

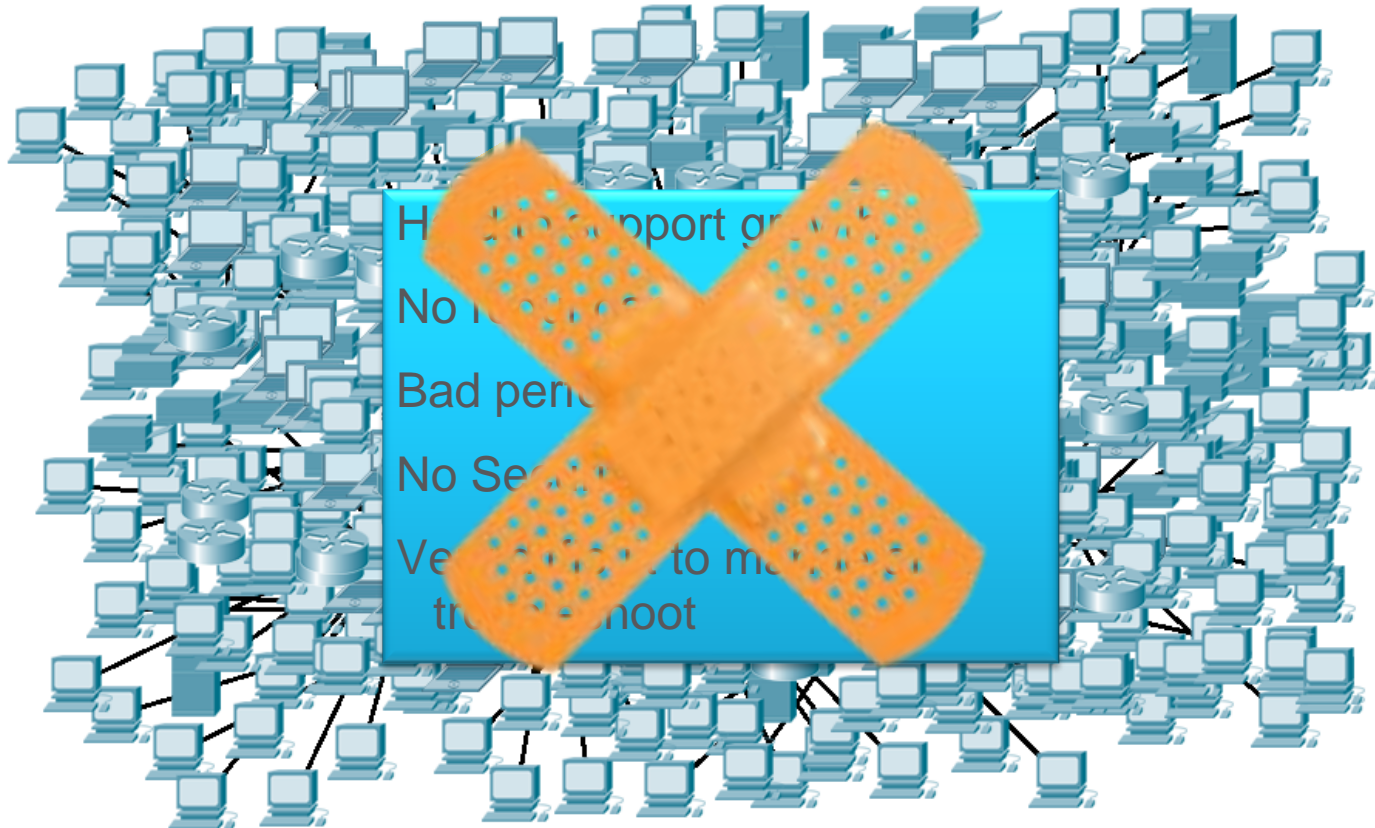
27 Network Design



27.1 Hierarchical Networks

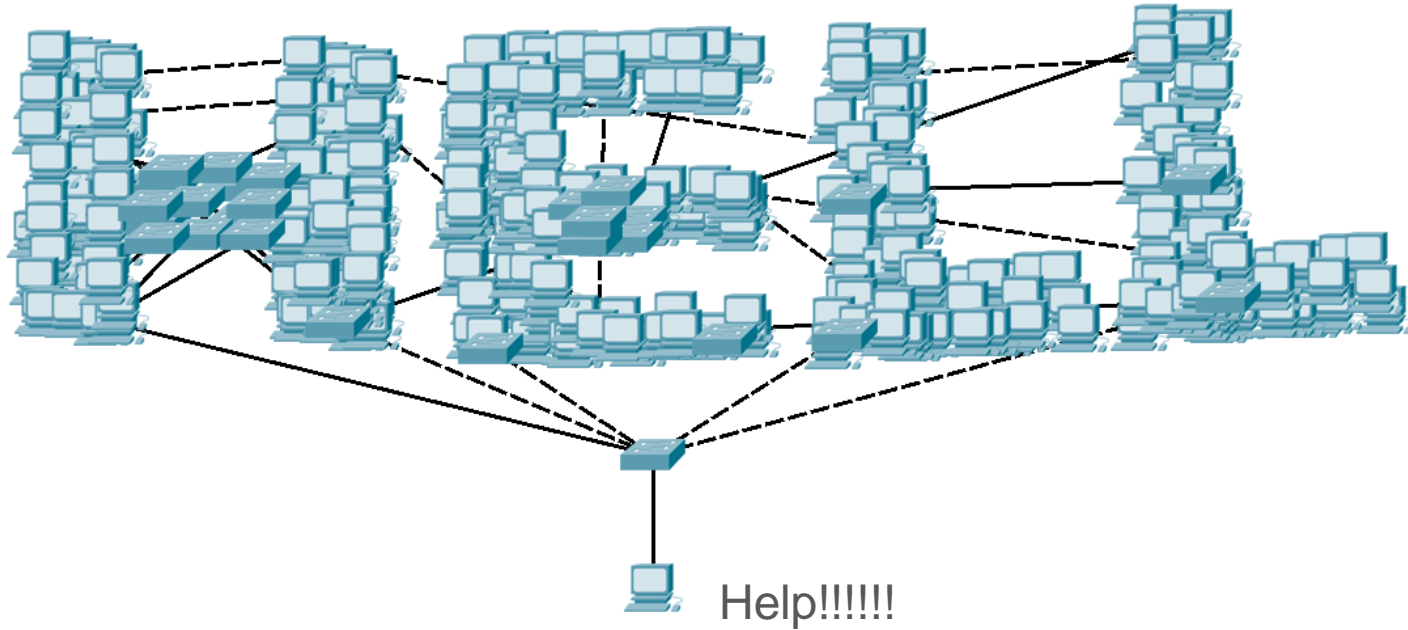
分层网络

You want to manage this network?



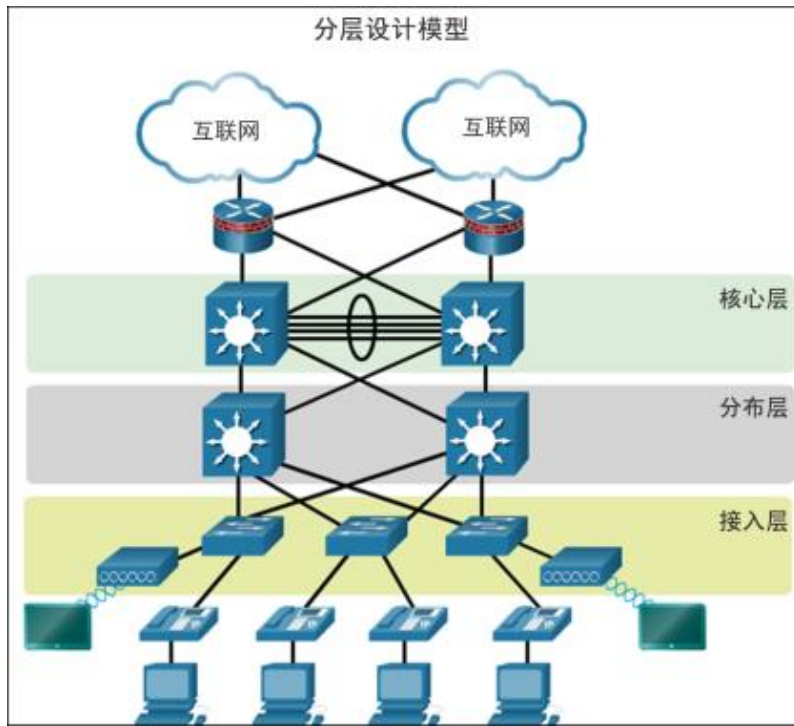
How the support group
No resources
Bad performance
No Security
Very difficult to manage
troubleshoot

You want to manage this network?



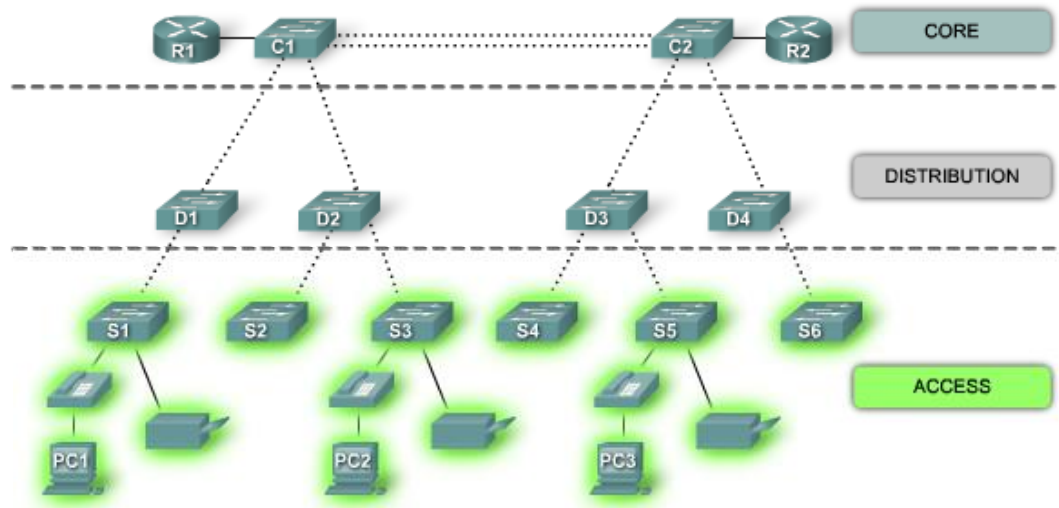
接入层、分布层、核心层功能

- 接入层向终端设备和用户提供对网络的直接访问。为了满足网络应用程序和最终用户的需求，现在下一代交换平台在网络边缘向各种类型的端点提供更多融合、集成和智能服务。接入层交换机中智能的构建使应用程序能够在网络上更加安全有效地运行。
- 分布层汇聚各接入层并提供服务连接。
 - ✓ 聚合大规模的配线间网络
 - ✓ 聚合第 2 层广播域和第 3 层路由边界
 - ✓ 提供智能交换、路由和网络访问策略功能来访问网络的其余部分
 - ✓ 通过冗余的分布层交换机，为终端用户提供高可用性，并提供去往核心层的等价路径。
 - ✓ 在网络边缘为各种类别的服务应用程序提供区别服务
- 核心层充当了所有分布层设备的聚合点，并把园区网与网络的其他部分连接起来。核心层的主要用途是提供错误隔离和高速主干连接。



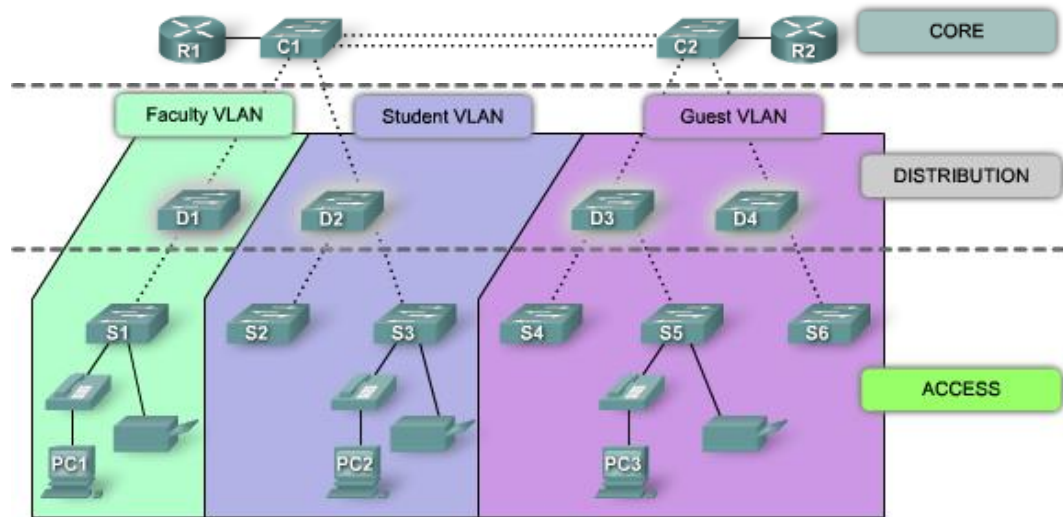
The Hierarchical Network Model

- The main purpose of the **access layer** is to provide a means of **connecting devices to the network** and **controlling which devices are allowed** to communicate on the network.



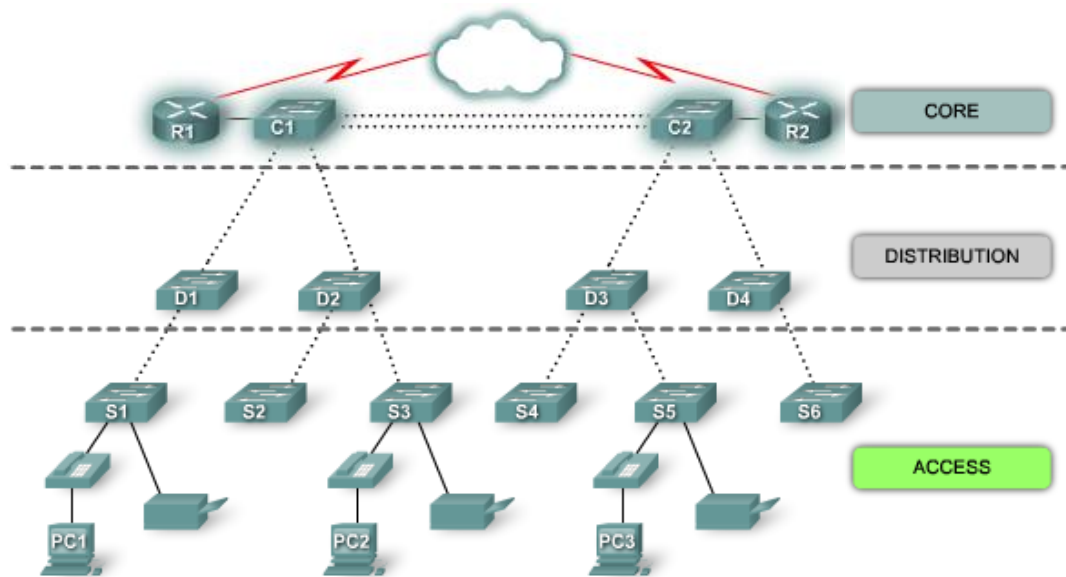
The Hierarchical Network Model

- The **distribution layer** **aggregates the data** received from the access layer switches before it is transmitted to the core layer for routing to its final destination.

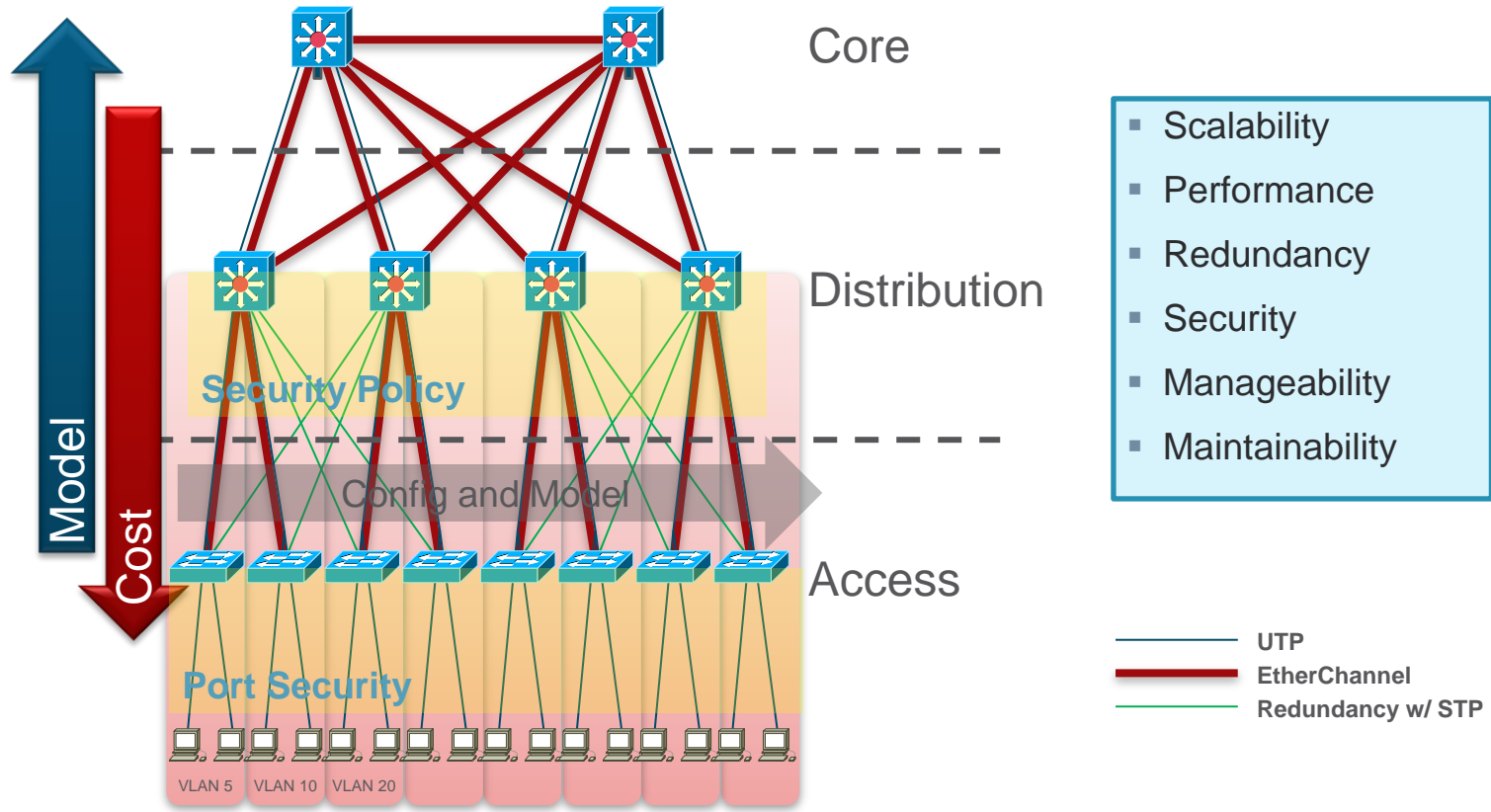


The Hierarchical Network Model

- The **core layer** of the hierarchical design is the **high-speed backbone** of the internetwork. The core area can also connect to Internet resources.



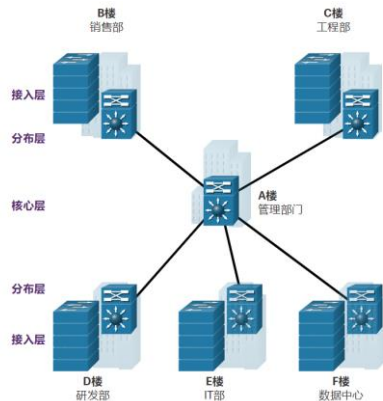
Benefit of Hierarchical Network



分层网络 三层和两层举例

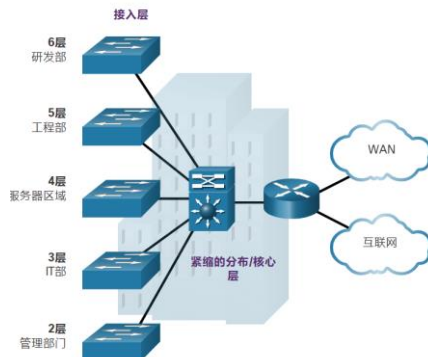
Three-tier Campus Network

- 由需要接入层、分布层和核心层的组织使用。
- 建议建立一个扩展的星形物理网络拓扑结构, 从一个集中的建筑位置到同一校园内的所有其他建筑。



Two-tier Campus Network

- 不需要单独分布层和核心层时使用。
- 适用于较小的校园位置, 或由单个建筑组成的园区网。
- 也被称为折叠的核心网络设计。



27.2 Scalable Networks

扩展网络

扩展性是一个网络的术语，指网络增长的情况下不损失网络的可用性和可靠性。

为了支持大型、中型或小型网络，网络设计人员必须制定策略使网络可用且能够高效便捷地扩展。

基本的网络设计策略包括以下建议：

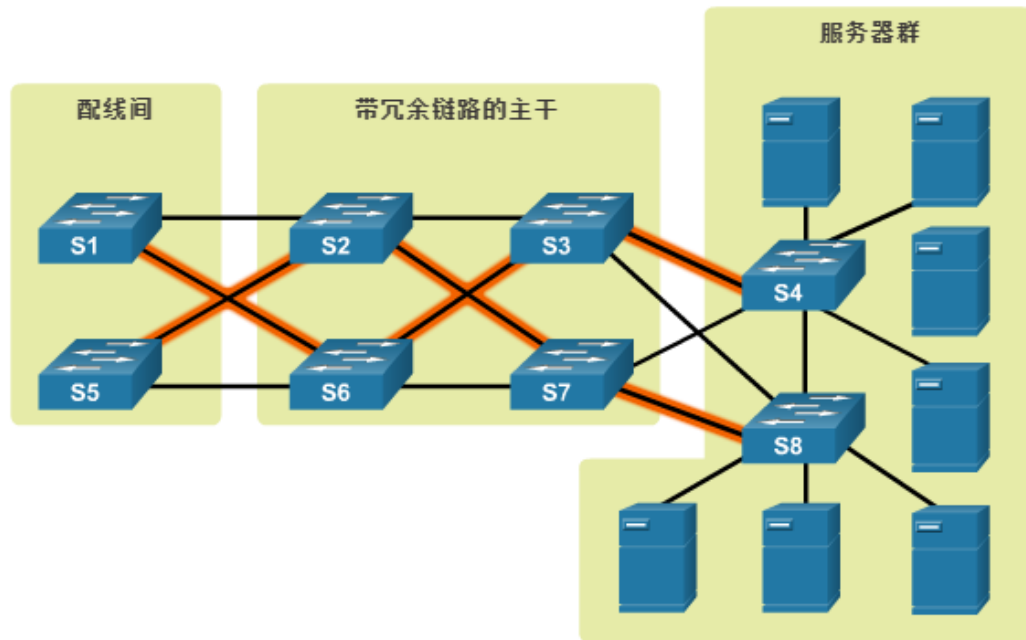
- 使用可扩展的模块化设备或群集设备，能轻松升级以增强性能。
- 设计分层网络来包含某些模块，可根据需要对模块进行添加、升级和修改，同时不影响对网络其他功能区的设计。
- 创建分层的IPv4或IPv6地址策略。
- 选择路由器或多层交换机，限制广播，过滤网络中其它不需要的流量。
- 使用第3层设备来过滤和减少到网络核心的流量。

使用方案：

- Redundancy
- Multiple Links
- Scalable Routing protocol

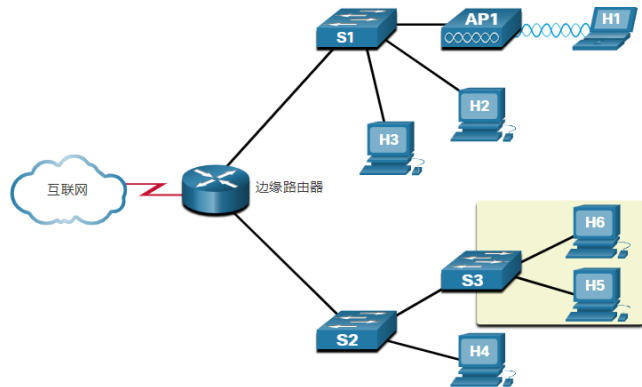
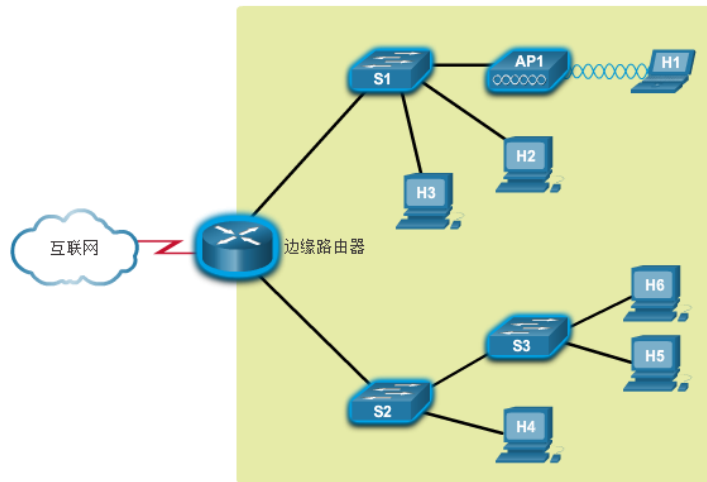
扩展网络 规划冗余

- 冗余功能是网络设计的重要部分，它通过减少单点故障的几率来防止网络服务的中断。
- 实施冗余的一种方法是安装重复设备并向关键设备提供故障切换服务。
- 实施冗余的另一种方法是冗余路径。交换网络中的冗余路径支持高可用性。然而，由于交换机的运行，交换以太网中的冗余路径可能会导致逻辑第 2 层环路。因此，需要使用生成树协议 (STP)。



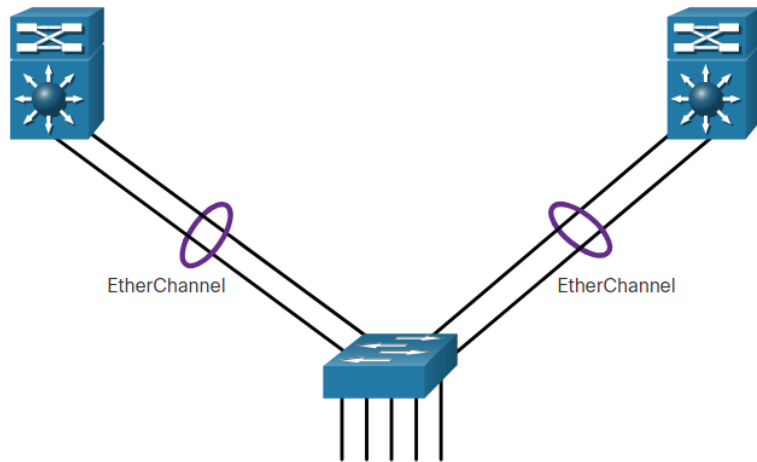
扩展网络 限制故障域的大小

- 设计优良的网络不仅可以控制流量，还可以限制故障域的大小。故障域是指在关键设备或网络服务出现问题时受影响的网络区域。
- 使用冗余链路和可靠的企业级设备可以将网络中断的几率降至最低限度。减小故障域可以降低故障对公司生产效率的影响。
- 减小故障域还可简化故障排除过程，从而缩短所有用户的停机时间。
- 路由器或多层交换机通常成对部署，接入层交换机均匀分布在这些成对设备中间。这种配置称为大楼或部门交换块。各交换块独立运作。这样，单台设备发生故障便不会造成整个网络瘫痪，甚至整个交换块的故障也不会影响到太多终端用户。



链路汇聚允许管理员通过创建一条由多个物理链路组成的逻辑链路来增加设备之间的带宽。EtherChannel 是交换网络中所使用的一种链路汇聚形式。

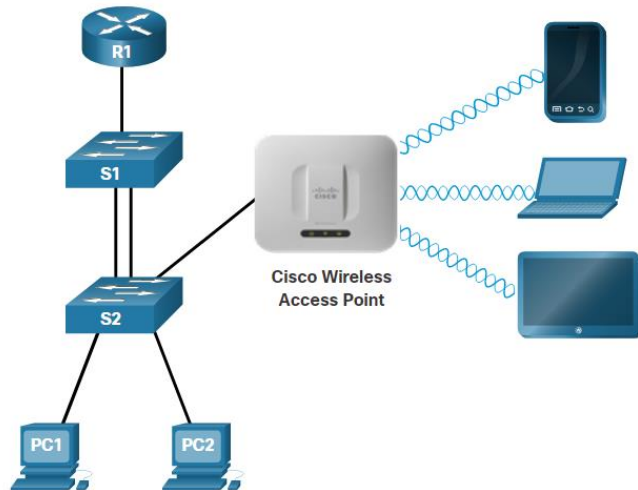
- EtherChannel 使用现有交换机端口;没有必要进行其他的花费来将链路升级为更快、更昂贵的连接。
- EtherChannel 被视为一条使用 EtherChannel 接口的逻辑链路。大多数的配置任务在 EtherChannel 接口(而不是在各个端口)上完成,这能确保链路中的配置一致。
- EtherChannel 配置利用了同一 EtherChannel 中链路间的负载均衡,并且可根据硬件平台实施一个或多个负载均衡方法。



扩展网络 扩展接入层

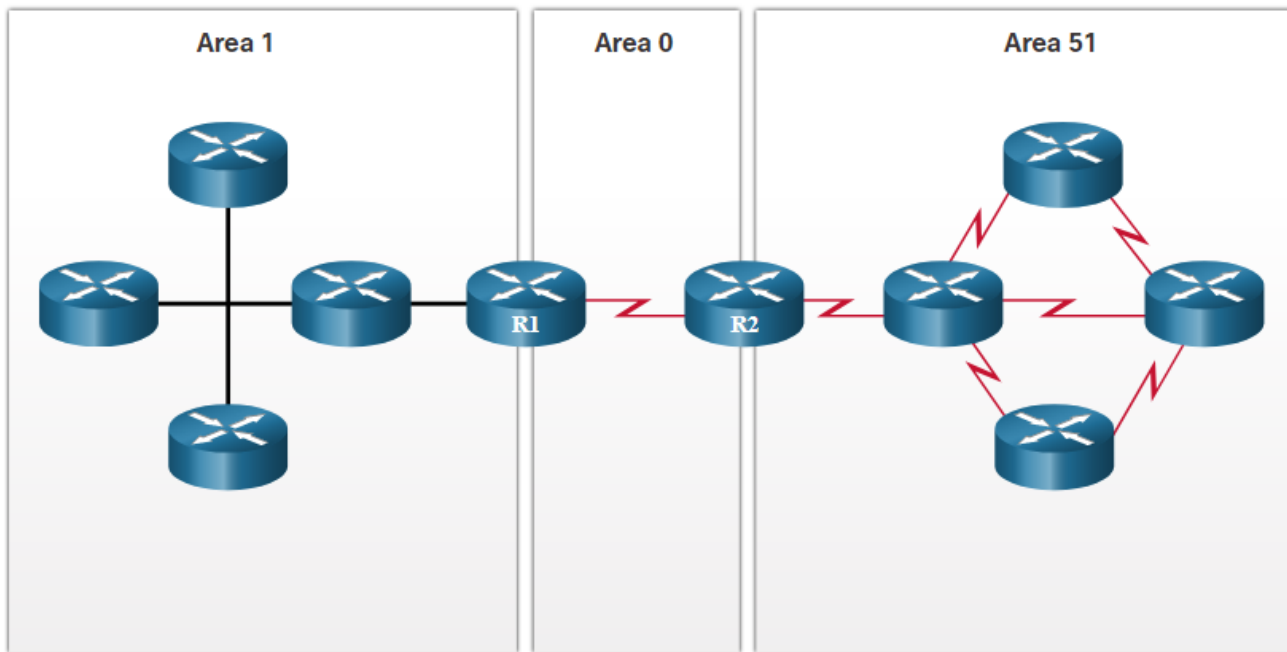
必须将网络设计为能够根据需要将网络访问扩展到个人和设备。扩展接入层连接的一个越来越重要的方面是通过无线连接。提供无线连接有许多优点，例如提高灵活性，降低成本，能够发展且适应不断变化的网络和业务需求。

要进行无线通信，终端设备需要配备无线网络接口卡（NIC），将无线电发射器/接收器以及所需的软件驱动程序集成在一起，使其可以正常工作。此外，如图所示，用户需要使用无线路由器或无线接入点（AP）才能进行连接。



扩展网络 调整路由协议

链路状态路由协议（例如开放最短路径优先 [OSPF]），非常适用于快速收敛具有重要作用的大型分层网络。OSPF 路由器会建立和维护与其他相连 OSPF 路由器的单个或多个邻居邻接关系。



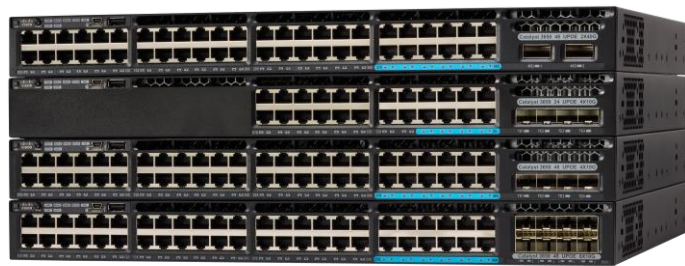
27.3 Switch Hardware

交换机硬件

交换机硬件 Switch 平台

在选择交换机之前，必须考虑各种交换机平台、形状因素和其他功能。在设计网络时，选择合适的硬件来满足当前的网络需求，并允许网络增长是很重要的。在企业网络中，交换机和路由器在网络通信中起着至关重要的作用。

区网交换机—如这里所示的Cisco 3850系列，以适合企业网络的速度和安全性支持高密度的用户连接。



云管理型交换机 - 思科 Meraki 云管理接入交换机支持交换机的虚拟堆叠。它们通过Web 监控和配置数千个交换机端口，而不需要现场 IT 人员的干预。



数据中心交换机-应该根据交换机构建数据中心，以提高基础架构的可扩展性、操作连续性和传输灵活性。数据中心交换机平台包括思科 Nexus 系列交换机和思科 Catalyst 6500 系列交换机。



运营商交换机 - 服务提供商交换机分为两类
汇聚交换机和以太网接入交换机。汇聚交换机是运营商级以太网交换机，它能够在网络边缘汇聚流量。服务提供商以太网接入交换机具备应用层智能、统一服务、虚拟化、集成安全性和简化管理功能。



虚拟网络 - 网络正变的越来越虚拟化。思科 Nexus 虚拟网络交换机平台通过将虚拟化智能技术添加到数据中心网络来提供安全的多用户服务。



交换机硬件 Switch 平台

在选择交换机时，网络管理员必须确定交换机的外形因素。这包括固定端口配置、模块化配置、堆叠式或非堆叠式。



交换机的厚度(以机架单元数表示)对于在机架中安装的交换机也很重要。比如图中所示的固定配置交换机的高度都是1机架单元(1U)或1.75英尺(44.45毫米)的。



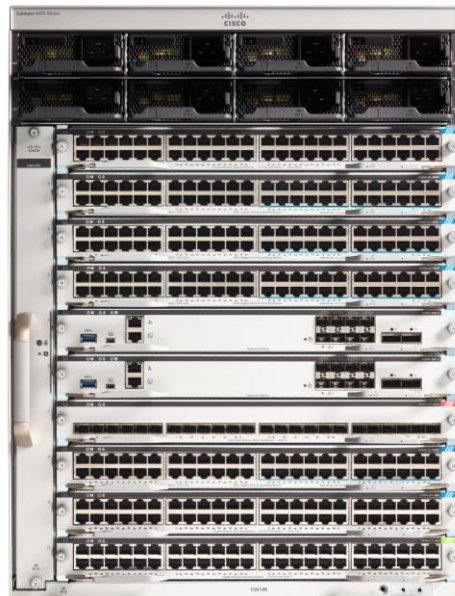
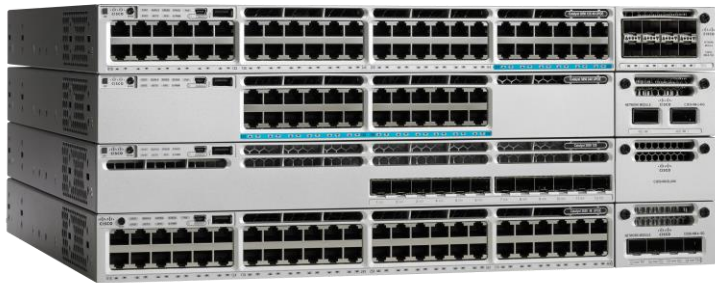
交换机硬件

端口密度Port Density

交换机的端口密度是指单个交换机上可用端口的数量。

非模块化配置交换机支持各种端口密度配置。思科 Catalyst 3850 24 端口交换机和 48 端口交换机。

模块化交换机可以通过增加多个交换机端口线卡来支持非常高的端口密度。模块化 Catalyst 9400 交换机可支持384个交换机端口。



转发速率Forwarding Rates

- 转发速率通过标定交换机每秒能够处理的数据量来定义交换机的处理能力。
- 如果交换机的转发速率太低, 则它无法支持在其所有端口之间实现全线速通信。线速是指交换机上每个以太网端口能够达到的数据速率。数据速率可达 100 Mb/s、1 Gb/s、10 Gb/s 或 100 Gb/s。
- 接入层交换机通常不需要全线速运行, 因为它们实际上会受到通往分布层的上行链路的限制。
- 分布层和核心层可以使用价格更高、性能更高的交换机。

24 端口千兆以太网交换机



能够交换 24 Gb/s 的流量

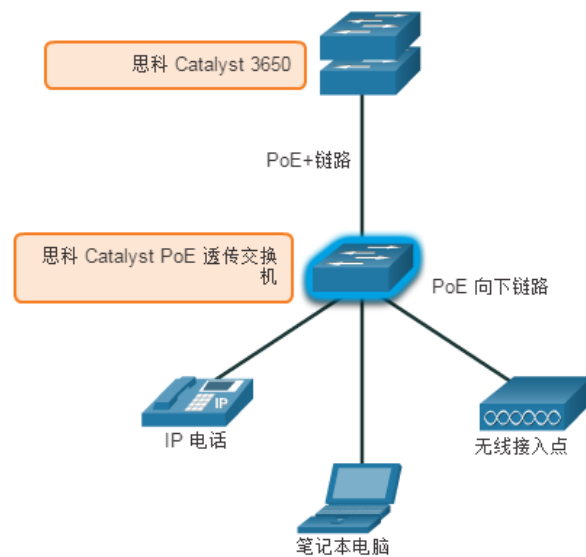
48 端口千兆以太网交换机



能够交换 48 Gb/s 的流量

交换机硬件 以太网供电 Power over Ethernet

- 以太网供电 (PoE) 允许交换机通过现有的以太网电缆对设备进行供电。可通过 IP 电话和某些无线接入点来使用此功能。
- PoE 大大提高了安装无线接入点和 IP 电话时的灵活性，允许它们在所有存在以太网电缆的地方进行安装。
- 网络管理员应该确保 PoE 功能是必需的，因为支持 PoE 的交换机非常昂贵。



多层交换Multilayer Switching

- 多层交换机通常部署在组织交换网络的核心层和分布层。多层交换机的特点是它们能够构建路由表，支持一些路由协议并转发 IP 数据包，其转发速率接近第 2 层转发速率。多层交换机通常支持专用硬件，例如专用集成电路（ASICs）。ASIC 与专用软件数据结构配合使用可简化与 CPU 无关的 IP 数据包的转发。
- 网络中存在向纯第 3 层交换环境发展的趋势。在网络中首次使用交换机时，没有一台交换机支持路由；但是现在，几乎所有交换机都可支持路由。不久之后，可能所有的交换机都会集成路由处理器，因为相对于其他限制而言，这样做的成本可降低。



选择交换机的商业考虑

- 成本 - 交换机的成本取决于接口的数量和速度、支持的功能和扩展能力。
- 端口密度 - 网络交换机必须支持网络中相应数量的设备。
- 电源 - 通过以太网供电 (PoE) 为接入点、IP 电话, 甚至紧凑型交换机供电现在都很常见。除了考虑使用 PoE 外, 一些机箱式交换机支持冗余电源。
- 可靠性 - 交换机应提供对网络的持续访问。
- 端口速度 - 网络连接的速度是最终用户关注的主要问题。
- 帧缓冲区 - 交换机存储帧的能力在可能存在通往服务器或网络其他区域的拥塞端口的网络中非常重要。
- 可扩展性 - 网络中的用户数量通常随时间增长; 因此, 交换机应提供增长的机会。

27.4 Router Hardware

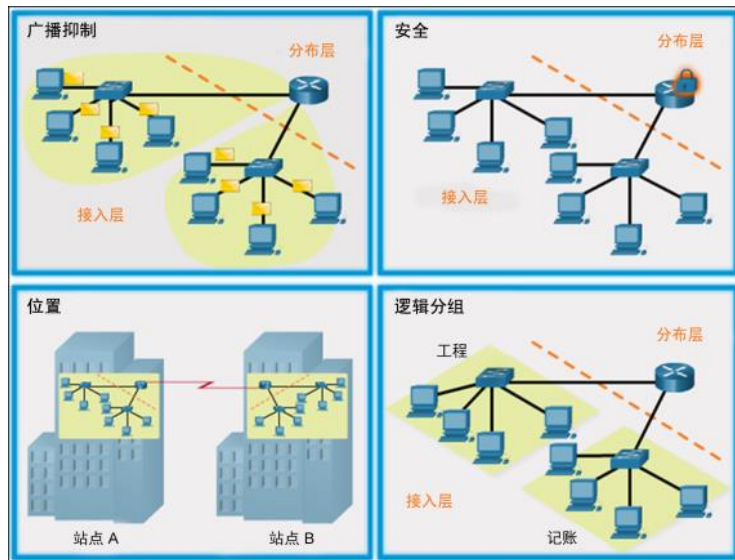
路由器硬件

路由器硬件 路由器需求

- 路由器在网络中扮演着重要的角色，它将家庭和企业连接到互联网，将企业网络内的多个站点连接在一起，提供冗余路径并通过互联网连接 ISP。它们也可用作不同类型介质和协议之间的转换器。
- 路由器使用目的 IP 地址的网络部分来将数据包路由到适当的目的地。如果链接或路径断开，它们会选择替代路径。本地网络中的所有主机都会在自己的 IP 配置中指定本地路由器接口的 IP 地址。该路由器接口即为默认网关。有效路由以及网络链路故障恢复的能力对于传递数据包到目的地极为关键。

路由器还具有其它一些有用的功能：

- ✓ 广播限定功能
- ✓ 连接远程地点
- ✓ 按应用或部门对用户进行逻辑分组
- ✓ 提供更强的安全性



分支机构路由器 - 分支机构路由器可优化单一平台上的分支机构服务，同时在分支机构和 WAN 基础架构上提供最佳应用体验。要最大限度地提高分支机构的服务可用性，网络需要能够全天候正常运行。高度可用的分支网络必须确保能够从传统故障中快速恢复，同时尽量减少或消除对服务的影响，并提供简单的网络配置和管理。

Cisco Integrated Services Router (ISR) 4000 Series Routers.



路由器硬件

Cisco Routers (Cont.)

网络边缘路由器 - 网络边缘路由器使网络边缘能够提供高性能、高安全性和可靠的服务，用于联合园区、数据中心及分支机构网络。

Cisco Aggregation Services Routers (ASR) 9000 Series Routers.



Cisco Routers (Cont.)

服务提供商路由器 - 服务提供商路由器可区分服务产品组合，并通过提供端到端的可扩展解决方案及用户感知服务来增加收入。运营商必须优化运营、降低费用并提高可扩展性和灵活性，以便于在所有的设备和位置上提供下一代互联网体验。

Cisco Network Convergence System (NCS) 6000 Series Routers.



Door Closed



Door Open

路由器硬件

Cisco Routers (Cont.)

工业路由器-设计用于在恶劣的环境中提供企业级功能。
Cisco 1100 Series Industrial Integrated Services Routers.



路由器硬件

Router Form Factors

Cisco 900 Series:这是一个小型的分支办公室路由器。它将广域网、交换、安全和高级连接选项结合在一个面向中小型企业的小型无风扇平台中。



路由器硬件

Router Form Factors

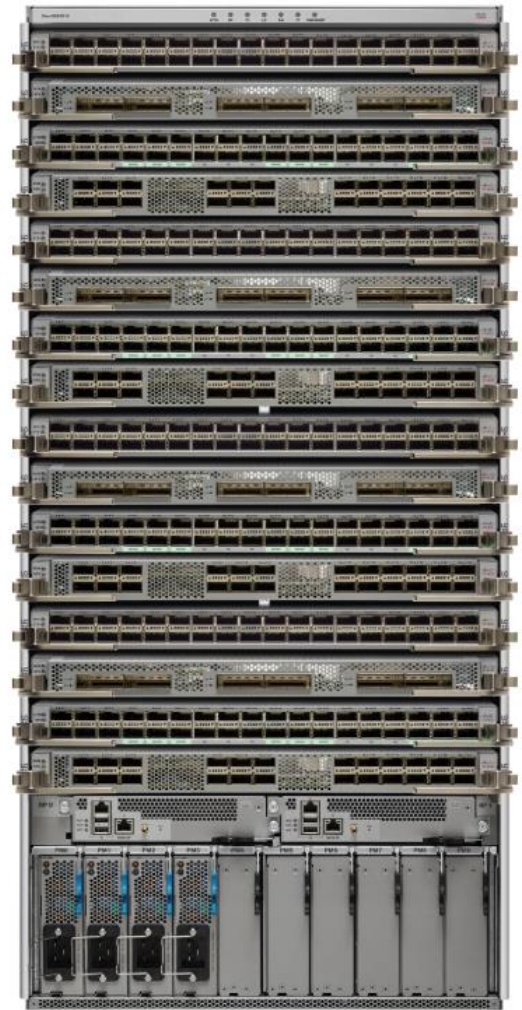
Cisco ASR 9000 and 1000 Series Aggregation Services Routers: 这些路由器为可扩展的网络边缘提供可编程的密度和弹性。



路由器硬件

Router Form Factors

Cisco Network Convergence System 5500 Series Routers: 这些路由器被设计成在大型数据中心和大型企业网络、web、服务提供商广域网和聚合网络之间高效扩展。



路由器硬件

Router Form Factors

Cisco 800 Industrial Integrated Services Router: 该路由器结构紧凑，专为恶劣环境设计。



