



思科智能联网生产解决方案

目录 CONTENTS

1

前言

1

1.1 制造业企业的发展趋势——“网络就绪”

1.2 如何建成“网络就绪”的制造企业

2

制造业企业智能联网应用及特点分析

3

2.1 企业管理的信息化

2.2 企业核心生产业务系统的信息化

2.3 企业研发和设计系统的数字化

2.4 咨询、服务及销售的网络化

2.5 如何正确理解制造业企业智能联网的网络属性

3

制造业企业智能联网典型解决方案简介

8

3.1 管理信息系统网络

3.2 制造及生产系统核心网络

3.3 设计系统核心网络

3.4 咨询及服务销售网络

4

制造业企业智能联网生产相关网络技术及解决方案简介

13

4.1 适用于生产系统和管理信息系统的高可靠性、高性能和高扩展性的园区网络

4.2 适用于生产系统和办公系统的灵活可靠的无线网络

4.3 适用于网络化销售的经济有效的企业广域网络连接

4.4 远程移动办公人员网络接入

4.5 适用于企业通讯系统的基于融合型网络的 IP 电话与视频会议系统

4.6 适用于企业文化传播与员工教育的电子化学习系统

4.7 借助 Cisco Catalyst 6500 系列交换机增强企业网络的安全性 42

4.8 企业数据库服务器与应用服务器的负载均衡

4.9 企业网络管理同样重要

4.10 思科网络对企业 ERP 应用的网络优化

5

总结——为什么选择思科公司

34

1 前言

制造业企业的发展趋势——“网络就绪”

随着全球经济的发展，制造企业的生存环境出现了前所未有的深刻变化：

一是企业经营的行业和地理界限日渐消失，跨行业、跨地区经营成为企业扩大规模、持续发展的必由之路。海尔集团是从冰箱做起的，现在已广泛涉足家电、电脑、通信、物流等多个领域，经营范围遍布全球。思科公司最早生产的是路由器，现已成为全方位的电信级、企业级以至家庭级网络设备供应商。

二是客户需求不断改变，靠单一的产品已经不能满足客户需求。从某种角度说，不是客户需求本身在变，而是因为竞争使产品更加丰富，客户选择的余地越来越大。今天你的这款产品还很畅销，也许明天就有竞争厂家推出另一款能更好地满足客户需求的替代品。如果你不求变，你的产品就卖不出去。在发展节奏日益加快的 21 世纪，“变”就是永恒的主题，“不变”就会面临吃不上“奶酪”的困境。

企业要如何改变？如何才能做到与时俱进？用逆推的方式考虑，企业要有更强的产品研发能力，适时推出新产品；要压缩产品生产周期，尽量缩短产品从研发到上市的时间；要提高产品精度和加工装配效率，提高产品质量。与此同时，降低成本、增加利润，用更小的投入产出更多的产品，也是企业经营管理的应有之义。

在面对这些变化的早期阶段，企业因应变化的策略是细化分工，在产品研发、生产制造、市场营销三个环节中侧重于自己专长的环节。

拥有核心技术优势的企业专注于产品研发，靠独有技术、专利产品获得价值，而把制造、产品销售的工作交给下游企业完成，Intel、微软、思科等都是这类企业的代表。

另一部分企业则选择大规模加工生产、组装、集成作为自己的立足点，以高效率、低成本的产品制造赢得客户，在我国台湾地区就有大量这类的 OEM 制造商。

还有一类企业，专注于掌握产品销售渠道，甚至经营自己的品牌，研发和制造都借助外力完成，这类企业一般需要熟悉市场、接近客户，神州数码、晓通电子等都在朝这个方向发展。

分工的结果，是扬长避短，各自都有美好的前程。

做企业犹如逆水行舟，不进则退。那么，分工之后的下一步是什么？分工带来了上下游企业协作的问题，原来在一个企业内部的事情，分散到不同的企业去了。新研发出来的产品如何准确、及时交给制造企业实现规模化生产？生产与销售（客户需求）如何保持有效沟通，做到既满足市场需要，也不供过于求？销售端获得的市场反馈如何反应到研发环节去？企业内部如何进一步提高管理效率？一系列问题浮现出来。怎么办？

答案就是“网络就绪”（Net Ready）。

“网络就绪”就是企业的研发、生产、经营、管理、对外协作等各项活动完成智能联网，实现高效的信息沟通，提高管理效率，提高车间生产的控制精度，实现柔性制造。“网络就绪”是思科的网络产品技术在本公司实践经验的总结，思科著名电子商务专家以此为题撰写的专著，在全球企业界引起极大的轰动。《网络就绪》目前也是当前清华、北大、复旦、对外经贸等高校的一门 MBA 课程。

如何建成“网络就绪”的制造企业

一家“网络就绪”的企业通常拥有如下图所示的网络总体格局，它从企业各部门职能上可划分为企业管理网络、企业研发网络、企业生产系统网络、企业营销网络四个部分。

企业管理网络

企业管理网络主要涉及办公管理系统和决策信息系统两类应用。例如，日程安排、法律文书管理、会议管理、信息发布、电子邮件、电话系统、远程电视会议系统、电子化学习系统等就属于办公管理系统应用，而企业资源计划（ERP）、人事管理（HR）、客户关系管理（CRM）、供应链管理（SCM）则属于决策信息系统应用。

企业研发网络

企业研发网络主要涵盖二维和三维电脑辅助设计应用、实验模拟及测试数据分析、客户采购行为的大量资料分析、分散式网络协同设计四类应用。

生产系统网络

企业生产系统网络，也就是车间网络，主要包括计算机辅助制造（CAM）、过程自动化控制、数据采集和测试三个方面。

营销服务网络

营销服务网络是连接企业各分支机构、营销点和加盟店的神经中枢。通过它实现销售数据实时传递、总部新政策/新产品信息发布、企业门户网站以及店面监控、广告播放等特殊应用。

图 1 网络整体格局



网络在企业生产、流通、服务等关键环节中正以不可替代的优势，扮演着“利用信息资源，协调生产成本，提高经济效益”的重要角色，它更多的超出了技术领域，而深具经济学内涵。其发挥的作用归根结底就是降低生产成本，增加经济效益。格罗莫夫（Gregory Gromov）曾经说过：“网络本身是一种计算机科学概念”。随着网络应用的发展，现在有了更丰富的注解：网络本身更具有经济学内涵。

我们愿用多年来在网络技术领域的专业经验，在制造业网络化管理、生产、经营和服务的征途中贡献我们的一份力量，为制造业的又一个春天增添几分色彩。

在这本小册子中，我们将深入分析制造业企业的各类应用，探讨如何通过思科端到端的网络解决方案，帮助制造业企业奠定坚实的基础，最终实现“网络就绪”。

2 制造业 企业智能 联网应用及 特点分析

任何一个成功网络的实施绝不是各种先进网络技术的堆砌,网络实施的最终目的是帮助企业经营者更好的拓展自己的业务,获得更大的投资回报。

网络系统的部署必须能够达到两个最根本的目的:一是帮助企业省钱,二是帮助企业赚钱。深刻理解制造业企业经营者所面临的问题,区分企业各类应用,是成功实施网络技术及部署的根本。

网络就绪的制造业企业在网络建设过程中应在以下四个领域,把握应用特点,选择最佳的厂商和解决方案。

图 1 网络建设的四个领域



企业管理的信息化

企业管理的信息化应用主要可分为两大类:办公自动化系统和决策信息系统。

办公自动化系统应用如:

OA 系统: 如日程安排、法文管理、会议管理、信息发布、业务讨论、电子邮件、信息流程的跟踪与监控等

电子化学习系统: 支撑企业员工的学习能力和企业文化的转变

办公通讯系统: 电话系统, 远程电视会议系统

决策信息系统应用如:

企业资源管理(ERP), 人事管理(HR), 客户关系管理(CRM), 供应链管理(SCM)

管理信息系统从用户分布上考虑, 涉及企业内部各职能部门。从地理位置考虑, 涉及企业总部、各地分公司和部分移动办公用户。从各类应用的数据流特性方面考虑, 有大批量的数据传输应用, 如文件传输、电子邮件等; 有对带宽和时延敏感的多媒体应用, 如 IP 电话、视频会议、电子学习等; 有关键的、实时性较强同时数据量较大的决策信息系统应用, 如 ERP、CRM。

大批量的数据交换要求网络设备具备良好的交换性能。一份业内分析报告指出, 随着企业规模和网络应用的种类的不断扩大, 未来三年内企业局域网的带宽需求将提升 10 到 20 倍, 广域网的带

宽需求提升 3 倍，这要求企业采用合理的网络规划设计，正确选择能适应当前网络需求并满足未来网络规模增长和新业务需求的网络设备。

各类决策信息应用需要后台的数据中心支撑，大量的应用服务器与数据库服务器需要能够提供高速的不间断访问服务，网络必须具备高可靠性。在网络交换设备以及服务器连接链路方面应充分考虑容错功能，并结合智能网络软件系统来实现故障的自动监测和恢复。

管理信息系统涉及的用户种类多，分布广，网络系统的安全性自然成为客户最关心的问题之一。如何保证企业核心数据不受内部及外部黑客的获取和篡改，如何保证应用服务器不受网络攻击的威胁等都是在网络建设中必须考虑和解决的问题。

制造业企业分散的生产及销售模式使各种基于 IP 数据网络的多媒体系统如 IP 电话系统应用、远程会议，电子学习等在办公系统中显示出重要的意义，与此同时，如何在相同的物理网络上支持不同类型应用的问题需要妥善解决。管理信息系统要求一个智能的、面向应用的网络平台，所有应用所要求的不仅仅是带宽，同样重要的是在具有识别、分类、划分优先级和保护关键业务应用能力的同时，还应具有对带宽敏感的多媒体及实时延敏感的话音应用的支持能力。

分支机构和出差在外的员工能否通过有效的方式远程连接企业的系统资源也是一个需要解决的问题。

管理信息系统的应用特点决定了办公管理网络对高可用性、网络安全及服务质量有特殊的要求。

企业核心生产业务系统的信息化

企业核心生产系统从用户分布上考虑，主要涉及一线作业的职能部门。从地理位置考虑，主要涉及企业各厂区，车间和相关设计单位。从各类应用的数据流特性方面考虑，有部分批量的数据传输应用，如 CAD 图纸的传输；有对移动性要求较高的应用，如库房的产品相关信息的处理；最为主要的是有大量关键的、不可中断的、实时性极强的应用，如流水线设备的实时监控数据的采集和产品测试结果的采集等。

向生产系统发送控制指令、从生产系统采集实时监控数据和产品测试数据，单次数据量较小，但频度高，次数多，最为关键的是不能有任何中断，网络系统的稳定可靠是该系统设计的重点。要求网络系统能提供 7 × 24 小时的稳定可靠服务，在网络交换设备、模块以及连接链路方面应充分考虑冗余备份功能。

核心生产系统要求绝对稳定可靠，网络系统的安全性自然是关键。如何保证企业核心生产系统不受内部及外部的网络攻击威胁是在网络建设中必须重点考虑和解决的问题。

分布在厂房和车间等地的信息点数量较多，随着企业规模不断扩大，该部分信息点的急剧增加需要在网络规划设计时认真考虑，网络设备应能适应当前网络需求并满足未来网络规模增长的需求。

光纤和双绞线的连接方式可以满足大楼内部的网络连接需求，但对于企业厂区内部分厂房，仓库等一些不利于布线或布线成本高的环境，经济有效的网络连接解决方案需要考虑。

核心生产系统的应用特点决定了企业生产系统网络，也就是车间网络，主要包括计算机辅助制造 (CAM)、过程自动化控制、数据采集和测试三个方面。用户主要分布在一一线作业的职能部门，涉及企业各厂区、车间和库房等。其应用特点是：有大量关键的、不可中断的、实时性极强的应用，如流水线设备的实时监控数据采集和产品测试结果采集等，网络一旦中断，将造成生产停顿、材

料和零部件报废等重大损失；有对移动性要求较高的应用，如库房的产品相关信息的处理。因此，这部分网络系统对于高可用性及高扩展性有特殊的要求。

企业研发和设计系统的数字化

企业研发和设计网络主要涵盖二维和三维电脑辅助设计应用、实验模拟及测试数据分析、客户采购行为的大量资料分析、分散式网络协同设计四类应用。

其用户分布涉及企业各设计科室和相关协同设计单位，其特点是：有部分大批量的数据传输应用，如访问产品设计资料库和CAD数据的传输等；有部分多媒体数据流的传输需求，例如在线视频交流。

该网络系统对高性能及网络安全有特殊的要求。

咨询、服务及销售的网络化

咨询、服务及销售的网络化主要包含两类应用：企业门户网站建设和网络服务和营销系统

企业门户网站建设：提供企业相关信息、服务对象覆盖的范围和可提供的服务内容等

网络营销系统：如网上销售系统

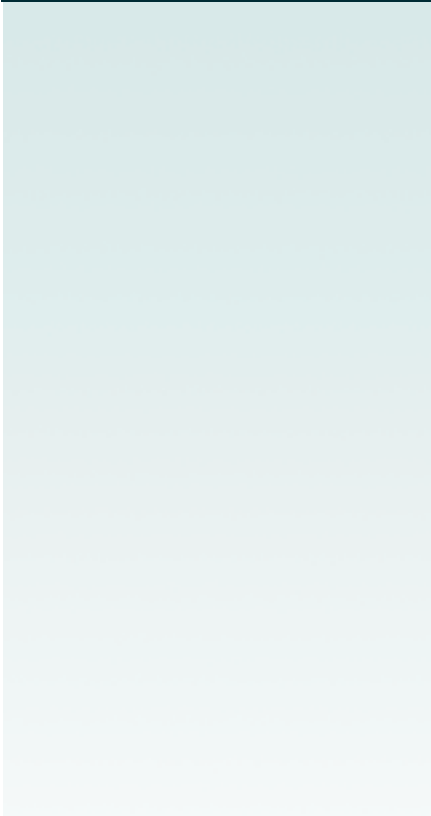
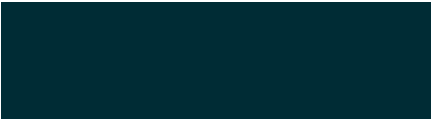
咨询、服务及销售的网络化系统从用户分布上考虑，主要涉及服务和销售部门。从地理位置考虑，主要涉及异地和远程的分支机构、分公司、办事处等。从各类应用的数据流特性方面考虑，有部分批量的数据传输应用，如文件传输、电子邮件等；有对带宽和时延敏感的多媒体应用，如IP电话、视频会议、电子学习等；有关键的、实时性较强的应用，如网上销售系统。

对于一定规模的制造/销售型企业来说，企业在各地大多会有制造基地或销售分支机构，如何将企业分支机构网络与总公司进行经济有效的跨地域网络连接是该部分网络设计所要解决的问题。传统的DDN或帧中继等专线连接方式对企业造成了高昂的线路租用费用，这些费用可能占到企业网络成本的40%-60%。

分散的服务及销售机构使基于IP数据网络的通讯系统如IP电话系统、远程视频会议等体现出较大的应用优势，同时电子化学习也显示出重要的意义。在广域网链接带宽非常宝贵的情况下，支持包含多媒体应用在内的不同类型应用的问题需要妥善解决。

咨询、服务及销售系统涉及的用户分布广泛，同时由于网络销售等系统直接连接至Internet，网络系统的安全性自然是该部分网络设计的重点。如何保证企业合法用户充分享用网络资源，同时保障核心数据不受内部及外部攻击的威胁，是在网络建设中必须考虑和解决的问题。

咨询、服务及销售系统的应用特点决定了该部分网络对高可用性、虚拟专网、高扩展性、网络安全及服务质量有特殊的要求。



如何正确理解制造业企业智能联网的网络属性

综合制造业企业网络各个部分对网络属性的需求如下表：

表 1 网络各个部分对网络属性的需求

	企业管理网络	企业研发网络	生产系统网络	销售服务网络
高可用性	★		★	★
高性能		★		
高可扩展性			★	★
虚拟专网				★
服务质量	★			★
网络安全性	★	★	★	★
一体化网络	★			★
网络管理	★	★	★	★

真正理解各项网络属性是网络建设成败的关键

什么是真正的高可用性？

高可用性必须是一个端到端的网络目标。网络设备、服务器集群、操作系统及网络接口卡必须作为一个统一的生态系统协同工作，以恢复任何服务器、链路或网络设备的故障。

在考虑设备硬件可靠性和连接链路冗余性的同时，应关注网络系统在不同层次上对系统可用性的软件功能支持能力，另外容易被忽略的高可用性因素——系统软件发布的质量。网络设备中运行的软件必须是经过严格测试的成熟软件，如果一台设备已经到了现场还在修改，那肯定不能说是高可用的，更不能说这表明供应商服务到位，量身定制。因为这种修改未经严格测试，在使用过程中极有可能发生意想不到的故障，造成网络瘫痪和经济损失。

高性能不能只看个别指标

在选择网络设备的时候，在对个别性能指标例如背板带宽、包转发速度等进行比较的同时，更应考虑网络在真实应用运行环境中的性能。例如，在大量组播、对时延敏感的应用存在的情况下，设备的性能怎么样？同样是 720Gbps 的背板带宽、400M PPS 的包转发速度，可能某些设备在各种复杂应用环境下都能保持高性能，而部分设备，在真实网络环境中的性能，也许还不及标称性能的 10%，因为通常他们标定的性能指标只是在特定环境下测试出来的数值。

除了设备可扩展性，还要考虑业务可扩展性

传统的可扩展性观念，主要是考虑是否可以增加模块、是否可堆叠以增加端口、是否可以增加设备等等，这只是网络可扩展性的一个方面。而人们长期忽视的另一个重要方面，就是网络在支持新应用和新业务方面的可扩展性。例如，你现在部署的网络，可能暂时不需要考虑 VoIP 语音应用、VPN 应用，可是当企业今后需要这些应用的时候，网络架构能支持吗？还是需要全部推倒重来？

虚拟专用网（VPN）需要端到端的解决方案

虚拟专用网（VPN）是一项对制造企业非常有用的技术，它可以给企业网络带来极大的安全性、经济性和移动性。但是，VPN 的部署是一项比较复杂的技术，因为它涉及遍布于广域网之上的多个设备，包括路由器、交换机、防火墙等等，涉及到语音、数据、视频等综合业务的支持。因此，

不能只看单个设备对VPN的支持,而要看整个解决方案的支持情况,要看厂商是否能够提供一个强大的VPN部署工具。

多一个心眼看 QoS

服务质量在应用系统较为简单的网络发展的初期,常常被对应于简单的概念,例如设备可以支持的队列数量等。在网络应用日趋复杂的环境下,如何在有限的网络资源里充分保障各类应用的实施,是一个非常复杂的问题,实施QoS,是端到端的概念,不是单个设备的问题,而是涉及整个园区网、甚至跨广域网的问题,就像城市交通一样,只是某一个路段宽阔,对于保持畅通几乎没有任何意义。QoS的管理和部署可能需要涉及到不同城市、不同厂区、不同大楼的每一台网络设备,甚至每一个端口。因此,在选择网络设备和供应商的时候,要擦亮眼睛看看供应商的QoS能做到什么程度。

网络安全性是一个系统问题

企业网络覆盖的范围越来越大,应用越来越丰富,可能受到的攻击无处不在。网络安全性首先是一个系统的概念,防火墙是网络安全中的关键组件,但防火墙不是一把万能的安全锁,数据传输的安全性、入侵检测以及用户安全认证等都十分重要。网络需要全方位、端到端的安全性,网络安全性的需求不仅限于园区网络,还要考虑与合作伙伴以及外网连接的安全性。在网络安全部署方面,如何高效地实施网络安全策略并有效管理各类网络安全设备,也是十分重要的。专业的网络安全厂商,应该对网络安全有全面的理解,循序渐进地为用户提供网络安全解决方案。

能否支持“一体化网络”

“一体化网络”是网络发展的必然趋势,国际上领先的企业,都部署了“一体化网络”的架构,在具备服务质量保证(QoS)的IP基础架构上,可以迅速部署许多创新的应用,例如统一消息、IP联络中心、端到端IP电话、视频系统等等。

从管理网络设备到服务管理

网络中设备日渐增多,交换机、路由器、防火墙、拨号访问服务器等等,不一而足;技术日趋复杂,以太网、千兆以太网、多媒体技术、语音、数据、视频集成、安全策略等等。随着IT基础设施规模不断扩大,复杂程度不断提高,用户的要求更加苛刻,管理费用逐渐增加,故障费用越来越高,网络边界不断延伸,安全威胁越来越大。发生问题时无从下手;人才市场缺乏经验丰富、受过专业培训的网路管理人员,所以这些因素都说明了一点,网络管理的方便性和人工成本是建设和改造网络时必须认真考虑的问题。目前,领先的网络设备供应商提供的网络管理工具已经实现了管理网络设备到服务管理的飞跃,而后起的网络设备供应商仍停留在简单的网络设备管理、看拓扑图的水平上。因此,只有选择领先的网络设备供应商,才能获得方便易用的网络管理方案。

针对制造业企业网络应用的特点和重点需要解决的问题,我们将在下面的内容中进行详细分析,并提出思科公司的完整的端到端的解决方案。

3 制造业 企业智能 联网典型 解决方案简介

制造业网络在不同领域的应用决定了网络系统设计模式、相关网络技术及网络产品的选型：

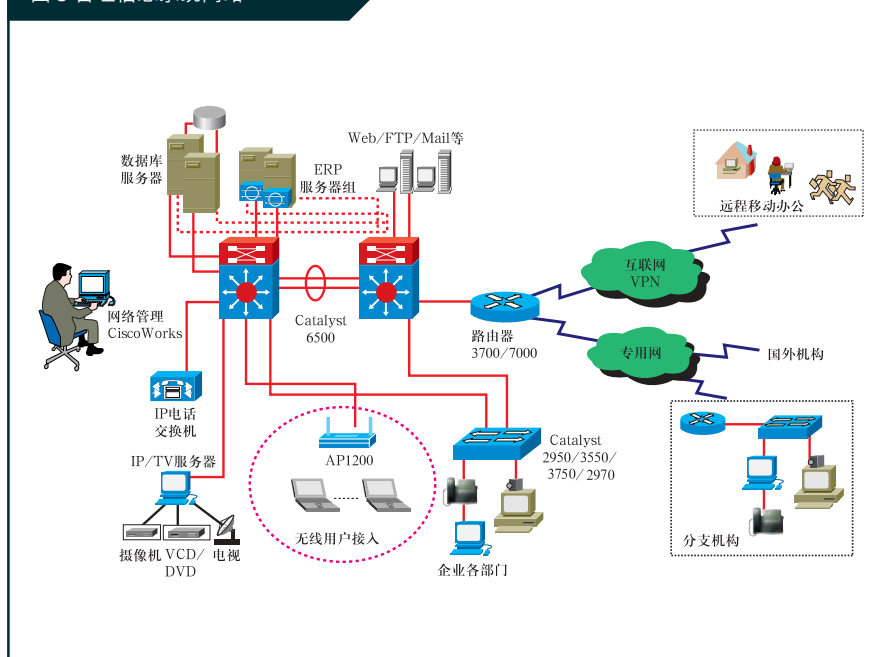
管理信息系统网络

可支持的应用包括：

- 办公自动化系统
- 电子化学习系统
- 企业通讯系统
- 远程用户接入系统
- 决策信息系统(ERP,HR,CRM,SCM)

网络设计如下图所示：

图 3 管理信息系统网络



高性能、高可靠性和高可扩展性

网络骨干采用两台思科公司高性能千兆主干交换机 Catalyst 6500 系列，每台交换机具有 720G 的背板交换能力，400MPPS 的包转发能力。二级交换机选用 Catalyst 3750、Catalyst 3550 或 Catalyst 2950，通过多条百兆或千兆链路与主干交换机连接，并提供 100M 到桌面。两台 Catalyst 6500 系列交换机互为备份，保证核心应用系统的不间断连接。

思科新推出的 Cisco Catalyst 3750 系列交换机是一个创新的产品系列，它结合业界领先的易用性和最高的冗余性，里程碑地提升了堆叠式交换机在局域网中的工作效率。这个新的产品系列采用了最新的思科 StackWise 技术，不但实现高达 32Gbps 的堆叠互联，还从物理上到逻辑上使若干独立交换机在堆叠时集成在一起，便于用户建立一个统一、高度灵活的交换系统--就好像是一整台交换机一样。这代表了堆叠式交换机新的工业技术水平和标准。

对于中型组织和企业分支机构而言，Cisco Catalyst 3750 系列可以通过提供配置灵活性，支持融合网络模式，已经自动配置智能化网络服务，降低融合应用的部署难度，适应不断变化的业务需求。此外，Cisco Catalyst 3750 系列针对高密度千兆位以太网部署进行了专门的优化，其中包含多种可以满足接入、汇聚或者小型网络骨干网连接需求的交换机。

主干交换机Catalyst 6500系列采用全模块化设计, 客户可根据需求任意组合接口模块, 通过增加新的接口模块也保证了系统可以根据用户业务发展的需要不断升级。

灵活的无线网接入

在企业办公区域中引入Cisco Aironet 1200无线网络解决方案, 既消除了布线成本和施工难度, 又提高了用户的流动接入网络能力。

服务品质保证 QoS

思科的所有网络设备均支持 QoS 功能, 保证了端到端 ERP 应用在任何情况下的优先传输。经过测试, 采用 QoS 后可以使 ERP 应用系统在网络发生拥塞时的响应时间提升 40% 以上。

安全性

采用 Catalyst 6500 系列交换机的防火墙服务模块 (FWSM)、安全插接层 (SSL)、服务模块和网络分析模块 (NAM) 以及入侵检测系统模块 (IDSM) 对网络进行全方位实时的监控, 一旦发生任何网络中的异常行为或非法侵入, 系统可根据客户预先设定的策略进行应对, 包括生成系统报警并中断非法连接等。另外运行于关键业务应用服务器 (如 ERP 服务器) 上的 IDS 软件系统可以为服务器提供专门的入侵检测和应对功能。网络 IDS 与服务器 IDS 方案的结合使用可以完全满足用户对网络安全的需要。

服务器负载均衡

采用 Catalyst 6500 系列交换机的内容交换模块, 为企业关键应用服务器 (如 ERP 服务器组) 提供高性能、经济有效的负载均衡解决方案。

经济实用的虚拟专用网

采用 VPN 技术通过 Internet 进行异地办公机构的远程连接可以大大地降低网络的运营开销和成本, 同时还大大增加了网络接入地域的范围, 十分适用于本客户高速发展的业务拓展需求。

完善的网络应用

IP 电话, 电视会议以及电子学习系统, 可以在办公管理和企业通讯领域帮助企业降低成本, 提高效率, 从而在激烈的竞争中取胜。

分支机构的连接

Cisco 1700/2600XM/3700 系列路由器可以支持各种类型的广域网连接方式, 支持 VoIP 技术, 支持 VPN, 当广域网服务供应商提供的线路可以满足语音传输的品质要求时, 用户可以利用 Internet 构造与企业总部的 VPN 连接以进一步降低成本。路由器中的 IOS 软件还可以提供防火墙和入侵检测功能, 经济有效地保证分支机构网络的安全可靠。

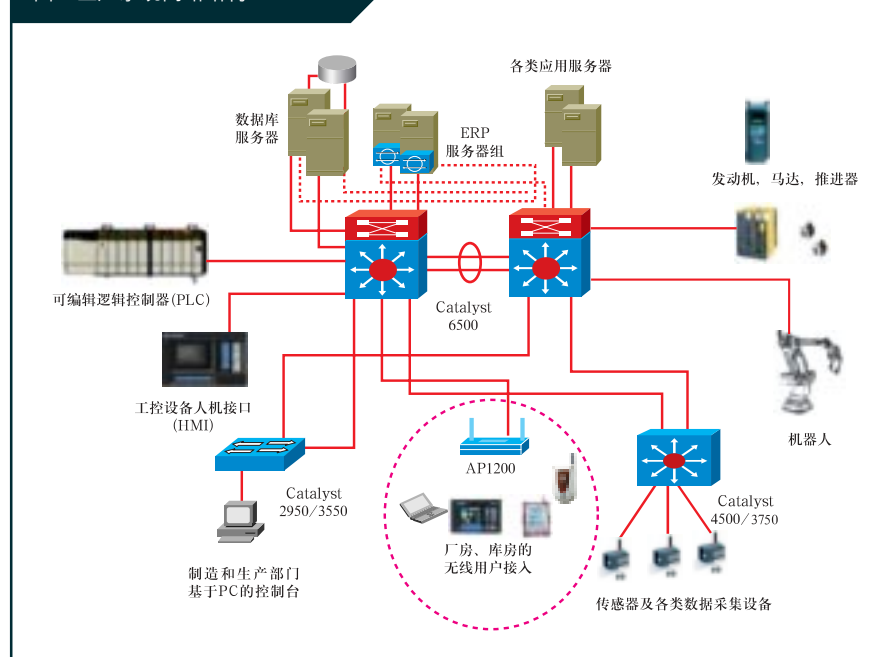
制造及生产系统核心网络

可支持的应用包括：

- 计算机辅助制造（CAM）
- 过程自动化控制
- 数据采集和测试

网络设计如下图所示：

图 4 生产系统网络结构



高性能、高可靠性和高可扩展性

网络骨干采用两台思科公司高性能千兆主干交换机 Catalyst 6500 系列，每台交换机具有 720G 的背板交换能力，400MPPS 的包转发能力。二级交换机可选用 Catalyst 3750、Catalyst 3550、Catalyst 2950 或 Catalyst 4500 以及 Catalyst 6500 的以太网接口模块，关键是考虑可靠性。

两台 Catalyst 6500 系列交换机互为备份，同时所有二级交换机通过多条百兆或千兆链路分别于两台主干交换机，从而保证了生产系统的 7 天 × 24 小时不间断运行。

灵活的无线网接入

在厂房和库房等区域中可以引入 Cisco Aironet 1200 无线网络解决方案，既消除了布线成本和施工难度，又提高了用户的流动接入网络能力。

安全性

采用 Catalyst 6500 系列交换机的防火墙服务模块（FWSM）、安全插接层（SSL）、服务模块和网络分析模块（NAM）以及入侵检测系统模块（IDSM）对网络进行全方位实时的监控，一旦发生任何网络中的异常行为或非法侵入，系统可根据客户预先设定的策略进行应对，包括生成系统报警并中断非法连接等。

通常企业生产网络应与其它网络应用系统有较好的隔离。

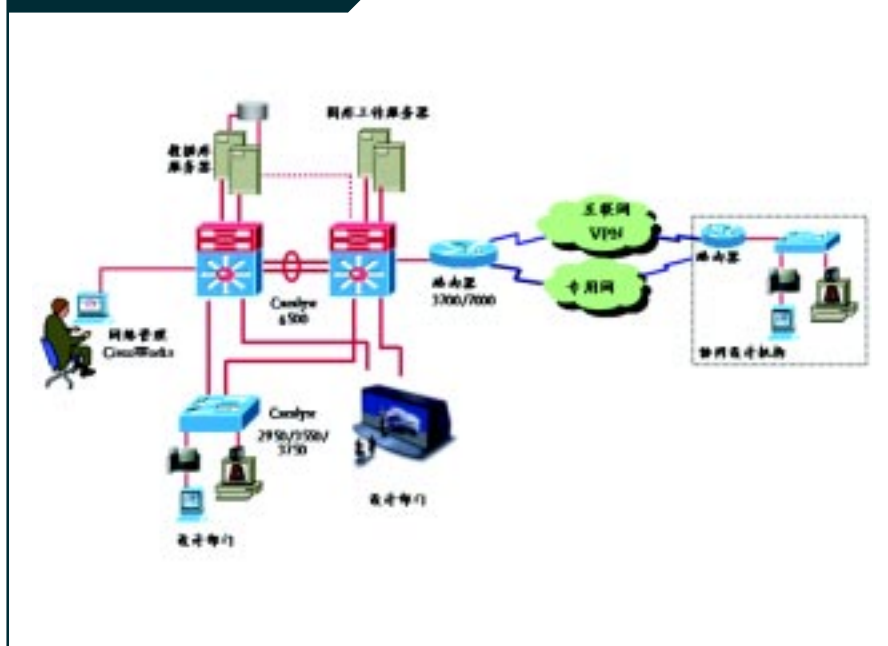
设计系统核心网络

可支持的应用包括:

- 二维和三维电脑辅助设计应用
- 实验模拟及测试数据分析
- 客户采购行为的大量资料分析
- 分散式网络协同设计

网络设计如下图所示:

图 5 设计系统网络结构



高性能、高可靠性和高可扩展性

网络骨干采用两台思科公司高性能千兆主干交换机 Catalyst 6500 系列，每台交换机具有 720G 的背板交换能力，400MPPS 包转发能力，可以充分满足大量的多媒体数据的传输要求。

二级交换机可选用 Catalyst 3750、Catalyst 3550 或 Catalyst 2950，通过百兆或千兆链路与主干交换机连接，并提供 100M 到桌面。

两台 Catalyst 6500 系列交换机互为备份，从而保证了系统的不间断运行。

主干交换机 Catalyst 6500 系列采用全模块化设计，客户可根据需求任意组合接口模块，通过增加新的接口模块也保证了系统可以根据用户业务发展的需要不断升级。

安全性

采用 Catalyst 6500 系列交换机的防火墙服务模块（FWSM）、安全插接层（SSL）、服务模块和网络分析模块（NAM）以及入侵检测系统模块（IDSM）对网络进行全方位实时的监控，一旦发生任何网络中的异常行为或非法侵入，系统可根据客户预先设定的策略进行应对，包括生成系统报警并中断非法连接等。另外运行于关键业务应用服务器上的 IDS 软件系统可以为服务器提供专门的入侵检测和应对功能。存储关键研发信息的服务器前端应设置虚拟防火墙和入侵检测系统。

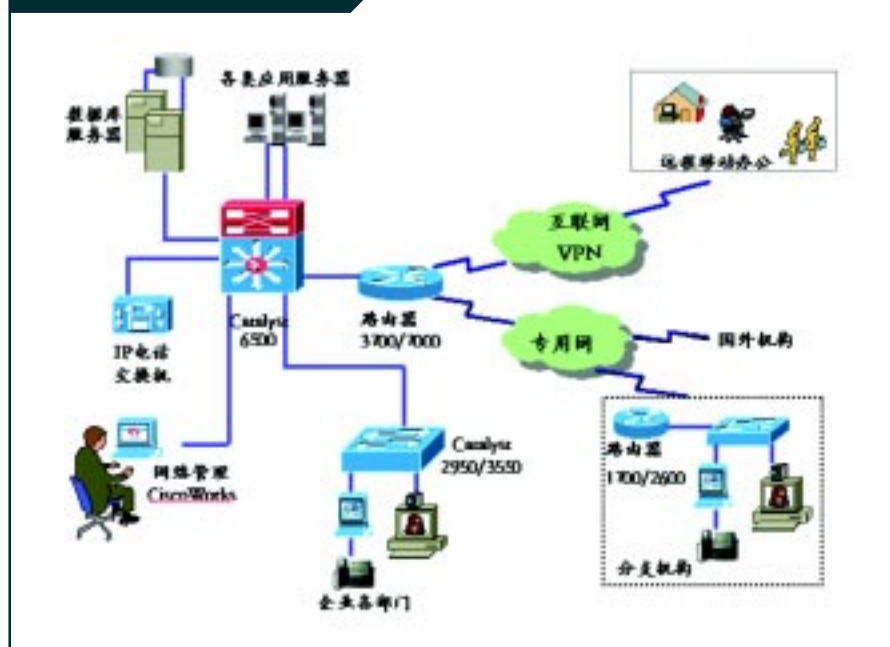
咨询及服务销售网络

可支持的应用包括:

- 办公自动化系统
- 电子化学习系统
- 企业通讯系统
- 远程用户接入系统
- 电子商务系统

网络设计如下图所示:

图 6 销售系统网络



分支机构的连接

Cisco 1700/2600XM/3700 系列路由器可以支持各种类型的广域网连接方式，支持 VoIP 技术，支持 VPN，当广域网服务提供商提供的线路可以满足语音传输的品质要求时，用户可以利用 Internet 构造与企业总部的 VPN 连接以进一步降低成本。路由器中的 IOS 软件还可以提供防火墙功能，经济有效地保证分支机构网络的安全可靠。

经济实用的虚拟专用网

采用 VPN 技术通过 Internet 进行异地办公机构的远程连接可以大大地降低网络的运营开销和成本，同时还大大增加了网络接入地域的范围，十分适用于本客户高速发展的业务拓展需求。

完善的网络应用

对于异地分支机构的通讯和企业文化传播，IP 电话，电视会议以及电子学习系统，可以帮助企业降低成本，提高效率，从而在激烈的竞争中取胜。

服务品质保证 QoS

思科的所有网络设备均支持 QoS 功能，保证了关键业务和多媒体应用在广域网低带宽条件下的有效传输。在广域网上实施 QoS，需根据实际的连接方式和带宽条件，有选择地运用 QoS 的技术。

4 制造业 企业智能 联网生产 网络技术及 解决方案介绍

适用于生产系统和管理信息系统的高可靠性、 高性能和高扩展性的园区网络

随着服务器组在网络中的集中放置成为趋势，传统的关于网络数据流的80/20原则已被颠倒，大量的数据流将在网络主干上传输。这一结构的产生也来自于越来越多的集中式企业应用服务，如基于WEB的企业内部网，电子邮件及信息服务，以及集中式企业应用如ERP。客户端对网络中心应用系统资源的访问必然会带来大量的跨骨干数据传输。此外，企业内部大量话音，视频和其它多媒体应用对系统交换性能和智能化控制也提出了一定的要求。

为保证即使在网络负载最严重的时候也不能成为瓶颈，必须对数据中心网络架构进行合理规划，以确定其规模和处理能力。随着当前服务器处理器芯片的飞速发展和多媒体网络应用的不断增加，采用千兆以太网作为服务器连接方式已成为趋势，下一代万兆以太网应用也已出现并开始应用于高性能数据中心网络结构中。

高可靠性对于制造业企业核心生产系统的重要性更是不言而喻，任何网络故障影响生产系统将造成巨大的损失。

考虑网络的高可靠性、高性能和整体网络扩展性的需要，制造业企业管理信息系统局域网和核心生产系统网络通常采用网络核心交换机和接入层交换机连接的二级网络架构。

高可靠性

很明显，高可靠性必须是一个端到端网络目标。网络设备，服务器集群，操作系统及网络接口卡必须作为一个统一的生态系统协同工作，以恢复任何服务器，链路或网络设备的故障。在一个严格定义的网络结构中，在关键点上必须有特定的能力来确保网络自恢复和稳定。

• 配线间

最终用户进入网络的前段连接，要求多条路径（双路主线）进入到分配/干线网中。
负载均衡接续，以获得最佳网络利用。
快速会聚 L2/L3，以最小的网络中断来从网络故障进行恢复

• 分配/干线

网络的中心汇集点，在配线间、服务器组和 WAN/LAN 之间全冗余连接
负载均衡接续以优化带宽利用
快速会聚，很适合 L3，以最小的网络中断来从网络故障进行恢复。
冗余 L3 转发路径来优化网络 L3 汇聚

上图中的网络交换核心配置包含两台互为备份的Catalyst 6500交换机。当任意交换机发生故障时，包括交换机的接口卡，连接链路或与之相连的数据库服务器发生故障，都会引发系统的自动功能切换，将故障影响的服务和功能由其备份组件接管。通过采用思科设备的高可靠性功能设计入路由热备份协议(HSRP)，任何受故障影响的第三层应用，如默认网关和路由职能，都可以在几秒内切换到备份交换机上去，而这种切换是对客户端及服务器透明的，他们不会感觉到网络的任何变化。在任何情况下，除非故障涉及到数据库服务器本身，这种故障切换都不会造成系统应用进程的中断，因此用户感觉不到任何的网络故障影响。

连接企业各部门的二级交换机与交换核心的链路具备下表中的可靠性属性。

表 2 主干链路的高可靠性服务

特性	功能	好处
上行链负载均衡	直接控制在中继群上 VLAN 的生成树端口成本	双路主线能使用全部上行链带宽
每个 VLAN 的生成树	每个 VLAN 的各生成树例子	允许控制每个子网的转发路径。提供简单技术用于用于 L2 冗余。
快速上行链路	生成树优化	尽量减少网络故障时间。较快的生成树会聚时间。
快速端口	对最终用户端口而言，链接期间没有生成树延迟。	保护生成树，不影响最终用户的端口连接
快速 / 千兆以太网通道	多条链路一起进行负载均衡来形成一个逻辑传输网络。	到核心 / 干线和服务器的高速连接。快速会聚，时间不到 1 秒。
热待机路由器协议	L3 冗余	核心分配 L3 转发负载均衡。快速会聚用于 L3 冗余。
OSPF/EIGRP 定时器	快速路由选择表会聚	快速恢复 L3 网络故障。
快速主干	L2 骨干网生成树优化	尽量缩短网络故障时间。缩短了骨干网中间接故障的会聚时间。

网络可靠性除了设备及链路方面的考虑外，还必须设计成能向网络操作人员通知网络故障，提供有关导致故障的详细信息，以帮助隔离和修理故障。Cisco 提供了系统级工具和管理应用，如：Cisco 资源管理器、网络时间协议（NTP）、系统日志等大量工具。

- 配置管理—— 为路由器和交换机归档、搜索、比较和输出配置文件。
- 变更审计服务—— 网络变化的审计记录和报告。
- 库存管理器—— 容量规划工具和库存详细情况。
- 软件镜像管理器—— 软件镜像的分发、归档和缺陷估计。
- 可用性管理器—— 可到达性、重新装载、响应时间和堆栈译码器
- 系统日志分析器—— 过滤的、灵活的系统日志错误报告

用于评估网络高可靠性的另一个准则是软件发布的质量。在 Cisco 发布其新的软件镜像以前，它经过了严格的质量保证测试和分析。

Cisco 拥有 250 多名专业测试工程师，开发了 150,000 多个专用特性和回归测试，每星期进行 50 万次自动回归测试。

总之，不能在单个机箱基础上进行高可靠性评估。Cisco 利用设备冗余、高可用性网络服务、网络管理和专门的高质量软件发布来提供完整的网络高可靠性解决方案。

高性能和可扩展性

为了支持企业内部大量的用户和多种不同类型的应用，一个高性能、高扩展性的网络环境，网络核心交换机必须具有几百 GB 的交换能力，并能以每秒上百万个数据包的速度进行二，三层交换和路由处理，这样才能保证一个健康的网络交换环境。

采用 Catalyst 6500 高性能交换机作为网络核心设备可以充分满足性能和扩展性要求。Catalyst 6500 系列具有 720G 背板带宽，可扩展到 400MPPS 的包转发能力，同时可支持数百个千兆以太网端口。对于中小企业的网络中心，Catalyst 4500 系列也是可选择的交换核心设备。Catalyst 4506 具有 64G 的背板交换能力，采用模块化设计，可以根据客户网络规模任意配置数据端口种类和数量，可以减少用户的初期网络投资并最大限度的满足用户未来网络灵活扩展的需要，最多支持 240 个千兆或百兆快速以太网端口。

网络接入层交换机一般选用 Catalyst 2950 或 Catalyst 3550 以及 Catalyst 3750 系列，为用户提供 100M 高速网络接入并通过千兆链路和网络核心交换机互连。上述系列接入层交换机均支持堆叠技术，可以灵活的通过多台设备的堆叠来提高端口密度。其先进的端口安全和服务品质保证 (QoS) 技术等的应用可以为企业的网络管理和多媒体应用提供有力的支持。对于大型配线间网络环境，可以采用 Catalyst 4500 系列模块化交换机产品。

适用于生产系统和办公系统的灵活可靠的无线网络

制造业企业的工厂园区一般由办公区，生产厂房和仓库组成。办公区信息点比较集中而厂房内和仓库的信息点则比较分散，在上述地点用户的移动非常频繁，客户需要一种灵活而有经济的组网方式来解决厂房，仓库与办公区内大量信息点网络接入问题。

针对制造业工厂园区的特点，我们采用无线网络技术进行厂房，仓库内部以及办公区内的互连。如下图

图 7 建筑物内部无线网络



图 8 建筑物间无线网络



Cisco Aironet 1100 / 1200 系列为大楼内和大楼到大楼间的无线局域网（WLAN）应用提供了基于标准、经过实践的高速无线网络解决方案。

图 9 思科无线网络产品



思科的无线产品易于管理，可为那些要求移动性、灵活性和自由性的 WLAN 用户提供完整的解决方案，来补充或作为有线 LAN 的备份系统。对于制造业园区网络来说，无线网技术可提供理想的高附加值特性。

对于生产系统，无线网络系统在厂房或仓库的应用体现出突出的优点，员工可以十分方便地通过笔记本电脑中的无线网卡接入公司内部网络，将生产线上的最新数据实时输入管理信息系统，或进行信息查询。

办公区域企业员工在不同的工作空间需要随时方便的网络接入，会议室等用户密度大且不易密集布线的场所使用无线变得十分重要。

因为建筑物或预算的限制，例如因为老旧的建筑、租用的空间、临时性地点等原因，有些企业不能采用传统的布线方式联网，无线网络也是一种选择。

无线网络技术还可应用在视距内的大楼到大楼间远程网络连接，能够避免铺设光纤所需的昂贵费用，同时不会产生挖掘、线路租用、道路使用权等问题，从而节约了网络建设投资和运营成本。

Cisco Aironet 1200系列可以为无线基础设施提供最大限度的灵活性和可扩展性。它的双频设计可以支持基于 2.4GHz 和 5GHz 标准的设备。它让企业可以在工作场所中采用不同的客户端设备，但通过一个由双频接入点构成的单一网络来为这些不同类型的客户端提供支持。事实上，Cisco Aironet 1200 系列可以方便地进行现场升级，这使得管理员可以轻松添加另外一个无线收发装置，或者卸载某个无线收发装置，再用另外一个装置来代替它。作为一个无线接入点，该设备可以为用户提供前所未有的十一个无线通道——八个用于 5GHz 频段，另外三个用于 2.4GHz 频段。因此，Cisco Aironet 1200 系列可以方便地扩展规模，以添加无线设备和无线用户。

Cisco Aironet 1200系列接入点可以提供企业目前所需要的强大的无线连接，确保向后兼容性和未来的投资保护。而且，这种无线接入点还可以提供业界领先的性能、现场升级能力和灵活性，从而可以支持多种无线标准，满足企业在相当长一段时期内的无线访问需求。

思科无线网解决方案先进的性能和安全认证机制保证了 无线网络的灵活和可靠性

在采用了 WLAN 以后，网络的边界发生了变化。访问网络的客户端需要检查他们当前加入的是哪个网络。网络管理人员需要尽快地发现并阻止网络攻击。

今天，采用 WLAN 的企业正在部署四种不同级别的 WLAN 安全措施：没有安全、基本安全、增强安全和专业安全。像所有其他有关安全的部署一样，思科建议企业在选择和部署任何一种 WLAN 安全解决方案之前先进行网络风险评估。

如果没有采取正确的安全措施，一个采用无线网络的公司最终就会像是在公司停车场中安放了一个没有任何保护的 RJ-45 端口。

基本安全通常指的都是采用静态的有线等同保密（WEP）密钥的基本安全。静态 WEP 密钥是一种在会话过程中不发生变化也不针对各个用户而变化的密钥。网络管理员可以设置一个 40 位或者 128 位的静态 WEP 密钥，用其进行身份认证和加密，它使得 WLAN 很容易受到“密码再度使用”式攻击。

静态 WEP 密钥对于 WLAN 上的所有用户都是通用的。这意味着如果某个无线设备丢失或者被盗，所有其他设备上的静态 WEP 密钥都必须进行修改，以保持相同等级的安全性。退一步说，这将给企业网络的管理员带来非常费时费力的、不切实际的管理任务。

我们建议不要在大型企业中使用静态 WEP 密钥。像 AirSnort 这样的破解工具使攻击者可以主动地监控、接收和分析数据分组，破解静态 WEP 密钥。

增强的及专业的安全保护

增强安全解决方案利用针对每个用户、每个会话的动态 WEP 密钥来阻止未经授权的网络访问。该解决方案建立在 802.1x 身份认证框架和 EAP 的基础之上，可以提供基于用户的身份认证。

思科的无线安全套件采用了一种专业的安全解决方案。思科扩展了 EAP，创建了 Cisco LEAP，它也被称为 EAP Cisco Wireless。思科无线安全套件的企业级安全架构包括双向身份认证、消息完整性检查（MIC）、逐个分组密钥散列、基于策略的密钥旋转、初始化向量（VI）变化，以及远程拨号用户认证服务（RADIUS）记账记录的可用性。

思科解决方案可以阻止各种攻击。该解决方案可以防范 AirSnort 攻击和强力攻击，以及通过丢失或者被盗的设备发动的入侵和中间人攻击。

AirSnort 攻击

思科无线安全套件可以通过提供针对分组的密钥散列以及针对主动的重置密钥的集中式策略配置阻止“weak IV”式攻击。这些特性可以防止黑客利用 weak IV 获得足够多的分组以破解密钥。

强力攻击

尽管在理论上存在可能性，但是实际上强力攻击非常难以发起，实际上也不会产生任何效果，这要归功于 Cisco Aironet 针对用户、针对会话的动态 WEP 密钥和频繁的重置密钥功能。而其他使用基于动态 WEP 的系统的厂商则很容易受到这种攻击的威胁。

通过丢失或者被盗的设备发动的攻击

思科无线安全套件可以最大限度地降低由于丢失设备和网络接口卡（NIC）而带来的风险。在我们基于 802.1x 的架构中，思科的认证对象是用户，而不是 NIC 卡。

中间人攻击

这种攻击可能是主动式或者被动式的。Cisco Aironet 的双向认证机制（EAP Cisco Wireless）可以阻止这种攻击。企业可以放心地部署思科解决方案，而无须担心来自伪装的访问点的威胁。

用户密码和会话密钥在无线链路上决不会用明文传送。在这种情况下，无须管理员干预，终端用户就可以自动获得一个独特的会话密钥，从而以一种加密的方式获得对网络的访问。管理员可以通过安排他们的 WLAN，根据他们的需要，每隔一段时间重新进行一次身份认证。

IEEE 802.11 安全任务组（TGi）已经将 802.1x 和 EAP 集成到了它的基本安全框架中。在启用了这些 802.1x 安全特性以后，一个连接到某个访问点的无线客户端只有在用户通过企业 RADIUS 服务器的身份认证以后才能获得对网络的访问权限。

很多第三方 AAA RADIUS 服务器现在也可以支持 Cisco Aironet 安全框架，包括对 EAP Cisco Wireless 双向认证的支持。这些服务器，加上思科安全访问控制服务器（ACS）和思科访问注册器（AR），可以帮助网络管理员灵活地选择后端服务，而不需要降低 WLAN 的安全性。

利用针对分组的密钥散列阻止“Weak IV”式攻击

思科无线安全套件可以组织很多类型的攻击，其中包括通过分析一串使用相同密钥的加密流量中的多个不安全的初始化向量而发动的 Weak IV 式攻击。利用客户端和访问点都支持的高级散列技术，WEP 密钥会在每个分组的基础上动态变化，从而有效地阻止这种攻击。IV 和 WEP 密钥都会被散列，以生成一个独特的分组密钥，这可以防止黑客利用不安全的 IV 获得 WEP 密钥。

为了防止利用 IV 冲突而发动的攻击，必须在 IV 发生重复之前更改 IV 密钥。由于在一个繁忙的网络上 IV 可能会几个小时重复出现一次，所以管理员可以利用像 EAP Cisco Wireless 这样的机制进行重置密钥操作。

消息完整性检查

对 WEP 的另外一个担忧是它对重复攻击的抵抗能力。思科无线安全套件可以执行消息完整性检查（MIC）来防止 WEP 帧受到修改。Cisco Aironet WLAN 可以利用 MIC 检测并丢弃那些在传输过程中被（恶意）修改的分组。由于采用了 MIC 的 Cisco Aironet 产品可以发现并丢弃被修改的分组，所以攻击者无法利用位切换或者主动的重复攻击来欺骗网络以通过身份认证。

面向组播密钥的基于策略的密钥旋转

利用 Cisco Aironet 的密钥旋转系统，WLAN 可以支持针对用户、针对会话的密钥和广播密钥。单播密钥的重置超时策略在思科安全 ACS（基于 Windows）或者 Cisco AR（基于 UNIX）集中配置。这个密钥旋转过程对于用户来说是透明的。网络管理人员可以在访问点配置组播密钥旋转策略。

RADIUS 记账记录

思科无线安全套件的另外一个附加特性是能够为每个客户端进程生成详细的 RADIUS 记账记录。这些记录可以被发送到 AAA 服务器，用于记录、审计和针对 WLAN 的使用收取费用。企业还可以利用这些数据审查账目。

尽管没有哪种 WLAN 安全方法是 100% 无懈可击的，但是思科无线安全套件可以为企业环境提供强大的安全性。在采用了思科无线安全套件以后，企业员工可以安全地使用无线网络，随时随地投入工作。

适用于网络化销售的经济有效的企业广域网络连接

由于制造业企业的公司管理和销售总部往往位于经济发达的大城市，而制造基地则处于交通便利，劳动力成本低廉的周边地区，同时在全国各大中城市往往会有企业的销售和服务分支机构，因此企业总部与分支机构间的跨地域广域网建设就具有十分关键的地位。据统计近 50% 的企业 ERP 应用客户端位于企业本地厂区内部网外，因此提供一个可靠的可扩展的远程连接就非常重要。大多数企业的目标是在保证高性能，高可靠的网络连接前提下，尽可能的降低连接分支机构的广域网运行开销，而这部分开销通常占到网络总体运营成本的 40%-60%。

广域网中的关键设备是路由器，思科的高端路由器和访问路由器产品可以很好的应用于企业中心和远程分支节点。思科路由器产品支持广泛的广域网连接配置及不同的广域网传输介质。思科全线产品均运行 Cisco IOS 软件平台，从而保证了全面的兼容和互连性，并可以通过软件升级以支持最新的标准和应用。思科的路由器产品还支持数据，语音和视频集成的多业务应用，保证了对昂贵的广域网带宽的最高利用率。对 ERP 及语音应用跨广域网传输的最重要因素就是服务质量保证(QoS)。

目前，虚拟专用网 (VPN) 技术被越来越多的应用于企业与分支机构，供应商，客户和远程用户的连接，最终目的是建立与企业应用系统用户的广泛而经济的连接。通过采用 IPSec 等基于标准的用户认证和数据加密技术，以及基于防火墙的边界安全技术，网络连接的安全性可以得到保证。

随着 Internet 基础设施建设的发展，Internet 宽带接入在很多城市已很普及，采用 VPN 技术进行企业内部远程网络连接可以很好的利用 Internet 宽带接入服务来实现广域网连接。解决方案的主要优点包括：

A. 降低成本

- 无需专线租用费用

VPN 利用公共互联网或者服务提供商所共享的 IP 网络来做为访问内部网络的传输媒介，从而避免了采用 DDN 等其他广域网连接方式所需的昂贵的专线租用费用。

- 减少日常运行开支

VPN 能减少经常性的管理费用以及远程访问所需的投资。由于各分支机构均通过当地的服务提供商接入 Internet，因此只需要支付较少的接入费用。

B. 扩展连接

- 无长途费用

保证在世界上的任何一个地方能以本地访问费用来安全地访问企业内部网络，已由 VPN 变成了现实，这就将企业在提高网络接入速度的同时无需支付长途连接费用，甚至大型的文件也能通过 VPN 经济高效地从网上下载。

- 利用宽带投资优势

宽带电缆和数字用户线 (DSL) 基础设施日益增长的运用，使得远程访问的容量逐步增加。没有 VPN，宽带仅仅是一个快速访问互联网的途径。然而，通过整合加密的 VPN 隧道和高速宽带互

联网服务，远程用户可以享受到 LAN 般的速度和“持续在线”访问（假如企业容许的话）。而诸如 e-mail 这样的应用可以进行实时地运行，而不再需要通过频繁的（乏味的）拨入来同步或者复制信息。

- 允许新的应用和用户类别

VPN 是一项允许进行大量 B2B 应用的技术。例如，在客户处工作的咨询人员仍可以与他们自己公司的 IT 资源保持高速连接，咨询人员只要简单地通过客户的 LAN 将他的便携式电脑与互联网连接，并建立一个通向他（或她）的公司网络的高速隧道。这意味着咨询人员可以即刻访问他自己的 LAN 资源，如电子邮件、文件共享、计时和计费应用以及技术库——所有这些都保存在远程地点。

思科虚拟专用网解决方案，包括 Cisco 7000 系列和 Cisco 3700/3600/2600/1700/800 系列路由器，可以用于网络中心和分支节点的 VPN 解决方案。

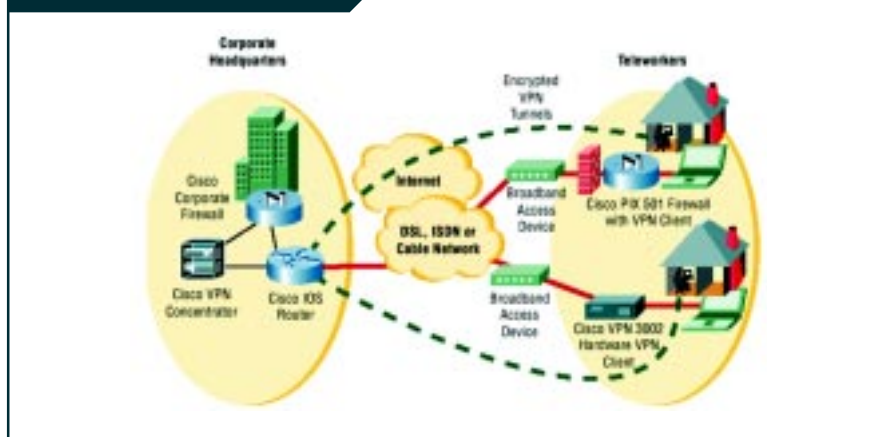
当大部分企业实施跨广域网 ERP 系统的时候，广域网可靠性总是关键性的考虑因素。为了分支节点连接的冗余性，所有主要网络中心汇接点都要采用与广域网的双点连接，采用双路由器结构提供均衡负载并通过 HSRP 协议互为备份。对于小型汇接点，可以采用拨号备份连接。在有些地点，当本地的多接入服务不可得时，企业通常采用其它的备份连接手段如卫星链路。

远程移动办公人员网络接入

在企业网络用户中，很大一部分是企业的销售和管理人员，这些人员经常处于频繁的出差旅行中，如何使他们能通过有效的方式在旅途或外地仍能访问企业的系统资源就是一个网络实施中的需要考虑的问题。对于高层经营管理人员来说，在家办公也是他们经常所需的，所以对企业网络的连接也应拓展到员工家庭及其他厂区外的地点。

远程接入网络的建设可以很好的满足企业用户的这些需求。采用 Cisco 的路由器及远程接入服务器可以为流动用户提供多种远程接入方式，如电话拨号（PSTN），综合业务数据网（ISDN）等，也包括通过数字中继线路（DSL）和有线电视网（Cable Modem）的接入用户。

图 10 流动人员的网络接入



为进一步降低用户接入成本并保证数据传输的可靠性，流动办公人员的网络接入可以采用虚拟专用网 VPN 技术。这样出差人员只需在外地接入当地的 Internet 就可以与企业总部网络建立安全可靠的数据连接，从而可以及时地获取企业信息资源。与企业网络的随时随地连接可以为企业前台销售人员提供有效的销售工具和用力的系统支持。VPN 技术的采用可以大量降低远程拨号接入手段产生的长途通话费用，利用当地的公用宽带网络接入也可以大大提升远程连接的速度和带宽，提高工作效率。

适用于企业通讯系统的基于融合型网络的IP电话与视频会议系统

通讯费用总是在企业运营成本中占有很大的比重，尤其是对于跨国销售型企业。如何降低企业通讯费用已成为降低企业成本的重要一环。

Cisco AVVID (Architecture for Voice, Video and Intergrated Data) 是Cisco公司针对多服务网络建立的一个基于标准的、开放的语音、视频及综合数据体系结构。

Cisco AVVID 不仅仅具备在 IP 基础架构上与已存在的传统通信系统互通共存，更主要的是 Cisco AVVID 的实施使得在很多情况下可以完全代替对传统系统的需求。同时，在具备服务质量保证 (QoS) 的 IP 基础架构上可以迅速部署许多新型充满创造力的应用，比如统一消息、Cisco IP 联络中心、端到端 IP 电话以及视频系统等等。

此外，Cisco AVVID 语音、视频及综合数据体系结构引入了一个 Internet 生态系统，由于具有开放标准，鼓励不同厂商不同产品解决方案发展和互操作等特点具备长足发展的条件。与传统专有系统分立的解决方案相比，其所具有的优势将超越单一经济，创造崭新商业经济方案并得到快速实现。

IP 电话系统

随着网络技术和语音数字化技术的成熟，利用IP网络传输语音信息已成为一种成熟的技术。电话网络与数据网络的融合可以节省客户的长途电话费用，减少维护两套系统的成本，并引入新的服务。

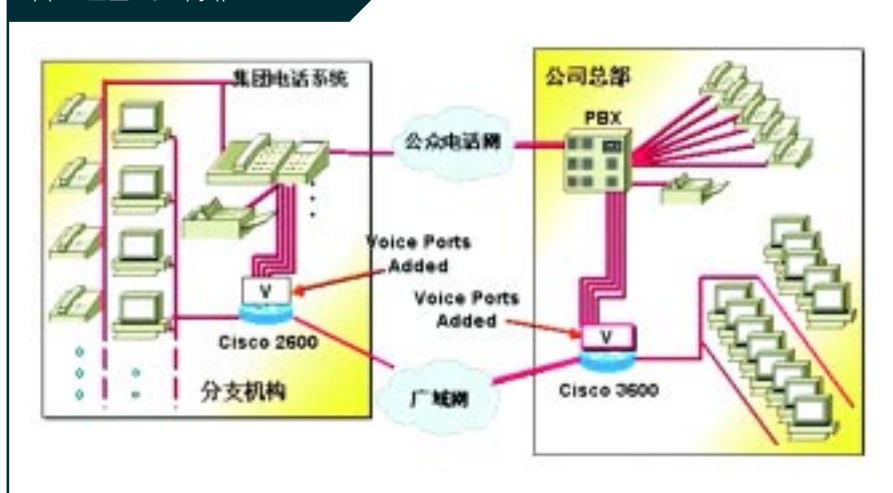
电话系统与数据网络的融合分为两个阶段：

首先是针对已有 PBX 电话系统的用户，在保持现有电话系统运行的同时，采用 VoIP 技术节省用户的长途电话费用。进一步的，对于新建网络系统的用户，可以选择 IP 电话技术，彻底的抛弃传统的 PBX 交换机和电话系统，运行真正基于网络的 IP 电话应用。这样不仅可以降低话费成本，还可以降低系统维护成本。同时IP电话引入了一系列新的服务和应用，如一体化信息留言系统，WEB 电话等等。

与传统电话系统并存的 VoIP 技术

VoIP 技术的实施十分简单，只需在连接用户广域网的路由器设备中配制语音模块，并将其与企业现有的 PBX 互连，则可以实现将长途电话呼叫通过已有的广域网数据线路传输。

图 11 企业 VoIP 网络



上图中的企业 VoIP 网络可以实现：

- 企业总部与分支机构内部间长话通过 IP 网络传输，没有通话费用。
- 公司总部打往分支机构所在地外部的长话通过 IP 网络传输到分支机构后接入当地市话网，收取当地市话费用。
- 分支机构打往公司总部所在地外部的长话通过 IP 网络传输到公司总部后接入当地市话网，收取当地市话费用。

VoIP 技术的实施可以有效的降低公司总部与各分支机构间的长途通话费用，从而降低企业运营成本。

新一代的 IP 电话技术

新一代 IP 语音技术是在 VoIP 技术和最新的 TCP/IP 技术的基础上发展起来的。由于 IP PBX、IP 电话的诞生，语音信号可以在语音终端即以 IP 数据包的形式表现，因此能够从语音终端开始就采用 IP 技术对语音信号进行传输。

在新一代 IP 语音网络中，基本交换技术是包交换技术，不再需要传统的基于电路交换的数字程控交换机。所有的语音 IP 包通过 IP 路由技术在统一的 IP 网络中传输。其语音的信令和寻址是由 IP PBX 来完成，而语音数据包的路由则与传统的 IP 网络一样，通过路由器来完成。同时由于 IP 电话具有极为强大的智能处理能力，能够提供比传统电话强大得多功能，包括电话会议、转移呼叫、在线等待、基于人名拨号、接收天气预报、股市行情等等。如果与消息处理服务器协同工作，还能够提供语音邮件、统一消息处理（即使用同一个终端就能够处理电子邮件、语音邮件和传真）等功能。

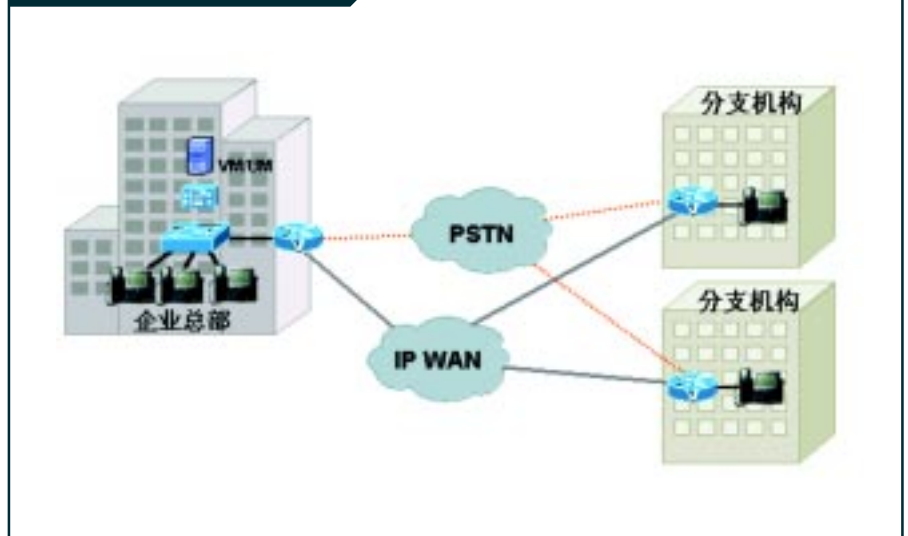
IP 电话系统有五个关键部分组成：（如下图）

图 12 IP 电话系统的组成



典型的制造业企业 IP 电话部署方式如图：

图 13 多点实施——集中式电话处理



IP 电话系统部分应用特点：

- 不需对现有布线系统作任何修改：
电话与数据网络共用一套布线系统。电话和PC连接到局域网交换机，电话机的软件装载在 PC 上。
- 不必在每个分支机构均配备 PBX。
- 电话会议功能：会议建立支持二种方式。
Meet-Me: 由管理员预先设置一个会议号码，由会议主席按“Meet-Me”，并拨打会议号码，启动一个会议。其他参会者也拨打此号码加入会议。
Ad-hoc: 由会议主席邀请每一个参会者，当会议主席退出会议，会议仍可继续进行。当会议建立后，可在参会者之间分享桌面应用。
- 自助转接电话的服务：
通过记录用户输入的数字或字母，系统将电话转接到相应的分机。
- 交互语音响应系统：
根据预订制的流程，提示拨叫者输入信息，系统在数据库中查找结果，给出相应的响应。该系统可部署在网络的任何地方，流程的修改具备方便的工具。
- 支持装在 PC 机上的电话应用。
- 未来可支持基于开放标准的全网络 IP 呼叫中心。
- 支持统一的应用平台：用一个信箱实现接收语音、邮件、传真。

提供以下功能：

- 可根据不同的时间（上班、下班），或不同的线路（忙、无人应答）录制个人留言提示语。
- 支持“Return Call”，“Forward Message”。
- 可将一个留言同时给多个人。
- 可通过姓名、电话号码访问语音信箱。
- 可将语音留言作为附属文件 e-mail 给其他人。
- 用户可通过访问 e-mail 信箱识别信箱中的信息类别。
- 可通过“text-to-speech”功能，用电话听 e-mail。

- 可用电话回复 email，将回复留言作为附属文件。
- 用户可获得传真打印的私密性
- 通过电话可获知传真是否已到及收到的时间，发送人
- 通过email可阅读.tif的传真
- 可将传真的.tif文件作为email的附属文件forward给其他人

适用于企业文化传播与员工教育的电子化学习系统

经济全球化使时间和空间距离缩短，并消除了许多传统的竞争障碍，全球经济越来越大的部分以知识和信息为主，这一点可能是迫使企业员工不断接受教育和培训的最重要的因素。

对于跨国性、跨区域性的机构，传统的基于培训教室方式的学习成本非常高，而且难以控制。就算员工有时间参加所有的课程或讲座，并能够阅读所有相关的资料保持所在领域知识的及时更新，学习的成本也会不可预测。企业电子学习的使命就是为员工提供时效性非常强，成本又非常合算的培训项目，从而创造出主动而且富有经验的忠诚员工。据统计，仅仅美国每年企业投入在员工培训上的费用就高达 600 亿美元，而电子学习估计可以为企业节省约 30% 的费用，而且可以提高 40% 的培训效果 (以达到相同效果的时间来比较)。

企业电子学习的任务是为员工提供最新、最经济有效的计划，帮助他们成为富有进取精神、技能水平较高、忠诚的知识工人。

电子学习有几个特点，能够缩短学习者掌握特殊知识和技能所需的时间。这些特点包括：

- 可访问性
与由教师带领的教育或者基于教室的教育相比，电子化学习使学习者能够随时随地通过互联网访问内容。
- 速度快、及时
基于互联网的内容可以快速更新，以便响应不断变化的条件或需求，因而能为学生或工人提供最新信息。
- 个性化
人们可以学习不同等级的内容，起始知识水平可以各不相同。在传统教育方式中，个性化指导既困难又昂贵。电子化学习则能够实现内容和提供方法高度个性化，而且几乎不需要追加成本或者只需要追加少量成本。
- 易评估
互联网上提供的联机评估工具可以说是老师遇到的最实时、最灵活的评估方法。评估的内容是学习了多少东西，而不是在教室中学习了多少个小时。
- 方便性
如果只在少数预定时间和地点提供培训，从事全职工作的成人就很少有时间和机会参加。借助电子化学习，学生和工人可以根据自己的进度、在最适合自己的时间里学习课程。
- 降低供应成本
一旦电子化学习系统安装成功，每位学习者的成本将大大低于传统学习方法。由于电子化学习还能减少需要出差才能参加培训课程的员工数量，因而学习成本还会进一步降低。
- 扩展能力
如果需求突然增加，基于教师的传统方式很难扩充。相反，电子化学习则能够非常有效地利用有限资源，使数十万能够接受以前只能少数人才能接受到的教育。

随着企业信息化建设的不断发展，大量培训信息以及资源以视频信息格式存储与网络系统中，企业需要一个真正的网上视频应用系统来进行员工培训和公司信息发布等。

Cisco IP/TV解决方案能够为企业带来一个全面的网络视频流系统，IP/TV系统可以非常好的应用于企业员工的电子学习。它能为台式PC、办公室和会议室提供电视质量的实时视频节目——包括管理广播，培训教学，企业电视，卫星节目等等。因为它采用了高效率的网络多播技术，所以企业可以通过它以最佳的网络性能，提供高质量的视频内容。

Cisco IP/TV 产品采用了运行在现有 IP 网络上的各种标准协议，以及一些被业界普遍使用的技术，例如微软公司的 Windows Media 技术。为了实现实时传输，企业需要一个 Cisco 3400 系列广播服务器和内容服务器，以及一个 IP/TV 收看客户端。另外还可以添加档案服务器，用于点播节目，或者预先安排重播。

Cisco IP/TV 广播服务器用采集卡进行数据编码，并按照它们从控制服务器所接收到的指示传输节目。广播服务器主要用于多点播送实时的或者预先录制的节目，这些节目可以来自于各种设备（例如摄像机、VCR、DVD、卫星和电缆馈线），或者来自于预先录制的 Window Media、AVI、MP3 和 MPEG 文件。

Cisco IP/TV 控制服务器负责管理策略。它将时间安排信息、可用的视频格式、带宽考虑因素和其他信息发送给 Cisco IP/TV 广播服务器，并将节目信息发送给 IP/TV 收看客户端。Cisco IP/TV 控制服务器还可以自动均衡网络视频负载和性能，而不需要网络管理员进行任何干预。

Cisco IPTV 系统应用实例见下图：



借助Cisco Catalyst 6500系列交换机增强企业网络的安全性

借助当今先进的智能企业网，企业能够有效地部署电子商务等应用，因而能实现劳动力的优化组合以及业务的全球化。这些强大的网络能够将许多远程站点、分支机构、移动员工、合作伙伴和客户连接在一起，因而能够为数千用户提供服务。但是，还存在一个问题——所有网络都越来越多地受到了企业园区网和互联网上越来越多的安全隐患的威胁。另外，对电子商务应用需求的增加，以及服务向公共领域的集中也增加了流量经过网络时的危险，在可能的地方，都需要对流量进行加密。

不同的安全措施和预防技术适用于大小、预算和企业要求不同的网络。机构在设计网络安全体系结构时，必须考虑多种因素，包括成本—利益分析、企业需求、安全政策以及需要保护的网络安全类型等。

思科公司作为网络设备的领导厂商深刻了解网络安全对于客户的重要性，思科对网络的了解使思科在实施网络安全解决方案上具有得天独厚的优势。

Cisco Catalyst® 6500 系列交换机提供的解决方案能够防止网络受到来自园区网和公共网的安全隐患的侵害。

新型思科高级安全模块包括防火墙服务模块（FWSM）、安全插接层（SSL）、IP 安全虚拟专用网（IPSec VPN）服务模块和网络分析模块（NAM）。如果将这些模块与现有的入侵检测系统模块（IDS）结合在一起，客户将能够在交换机上部署综合安全性，而无需分别管理的不同设备，然后再与基本的基础设施相连，因此，这种方式可以大大提高性能、可管理性和整个系统的性价比。

IPSec VPN 服务模块

在 Cisco Catalyst 6500 系列上提供经济有效的 VPN 性能，适合进行多种部署。例如，在 WAN 边缘部署中，VPN 模块能够在 WAN 集中路由器上提供 VPN 终端服务。

主要特性包括：

- 与网络基础设施集成在一起
将 VPN 融入 Catalyst 6500 交换机，无需添加设备或修改网络就能保护网络。
- 高性能和可扩展性
采用最新的加密硬件加速技术之后，IPSec VPN 模块能够为大型分组（500 字节以上）提供 1.9Gbps 的三重数据加密标准（3DES）流量，为平均分组（300 字节）提供 1.6Gbps 的 3DES 流量。与当前产品相比，这个模块能以更高速率同时端接 8,000 个 IPSec 通道。
- 高级安全服务
能够将加密、认证和完整性集成为网络服务，因而可以简化安全园区网、供应商边缘、VPN 终端和安全综合网络服务的部署，例如 IP 语音（VoIP）和存储区域网。

Cisco 防火墙服务模块（FWSM）

安装在 Cisco Catalyst 6500 系列交换机中，不但适合作为数据中心和外部网的边缘分布层，制定服务器流量策略，还适合作为网络管理层。

Cisco FWSM 是业界性能最高的防火墙解决方案，每个模块的吞吐量能够扩展到 5GB 以上。借助多个模块，带宽可高达 20GB。FWSM 完全支持 VLAN，提供动态路由，而且可以完全集成在 Cisco Catalyst 6500 系列交换机内。FWSM 基于 Cisco PIX™ Firewall 技术，因而能够提供与屡获大奖的 Cisco PIX™ 安全设备系列相同的安全性和可靠性。FWSM 采用了通过软件下载增强特性的网络处理器技术，能最大限度地适应未来需求和特性。

主要特性包括：

- 可扩展性
能够以业界最高的性能生成受状态防火墙保护的多个安全域，从而消除来自企业园区网的越来越多的安全威胁。每个 FWSM 模块提供 5GB 吞吐量。如果安装多个模块，每个机箱的总带宽可以扩展到 20GB。
- 可靠性
以 Cisco PIX 技术为基础，FWSM 使用了同一个经过时间检验的 Cisco PIX 操作系统，这是一种安全的硬化实时操作系统。借助切实可行的 Cisco PIX 分组检查引擎，FWSM 能够在一个平台上同时提供高性能和高安全性。另外，它还能在活跃/等待 FWSM 环境中提供基于 LAN 的故障恢复。
- 易于使用
FWSM 使用思科大家非常熟悉、切实可行的 Cisco PIX 管理界面保持安全性及网络管理界面的独立性。Cisco 管理框架和 Cisco AVVID（集成化视频、视频和数据体系结构）合作伙伴都支持 FWSM 的配置和监控。

Cisco 安全插接层 (SSL) 服务模块

为 Cisco Catalyst 6500 系列设计，非常适合部署在数据中心内，它能够提高 Web 应用的性能和安全性，提供综合安全内容联网，并保证最优客户体验。由于能卸载与利用 SSL 协议保护流量相关的处理器密集型任务，因而能增加 Web 站点支持的安全连接数量。

如果将 SSL 与 Cisco 内容交换模块 (CSM) 集成在一起，将能够加速加密和非加密流量，同时从 Web 服务器卸载资源密集型功能，从而提供高性能、可扩展、安全的服务器负载均衡解决方案。

主要特性包括：

- 证书优化
对传输到 Web 服务器的用户数据进行加密，提供私密性、保密性和认证。SSL 使用驻留在模块上的多种证书，能集中证书管理。由于无需在单独的服务器上管理证书，只需一份证书就能完成管理，因而能显著降低成本。
- 确定性能
提供业界最快的 SSL 对话建立速度和最高的加密吞吐量：每个模块每秒建立 3,000 条连接（每个机箱 12,000 条），每个模块的加密吞吐量高达 300Mbps（每个机箱 1.2Gbps），能同时保留 50,000 条客户机连接（每个机箱 200,000 个）。
- 永久连接
用 Cisco CSM（集成模式）操作时，及时客户机请求新对话 ID 时，也能保持永久连接。
- 服务器 SSL 卸载
集成 SSL 处理，执行与 SSL 相关的所有任务，使服务器能处理高速纯文本流量。

新型高性能 Cisco 网络分析模块 (NAM)

非常适合数据中心、企业边缘、分布层使用，也可以作为网络的关键业务接入层，为网络提供应用级可视性，在千兆位环境中实现实时流量分析、性能监控和故障排除。

主要特性包括：

- 应用级可视性
NAM 能够为网络基础设施提供应用级可视性，以便实现性能监控、故障排除和容量规划。它提供 NAM Traffic Analyzer，除统计数据收集功能外，还能提供流量监控和分析功能。
- 另外，NAM 还是在 Cisco LAN 网络中确定多服务交换方式的 Cisco AVVID 的一个组件。NAM 能够收集以各种方式到达应用层的数据和语音的多层信息，以便以更简单的方式管理当今支持多种数据、语音和视频应用的复杂的多服务交换 LAN。
- 高性能
新型高性能 NAM-1 和 NAM-2 能够以千兆位速度为可扩展的交换环境提供更强大的流量监控。
- 易于使用
基于 Web 的嵌入式流量分析器能够为数据、VoIP 和 QoS 提供全面的流量监控和数据获取功能。

Cisco 入侵探测系统模块

可以部署在分布层和数据中心内，提供全面的预防性安全解决方案，防止非授权入侵、恶意互联网病毒以及带宽和电子商务应用袭击。

Cisco IDS 利用了全新的入侵检测技术，包括状态样式识别、协议解析、启发式检测和异常情况检测等，能够防止多种已知和未知计算机安全问题带来的威胁。

集成在 Cisco Catalyst 6500 系列交换机中的这些服务模块，如果能够部署在推荐的网络层中，并与 Cisco Catalyst 6500 交换机的软件安全产品一起使用，将能够有效防止内部网络遭受非法设备和用户的侵害，使网络免受外部安全隐患的威胁。

Cisco Catalyst 6500 系列交换机能够为企业园区网提供全面的安全解决方案。

企业数据库服务器与应用服务器的负载均衡

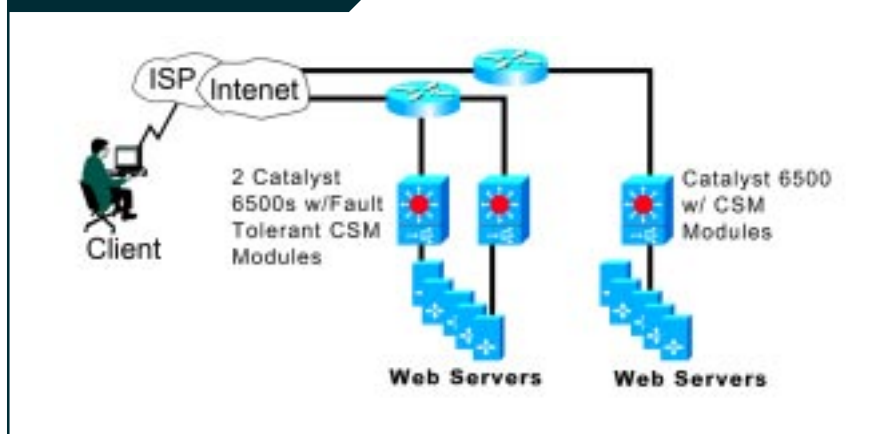
制造业企业拥有大量的应用系统，支撑着应用系统的服务器数量庞大，关键应用服务器和数据库服务器一般使用2台以上，用以备份和均衡负载。Cisco 可以提供优秀的网络解决方案来解决服务器连接问题。

Cisco 内容交换模块（CSM）是一种 Catalyst 6500 线卡，专门用于在服务器群、防火墙、SSL 设备或 VPN 终端设备间均衡分布客户端流量。CSM 为企业网络提供了一种高性能、经济有效的负载均衡解决方案。CSM 满足了用户对高速内容传输网络的需求，能够实时跟踪网络会话和服务器负载状况并将每个会话导向最合适的服务器。冗错型 CSM 配置能够保留全状态信息并提供关键任务功能所需的真正的故障恢复功能。

CSM 提供了以下主要优势：

- 市场领先的性能
每秒能够建立 200,000 个第 4 层连接，提供了高速内容交换，同时可支持 100 万个并发性连接。
- 面向大型数据中心与 ISP 的出色的性能价格比
连接成本低，占地面积小。CSM 可插在一个新的或现有的 Catalyst 6500 的插槽中，并使 Catalyst 6500 中的所有端口支持第 4 到第 7 层内容交换。同一个 Catalyst 6500 中可以安装多个 CSM。
- 易于配置
使用用于配置 Catalyst 6500 交换机的 Cisco IOS 命令行界面（CLI）。

图 15 负载均衡



内容交换模块的主要特性

防火墙负载均衡

CSM 可以在每个连接的基础上将流量分布到多个防火墙，从而使您能够增强防火墙保护功能，CSM 还能够确保所有属于某个连接的分组通过同一个防火墙。特殊与普通防火墙均受 CSM 支持。

基于 URL 和信息块的负载均衡

CSM 允许为基于 URL、信息块和 HTTP 报头字段的策略提供定期表达模式匹配。CSM 支持任何 URL 或信息块格式，因此无需更改 URL/ 信息块格式就可以对现有的 Web 内容进行负载均衡。

高性能

CSM 每秒能够进行 200,000 次新的第 4 层 TCP 连接设置。这些连接可以分布到 4096 种虚拟服务（16,384 台服务器）和 Catalyst 6500 所有的端口上，也可以集中在一个端口上。这是一种独特的优势，因为竞争对手的产品使用的分布式体系结构只有在同时使用所有端口时才能达到最高性能。

网络配置

CSM支持许多种不同的网络拓扑。CSM可以用于混合的桥接和路由配置,从而使流量能够在相同或不同的IP子网上从客户端流向服务器端。

IP 协议支持

CSM支持大量常用的IP协议,包括TCP,用户数据报协议(UDP)。此外,CSM还支持一些高层协议,包括超文本传输协议(HTTP),文件传输协议(FTP),Telnet,实时流协议(RTSP),域名服务器(DNS)和简单邮件传输协议(SMTP)。

用户会话附着

在进行任何加密或电子商务运作时,必须始终将最终用户导向同一台服务器,即用户的购物车所在的服务器或加密隧道端接的服务器。CSM的用户会话附着特性能够不断将用户导向同一台服务器——基于安全套接层(SSL)会话ID,IP地址,信息块或HTTP重定向。

负载均衡算法

CSM支持以下负载均衡算法:

- 循环
- 加权循环
- 最低连接数量
- 加权最低连接数量
- 源和/或目的地IP散列(子网掩码也是可配置的)
- URL散列

服务质量

在通过内容赢利时为最终用户提供不同水平的服务非常重要。CSM利用Catalyst 6500强大的QoS功能实现了流量差异化:

根据第7层规则为分组分配正确的优先级

将所付服务费较高的用户导向速度更快或负载较少的服务器。

高可用性

CSM利用状态监控探测器、带内状态监控、返回代码检查和动态反馈协议(DFP)对服务器与应用可用性进行持续监控。在一个服务器或网关发生故障时,CSM将把流量重新导向一个不同的地点。用户可以在不影响服务的情况下添加并删除服务器——可以轻松地扩大或缩小系统的规模。

连接冗余性

用户可以在一个冗错配置中配置两个CSM,以便共享用户会话的状态信息并提供连接冗余性。如果运行中的CSM发生故障,备用的CSM可在不中断运作的情况下处理打开的连接,用户将实现顺利的故障恢复——这是电子商务地点与使用加密功能的地点的重要要求。

企业网络管理同样重要

制造业企业的IT员工正在面临着自己事业上最艰难的网络挑战，他们必须能够管理作为企业商业基础的关键基础设施。今天的商业应用存储在服务器组中，基于内部网、外部网和Internet电子商务，随着这些网络化的应用变得越来越复杂，企业需要更为稳固的网络服务。为使自己所在的企业网络拥有 7 天 x24 小时可用性，选择优秀的网络硬件设备非常重要，同样重要的是必须部署网络管理系统来对这一环境进行高效的管理。网络管理除了一般概念上的网络设备管理，端到端的 QOS，端到端的网络安全，端到端的语音系统，如果没有有效的管理系统，对于企业网络管理员来说，是非常头疼的问题。

CiscoWorks产品易于购买、部署和更新，将新的和现有的网络管理应用捆绑为四个解决方案，基于Internet的网络管理是企业网络管理员工的得力帮手。

CiscoWorks企业管理解决方案简介

CiscoWorks企业管理解决方案的重点集中在四个关键领域：广域网（WAN）、局域网（LAN）、服务级别管理、虚拟专网（VPN）和安全性管理。

CiscoWorks产品引入了创建“管理内部网”以连接多供应商应用的概念，这在整个行业是独一无二的。通过改进的基于 Web 的技术以及能够共享数据和系统处理过程的任务驱动的设计，这些解决方案可以节省时间，减少错误，从而提高了系统的总体管理水平。

表 3

应用	主要特点
路由WAN管理解决方案	● 路由 WAN 管理解决方案 ● 提高路由器性能 ● 基于模板的访问控制列表（ACL） ● 快速识别影响延迟的设备 ● 减少 WAN 通信流和成本 ● 广泛的监视和变化管理功能
LAN管理解决方案	● 提供可以对园区网进行配置、监视和问题诊断的单一解决方案 ● 支持对变化进行早期检测，保证 LAN 的正常运行 ● 支持可扩展的园区网拓扑视图 ● 通过使用标准实现数据共享，培养管理“生态系统” ● 所有内容都可通过浏览器访问
服务管理解决方案	● 使用户能够验证外部广域服务供应商或内部组织的 service 级别 ● 提供打印报告 ● 网络问题诊断 ● 允许服务供应商向自己的客户展示 SLA 一致性
VPN 和安全管理解决方案	● 提供 VPN 端接的一览视图 ● 提供设备工作情况的一览视图 ● 支持使用特征采集 ● 优化对 VPN 的使用 ● 支持对网络入侵和安全问题进行快速识别

CiscoWorks 企业管理高级应用

CiscoWorks网络管理产品系列可以满足您一般组网领域的所有网络管理需求, 如LAN管理或服务级别管理。对于更复杂的需求, CiscoWorks 高级应用的目标定位于对特定技术进行深层次管理。大多数客户可以选择一个或更多的 CiscoWorks 解决方案, 以涵盖更广泛的网络管理领域和用于添加高级特殊应用。

表 4

应用	主要优点
Cisco 语音管理器 允许您在能够支持语音功能的 Cisco 路由器上创建和维护拨号计划	• 为语音网络实现一个单一管理点 • 支持图形用户接口 (GUI) 语音服务供应 • 部署基于多语音协议的拨号计划 • 减少花费在服务供应上的时间 • 提供可扩展性, 允许实现快速的网络扩展和语音网络的重配置
Cisco QoS 策略管理器 (QPM) 帮助您对整个网络内的应用通信流进行分类并确定其优先级, 确保可靠的关键商业应用性能	• 为 LAN 和 WAN 实现基于 GUI 的中央策略部署 • 基于内容的通信流分类 • 可为语音通信流提供绝对优先级的高级语音 QoS 功能 • 确保语音、视频和音频这样的应用对吞吐量和延迟的要求能够得到满足 • 拥塞管理、拥塞避免和通信流整形服务 • 可控和可靠的 QoS 策略部署
Csico 安全策略管理器 通过配置 Cisco 防火墙和虚拟专网 (VPN) 路由器, 对网络边界安全性进行管理	• 从中央地点定义、分发、加强和核查整个网络内部的安全策略 • 简化复杂网络安全要素管理任务并提高其效率, 如边界访问控制、网络地址转换 (NAT) 和基于 IPsec 的 VPN • 使组织能够针对网络中的不同设备和技术准确地定义自己的安全策略
Cisco 安全访问控制服务器 (ACS) 提供用户身份验证、授权和记录 (AAA) 访问控制框架, 可以管理针对网络的用户和管理访问	• 从一个中央管理工具管理所有的用户身份验证、授权和记录 (AAA), 可以节省时间 • 通过控制用户和管理人员对网络的访问, 增强网络的安全性 • 通过记录服务跟踪和核查用户及管理人员的行为 • 能够与 Cisco 和所有能够支持远程访问拨入用户服务 (RADIUS) 或 TACACS+ 协议的组网解决方案实现互操作
Cisco 安全入侵检测控制器 监视和配置 CiscoSecure 入侵检测系统 (IDS) 传感器, 以检测和防止网络攻击	• 检测和终止来自内部和外部的未经授权的网络活动 • 将报警转发到一个寻呼系统并发出电子邮件, 以帮助对事件进行跟踪 • 允许网络管理员以一种可计量的方式与高级经理人员就安全问题进行通信

思科网络对企业 ERP 应用的网络优化

ERP 应用通常不会是网络上运行的唯一应用系统，而在多数情况下是要将 ERP 应用融入已有的其它应用中，共同运行于现有的网络基础架构。因此，ERP 系统将和大量的其它应用系统竞争有限的网络资源。

根据 Gartner Group 的调查，到 2003 年，基于 IP 的应用系统将成为网络带宽需求增长的主要拉动因素，局域网骨干带宽将增长 10 到 20 倍，广域网带宽将增长 300%。

到 2000 年，超过 20% 的网络应用将面临服务器响应性能所带来的问题，而起因是 IT 管理人员没有正确的理解网络与应用系统性能的交互作用，并进行合理规划。

更多的网络应用将对 QoS 及网络传输性能提出要求，而传统的仅靠增加网络带宽来提升网络性能的做法已不再有效。

无论对于新建或在建的 ERP 系统，对 QoS 的需求都是存在的。QoS 是指网络对于指定应用提供更好服务的能力。当一个企业的 ERP 系统因网络拥塞而产生问题的时候，对 QoS 的需求是显而易见的。虽然增加更多的带宽看上去是另一个解决方案，但它只能暂时地缓解问题，因位于 ERP 竞争带宽的应用会持续增长。同时增加带宽也是花费最大的解决方案，尤其对于广域网的应用环境。

有些企业为了保证 ERP 系统在网络中的运行而推迟了其它关键性应用的实施，如语音和多媒体应用。这样则使得企业不能享受通过网络化集成数据，语音和视频应用所带来的生产力提高和竞争优势，而且也不能使企业的网络资源最大化利用。

采用基于应用的 QoS 则可以解决这些问题并可带来如下好处：

- ERP 应用的快速响应将提高最终用户满意度
- 网络拥塞问题的解决将有助于更加快速有效的 ERP 实施。
- 减少对网络基础设施建设的投入将降低用户系统应用成本（TCO）。

采用基于应用的 QoS 可以在降低系统成本的同时提高系统应用性能，是最佳的解决方案。

QoS 的实施将为 ERP 应用数据流提供更优先的传输级别，以区别于其它非关键性的网络数据流如网页浏览，电子邮件和文件传输。在三级架构下的 ERP 系统包含多种不同的数据流类型。实施 QoS 应优先考虑客户桌面机与应用服务器间的连接，原因在于：

- 客户—服务器间数据流于其它应用数据流共享网络并竞争带宽。
- 数据流的传输会经过大量的网络设备和广域网链路。
- 网络带宽资源的有限，尤其在广域网环境下。

数据库—服务器间数据流通常不是 QoS 所关心的重点，因为这些数据流是在一个高性能的数据中心内部网络中传输的。但当出现下列情况时，服务器间的数据流也会是 QoS 应用的关注点：

- 采用数据库同步或异步备份及灾难恢复方案中的数据库间数据流传输。
- 采用分布式应用服务器结构时，服务器间需进行跨网络交互通讯。
- 电子商务或客户服务等前台应用与后台 ERP 应用系统数据流。

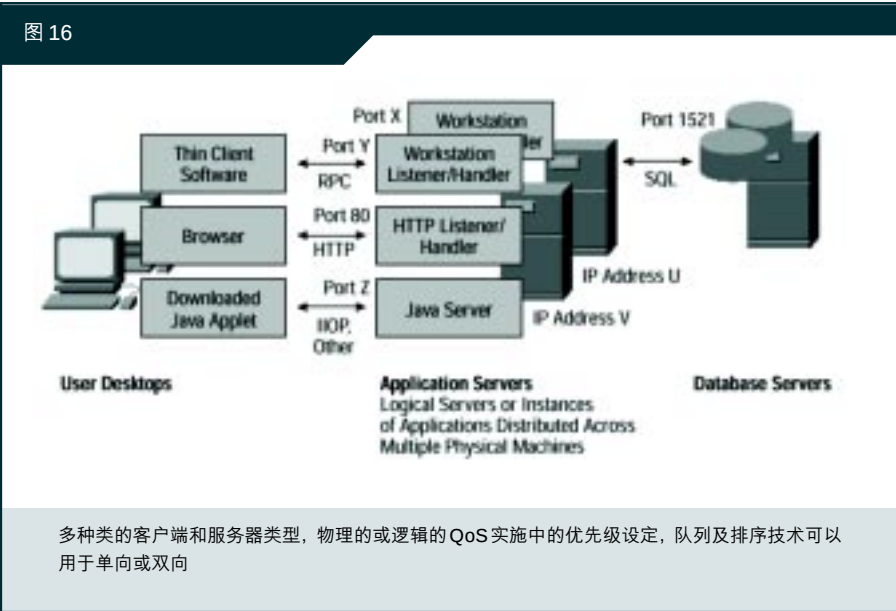
另一种需要进行区分的数据流是打印数据流，如报表打印。打印数据流需要占用大量的带宽，虽然不是十分关键的应用但仍需通过骨干网络传输。

网络对不同数据流的分类可以基于网络第三层和第四层参数进行，也可基于设备的物理端口，这样用户可以根据不同的应用定义不同的QoS的等级。此外，不断的开发研究将提供更加方便灵活的数据流区分方法，直到扩展到网络的第七层。在这里我们仅讨论利用三，四层参数进行数据流划分，这已经可以满足大多数ERP应用的需求，这些参数包括：

- IP 源地址和目的地址
- 网络协议
- TCP 或 UDP 源和目的端口号

大多数的大型ERP实施利用多应用服务器解决方案。在有些情况下多台的服务器运行同样的应用，但可能服务于不同的用户或用途，如针对事务处理的服务器或针对报告处理的服务器。不同的功能模块通常被安装于不同的服务器上。在这种情况下，QoS的定义可以是基于服务器的源IP地址和目的IP地址。

更进一步的ERP数据流划分可以根据第四层的端口号，端口号是在通过IP建立TCP/UDP连接时所使用的。多数厂商使用一些众所周知的特定端口号或特定范围内的端口号。如在Oracle 8数据库上的SQL listener就使用TCP端口1521，三层结构中的Oracle客户端则通过TCP端口9000连接到应用服务器上。在应用系统安装中可以使用默认的端口号或定义新的端口号以对应不同的连接类型。中间级的设备中包含多个不同地处理进程，每一个都有唯一的端口对应，如HTTP listener.server, Java server和message server等。



数据流传输，取决于那些是最关键的，最占用带宽的以及最容易产生拥塞的数据流。虽然一些ERP事务处理数据的传输是双向均衡的，但对于互联网浏览应用来说，服务器到客户端的数据流要远远超过反方向数据流。

QoS 的实施有两种方法。一种是按照不同的应用，不同的用户或内容将数据流划分不同的传输优先等级。这种方法适用于满足多数关键性应用对低传输延迟和低误码率的要求。另一种方法是为特定的应用保留其传输所需的带宽，这种方法最适于视频数据流，满足其对持续传输带宽保证的需要。

ERP 系统具有以下的特点在定义其服务等级时需要考虑：

- 对延迟和传输错误敏感,但对带宽不敏感(Delay and error sensitive but not bandwidth sensitive)
- 允许一定的传输延迟差(Tolerance for some variation in delay)
- 多进程数据流但每个数据流占用很少的带宽 (Many session flows each using small amounts of bandwidth)
- 不同的处理功能占用不同的带宽。

因为 ERP 应用系统的种类繁多，其运行的网络架构也不尽相同，因此要求网络具有范围广泛的 QoS 应用机制，以满足全网范围内端到端的 ERP 系统实施需要，而不用考虑网络设备的类型和连接媒体的种类。此外，还应该采用信令机制以保证不同应用的优先级设定可以通过信令在网络中传输。

Cisco IOS 软件可以提供多种的 QoS 工具以满足 ERP 应用对网络服务的要求。在典型应用中，这些工具作用于网络端口配置上，为特殊的网络应用提供相应的 QoS 参数设制。Cisco IOS 工具提供三个主要功能 --- 拥塞管理（队列及排序），拥塞避免及流量整形。对于特定的 ERP 应用进行测试可以使企业最优化使用 QoS 工具来支持他们的 ERP 应用系统。

5 总结

为什么选择思科公司

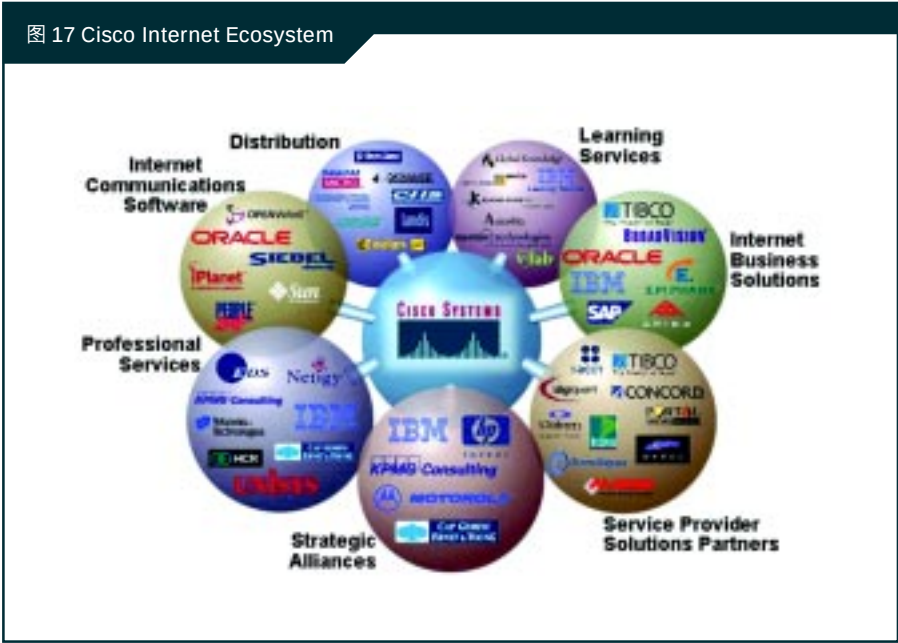
思科公司可以提供创建一个制造业企业端到端网络应用所必需的所有产品——局域网、广域网、网络安全、网络管理、无线网络以及 IP 通讯系统等。

采用思科公司的网络解决方案，网络便于管理，更加可靠，具有更好的性能，可以提供更多先进的功能，使网络基础设施真正帮助企业确立竞争优势。

思科公司已经发展成为一个庞大的企业，在全球拥有超过三万八千五百名员工，其中超过一万一千名工程师一直保持着我们在网络技术上的领先地位，而我们超过七千名的销售和技术支持人员一直与客户保持着密切的联系。思科公司的员工目前分布在 67 个国家，为我们在全球的客户提供支持，并致力于在全球建设 Internet 基础设施。

思科系统公司在中国的服务与支持日臻完善。目前，除已建成北京技术支持中心（TAC）和北京、上海、广州、成都备件库外，还提供中文 3W 服务与支持，包括 24 小时全球电话热线服务和中文电子邮件服务以及各种技术培训。经验丰富的思科工程师不仅为用户解决各种问题带来了极大方便，更重要的是加强了思科系统（中国）网络技术有限公司代理商的技术能力，使其能更好地在第一线为用户提供直接的支持。

另外，思科与众多业界领先的应用厂商合作，保证各类应用系统可以在思科先进的网络技术及设备平台上的性能，为用户提供完整的企业信息化解决方案。



思科愿以自己的先进产品和服务帮助企业建立适合自己系统应用的网络，借助网络的力量，使企业的管理和经营迈上新的台阶，在全球经济一体化的大潮中立于不败之地，在竞争中脱颖而出！



思科系统（中国）网络技术有限公司

北京

北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19~21层
邮编: 100738
电话: (8610)65267777
传真: (8610)85181881

上海

上海市淮海中路222号
力宝广场32~33层
邮编: 200021
电话: (8621)33104777
传真: (8621)53966750

广州

广州市天河北路233号
中信广场43楼
邮编: 510620
电话: (8620)87007000
传真: (8620)38770077

成都

成都市顺城大街308号
冠城广场23层
邮编: 610017
电话: (8628)86758000
传真: (8628)86528999

如需了解思科公司的更多信息, 请浏览<http://www.cisco.com/cn>

2004年思科系统（中国）网络技术有限公司北京印刷。版权所有。

2004 ©思科系统公司版权所有。该版权和/或其它所有权利均由思科系统公司拥有并保留。Cisco, Cisco IOS, Cisco IOS标识, Cisco Systems, Cisco Systems标识, Cisco Systems Cisco Press标识等均为思科系统公司或其在美国和其他国家的附属机构的注册商标。这份文档中所提到的所有其它品牌, 名称或商标均为其各自所有人的财产。合作伙伴一词的使用并不意味着在思科和任何其他公司之间存在合伙经营的关系。