综合实训 2

某医疗机构智能网络建设

某医疗机构要进行智能网改造和升级。此次网络工程包括医疗机构总部、附属分支机构网络架设。随着医疗机构对网络的依赖日益增加，其原有网络已经不能满足高效管理的需要，为了适应业务的需求，决定构建一个高速、稳定、安全的办公网络。

2.1 项目分析

本项目总体结构包含某医疗机构总部的网络建设和分支机构的网络建设。服务器都集中部署在总部的数据中心，分支机构通过 ISP 和总部互连，访问总部的服务器。为了确保总部和分支机构在互相访问过程中的数据安全，在总部和分支机构 2 之间配置站点到站点之间的 VPN(GRE over IPSec)，加密并保护流量。

总部用一台 2960 和一台 3560 交换机接入所有的服务器、无线网络用户、语音用户。由于网络中访问 Server2 的流量比较大，所以在 2960 和 3560 两台交换机之间配置端口汇聚，提高带宽。

为了防止不合法的用户通过 IP 电话机接入网络，在 Core_SW 交换机上配置适当的安全的策略。

总部有两间会议室，为了使会议室整洁和使用方便，采用无线 AP 接入公司网络。

总部的市场部和销售部分别有一台 IP 电话，可以节约该机构的电话费用。

为了方便工作人员上网，在总部和两个分支机构都采用 DHCP 自动分配 IP 地址。

为了适应新业务的需要，总部和分支机构都要部署 IPV6 。

分支机构 1 因为网络规模小，建议采用 RIP 路由协议跟总部互连；总部和分支机构 2 之间运行 OSPF 路由协议，为了提高路由器的工作效率，尽量通过技术的实施，使路由器的路由条目数量少。

通过某种技术的应用，保护分支机构 1 的用户安全。

分支机构 2 有一部软件 IP 电话，为了确保电话的语音质量，在 Branch_2 路由器上配置 QoS 策略。

另外，保证所有网络设备的时间自动同步。

2.2　项目设计

2.2.1　网络设备及拓扑结构描述

首先，要确定网络中的设备型号及 IOS 要求，如表 2-1 所示。

表 2-1　　设备型号及 IOS 版本

序号	设备名	设备型号	IOS 要求
1	Branch _1	Cisco 2801 路由器	12.4T Advanced IP Services 特性集
2	Branch_ 2	Cisco 2801 路由器	12.4T Advanced IP Services 特性集
3	HQ	Cisco 2801 路由器	12.4T Advanced IP Services 特性集
4	Core_SW	Cisco 3560 交换机	12.2 IP Services 特性集
5	AP	Cisco 1130 系列 AP	内置默认 IOS 即可
6	Branch2_Access	Cisco 2960 系列交换机	内置默认 IOS 即可
7	HQ_Access	Cisco 2960 系列交换机	内置默认 IOS 即可

然后，根据项目需求，设计项目拓扑结构，如图 2-1 所示。

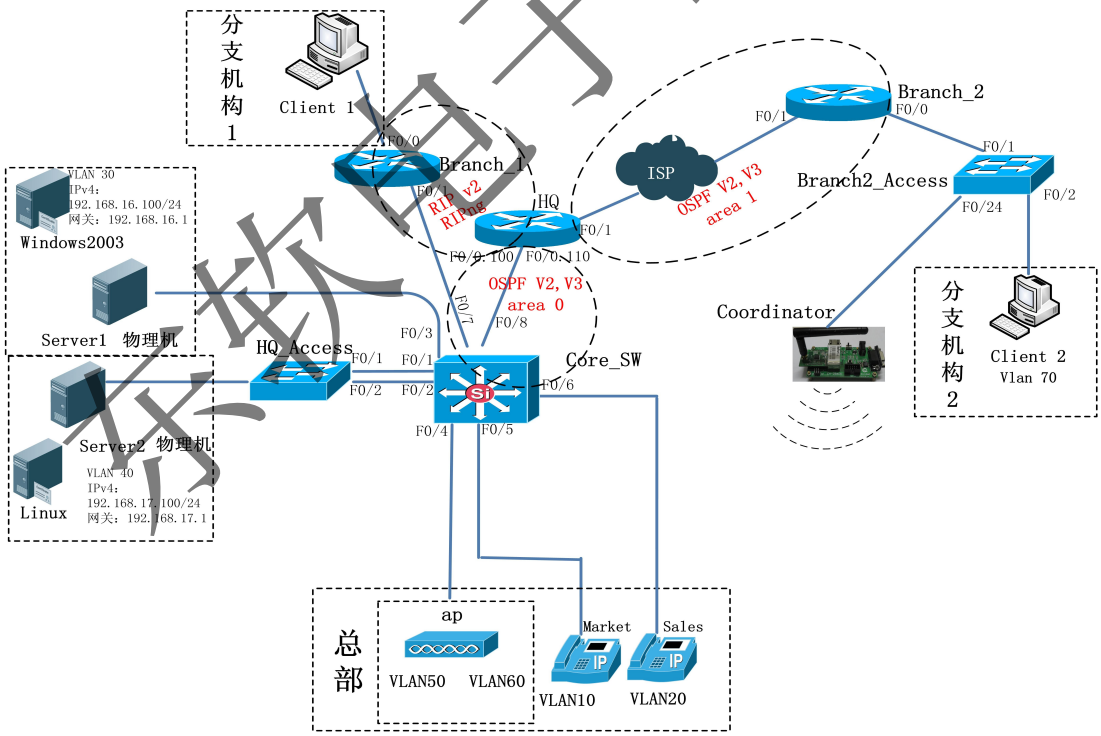

图 2-1　网络拓扑

2.2.2 VLAN 规划

首先，在交换机上创建 VLAN，并将端口加入到相应的 VLAN 中，如表 2-2 所示。

表 2-2 VLAN 分配表

设备	VLAN-ID	VLAN 名称	端口
HQ_Access	40	Server2	Fa0/3
	2012	mgmt-vlan	
Branch2_Access	70	无	Fa0/2，启用 portfast
	75	无	
	80	无	
	85	无	
	2011	Branch2-mgmt	
Core_SW	10	v7911	Fa0/5
	20	V7945	Fa0/6
	30	Server1	Fa0/8
	40	Server2	
	50	SSID1	
	60	SSID2	
	100	Branch_1	Fa0/7
	110	无	
	300	AP_guest	
	2012	mgmt-vlan	

然后，需要确定交换机接口模式以及 Channel 模式，如表 2-3 所示。

表 2-3 交换机接口 Trunk 模式、Channel 模式配置表

设备名称	接口	要求
Core_SW	Port-Channel 1	Trunk 不协商 Channel 模式，直接启用 Fa0/1，Fa0/2 加入到这个 Port-Channel 中 根据源和目的 MAC 做负载均衡
	Fa0/4	Trunk 模式，指定使用 dot1q 封装 仅允许通过 vlan50，60，300 禁用 Trunk 协商
	Fa0/8	Trunk 模式，指定使用 dot1q 封装 仅允许通过 vlan 100，110 禁用 Trunk 协商
HQ_Access	Port-Channel 1	Trunk 不协商 Channel 模式，直接启用 Fa0/1，Fa0/2 加入到这个 Port-Channel 中 根据源和目的 MAC 做负载均衡
Branch2_Access	Fa0/1	Trunk 仅允许通过 vlan70，75，80，85，2011

2.2.3　交换机上安全策略的设计方案

Core_SW 交换机的 Fa0/5 口上连接的是一台 Cisco 7911 IP 电话机，请在该端口上应用恰当的端口安全策略以便实现下面需求：

- 仅允许 IP 电话机使用这个端口，如果有其他用户通过 IP 电话机又连接了一个电脑，则该端口自动进入 shutdown 模式。
- 120 秒后自动取消 shutdown 模式。

Core_SW 交换机的 Fa0/6 口上连接的是一台 Cisco 7945 IP 电话机，请在该端口上应用恰当的端口安全策略以便实现下面需求：

- 允许用户通过该 IP 电话机再连接 1 台电脑上网，如果用户连接了超过 1 台电脑，则该端口自动进入 shutdown 模式。
- 120 秒后自动取消 shutdown 模式。

2.2.4　无线网络部署

你可以使用图形界面或者命令行工具来配置无线 AP。无线 AP 将为两个不同功能的会议室提供服务，恰当配置无线 AP，无线 AP 的配置参数如表 2-4 所示，实现下面需求：

- 无线 AP 的机器名设置为 ap。
- Enable 口令设置为 2012comp。
- 禁用 service password-encryption 服务。
- 仅使用 2.4GHz 频段。
- 根据下面表格设置 SSID(**注意**：为防止各组间无线 SSID 重名冲突，请在 SSID 命名中以您的身份证号码后 4 位为结尾)。

表 2-4　　无线 AP 配置参数表

SSID 命名方式	对应 VLAN	安全策略
guestnet-身份证号码后 4 位	300	无认证、无加密、广播 SSID
Meeting-Room1-身份证号码后 4 位	50	WPA2，密钥为“2012comp”，AES-CCM，不广播 SSID
Meeting-Room2-身份证号码后 4 位	60	WPA2，密钥为“2012comp”，AES-CCM，不广播 SSID

2.2.5　IP 地址规划

需要对网络设备进行命名并配置 IP 地址，IP 地址规划如表 2-5 所示。

表 2-5　　IP 地址规划表

设备	设备名称	设备接口	IP 地址和相关信息	IPv6 地址
二层交换机	HQ_Access	Vlan 2012	192.168.18.2/24 默认网关 192.168.18.1	2012:0:0:12::2/64
	Branch2_Access	Vlan 2011	192.168.19.2/24 默认网关 192.168.19.1	2012:0:0:13::2/64

（续表）

设备	设备名称	设备接口	IP 地址和相关信息	IPv6 地址
路由器	Branch_1	Fa0/0	192.168.6.1/24	2012:0:0:6::1/64
		Fa0/1	192.168.5.1/30	2012:0:0:50::/最节省地址的掩码
	Branch_2	Tunnel 1	192.168.5.6/30 Tunnel 源接口 Fa0/1 Tunnel 目的地址 200.200.200.1	2012:0:0:54::1/ 最节省地址的掩码
		Fa0/0.1	192.168.8.1/24 封装 dot1q 70	2012:0:0:8::1/64
		Fa0/0.2	192.168.9.1/24 封装 dot1q 75	2012:0:0:9::1/64
		Fa0/0.3	192.168.10.1/24 封装 dot1q 80	2012:0:0:A::1/64
		Fa0/0.4	192.168.11.1/24 封装 dot1q85	2012:0:0:B::1/64
		Fa0/0.2011	192.168.19.1 封装 dot1q2011	2012:0:0:13::1/64
		Fa0/1	200.200.200.2/30	无 IPv6 地址
	HQ	Tunnel 1	192.168.5.5/30 Tunnel 源接口 Fa0/1 Tunnel 目的地址 200.200.200.2	2012:0:0:54::/ 最节省地址的掩码
		Fa0/0.100	192.168.5.2/30 封装 dot1q 100	2012:0:0:50::1/ 最节省地址的掩码
		Fa0/0.110	192.168.5.10/30 封装 dot1q 110	2012:0:0:58::1/ 最节省地址的掩码
		Fa0/1	200.200.200.1/30	无 IPv6 地址
三层交换机	Core_SW	vlan 10	192.168.14.1/24	2012:0:0:E::1/64
		vlan 20	192.168.15.1/24	2012:0:0:F::1/64
		vlan 30	192.168.16.1/24	2012:0:0:10::1/64
		vlan 40	192.168.17.1/24	2012:0:0:11::1/64
		vlan 50	192.168.12.1/24	2012:0:0:C::1/64
		vlan 60	192.168.13.1/24	2012:0:0:D::1/64
		vlan 110	192.168.5.9/30	2012:0:0:58::/最节省地址的掩码
		vlan 2012	192.168.18.1/24	2012:0:0:12::1/64

2.2.6　网络中 DHCP 服务的设计方案

为了方便实现工作人员上网，要求在下列设备上启用 DHCP 服务，请根据需求进行配置。

1. IPv4 地址规划

(1)路由器 Branch_1 为所连接的分支机构用户提供 DHCP 服务。

①禁止分配地址范围：192.168.6.1 到 192.168.6.9

②DHCP 地址池名称：voip3

- 地址分配范围：192.168.6.0/24
- 默认网关为该网段对应的路由器接口地址
- DNS 服务器：192.168.17.100

(2)路由器 Branch_2 为所连接的分支机构用户提供 DHCP 服务。

①禁止分配地址范围：192.168.8.1 到 192.168.8.9

②DHCP 地址池名称：voip4

- 地址分配范围：192.168.8.0/24
- 默认网关为该网段对应的路由器接口地址
- DNS 服务器：192.168.17.100

(3)总部核心交换机 Core_SW 为所连接的总部用户提供 DHCP 服务。

①禁止分配地址范围：

- 192.168.14.1 到 192.168.14.9
- 192.168.15.1 到 192.168.15.9
- 192.168.12.1 到 192.168.12.9
- 192.168.13.1 到 192.168.13.9

②为 Market 部门 IP 电话启用 DHCP 服务：

- DHCP 地址池名称：voip1
- 地址分配范围：192.168.14.0/24
- DNS 服务器：192.168.17.100
- 默认网关：192.168.14.1

③为 Sales 部门 IP 电话启用 DHCP 服务：

- DHCP 地址池名称：voip2
- 地址分配范围：192.168.15.0/24
- DNS 服务器：192.168.17.100
- 默认网关：192.168.15.1

④为总部会议室 Meeting-Room1 的无线网络启用 DHCP 服务：

- DHCP 地址池名称：Ap-Meeting-Room1
- 地址分配范围：192.168.12.0/24
- DNS 服务器：192.168.17.100
- 默认网关：192.168.12.1

⑤为总部会议室 Meeting-Room2 的无线网络启用 DHCP 服务：

- DHCP 地址池名称：Ap-Meeting-Room2
- 地址分配范围：192.168.13.0/24
- DNS 服务器：192.168.17.100
- 默认网关：192.168.13.1

2. IPv6 地址规划

(1)在总部核心交换机 Core_SW 上启用全网 IPv6 DHCP 服务，利用 VLAN110 的 SVI 接口提供服务。

(2)自动为路由器 Branch2 所连接的分支机构用户分配 IPv6 地址。

- 在 Fa0/0.1 接口上禁用 IPv6 无状态方式的自动地址分配并配置 IPv6 DHCP 中继，目标地址 2012:0:0:58::
- IPv6 地址池名称：Branch2
- 地址前缀：2012:0:0:8::/64
- 链路地址：2012:0:0:8::/64

(3)自动为路由器 Branch1 所连接的分支机构分配 Ipv6 地址。

- 在 Fa0/0 接口上禁用 IPv6 无状态方式的自动地址分配并配置 IPv6 DHCP 中继，目标地址 2012:0:0:58::
- IPv6 地址池名称：Branch1
- 地址前缀：2012:0:0:6::/64
- 链路地址：2012:0:0:6::/64

2.2.7 IPv4 路由协议部署方案

1. Branch1 和 HQ 路由器之间运行了 RIPv2 路由协议

(1)在 Branch1 上通告直连的两个接口。

(2)在 HQ 上通告对应的接口。

(3)在 HQ 上禁止向 Tunnel1 和 Fa0/0.110 发送路由更新。

(4)HQ 产生一条默认路由，并将该路由送向 Branch1。

(5)为了节约 Branch1 设备的内存，请在 HQ 上做路由过滤，要求仅向 Branch1 送出一条默认路由，只能使用 1 条 prefix-list 命令(名称 fil_rip，序号 5)做路由过滤。

(6)在 HQ 上禁用 RIP 自动汇总。

2. Core_SW、HQ 之间启用了 OSPF 路由协议，Process ID 均为 1

(1)Core_SW 与 HQ 连线的子网属于 Area 0。

(2)Core_SW 上的路由实施方案：

- 请依次直接通告所有直连的 3 层接口所在的子网号。
- VLAN110 上启用基于接口的 MD5 认证，认证密码为2012comp，key ID 编号为 1。

(3)HQ 上的路由实施方案：

- 请在 Fa0/0.110 上启用基于接口的 MD5 认证，参数应与 Core_SW 匹配。
- 请仅将 Fa0/0.110 对应的地址范围通告到 Area0 中。
- 在 OSPF 中产生一条默认路由，并送给 HQ 的所有 OSPF 邻居。

■ 手工将 HQ 从 Core_SW 学到的 OSPF 路由汇总(要求精确汇总),使得向 Branch2 发送的路由条目最少。

■ 使用恰当的参数将通过 RIP 学习到的路由条目重分布到 OSPF 中。

3. HQ、Branch2 之间启用了 OSPF 路由协议,Process ID 均为 1

(1)HQ 与 Branch2 连线的子网属于 Area1。

(2)HQ 上的路由实施方案:

■ 请仅通告与 Branch2 相连的 Tunnel 网段到 Area1 中。

■ Area1 为末节(stub)区域,禁止将从 RIP 重分布到 OSPF 中的外部路由传播到 Branch2 上,但不能影响 Branch2 的内网与 Branch1 内网之间的通信。

(3)Branch2 上的路由实施方案:

■ 请仅直接通告与 HQ 相连的 Tunnel 网段到 Area1 中,确认两台路由器通过 Tunnel 接口建立邻居关系。

■ 重分布内网直连的网段(朝向 Branch2_Access 的网段)进入到 Area1 中。

■ Area1 为末节区域,但要求能够将重分布的直连网段路由发送到 HQ 路由器上。

■ 不能在 Branch2 上配置任何静态路由。

■ 要求对路由更新做精确汇总,使得 HQ 学到的路由条目最少。

■ 如果要做路由过滤请使用 route-map(名称 filter_con)过滤重分布的网段,要求使用前缀列表(名称 con_net)。

2.2.8　IPv6 路由协议部署方案

1. 所有路由器和三层交换机上均需启用 IPv6 单播路由。

2. Branch1 和 HQ 之间启用 RIPng。

(1)Branch1 使用的 process 标识为 Branch1。

(2)HQ 使用的 process 标识为 HQ。

(3)Branch1 在 Fa0/0 和 Fa0/1 接口上都启用 RIPng。

(4)HQ 在 Fa0/0.100 上启用 RIPng,并向 Branch1 送出一条 IPv6 的默认路由。

3. Core_SW、HQ、Branch2 之间启用 OSPFv3,process ID 都为 1。

(1)Core_SW 的所有 SVI 接口都在 OSPFv3 的 Area0 中。

(2)手动指定 Core_SW 的 OSPFv3 Router-ID 为 192.168.13.1。

(3)HQ 的 Fa0/0.110 接口在 OSPFv3 Area0 中。

(4)Branch2 和 HQ 的 Tunnel 1 接口在 OSPFv3 Area1 中,请确认两台路由器可以通过 Tunnel 建立 OSPFv3 邻居。

(5)HQ 上手动指定 OSPFv3 的 Router-ID 为 200.200.200.1。

(6)在 HQ 上将 Area0 的 IPv6 路由精确汇总。

(7)在 HQ 上将 RIPng 路由条目重分布到 OSPFv3 中,metric 设置为 30。

(8)在 HQ 上设置 Area1 为末节区域,禁止将从 RIPng 重分布到 OSPFv3 中的外部路由传播到的 Branch2 上,但不能影响 Branch2 的内网与 Branch1 内网之间的 IPv6 通信。

(9)在 Branch2 上手工指定 OSPFv3 Router-ID 为 200.200.200.2。

(10)将 Branch2 上的直连接口重分布到 Area 1 中。

(11)在 Branch2 上设置 Area1 为末节区域,但要求能够将重分布的直连网段路由发送到 HQ 路由器上。

(12)不能在 Branch2 上配置任何静态路由。

(13)在 Branch2 上配置路由汇总信息,将 Area1 的路由条目精确汇总。

2.2.9 在总部和分支机构 2 之间部署站点到站点间的 VPN

在 HQ 和 Branch2 之间配置站点到站点间的 GRE over IPSec。

1. 在前面需求中 Branch2 和 HQ 之间已经建立了 GRE 隧道(Tunnel 1),IPv4 和 IPv6 流量应都透过 GRE 隧道传递。

2. 在 HQ 和 Branch2 应用下列参数配置 GRE over IPSec。

(1)Isakmp policy 序号 10。

- 3DES 加密。
- Pre-share 方式密码验证。
- Group2。
- 有效时间 4 小时。

(2)Isakmp 预共享密钥为 2012comp,互相指向直连物理接口的地址(200.200.200.x)。

(3)IPSec 转换集名称 set1。

- 策略应用为 AH,SHA 完整性检查。
- AES 192 位加密。

(4)Crypto map 名称 map1 序号 10。

- 完美向前检查 group2。
- 使用名为 101 的 ACL 匹配要加密的 GRE 流量。

请直接在物理接口上应用 crypto map,应用后请检查路由协议仍能正常工作。

2.2.10 在总部路由器 HQ 上配置 EzVPN

在 HQ 路由器上配置 EzVPN 服务器。

1. 在 HQ 上启用 AAA。

(1)用户名 user1,密码 2012comp,请确保这个信息在配置文件中以明文方式保存。

(2)AAA 认证列表名 GSVPN,本地验证方式。

(3)AAA 授权列表名 GSVPN,本地授权方式。

2. EzVPN 组名 gsgroup1。

(1)组密钥 12345。

(2)DNS 服务器 192.168.17.100。

(3)使用本地地址池分配地址,地址池名称 EZVPNP1,地址范围 192.168.7.10 到 192.168.7.50。

3. EzVPN 转换集名称 ezset,使用 ESP-3DES 加密,ESP-SHA 方式验证数据完整性。

(1)静态 crypto map 名称 ezmap,序号 10。

(2)动态 crypto map 名称 dm1,序号 10,要求注入拨入的客户端的主机路由到路由表中。

(3)要求加密所有从 Client1 外出的流量。

(4)在 IP 地址为 192.168.5.2 的接口上应用 crypto map ezmap。

4.在 Client1 上使用 VPN 客户端软件拨入到 HQ,验证 EzVPN 可否正常工作。

2.2.11　IP 语音系统设计

在总部 Market 部门和 Sales 部门分别安装两台 IP 电话,提供 VoIP 服务;为了节约成本,在分支机构 1 的 Client1 上和分支机构 2 的 Client2 上分别安装软件 IP 电话,在 HQ 上和 Branch2 路由器上启用 Call Manager Express,为软、硬件 IP 电话提供电话服务。

1.配置 IP 电话号码,所有 Branch2、HQ 上的电话均应支持在其本地注册的 CME 实现三方通话,配置参数如表 2-6 所示。

表 2-6　　IP 电话配置参数表

电话设备	对应的 CME 设备	电话号码	电话号码对应的名称	电话号码 DN 编号	提供 CME 注册服务的 IP 地址
Client1 上的软件电话	HQ	6001	Branch1	3	192.168.5.10
7911 硬件电话	HQ	1001	Market	1	192.168.5.10
7945 硬件电话	HQ	2001	Sales	2	192.168.5.10
Client2 上的软件电话	Branch2	3001	Branch2-1	1	192.168.8.1
暂无	Branch2	3002	Branch2-2	2	192.168.8.1

2.在 Branch2 的 CME 上配置如下参数:

(1)最多支持 3 个电话。

(2)最多支持 5 个电话号码,自动分配这 5 个电话号码。

(3)以 192.168.8.1 端口 2000 提供服务。

(4)所有到 60xx、10xx、20xx 的呼叫送到 192.168.5.5 (HQ)。

(5)所有注册到 HQ 的 IP 电话应显示一条信息:“ 2012COMP”(不包括引号)。

(6)所有电话采用中国时区,时间为 24 小时格式,日期格式为日-月-年。

3.在 HQ 上的 CME 上配置如下参数:

(1)最多支持 5 个电话。

(2)最多支持 10 个电话号码。

(3)以 192.168.5.10 端口 2000 提供服务。

(4)所有到 30xx 的呼叫送到 192.168.5.6(Branch2)。

(5)所有注册到 HQ 的 IP 电话应显示一条信息:“ 2012COMP”(不包括引号)。

(6)所有电话采用中国时区,时间为 24 小时格式,日期格式为日-月-年。

4.使用 IP 电话互相呼叫验证是否正常工作。对于 Client1 ,要求在成功建立 EzVPN 之后再拨叫 IP 电话验证。

2.2.12　在 Branch_1 上启用基于区域的防火墙(Zone Base Firewall)

为了保护 Branch_1 上的用户安全,请按照下面规则在该设备上启用基于区域的防火墙:

1. 区域名称 Inside，对应接口 Fa0/0。

2. 区域名称 Outside，对应接口 Fa0/1。

3. 由外向内的 zone-pair 命名为 Out-To-In，对应的策略名为 Outside-To-Inside。

4. 由内向外的 zone-pair 命名为 In-To-Out，对应的策略名为 Inside-To-Outside。

5. 内网访问外网的策略要求为：

(1)设置名为 inside-to-outside-Pa 的参数，要求针对 TCP 半开连接的保护底限为 1000，高限为 1500，TCP 三次握手应在 15 秒内完成。

(2)针对内网访问外网的流量，对下列协议采用 inspect 策略，并应用上面设置的保护参数：http、ftp、icmp、isakmp，对应的 class-map 名称为 PROTOCOL-In-to-Out。

(3)针对内网访问外网的 VPN ESP 流量直接允许通过，使用名为 PROTOCOL-In-to-Out-SEC 的 class-map 来匹配，要求调用名为 SEC 的 ACL 来匹配所有 ESP 流量。

(4)其余所有流量直接丢弃。

6. 外网访问内网的策略要求为：

(1)设置名为 outside-to-inside-Pa 的参数，要求针对 TCP 半开连接的保护底限为 100，高限为 150。

(2)针对 VPN ESP 流量直接允许通过，使用名为 PROTOCOL-Out-to-In-SEC 的 class-map 来匹配，要求调用名为 SEC 的 ACL 来匹配所有 ESP 流量。

(3)内网将会有一台 HTTP 服务器(IP：201.201.201.100，目前没有实际连接到网络中)，请设置一个 ACL 匹配这个机器的 IP 地址(ACL 名称：Out-to-In)。

(4)设置一个名为 PROTOCOL-Out-to-In 的 class-map，匹配 http 流量和 Out-to-In ACL，利用该 class-map 实现对内网 HTTP 服务器的 inspect 保护，并调用前面设置的 outside-to-inside-Pa 参数实现防止 DoS 攻击。

(5)丢弃所有其他流量。

2.2.13 部署 QoS 对流量进行优化

在路由器 Branch_2 上配置 QoS 策略，对要通过隧道到 HQ 的流量进行优化。

1. 对进入 Fa0/0.1 接口的流量调用名为 phone-in 的规则，对流量打标记。

(1)使用 class-map 的 soft-phone 匹配 RTP 流量。

(2)对 RTP 流量打标记为 IP DSCP EF

(3)在 Fa0/0.1 和 Fa0/0 接口上启用服务识别 RTP 流量。

2. 在 Fa0/1 出向调用 phone-out 策略，对流量进行排队。

(1)使用名为 EF 的 class-map 匹配 DSCP 为 EF 的数据包，优先保证 300Kbps 带宽。

(2)使用名为 QoS-Routing 的 class-map 匹配 ip precedence 7 或 ip precedence 6 的数据包，优先保证 100Kbps 带宽。

(3)默认其他所有流量不保证带宽，并且做基于 DSCP 的 WRED。

3. 由于所有的流量要通过 Tunnel，并且要做 IPSec 加密，请在 Tunnel 口做出配置保留加密前的 IP 包头中的 TOS 字段。

2.2.14　设备管理

1. 在设备上启用 NTP 服务

(1)Branch_1 使用的 NTP 服务器地址 192.168.5.2。

(2)Branch_2 使用的 NTP 服务器地址 192.168.5.5。

(3)Core_SW 使用的 NTP 服务器地址 192.168.5.2。

(4)请在 HQ 上手动设定时间为当前时间和日期,并且将其作为 NTP 服务器,级别为 1。

(5)所有设备设定时区为东八区(+8),时区名称 BJ。

2. 在 3560 PoE 交换机上配置节电策略

(1)利用 EnergyWise 实现节电功能。

(2)EnergyWise domain 名称为 2012comp,预共享密钥 12345,以明文方式保存密钥。

(3)在 Fa0/5 接口上应用下面策略:

- 工作日全天 24 小时供电,供电级别 10,重要性 90,使用 time-range t1 实现。
- 周末全天 24 小时不供电,重要性为 90,使用 time-range t2 实现。

3. 在 Core_SW 和 HQ 上配置 SSH 版本 2

(1)使用的域名为 abc.com。

(2)要求仅启用 SSH 版本 2。

(3)SSH 超时时间 60 秒。

(4)使用用户名 user1,密码 2012comp 作为用户账户信息,采用本地认证。

2.3　项目实施

在网络项目实施过程中,通常我们要先实施二层技术,二层技术中首先就是要在交换机上把事先规划好的 VLAN 配上,并且把相应的端口分配给相应的 VLAN,完成这一步,在网络中分布的各个部门和各种应用就清晰了;从技术上说,分割了广播域,划分出不同的子网。然后,考虑哪些端口需要启用 Trunk,哪些端口需要应用端口聚合等二层技术。

2.3.1　创建 VLAN 并为 VLAN 分配对应的端口

1. 任务描述

在本项目中,总部有两台交换机,一台 2960 的二层交换机,我们命名为 HQ_Access,一台 3560 三层交换机,我们命名为 Core_SW。在 HQ_Access 交换机上有两个 VLAN:VLAN 40 和 VLAN 2012。VLAN 40 是连接服务器 Server2 的网络,VLAN 2012 是这台交换机的管理 VLAN。在 Core_SW 交换机上有十个 VLAN,其中 VLAN 10 和 VLAN 20 分别是连接两台硬件 IP 电话机;VLAN 30 和 VLAN 40 分别是连接服务器区的 Server1 和 Server2 两台服务器;VLAN 50 和 VLAN 60 分别是连接从无线 AP 接入进来的两个会议室的网络;VLAN 300 是从无线 AP 接入的非会议室的其他用户临时使用;VLAN 100 是路由器 Branch_1 和路由器 HQ 互连的网络;VLAN 110 是路由器 HQ 和三层交换机 Core_SW 互连的网络;VLAN 2012 是交