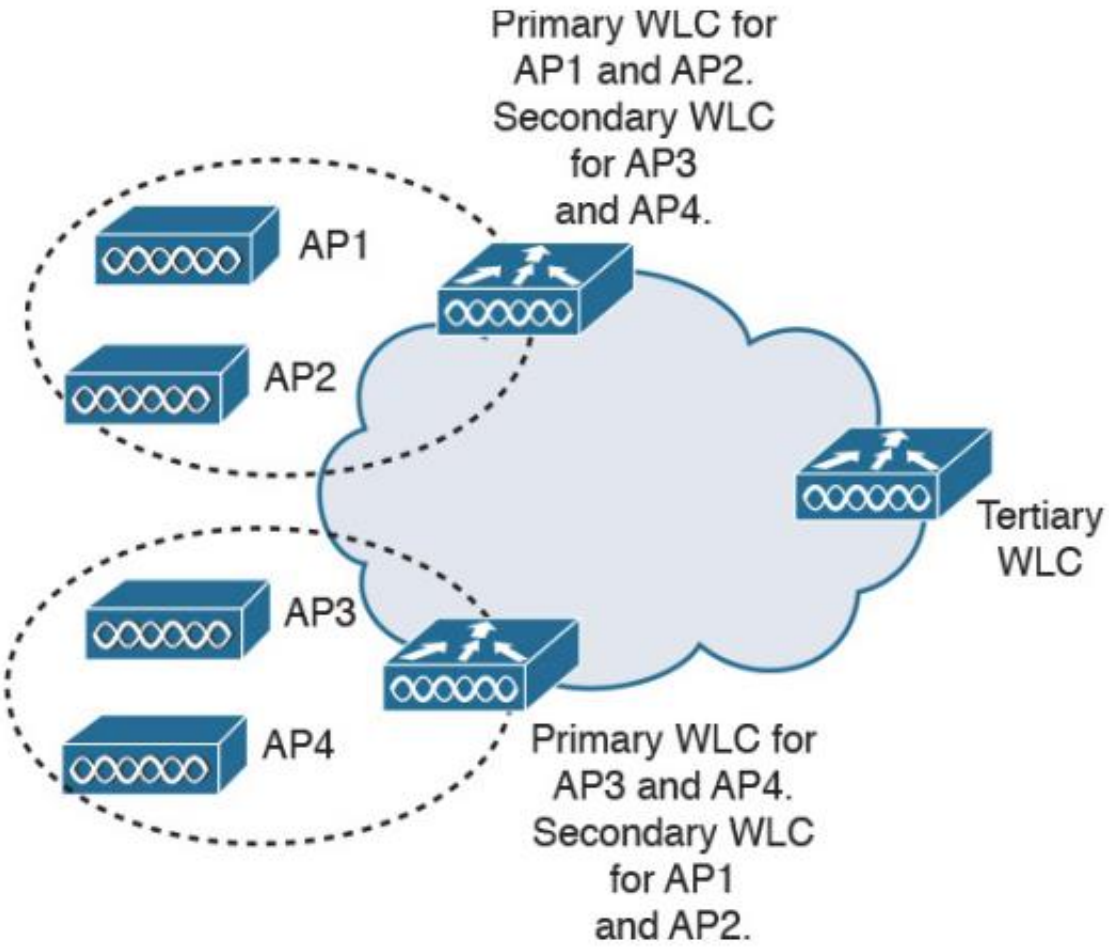


Figure 5-15 *N+N+1 controller redundancy*

总结

Table 5-10 summarizes WLC redundancy.

WLC Redundancy	Description
N+1	A single WLC acts as the backup for multiple WLCs. The backup WLC is configured as the secondary on APs.
N+N	An equal number of controllers back up each other.
N+N+1	An equal number of controllers back up each other. The backup WLC is configured as the tertiary on APs.

Table 5-10 WLC Redundancy

访客服务
Guest Services

访客服务

- 方法1：
  - 可使用分离的VLAN为访客和用户服务。
  - 访客用的AP，广播SSID。
  - 用户用的AP，不广播SSID，并设置密码
- 方法2：
  - 使用Ethernet over IP (EoIP) 构建隧道，将流量导入到 anchor WLC。

访客服务

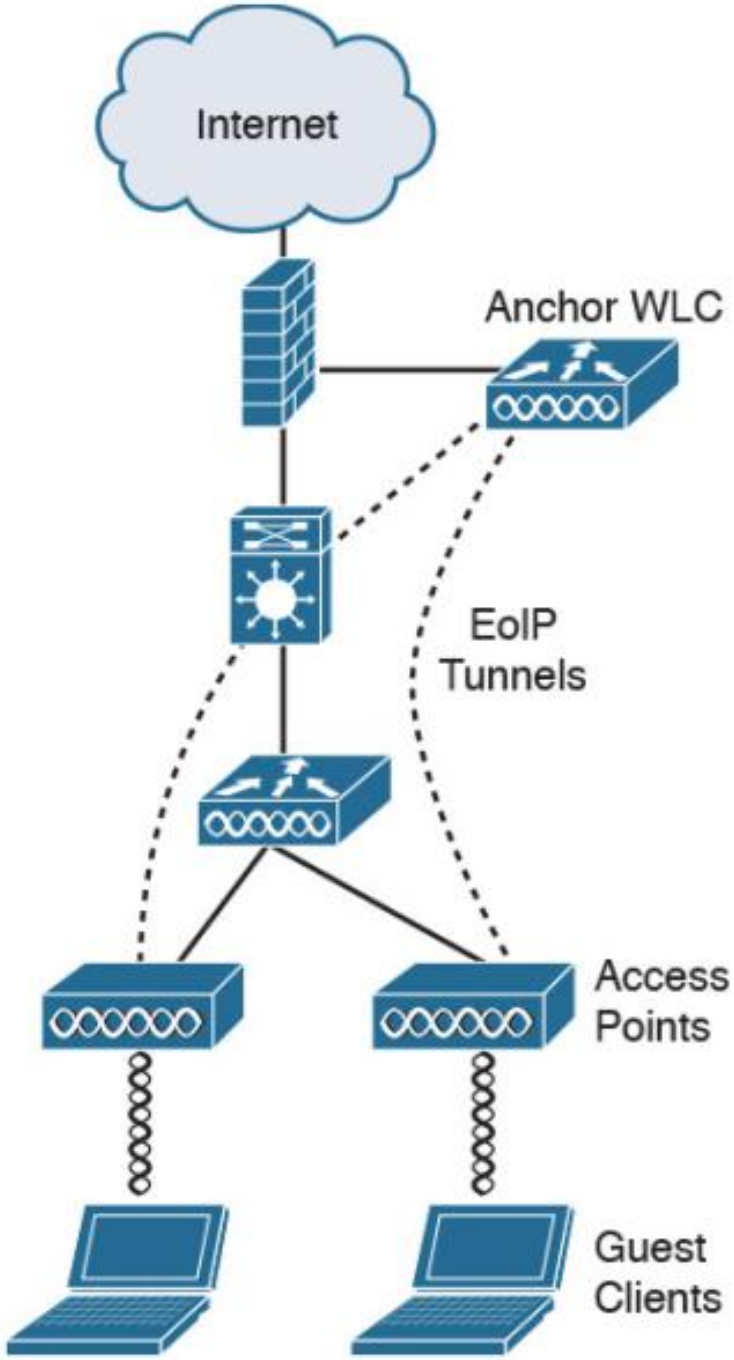


Figure 5-17 *EoIP tunnels*

WLAN 设计考虑

Design Item	Description
Number of APs	The design should have enough APs to provide full RF coverage for wireless clients for all the expected locations in the enterprise. Cisco recommends 20 data devices per AP and seven G.711 concurrent or eight G.729 concurrent VoWLAN calls.
Placement of APs	APs are placed in a centralized location of the expected area for which they are to provide access. APs are placed in conference rooms to accommodate peak requirements.
Power for APs	Traditional wall power can be used, but the preferred solution is to use Power over Ethernet (PoE) to power APs and provide wired access. Monitor the power budget of the LAN switch.
Number of WLCs	The number of WLCs depends on the selected redundancy model based on the client's requirements. The number of controllers is also dependent on the number of required APs and the number of APs supported by the differing WLC models.
Placement of WLCs	WLCs are placed in secured wiring closets or in the data center. Deterministic redundancy is recommended, and intercontroller roaming should be minimized. WLCs can be placed in a central location or distributed in the campus distribution layer. WLCs can also be placed in the cloud, where only management traffic is routed to the cloud (user traffic remains on the local network).*

无线网状网络

Wireless Mesh

Wireless Mesh Component	Description
Wireless Control System (WCS)	The wireless mesh SNMP management system allows networkwide configuration and management.
WLAN controller (WLC)	Links the mesh APs to the wired network and performs all the tasks previously described for a WLC, such as managing multiple APs, mitigating radio interference, managing security, and providing Layer 3 mobility.
Rooftop AP (RAP)	Connects the mesh to the wired network and serves as the root. It also communicates with the MAPs. RAPs are typically located on rooftops or towers.
Mesh access point (MAP)	Remote APs that provide access to wireless clients. They communicate with the RAP to connect to the wired network. MAPs are typically located on top of a pole, such as a lamp post.

Table 5-11 Wireless Mesh Components

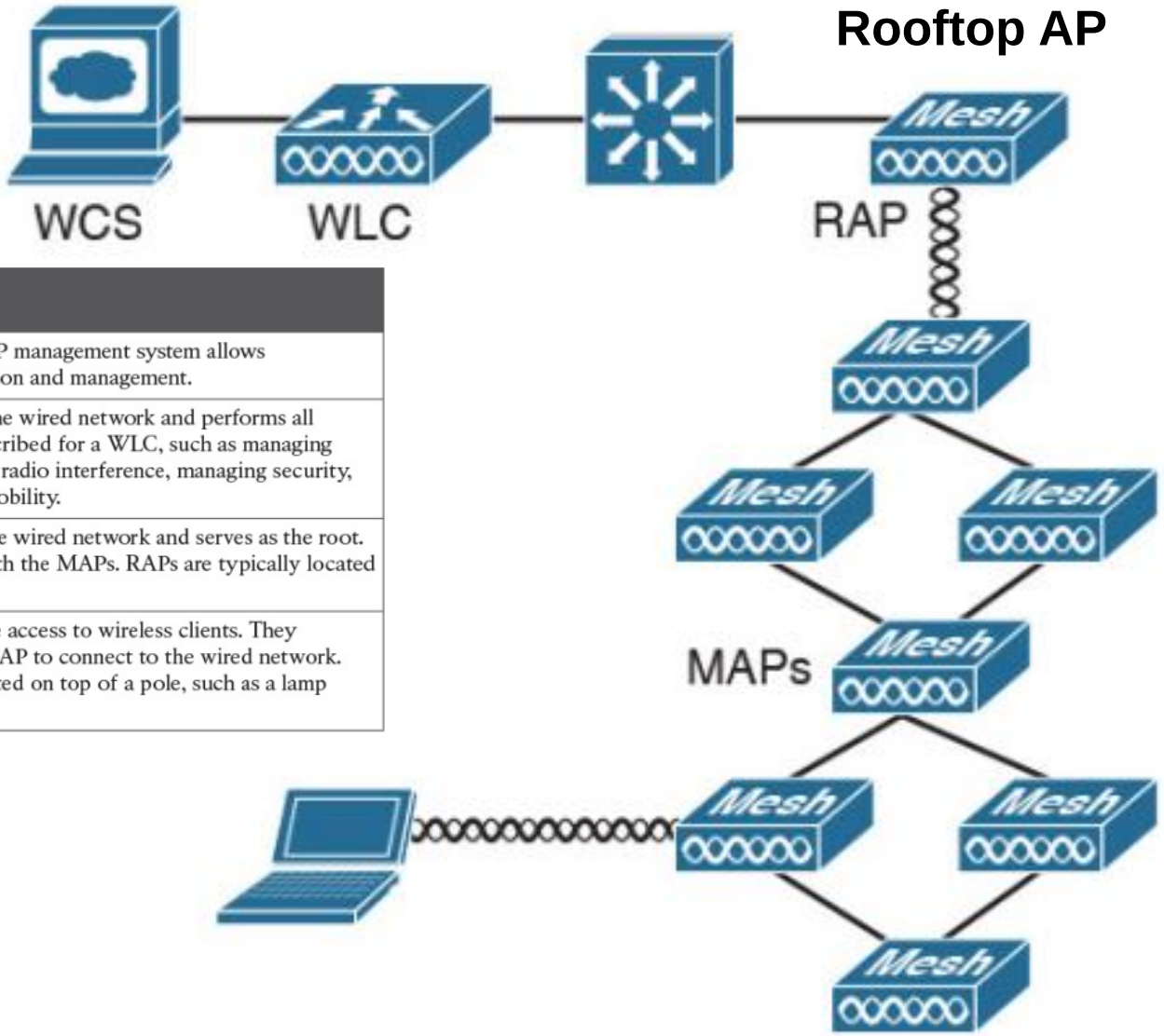
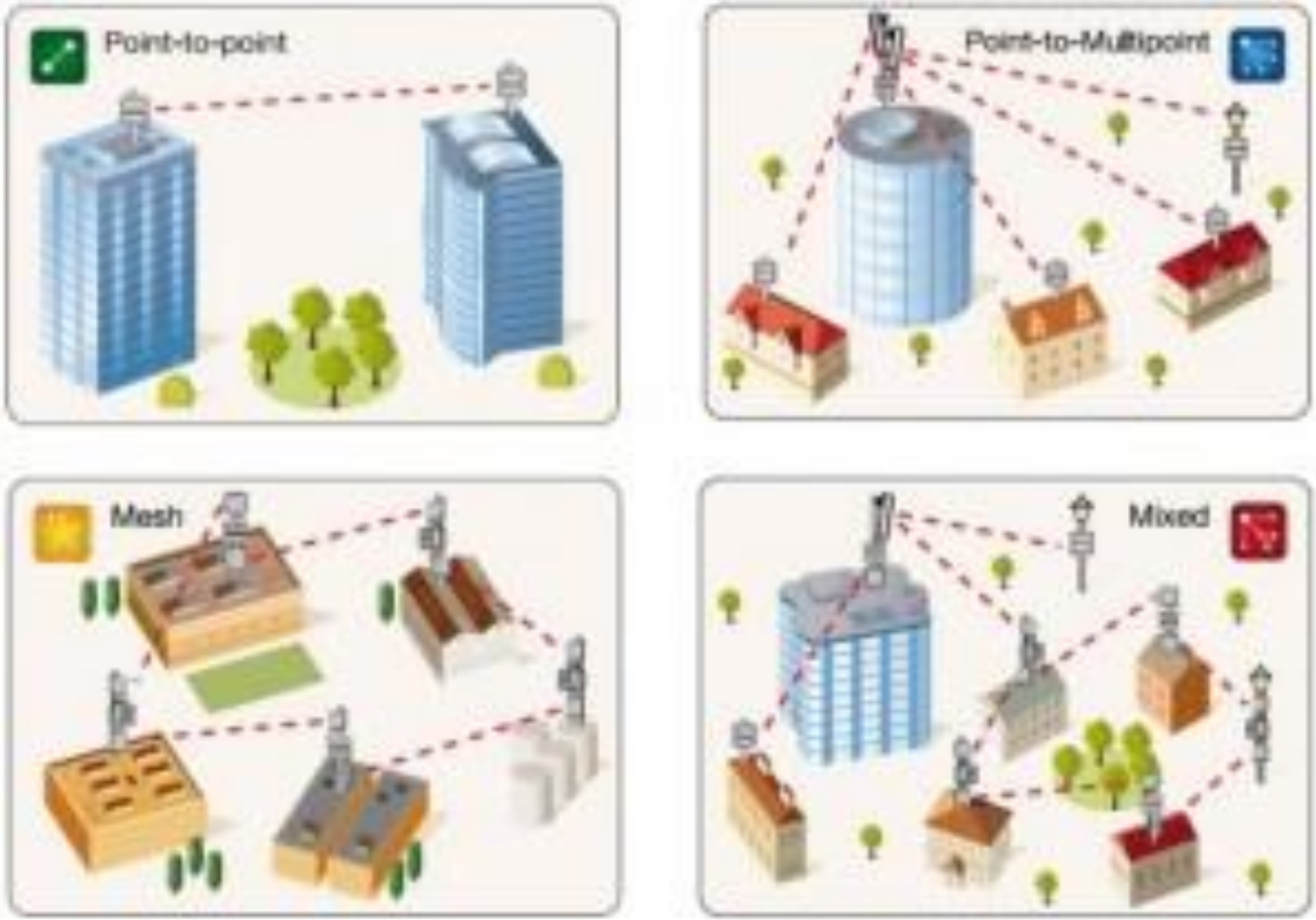
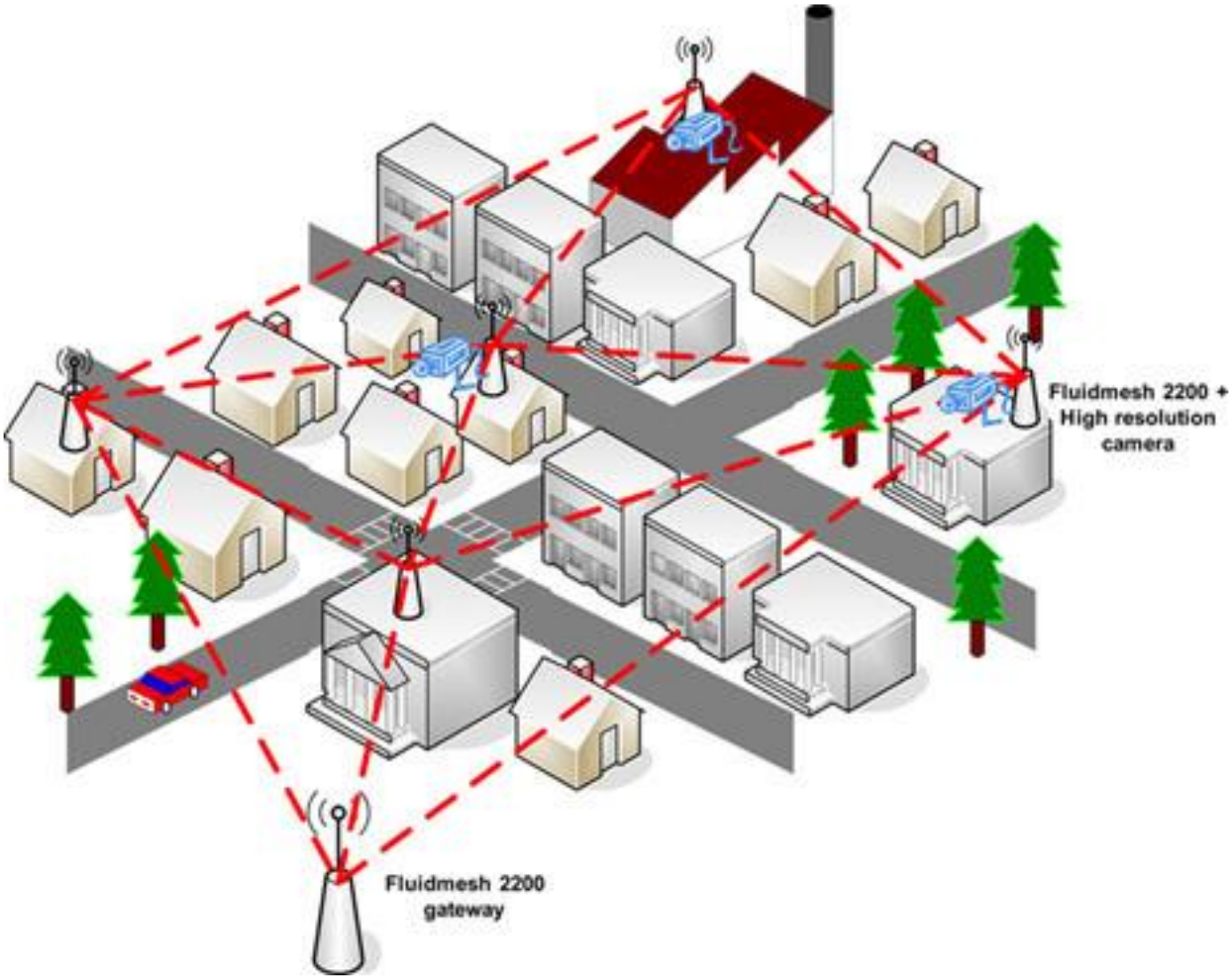


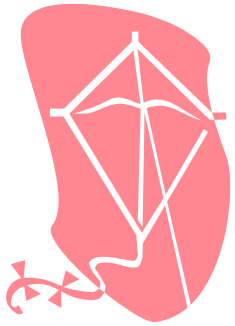
Figure 5-18 *Wireless mesh components*

演变



实例


Fluidmesh 2200 +
High resolution
camera
Fluidmesh 2200
gateway



安全性支持（Security）

安全性支持

- **安全服务**通过保护资源和用户免受内部和外部的威胁，从而提高网络的完整性。
- 关键在于
  - 要对所涉及的威胁有一个完整的了解。
  - 否则会出现
    - 网络安全部署配置不正确，
    - 过于集中在安全设备，
    - 或缺乏适当的威胁响应机制等问题。

Threat Description	Threat Category
Gathering information about a host/network segment	Reconnaissance
Attacks aimed at overwhelming resources such as memory, CPU, and bandwidth of an attacked system and the use of adware/malware/spyware	Service Disruption
Act of attacking or exploiting the target host system	Unauthorized access
Attackers using packet sniffing tools and conducting man-in-the-middle attacks	Disclosure and modification of data
Peer-to-peer file sharing, out-of-policy network browsing, and the spamming of instant messaging systems	Network Abuse
Loss of data from servers or user workstations	Data Leaks
Phishing with SPAM to gather personal information	Identity Theft and Fraud

SAFE 解决方案

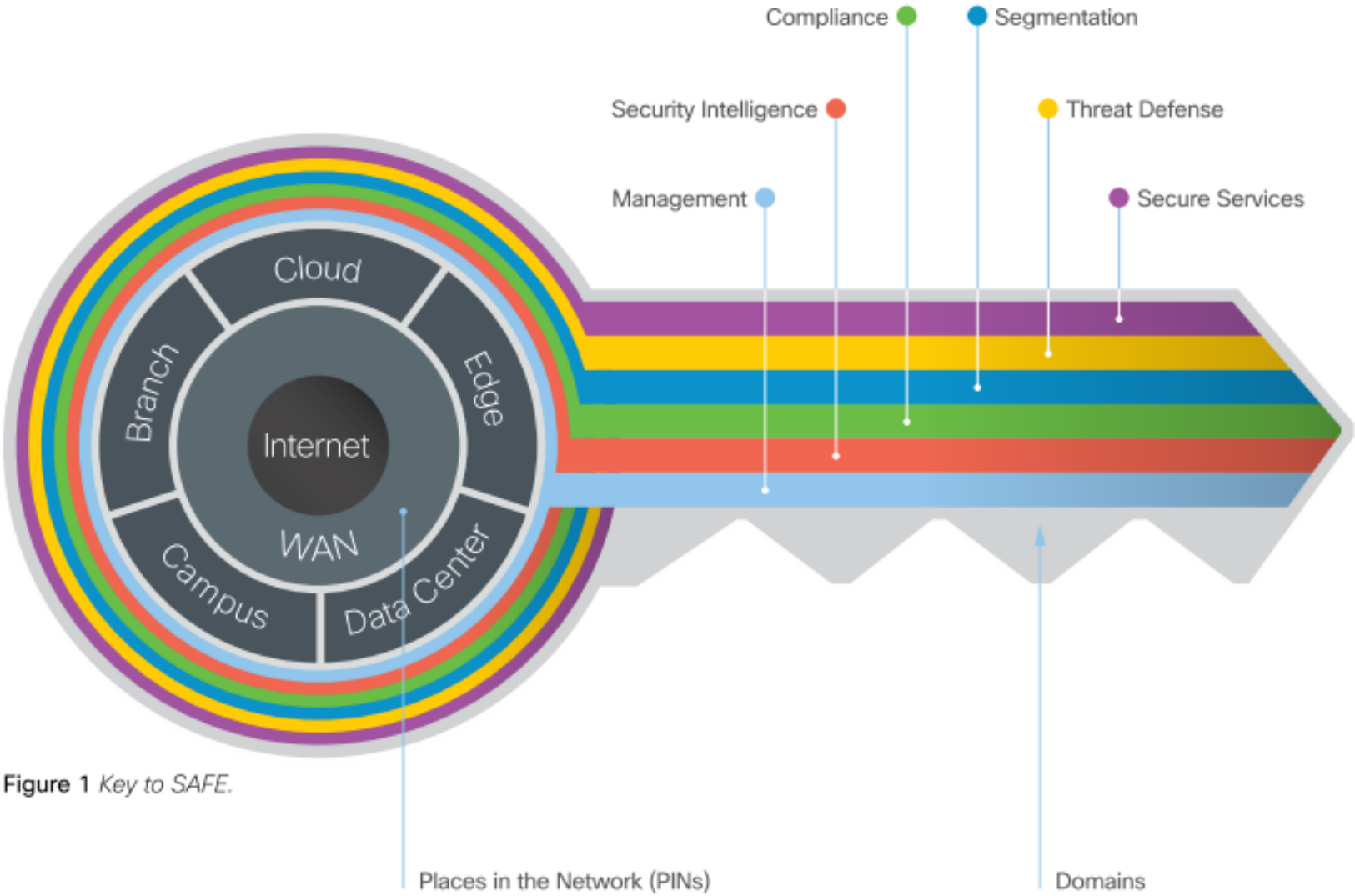


Figure 1 *Key to SAFE.*

Cisco Security Architecture for the Enterprise (SAFE)

常用设备和技术

- Secure network access
- VPN technologies
- Firewalls/IPS
- Infrastructure protection
- Content and application security
- Network and security management

应对内部威胁

IPS（Intrusion Prevention System，入侵防御系统）

IDS (Intrusion Detection System，入侵检测系统）

one-time password (OTP)

使用端口安全控制接入

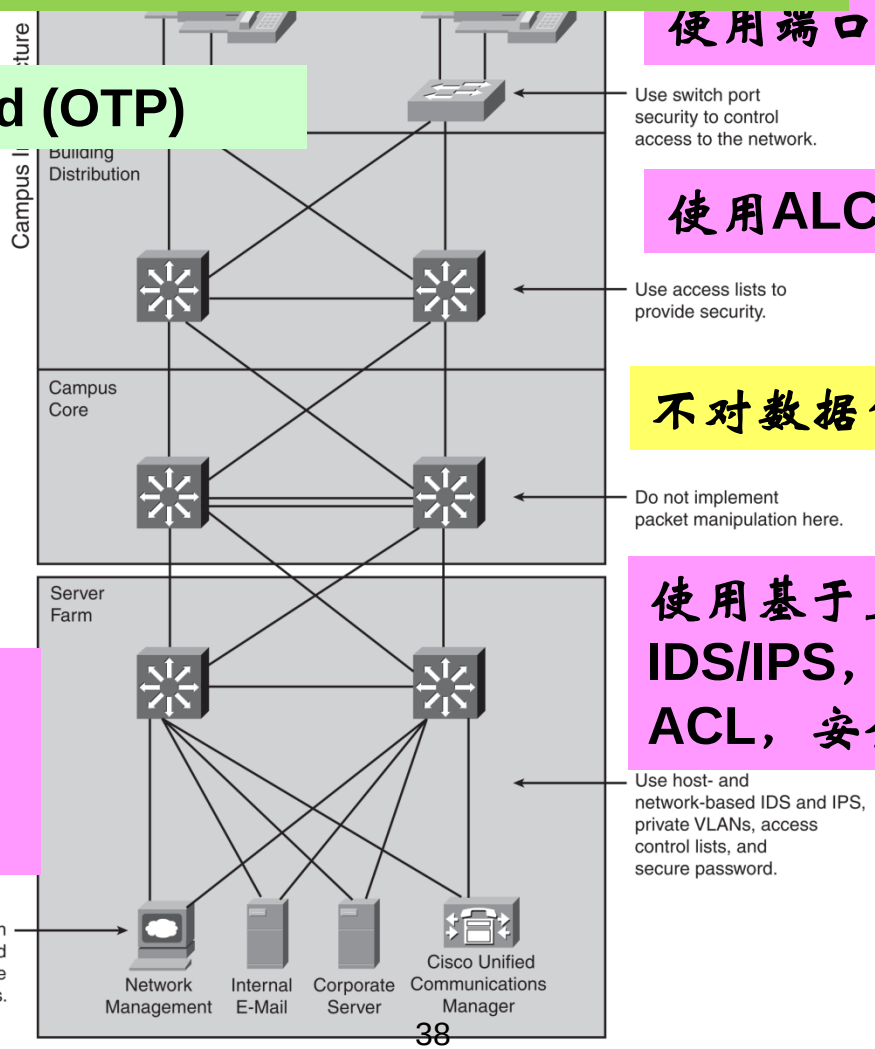
使用ALC提供安全服务

不对数据包进行专门控制

使用基于主机和基于网络的IDS/IPS，私有 VLAN，ACL，安全密码。

使用认证服务器，OTPs, IPS,

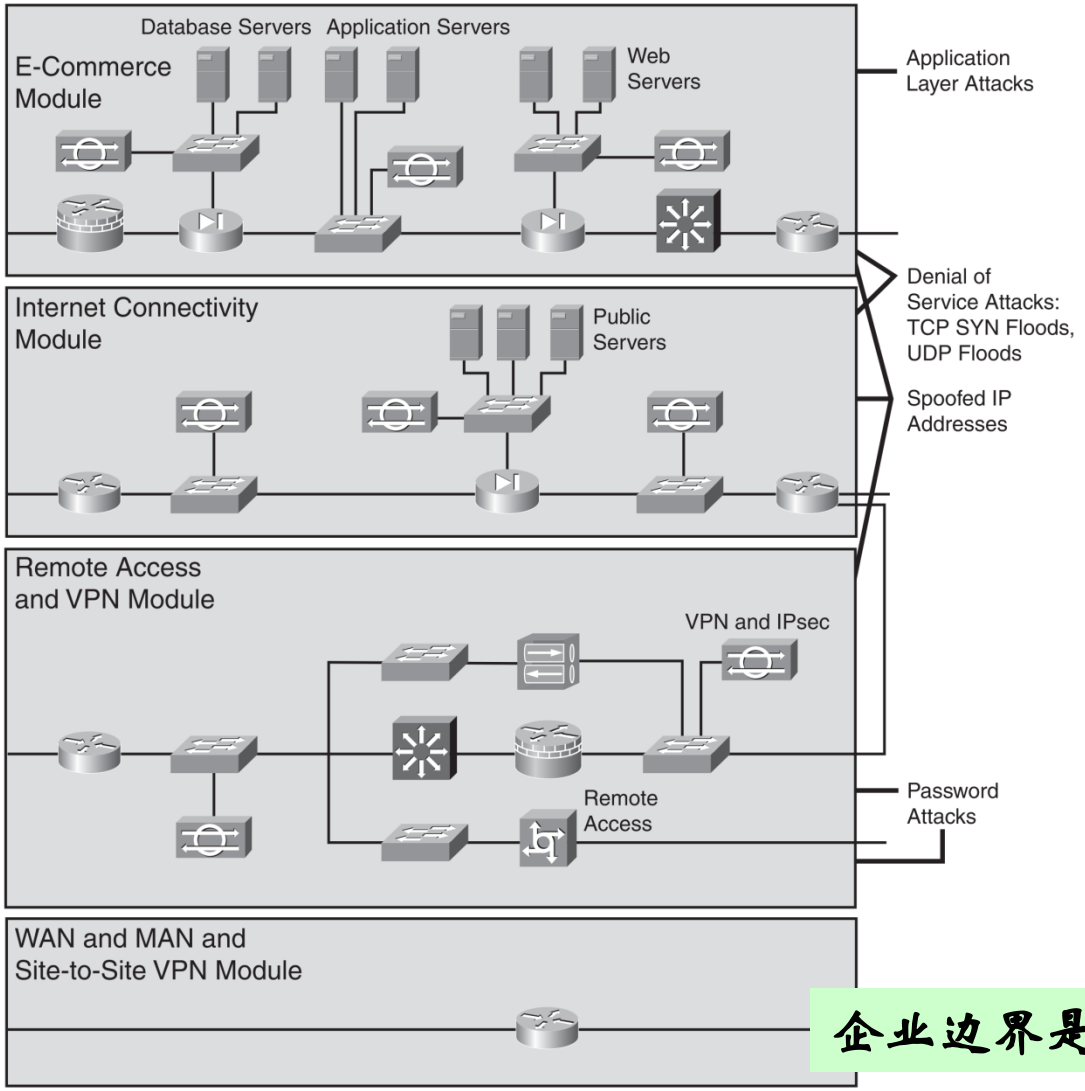
日志来减轻安全威胁.



07:44

应对外部威胁

Figure 3-16 *External Threats*



应用层攻击

拒绝服务攻击

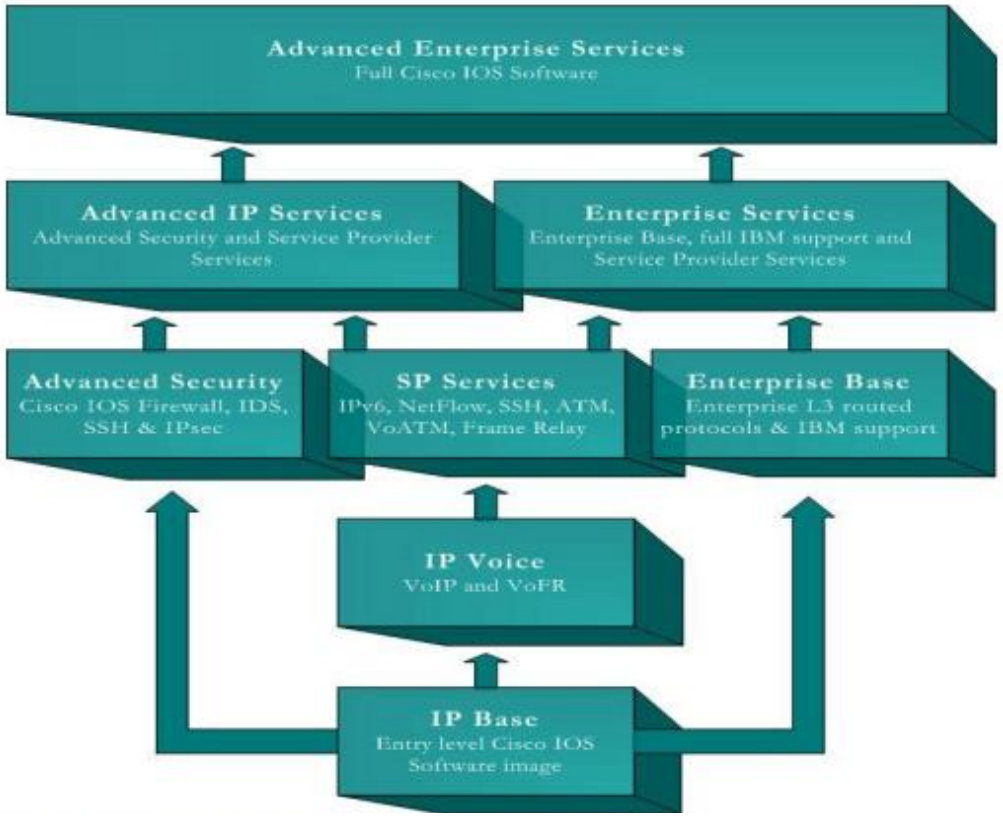
- TCP SYN Floods,
- UDP Floods

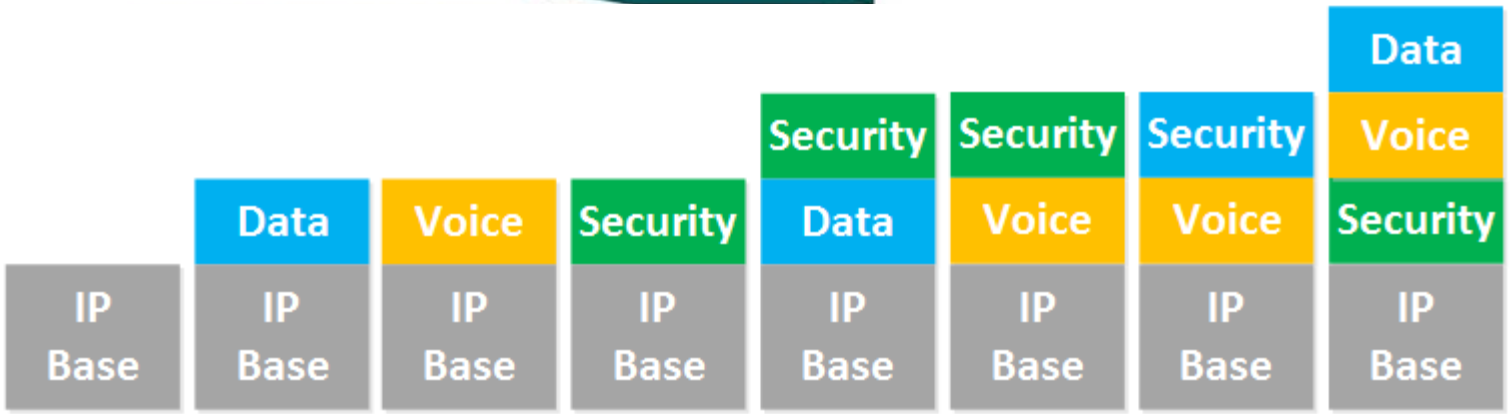
IP地址欺骗攻击

暴力密码破解攻击

企业边界是应对外部威胁的第一道防线。

IOS版本差异


Advanced Enterprise Services
Full Cisco IOS Software
Advanced IP Services
Advanced Security and Service Provider Services
Enterprise Services
Enterprise Base, full IBM support and Service Provider Services
Advanced Security
Cisco IOS Firewall, IDS, SSH & IPsec
SP Services
IPv6, NetFlow, SSH, ATM, VoATM, Frame Relay
Enterprise Base
Enterprise L3 routed protocols & IBM support
IP Voice
VoIP and VoFR
IP Base
Entry level Cisco IOS Software image


IP Base
Data
IP Base
Voice
IP Base
Security
IP Base
Security
Data
IP Base
Security
Voice
IP Base
Security
Voice
IP Base
Data
Voice
Security
IP Base

移动性支持

防火墙

使用防火墙划分安全区

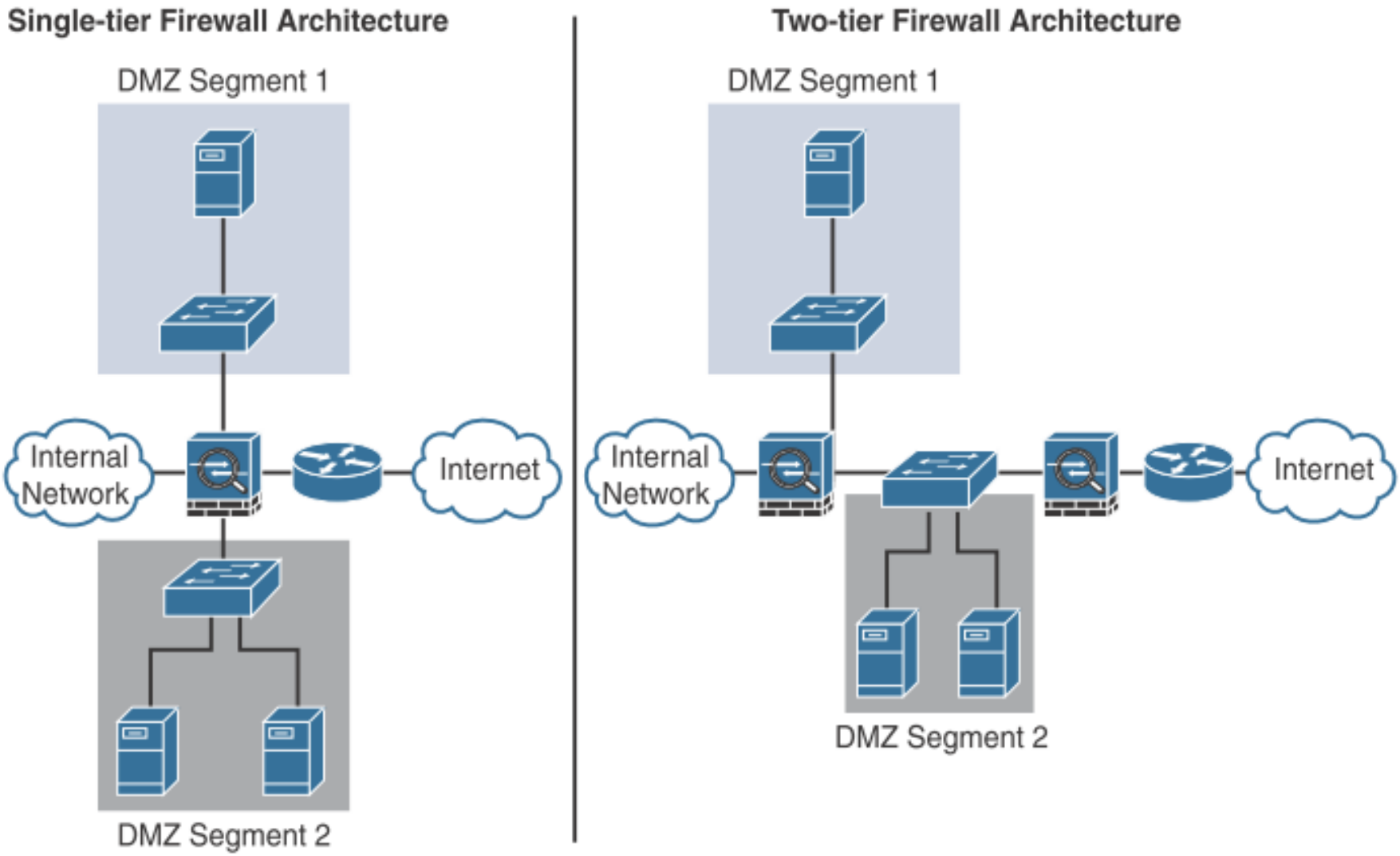
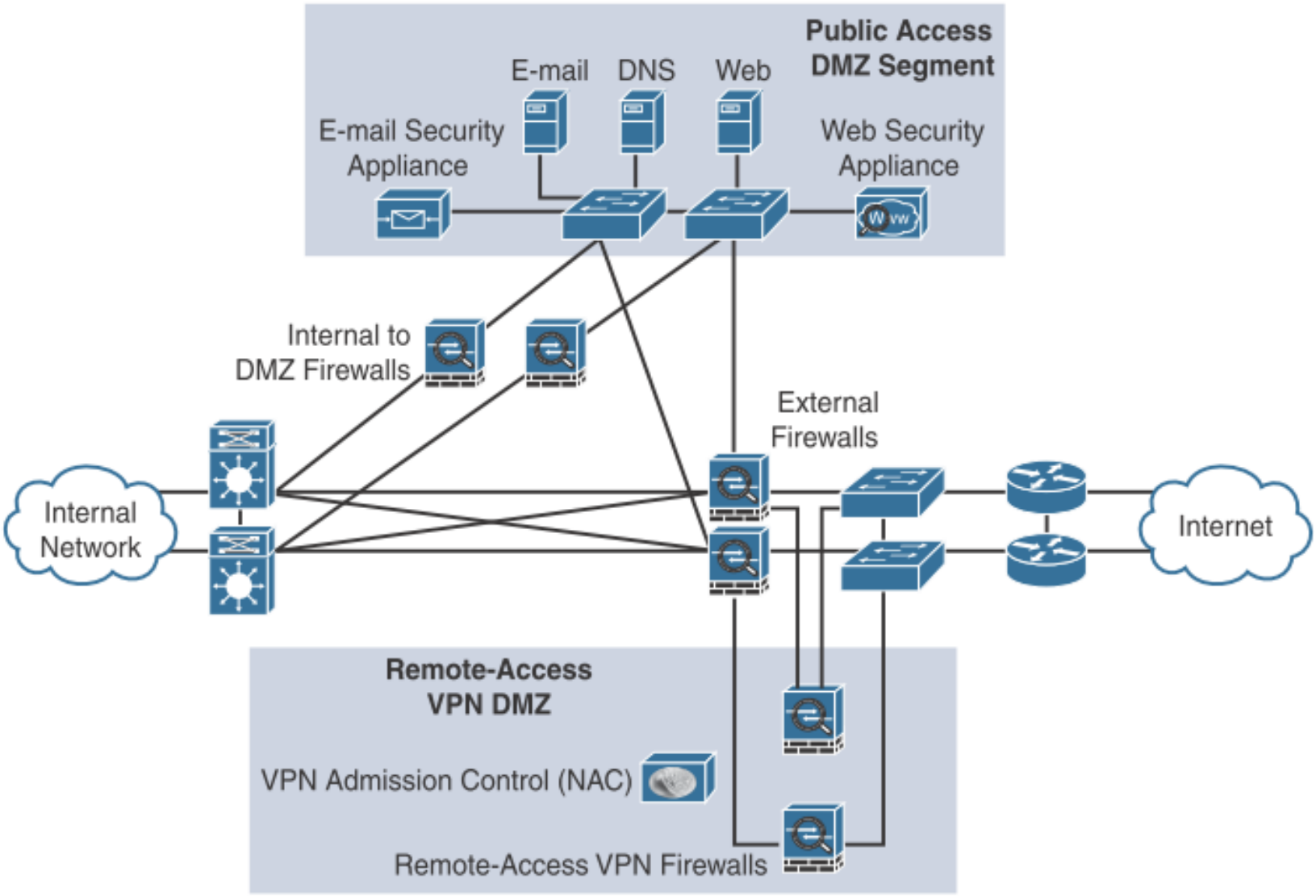


Figure 23-1 *Common Firewall Design Architectures*

ESA & WSA


Public Access
DMZ Segment
E-mail
DNS
Web
E-mail Security
Appliance
Web Security
Appliance
Internal to
DMZ Firewalls
External
Firewalls
Internal
Network
Internet
Remote-Access
VPN DMZ
VPN Admission Control (NAC)
Remote-Access VPN Firewalls

单设备,多接口

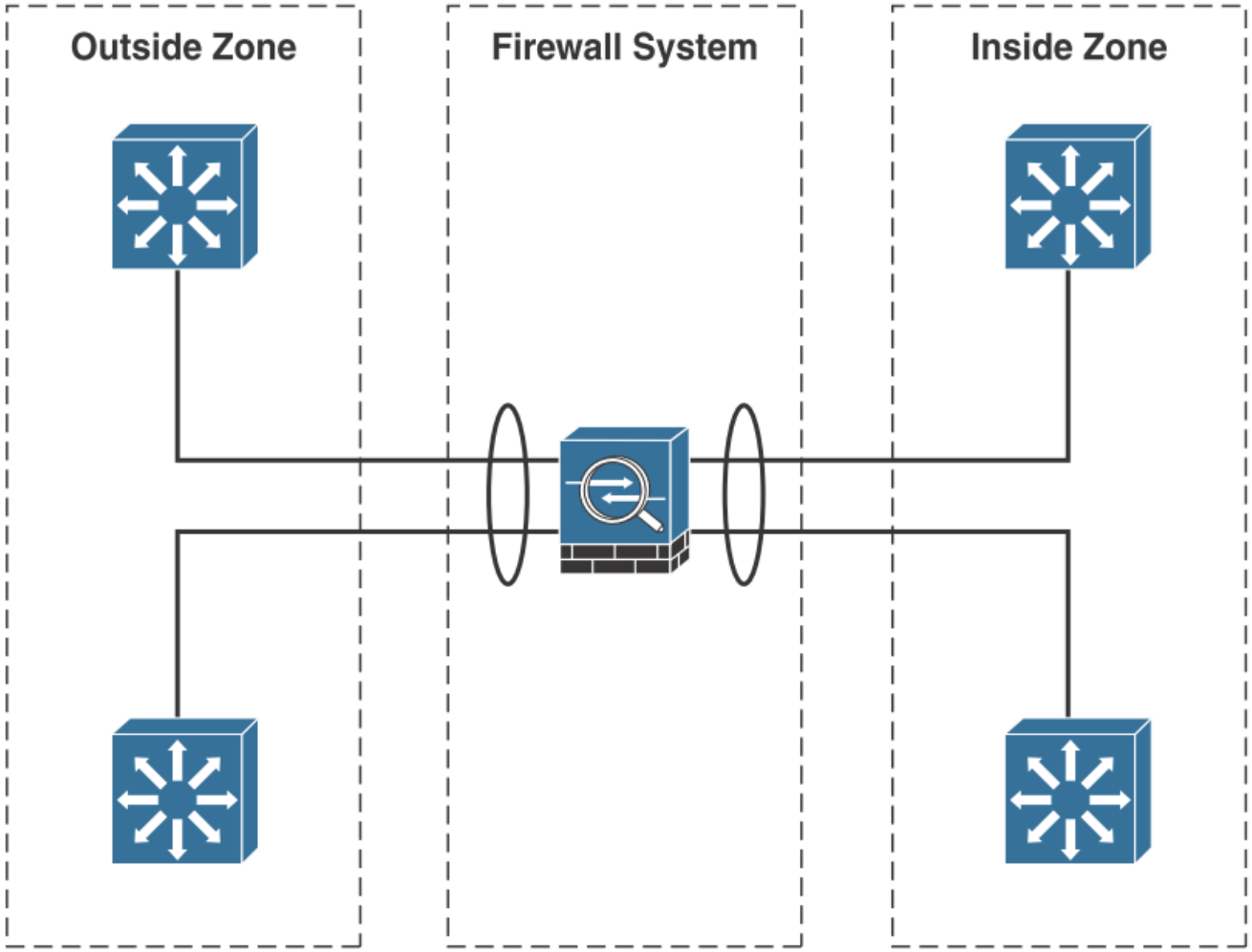


Figure 23-10 *Nonredundant Firewall Connectivity Design*

主动/被动

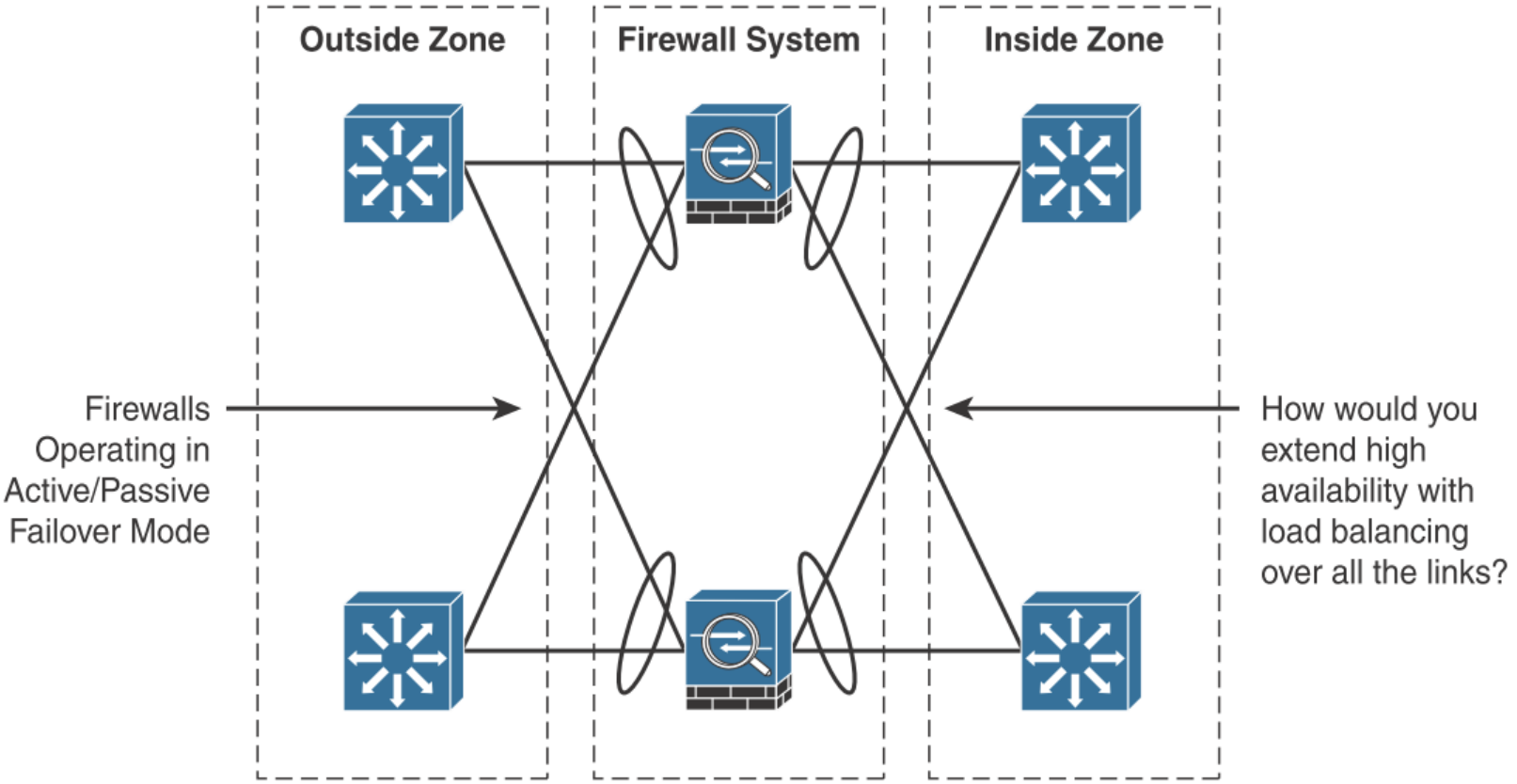
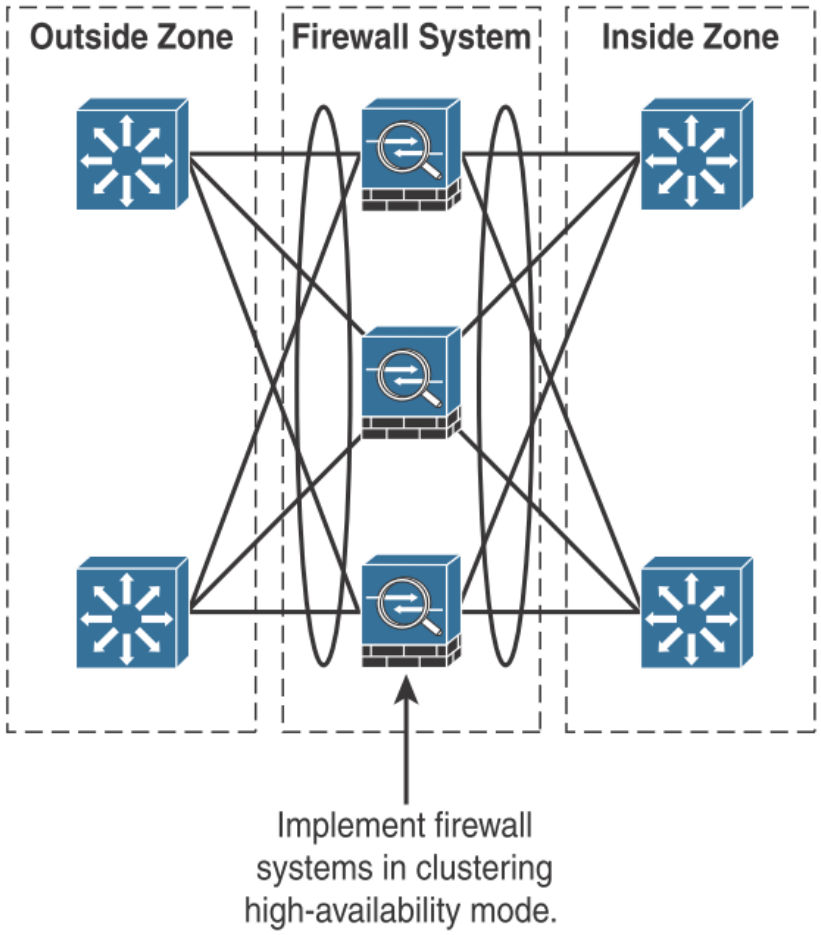


Figure 23-11 *ASA Firewall Active/Passive Failover Mode*

集群



ASA Clustering Benefits:

- The capability to aggregate traffic to achieve higher throughput
- The capability to scale the number of ASA appliances into one logical firewall within the data center architecture
- True active/active model; in multicontext mode, every member for all contexts of the cluster are capable of forwarding every traffic flow
- Can force stateful flows to take a more symmetrical path, which improves predictability and session consistency
- Can operate in either Layer 2 or Layer 3 mode
- Supports single and multiple contexts (firewall virtualization)
- Clusterwide statistics are provided to track resource usage
- A single configuration is maintained across all units in the cluster using automatic configuration sync

Figure 23-12 *ASA Firewall Clustering*

IPS的放置

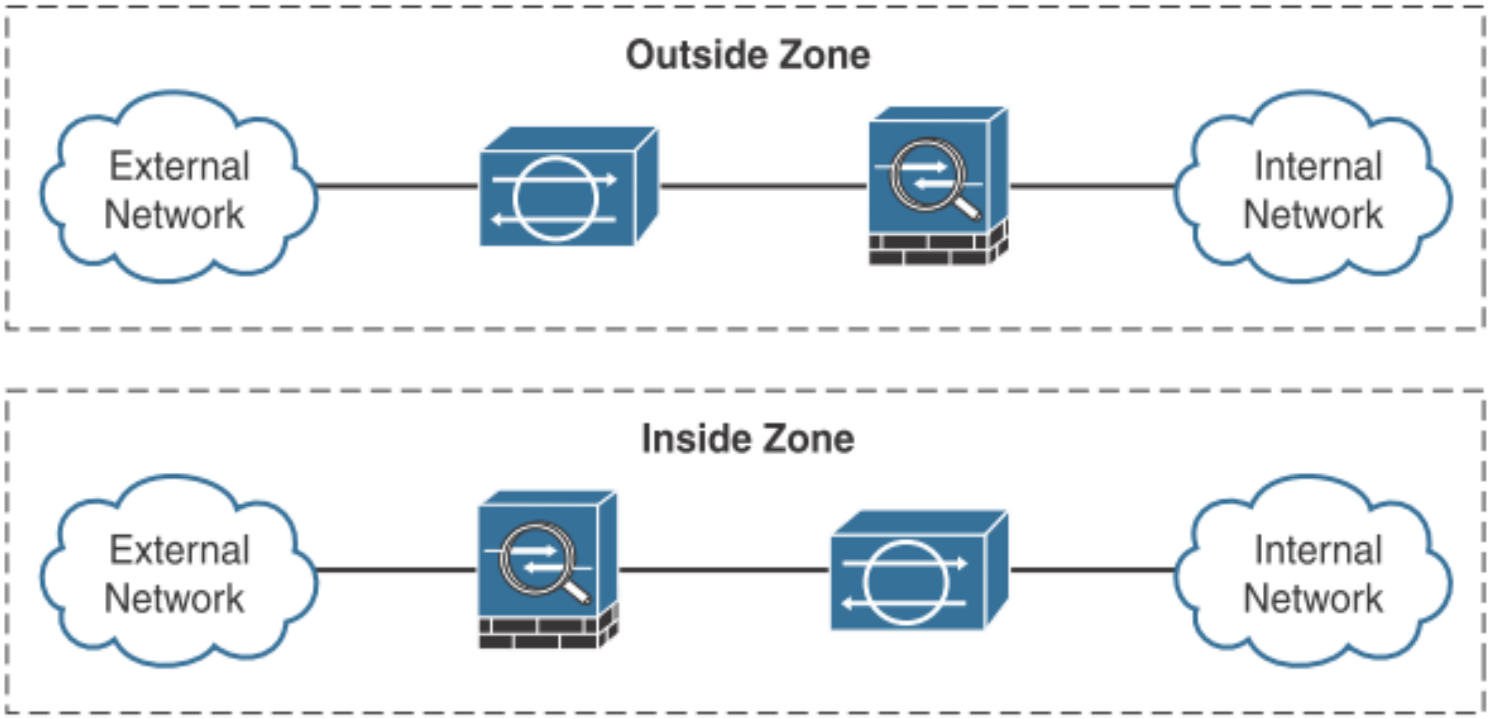
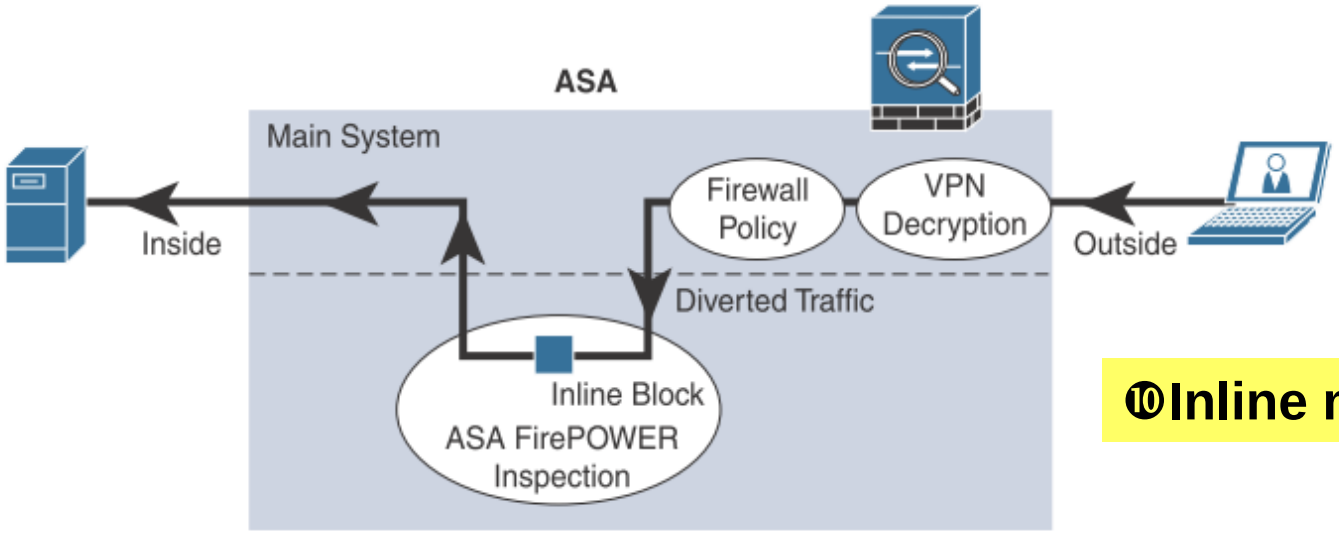


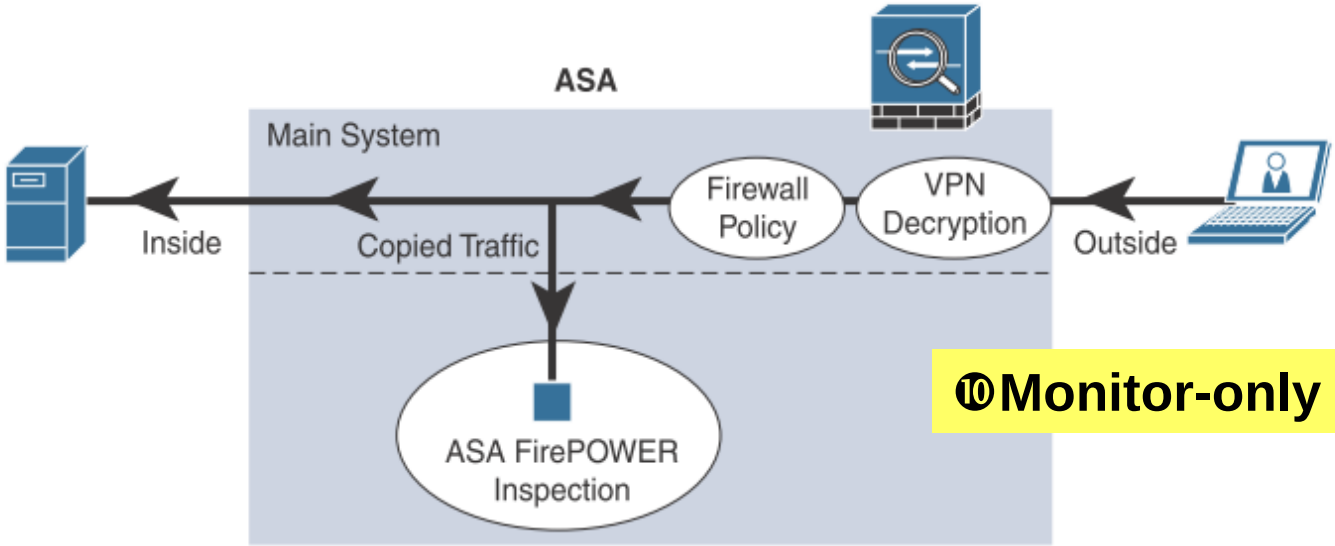
Figure 23-15 *IPS Placement*

IPS作为ASA模块



⑩Inline mode

⑩Cisco FirePOWER is a next-generation IPS (NGIPS)



⑩Monitor-only mode:

IPS作为独立模块

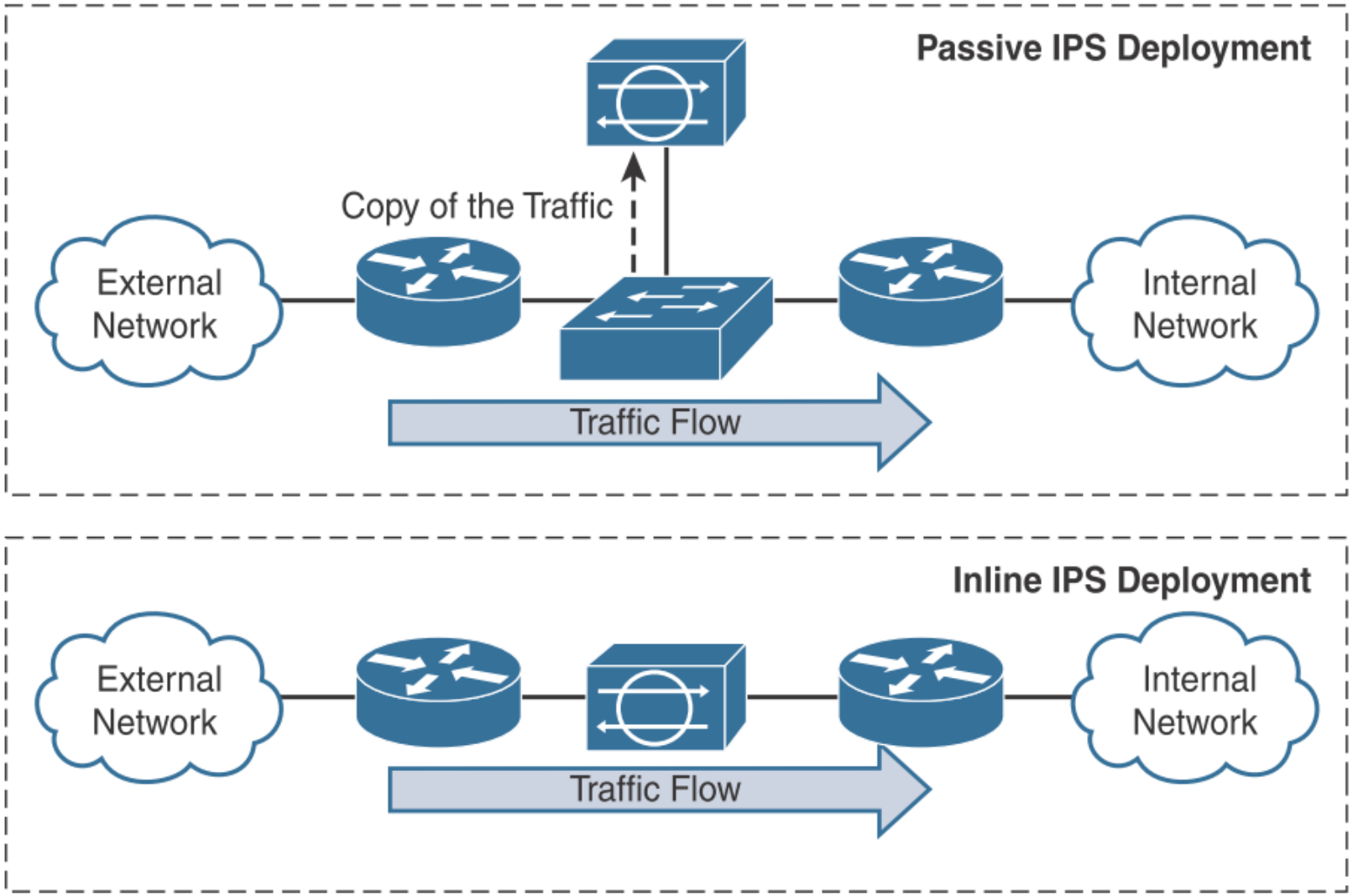
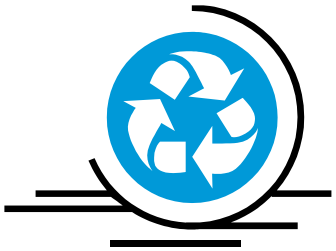


Figure 23-17 *Standalone Cisco FirePOWER IPS Deployment Modes*



VPN tunnel

L2 MPLS VPN

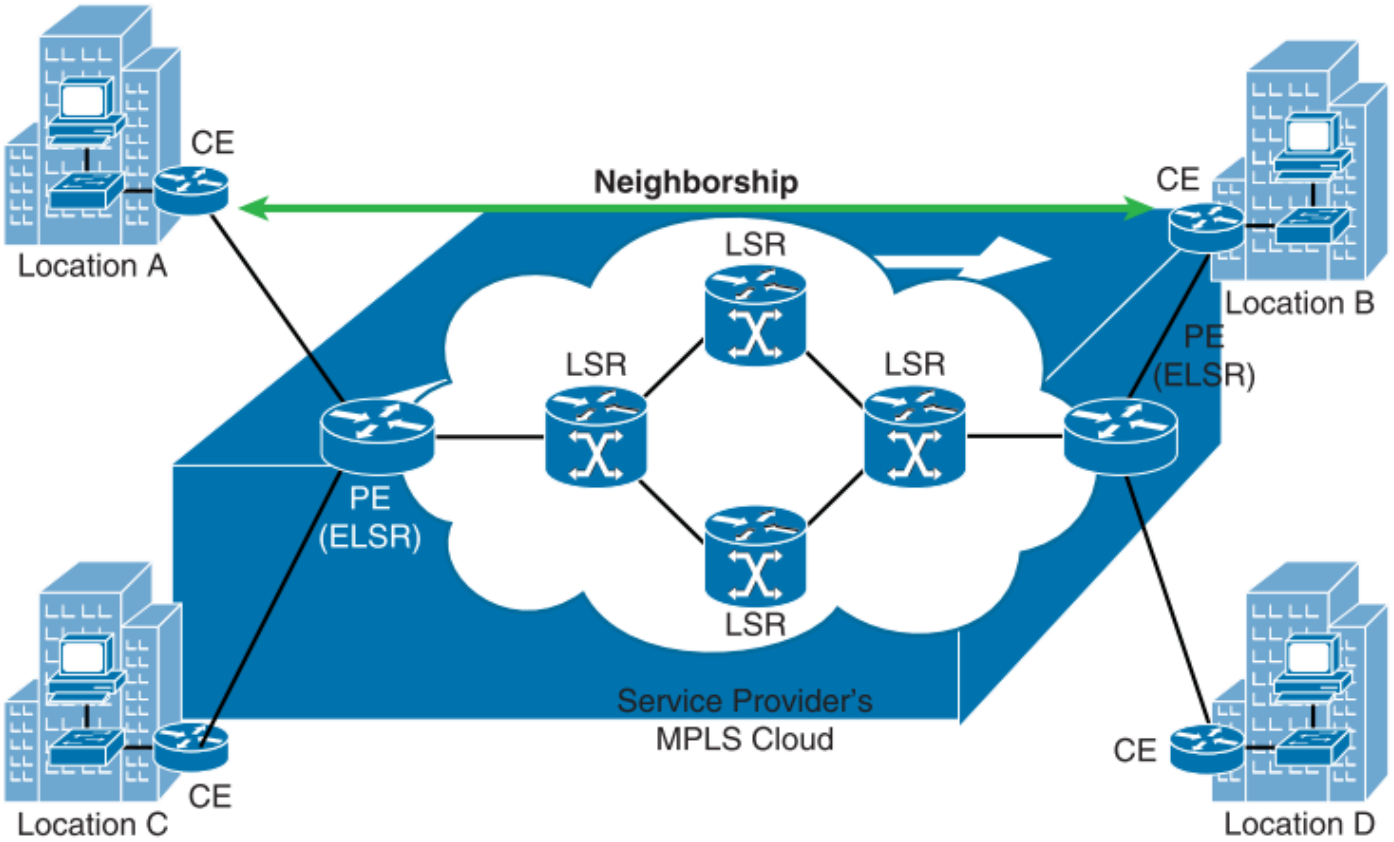


Figure 2-1 *Logical View of a Layer 2 MPLS VPN*

L3 MPLS VPN

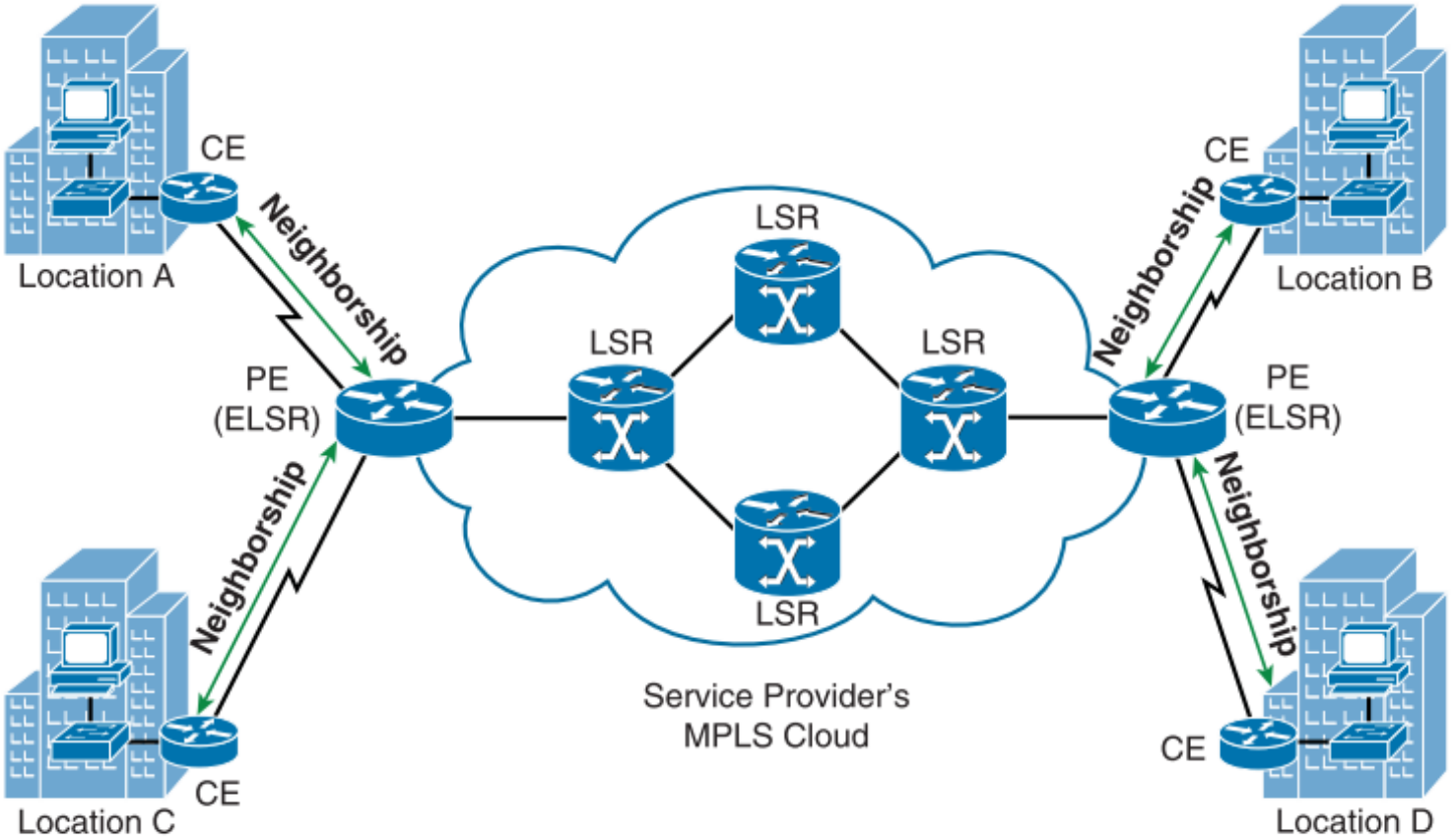


Figure 2-2 *Layer 3 MPLS VPN*

GRE Tunnel

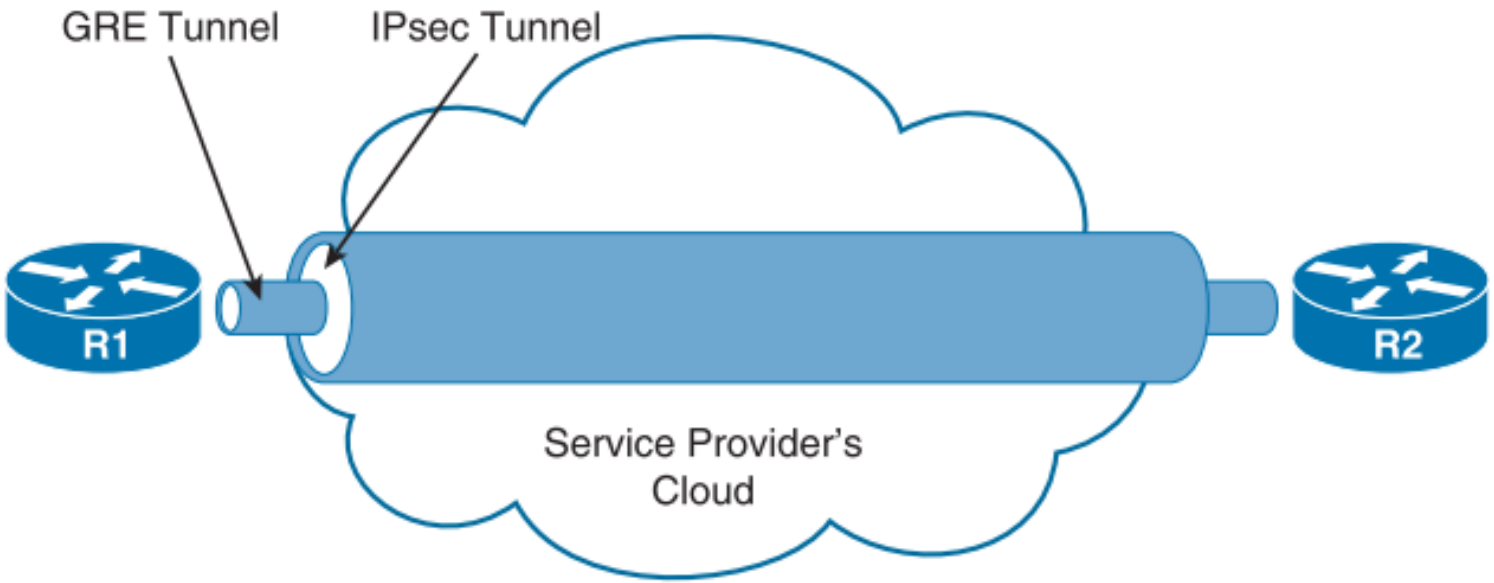


Figure 2-3 *GRE over IPsec Tunnel*

Ipsec 安全特性

- **The following four security features are offered by IPsec:**
  - **Confidentiality: Data confidentiality is provided by encrypting data. If a third party intercepts the encrypted data, the party would not be able to interpret the data.**
  - **Integrity: Data integrity ensures that data is not modified in transit.**
  - **Authentication: Data authentication allows parties involved in a conversation to verify that the other party is the party it claims to be.**
  - **Antireplay: IPsec uses antireplay protection to ensure that packets being sent are not duplicate packets.**

VPN 模式

- **Following is a detailed description of these two modes:**
  - **Transport Mode: Transport mode uses a packet's original IP header, as opposed to adding an additional tunnel header. This approach works well in networks where increasing a packet's size could cause an issue. Also, transport mode is frequently used for client-to-site VPNs, where a PC running VPN client software connects back to a VPN termination device at a headquarters location.**
  - **Tunnel Mode: Tunnel mode, unlike transport mode, encapsulates an entire packet. As a result, the encapsulated packet has a new header (that is, an IPsec header). This new header has source and destination IP address information that reflects the two VPN termination devices at different sites. Therefore, tunnel mode is frequently used in an IPsec site-to-site VPN.**

VPN模式

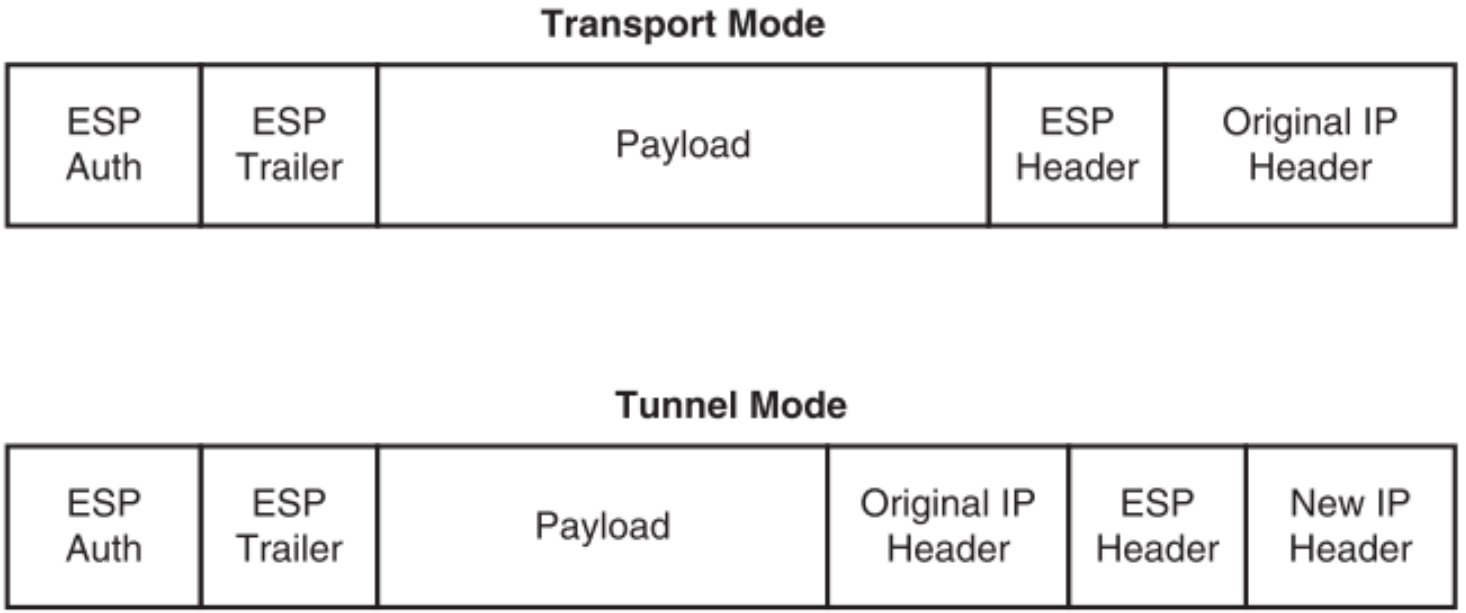


Figure 2-10 *Transport Mode Versus Tunnel Mode*

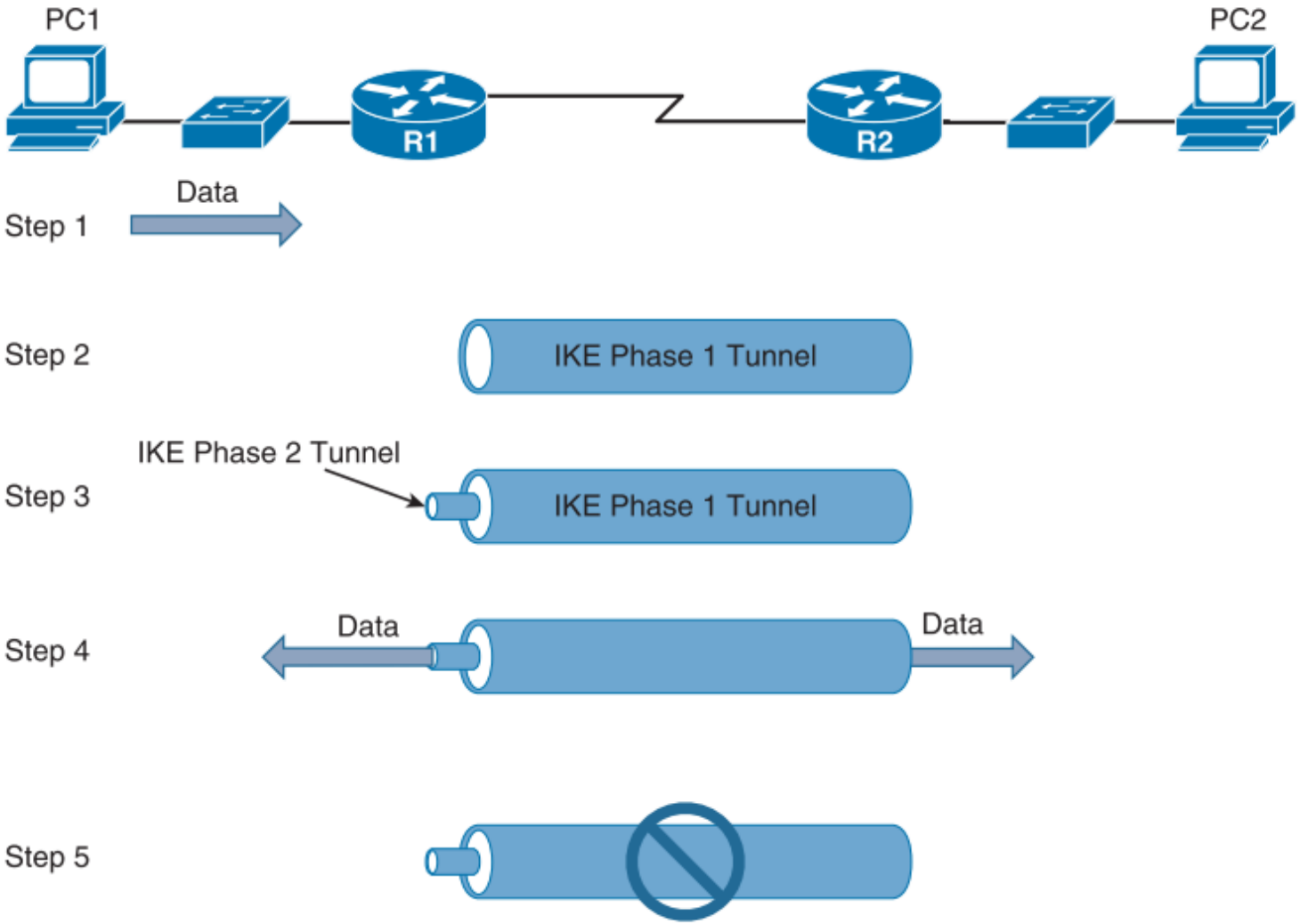
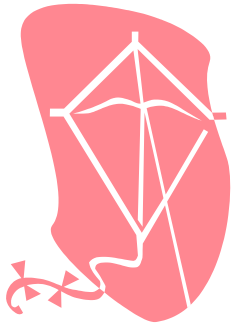


Figure 2-11 *IPsec VPN Steps*



性能支持
（Performance）

应用性能支持

- 网络对应用的性能支持通过应用识别功能实现。（不能用简单增加带宽来实现）。
  - Cisco Application Network Services (ANS)

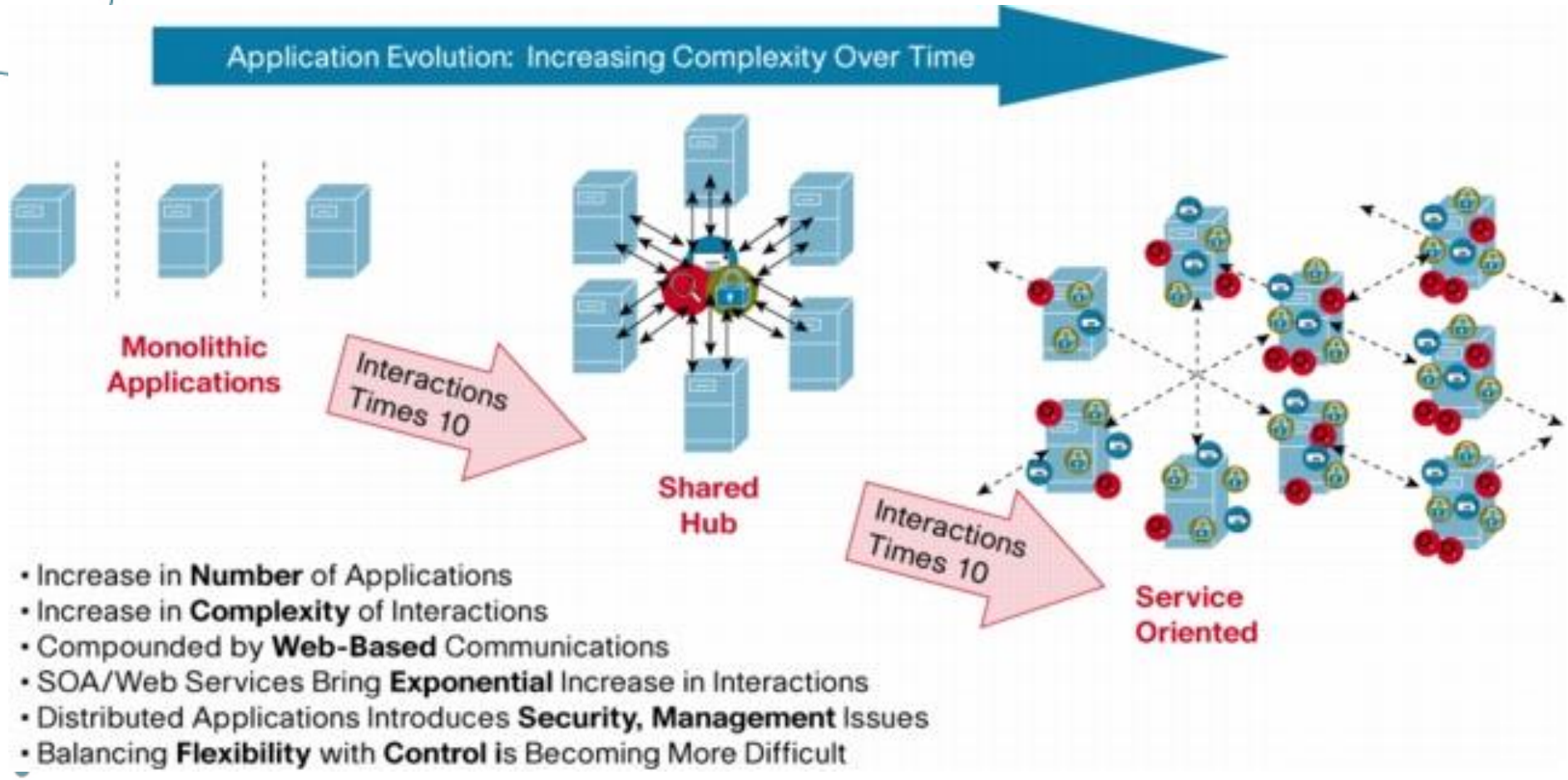
思科应用网络服务

- Cisco Application Network Services (ANS)
  - 提供压缩、缓存、内容优化功能：实现广域网应用（分支机构）的响应速度和局域网类似。
  - 提供优化功能：对发往门户网站的网络信息流进行，以减少延时，避免不必要的网络对象重新加载；将底层的任务从服务器移出。
  - 提供安全性和远程连接功能：可以自动验证合作伙伴的请求，将其路由到适当的后台应用程序，并对响应进行加密和设置优先级。
  - 提供应用信息服务功能：可以根据设置的规则截取订单，获取金额等信息存入数据库。

AON

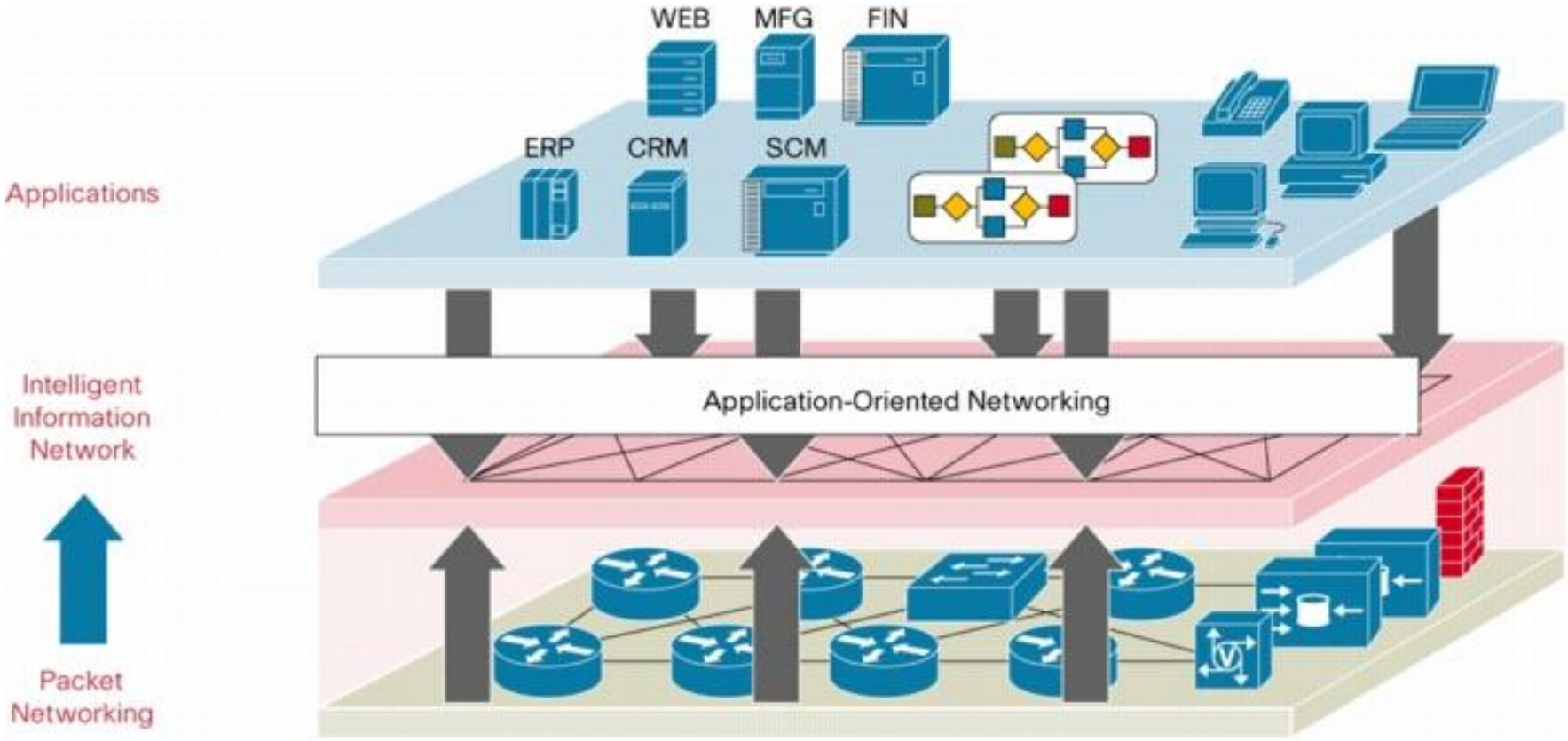
- **Cisco Application-Oriented Network**
  - **Cisco AON uses the underlying network to provide an essential communications infrastructure for messaging, security, and other shared services.**
  - **A Cisco AON-based network can transparently intercept and selectively filter all traffic, understand and translate relevant traffic across different applications at the message level, and deliver wire-speed inspection and processing of information.**

应用的进化



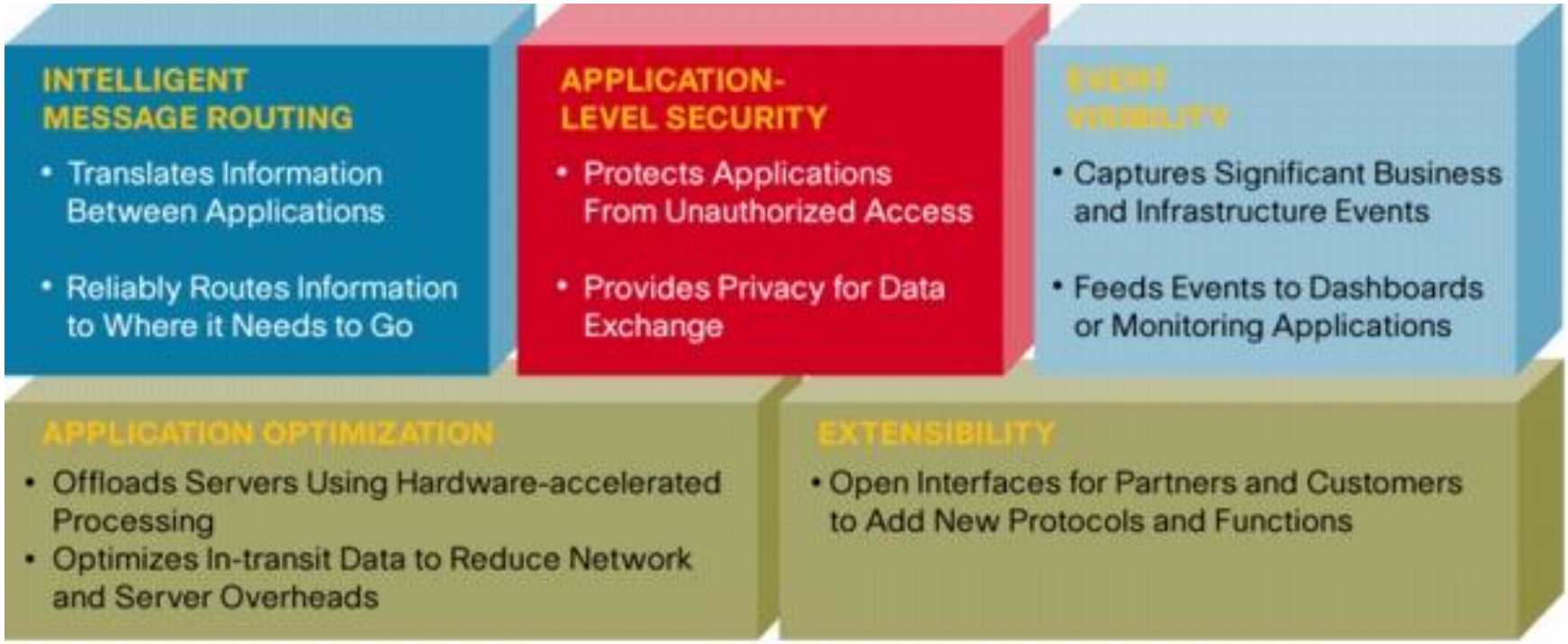
⑩Figure 1. Applications Have Been Moving to a Distributed Architecture

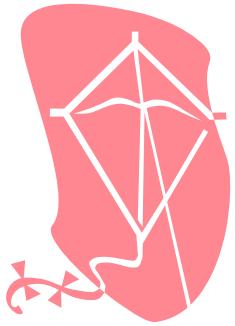
网络和应用的合作



Improved Collaboration Between Applications and the Network

AON 核心功能


INTELLIGENT MESSAGE ROUTING
• Translates Information Between Applications
• Reliably Routes Information to Where it Needs to Go
APPLICATION-LEVEL SECURITY
• Protects Applications From Unauthorized Access
• Provides Privacy for Data Exchange
• Captures Significant Business and Infrastructure Events
• Feeds Events to Dashboards or Monitoring Applications
APPLICATION OPTIMIZATION
• Offloads Servers Using Hardware-accelerated Processing
• Optimizes In-transit Data to Reduce Network and Server Overheads
EXTENSIBILITY
• Open Interfaces for Partners and Customers to Add New Protocols and Functions



IP通讯支持
（IP communication）

VoIP功能区域划分

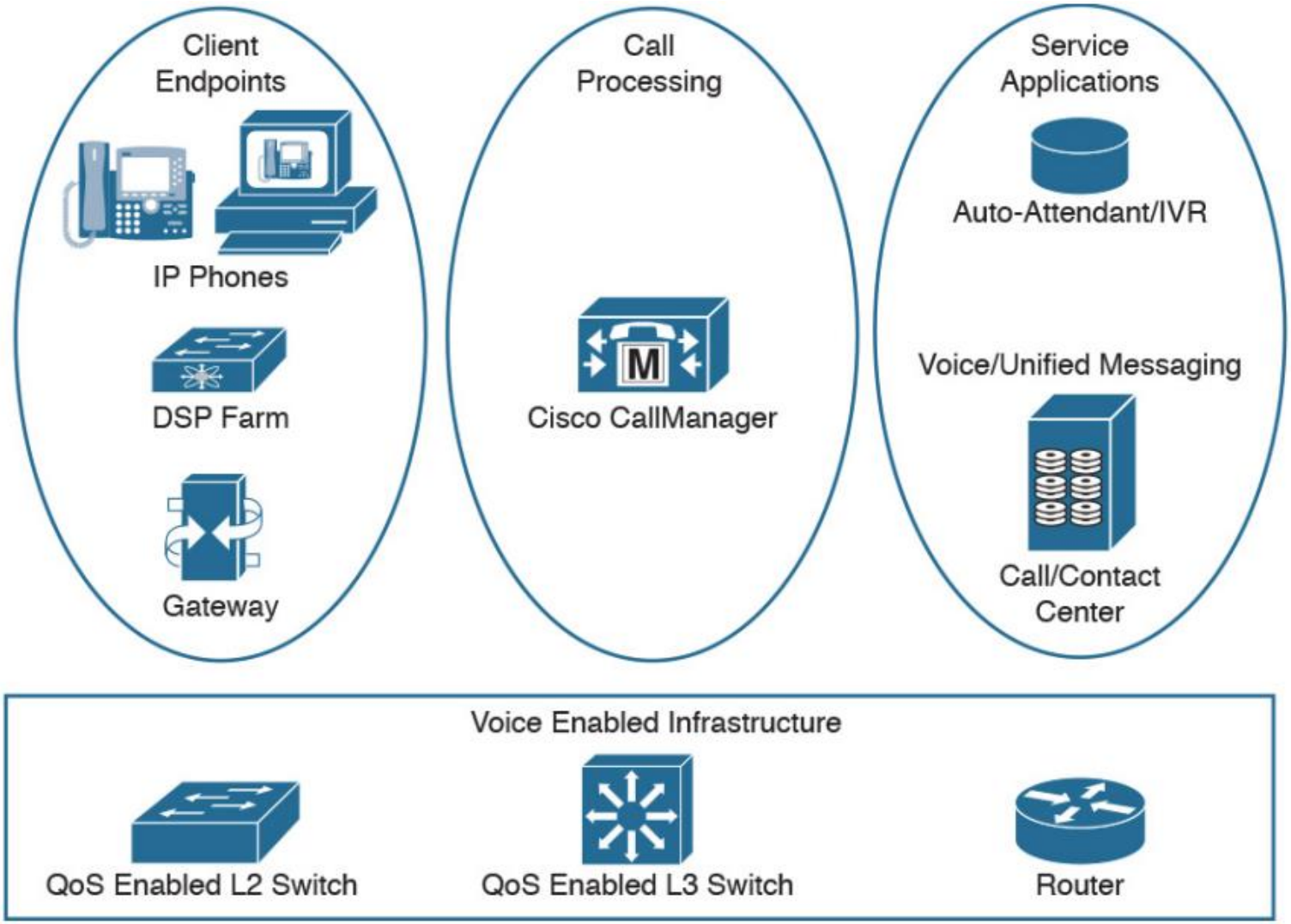


Figure 14-9 *Cisco IPT functional areas*

⑩VoIP is also referred to as IP telephony (IPT)

VoIP相关设备


Operations & Serviceability
User and Device Provisioning
Voice Quality Monitoring & Alerting
Operations & Fault Monitoring
Network & Application Probing
Applications & Services
Voice Messaging
Rich Media Conferencing
HDTV
Presence Services
Mobility
Contact Center
Collaboration Clients
Call Control
LDAP & Directory Services
Media Resources
MoH
End Points
ICM
Unified CUCM Applications
Device Mobility
Call Routing
Call Processing
Dial Plan & Call Admission Control
Video Telephony
PSTN & IP Gateways
PSTN Services
Remote Site Survivability
Network
Access Switch
Wireless
Distribution & Core Switching
WAN Router
Firewall Security
Quality of Service
IP
IP WAN & Internet Access

独立的语音和数据网络

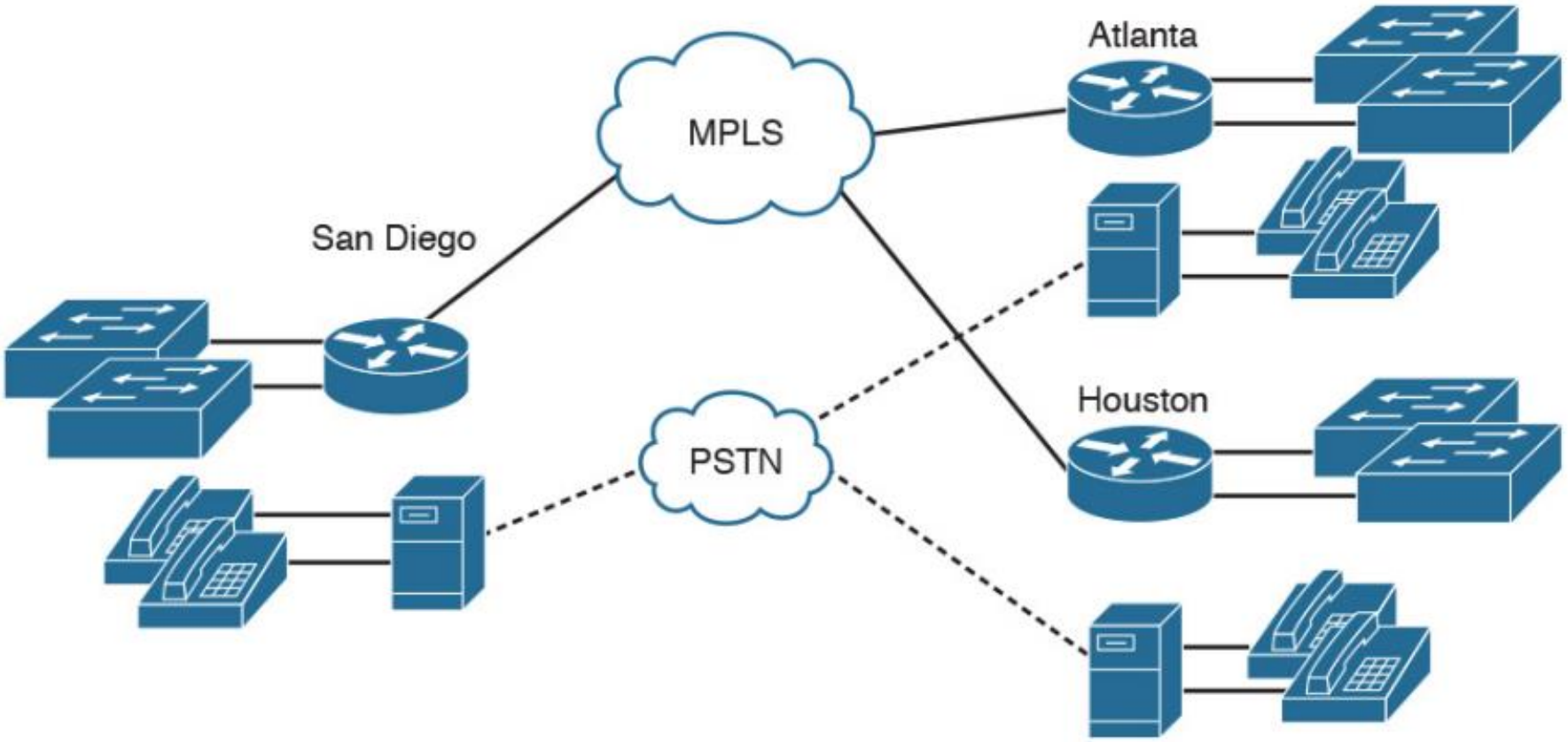


Figure 14-7 *Separate voice and data networks*

融合的VOIP网络

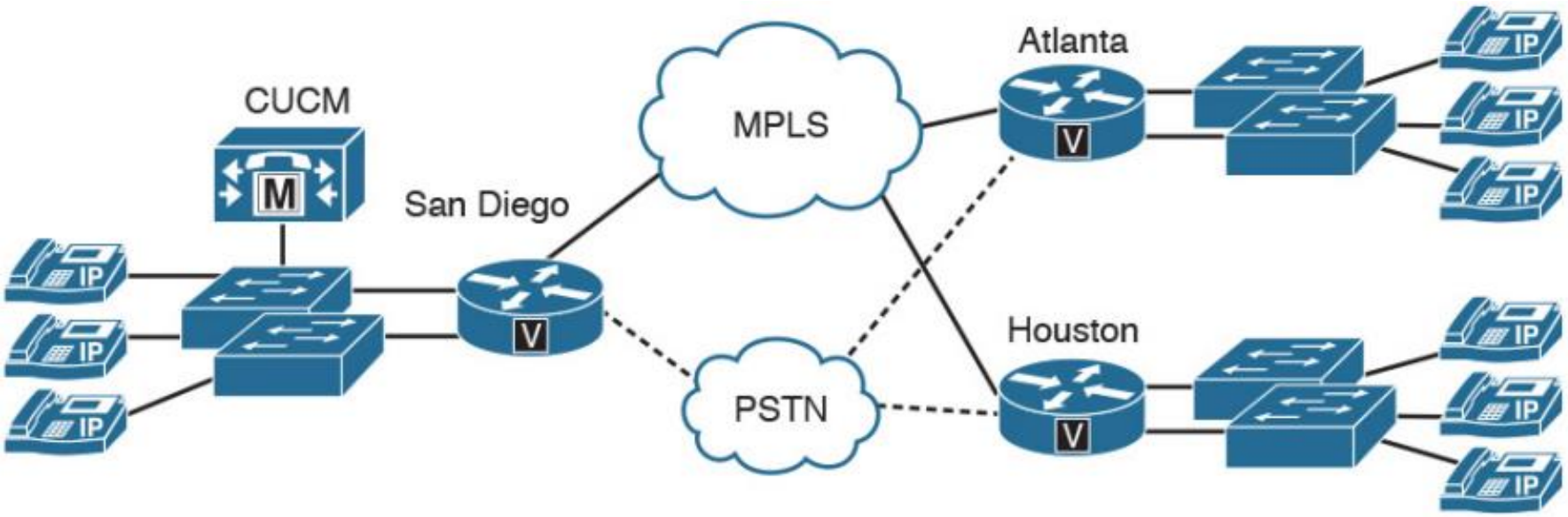


Figure 14-8 *Converged VoIP network*

单区域

呼叫管理：Call-processing manager

IP 电话机：IP phones

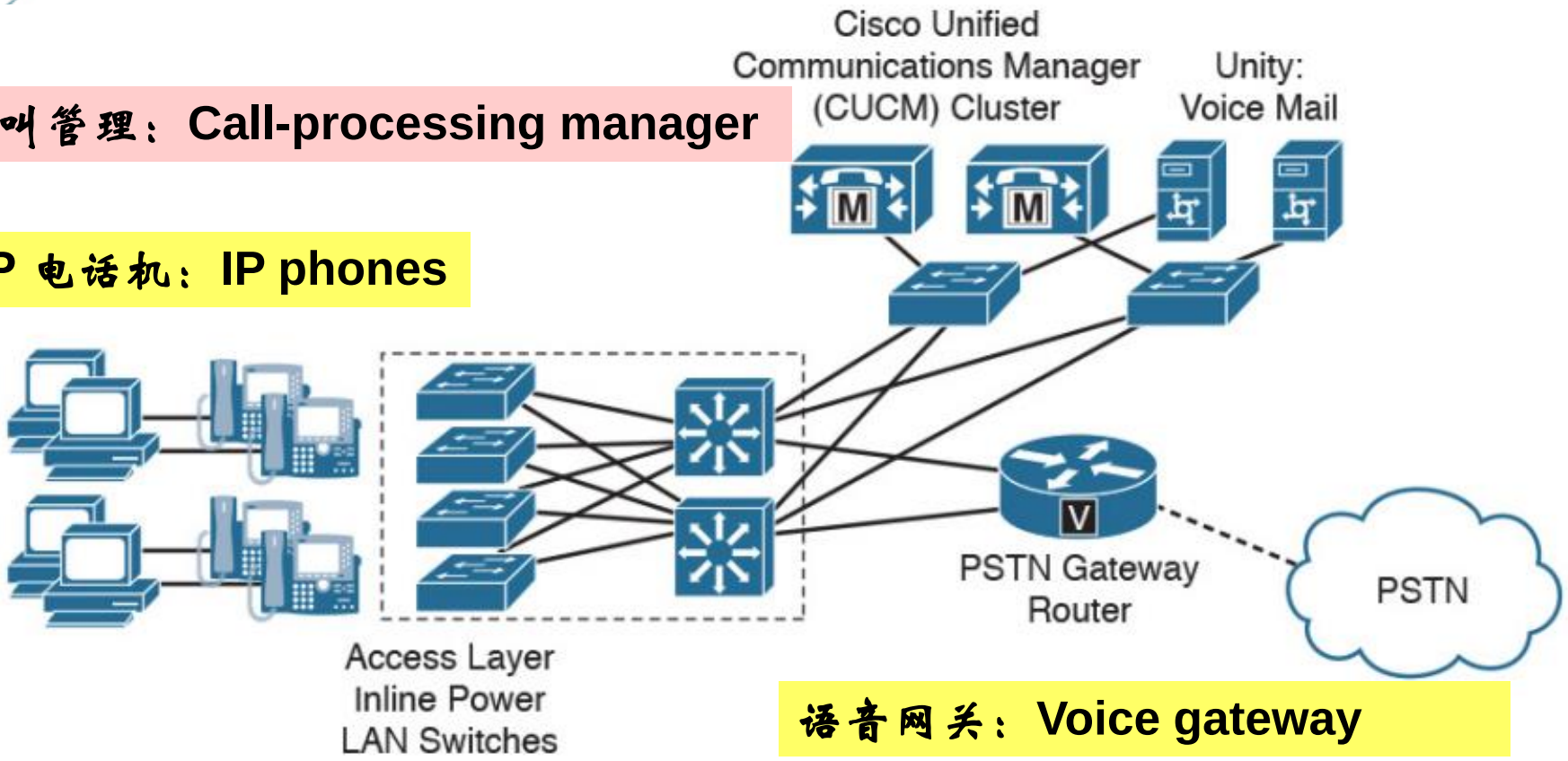


Figure 14-10 *Single-site deployment model*

语音网关：Voice gateway

带供电功能的交换机：Switches with inline power

多区域集中控制

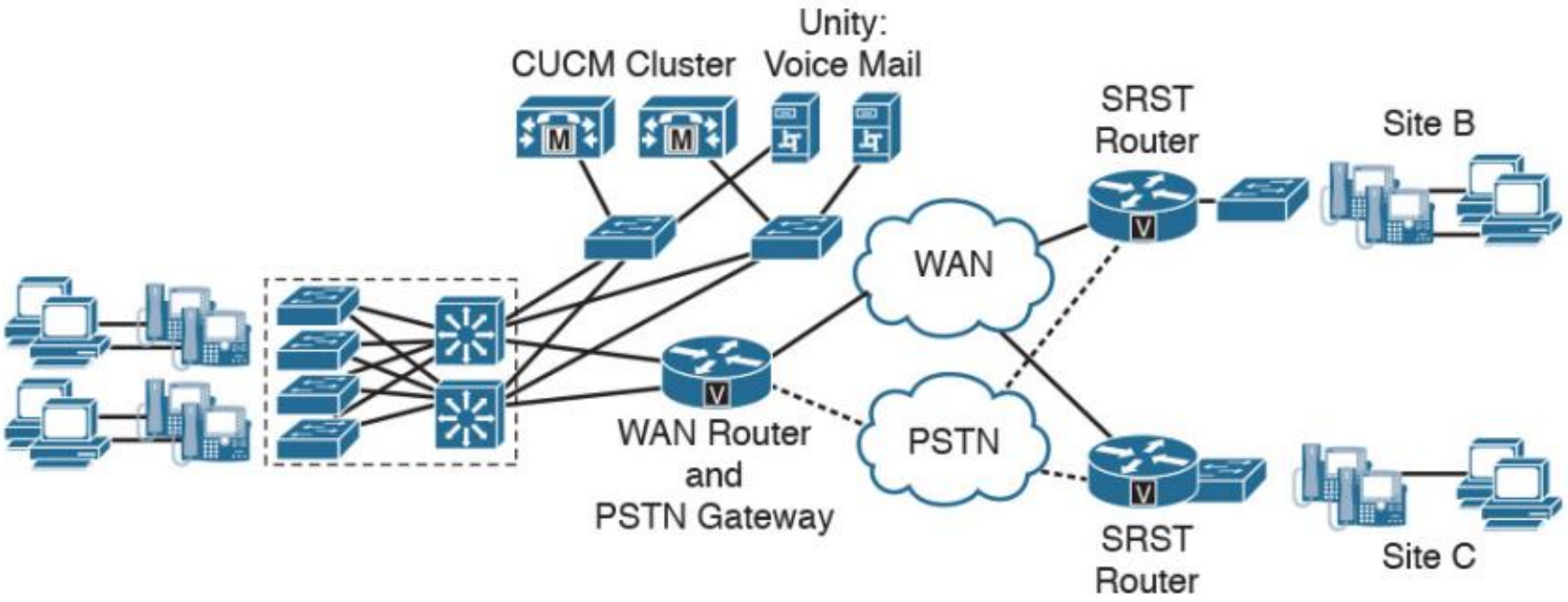


Figure 14-11 *Multisite WAN with centralized CM deployment model*

多区域分布控制

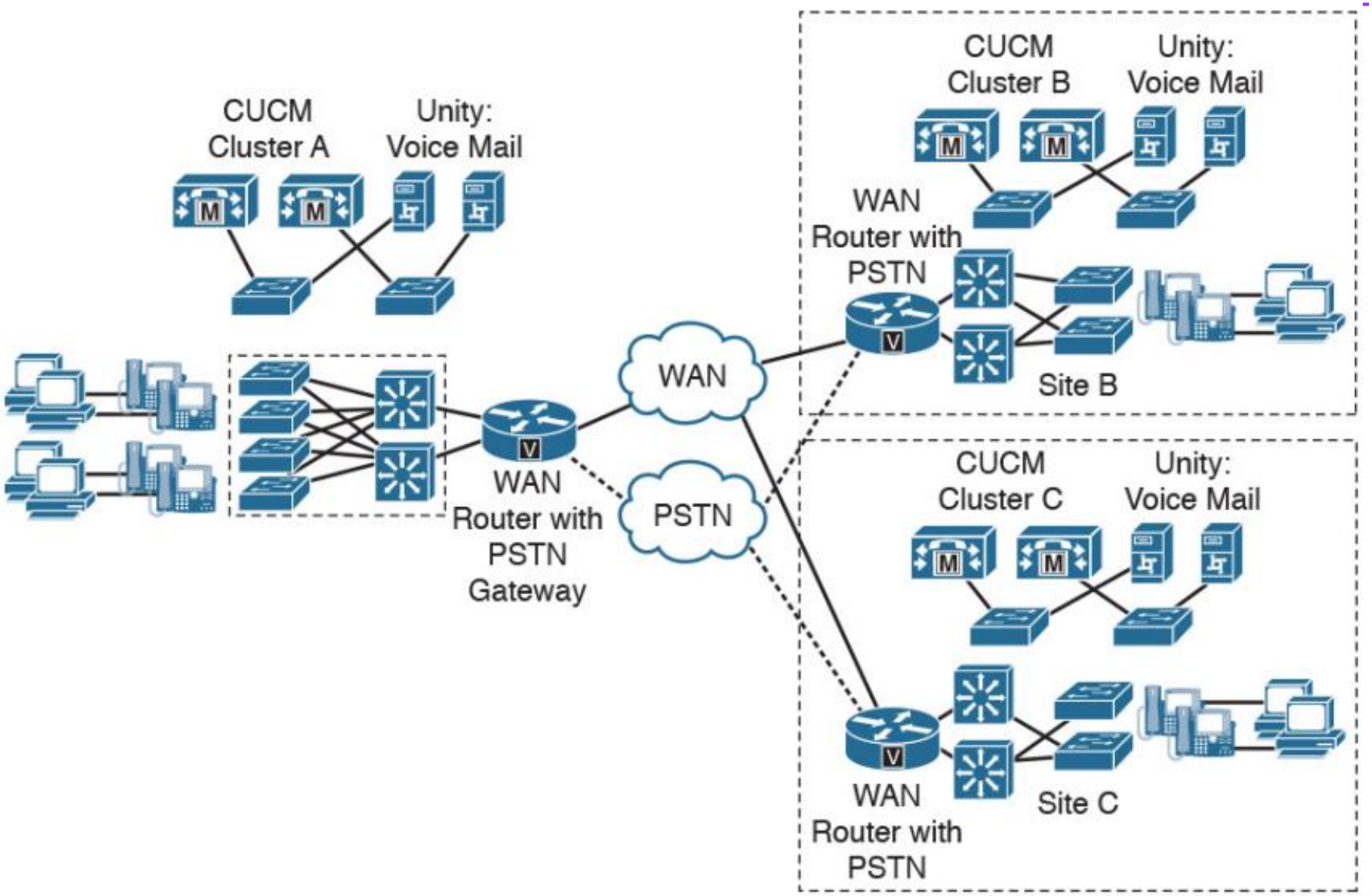
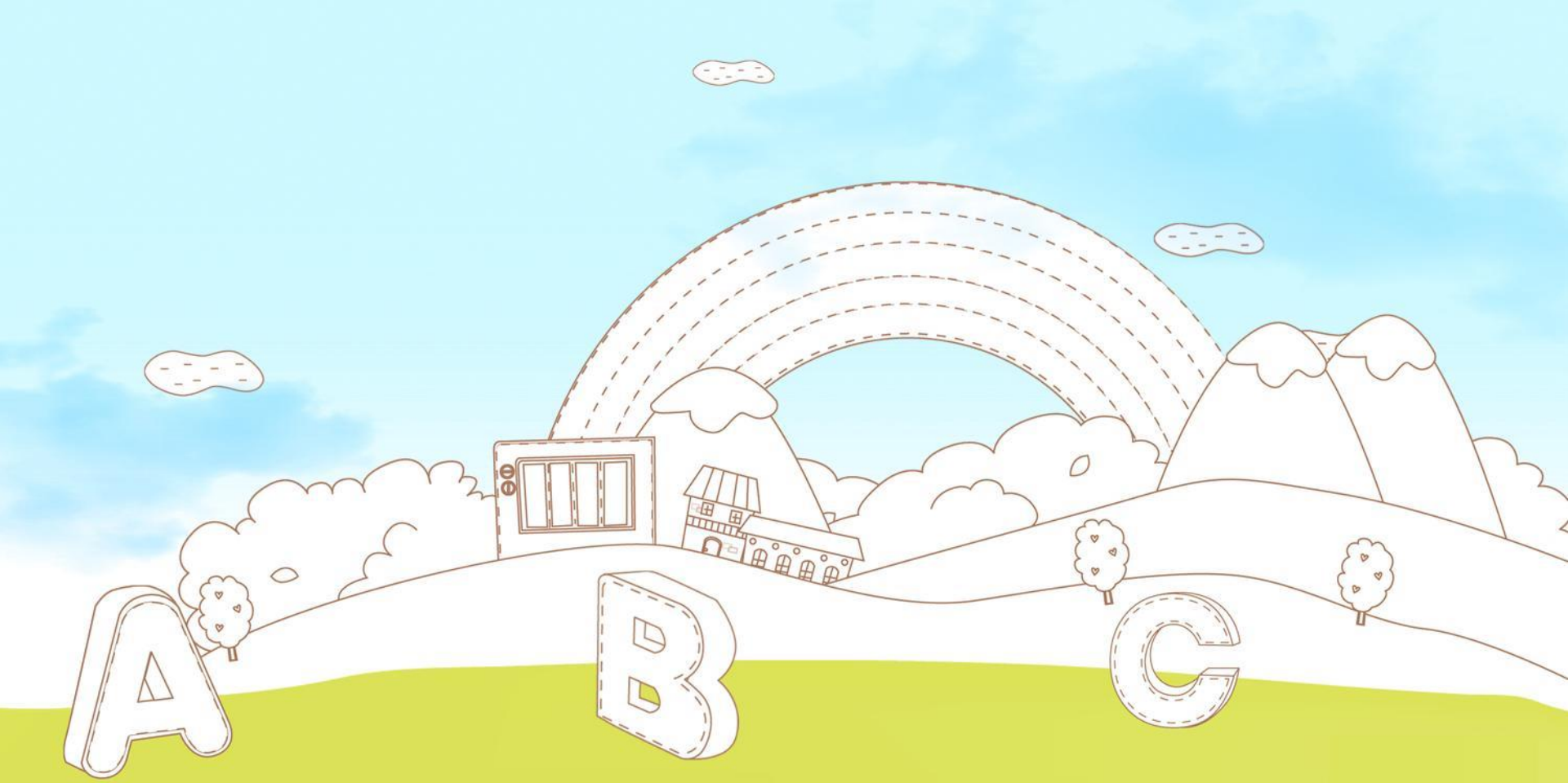


Figure 14-12 *Multisite WAN with distributed CM deployment model*



Thank You !