设备命名：

Ruijie>en

Ruijie#

Ruijie#con

Ruijie(config)#hostname ISP-RSR20-01

ISP-RSR20-01(config)#

为交换机和无线控制器开启SSH服务端功能，用户名和密码为admin，密码为明文类型,特权密码为admin；

ISP-RSR20-01(config)#username admin password admin

ISP-RSR20-01(config)#enable service ssh-server

ISP-RSR20-01(config)#enable password admin

ISP-RSR20-01(config)#line vty 0 4

ISP-RSR20-01(config-line)#login local

ISP-RSR20-01(config-line)#transport input ssh

ISP-RSR20-01(config-line)#exit

配置所有设备SNMP消息，向主机172.16.0.254发送Trap消息版本采用V2C，读写的Community为“ruijie”，只读的Community为“public”，开启Trap消息。

ISP-RSR20-01(config)#snmp-server host 172.16.0.254 traps version 2c ruijie

ISP-RSR20-01(config)#snmp-server host 172.16.0.254 traps version 2c public

ISP-RSR20-01(config)#snmp-server enable traps

ISP-RSR20-01(config)#snmp-server community ruijie rw

ISP-RSR20-01(config)#snmp-server community public ro

AP版本升级：

Ap的默认ip地址为192.168.110.1,设置pc机的ip地址与其在同一网段，确保能web登录至ap,登录后升级。

交换机版本升级：

在交换机控制台输入enable service web-server，然后配置PC与交换机处于同一网段，web登录升级。

S3聚合口AG1：

BX-S5750-01(config)#int aggregatePort 1

BX-S5750-01(config-if-AggregatePort 1)#switchport mode trunk

BX-S5750-01(config-if-AggregatePort 1)#switchport trunk allowed vlan only 10,20,30,40,50,60,100

BX-S5750-01(config)#int r gi0/1 -2

BX-S5750-01(config-if-range)#port-group 1

S3聚合口AG3：

BX-S5750-01(config)#int aggregatePort 3

BX-S5750-01(config-if-AggregatePort 3)#switchport mode trunk

BX-S5750-01(config-if-AggregatePort 3)# switchport trunk allowed vlan only 10,20,30,40,50,60,100

BX-S5750-01(config-if-AggregatePort 3)#exi

BX-S5750-01(config)#int r gi0/4 -5

BX-S5750-01(config-if-range)#port-group 3

S3 Gi0/3口：

BX-S5750-01(config)#int gi0/3

BX-S5750-01(config-if-GigabitEthernet 0/3)#switchport mode trunk

BX-S5750-01(config-if-GigabitEthernet 0/3)# switchport trunk allowed vlan only 50,60,100

S1/S2 隐含配置：

BX-VSU-S2910(config)#int aggregateport 1

BX-VSU-S2910(config-if-AggregatePort 1)#switchport mode trunk

BX-VSU-S2910(config-if-AggregatePort 1)#switchport trunk allowed vlan only 10,20,30,40,50,60,100

BX-VSU-S2910(config-if-AggregatePort 1)#exi

BX-VSU-S2910(config)#int aggregateport 2

BX-VSU-S2910(config-if-AggregatePort 2)#switchport mode trunk

BX-VSU-S2910(config-if-AggregatePort 2)# switchport trunk allowed vlan only 10,20,30,40,50,60,100

BX-VSU-S2910(config-if-AggregatePort 2)#exi

BX-VSU-S2910(config)#int r gi1/0/23 , 2/0/23

BX-VSU-S2910(config-if-range)#port-group 1

BX-VSU-S2910(config-if-range)#exi

BX-VSU-S2910(config)#int r gi1/0/24 , 2/0/24

BX-VSU-S2910(config-if-range)#port-group 2

S5 私有vlan配置：

FX-S5750-01(config)#vlan 11

FX-S5750-01(config-vlan)#name Community\_vlan

FX-S5750-01(config-vlan)#private-vlan community

FX-S5750-01(config-vlan)#exi

FX-S5750-01(config)#vlan 12

FX-S5750-01(config-vlan)#name Isolated\_vlan

FX-S5750-01(config-vlan)#private-vlan Isolated

FX-S5750-01(config-vlan)#EXI

FX-S5750-01(config)#vlan 10

FX-S5750-01(config-vlan)#name Primary\_vlan

FX-S5750-01(config-vlan)#private-vlan primary

FX-S5750-01(config-vlan)#private-vlan association add 11-12

FX-S5750-01(config)#int vlan 10

FX-S5750-01(config-if-VLAN 10)#

FX-S5750-01(config-if-VLAN 10)#sw

FX-S5750-01(config-if-VLAN 10)#switchport m

FX-S5750-01(config-if-VLAN 10)#switchport mo

FX-S5750-01(config-if-VLAN 10)#exi

FX-S5750-01(config)#

FX-S5750-01(config)#

FX-S5750-01(config)#int r gi0/1 -4

FX-S5750-01(config-if-range)#switchport mode private-vlan host

FX-S5750-01(config-if-range)#switchport private-vlan host-association 10 11

FX-S5750-01(config-if-range)#exi

FX-S5750-01(config)#int r gi0/5 -8

FX-S5750-01(config-if-range)#switchport mode private-vlan host

FX-S5750-01(config-if-range)#switchport private-vlan host-association 10 12

S6 tunnel口ipv6配置：

ZW-S6000C-01(config)#ipv6 unicast-routing

ZW-S6000C-01(config)#int tunnel 0

ZW-S6000C-01(config-if-Tunnel 0)#ipv6 enable

ZW-S6000C-01(config-if-Tunnel 0)#ipv6 address 2001:193:10::253/64

ZW-S6000C-01(config-if-Tunnel 0)#tunnel source 50.1.0.10

ZW-S6000C-01(config-if-Tunnel 0)#tunnel destination 50.1.0.14

以tunnel口建立隧道(只要tunnel的源和目的互通状态就up了)

S3 ipv6(及vrrp)配置：(S4同理)

BX-S5750-01(config)#int vlan 10

BX-S5750-01(config-if-VLAN 10)#ipv6 enable

BX-S5750-01(config-if-VLAN 10)#ipv6 address 2001:192:10::252/64

BX-S5750-01(config-if-VLAN 10)#no ipv6 nd suppress-ra

BX-S5750-01(config-if-VLAN 10)#vrrp 10 ipv6 fe80::1

BX-S5750-01(config-if-VLAN 10)#vrrp 10 ipv6 2001:192:10::254

BX-S5750-01(config-if-VLAN 10)#vrrp ipv6 10 priority 150

BX-S5750-01(config-if-VLAN 10)#vrrp ipv6 10 accept\_mode

BX-S5750-01(config-if-VLAN 10)#int vlan 20

BX-S5750-01(config-if-VLAN 20)# vrrp 20 ipv6 FE80::1

BX-S5750-01(config-if-VLAN 20)# vrrp 20 ipv6 2001:192:20::254

BX-S5750-01(config-if-VLAN 20)# ipv6 address 2001:192:20::252/64

BX-S5750-01(config-if-VLAN 20)# ipv6 enable

BX-S5750-01(config-if-VLAN 20)# no ipv6 nd suppress-ra

BX-S5750-01(config-if-VLAN 20)# vrrp ipv6 20 priority 150

BX-S5750-01(config-if-VLAN 20)# vrrp ipv6 20 accept\_mode

BX-S5750-01(config-if-VLAN 20)#int vlan 30

BX-S5750-01(config-if-VLAN 30)# vrrp 30 ipv6 FE80::1

BX-S5750-01(config-if-VLAN 30)# vrrp 30 ipv6 2001:192:30::254

BX-S5750-01(config-if-VLAN 30)# ipv6 address 2001:192:30::252/64

BX-S5750-01(config-if-VLAN 30)# ipv6 enable

BX-S5750-01(config-if-VLAN 30)# no ipv6 nd suppress-ra

BX-S5750-01(config-if-VLAN 30)# vrrp ipv6 30 priority 150

BX-S5750-01(config-if-VLAN 30)# vrrp ipv6 30 accept\_mode

BX-S5750-01(config-if-VLAN 30)#int vlan 40

BX-S5750-01(config-if-VLAN 40)# vrrp 40 ipv6 FE80::1

BX-S5750-01(config-if-VLAN 40)# vrrp 40 ipv6 2001:192:40::254

BX-S5750-01(config-if-VLAN 40)# ipv6 address 2001:192:40::252/64

BX-S5750-01(config-if-VLAN 40)# ipv6 enable

BX-S5750-01(config-if-VLAN 40)# no ipv6 nd suppress-ra

BX-S5750-01(config-if-VLAN 40)# vrrp ipv6 40 priority 150

BX-S5750-01(config-if-VLAN 40)# vrrp ipv6 40 accept\_mode

在交换机S3、S4上配置DHCP中继

BX-S5750-01(config)#service dhcp

BX-S5750-01(config)#ip helper-address 11.1.0.11

DHCP服务器搭建于EG1上，地址池命名为Pool\_VLAN10，DHCP对外服务使用loopback 0地址；

BX-EG2000-01(config)#service dhcp

BX-EG2000-01(config)#ip dhcp pool Pool\_VLAN10

BX-EG2000-01(dhcp-config)#network 192.1.10.0 255.255.255.0

BX-EG2000-01(dhcp-config)#default-router 192.1.10.254

 规避高流量报文风暴对网络的冲击，在交换机S5上针对用户终端接口的广播，组播，未知名单播启用风暴限制，限制级别2

FX-S5750-01(config)#int r gi0/1-16

FX-S5750-01(config-if-range)#storm-control broadcast level 2

FX-S5750-01(config-if-range)#storm-control multicast level 2

FX-S5750-01(config-if-range)#storm-control unicast level 2

 为了防止伪IP源地址攻击，导致出口路由器会话占满，要求S5交换机部署端口安全，接口Gi0/1只允许PC3通过。

FX-S5750-01(config)#int gi0/1

FX-S5750-01(config-if-GigabitEthernet 0/1)#switchport port-security

FX-S5750-01(config-if-GigabitEthernet 0/1)#switchport port-security max 1

FX-S5750-01(config-if-GigabitEthernet 0/1)#$ort-security mac 00ff.ffff.ffff

在总部交换机S1、S2、S3、S4上配置MSTP防止两层环路；要求所有有线数据流经过S3转发，S3失效时经过S4转发。所配置的参数要求如下：

 region-name为ruijie；

 revision版本为1；

 S3作为实例中的主根，S4作为实例中的从根；

 主根优先级为4096，从根优先级为8192；

 在S3和S4上配置VRRP，实现主机的网关冗余，所配置的参数要求如表1-11；

 S3、S4各VRRP组中高优先级设置为150，低优先级设置为120。

S3：

BX-S5750-01(config)#spanning-tree mode mstp

BX-S5750-01(config)#spanning-tree mst configuration

BX-S5750-01(config-mst)#re 1

BX-S5750-01(config-mst)#name ruijie

BX-S5750-01(config-mst)#exit

BX-S5750-01(config)#spanning-tree mst 0 pri 4096

S4：

BX-S5750-02(config)#spanning-tree mode mstp

BX-S5750-02(config)#spanning-tree mst configuration

BX-S5750-02(config-mst)#re 1

BX-S5750-02(config-mst)#name ruijie

BX-S5750-02(config-mst)#exit

BX-S5750-02(config)#spanning-tree mst 0 pri 8192

S3：

BX-S5750-01(config)#int vlan 10

BX-S5750-01(config-if-VLAN 10)#vrrp 10 ip 192.1.10.254

BX-S5750-01(config-if-VLAN 10)#vrrp 10 priority 150

S4：

BX-S5750-02(config)#int vlan 10

BX-S5750-02(config-if-VLAN 10)#vrrp 10 ip 192.1.10.254

BX-S5750-02(config-if-VLAN 10)#vrrp 10 priority 120

规划S1和S2间的Te0/27-28端口作为VSL链路，使用VSU技术实现网络设备虚拟化。其中S1为主，S2为备；

* 规划S1和S2间的Gi0/22端口作为双主机检测链路，配置基于BFD的双主机检测，当VSL的所有物理链路都异常断开时，备机会切换成主机，从而保障网络正常；
* 主设备：Domain id：1,switch id:1,priority 150，description：S2910-1;
* 备设备：Domain id：1,switch id：2，priority 120，description：S2910-2。

主设备：

Ruijie(config)#switch virtual domain 1

Ruijie(config-vs-domain)#switch 1 priority 150

Ruijie(config-vs-domain)#switch 1 description S2910-1

Ruijie(config-vs-domain)#exi

Ruijie(config)#vsl-port

Ruijie(config-vsl-port)#port-member interface tenGigabitEthernet 0/27

Ruijie(config-vsl-port)#port-member interface tenGigabitEthernet 0/28

Ruijie(config-vsl-port)#end

\*Jun 22 09:53:29: %SYS-5-CONFIG\_I: Configured from console by console

Ruijie#

Ruijie#wr

Ruijie#switch convert mode virtual

Convert mode will backup and delete config file, and reload the switch. Are you sure to continue[yes/no]:y

备设备：

Ruijie(config)#switch virtual domain 1

Ruijie(config-vs-domain)#switch 2 priority 120

Ruijie(config-vs-domain)#switch 2 description S2910-2

Ruijie(config-vs-domain)#exi

Ruijie(config)#vsl-port

Ruijie(config-vsl-port)#port-member interface tenGigabitEthernet 0/27

Ruijie(config-vsl-port)#port-member interface tenGigabitEthernet 0/28

Ruijie(config-vsl-port)#end

\*Jun 22 09:53:29: %SYS-5-CONFIG\_I: Configured from console by console

Ruijie#

Ruijie#wr

Ruijie#switch convert mode virtual

Convert mode will backup and delete config file, and reload the switch. Are you sure to continue[yes/no]:y

BFD检测：

Ruijie(config)#hostname BX-VSU-S2910

BX-VSU-S2910(config)#int r gi1/0/22 , 2/0/22

BX-VSU-S2910(config-if-range)#no switchport

BX-VSU-S2910(config-if-range)#exi

BX-VSU-S2910(config)#switch virtual domain 1

BX-VSU-S2910(config-vs-domain)#dual-active detection bfd

BX-VSU-S2910(config-vs-domain)# dual-active bfd interface gigabitEthernet 1/0/22

BX-VSU-S2910(config-vs-domain)# dual-active bfd interface gigabitEthernet 2/0/22

为规避网络末端接入设备上出现环路影响全网，要求在总部接入设备S1、S2进行防环处理。具体要求如下：

* 终端接口开启BPDU防护不能接收BPDU 报文；
* 终端接口下开启RLDP防止环路，检测到环路后处理方式为Shutdown-Port；
* 连接终端的所有端口配置为边缘端口；
* 如果端口被BPDU Guard检测进入Err-Disabled状态，再过300秒后会自动恢复（基于接口部署策略），重新检测是否有环路；

BX-VSU-S2910(config)#rldp enable

BX-VSU-S2910(config)#errdisable recovery interval 300

BX-VSU-S2910(config)#int r gi0/1 -16

BX-VSU-S2910(config-if-range)#spanning-tree bpduguard enable

BX-VSU-S2910(config-if-range)#rldp port loop-detect shutdown-port

BX-VSU-S2910(config-if-range)#spanning-tree portfast

BX-VSU-S2910(config-if-range)#errdisable recovery interval 300

* 为了防御动态环境局域网伪DHCP服务欺骗，在S1、S2交换机部署DHCP Snooping功能；
* 为了防止大量网关发送的正常的相关报文被接入交换机误认为是攻击被丢弃，从而导致下联用户无法获取网关的ARP信息而无法上网，要求关闭S1/S2上联口的NFPP功能；
* 全局设置NFPP日志缓存容量为1024，打印相同log的阈值为300s;
* 调整CPU保护机制中ARP阈值500pps；

BX-VSU-S2910(config)#ip dhcp snooping

BX-VSU-S2910(config)#cpu-protect type arp pps 500

BX-VSU-S2910(config)#int aggregateport 1

BX-VSU-S2910(config-if-AggregatePort 1)#ip dhcp snooping trust

BX-VSU-S2910(config-if-AggregatePort 1)#exi

BX-VSU-S2910(config)#int aggregateport 2

BX-VSU-S2910(config-if-AggregatePort 2)#ip dhcp snooping trust

BX-VSU-S2910(config-if-AggregatePort 2)#exi

BX-VSU-S2910(config)#nfpp

BX-VSU-S2910(config-nfpp)#log-buffer enable

BX-VSU-S2910(config-nfpp)#log-buffer entries 1024

BX-VSU-S2910(config-nfpp)#log-buffer logs 1 interval 300

BX-VSU-S2910(config)#cpu-protect type arp pps 500

BX-VSU-S2910(config)#int r gi1/0/23 ,2/0/23 ,1/0/24 ,2/0/24

BX-VSU-S2910(config-if-range)#no nfpp arp-guard enable

BX-VSU-S2910(config-if-range)#no nfpp icmp-guard enable

BX-VSU-S2910(config-if-range)#no nfpp ip-guard enable

BX-VSU-S2910(config-if-range)#no nfpp dhcp-guard enable

BX-VSU-S2910(config-if-range)#no nfpp nd-guard enable

BX-VSU-S2910(config-if-range)#no nfpp dhcpv6-guard enable

总部与分校内网均使用OSPF协议组网，总部、分校与互联网间使用静态路由协议。具体要求如下：

 总部S3、S4、EG1、AC1、AC2间运行OSPF，进程号为10，规划多区域：区域0（S3、S4、EG1），区域1（S3、S4、AC1、AC2）；

 AC1、AC2 OSPF接口不参与DR/BDR选举；

 区域1部署为完全NSSA类型进而简化AC1,AC2路由条目；

 分部EG2、S5间运行OSPF，进程号为10，规划单区域：区域0（EG2、S5）；

 要求业务网段中不出现协议报文；

 要求所有路由协议都发布具体网段；

 为了管理方便，需要发布Loopback地址;

 优化OSPF相关配置，以尽量加快OSPF收敛；

 重发布路由进OSPF中使用类型1。

注意：S3需要重发布云平台（172.16.0.0/22）静态路由至总部内网。

S3：

BX-S5750-01(config)#rou ospf 10

BX-S5750-01(config-router)#network 10.1.0.2 0.0.0.3 a 0

BX-S5750-01(config-router)#network 11.1.0.33 0.0.0.0 a 0

BX-S5750-01(config-router)#network 192.1.10.0 0.0.0.255 a 0

BX-S5750-01(config-router)#network 192.1.20.0 0.0.0.255 a 0

BX-S5750-01(config-router)#network 192.1.30.0 0.0.0.255 a 0

BX-S5750-01(config-router)#network 192.1.40.0 0.0.0.255 a 0

BX-S5750-01(config-router)#network 192.1.100.0 0.0.0.255 a 1

BX-S5750-01(config-router)#redistribute static metric-type 1 subnets

BX-S5750-01(config)#ip rou 172.16.0.0 255.255.252.0 193.1.0.2

BX-S5750-01(config)#int gi0/24

BX-S5750-01(config-if-GigabitEthernet 0/24)#ip ospf ne point-to-point （优化OSPF相关配置，以尽量加快OSPF收敛）

S4：

BX-S5750-02(config)#rou ospf 10

BX-S5750-02(config-router)# passive-interface VLAN 10

BX-S5750-02(config-router)# passive-interface VLAN 20

BX-S5750-02(config-router)# passive-interface VLAN 30

BX-S5750-02(config-router)# passive-interface VLAN 40

BX-S5750-02(config-router)# area 1 nssa no-summary

BX-S5750-02(config-router)# network 10.1.0.4 0.0.0.3 area 0

BX-S5750-02(config-router)# network 11.1.0.34 0.0.0.0 area 0

BX-S5750-02(config-router)# network 192.1.10.0 0.0.0.255 area 0

BX-S5750-02(config-router)# network 192.1.20.0 0.0.0.255 area 0

BX-S5750-02(config-router)# network 192.1.30.0 0.0.0.255 area 0

BX-S5750-02(config-router)# network 192.1.40.0 0.0.0.255 area 0

BX-S5750-02(config-router)# network 192.1.100.0 0.0.0.255 area 1

BX-S5750-02(config-if-GigabitEthernet 0/24)#ip ospf ne point-to-point （优化OSPF相关配置，以尽量加快OSPF收敛）

EG1

BX-EG2000-01(config)#rou ospf 10

BX-EG2000-01(config-router)#network 10.1.0.1 0.0.0.3 a 0

BX-EG2000-01(config-router)#network 10.1.0.5 0.0.0.3 a 0

BX-EG2000-01(config-router)#network 11.1.0.11 0.0.0.0 a 0

BX-EG2000-01(config-router)#default-information originate metric-type 1

BX-EG2000-01(config)#int gi0/0

BX-EG2000-01(config-if-GigabitEthernet 0/0)#ip ospf ne point-to-point

BX-EG2000-01(config)#int gi0/1

BX-EG2000-01(config-if-GigabitEthernet 0/0)#ip ospf ne point-to-point

AC1：

BX-WS6008-01(config)#rou ospf 10

BX-WS6008-01(config-router)#network 11.1.0.204 0.0.0.0 a 1

BX-WS6008-01(config-router)#network 192.1.50.0 0.0.0.255 a 1

BX-WS6008-01(config-router)#network 192.1.60.0 0.0.0.255 a 1

BX-WS6008-01(config-router)#area 1 nssa no-summary

BX-WS6008-01(config-router)#network 192.1.100.0 0.0.0.255 a 1

BX-WS6008-01(config-router)#int vlan 100

BX-WS6008-01(config-if-VLAN 100)#ip ospf priority 0 （不参与ospf DR/BDR选举）

AC2：

BX-WS6008-02(config)#rou ospf 10

BX-WS6008-02(config-router)#network 11.1.0.205 0.0.0.0 a 1

BX-WS6008-02(config-router)#network 192.1.50.0 0.0.0.255 a 1

BX-WS6008-02(config-router)#network 192.1.60.0 0.0.0.255 a 1

BX-WS6008-02(config-router)#area 1 nssa no-summary

BX-WS6008-02(config-router)#network 192.1.100.0 0.0.0.255 a 1

BX-WS6008-02(config-router)#int vlan 100

BX-WS6008-02(config-if-VLAN 100)#ip ospf priority 0 （不参与ospf DR/BDR选举）

S5：

FX-S5750-01(config)#rou ospf 10

FX-S5750-01(config-router)#network 10.1.0.10 0.0.0.3 a 0

FX-S5750-01(config-router)#network 11.1.0.5 0.0.0.0 a 0

FX-S5750-01(config-router)#network 194.1.10.0 0.0.0.255 a 0

FX-S5750-01(config-router)#network 194.1.20.0 0.0.0.255 a 0

FX-S5750-01(config-router)#network 194.1.30.0 0.0.0.255 a 0

FX-S5750-01(config-router)#network 194.1.40.0 0.0.0.255 a 0

FX-S5750-01(config-router)#passive-interface vlan 10

FX-S5750-01(config-router)#passive-interface vlan 20

FX-S5750-01(config-router)#passive-interface vlan 30

FX-S5750-01(config-router)#passive-interface vlan 40

FX-S5750-01(config-router)#int gi0/24

FX-S5750-01(config-if-GigabitEthernet 0/24)#ip ospf ne point-to-point

EG2：

FX-EG2000-01(config)#rou ospf 10

FX-EG2000-01(config-router)#network 10.1.0.9 0.0.0.3 a 0

FX-EG2000-01(config-router)#network 11.1.0.12 0.0.0.0 a 0

FX-EG2000-01(config-router)#int gi0/0

FX-EG2000-01(config-if-GigabitEthernet 0/0)#ip ospf ne point-to-point

* 驻外办事处内网均部署OSPFV3协议，进程号10，区域号为0；
* 驻外办事处间S6/S7通过Gre隧道实现办事处间局域网IPV6终端互联互通,且隧道内运行OSPFV3协议。

例：S7

ZW-S6000C-02(config)#ipv6 router ospf 10

ZW-S6000C-02(config-router)#exi

ZW-S6000C-02(config)#int vlan 10

ZW-S6000C-02(config-if-VLAN 10)#ipv6 ospf 10 area 0

ZW-S6000C-02(config-if-VLAN 10)#exi

ZW-S6000C-02(config)#int vlan 20

ZW-S6000C-02(config-if-VLAN 20)#ipv6 ospf 10 area 0

ZW-S6000C-02(config-if-VLAN 20)#exi

ZW-S6000C-02(config)#int tu

ZW-S6000C-02(config)#int tunnel 0

ZW-S6000C-02(config-if-Tunnel 0)#ipv6 ospf 10 area 0

ZW-S6000C-02(config-if-Tunnel 0)#exi

1. **QoS部署**

为了防止突发数据过大并导致网络拥挤，必须对接入的用户流量加以限制。具体要求如下：

* 分校接入设备S5的Gi0/1至Gi0/16接口入方向设置接口限速，限速10Mbps,猝发流量1024 kbytes；

FX-S5750-01(config)#int r gi0/1 -16

FX-S5750-01(config-if-range)#rate-limit input 10000 1024

二级运营商R3服务节点在带宽为2Mbps的S3/0接口做流量整形；

ISP-RSR20-03(config)#int s3/0

ISP-RSR20-03(config-if-Serial 3/0)#traffic-shape rate 2000000

二级运营商R3服务节点在G0/0接口做流量监管，上行报文流量不能超过10Mbps，Burst-normal为1M bytes，burst-max为2M bytes如果超过流量限制则将违规报文丢弃。

ISP-RSR20-03(config)#int gi0/0

ISP-RSR20-03(config-if-GigabitEthernet 0/0)#rate-limit input 10000000 1000000 2000000 conform-action continue exceed-action drop

上海办事处与杭州办事处均有生产与研发部门，为了确保办事处间各业务部门互联互通的效率和质量为此申请二级运营商专线业务。针对运营商组网及驻外办事处网络部署要求如下：

 R1、R2、R3直连接口封装PPP协议，部署IGP中OSPF动态路由实现直连网段互联互通；

R1：

ISP-RSR20-01(config)#rou ospf 10

ISP-RSR20-01(config-router)#network 50.1.0.1 0.0.0.3 a 0

ISP-RSR20-01(config-router)#net 11.1.0.1 0.0.0.0 a 0

ISP-RSR20-01(config-router)#int s2/0

ISP-RSR20-01(config-if-Serial 2/0)#enc ppp

R2：

ISP-RSR20-02(config)#rou ospf 10

ISP-RSR20-02(config-router)#network 50.1.0.5 0.0.0.3 a 0

ISP-RSR20-02(config-router)#network 50.1.0.2 0.0.0.3 a 0

ISP-RSR20-02(config-router)#network 11.1.0.2 0.0.0.0 a 0

ISP-RSR20-02(config-router)#int s2/0

ISP-RSR20-02(config-if-Serial 2/0)#enc ppp

ISP-RSR20-02(config-router)#int s3/0

ISP-RSR20-02(config-if-Serial 3/0)#enc ppp

R3:

ISP-RSR20-03(config)#rou ospf 10

ISP-RSR20-03(config-router)#network 50.1.0.6 0.0.0.3 a 0

ISP-RSR20-03(config-router)#network 11.1.0.3 0.0.0.0 a 0

ISP-RSR20-03(config-router)#int s3/0

ISP-RSR20-03(config-if-Serial 3/0)#enc ppp

 S6、S7关于IGP协议只维护直连路由，不使用任何路由协议；

 R1、R2及R2、R3间部署IBGP,AS号为100，使用Loopback接口建立Peer；

R3:

ISP-RSR20-03(config)#rou bgp 100

ISP-RSR20-03(config-router)#neighbor 11.1.0.2 remote-as 100

ISP-RSR20-03(config-router)#neighbor 11.1.0.2 update-source loop 0

ISP-RSR20-03(config-router)#neighbor 11.1.0.2 next-hop-self

R1:

ISP-RSR20-01(config)#rou bgp 100

ISP-RSR20-01(config-router)#neighbor 11.1.0.2 remote-as 100

ISP-RSR20-01(config-router)#neighbor 11.1.0.2 update-source loop 0

ISP-RSR20-01(config-router)#neighbor 11.1.0.2 next-hop-self

 部署R2作为R1与R3的路由反射器RR；

R2:

ISP-RSR20-02(config)#rou bgp 100

ISP-RSR20-02(config-router)#neighbor 11.1.0.1 remote-as 100

ISP-RSR20-02(config-router)#neighbor 11.1.0.1 update-source loop 0

ISP-RSR20-02(config-router)#neighbor 11.1.0.1 next-hop-self

ISP-RSR20-02(config-router)#neighbor 11.1.0.3 remote-as 100

ISP-RSR20-02(config-router)#neighbor 11.1.0.3 update-source loop 0

ISP-RSR20-02(config-router)#neighbor 11.1.0.3 next-hop-self

ISP-RSR20-02(config-router)#neighbor 11.1.0.1 route-reflector-client

ISP-RSR20-02(config-router)#neighbor 11.1.0.3 route-reflector-client

 R1、S6部署EBGP，AS号为110，使用直连接口建立Peer；

R1:

ISP-RSR20-01(config-router)#neighbor 50.1.0.10 remote-as 110

S6:

ZW-S6000C-01(config)#rou bgp 110

ZW-S6000C-01(config-router)#neighbor 50.1.0.9 remote-as 100

 R3、S7部署EBGP，AS号为120,使用直连接口建立Peer；

R3:

ISP-RSR20-03(config)#rou bgp 100

ISP-RSR20-03(config-router)#neighbor 50.1.0.14 remote-as 120

S7:

ZW-S6000C-02(config)#rou bgp 120

ZW-S6000C-02(config-router)#neighbor 50.1.0.13 remote-as 100

 办事处业务网段通告至二级运营商的路由条目只有一条汇总后的B段路由，且保证汇总后路径信息不丢失；

S6:

ZW-S6000C-01(config)#rou bgp 110

ZW-S6000C-01(config-router)#network 60.1.10.0 mask 255.255.255.0

ZW-S6000C-01(config-router)#network 60.1.20.0 mask 255.255.255.0

ZW-S6000C-01(config-router)#aggregate-address 60.1.0.0 255.255.0.0 summary-only

ZW-S6000C-01(config-router)#network 50.1.0.10 mask 255.255.255.252

ZW-S6000C-01(config-router)#netwo 11.1.0.6 ma 255.255.255.255

S7:

ZW-S6000C-02(config-router)#network 70.1.10.0 mask 255.255.255.0

ZW-S6000C-02(config-router)#network 70.1.20.0 mask 255.255.255.0

ZW-S6000C-02(config-router)#aggregate-address 70.1.0.0 255.255.0.0 summary-only

ZW-S6000C-02(config-router)#network 50.1.0.12 mask 255.255.255.252

ZW-S6000C-02(config-router)#netwo 11.1.0.7 ma 255.255.255.255

 二级运营商通告宽带业务接入网段至办事处，R1处以汇总B段静态路由的方式进行发布。

R1:

ISP-RSR20-01(config)#ip rou 20.1.0.0 255.255.0.0 nu 0

ISP-RSR20-01(config)#ip rou 30.1.0.0 255.255.0.0 nu 0

ISP-RSR20-01(config)#ip rou 40.1.0.0 255.255.0.0 nu 0

ISP-RSR20-01(config)#rou bgp 100

ISP-RSR20-01(config-router)#network 20.1.0.0 mask 255.255.0.0

ISP-RSR20-01(config-router)#network 30.1.0.0 mask 255.255.0.0

ISP-RSR20-01(config-router)#network 40.1.0.0 mask 255.255.0.0

北京分校不同业务部门对于上海与杭州驻外办事处有业务互访需求，具体要求如下：

 分校内网VLAN10终端通过R1服务节点中转访问上海办事处；

 分校内网VLAN40终端通过R3服务节点中转访问杭州办事处；

 当EG2与R1、R3服务节点间链路失效时，可自动切换到R2服务节点进行转发；

 Route-map策略名为Fenliu；

 分校VLAN10流量由ACL101（编号101）来定义；

 分校VLAN40流量由ACL102（编号102）来定义；

 为加快广域网线路异常时策略路由可快速收敛转发，为此部署Track检测，编号Track1,Track2,Track3分别检测本端广域网联通、电信、教育网接口状态，一旦接口协议状态为DOWN即刻进行切换。

EG2:

FX-EG2000-01(config)#track 1 interface gi0/2 line-protocol

FX-EG2000-01(config-track)#delay up 0 down 0

FX-EG2000-01(config-track)#exit

FX-EG2000-01(config)#track 2 interface gi0/3 line-protocol

FX-EG2000-01(config-track)#delay up 0 down 0

FX-EG2000-01(config-track)#exit

FX-EG2000-01(config)#track 3 interface gi0/4 line-protocol

FX-EG2000-01(config-track)#delay up 0 down 0

FX-EG2000-01(config-track)#exit

FX-EG2000-01(config)#ip access-list ex 101

FX-EG2000-01(config-ext-nacl)#per ip 194.1.10.0 0.0.0.255 60.1.0.0 0.0.255.255

FX-EG2000-01(config)#ip access-list ex 102

FX-EG2000-01(config-ext-nacl)#per ip 194.1.40.0 0.0.0.255 70.1.0.0 0.0.255.255

FX-EG2000-01(config)#route-map Fenliu permit 10

FX-EG2000-01(config-route-map)#match ip address 101

FX-EG2000-01(config-route-map)#set ip next-hop verify-availability 20.1.0.9 track 1

FX-EG2000-01(config-route-map)#set ip next-hop verify-availability 30.1.0.9 track 2

FX-EG2000-01(config)#route-map Fenliu permit 20

FX-EG2000-01(config-route-map)#match ip address 102

FX-EG2000-01(config-route-map)#set ip next-hop verify-availability 40.1.0.9 track 3

FX-EG2000-01(config-route-map)#set ip next-hop verify-availability 30.1.0.9 track 2

FX-EG2000-01(config-route-map)#int gi0/0

FX-EG2000-01(config-if-GigabitEthernet 0/0)#ip policy route-map Fenliu

路由选路部署

考虑到数据分流及负载均衡的目的，具体要求如下：

 可通过修改OSPF路由COST达到分流的目的，且其值必须为5或10；

 总部有线IPV4用户与互联网互通主路径规划为：VSU-S3-EG1；

 总部无线IPV4用户与互联网互通主路径规划为：AC2-S4-EG1；

 主链路故障时可无缝切换到多条备用链路上。

S3:

BX-S5750-01(config)#int vlan 10

BX-S5750-01(config-if-VLAN 10)#ip ospf c

BX-S5750-01(config-if-VLAN 10)#ip ospf cost 5

BX-S5750-01(config-if-VLAN 10)#int vlan 20

BX-S5750-01(config-if-VLAN 20)#ip ospf cost 5

BX-S5750-01(config-if-VLAN 20)#int vlan 30

BX-S5750-01(config-if-VLAN 30)#ip ospf cost 5

BX-S5750-01(config-if-VLAN 30)#int vlan 40

BX-S5750-01(config-if-VLAN 40)#ip ospf cost 5

BX-S5750-01(config-if-VLAN 40)#int vlan 100

BX-S5750-01(config-if-VLAN 100)#ip ospf cost 10

BX-S5750-01(config)#rou ospf 10

BX-S5750-01(config-router)#area 1 default-cost 10

S4:

BX-S5750-02(config)#int vlan 10

BX-S5750-02(config-if-VLAN 10)#ip ospf cost 10

BX-S5750-02(config-if-VLAN 10)#int vlan 20

BX-S5750-02(config-if-VLAN 20)#ip ospf cost 10

BX-S5750-02(config-if-VLAN 20)#int vlan 30

BX-S5750-02(config-if-VLAN 30)#ip ospf cost 10

BX-S5750-02(config-if-VLAN 30)#int vlan 40

BX-S5750-02(config-if-VLAN 40)#ip ospf cost 10

BX-S5750-02(config-if-VLAN 40)#int vlan 100

BX-S5750-02(config-if-VLAN 100)#ip ospf cost 5

BX-S5750-02(config)#route ospf 10

BX-S5750-02(config-router)#area 1 default-cost 5

1. **无线网络基础部署**

* 使用AC1和AC2作为总部无线用户和无线AP的DHCP服务器，使用S5作为分校无线用户和无线AP的DHCP服务器；
* AP3以透明模式进行部署，S5部署DHCP服务为无线终端及AP分配地址,且AP每次均获取地址均为194.XX.20.2(XX现场提供)；

AC1配置：

BX-WS6008-01(config)#ip dhcp excluded-address 192.1.50.252 192.1.50.254

BX-WS6008-01(config)#ip dhcp excluded-address 192.1.60.252 192.1.60.254

BX-WS6008-01(config)#service dhcp

BX-WS6008-01(config)#ip dhcp pool AP

BX-WS6008-01(dhcp-config)# option 138 ip 11.1.0.204 11.1.0.205

BX-WS6008-01(dhcp-config)#network 192.1.50.0 255.255.255.0

BX-WS6008-01(dhcp-config)#default-router 192.1.50.254

BX-WS6008-01(dhcp-config)#exi

BX-WS6008-01(config)#ip dhcp pool yonghu

BX-WS6008-01(dhcp-config)#network 192.1.60.0 255.255.255.0

BX-WS6008-01(dhcp-config)#default-router 192.1.60.254

BX-WS6008-01(dhcp-config)#exi

S5配置(连接ap的端口必须放通的vlan)

FX-S5750-01(config)#int gi0/21

FX-S5750-01(config-if-GigabitEthernet 0/21)#switchport mode trunk

FX-S5750-01(config-if-GigabitEthernet 0/21)#switchport trunk allowed vlan only 20,30,40

FX-S5750-01(config-if-GigabitEthernet 0/21)#switchport trunk native vlan 20

FX-S5750-01(config-if-GigabitEthernet 0/21)#exi

FX-S5750-01(config)#service dhcp

FX-S5750-01(config)#ip dhcp pool AP

FX-S5750-01(dhcp-config)#hardware-address 0074.9c22.f6c4 (mac地址为ap的mac地址)

FX-S5750-01(dhcp-config)#host 194.1.20.2 255.255.255.0

FX-S5750-01(dhcp-config)#default-router 194.1.20.254

FX-S5750-01(dhcp-config)#exi

FX-S5750-01(config)#ip dhcp pool Wiressless\_users1

FX-S5750-01(dhcp-config)#network 194.1.30.0 255.255.255.0

FX-S5750-01(dhcp-config)#default-router 194.1.30.254

FX-S5750-01(dhcp-config)#exi

FX-S5750-01(config)#ip dhcp pool Wiressless\_users2

FX-S5750-01(dhcp-config)#network 194.1.40.0 255.255.255.0

FX-S5750-01(dhcp-config)#default-router 194.1.40.254

* 创建总部内网SSID为Ruijie-BX\_XX(XX现场提供)，WLAN ID为1，AP-Group为BX，总部内网无线用户关联SSID后可自动获取地址。
* 要求总部内网无线网络启用本地转发模式；
* 为了保障总部每个用户的无线体验，针对WLAN ID 1下的每个用户的下行平均速率为800kB/s，突发速率为1600kB/s；

BX-WS6008-01(config)#wlan-config 1 Ruijie-BX\_1

BX-WS6008-01(config-wlan)#tunnel local

BX-WS6008-01(config-wlan)#wlan-based per-user-limit down-streams average-data-rate 800 burst-data-rate 1600

BX-WS6008-01(config)#ap-group BX

BX-WS6008-01(config-group)#interface-mapping 1 60 ap-wlan-id 1

BX-WS6008-01(config-group)#tunnel local wlan 1 vlan 60

1. **AC热备部署**

* 总部AC2为主用，AC1为备用。AP与AC1、AC2均建立隧道，当AP与AC2失去连接时能无缝切换至AC1并提供服务。

AC1配置：

BX-WS6008-01(config)#wlan hot-backup 11.1.0.205

BX-WS6008-01(config-hotbackup)#context 10

BX-WS6008-01(config-hotbackup-ctx)#ap-group BX

BX-WS6008-01(config-hotbackup-ctx)#exi

BX-WS6008-01(config-hotbackup)#wlan hot-backup enable

\*Jun 22 14:50:32: %WLAN\_HOTBACKUP-6-PEER: wlan hot-backup start doing ENABLE, please wait.

\*Jun 22 14:50:32: %WLAN\_HOTBACKUP-6-PEER: Peer(11.1.0.205) hot-backup enable.

AC2配置：

BX-WS6008-01(config)#wlan hot-backup 11.1.0.204

BX-WS6008-01(config-hotbackup)#context 10

BX-WS6008-01(config-hotbackup-ctx)#priority level 7

BX-WS6008-01(config-hotbackup-ctx)#ap-group BX

BX-WS6008-01(config-hotbackup-ctx)#exi

BX-WS6008-01(config-hotbackup)#wlan hot-backup enable

1. **无线安全部署**

* 总部无线用户接入无线网络时需要采用WPA2加密方式，密码为XX(现场提供)；
* 为了防御无线局域网ARP欺骗影响用户上网体验，总部配置无线环境ARP欺骗防御功能。

BX-WS6008-01(config)#wlansec 1

BX-WS6008-01(config-wlansec)#security rsn enable

BX-WS6008-01(config-wlansec)#security rsn ciphers aes enable

BX-WS6008-01(config-wlansec)#security rsn akm psk enable

BX-WS6008-01(config-wlansec)#security rsn akm psk set-key ascii 12345678

BX-WS6008-01(config-wlansec)#exi

BX-WS6008-01(config)#ip dhcp snooping

BX-WS6008-01(config)#int gi0/1

BX-WS6008-01(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust

BX-WS6008-01(config)#wlansec 1

BX-WS6008-01(config-wlansec)#ip verify source port-security

BX-WS6008-01(config-wlansec)#arp-check

BX-WS6008-01(config-wlansec)#exi

* 分校启用白名单校验，仅放通PC3无线终端；

BX-WS6008-01(config)#wids

BX-WS6008-01(config-wids)#whitelist mac-address 00ff.ffff.ffff

BX-WS6008-01(config-wids)#whitelist max 1

* 总部每AP最大带点人数为45人；
* 总部通过时间调度，要求每周一至周五的21:00至23:30期间关闭无线服务；
* 总部设置用户最小接入信号强度为-65dBm；

BX-WS6008-01(config)#schedule session 1

Session 1 is created now.

BX-WS6008-01(config)#schedule session 1 time-range 1 period Mon to Fri time 21:00 to 23:30

BX-WS6008-01(config)#ap-config 5869.6cd6.8fc5

You are going to config AP(5869.6cd6.8fc5), which is online now.

BX-WS6008-01(config-ap)#ap-name BX-AP520-01

The AP(BX-AP520-01) is on line.

BX-WS6008-01(config-ap)#ap-group BX

BX-WS6008-01(config-ap)#sta-limit 45

BX-WS6008-01(config-ap)#response-rssi 30 radio 1

BX-WS6008-01(config-ap)#response-rssi 30 radio 2

BX-WS6008-01(config-ap)#quiet-mode session 1

BX-WS6008-01(config-ap)#no 11acsupport enable radio 2

BX-WS6008-01(config-ap)#channel 1 radio 1

BX-WS6008-01(config-ap)#exi

BX-WS6008-01(config)#ac-controller

BX-WS6008-01(config-ac)#802.11a network rate 6 disabled

BX-WS6008-01(config-ac)#802.11a network rate 9 disabled

BX-WS6008-01(config-ac)#802.11b network rate 1 disabled

BX-WS6008-01(config-ac)#802.11b network rate 2 disabled

BX-WS6008-01(config-ac)#802.11b network rate 5 disabled

BX-WS6008-01(config-ac)#802.11g network rate 5 disabled

BX-WS6008-01(config-ac)#802.11g network rate 2 disabled

BX-WS6008-01(config-ac)#802.11g network rate 1 disabled

BX-WS6008-01(config-ac)#exi

1. **胖AP部署**

北京校区使用无线AP胖模式进行部署，具体要求如下：

* AP3创建SSID(WLAN-ID 1)为Ruijie-BJ\_XX\_1(XX现场提供),分校内网无线用户关联SSID后可自动获取分校VLAN30网段地址；
* AP3创建SSID(WLAN-ID 2)为Ruijie-BJ\_XX\_2(XX现场提供),分校内网无线用户关联SSID后可自动获取分校VLAN40网段地址。

AP3配置：

FX-AP520-01(config)#int gi0/1

FX-AP520-01(config-if-GigabitEthernet 0/1)#ip address dhcp

FX-AP520-01(config-if-GigabitEthernet 0/1)#exi

00:03:54: %DHCP\_CLIENT-6-ADDRESS\_ASSIGN: Interface GigabitEthernet 0/1 assigned DHCP address 194.1.20.2, mask 255.255.255.0.

FX-AP520-01(config)#vlan 30

FX-AP520-01(config-vlan)#exi

FX-AP520-01(config)#vlan 40

FX-AP520-01(config-vlan)#exit

FX-AP520-01(config)#dot11 wlan 1

FX-AP520-01(dot11-wlan-config)#vlan 30

FX-AP520-01(dot11-wlan-config)#ssid Ruijie-BJ\_1\_1

FX-AP520-01(dot11-wlan-config)#exi

FX-AP520-01(config)#dot11 wlan 2

FX-AP520-01(dot11-wlan-config)#vlan 40

FX-AP520-01(dot11-wlan-config)#ssid Ruijie-BJ\_1\_2

FX-AP520-01(dot11-wlan-config)#exi

FX-AP520-01(config)#int gi0/1.3

FX-AP520-01(config-subif-GigabitEthernet 0/1.3)#encapsulation dot1Q 30

FX-AP520-01(config-subif-GigabitEthernet 0/1.3)#exi

FX-AP520-01(config)#int gi0/1.4

FX-AP520-01(config-subif-GigabitEthernet 0/1.4)#encapsulation dot1Q 40

FX-AP520-01(config-subif-GigabitEthernet 0/1.4)#exi

FX-AP520-01(config)#int dot11radio 1/0.3

FX-AP520-01(config-subif-Dot11radio 1/0.3)#encapsulation dot1Q 30

FX-AP520-01(config-subif-Dot11radio 1/0.3)#wlan-id 1

FX-AP520-01(config-subif-Dot11radio 1/0.3)#exi

FX-AP520-01(config)#int dot11radio 1/0.4

FX-AP520-01(config-subif-Dot11radio 1/0.4)#encapsulation dot1Q 40

FX-AP520-01(config-subif-Dot11radio 1/0.4)#wlan-id 2

出口NAT部署

具体配置参数如下：

 出口网关上进行NAT配置实现总部与分校的所有用户均可访问互联网，通过NAPT方式将内网用户IP地址转换到互联网接口上，同时总部用户仅可在周一到周五工作时间09：00-17:00（命名为work）访问互联网；

EG1:

BX-EG2000-01(config)#time-range work

BX-EG2000-01(config-time-range)#periodic weekdays 09:00 to 17:00

BX-EG2000-01(config)#ip access-list ex 110

BX-EG2000-01(config-ext-nacl)#permit ip 192.1.0.0 0.0.255.255 any time-range work

BX-EG2000-01(config-ext-nacl)#permit ip 172.16.0.0 0.0.3.255 any time-range work

BX-EG2000-01(config-ext-nacl)#int gi0/0

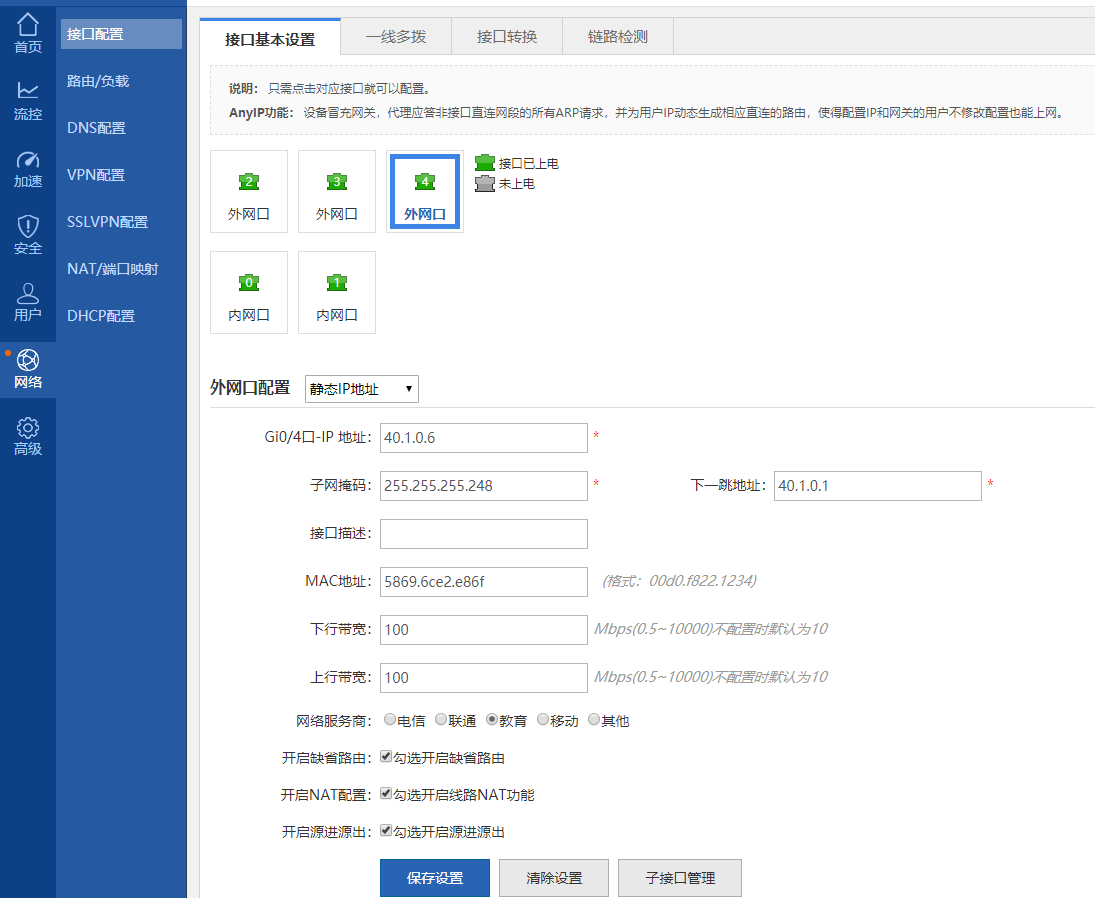
BX-EG2000-01(config-if-GigabitEthernet 0/0)#ip nat in

BX-EG2000-01(config-if-GigabitEthernet 0/0)#int gi0/1

BX-EG2000-01(config-if-GigabitEthernet 0/1)#ip nat in









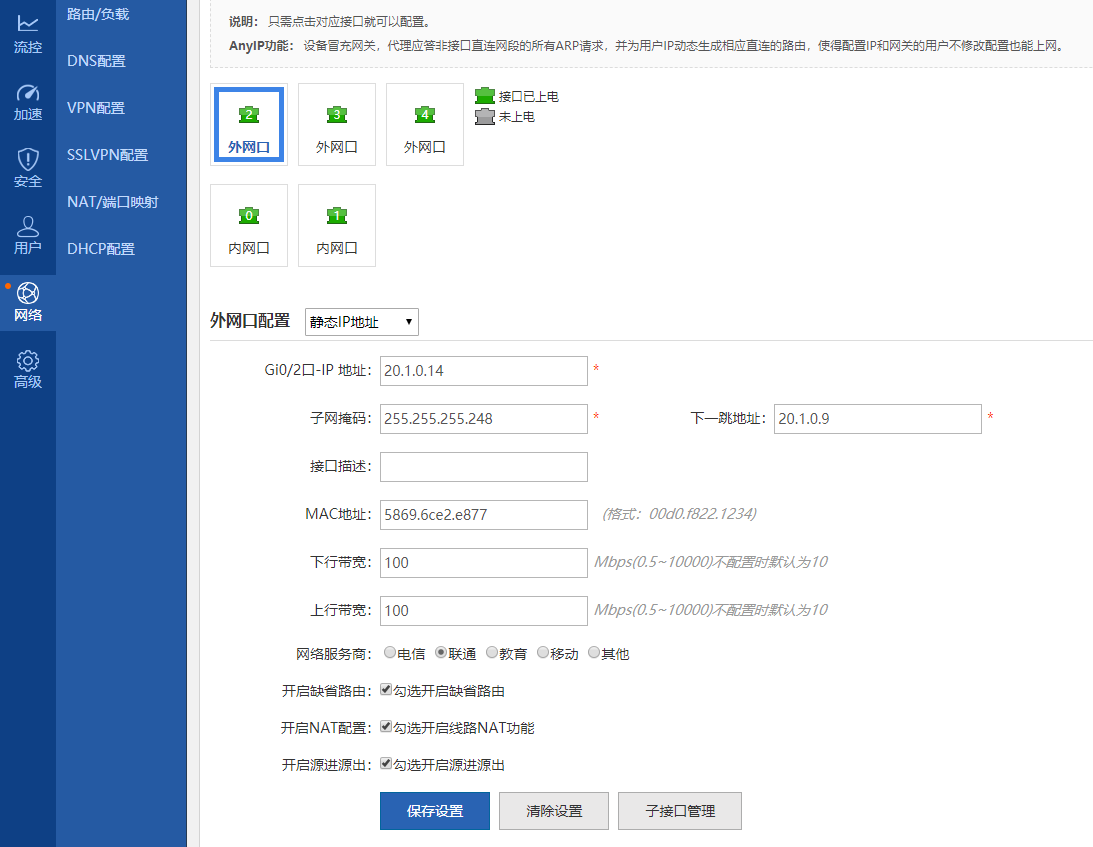
EG2:

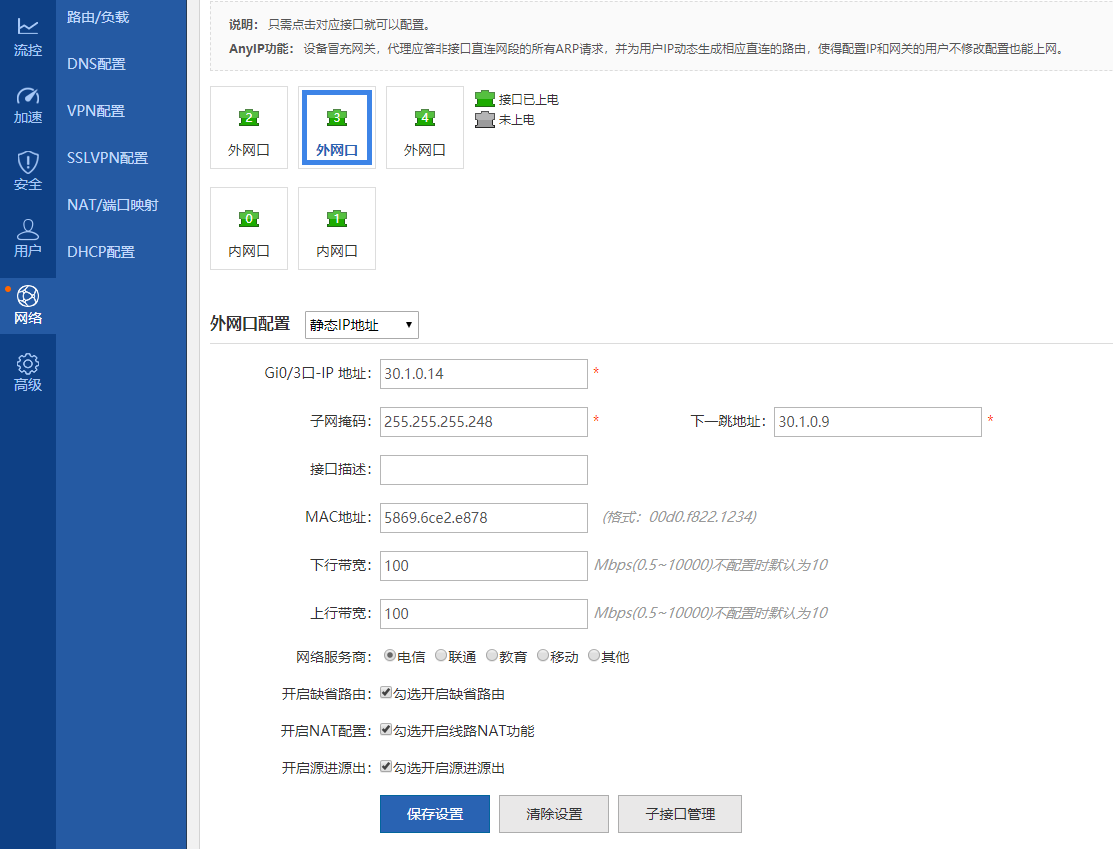
FX-EG2000-01(config)#ip access-list ex 110

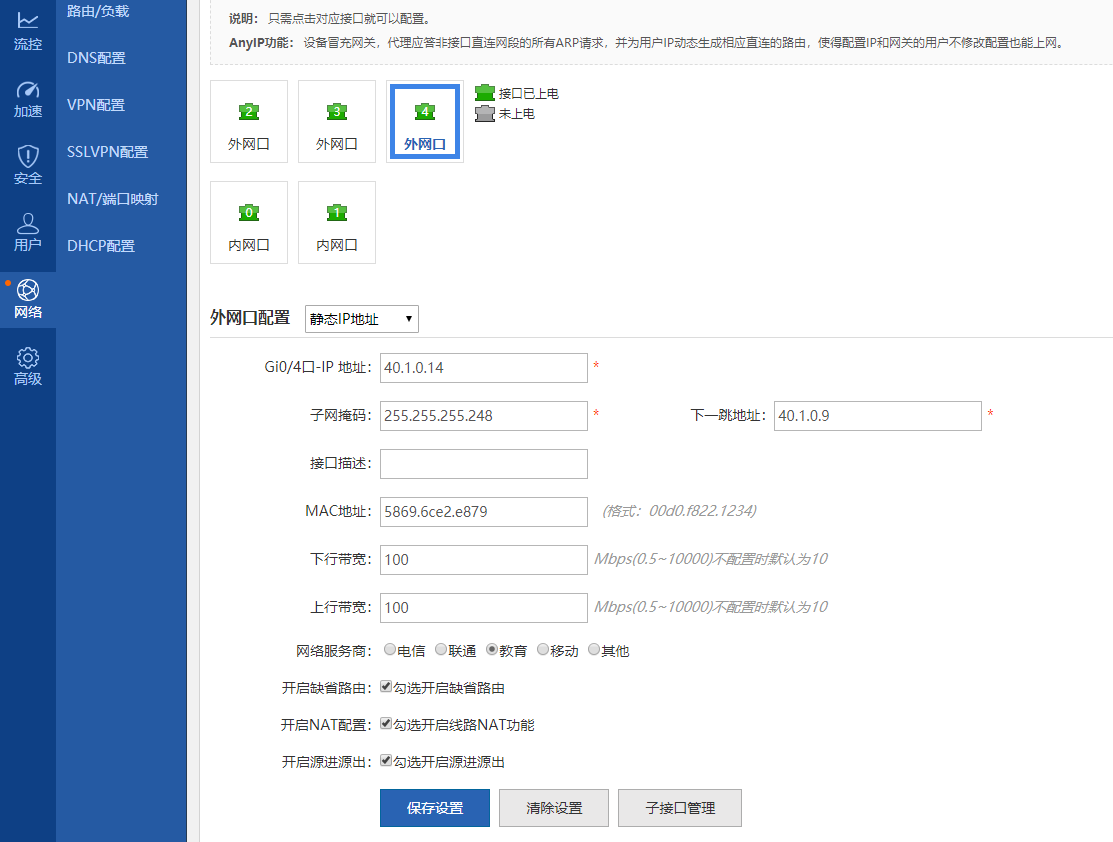
FX-EG2000-01(config-ext-nacl)#permit ip 194.1.0.0 0.0.255.255 any

FX-EG2000-01(config-ext-nacl)#int gi0/0

FX-EG2000-01(config-if-GigabitEthernet 0/0)#ip nat in









 在总部EG1上配置，使总部核心交换S4（11.1.0.34）设备的SSH服务可以通过互联网被访问，将其地址映射至联通线路上，映射地址为20.1.0.2；

EG1:

BX-EG2000-01(config)#ip nat in source static tcp 11.1.0.34 22 20.1.0.2 22 permit-inside

 总部内网主机有访问上海办事处S6设备的Telnet服务需求，但总部内网因网络规划要求不能引入外部路由，同时上海办事处网络运维人员考虑安全起见也不希望将S6设备（11.1.0.6）地址对外公布。为此规划在出口网关上进行NAT地址转化将S6真实地址映射至20.1.0.20。

EG1:

BX-EG2000-01(config)#ip nat outside source static tcp 11.1.0.6 23 20.1.0.20 23

全局流表策略部署

在用户没有防火墙做限制的情况下，如果遇到大量的伪源IP攻击，或者是端口扫描时，会把设备的流表给占满，而导致正常的数据无法建流而被丢弃，为此要求总部部署全局流表防火墙，ACL（编号为102）策略要求如下：

 放通所有IP到本设备外网接口的ICMP、Telnet协议；

 放通内网终端IP到外网所有资源的访问；

 放通任意IP来访问映射的内网交换机的资源；

 根据上下文要求放通设备已启用的功能协议端口

EG1:

BX-EG2000-01(config)#ip access-list ex 102

BX-EG2000-01(config-ext-nacl)# permit icmp any host 20.1.0.6

BX-EG2000-01(config-ext-nacl)# permit icmp any host 30.1.0.6

BX-EG2000-01(config-ext-nacl)# permit icmp any host 40.1.0.6

BX-EG2000-01(config-ext-nacl)# permit tcp any host 20.1.0.6 eq telnet

BX-EG2000-01(config-ext-nacl)# permit tcp any host 30.1.0.6 eq telnet

BX-EG2000-01(config-ext-nacl)# permit tcp any host 40.1.0.6 eq telnet

BX-EG2000-01(config-ext-nacl)# permit ip 192.1.0.0 0.0.255.255 any

BX-EG2000-01(config-ext-nacl)# permit ip 172.16.0.0 0.0.3.255 any

BX-EG2000-01(config-ext-nacl)# permit tcp any host 20.1.0.2 eq 22

BX-EG2000-01(config-ext-nacl)# permit ospf any any

BX-EG2000-01(config-ext-nacl)# permit udp any any eq snmp

BX-EG2000-01(config-ext-nacl)# permit udp any any eq snmptrap

BX-EG2000-01(config-ext-nacl)# permit esp any any

BX-EG2000-01(config-ext-nacl)# permit udp any eq bootpc any eq bootps

BX-EG2000-01(config-ext-nacl)# permit udp any eq bootps any eq bootpc

BX-EG2000-01(config-ext-nacl)# permit udp any any eq 1701

Web Portal用户认证部署

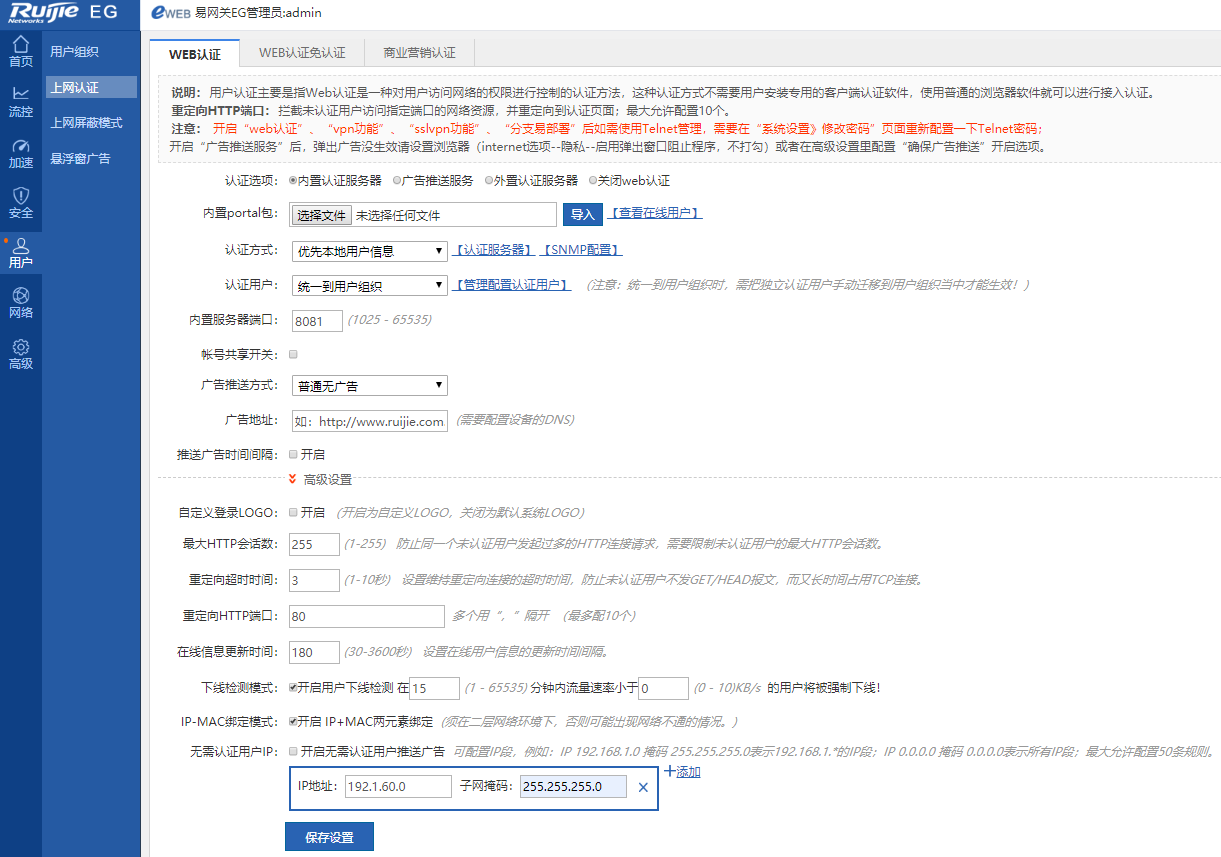
 在总部网关上启用Web Portal认证服务，并创建user1、user2，密码均为XX（现场提供）；

 总部有线用户需进行WEB认证访问互联网；

 总部无线用户不需在EG上进行WEB认证即可访问互联网。

EG1:





应用流量控制部署

 分校EG2联通线路针对访问外网WEB流量限速每IP 1000kbps，内网WEB总流量不超过50Mbps。







用户行为策略部署

 分校EG2基于网站访问、邮件收发、IM聊天、论坛发帖、搜索引擎多应用启用审计功能；



 分校EG2周一到周五工作时间09：00-17:00（命名为work）阻断并审计P2P应用软件使用；



禁止分校内网用户通过浏览器访问http://40.1.0.9。数据分流与负载均衡

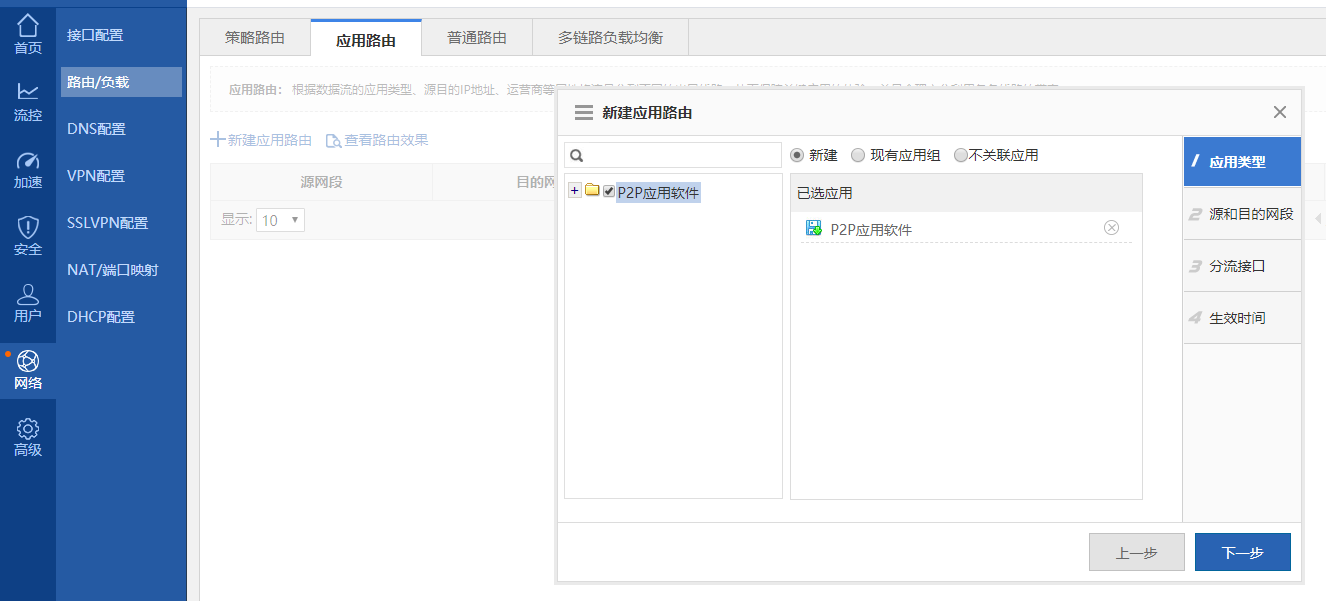


数据分流与负载均衡

 总部与分校用户数据流匹配EG内置联通、电信与教育地址库，实现访问联通资源走联通线路，访问电信资源走电信线路，访问教育网资源走教育网线路；

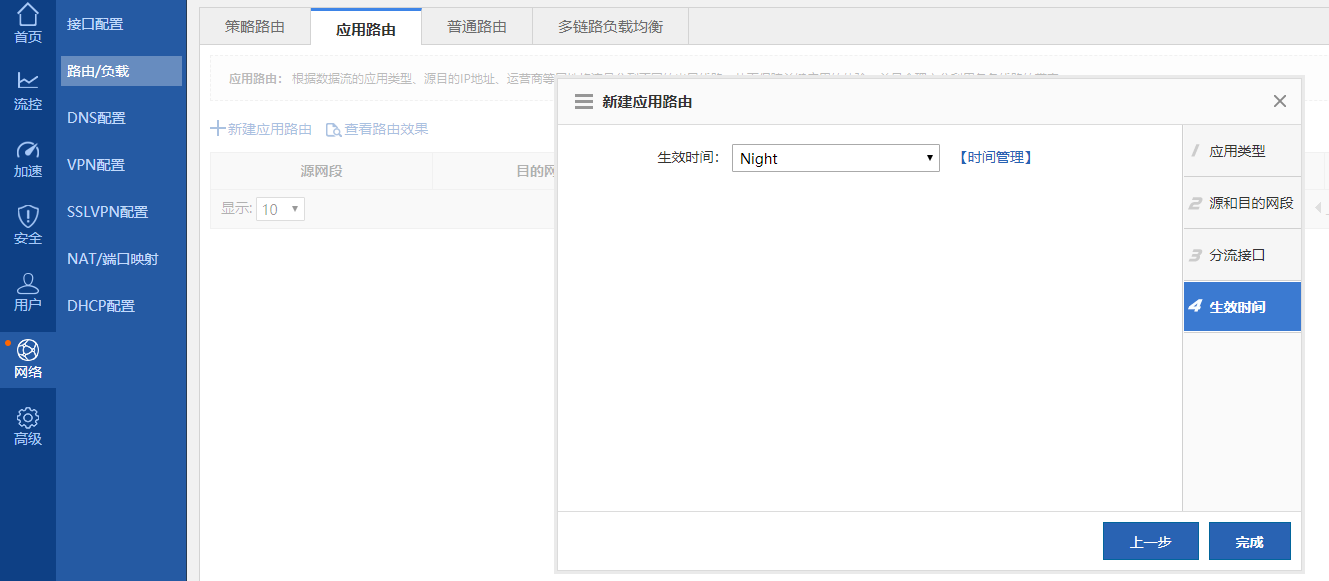
 除联通、电信、教育资源之外默认所有数据流在三条线路间进行负载转发；

 分校EG2每天晚上6点到10点（命名为Night）联通线路上网流量压力较大，将P2P应用软件流量在此时间段内引流到电信线路。









VPN部署

为了实现总部与分部互访数据的安全性，同时要求总部对分部路由器采用本地的用户名、密码方式进行验证，为此规划如下：

 部署L2TP隧道进行总部对分部路由的对接验证，验证用户名密码均为ruijie，L2TP隧道密码为ruijie；

 L2TP用户地址池为12.1.0.1—12.1.0.254，Virtual-Template及Virtual-ppp接口均引用本地loopback 1接口地址；

 L2TP隧道中承载OSPF协议，使其总部与分部通过OSPF进行路由交互，区域号0；

 部署IPSec对L2TP隧道中的业务数据加密；

 IPSec VPN需要采用传输模式，预共享密码为ruijie，加密认证方式为ESP-3DES、ESP-MD5-HMAC，DH使用组2；

 总分机构间数据通信及加密通过二级运营商R1联通节点作为中转设备；

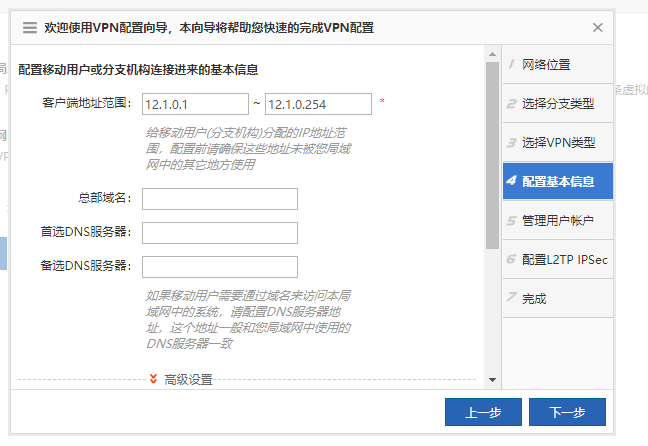
 总部有线IPV4用户与分部IPV4用户互通主路径规划为：VSU-S3-EG1-EG2-S5(EG1/EG2间运行VPN隧道)。

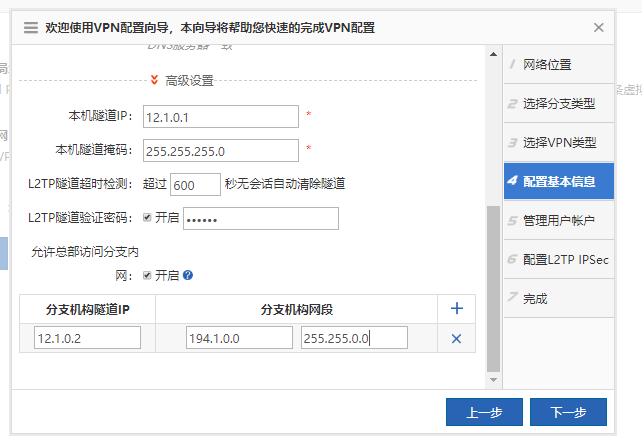
EG1:



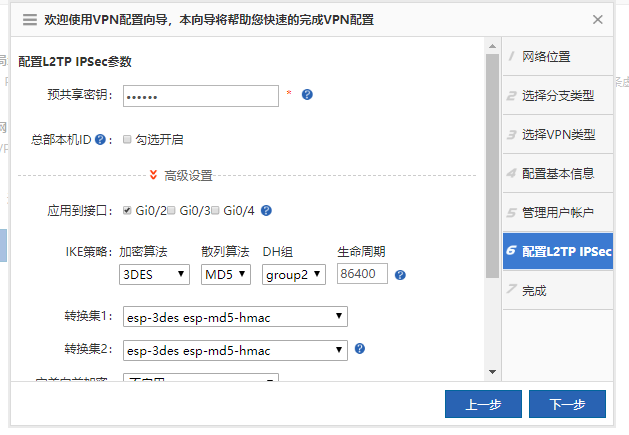


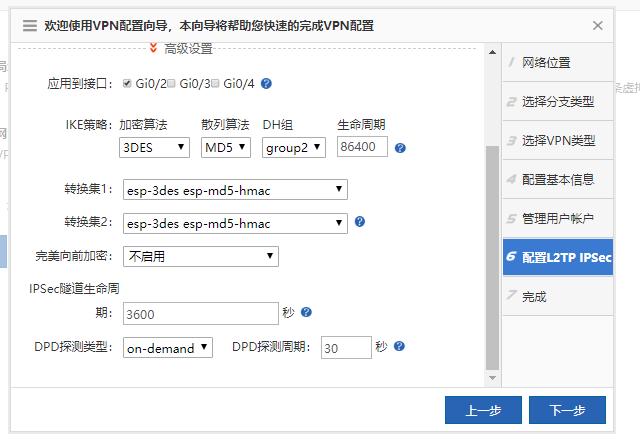












BX-EG2000-01(config)#rou ospf 10

BX-EG2000-01(config-router)#net 12.1.0.1 0.0.0.255 a 0

EG2:







FX-EG2000-01(config)#rou ospf 10

FX-EG2000-01(config-router)#network 12.1.0.2 0.0.0.255 a 0