

# 第 1 篇 园区网概述

---

## 第 1 章 企业网模型

## 第 2 章 园区网的网络模型发展历程

## 第 3 章 典型园区网的业务部署

# 第1章 企业网模型

随着应用的发展，各种需求不断出现。作为企业 IT 系统基础的计算机网络，其未来的发展必须适应企业业务和应用对 IT 系统越来越高的要求。

本章将介绍 H3C 面向服务的 IToIP 解决方案，并给出指导企业网络构建的层级化网络模型和模块化企业网架构。

## 1.1 本章目标

### 课程目标

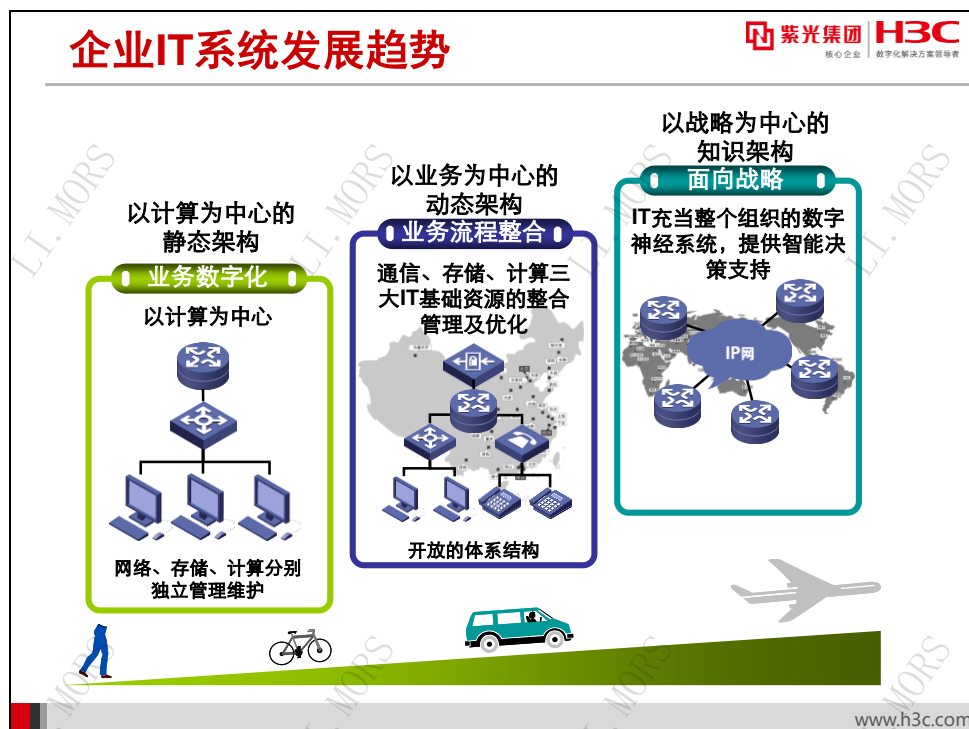
● 学习完本课程，您应该能够：

- 描述IToIP面向服务的解决方案
- 描述层级化网络模型
- 描述典型企业网结构
- 描述H3C模块化企业网架构



www.h3c.com

## 1.2 趋势和挑战



信息技术发展至今，包括企业在内的各种组织几乎都已部署了各种各样的 IT 系统，这些系统大部分基于各种类型的计算机网络。应对企业不断发展的需求，IT 系统也处于不断的发展进化之中。

IT 系统的发展可分为业务数字化、业务流程整合及面向战略三个阶段：

- **业务数字化**：在这个阶段，IT 应用主要集中在业务流程数字化和办公自动化等以数字化代替人工操作的方面。从技术架构来看，此时的 IT 系统以计算为中心，计算、存储和应用呈现出静态绑定的关系。应用依赖于特定厂商、特定型号的计算、存储设备。IT 资源为满足业务应用的峰值需求而配置，其平均利用率则很低，造成 IT 投资的严重浪费；网络、存储、计算分别独立管理维护，管理复杂，维护难度高，过度依赖于原厂商提供的服务；系统扩展性差，难以快速适应机构内部和外部挑战带来的变化。这一阶段的网络技术也呈现纷繁复杂的局面，存在多种互不兼容的协议体系，例如用于 Novell 文件和打印共享的 IPX/SPX（Internet Packet eXchange/Sequential Packet eXchange，网间分组交换/序列包交换），用于 IBM 大型机和服务器的 SNA（Systems Network Architecture，系统网络体系结构），以及用于访问 Internet 的 TCP/IP（Transfer Control Protocol/ Internet Protocol，传输控制协议/互联网协议）等。
- **业务流程整合**：以客户为中心的业务流程整合，需要打破部门壁垒，实现如 ERP、集成供应链、客户关系管理、营销管理、产品研发管理等业务流程整合。业务需求催生出以业务为中心的动态 IT 架构，这种架构有两大特征，一是能够实现通信、存储、计

算三大 IT 基础资源的整合管理及优化；二是具备开放的体系结构，可满足业务流程定制与优化的要求。而今天的网络系统也正在发展为基于 IP 的统一平台，这种开放架构可以大幅度降低 IT 系统的复杂度，提高性能和兼容性。例如，基于 IP 的网络和存储协同优化可以提高 IT 整体性能 50% 以上。

- 面向战略：未来的 IT 系统将发展为以战略为中心的知识系统，业务战略与 IT 战略将融为一体，成为整个组织肌体的一部分。IT 将充当整个组织的数字神经系统，提供智能决策支持。计算机网络必须适应这一发展趋势，不仅提供网络连通性，提高性能和可靠性，更要为 IT 系统上层应用提供灵活而智能的服务。

## IT系统面临的挑战

紫光集团 H3C  
核心企业 数字化转型领导者

- IT资源整合
  - 包括通信、计算、存储等在内的基础资源的整合
- IT管理
  - 内容管理
  - 流量管理
  - 安全管理
  - 配置管理
- IT业务个性化
  - 传统IT设施难以提供企业所需的灵活性、智能性和个性化

www.h3c.com

当今的 IT 系统正在从业务数字化阶段向业务流程整合阶段的过渡。一方面，经过多年的建设，IT 系统为组织机构带来高效率、低成本的好处；另一方面，面临业务流程整合的压力，组织机构在 IT 资源整合、IT 资源管理和 IT 业务个性化等方面都面临重大挑战。

### IT 资源整合

设想一个涵盖总部到分支机构的大规模企业 IT 系统。企业不断采用新技术来扩充 IT 基础设施。例如，采用基于传统 PBX（Private Branch eXchange，私有分支交换）交换机的语音系统；采用基于 IPX/SPX 的网络实现内部文件服务器和打印机共享；在桌面部署 IP 协议以实现 Internet 访问；采用从早期的 X.25、帧中继（Frame Relay）、T1/E1 专线，到 ATM

（Asynchronous Transfer Mode，异步传输模式）等各种技术构建广域网，连接分支机构；采用独立的基于专线的专用网络实现视频电话和会议；采用基于模拟信号传输、单机硬盘存储的传统监控系统；采用专用光纤、专用存储交换机和专用协议构建存储区域网，部署存储系统等等。

这样的 IT 设施条块分割，无法实现协同办公和协同商务。例如，语音网、视频会议网、数据通信网、监控信号传输网、存储网络等并立，企业在部署大量线路的同时，还无法在各系统之间共享数据；由于多种协议共存，难以互相兼容，各应用系统之间的互通极为昂贵和困难，效率低下；并且在一部分系统网络资源不足的情况下，另一部分系统的网络资源却可能闲置浪费。

因此，包括通信、计算、存储等在内的基础资源的整合是 IT 系统建设面临的难题之一。

### IT 管理

在业务流程整合的阶段，IT 管理需要从简单的网管管理转向全面的资源管理及业务管理。优化 IT 资源，提高 IT 的 ROI（Return On Investment，投资回报率），需要更加精细的管理能力。

当前计算机网络系统面临的主要管理难点主要包括：

- 内容管理：对各种信息资源和 Internet 访问的便捷性，在提高工作效率的同时，也可能导致员工有效工作时间的降低。例如员工与工作无关的 Internet 访问不但浪费了工作时间，而且加重了网络负担。控制员工的此类行为成为一个管理难点。
- 流量管理：计算机网络承载了越来越多的实时业务和生产相关的关键业务，某些节点极可能成为网络的瓶颈。深度的业务识别、实时动态的流量监控和调节、网络资源优化配置成为当务之急。
- 安全管理：由于业务的多样性和网络的开放性，各种各样的攻击威胁着 IT 系统。加上承载网络日趋归一，IT 系统面临的威胁也日益加重。包括接入安全、内容安全、网络安全、存储安全等在内的整体安全性成为一个关键问题。
- 配置管理：随着企业规模的扩大，大量的网络设备需要广域互连。一旦需要变更配置，位于分支网点的大量设备要在短时间内进行全面的配置变更或升级。如何此类业务批量部署和配置成为一个难题。

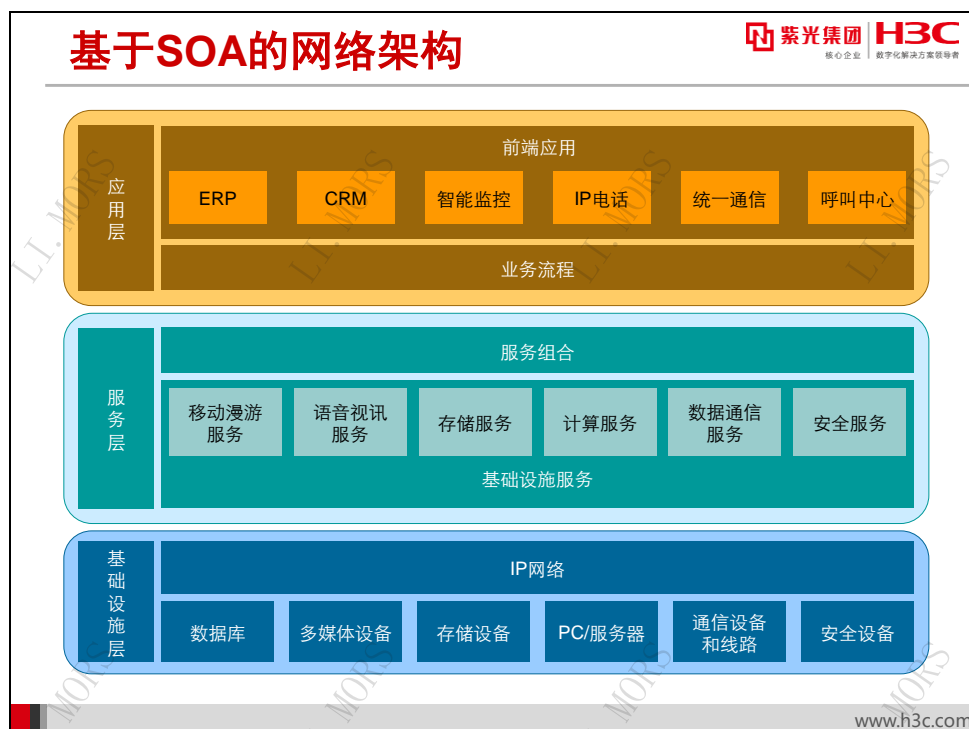
综上所述，组织机构不但需要不断提高网络性能，更需要构建可维护、可管理、可优化的品质网络。要解决各种难题，实现这个目标，就需要构建一个全面、精细、架构开放的智能管理系统。

### IT 业务个性化

自工业革命以来，世界经济商务关系和模型发生巨变，经历了从生产为中心到顾客为中心；从大规模标准化生产到大规模客户个性化定制的转变。传统的 IT 设施难以提供企业为大批量用户提供个性化、定制化和优化方案所需的灵活性和智能性。

此外，组织机构的 IT 系统正从单一应用的集合体转向业务流程整合。每个组织都有与自身战略紧密相关的特色业务，并希望获得个性化的 IT 解决方案。这要求计算机网络由解决基本通信需求向灵活服务于上层的个性化应用进行转变。建设一个技术标准而开放的网络，实现通信、计算、存储等各种资源的整合、管理与优化是解决问题的关键。

## 1.3 IToIP面向服务的解决方案

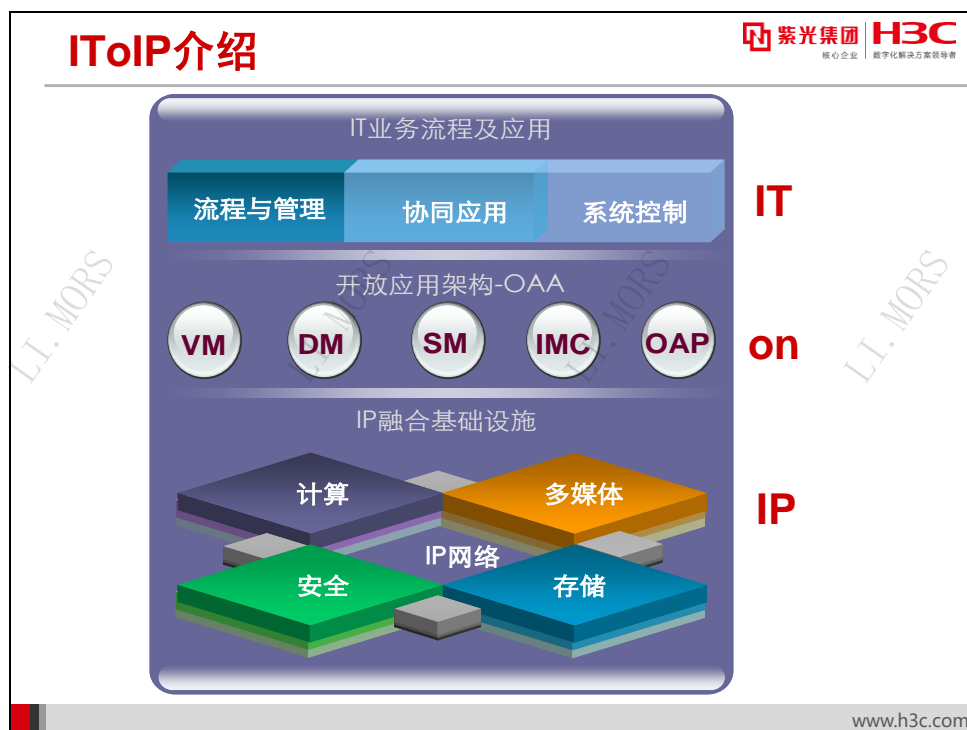


SOA（Service Oriented Architecture，面向服务的体系结构）是一种定义和提供 IT 基础设施的方式。体现 SOA 思想的企业级 IT 系统设计，应允许不同应用功能或应用系统之间共享数据、资源和能力，参与业务流程，无论它们各自背后使用的是何种软件和硬件。

基于 SOA 的网络架构将企业 IT 系统划分成若干层次：

- **基础设施层：**在这一层中，分布与各个逻辑和物理位置的资源通过统一而标准化的计算机网络被连接起来，形成 IT 系统的基础设施。所有资源在任意地点都可以被随时访问。
- **服务层：**这一层将基础的设施和资源结合起来，形成一系列灵活而相对独立的基础设施服务，例如计算服务、安全服务、存储服务等。基础设施服务不包含业务逻辑，其提供的是非业务性的功能。若干基础设施服务可以进一步形成服务组合。一个服务组合可以实现一项组合的业务任务。任何新的业务任务均可以方便地由基础设施服务组合而成，而无须改变已有的服务组合。
- **应用层：**企业的业务流程实际上可以由一系列的业务任务或复合业务任务构成，也就是说，任何复杂应用均可以通过调用一系列服务组合接口来实现。

依托 SOA 思想设计的企业级网络系统，允许灵活、快速、高效地构建企业智能应用，能快速适应企业业务流程的变化。



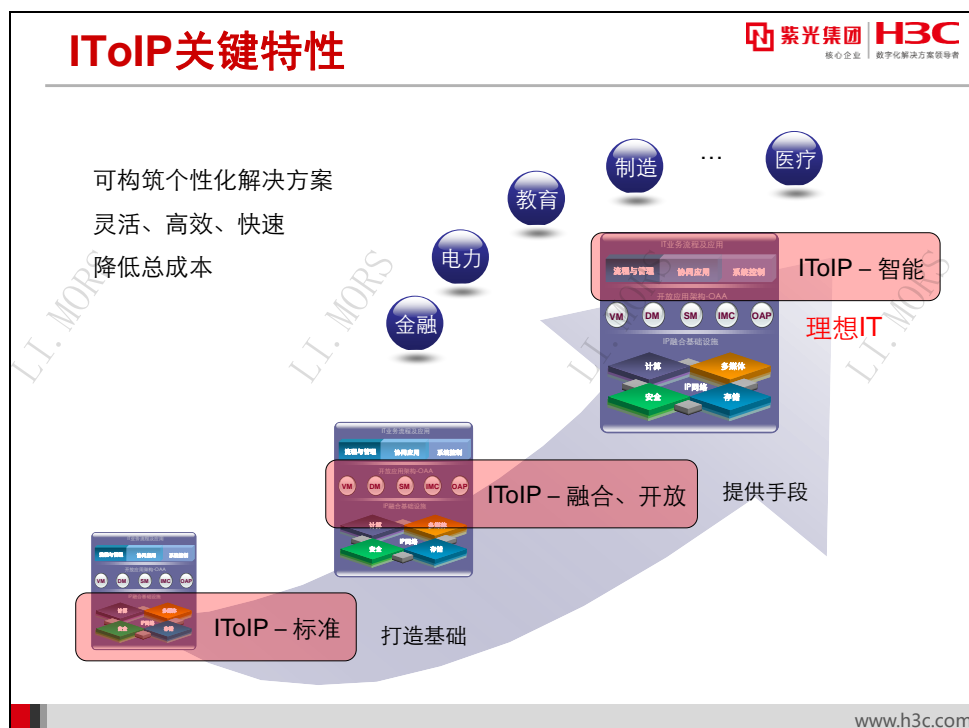
为解决 IT 系统和计算机网络发展过程中面临的种种挑战，H3C 在 2004 年提出了 NGen（下一代 e 网）架构。基于这个架构，H3C 不断完善 IP 基础网络、IP 通信、IP 管理、IP 存储等解决方案板块，最终形成完全基于 IP 技术的新一代 IT 解决方案——IToIP（IT on IP）。

IToIP 是 SOA 核心思想的一种表现形式。IToIP 通过一个开放的架构把先进的技术及客户需求统一为一个整体，使技术手段及商业方法最终都能服务于用户及合作伙伴，所有这些都能最大限度地满足用户的业务需求。

IToIP 解决方案要求对 IT 基础架构进行整合。其含义是基于 IP 技术搭建统一的 IT 基础架构平台，以 IP 网络为基础，消除异构系统带来的信息鸿沟，整合 IP 存储、安全、多媒体等各种服务，实现 IT 基础设施的构件化和资源化。

IToIP 以智能的业务管理衔接应用与 IT 基础平台，从而实现基于业务的底层资源配置和管理。IToIP 以开放架构完成 IT 应用层和 IT 基础资源层的完美对接，使得 IT 系统真正成为用户的价值平台。

当今的 IT 系统建设进入整合时代，需求的重心从单系统的性能转向跨系统的性能、连通、业务互动。依托 IP 网络融合 IT 基础架构，提供整合平台，实现基础架构资源化，基于应用灵活组织 IT 资源来支撑复杂多变的业务，这些已经成为 IT 系统建设中普遍认同的理念。IToIP 解决方案指明了实现这一目标的途径，给出了达到这样目标的方案，使组织机构得以全面而系统地规划，并有序而分步地部署 IT 系统。

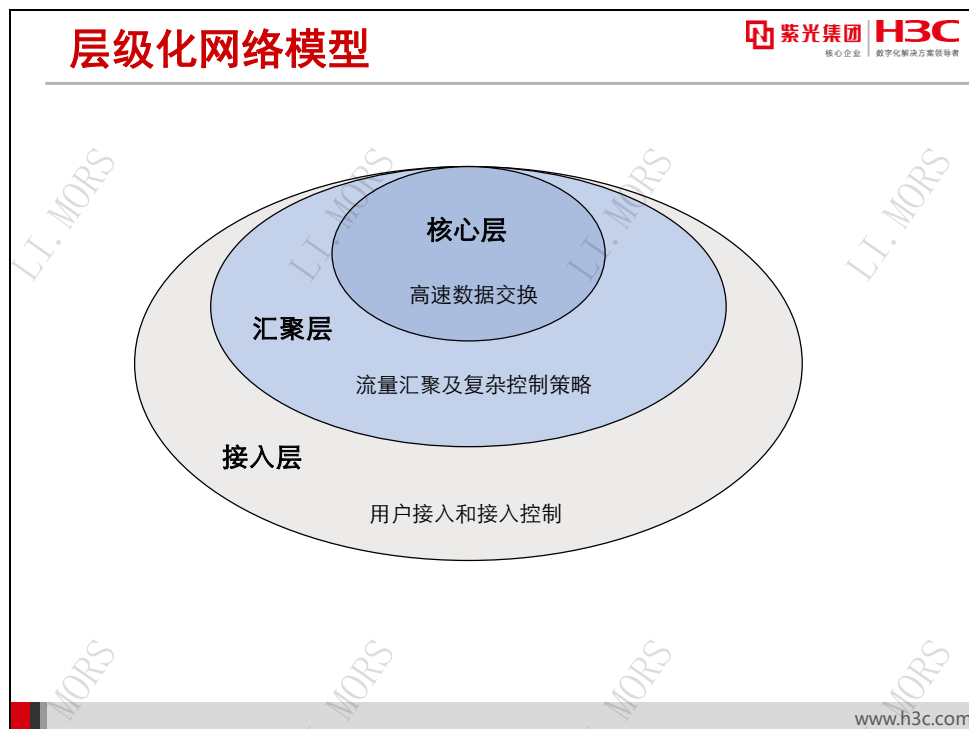


IToIP 解决方案具备以下关键特性：

- **标准**——IToIP 理念的实现首先指向 IT 基础设施的标准化。从技术的发展趋势来看，IP 已成为计算机网络的事实标准，IT 系统以 IP 网络为基础设施是一个清晰而不可置疑的发展方向。标准化是其他一切特性的前提。H3C 基于 IP 的全系列数据通信网络产品完全实现了标准化的特性。
- **融合**——在标准化实现之后，基于标准的 IP 基础设施，各种 IT 资源可以方便地共享和使用，通信、计算、存储、网络等各种技术和应用进一步实现融合。H3C 推出的包括统一通信、存储、监控、数据中心、安全等一系列解决方案是实现这一特性的坚实基础。
- **开放**——在同构的 IT 基础设施之上的中间件及开放平台可以提供行业应用定制的接口，实现了应用和基础架构上的分离。H3C OAA（Open Application Architecture，开放应用体系结构）开放合作计划正是为实现这一目标而推出的。
- **智能**——应用可以通过开放的接口来动态调用 IT 资源，最终为用户构建一个标准、兼容、安全、智能和可管理的 IT 应用环境。基于 IP 标准对 IT 基础架构进行整合，通过开放的手段，为各行各业构筑灵活、高效、快速、低成本、个性化的 IT 解决方案，实现智能化的 IT 系统，这是 IToIP 持续演进的目标。



## 1.4 层级化网络模型



现代网络设计普遍采用了层级化网络模型。层级化网络模型将网络划分为三层，在层级化网络模型中，每一层都定义了特定而必要的功能，通过各层功能的配合，可以构建一个功能完善的 IP 网：

- **接入层：**这一层提供丰富的端口，负责接入工作组用户，使其可以获得网络服务。接入层还可以对用户实施接入控制。
- **汇聚层：**这一层通过大量的链路连接接入层设备，将接入层数据汇集起来。同时，这一层依据复杂的策略对数据、信息等实施控制。其典型行为包括路由聚合和访问控制等。
- **核心层：**这一层是网络的骨干，主要负责对来自汇聚层的数据进行尽可能快速的交换。

理论上，即使目前最大规模的网络，其网络设计也不超过 3 个层次。小型或者中型网络设计可以根据情况合并某些层次的功能，将网络层次减少到 1~2 层。

## 接入层

- 为用户提供网络的访问接口
- 丰富大量的接口
- 接入安全控制
- 接入速率控制、基于策略的分类、数据包标记等
- 较少考虑冗余性

紫光集团 H3C  
核心企业 数字化转型领导者

www.h3c.com

接入层处于网络的最底层，负责接入终端用户。接入层为用户提供网络的访问接口，是整个网络的对外可见部分，也是用户与网络的连接场所。因此接入层应具有种类丰富的大量端口，提供强大的接入能力。接入安全性也是一个必须考虑的因素。


一方面，如果接入层设备或链路出现故障，只会对设备接入的用户造成影响，影响范围较小；另一方面，接入层设备和连接数量相对较多，用户设备数量也比较多，不便于一一实现设备和链路冗余。因此，通常不考虑接入层设备和链路的冗余性。当然，如果接入层设备接入了重要用户或服务器，可以采用链路或设备冗余来提高其可靠性。

另外，由于接入层是用户与网络的接入点，也是入侵者试图闯入的地方，因此可以在访问接入层实施安全接入控制策略，以保障网络的安全。例如通过 802.1X 这样的端口安全技术防止非法用户接入网络，或采用包过滤技术过滤伪造源地址的数据包，阻止利用伪造地址方式实施的攻击。

在接入层还可以实现对数据的分类和标记。接入层直接为用户提供多样的服务，在用户数据进入网络时，可以立即控制其流量，进行基于策略的分类，并给以适当的标记。这样网络中的其它设备就可以根据这些标记直接为这些数据提供适当的 QoS（Quality of Service，服务品质）服务。

## 汇聚层

- 将接入层数据汇集起来，依据策略对数据、信息等实施控制
- 必要的冗余设计
- 复杂的策略配置
  - 包括路由策略、安全策略、QoS策略等



核心企业 数字化转型领导者

www.h3c.com

汇聚层处于三层结构的中间。汇聚层设备是大量接入层设备的集中点，负责汇集来自接入层的数据，并对数据和控制信息进行基于策略的控制。


汇聚层从位置上处于核心层与接入层的分界，面对大量来自接入层的链路，汇聚层必须将其数据汇集在一起，通过少量的高速链路传递给核心层。这样可以减少昂贵的高端设备接口，提高网络转发效率。

如果不采用冗余设计，则某台汇聚层设备或某条汇聚层链路的失效将导致其下面连接的所有接入层设备用户无法访问网络。因此，汇聚层设备的可靠性较为重要。考虑到成本因素，汇聚层往往采用中端网络设备，并采用冗余链路连接核心层和接入层设备，提高网络可靠性。必要时也可以对汇聚层设备采用设备冗余的形式提高可靠性。

汇聚层还负责实现网络中的大量复杂策略，这些策略包括路由策略、安全策略、QoS 策略等等。通过适当的地址分配并在汇聚层实行路由聚合，可以减少核心层设备的路由数量，并以汇聚层为模块，对核心层实现网络拓扑变化的隔离，这不但可以提高转发速度，而且可以增强网络的稳定性。在汇聚层配置安全策略可以实现高效部署和丰富的安全特性。基于接入层设备提供的数据包标记，汇聚层设备可以为数据提供丰富的 QoS 服务。

## 核心层

- 对来自汇聚层的数据进行尽可能快速的交换
- 强大的数据交换能力
- 稳定、可靠的高冗余设计
- 不配置复杂策略



核心企业 数字化转型领导者

www.h3c.com

核心层处于网络的中心，负责对网络中的大量数据流量进行高速交换转发。网络中各部分之间互相访问的数据流都通过汇聚层设备汇集于核心层，核心层设备以尽可能高的速度对其进行转发。

核心层的性能会影响整个网络的性能，核心层设备或链路一旦发生故障，整个网络就面临瘫痪的危险。因此在选择核心层设备时，不仅要求其具有强大的数据交换能力，而且要求其具有很高的可靠性。通常应选择高端网络设备作为核心层设备。这不仅是因为高端设备的数据处理能力强，转发速度快，也是因为高端设备本身通常具有高可靠性设计。高端网络设备的主要组件通常都采用冗余设计，例如采用互为主备的双处理板、双交换网板、双电源等，确保设备不易宕机。而核心层链路多采用高速局域网技术，确保较高的速率和转发效率。


为了确保核心网络的可靠性，可以对核心层设备和链路实现双冗余甚至多冗余，实现网状、环型，或部分网状拓扑。即对核心层设备和链路一律增加一个以上的备份，一旦主用设备整机或主用链路出现故障，立即切换到备用设备或备用链路，确保核心层的高度可靠性。

由于网络策略对网络性能会产生不可避免地影响，因此在核心层中不能部署过多或过于复杂的策略。通常在核心层较少采用任何降低核心层设备处理能力，或增加数据包交换延迟时间的配置，尽量避免增加核心层路由器配置的复杂程度。通常只根据汇聚层提供的信息进行数据转发。

核心层对网络中每个目的地应具备充分的可达性。核心层设备应具有足够的路由信息来转发去往网络中任意目的的数据包。这一要求与加速转发的要求是互相矛盾的，因此应在汇聚层采用适当的路由聚合策略来减少核心层路由表大小。

## 层级化网络模型的优点

- 网络结构清晰
- 便于规划和维护
- 增强网络稳定性
- 增强网络可扩展性



核心企业 | 数字化转型领导者

www.h3c.com

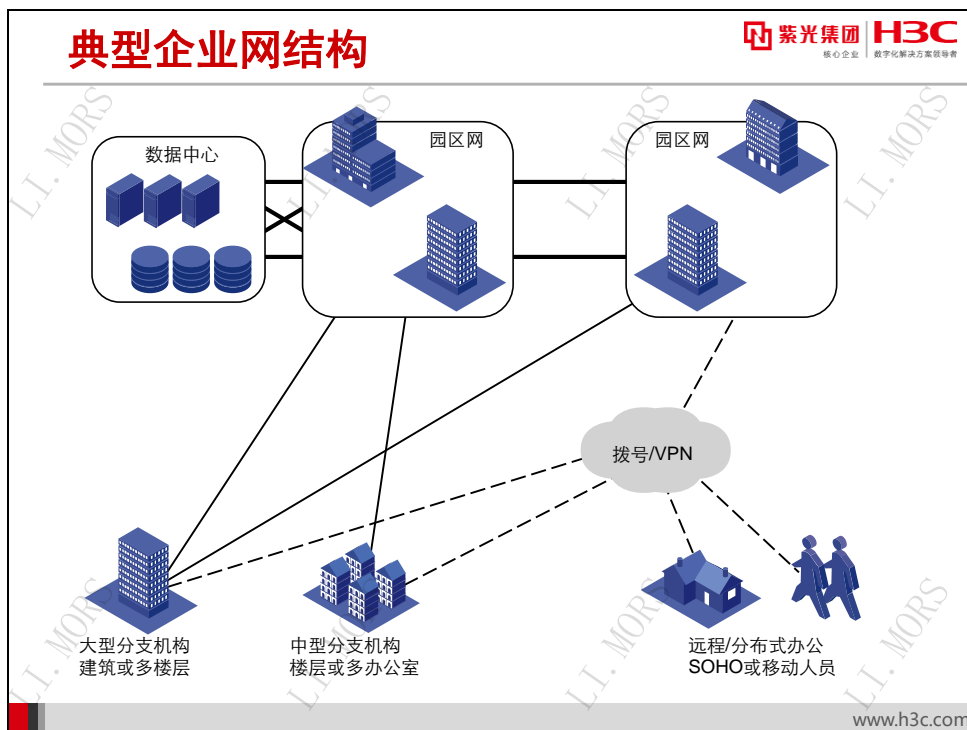
层级化网络模型的引入具有以下优点：

- 网络结构清晰化：网络被分为具有明确功能和特性的三个层次，使原本复杂无序的网络结构显得更加清晰，易于理解和分析。
- 便于规划和维护：清晰的结构和明确的功能特性定义使网络的规划设计更加合理，管理维护更加方便。
- 增强网络稳定性：三个层次之间各有分工，彼此相对独立，网络变化和故障的影响范围可以被降至最低，网络稳定性大大增强。
- 增强网络可扩展性：层级化网络模型使网络性能大大提高，功能分布更为合理，大大增强了网络的扩展能力。

当然，层级化网络模型只是个一般性的参考模型。在设计部署具体的网络时，还必须依据用户的实际需求进行具体分析。例如，某组织的全部业务都非常关键，不允许长时间中断，这就要求在整个网络中所有可能的位置都实现冗余；而某公司的业务并不严格依赖于网络，可靠性要求不高，则整个网络中的所有环节可能都无需实现冗余。

## 1.5 H3C企业网架构

### 1.5.1 典型企业网结构



典型的企业网由下列部分组成：

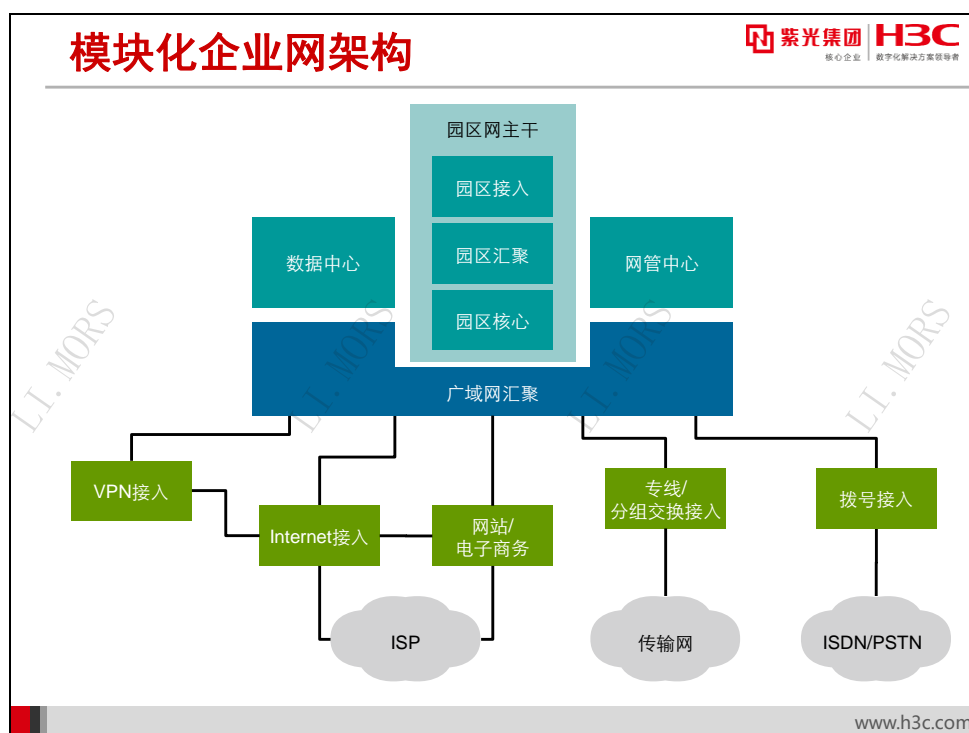
- **园区网**：园区网通常是大型企业网络的核心，每个园区包括若干建筑物。园区网通常采用包括核心层、汇聚层和接入层在内的 3 层网络结构。园区每一建筑内的网络都包括汇聚层和接入层，在汇聚层采用性能较高的三层交换机实现建筑内的汇聚；在接入层使用楼层交换机连接到桌面计算机。各建筑网络通过高速局域网技术连接到高性能的园区网核心层设备上。园区网之间通过高速城域网或广域网进行连接。
- **大型分支机构网**：这种机构通常是区域性的行政中心，可能独占一栋大楼或占据大楼中的多个楼层。其自身可能采用 2~3 层网络结构。其接入层和汇聚层与园区内的建筑网类似。大型分支机构网通常需要使用性能较好、可靠性较高、支撑业务较丰富的路由器，通过高速专线连接到核心园区网。
- **中型分支机构网**：多个中型分支机构，可能独占一个楼层或几个办公室。通常采用包括汇聚层和接入层的 2 层网络结构，使用中低端网络设备，通过专线连接到核心园区网或大型分支机构网。
- **小型分支机构网和远程/分布式办公人员**：可能是拥有几个人员的一个办公室，或在家中办公的 SOHO 人员，或出差在外的移动办公人员等。这些人员根据其需求通过拨号、VPN 等技术连接到园区网或适当的分支机构。小型分支机构可能部署一台路由器和简单的局域网，SOHO 和移动办公人员则直接使用其桌面 PC 或便携式计算机。

- **数据中心：**由高性能存储设备和服务器群构成，通常在物理上位于园区网或大型分支机构中，使用高速以太网技术连接到网络骨干。

各种规模的企业网可能由不同数量的上述网络和人员构成。例如，一个大型企业网可能由1个研发园区网、1个生产园区网、2个分别位于北京和上海的大型分支机构网、30个位于各大城市的中型分支机构网、200个小型分支机构网和数百名经常在外移动的商务人员构成。而一个中型企业可能由位于总部大楼的大型分支机构网和位于各主要城市的几十个小型分支机构网和几十名移动商务人员构成。

### 1.5.2 H3C 模块化企业网架构

为了更好地设计、部署、维护、管理企业网，必须理解 H3C 模块化企业网架构。



典型大型企业网以园区网为核心。根据网络各部分功能和特点的不同，企业网可以被划分为下列模块：

- **园区网主干：**提供园区各个信息点的接入，并作为整个企业网的核心，提供其他各个模块的互联。此模块又可分为下列子模块：
  - ◆ **园区网接入：**这一模块实际上分散于园区各建筑内，因此也称为建筑接入模块。它负责采对园区用户提供接入。这一模块需提供充足的端口密度、丰富的端口类型、高接入带宽、准确的用户数据类型识别、完善的接入控制等。
  - ◆ **园区网汇聚：**这一模块实际上也分散于园区各建筑内，因此也称为建筑汇聚模块。它负责汇集整个建筑内部的流量，将建筑内部网络与园区网核心连接起来。这一模块需提供足够高的带宽和交换性能，较高的冗余性和可靠性，以及充分的控制策略。




- ◆ 园区网核心：这一模块不但是园区网的核心，而且通常是整个企业网的核心。它负责对来自各建筑网络、各分支机构、数据中心等各处的数据进行高速交换。这一模块需提供极高的带宽和交换性能，以及极高的冗余性和可靠性。
- 数据中心（Data Center, DC）：是各种 IT 应用业务的提供中心，可以包括服务器群（Server Farm）、存储设备群、灾备中心等。数据中心实现了企业数据的一致性，提供企业应用和数据的安全、高速、可靠、有效的访问。数据中心要求具备高可靠性、高可扩展性、高安全性、高带宽、高稳定性。数据中心通常通过多条高速冗余链路连接园区网核心，其要求具有高交换能力和突发流量适应能力，高密度千兆/万兆以太网接入，不间断转发能力，强大的安全控制能力等，对网络性能提出极高的要求。
- 网管中心：提供对整个企业网络配置、性能、故障、安全和记账的综合管理。其提供的功能包括拓扑探测、日志存储、自动告警、设备配置、性能监视等等。通常要求对全网被管理设备具有可达性，并需要严格的安全保障。
- 广域网汇聚：负责将复杂多样的广域网和 Internet 接入模块与园区网主干连接起来。其性能直接影响广域网和 Internet 接入性能。这一模块需提供充足的速度和性能和充分的控制策略。
- 专线/分组交换接入：此模块面向运营商传输网络，使用基于专线的 PPP 链路，帧中继/ATM 等分组交换链路，以及基于租用光纤的高速城域网链路等，提供大中型分支机构的远程连接。此模块要求支持足够的传统广域网和城域网类型，提供充足的接口带宽。
- 拨号接入：此模块通过运营商 PSTN/ISDN 网络提供企业骨干网与中小型分支机构、SOHO 和移动办公人员的低速连接。此模块要求提供足够的拨号端口数量，并加强包括身份验证在内的安全性。
- VPN 接入：主要负责基于包括 Internet 在内的各种公共网络实现分支机构与企业骨干网的连通。此模块需配置复杂的 VPN 策略和路由策略等，因此需要支持多种 VPN 技术，并提供足够强大的接入安全性。
- Internet 接入：主要负责提供企业网用户对 Internet 的访问。要求提供充足的访问带宽，足够的 Internet 全局地址。其对安全性要求较高，需要防范来自 Internet 的各种潜在安全威胁。为确保不间断访问 Internet 的，往往需要通过多条链路或多个 ISP 连接到 Internet，以提高冗余性。
- 网站/电子商务：此模块对位于企业内部和外部的用户提供 Web 服务，或基于 Internet 实现电子商务业务。此模块处应具有充足的计算和存储能力之外，还要求对 Internet 和数据中心都具备足够的连接带宽，其安全性要求和可靠性要求甚至超过 Internet 接入模块的要求。



## 模块化网络架构的益处

- 确定网络，边界清晰，流量类型清楚
- 便于规划，增加伸缩性
- 模块方便增删，降低复杂性
- 设计的完整性



紫光集团 H3C  
核心企业 数字化转型领导者

www.h3c.com

由于网络规模的扩大，网络复杂性的提高，单一的三层网络模型无法适应各种网络的规划设计。H3C 模块化网络架构将复杂网络划分为若干边界清晰、功能明确的模块，任何规模的企业网都可以通过若干模块或子模块组合构建而成。这种架构在当今的网络建设中日益体现出其优势：

- 模块之间相互独立，对每一模块可以分别进行规划和部署，一个模块内部的变化不影响其他模块，便于设计部署和管理维护。
- 可以通过增删模块来方便地扩展或去除网络的功能，伸缩性强。
- 各模块流量类型和服务类型各不相同，便于控制流量，提供适当的服务。
- 在每一模块内部，传统的层级化网络模型仍然有效，便于构建复杂的大规模网络。

## 1.6 本章总结

### 本章总结

- IToIP是基于SOA思想的解决方案，具有标准、融合、开放、智能的特性
- 层级化网络模型将网络划分为核心层、汇聚层、接入层
- H3C模块化企业网架构实现了网络规划、部署、管理的灵活性、伸缩性、可控性，便于构建复杂的大规模网络

www.h3c.com

## 1.7 习题和解答

### 1.7.1 习题

1. 以下属于 ITolP 特性的有 ( )  
A. 智能      B. 开放      C. 融合      D. 标准
2. 层级化网络模型将网络划分为哪些层次? ( )  
A. 汇聚层      B. 园区网核心层  
C. 核心层      D. 接入层
3. H3C 模块化架构包含下列哪些模块? ( )  
A. 灾备中心      B. VPN 接入  
C. 服务器群      D. 广域网汇聚
4. 以下哪一层次负责复杂控制策略? ( )  
A. 汇聚层  
B. 核心层  
C. 接入层

### 1.7.2 习题答案

1. ABCD
2. ACD
3. BD
4. A

## 第2章 园区网的网络模型发展历程

如同认识一个新生事物一样，对网络的认识也需要按照一定的认知方法，循序渐进的学习掌握直至精通。本章将从园区网的发展历史入手，对网络的宏观面貌进行简要介绍。以便在掌握网络整体概况的基础上继续进行后续知识的学习。

### 2.1 本章目标

#### 课程目标

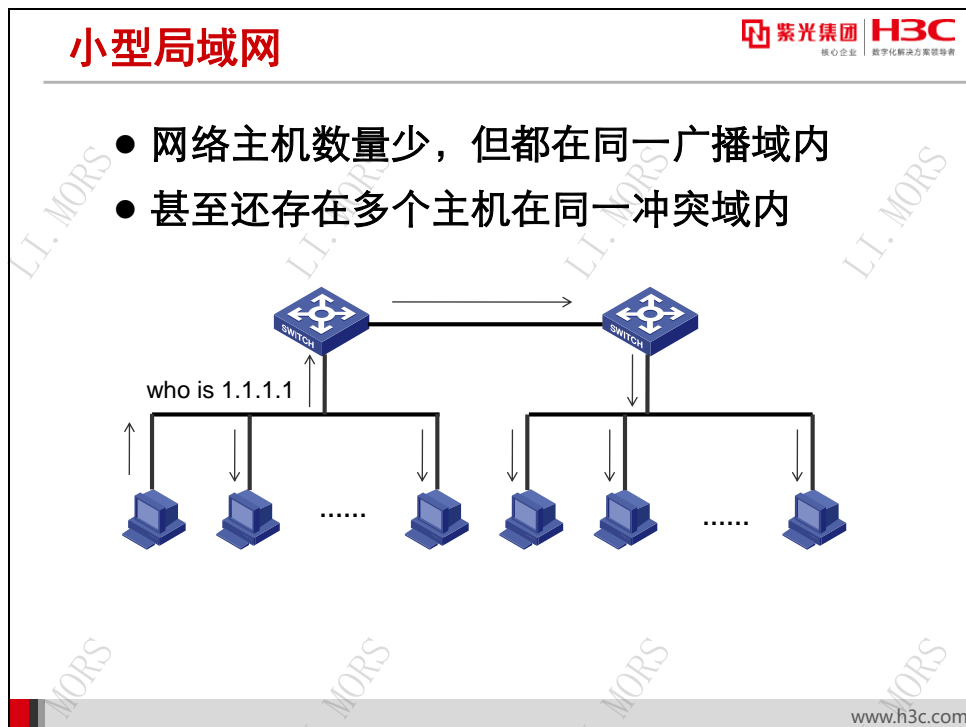
● 学习完本课程，您应该能够：

- 了解园区网发展历程
- 了解扁平网络的缺点
- 了解分层网络的优缺点
- 掌握网络结构的核心层、汇聚层和接入层的功能和业务部署
- 掌握局域网在园区网络中的应用



www.h3c.com

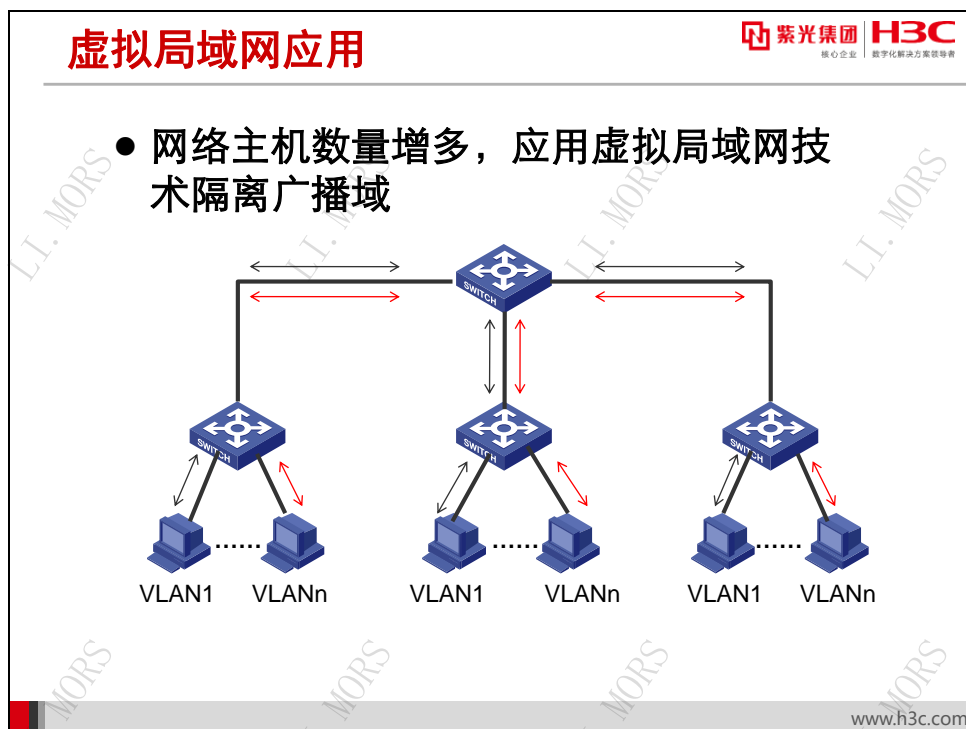
## 2.2 小型局域网



局域网的典型代表以太网最初发展实际上局限于在近距离的主机之间进行报文交付。而在其发展初期的典型网络设备则是目前已经淘汰的 **Hub**。在此类网络中，所有网络主机在同一个冲突域内工作，冲突域内仅能同时允许一台主机发送报文。而今可见的典型小型局域网结构则如图所示，主机之间的报文交互已经不再受冲突域的限制从而可以同时进行。这也是交换网络带来的优势。

但是上述典型小型局域网仍然存在广播泛滥问题。因为在此类网络中，主机发送的广播报文都将传播到整个网络的每个角落。而广播又是目前 **IP** 通信必不可少的手段之一，为了保证网络的效率，网络规模就必须限定在一定的范围内，而不是无止境的扩展。所以在小型局域网中，主机数量较少，只能适用于工作组应用。而且在交换网络产生初期，网络本身没有安全机制，无法保障网络安全可靠的运行。

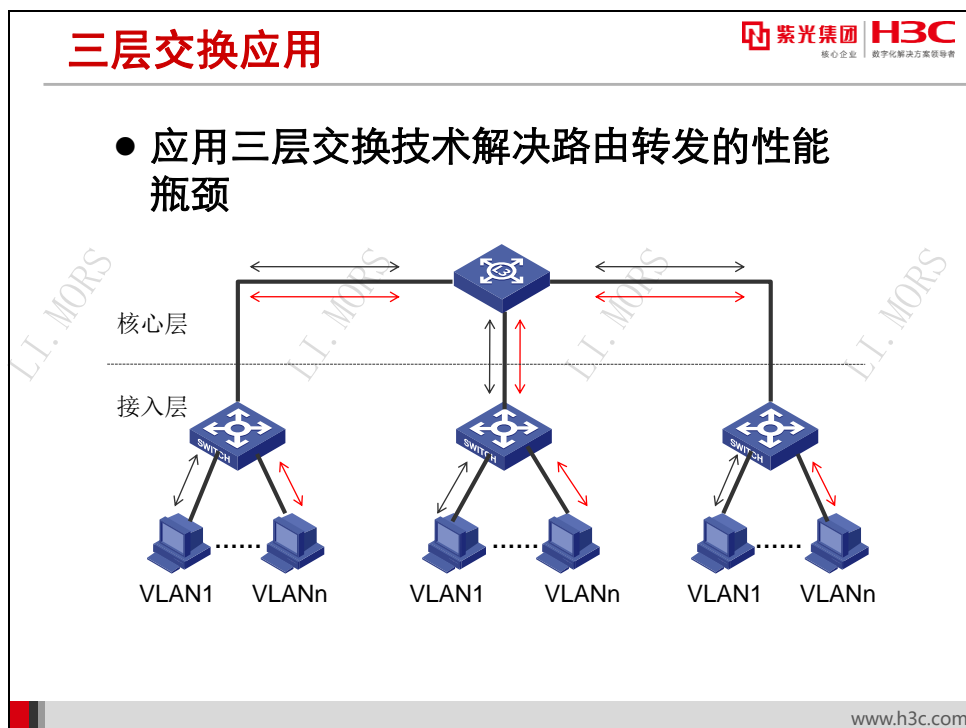
## 2.3 中型局域网



在小型局域网的基础上，如果用户数量进一步增加势必导致网络中的广播流量比例加大，网络传输效率降低。被广泛应用的 VLAN（虚拟局域网）技术可以解决此问题。

VLAN 利用特殊的报文头部特征对用户数据报文进行标识，从而可以将物理连接在一起的大型网络分割成逻辑上相互独立的多个小型局域网。这样在局域网上泛滥的广播流量将被限定在逻辑上相互独立的小型局域网内部。另一方面，VLAN 的 Trunk（干道）链路则给多个逻辑小型局域网带来了共享相同物理链路的便利性，降低了网络建设成本。

为了降低数据报文转发的开销，星形结构目前被广泛应用于中型网络中。网络以具有高转发性能的设备通过 Trunk 链路互连各个接入层二层交换设备，满足不同 VLAN 的用户分布于不同物理位置的需求，也满足多个 VLAN 共享同一物理链路的需求。

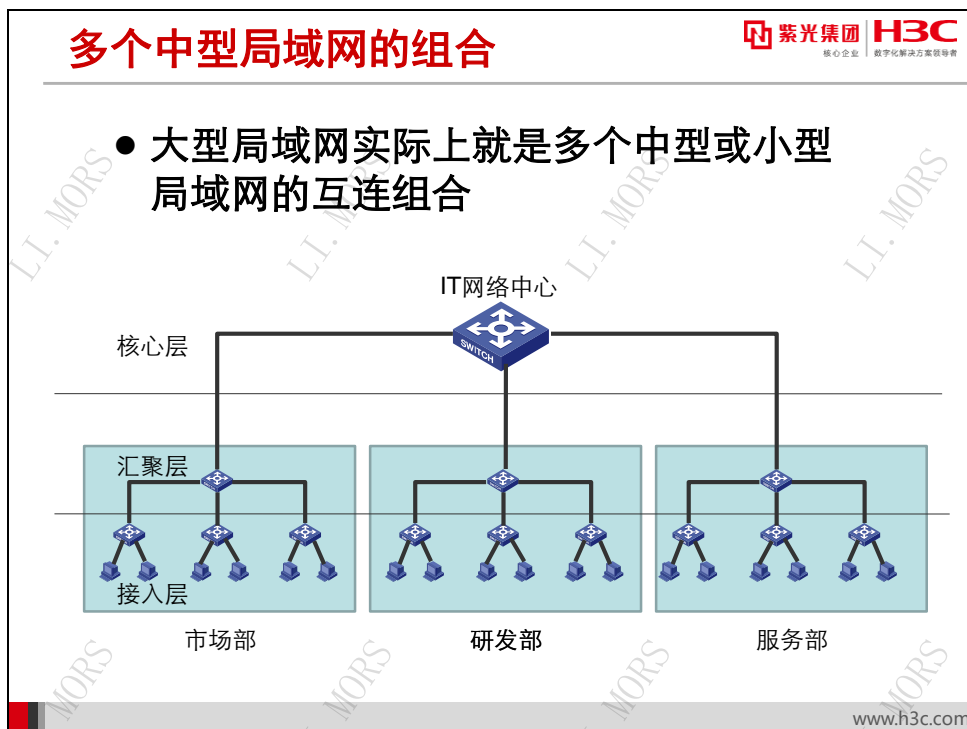


VLAN 的应用尽管解决了物理链路的共享、广播流量的泛滥等问题，但同时带来了一个新的问题，即各个 VLAN 之间的用户无法很好的互通。在 VLAN 应用初期，路由器被用来实现 VLAN 之间的互通，可是路由器的软件转发机制导致要么网络建设成本剧增，要么在路由器的转发上面形成瓶颈。

三层交换机的诞生解决了性能瓶颈的难题。三层交换机实现了基于硬件快速转发的三层路由功能，既降低了成本又提升了三层转发性能。因此在应用三层交换机的情况下，网络结构变得更加清晰，网络也变得更加健壮。首先，可以从逻辑上将三层交换机所在的中心网络划分为核心层，而二层交换机所在的边缘网络为接入层。接入层的二层交换机利用已有的 VLAN 划分、安全接入认证等成熟技术保证网络的高效、安全运转。核心层的三层交换机在满足各 VLAN 的互通的情况下，还可以采用 ACL 包过滤等机制实现 VLAN 之间的受控互访，增强安全性。

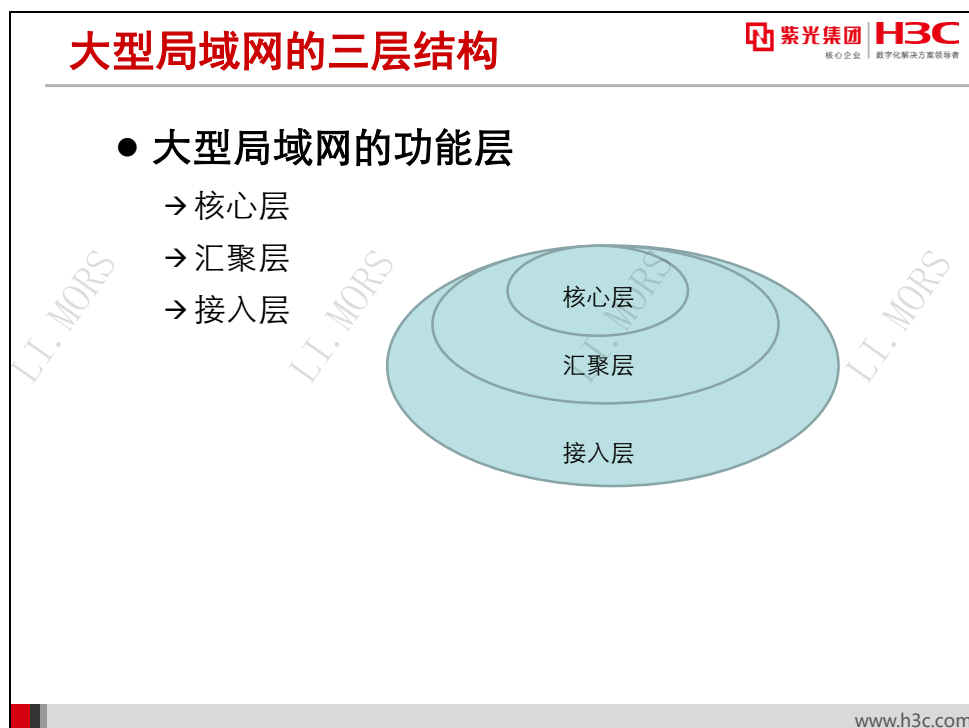
但在应用三层交换机时，单个三层交换机处理的事务非常繁重，在网络规模增大的情况下，核心设备的性能可能发生不足。另一方面此类星形网络连接存在一个致命的故障风险，即核心设备的单点故障。一旦核心设备发生故障，整个网络将形成多个孤岛而无法互通。

## 2.4 大型局域网



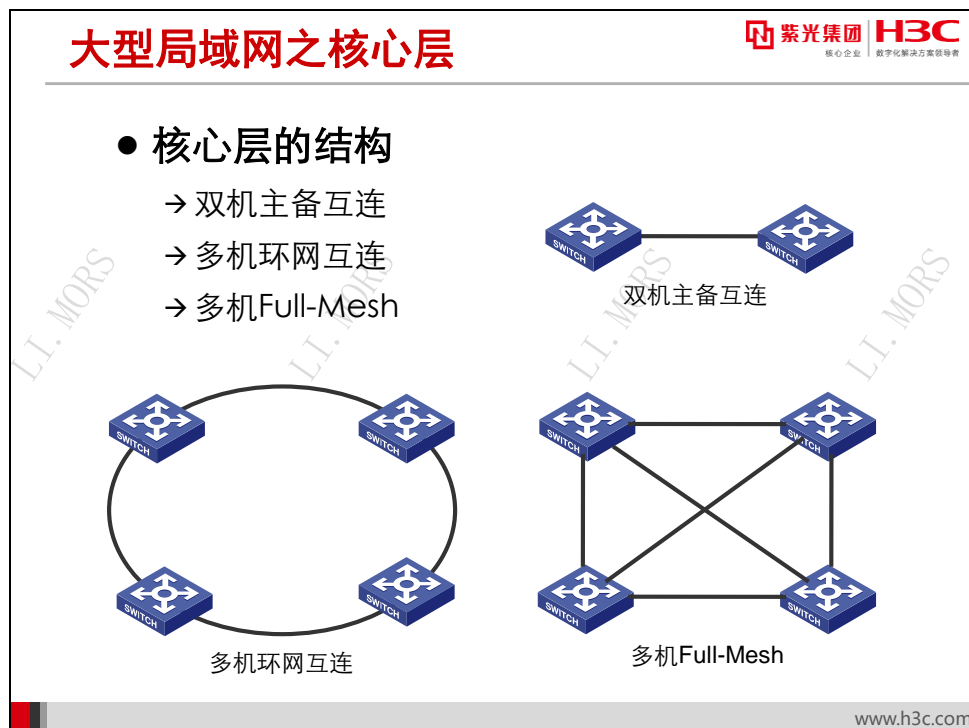
大型企业从行政管理上来看往往存在多级管理，首先整个企业被分为多个一级部门，如研发部，市场部，服务部等，而各一级部门会进一步划分成二级部门。中型局域网则仅仅适合大型企业的某个一级部门的管理结构。而各一级部门之间还需要额外的网络设备或网络来实现互连互通。因此最容易想到的是对中型局域网的结构进行扩展，在现有一级部门的星形结构的基础上，仍然采用星形结构将各一级部门进行互连。这样就形成了如上图所示的三级树形网络结构。





可以将大型局域网的功能模型简化为如图所示的三层结构：

- 核心层处在网络的最核心位置，为来自汇聚层设备的数据提供高速转发，在某些情况下还直接接入服务器集群等核心资源。通常并不在核心层部署复杂的控制策略。
- 汇聚层处在网络的中间位置，对来自接入层的数据进行汇聚，以降低核心设备的压力。汇聚层设备往往作为网关存在，而且还需要实施一定的控制策略以保证网络安全高效地运行。
- 接入层处在网络的边缘，其主要目的是实现业务的接入。可以在接入层部署安全认证等措施保证合法用户的正确接入，防范非法用户对网络资源的占用或者攻击网络。

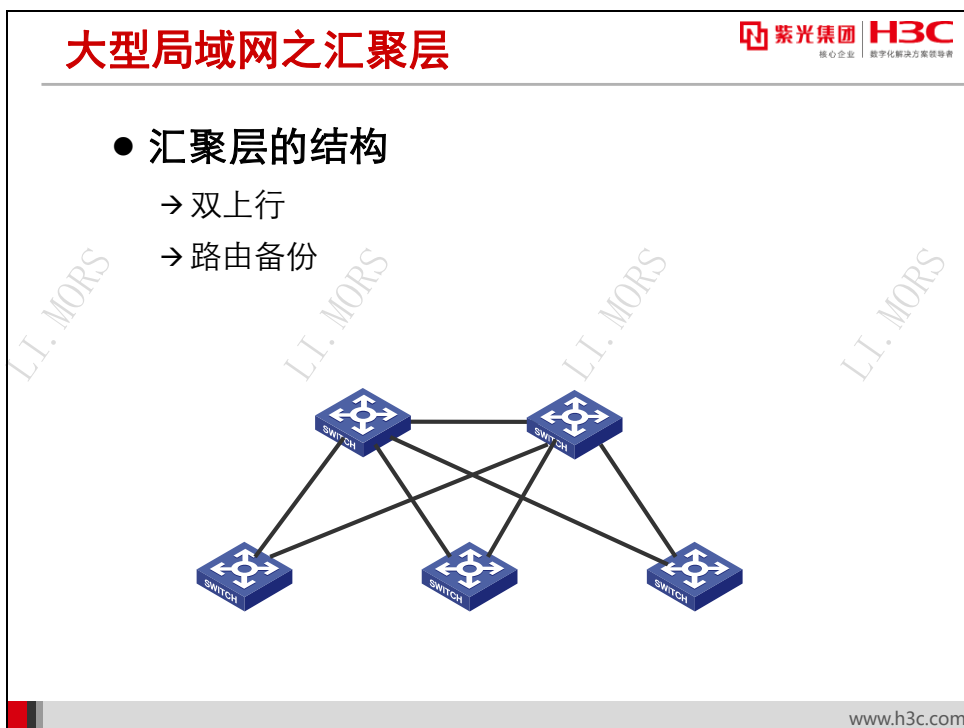


大型局域网的核心层一旦发生故障将导致全网故障，因此保证核心层的健康稳定运行成为重中之重。因此核心层网络通常不采用存在单点故障的单核心网络，而常用双机主备互连、多机环网互连和多机 **Full-Mesh** 互连等。

双机主备互连是核心层建设最为主流和经济的方案之一。在核心层架设两个高性能的核心路由器或核心三层交换机，两个核心设备之间采用高速链路互连，汇聚层设备则采用常规的双归属接入方案同时接入到核心层的主机和备机。

多机环网互连也是核心层建设的主流方案之一，它主要应用在规模巨大，核心设备数量较多的网络中。多机环网互连仅需要较少数量的高速链路即可在核心层设备间建立起备份路径，因此可以在不增加成本的情况下，实现一定的核心层设备和链路的冗余备份。

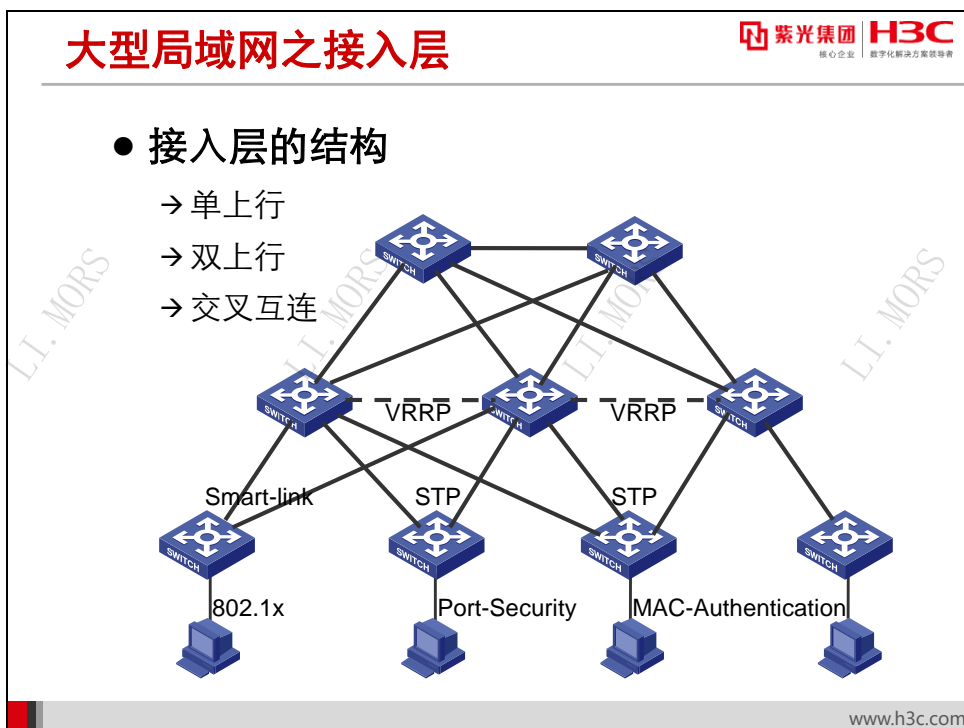
多机 **Full-Mesh** 互连是一种高可靠性的方案，它主要应用在网络规模巨大，核心设备数量较多且对可靠性要求很高的网络中。但此方案需要在核心设备间采用更多的高速链路进行直连，大幅增加了核心层网络的成本。



为了配合核心层无单点故障，汇聚层必须保证主备链路双归属接入到核心层的两个不同的设备，防止核心层单个设备的故障导致业务中断。如图所示，在核心层双机主备互连的情况下，汇聚层设备分别采用两条链路连接到核心层。当主机出现故障时可以快速切换到备机转发而不中断业务。在业务流量较大的网络中还可以实现主备链路的负载分担。

汇聚层与核心层之间的链路负载分担或主备备份既可以采取二层方案也可以采取三层方案。但为了降低核心设备的压力，通常采用三层方案，即将网关置于汇聚层，核心层和汇聚层设备运行动态路由协议，既可以实现负载分担，也可以实现冗余备份。

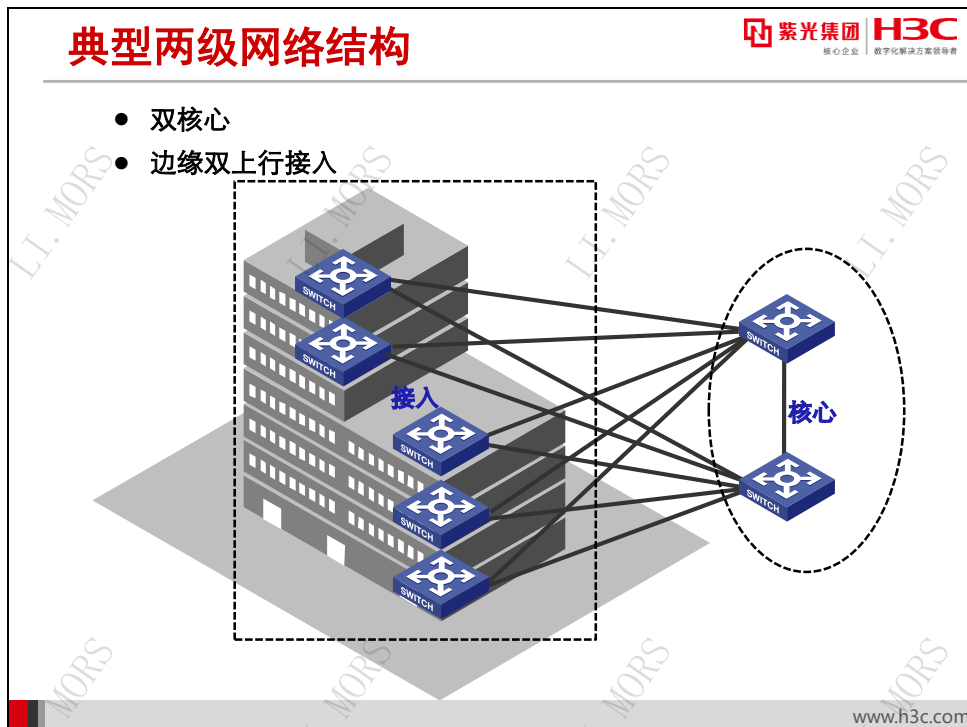
在互连接入层设备的基础上，汇聚层同时还实施复杂的控制策略，例如采用包过滤和策略路由等技术实现的访问控制和路由控制流量控制等。



接入层作为网络的边缘，主要任务是实现多业务的安全接入。根据接入业务的重要性，可以采用单链路上行或者双链路上行。采用双链路上行时，需要根据实际情况选择恰当的负载分担和冗余备份技术。目前常用的备份技术有 VRRP、STP、Smart-Link 等技术。VRRP 的真正实施在汇聚层网关上，接入层终端用户可以以 VRRP 的虚拟 IP 为网关，实现网关的备份。STP 可以选择单生成树实现链路的冗余备份，也可以选择多生成树实现链路的负载分担。Smart-Link 则是双归属网络中针对 STP 的优化技术，可以实现更快的倒换收敛速度。

接入层根据接入用户的安全性选择不同的接入认证方式，如 802.1x 认证，端口安全等。802.1x 认证是目前以太网中应用最为广泛的接入认证技术，而 MAC 认证则是 802.1x 认证的一种变化，简化了客户端的操作。端口安全则是综合接入认证的典型代表，它是 802.1x 认证、MAC 认证以及 Voice VLAN 等应用的综合体，可以在同一端口实现多种认证方式的组合。

## 2.5 局域网应用



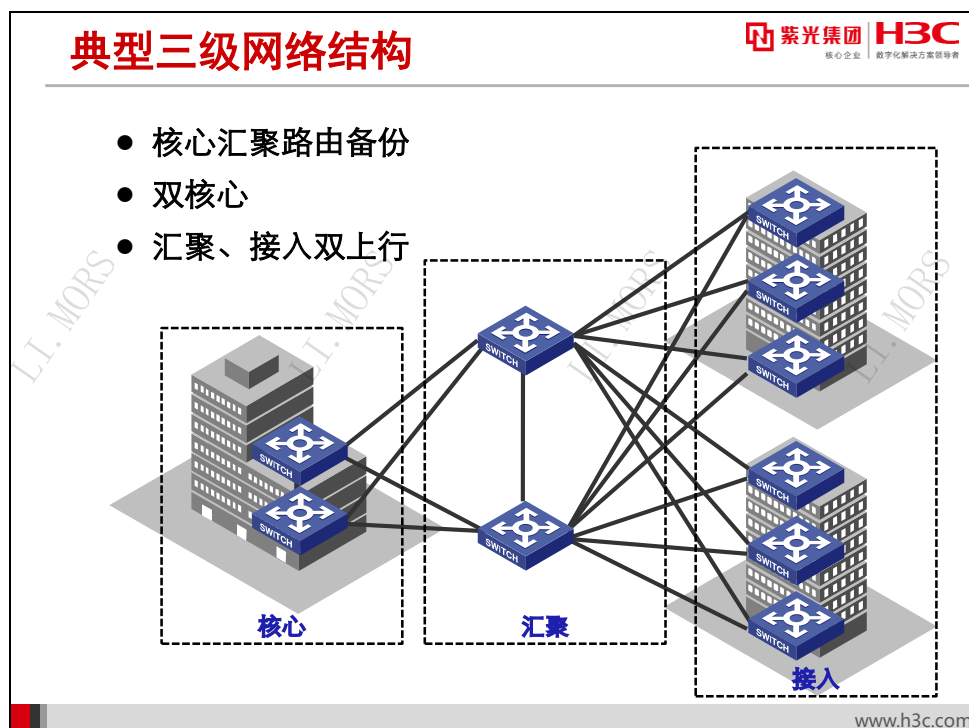
如图所示为一个中型企业的办公楼。每个楼层都需要部署一定数量的信息接入点，整个大楼有将近 1000 个信息接入点。网络中心在大楼一层的 IT 机房。要求各业务部门之间的二层网络相互独立，业务部门之间的信息接入点互访必须通过网络中心的核心设备，在核心设备实施流量控制。

针对上述需求，可以采用典型的中型局域网的拓扑结构来部署该企业的办公网络。在网络中心采用双机互连形成核心网络，各楼层根据信息点数量的需求决定选择一个或多个接入层交换机双上行连接到两核心设备。

核心设备必须选择具有路由功能的三层设备，推荐采用线速转发的高性能三层交换机实现无阻塞交换。同时还要求设备支持较强的 ACL 功能，可以灵活的部署 ACL 进行访问控制。另外需根据网络规模确定设备需要支持的路由、ARP 和 MAC 等规格。

接入设备建议选择具备 VLAN 划分、接入认证、STP 等功能的二层交换机。在业务接入端口采用接入认证并根据业务部门的要求进行 VLAN 划分。上行链路选择 Smart-Link 或 STP 等冗余备份技术。

上述中型园区网适合大多数中小企业或者中小学校的网络建设。此类网络信息接入点的数量一般不多于 1000，要求实现一定的安全防范和可靠性，但对网络建设成本较为敏感。



与中小型企业网不同，大型企业园区办公网和高校校园网物理位置分布更加广泛，一般都分布在同一园区的多栋大楼内。如图所示即为一个典型的大型企业在一个园区内的网络分布情况。

按照办公楼的分布情况，将物理位置相对处于中心的大楼选为网络核心所在地，可以更程度的降低传输线路的建设成本。而在网络核心层，根据企业对网络可靠性的要求选择核心网常见组网结构中的恰当类型，如最为常见的双机主备互连。在网络核心所在大楼和其他办公大楼再以双机热备的形式组建汇聚层网络，最后将接入层设备按照双归属或者单上行的方案就近接入到本大楼的汇聚设备，从而形成典型的三层网络结构。

核心设备作为全网核心和高速交换中心，必须保证设备自身具备高可靠性，关键部件具备冗余备份功能。设备转发性能具备可扩展性，网络建设初期其实际被耗用的性能占其当前最大性能的 50%为宜，便于后期网络的扩容改造。

汇聚层设备与中小型网络的核心设备相当，因此同样具备一定的设备级可靠性和相应的硬件性能规格，如 ARP 表项、MAC 地址表项、路由表项等规格应该能够满足当前及后期网络扩容需求。除此之外还必须具备各种冗余备份技术的能力，对上和核心层设备实现三层的冗余备份。对下和接入层设备实现二层的冗余备份。

接入层设备则与中小型网络的接入层设备要求相当，或者根据企业的安全性和可靠性要求适当提升设备性能和业务支撑能力。但冗余备份和安全接入等基本技术采取相同的策略和部署原则。

## 2.6 本章总结

### 本章总结

- 局域网的发展和三种结构
- 局域网的核心、汇聚和接入
- 典型二级网络结构的应用
- 典型三级网络结构的应用

## 2.7 习题和解答

### 2.7.1 习题

1. 当前构建局域网主要采用的设备是（ ）  
A. HUB（集线器）                      B. Switch（交换机）  
C. Router（路由器）                  D. Server（服务器）
2. 大型局域网通常分为（ ）  
A. 核心层                                  B. 汇聚层  
C. 接入层                                  D. 网络层
3. 大型局域网的核心层网络常见的组网结构有（ ）  
A. 单核心组网                              B. 双机主备互连  
C. 多机环网互连                          D. Full-Mesh 互连
4. 大型局域网中常见的冗余备份技术有（ ）  
A. VRRP                                      B. MSTP  
C. Smart-Link                                D. 动态路由协议
5. 接入层网络的常用安全接入认证技术有（ ）  
A. 802.1X 认证                              B. MAC 集中认证  
C. 端口安全                                  D. Voice VLAN
6. 大型园区网的网络结构必须采用常见的树形结构。（ ）  
T. 正确    F. 错误

### 2.7.2 习题答案

1. B
2. ABC
3. BCD
4. ABCD
5. ABC
6. F



## 第3章 典型园区网的业务部署

在网络的各层次采取何种技术来满足网络需求,需要细致的分析才能得出最佳的解决方案。

本章从网络的业务需求,可靠性需求以及管理需求等多方面阐述各种网络技术的应用场景和应用优势,以利于对园区网内主要业务类型的部署形成整体性的认识。

### 3.1 本章目标

#### 课程目标

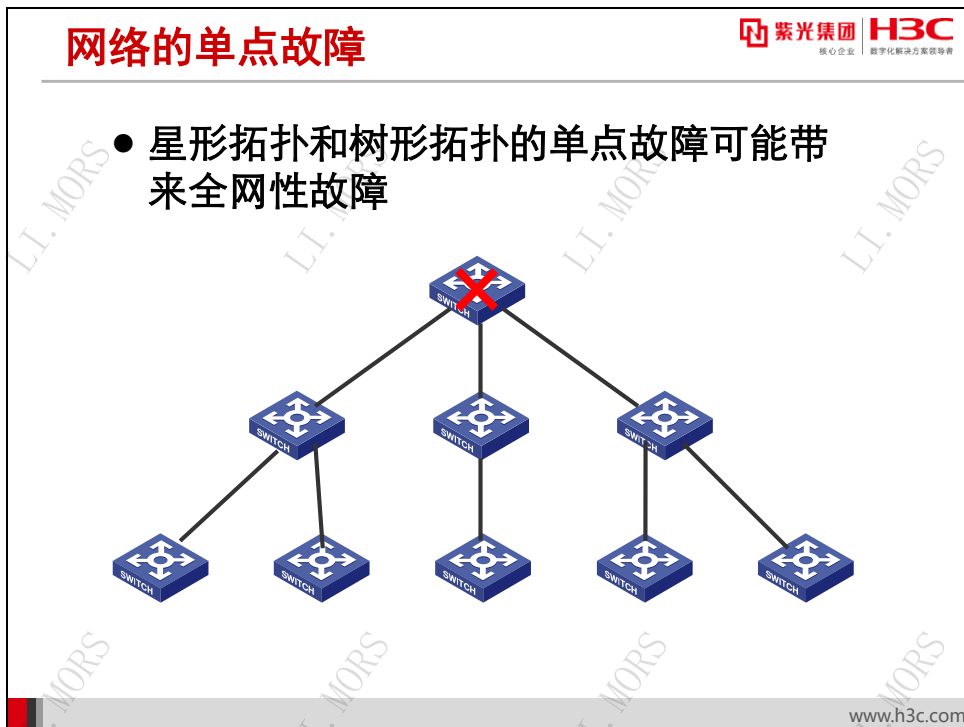
● 学习完本课程, 您应该能够:

- 熟悉园区网的几种常见业务
- 了解园区网常见的冗余备份技术
- 了解组播业务的相关技术和协议类型
- 了解语音业务部署的特殊任务
- 了解常见的网络安全接入认证技术
- 了解常见的网络管理和维护的技术



www.h3c.com

## 3.2 高可靠冗余网络



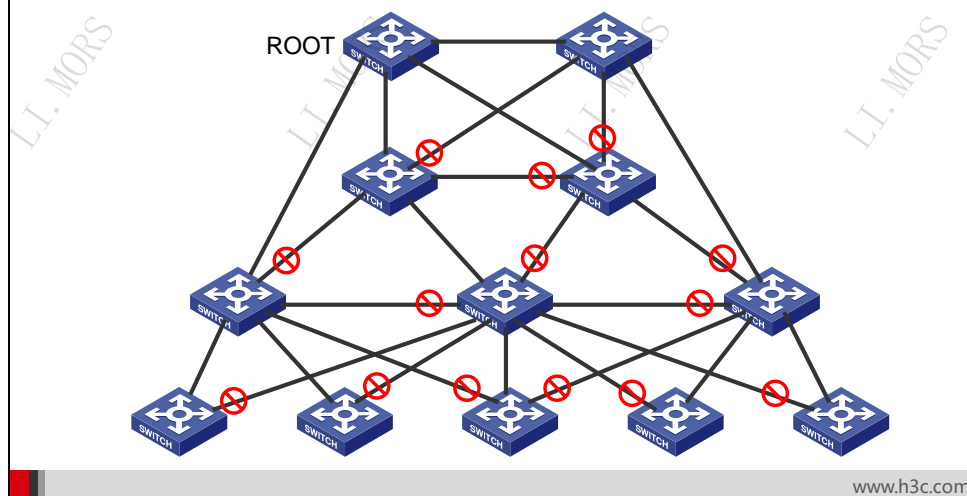
如图所示的树形拓扑网络中，如果核心设备宕机或者掉电，将导致全网故障，即各汇聚层设备被分割开来，相互独立而无法互通。这是星形和树形网络存在的单点故障缺陷。

为了避免单点故障，或者降低单点故障发生时的受影响范围，可通过核心层网络的双核心、环网或者 Full-mesh 互连的方式来提高网络的健壮性。

然而物理环路的引入带来新的难题——如何消除数据报文转发时存在的环路？为此可以采用如 STP、RRPP 等协议来计算数据报文转发的路径，避免出现逻辑环路。

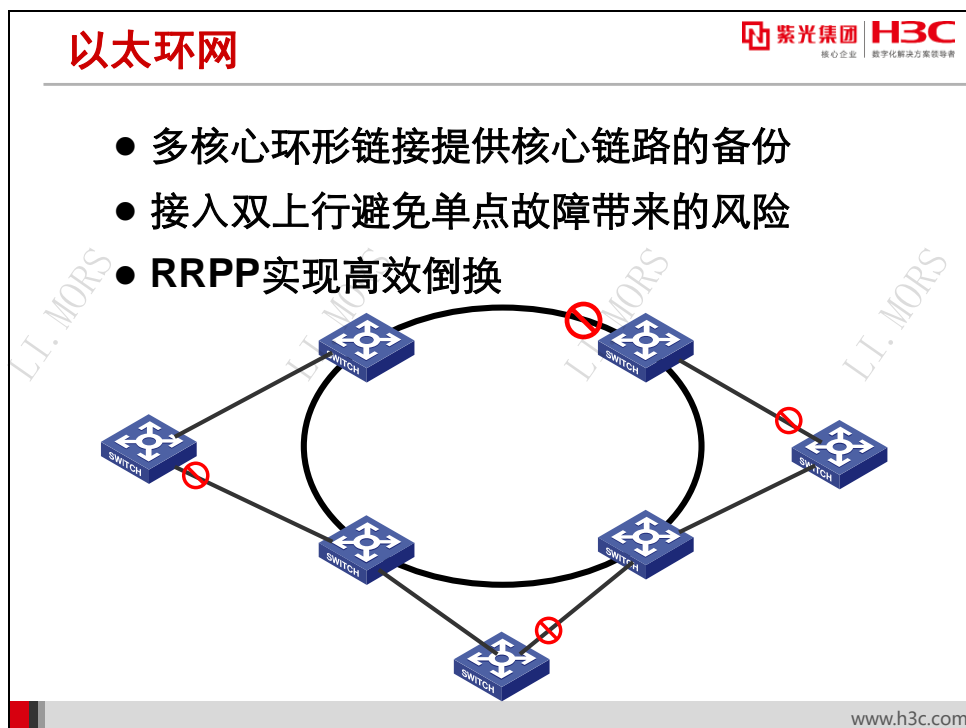
## 网状网络

- 多冗余链路避免单点故障带来的高风险
- STP阻塞冗余链路避免环路的形成



提高网络健壮性和避免单点故障的最常见的方法就是在各设备之间采用更多的冗余物理链路进行连接。如图所示，在核心层采用多台设备进行全互连防止单点故障，而在汇聚层和接入层则采用双归属甚至环形连接来达到上行链路的负载分担和冗余备份。但在此类网络中，一个数据报文从一个终端转发到另一个终端可能有多条路径，如果每条路径都转发一遍报文，则目的终端将收到大量重复的报文。广播报文也会在网络中被不断复制，最终形成广播风暴。因此不得不采用一定的算法来计算并选择终端之间的唯一转发路径。最先被开发设计来解决此问题的当属 STP（Spanning Tree Protocol，生成树协议）。

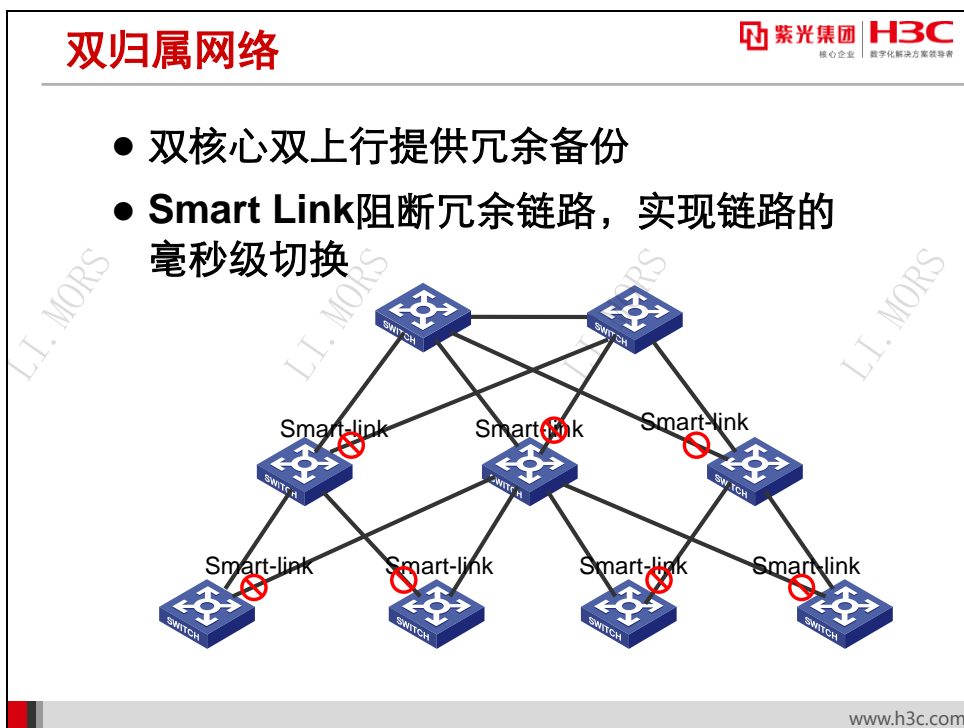
STP 的计算将错综复杂的物理网络整理成一棵逻辑转发树，将那些当前没有必要使用的链路进行逻辑阻塞，从而避免网络环路。而当某些当前在用的链路故障时，STP 又可以快速启用那些曾经被阻塞的链路来替代之，从而恢复网络的连通性。



全网状或半网状的网络采用大量的冗余物理链路来实现网络的不间断转发或者快速恢复，其建设成本则相对高昂。在一定的条件下，网络对可靠性和快速自愈能力的要求可以适当降低，因此可以根据需要适当裁剪部分冗余链路而形成更为简洁经济的网络拓扑。其中图示的环形网络就是典型代表之一。此类网络常常通过多个核心设备形成核心环网，每个核心设备再根据需要单链路或双链路接入接入层网络。在此种网络中部署 STP 仍然是行之有效的方法之一。但在环形网络中，STP 并不是最佳选择，RRPP 正是胜任此工作的协议之一。

RRPP 协议是专门针对环形网络拓扑开发设计的协议，它利用少量的冗余链路来完成环网上的冗余备份。RRPP 的核心思想是在正常情况下阻塞环上的某个链路，并通过协议报文的交互来监控其余链路的工作状态，一旦发现某链路发生故障，将快速恢复被阻塞的链路。相对于 STP，RRPP 具有更小的资源开销和更快的收敛速度。但由于实际物理冗余链路的匮乏，其可靠性在一定程度上有所损失，若环上如果同时发生了两个链路的故障，将导致网络被分割。

根据实际情况，边缘接入层则可以继续选择 RRPP 协议运行子环，或者选择其它针对性的冗余备份协议。



针对网状网络的拓扑优化，除环形网络之外，还有另一种应用更为广泛的网络拓扑。此上图所示，所有接入层设备都采用双上行链路分别接入到上一级的两个设备，因此被称之为双归属网络。

在如上所示的网络中，如果运行 STP 来实现冗余备份，网络的倒换收敛时间在秒级；而采用另一种更为高效的冗余备份协议——Smart Link（智能链路）来实现冗余备份，网络倒换收敛时间则降低到毫秒级。Smart Link 之所以能够达到如此高效的倒换性能，归因于此网络中任何一条链路的故障倒换都只需要直接相连的交换机一次动作即可完成，而不需要像 STP 那样等待协议报文的交互和再计算。

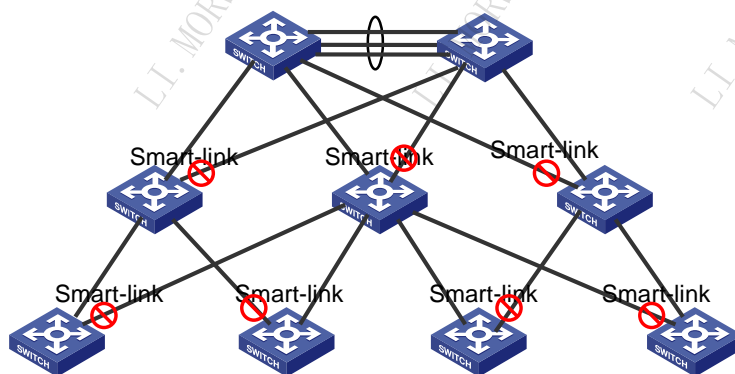
Smart Link 设备将上行的两条链路作为一个备份组来考虑，在任何时刻都保持其中一条链路工作，而阻塞另一条链路。当工作链路发生故障并被检测到时，Smart Link 设备立即启用阻塞链路而恢复网络连通。

在某些特殊情况下，Smart Link 也可能失去作用。例如当上一级交换机的所有上行链路都出现故障时，下一级交换机并不能够感知这种网络拓扑的变化。为了弥补 Smart Link 的缺陷，Monitor Link 应运而生。

Monitor Link 专门负责对上行链路的监控。一旦发现上行链路全部故障，设备可以立即关闭下行链路而触发 Smart Link 的倒换。Smart Link 与 Monitor Link 配合，可以实现网络链路快速高效的冗余备份。

## 链路聚合

- 链路聚合提高物理带宽，且实现负载分担和链路备份



www.h3c.com

在冗余备份网络中，无论采用网状链接、环形链接还是双归属结构，一旦某条当前在用的链路发生故障，必然导致网络路径的改变，也必然引起网络连通性的中断，其不同之处仅在于中断时间的长短。然而另一链路级备份协议则可以更好的完成链路的冗余备份，它就是链路聚合（Link Aggregation）。

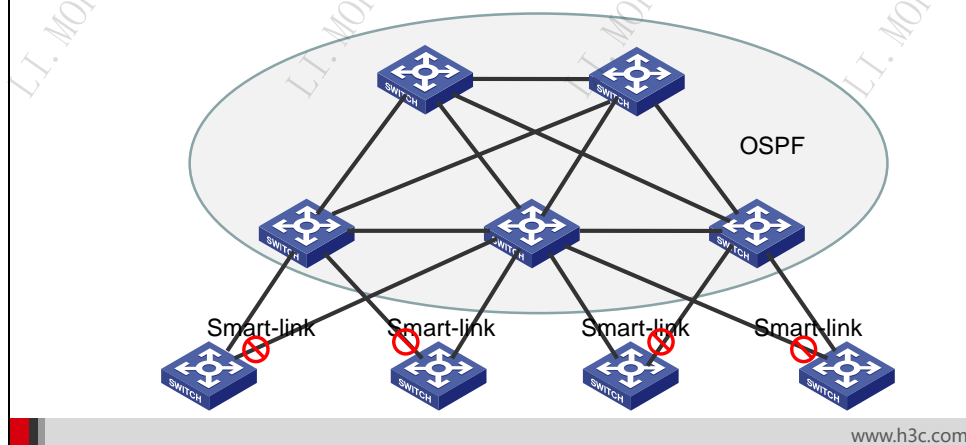
链路聚合采用多条物理链路捆绑形成逻辑链路聚合组，只要链路聚合组内的任何一条物理链路保持连通状态则整个逻辑链路仍然保持连通状态。因此当某条物理链路发生故障而失去连通性的时候并不影响整个逻辑聚合组的连通状态，从而保证了网络的不间断连通性。

除此之外，链路聚合技术还可以实现链路带宽的扩容。当多个物理链路聚合形成聚合链路时，其聚合链路的实际传输带宽为这些物理链路的传输带宽之和。链路上的实际流量将根据一定的算法自动分配到各物理链路上传输。

## 三层路由网络

紫光集团 H3C  
核心企业 数字化转型领导者

- 路由协议实现最短路径转发，冗余链路提供备份选择
- **ECMP**提供负载分担



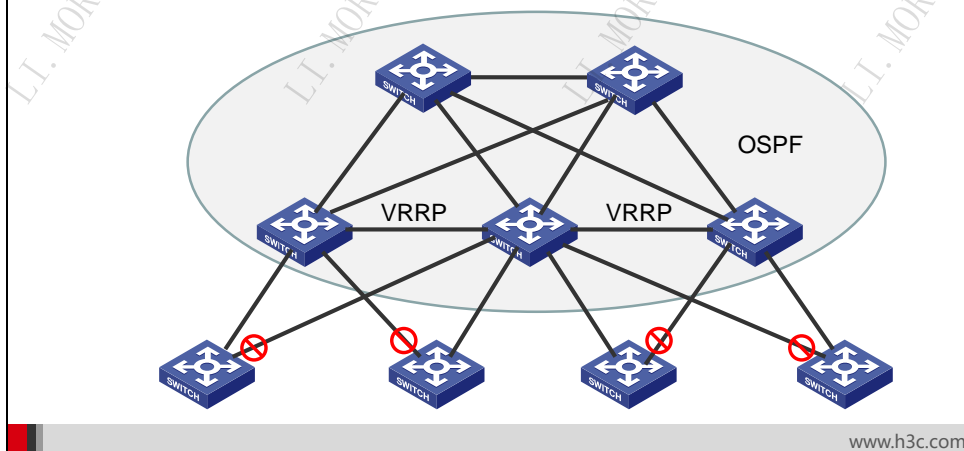
STP、RRPP、Smart Link 等技术基本上都针对二层网络而设计，但实际的大型网络并非纯二层网络。其在边缘接入层多采用二层网络，而在核心和汇聚则采用三层网络，以便将二层网络控制在可以接受的范围内，来降低广播报文对网络传输效率的影响。

在三层网络中，常用于指导数据转发的则是路由表，它由多种路由协议计算生成或手工配置完成。在网状或半网状链接的三层网络中，利用路由协议的自动选路则很容易的实现链路的冗余备份和倒换。值得一提的是，除了实现动态选路的冗余备份之外，大多数动态路由协议还可以实现 ECMP（Equal Cost Multiple Path，等价多路径）。ECMP 可以为同一目的地同时选择多条路径完成报文传送，从而提高链路利用率。

## 网关冗余备份

紫光集团 H3C  
核心企业 数字化转型领导者

- 边缘网关运行VRRP提供网关的主备备份
- 多备份组+MSTP提供负载分担



在常见的网络中，主机通常通过自己的网关将报文传送到远端目的地。但在主机上往往只能指定一个三层设备（以 IP 为标识）作为自己的网关。当网关发生故障时，不得不重新指定新的三层设备作为主机的网关。因此网关的不间断服务变得尤为重要。为了实现网关的不间断服务，就必须采用相应的备份手段来确保网关的可靠性，其中 VRRP（Virtual Router Redundancy Protocol）则是专门为此设计。

VRRP 将多个物理三层设备融合起来形成一个虚拟三层设备——虚拟路由器（Virtual Router），在这些物理三层设备之间通过选举的机制选举出一个 Master（主设备）来担当实际的三层网关，而其余三层设备则监控 Master 的工作状态，当 Master 一旦发生故障，将重新选择产生新的 Master 而恢复实现网关的不间断服务。在三层网关下面的主机则以虚拟路由器为自己的网关，由哪台物理设备担负实际的网关工作其并不关心。

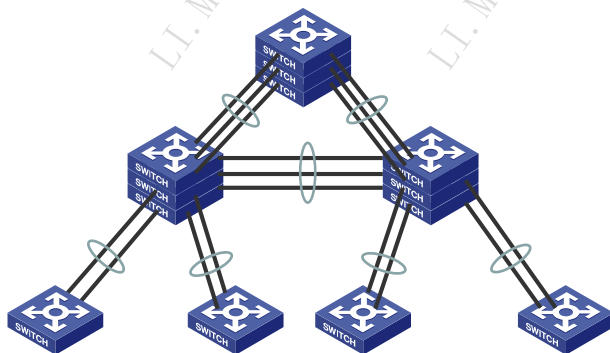
在网络设计时需要保证在 VRRP 发生主备倒换之后，主机仍然能够与新的 Master 保持连通。通常用 VRRP 与 STP 配合完成，并在主备设备之间采用物理链路保证协议报文的正常交互以及部分业务报文的转发。如果需要更加充分的利用当前物理链路的传输能力，还可以采用 VRRP 多备份组和 MSTP 来实现流量的负载分担。



## IRF设备级备份

紫光集团 H3C  
核心企业 数字化转型领导者

- IRF堆叠实现设备级的N+1冗余备份
- 分布式链路聚合实现链路负载分担

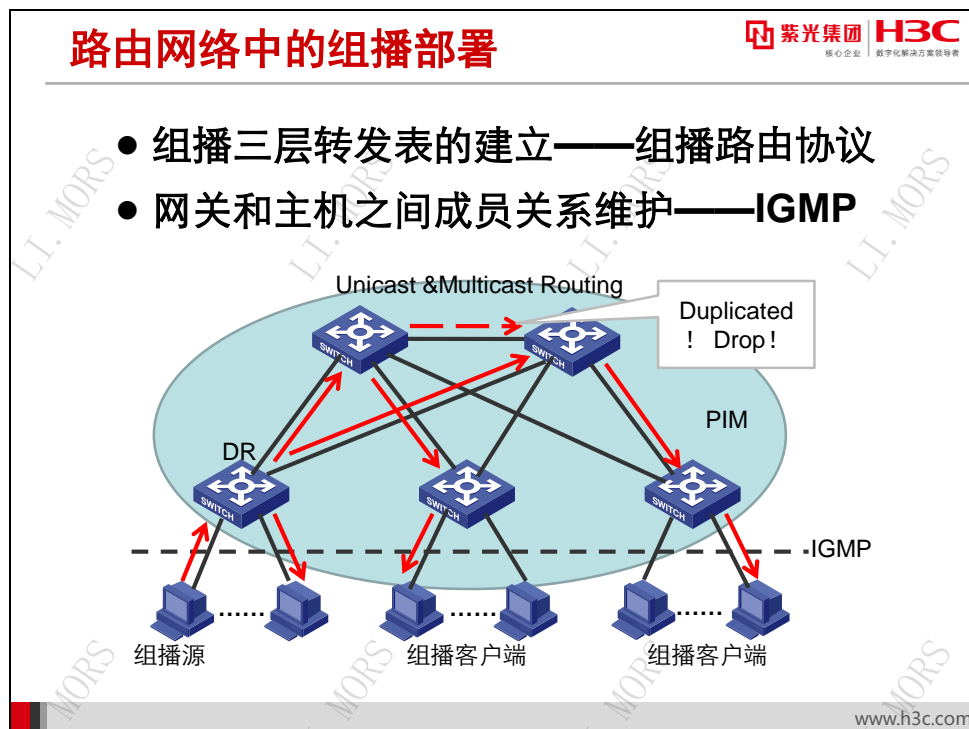


www.h3c.com

在实际网络中，核心设备常常采用关键部件冗余的框架式设备来提高核心设备，如主控板进行主备备份，电源实现 1+1 冗余备份等。但相对来说，成本高昂，利用率较低。如果采用如上图所示的堆叠技术将多个设备堆叠形成一个设备并组网时，则既可以满足高可靠性的要求，又可以充分利用设备的性能，同时降低成本。

IRF (Intelligent Resilient Framework, 智能弹性架构) 通过堆叠链路将多个设备联合起来形成一个联合体，多个设备之间相互备份实现 N+1 的冗余备份，大幅提高联合体的可靠性，保证不间断服务。同时还将普通的链路聚合组扩展到多个设备之间，形成跨设备链路聚合，让流量在多个设备之间实现负载分担。因此 IRF 既实现了链路级的冗余备份，也实现了设备级的冗余备份，是一种比较全面的冗余备份技术。

### 3.3 组播业务的快速开展



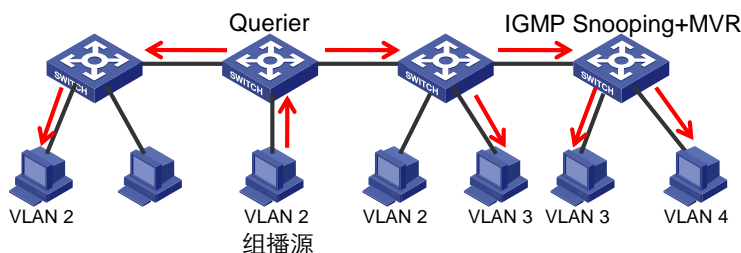
在 IP 网络不断发展壮大的情况下，多网合一的需求逐步形成。首先集成应用到 IP 网络中的则属广播电视等媒体传播应用。不同于传统的 C/S 应用，此类应用客户端数量巨大，如果客户端都与服务器建立一对一的连接，将导致服务器不堪重负。简单的广播虽然可以传递这些媒体数据，但将导致网络流量的大幅增加。因此在 IP 网络中出现了相对于单播和广播都不同的组播技术。

单播转发依靠报文中的目的 IP 地址实现报文的逐跳转发，最终传送到目的地。而组播并没有唯一标识接受者的目的 IP，在组播报文中携带的目的 IP 是表示一组接收者的组播 IP 地址。因此组播的转发机制也完全不同于单播转发。它依靠 RPF（Reverse Path Forwarding，逆向路径转发）技术来实现组播报文的转发。PIM（Protocol Independent Multicast）即是采用 RPF 技术转发组播报文的组播路由协议代表之一。它依靠单播路由信息检查组播报文的合法性，再根据自己维护的组播组出接口列表转发组播报文。而在三层网络的边缘，网关设备负责将组播报文发送给最终客户端，因此网关必须维护组播客户端在本地的连接情况。此项维护工作则交由运行在主机和网关之间的 IGMP（Internet Group Management Protocol）协议来完成。

## 二层网络中的组播部署

紫光集团 H3C  
核心企业 数字化解决方案领导者

- 查询器辅助二层交换机维护成员关系
- IGMP Snooping完成组播表维护
- MVR完成组播复制



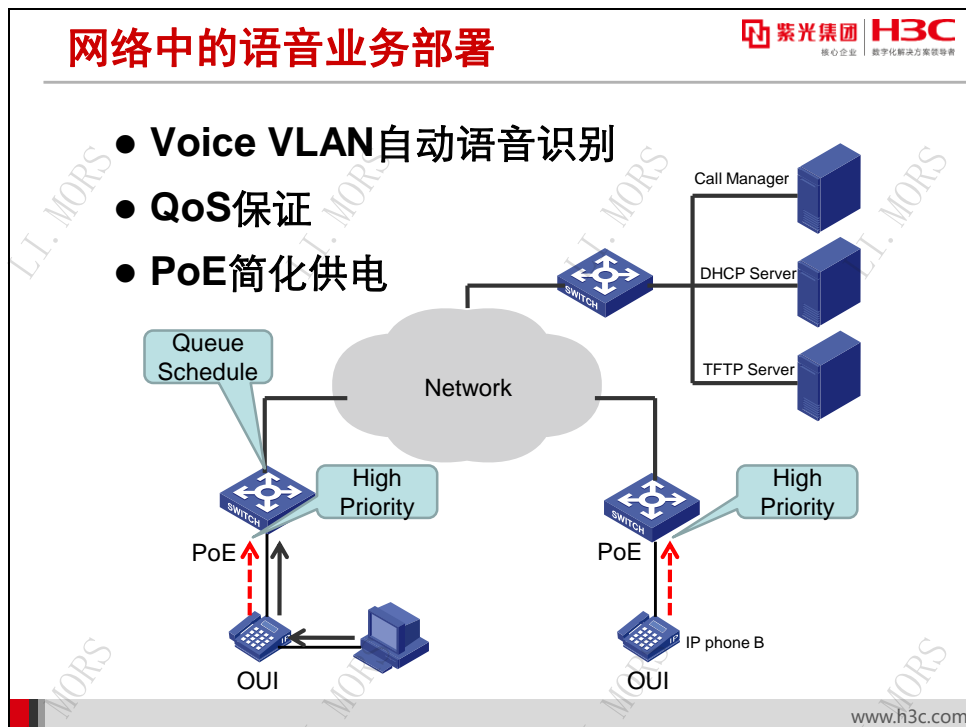
www.h3c.com

在二层网络中业务报文的转发不再依赖于报文的 IP 地址，而完全依赖于报文的 MAC 地址。MAC 地址和 IP 地址一样也被分为了单播，广播和组播等地址类型，因此在二层网络中，二层交换机只需要根据组播 MAC 地址维护好组播组和成员关系，即可有效的进行组播数据帧的转发。IGMP Snooping 以 IGMP 协议报文为基础，通过监听客户端和网关设备之间的交互来完成组播组与成员关系的维护。但在纯二层网络中，并没有一个网关设备运行 IGMP 来完成协议报文的交互。因此在二层网络中，还必须寻找一个设备来充当 IGMP 中的查询器，使得客户端和查询器之间的 IGMP 协议报文的正常交互得以进行，从而保证二层交换机可以正确维护成员关系。

IGMP Snooping 的监控和组播成员维护都是基于 VLAN 实现的。如果客户端在不同的 VLAN 中，则需要不同的 VLAN 内维护，而且还需要在不同的 VLAN 内转发相同的数据报文。这样将导致部分链路出现相同的两份组播数据报文（仅仅 VLAN ID 不同）而浪费网络带宽。为了解决这一问题，MVR（Multicast VLAN Register）提出了将组播数据流集中在同一 VLAN 传送的思想。

MVR 通过在特性的组播 VLAN 内维护组播成员关系。当客户端位于其它不同的 VLAN 时，交换机可以通过复制机制将组播报文从组播 VLAN 复制到客户端所在 VLAN，而避免组播报文的重复转发；或者利用 Hybrid 链路的特性将客户端所在链路都加入到组播 VLAN 中，组播报文仅在组播 VLAN 内转发。前者被称之为基于 VLAN 的 MVR，后者被称之为基于端口的 MVR。

### 3.4 语音业务的部署

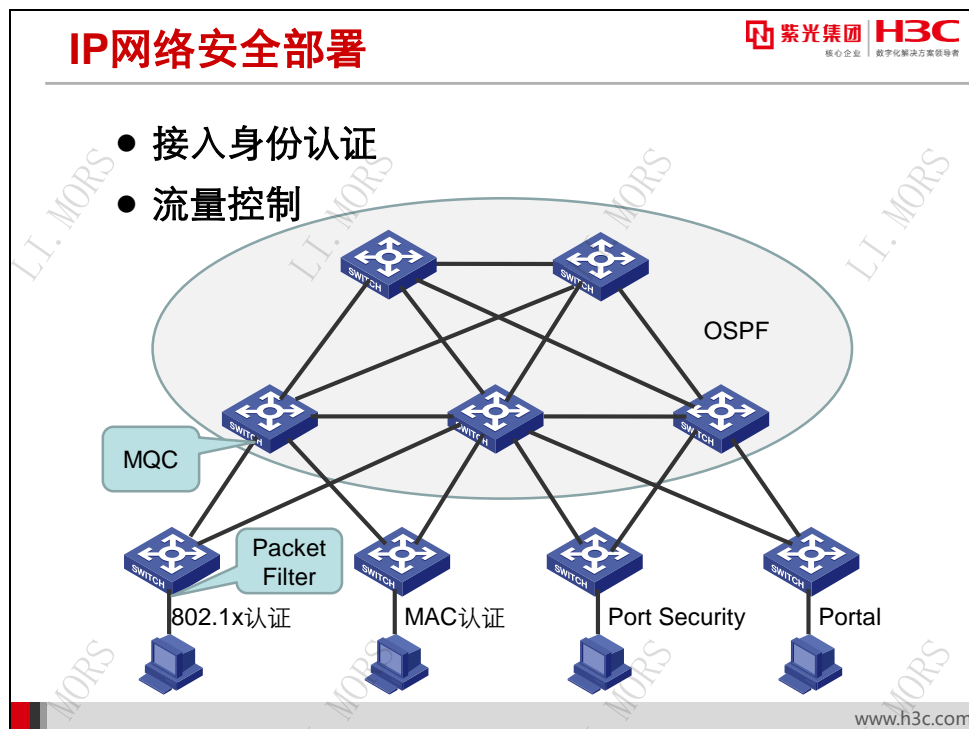


IP 网络另一集成应用则是对语音业务的支持，即将传统语音纳入到 IP 网络中传输。传统语音网络采用电路交换技术，它可以保证语音信号的实时传送，具有低延迟高带宽的特征。IP 网络采用的却是完全不同的交换技术。数据报文的传送很可能是具有不同延迟甚至是无序的。这将给语音通话带来严重的影响。为了保证语音报文有序均匀的抵达且具有最小延迟，网络设备不得不对语音报文加以区别并优先传送之。

Voice VLAN 技术能够自动识别语音报文。它在接入层根据语音报文的特征（如语音报文的 OUI）将其识别出来并将其标记为较高优先级，网络设备则根据其标定的优先级采用可靠的 QoS 保障机制确保语音报文的及时转发。

传统语音电话并不需要额外的供电即可工作，而 IP 电话如果采用独立的供电系统势必给网络建设带来一系列的麻烦。PoE（Power over Ethernet，以太网供电）技术允许通过以太网线和 PoE 以太网交换机对 IP 电话进行远程供电，为传统语音网络迁移到 IP 语音网络排除了重要障碍。

### 3.5 网络安全的部署

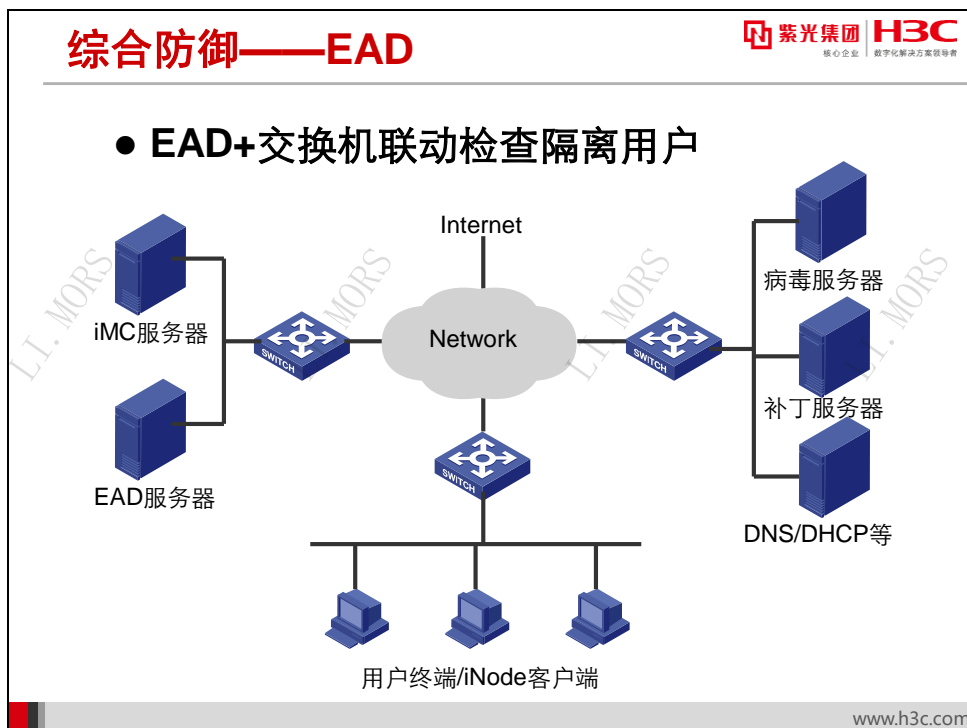


IP 网络最基本的功能是完成所有 IP 报文的正确传送，保证的业务正常运行。但这一切都基于网络的健康运行。如果网络发生故障或者受到攻击，正常的业务势必受到影响更或者导致业务中断。所以网络安全成为网络建设和维护考虑的重点。

确保网络安全的基本思想是正确的接入合法用户，防止非法用户的接入和攻击；控制流量沿正确的路径转发。针对合法用户和非法用户的判断区分，可以采用常用的各种身份认证和授权技术。针对流量控制则可以采用包过滤技术。

常见的身份认证和授权技术有 802.1x 认证、集中 MAC 地址认证、Portal 认证以及综合 802.1x 认证的端口安全技术。它们基本上都依赖于 RADIUS 或 TACACS 协议完成身份认证和授权。

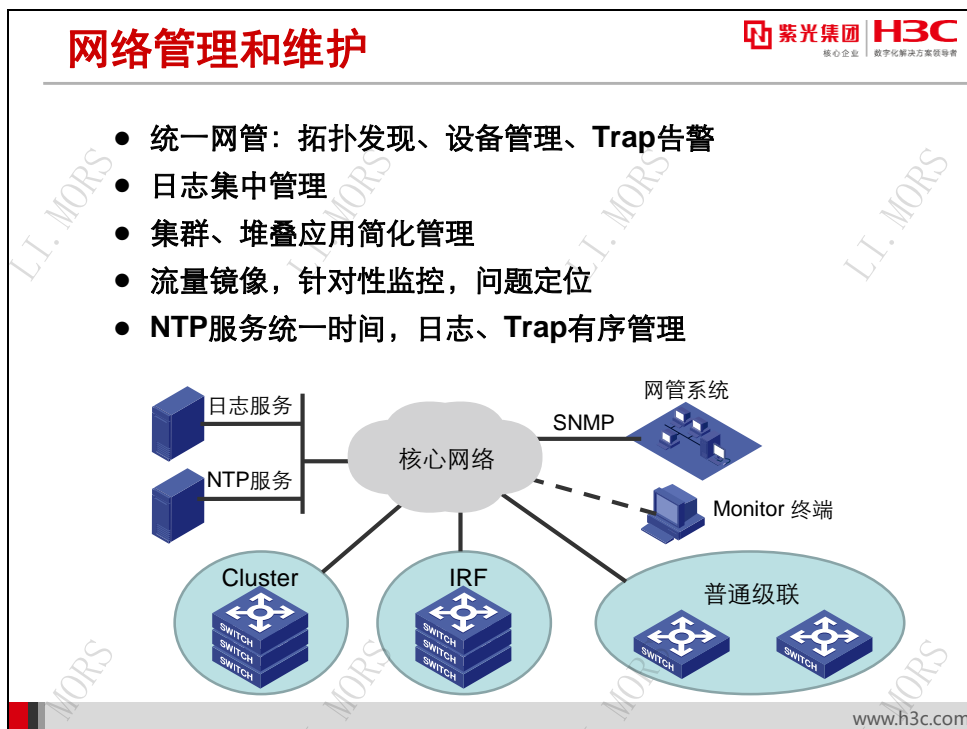
包过滤技术主要用于在网络接入层拒绝非法流量进入网络，或在汇聚层和核心层用于保护重要资源不被随意访问。



网络安全的部署从更广泛的意义来看，不能仅限于网络设备的安全技术，而应该采用立体式综合防御。它涉及网络设备、终端用户以及管理网络设备和终端用户的一系列服务器。H3C推出的EAD（Endpoint Access Defense）综合解决方案综合了多种安全技术，能够从全方位实施安全防御。

EAD解决方案采用服务器、客户端和网络设备联动的方案实现用户的身份认证、业务授权和行为控制。在终端用户安装客户端软件对主机进行身份认证和一系列的健康检查，并报告检查结果给服务器。服务器则根据检查结果通知网络设备执行相应的隔离或授权行为。对于被隔离用户通过客户端软件进行健康检查恢复，如更新防病毒软件的病毒库，下载操作系统补丁软件等。健康检查成功后即可接入网络。上述立体防御可确保接入到网络中的终端用户都是安全可靠的，从而从根源上保证了网络的安全。

### 3.6 网络管理和维护应用



网络的健康运行离不开有效的管理，网络故障的快速定位和恢复离不开有效的维护措施和维护技能。所以网络管理和维护同样成为网络建设者和网络使用者关注的焦点。

网络规模的进一步扩大化，业务的进一步复杂化使得网络管理员无法继续采用单台设备独立管理的模式。用于网络设备通用管理的 SNMP（Simple Network Management Protocol）协议发展起来。被管理设备上的标准 MIB（Management Information Base，管理信息库）实现了设备的工作状态记录。网管系统则通过 SNMP 协议对网络设备的工作状态进行查询，据此描绘网络拓扑，对参数进行设定，并接收来自网络设备的主动告警。这大大提高了网络管理的工作效率，加快了对网络故障的反应速度。

网络设备的日志是反映设备工作状态的另一重要信息，对网络设备日志信息的有效管理也犹如对告警信息的管理一样重要。采用日志服务器集中收集并处理各网络设备的日志信息也是常用的网络管理手段之一。

网络设备的急剧增长使得网管工作站的任务也变得非常繁重。网络设备和网络自身的简化也成为网络建设和管理关注的内容。由此应运而生的集群（Cluster）和堆叠（Stack）技术在简化网络管理方面也起到了重要作用。集群和堆叠都可以将多个设备联合起来形成一个管理单元，使得网管系统所见的管理单元大幅减少。

网络管理的另一重要任务是对网络健康状况进行检查和监控，并对网络的未来建设提出正确的方案。因此网络当前流量的分布和网络资源的占用状况也是网络管理员关注的内容。镜像技术是当前采用最多，部署最为简单的网络监控方法之一。除此之外，镜像技术也是网络故障

定位的必要手段之一。通过特定的镜像技术可以将指定的流量（如协议报文）镜像到指定服务器并对其进行详细分析而定位问题。

当网络管理员检查日志信息和设备告警信息时，会发现记录的时间信息变得杂乱无序，其原因在于各网络设备的时钟没有同步。**NTP（Network Time Protocol）**的部署即可很好的实现各网络设备的时间同步。



## 3.7 本章总结

### 本章总结

- 多种冗余备份技术的应用
- 组播、语音业务的规划部署及注意事项
- 网络安全的部署及EAD解决方案
- 应用网络管理技术简化管理，高效维护

www.h3c.com

## 3.8 习题和解答

### 3.8.1 习题

1. 最适合于双归属网络的冗余备份协议是（ ）  
A. STP                      B. RRPP  
C. Smart Link              D. VRRP
2. IRF 冗余备份技术不仅实现了链路级的备份，也实现了设备级的备份。（ ）  
T. 正确                      F. 错误
3. IP 网络中组播业务的部署包含哪些重要协议？（ ）  
A. PIM                      B. RPF  
C. IGMP                      D. GMRP
4. IP 语音业务部署的重要措施有（ ）  
A. PoE                      B. QoS  
C. 语音报文识别          D. 数模转换
5. 常见的网络管理措施有（ ）  
A. SNMP 集中管理          B. 镜像  
C. 集群和堆叠              D. NTP

### 3.8.2 习题答案

1. C
2. T
3. AC
4. ABC
5. ABCD