

## 基础设计概述

● ● ● 智能业务平台

# 前言

## 本指南的目标受众

Cisco®智能业务平台（IBA）指南主要面向承担以下职务的人员：

- 需要实施解决方案时的标准规范的系统工程师
- 需要撰写思科IBA实施项目工作说明书的项目经理
- 需要销售新技术或撰写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，您也可以将思科IBA指南作为工程师之间技术交流、项目实施经验分享的统一指导文件，或利用它更好地规划项目成本预算和项目工作范围。

## 版本系列

思科将定期对IBA指南进行更新和修订。在开发新的思科IBA指南系列时，我们将会对其进行整体评测。为确保思科IBA指南中各个设计之间的兼容性，您应当使用同一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。我们以某系列指南发布时的年份和月份来对该系列命名，如下所示：

年 月 系列

例如，我们把于2011年8月发布的系列指南命名为“2011年8月系列”。

您可以在以下网址查看最新的IBA指南系列：

客户访问：<http://www.cisco.com/go/cn/iba>

合作伙伴访问：<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
```

系统输出或设备配置文件中值得注意的部分以高亮方式显示，如下所示：

```
interface Vlan64  
ip address 10.5.204.5 255.255.255.0
```

## 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 .....	1	网络服务 .....	12
关于IBA.....	1	虚拟化.....	12
关于本指南.....	1	安全性.....	12
简介 .....	2	应用优化.....	13
业务概述 .....	3	服务器负载均衡.....	13
架构原理.....	3	访客无线接入.....	14
架构概述 .....	4	用户服务 .....	15
网络基础.....	4	企业应用服务.....	15
网络服务.....	5	统一通信.....	15
用户服务.....	5	Web会议和思科WebEx®解决方案.....	15
网络基础 .....	6	设计指南总结.....	16
局域网.....	6		
广域网和远程站点.....	8		
无线连接.....	9		
互联网边缘.....	10		

本手册中的所有设计、规格、陈述、信息和建议（统称为“设计”）均按“原样”提供，可能包含错误信息。思科及其供应商不提供任何保证，包括但不限于适销性、适合特定用途和非侵权保证，或与交易过程、使用或贸易惯例相关的保证。在任何情况下，思科及其供应商对任何间接的、特殊的、继发的或偶然性的损害均不承担责任，包括但不限于由于使用或未能使用本手册所造成的利润损失或数据丢失或损害，即使思科或其供应商已被告知存在此类损害的可能性。这些设计如有更改，恕不另行通知。用户对于这些设计的使用负有全部责任。这些设计不属于思科、供应商或合作伙伴的技术建议或其它专业建议。用户在采用这些设计之前应咨询他们的技术顾问。思科未测试的一些因素可能导致结果有所不同。

文中使用的任何互联网协议（IP）地址均非真实地址。文中的任何举例、命令显示输出和图示仅供说明之用。在图示中使用任何真实IP地址均属无意和巧合。

© 2012 思科系统公司。保留所有权利。

# 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企业需求的解决方案，而不必担心技术复杂性方面的问题。

了解更多信息，请参阅《思科IBA使用入门》文档：

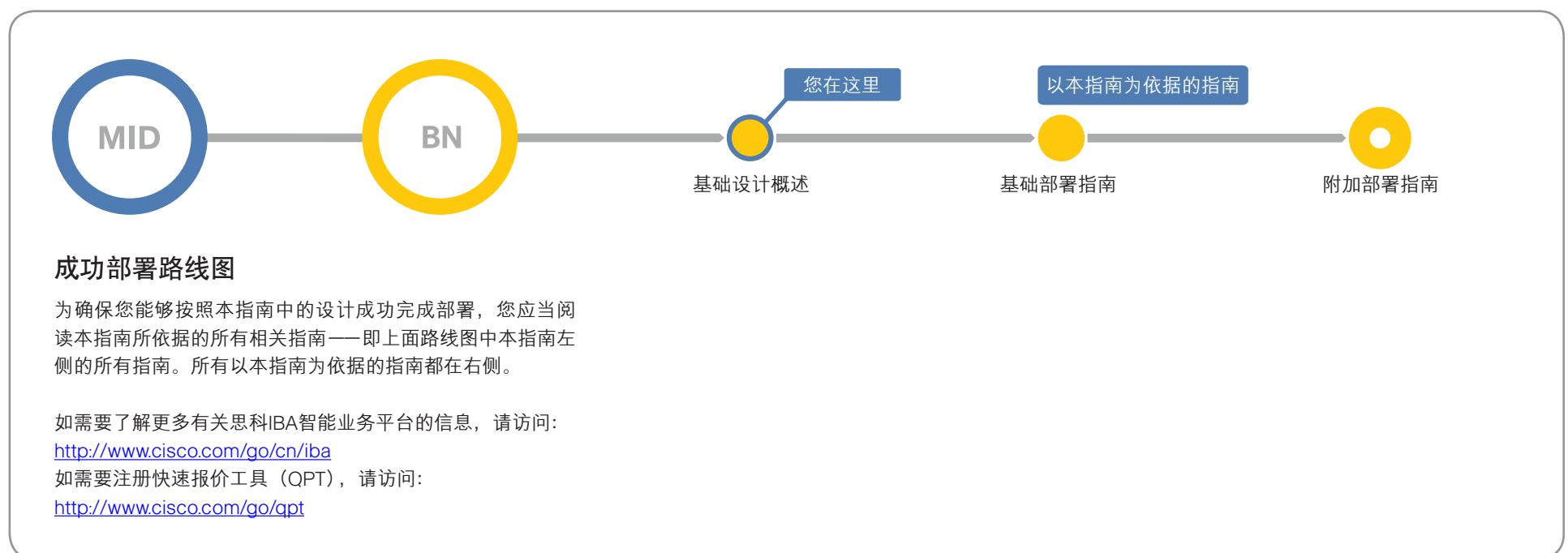
[http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless\\_Networks/Smart\\_Business\\_Architecture/SBA\\_Getting\\_Started.pdf](http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf)

## 关于本指南

此附加部署指南包含以下章节：

- **业务概述** — 您的企业所面临的挑战。业务决策者可通过本章内容来了解介绍的解决方案与其企业运营的相关性。
- **技术概述** — 思科如何应对上述挑战。技术决策者可以利用此章节的内容了解解决方案的工作原理。
- **部署详情** — 解决方案的具体实施步骤介绍。系统工程师可以在这些步骤的指导下快速可靠地配置和启用解决方案。

本指南假定您已经阅读了本指南所依据的指南，如成功部署路线图中所示。



# 简介

面向中小企业的思科®智能业务平台（IBA）无边界网络是一项全面的网络设计，适用于多达1000到2500名用户的环境。该架构结合了局域网（LAN）、广域网（WAN）、无线、安全、应用优化和基础设施组件来支持统一通信技术，提供全方位解决方案。

这一解决方案级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，使您可以自由选择真正满足企业需求的系统组件，而不必担心技术细节问题。

Cisco IBA的设计基于以下原则：

- **灵活性与可扩展性**——随着企业的发展，基础设施也必须随之扩展。因此所选择的产品必须具备可扩展性或能够在架构中进行重新定位。
- **重复使用**——我们的目标是在各种模块中尽可能重复使用相同的产品，以最大限度减少必须作为备件保存的产品的范围。
- **易于使用**——一个首要要求是开发的设计方案能够在部署时最大限度减少配置工作，且易于管理。
- **经济高效**——在选择产品时的另一个关键要求是符合中小企业的预算标准。

备注

# 业务概述

数据网络已成为企业取得成功所必须投资的一项重要资源。一个永续的高性能网络能够帮助确保企业成功实现目标。相反，设计低劣的网络则会阻碍企业的发展。如果网络能够可靠、有效地解决用户的数据访问和协作要求，则企业运营的各个环节都会更加高效。

依赖于数据网络来支持日常运营的企业必须解决以下网络设计和部署要求：

- 能够支持各种业务使用情况的标准化设计，以消除不确定因素并减少新购设备的闲置时间
- 专为中小企业设计但能提供出色的企业级可靠性的产品
- 能够确保随着企业在以下各个方面增长轻松进行升级和扩展的灵活架构：单个站点的规模、总的站点数量、企业员工数目，以及构成网络的终端数量和类型。
- 无论采用何种网络接入方式均提供一致的用户体验：在公司总部、远程站点或远程接入VPN的有线和无线网络连接
- 安全性与高可用性保障企业信息资源、服务器和互联网应用
- 不断提升广域网性能，同时降低网络管理成本
- 一款能够由具备中等技术水平的IT员工进行部署和运行的解决方案

## 架构原理

决定用户能否获得良好的应用使用体验的因素有许多。以简单的Web浏览器为例：我们打开一个URL，对应的页面在几秒钟内呈现在我们面前。为了获得较好体验，所有三个特定的层都需要协同运行，将Web内容交付给用户：

- 一个作为基础平台的网络
- 后台运行的网络服务，能够在用户无察觉的情况下提供和改进用户体验；
- 用户直接与之进行交互的应用或终端，称作用户服务。

数据网络必须能够支持企业充分发挥其投资在现代应用软件平台的能力。相比十年甚至五年以前，数据网络必须为应用数据提供更高速度和更广泛的支持，特别是语音和视频协作流量，以及在私有云和公共云服务平台上托管的应用。虚拟化桌面环境、广泛的用户终端、以及台式机与服务器机房之间的紧密集成，都要求网络提供一个快速稳定的平台，以确保应用能够出色运行，满足生产效率要求。

对于员工生产率依赖于不间断通信、应用和数据资源访问的企业来说，网络在其运营中起着至关重要的作用。通过采用分层方法，并以经过测试、可互操作的设计来构建网络，您将可以降低风险，减少运营问题，同时加快部署速度。

# 架构概述

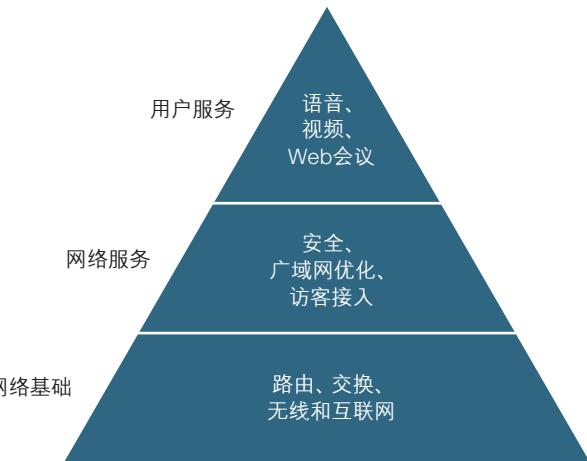
作为一种流程，建筑指设计和建造建筑物与其他物理结构的活动，主要用于提供庇护场所。更广义上的建筑通常包括整体环境的设计，从建筑物如何与周围风景融为一体的整体层面，到架构或建设细节，甚至是家具等微观层面。再广泛地说，架构设计在最广泛的意义上是设计一个为消费者提供实用服务的完整系统的活动。

同样地，面向中小企业的思科IBA无边界网络是使用结构化流程创建的系统，有助于确保重要业务流程和资产的稳定性。思科IBA智能业务平台侧重于多个关键方面：

- 由思科测试和提供支持的标准化设计可降低成本并帮助您加速思科技术的实施步伐
- 优化的架构，可支持拥有多达2,500名用户和75个远程站点的中小企业
- 灵活的架构，能够帮助保护您的投资，确保随着企业的发展轻松进行迁移
- 无缝支持有线和无线网络访问的快速部署，以支持数据传输、语音、远程员工和无线访客
- 安全性与高可用性，保障企业信息资源、服务器和互联网应用
- 通过应用优化提高广域网性能，降低成本
- 简化的设计，可由持有思科CCNA®认证或具备同等经验的IT员工进行部署和运营
- 专为对价格敏感的中小企业设计，依托思科产品出色的性能和可靠性

面向中小企业的思科IBA无边界网络可以分成三个主要的模块化而又相互依存的组件。它们是网络基础、网络服务和用户服务，三者之间存在着架构上的互相依赖关系，如下图所示。

图1. 思科IBA智能业务平台组成部分



## 网络基础

网络基础是面向中小企业的思科IBA智能业务平台的关键组件。与建筑物地基类似，网络基础为所有依赖于它的组件或服务提供了一个平台。作为一个独立的层面，网络基础有助于确保从一端可靠地发送信息，并在另一端接收。普通用户完全不需了解其如何实现，他们只知道，当他们点击鼠标，视频就开始播放，电子邮件开始发送或订单就开始处理，一切都这么简单自然。

正是思科智能基础设施设备，如交换机、路由器和无线设备等，使网络基础在后台卓越的发挥作用。

## 网络服务

网络服务位于网络基础之上。网络服务就像是建筑物的门、窗和锁。如果没有这些部件，建筑物只是一个密闭的盒子。而添加了这些服务，基础设施才能变成真正可以发挥作用的结构，为企业资产提供可靠性、安全性和可用性。一些用户了解网络服务提供的价值，但并不直接与这些服务进行交互。以VPN远程接入为例，用户需要启动VPN客户端来访问企业资源，但他们无需确切了解或关注这些服务是如何运行的。只要用户能够从所在地即时访问数据，他们就知道网络服务层工作正常。

思科的智能网络服务包括虚拟化、防火墙以及其他安全设备、应用优化和访客接入等。

备注

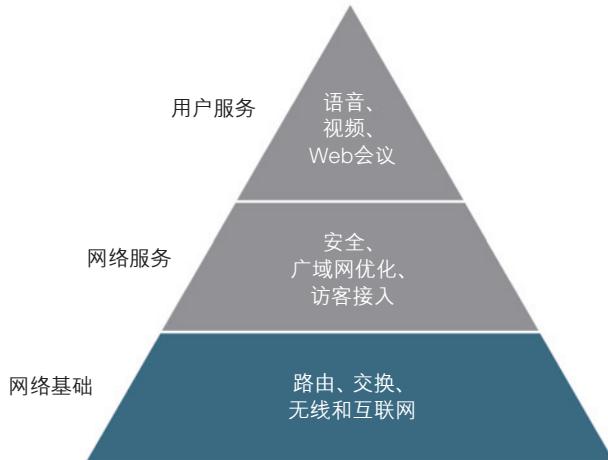
## 用户服务

最后，用户服务位于网络服务之上。用户服务就像是建筑物中的公用设施，包括水、电、电话、互联网和有线电视服务。用户通常需要在一天中直接使用这些服务。早上，开灯，电话响铃，有水可供清晨饮用。之后，利用普通公用设施，建筑物成为了舒适的工作场所。一些常见的用户服务包括电子商务应用软件、CRM系统、电子邮件和即时消息等。思科特有的用户服务包括思科统一通信以及协作、语音和视频系统。

# 网络基础

大多数用户认为网络只是一个公用传输机制，将数据尽可能快地从一点传输到另一点；其特点可总结为“快速信息馈送”。事实上，网络影响着所有通信流量，因此必须了解最终用户要求和提供的服务。即使在无限带宽环境中，时间敏感型应用也会受到抖动、延迟和丢包现象的影响。作为我们所有会话信息的传输层，其设计和运行对于所有服务都很重要，决定着在此平台上运行的任何服务能否成功。

图2. 网络基础



网络基础提供了一个高效的容错传输层，可将不同应用区分开来，以帮助确保每个应用都能够获得一定份额的资源，并保持所需的服务级别。在该架构内，有线和无线连接选项提供了先进的优先级划分和排队机制，作为实现综合服务质量（QoS）的一部分，确保资源得到最优利用。

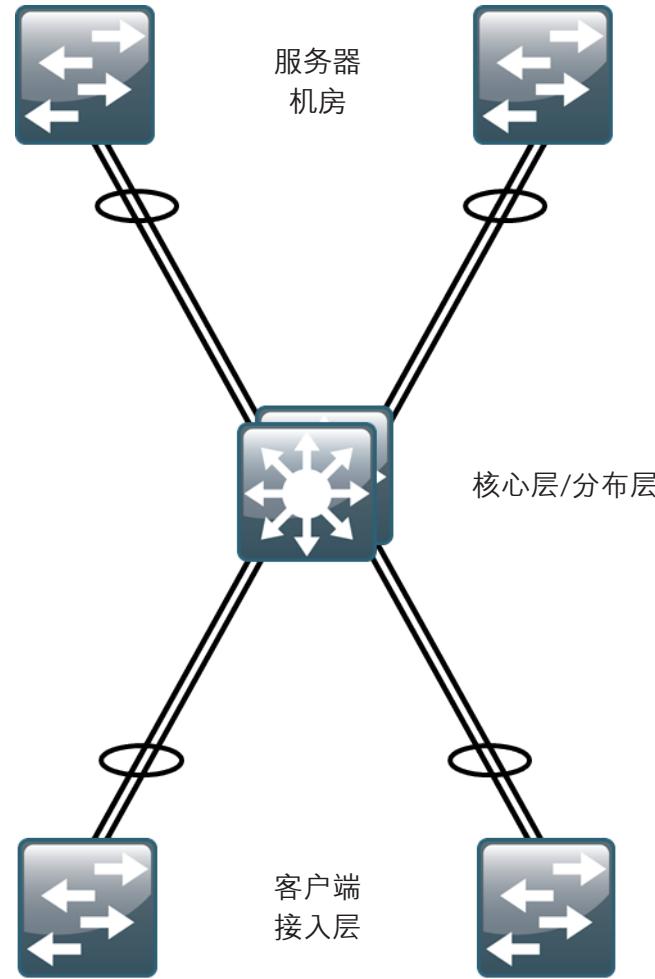
## 局域网

位于总部的局域网（LAN）核心层是网络的通信中枢。它将到总部的客户端访问进行汇聚，并为广域网（WAN）、服务器机房和互联网边缘提供了骨干连接，是网络中的关键组件。局域网需要具备高可用性，以支持关键任务应用和实时媒体。过去，高可用性意味着需要部署冗余、闲置的链路。而采用面向中小企业的思科IBA智能业务平台后，所有网络连接都将处于活跃状态，并真正传输流量。

局域网架构中的关键组件是Cisco Catalyst交换机系列。它可为思科客户带来以下优势：

- 永续的核心层，能够针对实时媒体流量提供极快的故障恢复
- 降低配置复杂性，简化了故障排除
- 充分利用所有网络链路，不会出现冗余配置中链路闲置的情况。

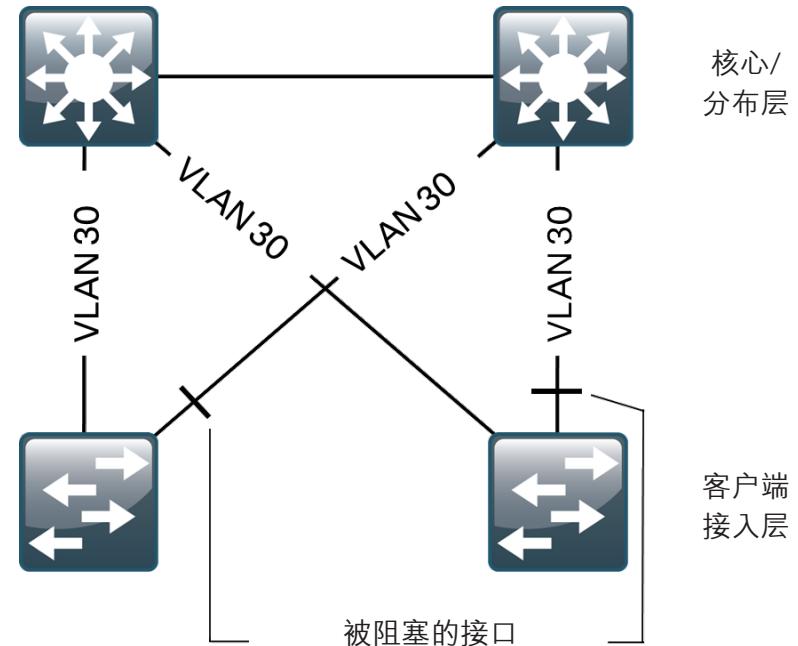
图3. 永续的局域网设计



在许多设计中，高可用性会增加复杂度，使网络故障排除更为困难，降低网络的易用性，迫使用户在高可用性和易用性之间进行取舍。与传统的双核心设计相比，面向中小企业的思科IBA无边界网络局域网设计能在保持可用性的同时降低复杂度。永续核心层将所需的核心层配置工作减少了80%以上，也简化了网络故障排除，在发生故障时仍能极为快速地恢复。

在传统的双核心设计中，多个接入层交换机使用同一个VLAN，且运行生成树协议（STP）来防止网络中发生二层回环。STP有两个主要缺陷——它从故障中恢复较慢，需要几秒甚或更长的时间（如果网络流量为语音或视频等实时媒体，若这一时间过长，则难以接受），另外它会阻塞网络中的冗余链路，从而将可用带宽减半。在双核心网络中，是通过主动调整STP和为每个接入层交换机配置独特的VLAN，来解决这些问题的。

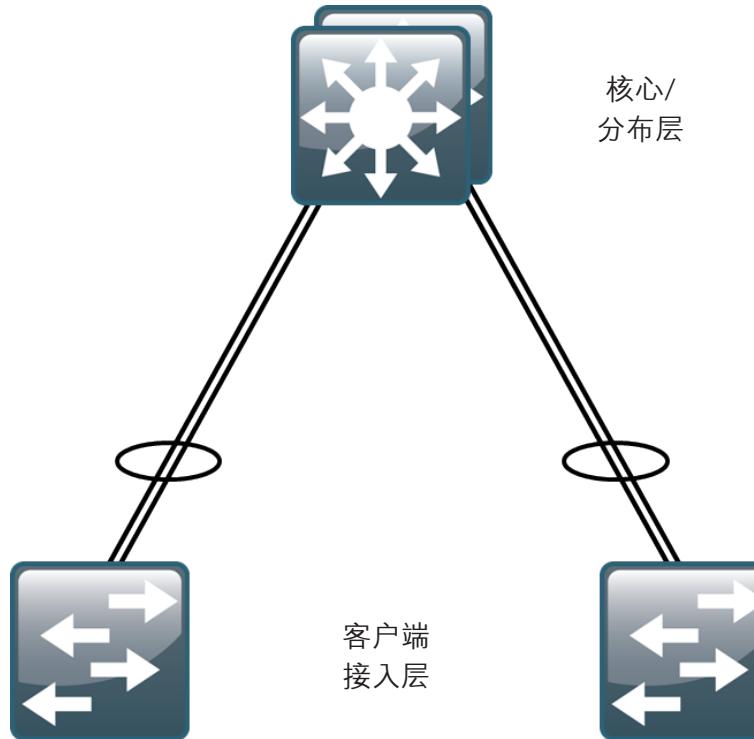
图4. 传统的双核心设计



而在多服务网络中，用户在一个普通工作日中就会访问四、五个VLAN。因此，为弥补STP的不足，需要在双核心设计中配置的VLAN和子网数目会十分巨大。

面向中小企业的思科IBA无边界网络核心层设计轻松解决了这些问题，因为它不依赖STP进行故障恢复，所以多个接入层交换机能使用一个VLAN。下一代局域网设计不必进一步调整，就能实现快速恢复。

图5. 思科IBA局域网：提高的永续性和性能



客户端接入层是由用户控制的和用户可访问的设备与网络的连接点。面向中小企业的思科IBA无边界网络局域网设计提高了从网络接入层到核心层的链路利用率。接入层交换机的两条上行链路都能有效传输流量，与一条上行链路被STP阻塞的传统设计相比，可用带宽提高了一倍。另外，通过增加上行链路数目，能够提高接入层或服务器机房的吞吐率，使设计具备高可扩展性，能够满足带宽需求。因为接入层将客户端设备连接到网络服务，所以它在保护用户、应用资源和网络本身免遭人为错误和恶意攻击的影响方面起着重要作用。接入层还提供自动服务，如增强型以太网供电（PoE+）、QoS标记和IP电话VLAN分配等，以降低用户操作要求。

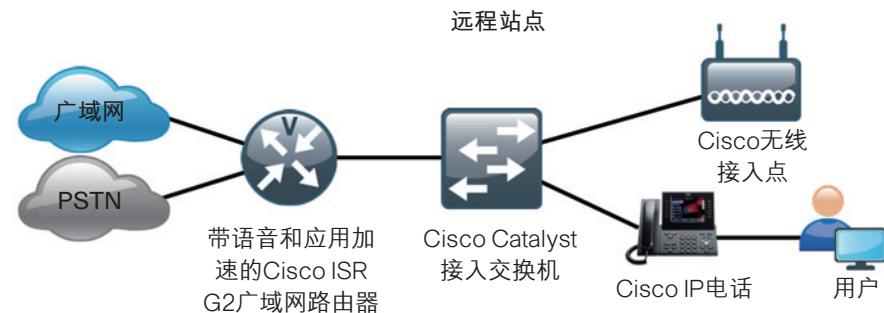
面向中小企业的思科IBA无边界网络全新局域网设计提高了网络传输速度和可用性，降低了复杂性，简化了网络的故障排除和管理。这意味着缩短了故障停机时间，同时能够减少运行中小企业网络所需的网络管理员数量。

## 广域网和远程站点

企业需要信息不间断、无干扰地进出公司网络。面向中小企业的思科IBA采用了强大的广域网设计，采用了与确保大型企业网络持续运行所使用的相同的技术。高度可用的广域网有助于确保业务信息流的传输不会受到干扰。

远程站点（分支机构办公室）是指员工代表企业处理业务的远程地点。远程站点需要具备和总部一样的访问公司应用的能力，只是规模较小。广域网通过专用网连接企业所有地点，并在总部汇聚所有远程站点流量。

图6. 远程站点集成多业务路由器



广域网架构中的关键组件是思科集成多业务路由器2代 (ISR G2)。它为思科客户带来了以下优势：

- 通过单一平台上集成多项服务（如语音、视频和数据等），降低运营开支；
- 采用灵活的模块化设计保护投资，支持企业按需添加语音和视频服务；
- 支持所有主要的电信运营商广域网连接、公共交换电话网络(PSTN)信令以及ISDN类型；
- 能够传输大量语音和视频流量，同时保持其他核心服务。

广域网路由器的主要功能是在远程站点和总部间传输数据。在面向中小企业的思科IBA无边界网络中，远程站点可支持20到40名用户的计算机、IP电话、无线、语音和数据传输。思科ISR G2提供了一个可满足当今远程站点中不断增长的服务数量和性能需求的出色平台。

用户需要对本地的，以及通过广域网对总部站点的网络服务进行无缝访问。采用应用优化和QoS服务旨在提高广域网性能，优化用户体验。应用优化使用压缩、高速缓存和其他优化技术，来将广域网带宽的链路传输速度提高四到五倍。远程用户使用T1/E1链路连接到总部，就感觉如同连接总部局域网一样。服务器在总部集中部署，减少了广域网流量。QoS将关键业务流量和延迟敏感型流量的优先级设为高于其他流量，能确保出色的语音和视频性能，使较低优先级的流量不会影响关键业务运营。

## 无线连接

在任意地点保持网络连接已成为商务和日常生活中不可或缺的一环。很少有建筑物部署了足够多的有线网络端口，能够满足所有人在任意地点连接企业网络的需要。无线网络能帮助用户保持联网，实现信息持续传输，突破建筑物的物理限制。

在中小企业中，总部和远程站点的无线连接使用Wi-Fi技术来传输语音、视频和数据。无线局域网（WLAN）架构的关键组件是思科统一无线网络产品系列。它可为思科客户提供以下优势：

- 网络灵活性延伸了网络边界，无需增加更多布线
- 集中控制无线基础设施，减轻了管理负担
- 经过预配置的网络核心层允许接入点连接到任意接入端口，从而简化了部署

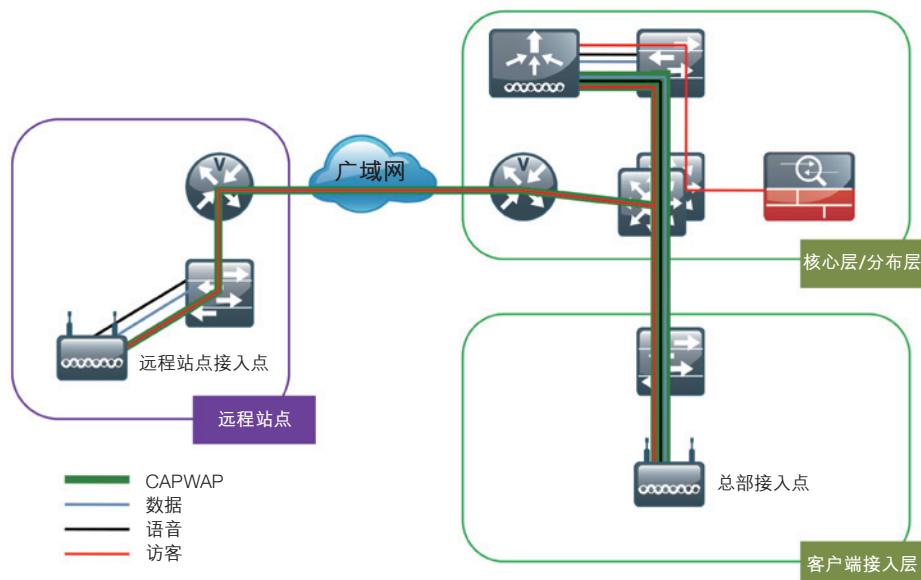
为满足架构中的移动性要求，设计中采用了特定产品和配置，来提供一个安全、灵活、可扩展且经济高效的解决方案。如果以独立模式部署接入点，那么要想在总部和远程工作地点提供全面的无线移动服务，并保持易用性和低拥有成本，会相当困难。自治接入点会增加需要配置、监控和管理的设备的数量。而采用思科无线局域网控制器，您可以集中控制所有接入点，减轻管理负担，简化部署。

除了集中管理外，思科无线局域网控制器还有许多优势。为确保始终能安全接入无线网络，所有员工都根据一个公司目录进行验证，无需在每个接入点都维护一个独立的用户名/密码库。此外，另一项挑战是，为访客提供网络接入，以便他们可连接其企业网络或访问互联网。借助思科无线局域网控制器，您不必投资建设单独的基础设施，就能在现有网络上部署一个虚拟访客网络。该控制器连接到位于互联网边缘的防火墙，仅为访客提供虚拟互联网连接，与公司网络隔离。

尽管思科无线局域网控制器硬件位于网络中央，但它还是可以通过远程站点无线网络提供到本地局域网的无线接入。这避免了流量不得不先传输到总部，然后再传输回远程站点网络的折回现象，减少广域网带宽的浪费。

为支持未来发展，采用思科无线局域网控制器的方式为支持更先进功能奠定了基础，这其中包括位置服务、未授权接入点检测，以及RF预测和策略配置等，这些都能在当前面向中小企业的思科IBA上进行实施。

图7.中小企业无线局域网拓扑



## 互联网边缘

互联网边缘是专用网与互联网的连接处。内部用户流量经此流出公司网络，而互联网流量经此流入公司网络，连接外部应用如Web和电子邮件等。由于这是一条允许外部流量接入网络始终在线的互联网连接，也使其成为主要攻击目标之一。

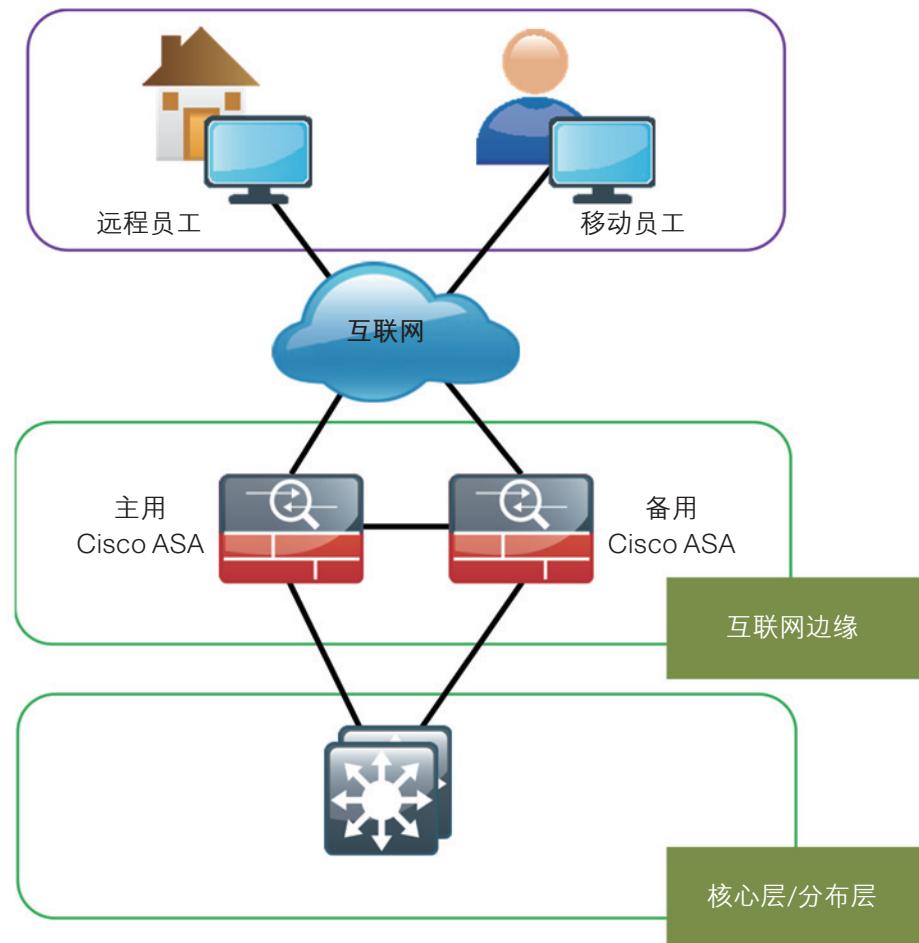
在互联网边缘，通常会采用防火墙和入侵防御系统（IPS）设备来防御常见的互联网威胁。在过去，企业至少需要四台设备来保护员工网络连接的安全。

互联网边缘架构中的关键组件是思科自适应安全设备(ASA)。它可为思科客户带来以下优势：

- 为公司提供快速、安全的互联网接入，提高员工生产率
- 拦截可能会破坏业务运营的互联网攻击
- 通过将所有安全功能综合到单一设备中，简化管理和配置

思科中小企业IBA无边界网络利用ASA在单一设备中提供三项功能，将所需设备从六台减少到两台。这不仅减少了须经过培训来支持相应设备的IT人员数目，还通过缩减网络中的设备总数，降低了软硬件维护成本。Cisco ASA为防火墙和IPS提供了全面的高可用性。防火墙为输入和输出流量、用户的外部访问，以及为需要通过互联网访问的服务器构建的隔离区（DMZ）网络提供了基于状态的应用层过滤功能。

图8. 互联网边缘



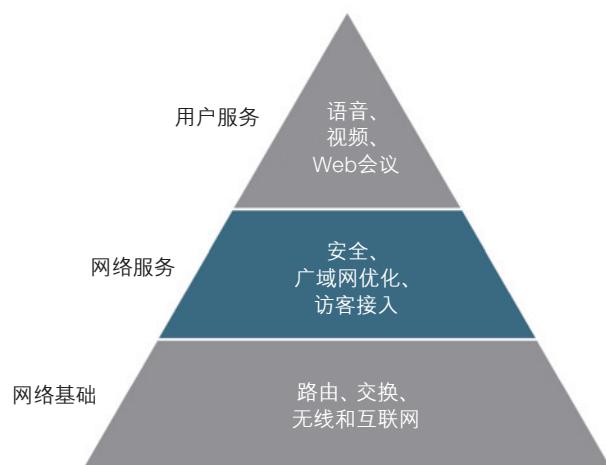
Cisco ASA支持全部IPS功能，能对攻击进行探测并拦截，全新Cisco SensorBase声誉过滤功能通过分析流量来源的声誉，更轻松地作出拦截哪些流量的决策。Cisco SensorBase能将Cisco IPS拦截的攻击数目增加一倍，基于流量来源声誉来检测攻击，使Cisco IPS能够拦截零日（zero-day）攻击，同时减少误报数目。仅使用一对以解决方案方式开发的思科设备，就能满足企业在互联网边缘的基本安全需求。

### 备注

# 网络服务

网络服务在后台运行，是用户服务赖以运行或提高可靠性和效率的基础。在某些情况下，如果没有它们，网络就无法使用。以Web浏览器为例，安装了浏览器的个人电脑可能使用动态地址服务（如动态主机配置协议DHCP）获得了一个网络地址。用户使用的URL通过名称解析服务，即域名系统（DNS），从一个名称（如www.cisco.com）转换为一个网络地址。请求通过最短路由被传送到网络中的一个负载均衡器，负载均衡器把流量分发给多台服务器，支持web应用扩展。网络安全服务有助于确保信息安全，并能够删除恶意流量或防止其到达其目标。

图9. 网络服务



除了DHCP和DNS，在该架构还包括许多网络服务，如虚拟化、安全、应用优化、服务器负载均衡，以及访客无线接入等等。

## 虚拟化

虚拟化技术能帮助您的企业将所有IT资源作为一组能够组合和重新组合的共享服务，从而提高效率，快速扩展。

您的企业运用其现有IT资产—服务器、存储、网络和其它设备的效率越高，您获得的投资回报也越出色。高效率还有助于您推迟新设备的部署，并大大降低用电和冷却成本。

虚拟化通常被视为提升服务器甚至存储工作负载容量的一种方式。但实际上，使您的整个网络实现虚拟化，会实现更高效率。通过一些重要技术革新，以及运营流程和结构的重新配置，网络能在创建虚拟基础设施、提高效率方面发挥重要作用。

我们的目标是构建一个无所不在、高度可扩展的基础设施，将过去的孤岛整合到一个共享虚拟服务阵列中，其配置所需时间远短于传统应用环境的配置时间。

面向中小企业的思科IBA无边界网络为虚拟服务创建了一个基础。在该设计中，使用虚拟局域网（VLAN）在网络上为语音、视频、数据、有线、无线和管理功能建立安全、可靠的逻辑分区。此设计还支持服务器机房/数据中心中的虚拟服务器和存储。

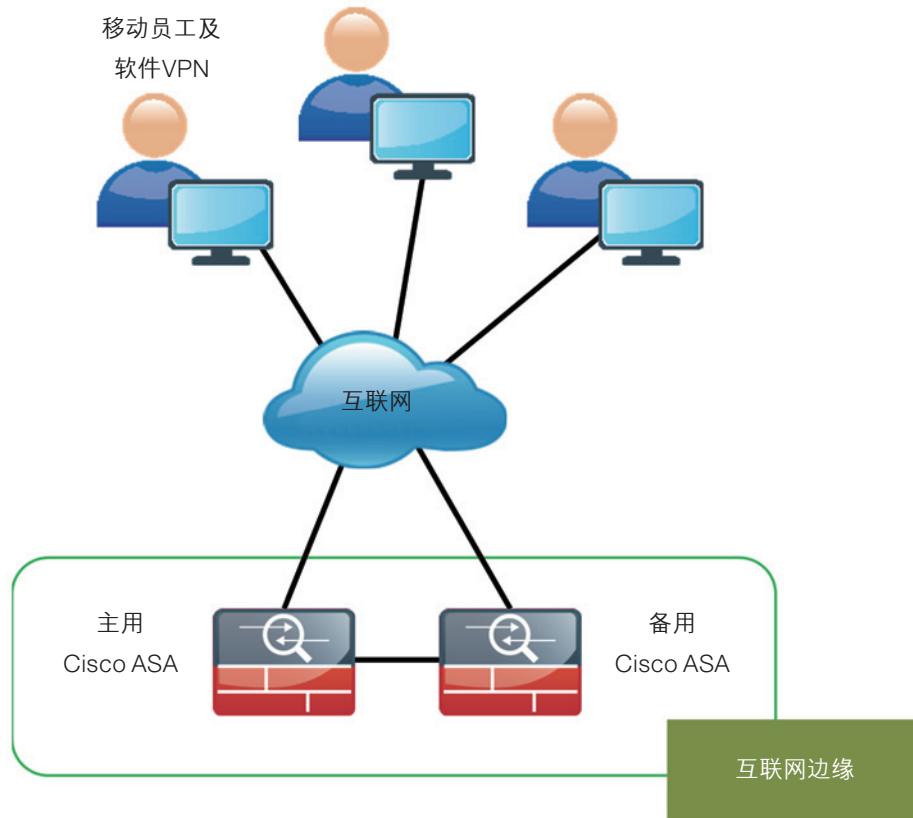
## 安全性

安全是每个网络部署中都必不可少的一部分。企业需要部署安全可靠的网络，保护信息资产，并满足法规遵从性要求，所以必须在网络设计时就内建安全服务，而不是等到之后再进行添加。此外，由于大多数网络都与互联网相连，面临着蠕虫、病毒和针对性攻击的持续威胁，企业必须时刻保护其网络基础设施、用户数据和客户信息。

## 优势

- 简化安全技术的部署，满足法规遵从性要求
- 为员工和合作伙伴的远程接入提供安全保护
- 保护网络中的用户和企业数据
- 通过硬件或软件VPN客户端，为用户提供最高灵活性

图10. 安全服务



对于在路途中或家中办公的员工来说，远程接入是一项必备服务。越来越多的企业允许合作伙伴远程接入其网络，以便更为经济高效地服务其系统。思科中小企业IBA无边界网络通过软件或硬件客户端，为用户提供了安全远程接入功能。思科ASA支持用于远程访问和站点间安全套接层（SSL）和IP安全（IPsec）VPN，为员工和合作伙伴提供了一条通过互联网连接到企业网络的安全途径。SSL VPN具有最高灵活性，即使员工和合作伙伴使用不在企业控制范围内的设备资产，也能安全连接到内部网络。如果目前已部署了远程接入解决方案，则该架构能够灵活地支持传统的IPsec VPN客户端。远程员工能通过一个硬件客户端获得始终在线的连接支持，以便他们在家中能够获得和在公司办公室中相同的使用体验。

多年来，企业一直使用入侵检测系统（IDS）和IPS来检测并拦截网络中的恶意流量，最近公布的法律和私营企业法规遵从性标准则使这些系统从可选的先进技术转变为公司网络中的必备组件。思科中小企业IBA无边界网络支持多种形式和性能水平的Cisco IPS。Cisco IPS可作为一项独立的服务部署，为高性能局域网和服务器部署提供基于设备的解决方案，也可集成到防火墙中，提供网络边界保护。其所有型号都支持在线（inline）和混杂（promiscuous）模式，使客户能够检测流量，并在探测到恶意流量时，实时发送报警或拦截。

## 应用优化

应用优化有助于确保最好地利用远程站点用户和总部间的网络资源。应用优化能够加速广域网上的应用运行，向远程站点交付视频，并提供远程站点IT服务的本地托管。思科广域应用服务（WAAS）使IT部门能在数据中心内集中应用和存储，并保持类似局域网的应用性能，提供本地托管的IT服务，同时缩减远程站点的设备占地空间。

## 优势

- 通过应用优化，提高远程员工的生产率
- 通过在总部集中服务和硬件，最大限度地降低远程站点的IT成本
- 对不断变化的业务需求作出迅速响应；可直接从总部 / 中心进行变更，而不必派遣一位技术人员前往远程站点
- 简化数据保护和法规遵从性，并提高业务连续性

## 服务器负载均衡

思科应用控制引擎（ACE）是思科最新推出的服务器负载均衡产品。其主要作用是提供第四到七层交换，此外Cisco ACE还提供了一系列加速和服务器卸载功能，包括TCP处理卸载、SSL卸载、压缩和其他各种加速技术。Cisco ACE部署在服务器机房的Web及其他应用服务器的前面，提供一系列服务来最大化服务器和应用可用性、安全性及服务器到客户端加速。Cisco ACE使企业能够更有力地控制应用和服务器基础设施，更轻松地管理和保护应用服务，同时提高性能。

## 优势

- 扩展服务器程序的性能，如对Web服务器，可将客户端请求分发到多台服务器上
- 提供高可用性，自动发现失效服务，将请求流量重分发到运行的服务上
- 减少延迟，提升应用性能及降低响应时间
- 卸载TCP及SSL处理，让企业在不增加服务器的情况下就可以支持更多的用户

## 访客无线接入

今天的企业必须适应各种访客在来访时需要接入互联网的情况。思科中小企业IBA无边界网络通过服务于公司用户的接入点，来为访客提供无线接入。访客的范围非常广泛，包括客户、来访者、合作伙伴和供应商等，为满足他们的不同需求，访客接入功能应部署在整个网络中，而不仅仅是在会议室中提供此功能。

## 优势

- 降低了无线访客接入服务的复杂度和成本
- 将访客用户流量与企业流量分开，从而保持企业流量的安全
- 访客接入由IT人员控制，能通过配置，提供通用访客接入或为每个用户提供一个帐户
- 思科中小企业IBA无边界网络在设计中内置了安全访客接入功能，无需额外添加任何硬件

利用思科中小企业IBA无边界网络中的无线网络，企业能借助与内部员工接入使用的相同的接入点来提供访客接入。这种使用相同设备提供多项服务的方式，不但简化了网络运行，降低了成本，而且同时能保障访客的安全接入。

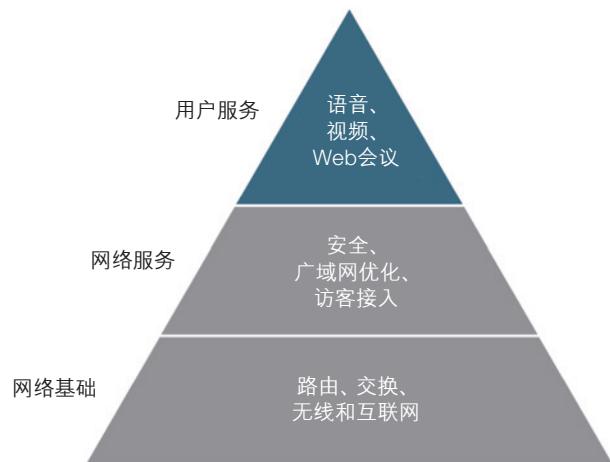
该架构能确保访客网络不会影响到公司网络的安全性。访客流量通过独立无线网段进行传输，当它进入有线网络后，访客流量就被导入一个无线控制器，输出到防火墙上的一个DMZ接口。这既能防止访客影响企业网络的安全，又能为他们提供互联网接入功能。

当访客连接到无线网络，他们被重导向到一个Web登录屏幕，必须输入用户名和密码，才能接入互联网。企业可以创建一个通用的访客帐户，每天或每周重置新密码，也可以为不同用户创建不同访客帐户。该架构十分灵活，能够在复杂性和企业的安全需求间实现平衡。

# 用户服务

用户服务层是每个人都十分熟悉的。我们每天都会直接使用这些服务或应用，从简单的打电话到使用各种电话服务，再到用电子邮件客户端收阅读电子邮件等。用户体验也是从这里开始。应用或产品的设计、构建方式直接影响着它的直观性和易用程度。用户服务与网络服务的交互程度则决定了用户实际使用时所获得的性能。

图11. 用户服务



## 思科统一通信

思科的统一通信产品能为几位用户乃至数万用户提供高质量的语音和视频通信。中小企业可从大量特性和功能中进行选择，无论是简单的语音留言还是复杂的呼叫中心，都能满足其特定需求。

## Web会议和思科WebEx®解决方案

会议不再需要大家集中到一个地点，面对面地召开。对于一个在激烈竞争中求生存、求发展的企业来说，往往必须跨多个时区和地区开展业务。互联网成为了无边界通信的常用媒介，使位于任何地点的人们都能进行协作。

## 企业应用服务

企业在互联网上的表现对于其成功至关重要。即使对于简单的信息网站来说，系统和服务的停止也会导致大量机会丧失。内外部用户都必须能够全天候使用电子邮件、电子商务、Web门户和企业资源规划（ERP）等关键应用，提供不间断的企业服务。这些应用的可用性会受到网络过载和资源利用率低下，以及网络和设备故障的威胁。思科IBA的高可用性设计在互联网边缘提供了冗余防火墙；通过一个永续局域网设计来支持核心层、接入层、服务器机房和无线网络，并提供QoS；而且内置安全性，从而全面保护应用可用性。

# 设计指南总结

## 备注

无论是语音、视频还是数据，信息都是决定了企业运营成败的关键资产。过去，网络产品一直给企业造成很大困扰，因为它们复杂且难以使用、部署和管理。

面向中小企业的思科IBA智能业务平台无边界网络由三个模块化而又相互依存的层构成。它们分别是网络基础层、网络服务层和用户服务层，这三层相互依存，其中每一层都以其下方的层为基础。为了在企业物理地点内外都能可靠地交付业务应用和服务，这三个层必须协调一致地运行。否则，语音、视频和数据传输可能会失败或者遭到破坏，从而将企业置于风险之中。

面向中小企业的思科IBA智能业务平台无边界网络提供了一个规范性设计，而配套的《无边界网络基础部署指南》和《无边界网络配置文件指南》则为该解决方案的部署提供了逐步指导和说明。其中大多数内容都适用于您的情况。思科已经在保留每个产品的智能特性的同时，简化了流程——每一个产品都经过精心挑选，并针对中小企业进行了测试。

通过部署面向中小企业的思科IBA智能业务平台无边界网络设计，可以为企业提供一个稳定、安全、可扩展的网络服务基础设施，从而帮助确保您企业未来的健康运营。



## 智能业务平台



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](http://www.cisco.com/go/offices).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)