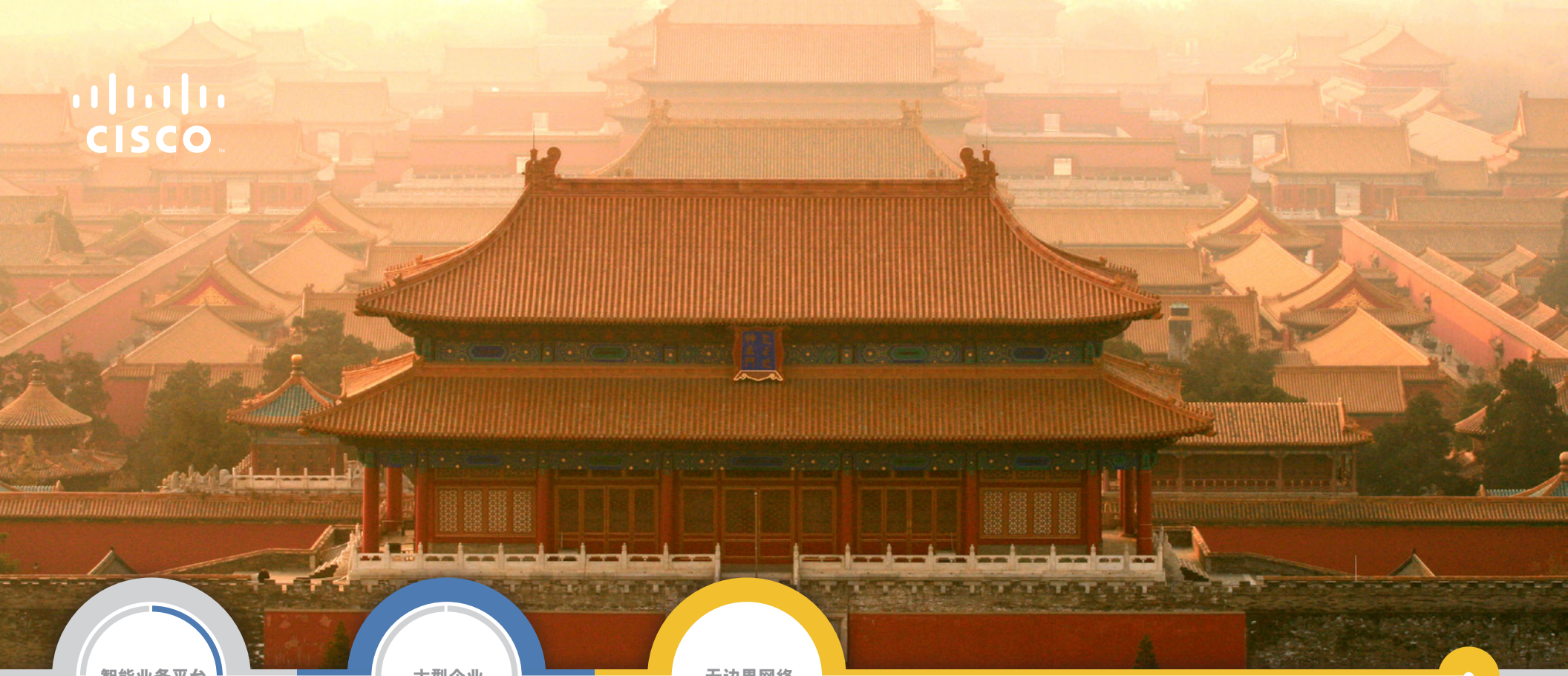
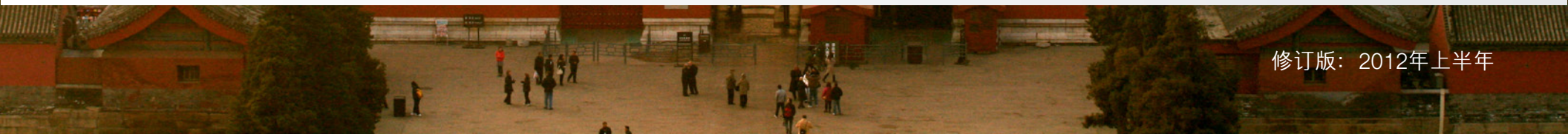


接入层紧凑型交换机部署指南

智能业务平台



修订版：2012年上半年

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

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。

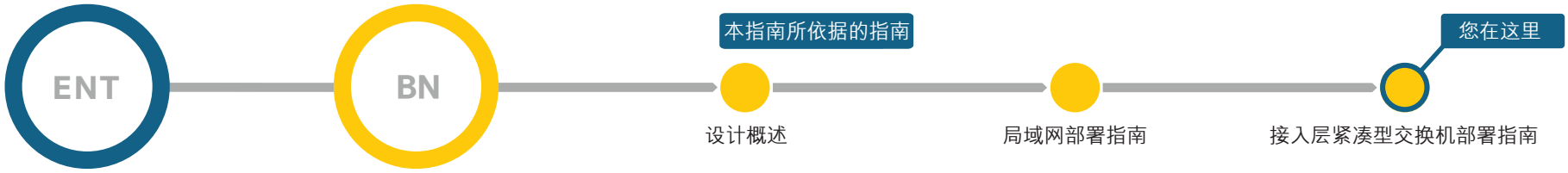
了解更多信息，请参阅《思科IBA使用入门》文档：
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

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。



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

业务概述

在某些情况下，组织需要能够灵活地为特定地点提供更多的接入端口，同时不增加线缆数量。这可能是一个临时性要求，如某天在会议室开展一次培训会议。也可能是增加线缆非常困难或成本过高的情况，如零售环境、游轮或古建筑等。此外，组织也常常需要快速应对增加端口密度的突发性要求，而没有足够的时间部署并测试新的线缆。在此类情形中，将一台额外的紧凑型交换机直接连接到现有接入层将能够在现有电缆设备的限制范围内，提供所需的连接能力。

技术概述

思科IBA智能业务平台局域网接入层为工作环境中的最终用户电脑、笔记本电脑、电话、打印机和其他设备提供了网络连接。主用接入层交换机设计用于放置在19英寸设备机架、配线间或适合此类设备的其他房间内。常见布线设备要求为每一个需要接入网络的设备提供一个专用端口。该端口用于将工作环境与距离最近的接入层交换机连接起来。

如果某个位置的联网设备数量经常发生变化，那么此类动态要求有时可以通过使用无线网络技术来得到满足，以获得灵活性。然而，如果设备要求以太网供电（PoE）能力或者仅支持有线网络连接，您将需要采用其他方案来满足这些要求。在这种情况下，思科IBA智能业务平台接入层能够将永续端口从现有的接入层交换机或交换机堆栈扩展到直接安装在该工作区域内的其他小型交换机，提供多达8个端口的网络连接能力。Cisco Catalyst 3560-C和2960-C系列紧凑型交换机设计用于在配线间之外部署，是满足这一用途的理想选择。

网络特性

思科IBA智能业务平台接入层用于提供实现稳定运营所需的永续性和安全性。Cisco Catalyst基础设施安全特性（CISF）能够帮助易受攻击的网络边缘抵御各种常见攻击，这些特性包括动态主机配置协议(DHCP)监听、IP源防护、端口安全、动态地址解析协议(ARP)检测(DAI)和PortFast桥协议数据单元(BPDU)防护等。语音和视频支持通过多种网络服务实现，包括以太网供电+（PoE+）、服务质量（QoS）、IP组播、思科发现协议（CDP）和语音虚拟局域网等。当通过额外的紧凑型交换机扩展接入层时，您需要确保为这些额外的接入层端口提供一致的特性支持。Cisco Catalyst紧凑型交换机系列支持已在您的思科IBA智能业务平台接入层上部署的网络平台具备的通用特性集。思科IBA智能业务平台配置程序与您的接入层交换机使用的程序相似，从而可有效简化部署工作。

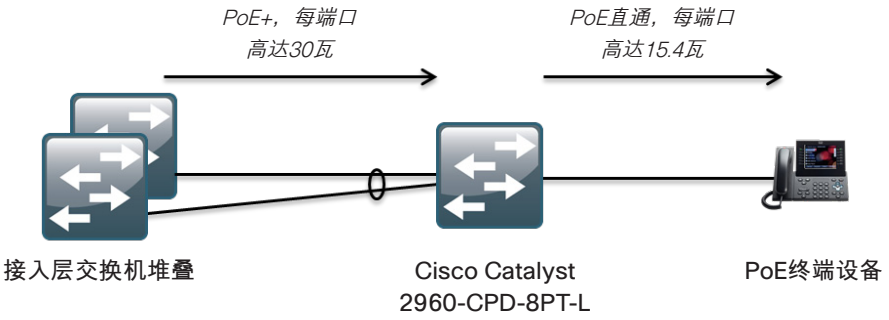
以太网供电选项

PoE直通特性支持交换机使用从上游配线间交换机获得的电力，为PoE终端设备供电。Cisco Catalyst 2960CPD-8PT-L提供了八个10/100 Mbps PoE以太网端口为边缘设备供电，同时具有两个千兆以太网上行链路端口来通过上游交换机接收PoE+电力。这一交换机不需要使用单独的墙壁插座连接供电，通过使用上游交换机提供的电力即可运行。此功能使得紧凑型交换机能够有效受益于上游配线间提供的电力永续性。

要向交换机以及一个或多个相连的设备供电，上游交换机必须能够通过上行链路提供足够的电力，以满足总体设备电力要求。在拥有两个PoE+上行链路的典型配置中，针对所有边缘端口的可用电力总计为22.4瓦。

Cisco Catalyst 2960CPD-8PT-L也可以通过外部辅助适配器进行供电，从而能够支持在上游交换机不提供PoE功能的环境中使用该交换机。当其中一个上行链路连接发生故障时，您也可以使用辅助适配器为连接的PoE设备提供更高的永续性。当使用辅助适配器时，边缘端口可以获得的最大可用电力仍然为22.4瓦。如需了解有关不同上行链路配置的可用电力的详细信息，请参阅cisco.com上的《Cisco Catalyst 3560-C和2960-C系列紧凑型交换机产品简介》。

图1. 直通式PoE

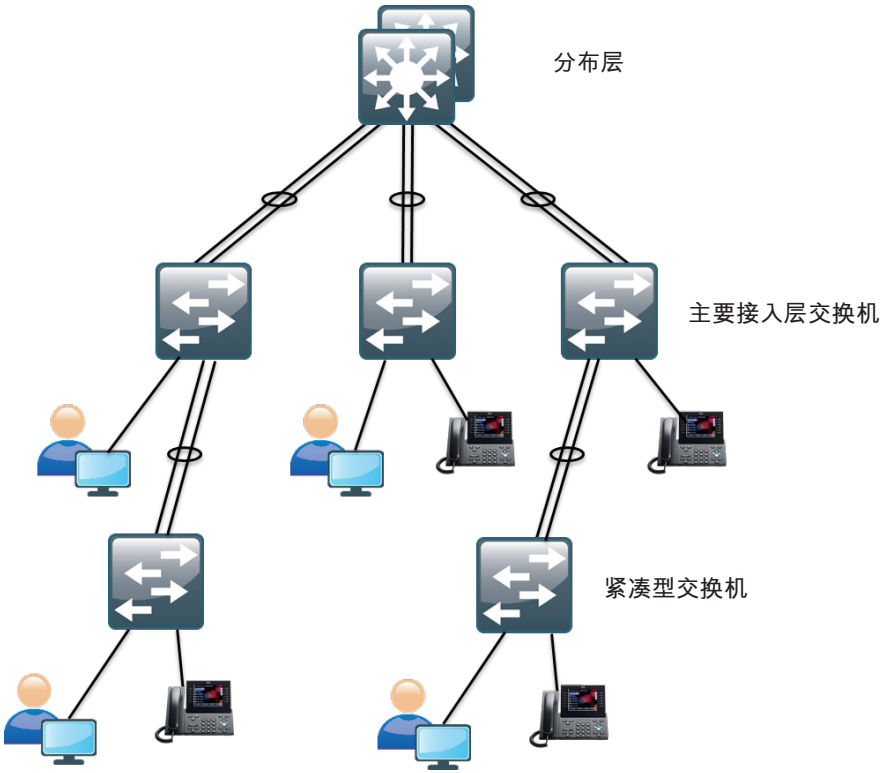


Cisco Catalyst 3560CG-8PC使用了必须单独接入的传统内部电源，能够同时为全部八个边缘端口提供15.4瓦的PoE电力。该交换机最高能够为不同组合的全部端口提供124瓦的电力，并支持为任意使用思科POE+的单个端口提供高达30瓦的电力。如果您需要使用它来支持多种PoE+设备，如IP电话、无线接入点或视频监控摄像头，这一交换机将是最佳选择。此外，3560CG-8PC还在每一端口上提供了千兆以太网支持，从而能够为每个连接带来更高的网络速度。

紧凑型交换机接入拓扑结构

由于在典型网络环境中线缆会最终连接到距离最近的接入层配线间，常见做法为将小型交换机与距离最近的接入层交换机相连。这一方法能够扩展工作场所内的本地局域网接入端口，在特定地点支持连接更多数量的设备。紧凑型交换机能够无缝融入到现有的思科IBA智能业务平台设计之中，如下图所示。

图2. 紧凑型交换机接入拓扑结构



尽管紧凑型交换机也可以直接连接到分布层并配置为接入交换机，但这种用法较为少见。实际物理环境中的布线设备将会决定在您网络中的可用方案。工作场所通常通过铜缆与距离最近的配线间相连，而配线间中的接入层交换机通常通过光纤与分布层相连。思科紧凑型交换机使用铜缆用作上行链路，可直接放置在工作场所内。本指南介绍的解决方案致力于在现有线缆情况下，快速扩展工作场所的端口数量。

部署详情

理想情况下，当您扩展接入层端口以增加工作场所内的端口密度时，需要保持思科IBA智能业务平台网络架构内在的永续性。使用两个上行链路端口能够支持即使一个线缆连接发生故障，紧凑型交换机仍能够保持与网络的连接。此外，第二个上行链路还能够提供更高的整体电力分配范围，然而，某些直通式PoE边缘设备可能会在一个上行链路发生故障时失去电力，尽管交换机本身仍然有电。为了保持最高的永续性，应选择来自机箱式接入层交换机的不同线卡的端口，或者在您使用堆叠接入层的情况下选择来自不同物理堆叠成员的端口。建立这一配置可能要求进入配线间，重新分配工作场所中的特定局域网端口。当然，使用两个上行链路端口要求工作场所内具有足够的铜缆。

读者提示

本部分提供的部署程序用于同当前正常运行的思科IBA智能业务平台接入层配合使用。如需了解有关这一配置的详细信息，请参阅《IBA智能业务平台大型企业局域网部署指南》或《IBA智能业务平台中小企业基础部署指南》。

紧凑型交换机的配置流程与其他接入层交换机类似。主要区别在于其上游交换机是当前第二层接入层交换机的一员，而不是具备第三层功能的分布层交换机。在将链路连接到紧凑型交换机之前，需要首先配置上游接入层交换机。这一流程可确保IBA智能业务平台接入层不会在发现来自紧凑型交换机的生成树BPDU数据包时，错误禁用接入交换机上的上行链路端口。

流程

准备接入层交换机端口

1、确定接入层交换机端口

2、配置中继（trunk）和端口信道

程序1　确定接入层交换机端口

步骤1：确定将用于支持紧凑型交换机上行链路的交换机端口，并确保来自工作场所的线缆插入到正确的交换机端口。请可能选择来自不同线卡或交换机堆叠成员的端口来连接紧凑型交换机。

步骤2：访问控制台或建立telnet会话，以进入接入交换机，检查交换机端口的当前配置。如果选定端口的配置当前为空，前进到程序2。

步骤3：如果当前交换机端口设置有接入层边缘端口配置，这些命令应在将端口设置为紧凑型交换机的中继连接之前予以移除。使用缺省的接口命令退出配置。

```
default interface GigabitEthernet [slot/port]
```

程序2　配置中继（trunk）和端口信道

步骤1：配置EtherChannel成员接口。

在配置逻辑端口信道接口前，先配置属于第二层EtherChannel成员的物理接口。按此顺序进行配置能够最大限度减少所需操作，因为大多数输入端口信道接口的命令会复制到其成员接口，而无需人工复制。

链路聚合控制协议（LACP）协商功能在两端均设置为活动状态，以确保形成正确的EtherChannel。如果接入层交换机连接到思科IBA智能业务平台配置，与正在使用的接入平台相关的出口QoS宏将被配置并设置为可用状态。

```
interface range [interface type] [port 1], [interface type]
[port 2]
 switchport
 macro apply EgressQoS
 channel-protocol lacp
 channel-group [number] mode active
 logging event link-status
 logging event trunk-status
 logging event bundle-status
```

步骤2：配置中继。

一个802.1Q中继用于连接该紧凑型交换机，为接入层交换机上定义的所有VLAN提供连接。中继上支持的VLAN将被精简到只有必需的VLAN。DHCP监听和ARP检测被设置为可信。当使用EtherChannel时，接口类型为端口信道，编码必须与在步骤1中配置的信道组相匹配。

```
interface [interface type] [number]
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan [data vlan],[voice vlan], [mgmt
vlan]
 switchport trunk native vlan 999
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
 logging event link-status
 no shutdown
```

技术提示

Catalyst 2960-S和4500不需要switchport trunk encapsulation dot1q命令。

步骤3：为中继添加VLAN跳跃攻击抑制。

```
interface Port-channel [number]
switchport trunk native vlan 999
```

示例

```
interface range GigabitEthernet 1/0/24, GigabitEthernet 2/0/24
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 channel-protocol lacp
 channel-group 7 mode active
 no shutdown
!
interface Port-channel 7
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100,102,115
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
 no shutdown
```

流程

设置紧凑型交换机

1、配置平台

2、配置局域网交换机

3、配置接入交换机

4、配置客户端连接

5、配置上游交换机连接

开始以下流程之前，需要将紧凑型交换机的上行链路端口连接到接入层交换机上您配置作为中继（trunk）和端口信道的端口。此步骤使得您在完成配置后可以使用端口信道。在Cisco Catalyst 2960-C中，如果您使用直通式PoE，此连接也将为交换机供电。

程序1　配置平台

步骤1：输入以下命令顺序创建两个QoS宏：一个用于面向终端主机的边缘端口，另一个用于支持出口流量的上行链路。

```
macro name AccessEdgeQoS
 auto qos voip cisco-phone
@
!
macro name EgressQoS
 mls qos trust dscp
 queue-set 2
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
@
```

程序2　配置局域网交换机

在此设计中，有一些功能和服务是所有局域网交换机所通用的，与平台类型或在网络中扮演的角色无关。这些系统设置能够简化并保护解决方案的管理。

本程序提供了其中部分此类设置的示例。实际设置和值将取决于您当前的网络配置。

表1：部署中使用的通用网络服务示例

服务	地址
域名	cisco.local
Active Directory、DNS、DHCP服务器	10.4.48.10
身份验证控制系统	10.4.48.15
网络时间协议服务器	10.4.48.17

步骤1：配置设备主机名称，以便轻松识别设备。

```
hostname [hostname]
```

步骤2：配置VTP透明模式

VLAN 中继协议 （VTP） 允许网络管理员在网络中的某个地点配置一个VLAN，并将此配置动态传播到其它网络设备。然而，在大多数情况下，VLAN只在交换机设置期间定义一次，之后几乎不进行修改。

与在网络中动态传播VLAN信息的优势相比，因操作错误而发生意外行为带来的风险更大。因此，我们在此架构中配置了VTP透明模式。

```
vtp mode transparent
```

步骤3：启用快速每VLAN生成树增强型（PVST+）。PVST+提供了每VLAN的RSTP（802.1w）实例。与传统的生成树（802.1D）相比，快速PVST+大大提高了检测间接故障或链接恢复事件的能力。

虽然此架构没有任何第二层环路，但您仍必须启用生成树。启用生成树能够确保，如果意外配置了任何物理或逻辑环路，在实际拓扑中也不会出现第二层环路。

```
spanning-tree mode rapid-pvst
```

步骤4：启用单向链路检测（UDLD）。UDLD是一个第二层协议，支持通过光纤或以太网双绞线连接的设备，以监控线缆的物理配置，并检测是否存在单向链路。当UDLD发现单向链路时，它会禁用受影响的接口并向您报警。单向链路会导致一系列问题的发生，包括生成树环路、黑洞和其他不确定性数据包转发等。此外，UDLD能更快检测出链路故障，并支持接口中继的快速重新收敛，特别是采用易于发生单向故障的光纤时更是如此。

```
udld enable
```

步骤5：设置EtherChannels来使用流量源和目的地IP地址。在此设计中，我们广泛使用了EtherChannel，因为它们具有出色的永续性。为了对EtherChannel成员链路间流量负载共享的方法规范化，所有交换机都应设置为在计算通过哪条链路发送流量时使用流量源和目的地IP地址。

```
port-channel load-balance src-dst-ip
```

步骤6：配置设备管理协议。

安全HTTP（HTTPS）和安全外壳（SSH）是HTTP和Telnet协议的安全替代品。它们使用安全套接字层（SSL）和传输层安全（TLS）提供了设备身份验证和数据加密功能。

SSH和HTTPS协议可实现对LAN设备的安全管理。这两个协议都进行加密，提供信息保密性，而不安全协议Telnet和HTTP则被关闭。

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
 transport input ssh
```

简单网络管理协议（SNMP）用于支持使用网络管理系统（NMS）管理网络基础设施设备。SNMPv2c针对只读和读写团体字符串（community string）进行了配置。

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

步骤7：配置安全用户身份认证。

系统启用身份认证、授权和记帐（AAA）以进行访问控制。所有对于网络基础设施设备的管理访问（SSH和HTTPS）都由AAA控制。

本架构中使用的AAA服务器是思科身份认证控制系统。ACS的配置在网络设备身份认证和授权部署指南中进行讨论。

TACACS+是用于验证基础设施设备上对AAA服务器的管理登录的主要协议。此外，系统还针对每个网络基础设施设备定义了一个本地AAA用户数据库，用于在中央TACACS+服务器不可用时，提供备用身份认证源。

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa authorization console
ip http authentication aaa
tacacs-server host 10.4.48.15 key SecretKey
```

步骤8：配置时钟同步。

网络时间协议（NTP）用于同步网络设备。NTP网络通常从权威时间源，如与时间服务器相连的无线电时钟或原子钟那里获取时间信息。然后NTP在机构的网络中分发此信息。

网络设备应设定为与网络中的本地NTP服务器保持同步。本地NTP服务器通常会参考来自外部来源的更准确的时钟信息。对控制台消息、日志和纠错输出进行配置，在输出中提供时间戳，这样就可以实现对网络中所发生事件的交叉参考。

```
ntp server 10.4.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

程序3　配置接入交换机

接入层设备使用VLAN，将来自不同设备的流量划分到三个逻辑网络：

- 数据VLAN为除了IP电话在内的所有联网设备提供网络访问功能。网络在所有面向用户的界面上进行配置。
- 语音VLAN为IP电话提供网络访问功能。网络在所有面向用户的界面上进行配置。
- 管理VLAN为交换机管理接口提供带内网络访问功能。管理VLAN不在任何面向用户的接口上配置，交换机的VLAN接口是其唯一成员。

步骤1：在交换机上配置数据、语音和管理VLAN，以便能够配置到客户端、IP电话和带内管理接口的连接。

```
vlan [data vlan],[voice vlan],[management vlan]
```

步骤2：配置带内管理

为交换机配置一个IP地址，以便能够通过带内连接对其进行管理。

```
interface vlan [management vlan]
 ip address [ip address] [mask]
 no shutdown
ip default-gateway [default router]
```

由于Catalyst 4500已默认启用IP routing，所以请勿在该产品上使用ip default-gateway命令，使用该命令将不会产生任何效果。

```
ip route 0.0.0.0 0.0.0.0 [default router]
```

步骤3：配置DHCP监听和ARP检测。

DHCP监听是一个DHCP安全功能，负责拦截不可信接口上的DHCP回复。不可信接口是指交换机上未明确配置为已知DHCP服务器或指向已知DHCP服务器的路径的任意接口。

当您在VLAN上启用DHCP监听时，交换机将截获并保护VLAN中的DHCP消息。这可确保未授权DHCP服务器无法向最终用户设备分配地址。

为简化管理和排障，DHCP监听功能跟踪对应于交换机上本地不可信接口的MAC地址、IP地址、租用时间、捆绑类型、VLAN编号和接口信息。DHCP监听将这些信息存储在DHCP绑定表中。如需配置DHCP监听，请输入以下全局交换机命令：

```
ip dhcp snooping vlan [data vlan],[voice vlan]
no ip dhcp snooping information option
ip dhcp snooping
```

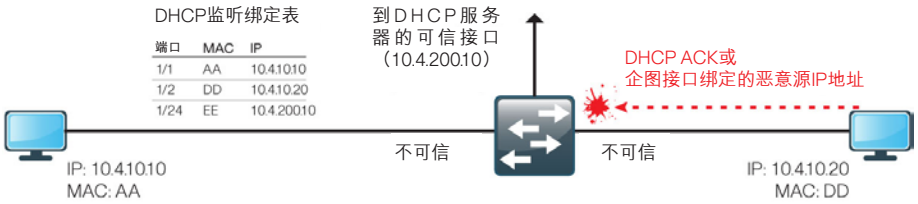
动态ARP检测（DAI）可以减轻ARP欺骗攻击。ARP欺骗攻击是攻击者向本地网段发送伪ARP信息的一种攻击方法。这一信息旨在欺骗局域网上设备的ARP高速缓存，以便攻击者执行中间人攻击。

DAI使用DHCP监听功能生成的数据，并在不可信接口上截获和验证所有ARP数据包的IP到MAC地址关系。在可信接口上接收到的ARP数据包不进行验证，在不可信接口上接收的无效数据包则被丢弃。

配置ARP检测。

```
ip arp inspection vlan [data vlan],[voice vlan]
```

图3. DHCP 监听和ARP检测

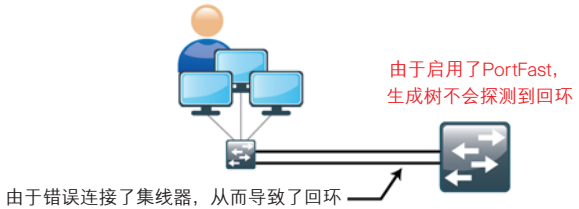


步骤4：在接口上配置BPDU防护。

BPDU防护能防止用户将交换机插入接入端口中，这会导致无法检测出的、灾难性的生成树环路。

如果一个配置了PortFast的接口接收到一个BPDU，则表明存在无效配置，如连接了未授权设备等。BPDU防护功能在启用PortFast的情况下，当接口收到BPDU时，会将非汇聚（nontrunking）接口置于假死（errdisable）状态，从而防止环路。

图4. BPDU防护功能帮助保护端口的情形



如果另一交换机插入了端口，则禁用该接口。

```
spanning-tree portfast bpudguard default
```

程序4　配置客户端连接

当向交换机上的多个接口应用相同配置时，为简化配置，请使用interface range命令。您只需发出一次该命令，就能将其同时应用到多个接口。因为接入层中大多数接口的配置均相同，这一操作能节省大量时间。例如，以下命令使您能同时在全部8个接口（Gig 0/1到Gig 0/8）上输入命令。

```
interface range GigabitEthernet 0/1-8
```

步骤1：配置交换机接口，以支持客户端和IP电话。

主机接口配置支持PC、电话或无线接入点。交换机上提供有内嵌电源，可以为相关设备提供802.3AF/AT支持。

```
interface range [interface type] [port number]-[port number]
 switchport access vlan [data vlan]
 switchport voice vlan [voice vlan]
```

因为接入层只提供终端设备连接，所以可通过启用PortFast、禁用802.1q端口汇聚（trunking）和通道组，缩短接口进入转发状态所需的时间。

```
switchport host
```

所有面向客户端的接口都允许一个不可信PC和/或一个可信思科IP电话连接到交换机，然后自动设置QoS参数。当连接了思科电话后，信任将扩展到这部电话，与此电话相连的任何设备都被认为不可信，所有来自此设备的流量都被重标记为尽力而为或服务类别（CoS）0。

要启用QoS，请应用在平台配置程序中定义的接入边缘QoS宏。

```
macro apply AccessEdgeQoS
```

步骤2：在接口上配置端口安全。

MAC泛洪攻击用来迫使局域网交换机将其全部流量泛洪输出至所有交换机接口。端口安全能限制单一端口上活跃的MAC地址数目，从而防御MAC泛洪攻击。

端口安全使您能将第二层接口配置为只允许来自于有限地址集的MAC地址的输入流量通过。位于有限地址集内的MAC地址被称为安全MAC地址。此外，在同一VLAN中的其他接口上，设备将不允许来自这些MAC地址的流量通过。

设备能保护的MAC地址的数目能够按接口进行配置。为便于管理，设备能够动态学习地址。利用动态学习方法，该设备在输入流量通过接口时保护MAC地址。如果地址还未得到保护，且设备未达到其支持地址的最高限，则设备保护该地址并允许流量通过。一旦到达老化时限，设备将动态地址过期并丢弃它们。

每个接口上允许支持的MAC地址数目根据每个机构的情况而定。但是，虚拟化应用、IP电话和桌面无源集线器等的普及提高了机构在这方面的需求，所需的数目一般要高于人们初步猜测的数目。本设计中使用的数值既为企业带来了灵活性，又保护了网络基础设施。

在接口上进行配置，同时激活11个MAC地址；其他MAC地址则被认为违规，其流量将被丢弃：

```
switchport port-security maximum 11
switchport port-security
```

设置老化时间，在2分钟未被使用后就将所获知的MAC地址从受保护的列表中删除：

```
switchport port-security aging time 2
switchport port-security aging type inactivity
```

配置限制选项，丢弃违规的MAC地址的流量，但不要关闭端口。该配置可确保IP电话在发生端口安全违背的接口上仍能运行：

```
switchport port-security violation restrict
```

步骤3：在接口上配置DHCP监听和ARP检测

在端口上启用ARP检测和DHCP监听，以100pps的速度处理流量。

```
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
```

步骤4：在接口上配置IP源防护。

IP源防护是一种防止分组使用错误源IP地址来掩盖其真正来源（即IP电子欺骗）的手段。IP源防护使用来自DHCP监听的信息，在接口上动态配置一个端口访问控制列表（PACL），拒绝任何来自不属于DHCP捆绑表中的IP地址的流量通过。

```
ip verify source
```

程序3和4示例


```
vlan 100
 name Data
vlan 102
 name Voice
vlan 115
 name Management
!
interface Vlan 115
 description in-band management
 ip address 10.10.15.57 255.255.255.0
 no shutdown
!
ip default-gateway 10.10.15.1
!
ip dhcp snooping vlan 100,102
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 100,102
!
interface range GigabitEthernet 0/1-8
 switchport access vlan 100
 switchport voice vlan 102
 switchport host
 macro apply AccessEdgeQoS
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security aging type inactivity
 switchport port-security violation restrict
 ip arp inspection limit rate 100
 ip dhcp snooping limit rate 100
 ip verify source
```

程序5　配置上游交换机连接

此程序详细介绍了如何配置从紧凑型交换机到上游接入层交换机的链路。

读者提示

应用于紧凑型交换机来创建上游中继和端口通道的配置步骤与早前用于接入交换机的步骤相同。此处重申的目的是指明上下文。

步骤1：配置EtherChannel成员接口。

在配置逻辑端口信道接口前，先配置属于第二层EtherChannel成员的物理接口。按此顺序进行配置能够最大限度减少所需操作，因为大多数输入端口信道接口的命令会复制到其成员接口，而无需人工复制。

将链路聚合控制协议（LACP）协商功能在两端均设置为活动状态，以确保形成正确的EtherChannel。同时在出口配置QoS的宏命令（在**程序1**平台配置中定义），保证流量的优先级。

```
interface range [interface type] [port 1], [interface type]
[port 2]
 switchport
 macro apply EgressQoS
 channel-protocol lacp
 channel-group [number] mode active
 logging event link-status
 logging event trunk-status
 logging event bundle-status
```

步骤2：配置中继（trunk）。

一个802.1Q中继（trunk）用于连接此上游设备，为接入层交换机上定义的所有VLAN提供第三层服务。该中继上所支持的VLAN仅限于接入层交换机上激活的VLAN。DHCP监听和ARP检测设置为可信。当采用EtherChannel时，接口类型为端口信道，编码必须与在步骤1中配置的信道组相匹配。

```
interface [interface type] [number]
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan [data vlan],[voice vlan], [mgmt vlan]
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
 logging event link-status
 no shutdown
```

步骤3：抑制中继上的VLAN Hopping（跳跃攻击）

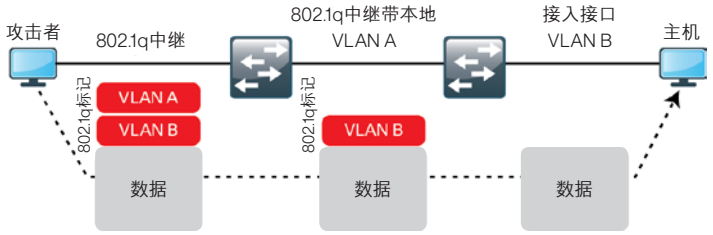
此外，虽然可能性很小，但存在着攻击者创建一个双802.1Q 封装分组的可能性。如果攻击者详细了解802.1Q本地VLAN，那么能够创建一个分组，当它交换到无标记本地VLAN上时，第一个或最外面的标记被删除。当该分组到达目标交换机时，内部或第二个标记将被处理，这个有潜在恶意的分组则交换到目标VLAN中。

初看上去，这似乎是一项严重的威胁。但这一攻击中的流量是单向的，该机制不会交换返回流量。而且，除非攻击者知道本地VLAN ID，否则无法进行此攻击。

消除这一攻击类型远程风险的简单办法是在从接入层到分布层的所有交换机到交换机802.1Q中继链路上配置一个不使用的VLAN。使用难以猜测、不使用的VLAN作为本机VLAN可以减少双802.1Q标记分组进行VLAN跳跃攻击的可能性。

```
Vlan 999
!
interface [interface type] [number]
 switchport trunk native vlan 999
```

图5. VLAN跳跃攻击



示例

```
interface range GigabitEthernet 0/9, GigabitEthernet 0/10
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 logging event bundle-status
 channel-protocol lacp
 channel-group 7 mode active
 no shutdown
!
interface Port-channel 7
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100,102,115
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
 no shutdown
```

附录A: 产品列表

以下产品与软件版本经验证适用于思科IBA智能业务平台:

功能区域	产品	产品编号	软件版本
紧凑型交换机	Catalyst 2960-C 紧凑型交换机	WS-2960CPD-8PT-L	12.2 (55) EX2
紧凑型交换机	Catalyst 3560-C 紧凑型交换机	WS-3560CG-8PC-S	12.2 (55) EX2
接入交换机	Catalyst 2960S Stackable Ethernet 10/100/1000 端口，带PoE+ 和堆叠模块	WS-C2960S-24PD-L Catalyst 2960S 24 GigE PoE+, 2 x 10G SFP+ LAN Base WS-C2960S-48FPD-L Catalyst 2960S 48 GigE PoE +, 2 x 10G SFP+ LAN Base WS-C2960S-24PS-L Catalyst 2960S 24 GigE PoE+, 4 x SFP LAN Base WS-C2960S-48FPS-L Catalyst 2960S 48 GigE PoE+, 4 x SFP LAN Base C2960S-STACK= Catalyst 2960S Flexstack Stack Module	15.0 (1) SE1
接入交换机	Catalyst 3560X Ethernet 10/100/1000 端口，带PoE+和上行链路模块	WS-C3560X-24P-S Catalyst 3750 24 10/100/1000T PoE + and IPB Image WS-C3560X-48PF-S Catalyst 3750 48 10/100/1000T Full PoE + and IPB Image C3KX-NM-1G Catalyst 3750X 1Gig SFP Uplink Module C3KX-NM-10G Catalyst 3750X 10Gig SFP+ Uplink Module	15.0 (1) SE1
接入交换机	Catalyst 3750X Stackable Ethernet 10/100/1000端口，带PoE+ 和上行链路模块	WS-C3750X-24P-S Catalyst 3750 24 10/100/1000T PoE + and IPB Image WS-C3750X-48PF-S Catalyst 3750 48 10/100/1000T Full PoE + and IPB Image C3KX-NM-1G Catalyst 3750X 1Gig SFP Uplink Module C3KX-NM-10G Catalyst 3750X 10Gig SFP+ Uplink Module	15.0 (1) SE1
接入交换机	Catalyst 4507R+E 双管理引擎 双电源	WS-C4507R+E Catalyst 4500 E-Series 7-Slot Chassis with 48Gbps per Slot WS-X45-SUP7L-E Catalyst 4500 E-Series Supervisor LE, 520Gbps WS-X4648-RJ45V+E 4500 E-Series 48-Port PoE+ Ready 10/100/1000（RJ45）	15.0 (2) XO

附录B:
配置示例

```
Current configuration : 12081 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname A2960C-1
!
boot-start-marker
boot-end-marker
!
username admin privilege 15 password 7 130646010803557878'
enable secret 5 $1$2HEt$LSzYeOPaxOEV1ky2AAmdZ0
!
macro name AccessEdgeQoS
 auto qos voip cisco-phone
@
macro name EgressQoS
 mls qos trust dscp
 queue-set 2
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
@
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization exec default group tacacs+ local
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PDT recurring
system mtu routing 1500
!
!
ip dhcp snooping vlan 100,102
no ip dhcp snooping information option
ip dhcp snooping
ip domain-name cisco.local
ip arp inspection vlan 100-102
vtp mode transparent
udld enable

!
mls qos map policed-dscp 0 10 18 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
```

```
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19
20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29
30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
crypto pki trustpoint TP-self-signed-2192690432
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2192690432
 revocation-check none
 rsakeypair TP-self-signed-2192690432
!
!
crypto pki certificate chain TP-self-signed-2192690432
 certificate self-signed 01
 3082024C 308201B5 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  . . .
 7A55723A F61A0F5D 25DE945F 9D700C39
 quit
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree portfast bpudguard default
!
auto qos srnd4
!
!
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 100
 name Data
!
vlan 102
 name Voice
!
vlan 115
 name Management
!
vlan 999
 name VlanHopping
!
ip ssh version 2
!
class-map match-all AUTOQOS_VOIP_DATA_CLASS
 match ip dscp ef
class-map match-all AUTOQOS_DEFAULT_CLASS
```

```
 match access-group name AUTOQOS-ACL-DEFAULT
class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
 match ip dscp cs3
!
!
policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
 class AUTOQOS_VOIP_DATA_CLASS
 set dscp ef
 police 128000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_VOIP_SIGNAL_CLASS
 set dscp cs3
 police 32000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_DEFAULT_CLASS
 set dscp default
 police 10000000 8000 exceed-action policed-dscp-transmit
!
!
!
interface Port-channel1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100,101,115
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
!
interface FastEthernet0/1
 switchport access vlan 100
 switchport mode access
 switchport voice vlan 102
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description AccessEdgeQoS
 auto qos voip cisco-phone
 spanning-tree portfast
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
 ip verify source
 ip dhcp snooping limit rate 100
!
. . .
!
interface FastEthernet0/8
 switchport access vlan 100
 switchport mode access
 switchport voice vlan 102
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description AccessEdgeQoS
 auto qos voip cisco-phone
 spanning-tree portfast
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100,102,115
 switchport mode trunk
 ip arp inspection trust
```

```
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 30 35 5
 queue-set 2
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 channel-protocol lacp
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface GigabitEthernet0/2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100,102,115
 switchport mode trunk
 ip arp inspection trust
 logging event trunk-status
 logging event bundle-status
 srr-queue bandwidth share 1 30 35 5
 queue-set 2
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 channel-protocol lacp
 channel-group 1 mode active
 ip dhcp snooping trust
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan115
 ip address 10.10.115.56 255.255.255.0
!
ip default-gateway 10.10.15.1
ip http server
ip http secure-server
!
ip access-list extended AUTOQOS-ACL-DEFAULT
 permit ip any any
ip sla enable reaction-alerts
snmp-server community cisco RO
snmp-server community cisco123 RW
tacacs-server host 10.4.48.15 key 7 113A1C0605171F270133
tacacs-server directed-request
!
line con 0
line vty 0 4
 length 0
 transport input ssh
line vty 5 15
 length 0
 transport input ssh
!
ntp clock-period 36028990
ntp server 10.4.48.17
end
```

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.**

B-0000103-1 12/11