思科中小型制造业企业整体解决方案

2011

目　录

1 概述

1.1 制造行业的市场现状

当前，全球制造业正在发生深刻的变化，行业与地理界限日渐消失，客户需求不断改变。这要求制造企业研发更具竞争力的产品，压缩产品生产周期，提高产品精度和加工装配效率。同时，在生产经营上，降低成本，增加利润，用更小的运营成本做更多的事情。为适应这一不断变化的趋势，全球制造企业纷纷求助于先进的 IT、网络技术。据 IDC 的数据，2006 年，全球制造业 IT 投资将达到 3749 亿美元，排在金融服务、公共事业、零售业、运营商、医疗等各行业之首。

中国正在从制造业大国向制造业强国的目标迈进。制造业将在很长的一段时期内保持高速增长。根据预测，下一个五年里中国的工业年增长率将高达 14-15%。工业增长率对 GDP 增长率的贡献将达 65-70%，并且 GDP 中工业所占比重将高达 50%(目前为 46%)。制造业将是中国 GDP 增长的主要推动因素。在中国即将成为世界工厂的前夜，为了加强企业的竞争力，制造业企业将会保持对 ERP、CRM 以及 SCM 等系统的强劲投入，从而带动制造业企业 IT 的整体投资走强。

1.2 制造行业信息化需求与应对

具体地分析，发现制造企业主要面临三大挑战：

最主要的挑战来自于制造业的全球化。随着生产基地和产品销售的全球化，产品和生产基地都需要在全球流动，因此，发展全球化的商业模式是最主要的挑战。

第二个挑战来自产品设计和生产的协同。由于产品可以在很多地区设计，也可以在很多地区生产，并且销售到很多地区的市场，因此，产品设计和生产之间的协同非常重要。从供应链的角度看，以前的话题是如何满足需求，而目前的挑战则变成如何在多个地点运送产品以满足供应，并且和竞争对手差异化。

另外，制造业企业面临一个共同的挑战，那就是成本控制。由于产品自身的利润下滑，售后服务将成为未来的利润增长点。由于售后服务涉及供应链的支持，因此，如何打造一个全面的供应链是制造业企业要面临的另外一个挑战。

应对以上挑战，制造企业需要网络的强大支持能力。传统的制造业网络基础设施，生产控制网络一般是分离的。早些时候，控制设备生产厂商没有统一、可靠的标准满足实时数据传输的要求，所以大家各自为阵，形成专用的网络，导致了生产控制网络与数据网络是不兼容。生产控制网络需要通过专门的网关与企业网络相连，二者之间交换的数据非常少，网络的效率低下。而者，网关设备昂贵，花费了企业大量的开支。由于需要专门技能的工程师维护，维护成本也相当高。

当前，比较明智的做法是，通过 IP 网络统一连接生产控制设备。由于以太网标准应用广泛，已经被生产控制厂商采纳，绝大多数生产控制设备都支持以太网。从安全、可靠性的角度考虑，通过虚网（VLAN）技术，可以在逻辑上将生产控制网络与办公、财务、研发等网络相对隔离，保证生产控制网络安全、可靠运行。

这样，IP 网络成了制造企业网络的通用协议，企业的 ERP、CRM、财务、采购、销售、生产、研发等系统，全部建立在 IP 网络之上。

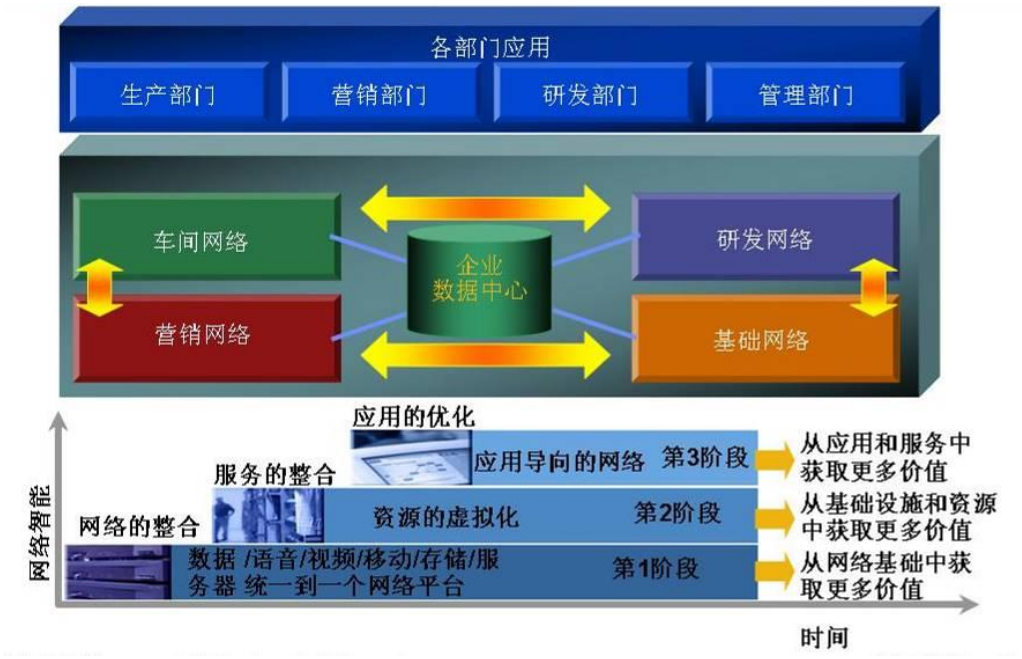
进一步，网络的功能向应用端扩展，不只是提供简单的数据传输功能。通集成一些过通用的共享应用和资源服务、虚拟化的组件，简化应用系统的开发，优化系统设计。

1.3 思科建设制造业智能化信息网络的整体思想

网络已经成为所有企业应用的基础。思科公司基于自身在协议优化、路由交换以及多业务集成方面的专业经验，提出了面向应用的网络架构，将一些普遍使用的服务集成至网络中，从而更加方便的向应用提供这些服务。

具体地说，在网络基础设备层的基础上，可以将安全服务、移动服务、存储服务、语音和协作服务、计算服务、身份识别服务等虚拟化，通过中间件和应用平台统一提供给应用层。方便企业构建及时消息、统一消息、多媒体会议、IP 呼叫中心、IP 电话、视频传输等协作应用，亦可以将这些服务集成到 OA、CRM、ERP、SCM、研发管理、E-Learning 等系统当中。

以上我们看到网络在功能方面向高层应用扩展的路径。下面，我们从一个企业的角度，看看网络建设的发展过程。思科公司根据自己对网络的深刻理解和把握，提出了建设制造行业智能化信息网络发展三个阶段的蓝图：第一阶段实现网络的整合，将数据、语音、视频、移动、存储、服务器统一到一个网络平台，企业可以从网络基础设施获取更多价值；第二阶段服务的整合，让资源的虚拟化，从而更加有效、灵活地利用联网的资源；第三阶段实现应用的优化，网络以应用为导向，用户可以随时以任何方式访问他们所需要的应用和信息。



2 制造业网络基础平台技术方案

2.1 技术方案总体设计目标

2.1.1 高可用性

对于制造业企业的生产网络，高可用性是进行网络设计的基本目标。高可用性是指一方面要保证导致网络不可用的设备故障时间极短，另一方面，还要要保证网络能够满足各类数据传输的需求，不会因性能下降而导致不可接受的响应时间；

在达到高可用性的目标网络设计中要把先进的技术与现有的成熟技术结合起来，充分考虑到制造业生产网络应用的现状和未来发展趋势。设计中将采用高可靠性的网络产品和完备的网络备份策略来满足可靠性的要求，对于不同层次的设备和线路进行不同级别的可靠性设计，使网络具有故障自愈的能力。可靠性设计不仅包括网络设备等物理设计的可靠性，同时包括路由等逻辑设计的可靠性。制造业企业的骨干网络的可用性应当达到99.999%的目标。

2.1.2 高安全性

特殊的生产型业务性质决定了网络安全对于制造业企业有着极为重要的意义，在网络设计过程中采用一体化的网络安全设计思想，从而充分保证网核心骨干、汇聚、边缘接入多个部分网络访问的高安全性，将来可以实现到自防御网络体系的平滑升级。

2.1.3 可扩展性

业务的发展对网络的需求是不断变化的，网络应用系统为了满足这些需求也会随之变化。面对不断变化的情况和需求，网络应当能够作出快速和有效的反应。因此，网络必须具备良好的可扩展性，应支持核心业务系统的不断扩展，适应未来业务的发展和变化。同时，网络结构应当能够变化，具有灵活的伸缩能力，网络设备可以扩充和升级。

2.1.4 可管理性

随着网络规模的不断扩大和网络的不断复杂，网络的维护量随之增加。整个网络的可管理性变得尤为重要。因此，网络系统应当具有统一的可管理性，建立统一的网络管理平台。不仅实现对网络设备的管理，同时实现对网络策略的管理和不同协议的多级维护。

2.1.5 先进性

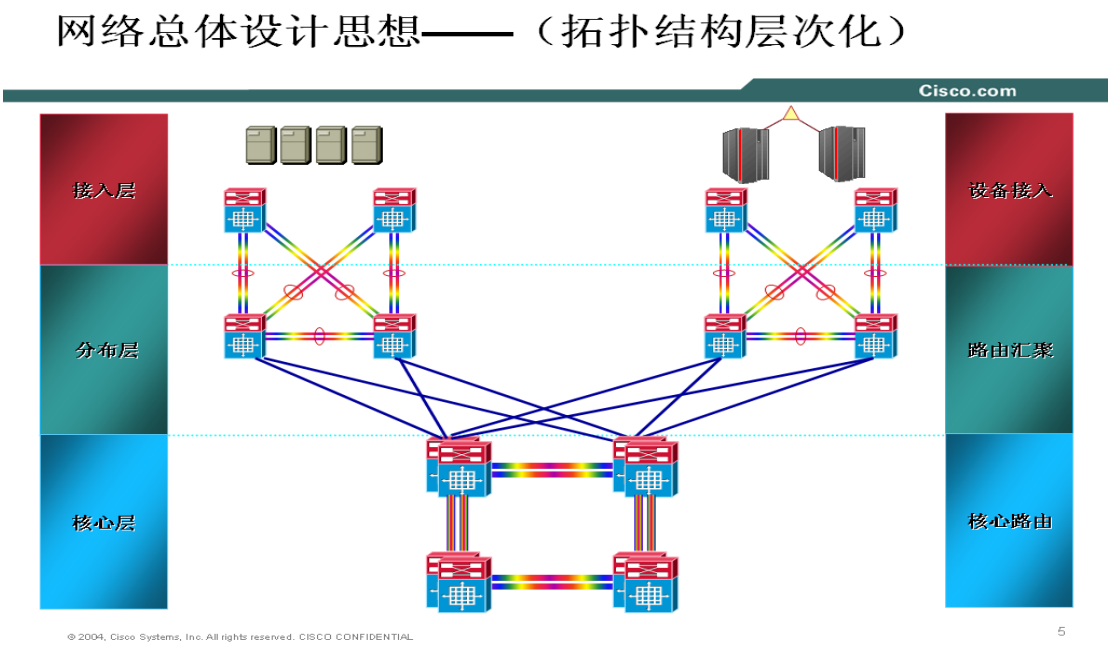
采用国际领先的网络产品和相关技术，支持业界最丰富的网络应用协议，支持现有业务和将来增加的新业务，保证骨干网上各类业务可靠传输和服务质量，满足制造业企业未来业务快速发展的需求。

2.2 技术方案设计原则

2.2.1 层次化原则

在制造业企业未来网络架构设计中，为了实现一个可管理的、可靠的、高性能网络，我们将采用层次化的方法，将网络分为核心层、分布层和接入层三个层次进行设计。这种层次结构划分方法也是目前国内外网络建设中普遍采用的网络拓扑结构。在这种结构下，三个层次的网络设备各司其职又相互协同工作，从而有效保证了整个网络的高可靠性、高性能、高安全性和灵活的扩展性。

拓扑结构如下图所示：



其每一层的网络设备功能描述如下：

- 核心层：提供高速的三层交换骨干
  - 核心层不进行终端系统的连接；
  - 核心层少用或不实施影响高速交换性能的 ACL 等功能。
- 分布层：作为接入层和核心层的分界层，分布层完成以下的功能：
  - 本功能区 VLAN 间的路由；
  - IP 地址或路由区域的汇聚；
- 接入层：提供 Layer2 或 Layer3 的网络接入，通过 VLAN 定义实现接入的隔离。网络接入层具有以下特点：

– 接入层接入端口规划容量根据实际使用情况具有一定的扩展性；

上述每一个层次结构内部需要采用冗余的架构来保障该层功能的稳定可靠。

2.2.2 标准化原则

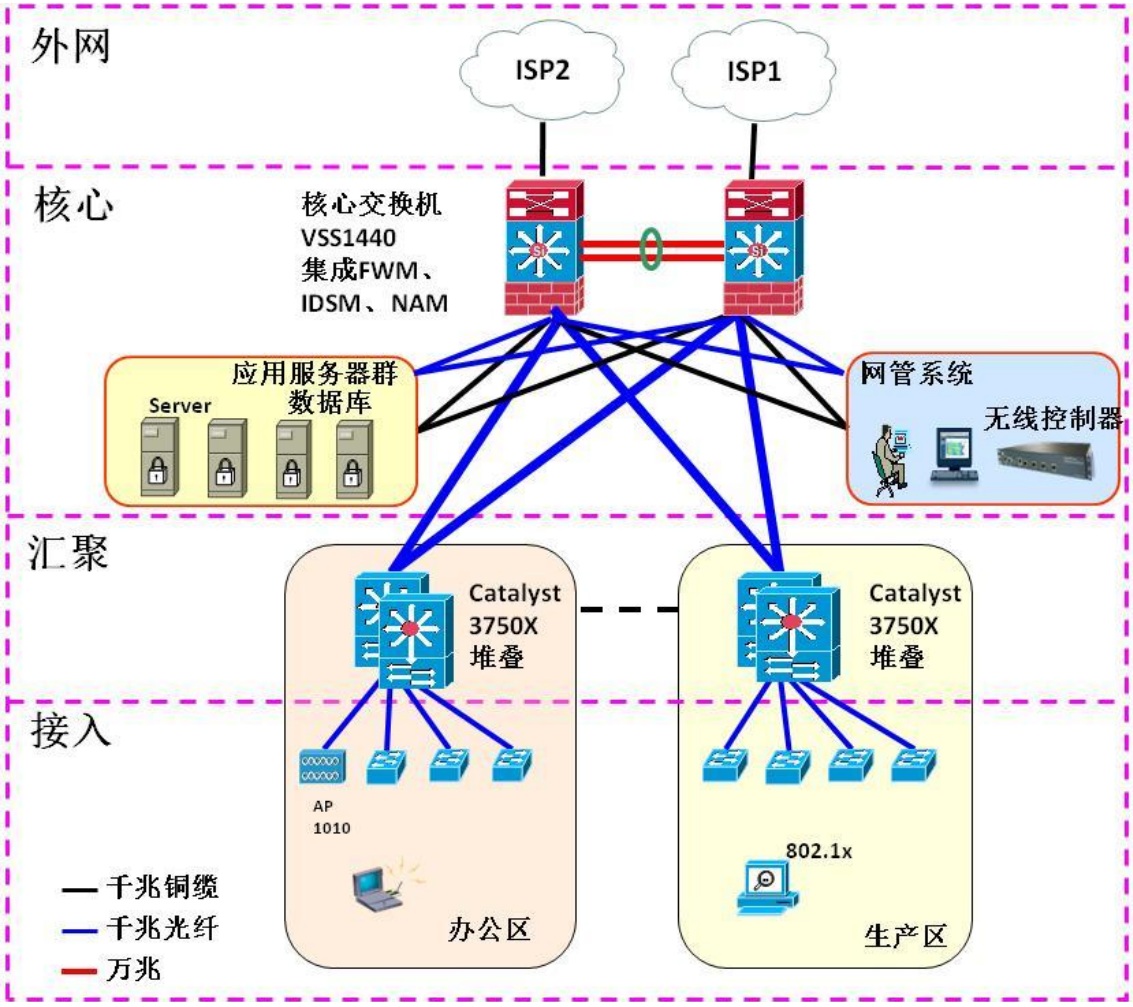
网络设计中所用的各种管理信令、接口规程、协议须符合国际标准，便于扩展和网络的互连互通。支持国际上各种通用标准的网络协议和标准等，支持大型的动态路由协议，支持策略路由功能。保证与其它网络（如互联网等）之间的平滑连接。

2.3 制造业企业网络架构设计

2.3.1 整体网络拓朴结构设计

整个网络采用层次化设计原则，从网络的逻辑结构来看，网络分为三层，即：核心层、汇聚层和接入层。核心层由 2 台核心路由交换机组成，核心路由交换机之间通过 10G 万兆光纤冗余互联形成高速万兆核心层。各汇聚层路由交换机通过千兆光纤分别冗余上联至核心路由交换机。各个接入交换机也通过双千兆光纤冗余上联至两台汇聚路由交换机。

网络的总体结构设计如下图所示：



2.3.2 网络系统功能

本方案选用核心 10GE 万兆以太网络技术，同时选用了 Cisco 公司成熟、稳定、先进的企业级最高端路由交换机，并对企业网络进行优化设计，使园区网络系统具备丰富的网络系统功能，为企业生产业务系统的稳定运行奠定了坚实的基础。

企业智能化信息网络系统功能总结如下：

- 高速 L2/L3 层数据传输：核心层至汇聚层可选 10GE 或 1GE 冗余链路，汇聚层至接入层 1GE 冗余链路。
- 持续可用性（高可靠性）：核心节点、汇聚节点采用冗余双设备，核心节点之间网状冗余连接，核心节点和汇聚节点之间双链路冗余互连，接入节点双链路冗余上联至汇聚节点，使用高度智能的动态路由协议，核心和汇聚设备均采用双电源的冗余配备。网络系统在设备级、链路级、系统级均具备极高可靠性。
- 支持 MPLS VPN 功能：所有核心节点路由交换机及所有板卡具备全部 MPLS 功能，可以为制造业企业园区网络提供完善的 MPLS VPN 功能。
- 提供 Multicast 组功能：本方案中选用的所有 Cisco 路由交换机均具备丰富的组播功能，不仅具备所有其它厂商设备所有组播功能外，Cisco 还提供其它厂商不具备的更优化、更高性能的 SSM 和 IGMPv3 功能,同时 Cisco 网络系统还提供独有的 MPLS-VPN 内组播功能－－－该功能对制造业企业网络视频监控业务非常有用。方案中选用的 CISCO 路由交换机都支持组播管理 MIB，可以通过 Cisco 组播网络管理软件（CMM）进行组播管理，可以打消用户对组播流像是“黑夜行船”无法控制的顾虑。
- 提供丰富的 Qos 功能：本网络系统提供 DiffServ Qos 机制，避免了瞬时拥塞造成关键业务、关键数据丢失，确保网络系统的持续可用。
- 提供了丰富的网络安全功能：Cisco 网络设备本身具备许多丰富的安全防护功能，从而使网络系统自身具备极高的威胁抵御能力，同时利用 ASA

自适应安全设备、IPS/IDS 入侵检测设备，或采用 6500 平台上的安全服务模块，更进一步提高了网络系统的安全防御能力。

2.3.3 核心层设计

对于企业生产网络的核心层，我们建议采用思科部署在 Catalyst 6500 交换机平台上的虚拟交换系统（VSS）技术进行构建。

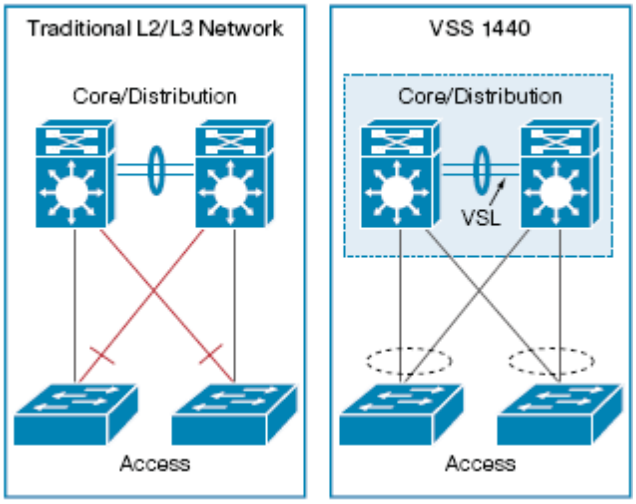
Catalyst 6500 交换机上采用的虚拟交换系统技术为 IT 经理设立了一个新标准，能够帮助他们在构建永续、高度可用的状态化网络的同时，优化网络资源的使用。VSS 将在数据中心接入层以及园区和数据中心分布层/核心层设计中发挥重要作用。

Cisco Catalyst 6500 系列交换机虚拟交换系统（VSS）1440

Cisco® Catalyst® 6500 系列交换机虚拟交换系统（VSS）1440 是一种网络系统虚拟化技术，将两台采用了 Virtual Switching Supervisor 720-10G VSS 的 Cisco Catalyst 6500 系列交换机组合为单一虚拟交换机。在 VSS 中，这两个交换机中的管理引擎的数据面板和交换阵列能同时激活，因此总系统交换能力可达 1440Gbps。

VSS 成员通过虚拟交换机链路（VSL）连接。VSL 在虚拟交换机成员之间使用标准万兆以太网连接（多达 8 条，以提供冗余性）。通过在 Virtual Switching Supervisor 720-10G 或 WS-X6708-10G 模块的任意端口上使用万兆以太网上行链路，即能形成 VSL。除在 VSS 成员间进行控制面板通信外，VSL 也能传输普通用户流量。

VSS 支持所有采用集中或分布式（利用 DFC3C 或 DFC3CXL）转发模式的 Cisco Catalyst 6500 系列交换机 6700 系列模块。



传统L2/L3网络
核心/分布层
接入层

VSS 1440
核心/分布层
接入层

VSS 1440 有哪些优势？

与传统的 L2/L3 网络设计相比，VSS 1440 提供了多项显著优势。大体说来，其优势可归纳为以下三个主要方面：

- VSS 能够提高运营效率
  - 单管理点，包括配置文件和单一网关IP地址（无需HSRP/ VRRP/GLBP）
  - 多机箱EtherChannel®（MEC）创建了简单的无环路拓扑结构，不再依靠生成树协议（STP）
  - 底层物理交换机经由标准万兆以太网接口相连，在位置方面提供了灵活的部署选项
- VSS 能够优化不间断通信
  - 机箱间状态化故障切换不会干扰需要使用网络状态信息的应用。凭借VSS，在一个虚拟交换机成员发生故障时，不再需要进行L2/L3重收敛，能在一秒内实现确定性虚拟交换机的恢复。
  - 与基于生成树协议的收敛不同，使用EtherChannel（802.3ad或PAgP）能在一秒内完成确定性L2链路恢复。
- VSS 能够将系统带宽容量扩展到 1.4 Tbps
  - 在冗余Cisco Catalyst 6500系列交换机上激活所有可用的L2带宽，在EtherChannel基础上进行精确的负载均衡。
  - 为冗余数据中心交换机上的服务器网络接口卡（NIC）提供基于标准的链路汇聚，实现最高服务器带宽吞吐率。
- 消除了因非对称路由引起的单播洪泛，减少了园区内流量的跳数，从而节省了带宽。

2.3.4 汇聚层设计

汇聚层建议配置思科企业级的堆叠式交换机 Catalyst 3750-X 系列。


Catalyst 3750-X 系列可利用思科 StackWise Plus 技术创建一个由多达九台交换机组成的统一堆叠系统，有很强的恢复能力，它使用单个 IP 地址、单个 Telnet 会话、单个命令行界面 (CLI)、自动版本检查、自动配置等提供简化的管理。StackWise Plus 提供了与现有 Cisco Catalyst 3750 系列交换机的向后兼容，同时将堆叠系统吞吐量提升到 64 Gbps。StackWise Plus 也支持 Cisco Catalyst 3750-X 系列交换机中的本地交换功能。如果本地交换数据包进入 Cisco Catalyst 3750-X 系列或 3750-E 系列交换机中的某个端口，而其目的地是同一交换机中的另一个端口，则数据包不必遍历整个堆叠环，从而提高交换机的转发容量。

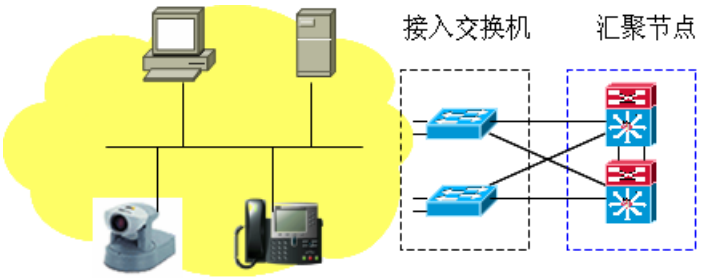
此外，Cisco Catalyst 3750-X 系列在业界率先引入了 Cisco StackPower 技术，这个创新的电源互连系统能让堆叠中的电源作为公共资源，在所有的交换机之间进行共享。使用 StackPower 电缆（，通过交换机背面的特殊连接器，可以在 StackPower 堆叠中配置多达四台交换机。

位于汇聚层的 Catalyst 3750-X 堆叠交换机可以通过千兆光纤主干上连核心交换机的千兆端口，同时也保留了未来升级为万兆主干的能力。该系列交换机支持两种 4 端口的上行链路网络模块。


用户可以灵活选择 4 个 GbE 端口 (3KX-NM-1G) 或 2 个 10GbE 端口 (3KX-NM-10G) 的网络模块。10GbE 上行链路模块提供 4 个物理端口，各包括 2 个 SFP+ 和常规 SFP 端口。SFP+ 接口支持 10GbE 和 GbE 端口，能让客

户利用在 GbE SFP 中的投资，并随业务需求的变化升级到 10GbE，而不必进行访问交换机的全面升级。上行链路模块可热插拔。

2.3.5 接入层设计



- 接入层节点需根据业务要求来确定，分别配置 2 类接入交换机：

高性能接入交换机	• 支持 3 层交换功能，提供大业务量或节点业务服务器等关键设备的接入，并可作为 MPLS VPN 的多业务 CE 设备
一般性能交换机	• 支持 2 层交换功能，实现业务隔离，提供大量信息终端设备的接入

-
- 接入层是网络的最边缘部分，直接连接网络用户终端（MES/ERP 系统等）。接入层交换机由于数量很大，所以在选择时要考虑要有较高性价比。
- 同时接入层交换机还应该有较为完善的功能，如较强的 QoS 能力，一定的安全控制能力，支持 VLAN 技术等。在本方案中，可选用三款交换机：Catalyst3750、Catalyst3560、Catalyst2960。
- 所有接入交换机采用 2 条千兆单模光纤线路双上联至汇聚层路由交换机，Catalyst3750/3560/2960 交换机提供 48 个 10/100M 或 1000M 电口（依具体型号而定）连接终端。

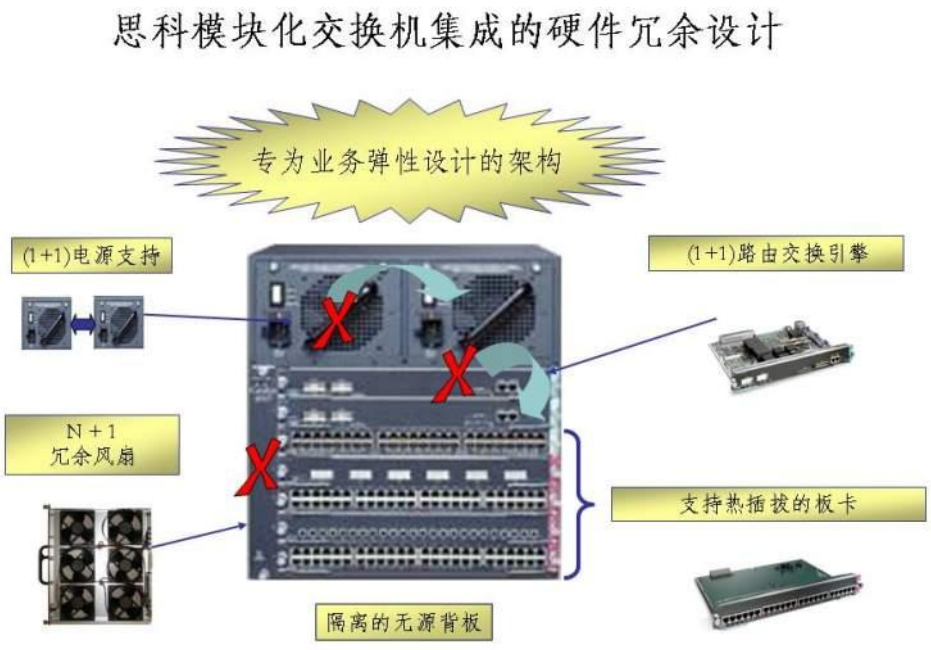
2.3.6 网络高可靠性设计

网络的可靠性是为了避免单点故障的出现。主要体现在两个方面：一方面在于网络拓扑的设计，尽量使网络上不存在单点故障；另一方面，网络设备必须支持插卡、接口、电源等部件的冗余与热插拔能力以及支持例如 VRRP/HSRP/GLBP 等冗余协议。但是网络的可靠性并不是单一设备可靠性的简单叠加，它主要包括：

- 设备级别的可靠性
- 链路级别的可靠性
- 软件级别或系统级别的可靠性

下面将详细介绍思科公司是如何使用独特的可靠性机制和技术创新来保障企业用户关键信息的可靠传递。

设备级别的可靠性



设备级别的高可靠性设计是网络核心设备选型时最关键因素。此时我们往往只考虑设备硬件的冗余，忽略了运行和存储于硬件上的软件、网络信息和管理信息。

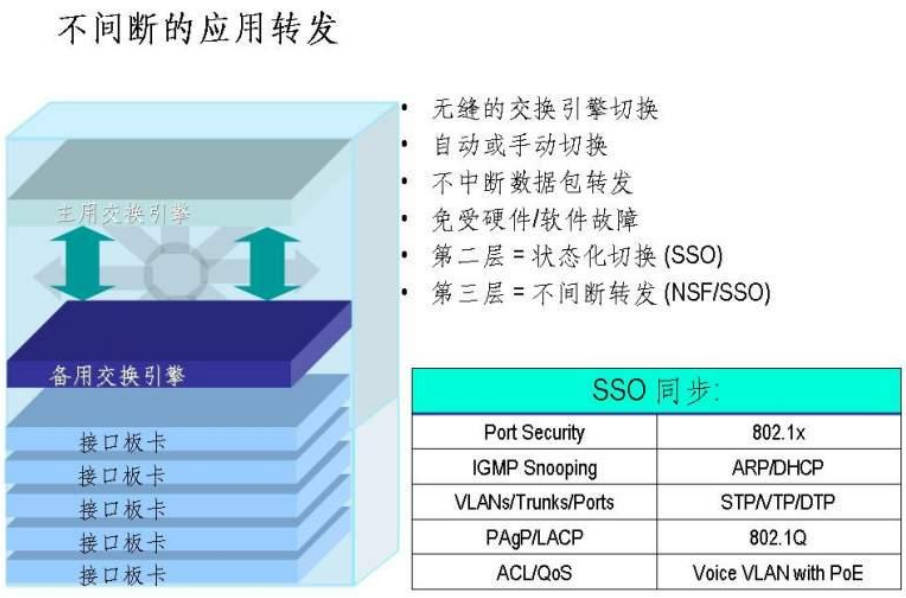
一般情况下，设备级别的可靠性主要包括：

1. 物理冗余：提供双电源、双引擎、双交换矩阵和双时钟，甚至双核心设备。

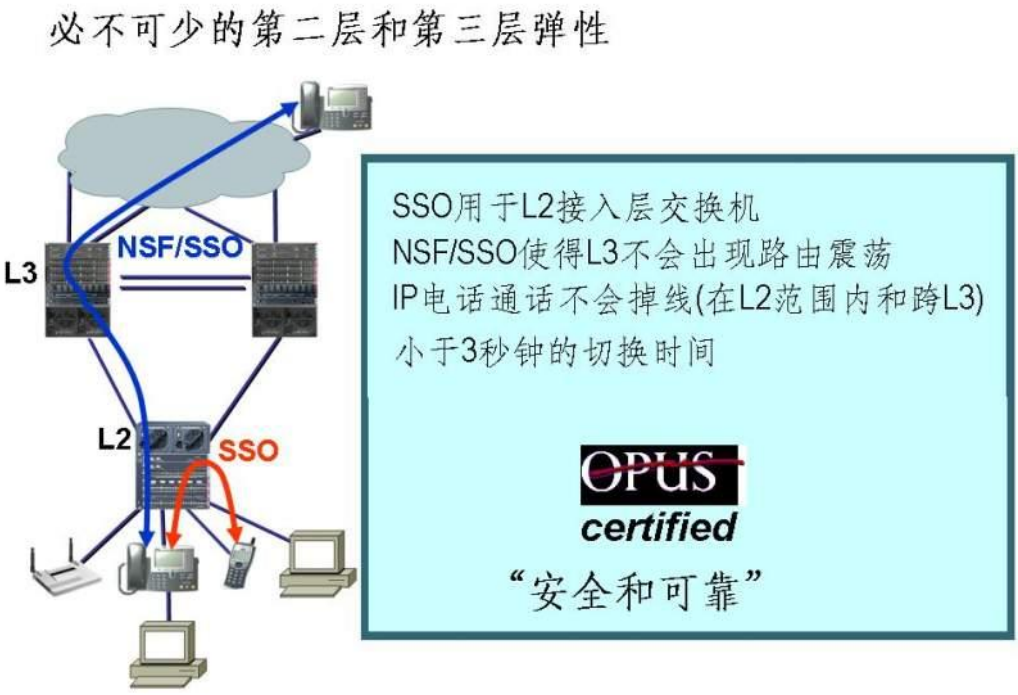
思科的模块化交换机，包括 Catalyst 6500 的体系架构都是专为保证企业业务弹性而设计的，所有关键部件如路由交换引擎、电源、风扇均支持 1+1 或 N+1 冗余备份，所有的板卡都支持热插拔，并且采用隔离的无源背板连接各个部件，避免了某些厂商使用有源背板带来的单点故障问题。

2. 逻辑冗余：利用 Ethernet Channel、FastEthernet Channel 和 Gigabit Ethernet Channel 技术为设备间链路提供负载的分担和链路的冗余；利用 VRRP/HSRP/GLBP 技术为第三层路由提供冗余，并利用所形成的虚拟路由器实现路由器之间的负载分担和冗余操作。后面的章节会详细介绍思科冗余网关协议的选择。
3. 不间断转发（Nonstop Forwarding，NSF）和状态化切换（Stateful Switchover，SSO）功能：用于维护路由器中两个交换引擎之间路由状态信息，使主备引擎可以在不中断网络运行或丢弃包的情况下进行切换；在切换期间， Cisco SSO 提供零中断的第二层连接，而 Cisco NSF 保证转发第三层数据包时保证不丢失分组，或丢失量最小。分组连续转发可以重新建立对等关系，而无需在整个网络中再次收敛路由协议。

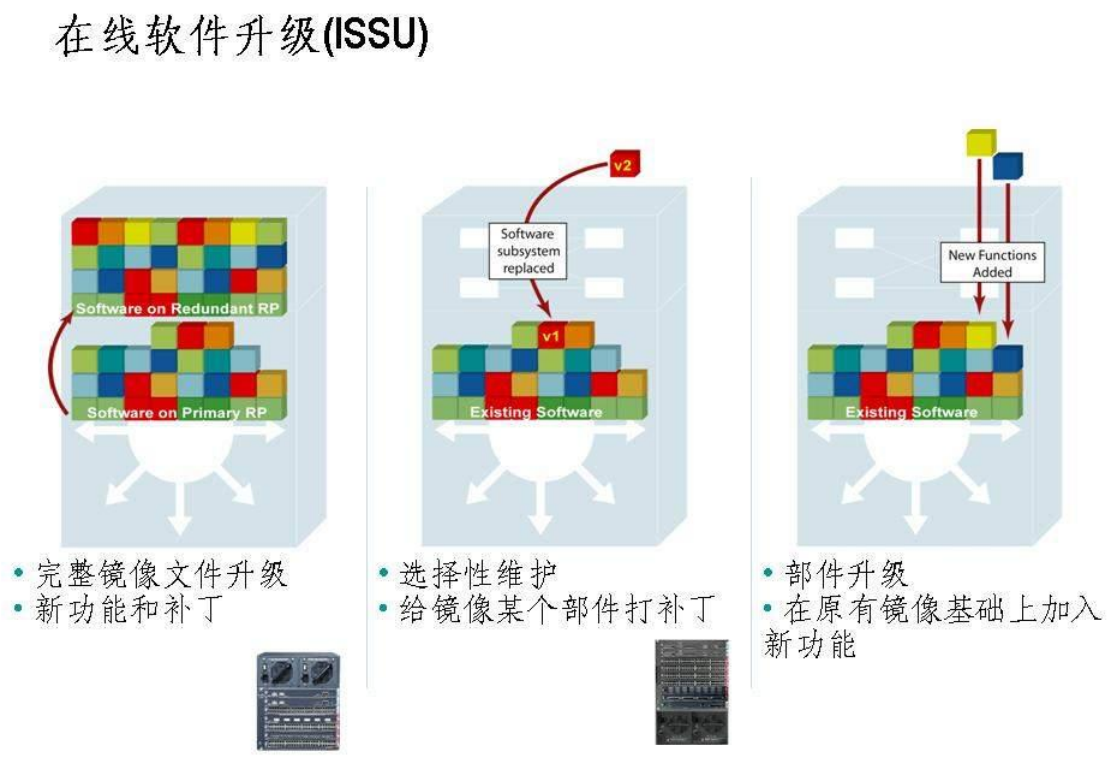
Catalyst 6500 支持 NSF/SSO 特性。



NSF/SSO 是制造企业未来多业务融合网络必不可少的关键特性，第三方权威测试机构 OPUS 实验室对思科模块化交换机的 NSF/SSO 特性作了严格测试。测试网络中部署了思科 IP 电话系统和无线局域网接入点。测试结果表明思科 NSF/SSO 特性充分保证了第二层和第三层的弹性，L2 的状态在引擎切换过程中保持，L3 的路由也不会发生震荡。网络上的关键业务，尤其象 IP 语音通信这样的时延敏感应用也不会受影响，正在通话的 IP 电话通话不会掉线，无论此通话是保持在 L2 范围内还是跨过了 L3 的网络。进一步的测试还表明 NSF/SSO 特性不会降低用户网络的安全性，即在主备引擎切换过程中，所有设置的安全机制 ACL 策略等等都保持工作，不会给外来黑客有可趁之机。



4. 在线软件升级（ISSU）：此功能指的是在升级系统的软件或软件模块不会中断或影响系统的操作。在线软件升级功能是

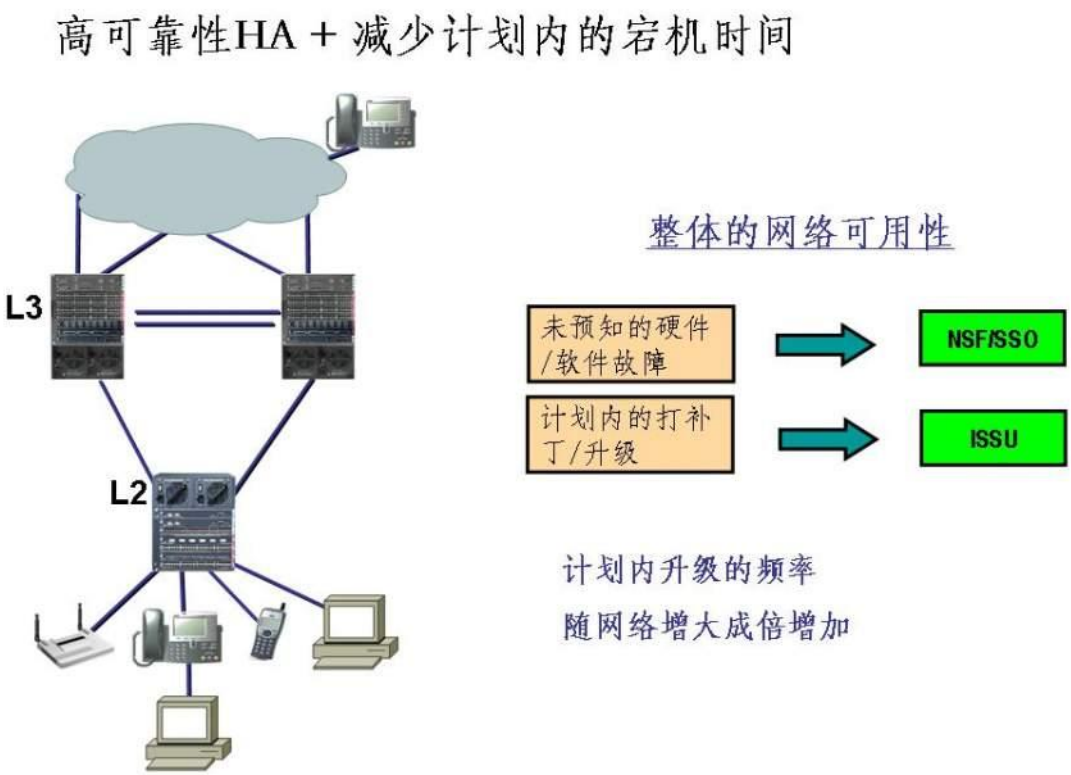


思科 Catalyst 6500 系列中的 IOS 软件模块化特性主要有简化软件变更、最小化计划外宕机时间和实现自动化策略控制三个方面的好处：

- 首先，IOS 模块化简化了软件变更。通常，企业 IT 部门部署新软件之前都要经过验证，规划宕机时间表，最终部署。而模块化的 IOS 软件大大加快了验证速度，减小了软件兼容风险，另外，通过不间断软件升级（ISSU）子系统，可以在其他组件正常运行的同时更改代码，从而实现零宕机时间。根据客户调查的结果，企业可以将验证和部署新软件的时间从几个月缩短到几周，这对于保障关键业务，诸如交易平台、医疗应用、支持音频和视频的实时网络服务等业务都非常重要。简化的软件变更还大大加强了企业的网络安全水平。
- 其次，通过可自行恢复的独立进程，IOS 模块化可以最小化计划外宕机时间。IOS 模块化将不同的进程限制在独立的受保护的存储空间中，这项创新使系统可以单独重启某项进程，并提供不同进程的状态检测，这样，出错的进程就可以重新启动并恢复到上一个已知的状态和配置，而不必重新启动整个系统。重启恢复时间也从数分钟缩短到数毫秒。

- 第三，通过整合内置事件管理器（EEM）提供进程级别的自动化策略控制。自动化策略控制将耗时的任务下放给网络，让 IT 部门可以专注于更有价值的工作。这就帮助企业减小了"运营鸿沟"的不利影响。网络管理员可以用思科命令行界面（CLI）或工具通用语言（TCL）代码来制定策略，这些策略可用于不同方面，包括检测服务器上可用的升级补丁，下载补丁，并在预先指定的时间安装等。

Catalyst 6500 的在线软件升级功能极大地增强了网络的整体可靠性，从硬件/软件一体化可靠性的角度帮助客户提升了整个业务的永续性，是在过去硬件冗余性基础上的一大进步。近一步来说，NSF/SSO、ISSU 和 Catalyst 6500 现在拥有的模块化 IOS 互相配合工作，可以大大减少用户计划外和计划内的宕机时间，并且可以非常方便地进行软件升级、功能升级和 Bug 修复等维护工作。



链路级别的可靠性

网络链路级可靠性可以分为 2 层路由链路和 3 层路由链路两个方面：

1. 更快的链路灾备
    - 快速生成树：为了解决了物理线路中断所造成的网络终端，我们往往会设置备份的物理线路，但是它们往往会形成环路，回路会产生无休止的数据路径，导致网络服务的中断以及额外的系统管理费用。IEEE802.1D 生成树协议通过从网格化物理拓扑结构而构建一个无环路逻辑转发拓扑结构，提供了冗余连接，消除了数据流量环路的威胁。原始生成树协议 IEEE 802.1D 通常在 50 秒内就可以恢复一个链接故障[融合时间=(2xForward_Delay)+Max_Age]。当设计此协议时，这种停机还是可接受的，但是当前的关键任务应用（如语音和视频）却要求更快速的网络融合。为加速网络融合并解决与生成树和虚拟 LAN（VLAN）交互相关的地址可扩展性限制的问题，IEEE 委员会开发了两种新标准：在 IEEE 802.1w 中定义的快速生成树

协议（RSTP）和在 IEEE 802.1s 中定义的多生成树协议（MST）。如果使用适当的话，RSTP 能将在连接故障和恢复时所需的重新配置和恢复服务时间，减少到低于秒的量级，并保持同基于 STP 设备的兼容性。RSTP 可以保证在一个桥接/ 交换、桥接端口或 LAN 发生故障之后，其连接性的快速恢复。一个新的根端口可以快速转换至传送端口状态。在 LAN 中桥接与转换之间明确的应答，允许指定端口快速转换至传送端口状态，此时，桥接端口可被配置在桥接/交换重新初始化时直接转换为传送端口状态。当特定的桥接端口连接于 LAN 边缘的一个 LAN 段时，这一点将十分有用，例如在该 LAN 段没有其它的桥接或交换可用的情况时。Catalyst 全线交换机均支持 IEEE 802.1w 和 IEEE 802.1s 协议。

- PortFast：生成树协议会运行在交换机的所有端口上，但接入层交换机的许多端口连接着工作站或服务器，这些点到点连接是不会出现环路的。PortFast 技术将这类端口从 STP 的计算中排除出去。当主机连接到交换机时，启动 PortFast 的端口将直接成为转发状态，避免了 STP 计算造成用户在最初一段时间不能使用网络的情况，将工作站或服务器连接上网的时间减至最短。针对 Access 端口跳过 listening-learning 阶段。
- UplinkFast：当接入层交换机有两条链路连接汇聚层设备时，如果出现环路肯定会有一条链路在 STP 计算时被阻断掉。在主链路断掉时，被生成树阻断的端口需要重新进行计算，在经过 50 秒后被打开参与用户数据的转发。在访问层交换机上启动 UplinkFast 功能后，如果交换机在直连的主链路上检测到失效，那么交换机会立即将被阻断的备份端口打开转发数据，通常情况下只需要 2 到 4 秒钟的时间。这样就可以通过 UplinkFast 提高交换网络的收敛速度。
- BackboneFast：汇聚层交换机与主干交换机之间为保证链路的可靠性，往往会形成环形链路，环形链路上某个链路或接口的故障会引起生成树的重新计算。在主链路断掉时，被生成树阻断的端口需要

重新进行计算，在经过 20 秒的最大等待时间（Max_Age）后进入侦听（listening）状态，在经过 30 秒后被打开参与用户数据的转发。在汇聚层交换机上启动 BackboneFast 功能后，如果交换机在非直连的主链路上，即迂回链路上检测到失效，交换机快速收敛去掉最大等待时间（Max_Age）20 秒，因此可以节省生成树的计算时间至 8~30 秒。

- 增强功能： UDLD（线路单向连通问题自动诊断功能），用于检测光纤或铜缆以太网链路上的故障。由于生成树具有单向的 BPDU 流，对这种故障相当敏感。在一个端口突然不能发送 BPDUs 的时候，引起邻居的 STP 状态改变，导致邻居的“blocking”端口切换到“forwarding”状态。由于原 forwarding 端口仍然可以接收包，从而引起环路。因此，UDLD 可以监视物理电缆的配置，并将通过“ErrDisabled”状态将配置不正确的端口给 down 掉。避免出现单向连接，当检测到一个因为介质或端口故障导致的单向连接时，将端口 shutdown 并标识为“ErrDisabled”状态，同时产生一个 syslog 信息。

2. 更全的链路捆绑

- Cisco PAgP 和 IEEE 802.3ad：PAgP 是一个用于在检查 Channel 两端的参数的一致性以及在出现增加链路或链路失效时的重新适配的一个管理协议，PAgP 协议控制每个独立的物理或逻辑端口打成 Channel 的行为，如果一个 Channel 中的某个链路失效（拨掉光纤或光纤断了）了，agport 会进行更新，流量会在现有的端口上重新进行 hash 计算，不会有包丢失。源自思科 ISL 的 802.3ad 把两个或多个 Link 捆绑成逻辑的虚拟的单一通道，子 Link 之间提供自动流量负载平衡和冗余，很大程度上会简化系统集成，减少升级骨干网络的投资。
- 点到点的冗余连接在重新建立的链路仍可进行负载均衡，链路恢复时间小于 1 秒

3. 更强大的路由灾备

- VRRP/HSRP：虚拟路由器冗余协议/ 热备份路由器协议，实现 VRRP/HSRP 的条件是系统中有多台路由器，它们组成一个“热备份组”，这个组形成一个虚拟路由器。在任一时刻，一个组内只有一个路由器是活动的，并由它来转发数据包，如果活动路由器发生了故障，将选择一个备份路由器来替代活动路由器，但是在本网络内的主机看来，虚拟路由器没有改变。所以主机仍然保持连接，没有受到故障的影响，这样就较好地解决了路由器切换的问题。
- GLBP：网关负载平衡协议，相对于 HSRP 与 VRRP，GLBP 具有很多的优点，在保护第一个跳动路由器的同时能在所有可用路径上分配分组负载，使得网络带宽的利用率更高。以前，如果主路由器或路径中出现错误，则第一个跳动冗余功能只能在备份 WAN 路径上转发分组。GLBP 可使组中的任一路由器担当备份作用，并能简化配置。最大的区别是在 HSRP 和 VRRP 中同一个 GROUP 中只有一个路由器在转发流量，其余路由器只是起备份作用，而在 GLBP 中，同一个 GROUP 的所有路由器（最多 4 个）可以同时转发流量。这样就起到了负载均衡的作用。

系统级可靠性

系统级可靠性是指软件重新加载或升级时，系统重新启动对网络运行所造成的影响。系统级可靠性在组网的过程中往往容易忽略，但是对于主干网络设备来说，连接中断所造成的影响会很快波及整个网络。因此，尽可能大的缩短系统软件的加载时间才可以有效提供系统级可靠性。

2.4 基础网络平台主要产品组合（参考）

- 核心层路由交换设备

Cisco Catalyst 6500 系列交换机

Cisco 7600 系列路由器

VSS 1440 虚拟交互系统

- 汇聚层设备：

Cisco Catalyst 4500 系列

Cisco Catalyst 3750-X 系列

- 接入层设备：

Cisco Catalyst 2960 系列

Cisco SF 300 系列

- 工业以太网交换机

Cisco IE3000 系列

3 制造业智能化信息网络的集成安全设计

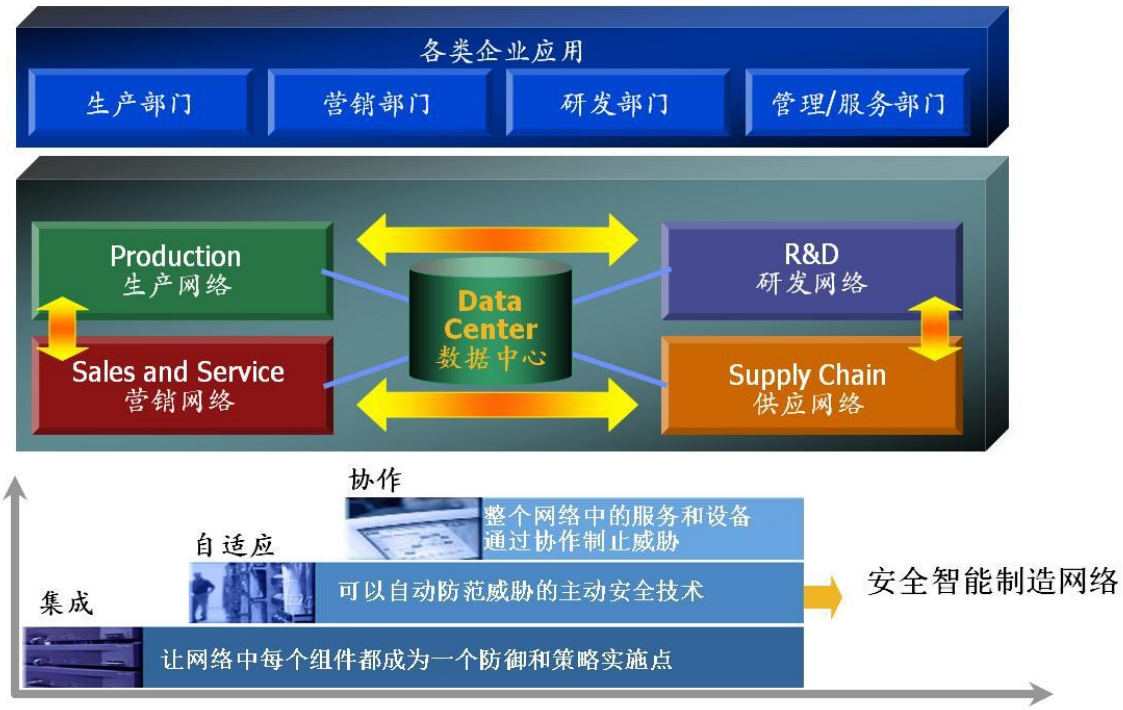
3.1 安全防护体系设计思想

从系统角度来看，网络安全不是一个简单的产品问题，网络安全首先是个系统问题。从技术角度而言，网络安全主要应考虑以下几个方面：

1. 设备安全——网络中应该重点保护的设备，设备出现安全问题时对整个网络的影响力，以及设备本身对安全攻击的抵抗和处理能力。
2. 身份鉴别与授权——身份包括鉴别和授权。鉴别回答了“你是谁”和“你在哪？”这两个问题，授权回答“你可以访问什么”。需要对身份机制谨慎部署，否则即便是最严谨的安全策略也有可能被避开。
3. 边界安全——边界安全涉及到防火墙种类的功能，决定网络的不同区域允许或拒绝何种业务，特别是在 Internet 和主干网或拨入网之间。
4. 数据的保密性和完整性——数据的保密性指的是确保只有获准能够阅读数据的实体以有效的形式阅读数据，而数据完整性指的是确保数据在传输过程中未被改动。
5. 安全监测——为检验安全基础设施的有效性，应经常进行定期的安全审查，包括新系统安装检查，发现恶意入侵行为，出现的特殊问题(拒绝业务攻击)以及对安全策略是否全面遵守等方面。
6. 策略管理——由于网络安全涉及到以上的多个方面，每一个方面都使用多种产品和技术，对这些产品进行集中有效的管理可以帮助网络管理者有效地部署和更新自己的安全策略。具有一个统一的安全策略对安全防范的实施非常有帮助，Cisco 在网络方面提出一个完整的安全解决方案。

3.2 思科制造业智能安全网络平台概述

下图描述了思科提出的制造业智能安全网络平台的整体架构：



在这个架构中，思科通过新一代的无边界网络安全解决方案，为制造业企业的生产网络、营销服务网络、研发网络、供应链网络以及企业数据中心等五大核心业务网络提供完善的安全防御保障机制。

3.3 基础网络平台的安全

3.3.1 网络基础设施的集成安全防护

思科网络自身安全解决方案，通过网络基础架构的主要组成部分－网络设备的安全保护，各自分工，系统协作，全面部署，从网络到主机，从核心层到分布层、接入层，我们要采取全面的企业安全策略来保护整个网络基础构架和其所连接的系统，即使当攻击，蠕虫和病毒发生时，思科的网络基础设施要具备相当的抵抗和承受能力，在自动适应“变化”的基础上，充分利用网络基础平台的优势，协助专门的安全系统，定位问题，提供数据，有效隔离，快速清楚，确保整体网络的稳定运行。

3.3.1.1 设备的安全访问权限

1. 用户口令的认证，可通过 Cisco 设备进行本地认证或 Radius、TACACS

2. 用户级别的划分，将可进入到设备的管理用户分为多个级别，对不同级别的用户具有不通的访问权限。
3. 设置 log 记录，对网络设备的任何有效配置和改动均需要相应的记录。

对于用户口令安全方面的考虑，建议采用集中管理的方式，在企业信息中心配置 CiscoSecure 访问控制器，所有设备的用户名、口令、权限控制都统一管理，避免因分散式管理带来的安全漏洞和管理的复杂性。

在用户的资格认证方面，有四种常用的认证方式，分别是：

1. 固定用户名/口令；
2. 时效用户名/口令；
3. 一次性口令；
4. 令牌卡/软令牌。

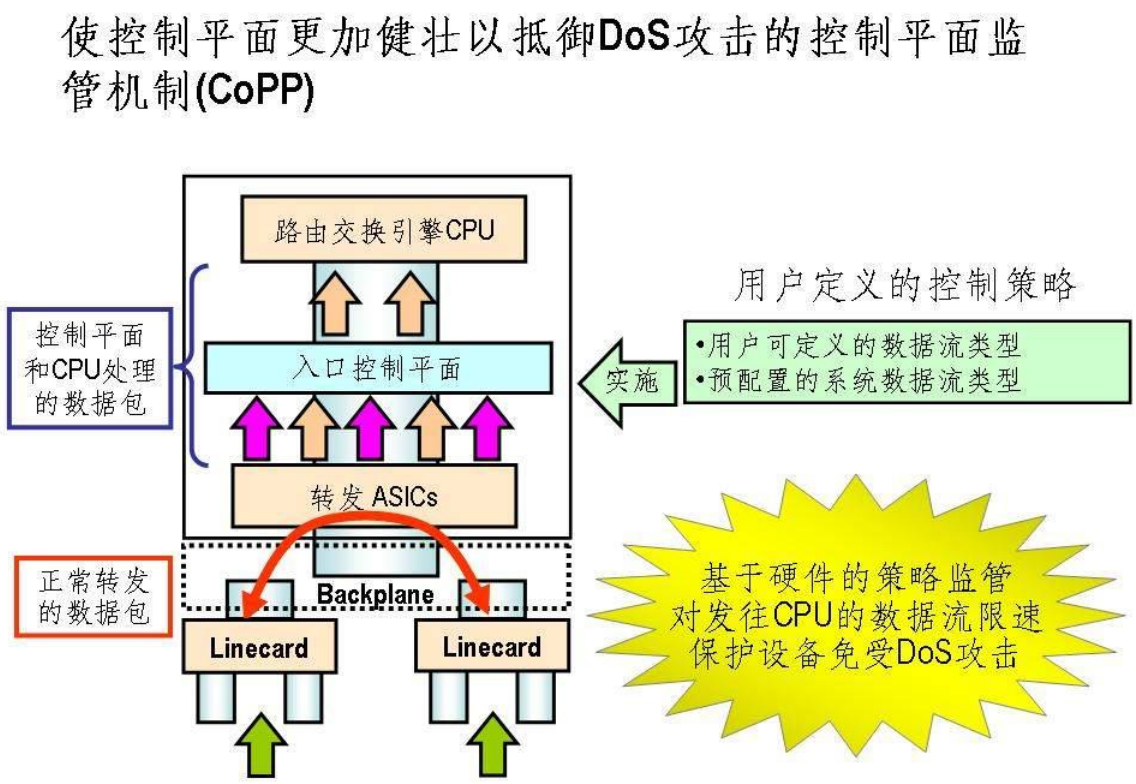
这四种方式中，在资格认证的可靠性方面，以第一种最低，第四种最高，在使用的方便性方面，则以第四种最低，第一种最高。可见安全和易用是一对矛盾体，要获得较高的安全性，就需要牺牲一些易于使用性。

大型制造企业启用 ERP 和 MES 系统后，对网络安全性的要求会更高，因此我们建议采用安全性较高的令牌卡或软令牌方式，对企业管理人员，特别是高级管理用户进行严格的资格认证，保证系统的安全性。

在资格认证上，为防止他人非法盗用、破坏口令，除采用高可靠性的令牌卡方式外，还可以设置拨入者在输入 N 次口令仍失败后帐户失效，并及时向系统管理员通知。

CiscoSecure ACS 同时支持 TACACS+和 RADIUS，为二者提供同等功能，客户可以自由选择。在本方案中，我们建议用户选择 TACACS+，它比 RADIUS 具有更好的安全性和伸缩性。

3.3.1.2 核心网络设备的控制平面监管



为了阻止伪装成特定类型的控制数据包直插网络心脏的类似威胁，Cisco IOS 软件在 Catalyst 6500 交换机上提供了可编程的监管功能，以限制目的地为控制层面处理器的流量的速度。这个名为“控制层面监管(CoPP)”的特性可用于识别特定类型的流量并对其进行完全或一定程度的限制，防止路由处理器 CPU 过载死机。

3.3.1.3 端口安全控制技术 Port Security

MAC 泛滥攻击的原理和危害

交换机主动学习客户端的 MAC 地址，并建立和维护端口和 MAC 地址的对应表以此建立交换路径，这个表就是通常我们所说的 CAM 表。CAM 表的大小是固定的，不同的交换机的 CAM 表大小不同。MAC/CAM 攻击是指利用工具产生欺骗 MAC，快速填满 CAM 表，交换机 CAM 表被填满。黑客发送大量带有随机源 MAC 地址的数据包，这些新 MAC 地址被交换机 CAM 学习，很快塞满 MAC 地址表，这时新目的 MAC 地址的数据包就会广播到交换机所有端口，交换机就像共享 HUB 一样工作，黑客

可以用 sniffer 工具监听所有端口的流量。此类攻击不仅造成安全性的破坏，同时大量的广播包降低了交换机的性能。

防范方法

限制单个端口所连接 MAC 地址的数目可以有效防止类似 macof 工具和 SQL 蠕虫病毒发起的攻击，macof 可被网络用户用来产生随机源 MAC 地址和随机目的 MAC 地址的数据包，可以在不到 10 秒的时间内填满交换机的 CAM 表。Cisco Catalyst 交换机的端口安全（Port Security）和动态端口安全功能可被用来阻止 MAC 泛滥攻击。例如交换机连接单台工作站的端口，可以限制所学 MAC 地址数为 1；连接 IP 电话和工作站的端口可限制所学 MAC 地址数为 3：IP 电话、工作站和 IP 电话内的交换机。

通过端口安全功能，网络管理员也可以静态设置每个端口所允许连接的合法 MAC 地址，实现设备级的安全授权。动态端口安全则设置端口允许合法 MAC 地址的数目，并以一定时间内所学习到的地址作为合法 MAC 地址。

通过配置 Port Security 可以控制：

- 端口上最大可以通过的 MAC 地址数量
- 端口上学习或通过哪些 MAC 地址
- 对于超过规定数量的 MAC 处理进行违背处理

端口上学习或通过哪些 MAC 地址，可以通过静态手工定义，也可以在交换机自动学习。交换机动态学习端口 MAC，直到指定的 MAC 地址数量，交换机关机后重新学习。目前较新的技术是 Sticky Port Security，交换机将学到的 mac 地址写到端口配置中，交换机重启后配置仍然存在。

对于超过规定数量的 MAC 处理进行处理一般有三种方式 ：

- Shutdown：端口关闭。
- Protect：丢弃非法流量，不报警。
- Restrict：丢弃非法流量，报警。

3.3.1.4 DHCP 窥探保护 DHCP Snooping

采用 DHCP server 可以自动为用户设置网络 IP 地址、掩码、网关、DNS、WINS 等网络参数，简化了用户网络设置，提高了管理效率。但在 DHCP 管理使用上也

存在着一些另网管人员比较问题，常见的有：

- DHCP server 的冒充。
- DHCP server 的 DOS 攻击。
- 有些用户随便指定地址，造成网络地址冲突。
- 由于 DHCP 的运作机制，通常服务器和客户端没有认证机制，如果网络上存在多台 DHCP 服务器将会给网络照成混乱。
- 由于不小心配置了 DHCP 服务器引起的网络混乱也非常常见。

黑客利用类似 Goobler 的工具可以发出大量带有不同源 MAC 地址的 DHCP 请求，直到 DHCP 服务器对应网段的所有地址被占用，此类攻击既可以造成 DOS 的破坏，也可和 DHCP 服务器欺诈结合将流量重指到意图进行流量截取的恶意节点。

DHCP 服务器欺诈可能是故意的，也可能是无意启动 DHCP 服务器功能，恶意用户发放错误的 IP 地址、DNS 服务器信息或默认网关信息，以此来实现流量的截取。

DHCP Snooping 技术

DHCP Snooping 技术是 DHCP 安全特性，通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息，这些信息是指来自不信任区域的 DHCP 信息。通过截取一个虚拟局域网内的 DHCP 信息，交换机可以在用户和 DHCP 服务器之间担任就像小型安全防火墙这样的角色，“DHCP 监听”功能基于动态地址分配建立了一个 DHCP 绑定表，并将该表存贮在交换机里。在没有 DHCP 的环境中，绑定条目可能被静态定义，每个 DHCP 绑定条目包含客户端地址（一个静态地址或者一个从 DHCP 服务器上获取的地址）、客户端 MAC 地址、端口、VLAN ID、租借时间、绑定类型（静态的或者动态的）。如下表所示：

```
CatHQ1#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN
Interface
------------------  ---------------  ----------  -------------  ----
----------------------
00:0D:60:2D:45:0D      10.149.3.13    600735    dhcp-snooping    100
```

```
GigabitEthernet1/0/7
```

这张表不仅解决了 DHCP 用户的 IP 和端口跟踪定位问题，为用户管理提供方便，而且还供给动态 ARP 检测 (DAI) 和 IP Source Guard 使用。

防范方法

为了防止这种类型的攻击，Catalyst DHCP 侦听 (DHCP Snooping) 功能可有效阻止此类攻击，当打开此功能，所有用户端口除非特别设置，被认为不可信任端口，不应该作出任何 DHCP 响应，因此欺诈 DHCP 响应包被交换机阻断，合法的 DHCP 服务器端口或上连端口应被设置为信任端口。

首先定义交换机上的信任端口和不信任端口，对于不信任端口的 DHCP 报文进行截获和嗅探，DROP 掉来自这些端口的非正常 DHCP 响应应报文。

3.3.1.5 IP 源地址保护技术 IP Source Guard

常见的欺骗攻击的种类和目的

黑客经常使用的另一手法是 IP 地址欺骗。常见的欺骗种类有 MAC 欺骗、IP 欺骗、IP/MAC 欺骗，其目的一般为伪造身份或者获取针对 IP/MAC 的特权。此方法也被广泛用作 DOS 攻击，目前较多的攻击是：Ping Of Death、Syn flood、ICMP Unreacheable Storm。如黑客冒用 A 地址对 B 地址发出大量的 ping 包，所有 ping 应答都会返回到 B 地址，通过这种方式来实施拒绝服务 (DoS) 攻击，这样可以掩盖攻击系统的真实身份。富有侵略性的 TCP SYN 洪泛攻击来源于一个欺骗性的 IP 地址，它是利用 TCP 三次握手会话对服务器进行颠覆的又一种攻击方式。一个 IP 地址欺骗攻击者可以通过手动修改地址或者运行一个实施地址欺骗的程序来假冒一个合法地址。

另外病毒和木马的攻击也会使用欺骗的源 IP 地址。互联网上的蠕虫病毒也往往利用欺骗技术来掩盖它们真实的源头主机。

防范方法

Catalyst IP 源地址保护 (IP Source Guard) 功能打开后，可以根据 DHCP 侦听记录的 IP 绑定表动态产生 PVACL，强制来自此端口流量的源地址符合 DHCP 绑定表的记录，这样攻击者就无法通过假定一个合法用户的 IP 地址来实施攻击了，这个功能将只允许对拥有合法源地址的数据保进行转发，合法源地址是与

IP 地址绑定表保持一致的，它也是来源于 DHCP Snooping 绑定表。因此，DHCP Snooping 功能对于这个功能的动态实现也是必不可少的，对于那些没有用到 DHCP 的网络环境来说，该绑定表也可以静态配置。

IP Source Guard 不但可以配置成对 IP 地址的过滤也可以配置成对 MAC 地址的过滤，这样，就只有 IP 地址和 MAC 地址都于 DHCP Snooping 绑定表匹配的通信包才能够被允许传输。此时，必须将 IP 源地址保护 IP Source Guard 与端口安全 Port Security 功能共同使用，并且需要 DHCP 服务器支持 Option 82 时，才可以抵御 IP 地址＋MAC 地址的欺骗。

3.3.1.6 基于网络的应用识别定位病毒 NBAR

当攻击，蠕虫和病毒发生时，网络基础设施具备相当的抵抗和承受能力，不管是设备级还是网络级，再协助与专门的安全系统，定位问题，确认攻击源，有效隔离，快速响应，确保整体网络的稳定运行和业务的持续发展。

我们只要能够通过各种网络技术定位传播源，过滤传播扫描数据包，限制被感染终端的接入，同样也会大大增强整个网络的抵抗能力

基于网络的应用识别 (NBAR) 是 Cisco IOS® 软件中的分类引擎，可以通过 URL/多目的互联网邮件扩展 (MIME) 类型和使用动态端口分配技术的协议识别多种应用级协议，包括 HTTP。NBAR 对流量进行分类之后，可以将相应的服务质量 (QoS) 策略应用到流量等级。NBAR 能识别 CRv1 和 CRv2 URL 请求，但不能识别 Code-Red 红色代码 II URL 请求，因为 Code-Red 红色代码 II 通过多个分组传播 GET 请求，而 NBAR 目前只检查第一个分组。与 NIDS 不同，NBAR 可以立即对 CRv1 和 CRv2 流量进行分类，并在流量到达服务器之前丢弃分组。另外，NBAR 还可以双向使用，减轻 Code-Red 红色代码的危害。

3.3.2 安全域隔离与网络出口

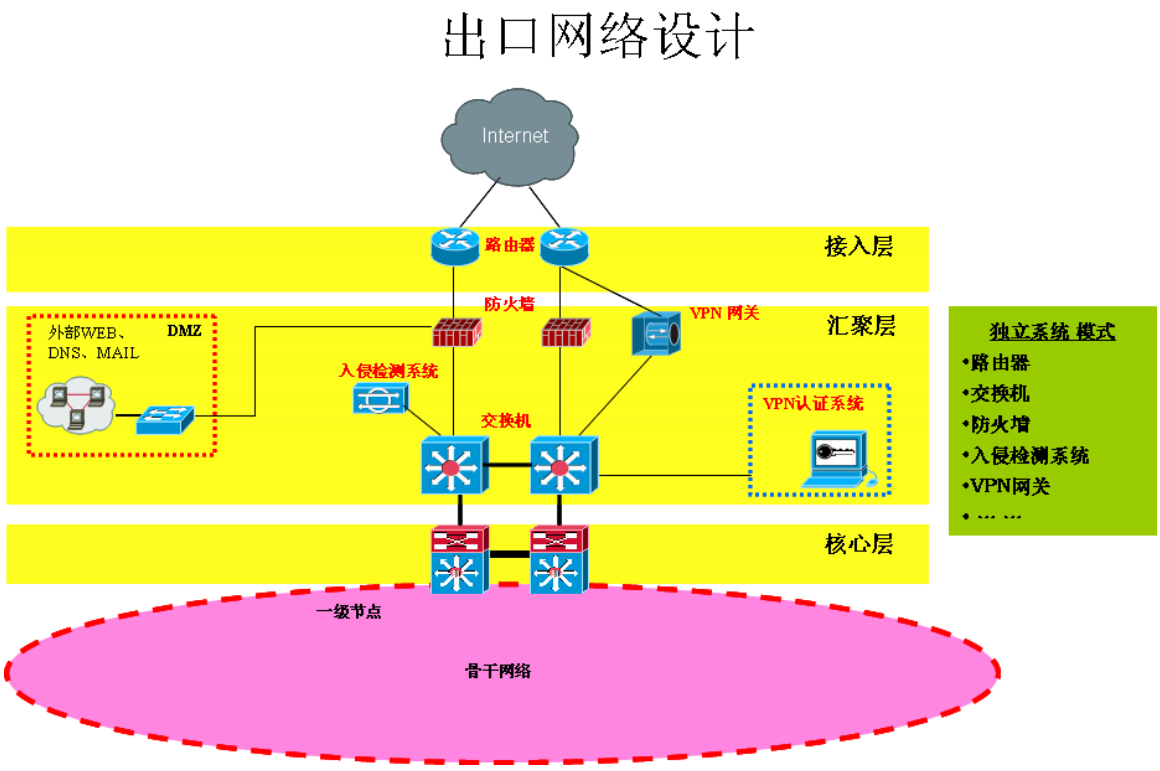
随着企业生产技术的不断改进和生产规模的不断扩大，企业内部的应用也越来越多，部门的分工也越来越细。与之相对应，企业的基础网络平台也必然存在不同的功能模块与区域。不同的安全域之间，不同业务部门、应用系统之间存在着权限区分、安全隔离等需求。为此，我们需要在 IT 平台建设的初始阶段就充

分考虑上述的安全需求。

思科 Catalyst6500 交换机支持可扩展的硬件防火墙模块 FWSM。采用思科 FWSM，当应用系统增加时，业务部门变更时，只需要在 FWSM 上进行资源的分配和划分，就能使系统得到安全域的隔离保护，而无需增加硬件设备、无需变更布线。FWSM 带来最大的灵活性、扩展性，并节省投资成本。

另一方面，制造业网络需要与互联网/相关外部网络连接，网络安全是主要的考虑要素。需要部署防火墙和入侵检测系统，进行安全控制和管理，入侵检测系统对非法入侵进行检测和报告。如下图所示：

选项一、采用独立系统的出口网络设计



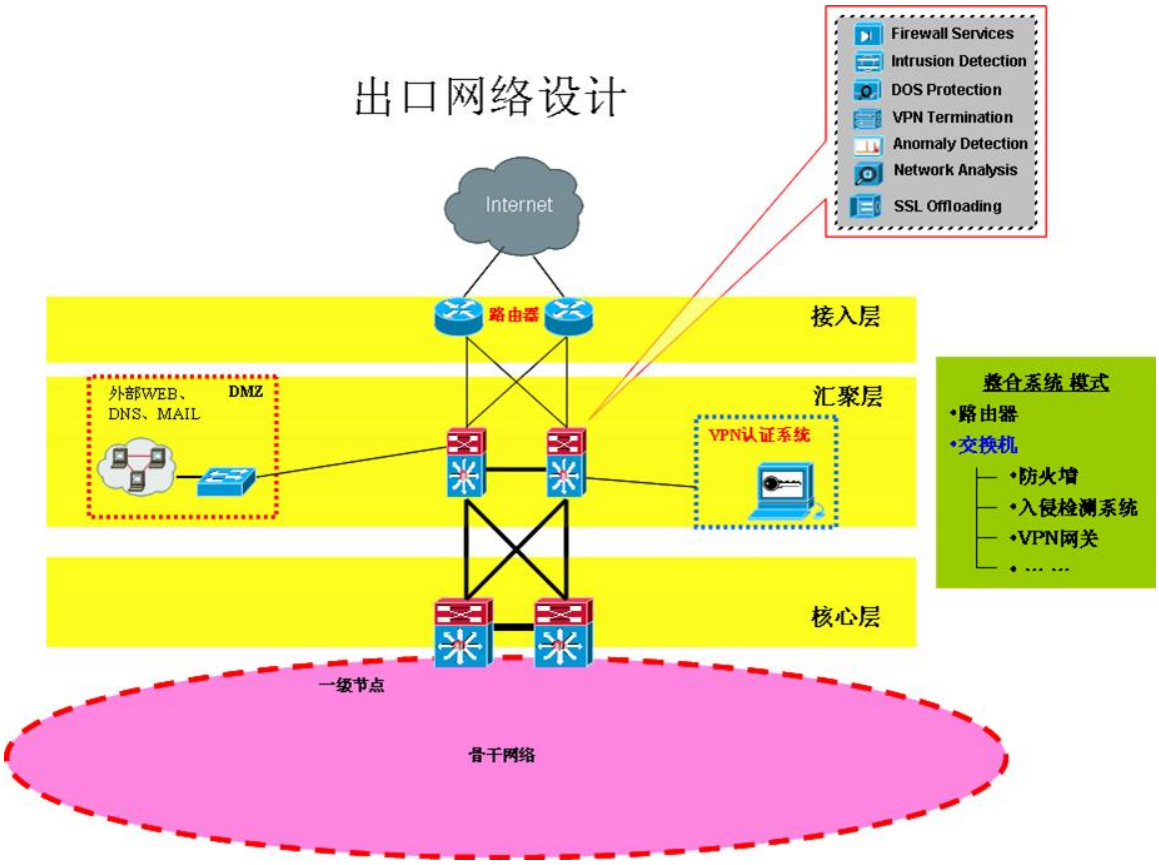
如上图所示，

路由器、交换机、各类安全产品集成在一起，实现网络出口功能。但由此带来网络结构复杂，同时由于不同的系统和设备功能和性能的差异，很容易形成网络瓶颈，影响业务使用效果。

为避免不同功能的设备出现单点故障，一般采取双机冗余配置，不可避免导致技术集成难度加大，对网络管理维护的难度也随之提高。

因此，我们建议在企业网络中一般采用以下整合的出口网络设计。

选项二、采用整合系统的出口网络设计



思科 Catalyst6500 交换机提供了一个高性能的综合业务交换平台，集成了各类安全服务模块：

- 思科 Catalyst 6500 防火墙系统（FWSM）服务模块
- 思科 Catalyst 6500 系列入侵检测系统（IDSM-2）服务模块
- 思科 Catalyst 6500 系列网络分析（NAM）服务模块
- 思科 Catalyst 6500 系列网络异常检测（ADSM）服务模块
- 思科 Catalyst 6500 系列网络异常防护（AGSM）服务模块
- 思科 Catalyst 6500 系列 Web VPN 服务模块
- 思科 Catalyst 6500 系列 IPSec VPN 服务 SPA 模块

同时兼具 Catalyst 6500 交换机的高可靠性、高性能的技术优势，能够满足客户最全面的安全技术需求，简化了网络结构的复杂度，并提供更优的设备兼容性和更高效简单的综合管理。

3.3.3 思科 Netflow 技术

今天的企业越来越多地把关键业务应用、语音、视频等新型应用融合到 IP 网络上，一个安全、可靠的网络是企业业务成功的关键。而企业网络的内部和外部的界限越来越模糊，用户的移动性越来越强，过去我们认为是安全的内部局域网已经潜伏着威胁。我们很难保证病毒不会被带入我们的企业网络，而局域网的广泛分布和高速连接，也使其很可能成为蠕虫快速泛滥的温床。

实践证明思科 Catalyst 6500 系列交换机通过硬件提供的 Netflow 功能可以有效阻止病毒和蠕虫的泛滥。

首先我们要了解蠕虫的异常行为，并有手段来尽早发现其异常行为。发现可疑行为后要能很快定位其来源，即跟踪到其源 IP 地址、MAC 地址、登录用户名、所连接的交换机和端口号等等。要搜集到证据并作出判断，如果确是蠕虫病毒，就要及时做出响应的动作，例如关闭端口，对被感染机器进行处理。但是我们知道，接入交换机遍布于每个配线间，为企业的桌面系统提供边缘接入，由于成本和管理的原因，我们不可能在每个接入层交换机旁都放置一台 IDS 设备。如果是在汇聚层或核心层中部署 IDS，对于汇聚了成百上千个百兆/千兆以太网流量的汇聚层或核心层来说，工作在第 7 层的软件实现的 IDS 无法处理海量的数据，所以不加选择地对所有流量都进行监控是不实际的。

Netflow 技术是集成在 Cisco IOS 软件里的一个智能 IP 服务，它能收集和测量路由器或交换机接口的数据流量。通过分析 Netflow 数据，网络工程师可以判断网络拥塞的原因、确定用户和应用的服务级别、了解网络流量状况等等。因为 Netflow 是 Cisco IOS 的一部分，所以不需要购买外置的探测设备就可以进行 IP 流量分析——这对于我们的园区或大楼局域网是非常经济的流量分析工具。

首先分析一下怎么才能实现快速、可扩展、经济有效地监测蠕虫病毒的目标：

1. 发现可疑流量。 我们利用 Cisco Netflow 所采集和输出的网络流量的统计信息，可以发现单个主机发出超出正常数量的连接请求，这种不正常的大数量流量往往是蠕虫爆发或网络滥用的迹象。因为蠕虫的特性就是在发作时会扫描大量随机 IP 地址来寻找可能的目标，会产生大量的 TCP 或

ICMP 流。流记录里其实没有数据包的载荷（payload）信息。这是 Netflow 和传统 IDS 的一个重要区别，一个流记录里不包含高层信息，这样的好处则是可以高速地以硬件方式处理，适合于繁忙的高速局域网环境。通常部署在核心层和汇聚层的 Catalyst 6500 交换机都支持基于硬件的 Netflow。Netflow 不对数据包做出深层分析，但是已经有足够的信息来发现可疑流量，而且不受“0 日”的局限。如果分析和利用得当，Netflow 记录非常适用于早期的蠕虫或其他网络滥用行为的检测。了解流量模式的基线非常重要。例如，一个用户同时有 50-100 个活动的连接是正常的，但是如果一个用户发起大量的（例如 1000 个）活动的流就是非正常的了。

2. 追踪可疑的源头。识别出可疑流量后，同样重要的是追踪到源头（包括物理位置和用户 ID）。在今天的移动环境中，用户可以在整个园区网中随意漫游，仅仅知道源 IP 地址是很难快速定位用户的。而且我们还要防止 IP 地址假冒，否则检测出的源 IP 地址无助于我们追查可疑源头。另外我们不仅要定位到连接的端口，还要定位登录的用户名。
3. 搜集可疑流量。一旦可疑流量被监测到，我们需要捕获这些数据包来判断这个不正常的流量到底是不是发生了新的蠕虫攻击。正如上面所述，Netflow 并不对数据包做深层分析，我们需要网络分析工具或入侵检测设备来做进一步的判断。但是，如何能方便快捷地捕获可疑流量并导向网络分析工具呢？速度是很重要的，否则你就错过了把蠕虫扼杀在早期的机会。除了要很快定位可疑设备的物理位置，还要有手段能尽快搜集到证据。我们不可能在每个接入交换机旁放置网络分析或入侵检测设备，也不可能在发现可疑流量时扛着分析仪跑去配线间。

Netflow 技术能对 IP/MPLS 网络的通信流量进行详细的行为模式分析和计量，并提供网络运行的准确统计数据，这些功能都是企业在进行网络安全管理时实现异常通信流量检测和参数定性分析所必需的。

IP 网络中的数据流（Flow）信息

为对企业网络中的异常流量进行检测，首先需要对网络中不同类型业务的正

常通信进行基线分析，包括测量和统计不同业务日常的流量和流向数据并计算基线的合理范围。

为完成上述对不同类型业务的测量工作，首先需要对网络中传输的各种类型数据包进行区分。由于 IP 网络的非面向连接特性，网络中不同类型业务的通信可能是任意一台终端设备向另一台终端设备发送的一组 IP 数据包，这组数据包实际上就构成了企业网络中某种业务的一个数据流（Flow）。如果管理系统能对全网传送的所有 Flow 进行区分，准确记录每个 Flow 的传送时间、占用的网络端口、传送源/目的地址和数据流的大小，就可以对企业全网所有通信的流量和流向进行分析和统计，进而计算出正常通信的基线以及发现突发的异常通信流量。

通过分析网络中不同 Flow 间的差别，可以发现判断任何两个 IP 数据包是否属于同一个 Flow 实际上可以通过分析 IP 数据包的下属 7 个属性来实现，即数据包的：

- 源 IP 地址
- 目标 IP 地址
- 源通信端口号
- 目标通信端口号
- 第三层协议类型
- TOS 字节（DSCP）
- 网络设备输入（或输出）的逻辑网络端口（ifIndex）

思科公司的 Netflow 技术就是利用分析 IP 数据包的上述 7 个属性，可以快速区分网络中传送的各种不同类型业务的 Flow。对区分出的每个数据流 Netflow 可以进行单独地跟踪和准确计量，记录其传送方向和目的地等流向特性，统计其起始和结束时间，服务类型，包含的数据包数量和字节数量等流量信息。对采集到的数据流流量和流向信息，Netflow 可以定期输出原始记录，也可以对原始记录进行自动汇聚后输出统计结果。

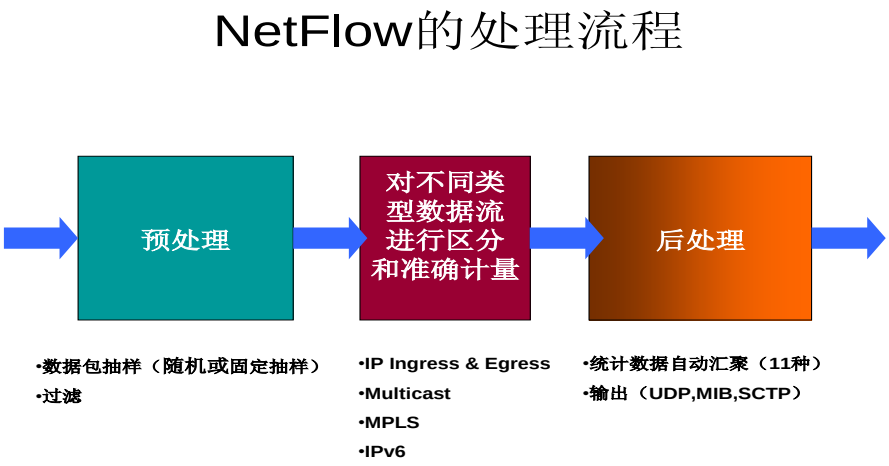
Netflow 的处理机制

从发明之初思科公司的 Netflow 技术就已完全融入了 IOS 操作系统中。由于 Netflow 技术支持几乎所有类型的网络端口类型，所以每台内置有 Netflow 功能的思科网络设备都可以作为网络中一台能够测量、采集和输出网络流量和流向管

理信息的实时数据采集器。而且因为 Netflow 实现的管理功能是由网络设备本身完成的，所以企业无需购买额外的硬件设备，也无需为安装这些硬件设备占用宝贵的网络端口或改变网络链路的连接关系。这些都将转化成对网络运营成本的大幅度降低，对企业级的大型网络优势尤其明显。

同时作为一种网络通信的宏观分析工具，Netflow 技术并不分析网络中每一个数据包中包含的具体信息，只是对传送的数据流的特性进行检测，这就确保了 Netflow 技术具有极大的规模可扩展性：支持高速网络端口和大型的企业网络。

为进一步提高 Netflow 技术对网络流量/流向信息进行采集和统计的效率和灵活性，Netflow 还引进了多级的处理流程，如下图所示：



在预处理阶段，Netflow 可以首先根据网络管理的需要对特定级别的数据流进行过滤或对高速网络端口进行数据包抽样，这样可以在确保需要的管理信息被采集和统计的同时，减少网络设备的处理负荷，增加全系统的可扩展性。

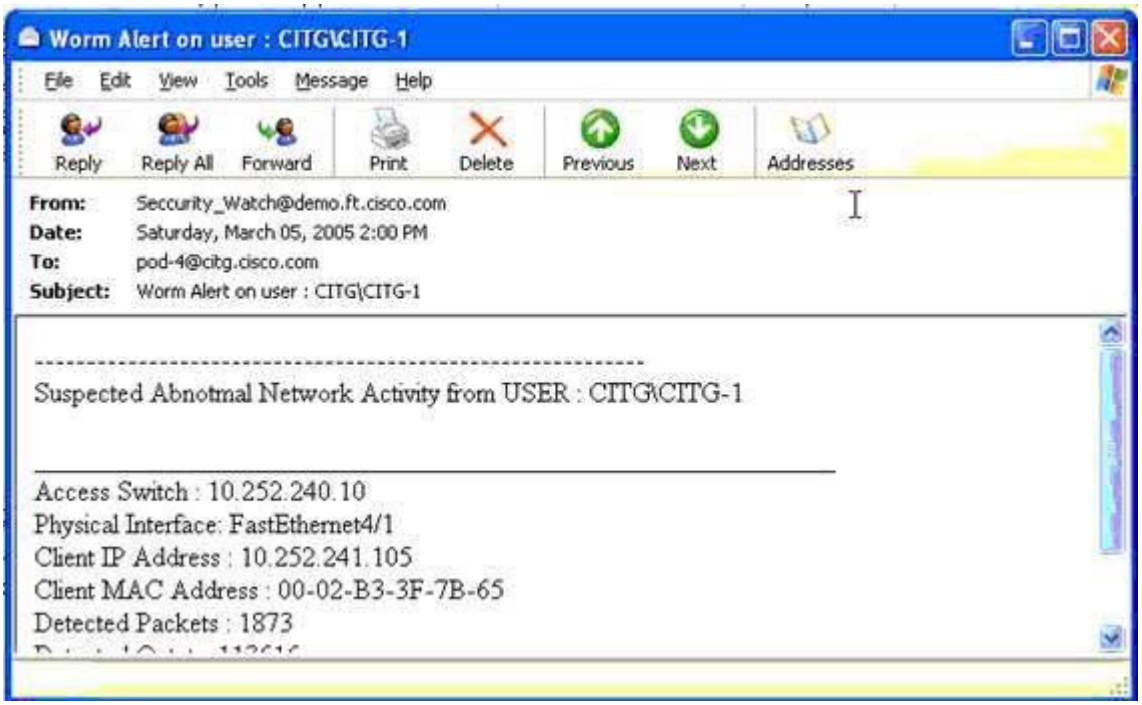
在后处理阶段，Netflow 可以选择把采集到的数据流原始统计信息全部输出，由上层管理服务器统一接收后再进行数据的分类处理和汇总；也可以选择由网络设备自身对原始统计信息进行多种形式的数据汇聚，只把汇总后的统计结果发送给上层管理服务器。由网络设备进行原始统计信息的汇聚可以大大减少网络设备输出的数据量，降低对上层管理服务器的配置要求，提高上层管理系统的扩展性和工作效率。

Netflow 支持同时向两个管理服务器地址输出采集到的网络流量和流向统计信息，输出数据的方式有三种：

- 简单高效 UDP 传输协议方式（传统方式）。但由于采用了 UDP 协议，数据传输的可靠性是不保证的。
- SNMP MIB 方式。管理服务器可以通过 SNMP 协议访问网络设备 Netflow MIB 库中存储的数据流 Top N 统计结果。
- 可靠的 SCTP 传输协议方式。利用 SCTP 传输协议，支持拥塞识别，重传和排队机制，确保 Netflow 统计结果数据正确发送给上层管理服务器。

有了上面的分析，下面介绍如何利用 Catalyst 的功能来满足这些需要：

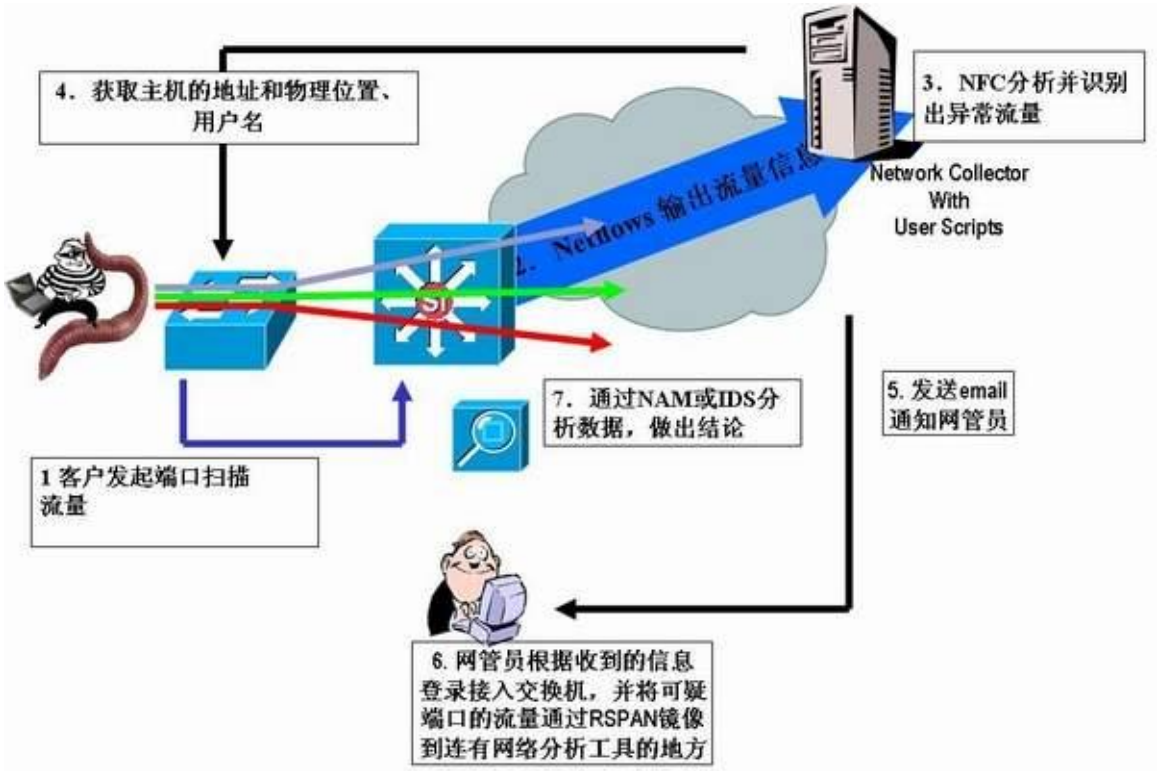
1. 检测可疑流量:Cat6500 提供了基于硬件的 Netflow 功能，采集流经网络的流量信息。这些信息采集和统计都通过硬件 ASCI 完成，所以对系统性能没有影响并且不需增加投资。
2. 追踪可疑源头:Catalyst 集成的安全特性提供了基于身份的网络服务（IBNS），以及 DHCP 监听、源 IP 防护、和动态 ARP 检测等功能。这些功能提供了用户的 IP 地址和 MAC 地址、物理端口的绑定信息，同时防范 IP 地址假冒。这点非常重要，如果不能防范 IP 地址假冒，那么 Netflow 搜集到的信息就没有意义了。 用户一旦登录网络，就可获得这些信息。结合 ACS，还可以定位用户登录的用户名。在 Netflow 收集器（Netflow Collector）上编写一个脚本文件，当发现可疑流量时，就能以 email 的方式，把相关信息发送给网络管理员，下图是一个例子：



我们可以看到，在通知 email 里，报告了有不正常网络活动的用户 CITG，所属组是 CITG-1（这是 802.1x 登录所用的）。接入层交换机的 IP 地址是 10.252.240.10，物理接口是 FastEthernet4/1，另外还有客户端 IP 地址和 MAC 地址 ，以及其在 5 分钟内（这个时间是脚本所定义的）发出的 flow 和 packet 数量。

掌握了这些信息后，网管员就可以马上采取以下行动：

1. 通过远程 SPAN 捕获可疑流量。Catalyst 交换机上所支持的远程端口镜像功能可以将流量捕获镜像到一个远程交换机上，例如将接入层交换机上某个端口或 VLAN 的流量穿过中继镜像到汇聚层或核心层的某个端口，只需非常简单的几条命令即可完成。流量被捕获到网络分析或入侵检测设备（例如 Cat6500 集成的网络分析模块 NAM 或 IDS 模块），作进一步的分析和做出相应的动作。对于一个有经验的网管员来说，在蠕虫发生的 5 分钟内就能完成，而且他不需要离开他的座位。如下图所示：



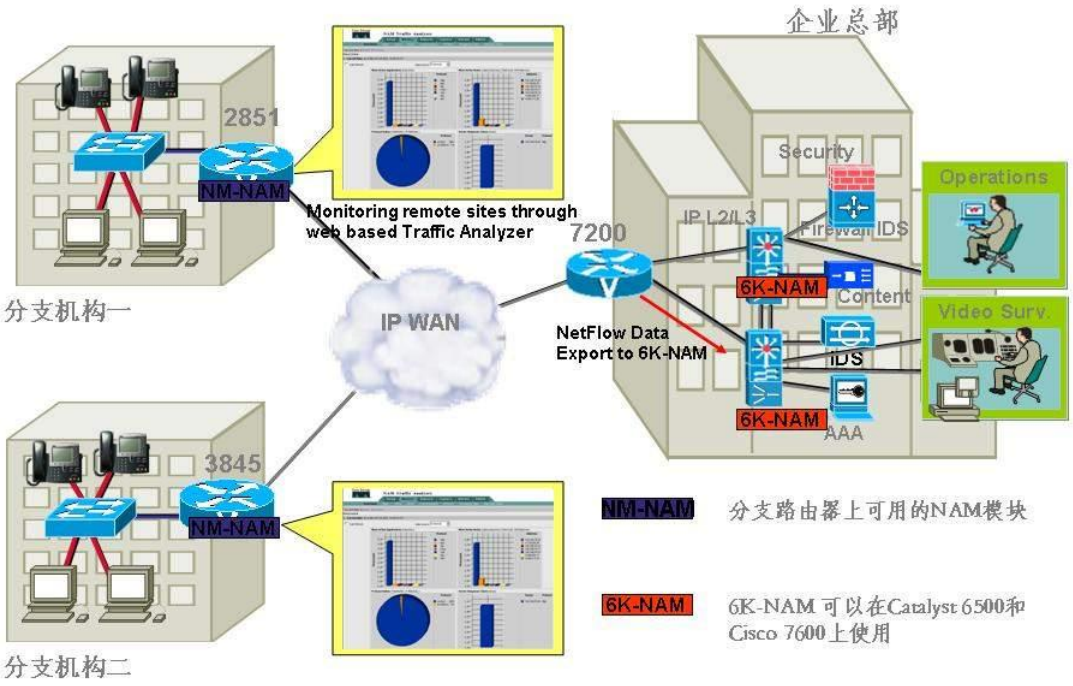
Netflow 解决方案结合了 Catalyst 交换机上集成的多种安全特性功能，从扩展的 802.1x，到 DHCP 监听、动态 ARP 检测、源 IP 防护和 Netflow。这些安全特性的综合使用，为我们提供了一个在企业局域网上有效防范蠕虫攻击的解决方案，这个方案不需更多额外投资，因为利用的是集成在 Catalyst 上的 IOS 中的功能特性，也带给我们一个思考：如何利用网络来保护网络？这些用户在选择交换机时可能忽略的特性，会带给用户意想不到的行之有效的安全解决方案！

3.3.4 思科网络分析模块系统

过去，局域网交换机虽然已提高了网络性能，但仍旧阻碍了网络管理员对交换流量进行监控。远程监控（RMON）在共享网络上最有效果，在那里，它可以看到所有流量。LAN 交换机需要有力的监控，因为它们会过滤信息流量，以便这些信息只出现在与其发送设备和目的地设备相连的端口上。这种对不同网段的网络活动“不断提高的可视性”要求，使管理员很难调整网络性能，而且它也给交换网络中的纠错带来了不便。

基于此原因，思科推出了针对 Catalyst 6500 交换机系列的、带网络分析模块（NAM）和全套交换机探针系统，以及中低端路由器和 ISR 上的网络分析模块的集成化解决方案，可满足交换以太网 LAN 和 WAN 中多服务网络管理和监控的需要。基于路由器的网络分析模块支持以下思科路由器：Cisco 2600XM/2691/2800/3660 /3700/3800。部署了思科 Catalyst 6500 交换机和 Cisco ISR 的企业都可以应用 NAM 模块来帮助管理人员对自己网络中的流量了如指掌。这一点非常非常有助于提升大型制造企业网络整体的安全性。

思科NAM在企业局域网和广域网中的统一部署



NAM 工作机制

NAM 根据 RMON 和 RMON－2 管理信息库（MIB）提供远程监控功能，在所有层收集数据，以便网络管理员可获得实用分析，同于故障隔离和纠正、容量规划和管理、性能管理、应用监控以及调试。

NAM 是 Cisco 端到端网络管理和监控解决方案的一部分。NAM 是 Cisco 集成化语音、视频和数据体系结构（AVVID）的一个元件，在 Cisco LAN 网络中定义了强大的多服务交换。随着企业部署融合网络，管理员也需收集有关应用或视频

应用的统计数据。NAM 收集一直传输至应用层的数据和语音流的多层信息，有助于简化管理当今复杂多服务交换 LAN 的任务，这种 LAN 支持各种数据、语音和视频应用，其中包括 H.323 系列。

功能支持

NAM 已包括全面监控所需的所有特性集。NAM 可从数据和语音流收集统计信息，简化整体管理并降低开支成本。它使用交换端口分析器（SPAN）或远程 SPAN（RSPAN）来接收来自物理端口、虚拟 LAN（VLAN）、以太通道和 Netflow 数据输出帧的数据。它同时监控多个交换机端口或 VLAN，为每个数据源提供独立 RMON/RMON2 统计数据。NAM 为每个 VLAN 保持一套专用的 RMON 和 RMON2 MLB 组数据表。

NAM 使用简单网络管理协议（SNMP）将所收集的统计数据上载至基于图形化用户界面（GUI）的流量管理应用，如 Cisco TrafficDirector 等。NAM 与所有符合 IETF RFC 的 RMON/RMON－2 网络管理软件完全兼容。它提供了与管理应用间的可靠通信，即便是模块因 CPU 过载或缓存过度运行而丢弃了分组，其性能也不会受到影响。

NAM 在监督器模块发生故障、备用监控器接替时将每个数据源与新信息相对比，从而实现 Catalyst 6500 平台的弹性体系结构。NAM 假定数据源仍有效且所有正在进行的收集未丢失也未遭破坏。

NAM 支持的 MIB 组

NAM 为以下 MIB 收集数据：RMON1，RMON2，交换监控（SMON）、HC－RMON、MIB－Ⅱ系统组和 MIB－Ⅱ接口组，且支持 RFC 2074。

NAM 支持以下 RMON 组：微型 RMON、完全 RMON 和完全 RMON2。

网络接口

NAM 无网络接口。所监控的分组经由 SPAN 或远程 SPAN（RSPAN）功能传送到线路模块。这映射了 NAM 上的所有交换机端口或 VLAN，提供七层监控和强大的详细纠错功能。NAM 支持对多个端口或 VLAN 的同时监控，并为每个数据源维持

独立组统计数据。支持可经由 SPAN 或 RSPAN 功能引导至 NAM 的所有类型的数据源（物理端口、VLAN、以太通道和 Netflow 数据输出帧），用于 RMON 数据收集。

VLAN 监控

NAM 在一条中继链路上为每条 Cisco 交换机间链路或 IEEE 802.1Q VLAN 提供了独立的 RMON/RMON2 统计数据。有两种类型的监控：由 VLAN id 索引的分组和八位统计数据，以及 VLAN 代理。

由 VLAN id 索引的分组和八位统计数据提供了众多信息，如哪些 VLAN 正在数据源上使用以及每个在用 VLAN 上的实际流量数目等。

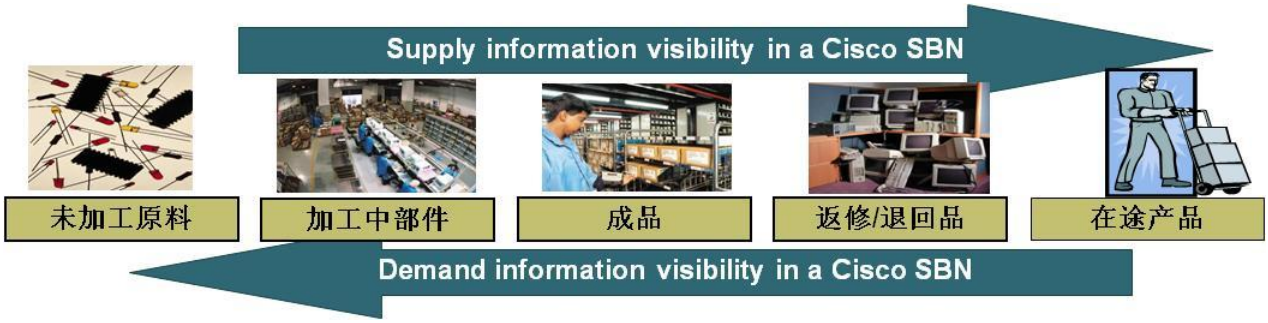
VLAN 代理将特定 VLAN 上的流量用作针对所需 RMON 收集的数据源。VLAN 代理随后会进一步进行分析，允许用户为每个感兴趣的 VLAN 上的流量安装所需 RMON/RMON2 组。例如，可能会有网络层主机和参数表监控 VLAN2 上的流量，而同时监控 VLAN3 上的网络层主机和应用层主机表，并在 VLAN4 上执行分组获取。

网络流数据输出监控

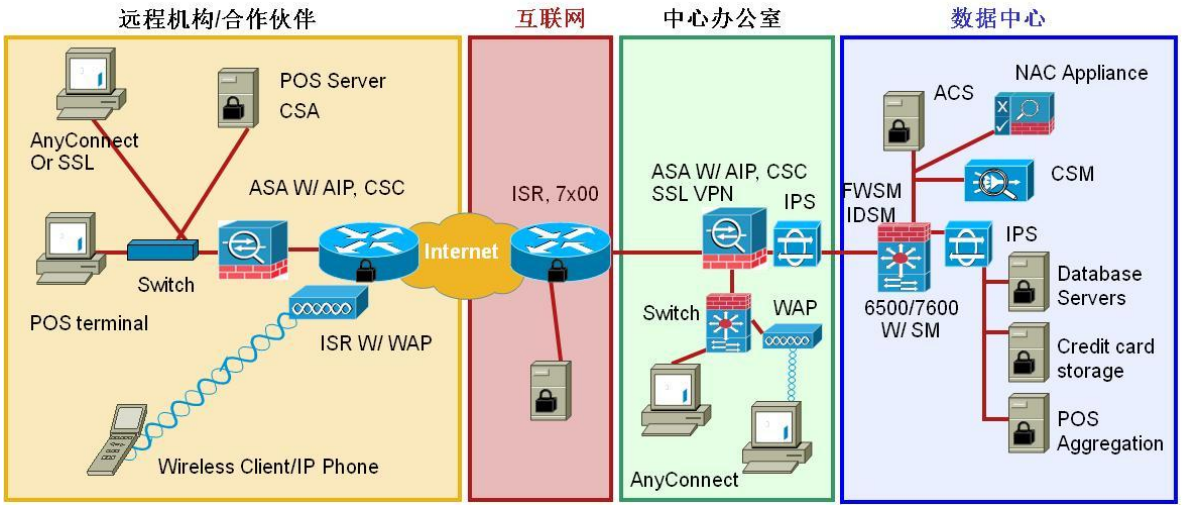
Catalyst 6500 交换机可进行配置，生成网络流数据输出（NDE）帧，以在流建立和结束时报告基于流的统计数据。NAM 上的 RMON 软件可使用这些分组来传播 RMON－2 主机和参数表。每个 NDE 分组包含一套针对特定流的记录集。Catalyst 6500 交换机中有两个 NED 分组来源，第一个是针对新网络流或当前未高速缓存在监督器传送硬件中的流的软件源。另一个是在流结束时的监督器传送硬件本身。这两个 NDE 分组源均与 NAM 一起工作。

3.4 制造业供应链网络的安全

供应链网络是生产企业最为重要的业务网络系统，它全面覆盖了原材料供应、产品制造、渠道销售、综合服务支持、最终用户等方方面面。如何保证整条链路的安全是制造业企业需要考虑的核心安全问题。在思科无边界网络安全的架构下，供应链中的需求信息与供应信息是两大核心信息，企业必须随时掌握供求关系的数据，并且确保这些数据的真实性和可信性。



思科认为，在一个需求驱动的供应链安全模型中，应该包括以下几个核心环节，如图所示：



3.4.1 企业与远程机构/合作伙伴的安全互联

生产企业有众多的原材料供应商和合作伙伴，另一方面，企业为顺应生产快速发展的需求，也设立了众多的远程分支机构。如何保障企业与合作伙伴、分支机构、供应商之间的安全高效互联，同时又能有效降低 IT 运维的投入？

此外，移动办公应用也是日趋普遍的行业应用，公司安全管理员必须提供背景感知（包括用户角色、环境等 ）的安全和策略实施，无论最终用户身在任何地点、使用何种设备以及访问的信息存于何处。管理员还必须能够支持各种类型的笔记本电脑和移动设备，以让他们的客户（即最终用户）有更多的选择余地。最后，他们还需要不显著地提供安全保护，以最大程度方便最终用户的使用。

思科 AnyConnect Secure Mobility 解决方案是当今市场上最成熟、最安全的企业移动解决方案，它将思科行业领先的安全技术和下一代智能远程访问技术结合在一起，为移动用户提供智能、持续、易用、安全的连接体验，使其能轻松

利用移动设备(包括笔记本电脑和手持设备)安全地访问工作所需的应用程序和信息 ；移动用户回到公司后仍能享受到持续的网络连接，IT 管理员则可实现智能的、背景感知的安全策略来保护公司资产， 让企业轻松管理无边界网络的安全风险。

Cisco AnyConnect Secure Mobility 方案组件如图 1。在头端使用 Cisco ASA 5500 系列 Adaptive Security Appliance 的 Cisco AnyConnect 版本 2.5 提供远程连接部分。用户和设备必须经过身份验证后,才能获得访问网络的权限。一旦用户通过身份验证， Cisco AnyConnect Secure Mobility 解决方案就可以决定用户可访问哪些应用程序和资 源。理想状态下,此身份验证对用户透明。对于需要进行验证的设备而言,则必须符合 公司策略且具有最新的安全性。

Cisco IronPort® S- 系列 Web Security Appliance 应用背景感知策略,包括为所有用户 实施可接受的用途,并提供针对恶意软件的保护。Web Security Appliance 也接受来自 AnyConnec 客户端的用户身份验证信息,为用户访问其 Web 内容提供自动身份验证步骤。

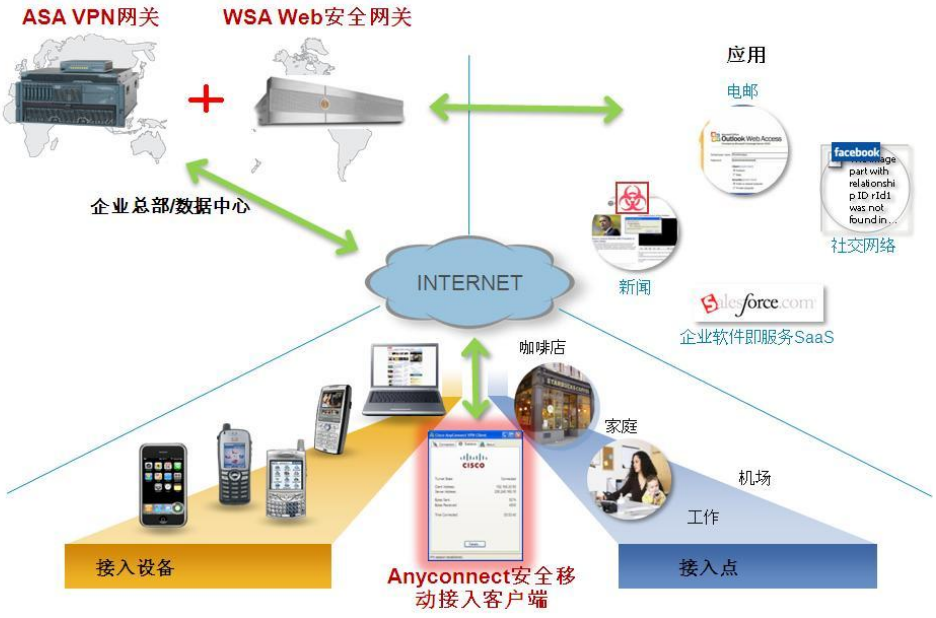


图 1. 思科 AnyConnect Secure Mobility 解决方案一览

总的来说，思科 AnyConnect Secure Mobility 解决方案能够为制造业提供如下功能和优势，

- 远程信息安全访问：建立思科 SSL VPN 远程统一安全资源访问平台

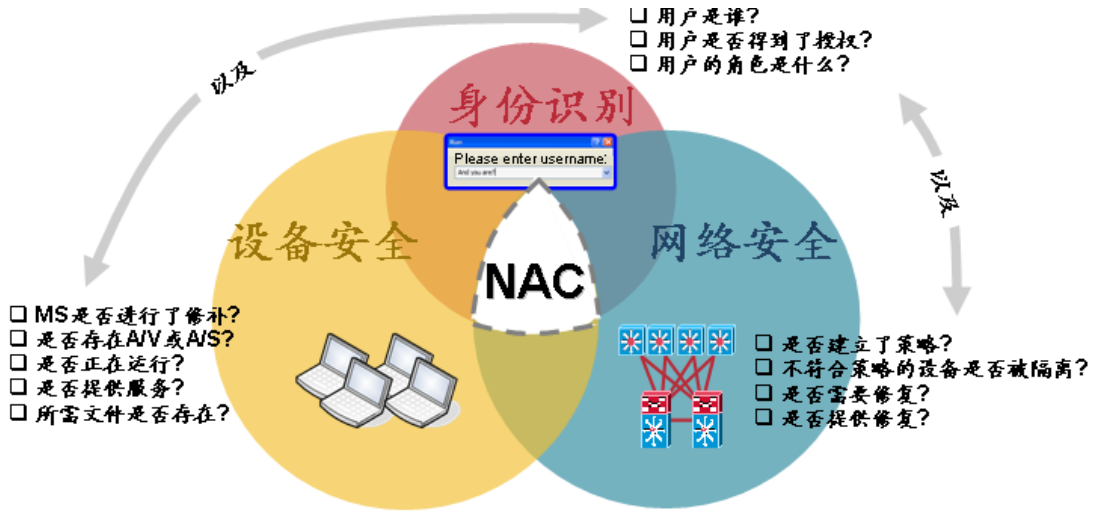
- 解决资源对外开放和安全性的矛盾
- 基于身份、接入设备和位置的资源访问控制，保护敏感数据和业务
- 虚拟桌面，强大的终端安全检测
- 多平台支持，包括 Iphone/Windows Mobile 手机平台
- 高可靠性，扩展能力强，内置负载均衡

3.4.2 终端的访问控制和网络准入技术

生产企业的网络中存在着大量开放的终端系统。在现在的信息技术框架里，终端已广义的涵盖了所有客户终端（包括工作站或 PC）、提供服务的服务器及其上的操作系统、数据库和应用，是各种业务的承载体和表现实体。对于用户业务来讲，终端是基础的承载平台，所有应用、数据都驻留在主机上，因此终端的安全是用户业务安全的最后堡垒，也是最重要的一环！

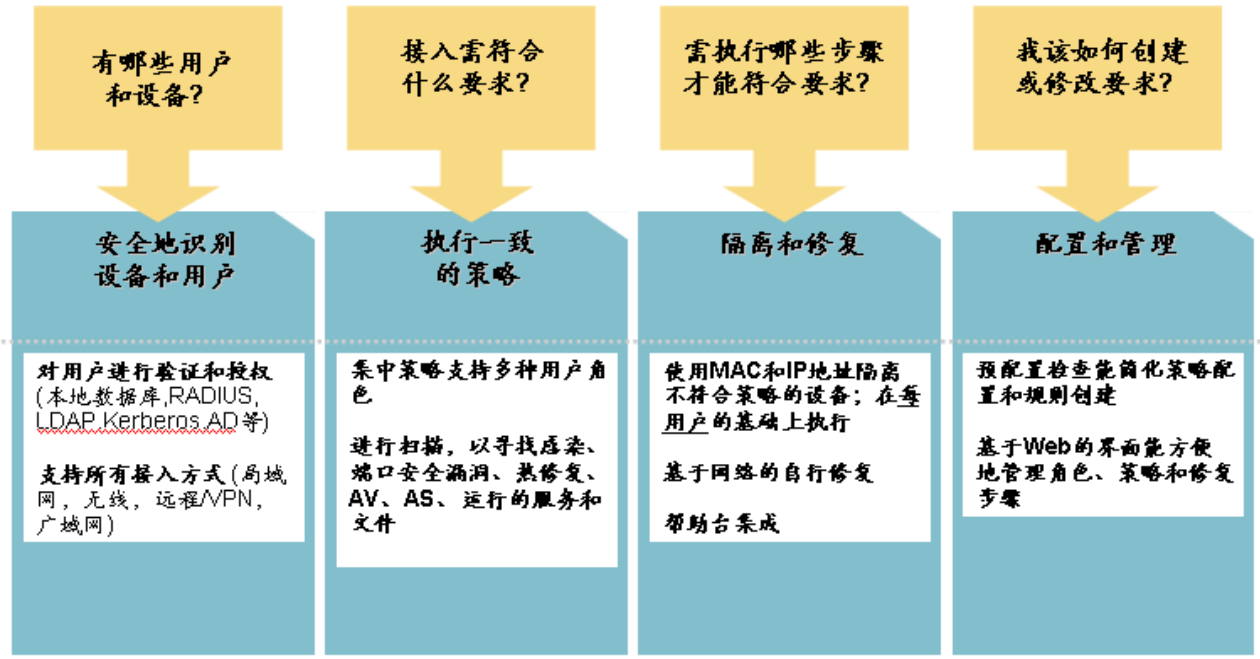
对于企业的终端安全防护，我们需要解决两个问题：传统使用的基于特征码的防护软件不能有效防御新的安全威胁，防病毒软件在蠕虫刚开始传播的过程中是无法提供保护的，要改变的被动局面，必须采用新的技术解决当前 zero-day 攻击威胁；在复杂环境里仅有单一的防御方式是不充分的，单一的防护手段存在着覆盖不到的薄弱点，需要层次化、多样性的安全防护策略，并且各种防护措施之间需要能够很好的配合协作。

为此，思科提出了一个把设备安全、身份识别、网络安全有机结合的准入控制（NAC）解决方案。



思科 NAC 设备是一个端到端网络注册和策略执行解决方案，使网络管理员能在允许用户进入网络前，对用户及其机器进行验证、授权、评估和修补。这款先进的网络安全产品能够：

- 确认用户、用户设备和他们在网络中的角色。这是在验证时实施的第一步，此时恶意代码还无法造成破坏。
- 评估机器是否符合安全策略。安全策略可根据用户类型、设备类型或操作系统的不同而不同。
- 通过阻止、隔离和修复不符合安全策略的机器，来执行安全策略。机器被重导向到一个隔离区，在管理员的指导下进行修补。



实施思科 NAC 设备的网络能够：

- 因将安全策略符合性作为接入网络的先决条件，实现了健康网络状态
- 主动防御病毒、蠕虫、间谍软件和其他恶意应用
- 通过定期评估和修补，最大限度地减少了用户机器上的安全漏洞
- 能自动修复和更新用户机器，大幅节约了成本

思科网络准入控制（NAC）的主要功能及优势体现为：

适用于多种网络环境

- Lan 客户端
- VPN 客户端
- 无线客户端
- 支持 Windows Active Directory 域的单一登录

能检测设备多种状态，确保机器符合安全策略要求：

- 检测 MS 是否进行了修补
- 检测是否安装了防病毒软件/防间谍软件
- 是否存在安全防护软件
- 是否指定的安全防护软件正在运行?
- 是否提供服务
- 所需文件是否存在

对用户进行身份验证，不同角色不同授权

- 用户必须为合法授权用户
- 可设置多种角色，如访客，员工，涉密员工等
- 提供 WEB 登录、Agent 登录，不同角色可定制不同登录方式，
- 用户按照不同角色进行授权

支持多种验证形式

可实施本地验证，也能作为验证代理，与Kerberos、LDAP、RADIUS、Active Directory、S/Ident等集成。

能对各种接入终端进行检测，包括多种操作系统、机器及非PC联网设备：

- Windows
- Mac OS
- Linux 操作系统
- IP 电话
- PDA、
- 游戏控制台
- 打印机

设备安全隔离

- 能将不符合策略的机器隔离，防止感染传播
- 使用小至/30 的子网或隔离 VLAN
- 隔离的机器依然能授权访问修补资源，如进行补丁升级

Step-by-step 修补和维修指导

- 提供多种方式让不符合安全策略的设备进行修复
- 可自动推送升级链接和文件
- 提供 Step-by-step 指导用户进行修复操作

灵活的部署模式

- 适合异构网络设备环境：思科、非思科环境
- 任何设备接入前强制进行用户及设备安全状态认证
- 无需预先部署客户端软件
- 准入控制设备可中央部署或边缘部署
- 提供第二层或第三层客户端接入

- 可带内或带外处理网络流量
- 高可靠性保证，支持 HA 功能

集中管理

- 支持分布式部署，集中控制管理
- 基于安全 Web 的管理控制台管理
- 能为每个角色定义所需的扫描类型
- 为每个策略提供恢复时所需的相关修补产品包

3.4.3 端到端的无线安全架构

当前，无线局域网在工业生产中有着非常广泛的应用，例如利用 WIFI 对生产线信息进行实时采集和传送、通过 RFID 标签对企业资产进行定位和跟踪等等。

由于无线信号的空间泄漏特性，以及 802.11 技术的普及，随之而来的无线网络安全问题也被广大用户普遍关注。如何在保证 802.11WLAN 的高带宽，便利访问的同时，增加强有力的安全特性？业界的厂商纷纷研究发展了 802.11 技术，增强了无线局域网安全的各个方面，并促成了诸如 802.1x/EAP，802.11i，WPA/WPA2 等标准的诞生，以及后续标准（如 802.11w）的制定。

Cisco 在无线局域网安全技术和标准制定方面，扮演了极为重要的角色，是 802.1x/EAP 无线环境应用的最早支持厂商，并在无线安全标准工作组中占据领导地位。

与其他网络一样，WLAN 的安全性主要集中于访问控制和隐私保护。健全的 WLAN 访问控制－－也被称为身份验证－－可以防止未经授权的用户通过接入点收发信息。严格的 WLAN 访问控制措施有助于确保合法的客户端基站只与可靠的接入点－－而不是恶意的或者未经授权的接入点－－建立联系。

WLAN 隐私保护有助于确保只有预定的接收者才能了解所传输的数据。在数据通过一个只供数据的预定接收者使用的密钥进行加密时，所传输的 WLAN 数据的隐私才视为得到了妥善保护。数据加密有助于确保数据在收发传输过程中不会遭到破坏。

但是，无线局域网的安全并不仅仅局限于接入认证和数据加密。无线接入

设备 AP 的物理安全性，AP 连接到有线网络交换机的安全认证，基于无线访问位置的物理防护手段，如何避免攻击，如何快速发现非法/假冒 AP，对一个网络系统来讲也是十分重要的。

同时，随着最新的无线安全技术的发展，新的 802.11w 标准也被提上了议事日程，802.11w 是对无线信号的管理帧进行安全管理的一种标准，思科已经在无线网络接入点和控制器以及 CCX 的计划上支持了 MFP。

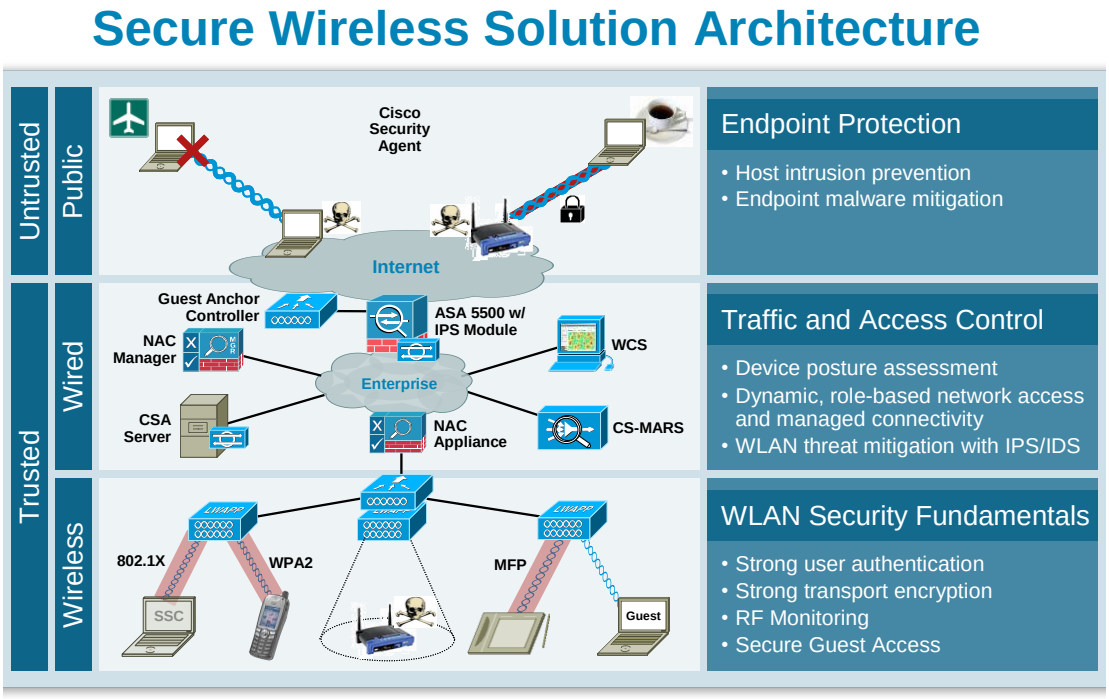
在部署 Mesh 网络的时候，由于所有信令和数据的传输都是通过 802.11a 的 Backhaul 进行回传，那么对于 11a 上的数据加密也是我们需要关心的安全问题。

思科无线网络的解决方案支持高效、多级别、多种类、多级的认证方式和加密技术，具体如下：

- 无线终端用户的用户认证（用户名/密码，数字证书）
- 无线终端用户的数据加密（WEP，TKIP，AES）
- 无线接入点的接入认证
- 无线控制帧的安全管理（MFP）
- 基于 2-7 层内容的入侵检测系统（无线 IPS、IDS 系统）
- 支持精确的非法 AP 定位和隔离
- 射频干扰的检测和辨别
- 终端的安全接入保证（NAC）
- Mesh 回传链路数据的安全加密
- 终端快速、安全漫游机制的实现（CCKM）
- 独特的访客隔离机制，保证跨地区漫游用户与无线网内部用户的隔离。将访客和无线网络完全逻辑隔离，在允许访客跨地区无线网络漫游访问互联网的同时保证内部无线用户的安全
- 网络的安全管理

所以，思科提供了基于有线无线集成的统一的端到端的安全架构，系统构

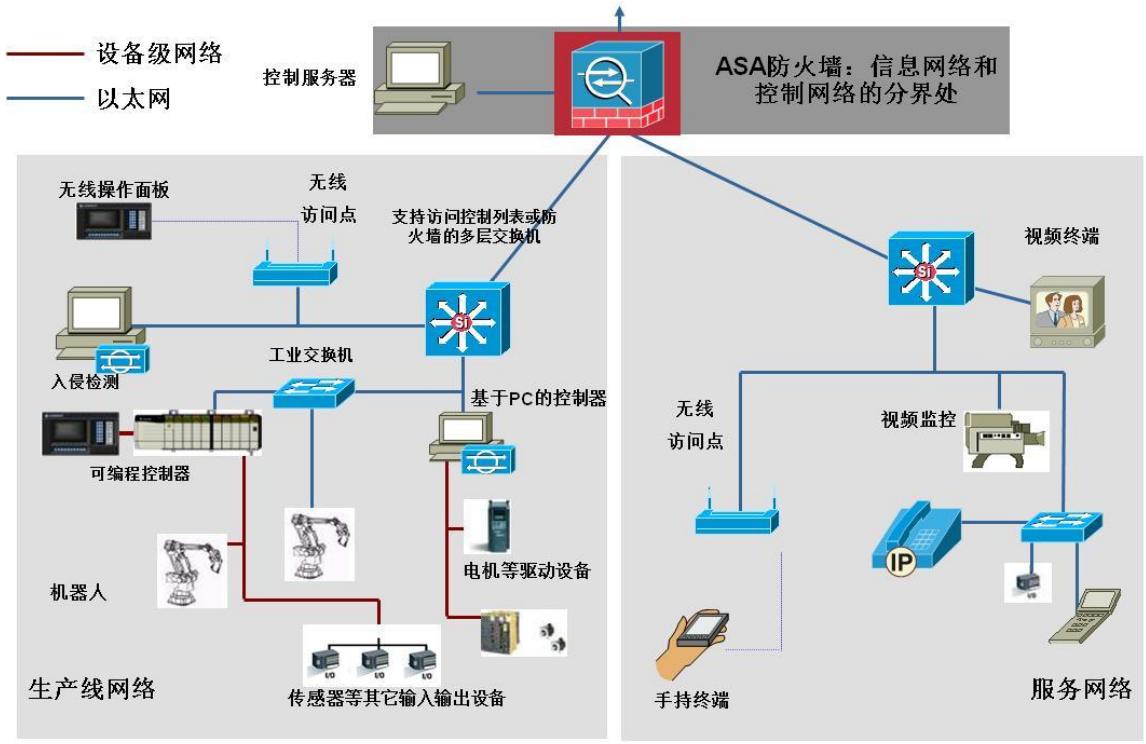
架如下



3.5 工业以太网的安全

当前，随着 IP 网络技术的发展，传统的工业自动化网络正逐步迁移到使用统一标准的工业以太网（ETTF）平台上。

下图描述了一个典型的基于以太网的车间生产网络。



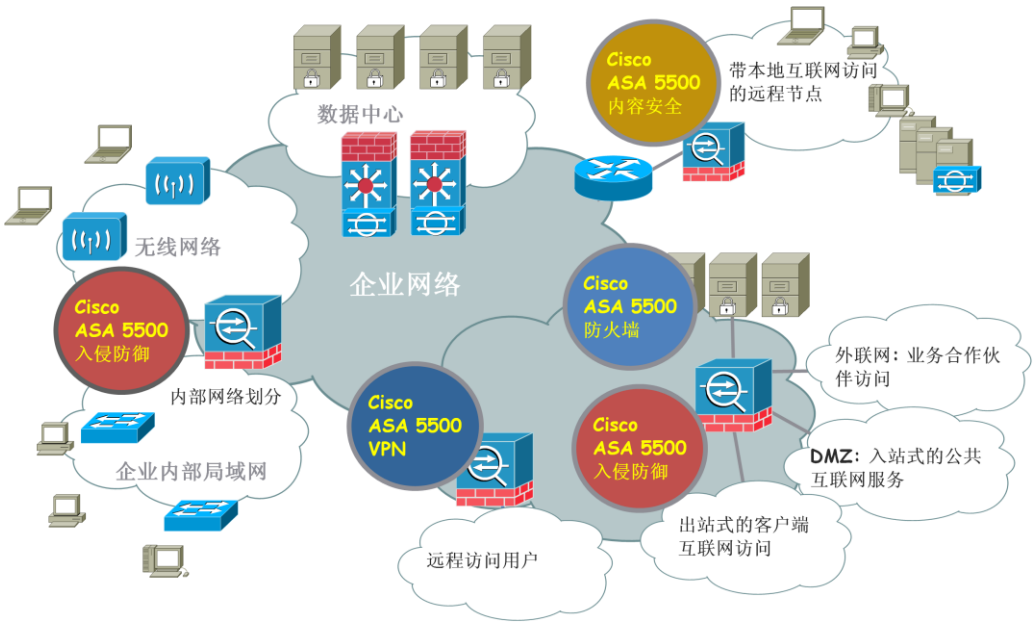
对于生产企业来说，车间生产网络的安全直接关系到企业的产品质量、生产效率、生产经营成本等关乎企业生存发展的核心环节。

对于车间生产网络的安全设计，我们建议对以下几个关键点进行着重的考虑：

3.5.1 信息网络和控制网络的安全分隔

通过部署思科 ASA5500 系列自适应安全设备对工业以太网中的信息网络和控制网络进行安全分隔。利用 ASA 系列，生产部门与企业数据中心之间能够安全传送相关的生产信息，同时也提供了完善的安全通道让生产线工程师能够方便的对生产流程进行远程监视和修定。

Cisco ASA 5500 系列提供了一个易于使用且符合工业以太网安全需求的一体化解决方案。它结合了防火墙隔离、入侵保护、Anti-X 和 VPN 功能，能够为企业的生产网络提供完善的安全防护。通过终止垃圾邮件、间谍软件和其他互联网威胁，员工生产率得到了提高。IT 人员也从处理病毒和间谍软件消除以及系统清洁任务中解放出来。企业可集中精力发展业务，而无需为最新病毒和威胁担忧。



3.5.2 工业以太网交换机的安全

思科工业以太网交换机 Industrial Ethernet 3000 (IE3000)系列交换机是一个全新的交换机系列，提供了坚固、易用、安全的交换基础设施，适用于恶劣环境。Cisco IE3000 系列采用了工业设计，符合工业规范；其工具简化了工业网络的部署、管理和更换；且在开放标准的基础上提供了很好的网络安全性。Cisco IE3000 是支持工业以太网应用的理想产品，这其中包括工厂自动化、智能交通运输系统(ITS)、变电站和其他恶劣环境中的部署。

IE3000 交换机提供了完善的工业以太网安全特性：

- 带 VLAN 分配功能、访客 VLAN 和语音 VLAN 的 IEEE 802.1x 支持基于端口的动态安全性，提供用户身份验证。
- 用于第二层接口、基于端口的 ACL 能在各交换机端口上应用安全策略。

- MAC 地址过滤能通过一个匹配 MAC 地址来防止转发任意类型的数据包。
- SSHv2 和 SNMPv3 能够通过在 Telnet 和 SNMP 会话中加密管理员流量来提供网络安全。由于美国出口法律的限制，SSHv2 和 SNMPv3 的加密版本需要一种特殊的加密软件镜像。
- TACACS+和 RADIUS 身份验证能对交换机进行集中控制，并防止未经授权的用户更改配置。
- MAC 地址通知使管理员能在网络添加或者删除用户时获得通知。.
- DHCP 监听使管理员能确保 IP 到 MAC 地址的一致镜像。这能用于防止企图破坏 DHCP 捆绑数据库的攻击，并对进入交换机端口的 DHCP 流量进行限速。
- DHCP 接口跟踪程序(option 82)在主机 IP 地址请求中增加了交换机端口 ID。
- 端口安全性可根据 MAC 地址，保护对某个接入或者汇聚端口的访问权限。
- 在一段特定的时间之后，老化功能会将 MAC 地址从交换机中删除，以便让另外一个设备连接到同一个端口。
- 可信边界能在具有 IP 电话时信任 QoS 优先级设置，并在 IP 电话拆除后禁用信任设置，由此防止恶意用户篡改网络中的优先级划分策略。
- 支持多达 512 个 ACL，有两种类别：安全性(384 个安全 ACL 项和 128 个 QoS 策略)，以及 QoS (128 个安全 ACL 项和 384 个 QoS 策略)。

3.5.3 无线网络的安全

参考上文关于端到端无线安全架构的描述。

3.6 制造业营销服务网络的安全

企业的营销服务网络属于客户交互型网络，销售/服务人员通过各种方式与企业客户进行多样化的沟通，例如：语音、电子邮件、基于 WEB 方式的即时通讯等，藉此维系企业的核心客户关系并对之进行有效的管理。营销服务网络的交互性决定了它的运作必须依赖于开放的公众互联网平台，也决定了它必然要面对日新月异的互联网安全威胁和当前日益严峻的互联网安全形势。

当前，基于互联网 Web 数据流传播的各种安全威胁，开始在全球范围盛行，使商用网络暴露在这些威胁带来的内在危险之下。现行的网关防御机制已经证明不足以抵御多种基于 Web 的恶意软件入侵。据业内估计，大约 75%的商用电脑感染了间谍软件，但是在网络周边部署了恶意软件防御系统的企业却不足 10%。基于 Web 的恶意软件传播速度快，变种能力强，其危害性日益严重，对企业的营销服务网络来说，拥有一个强健的能够保护网络周边并抵御这些安全威胁侵害的安全平台就显得极为重要。

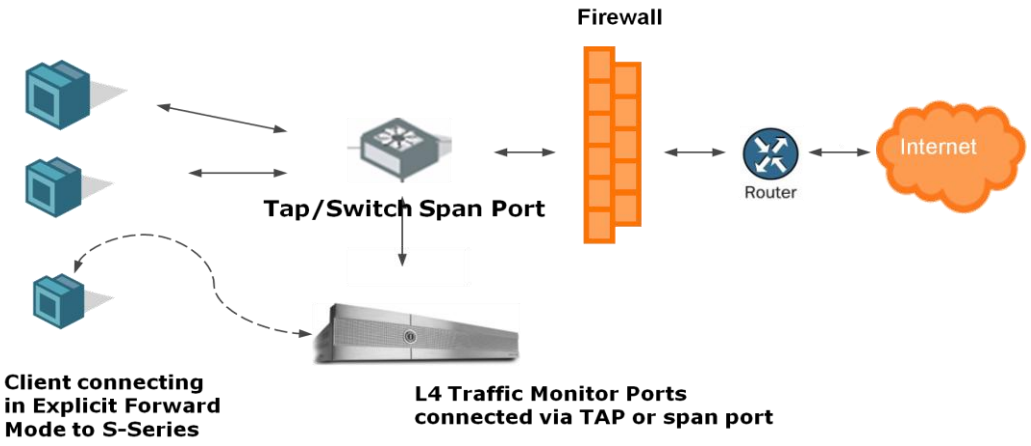
除此以外，当今基于 Web 的威胁 87％是通过合法的网站发出的。基于 Web 的恶意软件有着速度快、多样性强和变种频繁出现的攻击威胁特点，这要求企业必须使用一个强大的、安全平台才能将日益严峻的上网威胁屏蔽在企业网络之外。

Cisco® IronPort S 系列 Web 安全网关是业界开创先河的，也是唯一的将传统的 URL 过滤、信誉过滤和恶意软件过滤功能集中到单一平台来消除上述风险的 Web 安全设备。通过综合利用这些创新的技术，Csico IronPort S 系列网关能够帮助企业在保证 Web 数据流安全和控制 Web 数据流风险方面，应对所面临的日益严峻的挑战。

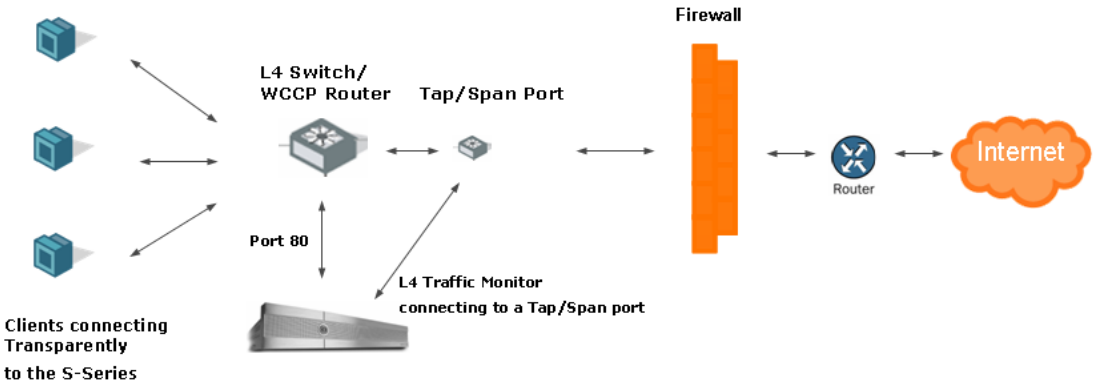
Cisco IronPort S 系列网关结合了多种先进技术，通过单台、集成的网关抵御恶意软件，帮助企业实施安全策略及控制网络流量。提供的多层防护包括 Cisco IronPort Web 名誉过滤器™，多层防恶意软件扫描引擎和第四层(L4)数据流监视器，它可以监控非 80 端口的恶意软件活动。所有这一切为企业提供了一个强大的具有最优性能和功效的 Web 安全平台。同时 Cisco IronPort S 系列提供智能化的 HTTPS 解密的能力，从而对加密数据流应用所有的安全及访问策略。

在实际的应用环境中，企业可以选择以下两种模式部署 S 系列网关

- 直连模式：客户机直接连接到 S 系列，由 S 系列提供 HTTP/HTTPS/FTP 流量的代理支持。



- 透明模式：由第四层交换机或 WCCP 路由器转发流量至 S 系列，由 S 系列提供对客户机透明的代理支持。



部署 Cisco IronPort C 系列电子邮件安全网关应对来自互联网电子邮件的安全威胁

垃圾邮件以及随邮件传播的病毒、恶意程序、间谍软件等是当前来自互联网的另一种主要的安全威胁。对于有大量电子邮件应用的企业营销服务网络来说，这种威胁往往会带来极大的安全风险：随意打开来历不明的电子邮件或者点击邮件中的附件或链接都有可能形成对业务系统的攻击。此外，网络管理人员需要耗费大量精力用于清理垃圾邮件，也严重影响了对正常业务系统的管理和维护。因此，如何对电子邮件应用进行高效的安全防御和管理，也是当前企业部署安全解决方案时需要重点考虑的内容。

Cisco IronPort C 系列电子邮件安全网关是针对电子邮件安全威胁的最佳解决方案。基于 Cisco IronPort 专有的为企业目标设定的 AsyncOS™操作系统，

IronPort C 系列能够满足对电子邮件的大容量和高可用性的扫描需求，减少与垃圾邮件、病毒和其他各种威胁相关的系统宕机时间，从而支持对企业邮件系统的高效管理并有效减轻网络管理人员的工作负担。

IronPort C 系列在一个网关设备上集成了思科独有的预防性过滤器和基于特征码的反应性过滤器，配合内容过滤和高级加密技术，为客户提供了目前业界最高级的邮件安全服务。同时，利用思科安全情报运营中心和全球威胁协作组织使 Cisco IronPort 网关产品更聪明，更迅速。这一先进技术使企业可以从最新的互联网威胁中提高他们的安全性，并且使得保护用户更加透明化。

下图描述了 C 系列邮件安全网关的部署方式：

3.7 研发网络的安全－保护企业的核心机密信息

制造业企业的产品研发数据是企业的核心机密信息，是企业核心竞争力的最集中的体现。数据丢失、泄露将直接导致企业的竞争力下降、信誉受损、失去客户信任等严重后果。

针对企业核心机密信息的保护，思科提出了名为 DLP（Data Loss Prevention）的多层次战略解决方案，旨在为企业提供全方位的机密数据、敏感信息的保护。

DLP 解决方案包括以下几个核心组件：

- 部署 Cisco IronPort C 系列电子邮件安全网关提供邮件保护，监视和阻断包含敏感、机密信息的邮件；
- 部署 Cisco Ironport S 系列 Web 安全网关，通过 Web 信誉过滤防止员工访问恶意的/被感染的网站，通过流量扫描防止被感染的 PC 向外发送敏感信息。
- 通过终端保护和准入控制，防止未授权或带有安全风险的终端设备接入网络，防止机密数据通过 USB、光盘、打印等方式从终端泄露。

详细的产品信息请参阅上文关于 IronPort 和 NAC 解决方案的描述。

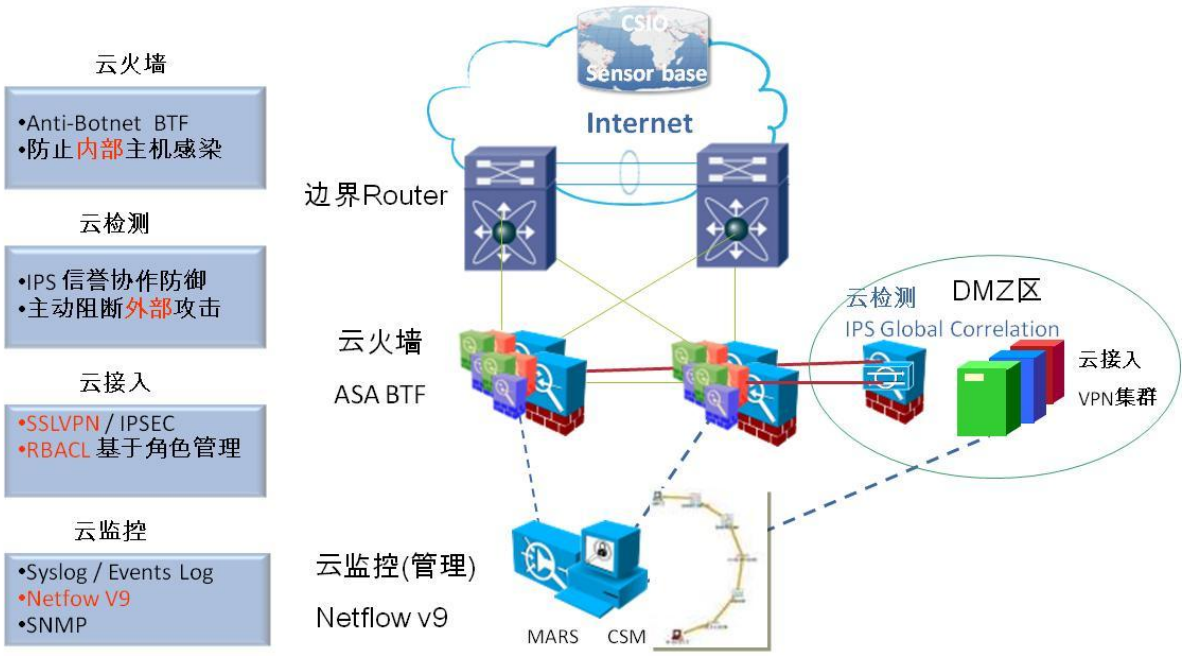
3.8 思科云安全架构－企业新一代的安全数据中心

数据中心作为承载企业核心业务应用的数据处理平台，面临着一系列的安全挑战。在企业构建新一代数据中心的过程中，以下的安全课题需要重点关注：

- 信息的安全访问控制：从传统商务到电子商务的转变意味着增加对敏感信息的访问，同时也增加了风险
- 数据中心威胁防范：保护数据中心免受感染、攻击及入侵 ，数据中心可用性和安全性是非常重要的，任何中断都可能导致严重的商业后果
- 防止数据泄漏与盗窃：敏感及关键数据需要保护免受盗窃或者不合法的传播
- 法规遵从和安全管理：企业必须遵从相关的安全条例，以保障敏感和隐私信息的安全

对于企业而言，数据中心比以往更为重要。数据中心中的数据服务密度的上升，导致对高性能和可扩展网络安全性需求的相应上升。另一方面，Web 2.0 应用程序的出现带来了新型设备的显著增长和复杂内容的广泛使用，这对现有安全基础结构施加了很大的压力。现在的安全系统通常无法满足这些环境中所需的高事务处理速度或安全策略的深度。

为此，思科基于新一代的“云火墙”技术，提出了以下一代 ASA5585-X 高性能自适应安全设备为核心的数据中心云安全架构，为企业数据中心提供动态的、多层次的安全防护，如下图所示：



3.9 思科安全管理

随着企业网络建设的深入，安全产品不断增加，整体缺乏统一管理，相互间没有沟通交互，信息无法有效整合，是一些信息安全的孤岛。就象现在人们在关注和谈论的 IT 孤岛问题一样，各个应用系统之间缺乏有效联系，信息得不到整合，发挥不出其应有的价值。同样的问题放在网络安全上，这一效应就有可能放大成为风险，给企业 IT 系统的持续运转埋下隐患。

思科安全管理器（Cisco Security Manager，CSM）是思科安全管理套件的一部分，能够为思科自防御网络全面管理并执行各种策略。与无法协同运行、存在很多漏洞的多家厂商提供的单点安全产品不同，该套件提供了一个全面的配置、监控、移植和身份识别解决方案，能够有效提高网络的安全性、永续性和易操作性。它可充分利用企业现有的网络和安全投资，来识别、隔离被攻击的组件和建议对其精确删除的方式。它也有助于保持企业内部策略符合性，可作为整体法规符合性解决方案工具中一个不可缺少的部件。

企业安全和网络管理员所面临的问题有：

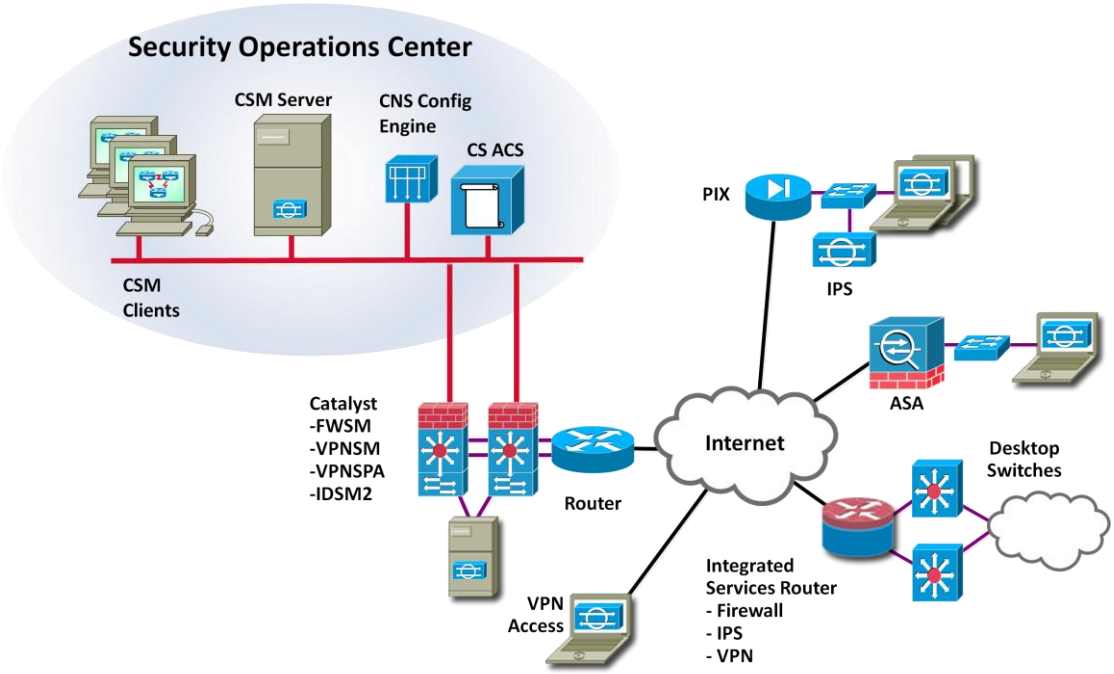
- 安全和网络信息过载
- 性能不佳的攻击和故障识别、优先级划分和响应

- 更高攻击先进程度、速度和修复成本
- 满足法规符合性和审查要求
- 较少的安全人员和预算

思科 CSM 可通过以下功能满足其需要：

- 集成网络智能，进行网络异常事件和安全事件的先进关联
- 察看校正后的事件并自动执行调查
- 通过全面充分利用网络和安全基础设施来防御攻击
- 监控系统、网络和安全运行来帮助企业达到法规符合性
- 以最低 TCO 提供一个易于部署和使用的、可扩展的设备
- 将网络安全设备大量的告警信息进行综合整理归纳使其具有可读性

下图为 CSM 的部署方式：



思科安全管理器采用了基于策略的强大管理技术，能有效管理各种规模的网络，而它功能丰富的客户端图形用户界面则提供了出色的易用性。为完成不同的任务，满足用户的不同要求，思科安全管理器提供多种应用视图，例如图 1 所示的以设备为中心的视图，以及图 2 所示的以地图为中心的视图。

图 1 以设备为中心的视图提供了一个简化界面，用于添加设备以及编辑和部署安全策略

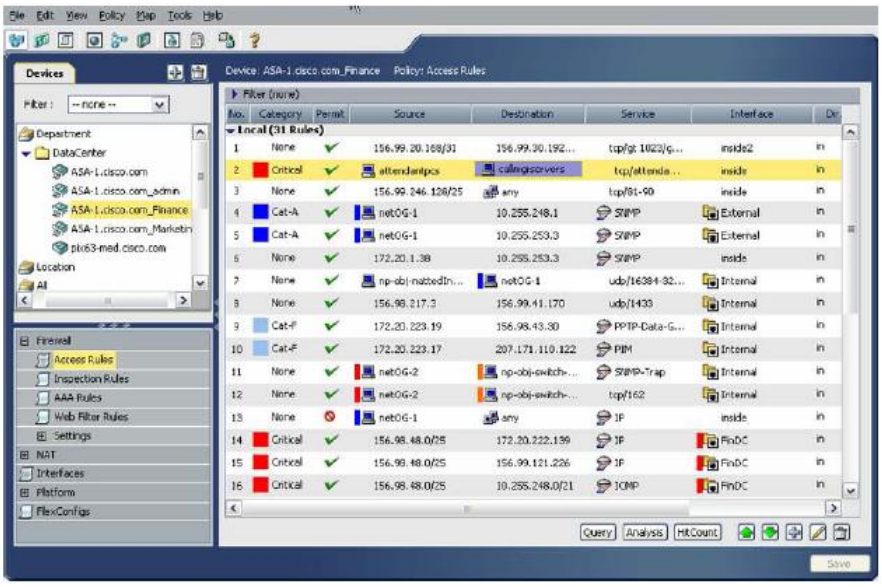
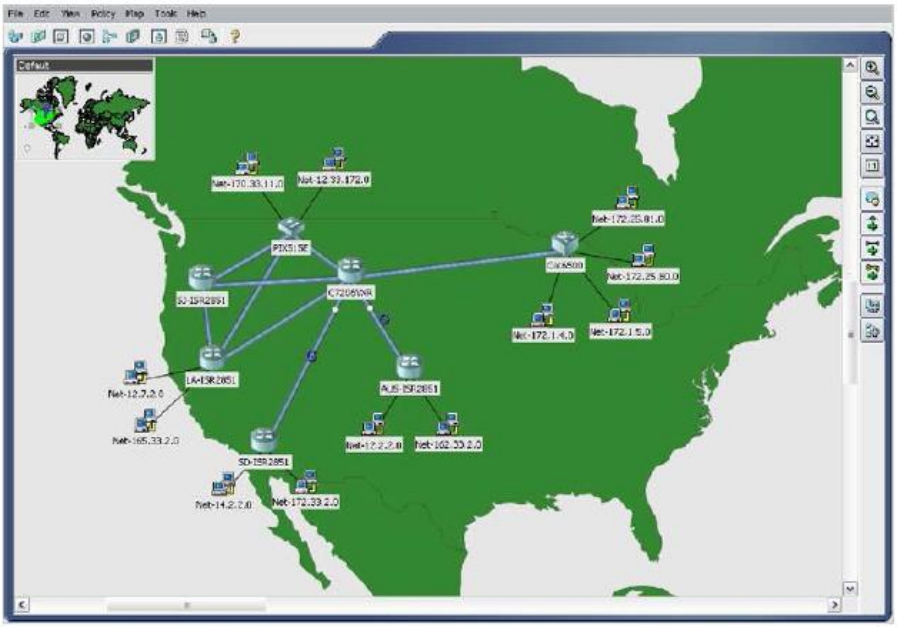


图 2 以地图为中心的视图使用户能以可视方式管理策略和设备



3.10 主要安全产品组合（参考）

- 基础网络安全：

Catalyst 6500 交换机及安全业务模块

Cisco IE3000 工业以太网交换机

ASA 5500 系列自适应安全设备

- 远程安全互联：

ASA5500 + AnyConnect 安全移动解决方案

- 电子邮件安全：

IronPort C 系列电子邮件安全网关

- Web 安全：

IronPort S 系列 Web 网页安全网关

- 终端保护与准入控制：

Cisco NAC Manager

Cisco NAC Server

Cisco NAC Profiler Server

Cisco NAC Guest Server

Cisco NAC Agent

- 安全管理：

Cisco Security Manager 安全管理套件

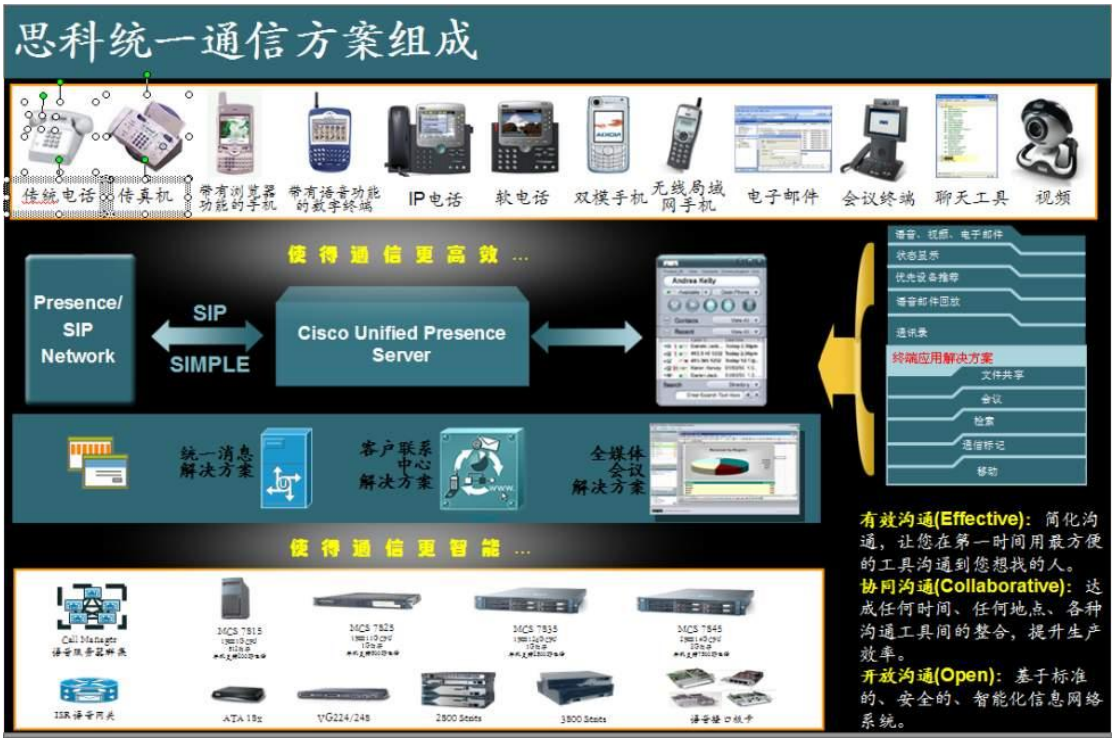
4 制造业的统一通信与协作解决方案

4.1 思科统一通信系统概述

思科统一通信系列是思科商业通信解决方案的一个重要组件，思科商业通信解决方案是一个集成解决方案，适用于各种规模的企业，它包括网络基础设施、安全和网络管理产品、无线连接、生命周期服务 ，以及灵活的部署和管理方式 、融资服务包，以及第三方通信应用。

4.1.1 思科统一通信系统

思科系统公司® 利用其广泛的产品，提供了一个可满足任意规模企业的需求的解决方案。而且通过灵活、透明的移植功能，企业能按照自己设定的速度部署思科统一通信产品。



4.1.2 IP 电话

Cisco Unified CommunicationManager 是思科统一通信系统中基于软件的

呼叫处理组件，提供了一个便于扩展、高度可用的 IP 电话呼叫处理解决方案。凭借其灵活的部署选项，Cisco Unified CommunicationManager 可满足从远程工作人员、移动员工和分散的机构到最大型企业的各种需求。借助思科独有的、集群多个 Cisco Unified CommunicationManager 服务器并将其作为单一实体管理的能力，系统容量可扩展到在一个有 100 或更多站点的网络中支持 100 万用户，且内置了冗余性，可确保提供可靠服务。Cisco Unified CommunicationManager 配备了一系列创新、强大的特性，包括可简化拨号的与 Microsoft Outlook 地址簿的集成、用于具体呼叫记录的分析和报告工具、一个接线员控制台，以及会议呼叫功能。

除为各种规模的机构提供呼叫处理选项外，思科还提供了 Cisco Unified CommunicationManager Express，这是一个位于思科接入路由器中的集成呼叫处理系统。它为小型企业和大型企业分支机构提供了基本的呼叫路由和队列、meet-me 会议、寻呼、内部通信等功能。

尽管这些基于标准的系统能与大量第三方电话共用， 思科仍提供了业界最为丰富的 IP 电话系列 。该系列包括 Cisco Unified IP 电话的基本型号、商业型号和管理人员型号，Cisco Unified 无线 IP 电话 7920、Cisco Unified IP 电话 7985G 可视电话，和众多思科统一通信客户端。

4.1.3 思科统一通信客户端

Cisco Unified CommunicationManager 和 Cisco Unified CommunicationManager Express 支持大量多媒体客户端应用，进一步提高了用户生产率，简化了业务流程。

Cisco Unified Personal Communicator 适用于 Cisco Unified CommunicationManager 用户，将多种通信应用和服务透明地集成到一个桌面 PC 应用之中。它使用户可通过一个易于使用的界面，快速访问强大的通信工具，通过语音、视频、Web 会议、呼叫管理、目录和在网状态信息等 ， 更高效地通信。它简化了通信体验，使团队和知识型员工能更智能、更快速、更安全地工作。

另一个选项，Cisco IP Communicator 是向基于 Microsoft Windows 的个人计算机提供高级电话功能的软件，适用于 Cisco Unified CommunicationManager 和 Cisco Unified CommunicationManager Express 用户。无论用户从何地连接到公司网络，该应用都提供高质量的语音呼叫，以及与用户在办公室中完全相同的特性，包括呼叫转接、呼叫转移和会议呼叫等。无论用户是在办公室、家中，还是在路上，都可保持高生产率。

与 Cisco Unified IP 电话一样，Cisco IP Communicator 也可与 Cisco Unified Video Advantage 共用，后者结合了软件与 Cisco VT Camera，以支持可视电话。Cisco Unified Video Advantage 让用户可通过熟悉的电话界面进行呼叫，在其 PC 上显示视频。思科视频电话解决方案的配置与任意 Cisco Unified IP 电话一样简单，可提供一个经济有效、便于扩展、可视互动的通信解决方案。

4.1.4 企业在网状态和即时消息

CiscoUnified Presence Server 为工具添加了另一层 功能 ，包括 Cisco Unified Personal Communicator。利用动态在网状态信息，用户可实时查看同事的状态，减少“ 电话尾随”问题并提高生产率。Cisco Unified Presence Server 还提供了一项基于标准的在网状态服务，可与连接到 Cisco Unified CommunicationManager 的 Cisco Unified IP 电话共用。对开放标准的支持可使其集成到采用 SIP 和 SIP/SIMPLE 的其他系统，如 IBM/Lotus 解决方案。Cisco Unified CommunicationManager 和 Cisco Unified Presence Server 还支持 Microsoft Live Communications Server 2005 和与 Live Communications Server 连接的 Microsoft Office Communicator 客户端。简而言之，Cisco Unified Presence Server 能帮助客户在任意时间，采用最适合的通信方式 ，最快地 联系到他们的同事。

4.1.5 语音和统一消息

Cisco Unity® 消息处理解决方案也提供了出色的 IP 通信功能和范围。除支持一个强大的语音留言信息处理系统外，Cisco Unity 解决方案还可帮助客户通过电话收听其电子邮件、从互联网查看语音留言，并可在任意地点发送、接收和转发传真。各用户以他们最方便的方式与系统交互，这也使他们能更好地响应客户要求。Cisco Unity 解决方案提供了语音留言、集成消息和统一消息选项，具高可扩展性，能满足大型企业的需求。此外，Cisco Unity Connection 是专为满足员工数不超过 1500 的机构的需求而定制的，具有语音留言、集成消息，以及语音姓名拨号和语音留言浏览等高级特性。Cisco Unity Express 在思科路由器内部提供，支持最多 250 名用户。它们均提供了经济有效的自动接听功能，和集成消息选项。

4.1.6 多媒体会议

Cisco Webex 会议解决方案是只有 IP 可提供的又一类集成通信产品。Cisco Webex 透明地集成了语音、视频和 Web 会议功能，可真正简单地发起和进行高效率的远程会议，帮助您更快完成项目、增强销售支持，并加速决策制订。Cisco Webex 可与 Microsoft Outlook 和 IBM Lotus Notes 日历集成，使用户就像他们召开其他任何会议一样，方便地设置和参加多媒体会议。此系统可部署在客户端现场，或离站托管，可由客户管理，也可外包。对于中型机构来说，Cisco Webex 是一个便于部署和管理、特性丰富的会议解决方案，包括 Cisco Unified IP 电话、触摸屏电话，和用于设置、参加及管理会议的 Web 界面。

4.1.7 移动解决方案

思科为移动员工工作于不同环境的机构提供了多种解决方案。经常处于移动状态的员工将受益于 Cisco Unified MobilityManager，它提供 Cisco Mobile Connect 服务，籍此，这些员工可向客户、同事和合作伙伴公布单一号码，并随时可将呼叫路由到对他们来说最方便的设备：办公室电话、家庭电话或手机。

Cisco Mobile Connect 服务甚至可帮助员工在到达办公室后， 将呼叫透明地从手机转接到办公室电话（反之亦然），且不必中断呼叫。在旅行时，移动员工也可获得企业 IP 通信特性，包括使用公司网络进行呼叫等，从而降低成本。

为进一步提高移动性，思科统一通信系统为诺基亚和其他厂商的一类新手机提供了双模支持。这些双模电话支持 GSM 和 Wi-Fi 射频，可用于数据和语音应用。另一业界领先厂商摩托罗拉也正在开发双模设备，并通过其无线服务管理器支持网络移动性。利用 SIP 技术， 移动客户端 在企业中基于 802.11a 技术连接到网络，在 其他地点 使用蜂窝电话 ，从而 实现透明的 转移通信，使移动员工始终保持网络连接。

4.1.8 客户联系解决方案

思科统一通信还为客户联系中心提供了激动人心的新功能，帮助用户随时处理大量客户交互，如语音电话呼叫、电子邮件或基于 Web 的通信 。包括 Cisco Unified Intelligent Contact Management 和 Cisco Unified Contact Center 产品系列在内的全面的思科客户联系解决方案系列，提供了出色服务，提高了客户满意度。联系信息会根据业务规则和目标，转接到最适合的服务人员。先进的计算机电话集成功能为服务人员的桌面提供了呼叫事件和客户档案信息。凭借 Cisco Unified Mobile Agent 等产品提供的灵活性，服务人员可从家中工作，也可在差旅时工作。

利用自动语音自助服务解决方案—其中包括 Cisco Unified 客户语音门户

和 Cisco Unified IP IVR［交互式语音响应］—许多呼叫无需服务人员的帮助即可完成。思科语音自助服务解决方案使用自动语音识别和文本到语音功能，使主叫方能获得个性化的应答，来解决其日益复杂的问题，并以创新方式处理业务。例如，客户可在无需一位实际服务人员帮助的情况下，支付帐单、订购产品和跟踪产品供货。通过 Cisco Unified 客户语音门户的可扩展标记语言(XML)语音功能，主叫方能访问 Web 交互中所使用的内容，从而无论使用哪种自助服务渠道，都可获得一致的客户体验。

Cisco Unified Customer Interaction Analyzer 提供了针对每个客户交互的新视角，能够转变呼叫中心服务和挽留客户的方式，以及它们招聘、培训和评估客户服务代表的方式。

4.1.9 管理解决方案

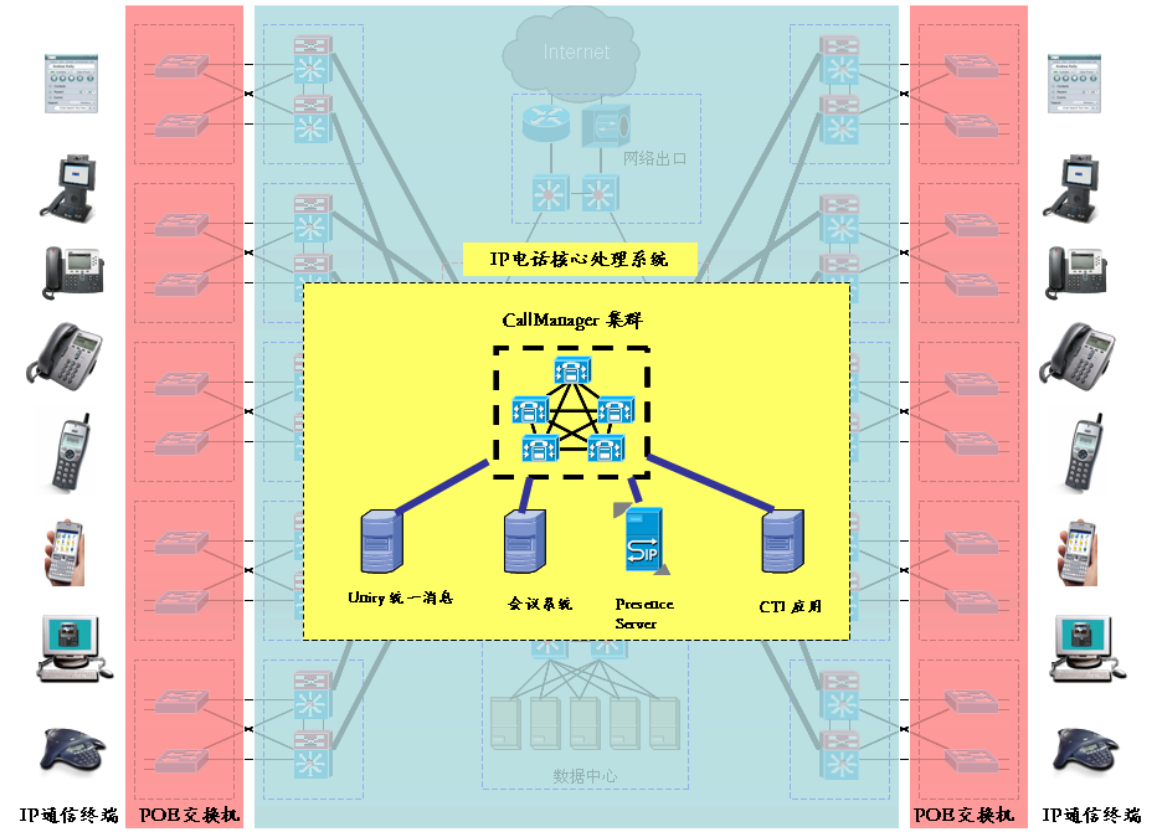
利用 Cisco Unified 通用管理套件可主动监控网络中的思科语音组件，以发现潜在问题、保持通话质量和用户满意度，并缩短服务中断时间。

4.2 制造业统一通信系统的设计与部署

统一通信系统必须满足生产制造型企业的各种呼叫应用,包括基本呼叫功能、扩展呼叫功能、语音留言功能、语音会议功能、CTI 功能等。

4.2.1 统一通信系统架构

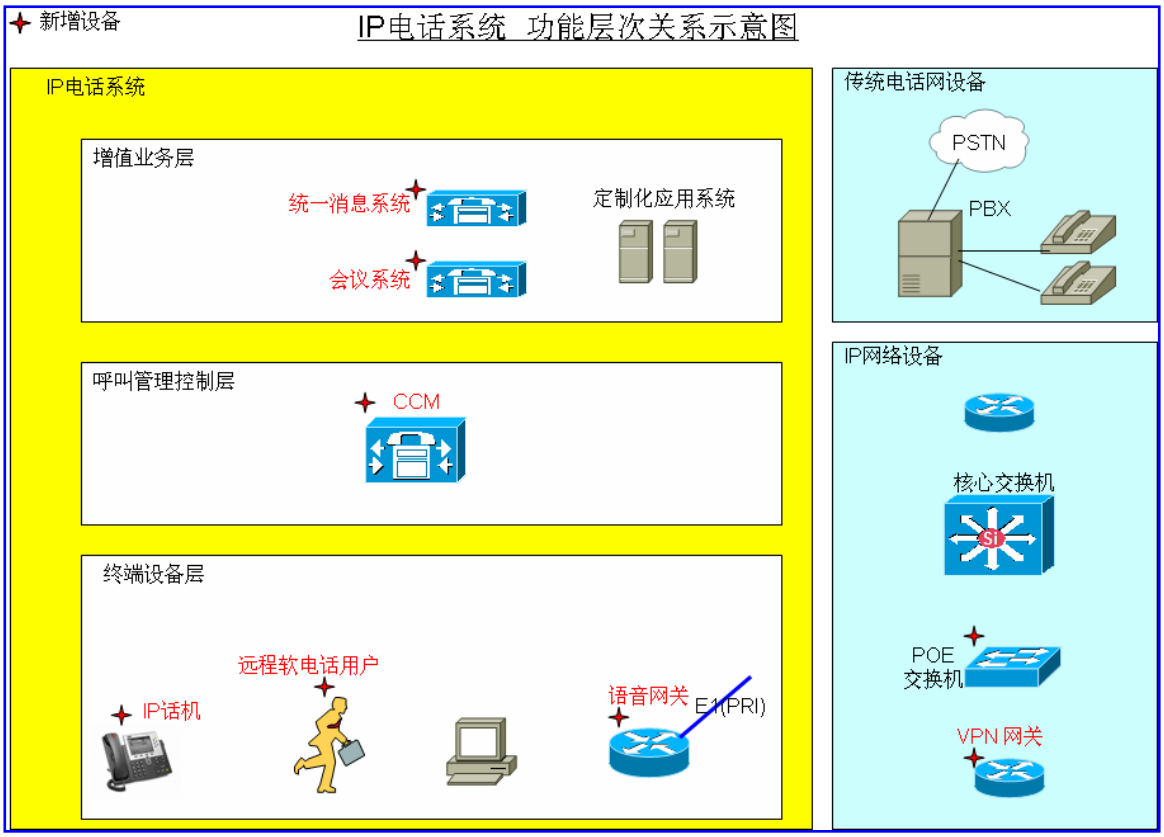
采用基于 IP 网络平台的思科统一通信解决方案，基于纯 IP 网络环境的融合通信，结合有线和无线通信的特点，灵活的部署和调整终端部署和功能设置，可以满足不断变化的业务要求，并提供高度的可靠性和运行稳定性。



企业统一通信系统架构示意图

接入层的 POE 交换机，可以为各类有线 IP 终端提供可靠的供电，并根据终端划分独立的 Voice VLAN。

用户可以根据业务的需要，选用各种类型的有线或无线 IP 通信终端，或使用基于 PC 的软终端实现统一通信。



IP 电话系统按功能划分为三个不同层次:

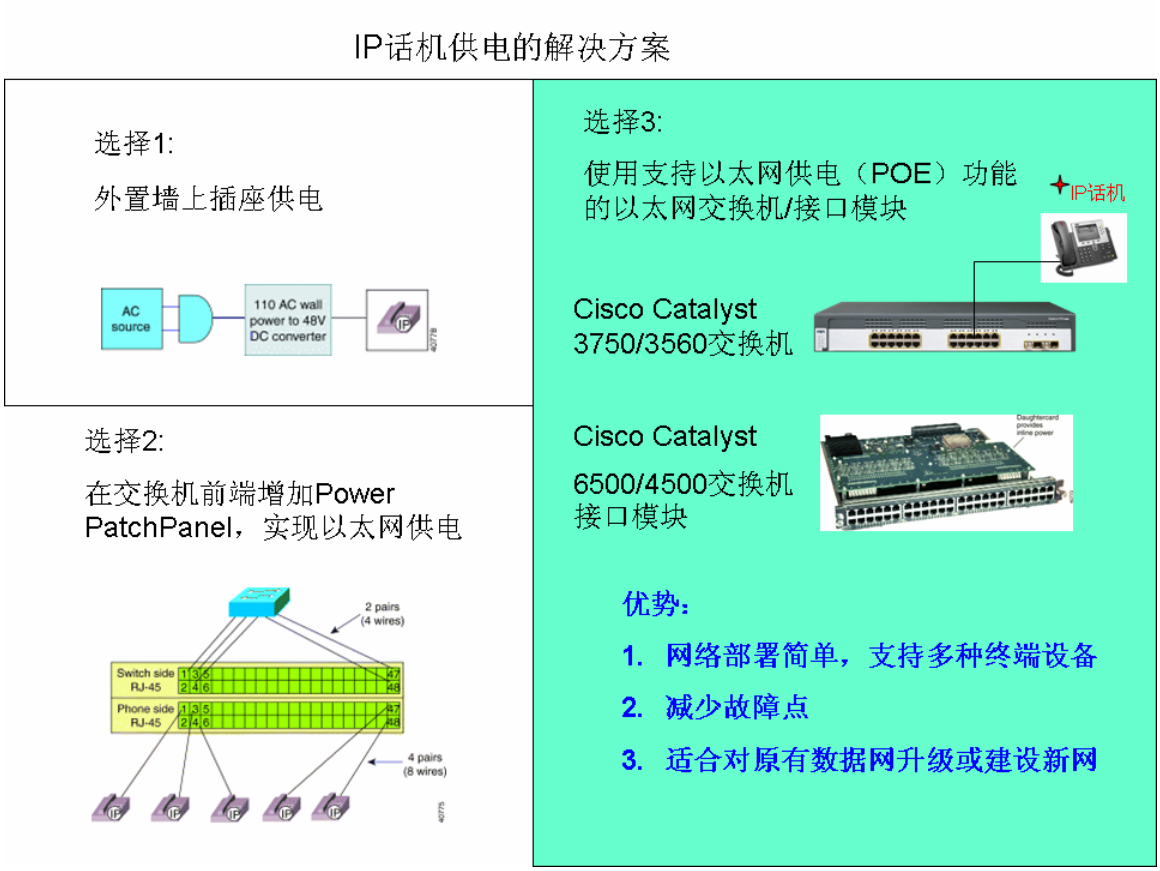
层次	功能部件	描述
呼叫管理控制层:	CUCM	Cisco Unified CommunicationManager 是 IP 电话的呼叫信令处理中心，根据 IP 话机终端或语音网关的呼叫信令信息，对终端、网关、呼叫进行统一管理，是思科统一通信架构中的重要部件之一。
增值业务层	统一消息系统	在语音信箱的基础上,提供支持 PC/模拟电话等多种终端访问形势的统一消息。
	会议系统	提供基于语音和 Web 的会议通信系统
终端设备层	语音网关	实现 IP 话音和传统 TDM 话音之间的媒介转换和信令消息中继。
	IP 话机	IP 话音的终端设备，将语音直接转换成 IP 数据包，可视话机同时支持 IP 视频，显示屏清晰的图形功能支持可扩展标记语言 (XML)应用。

	软电话	以软件形式运行在 PC 上的 IP 电话终端

IP 网络承载语音业务的关键因素考虑

实现 IP 数据交换的同时，在 IP 网上承载 IP 电话业务，有如下两个关键因素需要考虑：

关键因素 1	说明	思科交换机
使用方便： 交换机支持 POE 供电	采用支持 POE 方式的局域网交换机，将消除 IP 电话外接电源存在的故障点，极大的方便用户使用。（如下图所示）	**支持**



关键因素 2	说明	思科交换机
话音质量： 语音流量和数据流量的隔离	思科的 IP 电话机已内置了对语音/数据 VLAN 的隔离支持，并可以进行 QoS 的设置。 思科交换机能够支持 Voice VLAN，在交换机和	**支持**

及 QoS 保证	思科 IP 电话之间使用 802.1Q，将语音和数据流量分配到不同的 VLAN 中，并赋予不同的 QoS 参数，实现语音流量的优先处理。 （如下图所示）	

为保证 IP 语音在局域网或广域网中的有效可靠传输，我们建议除了上面提到的 VLAN 标记区分 IP 语音数据报和 PC 数据报之外，对语音包采用以下的 QoS 标记：

Application	L3 Classification			L2	L2
	IPP	PHB	DSCP	CoS	MPLS EV
Reserved	7	-	56-63	7	7
Reserved	6	-	48-55	6	6
Voice Bearer	5	EF	46	5	5
Video Conferencing	4	AF41	34	4	4
Call Signaling	3	AF31	26	3	3
High Priority Data	2	AF2y	18,20,22	2	2
Medium Priority Data	1	AF1y	10,14,16	1	1
Best Effort Data	0	BE	0	0	0
Less-than-Best-Effort Data	0	-	2,4,6	0	0

局域网语音压缩标准：G.711

广域网语音压缩标准：G.729

以下为在一定条件下的 IP 语音带宽计算值：

压缩技术	语音数据负荷大小	完整的 MLPPP 带宽	cRTP & MLPPP 情况下的带宽	VAD & MLPPP 情况下的带宽	cRTP & VAD & MLPPP 情况下的带宽
G.711(64Kbps)	120	89	68	58	44
G.726(32Kbps)	60	57	36	37	24
G.726(24Kbps)	40	52	29	34	19
G.728(16Kbps)	40	35	19	23	13
G.729(8Kbps)	**20**	**26.4**	**11.2**	**17.2**	**7.3**
G.723.1(6.3Kbps)	24	18.4	8.4	12	5.5
G.723.1(5.3Kbps)	20	17.5	7.4	11.4	4.8

数据网络要求：

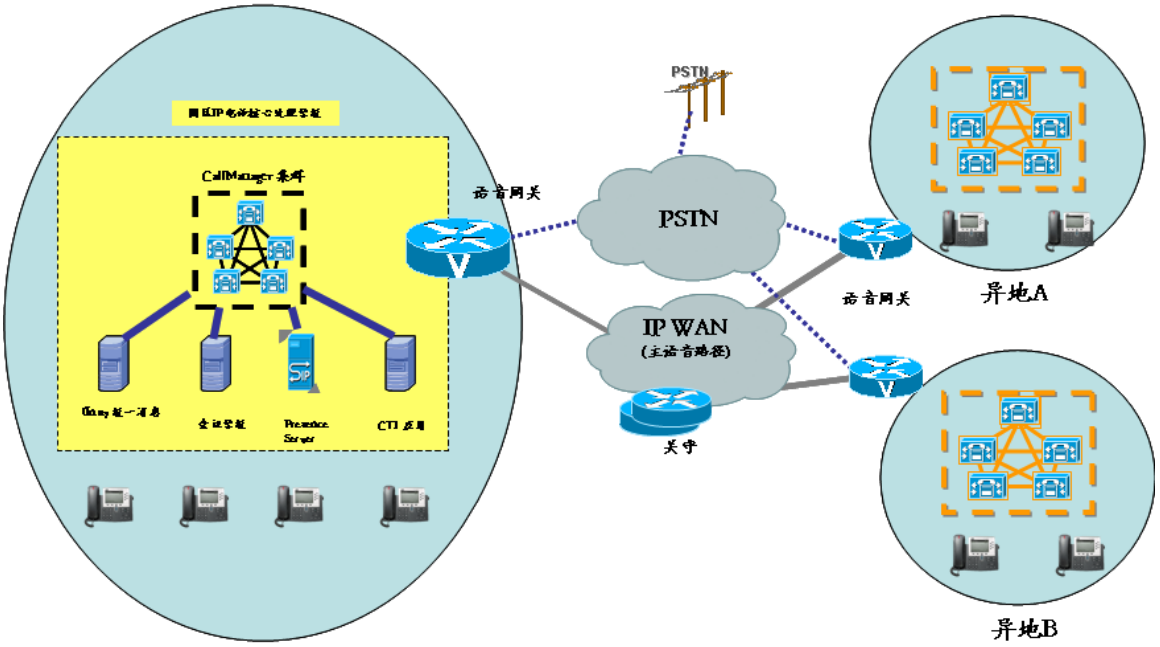
- 数据包延迟：<180ms
- 抖动(Jitter)：<20ms
- 丢包率：<3%

与外部语音网络的连接

企业的统一通信系统可以通过多种不同的接口方式与 PSTN 和异地的 IP 语音网络实现互通，思科语音网关提供丰富的 E1 Trunk、ISDN、FXO 或 IP 接口，支持国际标准的 H.323/SIP/MGCP 等 IP 语音通信协议。

当 IP 广域网出现异常时，出网的 IP 语音呼叫系统会自动将语音呼叫路由至 PSTN，并在 IP 广域网恢复时自动回退至正常呼叫路由。

如下是制造业企业 IP 语音系统与外部电话系统之间的连接示意图：

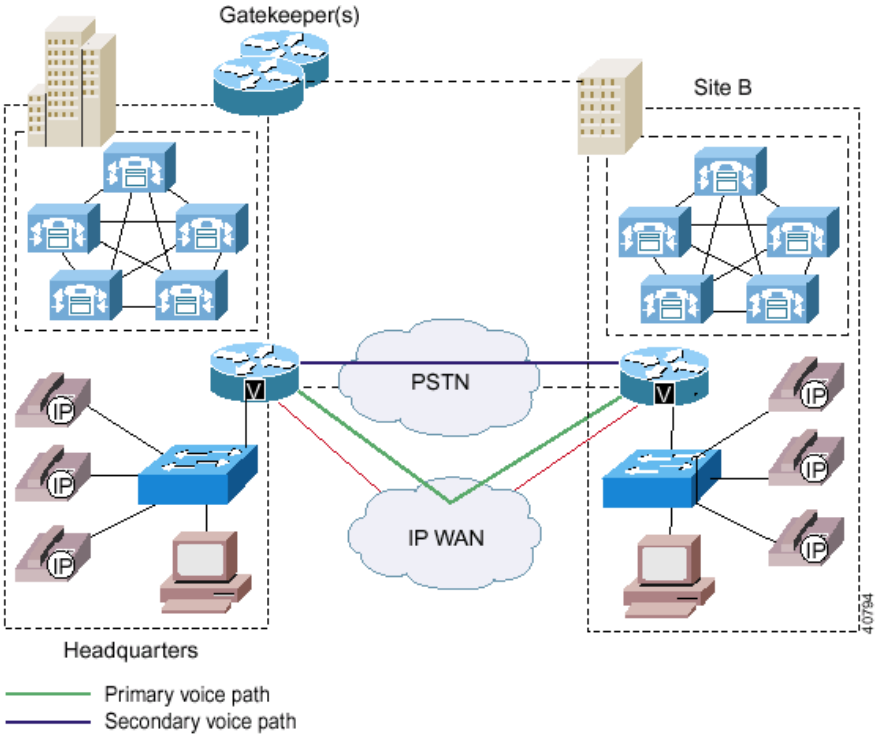


4.2.2 拨号方案规划

IP 通信拨号方案体系结构中包含了对以下两种类型的呼叫处理：

- Cisco CommunicationManager Cluster 内的 IP Phone 之间的内部呼叫
- 通过 PSTN 网关的外部呼叫

下图显示了能处理上述两种类型呼叫的网络。通过合理的拨号方案，语音呼叫优先使用 IP WAN 的连接，只有当 IP WAN 故障或拥挤时才溢出到 PSTN 进行处理。这种溢出对用户是透明的，即我们可以事先进行设置，并且当呼叫溢出时我们可以知道并且可以采取相应措施。



对于注册到同一个 CommunicationManager 集群的 IP 电话之间的呼叫的拨号方案是非常简单的。在初始配置时，每一 IP 电话设置一个电话号码（DN）。当 IP 电话注册到 CommunicationManager 集群时，电话号码保持不变，但是会将动态获得的新 IP 地址提交给该 CommunicationManager 集群。内部呼叫拨号的长度是可以设置的。上述拨号方式中，IP 电话并非唯一的电话终端，还包括了 Cisco IP SoftPhone（软电话）、Cisco IP Communicator（软电话）、采用 MGCP 或 Skinny 网关协议连接到语音网关的模拟电话和传真机。

CommunicationManager 的拨号方案体系结构中包括了分区（Partition）、呼叫搜索空间（CSS，Calling Search Space）、路由计划（Route Plan）。Partition 定义了相同“reachability” 特性的设备，包括 IP 电话、电话号码、网关和 Route Pattern。CSS 是一组规则，它定义了针对一个拨的号码，不同的设备应该搜索哪一个 Partition，CSS 还提供拨号许可/限制，每个设备都可指定一个 CSS。通过分区和呼叫搜索空间的定义，可以定义每个分机的呼叫限制等级，如国内、国际、市话、园区内、首钢系统内、紧急特服号等。

4.2.3 内网中防火墙穿越的解决

为了解决网络安全问题和地址资源匮乏等问题，大量企业和驻地网采用了

私有编址(RFC1918)，并通过 NAT/防火墙来控制与公共网络的通信。NAT/防火墙能够完成私有编址与公网编址的相互转化，并设置相应的包过滤规则，让不满足条件的 IP 包不能够穿透 NAT/防火墙。NAT/防火墙对 HTTP 等端口固定的一般应用协议，只需要转换 IP/TCP/UDP 头，即可很好地实现穿透.

但对于 H.323/SIP/H.248/MGCP 应用来说，是在控制信息中动态地协商媒体流端口，信令协议里面的 IP 地址也是私有的，而私有 IP 地址在公网上是不能路由的，动态分配的端口为在 NAT/防火墙上配置固定的包过滤策略带来了困难。

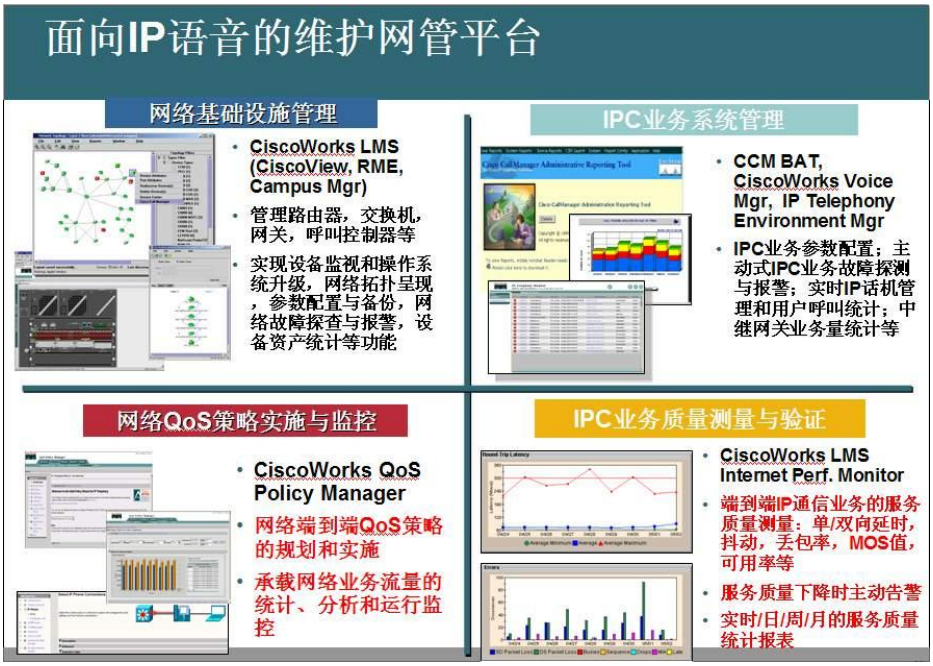
ALG（Application Level Gateway）方式是最早出现的 NAT 穿越解决方案。ALG 是在传统的 NAT 上进行协议扩展,使之具备感知 SIP、H.323、H.324 和 MGCP 等呼叫控制协议的能力，从而完成呼叫控制协议的解析和地址翻译功能。

思科的防火墙系统，能够支持 ALG 功能，可根据需要在内网中进行安全隔离的位置部署，以解决语音业务的穿越问题。

4.2.4 统一通信系统的管理

当前企业选择 IP 语音系统，常将关注点集中在 IP 语音的呼叫处理设备和终端设备，而忽视 IP 网络平台性能、QoS、稳定等关键要素对 IP 语音业务的重要影响，从而陷入高投入低效能的投资误区。

思科具备全面的数据和语音产品线，并提供丰富的语音业务管理手段，帮助企业客户用好、管好 IP 语音系统。



4.2.4.1IP 通信业务系统管理

CUCM 系统自带的系统管理工具包括：

- BAT 批量管理工具：大批量定义设置 IP 电话机和用户的增加、删除、更新。
- CDR 呼叫详细记录：提供呼叫全程包括主叫、被叫、转接号码、起止时间等的内部和外部呼叫的记录，第三方计费系统可以通过 ODBC 等 SQL 数据库访问工具获得实时的 CDR 信息。
- CDR 呼叫详细记录分析和报告（CAR）：提供所有通话包括话机和网关的统计和分析报表，包括详细的、总结和使用情况的报告。
- CommunicationManager 实时监视工具（RTMT）：监视 Call Manager 集群的设备状态、系统性能、设备联接、CTI 应用。
- Cisco CommunicationManager Serviceability Trace：提供 trace 跟踪和分析。

CiscoWorks 中提供的通信业务系统管理工具包括：

- CiscoWorks 语音管理（CiscoWorks Voice Manager）
- IP 语音环境管理（ITEM，IP Telephony Environment Manager）

这些工具提供了 IP 通信业务参数配置；主动式 IP 通信业务故障探测与报警；实时 IP 话机管理和用户呼叫统计；中继网关业务量统计等。从远程维护的角度，CommunicationManager 系统提供了以下工具：

- Cisco 安全 Telnet
- Show 命令行接口
- Microsoft Windows 2000 Performance Monitoring
- ISDN 跟踪日志消息翻译器
- CiscoWorks2000 网管系统
- 路径分析接口
- 系统日志管理
- SNMP Instrumentation
- CDP 支持

4.2.4.2网络基础设施管理

CiscoWorks LMS （CiscoView，RME， Campus Manager）提供：

- 路由器，交换机，网关，呼叫控制器等的管理；
- 实现设备监视和操作系统升级，网络拓扑呈现，参数配置与备份，网络故障探查与报警，设备资产统计等功能。

4.2.4.3网络 QoS 策略实施与监控

CiscoWorks QoS Policy Manager（QPM）对全网进行集中式的 QoS 策略创建、部署和结果分析，它提供：

- 网络端到端 QoS 策略的规划和实施（包括为 IP 电话业务提供智能 QoS 策略建议）；
- 承载网络业务流量的统计、分析和运行监控。

4.2.4.4IPC 业务质量测量与验证

CiscoWorks LMS Internet Performance Monitor 提供：

- 端到端 IP 通信业务的服务质量测量：单/双向延时，抖动，丢包率，MOS 值，可用率等；
- 服务质量下降时主动告警；
- 实时/日/周/月的服务质量统计报表。

4.3 统一通信与协作主要产品组合（参考）

呼叫控制

- Cisco Unified Communication Manager 8.0 或以上
- 集成 Cisco Unifiede Communication Manager Express 的 ISR G2 路由器
- MCS78 系列，安装 CUCM 的硬件服务器

IP 电话系列

- 79/69 系列 IP 话机
- IP Comunicator 客户端

模拟电话网关

- VG224
- VG202
- VG204

客户联络中心解决方案

- Cisco Unified Contact Center Express （UCCX）

5 基于 IP 网络的制造业应用解决方案

5.1 思科工业以太网解决方案

5.1.1 思科工业以太网解决方案概述

为了在竞争越来越激烈的制造业中取得成功，无论企业的规模如何，都必须更加快速地响应客户的要求，并为客户提供优质产品之外的其它价值。实现这些目标的最佳方式是实时、深入地了解整个制造企业的全部重要数据和商业资源。

思科系统®公司能够帮助制造商建立协作制造环境，实现思科®智能网络制造（INM），为制造运作提供顺畅、安全的数据可视性和极高的灵活性。

作为思科 INM 计划的一部分，思科工业以太网解决方案能够弥补办公室与生产车间之间的缺口，同时提供可视性和灵活性，帮助制造企业将制造车间转变成战略性企业资源。

思科工业以太网（EttF）不但能帮助企业为车间设备增加以太网连接，还能为企业提供所需的高新技术。由于思科可管理交换机能够以可控方式接入网络，因此，企业不但能对实时数据作出适当的响应，还能延长关键流程的正常运行时间。

图 1 网络拓扑图

5.1.2 思科 IE3000 工业以太网交换机

IE3000 系列是一个全新的交换机系列，提供了坚固、易用、安全的交换基础设施，适用于恶劣环境。Cisco IE3000 系列采用了工业设计，符合工业规范；其工具简化了工业网络的部署、管理和更换；且在开放标准的基础上提供了很好的网络安全性。Cisco IE3000 是支持工业以太网应用的理想产品，这其中包括工厂自动化、智能交通运输系统(ITS)、变电站和其他恶劣环境中的部署。

Cisco IE3000 提供了一系列针对工业以太网应用进行的优化设计，包括：

- 面向工业以太网应用的设计，包括扩展的环境参数、冲击/振动和电击；全面的电源输入选项；对流冷却；以及DIN轨或19”机架安装
- 支持300种不同的硬件配置
- 能使用思科设备管理器Web界面，以及思科网络助理和CiscoWorks等支持工具，方便地设置和管理
- 使用可拆除内存，简化了交换机更换，使用户无需重新配置，即能更换交换机
- 通过Cisco IOS®软件提供高可用性、关键数据传输保证和可靠安全性
- 只需按下一个按键，即能获得针对工业应用的建议软件配置
- 符合广泛的工业以太网规范，适用于工业自动化、ITS、变电站、铁路和其他市场
- 支持IEEE1588v2，这一计时协议为高性能应用提供了纳秒级精确度

基于以上的特性，IE3000 系列能够支持多种工业以太网的应用，具体包括：

工业自动化：

Cisco IE3000的设计支持丰富的自动化领域工业以太网协议。Cisco IE3000采用了可编程逻辑控制器(PLC)机型设计，具有扩展的环境参数、对流冷却、DIN轨道安装、冗余24VDC/48VDC电源输入、告警继电器和浪涌/噪音抗干扰性等特性。Cisco IE3000软件和配置工具支持简单设置，适用于多个工业以太网应用，包括Ethernet/IP、ProfiNet、Modbus TCP、FoundationFieldbus 高速以太网(FFB HSE)等。在建议用于这些协议的默认模板中，指定了组播控制、流量优先级划分和安全特性。

ITS：

Cisco IE3000支持ITS和其他用于室外视频和流量传输或交通运输系统控制的应用。该交换机支持NEMA TS-2法规遵从性、多种千兆光纤上行链路，以及交流和直流电源输入选项，而Cisco IOS软件则支持关键ITS特性，包括虚拟局域网(VLAN)、QoS、IGMP监听和安全访问控制列表(ACL)等。

变电站：

Cisco IE3000完全符合变电站自动化规范，包括IEC61850和IEEE1613。该交换机支持高速环网恢复；光纤接入和上行链路端口；以及交流、48V直流和125V直流电源输入选项，适用于变电站环境。

其他应用：

Cisco IE3000适用于铁路、军用环境、城域以太网，以及其他需要独特环境参数、机型或电源输入的恶劣环境中的应用。

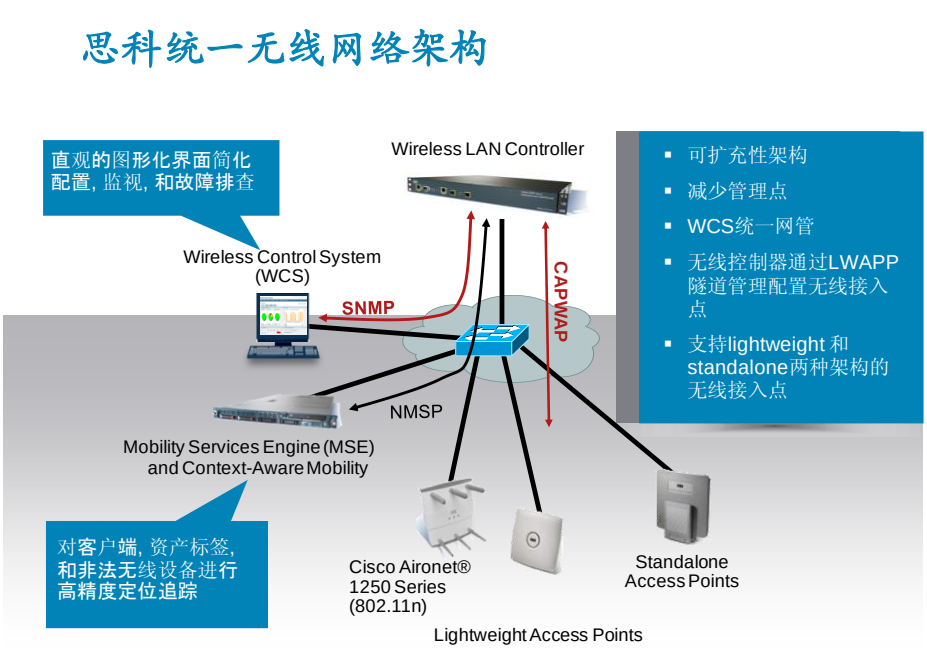
5.2 思科统一无线网络在制造业的应用

5.2.1 思科统一无线网络架构概述

思科统一无线网络架构主要包含以下部分：无线控制器，无线访问接入点AP，无线网管系统 WCS，无线定位服务系统 MSE，用户认证系统 Radius 服务器，以及支持以太网供电的接入交换机和负责数据交换的汇聚及核心交换机。

无线控制器和 AP 是无线网完成数据转发的基础部件。在控制器加 AP 的网络架构下，所有关于无线射频管理、网络安全管理等的智能处理都在控制器上集中处理，而 AP 只完成空口侧数据的收发。在实际工作中，每台控制器会管理一定数量的 AP，并与每台 AP 建立 CAPWAP 隧道。用户数据经无线介质到达 AP 后，AP 将数据封装到隧道中传送到控制器。控制器将数据解出，并根据管理员设定的安全、QoS 等管理策略，进行处理。最后经有线网络发送。

思科无线网络产品系列是为那些希望为本身业务、IP 电话和融合多媒体应用系统广泛部署无线覆盖的一款完整 802.11 解决方案。这款解决方案将最新的行业标准与一种集中架构和先进功能结合起来，创建一种安全、经济有效并且极具扩展性的无线局域网(WLAN)基础设施。思科无线网络产品系列包括规划和实施所需的工具和功能，使首次部署无线局域网(WLAN) 能快捷简便的完成，也适合于企业逐步演进事先精确设计的无线移动基础设施。



5.2.2 思科 CleanAir 技术保障企业关键业务的不间断运行

Cisco CleanAir 技术提供 802.11n 的性能和支持关键任务应用程序所需的可靠性，同时还能以智能方式避免干扰的影响。CleanAir 技术是思科统一无线网络的一个系统范围功能，可通过提供无线频谱的完整情况，简化操作和改进无线性能。CleanAir 具有独特的能力，可检测其他系统检测不到的 RF 干扰，识别干扰源，在地图上找到它，然后进行自动调整来优化无线覆盖范围。通过 CleanAir，您可以访问无线网络中任何位置的设备和资产的实时信息和历史信息。如今，IT 经理可以根据智能信息实施策略，快速采取行动来改进网络性能。

CleanAir 技术包括 Cisco Aironet® 3500 系列接入点的高级硅片设计以及思科无线控制器、思科无线控制系统 (WCS) 和 Cisco 3300 移动服务引擎启用。

Cisco CleanAir 可使企业：

- 自动优化无线 LAN 以提高可靠性和性能
- 执行远程故障排除，以便快速解决问题并减少停机
- 检测非 Wi-Fi 安全威胁并实时解决问题
- 查看历史干扰信息，以便进行回溯分析并快速解决问题
- 通过无线设备的智能识别来设置和实施策略

自行恢复、自行优化的无线网络

如果干扰源足够强，能够完全干扰 Wi-Fi 频道，那么应用 CleanAir 技术，系统就会在 30 秒内更改频道，以避免干扰，并继续在受影响区域以外的其他频道上进行客户端活动。系统能记住从微波炉、网桥或无线视频摄像头发出的间歇性干扰，避免使用运营这些设备的频道，以防将来造成干扰。

许多公司都声称自己拥有集成干扰检测系统，但他们的产品无法区分 Wi-Fi 和非 Wi-Fi 干扰。其他制造商的频谱智能产品可能会错误地将网络噪音解释为干扰并随机切换频道，这会危及网络稳定性，而且可能会降低整体网络性能。Cisco CleanAir 技术使用硅片级智能，可精确地检测 20 多种干扰类型并加以分类，只有在它认为干扰非常严重，以致影响网络性能时，才会更改频道。如果 CleanAir 更改频道，它会考虑整个网络频道策略，然后确定首选的频道更改。所有这些智能功能可创建一个自行恢复、自行优化的无线网络，从而为 802.11n 网络提供性能保护。

故障排除调查分析可快速解决干扰并主动采取措施

通过 CleanAir 技术，您可以利用易读的“空气介质质量指数”，充分了解无线频谱的性能和安全性。该指数可识别出现问题的区域，并在接入点、楼层、建筑物和园区环境中找出问题区域

CleanAir 可减少停机。网络管理员可以设置警报，以便在空气介质质量低于预期阈值时得到通知。另外，还可以将系统配置为自动实施安全或管理策略。Cisco CleanAir 生成报告来帮助网络管理员对亟需关注的干扰问题排定优先级，便于网络管理员轻松地了解细节，以进行进一步的网络分析。报告包括最差 RF 条件汇总、最近的安全风险干扰源、阈值警报和历史图表。通过主动监控“空气介质质量指数”图表和 30 天的干扰报告，管理员可以规范正常行为并监控网络趋势，从中看出未来可能发生的问题，以免影响网络性能。

快速、准确的干扰检测可减少误报

由于大多数设备都不断地在移动或者开启和关闭的速度很快，因此很难跟踪干扰。即使成百上千个设备在极为繁忙的 RF 环境中同时运行，CleanAir 也能在 5 至 30 秒内对 20 多种干扰进行分类。CleanAir 分类的准确性和快速性是其主要优势，因为它可减少无干扰时（“仿真干扰”）的干扰报告，并消除多个 AP 检测到的同一设备的重复报告。另外，它还可减少发生错误标记干扰源的情

况，从而减少管理员通常浪费在搜索错误类型设备上的时间。

提供远程访问，可更有效地解决问题并减少差旅

对于远程故障排除，频谱专家连接模式从专家视角提供来自个别接入点覆盖区域的物理级别频谱图。虽然 CleanAir 技术提供大量更高级别的分析数据，包括对设备进行分类和评估无线空气介质质量的报告，但有时难免需要查看实时、原始频谱数据，以找到难以诊断的干扰问题。这在干扰类型没有包含在标准分类列表中时非常有用。

高效的策略实施

通过实施策略来阻止干扰 Wi-Fi 网络的设备一直以来都是网络管理员难以解决的问题。应用 CleanAir 技术，网络管理员便能够跟踪网络性能，找到并查看非 Wi-Fi 设备产生的影响，实施策略，防止已知干扰源影响网络速度或危害网络安全。

强大的安全性

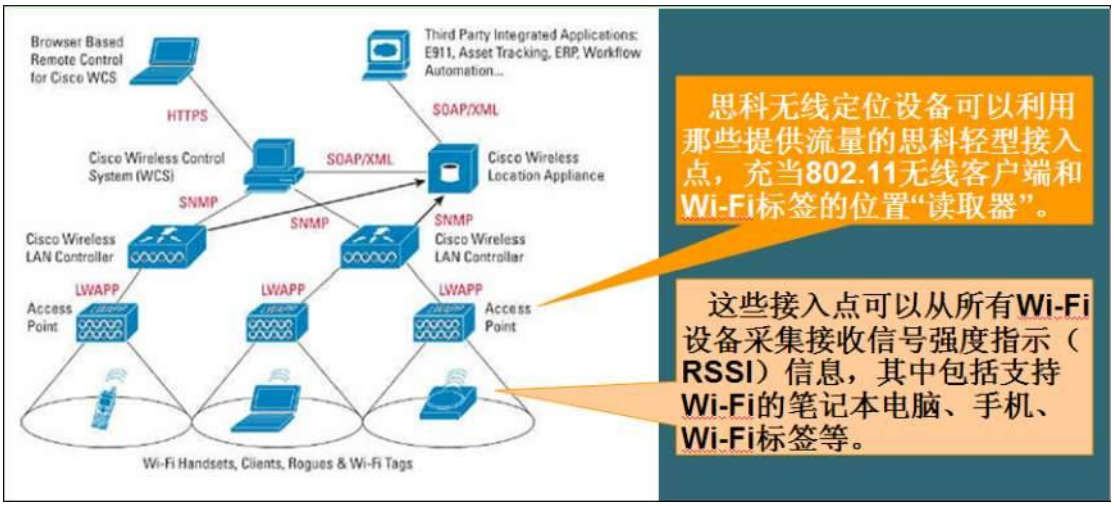
从安全性角度看，在地图上跟踪设备可使您立刻了解要将安保人员派往哪里。有许多网络威胁是传统的 IDS/IPS 系统检测不到的——原因在于只能在 RF 级别检测到它们。这些威胁包括专有无线网桥，以及较早的标准，如 802.11FH。这些威胁还包括在非标准运行频率上运行或使用非标准调制的恶意 Wi-Fi 设备。当然，干扰设备也会经常发生拒绝服务类型攻击。

除在地图上查看影响安全的设备外，管理员还可以根据设备或位置来配置定制警报。这是一种强大的功能，因为某些设备在建筑物的一些区域（例如，交易翼）内可能被认为是威胁，但在其他区域（如建筑物大厅）则不被认为是威胁。

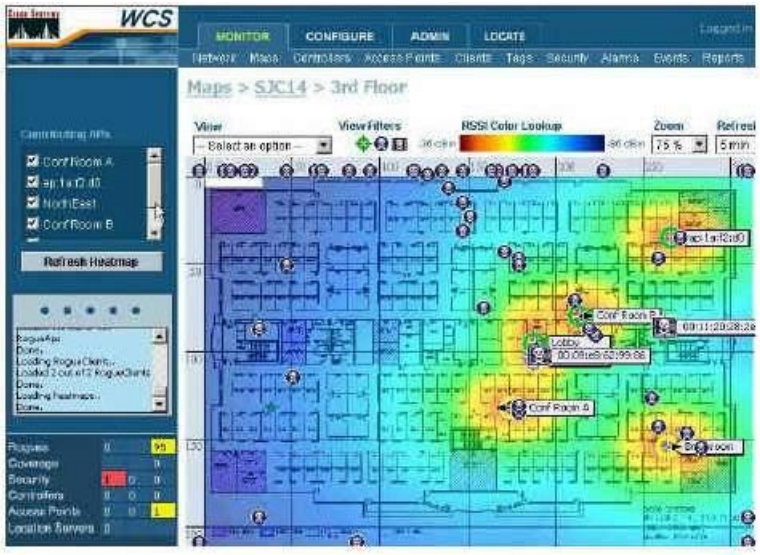
5.2.3 无线定位在制造业的应用

思科无线定位设备可以利用思科无线局域网控制器和思科轻型接入点，跟踪无线设备的物理位置，结果可以准确到几米之内。

通过高效的无线位置管理，帮助企业完善资产管理和工作流自动化！



思科无线控制系统（WCS）的集中 WLAN 管理功能和简单明了的 GUI 可用于管理和设置思科无线定位设备，从而让安装过程变得非常迅速和直观。



网络拓扑和接入点被添加到该设备中，它就会生成 RF 预测和热点地图，在当地的建筑平面图上显示数千个设备的位置。

5.2.4 统一无线网络主要产品组合（参考）

- 工业用无线接入点 AP（LAP 与 AP 可以胖瘦灵活转换）

  - LAP / AP：1252（802.11a/b/g/n，外接天线)

  - LAP / AP：1262（802.11a/b/g/n，外接天线)

- CAP：3500e(802.11a/b/g/n，外接天线，支持 CleanAir 技术)

- 无线控制器 WLC（可以冗余配置、可以集群管理）

  - NME-AIR-WLC6-K9（ISR 无线控制器模块：支持 6 个 AP）
  - NME-AIR-WLC8-K9 （ISR 无线控制器模块：支持 8 个 AP）
  - NME-AIR-WLC12-K9 （ISR 无线控制器模块：支持 12 个 AP）
  - NME-AIR-WLC25-K9 （ISR 无线控制器模块：支持 25 个 AP）
  - AIR-WLC5508-X-K9（独立的无线控制器 5508：分别支持 12,25,50,100,250,500 个 AP，并可通过购买 License 升级支持的 AP 数量）

- 安全认证与管理服务器（可以冗余配置）

  - CSACS-5.0-EXP-K9（Cisco Secure ACS Express：软件）
  - CSACS-1120-K9（Cisco Secure ACS：软硬件一体）

- 无线网络管理（根据 AP 数量选择）

  - WCS-APBASE-50（50 个 AP 的无线网管）
  - WCS-APBASE-100（100 个 AP 的无线网管）

- 无线定位服务器

  - AIR-MSE-33xx-K9 及相应 License

5.3 协同通信系统－IPICS

5.3.1 IPICS 概况及对制造业企业的价值

思科 IP互操作性和协作系统(IPICS)是业界领先的智能网络系统，它将独立的无线对讲系统或双向语音通信系统，与其他语音、视频和数据网络相集成，支持多个网络、多个运营流程或多个机构之间的协作。思科IPICS为实时信息共享提供了一个灵活、动态且高度安全的通信互操作性和应用平台。它既有助于改善日常企业运营，也能有效支持紧急安全管理。思科IPICS的理念是，“在适当的时间以适当的格式为适当的人提供适当的信息”。

IPICS解决方案为制造业企业运营部门、安全部门和紧急事件管理人员提供了以下优势：

• 下一代通信互操作性系统架构。该架构支持语音、数据、视频和传感器网络在运营环境中的集成，提供全面的语音互操作性。

• 全面的语音互操作性—建立在思科智能化信息网络上的随处可达的无线对讲(PTT)特性。无需任何升级，即能实现与所有现有无线对讲网络的无线互操作性。这提供了无线对讲的应用移动性和网络永续性。

• 使用基于Web、直观、自适应的用户界面，根据角色、职责和策略（用户，调度员，操作员，管理员）来进行实时运营管理。

• 集中管理分布式网络资源和服务，以满足互操作性需求。

• 通过审查跟踪实现法规符合性、归档和培训。

思科IPICS能部署在移动指挥中心、总部、分支机构或运营中心。对于制造业企业来说，运用思科IPICS，能够集成独立的无线对讲系统和其他语音通信系统；改进运营的效率和灵活性；并简化机构决策制订过程。

5.3.2 IPICS 系统拓扑

思科IPICS提供了一个基于IP网络的系统级解决方案，来实现语音通信互操作性，并能无缝地从语音互操作性移植，集成其他的独立语音、视频和传感器网络。除提供可扩展性和投资保护外，思科IPICS充分利用IP标准和网络基础设施的优势，提供了更高永续性、可扩展性和安全性。

思科IPICS系统架构分三层，使我们能在适当的时间以适当的格式为适当的人提供适当的信息。

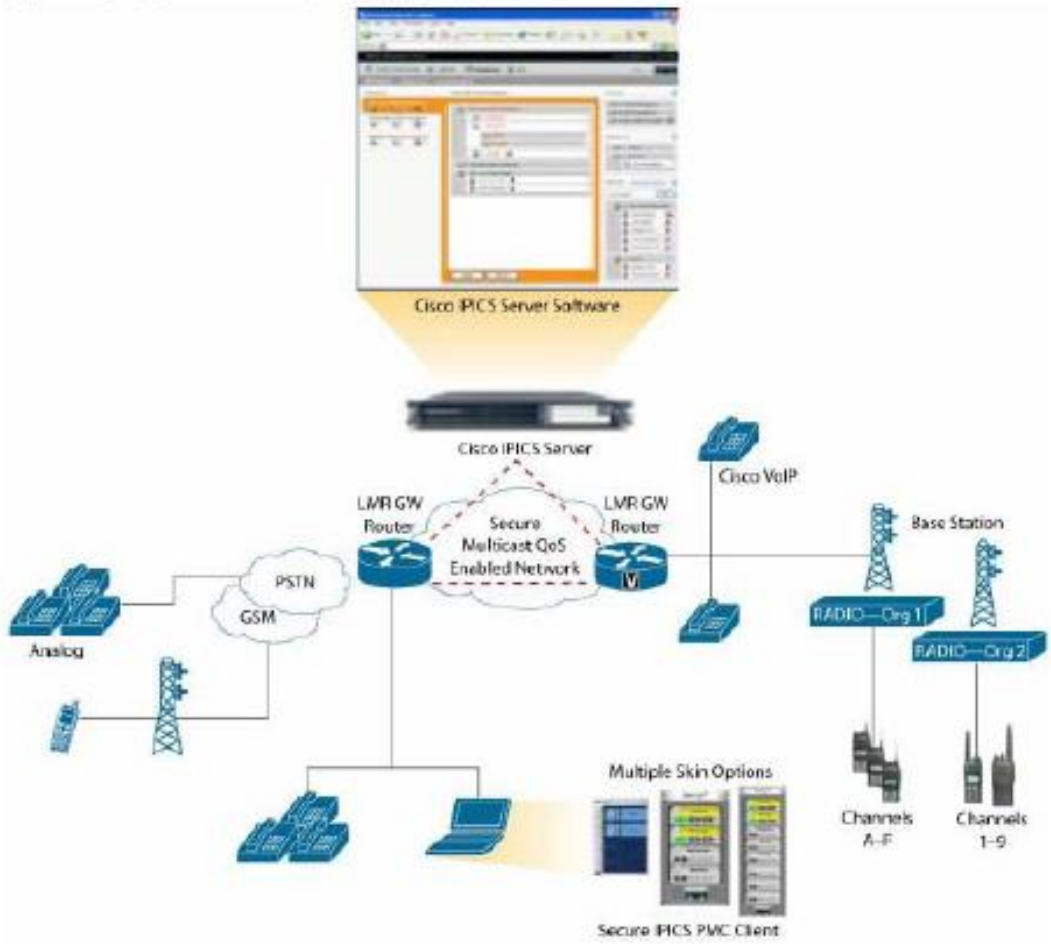
1）演示层是一个统一的应用套件，拥有一个直观的图形界面，根据用户的角色、职责和权限，以及设备的功能，提供相关信息。所提供的信息可能涉及多个网络、多个运营流程或多个机构。请注意在发生意外事件期间，根据运营的需要，角色可能会有所改变，以适应安全、性能和其他网络特性的要求。

2）思科IPICS服务器软件是此解决方案的核心，包括意外事件管理应用、策略引擎、数据库信息、身份验证和安全服务、用户管理以及其他后端功能。应用位于思科IPICS服务器上，能通过Web界面访问。思科IPICS软件还能集中管

理网络资源和控制层面功能，以满足特定事件或运营活动的互操作性需要。

3）思科智能化信息网络(IIN)为管理媒体资源和网关功能提供了分布式智能，能与传统网络或通信系统集成。该网络支持跨网络的关键服务，如安全、组播、QoS、移动、VOIP和高可用性等。通常VOIP电话、无线手机和基站、移动设备、计算机等终端设备与网络中的这一层相连。

图1. 思科IPICS网络部署架构



利用思科LMR网关和路由器，模拟无线流量将转换为IP流量，从而将无线可达性扩展到IP可达性，并保护传统无线系统的投资。每个无线信道都映射为一个IP组播地址。类似的，在hoot and holler系统中，每个通话组都映射为一个IP组播地址。使用IP设备，如支持PMC的思科IPICS PC的用户，能通过一个组播IP地址或通过一个采用SIP的单播远程连接，使用这些信道。

5.3.3 IPICS 系统的主要产品组合（参考）

- 运行在 MCS78**系列上的 IPICS 服务器
- Cisco Unified Communication Manager 8.0
- 语音网关：配备 E/M 模块的 ISR 路由器，用于接入无线对讲设备

6 思科统一计算及 C 系列服务器在制造业的应用

6.1 思科统一计算与虚拟化概述

当前，制造业企业数据中心存在着多种的生产业务应用系统，随着企业生产规模的不断扩大和生产技术的不断改进，越来越多的新业务、新应用将会部署到企业的数据中心。按照传统的数据中心部署模式，存在着各应用系统无法有效融合、设备重复投资、设备性能利用率不高、系统稳定性不一等问题。造成这些问题的其中一个主要原因是各种应用程序未能与执行它们的物理运算平台有效分离。而虚拟化技术正是解决这一问题的有效途径，通过把应用程序部署在一个多个统一的物理服务器资源池中，虚拟化能够带来以下的优势：

- 整合工作负载；提高利用率；降低运营、投资、空间、耗电和冷却等。
- 在虚拟池中动态地移动工作负载，提高使服务器离线或增加新服务器的灵活性。
- 管理虚拟机与物理机之间的关系，优化性能，保证服务水平。
- 使用现有资源池创建更多虚拟机，从而扩展当前应用或部署新应用。
- 使用虚拟化软件的高可用性和灾难恢复功能，来解决本地和跨地区故障问题。

思科统一计算系统就旨在提供这样一个环境。专为虚拟化环境而优化的思科统一计算系统是下一代数据中心平台，在一个紧密结合的系统中整合了计算、网络、存储接入与虚拟化功能，旨在降低总体拥有成本（TCO），同时提高业务灵活性。该系统包含一个低延时无丢包万兆以太网统一阵列，以及多台企业级 x86 架构服务器。它是一个集成的可扩展多机箱平台，在统一的管理域中管理所有资源。

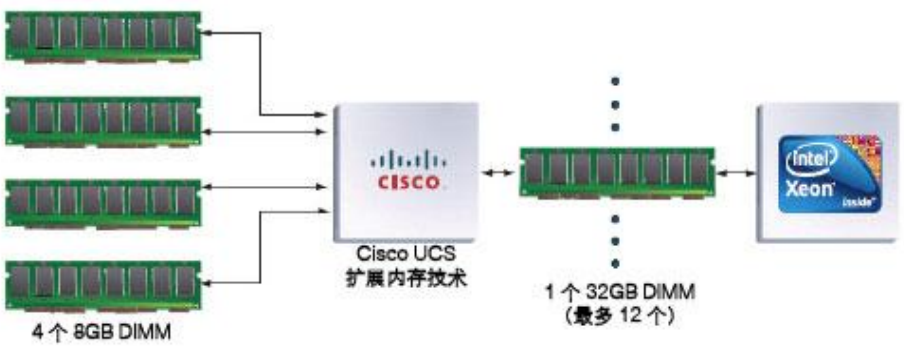
虚拟环境需要一致的 I/O 配置，为资源池中所有服务器的系统管理程序提供统一支持。它们还需要能够支持虚拟机（VM）在资源池中的各服务器间移动，同时又能满足各虚拟机带宽和安全要求的 I/O 配置。思科统一计算系统以一个低延时无丢包的 10-Gbps 统一网络阵列为基础，能够满足这一需要。此统一阵列不再需要在每个服务器中部署冗余以太网和光纤通道适配器，也不必采用独立布线连接接入层交换机，并为每种网络媒体使用不同

交换机，因此大大简化了机架布线。所有流量都路由到中央服务器互联，随后以太网和光纤通道流量可独立传输到本地非整合网络。

当服务器配置到资源池中以后，便可以根据需要进行管理，以满足不断变化的工作负载要求；在部署新应用时无需为其安装特定硬件；并能在服务器间移动虚拟机，以均衡工作负载、满足服务水平协议(SLA)或使某个服务器为计划内停机作好准备时，虚拟化能为数据中心发挥最大价值。Cisco UCS Manager 将思科统一计算系统的资源整合为单一综合系统，非常适于为虚拟环境建立资源池。

Cisco UCS Manager 是思科统一计算系统的中枢神经系统。它从端到端集成系统组件，因此系统能作为单一逻辑实体进行管理。Cisco UCS Manager 提供一个直观 GUI、一个命令行界面(CLI)和一个强大的 API，因此它能单独使用，也能与其他第三方工具集成使用。通过单一控制台，能够全方位管理服务器配置－系统身份、固件版本、网卡(NIC)设置、HBA 设置和网络配置文件等，无需每个系统组件配备单独的管理器。

虚拟化将更多关注服务器如何拥有更多以及更经济的内存配置，思科独创的扩展内存技术提供了最佳的解决方案。采用了思科扩展内存技术的 UCS C250 M1 机架式服务器将四个物理上独立的 DIMM 映射为单一逻辑 DIMM，在使用 8-GB DIMM 时最大内存高达 384 GB，从而能以更低 TCO 提高虚拟化密度，使企业的 IT 机构能够凭借更少资源完成更多任务。



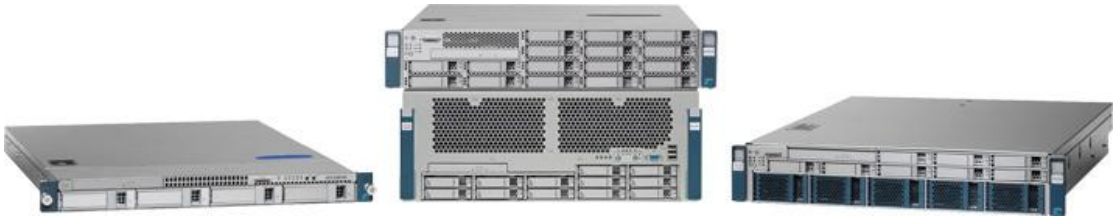
（图）思科扩展内存技术使 4 个物理 DIMM 对于 CPU 来说显示为单一大型逻辑 DIMM

思科统一计算系统将计算、网络、存储访问和虚拟化统一到一个综合平台中，进行集中管理，并使用 VMware ESX 服务器等虚拟化软件进行协协调。该系统在一个万兆以太网统一阵列中集成了企业级服务器，提供了虚拟机和虚拟化软件所需的 I/O 带宽和功能。思

科扩展内存技术为高度虚拟化所需要的大内存提供了一种极为经济的配置方法。最后，思科统一计算系统将网络访问层集成为一个能轻松管理的实体，在此实体中，能像物理链路一样配置、管理和移动虚拟机链路。

6.2 思科 C 系列机架式服务器的应用

Cisco UCS C 系列机架安装服务器将思科统一计算系统创新技术扩展到了机架安装机型，包括一个基于标准的统一网络阵列、Cisco VN-Link 虚拟化支持和思科扩展内存技术。这些服务器既能在独立环境中运行，也能作为思科统一计算系统的一部分运行，使企业用户能够逐步部署系统，也就是按照最适合的预算方式和时间安排来决定所用服务器的数量。



按照中小型企业的应用特点，数据中心服务器的部署和使用可以分为两个阶段：

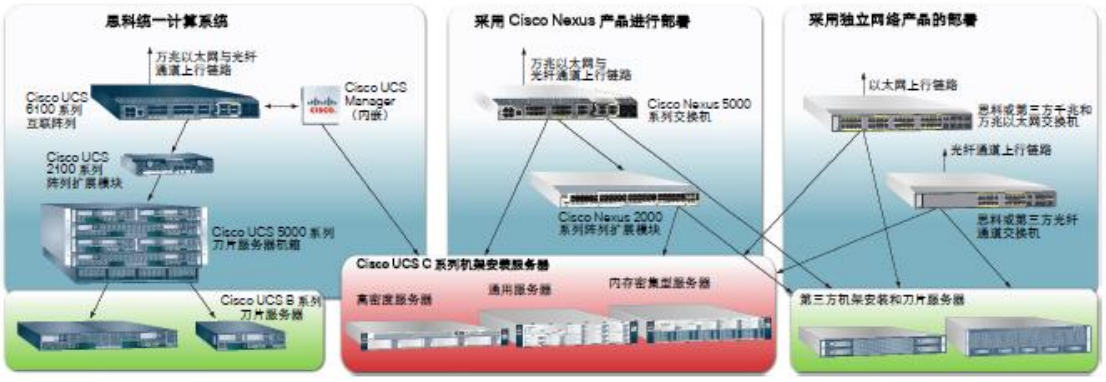
首先，在现阶段应用相对简单、投资预算有限的条件下，独立部署 Cisco UCS C 系列服务器，在异构环境中提供业界标准的管理和应用特性。

当作为独立服务器部署在异构环境中时，Cisco UCS C 系列服务器能像其他任何 x86 架构服务器一样进行管理。无需修改，即能运行使用 OS 主机代理的常用企业管理工具。Cisco UCS 集成管理控制器为管理员提供了所需工具，帮助他们以手动操作的方式控制服务器功能，包括远程键盘、视频和鼠标（KVM），电源开关，以及用于系统监控的标准 SNMP 陷阱。

第二，在未来，随着企业信息化的进一步发展，C 系列服务器可以作为思科统一计算系统的一部分，提供了出色的投资保护。

C 系列服务器能够与思科统一计算系统集成，成为单一综合系统的一部分，由一个集成、内嵌、高度可用的安全管理系统管理。该系统采用与机型无关的架构，在资源使用方面提供了出色灵活性。Cisco UCS C 系列服务器能够根据需要在思科统一计算系统中调整配置，且能在该系统中与 Cisco UCS B 系列刀片服务器一起运行。

使用这种分阶段的模式，企业能够按照自身的发展时机和预算情况，逐步部署系统，根据需要选择服务器数量。C 系列这种灵活的设计使其能够适用于广泛的数据中心环境，包括使用思科统一计算系统、Cisco Nexus 系列产品、以及来自思科和第三方的独立以太网与光纤通道交换机的环境。



图：C 系列服务器在各种数据中心环境下的灵活部署

与传统的机架式服务器相比，思科C 系列在广泛的应用环境下提供了多种独特的优势，包括：

- Cisco 扩展内存技术

相比传统的双路 CPU 服务器， 这一技术可带来两倍的内存空间（ 384GB），并能够通过使用 4 GB 而非 8 GB DIMM 实现更为经济的（192 GB）内存空间。它用于针对虚拟化和大数据集工作负载的需求，在处理能力与内存容量之间实现最佳平衡，让企业无需再为了提供更大内存空间而升级到昂贵的四路 CPU 服务器。同时，它还能够帮助降低资本开支与运营成本。

- 灵活的 I/O 与存储选件

该服务器拥有 5 个 PCI Express（PCIe）扩展插槽，提供了出色的 I/O 灵活性和带宽，能够全面集成传统千兆以太网 LAN 和光纤通道 SAN。服务器配备了多达 8 个内部小型（SFF）SAS 或 SATA 驱动器，其内部存储容量远远高于同类刀片外形服务器所能提供的水平。

- 万兆统一网络阵列

当配备了融合网络接口（CNA）或 Cisco UCS P81E 虚拟接口卡时，该服务器可以集成低延时无丢包 10 Gbps 以太网与工业标准以太网光纤通道（FCoE）阵列。这一技术支持“一次布线部署模式”，这意味着变更 I/O 配置不再需要安装相应的板卡，并对机架及交换机重新布线。

- 虚拟化优化

思科 VN-Link 技术、I/O 虚拟化和 Intel® Xeon® 5500 系列处理器将网络直接延伸到虚拟机。这一优化能够支持实现一致、可扩展的操作模式，帮助提高安全性和效率，同时降低复杂性。

- 统一管理

当集成至思科统一计算系统作为其一部分使用时，管理功能将被集成到系统的所有组件之中，通过 Cisco UCS Manager，管理整个解决方案就像管理一个单一实体一样，从而显著提高运营效率与灵活性。

- 服务配置文件

当集成作为思科统一计算系统的一部分时，Cisco UCS Manager 可使用服务配置文件和模板实施基于角色与策略的管理。服务配置文件可帮助自动化配置和增加业务灵活性，让数据中心经理能够在短短几分钟内完成应用配置，无需再花费几天的时间。

常用的思科统一计算 C 系列机架式服务器如下：

产品系列	说明
Cisco UCS C200 M2	2 路服务器，部署通用计算
Cisco UCS C210 M2	2 路服务器，部署通用计算
Cisco UCS C250 M2	2 路服务器，内存增强型应用，部署高密度虚拟机
Cisco UCS C460 M1	4 路服务器，CPU/内存增强型，部署关键业务/高可

	靠应用

7 结束语 制造行业用户为什么选择思科

思科企业级高质量、高稳定、技术先进的网络设备和解决方案，保障企业业务高可靠地运行，得到了业界的广泛认可。思科产品以其先进的软、硬件设计，针对用户需求的研发方向，大量的研发投入和先进的生产质量控制等成为最高质量和最稳定的网络设备和解决方案，这也通过大量的企业行业、金融行业和证券行业等用户的使用实践所证明，在这些对网络可靠性要求极高的行业中思科都具有大量的成功案例和极高的市场占有率。

思科具有大量的企业行业用户成功案例和丰富的企业网络建设经验。鉴于思科产品的在行业内的领先地位和技术先进性，思科在全球制造业企业中拥有大量的成功案例。思科拥有在国内外大量的制造业客户网络建设的实践基础，了解企业的应用和发展趋势，了解企业信息系统需要解决的问题，并拥有完整、独特、领先、有针对性的技术解决方案，因而具有丰富的企业网络建设经验，思科通过解决方案的形式将这些经验分享给制造业的用户，为企业网络建设提供咨询服务。

思科拥有全面的解决方案，满足企业现在和未来信息化建设发展的需求。思科是业界领先的提供承载生命的信息系统——企业信息系统整体网络解决方案的厂商，我们不但能够提供适合企业业务系统的高可靠、安全智能的基础网络系统，还能提供满足企业全面信息化建设需要的统一通信、统一无线、自适应网络安全和新型企业数据中心等全面的解决方案，思科在以上解决方案方面拥有丰富成熟的国内外建设和应用的成功案例经验可以供国内制造业用户参考。

思科是业界专注于网络且具有很强生命力的厂商，可以为企业行业用户提供持续不断的技术支持、技术升级和售后服务。思科是全球网络和通信领域公认领先的互联网解决方案供应商，思科在全球的网络市场占有率及国内企业行业的市场占有率都是遥遥领先的，财富五百强中 89％是思科的用户，全球电信用户95%是思科的用户。思科通过不断的技术创新，一直以来都是网络行业具有很强

生命力的引领网络发展方向的主流厂商。思科公司运营稳定持续增长，过去的一年思科的收入为 395 亿美金，研发投入 52 亿美金，思科公司的稳定发展和大量的研发投入，可以保障为制造业用户提供持续不断的技术支持、技术升级和售后服务。

思科非常重视制造业用户的投资保护，使制造业用户具有较低的网络总体拥有成本。如何更好的实现客户的投资保护一向是指导和修正思科产品研发和创新的指导思想之一，因此采用思科的整体方案具有较低的长期拥有成本（包括初次购买、运营维护管理、网络扩展、技术升级费用的总和），并能够通过减少宕机时间，使网络正常工作时间最大化，有力地支撑企业业务在网络上不间断地运行，避免给企业带来声誉和财务上的损失，并且提高企业服务质量。思科产品具有顽强的生命周期，比如：思科 1999 年开发推出的 Catalyst 6500 平台，其中的模块和接口板现今仍然能够在最新一代的 Catalyst 6500 平台上使用。目前全球有很多知名企业采用了思科的双 Catalyst 6500 交换机作为网络的核心交换机，为保证这些企业网络的可靠工作发挥了重要作用。

思科公司高效的服务体系，是制造业用户网络安全可靠运行的重要保障。思科公司秉承“服务至上”的原则，开发了独具特色的全球支持模式，通过互联网为用户打开了取之不尽、用之不竭的支持资源库，帮助用户妥善解决在整个网络生命周期内遇到的各种网络问题。为了响应中国市场不断提升的网络服务需求，对中国本地客户提供更加全面和直接的支持，2006 年 5 月，思科系统公司在北京注册成立了思科系统（中国）信息技术服务有限公司，专注于为中国客户提供全面的网络生命周期服务，帮助用户对网络进行规划、设计、实施、运营和优化，以成功部署和使用网络技术，为思科向包括制造业在内的中国客户提供高效优质的服务提供了强有力的支持。思科还将继续在资金投入、技术引进、原料采购和生产等各个方面加大对中国市场的投入。

客户满意是验证思科服务的最佳标准，思科愿意在大量的国内外制造业网络建设实践的基础上，向制造业的用户学习，并愿意分享在此过程中不断积累的丰富的企业信息化建设经验，思科将一如既往地与中国企业用户共同迎接网络经济的美好机遇，进一步推动中国企业信息化建设进程。