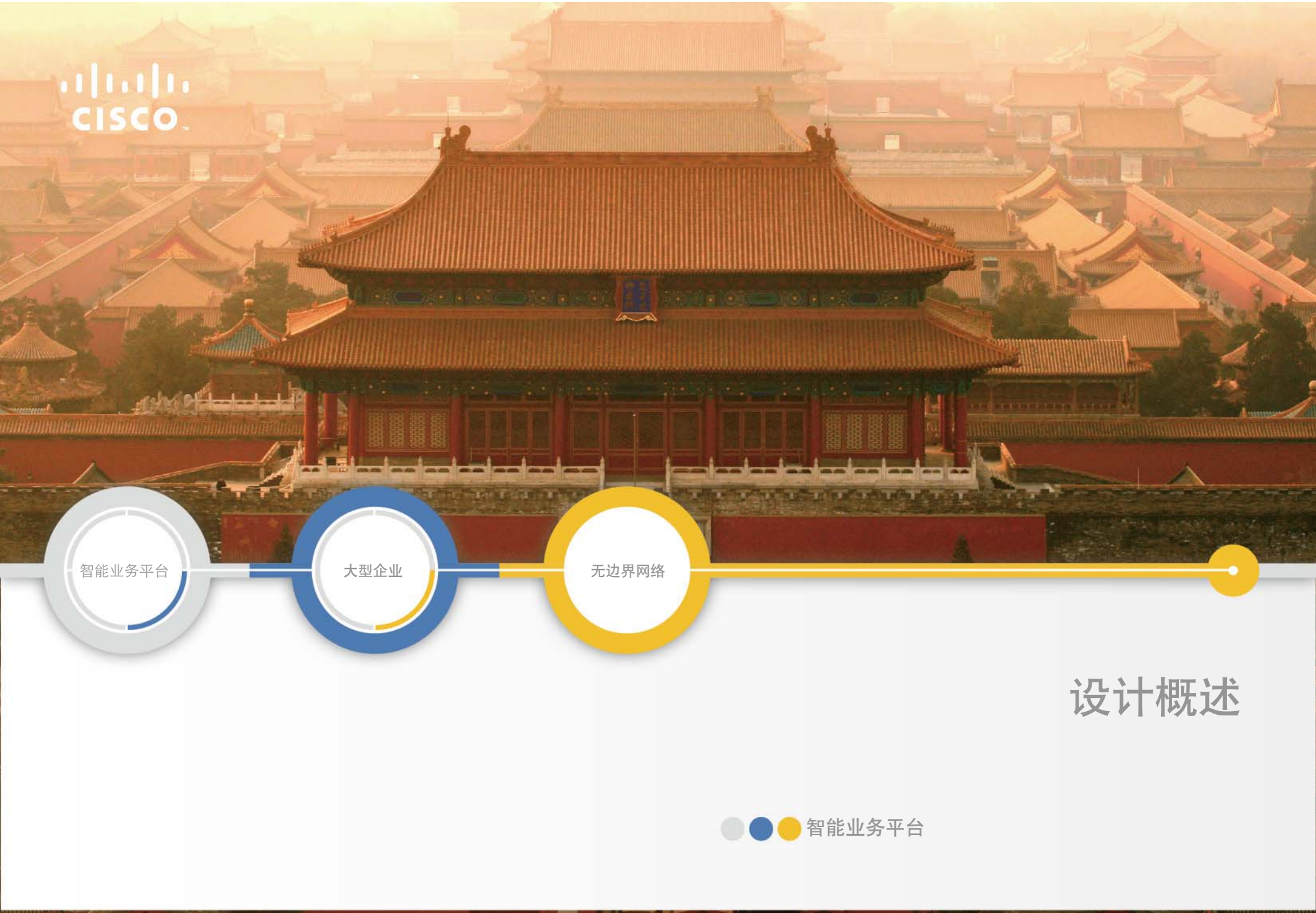


设计概述

智能业务平台

修订版：2011年下半年

前言

本指南适用于思科®智能业务平台（IBA）指南。

本指南的目标受众

本指南主要面向在企业中承担以下职务的人员：

- 需要解决方案标准实施规程的系统工程师
- 需要获取参考资料以撰写思科IBA实施项目工作说明书的项目经理
- 需要借助产品指南销售新技术或撰写自己的实施文档的销售合作伙伴
- 需要课堂讲授或在职培训材料的培训人员

一般来说，您也可以将IBA指南作为工程师之间和各个部署项目的统一指导文件，或利用它更好地规划部署任务的工作范围和成本预算。

版本系列

思科每年对IBA指南进行两次更新和修订。在发布思科IBA指南系列之前，我们将在IBA实验室对其进行整体评测。为确保思科IBA指南中各个设计之间的兼容性，您应使用同一IBA系列中的设计指南文档。

所有思科IBA指南的封面和每页的左下角均标有指南系列的名称。指南系列的命名方式如下：

- **年**2月指南系列
- **年**8月指南系列

其中的**年**表示发布该指南系列的公历年度。

您可以在以下网址查看最新的IBA指南系列：

客户登录：http://www.cisco.com/go/cn/iba

合作伙伴登录：http://www.cisco.com/go/cn/iba

如何阅读命令

许多思科IBA指南详细说明了思科网络设备的配置步骤，这些设备运行着Cisco IOS、Cisco NX-OS或其他需要通过命令行界面(CLI)进行配置的操作系统。下面描述了系统命令的指定规则，您需要按照这些规则来输入命令。

在CLI中输入的命令如下所示：

```
configure terminal
```

为某个变量指定一个值的命令如下所示：

```
ntp server 10.10.48.17
```

包含您必须定义的变量的命令如下所示：

```
class-map [highest class name]
```

以交互示例形式显示的命令（如脚本和包含提示的命令）如下所示：

```
Router# enable
```

包含自动换行的长命令以下划线表示。应将其作为一个命令进行输入：

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

问题和评论

如需要了解更多有关思科 IBA 智能业务平台的信息，请访问

http://www.cisco.com/go/cn/iba

如需要注册快速报价工具（QPT），请访问

http://www.cisco.com/go/qpt

如果您希望在出现新评论时获得通知，我们可以发送RSS信息。

目录

本 IBA 指南的内容

关于IBA

思科IBA能帮助您设计和快速部署一个全方位服务企业网络。IBA系统是一种规范式设计，即购即用，而且具备出色的可扩展性和灵活性。

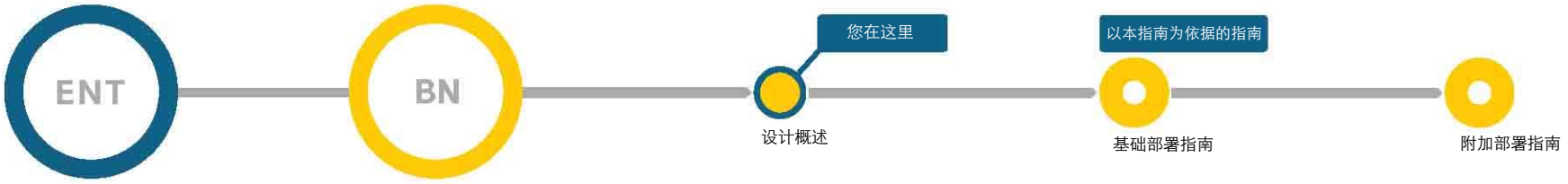
思科IBA在一个综合解决方案中集成了局域网、广域网、无线、安全、数据中心、应用优化和统一通信技术，并对其进行了严格测试，确保能够实现无缝协作。IBA采用的组件式方法简化了在采用多种技术时通常需要进行的系统集成工作，使您可以随意选择能够满足组织需求的解决方案，而不必担心技术复杂性方面的问题。

关于本指南

本指南是一份基础设计概述指南。包含如下内容：

- 对思科IBA基础设计的介绍
- 阐明该设计所涉及的各项要求
- 描述该设计将为您的组织带来的优势

所有成功部署的起点都是基础设计概述，如下所示。



成功部署路线图

为确保您能够按照本指南中的设计成功完成部署，您应当阅读本指南所依据的所有相关指南——即上面路线图中本指南左侧的所有指南。所有以本指南为依据的指南都在右侧。

如需要了解更多有关思科 IBA 智能业务平台的信息，请访问
http://www.cisco.com/go/cn/iba

如需要注册快速报价工具（QPT），请访问
http://www.cisco.com/go/qpt

简介

思科 IBA 智能业务平台——面向大型企业的无边界网络是一个综合性网络设计，专门面向拥有 2000 至 10,000 名互联用户的机构。面向企业的无边界网络架构融合了有线和无线用户的局域网（LAN）接入、广域网（WAN）连接、广域网应用优化和互联网边界安全基础设施，形成了一个统一的解决方案。这种解决方案级方法可降低不同技术和组件之间发生互操作性问题的风险，使客户能够在解决某个业务问题时自由选择所需的产品。在必要时，该架构还能够根据网络可扩展性或服务等级要求提供多种选择。

思科希望通过设计、构建和测试该架构达到以下目标：

- **易于部署：**企业可以将此解决方案统一部署到架构设计所包含的所有产品中。部署中使用的参考配置代表着实现快速、高弹性部署的最佳实践方案。
- **灵活性与可扩展性：**此架构的模块化特性使企业能够在需要时随时添加所需的组件，而且无需花费巨资进行全盘升级即可使架构与企业同步扩展。
- **永续性与安全性：**此架构设计消除了网络边界，在保护用户流量的同时提高了网络可用性，即使在意外停机或攻击期间网络也能保持正常运行。
- **易于管理：**部署和配置指南包含配置范例，允许通过一个网络管理系统或独特的网络管理员实施管理。
- **支持先进技术：**网络基础架构可支持企业更为轻松地部署协作等先进技术。

备注

架构优势

企业通过部署思科 IBA 智能业务平台——面向大型企业的无边界网络架构，可以享受诸多优势。

业务优势:

- 基于思科公认最佳案例降低部署标准化设计的成本
- 灵活的架构能够从小型运营地点扩展到大型园区，实现轻松迁移
- 通过专业的方法为拥有 2000 至 10,000 名用户和多达 500 个远程站点的机构构建高质量的网络基础架构，支持业务增长和平稳运营
- 借助应用优化提高广域网性能，有助于降低电路成本，推迟带宽升级
- 利用分层的方法提供安全的互联网接入设计，在不影响员工移动性的前提下增强保护
- 通过正确使用冗余特性，以及加强链路拓扑、平台特性和系统安全性，提高网络永续性和可用性
- 提供综合和简化的设计选项，使拥有 CCNA®认证或同等资质的 IT 人员能够部署和操作网络

为什么说以综合的方式构建网络架构将为贵机构带来巨大利益?

传统上，企业是通过保存在计算机本地文件中的信息来开展业务，但是这种信息使用方式将很快销声匿迹。最新的发展趋势是用户将通过接入网络访问关键任务信息、下载信息或使用网络应用。用户将共享通用的受保护存储、基于 Web 的应用，甚至是云服务。他们可能会在家中、办公室或酒店房间开始一天的工作，登录工作所需的应用、更新日程安排或查看电子邮件——这些任务对于企业运作非常重要。如今，登录网络来完成工作已经变得像打开电灯来看清办公桌一样简单自然，人们对它已经习以为常。更进一步讲，即使您计划采用的电力设施或其它设施陷于瘫痪，借助网络您也能继续工作，它可支持移动访问和远程访问，即使您换了办公室也能访问原有的应用和信息。

鉴于网络在企业运营和创新方面的重要地位，员工生产率的提高将建立在对通信功能和资源的不间断访问上。为了满足各种设备、多种连接类型和各地用户的需要，网络变得越来越复杂。低劣的设计、复杂的配置、维护任务的增多或软硬件故障等因素，加大了网络中断的风险。与此同时，企业希望快速高效地运用投资，达到简化运营、降低成本和提高投资回报的目的。

通过采用模块化的方法和经过测试的可互操作设计来构建网络，您将可以减少风险和运作问题，提高部署速度。

架构组件

在建筑设计中，架构是一门设计和建造建筑物的艺术与科学；在计算机设计中，架构指的是计算机系统、微处理器或系统程序的设计、结构和行为，包括每个组件的特点和它们之间的交互方式。服务导向架构是指两个计算实体（如程序）以一种特殊的方式进行交互，其中一个实体可代表另一个实体执行某种功能。了解了这些定义之后，我们将更容易理解思科 IBA 智能业务平台——面向大型企业的无边界网络的创建流程。该流程描述并说明了此架构的应用环境、所构建的产品的要求和特点，以及结合微观和宏观依存关系的能力。

我们利用结构化的流程创建了思科 IBA 智能业务平台，以确保重要业务流程及其支持的资产的稳定性。

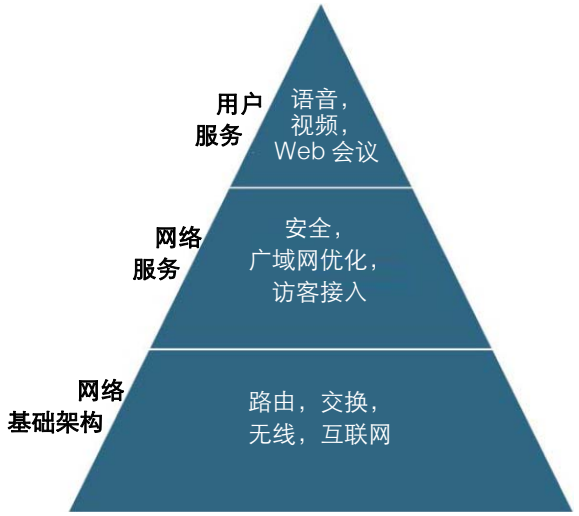
思科 IBA 智能业务平台由三个基本的模块化组件构成，分别是**网络基础架构**、**网络服务**和**用户服务**。它们之间各自独立又相互依存，呈一个层次化结构。

网络基础架构

网络基础架构是思科 IBA 智能业务平台的主要构建模块。与建筑物的底层基石一样，网络基础架构是其它所有服务和应用赖以生存的底层基础设施。作为整体架构的一个模块，网络基础架构可支持无缝传输，能够确保信息在两个地点之间可靠地传递。

对于普通用户来说，网络基础架构在正确部署后能够透明运行。用户只需将他们的台式机、笔记本电脑或智能设备连接到网络，就可以更新电子邮件、处理订单或点击打开网络链接。这一切都依赖智能思科设备构成的基础设施而实现，包括路由器、交换机和无线接入点等。

图 1. IBA 智能业务平台金字塔图



网络服务

虽然所有的建筑结构可能都会采用相同的建筑材料，但设计和结构精良的建筑会考虑使用要求，从而提高其使用价值。如果您的客人较多，可能需要一个面积较大的前厅；如果要照顾病人，就需要设计很多窗户，让室内阳光充足；如果需要提高安全性，就需要坚固的高墙和安全门；如果想提高环境质量，则需要良好的通风和空调系统。如果能充分考虑到这些服务和功能，建筑物将不再仅仅是空洞的墙体，而是增加了实用性。网络服务能够使网络环境更加适应您的独特需求，即使您采用的是标准设备。即便用户并未意识到他们的网络连接是借助 VPN 支持远程访问，或他们已经无缝穿越了一个防火墙，但这些服务的存在无疑为他们带来了更高的自由度和可用性。不在办公室时，用户可能只知道需要点击远程访问图标，然后输入密码，但他们不知道或并不关心这些服务的运行机制。

思科智能网络服务，包括防火墙、web 安全、广域网优化和访客接入等，旨在通过互操作提供无缝、透明的解决方案。

用户服务

用户服务位于网络基础架构和网络服务层之上，直接面向最终用户。在建筑环境中，用户服务指的是楼内用户直接使用的一些服务，例如电梯、办公室照明或电话。比如早上上班时，我们乘电梯到达办公室所在的楼层，进入办公室后打开电灯，按下电话按键收听语音留言。基于网络的用户服务，如电话、企业资源规划（ERP）应用、电子邮件和其它业务应用等，依靠与网络相连的桌面或便携式平台来传输信息。众多网络架构中常见的用户服务包括思科统一通信、WebEx 协作和网真。

备注

网络基础架构

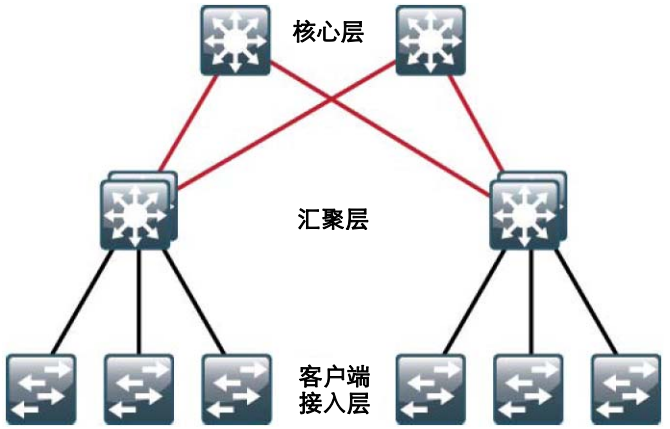
人们很容易将网络看作一个简单的管道系统，认为在设计网络时只需要考虑管道的大小和长度，或链路的速度和容量就行，其它都无足轻重。但是就像大型体育场或高楼大厦中的管道系统在设计时需要考虑尺寸、用途、冗余、防破坏或防故障措施，以及峰值承载能力一样，在设计网络时也应当考虑这些方面。由于用户依靠网络来获取工作所需的信息并可靠地传输语音或视频，网络必须具备永续、智能的传输功能。即使今天骨干局域网拥有大量带宽，仍然有一些性能敏感型应用容易受到抖动、延迟和丢包的影响。网络基础架构的功能就在于提供高效的容错传输机制，对应用流量进行区分，以便在网络出现短暂拥塞时做出合理的负载共享决策。不管用户采用的是有线还是无线网络连接、位于总部还是远程站点，网络都必须对流量实施优先级划分和排队，力争实现最高效的路由。

局域网和园区

大型局域网通常位于机构的总部或大型园区内。如果是在总部，局域网不但负责为本地用户提供连接，还充当着连接广域网、数据中心、服务器机房和互联网的枢纽，由此成为了网络的关键组成部分。在传统的有线局域网连接之外，本文的架构还包含无线局域网连接，用于支持用户移动性，并且允许将咖啡厅等功能单一的区域临时变成可全面访问网络资源的会议室。

大型局域网或园区网络需要高可用性（HA）设计，以支持推动机构正常运营的关键应用和实时多媒体通信。在其它许多局域网设计中，用于支持永续性的冗余链路处于备份和闲置状态。而在思科 IBA 智能业务平台——面向企业的无边界网络局域网设计中，所有链路都在积极地传输流量，这样不但避免了传统冗余设计的复杂性，还提高了网络性能。

图 2. 局域网层次化设计



为了适应用户由少到多的增长，网络工程师对局域网进行了分层设计。思科 IBA 智能业务平台——面向大型企业的无边界网络局域网可支持多达 5000 名用户，我们采用了分层方法来支持直观和无缝的可扩展性。

接入层是用户控制和操作的设备接入网络的位置。接入层可将以前成本不菲的千兆以太网或 802.11n 无线等高速连接作为标准配置提供。由于接入层承担着连接客户端设备与网络服务的任务，因此它在防止用户、应用资源及网络本身遭受人为错误和恶意攻击方面发挥着重要作用。接入层还可提供以太网供电、QoS 设置和 IP 电话语音 VLAN 分配等自动化服务，以降低运营要求。

网络汇聚层的主要作用在于，当某个地点需要多个接入层交换机来支持要求的用户数量时，它可以提供一个汇聚点。除简单的汇聚功能之外，许多设计中的分布层还充当 IP 第三层分组交换、路由和服务的第一站。由于分布层服务于大量的用户和接入地点，因此它需要具备 HA 设计，而这通常会为管理可用性和路径选择造成极其复杂的冗余链路和协议交织，如生成树协议（STP）和第一跳路由协议（FHRP）。在传统的双机箱分布层设计中，如果多个带有冗余上行链路的接入层交换机使用同一个语音或数据 VLAN，就会造成一个环路，STP 检测到环路后会通过关闭其中一个冗余上行链路来解决该问题。

这种主动的 STP 环路避免方法有几个缺陷：如果不关闭冗余上行链路，链路中断的恢复速度可能会显著降低；为了防止环路必须关闭冗余路径，而这会减少可用带宽；如果配置和使用不当容易发生错误，或导致单向通信故障。

图 3. 共享 VLAN 时的传统设计

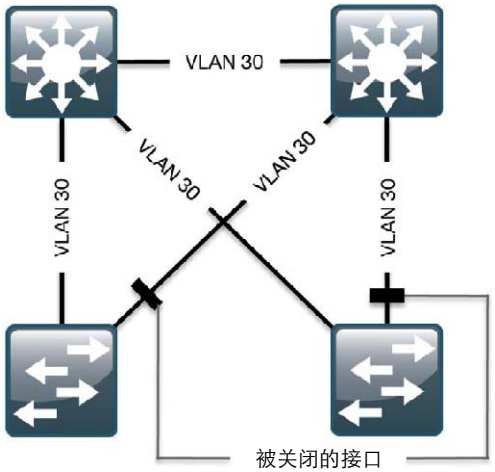
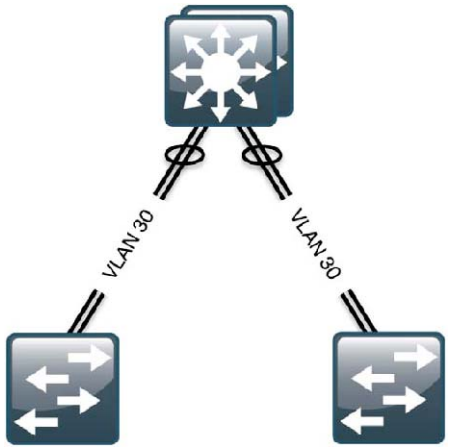


图 4. 共享 VLAN 时的简化设计



本文中的架构通过在分布层采用弹性的虚拟交换设计，对传统设计进行了改进。在虚拟交换设计中，两个物理交换机虚拟为单个交换机或一个机架，以此实现汇聚层设备冗余性，或使用单个带有冗余引擎和电源的交换机。这种简化的设计采用 EtherChannel 和多机箱 EtherChannel，来支持冗余接入层上行链路不间断传输流量。针对故障链路，EtherChannel 和多机箱 EtherChannel 能在毫秒级的时间内实现故障切换并消除 STP 环路。这种弹性设计无需 FHRP，将配置的复杂性降低了一半，简化了网络的故障排除操作，并能在发生故障时提供快速恢复。

优势:

- 弹性的汇聚层不但提高了故障恢复速度，还降低了复杂性
- 智能的接入层可在保持用户透明性的同时，防止用户和网络受到恶意攻击
- 冗余链路在传输流量时不会在网络中造成危险的二层环路
- 从较小的远程站点局域网到大型高密度园区局域网都采用统一的设计，降低了运营开支
- 不管用户接入总部局域网还是分支机构，都能获得一致的用户服务

核心层是局域网的第三层，也是最后一层。当有多个汇聚层在拓扑中存在而且只使用第三层 IP 路由链路时，核心层负责提供汇聚功能。由于它是大型局域网的核心层、广域网和互联网边缘的互联区域以及通往共置数据中心的连接点，因此核心层的设计遵循最高的可用性标准即 24x7x365。我们设计的核心层消除了复杂性较高或难实现的服务，以减少升级、维护或复杂配置更改过程中的计划内或计划外中断。核心层基于两个在物理上和逻辑上分离的交换机，实现了更高的可用性，同时又没有增加实现更多接入层服务的汇聚层的复杂性。

思科 IBA 智能业务平台——面向大型企业的无边界网络局域网降低了传统局域网的构建复杂性，同时增加了可用网络带宽，提高了永续性，简化了网络的部署、维护和故障排除工作。

无线网络

如果能让员工在任何地点都保持连接，企业将可以提高员工的工作效率和效益。有线端口网络设计能为身在办公室或其它有线网络覆盖的地点的用户提供连接，作为这一网络的组成部分，无线网络使用户能在前往会议地点的途中保持连接，而且可将咖啡厅或其它聚会场所改为临时会议室。借助无线网络，用户能够超越建筑物的物理限制，随时保持网络连接和信息的持续传输。

在思科 IBA 智能业务平台——面向大型企业的无边界网络架构中，无线网络采用 Wi-Fi 技术而非蜂窝技术来传输数据、语音甚至视频。

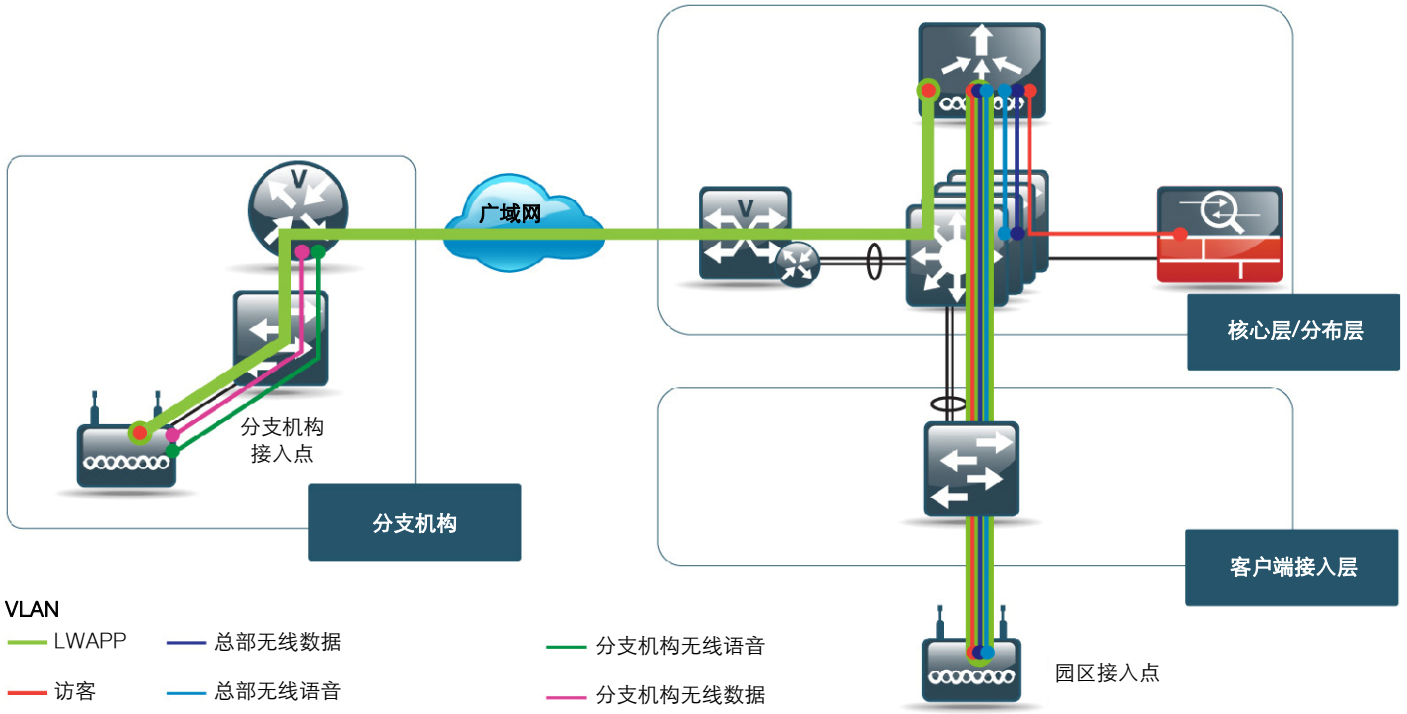
位于远程站点或总部的用户可以通过同样的方式连接到语音和数据服务，从而为企业创造了一个无缝的工作环境。

优势:

- 不受地点限制的网络访问提高了员工的工作效率
- 对于布线困难的地点，无需高成本的施工即可实现网络连接
- 对于分布式无线环境的集中控制，易于管理和运营
- 无线网络核心是一个预配置的即插即用型部署方案，可识别您连接到任何有线接入端口的新无线接入点

第一代无线局域网产品通常安全性不高，而且网络管理员难以对其进行管理。管理员自主配置和运行无线接入点，但是事实证明这是一种不可扩展的部署和运营模式。对于需要在总部和远程站点部署安全的无线基础设施的企业，这种传统的独立式接入点模式是一种成本高昂的解决方案。

图 5. 无线拓扑



思科的设计方案采用了集中式无线局域网控制器（WLC），能够对总部和远程站点的所有接入点进行控制。除了对无线接入点的集中管理之外，WLC 的集中控制方法还提供了许多其它优势。为确保安全地访问无线局域网，WLC 可支持所有用户基于一个公司目录进行身份验证，由此无需在每个接入点上保留单独的用户名和密码数据库。通过集成的访客模式，您可以为企业的重要访客和合作伙伴用户提供连接，他们的流量将与已验证的内部用户流量分开。您可以用多个 WLC 进行集群，来实现负载均衡、可扩展性和冗余性，实现系统维护并避免意外宕机的发生。

虽然 WLC 主要为总部和多数远程站点提供集中控制，您也可以在大型地点安装多个本地 WLC，以提供出色的漫游功能，同时保持中央管理。未安装本地 WLC 的远程站点的无线接入点允许非访客流量直接进入本地局域网，由此可以避免流量先传输到中央控制器，然后再返回远程站点，导致浪费宝贵的广域网带宽。

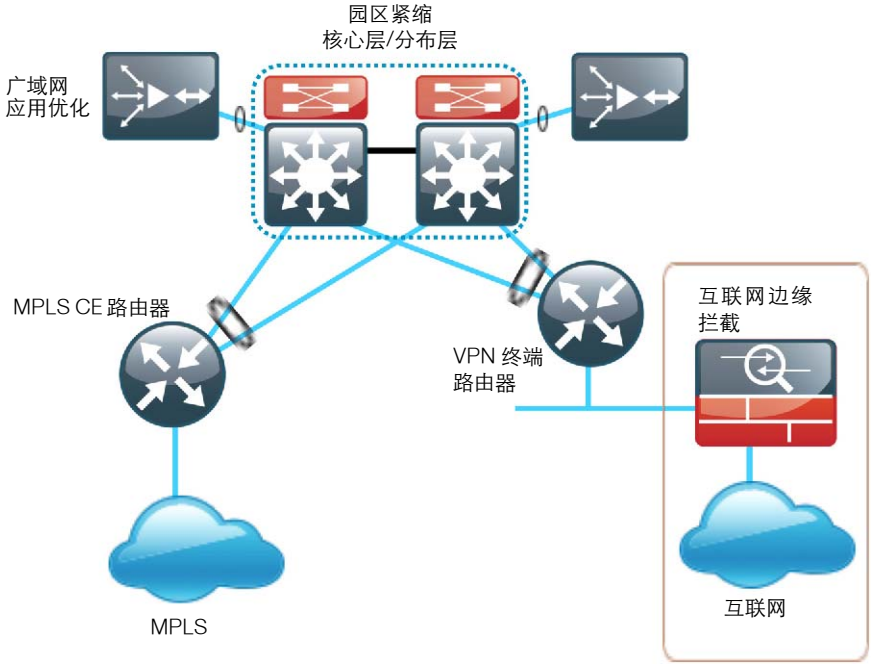
广域网和远程站点

不管是在总部还是在远程站点，信息访问和数据流的畅通与否将直接影响您日常工作的进行。企业对总部和远程站点的要求不尽相同，因此广域网架构必须具备灵活性和可扩展性。思科 IBA 智能业务平台——面向大型企业的无边界网络架构提供了一个强大的广域网设计，能够运用通用的技术和策略从较小的广域网规模扩展到 500 个远程站点。这种方法使该架构能够适应更多客户的部署要求，而无需大规模定制。此外，拥有小型广域网的企业还可以随着需求的增长以统一的方式构建并扩展广域网。

远程站点的专用网通过广域网连接到公共传输网络。远程站点是指员工代表企业经营业务的远程分支机构。远程员工需要获得与总部员工同等水平的应用访问权限，但远程站点的员工通常少于总部员工。根据远程站点业务的重要性和该业务能否移往他处，您可以采用不同级别的冗余性，以保护通信免受广域网中断的影响。典型的企业广域网能够互联所有的运营地点，并将所有远程站点流量汇聚到拥有共置数据中心的总部，或汇聚到一个包含主用或备份数据中心的独立运营地点。

广域网路由器的主要功能是在远程站点和应用所在的主站点之间传输数据。远程站点能够支持几个到数百个使用计算机、IP 电话和无线语音与数据服务的用户。远程站点路由器提供了一个公共平台，用于支持日益增多的服务和远程站点应用不断提高的性能要求。

图 6. 广域网 100 设计



优势:

- 通用的远程站点平台和集成服务降低了运营开支
- 基于 IP 的传输设计支持所有大型电信运营商的广域网连接服务
- 灵活、可扩展的设计提高了设计一致性，降低了复杂性
- 信息加密可保护在公共传输网络上传输的业务数据
- 远程站点连接包含基本连接选项和高永续性连接选项，以满足多种需求

公共广域网传输方案多种多样，从 MPLS VPN 到宽带互联网或传统的专用线路不一而足。思科架构设计基于 IP 分组传输，为保护互联网上数据的私密性提供了加密功能，由此适用于所有公共传输方案。其灵活性使您能够混合使用 MPLS VPN 服务和基于互联网的 VPN 重叠功能，提供多种连接选项，这样不但实现了永续性，还通过减少 IP 传输选项降低了复杂性。因此，现在企业可以利用标准的模块化方法构建适合自身需求的广域网。

不管用户位于总部还是广域网上的任何站点，他们都需要无缝地访问互联网服务。远程站点用户和总部用户获得的可用带宽可能有着显著的差别。可以通过应用优化和服务质量（QoS）等服务，来提高速度较低的广域网链路的性能。应用优化能够执行流量压缩、协议优化和拷贝流量缓存，从而提高广域网带宽性能。QoS 能够优先处理对延迟和丢包敏感的多媒体流量，还可以优先传输关键业务数据流量。本设计为总部或远程站点的用户提供了有线和无线数据、语音及视频访问。

互联网边缘

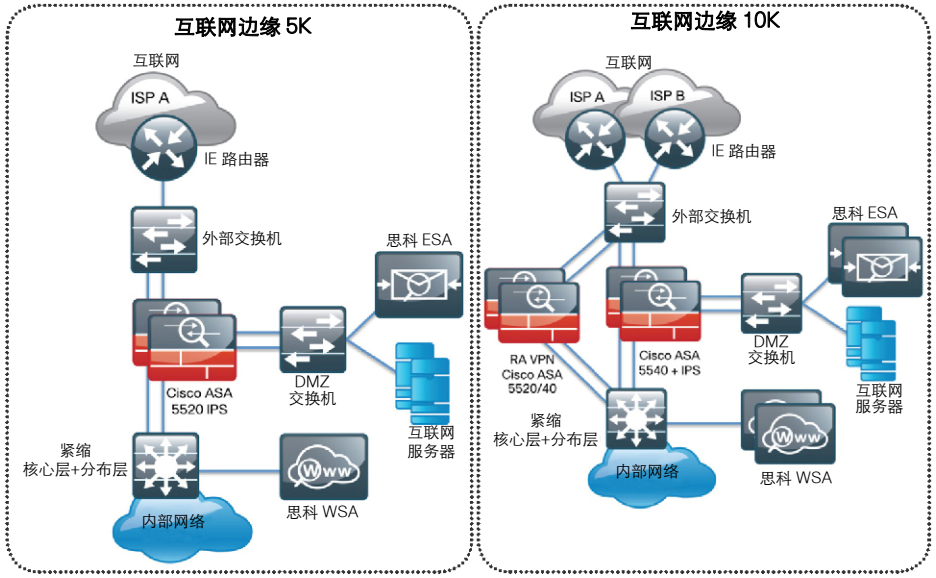
互联网边缘是企业进入互联网的网关。这一通往外部世界的网关必须提供安全的基础设施，以支持电子邮件和网络访问以及客户和合作伙伴对公司信息的公开访问。企业所面临的挑战在于，如何以一种安全的方式提供这种基本的接入服务，防止造成一个过度复杂的环境。

优势:

- 提供快速安全的互联网接入，提高生产效率
- 保护重要资产免遭互联网攻击，防止业务中断
- 利用高永续性设计避免单点故障
- 为面向基于网络的应用提供一个安全可靠的环境

常见的办法就是在互联网边缘部署防火墙、入侵防御设备和 VPN 设备，来保护网络接入。但是构建这种安全防护系统需要花费大量时间整合多个渠道和制造商的产品，对专业技术的要求也比较高。思科 IBA 智能业务平台——面向大型企业的无边界网络架构提供了一种简化的设计，可减少需要使用的网络设备，同时不影响可扩展性、安全性或永续性。由于互联网边缘设计的每个部分都提供有扩展可选方案，因此企业可以根据自身需求混合搭配各种服务可选方案。

图 7. 互联网边缘 5K 和 10K 设计



互联网边缘的防火墙作用在于负责对访问 DMZ 服务的互联网主机、访问互联网服务的内部主机以及访问内部和外部服务的 DMZ 主机进行接入控制。资源访问和授权使用方面的具体策略必须符合企业的安全策略。作为网络基础架构的一部分，互联网边缘设计使企业能够灵活控制用户的连接方式和允许的访问类型。防火墙采用完全冗余的配置，而且可以利用单个或双重互联网接入进一步减少单点故障，实现高可用性。

互联网网关使企业暴露在蠕虫、病毒、僵尸网络和其它攻击的威胁之下。防火墙中集成的入侵防御系统（IPS）模块可对防火墙策略准入的流量进行进一步检查，以检测和消除攻击。IPS 模块将检查流量来源的信誉，以快速决定是否阻挡流量。基于信誉的过滤使 IPS 模块能够根据信息源的信誉拦截两倍数量的攻击，从而提高可扩展性，此外它还可以不依赖签名提供零攻击防护，同时减少误报。

企业的形象和声誉通常与其互联网边缘的 web 服务器的能力有关，即能否为客户或合作伙伴提供高效的信息或应用访问。IT 机构面临的重大挑战在于如何可靠地交付这些应用和资源。应用交付技术能够帮助 IT 机构提高应用的可用性、性能和安全性。互联网边缘的应用感知服务器负载均衡器（SLB）可提供核心服务器负载均衡功能，将会话路由到最佳的服务器，同时防止正在运行的服务器上出现无效服务。安全和虚拟化服务支持服务器分割和基于角色的精确管理。这些服务与先进的应用加速相结合，为面向互联网的 Web 应用提供了一个健壮的架构。

为了提高生产效率，企业始终在不断进行业务扩张、提高员工移动能力并与研发机构和商业建立合作伙伴关系。利用传统的专用线路或拨号连接来提供连通性的成本极高，不是一种可行的方案。在思科的设计中，防火墙的另一个功能是提供集成 VPN，为员工、承包商或合作伙伴提供对企业网络的远程访问。系统将根据企业认证资源的策略控制和认证方式提供远程访问准入连接。灵活的 IPsec 和 SSL VPN 接入拥有与防火墙和 IPS 同样的 HA 设计。

防火墙和 IPS 提供了周边防御和检测功能，但如何才能确保员工正确使用互联网接入或防御而被嵌入在授权应用中的攻击呢？互联网边缘设计包含网络安全服务，可过滤电子邮件和确保网络冲浪安全及控制。

在这种综合设计中，只需少量思科设备即可满足互联网边缘的核心安全要求，这些设备由思科通过一个基于可扩展解决方案的方法开发而成，旨在满足企业的需求。

备注

网络服务

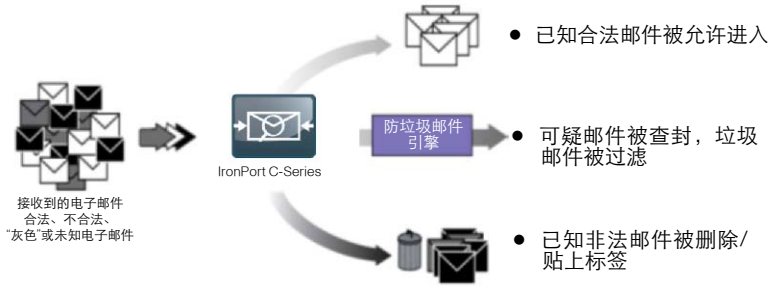
安全性

安全产品是每个网络部署不可或缺的组成部分，也可以作为网络基础架构的一部分，比如在互联网边缘就是如此。安全产品也可以作为一种服务部署，用于保护特定的使用案例或应用。法规遵从、信息保护、以及网络和桌面可靠性策略都要求您将安全服务融入基础设施中，而不是在事后进行添加。

优势:

- 防止电子邮件受到 SPAM 和嵌入式攻击的威胁
- 利用互联网上的攻击和攻击爆发信息，实现最可靠的威胁防御
- 为员工和合作伙伴提供安全可靠的远程接入
- 为基于硬件和基于软件的 VPN 客户端提供最大的灵活性
- Web 接入可允许使用控制策略，支持对浏览互联网的用户进行风险管理

图 8. 电子邮件安全性



对某些机构来说，电子邮件可能与电话服务一样重要，但是当前网络中的电子邮件却饱受两大问题的困扰。首先是大量不受欢迎或未经请求的电子邮件（垃圾邮件）浪费了用户的时间和资源，其次是电子邮件可以利用网络钓鱼攻击诱使客户发送敏感信息。思科 IBA 智能业务平台——面向大型企业的无边界网络架构无缝集成了一个基于电子邮件安全应用的解决方案，可利用多种机制提供强大的垃圾邮件和病毒过滤功能。该解决方案采用了基于信誉和基于上下文的过滤器，这些过滤器通过自动的每日攻击信息更新获取最新消息，以抵御垃圾邮件和病毒攻击。

越来越多的用户需要访问互联网上的 web 应用，对于未采取保护措施的用户，这一趋势加剧了他们受到嵌入式攻击的风险。思科架构中的 Web 安全性通过一个代理服务实现，该服务采用基于类别和基于信誉的控制、恶意软件过滤和数据保护措施，来防止资产受到恶意网络内容的影响。系统集成了不断更新的信誉数据库和动态内容分析功能，以实时判断内容的类别。Web 安全服务还提供可接受使用规则，确保用户不会访问非法内容。

随着企业逐渐认识到提高员工移动性和灵活性的重要性，在公司外部或远程站点访问网络的能力现已成为企业关注的焦点。借助远程接入，出行在外或是在家办公的员工可以收发电子邮件、访问网络应用或更新日程安排。许多公司利用远程接入为合作伙伴提供安全可靠的资源访问，同时利用安全策略控制他们能够访问的资源类型。本文的设计方案通过软件或硬件客户端为用户提供了安全的远程接入。SSL VPN 解决方案为用户和合作伙伴访问公司网络提供了最高的灵活性和安全的连接，即使他们是从公司无法管理的外部设备（如员工的家用电脑）接入也不成问题。该解决方案还支持现有的基于 IPsec 的设计，使企业能够根据自身需求定制设计。随着远程员工数量的增多，企业需要硬件 VPN 解决方案来支持更全面的远程或家庭办公解决方案，为桌面电脑和公司电话分机等多种设备提供 24x7 全天候安全访问。思科 IBA 智能业务平台——面向大型企业的无边界网络解决方案为在家办公的远程员工提供了与在办公室一样的工作体验。

应用优化

应用优化通过消除重复的数据和缓存服务保证了广域网带宽的最佳利用，从而提高了网络效率。在许多情况下，企业通过减少现有的非优化网络流量，可以避免在部署新应用时为广域网链路增加带宽。借助应用优化，IT 部门能够将远程站点的应用服务器集中放置在数据中心，同时可通过优化繁琐的局域网协议保持本地应用的性能。

您可以将应用层优化解决方案作为集群设备部署在广域网汇聚层，实现可扩展和永续的运行，也可以将此功能集成在远程站点路由器中，以减少占地面积，简化运营。该设计所采用的统一方法不受设备外形的限制，简化了部署和管理。此解决方案将把流量透明地重新定向到应用优化引擎，以最大限度降低对应用的影响，减少单点故障。思科广域网优化所采用的无隧道方法意味着，QoS 策略能够互操作同一链路上的优化流量和延迟敏感型多媒体流量。

优势:

- 通过优化传输的数据推迟成本高昂的广域网带宽升级
- 通过服务集中化，在不影响性能的前提下推动 IT 整合，最大限度降低每个远程站点的成本
- 通过集中管理所有的广域网优化引擎，简化管理，提供带宽节约反馈信息
- 通过服务器和存储集中化增强数据保护

访客与合作伙伴无线接入

企业经常接待各种来访者，他们在访问期间也需要访问网络。这些访客包括客户、合作伙伴和供应商，根据他们来访的目的，他们造访的公司部门和运营地点也有所不同。为了帮助这些访客用户保持高效工作状态并履行工作职责，您应该在网络内部全面部署访客接入，而不仅仅是在公司前台或会议室。

优势:

- 访客在贵公司造访期间生产效率更高，对贵公司帮助很大
- 员工和访客使用同一个基础设施，降低了成本和复杂性
- 安全的传输使访客流量能够与内部网络流量分开
- 访客接入由 IT 控制，但可由管理人员提供服务

思科 IBA 智能业务平台——面向大型企业的无边界网络架构具备出色的灵活性，允许无线网络在为员工提供无线语音和数据访问的同一无线接入点和控制器基础设施上提供访客接入。这种集成能力通过在单个基础设施上提供多种服务，简化了网络运营，降低了资本支出和运营支出。

思科架构的关键优势就在于，可确保访客网络接入不影响网络的安全性。总部和各远程站点的每个接入点都可以配置为受控的开放式无线连接。从无线接入点，访客流量将通过单独的网络隧道传输到位于互联网边缘 DMZ 的访客无线控制器。流量将从无线访客网络直接传送到负责保护公司私有资产的防火墙。

为了控制访客和合作伙伴的无线连接，访客用户将被转到登录界面，他们必须提供用户名和密码才能进入访客网络。前台接待人员或其他礼宾人员可以为他们提供一个临时访客账户，需要每天或每周更换一个新密码。这种高度灵活的设计使企业能够根据需要定制控制和管理措施，同时保持网络架构的安全性。

用户服务

大多数用户对于用户服务层非常熟悉，因为这一层负责提供用户日常使用的各种服务或应用。架构中的其它组件和应用都是为支持用户服务层而设。不管是打电话、查看语音留言、收发电子邮件，还是登录企业资源规划（ERP）应用，用户服务层都是用户体验的第一站。面向用户的应用或产品的设计直接影响着其易用性，用户服务与网络服务之间的交互情况也直接影响着用户服务在网络内部运行时的性能。思科设计的架构可支持用户在网络基础设施上轻松使用这些数据、语音和视频服务。

商业应用服务

企业在互联网上的表现对于业务的成功至关重要。即使简单信息门户的停运也会导致商业机会的丧失。电子邮件、电子商务、网络门户和 ERP 等关键应用必须全天候服务于内部和外部用户，以提供不间断的商业服务。网络过载、服务器宕机、应用故障或资源使用效率低下（即某些低耗资源负荷过高，某些高可用性资源闲置）都可能威胁到这些应用的可用性。互联网边缘的高可用性设计提供了冗余的防火墙、局域网交换机、路由器、ISP 连接和 IPS 来保护应用可用性。设计中最重要的高可用性服务之一是应用级服务器负载均衡，它能够检测应用和响应服务器故障并采取措施。除主流的第四层到第七层交换功能之外，服务器负载均衡还提供多种加速和服务器卸载特性，包括 TCP 处理功能卸载、SSL 卸载、压缩和其它各种加速技术。SLB 环境也可通过虚拟化分成多个逻辑设备，这些设备在拓扑、资源和功能使用以及管理方面可以单独配置，从而降低拥有成本。

通信与协作服务

通信和协作服务的发展改变了我们的工作和生活方式。多年来，计算机的角色在不断演变，已经从最初的文件处理和系统接入工具发展为了支持日常通信和协作的工具。桌面计算机与座机、手机和其它计算机以多种方式进行交互，共享信息。协作服务使我们能够灵活地改变沟通对象、沟通方式和沟通时间。随着我们利用便捷、安全的协作工具与公司内外的各种群体，包括合作伙伴、客户和知识型员工等进行合作，我们的沟通对象变得更加广泛和多样化。随着企业采用随时随地的业务运作模式来加速业务决策，用户不必再长时间在办公室工作，工作时间也变得灵活多变。而随着工作时间的变化，我们工作的地点也发生了相应的改变。利用移动功能和无线服务，我们可以在办公室开展业务，或者在家中参加清晨或晚上的会议，或是在机场等候航班的时候处理业务，或者利用视频协作避免出差。

以下章节介绍了贵公司可以采用的几种思科通信和协作服务。

统一通信

思科统一通信（UC）产品系列旨在为几个到数万名用户提供语音和视频通信服务。IP 通信解决方案和终端可帮助您将统一的通信服务扩展到所有工作地点的用户，不管他们是在总部局域网、远程站点、家中还是出行路上。Cisco Unified Communications Manager（Unified CM）是一个可扩展、可分布的高可用性企业级 IP 电话呼叫处理系统，既能提供传统的电话功能，也能提供移动、保持在线和偏好选择等高级功能。借助思科 IP 通信解决方案，企业还能利用现有的电话号码在互联网上发起高度安全、高质量的公司间语音和视频电话呼叫，从而提高通信系统的效率。Cisco Unified IP 电话可支持多种通信要求，包括视频交互、Wi-Fi 集成、高清晰语音等。如果与思科局域网交换机相连，这些 IP 电话还能协商参数，从而实现电源、QoS、VLAN 分配和基础设施安全设置的自动化。Cisco Unified Survivable Remote Site Telephony（Unified SRST）在远程路由器上的思科 IOS 中运行，当远程站点与 Unified CM 所在的主站点之间的连接发生中断时，能够为远程站点提供备份呼叫控制。呼叫处理资源的集中化降低了部署成本，同时保持了高可用性，而且能够与远程站点路由器提供的网络服务进行协作。

WebEx——视频协作

传统的会议局限于让参会人员在一个地点进行面对面的讨论，而现在的会议可以跨越多个边界和时区，有效地覆盖广大的区域。Cisco WebEx 解决方案可以通过任意系统、平台和浏览器或设备，满足更广泛的员工需求，从而帮助贵公司实现按需召开无边界会议的目标。WebEx 利用网络基础架构和服务提供了专门的电信运营级云计算服务，为灵活的实时网络会议、网络研讨会和网络广播提供了强大的支持。面向思科 ASR 路由器的 WebEx Node 网关卡提供的网络服务能在互联网边缘对数据和视频流进行本地复制，而不是在网络上发送所有流量，从而节省带宽。会议控制和管理以云计算的方式执行，提供了一个无缝、透明的解决方案。WebEx 功能可扩展到无线智能电话，通过应用插件模块来简化会议接入，同时支持浏览幻灯片和使用其它会议协作工具，进而满足移动用户的需求。

网真——视频协作

许多会议都需要进行面对面交流。在以前，这便要求所有的参会者必须同处一室，而思科网真解决方案创建了一种与面对面会议一样实时、逼真、与真人比例大小相同的通信体验。由于能够跨广域网同时向多个地点高效地传输高清视频和音频，企业可削减差旅成本，缩短会议延迟。有了思科统一通信解决方案的集成，使会议的召开如同拨打电话一样简单。WebEx 协作和现有的视频会议系统可添加到实时会话中，这进一步提高了功能的多样化。网络的集成有助于确保可靠性，并借助永续的网络基础架构和 QoS 提供了最佳体验。

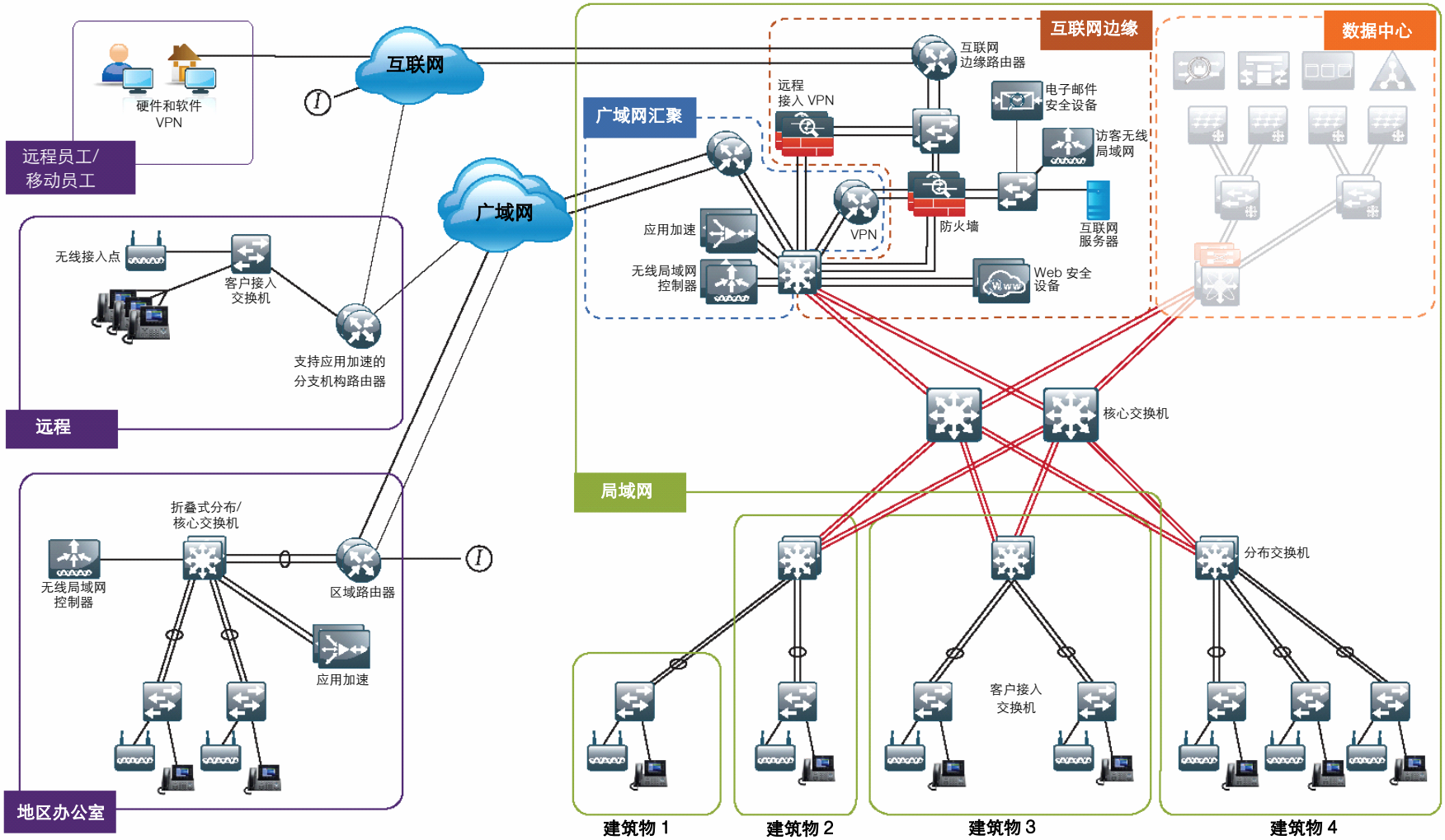
备注

思科 IBA 智能业务平台——面向大型企业的无边界网络设计指南总结

信息流顺畅与否是影响企业运营状况的关键指标。为了这一目标，企业力争将数据、语音和视频融合在单个强大的网络中，实现高效的部署、运营、故障排除，并降低复杂性和成本。

思科 IBA 智能业务平台——面向大型企业的无边界网络架构由三个模块化组件构成，分别是网络基础架构、网络服务和用户服务。三者相互依存，呈层次化独立结构，每层都以下面的一层为基础。三个层必须作为一个整体协同运行，才能提供企业运营所需的数据、语音和视频流量。

图 9. 企业无边界网络概览



思科 IBA 智能业务平台——面向大型企业的无边界网络设计基于最佳实例和已部署过的拓扑提供了一个正规性的解决方案，其网络可扩展性选项可适应公司的多种需求。配套的部署指南和产品配置指南为解决方案的部署提供了逐步指导。为了增强企业架构，我们提供了大量补充性指南，专门阐述对解决您的业务问题有重要帮助的具体功能、技术或特性。思科致力于简化贵公司网络的采购、部署和维护流程，同时在部署的产品中嵌入了智能特性。这些产品经过严格筛选和兼容性测试，专门用于构建无边界网络。

为贵公司的网络部署 IBA 智能业务平台，将有助于确保网络基础设施的可靠性、稳固性和安全性，从而高效传输对于企业成功至关重要的信息。

备注

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

C07-610749-02 06/11