

第 1 篇 大规模网络路由概述

第 1 章 企业网模型

第 2 章 大规模网络路由技术概述

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

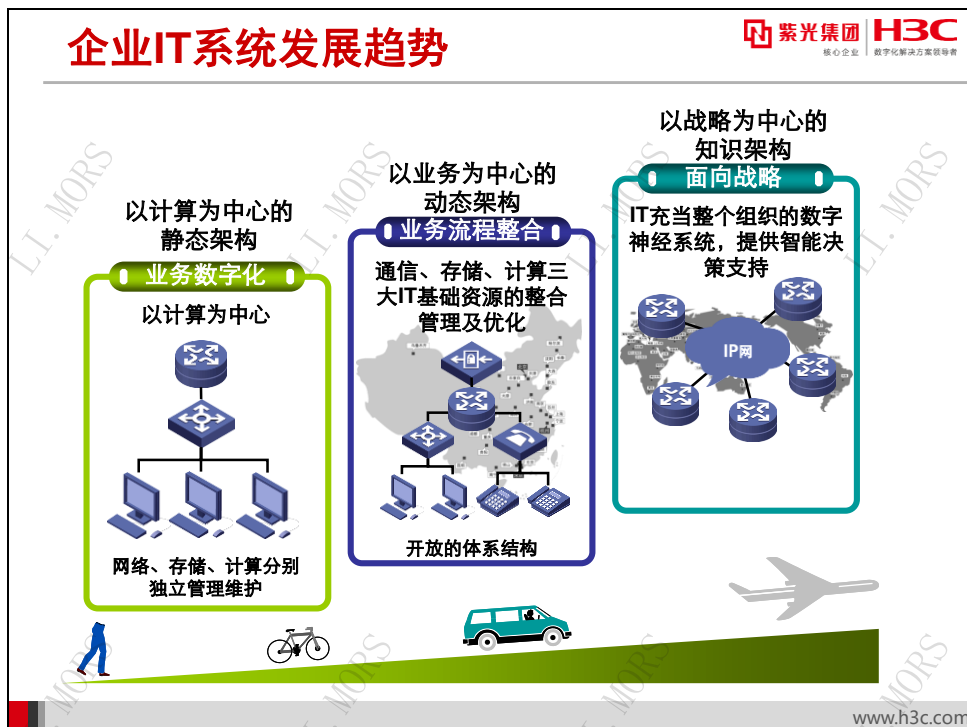
● 学习完本课程，您应该能够：

- 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。

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。

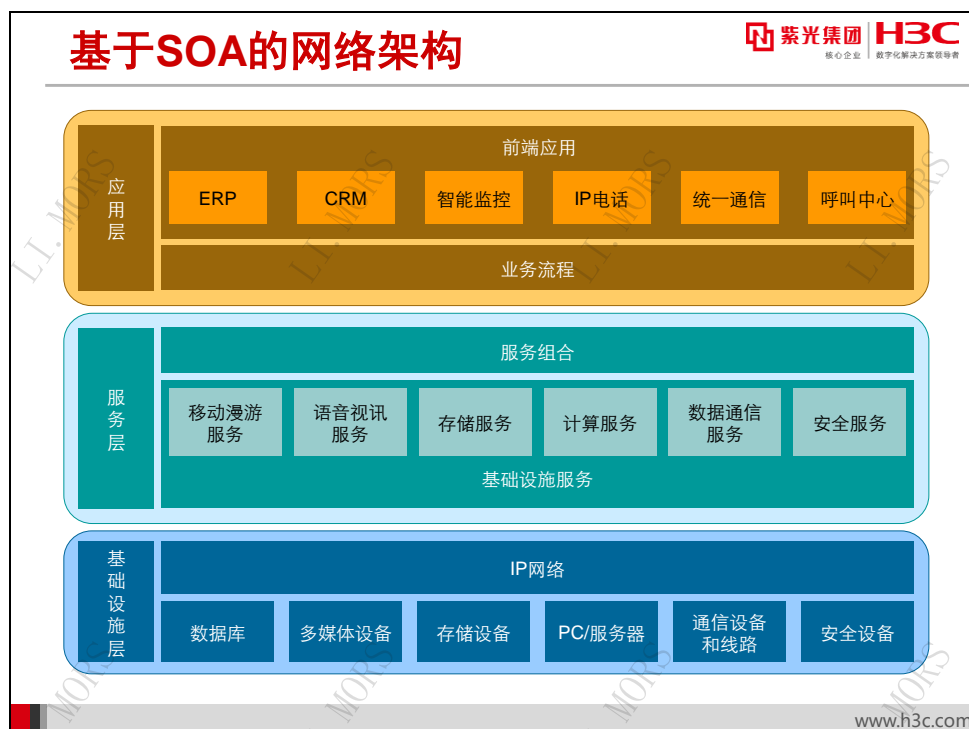
综上所述，组织机构不但需要不断提高网络性能，更需要构建可维护、可管理、可优化的品质网络。要解决各种难题，实现这个目标，就需要构建一个全面、精细、架构开放的智能管理系统。

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

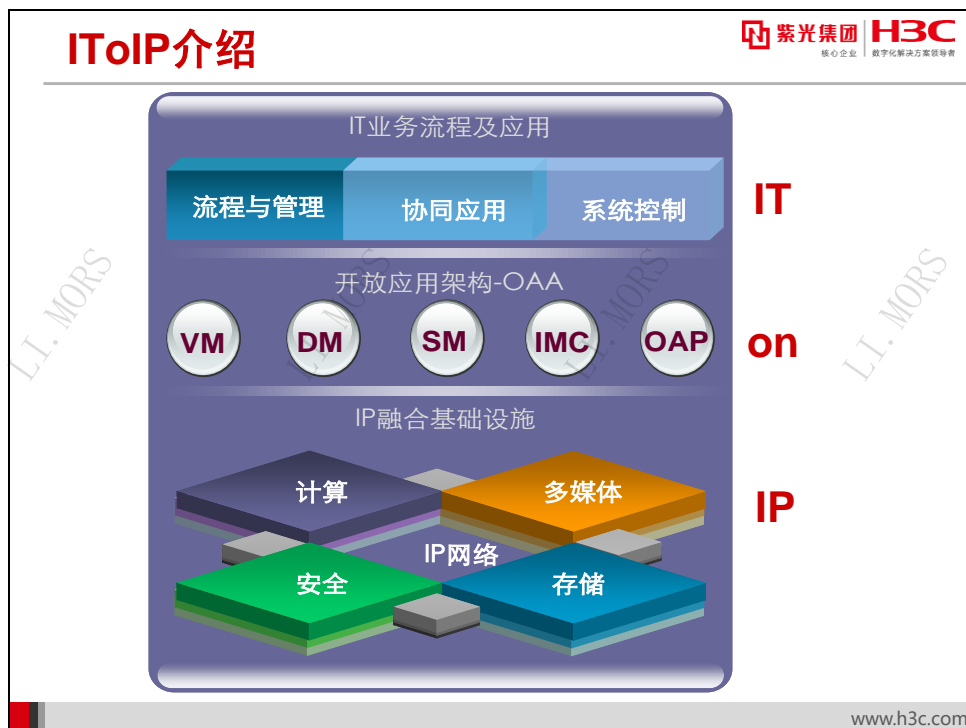


SOA（Service Oriented Architecture，面向服务的体系结构）是一种定义和提供 IT 基础设施的方式。体现 SOA 思想的企业级 IT 系统设计，应允许不同应用功能或应用系统之间共享数据、资源和能力，参与业务流程，无论它们各自背后使用的是何种软件和硬件。

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。



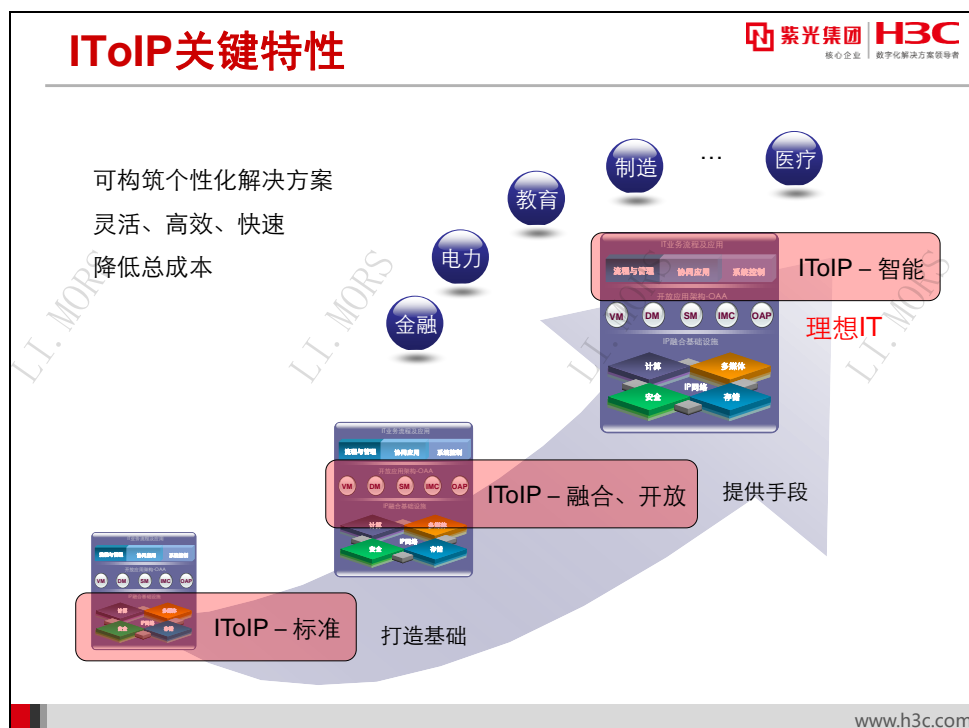
为解决 IT 系统和计算机网络发展过程中面临的种种挑战，H3C 在 2004 年提出了 NGen（下一代 e 网）架构。基于这个架构，H3C 不断完善 IP 基础网络、IP 通信、IP 管理、IP 存储等解决方案板块，最终形成完全基于 IP 技术的新一代 IT 解决方案——IToIP（IT on IP）。

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。

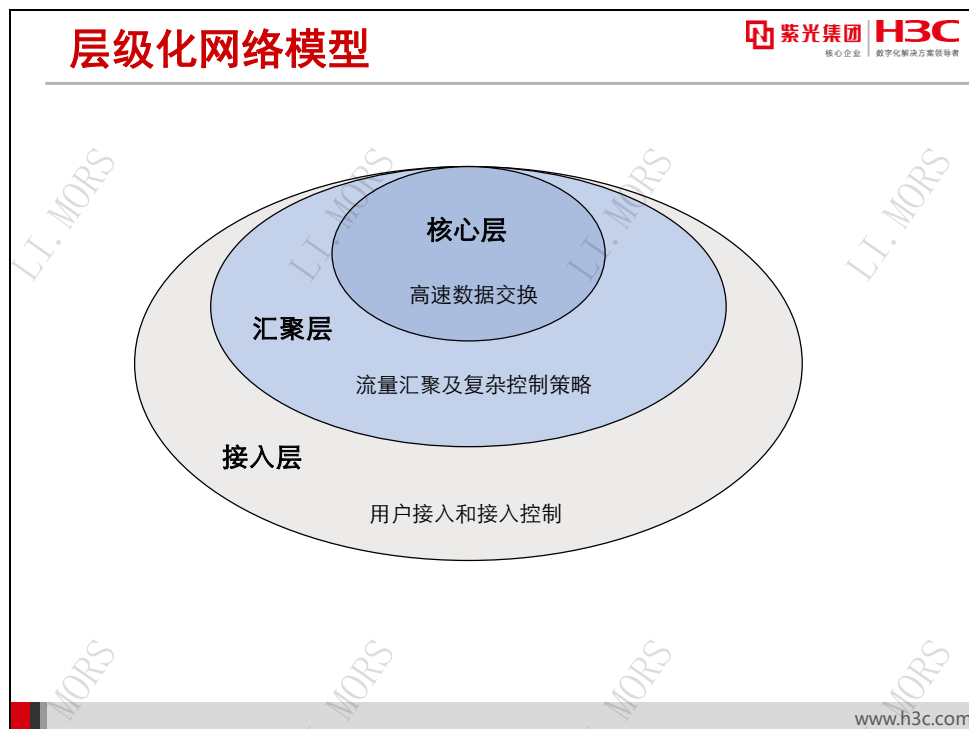
当今的 IT 系统建设进入整合时代，需求的重心从单系统的性能转向跨系统的性能、连通、业务互动。依托 IP 网络融合 IT 基础架构，提供整合平台，实现基础架构资源化，基于应用灵活组织 IT 资源来支撑复杂多变的业务，这些已经成为 IT 系统建设中普遍认同的理念。IToIP 解决方案指明了实现这一目标的途径，给出了达到这样目标的方案，使组织机构得以全面而系统地规划，并有序而分步地部署 IT 系统。



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 数字化解决方案领导者

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

紫光集团 H3C
核心企业 数字化转型领导者

www.h3c.com

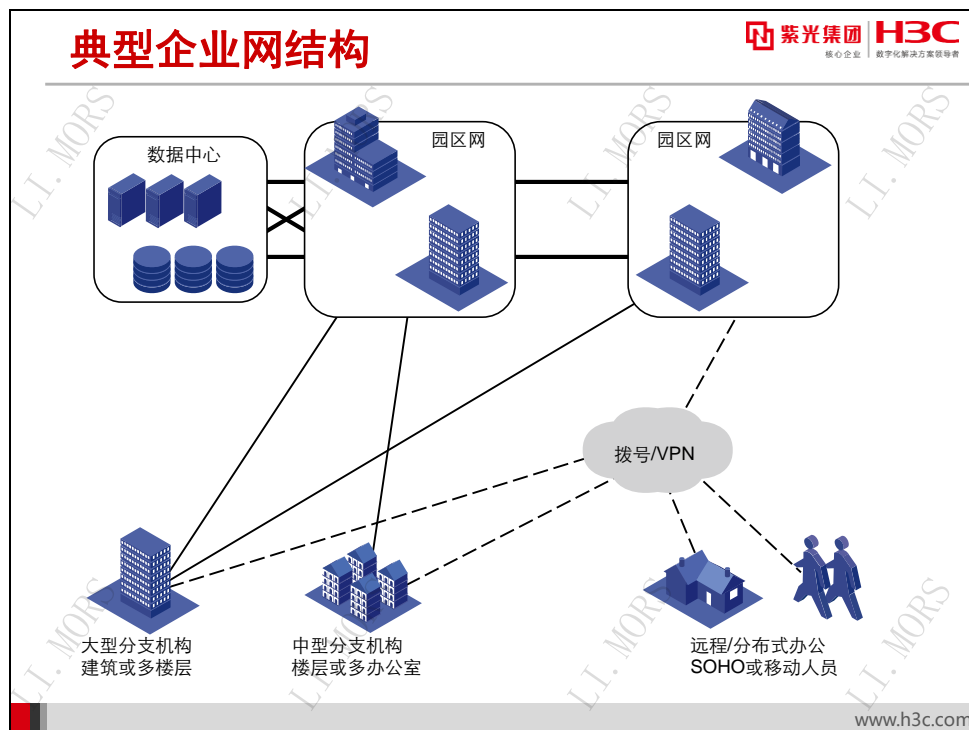
层级化网络模型的引入具有以下优点：

- 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：

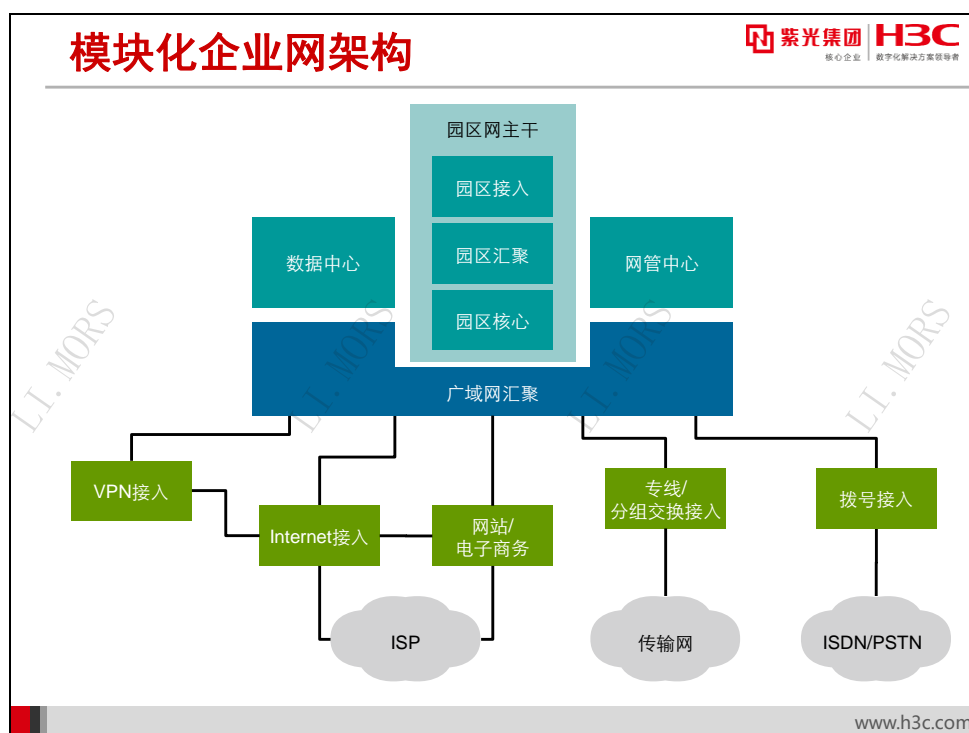
- **园区网**：园区网通常是大型企业网络的核心，每个园区包括若干建筑物。园区网通常采用包括核心层、汇聚层和接入层在内的 3 层网络结构。园区每一建筑内的网络都包括汇聚层和接入层，在汇聚层采用性能较高的三层交换机实现建筑内的汇聚；在接入层使用楼层交换机连接到桌面计算机。各建筑网络通过高速局域网技术连接到高性能的园区网核心层设备上。园区网之间通过高速城域网或广域网进行连接。
- **大型分支机构网**：这种机构通常是区域性的行政中心，可能独占一栋大楼或占据大楼中的多个楼层。其自身可能采用 2~3 层网络结构。其接入层和汇聚层与园区内的建筑网类似。大型分支机构网通常需要使用性能较好、可靠性较高、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 大规模网络路由技术概述

随着网络规模的扩大，其对路由技术的可靠性、可扩展性、可管理性的要求越来越高。本章介绍典型的大规模网络路由模型，及其对路由技术的需求等。

2.1 本章目标

课程目标

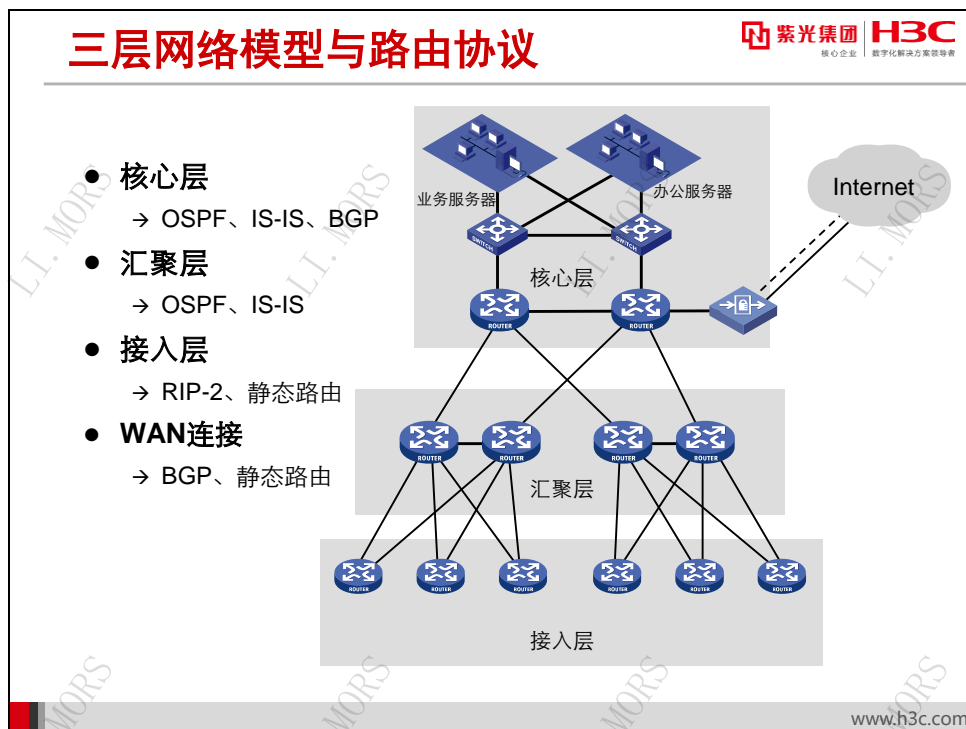
● 学习完本课程，您应该能够：

- 理解典型网络路由的模型
- 理解大规模网络对路由技术的需求



www.h3c.com

2.2 三层网络模型与路由技术



一个典型的大规模网络，根据功能可划分为接入层、汇聚层、核心层三层。各层对路由的要求有所不同，所推荐使用的路由协议也有所不同。

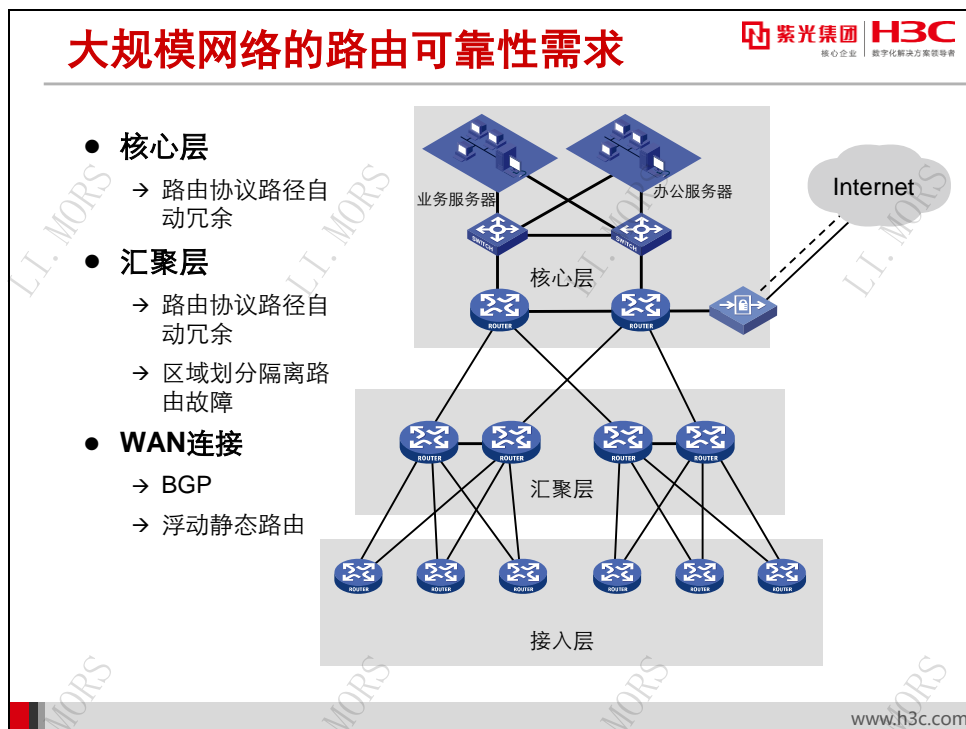
- **核心层：**核心层是网络的骨干，提供高速数据转发和路由快速收敛，具有较高的可靠性、稳定性和可扩展性等要求。所以，通常核心层采用收敛速度快、扩展性好的路由协议，如 OSPF、IS-IS 等。如果网络规模很大，如在 ISP 网络，为了便于实现路由控制，确保高速路由转发，也会采用 BGP 协议作为核心层协议。
- **汇聚层：**汇聚层负责汇聚来自接入层的流量并执行复杂策略，所实现的路由功能包括路由聚合、路由策略、负载均衡、快速收敛等。所以，在路由层面上，汇聚层通常采用收敛速度快，支持路由聚合、负载分担，易于实施路由策略的路由协议，如 OSPF、IS-IS 等。
- **接入层：**接入层提供网络的用户接入功能，所以通常接入层采用配置简单，占用系统资源少的路由协议如 RIPv2、静态路由等。也可以采用 OSPF 的 Stub 区域或 IS-IS 的 Level-1 区域，以减少区域中路由数量，并降低接入层路由变化对汇聚层的影响。

大规模路由网络通常使用 BGP 或静态路由接入 Internet。使用 BGP 接入可以更好地控制路由的发布与接收；而使用静态路由可以节省网络开销。

并不是所有的路由网络都必须划分为三层。层次越多，网络拓扑也就越复杂，所使用的协议可能也会越多，从而增加配置与维护的难度。在设备能力允许的情况下，也可将网络划分为

两层，将接入层的功能集成在汇聚层中。因 OSPF、IS-IS 协议支持两层划分，与两层网络契合可简化部署与配置。

2.3 大规模网络对路由技术的需求



在其发展初期，网络对可靠性的要求并不很高。而伴随着规模的扩大和业务的发展，越来越多的业务需要依靠 IP 网络来进行，对网络的可靠性需求越来越突出。

在大规模路由网络中，所有的数据流量都经由核心层和汇聚层转发，所以其可靠性要求尤其高。因此在设备层面，核心层和汇聚层通常都采取双设备配置，为下层设备提供双归属的上行链路；而在协议层面，核心层和汇聚层都采用动态的路由协议如 OSPF、IS-IS，利用路由协议自动发现冗余的下一跳，并在故障发生时能够自动切换。

同时，汇聚层还承担起故障隔离功能。当接入层路由产生故障时，使路由变化尽可能少地扩散到核心层，而不致引起核心层的路由动荡。可以通过在汇聚层上进行适当的路由协议区域划分，配合以路由聚合，来隔离接入层的路由故障。

如果网络只通过一个出口设备的两条链路连接到 ISP，则可以使用浮动静态路由。通过调整静态路由的优先级，使一条链路为主，另一条链路为备，或二者互为备份。

如果网络通过多个出口设备连接到 ISP，则使用 BGP 是较好的选择。BGP 可以动态学习到 ISP 发布的路由，且能够实现出口选择策略和多出口互相备份。

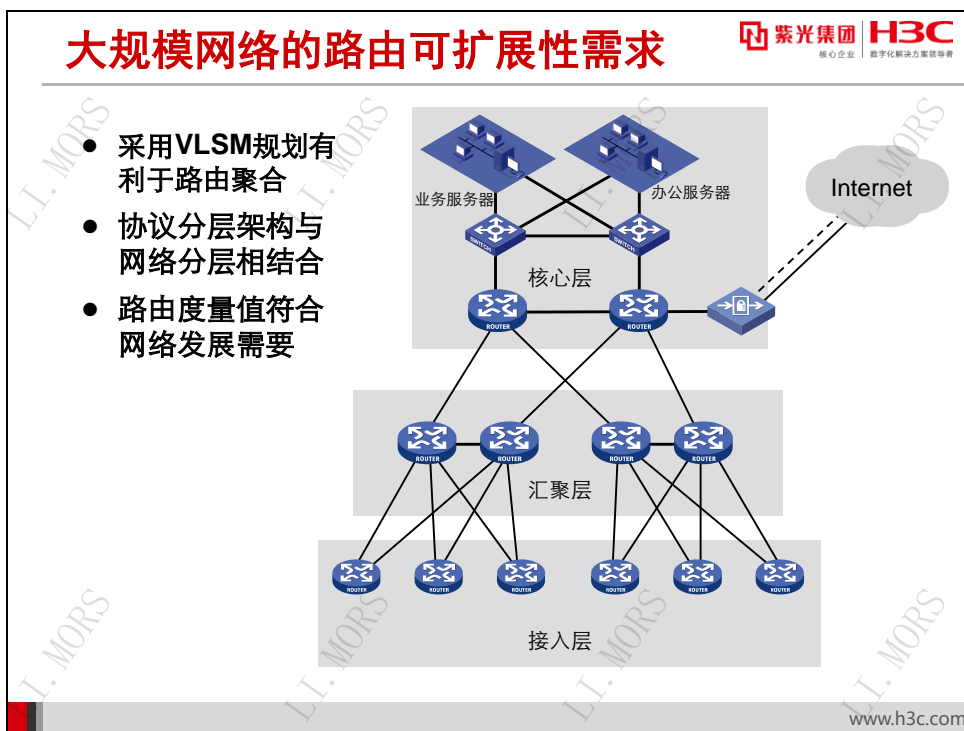
说明：

故障次数少、恢复时间短是高可靠性网络的两个特征。可以用“可用性 (Availability)”这一指标来度量网络的可靠性：

Availability=MTBF/ (MTBF+MTTR)

MTBF: 平均无故障时间 (Mean Time Between Failures)

MTTR: 平均修复时间 (Mean Time To Repair)



网络的可扩展性需求是一直存在的。而大规模网络重建成本高，对可扩展性的要求就更高。

网络的可扩展性体现在以下几方面：

- 站点与设备的增长不会引致路由增长不可控：

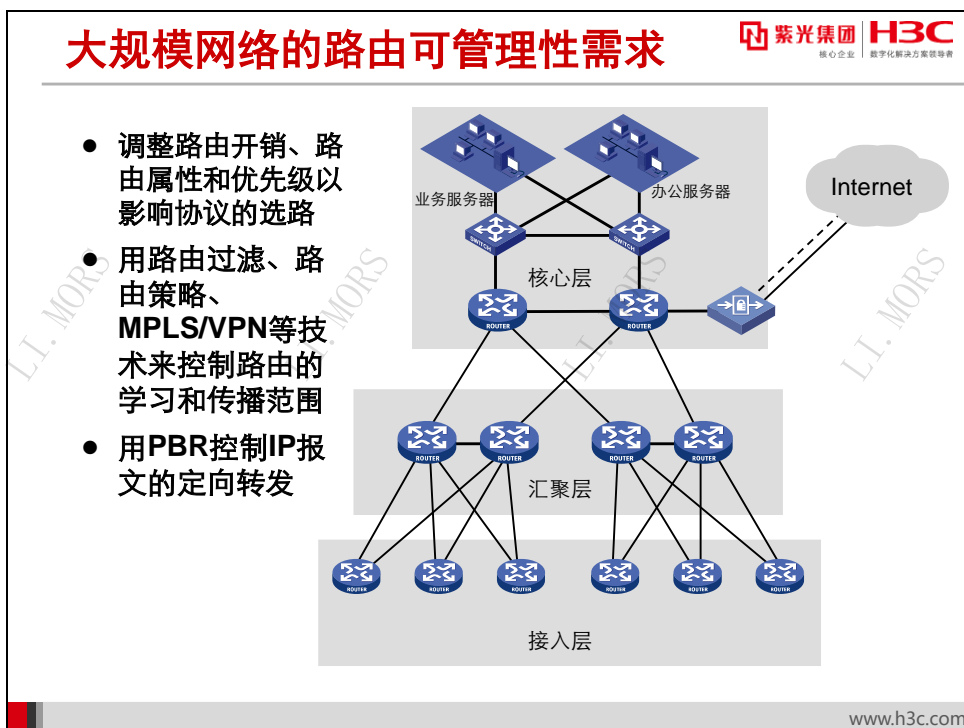
在划分 IP 地址时采用 VLSM 技术，全网统一管理 IP 地址资源，按需将 IP 地址分配给不同站点，并尽量做到地址块连续和可聚合；在每一层连接下一层的设备上，采用路由聚合技术，将下一层具体路由聚合成地址范围大的路由，从而减少核心设备上的路由数量，使站点数量的增长不会引起核心设备路由的爆炸增长。

- 网络的各层之间相对独立，某层内拓扑变化尽量不影响另一层：

使用分层架构的路由协议如 OSPF、IS-IS，并在设计上将协议的区域与网络层次结合起来，从而使某一区域（网络层次）中网络拓扑的变化尽可能不传到另一层中。

- 路由度量值能够适应网络规模与链路带宽的增长：

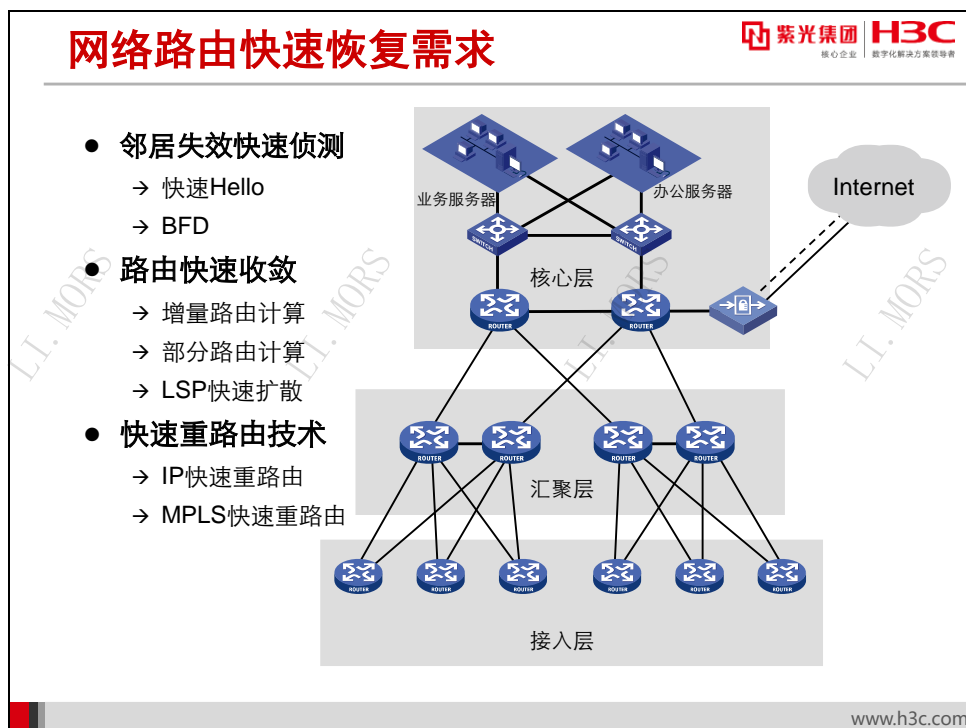
RIP 路由协议只能度量 15 跳的网络，且度量值以跳数为标准，不能正确反映网络中的链路带宽。而 OSPF 与 IS-IS 以路径开销（Cost）为度量，开销基于链路带宽计算，不但更加合理，而且能够度量更大规模的网络。



随着网络技术与通信技术的融合，在 IP 网络平台上可实现电话、传真、音视频会议、办公协作等众多应用服务的统一；同时，通过开放应用接口，网络可实现与企业 IT 应用、办公系统、及生产系统的融合，形成一个全 IP 的统一通信平台。在这个通信平台上，如何合理利用网络资源，满足各种应用需求就显得尤为重要了。

路由的可管理性可通过以下技术来实现：

- 通过调整路由开销、路由属性和优先级影响协议的选路：
各路由协议都能够进行开销的手工调整；BGP 协议还有丰富的路由属性（如本地优先级、MED 值）可以调整。
- 通过路由过滤、路由策略、MPLS/VPN 等技术控制路由的学习和传播范围。
- 通过 PBR（基于策略的路由）控制 IP 报文的定向转发。



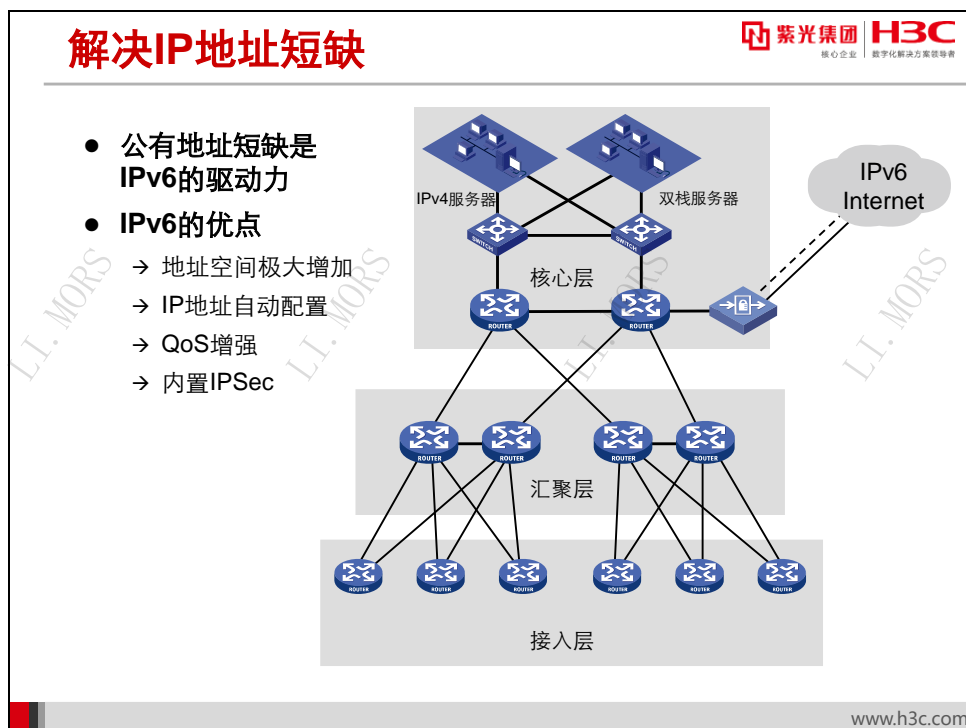
如 IP 电话、视频会议等实时业务对 IP 承载网的服务质量要求较高。一方面要求网络传输的时延要小，以满足业务的实时要求；另一方面要求网络发生故障时，能够快速侦测并避开故障点。

在大规模网络中，路由变化的传播距离远，收敛速度慢。为加快收敛速度，减少对实时业务的影响，可使用以下技术：

- 邻居失效快速侦测技术：路由协议都有邻居失效侦测机制，通常是用定时器来探测邻居失效。但定时器的缺省时间较长，邻居失效要用很长时间才能感知。通过适当调整定时器，如在 OSPF 中缩短 Hello 时间，可以更快的探测到邻居失效。

独立于路由协议之外的邻居检测技术，如 BFD（双向转发检测），可以为各上层协议如路由协议、MPLS 等统一地快速检测两台路由器间双向转发路径的故障。通过使用 BFD 与上层协议联动，可以使路由协议探测邻居失效的时间缩短至毫秒级。

- 路由快速收敛技术：不同的路由协议有不同的收敛速度，取决于路由算法和路由器的资源。通过采用一些机制，如在 IS-IS 协议中采用 I-SPF（增量路由计算）、PRC（部分路由计算）、LSP 快速扩散等机制，可以极大加快链路状态型路由协议的收敛速度。
- IP 快速重路由技术：在网络发生故障后，通常需要等待一定时间，待路由收敛后才能进行数据转发。而通过使用 IP、MPLS 快速重路由技术，能够使路由器在路由未收敛前，使用预先设定的备份下一跳替换失效下一跳，通过备份下一跳来指导报文的转发，从而大大缩短了流量中断时间。



随着因特网及其上所提供的服务不断地突飞猛进的发展，目前使用的 IPv4 已经暴露出一些不足之处，其中最主要的问题是 IP 地址短缺。IPv6（Internet Protocol Version 6，因特网协议版本 6）是 IPv4 的升级版本，能够从根本解决 IP 地址短缺的问题，另外其在地址自动配置、服务质量等方面有所改进。

IPv6 的地址长度为 128 位，地址空间为 3.4×10^{38} 个，大到可以使世界上的每个人都拥有 5.7×10^{28} 个地址。

另外，IPv6 具有其它的一些优点：

- IPv6 采用全新的邻居发现协议，能够不通过 DHCP 协议而对网络中的终端主机进行 IP 地址和网关的自动配置。
- IPv6 头中除了数据流类别（Traffic Class）字段外，还新增加了流标签（Flow Label）字段，用于识别数据流，以更好地支持 QoS。
- IPv6 提供了两种扩展报头，使得其天然支持 IPSec，为网络安全提供了一种标准的解决方案。

2.4 本章总结

本章总结

- 三层网络中各层对路由技术有不同的要求
- 大规模网络要求路由技术具备可靠性、可管理性、可扩展性
- IPv6技术彻底解决IPv4地址短缺

2.5 习题和解答

2.5.1 习题

1. 典型大规模路由网络可能包含以下哪些层？（ ）
A. 核心层 B. 汇聚层
C. 接入层 D. 物理层
2. 以下哪些特性是典型大规模路由网络的核心层所必须具备的？（ ）
A. 可靠性 B. 可扩展性
C. 接入服务 D. 丰富策略
3. 以下哪些路由协议比较适合在大规模路由网络的汇聚层中使用？（ ）
A. OSPF B. RIP
C. 静态路由 D. BGP
4. 以下哪些特性可以控制路由传播范围，从而增加网络的可管理性？（ ）
A. PBR B. 路由过滤
C. 路由策略 D. 快速重路由
5. 哪些技术能够最终解决 IP 地址短缺问题？（ ）
A. 路由快收敛 B. NAT
C. IPv6 D. BFD

2.5.2 习题答案

1. ABC
2. AB
3. A
4. BC
5. C