

Switch-community

-
-
-
-
-
- ESR
- EMS
- Switch Community ESR
-

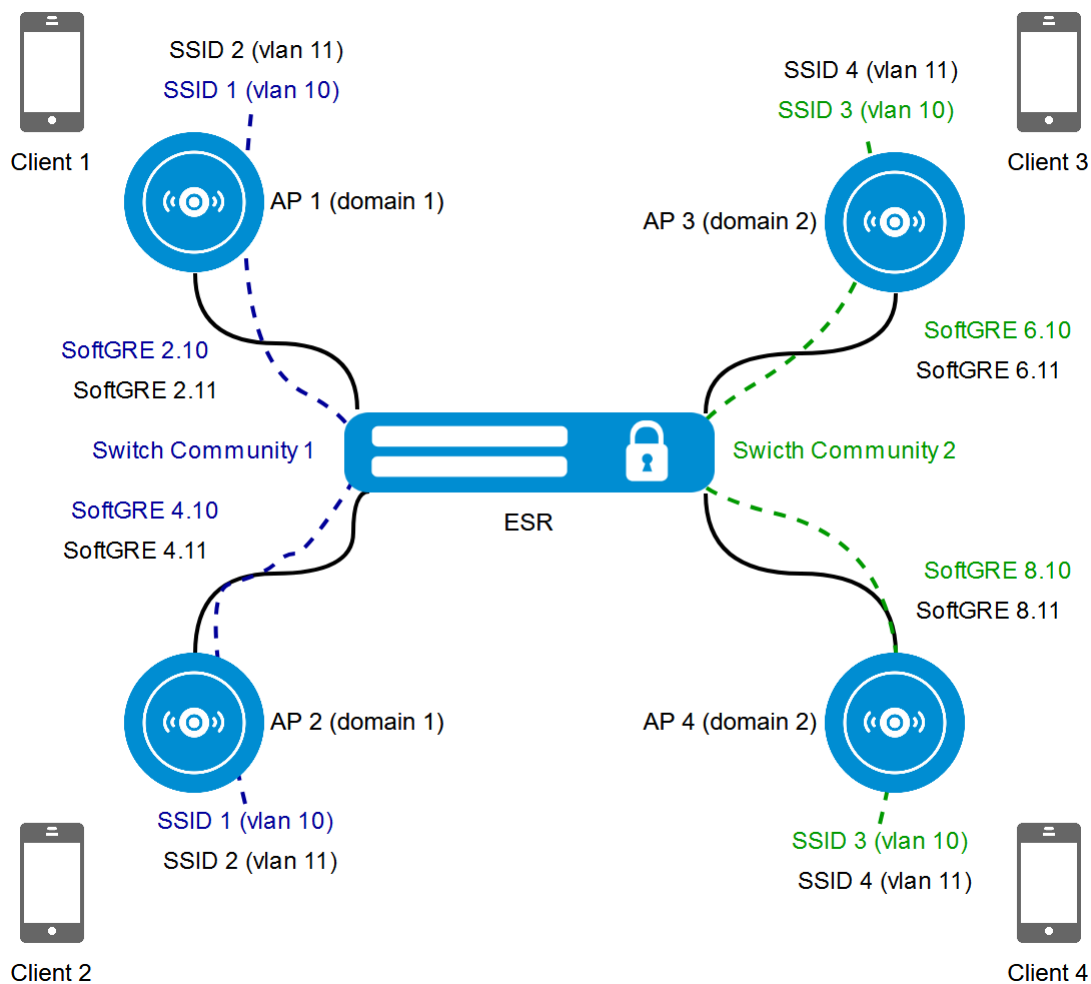
- :

- , SSID-ENTERPRISE, , SSID-PRINT;
- , .
- ESR .

ESR 1.11.0, SoftWLC 1.16. , .

L3 (softGRE) - PCRF.

Swicth Community (SC) - PCRF ESR, - .



. 1.

. 1. SC. SC - 4- , :

- 1) SC 1 (Switch Community 1) - SoftGRE 2.10 SoftGRE 4.10, AP 1 AP 2, domain 1.
- 2) SC 2 (Switch Community 2) - SoftGRE 6.10 SoftGRE 8.10, AP 3 AP 4, domain 2.

:

- 1) Client 1 Client 2 SSID 1 SC 1.
- 2) Client 3 Client 4 SSID 3 SC 2.
- 3) Client 1 2 c Client 3 .
- 4) SSID 2 4 SC , SSID , .

1. L3 (SoftGRE) - PCRF.
2. SC .
3. SC ESR, , ESR SC .
4. SSID , .
5. SC office-domain, vlan location. SC SSID , EMS, SSID, "bridge location" "vlan".
6. SSID , SSID () " " (" ",).
7. SSID, , , "Global isolation". SSID , ESR.
8. SC OTT.

ESR

ESR L3, - PCRF. ESR L3 (WiFi L3) ESR wireless-controller " ".

(-) "protected-ports radius" .

```
bridge 10
  location data10
  protected-ports radius
exit

bridge 11
  location data10
  protected-ports radius
exit
```

! "protected-ports radius" "location"!

ESR, EoGRE (ESR-1200/1500/1700) internal-usage-vlan (IUV). EoGRE vlan SC. vlan ESR, vlan, . - EoGRE 8000, 2 - SC ,
- 2000 SC. vlan "wireless-controller" "internal-usage-vlan", vlan, SC.



```
wireless-controller
  internal-usage-vlan 1001-2037,2500-3000,3200-3700
exit
```

! SC ESR-1200/1500/1700, EoGRE, internal-usage-vlan SC. internal-usage-vlan SC !

! ESR 1.11.0 "protected-ports":
"protected-ports local" - protected-ports, .
"protected-ports radius" - , SC, CoA, PCRF . - - .

EMS

SC (/) SSID - . SSID: "Wireless" " SSID" " SSID" (. 2):

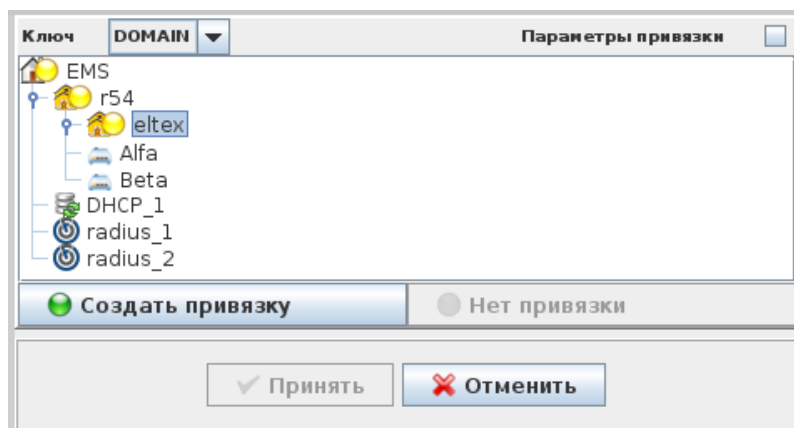
Тип	Hotspot
Имя	i-10
Описание	
Domain	eltex.r54.root
Статус SSID	Operational
Дата создания	2021-04-29 11:10:06
Дата изменения	2021-04-29 11:10:06
----- Параметры окружения -----	
Bridge Location	data10
VRF	1
Switch Community	<input checked="" type="checkbox"/>
Требовать наличие Opt82	<input type="checkbox"/>
DPI (Step Logic)	<input type="checkbox"/>
----- Опции -----	
Статус VAP	Up
Режим трафика VAP (только для GRE)	Tunnel
Broadcast SSID	<input checked="" type="checkbox"/>
Radio	All
Режим безопасности	Без шифрования
MAC Auth Type	Disable
Статус Client QoS	on
VLAN-ID	<input checked="" type="checkbox"/> 10
QoS method (down link)	802.1p
VLAN trunk	<input type="checkbox"/>
General Mode	<input type="checkbox"/>
General VLAN-ID	1
802.1p priority (up link)	0
Изоляция клиентов	<input type="checkbox"/>
Band steer	<input checked="" type="checkbox"/>
Support 802.11k	<input type="checkbox"/>
Wireless Multicast Forwarding	<input type="checkbox"/>
Hotspot 2.0	
DiffServ Policy Up	
<div>   </div>	

. 2.

"Bridge, Location" , ESR, -. "VLAN-ID". "Switch Community" SSID "".

, "" SSID, , .

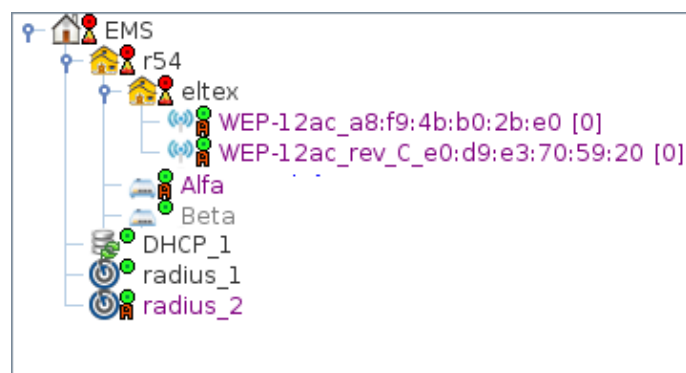
SSID " SSID " (. 3):



. 3.

, SSID, "DOMAIN" " ".

(. 3.):



. 4.

, SC SSID i-10.



!

SSID - SC. , SC.

SSID, "VLAN-ID" "Bridge, Location" SC - SSID SC SC SSID.

, ESR, - , , - SC CoA, PCRF:

1. Domain - "office:name=Eltex.r54.root"
2. VLAN-ID - - "vlan:id=10"
3. Bridge, Location - - "name=data10"
4. SC - "sc=1"

- SC ("sc=1").

"sc" CoA - SC.

, , SC SSID - "VLAN-ID", "Bridge, Location" "Switch Community", , SSID .

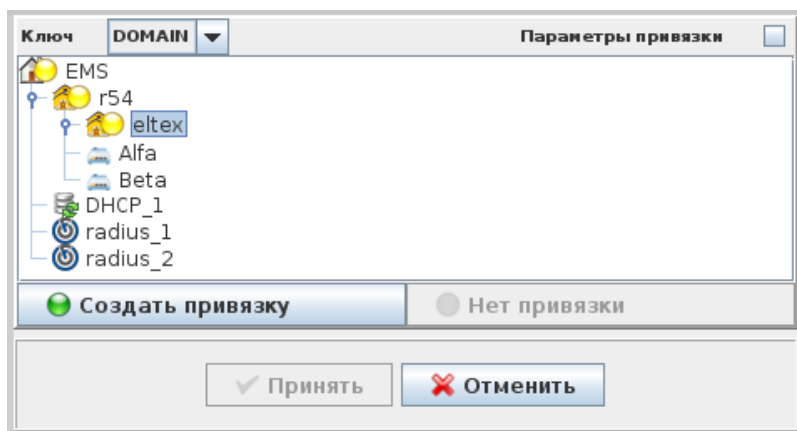
Тип	Hotspot
Имя	i-10-print
Описание	
Domain	eltex.r54.root
Статус SSID	Operational
Дата создания	2021-04-29 11:31:24
Дата изменения	2021-04-29 11:31:24
----- Параметры окружения -----	
Bridge Location	data10
VRF	1
Switch Community	<input checked="" type="checkbox"/>
Требовать наличие Opt82	<input type="checkbox"/>
DPI (Step Logic)	<input type="checkbox"/>
----- Опции -----	
Статус VAP	Up
Режим трафика VAP (только для GRE)	Tunnel
Broadcast SSID	<input checked="" type="checkbox"/>
Radio	All
Режим безопасности	WPA Personal
Поддержка WPA-TKIP	<input checked="" type="checkbox"/>
Поддержка WPA2-AES	<input checked="" type="checkbox"/>
Enable pre-authentication	<input type="checkbox"/>
Ключ (WPA)	12345678
MAC Auth Type	Disable
Broadcast Key Refresh Rate	0
Статус Client QoS	on
VLAN-ID	<input checked="" type="checkbox"/> 10
QoS method (down link)	802.1p
VLAN trunk	<input type="checkbox"/>
General Mode	<input type="checkbox"/>
General VLAN-ID	1
802.1p priority (up link)	0
Изоляция клиентов	<input type="checkbox"/>

✔ Принять
✖ Отменить

. 5.

SSID "i-10-print" (. 3) "VLAN-ID", "Bridge, Location" "Switch Community" SSID "i-10-ent", "WPA Personal".

, SSID "i-10-ent" (. 6).

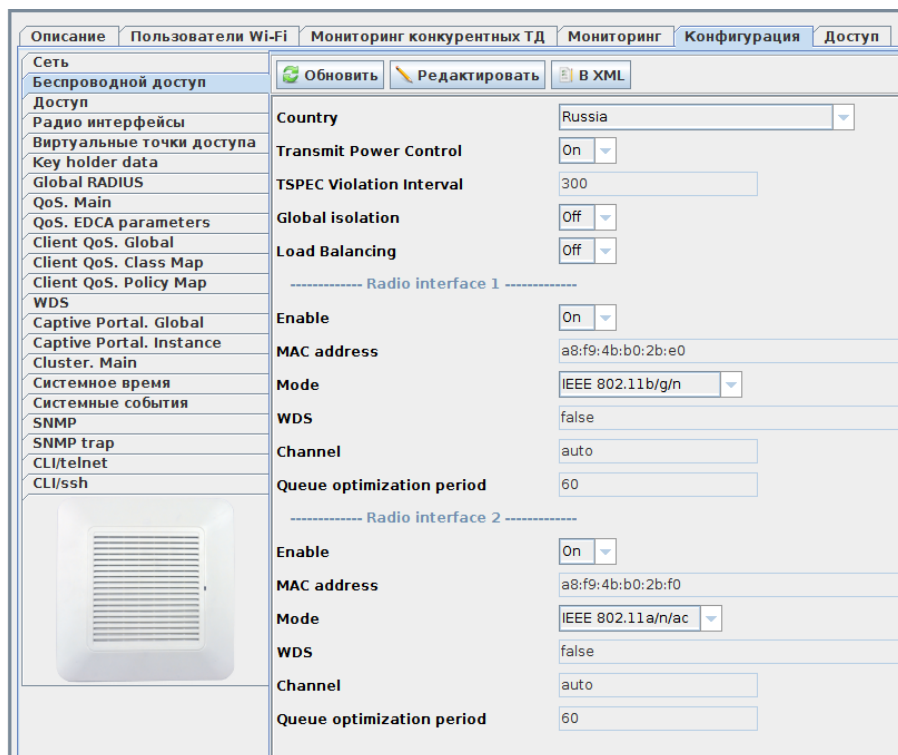


. 6.

- SSID "i-10-ent" "i-10-print" SC. , vlan- ESR - SSID.

.. SSID - SSID , SC . , " " "Global isolation" "off"

/ SC SSID / "Switch Community" SSID. , , SSID CoA "domain-update" ESR (. 7).



. 7.

SSID , , SSID. SSID, vlan . SSID, vlan .

Switch Community ESR

1. SC ESR "show interfaces bridge switch-communities":

```

esr1000# show interfaces bridge switch-communities
bridge 10
Location                               Community
Interfaces                             -----
-----
data10                                Eltex.r54.root                softgre 2.10, softgre 4.10,
softgre 6.10,                               softgre
8.10
data10                                Eltex.r54.root                softgre 2.310, softgre 4.310,
softgre                                     6.310, softgre
8.310

bridge 11
Location                               Community
Interfaces                             -----
-----
data11                                Eltex.r54.root                softgre 2.311, softgre 4.311,
softgre                                     6.311, softgre 8.311

```

, SC, . "Location" location;"Community" - , , SC, "Interfaces" -, SC.

2. SC, , "show interfaces bridge switch-communities <>":

```

esr1000# show interfaces bridge switch-communities 11
bridge 11
Location                               Community
Interfaces                             -----
-----
data11                                Eltex.r54.root                softgre 2.311, softgre 4.311,
softgre                                     6.311, softgre 8.311

```

3. SC, "show interfaces bridge switch-communities community < , , SC>":

5. SC "show interfaces bridge switch-communities summary":

```
esr1000# show interfaces bridge switch-communities summary
Bridges      Communities
-----
bridge 10    2
bridge 11    1
```

6. .3,4 5 :

```
esr1000# show interfaces bridge switch-communities community Eltex.Novosibirsk.Novosibirskaya_oblast.
MRF_Sibir.Local.AllClients.root 11
bridge 11
Location      Community
Interfaces
-----
data11        Eltex.r54.root        softgre 2.311, softgre 4.311,
softgre                               6.311, softgre 8.311

esr1000# show interfaces bridge switch-communities
bridge 10
Location      Community
Interfaces
-----
data10        Eltex.r54.root        softgre 2.10, softgre 4.10,
softgre 6.10,                               softgre
8.10

data10        Eltex.r54.root        softgre 2.310, softgre 4.310,
softgre                               6.310, softgre
8.310

esr1000# show interfaces bridge switch-communities summary 10
Bridges      Communities
-----
bridge 10    2
```

SC ESR-1200/1500/1700, EoGRE , SC IUUV:

```

esr1200# show int bridge interfaces switch-communities
  bridge 10
Location          Community          IUUV
Interfaces
-----
data10            Eltex.r54.root            1008  softgre 4.10, softgre 6.10,
softgre 10.10,                                     softgre
12.10
data10            Eltex.r54.root            1006  softgre 4.310, softgre 6.310,
softgre                                     10.310, softgre
12.310

  bridge 11
Location          Community          IUUV
Interfaces
-----
data11            Eltex.r54.root            1007  softgre 4.311, softgre 6.311,
softgre                                     10.311, softgre
12.311

```

ESR (ESR-1200, VRRP):

```

#!/usr/bin/clish
#18
hostname ALfa

ip firewall sessions allow-unknown
object-group service telnet
  port-range 23
exit
object-group service ssh
  port-range 22
exit
object-group service dhcp_server
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service ntp
  port-range 123
exit
object-group service snmp
  port-range 161-162
exit
object-group service COA
  port-range 3799
  port-range 31812-31813
exit
object-group service bgp
  port-range 179
exit
object-group service dns
  port-range 53
exit
object-group service aptd
  port-range 1337

```

```
exit
object-group service firewall_failover
  port-range 3333
exit

object-group network SoftWLC
  ip prefix 100.123.0.0/24
exit
object-group network gre_termination
  ip prefix 192.168.200.48/28
exit
object-group network mgmt_AP
  ip prefix 198.18.128.0/21
  ip prefix 198.18.136.0/22
  ip prefix 198.18.140.0/22
  ip prefix 100.64.0.56/30
exit
object-group network clients_AP
  ip prefix 198.18.136.0/22
  ip prefix 198.18.140.0/22
exit
object-group network Admnet
  ip prefix 100.123.0.0/24
  ip prefix 100.110.0.0/23
  ip prefix 192.168.200.48/28
  ip prefix 100.64.0.40/30
exit
object-group network nets
  ip prefix 10.0.0.0/8
  ip prefix 192.168.0.0/16
  ip prefix 172.16.0.0/12
exit
object-group network cross
  ip prefix 100.64.0.32/30
  ip prefix 100.64.0.40/30
  ip prefix 100.64.0.48/30
  ip prefix 100.64.0.56/30
exit
object-group network DNS
  ip prefix 100.123.0.0/24
exit
object-group network CoA_servers
  ip prefix 100.123.0.0/24
exit

aaa authentication login default radius local
radius-server timeout 10
radius-server retransmit 5
radius-server host 100.123.0.2
  key ascii-text testing123
  timeout 11
  priority 20
  source-address 198.18.128.2
  auth-port 31812
  acct-port 31813
  retransmit 10
  dead-interval 10
exit
aaa radius-profile PCRF
  radius-server host 100.123.0.2
exit
das-server COA
  key ascii-text testing123
  port 3799
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit

vlan 3
```

```
    force-up
exit
vlan 10
    force-up
exit
vlan 11
    force-up
exit
vlan 101
    force-up
exit
vlan 9
exit

security zone trusted
exit
security zone untrusted
exit
security zone gre
exit
security zone neighbour
exit
security zone user
exit
route-map out_BGP_GRE
    rule 10
        match ip address object-group gre_termination
        action permit
    exit
exit
route-map out_BGP_AP
    rule 10
        match ip address object-group mgmt_AP
        action permit
    exit
exit
route-map out_BGP_NAT
    rule 10
        match ip address object-group clients_AP
        action permit
    exit
exit
route-map in_PREF
    rule 10
        action permit
    exit
exit
router bgp 64603
    neighbor 100.64.0.33
        remote-as 65001
        update-source 100.64.0.34
        address-family ipv4 unicast
            route-map out_BGP_GRE out
            enable
        exit
    enable
exit
neighbor 100.64.0.41
    remote-as 65001
    update-source 100.64.0.42
    address-family ipv4 unicast
        route-map out_BGP_AP out
        enable
    exit
    enable
exit
neighbor 100.64.0.49
    remote-as 65001
    update-source 100.64.0.50
    address-family ipv4 unicast
        route-map out_BGP_NAT out
```

```

        enable
    exit
    enable
exit
neighbor 100.64.0.58
    remote-as 64603
    update-source 100.64.0.57
    address-family ipv4 unicast
        route-map in_PREF in
        next-hop-self
        enable
    exit
    enable
exit
address-family ipv4 unicast
    redistribute connected
    redistribute static
exit
enable
exit

snmp-server
snmp-server system-shutdown
snmp-server community "public11" ro
snmp-server community "private1" rw

snmp-server host 100.123.0.2
exit

snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment pwrin
snmp-server enable traps environment pwrin-insert
snmp-server enable traps environment fan
snmp-server enable traps environment fan-speed-changed
snmp-server enable traps environment fan-speed-high
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps environment board-overheat-temp
snmp-server enable traps environment board-supercooling-temp
snmp-server enable traps environment sfp-overheat-temp
snmp-server enable traps environment sfp-supercooling-temp
snmp-server enable traps environment switch-overheat-temp
snmp-server enable traps environment switch-supercooling-temp
snmp-server enable traps wifi
snmp-server enable traps wifi wifi-tunnels-number-in-bridge-high
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps bras
snmp-server enable traps bras sessions-number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood

```

```
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
snmp-server enable traps screen syn-frag
snmp-server enable traps screen unknown-proto
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon fan
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon supply
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog
```

```
bridge 1
    description "GRE_termination"
    vlan 101
    security-zone gre
    ip address 192.168.200.51/28
    vrrp id 1
    vrrp ip 192.168.200.49/32
    vrrp ip 192.168.200.50/32 secondary
    vrrp priority 200
    vrrp group 1
    vrrp preempt disable
    vrrp preempt delay 150
    vrrp timers garp delay 1
    vrrp timers garp repeat 10
    vrrp
    ipv6 enable
    protected-ports local
    protected-ports exclude vlan
    ports vrrp filtering enable
    ports vrrp filtering exclude vlan
    enable
```

exit

```
bridge 3
    description "mgmt_AP"
    vlan 3
    security-zone trusted
    ip address 198.18.128.2/21
    ip helper-address 100.123.0.2
    ip helper-address vrrp-group 1
    vrrp id 3
    vrrp ip 198.18.128.1/32
    vrrp priority 200
```

```
vrrp group 1
vrrp preempt disable
vrrp preempt delay 150
vrrp timers garp delay 1
vrrp timers garp repeat 10
vrrp
ip tcp adjust-mss 1458
protected-ports local
protected-ports exclude vlan
ports vrrp filtering enable
ports vrrp filtering exclude vlan
enable
exit
bridge 9
description "neighbour"
vlan 9
security-zone neighbour
ip address 100.64.0.57/30
enable
exit
bridge 10
description "data1_AP"
vlan 10
security-zone user
ip address 198.18.136.2/22
ip helper-address 100.123.0.2
ip helper-address vrrp-group 1
vrrp id 10
vrrp ip 198.18.136.1/32
vrrp priority 200
vrrp group 1
vrrp preempt disable
vrrp preempt delay 150
vrrp timers garp delay 1
vrrp timers garp repeat 10
vrrp
ip tcp adjust-mss 1458
location data10
protected-ports radius
protected-ports exclude vlan
enable
exit
bridge 11
description "data2_AP"
vlan 11
security-zone user
ip address 198.18.140.2/22
ip helper-address 100.123.0.2
ip helper-address vrrp-group 1
vrrp id 11
vrrp ip 198.18.140.1/32
vrrp priority 200
vrrp group 1
vrrp preempt disable
vrrp preempt delay 150
vrrp timers garp delay 1
vrrp timers garp repeat 10
vrrp
ip tcp adjust-mss 1458
location data11
protected-ports radius
protected-ports exclude vlan
ports vrrp filtering enable
ports vrrp filtering exclude vlan
enable
exit

interface gigabitethernet 1/0/1
description "UpLink"
mode hybrid
exit
```



```
interface gigabitethernet 1/0/1.206
  description "VRF_AP"
  security-zone gre
  ip firewall disable
  ip netflow export
  ip address 100.64.0.34/30
  ipv6 enable
exit
interface gigabitethernet 1/0/1.208
  description "VRF_CORE"
  security-zone trusted
  ip address 100.64.0.42/30
  ipv6 enable
exit
interface gigabitethernet 1/0/1.210
  description "VRF_NAT"
  security-zone untrusted
  ip address 100.64.0.50/30
  ipv6 enable
exit
interface gigabitethernet 1/0/2
  description "neighbour"
  mode hybrid
  switchport forbidden default-vlan
  switchport general acceptable-frame-type tagged-only
  switchport general allowed vlan add 3,9-11,101 tagged
exit
tunnel softgre 1
  description "mgmt"
  mode management
  local address 192.168.200.49
  default-profile
  enable
exit
tunnel softgre 1.1
  bridge-group 3
  enable
exit
tunnel softgre 2
  description "data"
  mode data
  local address 192.168.200.50
  default-profile
  enable
exit

security zone-pair gre self
  rule 1
    action permit
    match protocol gre
    enable
  exit
  rule 2
    action permit
    match protocol vrrp
    enable
  exit
  rule 3
    action permit
    match protocol tcp
    match destination-port aptd
    enable
  exit
  rule 4
    action permit
    match protocol icmp
    enable
  exit
  rule 10
    action permit
    match protocol tcp
```

```
        match source-address cross
        match source-port bgp
        match destination-port bgp
        enable
    exit
exit
security zone-pair trusted self
    rule 1
        action permit
        match protocol vrrp
        enable
    exit
    rule 2
        action permit
        match protocol udp
        match source-port dhcp_server
        match destination-port dhcp_server
        enable
    exit
    rule 3
        action permit
        match protocol udp
        match source-port dhcp_client
        match destination-port dhcp_server
        enable
    exit
    rule 4
        action permit
        match protocol icmp
        enable
    exit
    rule 10
        action permit
        match source-address SoftWLC
        enable
    exit
    rule 11
        action permit
        match source-address Admnet
        enable
    exit
    rule 20
        action permit
        match protocol tcp
        match source-address cross
        match source-port bgp
        match destination-port bgp
        enable
    exit
exit
security zone-pair trusted trusted
    rule 1
        action permit
        enable
    exit
exit
security zone-pair user untrusted
    rule 1
        action permit
        enable
    exit
exit
security zone-pair user self
    rule 1
        action permit
        match protocol icmp
        enable
    exit
    rule 2
        action permit
        match protocol udp
```

```
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
exit
rule 4
    action permit
    match protocol vrrp
    enable
exit
rule 5
    action permit
    match protocol udp
    match source-port dhcp_server
    match destination-port dhcp_server
    enable
exit
exit
security zone-pair user trusted
    rule 1
        action permit
        match protocol udp
        match source-port dhcp_client
        match destination-port dhcp_server
        enable
    exit
    rule 2
        action permit
        match protocol udp
        match destination-address DNS
        match destination-port dns
        enable
    exit
exit
security zone-pair trusted user
    rule 1
        action permit
        match protocol udp
        match source-port dhcp_server
        match destination-port dhcp_client
        enable
    exit
    rule 2
        action permit
        match protocol udp
        match source-port dhcp_server
        match destination-port dhcp_server
        enable
    exit
    rule 3
        action permit
        match protocol icmp
        enable
    exit
exit
security zone-pair trusted untrusted
    rule 1
        action permit
        enable
    exit
exit
security zone-pair gre gre
    rule 1
        action permit
        enable
    exit
exit
security zone-pair neighbour self
    rule 2
        action permit
        match protocol tcp
        match destination-port bgp
```

```
    enable
exit
rule 3
    action permit
    match protocol udp
    match destination-port firewall_failover
    enable
exit
rule 4
    action permit
    match protocol udp
    match source-port dhcp_server
exit
rule 10
    action permit
    match protocol gre
    enable
exit
rule 20
    action permit
    match protocol icmp
    enable
exit
rule 30
    action permit
    match protocol vrrp
    enable
exit
rule 40
    action permit
    match protocol udp
    match source-port dhcp_server
    match destination-port dhcp_server
    enable
exit
rule 50
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
exit
rule 60
    action permit
    match source-address SoftWLC
    enable
exit
rule 80
    action permit
    match source-address Admnet
    enable
exit
rule 90
    action permit
    match protocol tcp
    match destination-port aptd
    enable
exit
rule 100
    action permit
    match protocol tcp
    match destination-port telnet
    enable
exit
exit
security zone-pair neighbour trusted
    rule 10
        action permit
        enable
    exit
exit
```

```
security zone-pair neighbour untrusted
    rule 10
        action permit
        enable
    exit
exit
security zone-pair neighbour gre
    rule 10
        action permit
        enable
    exit
exit
security zone-pair neighbour user
    rule 10
        action permit
        match protocol udp
        match source-port dhcp_server
        match destination-port dhcp_client
        enable
    exit
exit
security zone-pair trusted neighbour
    rule 10
        action permit
        enable
    exit
exit
security zone-pair gre neighbour
    rule 10
        action permit
        enable
    exit
exit
security zone-pair user neighbour
    rule 10
        action permit
        match protocol udp
        match destination-port dns
        enable
    exit
    rule 20
        action permit
        match not source-address nets
        enable
    exit
exit
security zone-pair untrusted self
    rule 10
        action permit
        match protocol tcp
        match source-address cross
        match source-port bgp
        match destination-port bgp
        enable
    exit
exit

security passwords history 0
ip firewall failover sync-type unicast
ip firewall failover source-address 100.64.0.57
ip firewall failover destination-address 100.64.0.58
ip firewall failover port 3333
ip firewall failover vrrp-group 1
ip firewall failover

ip dhcp-relay

wireless-controller
    peer-address 100.64.0.58
    nas-ip-address 198.18.128.2
```

```
data-tunnel configuration radius
keepalive mode reactive
aaa das-profile COA
aaa radius-profile PCRF
internal-usage-vlan 1001-2037,2500-3000,3200-3700
enable
exit
ip telnet server
ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.123.0.2
exit
```

```
#!/usr/bin/clish
#18
hostname Beta

ip firewall sessions allow-unknown
object-group service telnet
    port-range 23
exit
object-group service ssh
    port-range 22
exit
object-group service dhcp_server
    port-range 67
exit
object-group service dhcp_client
    port-range 68
exit
object-group service ntp
    port-range 123
exit
object-group service snmp
    port-range 161-162
exit
object-group service COA
    port-range 3799
    port-range 31812-31813
exit
object-group service bgp
    port-range 179
exit
object-group service dns
    port-range 53
exit
object-group service aptd
    port-range 1337
exit
object-group service firewall_failover
    port-range 3333
exit

object-group network SoftWLC
    ip prefix 100.123.0.0/24
exit
object-group network gre_termination
    ip prefix 192.168.200.48/28
exit
object-group network mgmt_AP
    ip prefix 198.18.128.0/21
    ip prefix 198.18.136.0/22
    ip prefix 198.18.140.0/22
    ip prefix 100.64.0.56/30
exit
```

```
object-group network clients_AP
  ip prefix 198.18.136.0/22
  ip prefix 198.18.140.0/22
exit
object-group network Admnet
  ip prefix 100.123.0.0/24
  ip prefix 100.110.0.0/23
  ip prefix 192.168.200.48/28
  ip prefix 100.64.0.44/30
exit
object-group network nets
  ip prefix 10.0.0.0/8
  ip prefix 192.168.0.0/16
  ip prefix 172.16.0.0/12
exit
object-group network cross
  ip prefix 100.64.0.36/30
  ip prefix 100.64.0.44/30
  ip prefix 100.64.0.52/30
  ip prefix 100.64.0.56/30
exit
object-group network DNS
  ip address-range 8.8.8.8
  ip prefix 100.123.0.0/24
exit
object-group network CoA_servers
  ip prefix 100.123.0.0/24
exit

radius-server timeout 10
radius-server retransmit 5
radius-server host 100.123.0.2
  key ascii-text encrypted 88B11079B9014FAAF7B9
  timeout 11
  priority 20
  source-address 198.18.128.3
  auth-port 31812
  acct-port 31813
  retransmit 10
  dead-interval 10
exit
aaa radius-profile PCRF
  radius-server host 100.123.0.2
exit
das-server COA
  key ascii-text encrypted 88B11079B9014FAAF7B9
  port 3799
exit
aaa das-profile COA
  das-server COA
exit

vlan 3
  force-up
exit
vlan 10
  force-up
exit
vlan 11
  force-up
exit
vlan 101
  force-up
exit
vlan 9
exit

security zone trusted
exit
security zone untrusted
exit
```

```
security zone gre
exit
security zone neighbour
exit
security zone user
exit
route-map out_BGP_GRE
  rule 10
    match ip address object-group gre_termination
    action set as-path prepend 64603 track 1
    action set metric bgp 1000 track 1
    action permit
  exit
exit
route-map out_BGP_AP
  rule 10
    match ip address object-group mgmt_AP
    action set as-path prepend 64603 track 1
    action set metric bgp 1000 track 1
    action permit
  exit
exit
route-map out_BGP_NAT
  rule 10
    match ip address object-group clients_AP
    action set as-path prepend 64603 track 1
    action set metric bgp 1000 track 1
    action permit
  exit
exit
route-map in_PREF
  rule 10
    action set local-preference 20
    action permit
  exit
exit
router bgp 64603
  neighbor 100.64.0.37
    remote-as 65001
    update-source 100.64.0.38
    address-family ipv4 unicast
      route-map out_BGP_GRE out
    enable
  exit
  enable
exit
  neighbor 100.64.0.45
    remote-as 65001
    update-source 100.64.0.46
    address-family ipv4 unicast
      route-map out_BGP_AP out
    enable
  exit
  enable
exit
  neighbor 100.64.0.53
    remote-as 65001
    update-source 100.64.0.54
    address-family ipv4 unicast
      route-map out_BGP_NAT out
    enable
  exit
  enable
exit
  neighbor 100.64.0.57
    remote-as 64603
    update-source 100.64.0.58
    address-family ipv4 unicast
      route-map in_PREF in
    next-hop-self
    enable
```



```
    exit
    enable
exit
address-family ipv4 unicast
    redistribute connected
    redistribute static
exit
enable
exit

snmp-server
snmp-server community "public11" ro
snmp-server community "private1" rw

snmp-server host 100.123.0.2
exit

snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment pwrin
snmp-server enable traps environment pwrin-insert
snmp-server enable traps environment fan
snmp-server enable traps environment fan-speed-changed
snmp-server enable traps environment fan-speed-high
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps environment board-overheat-temp
snmp-server enable traps environment board-supercooling-temp
snmp-server enable traps environment sfp-overheat-temp
snmp-server enable traps environment sfp-supercooling-temp
snmp-server enable traps environment switch-overheat-temp
snmp-server enable traps environment switch-supercooling-temp
snmp-server enable traps wifi
snmp-server enable traps wifi wifi-tunnels-number-in-bridge-high
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps bras
snmp-server enable traps bras sessions-number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
snmp-server enable traps screen syn-frag
snmp-server enable traps screen unknown-proto
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
```

```
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon fan
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon supply
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog
```

```
bridge 1
  description "GRE_termination"
  vlan 101
  security-zone gre
  ip address 192.168.200.52/28
  vrrp id 1
  vrrp ip 192.168.200.49/32
  vrrp ip 192.168.200.50/32 secondary
  vrrp priority 190
  vrrp group 1
  vrrp preempt disable
  vrrp preempt delay 150
  vrrp
  ipv6 enable
  ports vrrp filtering enable
  ports vrrp filtering exclude vlan
  enable
```

```
exit
```

```
bridge 3
  description "mgmt_AP"
  vlan 3
  security-zone trusted
  ip address 198.18.128.3/21
  ip helper-address 100.123.0.2
  ip helper-address vrrp-group 1
  vrrp id 3
  vrrp ip 198.18.128.1/32
  vrrp priority 190
  vrrp group 1
  vrrp preempt disable
  vrrp preempt delay 150
  vrrp track-ip 100.64.0.45
  vrrp track-ip interval 9
  vrrp
  ip tcp adjust-mss 1458
  protected-ports local
  protected-ports exclude vlan
  ports vrrp filtering enable
  ports vrrp filtering exclude vlan
  enable
```

```
exit
```

```
bridge 9
  description "neighbour"
  vlan 9
```

```
security-zone neighbour
ip firewall disable
ip address 100.64.0.58/30
enable
exit
bridge 10
description "data1_AP"
vlan 10
security-zone user
ip firewall disable
ip address 198.18.136.3/22
ip helper-address 100.123.0.2
ip helper-address vrrp-group 1
vrrp id 10
vrrp ip 198.18.136.1/32
vrrp priority 190
vrrp group 1
vrrp preempt disable
vrrp preempt delay 150
vrrp
ip tcp adjust-mss 1458
location data10
protected-ports radius
protected-ports exclude vlan
ports vrrp filtering enable
ports vrrp filtering exclude vlan
enable
exit
bridge 11
description "data2_AP"
vlan 11
security-zone user
ip firewall disable
ip address 198.18.140.3/22
ip helper-address 100.123.0.2
ip helper-address vrrp-group 1
vrrp id 11
vrrp ip 198.18.140.1/32
vrrp priority 190
vrrp group 1
vrrp preempt disable
vrrp preempt delay 150
vrrp
ip tcp adjust-mss 1458
location data11
protected-ports radius
protected-ports exclude vlan
ports vrrp filtering enable
ports vrrp filtering exclude vlan
enable
exit
interface gigabitethernet 1/0/1.207
description "VRF_AP"
security-zone gre
ip firewall disable
ip address 100.64.0.38/30
ip tcp adjust-mss 1458
ipv6 enable
exit
interface gigabitethernet 1/0/1.209
description "VRF_CORE"
security-zone trusted
ip firewall disable
ip address 100.64.0.46/30
ip tcp adjust-mss 1458
ipv6 enable
exit
interface gigabitethernet 1/0/1.211
description "VRF_NAT"
security-zone untrusted
```

```
ip firewall disable
ip address 100.64.0.54/30
ip tcp adjust-mss 1458
ipv6 enable
exit
interface gigabitethernet 1/0/2
description "neighbour"
mode hybrid
switchport forbidden default-vlan
switchport general acceptable-frame-type tagged-only
switchport general allowed vlan add 3,9-11,101 tagged
exit
tunnel softgre 1
description "mgmt"
mode management
local address 192.168.200.49
default-profile
enable
exit
tunnel softgre 1.1
bridge-group 3
enable
exit
tunnel softgre 2
description "data"
mode data
local address 192.168.200.50
default-profile
enable
exit

security zone-pair gre self
rule 1
action permit
match protocol gre
enable
exit
rule 2
action permit
match protocol vrrp
enable
exit
rule 3
action permit
match protocol tcp
match destination-port aptd
enable
exit
rule 4
action permit
match protocol icmp
enable
exit
rule 10
action permit
match protocol tcp
match source-address cross
match source-port bgp
match destination-port bgp
enable
exit
exit
security zone-pair trusted self
rule 1
action permit
match protocol vrrp
enable
exit
rule 2
action permit
match protocol udp
```

```
    match source-port dhcp_server
    match destination-port dhcp_server
    enable
exit
rule 3
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
exit
rule 4
    action permit
    match protocol icmp
    enable
exit
rule 10
    action permit
    match source-address SoftWLC
    enable
exit
rule 11
    action permit
    match source-address Admnet
    enable
exit
rule 20
    action permit
    match protocol tcp
    match source-address cross
    match source-port bgp
    match destination-port bgp
    enable
exit
exit
security zone-pair trusted trusted
    rule 1
        action permit
        enable
    exit
exit
security zone-pair user untrusted
    rule 1
        action permit
        enable
    exit
exit
security zone-pair user self
    rule 1
        action permit
        match protocol icmp
        enable
    exit
rule 2
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
exit
rule 4
    action permit
    match protocol vrrp
    enable
exit
rule 5
    action permit
    match protocol udp
    match source-port dhcp_server
    match destination-port dhcp_server
    enable
```

```
    exit
exit
security zone-pair user trusted
    rule 1
        action permit
        match protocol udp
        match source-port dhcp_client
        match destination-port dhcp_server
        enable
    exit
    rule 2
        action permit
        match protocol udp
        match destination-address DNS
        match destination-port dns
        enable
    exit
exit
security zone-pair trusted user
    rule 1
        action permit
        match protocol udp
        match source-port dhcp_server
        match destination-port dhcp_client
        enable
    exit
    rule 2
        action permit
        match protocol udp
        match source-port dhcp_server
        match destination-port dhcp_server
        enable
    exit
    rule 3
        action permit
        match protocol icmp
        enable
    exit
exit
security zone-pair trusted untrusted
    rule 1
        action permit
        enable
    exit
exit
security zone-pair gre gre
    rule 1
        action permit
        enable
    exit
exit
security zone-pair neighbour self
    rule 2
        action permit
        match protocol tcp
        match destination-port bgp
        enable
    exit
    rule 3
        action permit
        match protocol udp
        match destination-port firewall_failover
        enable
    exit
    rule 4
        action permit
        match protocol udp
        match source-port dhcp_server
    exit
    rule 10
        action permit
```

```
    match protocol gre
    enable
exit
rule 20
    action permit
    match protocol icmp
    enable
exit
rule 30
    action permit
    match protocol vrrp
    enable
exit
rule 40
    action permit
    match protocol udp
    match source-port dhcp_server
    match destination-port dhcp_server
    enable
exit
rule 50
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
exit
rule 60
    action permit
    match source-address SoftWLC
    enable
exit
rule 80
    action permit
    match source-address Admnet
    enable
exit
rule 90
    action permit
    match protocol tcp
    match destination-port aptd
    enable
exit
rule 100
    action permit
    match protocol tcp
    match destination-port telnet
    enable
exit
exit
security zone-pair neighbour trusted
    rule 10
        action permit
        enable
    exit
exit
security zone-pair neighbour untrusted
    rule 10
        action permit
        enable
    exit
exit
security zone-pair neighbour gre
    rule 10
        action permit
        enable
    exit
exit
security zone-pair neighbour user
    rule 10
        action permit
```

```
        match protocol udp
        match source-port dhcp_server
        match destination-port dhcp_client
        enable
    exit
exit
security zone-pair trusted neighbour
    rule 10
        action permit
        enable
    exit
exit
security zone-pair gre neighbour
    rule 10
        action permit
        enable
    exit
exit
security zone-pair user neighbour
    rule 10
        action permit
        match protocol udp
        match destination-port dns
        enable
    exit
    rule 20
        action permit
        match not source-address nets
        enable
    exit
exit
security zone-pair untrusted self
    rule 10
        action permit
        match protocol tcp
        match source-address cross
        match source-port bgp
        match destination-port bgp
        enable
    exit
exit

security passwords history 0
ip firewall failover sync-type unicast
ip firewall failover source-address 198.18.128.3
ip firewall failover destination-address 100.64.0.57
ip firewall failover port 3333
ip firewall failover

ip dhcp-relay

wireless-controller
    peer-address 100.64.0.57
    nas-ip-address 198.18.128.3
    vrrp-group 1
    data-tunnel configuration radius
    keepalive mode reactive
    aaa das-profile COA
    aaa radius-profile PCRF
    internal-usage-vlan 1001-2037,2500-3000,3200-3700
    enable
exit
ip telnet server
ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.123.0.2
```


exit