7750SR/BRAS 维护与配置

（SR 功能篇）

1. 设备配置命令说明

1.1. System 基本配置

1. chassis-mode 要配置为 C，以支持新的 feature。
2. 关闭外部参考时钟（一般现场均没有接）
3. 多链路负载平衡
4. SNMP 报文大小 9216
5. telnet 的 session 限制为设置为最大数 7。
6. 最好定义预设登陆消息，避免设备信息泄露
7. 时间同步由用户提供时钟源（一般是上级路由器，也可能是一台服务器，可能加密）
8. 时区自定义为 GMT8 08 （BJ 08） （BEIJ 08）

配置示例：

```
configure  system
           name "ZJJIH-MC-CMNET-SR/BRAS3-DYYDJF1"
           chassis-mode c
           l4-load-balancing
           lsr-load-balancing lbl-ip
           sync-if-timing
               begin
               ref1
                   shutdown
               exit
               ref2
                   shutdown
               exit
               bits
                   shutdown
               exit
               commit
           exit
           snmp
               packet-size 9216
           exit
           login-control
               ftp
                   inbound-max-sessions 5
               exit
               telnet
                   inbound-max-sessions 7
                   outbound-max-sessions 7
```

```
                idle-timeout 15
            exit
            pre-login-message "Authorised access only ,
                               This system is the property of Internet ,
                               Disconnect IMMEDIATELY if you are not an authorised user!
                               Contact manager for help."
                no login-banner
            exit
            time
                ntp
                    authentication-key 1 key "OAwgNUlbzgI" hash2 type message-digest
                    server 61.174.90.1 key 1 version 3 prefer
                    server 61.174.90.2 key 1 version 3
                    server 61.175.255.59
                    no shutdown
                exit
                sntp
                    shutdown
                exit
                zone BJ 08 （zone GMT8 08   zone BEIJ 08）
            exit
            thresholds
                rmon
                exit
            exit
        exit

#------------------------------------------------
echo "Redundancy Configuration"
#------------------------------------------------
    redundancy
        synchronize config （boot-env）
    exit
```

检查命令：

show chassis **查看** chassis mode **是否为** C。

Show time **查看系统时间。**

修改时间

admin set-time 2010/11/12 19:04:38

admin set-time

- set-time <date> <time>

<date> : YYYY/MM/DD

<time> : hh:mm[:ss]

```
#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
   card 5
        card-type iom2-20g
        mda 1
            mda-type m10-1gb-sfp-b
            ingress
                mcast-path-management
                    shutdown
                exit
            exit
        exit
        mda 2
            mda-type m2-oc48-sfp
            ingress
                mcast-path-management
                    shutdown
                exit
            exit
        exit
    exit
```

注：mcast-path-management 为加强安全，关闭 mcast-path，

1.2. Log 配置

1. 配置本地 log 用于保存 7750SR 的日常设备信息，log-id 为 50，file-id 为 50。

配置示例：
根据 log 99 报告情况，适当抑制一些报告，避免系统报告太多

```
#--------------------------------------------------
echo "Log Configuration"
#--------------------------------------------------
    log
      event-control "chassis" 2063 generate
      event-control "system" 2006 suppress
      event-control "system" 2007 suppress
      event-control "system" 2008 suppress
      event-control "system" 2009 suppress
      event-control "system" 2011 suppress

      file-id 30
            location cf3:
            rollover 600 retention 24
      exit
      log-id 30
            time-format local
            from debug-trace
            to file 30
      exit
      syslog 1
            address 220.188.118.250
            facility local4
            level critical
      exit
      log-id 97
            from main security change
            to syslog 1
      exit
      syslog 2
            description "To-Syslog-Server"
            address 202.101.186.1
            facility local5
            level critical
        exit
        log-id 96
```

```
            from main security change
            to syslog 2
        exit

        snmp-trap-group 98 trap-target "211.140.137.84:162" address 211.140.137.84
             snmpv2c notify-community "SR/BRAS11-DYYDJF1"
        exit
        log-id 98
            from main
            to snmp
        exit
    exit
1 #------------------------------------------------
echo "Filter Log Configuration"
#------------------------------------------------
    filter
        log 102 create
        exit
    exit
```

检查命令：

Show log log-id 10 **查看本地 LOG**

Show log event-control **查看系统报告数量和开关情况**

1.3. Port 配置

1.3.1 上行端口和互联 PORT 端口配置

根据上行或互联的端口类型和协商方式配置。

1. 根据端口不同，配置相应协议 Ethernet, sonnet-sdh,
2. 根据时钟同步要求，确定是否提取时钟 clock-source node-timed
3. 多链路捆绑，多个端口属性必须一致
4. 多链路捆绑，链路协议需要和对端一致，对端启用 lacp，本地也启用 lacp
5. 多链路捆绑，active 表示主动发链路消息，passive 表示只是被动回应链路消息
   至少有一端必须是 active

例子一：10GE

```
config port 2/1/1
        description "To ZJJXI-MB-CMNET-RT02 ge-1/1/0 10G"
        ethernet
            mtu 1550
        exit
        no shutdown
```

例子二：1GE

```
configure port 1/1/1
        description "To_JH_JH_NE5000E_1ge"
        ethernet
            mtu 1550
            no autonegotiate
        exit
        no shutdown
```

例子三：10G POS

```
configure port 6/1/1
        description "TO-QZ-QZ-NJ-t320-so-2/1/1"
        sonet-sdh
            framing sdh
            clock-source node-timed
            path
                mtu 4472
                scramble
                no shutdown
            exit
        exit
        no shutdown
    exit
```

例子四：2.5G POS

```
 configure port 6/1/1
        description "To_QZ_XDL_R1_T320_1.MAN_so-6/0/1"
        sonet-sdh
            framing sdh
            path
                mtu 4470
                scramble
                report-alarm pais prdi prei
                no shutdown
            exit
        exit
        no shutdown
    exit
```

例子三：多端口捆绑 lag 2*1GE

```
configure port 1/1/1
        description "To ZJJXI-MC-CMNET-RT07-TXYDJF_7750 ge-1/1/1 1G lag1-1"
        ethernet
            mtu 1550
            no autonegotiate
        exit
        no shutdown
configure port 1/1/2
        description "To ZJJXI-MC-CMNET-RT07-TXYDJF_7750 ge-1/1/2 1G lag1-2"
        ethernet
            mtu 1550
            no autonegotiate
        exit
        no shutdown
-----------------------------------------------
configure lag 1
        description "To ZJJXI-MC-CMNET-RT07-TXYDJF_7750 lag1 2G"
        port 1/1/1
        port 1/1/2
        no shutdown
```

1.3.2 下联端口配置

根据下联交换机的端口类型和协商方式灵活配置。

1. 采用 7750 物理端口与下联设备直联就不需要封装 dot1Q，如果有 VLAN 则需要封装 dot1Q 或 qinq 目前移动要求全部采用 QINQ 方式。
2. 端口下配置的用户数据，如需配置 IES、VLL、VPLS、VPRN 等数据就需要设置 mode 为 access。

3. 与下联设备不需要协商需要配置 no autonegotiate。
4. 多链路捆绑，多个端口属性必须一致
5. 多链路捆绑，链路协议需要和对端一致，对端启用 lacp，本地也启用 lacp
6. 多链路捆绑，lactive 表示主动发链路消息，passive 表示只是被动回应链路消息

配置示例：

下联二层路由器: 单端口 QINQ

```
configure port 1/1/4
        description "NanH-S6503"
        ethernet
            mode access
            encap-type qinq
            no autonegotiate
        exit
        no shutdown
    exit
exit all
configure  port 1/1/15
        description "JHWY-xiacheng-OLT"
        ethernet
            mode access
            encap-type qinq
            no autonegotiate
        exit
        no shutdown
    exit
exit all
```

下联二层路由器：多链路捆绑

```
configure port 1/1/3
        description "LAG2-To-GuangDian-LAG-port1"
        ethernet
            mode access
            encap-type qinq
            no autonegotiate
        exit
        no shutdown
exit all
    configure port 1/1/4
        description "LAG2-To-GuangDian-LAG-port2"
        ethernet
            mode access
            encap-type qinq
            no autonegotiate
```

```
        exit
        no shutdown
configure lag 2
        description "To-GuangDian-LAG2"
        mode access
        encap-type qinq
        port 1/1/3
        port 1/1/4
        lacp active administrative-key 32768
        no shutdown
```

检查命令：

Show port　　**查看端口状态是否 UP。**

show lag　　查看 LAG 状态是否 up

```
*A:ZJJXI-MC-CMNET-RT002-XieXi_7750# show port

===============================================================================
Ports on Slot 1
===============================================================================
Port        Admin Link Port    Cfg  Oper LAG/ Port Port Port   SFP/XFP/
Id          State      State   MTU  MTU  Bndl Mode Encp Type   MDIMDX
-------------------------------------------------------------------------------
1/1/1       Up    Yes  Up      1550 1550    1 netw null xcme   GIGE-LX  10KM
1/1/2       Up    Yes  Up      1550 1550    1 netw null xcme   GIGE-LX  10KM
1/1/3       Down  No   Down    9212 9212    - netw null xcme   GIGE-LX  80KM
1/1/4       Down  No   Down    9212 9212    - netw null xcme   GIGE-LX  40KM
1/1/5       Up    Yes  Up      1522 1522    - accs qinq xcme   GIGE-LX  10KM
1/1/6       Up    Yes  Up      1522 1522    - accs qinq xcme   GIGE-LX  40KM
1/1/7       Up    Yes  Up      1522 1522    - accs qinq xcme   GIGE-LX  40KM
1/1/8       Up    No   Down    1522 1522    - accs qinq xcme   GIGE-LX  10KM
1/1/9       Up    Yes  Up      1522 1522    - accs qinq xcme   GIGE-LX  10KM
1/1/10      Up    Yes  Up      1522 1522    3 accs qinq xcme   GIGE-LX  40KM
1/1/11      Up    No   Down    1522 1522    3 accs qinq xcme   GIGE-LX  40KM
1/1/12      Up    Yes  Up      1522 1522    4 accs qinq xcme   GIGE-LX  40KM
1/1/13      Up    No   Down    1522 1522    4 accs qinq xcme   GIGE-LX  40KM
1/1/14      Up    Yes  Up      1522 1522    - accs qinq xcme   GIGE-LX  40KM
1/1/15      Up    Yes  Up      1522 1522    - accs qinq xcme   GIGE-LX  40KM
1/1/16      Up    Yes  Up      1522 1522    - accs qinq xcme   GIGE-LX  10KM
1/1/17      Up    Yes  Up      1522 1522    - accs qinq xcme   GIGE-LX  10KM
1/1/18      Up    Yes  Up      1518 1518    - accs dotq xcme   GIGE-LX  10KM
1/1/19      Up    No   Down    1522 1522    5 accs qinq xcme   GIGE-LX  80KM
```

```
1/1/20      Up    Yes  Up      1522 1522    5 accs qinq xcme   GIGE-LX  10KM

===============================================================================
Ports on Slot 2
===============================================================================
Port        Admin Link Port    Cfg  Oper LAG/ Port Port Port   SFP/XFP/
Id          State      State   MTU  MTU  Bndl Mode Encp Type   MDIMDX
-------------------------------------------------------------------------------
2/1/1       Up    Yes  Up      1550 1550    - netw null xgige  10GBASE-LR  10*

===============================================================================
Ports on Slot A
===============================================================================
Port        Admin Link Port    Cfg  Oper LAG/ Port Port Port   SFP/XFP/
Id          State      State   MTU  MTU  Bndl Mode Encp Type   MDIMDX
-------------------------------------------------------------------------------
A/1         Up    No   Down    1514 1514    - netw null faste

===============================================================================
Ports on Slot B
===============================================================================
Port        Admin Link Port    Cfg  Oper LAG/ Port Port Port   SFP/XFP/
Id          State      State   MTU  MTU  Bndl Mode Encp Type   MDIMDX
-------------------------------------------------------------------------------
B/1         Up    No   Down    1514 1514    - netw null faste
===============================================================================
*A:ZJJXI-MC-CMNET-RT002-XieXi_7750# show lag

===============================================================================
Lag Data
===============================================================================
Lag-id          Adm     Opr     Port-Threshold   Up-Link-Count   MC Act/Stdby
-------------------------------------------------------------------------------
1               up      up      0                2               N/A
2               down    down    0                0               N/A
3               up      up      0                1               N/A
4               up      up      0                1               N/A
5               up      up      0                1               N/A
11              down    down    0                0               N/A
-------------------------------------------------------------------------------
Total Lag-ids: 6        Single Chassis: 6        MC Act: 0       MC Stdby: 0
===============================================================================
*A:ZJJXI-MC-CMNET-RT002-XieXi_7750#
```

IGP 协议配置

1.4.1 OSPF 协议配置

1 设备的唯一标识地址系统默认名字为 system，配置 IP 地址 X.X.X.X 。
2 设备管理地址 loopback 配置 IP 地址 Y.Y.Y.Y
3 配置系统自治号为 64850。
4 打开多链路负载均衡 ECMP 设置为 16。
5 配置设备 router-id 为协议互联地址，必须是 loopback /32 地址，一般使用 system 地址。

配置示例：
a 定义 network 互联接口

```
#------------------------------------------------
echo "IP Configuration"
#------------------------------------------------
        interface "ge-2/1/1"
            address 221.131.199.230/30
            description "To ZJJXI-MB-CMNET-RT02 ge-1/0/1 10G"
            port 2/1/1
        exit
        interface "lag1"
            address 221.131.199.154/30
            description "To ZJJXI-MC-CMNET-RT03-NanHu_7750 lag1 2G"
            port lag-1
        exit
        interface "loopback0"
            address 221.131.199.17/32
            loopback
        exit
        interface "system"
            address 221.131.199.18/32
            local-dhcp-server "pppoe"
        exit
        autonomous-system 64850
        ecmp 8                              //equal cost multi-path
        router-id 221.131.199.18

exit all
```

b 定义 access 互联接口

```
configure service
        ies 10002 customer 10002 create
```

```
            interface "to-gaozhongyuanqu6503"  create
                address 211.140.102.93/30
                sap 1/1/14:18.0 create
                exit
            exit
            no shutdown
        exit
exit all
```

C 在 OSPF 协议加入接口

```
configure router  ospf
            asbr
            reference-bandwidth 40000000
            export "export-direct-to-ospf"
            graceful-restart
            exit
            area 0.0.0.4
                interface "system"
                exit
                interface "lag1"
                    metric 10
                exit
                interface "ge-2/1/1"
                exit
                interface "loopback0"
                exit
                interface "to-gaozhongyuanqu6503"
                exit
            exit
        exit
```

检查命令：

show router ospf interface　　**查看** interface **是否** UP。

show router ecmp　　**查看** ecmp **是否打开。**

show router ospf neighter　　**查看**邻居状态**是否**正常

show router ospf status

show router ospf database　查看 OSPF 路由数据库

-database[type{router|network|summary|asbr-summary|external|nssa|all}]　[area <area-id>] [adv-router <router-id>] [<link-state-id>] [detail]

```
*A:ZJJXI-MC-CMNET-RT002-XieXi_7750>config>service# show router ospf interface

===============================================================================
OSPF Interfaces
===============================================================================
```

```
If Name                 Area Id         Designated Rtr  Bkup Desig Rtr  Adm  Oper
-------------------------------------------------------------------------------
system                  0.0.0.4         221.131.199.17  0.0.0.0         Up   DR
lag1                    0.0.0.4         221.131.199.17  221.131.199.19  Up   DR
ge-2/1/1                0.0.0.4         211.140.0.236   221.131.199.17  Up   BDR
loopback0               0.0.0.4         221.131.199.17  0.0.0.0         Up   DR
to-gaozhongyuanqu6503 0.0.0.4         221.131.199.17  0.0.0.0         Up   DR
-------------------------------------------------------------------------------
No. of OSPF Interfaces: 5
===============================================================================
*A:ZJJXI-MC-CMNET-RT002-XieXi_7750>config>service#

*A:ZJJXI-MC-CMNET-RT002-XieXi_7750# show router ospf neighbor

===============================================================================
OSPF Neighbors
===============================================================================
Interface-Name                   Rtr Id          State      Pri   RetxQ   TTL
-------------------------------------------------------------------------------
lag1                             221.131.199.19  Full       1     0       37
ge-2/1/1                         211.140.0.236   Full       1     0       35
-------------------------------------------------------------------------------
No. of Neighbors: 2
===============================================================================
```

1.4.2 ISIS 协议配置

1. 配置 ISIS 为 leverl-1
2. 配置 area-id 为 86.4661.0573 （ 按照规划配置）
3. 将 system、上联，互联的接口、与下联设备互联接口加入到 ISIS 进程。

配置示例：

```
        isis
            level-capability level-1
            area-id 86.4665.0514
            traffic-engineering
            level 1
                wide-metrics-only
            exit
            interface "system"
                level-capability level-1
            exit
            interface "to_SYL12416-1_1"
                level-capability level-1
                level 1
                    metric 200
                exit
            exit
            interface "to_SYL12416-1_2"
                level-capability level-1
                level 1
                    metric 200
                exit
            exit
            interface "to_DBL12416-1_1"
                level-capability level-1
                level 1
                    metric 200
                exit
            exit
            interface "to_DBL12416-1_2"
                level-capability level-1
                level 1
                    metric 200
                exit
            exit
        exit
```

检查命令：

show router isis adjacency

查看 ISIS **邻接是否建立。**

Mpls、LDP 协议配置

1. 将 system、上联设备的接口，互联设备的接口加入到 MPLS 和 LDP 进程。
2. 按照需要将下联设备的接口加入到 MPLS 和 LDP 进程。

配置示例：

a 配置标签限制策略

```
configure router
        policy-options
            begin
            prefix-list "system1"
                prefix 0.0.0.0/0 prefix-length-range 32-32
            exit
            policy-statement "label-filter"
                entry 10
                    from
                        prefix-list "system1"
                    exit
                    action accept
                    exit
                exit
                entry 20
                    action reject
                exit
            exit
            commit
exit all
```

b 配置 MPLS 接口（router id 地址必须加入 MPLS）

```
configure router
     mpls
            no shutdown
            interface "system"
            exit
            interface "ge-1/1/1"
            exit
            interface "ge-1/1/2"
            exit
      exit
```

c 配置 LDP 接口（引用标签限制策略）

```
      ldp
           export "label-filter"
           interface-parameters
```

```
                interface "ge-1/1/1"
                exit
                interface "ge-1/1/2"
                exit
            exit
            targeted-session
        exit
    exit
exit all
```

检查命令：

show router mpls interface	查看 Mpls 接口是否正常 up
show router ldp session	查看 LDP 邻接是否成功建立 Established 。
show router ldp discovery	查看 LDP 邻接是否成功建立 Establ。
show router ldp binding	查看 LDP 标签发布情况 l。
show router ldp binding prefix x.x.x.x/32	查看 LDP 某个目的地的标签发布情况 。

```
*A:ZJJXI-MC-CMNET-RT002-XieXi_7750# show router mpls interface

===============================================
MPLS Interfaces
===============================================
Interface                          Port-id          Adm    Opr    TE-metric
-------------------------------------------------------------------------------
system                             system           Up     Up     None
  Admin Groups                     None
  Srlg Groups                      None
lag1                               lag-1            Up     Up     None
  Admin Groups                     None
  Srlg Groups                      None
ge-2/1/1                           2/1/1            Up     Up     None
  Admin Groups                     None
  Srlg Groups                      None
-------------------------------------------------------------------------------
Interfaces : 3
===============================================
*A:ZJJXI-MC-CMNET-RT002-XieXi_7750# show router ldp session

===============================================
LDP Sessions
===============================================
Peer LDP Id        Adj Type   State         Msg Sent  Msg Recv  Up Time
```

```
-------------------------------------------------------------------------------
211.138.130.10:0  Link       Established   4340179   4303139   18d 02:08:22
221.131.199.20:0  Link       Established   3049446   1887831   17d 17:09:49
-------------------------------------------------------------------------------
No. of Sessions: 2
===============================================
*A:ZJJXI-MC-CMNET-RT002-XieXi_7750#show router ldp discovery

===============================================
LDP Hello Adjacencies
===============================================
Interface Name                   Local Addr      Peer Addr       AdjType State
-------------------------------------------------------------------------------
lag1                             221.131.199.18  221.131.199.20  Link    Estab
ge-2/1/1                         221.131.199.18  211.138.130.10  Link    Estab
-------------------------------------------------------------------------------
No. of Hello Adjacencies: 2
===============================================
*A:ZJJXI-MC-CMNET-RT002-XieXi_7750#    show    router    ldp    bindings    prefix
221.131.199.40/32

===============================================
LDP LSR ID: 221.131.199.18
===============================================
Legend: U - Label In Use,  N - Label Not In Use, W - Label Withdrawn
    WP - Label Withdraw Pending
===============================================
LDP Prefix Bindings
===============================================
Prefix             Peer               IngLbl    EgrLbl  EgrIntf   EgrNextHop
-------------------------------------------------------------------------------
221.131.199.40/32 211.138.130.10 128578N   1202  2/1/1 221.131.199.229
221.131.199.40/32 221.131.199.20 128578U 128458   --          --
-------------------------------------------------------------------------------
No. of Prefix Bindings: 2
===============================================*A:ZJJXI-MC-CMNET-RT002-XieXi_775
0# show router ldp bindings active prefix  221.131.199.40/32

===============================================
Legend:  (S) - Static (M) - Multi-homed Secondary Support
         (B) - BGP Next Hop
===============================================
LDP Prefix Bindings (Active)
===============================================
```

```
Prefix                Op    IngLbl    EgrLbl    EgrIntf/LspId  EgrNextHop
-------------------------------------------------------------------------------
221.131.199.40/32  Push    --       1202      2/1/1          221.131.199.229
221.131.199.40/32  Swap 128578  1202      2/1/1          221.131.199.229
-------------------------------------------------------------------------------
No. of Prefix Active Bindings: 2
*A:ZJJXI-MC-CMNET-RT002-XieXi_7750#

show router ldp bindings
  - bindings [fec-type <prefixes|services>] [detail | summary] [session
<ip-addr[:label-space]>]
  - bindings [fec-type p2mp] [p2mp-id <identifier> root <ip-address>] [detail | summary]
[session <ip-addr[:label-space]>]
  - bindings <label-type> <start-label> [<end-label>]
  - bindings {prefix <ip-prefix/mask> [detail]}[session <ip-addr[:label-space]>]
  - bindings active [fec-type prefixes] [prefix <ip-prefix/mask>] [egress-nh
<ip-prefix/mask> | egress-if <port-id> | egress-lsp <tunnel-id>] [summary]
  - bindings active [fec-type p2mp] [p2mp-id <identifier> root <ip-address>] [egress-nh
<ip-prefix/mask> | egress-if <port-id> | egress-lsp <tunnel-id>]
    [summary]
  - bindings service-id <service-id> [detail]
  - bindings vc-type <vc-type> [{vc-id <vc-id>|agi <agi>} [session
<ip-addr[:label-space]>]]
  - bindings p2mp-id <identifier> root <ip-address> [detail]

 <fec-type>          : prefixes|services|p2mp - keywords
 <ip-addr[:label-sp*> : ip-addr     - a.b.c.d
                       label-space - [0..65535]
 <ip-prefix/mask>    : ip-prefix a.b.c.d (host bits must be 0)
                       mask      [0..32]
 <vc-type>                                                              :
<ethernet|vlan|mirror|frdlci|atmsdu|atmcell|atmvcc|atmvpc|ipipe|satop-e1|satop-t1|cesop
sn|cesopsn-cas> - keywords
 <vc-id>             : [1..4294967295]
 <service-id>        : [1..2147483648]|<svc-name:64 char max>
 <label-type>        : ingress-label|egress-label - keywords
 <start-label>       : [16..1048575]
 <end-label>         : [17..1048575]
 <active>            : keyword
 <detail>            : keyword
 <agi>                                                                  :
<ip-addr:comm-val>|<2byte-asnumber:ext-comm-val>|<4byte-asnumber:comm-val>
                       ip-addr        - a.b.c.d
                       comm-val       - [0..65535]
```

```
                    2byte-asnumber - [1..65535]
                    ext-comm-val   - [0..4294967295]
                    4byte-asnumber - [1..4294967295]
<identifier>        : [0..4294967295]
<ip-address>        : a.b.c.d
<tunnel-id>         : [0..4294967295]
<port-id>           : slot[/mda[/port]] or
                      slot/mda/port[.channel]
                      aps-id         - aps-<group-id>[.channel]
                        aps            - keyword
                        group-id       - [1..64]
                      ccag-id        - slot/mda/<path-id>[cc-type]
                        path-id        - [a|b]
                        cc-type        - [.sap-net|.net-sap]
```

设备安全配置（security）

1.6.1 设备访问安全

1. 开启 telnet、snmp 服务。并对访问 IP 进行限制。
2. 全网 7750SR 设备关闭 FTP，SSH 服务。
3. 配置 IPV6-filter。对每台 7750SR 的普通上网用户和每个 VPRN 用户都要进行 IPV6 包的过滤。

配置示例：

```
configure  system  security
      telnet-server
      no ftp-server
      management-access-filter
        ip-filter
          default-action permit
            entry  1
              description "for ssh,entry 001-100"
              src-ip 61.175.255.39/32
              dst-port 22 65535
              action permit
            exit
            entry   2
              src-ip 218.75.102.96/27
              dst-port 22 65535
              action permit
            exit
            entry 100
              description "for ssh security,reject other ip"
              dst-port 22 65535
              action deny
            exit
            entry 101
              description "for telnet,entry 101-200"
              src-ip 61.175.255.39/32
              dst-port 23 65535
              action permit
            exit
            entry 102
              src-ip 218.75.102.96/27
              dst-port 23 65535
```

```
            action permit
          exit
          entry 200
            description "for telnet security,reject other ip"
            dst-port 23 65535
            action deny
          exit
          entry 201
            description "for snmp security,entry 201-300"
            src-ip 202.96.102.0/23
            dst-port 161 65535
            action permit
          exit
          entry 202
            src-ip 220.188.118.240/28
            dst-port 161 65535
            action permit
          exit
          entry 300
            description "for snmp security,reject other ip"
            dst-port 161 65535
            action deny
          exit
        exit
      exit
      password
        authentication-order tacplus local  exit-on-reject
        attempts 3 time 5 lockout 0
      exit
      tacplus
        accounting
        authorization
          server 1 address 202.96.102.141 secret "cOU/mpLwwCO3lOPC3MHySE" hash2
          server 2 address 61.153.176.183 secret "WZBK9MwJl5FLJURrtaiD6." hash2
      exit
      source-address xxx.xxx.xxx.xxx  //default system address if not define
  exit all
```

注：exit-on-reject --提供AAA认证取TACPLUS内容,如果加了EXIT-ONF-REJECT，则3A服务器上没有这个用户名密码的话，则本地帐号也无法登陆

本地用户权限管理：

1 系统默认账号

```
user "admin"
    password "VeuGBy9agmYtpDhhWOyi359H.JvK5.8c" hash2
    access console ftp snmp
console
        member "administrative"
    exit
exit
```

1. 创建一个新权限，并且应用（注：对本地用户有效，AAA 认证由服务器控制）

例子 a：开放全部权限并应用与用户账号

```
profile "zcuc"
    default-action permit-all
exit
user "zcuc"
  password "f9GWVwczO8n3aMW6R1aHek" hash2
  access console ftp snmp
  console
    member "default"
    member "zcuc"
  exit
exit
```

例子 b： 有限制的权限并且应用于用户账号

```
profile "showonly"
     default-action permit-all
     entry 10
         match "configure"
         action deny
     exit
     entry 20
         match "admin"
         action deny
     exit
     entry 30
         match "debug"
         action deny
     exit
     entry 40
         match "tools"
         action deny
     exit
     entry 50
         match "clear"
         action deny
```

```
            exit
            entry 60
                match "file"
                action deny
            exit
            entry 70
                match "bof"
                action deny
            exit
        exit
    user "hzjk"
    password "Pa6ZqXTlv59OutAHE1WjJ." hash2
      access console ftp
        console
          no member "default"
          member "showonly"
        exit
    exit
```

1.6.2 主 CPU 保护

系统硬件保护 （注：复制添加注意首先关闭 ip-filter,修改完成后再打开）

```
configure system security
             per-peer-queuing
             cpm-queue
                queue 40 create
                    cbs 1000
                    mbs 1000
                    rate 3000 cir 2000
                exit
                queue 50 create
                    cbs 1000
                    mbs 1000
                    rate 2000 cir 2000
                exit
            exit
exit all

#------------------------------------------------
echo "System Security Cpm Hw Filters Configuration"
#------------------------------------------------
configure system security cpm-filter ip-filter
        shutdown
                    entry 10 create
                        action queue 40
                        match protocol tcp
                            tcp-syn true
                        exit
                    exit
                    entry 20 create
                        action queue 40
                        match protocol icmp
                        exit
                    exit
                    entry 50 create
                        action queue 50
                        match protocol tcp
                            src-ip 10.0.0.0/8
                            tcp-syn true
                        exit
                    exit
```

```
                entry 51 create
                    action queue 50
                    match protocol tcp
                        src-ip 172.16.0.0/12
                        tcp-syn true
                    exit
                exit
                entry 52 create
                    action queue 50
                    match protocol tcp
                        src-ip 192.168.0.0/16
                        tcp-syn true
                    exit
                exit
```

#以下是限制端口设置

```
            entry 101 create
              action drop
              match protocol udp
                 dst-port 69 65535
              exit
            exit
            entry 102 create
              action drop
              match protocol udp
                dst-port 135 65535
              exit
             exit
            entry 103 create
               action drop
               match protocol tcp
                  dst-port 135 65535
               exit
            exit
            entry 104 create
                 action drop
                 match protocol
                   dst-port 137 65535
                 exit
            exit
            entry 105 create
                   action drop
                   match protocol udp
                     dst-port 138 65535
                 exit
```

```
exit
entry 106 create
     action drop
     match protocol tcp
            dst-port 138 65535
            exit
 exit
 entry 107 create
            action drop
            match protocol udp
                dst-port 139 65535
            exit
 exit
 entry 108 create
            action drop
            match protocol tcp
                dst-port 139 65535
            exit
  exit
  entry 109 create
            action drop
            match protocol udp
                dst-port 445 65535
            exit
   exit
   entry 110 create
            action drop
            match protocol tcp
                dst-port 445 65535
            exit
   exit
   entry 111 create
            action drop
            match protocol udp
                dst-port 539 65535
            exit
    exit
    entry 112 create
            action drop
            match protocol tcp
                dst-port 539 65535
            exit
    exit
    entry 113 create
```

```
        action drop
        match protocol udp
            dst-port 593 65535
        exit
    exit
    entry 114 create
        action drop
        match protocol tcp
            dst-port 593 65535
        exit
    exit
    entry 115 create
        action drop
        match protocol tcp
            dst-port 1068 65535
        exit
    exit
    entry 116 create
        action drop
        match protocol udp
            dst-port 1433 65535
        exit
    exit
    entry 117 create
        action drop
        match protocol udp
            dst-port 1434 65535
        exit
    exit
    entry 118 create
        action drop
        match protocol tcp
            dst-port 1871 65535
        exit
    exit
    entry 119 create
        action drop
        match protocol tcp
            dst-port 3208 65535
        exit
    exit
    entry 120 create
        action drop
        match protocol tcp
```

```
            dst-port 3333 65535
        exit
    exit
    entry 121 create
        action drop
        match protocol tcp
            dst-port 4331 65535
        exit
    exit
    entry 122 create
        action drop
        match protocol udp
            dst-port 4334 65535
        exit
    exit
    entry 123 create
        action drop
        match protocol udp
            dst-port 4444 65535
        exit
    exit
    entry 124 create
        action drop
        match protocol tcp
            dst-port 4444 65535
        exit
    exit
    entry 125 create
        action drop
        match protocol tcp
            dst-port 4510 65535
        exit
    exit
    entry 126 create
        action drop
        match protocol tcp
            dst-port 4557 65535
        exit
    exit
    entry 127 create
        action drop
        match protocol tcp
            dst-port 5554 65535
        exit
```

```
                exit
                entry 128 create
                    action drop
                    match protocol tcp
                        dst-port 5800 65535
                    exit
                exit
                entry 129 create
                    action drop
                    match protocol tcp
                        dst-port 5900 65535
                    exit
                exit
                entry 130 create
                    action drop
                    match protocol tcp
                        dst-port 9995 65535
                    exit
                exit
                entry 131 create
                    action drop
                    match protocol tcp
                        dst-port 9996 65535
                    exit
                exit
                entry 132 create
                    action drop
                    match protocol tcp
                        dst-port 10080 65535
                    exit
                exit
                no shutdown    ←必须开启才起作用
            exit
        exit
    exit
exit
    cpu-protection
        policy 1 create
        exit
        policy 2 create
            overall-rate max
        exit
        port-overall-rate max
    exit
```

```
            ipv6-filter
                entry 10 create
                    log 110
                    match
                        router Base
                    exit
                exit
                entry 20 create
                    match
                        router ***(VPRN Service ID)
                    exit
                exit
                no shutdown
            exit
        exit
```

检查命令：

```
Show system security cpm-filter ip-filter
show system security cpm-filter ipv6-filter
```

查看 IPV6 包的数量。

注意：default-action permit 必须首先配置