网际操作系统

www.cisco.com

Cisco

网际操作系统

Cisco Systems

Empowering the Internet Generation℠

Cisco 网际操作系统

本手册概要

本单元的主题是介绍 Cisco 网际操作系统(IOS)。我们将复习 IOS 的框架及核心特性，并探讨 IOS 如何满足特定的技术和商务要求。这里将不再详细介绍具体的特性，而是就安全、服务质量(QoS)、VLANs、流量管理及协议处理等方面的特性来讨论 IOS。IOS 将作为提高 Cisco 市场竞争优势的一项核心技术。

本手册主要内容简介

1. 了解 Cisco 对其网际操作系统(IOS)品牌产品的定义。
2. 介绍 Cisco 如何向互联网络市场推广其 IOS 体系结构的主要优点。
3. 介绍 IOS 体系结构中的核心服务和网络服务的角色。
4. 介绍 IOS 软件的 4 个主要发展阶段。
5. 介绍 IOS 特性集(feature Sets)和 IOS 解决方案集(Solution Sets)之间的区别。
6. 针对一些特定的网际技术要求，如压缩、协议转换、带宽优化等等，介绍 IOS 满足这些需求的相应特性，以及它们在应用的解决方案中如何作用。
7. 了解满足互联网络内服务质量(QoS)要求的 IOS 特性。
8. 了解满足互联网络内企业级安全需求的 IOS 特性。
9. 了解满足互联网络内企业级 VLANs 需求的 IOS 特性。
10. 了解满足企业级流量管理需求的 IOS 特性。
11. 了解满足互联网络内企业级协议处理需求的 IOS 特性。
12. 介绍 Cisco 的 IOS 使其具有市场竞争优势的几个原因。
13. 介绍 Cisco 推广其 IOS 体系结构而主要围绕的 5 个特性域，并描述了每一个域相应的特定 IOS 特性。

Cisco 网际操作系统(IOS)

IOS 定义

Cisco的网际操作系统(IOS)是一个为网际互连优化的复杂的操作系统 —— 类似一个局域网操作系统(NOS)，如 Novell 的 NetWare，为 LANs 而进行优化。IOS为长时间经济有效地维护一个互联网络提供了统一的规则。简而言之，它是一个与硬件分离的软件体系结构，随网络技术的不断发展，可动态地升级以适应不断变化的技术(硬件和软件)。IOS 可以被视作一个网际互连中枢：一个高度智能的管理员，负责管理和控制复杂的分布式网络资源和功能。

IOS 模块性

IOS 是 Cisco 路由软件的初始品牌名称。随着 Cisco 技术的发展，IOS 不断扩展，成为 Cisco Central Engineering (中央工程部门) 所称之为的“一系列紧密连接的网际互连软件产品”。尽管在其品牌名识别中，IOS 可能仍然等同于路由软件，但是它的持续发展已经使之过渡到支持局域网和 ATM 交换机，并为网络管理应用提供重要的代理功能。必须强调的是，IOS 是 Cisco 开发的技术：一项企业资产。它给公司提供独特的市场竞争优势。目前许多竞争者许可 IOS 在其集线器和路由模块内运行，IOS 已经广泛成为网际互连软件事实上的工业标准。

Cisco IOS 的优点

灵活性

基于 Cisco 产品的工程开发以及用户可以获得适应变化的灵活性。IOS 软件提供一个可扩展的平台，Cisco 会随着需求和技术的发展集成新的功能。Cisco 可以更快地将新产品投向市场，我们的客户可以享用这种优势。

可伸缩性

IOS 遍布网际互连市场；广泛的 Cisco 合作伙伴及竞争者在他们的产品上支持 IOS。IOS 软件体系结构还允许其集成构造企业互联网络的所有部分。Cisco 已经定义了 4 个:

- 核心 / 中枢：网络中枢和 WAN 服务，包括大型骨干网路由器和 ATM 交换机。
- 工作组：从共享型局域网移植到局域网交换(VLANs 提供更优的网络分段和性能。)
- 远程访问：远程局域网连接解决方案：边际路由器、调制解调器等。
- IBM 网际互连：SNA 和 LAN 并行集成，从 SNA 转换到 IP。

Cisco 的 IOS 扩展了所有这些领域，提供了支持端到端网际互连的稳健性。

可操作性

IOS 提供最广泛的基于标准的物理和逻辑协议接口 —— 超过业界任何其他供应商：从双绞线到光纤，从局域网到园区网到广域网，Novell NetWare，UNIX，SNA 以及其他许多接口。即是说，一个围绕 IOS 建立的网络将支持非常广泛的应用。而且，Cisco 还一直是一个业界标准先驱，是许多知名业界标准机构(例如 IETF、ATM 论坛等)的积极成员和支持者。

可管理性

IOS 是 Cisco 将嵌入式智能植入网络设备：管理界面，例如 IOS 诊断界面，以及智能网络应用的代理软件，允许用于监视和排除广泛的网络设备的故障。随着 Cisco 转向智能代理和基于策略的自动化管理的大规模部署，IOS 将作为一个关键的技术组件。

投资保护(以及随时间推移降低拥有成本)

IOS 为客户提供信息基础设施的投资保护。IOS 今天支持的许多特性是大多数客户未来需要的特性。随着一家公司的成长和扩展到新的领地，随着兼并收购带来的基础机构复杂性以及协议转换或新流量模式的出现，IOS 提供的体系结构能使机构灵活地适应变化和经济有效地进行扩展以满足新的需求。IOS 允许我们的客户迅速调节适应新的模式，更长时间地保持其信息基础机构投资：其结果是随时间推移提供投资保护和降低拥有成本。

Cisco IOS 设计目标

IOS 设计目标

IOS 是围绕下列目标设计的:

- 模块性：IOS 为大量的协议和协议族提供支持，运行于多平台并坚持独立于硬件的设计标准(硬件隔离)。
- 速度最快：IOS 能使 Cisco 为网络协议提供最快的平台实现。
- 网际互连：IOS 支持包括路由、桥接和交换技术的需求。
- 高性能多平台：IOS 由多个 RISC 处理器体系结构(MIPS Rxxxx、Motorola 680xx)支持。
- 分布式：IOS 为分布式体系结构的部署提供基础。
- 环境：IOS 提供一个支持大型企业需求的软件开发环境。

多维支持

IOS 为 LAN 介质，WAN 协议，以及各种功能，包括路由、交换、信令、IBM、协议转换及许多其他服务提供支持。

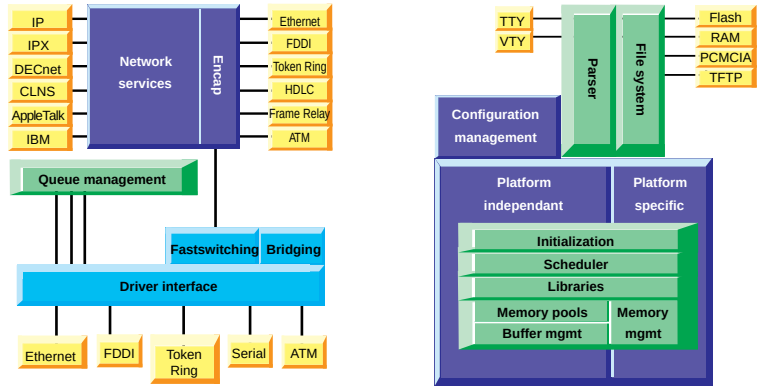
设计结果

IOS 设计为客户提供完成下列任务的能力:

- 建立特大规模的网络。
- 在远程访问链接中，维护多协议支持。
- 全面集成 IBM/SNA 和互联网络环境。
- 开发基于 IOS 功能的广泛的安全策略。
- 在互联网络内设计和维护优良的流量控制和服务质量参数。
- 优化网络带宽和操作资源。
- 支持互联网络上的多媒体应用。

Cisco IOS 体系结构

固态体系结构



IOS Solid State Architecture

核心服务和网络服务

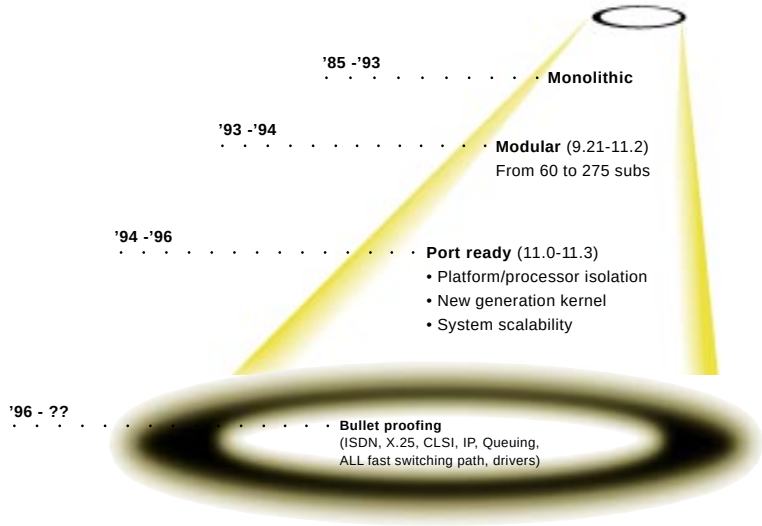
IOS 体系结构能够提供两种基本服务：核心服务和网络服务。IOS 核心服务提供实现 IOS 的多平台可移植性和可伸缩性所必需的所有功能。网络服务则是构筑于核心服务之上的所有功能服务，提供IOS 网际互连特性。例如，Classified under Network Services(网络服务下的分类)是连接局域网、广域网介质和协议以及桥接、交换服务及服务质量特性(例如协议封装和队列管理)的接口。核心服务可以被视作提供基本 IOS 工程参考平台，而网络服务则包括所有驻留在操作系统之上的增值特性。

Cisco IOS 发展历程

IOS 开发历史

模块化到多链接子系统结合

下图介绍了 IOS 从一个统一的操作系统到目前高度模块化操作系统的发展历程。



IOS Evolution

统一的

IOS 的早期版本是一个单独系统，基本上以路由器为中心。它被排列成一个过程(Procedure)集，允许任何过程之间相互呼叫。这种单一的结构使数据的隐蔽性和独立性不强；它的大多数操作代码拥有结构和操作的相关性。

模块化

IOS Releases 9.21 到 11.2 反映了将 IOS 重新设计成模块化组件或子系统的努力。每一个子系统被组织成一个层集(set of layers)，提供一个进入系统代码的独立入口点。子系统本身被定义为独立的模块，支持嵌入式(核心)系统的各种功能。这种分层的子系统设计允许工程人员将 IOS 划分成更可管理和更易于升级的特性集。

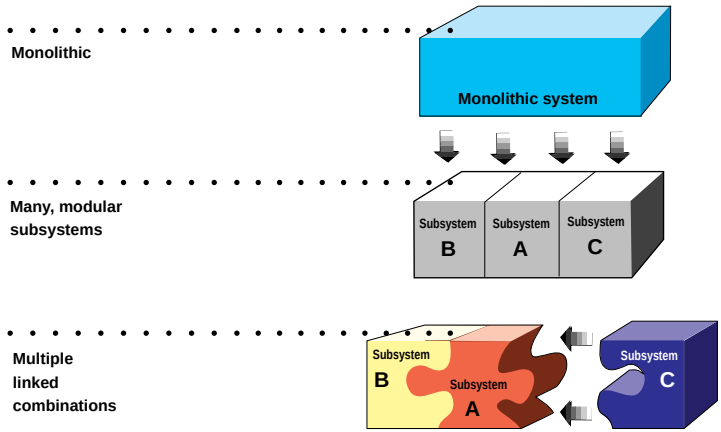
终极目标

IOS 向可移植化的发展表明，IOS 11.3 及更高版本更易于移植到新的平台。

Bulletproofing

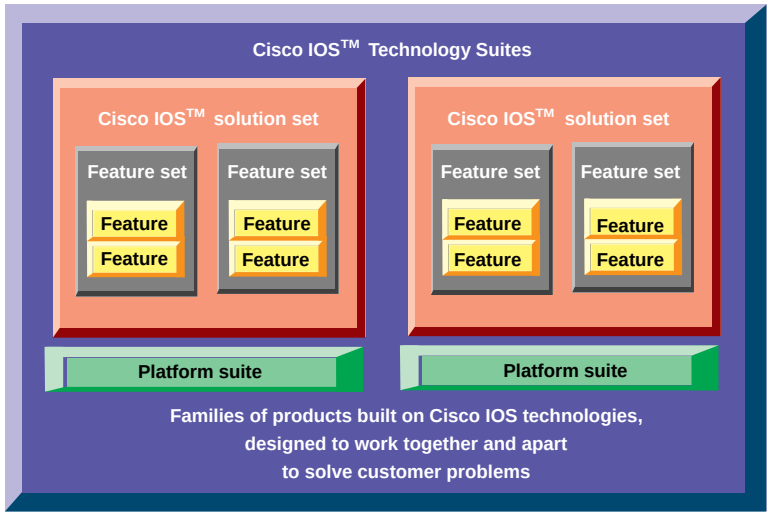
最终的目标是将 IOS 发展为静态的更为高级的模块化结构，它允许单独定义 IOS 特性而与其它特性(或子系统)不相关。Cisco 可根据客户的特定需求建立 IOS 特性 / 解决方案集。随着 IOS 继续发展，客户将能够混合和匹配专门的 IOS 特性，来满足其特定环境的要求。

模块化到
多链接子系统结合



IOS Modularity: Multiple Linked Combinations

解决方案集



IOS Solution Sets

从 IOS Granularity 到特性级

上图总结了 IOS 向解决方案集的发展过程。由于许多专门的网络服务特性已经从 IOS 核心分离，因而解决方案集是可能的。尽管 Cisco 目前能够提供它所说的特性集－例如企业特性集或桌面特性集，但是这些都是受到 IOS 核心和子系统相关性限制的预封装解决方案。随着解决方案集的发展，它们将获得更加高级的层次地位：作为专门的特性实体，而不是作为核心或子系统定义去发展(不过，一般总会有某些级别的子系统定义)。

解决方案集包括客户能够混合和匹配的特定特性，提供以下主要优点:

客户为重点的解决方案

- IOS 成为一种以客户为重点的技术；它提供专门满足客户主要的技术及商业需求的网际互连功能和特性。客户可以在 IOS 基本平台之上有效地设计他们自己的特性体系结构。

可伸缩性和投资保护

- 由于客户仅选择满足他们要求所需的核心特性，因此可以大幅度降低 IOS 开销。IOS 可以利用客户现有的硬件和基础设施投资进行更好地扩展，从而提供投资保护以及更好的网络寿命周期拥有成本。

降低复杂性

- IOS 复杂性降低，并进而带来客户互联网络复杂性的降低。由于 IOS 系统及特性间相关性减少，因此解决方案集有助于使统一系统中可能发生的并行损害最小化。实际上，许多与一个全面特性 IOS 的实现相关的要求都可以实现最小化。

Cisco IOS 框架

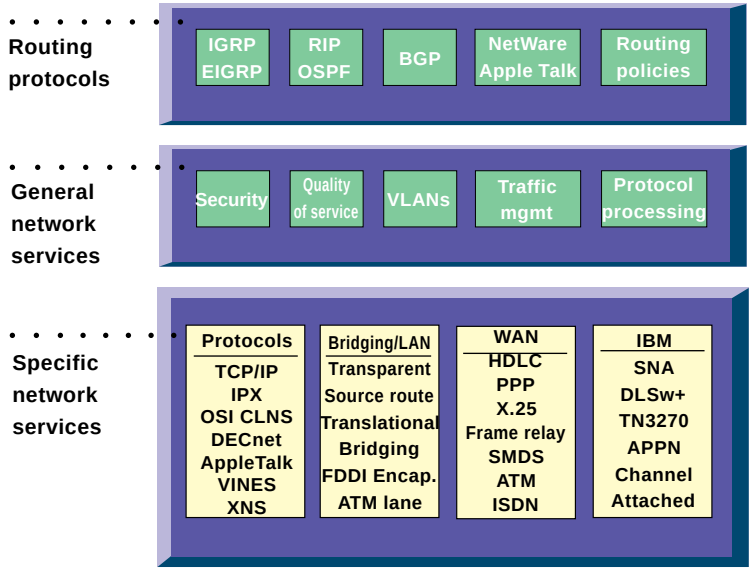
专用网络服务

IOS 可以概念化为一个操作系统，为一个全面的协议族提供全面的网络服务。网络服务可以被分成许多不同的功能；下图将它们分成通用和专用服务。专用服务包括交换、路由以及几乎适用于跨局域网、广域网和 IBM/SNA 环境的所有数据联网协议的专门化服务。

通用网络服务

通用网络服务包括支持 IOS 体系结构的增值功能，并提供企业级解决方案，来满足客户对安全、服务质量、VLANs 配置管理和路由以及(通信)流量管理的需求，进而提高网络性能和可靠性。通用网络服务还提供协议处理服务，例如转换、加密和压缩。

Cisco IOS 框架



Cisco IOS Framework

路由协议

通过网络互联，IOS 支持许多路径恢复协议以及其他路由协议特性供基于政策的路由配置和管理。

从这里开始到本单元结束，我们将与其通用网络服务(已在前面的图形中作过概述)联系起来介绍 IOS。我们将非常详细地讨论下列每一个领域:

安全

- 安全：重点强调特性要求，例如通过防火墙提供的资源保护，访问控制，以及与用户验证机制(例如锁定和密钥安全)的集成。

服务质量

- 服务质量：介绍在互联网内提供服务质量的 IOS 特性和功能。服务质量对多媒体应用程序支持至关重要。这里所讨论的 IOS 特性包括几种排队机制(这些可能在流量管理部分讨论)和资源保护协议(RSVP)。

虚拟局域网

- VLANs: 简要介绍Cisco在VLANs配置中部署路由和交换的IOS支持。

流量管理

- 流量管理: 包括根据用户(来源和目的地)、局域网和广域网记帐以及RMON 标准支持进行的流量模式测量。一般来说，流量管理是在网络管理单元作概要介绍。本部分将讨论 Cisco 的 NetFlow Switching(尽管理论上说可能属于服务质量部分)。

协议处理

- 协议处理: 介绍多媒体和协议类型的集成、协议转换、加密和压缩以及 IBM SNA 和 TCP/IP 网际互连(取决于多协议路由和转换)的一般类别。SNA 和 TCP/IP 集成在 InterWorks Business Unit 部分讨论。本部分将围绕压缩和协议转换介绍 IOS 特性。

总结

作为本单元的一个总结，我们将提供IOS 市场模型。该模型包括5 个功能性领域，所有领域都有许多相关的特性。它简单地提供了在一个网际互连解决方案的上下文内定位 IOS 特性的另一种方法。

Cisco IOS 通用网络服务: 安全

安全介绍

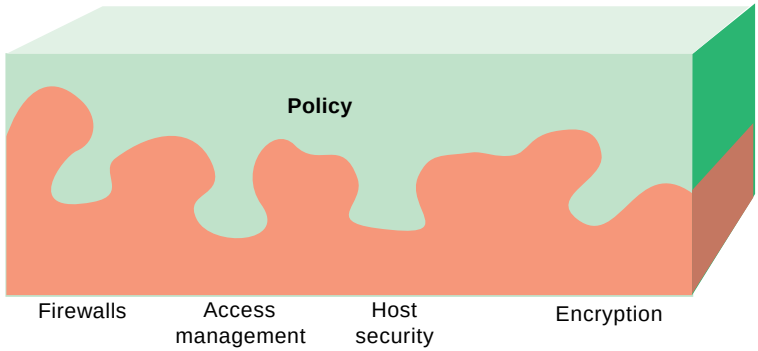
Cisco 从几个方面考虑安全问题。在企业设备中，安全通常基于安全保护、闭路电视和卡密钥入口系统。有了这些措施，企业可以放心，他们的物理及智力资产将得到保护。Cisco 的安全方案允许企业通过使用基于政策的组件及 IOS 安全体系结构，来扩展这一模型。IOS 安全体系机构已经经过 10 多年的技术革新发展历程，它为企业的安全政策提供基础。IOS 安全基于多个重叠的解决方案，这些解决方案一起维护企业的安全完整性。

访问安全与工作效率

企业必须决定何时在用户的访问和工作效率与可能被用户视为限制的安全措施之间进行折衷。一方是访问和工作效率，另一方是安全。一

个好的设计的目标是提供一个平衡，同时从用户的角度看尽可能少增加限制。有些非常合理的安全措施，例如加密，不限制访问和效率。另一方面，低劣的安全计划可能造成用户效率和性能的降低。那么，企业在维护安全的努力中要冒多大的访问和效率风险呢?

Cisco IOS 安全体系结构



IOS Security Architecture

防火墙

Cisco 通过建议客户首先定义他们的安全政策来解决这一问题。一旦定义了这些政策, 就可以采用多个安全组件来满足政策要求。Cisco IOS安全体系机构的组件包括: 防火墙、访问管理、宿主安全、加密。

过去几年, 路由器一般是企业的智力资产与其网络之间的唯一东西。路由器被独特地定位、设计和配备，以用来在各种级别的开放系统互连(例如 OSI reference model)模型中控制及报告数据包流。随着今天网络的可访问性及功能的提高, 以及公司通过经济有效的远程访问设备连接, 风险程度逐步降低。如果一个路由器被安排提供网络外围安全，那么它

通常是指“防火墙路由器”。防火墙路由器内维护访问控制目录(ACL)，ACL的主要功能是提供过滤。IOS安全提供大量的工具来帮助报告ACL违规(即非法访问):

ACL 违规记帐

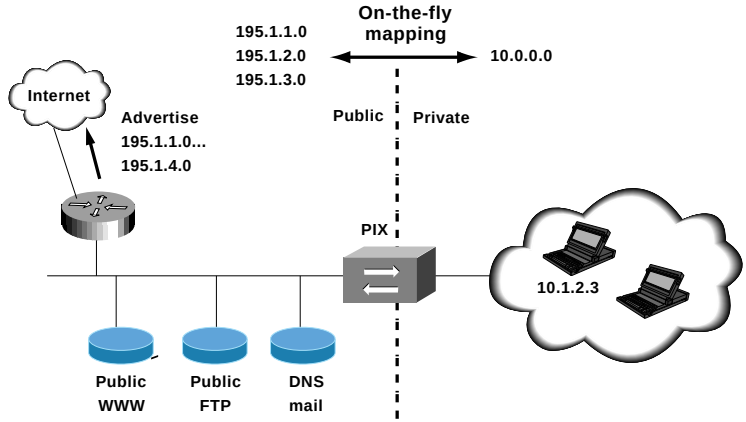
- ACL 违规记帐: 随着时间的推移，企业需要一个历史透视图来弄清哪些ACL 已经经过测试。这种知识给网络管理人员提供了对入侵者是如何尝试进入其企业网络的一个了解。ACL 违规记帐提供来源和目的地地址信息、来源和目的地端口号码以及包个数。

ACL 违规日志记录

- ACL 违规日志记录: 在今天的网络世界，提供强大的防火墙功能已不足以解决问题，网络管理人员需要一个集中化报告选项。过去，网络管理人员在发生损害之前不知道他们已经受到黑客的攻击。唯一可用的早期告警工具是扫瞄主机日志文件。尽管这仍然是一种优异的安全诊断方法，但是它不能很好地扩展。ACL 报告工具通过提供违规信息和网络周边预防，给管理人员提供帮助。IOS包含ACL 违规日志记录，给管理人员提供定期的系统日志记录，可以实时确定 ACL 违规。

网络地址转换

网络地址转换(NAT): 与全球 Internet 连接的网络数量急剧增加，造成了未来连接可用地址的迅速消耗。而 World Wide Web 对这种耗尽又起到了推波助澜的作用；而 Internet 正以每年 30%到 50%的速度发展。根据目前的估计，3 到 10 年内，剩下的所有 Internet 地址将全部用完。



Firewall Design with Private Internet Exchange

Cisco NAT 实现

Cisco NAT 的实现基于 Network Translation 公司的 Private Internet Exchange(PIX)，它通过维持“状态”提供自适应的应用安全。动态的地址转换仅为从内部网启动的连接而实现，而且有特定端口。例如，一个来自 WWW 客户机的超文本传输协议(HTTP)连接的转换仅转发来自外部 WWW 服务器的数据包，目的地是客户机的 80 端口。在 FTP(为其数据连接使用一个暂时端口)情况下，NAT记录由客户请求被动打开的端口号码，且对于从专用网内部启动的对话期来说，仅允许入站 FTP 数据。保持通过 NAT 技术建立的每一个 TCP 连接的状态信息，就可以实现这种级别的选择性。在转换入口有效期间，将为之保持一个包含目的地地址、端口号码、排序信息、字节数以及与特定主机地址转换相关的每一个TCP连接的内部标记的表。入站(数据)包与连接表中的入口相比较，并且只有在存在适当的连接使他们的传递生效时才被允许通过 NAT。因而， NAT 没有额外的管理开销，无需专门的客户机软件，就能够提供一个代理服务器的功能。典型的代理服务器以用户级在一个多用户操作系统上运行，并通过复制不同 TCP 连接之间的数据操作。Cisco 实现直接在数据包上操作，因而大大提高了性能。

访问管理

访问管理控制方法、方案以及资源的发布，并提供监督和控制。企业正面临管理主机和网络设备以及远程计算机的挑战。关键是给网络管理人员提供控制访问的多种方法。访问管理是Cisco IOS安全体系机构的一个重要方面。为了满足大量的访问要求，Cisco IOS安全体系结构为客户提供广泛的访问管理功能。

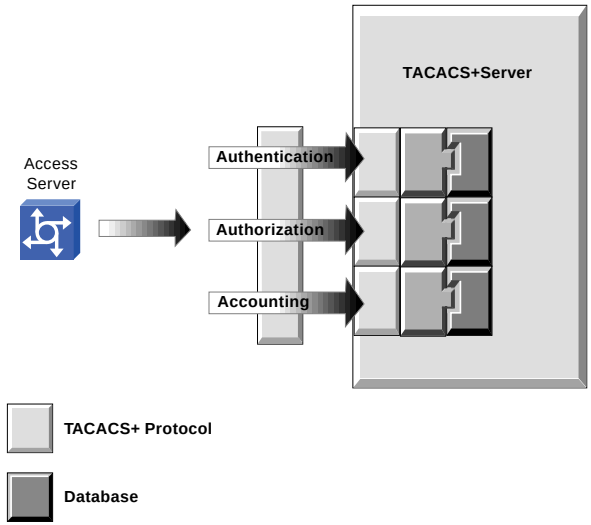
Message Digest 5

Internet的发展增加了改进路由信息验证的需求，特别是在服务供应商和拥有关键任务网络的客户之间。Message Digest 5(MD5)验证(RFC 1321)可用于边缘网关协议(BGP)和Open Shortest Path First(开放的最短路径优先OSPF)，它提供了一种基于标准的方法，大大增强了Cisco IOS软件检测和放弃敌意或错误的路由信息的可能性。Cisco的实现基于Internet Engineering Task Force(IETF)标准推荐。客户将获得针对伪造或修改信息的保护。这大大减少了对网络路由器的攻击机会，并保护更新信息免遭破坏。

TACACS ＋

终端访问控制器访问控制系统(TACACS)为在用户能接入路由器或访问服务器之前集中地确认各个不同用户提供了一种方法。TACACS源自美国国防部，并在RFC 1492中有说明。IOS软件实现TACACS，允许对何人能够访问路由器和服务器实行集中控制。Cisco还支持TACACS的一个全新版本－TACACS ＋。TACACS ＋提供独立和模块化的验证、授权以及记帐设备。TACACS ＋允许一个单一访问控制服务器(TACACS+服务器)独立提供每一项服务。每一项服务都可以被连接进其自己的数据库，从而利用该服务器或网络上的其他服务。TACACS＋的总体目标是为管理不同的网络访问服务器提供一种方法。

TACACS ＋服务器



TACACS+ Server

3 A 级设备

- 验证：提供在登录和口令对话之外验证用户的能力。管理员可以通过例行性地改变问题，改进对话完整性。TACACS＋验证服务非常灵活，可以向用户屏幕发送消息。例如，一条消息可能告诉用户，由于公司的口令老化政策，他们的口令需要改变。TACACS ＋协议提供访问服务器和 TACACS ＋服务器之间的验证，并确保数据包的机密性。
- 授权：TACACS ＋中的授权组件允许对用户行为进行更大程度的控制，并可以根据用户的功能创建独立的管理组。例如，网络管理人员可以限制一个用户在访问服务器或路由器的用户界面上仅执行某些功能。
- 记帐：网络管理人员可以使用记帐组件跟踪用户活动，以进行安全审计，或者提供用户记费信息。可以构建一个报告来提供用户身份、开始和中止时间、执行的命令(例如 PPP)、数据包数以及字节数。

TACACS ＋概要

Cisco为了将TACACS ＋服务器与一个第三方(例如令牌口令卡)或一个客户自己的验证、授权和记帐服务集成，提供一个一般目的的TACACS ＋协议规范。目的是使服务(例如Kerberos验证)能由一个第三方提供。TACACS＋不受一个单一访问模式的限制; 它通过SLIP、CSLIP、XRemote、PPP、ARAP、TN3270、X.25和哑终端(TTYs)而得到支持。

Kerberos

Kerberos是麻省理工学院(MIT)开发的一个密钥网络验证系统，它使用数据加密标准(DES)密码算法进行加密和验证。Kerberos被设计用来验证对网络资源的请求。Kerberos与其他密钥系统相似，也需要委托一个第三方－这里是指Kerberos服务器。Cisco已经在Cisco访问服务器的Cisco IOS软件内集成了Kerberos的客户验证部分。

Radius

远程验证拨号入网用户服务(RADIUS)是一个分布式安全系统，它防止对网络和网络服务进行未经授权的远程访问。RADIUS包括两个部分:一部验证服务器和客户协议。服务器被安装在客户站点的一台中央计算机上。RADIUS被设计用来通过分离安全技术和通信技术，进而简化安全过程。Cisco已经将RADIUS客户机软件集成进Cisco IOS软件。

Cisco IOS 特权级

每一个客户都拥有独特的访问管理要求。系统管理员可以定制对Cisco IOS软件用户界面的访问，从而使他们能够建立对路由器和服务器的访问特权级。他们可以建立多达16个访问级。融合多个特权级可以实现更加精细的访问层次。对于Cisco IOS用户界面的每一级来说，都可以建立一个储存的加密口令。

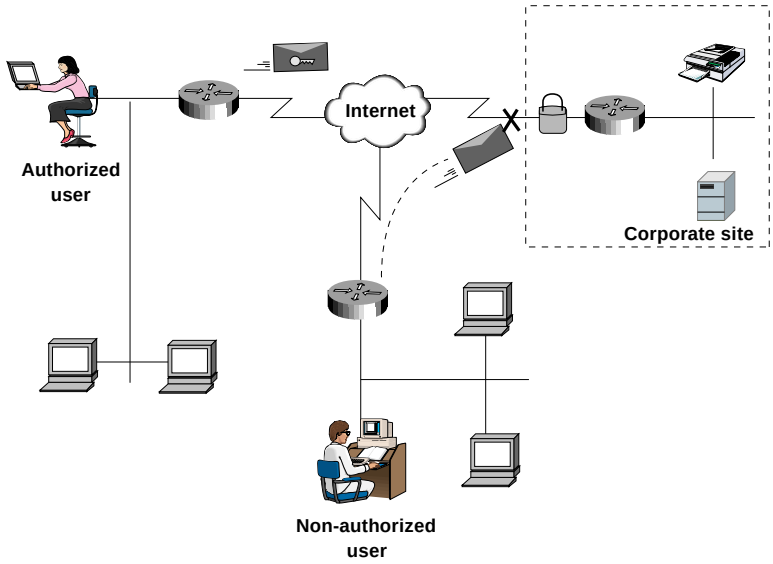
主机安全

应用程序和主机安全是整个安全设计的重要部分。主机操作系统有一个安全问题的历史，其中许多都可以通过适当的计划予以防止。应定期审计各个主机，以确保安全。通过结合主机和网络安全实践，可以获得高水准的协同效果。

锁定和密钥安全

许多家庭办公室都拥有局域网(LANs),他们的用户希望将他们的所有资源连接到中央站点。拥有广域网连接的分支办事处也希望提供独特的访问和验证特权。尽管远程登录为用户提供了灵活性，但是它们也给企业带来了安全问题。目前最常见的安全解决方案是使用访问控制目录来验证和授权远程主机。但是，这种机制难以扩展，而且不能在一个逻辑网络地址之外验证用户。远程网络活动为网络黑客的闯入提供了机会。Cisco IOS提供锁定和密钥,这种安全机制提供了将请求 / 响应系统和 ACLs 结合的能力。

锁定和密钥安全框架



Lock and Key Security

锁定和密钥验证

锁定和密钥机制在允许访问之前验证主机。锁定和密钥将要求用户在将一个独特的访问目录装入本地或远程路由器之前, 对一个登录和口令提示作出回应。网络管理员可以口授一个空闲超时或一个绝对周期,

来进行授权和重新授权。锁定和密钥与介质不相关：它与ISDN、帧中继、X.25、DDR和PPP等服务协作。锁定和密钥能够为本地及远程网络中的一个单一用户、多个用户和多个设备提供安全。

加密

目前的开放的网络技术给企业的整个安全造成了威胁。这种开放性可能意味着，一家公司几乎不能控制何人可以访问其信息资源以及信息流经的路径。传统安全系统基于点对点、未打包的传输介质，不是被设计用来解决不断发展的WAN和LAN技术，而当数据通过公共网络时，这些技术却是目前企业网络的核心。Cisco拥有加密支持的长期历史。几年前，Cisco通过美国政府的Blacker Front End(BFE)计划增加了加密支持。防御通信机构(DCA)为连接防御数据网络(DDN)，认证了Cisco Systems的行加密。使用NetFlow在网络层逐个流量加密比一个链接一个链接地加密所有流量更加经济有效和灵活。由于网络层加密对网络拓扑完全透明并能跨所有的介质类型进行操作，因此它能够跨越公共的网络服务实现敏感信息的安全传输。

美国政府的安全需求

Cisco的商业和政府客房知道最佳的安全技术就是加密，这一过程将清晰的信息转换成模糊状态或“密码文本”。Cisco与Cylink公司联合将Cylink的企业安全体系结构(由Cylink的SecurePacket技术组成)集成进IOS。

服务质量(QoS)介绍

企业互联网络已经从提供局域网组之间的简单连接发展到成为企业数据通信基础机构的一个有机组成部分。一般来说，企业的目标是部署和维护一个单一的企业网络，但是他们希望网络支持不同的应用程序、组织、技术和用户期望。因此，网络管理人员需要给所有用户提供一个适当的服务水准，并继续支持关键任务应用程序，与此同时还得有能力集成新技术。

或者，这种挑战可以被描述为给企业网络提供某种级别的集中控制和网络决定性，这种级别更加适应传统的基于主机的企业网络的要求，例如 IBM 的系统网络体系结构(SNA)。此外，运行一个网络的主要成本在于广域网线路收费，因此网络管理人员必须在带宽和广域网线路的成本以及提供给用户的服务级之间进行适当的折衷。为了满足这些挑战，管理人员必须在不增加非必要成本的情况下，优先排队、保留和管理网络资源，并确保不同技术的集成和迁移。

能够改进服务质量的特定 IOS 特性包括优先权排队、定制排队、政策路由以及加权合理排队。此外，通过资源保留协议(RSVP)，网络管理人员还能够支持需要动态但有保障服务级的应用程序，特别是多媒体应用程序。这些特性的简要介绍如下:

优先权排队

优先权排队确保一个特定协议或流量类型的及时交付，因为该流量总是在其他流量类型前传输。优先权排队的工作方式是将一系列过滤器或访问列表记录用于路由器转发的每一条消息。这些过滤器检查数据包的属性，例如来源和目的地标识、传输协议或应用程序，然后根据预先决定的网络要求排定消息的优先顺序。排队算法根据优先权将数据包放在一个队列中，并在传输中优先对待高优先权队列。在 IOS 11.0 版本中，优先权排队经过了优化，如果接口没有拥塞，数据包可以立即转发。否则，数据包被放在队列中的适当地方，直至依次被转发。这种排队以一种优化的方式进行，降低了路由器 CPU 开销。

定制排队

定制排队通过给不同类别的数据包分配不同数量的队列空间，然后以一种循环方式服务于队列，来处理流量。因而，可以给一个特定的协议、用户或应用程序分配更多的队列空间，尽管它永远不能独占整个带宽。与优先权排队相似，定制排队将一系列访问列表条目用于它所转发的每一条消息。这些访问列表条目检查属性，对消息进行分类，例如源和目的系统的标识、传输协议或应用程序。然后，排队算法将它们放在所选的队列中。随后，路由器将以循环方式服务于这些队列。每一次传递从一个队列移走的数量根据配置而变化。这种特性确保在线路吃紧时，没有任何数据包能够超过预先规定的容量比例。

定制排队已经通过Cisco IOS 11.0进行了优化，若接口没有拥塞，数据包可以立即转发。否则，数据包被放在队列中的适当地方，直至依次被转发。这种排队以一种优化的方式进行，降低了路由器CPU开销。

加权合理排队

对于某些类型的流量需要保证带宽或者最小的服务级(例如SNA密封)，并允许服务于其他流量，在这种环境中定制排队非常理想。

加权合理排队确保队列不会急缺带宽，适用于流量可预测的服务。低容量通信流可获得优先服务，从而及时传送它们的整个负荷。高容量通信流共享剩下的容量，获得均等或比例带宽。加权合理排队有助于给轻重用户提供一致的应答时间。

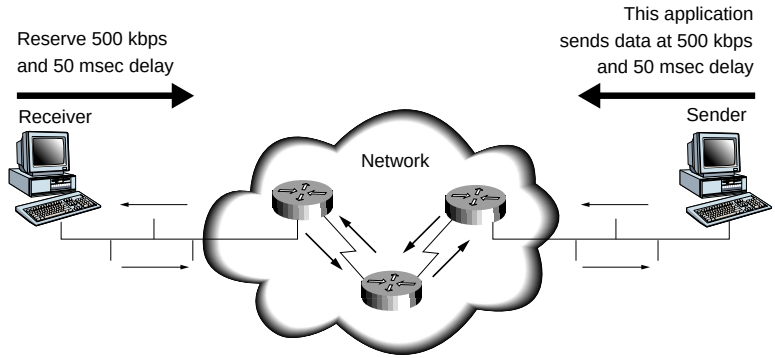
加权合理排队还可将不一致应答时间的主要原因分成不同的流或对话，并迫使它们交叉。算法还解决往返延迟变化的问题。如果多个高容量对话都有效，那么它们的传输速率和时间间隔可以预测。加权合理排队增强了算法(例如SNA的逻辑链路控制－LLC)以及传输控制协议(TCP)的拥塞控制和慢启动。

政策路由

网络管理人员可以根据预配置的政策而不是预定义的路径发送网络包，以实现政策路由。使用政策路由将导致数据包采用不同的路径，而不是源自路由协议的路径。例如，假定一家企业能够配置一个网络，因此，与特定活动相关的通信流量短时间使用一个更高带宽、更高成本的链路，而日常应用程序(例如电子邮件)的基本连接由一个带宽更低、成本更低的链路提供。为了确保更高带宽的链路仅在需要时使用，可以与政策路由结合使用 IOS 拨号服务。

资源保留协议 (RSVP)

资源保留协议(RSVP)是一个专为集成化的互联网络服务而设计的资源保留准备协议。应用程序调用RSVP为一个数据流请求特定的服务质量。主机和路由器使用 RSVP沿数据流的路径将这些请求提供给路由器，并维护路由器和主机状态进而提供所请求的服务。这通常要求在这些节点中保留资源。



Resource Reservation Protocol (RSVP)

RSVP 允许流(可能是任何流，但主要针对多媒体流)的参加者推荐它们需求的网络，并建议网络配置其本身以满足这些需求。参加者包括发送者、接收者和网络部件。在沿路径的每一个“节点” (路由器或主机)，RSVP 向一个许可控制例程发出一个新的资源保留请求，从而决定是否有充足的可用资源。如果有，节点将保留资源并更新其数据包调度程序和分类器控制参数，从而提供所请求的服务质量。

决定带宽保留

网络决定带宽保留所需的信息包括平均数据速率、一个路由器能够排队的最大数据量以及最小服务质量。在 RSVP 和 ATM 提供的服务质量选项之间有一个紧密的映象，它将促进企业范围的端到端服务质量的实现。RSVP 是一个 IETF 起草的标准，目前正在被 Cisco 以及其他主机系统和路由器供应商所实现。

Cisco IOS 通用网络服务: VLANs

介绍

IOS 为增强 VLAN 连接和通信提供大量的特性及功能。诸如安全、流量管理和服务质量等特性以及其他服务都在增强VLAN功能方面扮演着重要的角色。但是, 在大多数情况下, IOS通过其增强的路由功能提供VLANs间通信。IOS 为跨 VLANs 通信提供的一些主要特性包括:

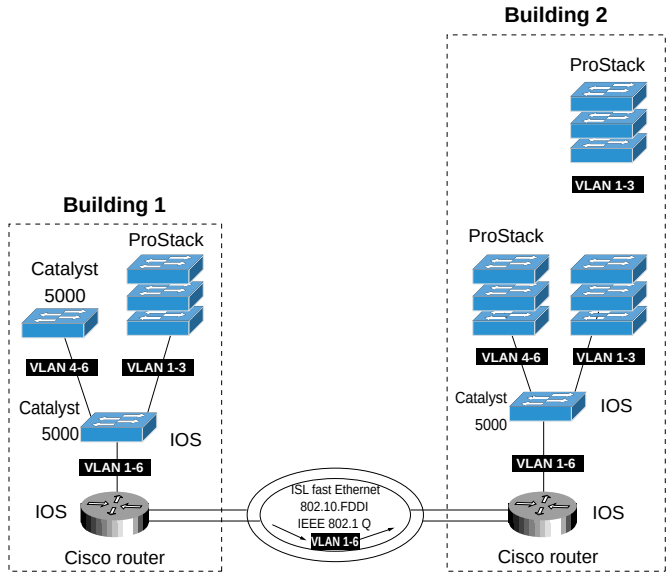
IOS VLAN 特性功能

- 一个单一 Cisco 7000 或 7500 路由器通过 IOS 子接口技术能够支持多达 255 个 VLANs。
- Cisco IOS 有能力并行处理第二层和第三层 VLANs(不可路由和可路由的端应用) – 这一特性也称为多层交换。
- 在局域网内以及跨广域网互连 VLANs 的能力。
- 在快速以太网和 FDDI 骨干网上的交换器之间提供高带宽通信，并支持中继协议，包括 ISL、802.10 和 802.1Q。Cisco IOS 还支持 ATMLAN 仿真(LANE)。
- Cisco IOS 提供第三层安全服务。

每路由器跨一个或多个高带宽接口可支持 255 个 VLANs，包括快速以太网、FDDI 和 ATM，减少了互连 VLANs 所需的路由器和接口数。它还确保一个通向交换器中枢的高带宽通信路径。如图所示，VLANs 跨一

个可路由的园区网或一个广域网的连接将 VLANs 的总体范围延伸到了局域网的边界之外；它还保护校园大楼之间现有的路由网络。

带有 Cisco IOS 的 VLANs 间的通信



Communications Between VLANs

中继(Trunking)协议支持

Cisco IOS通过在路由功能之上进一步增加VLANs解码层，提供VLAN通信的优点。这种解码功能包括以下能力：阅读Inter-Switch Link(ISL)以及通过Catalyst和ProStack交换器转发给路由器的802.10包；根据嵌入式子网地址决定数据包的目的地位置；运用适当的新子网地址重建数据包；在数据包被转发到目标VLAN时，给数据包增加新的VLANs标识；将数据包传递给光纤内的适当交换器。(数据包或帧标记以及中继协议，例如ISL和802.10及802.1Q，将在CiscoFusion单元详细讨论。而且，运行于Cisco交换器的IOS是一个IOS子集，有时是指IOS for Switched Internetworks。)

第二层转发

此外，针对那些仅在第二层运行的协议(如 NetBIOS、LAT 等)，基于 IOS 的路由器可以运行为一种 VLANs 转发模式(Layer 2)。在这种模式中，路由器将数据包转发给连接的 VLANs，同时保持 VLANs 标识的完整性。第三层路由和子网地址不用于这些仅第二层配置的 VLANs。

概要

IOS 内的 VLANs 功能利用 Cisco 路由产品许多现有的嵌入式特性。控制 VLANs 内外访问类型的安全访问目录可以使用基于 IOS 的路由器进行配置。而且，还可以配置并发路由和 VLAN 转发来提供更加广泛的 VLANs 配置选项，包括第二层和第三层应用驻留。此外，基于 IOS 的路由器还能够跨广域网连接 VLANs，极大地增加了配置选项和 VLAN 组成员。

IOS 支持桥接、路由和跨基础机构转发 VLANs 数据包的能力:

VLANs 桥接

- 路由器以一种网桥模式配置，与交换器类似地处理 VLAN 数据包。它根据一个桥接表检查 MAC 地址；如果数据包要求转发，桥接表将作出决定。此外，路由器(作为一个网桥)还检查 VLAN 标识，并根据这一 ID 作出一个转发决定。“桥接”VLANs 数据包一般被没有第三层路由功能的协议所需要，例如 LAT、NETBios 和 LLC2。

VLANs 路由

- VLANs 间通信需要路由功能。VLAN 可以根据协议类型配置；某些协议可以桥接在一起，因而创建了一个大规模 VLANs，而其他协议可以被路由，提供一个更加分散的方案。例如，网络管理人员可以将他们所有的 LAT 流量连接为一个大型 VLAN 组，将他们的 IP 和 IPX 流量连接为多个 VLANs 组(需要桥接和路由功能)。IOS 首先是在路由模式中运行，然后在桥接模式中运行。路由器首先决定它是否能够为一个数据包进行路由，这要根据协议是否已经为路由进行了配置。如果协议为路由进行了配置，路由器就发送数据包。如果协议没有为路由而进行配置，路由器将检查桥接是否启动。这种机制提供根据协议类型并行路由和桥接数据包的能力，根据基本协议，这是 VLANs 需要的一个功能。对于配置成路由器(

不是网桥)的路由器之间的VLAN通信来说，路由器收到一个标记有独特VLAN标识符的VLANs数据包。源和目的地的子网地址由路由器进行检查。如果数据包将被转发到另一个路由器(比如需要通过一个园区网的FDDI环)，那么它将被格式化为适当的类型，并发送到接收路由器。接收路由器也检查子网地址。如果数据包必须被转发给一个已定义的VLANs组(拥有一个直接附带的交换器连接)，路由器将增加适当的VLANs地址串，并将数据包转发给连接的交换器。IOS支持VLANs间路由以及同一VLANs组内的路由。

VLANs转发

- 另一个IOS特性是VLANs转发。这一功能自然转发VLANs数据包，不对它们进行检查、去除或更新标记。VLANs数据包在路由器之间自由转发。作为一种硬件辅助的功能，这种方案提供最高的性能，因为它很少需要地址或协议处理。当一个跨几栋大楼的VLANs(路由器用于建立互连)中需要高性能通信时，它可能是优选的方案。但是，该方案也有其限制，因为它不提供VLANs间通信。

Cisco IOS通用网络服务：通信流量管理

介绍

用户和计算机的存储量一样迅速增长，造成了资源饥渴的网络应用。如果没有适当的网络计划和流量管理技术，即便是一个设计良好的网络也会出现瓶颈。必须了解网络使用、流量模式以及对网络的总体要求。如果没有这种明确的流量分析，就会根据猜测去变化网络。这通常导致无法真正解决问题的代价高昂的调整。IOS提供一个集成的流量管理、缓冲管理以及积极的拥塞避免机制的功能。(与流量管理相关的是服务质量；IOS服务质量已在前面讨论过；该部分重点介绍队列管理，这是流量优先化的一个重要部分。)

流量管理

网络管理人员在不同的时间需要不同类型的管理信息。在日常情况下，他们需要监视网络连接和设备的使用。这些使用度量(在 MIB II 和 RMON MIB 中提供)类似一个病人的生命特征。通过号脉和查体温，医生可以决定病人是否活着以及是否处于严重的危险之中。同样，网络生命特征可以表明连接和设备是否有效和是否正确地工作。

应用级流量

尽管这些度量很好，但是它们不能表明网络是否处于健康营养状态。这种信息来自于对网络应用和用户的监视，可以判断网络是否在按预期使用或者某些应用程序或用户是否造成超常的大流量。这种信息是通过长期网络规划、建模应用以及分析和报告工具的使用而得来的。

IOS 和流量管理

通过RMON1和RMON2支持，IOS支持流量分析和报告。Cisco还将继续投入大量资源给网络设备配备流量管理软件。首先是IOS11.1，所有Cisco路由器都将提供RMON阈值功能。同样在Cisco IOS 11.1中，NetFlow Switching 和 NetFlow 数据输出机制将可用于带有 Route/Switch 处理器的 Cisco 7000 家族产品。

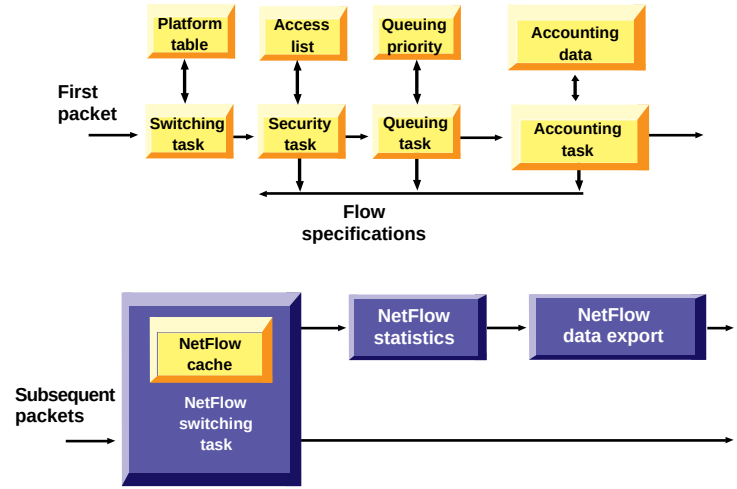
NETFLOW SWITCHING

说明

NetFlow Switching是一种IOS软件交换机制，它允许Cisco路由器将高性能的网络层交换与面向连接的网络服务应用相结合，从而在网络内提供安全、服务质量和流量记帐。为了实现这种性能，NetFlow Switching识别互联网端点之间的通信流，然后在面向连接的基础上，交换这些流中的数据包，同时采用相关的服务。通过使用网络层(IP 地址)和传输层(已知端口)信息识别流，NetFlow Switching允许根据每用户、每应用来采用IOS服务。

传统交换与 NetFlow Switching

在网络层的传统交换中，每一个入站数据包都独立处理，需要执行不同的任务和查表来为每一个数据包交换和采用每一项服务。这些不同的任务包括：检查安全访问过滤器使用，然后是更新流量记帐记录。通过 NetFlow Switching，这种过程仅发生在一个流中的第一个数据包上。当一个网络流已经被识别而且已经决定其相关的服务时，所有后续数据包均将在一个面向连接的基础上作为流的一部分予以处理。交换和服务以纵列方式用于后续数据包。数据包处理的这种流程化，如图所示，给 NetFlow Switching 提供了优异的性能特征。



NetFlow Switching

交换高速缓存

NetFlow Switching通过创建一个交换高速缓存来实现，它包含为所有有效流交换和执行适当服务所需的信息。NetFlow Switching高速缓存是通过在一个流建立交换和服务路径时处理该流的第一个数据包而建立的。因此，每一个流都与一个入站和出站端口号以及特定的安全访问许可和加密策略联系在一起。高速缓存还包括流量统计记录，这些记录被后续数据包交替更新。

活动流和非活动流

一旦创建了NetFlow高速缓存，被识别属于一个标识流的数据包可以根据高速缓存的信息进行交换，并且可以利用适当的服务，例如加密。流信息被保持在适用于所有活动流的NetFlow高速缓存内。当传输协议指示连接完成或在一段流量不活动期(一般大约30秒)之后，流变成不活动的，它们的信息被从高速缓存冲洗。不属于一个被标识的活动流的数据包被转发给其他交换机制。

产品支持

Cisco NetFlow Switching的最初实现在所有接口类型上支持IP流量，并通过以太网、FDDI和HDLC串行接口等提供优化的性能。NetFlow的IPX支持正在计划之中。目前的软件版本支持NetFlow Switching，从11.1(2)开始，用于Cisco 7500系列和Cisco 7000系列。NetFlow Switching支持将在1996年扩展到其他Cisco路由器平台，具体将在第三季度从中档系统开始。

NetFlow Switching特性和优点包括:

具有面向连接优点的无连接

- NetFlow Switching能够以一个无连接的、基于包的基础结构，提供通常是与面向连接的技术所提供的性能和服务。由于NetFlow Switching运用面向连接的技术进行包处理，因此在一个网际互连设备内这是可能的。不需要外部干涉，无论是对流量或数据包本身还是对任何其他网络设备。

网络透明

- NetFlow Switching能够实现面向连接技术的优点，同时对现有网络是透明的，包括端点、应用软件和网络设备，例如局域网交换器。由于NetFlow Switching可以在每一个互联网设备上独立运行，因此不需要在网络的每一个路由器上都操作NetFlow Switching，网络计划员可以有选择地调用NetFlow Switching，以获得流量性能，或对特定网络位置进行控制及记帐。

扩展Cisco IOS安全和流量管理服务

- 通过NetFlow Switching，网络用户可以扩展其现有Cisco IOS服务，例如安全访问目录或流量统计，而不会带来通常由这类处理所导致的性

能损耗。而性能的增加允许在网络内的更多地方更大规模地使用这些服务。由于网络必须支持远程用户访问和跨公共 Internet 服务的访问，因此扩展网络安全性变得日益重要。 NetFlow Switching 提供“呼叫细节报告”(Call detail reporting)信息来跟踪传输流、关键数据，以进行经济有效的网络容量规划。

网络层加密

- Cisco的网络加密服务允许网络管理人员对个人或小组之间的特定会话或应用程序进行加密。使用 NetFlow 在网络层逐个流地加密比一个链接一个链接地加密所有流量更加经济有效和灵活。由于网络层加密对网络拓扑完全透明并能跨所有的介质类型进行操作，因此它能够跨越公共的网络服务实现敏感信息的安全传输。

运用 NETFLOW DATA EXPORT 进行流量管理

NetFlow Switching 和流量统计

NetFlow Switching 允许以最小的性能价，用其交换功能纵列地收集和积累详细的流量统计。每一个活动流的流量统计都被保持在NetFlow Switching高速缓存中，并在每一个流内的数据包被交换时增大。每一个流的流量数据包括源和目的地地址以及端口号、协议类型、包和字节数、流持续时间、时间戳。在传统交换中，一个辅助记帐过程检查每一个数据包，并在一个系统记帐数据库中更新适当的流量记录。这对系统性能有着巨大的影响。而运用 NetFlow Switching，流量统计是在交换过程期间收集的，并经汇总后转发给系统IP记帐数据库。这种过程大大降低了进行详细流量统计的性能影响。

通过控制台接口(Console Port)使用一个Show命令，可以看到NetFlow Switching的流量统计。该命令显示根据每个协议及每个应用而总结的通信流统计。此外，每一个流或会话的详细信息还包括包和字节数以及持续时间和时间戳。

NetFlow Data Export

IOS 支持 NetFlow Data Export，它是一个能够实现 NetFlow Switching 统计批量输出的应用。通过使用 NetFlow Data Export，所有终止流的汇总流量统计可以通过数据报文定期输出到指定的目的地，包括流量指针、管理程序或其他数据区。

RMON2 超集(Superset)

NetFlow Data Export 提供的信息是 RMON2 中信息的一个超集。它提供了面向连接的、网络层的源和目的地之间的流量汇总，包括时间戳持续时间。它还将连接流与特定的路由器输入和输出端口相关联。RMON2 不提供连接的持续时间，仅能通过增加查询频率来了解当天特定次数的流量数据。由于 RMON2 探针带来了增加的流量负荷和处理需求，因此增加查询频率并不可行。而且，NetFlow Data Export 通常比基于 RMON2 的数据收集更加灵活有效。例如，它不必将所有流量统计映象到 RMON MIB，也不需要 SNMP 查询来收集信息

第三方应用程序支持

NetFlow Data Export 被多个 RMON 和性能管理应用程序的支持，包括 NETSYS performance Baseliner/Solver、Frontier 的 Net Visualizer、Axon 的 Traffix Manager 和 International Network Service(INS)NETracker。NetFlow Data Export 预期将成为把涉及流量记帐信息的大量数据从 Cisco 路由器输出到网管应用程序的优选方法。Cisco 还将通过一个机载 RMON2 代理把 NetFlow Switching 信息映象到 RMON2 MIBs 中。RMON2 MIB 和 SNMP 查询对于为故障诊断的目的而有选择地输出少量数据则非常有用。

Cisco IOS 通用网络服务：协议处理

介绍

一个互联网际的协议处理主要是指路由器如何在多协议 LAN 和 WAN 中处理包(和单元)。协议转换、压缩算法、SNA 和 TCP/IP 集成以

及几乎所有多协议网络都依赖于协议处理。Cisco 的协议处理方案包括 IOS 与一个提供专用协议处理引擎的路由器体系结构的紧密耦合。这些路由器体系结构将在 Core/ATM Business Unit 单元予以介绍，本单元将概要介绍 IOS 的压缩和协议转换支持。

WAN 连接上的带宽要求

局域网相互连接并通过广域网与企业骨干网连接在一起。今天，我们看到了对这些连接的几种需求趋势。一个趋势是从基于个人计算机的应用程序移至一个局域网上的共享应用程序。基于局域网的应用程序将跨越广域网连接产生不同类型的流量。典型的是：交互式应用产生的文件及面向事务流量的批量传输。信息传输服务(例如电子邮件)和文件服务器应用程序对连接带宽要求也增长了。此外，当这些应用程序的数据通过网络时，它们的显示方式也不同。

广域网连接速度

连接速度是目前广域网的另一个问题。10 年前，每秒 2400 位被认为是很高的传输速度。今天，64 kbps 的传输速度已很平常。传统的点对点专线和 X.25 封装格式已经普遍用于广域网传输服务。更新的服务，例如 PRI 和 BRI 速率的 ISDN、帧中继、SMDS(交换式多兆位数据服务)和 ATM 也已开始使用，并满足了对带宽增长的需求。这些传输信道本身可能非常昂贵。事实上，，在一个企业级网络中，仅传输连接的成本就可能消耗网络操作成本的相当部分。

广域网连接成本

对美国、欧洲以及穿越大西洋的专线服务的成本比较也表明，世界不同地方的带宽成本都非常高。由于发展中国家的网络基础设施没有充分开发，加上通信需求不断发展，因此他们的网络必须能够以最有效的方式利用广域网连接。降低广域网传输成本是基于 IOS 的广域网技术服务的目标之一。

优化广域网连接的 IOS

IOS 软件提供大量的特性，用于优化广域网连接，缓解广域网带宽瓶颈。这些特性包括优先输出排队、定制排队、访问列表、Novell 静态

服务广告协议(SAP)表以及 Novell IPX SAP 过滤器。不过，最有效的广域网优化方法是数据压缩。

数据压缩

说明

数据压缩可以大大减少一帧的长度，减少数据通过网络所需的时间。数据压缩通过在传输连接的每一端提供一个编码方案来实现。这些编码方案允许在发送方将字符从数据帧中删除，然后在接收方正确地予以恢复。由于压缩帧占用的带宽较少，因此每时间单元可以传送更多的帧。

有损耗的或不可逆的压缩

用于传输语音和图象数据的数据压缩方法是有损耗的或不可逆的压缩。这类压缩允许数据有一些丢失或降级，因而大大提高了压缩比率，降低了传输这类数据所需的带宽。IOS 软件支持 Apple QuichTime Conferencing, 这是一个模块化的软件体系结构，它支持电视会议标准，例如 Joint Photographic Experts Group(JPEG)和 Moving Pictures Experts Group(MPEG)。这些标准基于的压缩算法都是对包丢失敏感的，可缓和压缩对语音和图象数据的影响。

无损压缩

用于网际互连设备的数据压缩算法是指无损压缩算法。这些算法准确地再现最初的位流，而没有误码或丢失，这是路由器和其他设备通过网络传输数据所需要的一个特性。无损压缩算法使用两种基本类型的编码技术:统计(Statistical)和词典(dictionary)。

统计压缩

统计压缩使用一种固定的、非自适应的编码方法，它最适合数据相对一致和可预测的单一应用。由于网间流量既不一致，也不可预测，因此总体来说，统计压缩不适合作为路由器上的压缩算法对数据进行编码。

词典压缩

词典压缩的一个例子是Lempel-Ziv算法。这种算法基于一个动态编码

的词典，用代码替换一个连续的字符流。代码所表示的符号被存储在一个词典风格的存储器中。由于代码和最初符号之间的关系随数据变化而变化，因此这种方案对数据中的偏差更具有响应性。这种灵活性对局域网数据尤其重要，因为在任何时间都可能有许多不同的应用通过广域网进行传输。此外，随着数据改变，词典相应地改变，并适应不断变化的流量需求。尽管典型的小词典只有2000到32000个字节，但是压缩比例可以通过使用更大的字典而得到优化。Lempel-Ziv算法用于许多流行的压缩程序，例如ZIP和 UNIX 压缩实用程序。

Cisco IOS 压缩解决方案

STAC 算法

Cisco 互联网络设备使用 STAC 和 Predictor 数据压缩算法。STAC 是由STAC Electronicx开发的，它基于Lempel-Ziv压缩算法。IOS使用STAC的一个优化版本，提供良好的压缩比例，但是要想很好地执行压缩需要许多CPU 周期。STAC用于Cisco的Link Access Procedure、Balanced LAPB、HDLC、X.25 以及帧中继数据压缩解决方案。

Predictor 算法

Predictor压缩算法通过使用一个索引查阅压缩词典中的一个序列，试图预测数据流中的下一个字符序列。然后，它检查数据流中的下一个序列，看它是否匹配。如果是，那么该序列将替换在词典中查阅的序列。如果不是，算法将在索引中定位下一个字符序列，过程再次开始。索引通过从输入流得到一些最新的字符序列来更新自己。

Predictor 数据压缩算法是从公共域获得的，被 Cisco 工程师进行了优化。与 STAC 相比，它可以更有效地利用 CPU，但是需要更多的内存。Predictor 数据压缩算法可以与Cisco的点对点协议(PPP)或LAPB 协议一起使用。

IOS 目前提供下列这些数据压缩解决方案:

TCP/IP 标头压缩

- IOS 标头压缩策略支持 RFC 1144 中定义的 Van Jacobson 算法。它针对特定协议，而且对于包含只有很少数据字节的小数据包(例如 Telnet)的 TCP/IP 流量非常有效。TCP/IP 标头压缩降低了比例太大的 TCP/IP 标头在广域网传输时所产生的开销。Cisco 的标头压缩支持 X.25、帧中继和按需拨号广域网连接协议。一般情况下，面向事务的应用(例如 DEC LAT、Telnet、rlogin、Xwindows)以及确认包使用这种类型的压缩效果最佳。由于处理开销的考虑，标头压缩一般是以 64 kbps 的速率进行，而不是以目前局域网到广域网通信的更高速度。标头压缩可以根据线路速率对低速线路的吞吐量进行改进。例如，在一个 64 kbps 专线上可以实现 Telnet 流量 50%的吞吐量改进。

按接口压缩

- 为了处理更大的数据包，支持更高的数据速率，以及跨一个局域网上的多个协议改进性能，在整个数据流通过广域网传输时，压缩可以用于整个数据流。这种类型的压缩称为按接口压缩，它压缩整个广域网连接，就好象它是一个应用程序。与标头压缩不同，按接口压缩与协议不相关。按接口压缩算法使用 STAC 或 Predictor 来压缩流量，然后在另一个连接层(例如 PPP 或 LAPB)中封装压缩的流量，以确保错误纠正和包排序。按接口压缩的定义使之成为一个仅点对点解决方案，用于专线或 ISDN 等服务中。全部包(标头和数据)被压缩，而标头中的交换信息不能用于 WAN 交换网络。

按虚拟电路压缩

- 按虚拟电路压缩是跨虚拟 WAN 服务的操作所需的压缩方法。它通过 X.25 和帧中继 WAN 服务得到支持，并使用 Predictor 和 STAC 压缩方法。由于标头信息在按虚拟电路压缩期间没有被改变，因此包仍然可以通过一个 WAN 分组交换网络被交换，通过一个路由器网络被发送。因而，当网络利用更低费率的公共分组交换数据网络时，可以采用压缩。在设计一个互联网络时，客户不能假定一个应用将仅通过点对点线路传递。因此，软件必须非常智能，足以确保应用程序的数据包标头得到维护，路由器可以利用 WAN 封装执行压缩。

协议转换

介绍

协议转换是协议处理的另一个部分，它是指一个与软件结合的路由器（或网桥）将一个协议转换成另一个类似协议的能力。与协议转换相关的是封装。协议封装通常被用作桥接不同网络(例如 TCP/IP 和 SNA)的一种方法。在这种应用中，一个网络的整个帧被封入另一个网络的链路层协议所用的标头中。这通常是指转换桥接。

多协议环境中的 IOS 可伸缩性

在非常广泛的意义上，协议转换对于给当今的多协议互联网提供可伸缩性至关重要。IOS 是 Cisco 为当今所有标准数据协议、介质访问方式以及来自先进网络厂商的产品提供互连接性和互操作性的方法。转换桥接以及以太网、令牌环网和 FDDI LAN 之间的协议转换消除了主机环境中的多个接口和协议，从而降低了总体拥有成本。

路由协议再分布

使用不同路由协议进行两种环境之间的转换要求由一个协议生成的路径再分布到第二个路由协议环境。路径再分布给公司提供了在工作组或区域中运行不同路由协议的能力，其中每一个都非常有效。静态路径信息也能够再分布。此外，还可以分配缺省路由，从而使一个路由协议可以为所有再分布的路径使用同一度量，从而简化了路由再分布机制。

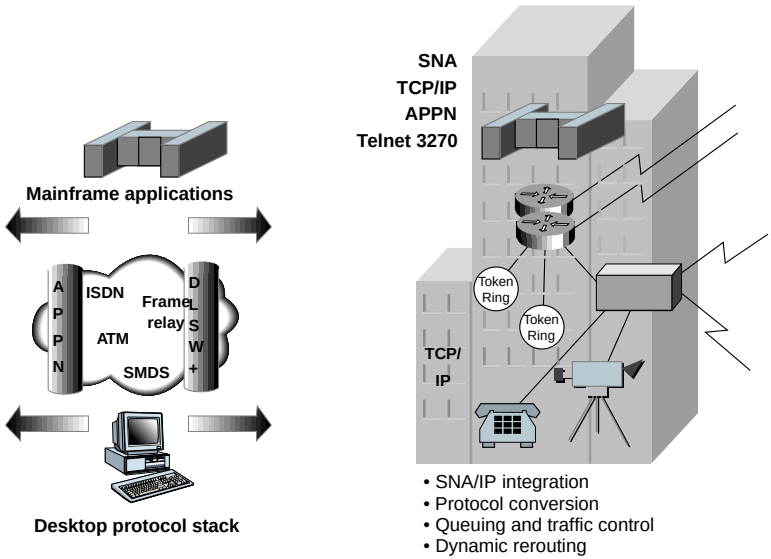
协议封装

协议封装是 Cisco IOS 完成转换的另一种方法。IOS 几乎支持所有 Novell IPX 封装方案，Cisco 是第一个宣布在 TCP/IP 中封装 SNA 协议的公司。

总结

总体上，IOS 协议转换和协议处理功能为支持多协议互联网络提供了大量的特性。没有哪里比 IBM 网际互连市场更为明显。本课程后面的 InterWorks Business Unit 单元将专门讲述特定的协议处理问题(TCP/IP、SNA 等)。下图简单地介绍了这种环境必须支持的一些协议，以及提供互操作性的 IOS 协议处理特性(协议转换、排队、广域网链接的流量压缩)。

IBM 互联网络中
的协议处理要求

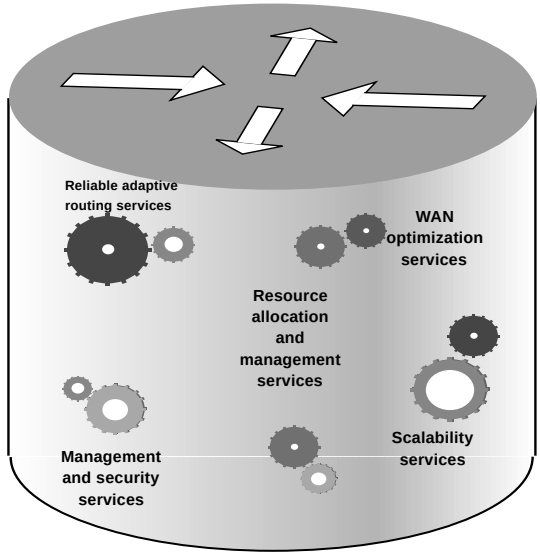


Cisco IOS Protocol Processing in IBM Internetworks

Cisco IOS 市场模式

Cisco IOS
市场模式简介

Cisco IOS 目前作为一个操作系统模式销售，它支持 5 个主要的服务功能组：自适应路由、WAN 服务、管理和安全服务、可伸缩性服务以及资源分配和管理服务。



Five Domains of Cisco IOS

尽管这种模式倾向以路由器为中心，但是IOS组件集成了 Cisco 所有产品系列。Cisco IOS还能够指导CiscoFusion多层交换框架的实现和网络管理。

自适应路由

自适应路由是一个与动态路由结合使用的广泛术语。动态路由取决于路由器的动态知识——一旦从网络收到新的拓扑信息，路径知识将通过一个路由过程自动更新。作为更新过程的一部分，动态知识中的变化在路由器之间交换(通过路由器－路由器通信协议)。自适应路由允许数据在最佳、最经济和提供最大性能的路径上传递。它根据网络故障提供流量导向，并在需要时调整适应拓扑变化。 Cisco IOS 支持基于政策的特性，例如路径过滤和转换。这些特性防止数据被不必要地传播，节省了网络资源。

WAN 服务

互连地理位置分散的局域网需要WAN服务。它们一般是通过一个第三方设备，第三方通常是指公共网络，因为电话公司或公共数据网络(PDN)供应商拥有和管理资源并向用户租赁这些服务。相反，局域网一般

是专有的。随着网际互连遍布全球，有效、经济、高性能的WAN服务变得更加至关重要。Cisco IOS为WAN服务提供全面的支持。它支持线路交换服务(例如ISDN)、交换型T1和拨号电话线路。按需拨号访问和拨号备份能力为昂贵的点对点交换型专线提供经济有效的替代选择。IOS还支持先进的分组交换型服务接口(例如X.25、帧中继和SMDS)以及信元交换型ATM服务。

集成与可伸缩性服务

随着企业的发展和变化，他们的信息系统基础结构也需要发展。随着技术的发展，企业网络也需要适应以支持新的功能，保持竞争性。一家企业满足这些需求的能力通常被称为可伸缩性。IOS特性，例如过滤、协议中止(termination)和转换、智能广播以及帮助地址服务(helper address services)相结合，创建了一个灵活、可伸缩的网络，该网络能够与企业的业务和技术需求同步发展。

管理和安全服务

管理和安全服务对当今大型、复杂的网络至关重要。随着企业部署互联网络，包括公用和专用网络，基础设施的管理和安全成为核心需求。Cisco IOS支持Cisco开发的以及第三方的管理应用程序，支持广泛的协议，为路由器和交换器的管理提供许多有价值的服务。IOS安全体系结构提供模块化的、可伸缩的安全性；安全性的基础构筑于下列组件之上：防火墙、访问管理、主机安全和加密。这些技术为企业根据他们特定的业务需求定义其自己的安全策略提供了构建块。

资源分配和管理服务

资源分配和管理服务为网间互连提供性能和成本方面的好处。当网络带宽紧张时，优先权排队和定制排队给重要会话提供优先权。负荷平衡在整个网络范围内对称扩展所有可用的路径，从而保护了带宽并改进了性能。NetFlow Switching在TCP/IP网络内提供面向连接的网络服务，并通过复杂的流量管理为网络管理人员通过网络监控应用流量提供了一种方法。这些类型的Cisco IOS特性有助于公司充分利用其网络的最大价值。

公司总部
Cisco Systems Inc.
70 West Tasenan Drive
San Jose, CA 95134-1706
USA
www.cisco.com

Cisco Systems 公司在世界范围内设有200多个销售办事处。Cisco Systems 公司美国加州总部的电话为408 526-4000，请与当地客户代表联系。在北美请拨打800 553-NETS (6387)。

北京代表处:
北京南礼士路66号
建威大厦18−19层
邮政编码:100045
电话:(8610)68023355
传真:(8610)68038348

广州代表处:
广州市环市东路362−366号
好世界广场3106−3107室
邮政编码:510060
电话:(8620)83870097
传真:(8620)83870070

上海代表处:
上海市遵义南路88号
协泰中心2205室
邮政编码:200335
电话:(8621)62198668
传真:(8621)62753431

成都代表处:
成都市西御街77号
四川国信大厦8楼A座
邮政编码:610015
电话:(8628)6198198
传真:(8628)6198305