

ESR wireless-controller " "

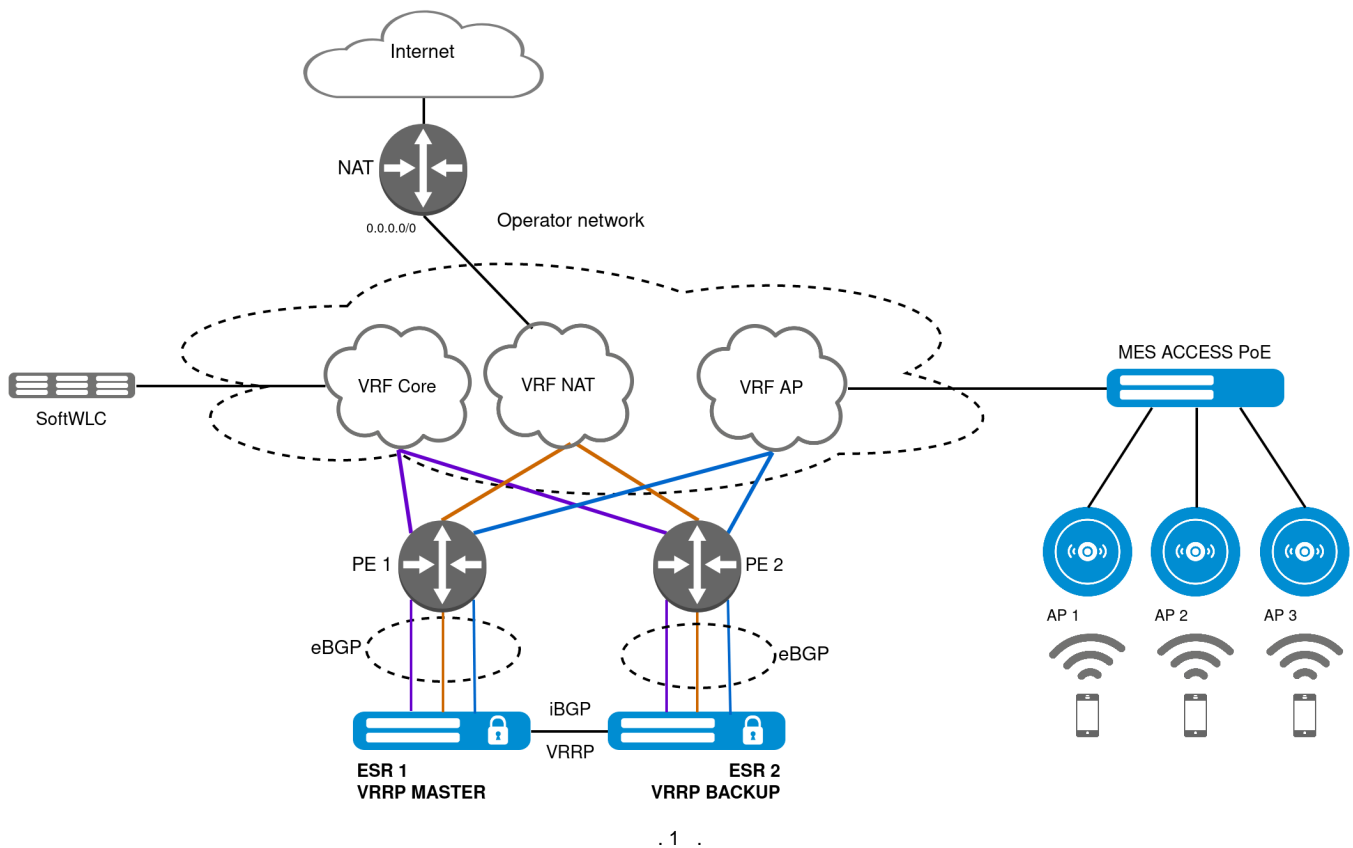
-
- GRE Wireless-Controller
 - ESR SoftGRE
 - ESR SoftGRE
 - - ESR
 - 1 -
 - 2 - EMS, SSID
 - 3 - ESR, EMS, SSID .
 - - EMS
 - 4 - data-tunnel create EMS, ESR
 - 5 - data-tunnel create EMS, ESR
 - 6 - EMS, SSID
 - 7 - ESR, data-tunnel create VRRP BACKUP
 - CoA PCRF domain update update location
 - ESR EMS
- ESR
 -
 -
 - ESR
 - ESR
 -
- VRRP ESR
 -
 - PE 1 master
 - ESR 1
 - ESR 1
- - ESR 1 Alfa ESR 2 Beta
 - DHCP

ESR " " PE, . 1. , , PoE, L3/ .

- , , VRF AP.
- , VRF NAT, NAT.
- VRF core, ESR SoftWLC.
- ESR PE (), .
- ESR GRE .

, PE ESR, -

.



GRE Wireless-Controller

L3, GRE (mgmt data), 43-, ESR . ESR , . wireless-controller. wireless-controller ESR "WIFI - Wi-Fi controller". , ESR . wireless-controller vlan. GRE ESR "SoftGRE".

:

1. ESR - " SoftGRE". ESR.
2. - - PCRF, - EMS SSID - " SoftGRE". PCRF.

✓ ESR, " SoftGRE", .

! wireless-controller ESR WiFi. show licence:

```
esr-1000# show licence
Licence information
-----
Name:      eltex
Version:   1.0
Type:      ESR-1000
S/N:       NP00000033
MAC:       A8:F9:4B:AB:B3:80
Features:
  WIFI - Wi-Fi controller
```

ESR SoftGRE

ESR:

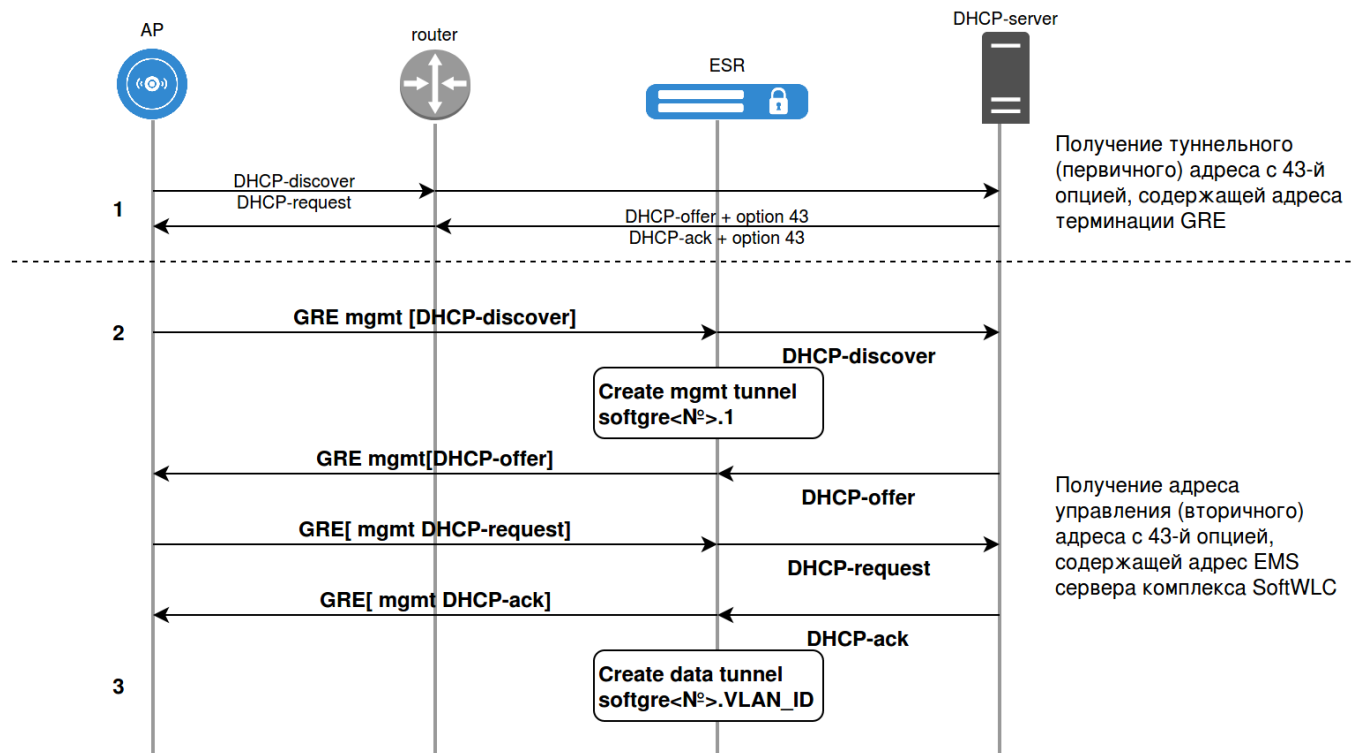
```

tunnel softgre 1
 mode management
 local address <IP address>
 default-profile
 enable
exit
tunnel softgre 1.1
 bridge-group <>
 enable
exit
tunnel softgre 2
 mode data
 local address <IP address>
 default-profile
 enable
exit
tunnel softgre 2.10
 bridge-group <>
 enable
exit
tunnel softgre 2.11
 bridge-group <>
 enable
exit

wireless-controller
 enable
exit

```

, .2, ESR .



. 2. ESR , SoftGRE.

1., 43, GRE (11 - mgmt, 12 -data), ESR.

2. 2 GRE GRE. mgmt GRE DHCP-discover 1- VLAN.

ESR, (GRE, DHCP-discover), , SoftGRE (mgmt) - 1- VLAN, bridge, .

DHCP-discover DHCP relay, DHCP-offer, ESR SoftGRE .

DHCP-request, DHCP relay.

3. , DHCP DHCP-ack , ESR data SoftGRE , data .

ESR , SoftWLC. , -, , . - ESR.

ESR SoftGRE

- ESR ELTEX-PCRF (PCRF), SoftWLC SSID, . RADIUS, UDP 3799, 31812, 31813 (PCRF). ELTEX-PCRF. :

```
object-group network SoftWLC
  ip address < ELTEX-PCRF SoftWLC>
exit

radius-server host < ELTEX-PCRF>
  key ascii-text <>
  auth-port 31812
  acct-port 31813
exit
aaa radius-profile PCRF
  radius-server host < ELTEX-PCRF>
exit
das-server COA
  key ascii-text <, ESR ELTEX-PCRF>
  port 3799
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit

tunnel softgre 1
  mode management
  local address <IP address>
  default-profile
  enable
exit
tunnel softgre 1.1
  bridge-group <>
  enable
exit
tunnel softgre 2
  mode data
  local address <IP address>
  default-profile
  enable
exit

wireless-controller
  data-tunnel configuration radius
  aaa das-profile COA
  aaa radius-profile PCRF
  enable
exit

bridge 10
  location <>
  enable
exit
```

SoftGRE 7, . - - ESR () - EMS. , -, - :

- ESR:

1. ESR,
2. ESR, EMS, SSID . - .
3. ESR, EMS, SSID . - .

- EMS:

4. data-tunnel create EMS, ESR.
5. data-tunnel create EMS, ESR.
6. data-tunnel create EMS, EMS, SSID .
7. ESR, data-tunnel create, VRRP BACKUP. , ESR, VRRP MASTER.

- ESR

PCRF ESR, . radius PCRF ip-shaper, NAS-IP ESR. PCRF IP, SSID (ESR), , :

1. office:name - SSID ,
2. vlan:id - vlan, SSID ("VLAN-ID")
3. name - Bridge, Location, SSID ("Bridge, Location")
4. sc - Switch Community(sc), SSID (sc=1, sc)
5. gre-location - , , NODE.<.>.<vlan> (NODE.8498.10). " " (,). Gre-location BRAS, L2 .

2-5 SSID , radius PCRF (20).

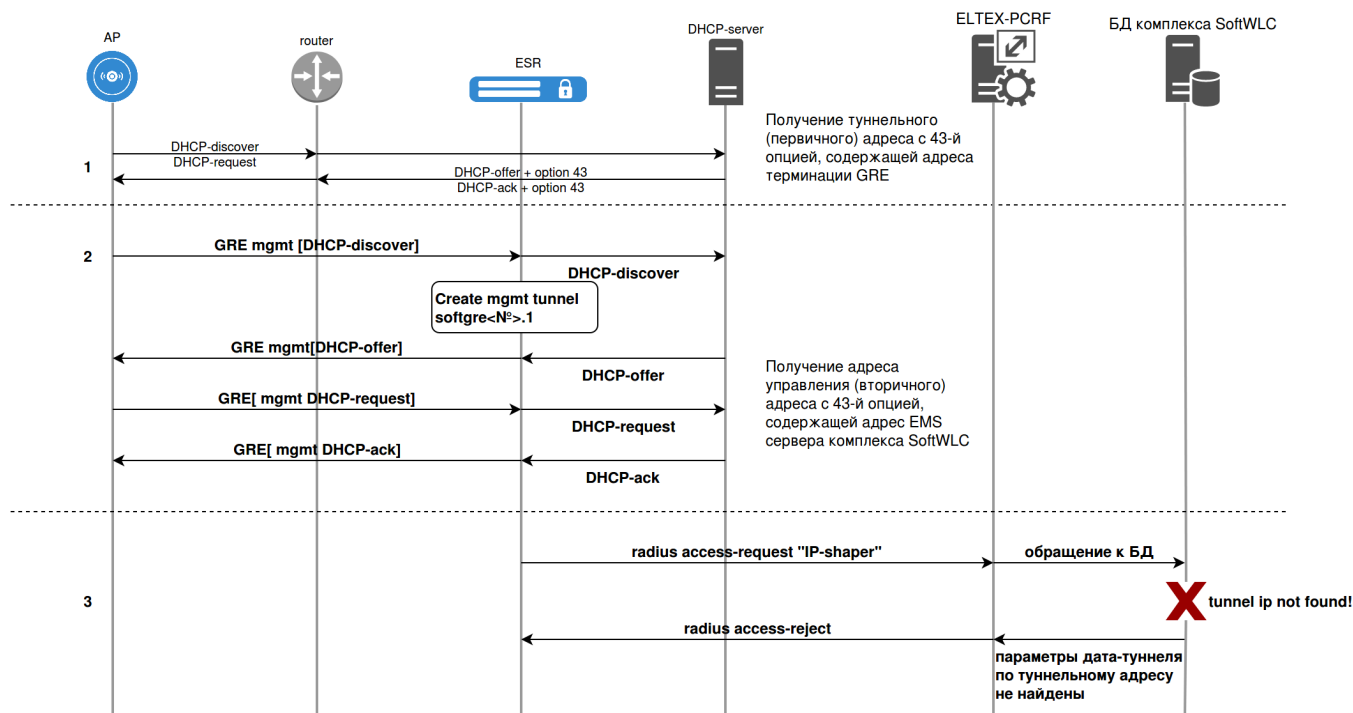
"Bridge Location" "location" ESR, .. , ESR .

"vlan:id", .. - .

1 -

- , EMS.

, . 3, PCRF:



. 3.

1. , 43, GRE (11 - mgmt, 12 -data), ESR.

2. 2 GRE GRE. mgmt GRE DHCP-discover 1- VLAN.

ESR, (GRE, DHCP-discover), , SoftGRE (mgmt) - 1- VLAN, bridge, .

DHCP-discover DHCP, DHCP-offer, ESR SoftGRE .

DHCP-request, DHCP .

3. , DHCP DHCP-ack :

) ESR radius ip-shaper PCRF, () NAS-IP ESR;

) PCRF SotWLC, ;
) () - ;
) PCRF, , radius access-reject ESR;

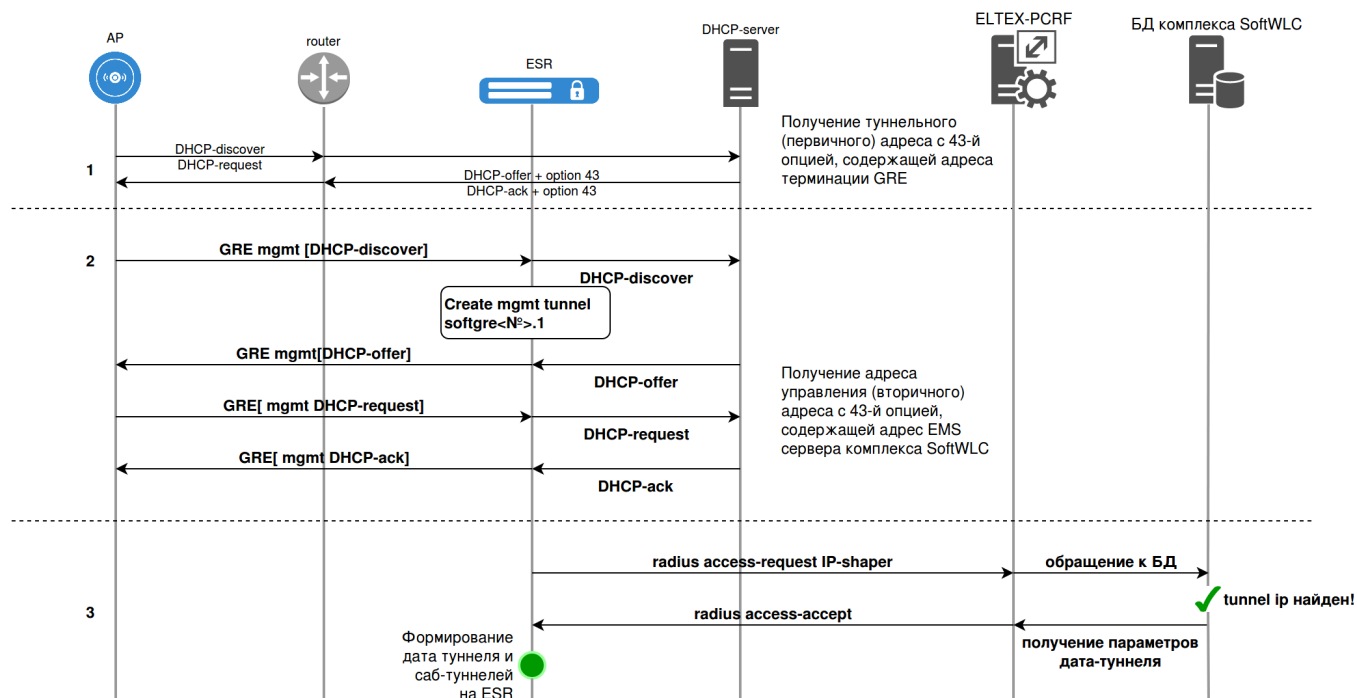
4. - ESR.

, - ESR . EMS .

2 - EMS, SSID

EMS, SSID - ESR.

, . 4, -:



. 4. -, PCRF.

1. 43, GRE (11 - mgmt, 12 -data), ESR.

2. 2 GRE GRE. mgmt GRE DHCP-discover 1- VLAN.

ESR, (GRE, DHCP-discover) , SoftGRE (mgmt) - 1- VLAN, bridge, .

DHCP-discover DHCP, DHCP-offer, ESR SoftGRE .

DHCP-request, DHCP .

3. , DHCP DHCP-ack :

) ESR ip-shaper PCRF, () ;

) PCRF SotWLC, ;

) (), -;

) , PCRF radius access-accept, - ESR;

) ESR, , -.

ESR - . EMS .

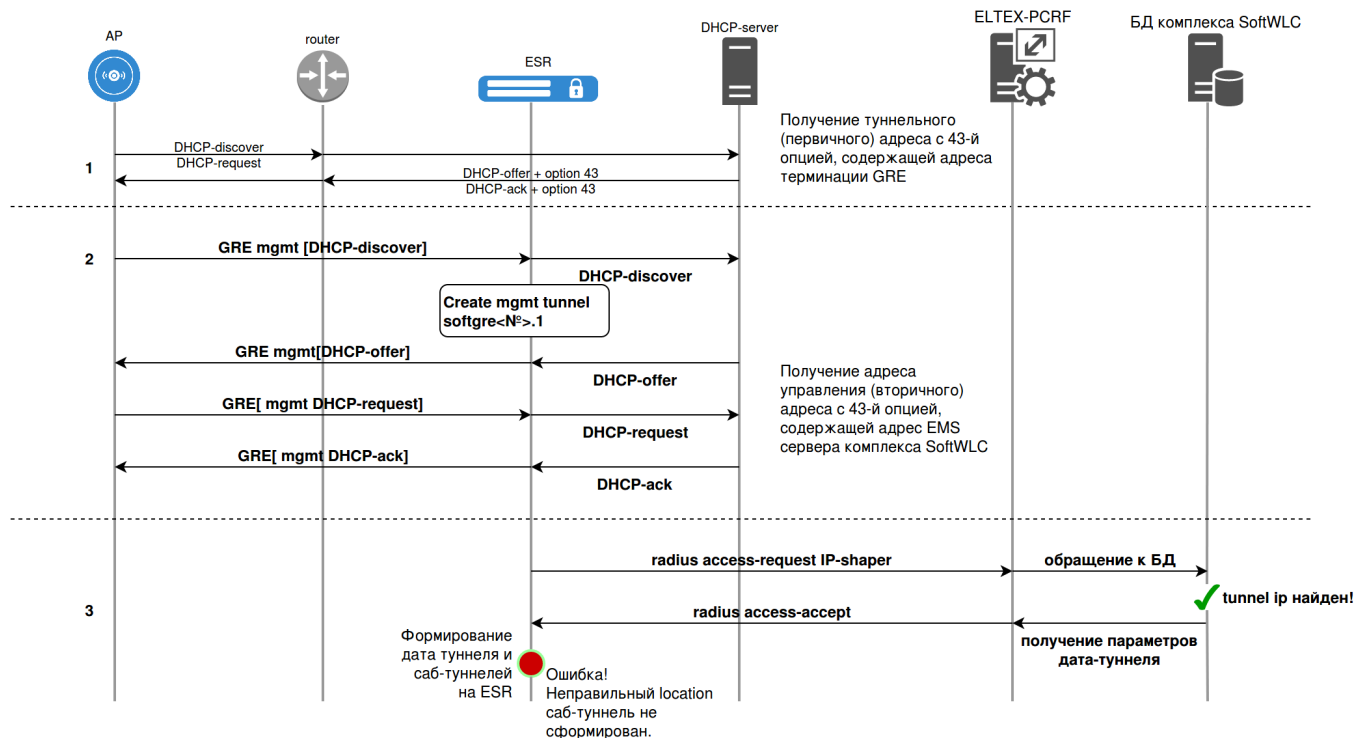
3 - ESR, EMS, SSID .

EMS, SSID .

! "Bridge Location" , ESR location.

! "VLAN-ID" - - ESR . ,.. SSID .
SSID , - - - ESR . ,.. SSID .

, . 5, - "Bridge, Location".



. 5.

"Bridge, Location" - ESR. ESR, APTD ERROR () :

```
%APTD-E-ERROR: <aptd_validate_access_data> AP <Tunnel IP >: SSID '< Bridge Location>' not found in locations!
```

- . EMS .

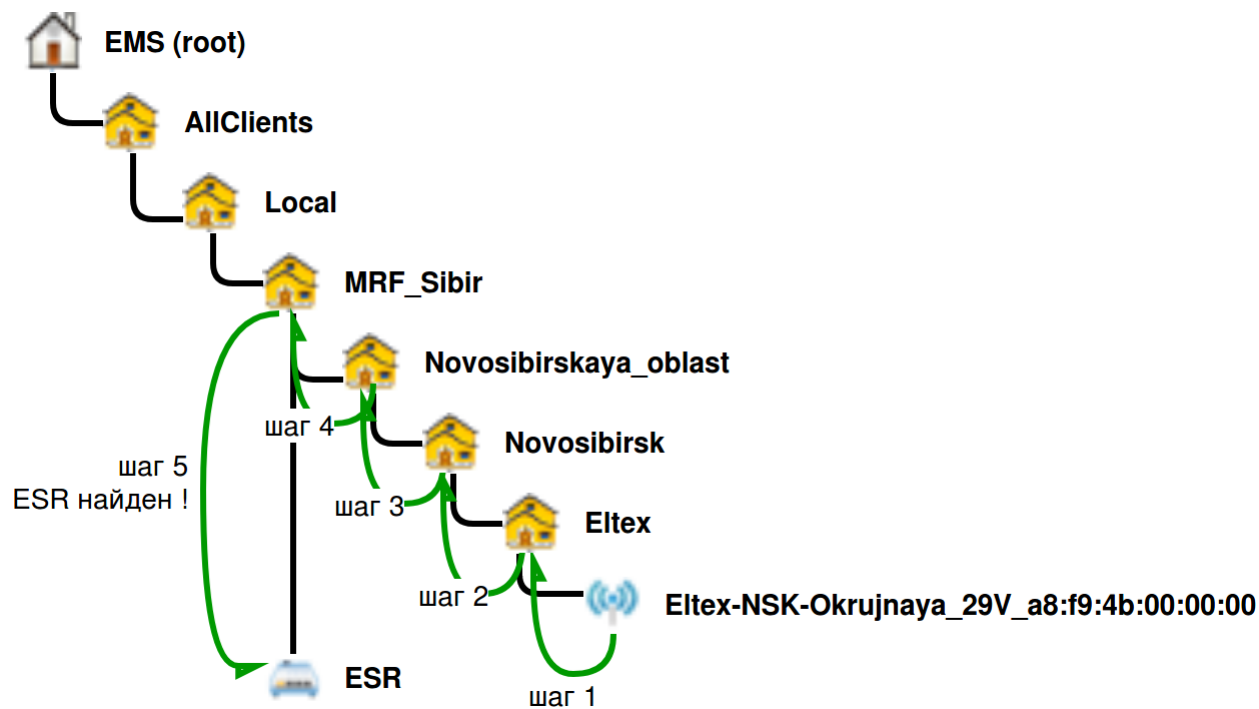
! ESR 1.11.0, ip-shaper -- "Bridge Location" -. , , -. .

- EMS

.. ESR , - , ESR EMS. :

1. .
2. .
3. ;
4. "data-tunnel ESR" EMS .

EMS, PCRF radius CoA-request ("data-tunnel create") UDP 3799 ESR. ESR . , ESR , EMS. ESR (. 6):



. 6.

- 1: , data-tunnel create Eltex;
- 2: Eltex ESR - , Novosibirsk;
- 3: Novosibirks ESR - , Novosibirskaya_oblast;
- 4: Novosibirskaya_oblast ESR - , MRF_Sibir;
- 5: MRF_Sibir ESR - ! .

ESR, - . CoA-request data-tunnel create , - NAS-IP ESR.

- EMS, , . , ESR, .

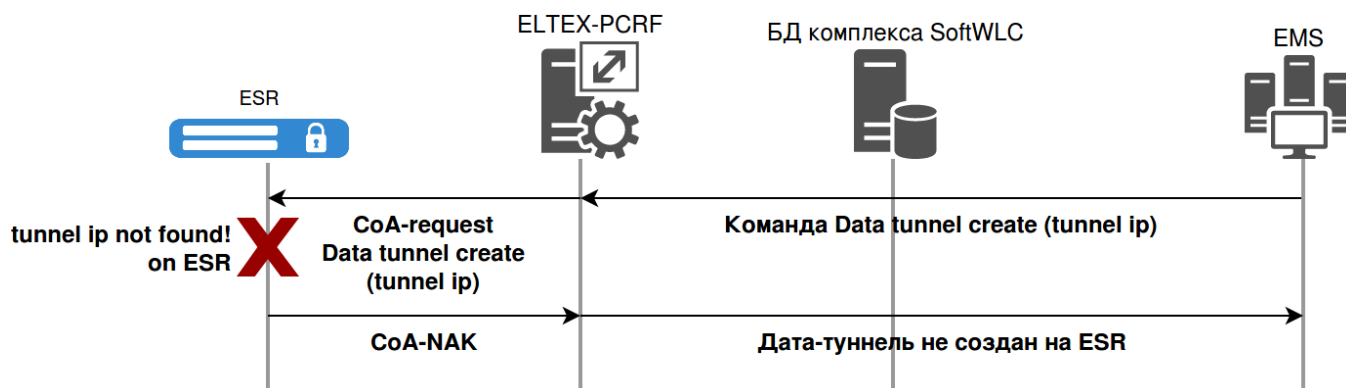
! ! data-tunnel create EMS SNMP-ping, snmp . SNMP-ping - , EMS :

FATAL SNMP : TIMEOUT/Timeout: 300 ms

ESR, data-tunnel create ESR - . ,.. ESR SoftGRE.

4 - data-tunnel create EMS, ESR

, . 7, , data-tunnel create EMS. ESR, , .



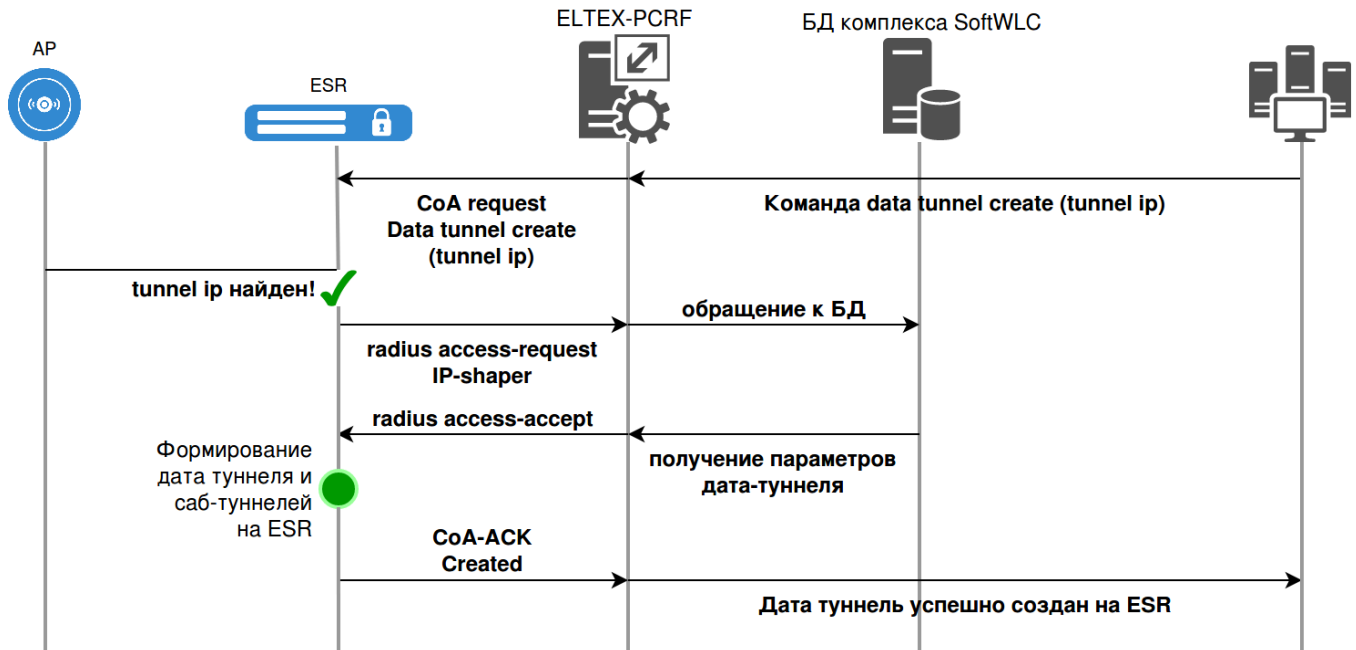
. 7.

- ESR. EMS, :

```
'data-tunnel create' ESR NAS ip <IP ESR>  
- 'Data-tunnel create' (ESR: < ESR>): Data- <Tunnel IP > <IP ESR>
```

5 - data-tunnel create EMS, ESR

, . 8, , ESR, SSID EMS .



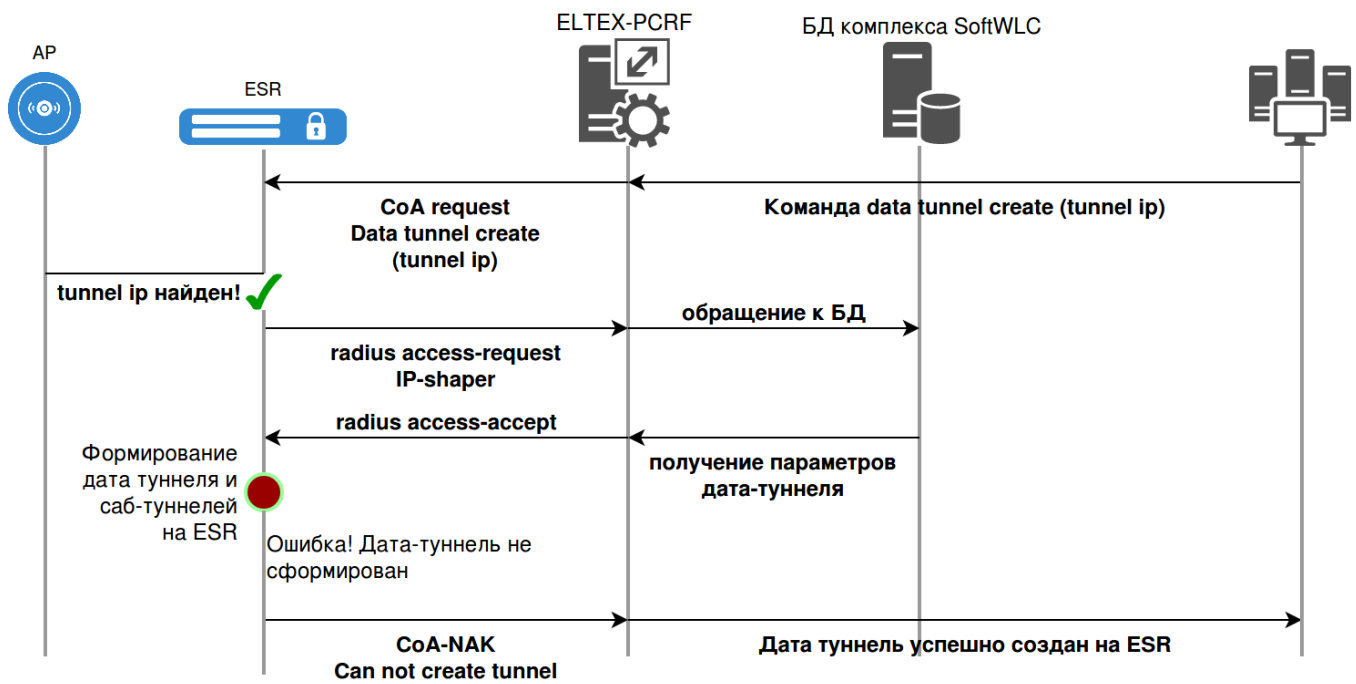
. 8.

. 8, 2, CoA . ESR, CoA request Data tunnel create , 2 CoA-ACK Created, - ESR. EMS :

```
'data-tunnel create' ESR NAS ip <IP ESR>  
- Data- <Tunnel IP > <IP ESR>
```

6 - EMS, SSID

, . 9, , ESR, SSID EMS . 3.



. 9.

EMS, :

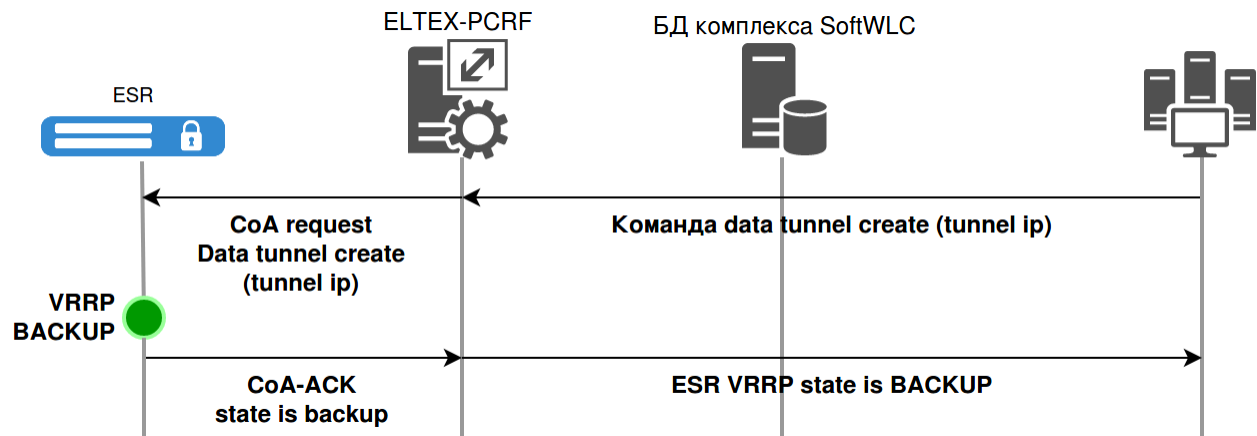
```

'data-tunnel create' ESR NAS ip <IP ESR>
- 'Data-tunnel create' (ESR: < ESR>): <Tunnel IP > <IP ESR>

```

7 - ESR, data-tunnel create VRRP BACKUP

VRRP ESR - . ESR VRRP BACKUP. ESR . 10.



. 10.

ESR, VRRP BACKUP "State is backup", EMS :

```

'data-tunnel create' ESR NAS ip <IP ESR>
- ESR with NAS IP '<IP ESR>' is in VRRP backup status

```

CoA PCRF domain update update location

, EMS SSID, -. SSID, ESR, :

- 1) "Bridge Location";
- 2) "Switch Community";
- 3) " VAP";
- 4) " VAP (GRE)";
- 5) "VLAN-ID";
- 6) / SSID ;

"domain:command=update" "data-tunnel:command=update-location". :

- 1) , SSID;
- 2) , (), SSID;
- 2) ESR, SSID , .6, "domain:command=update" (, gre-location, -);
- 3) PCRF "domain:command=update", "data-tunnel:command=update-location".
- 4) "data-tunnel:command=update-location", SSID, CoA (vlan:id gre-location). ESR, , .6;
- 5) ESR - .

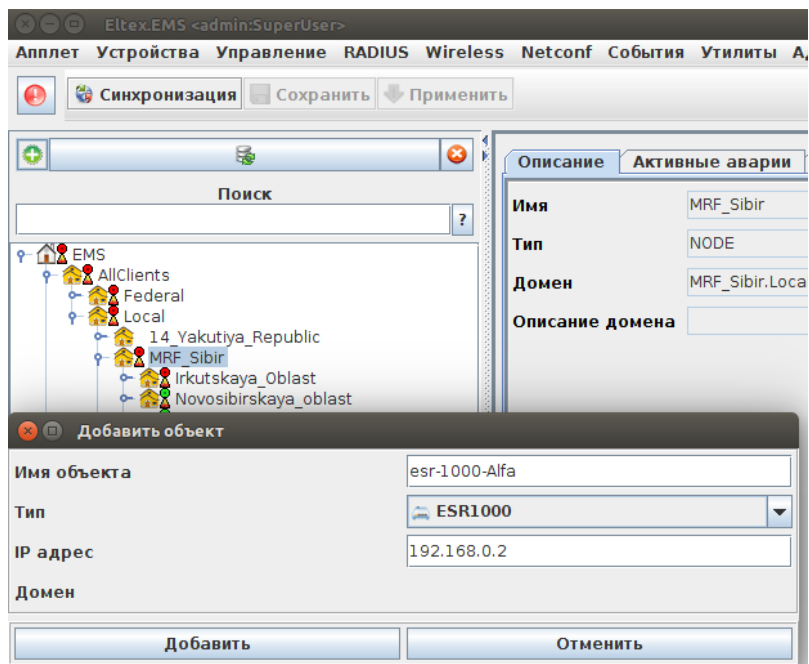
:

- 1) - - 4096 ([RFC2865](#));
- 2) SSID , ESR;
- 3) . . - update location CPU ESR -;
- 4) data-tunnel:command=update-location "domain:command=update", .

/ EMS .

ESR EMS

PCRF, ESR EMS. ESR , , . ESR "+" (>):



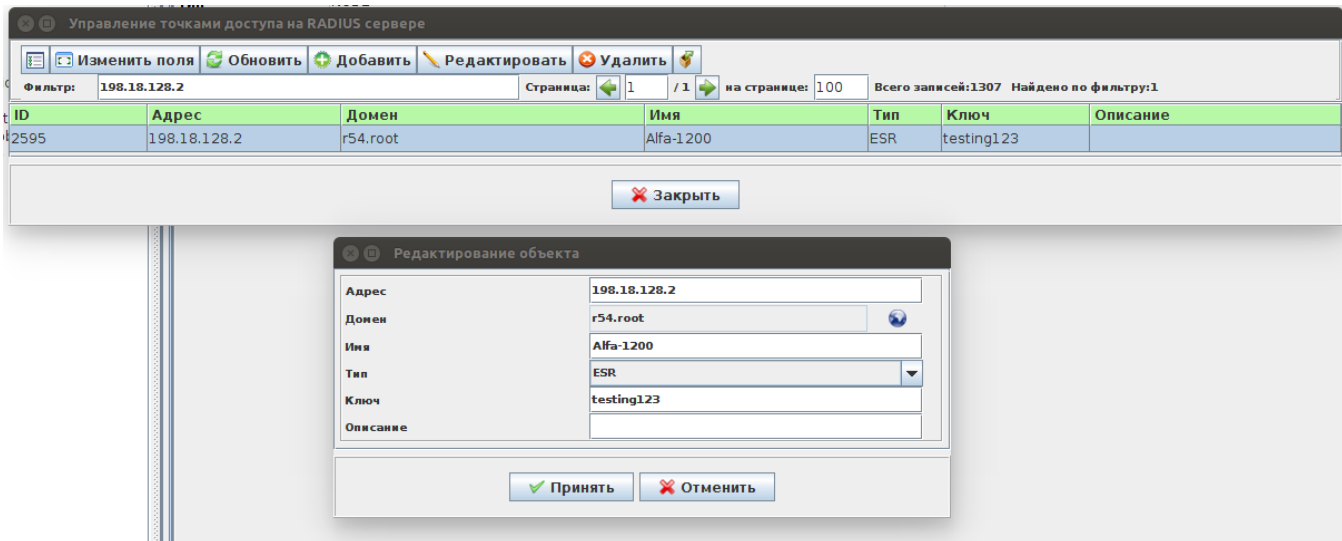
. 11.

(. 11), :

- - ESR.
- - ESR.
- IP - ip ESR.

""

"RADIUS" " " " ESR ESR ("testing123"):



. 12.

""

"" ESR read/write SNMP community ESR.



ESR-100/200 " ESR" " " "StationCE".

"Station", ESR - .

ESR

ESR L3 wireless-controller, - PCRF, , VRRF " ", ESR. . , SoftWLC .

:

1. , AS, (1).
2. ESR .
3. ESR, L3 ESR .
4. SoftWLC ESR.
5. ESR.
6. .

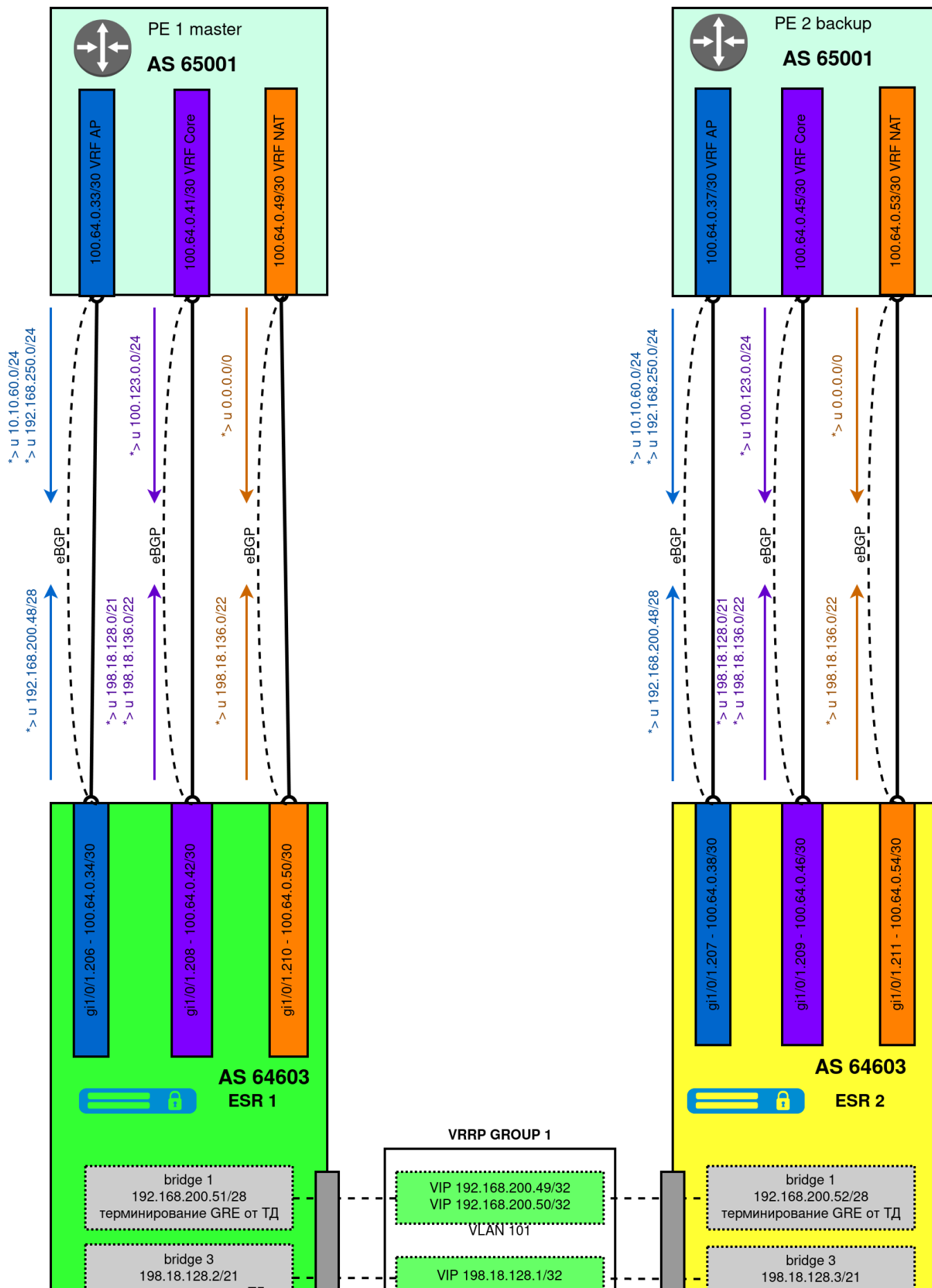
1, ESR 1 - , ESR 2 - .

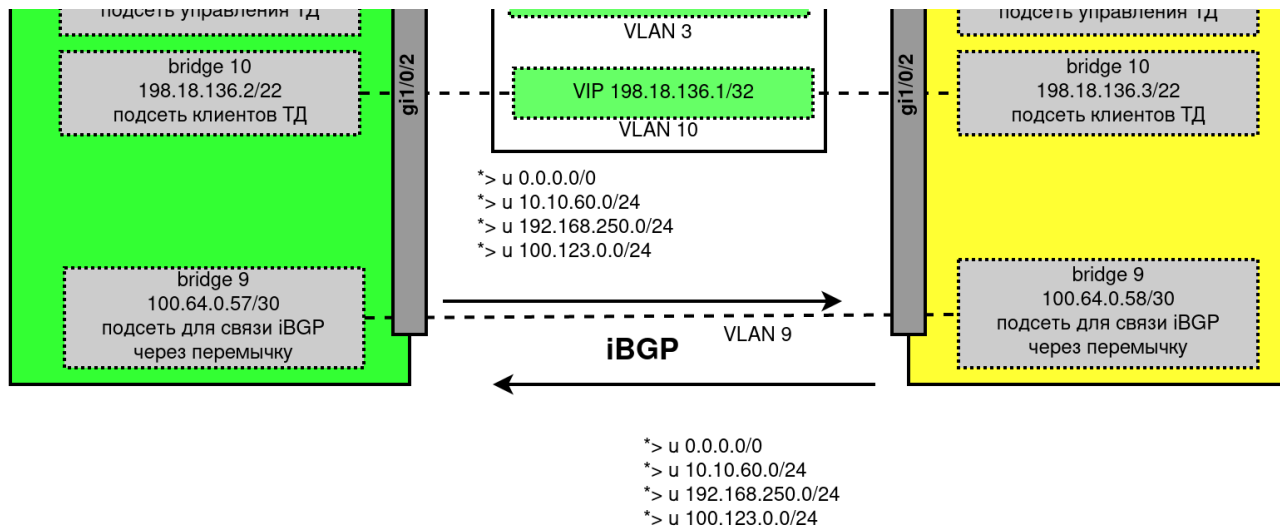
AS 64603	ESR 1			ESR 2	
		IP	VRRP IP		IP
VRF AP	gi1/0/1.206	100.64.0.34/30	n/a	gi1/0/1.207	100.64.0.38/30
VRF core	gi1/0/1.208	100.64.0.42/30	n/a	gi1/0/1.209	100.64.0.46/30
VRF NAT	gi1/0/1.210	100.64.0.50/30	n/a	gi1/0/1.211	100.64.0.54/30
GRE	bridge 1 / 101	192.168.200.51/28	192.168.200.49/32 192.168.200.50/32	bridge 1 / 101	192.168.200.52/28
	bridge 3 / 3	198.18.128.2/21	198.18.128.1/32	bridge 3 / 3	198.18.128.3/21

ESR-1	bridge 9 / 9	100.64.0.57/30	n/a	bridge 9 / 9	100.64.0.58/30
	bridge 10 / 10	198.18.136.2/22	198.18.140.1/32	bridge 10 / 10	198.18.140.3/22

1.

, . 13, .





. 13.

ESR (AS 64603) PE (AS 65001) , 3 - BGP 3 VRF:

- VRF AP - ESR.
- VRF core - SoftWLC , ESR , DHCP .
- VRF NAT - , NAT .

VRF AP ESR 10.10.60.0/24 192.168.250.0/24, . VRF ESR 192.168.200.48/28, GRE. GRE ESR 192.168.200.49 () 192.168.200.50 ().

VRF core ESR 100.123.0.0/24, SoftWLC (EMS, DHCP). VRF ESR : 198.18.128.0/21 () 198.18.136.0/22 (, ,).

VRF NAT ESR 0.0.0.0/0. VRF ESR 198.18.136.0/22 –

ESR (AS 64603), iBGP. Bridge 9. Port Channel, .

, . , " c VRRP+BGP". " ESR wireless-controller " " .

ESR

. . .

.. ESR - :

```
esr1000# copy system:default-config system:candidate-config
Entire candidate configuration will be reset to default, all settings will be lost upon commit.
Do you really want to continue? (y/N): y
|*****| 100% (52B) Default configuration loaded successfully.
```

ESR 1 ("Alfa") ESR 2 ("Beta"):

```
hostname Alfa

security zone trusted
exit
security zone untrusted
exit
security zone gre
exit
security zone neighbour
exit
security zone user
exit

interface gigabitethernet 1/0/1.206
  description "VRF_AP"
  security-zone gre
  ip firewall disable
  ip address 100.64.0.34/30
exit
interface gigabitethernet 1/0/1.208
  description "VRF_CORE"
  security-zone trusted
  ip firewall disable
  ip address 100.64.0.42/30
exit
interface gigabitethernet 1/0/1.210
  description "VRF_NAT"
  security-zone untrusted
  ip firewall disable
  ip address 100.64.0.50/30
exit

ip telnet server
ip ssh server
```



```

hostname Beta

security zone trusted
exit
security zone untrusted
exit
security zone gre
exit
security zone neighbour
exit
security zone user
exit

interface gigabitethernet 1/0/1.207
  description "VRF_AP"
  security-zone gre
  ip firewall disable
  ip address 100.64.0.38/30
exit
interface gigabitethernet 1/0/1.209
  description "VRF_CORE"
  security-zone trusted
  ip firewall disable
  ip address 100.64.0.46/30
exit
interface gigabitethernet 1/0/1.211
  description "VRF_NAT"
  security-zone untrusted
  ip firewall disable
  ip address 100.64.0.54/30
exit

ip telnet server
ip ssh server

```

ESR (PE) telnet ssh. , BGP ESR .

GRE, , ESR:

```

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

bridge 1
  description "GRE_termination"
  vlan 101
  security-zone gre
  ip firewall disable
  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 180
  vrrp
  enable
exit

```

```

bridge 3
  description "mgmt_AP"
  vlan 3
  security-zone trusted
  ip firewall disable
  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 180
  vrrp
  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 100.64.0.57/30
  enable
exit
bridge 10
  description "data_AP"
  vlan 10
  security-zone user
  ip firewall disable
  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 180
  vrrp
  location data10
  protected-ports local
  protected-ports exclude vlan
  ports vrrp filtering enable
  ports vrrp filtering exclude vlan
  enable
exit

interface gigabitethernet 1/0/2
  description "neighbour"
  mode switchport
  switchport general acceptable-frame-type tagged-only
  switchport general allowed vlan add 3,9-10,101 tagged
exit

```

```

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

```

```
exit
vlan 9
exit

bridge 1
  description "GRE_termination"
  vlan 101
  security-zone gre
  ip firewall disable
  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 20
  vrrp group 1
  vrrp preempt disable
  vrrp preempt delay 180
  vrrp
  enable
exit
bridge 3
  description "mgmt_AP"
  vlan 3
  security-zone trusted
  ip firewall disable
  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 20
  vrrp group 1
  vrrp preempt disable
  vrrp preempt delay 180
  vrrp
  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 "data_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 20
  vrrp group 1
  vrrp preempt disable
  vrrp preempt delay 180
  vrrp
  location data10
  protected-ports local
  protected-ports exclude vlan
  ports vrrp filtering enable
  ports vrrp filtering exclude vlan
  enable
exit
```

```
interface gigabitethernet 1/0/2
  description "neighbour"
  mode switchport
  switchport general acceptable-frame-type tagged-only
  switchport general allowed vlan add 3,9-10,101 tagged
exit
```

BGP:

```
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 100.64.0.56/30
exit
object-group network clients_AP
  ip prefix 198.18.136.0/22
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 set local-preference 20
    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
```

```
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 100.64.0.56/30
exit
object-group network clients_AP
    ip prefix 198.18.136.0/22
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 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
```

wireless-controller - PCRF:



SoftWLC Eltex-PCRF - ESR

aaa radius-profile! VRRP !

```
radius-server host 100.123.0.2
  key ascii-text testing123
  timeout 5
  source-address 198.18.128.2
  auth-port 31812
  acct-port 31813
  dead-interval 10
exit
radius-server host 100.123.0.3
  key ascii-text testing123
  timeout 5
  source-address 198.18.128.2
  auth-port 31812
  acct-port 31813
  dead-interval 10
exit
aaa radius-profile PCRF
  radius-server host 100.123.0.2
  radius-server host 100.123.0.3
exit
```

```
object-group network SoftWLC
  ip prefix 100.123.0.0/24
exit

radius-server retransmit 2
radius-server host 100.123.0.2
  key ascii-text testing123
  timeout 5
  source-address 198.18.128.2
  auth-port 31812
  acct-port 31813
  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

tunnel softgre 1
  mode management
  local address 192.168.200.49
  default-profile
  enable
exit
tunnel softgre 1.1
  bridge-group 3
  enable
exit
tunnel softgre 2
  mode data
  local address 192.168.200.50
  default-profile
  enable
exit

wireless-controller
  peer-address 100.64.0.58
  nas-ip-address 198.18.128.2
  vrrp-group 1
  data-tunnel configuration radius
  aaa das-profile COA
  aaa radius-profile PCRF
  enable
exit
```



```

object-group network SoftWLC
  ip prefix 100.123.0.0/24
exit

radius-server retransmit 2
radius-server host 100.123.0.2
  key ascii-text testing123
  timeout 5
  source-address 198.18.128.3
  auth-port 31812
  acct-port 31813
  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

tunnel softgre 1
  mode management
  local address 192.168.200.49
  default-profile
  enable
exit
tunnel softgre 1.1
  bridge-group 3
  enable
exit
tunnel softgre 2
  mode data
  local address 192.168.200.50
  default-profile
  enable
exit

wireless-controller
  peer-address 100.64.0.57
  nas-ip-address 198.18.128.3
  vrrp-group 1
  data-tunnel configuration radius
  aaa das-profile COA
  aaa radius-profile PCRF
  enable
exit

```

, source-address -, .. ESR . Peer-address, nas-ip-address, ESR.

SNMP ESR, :

```

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
```

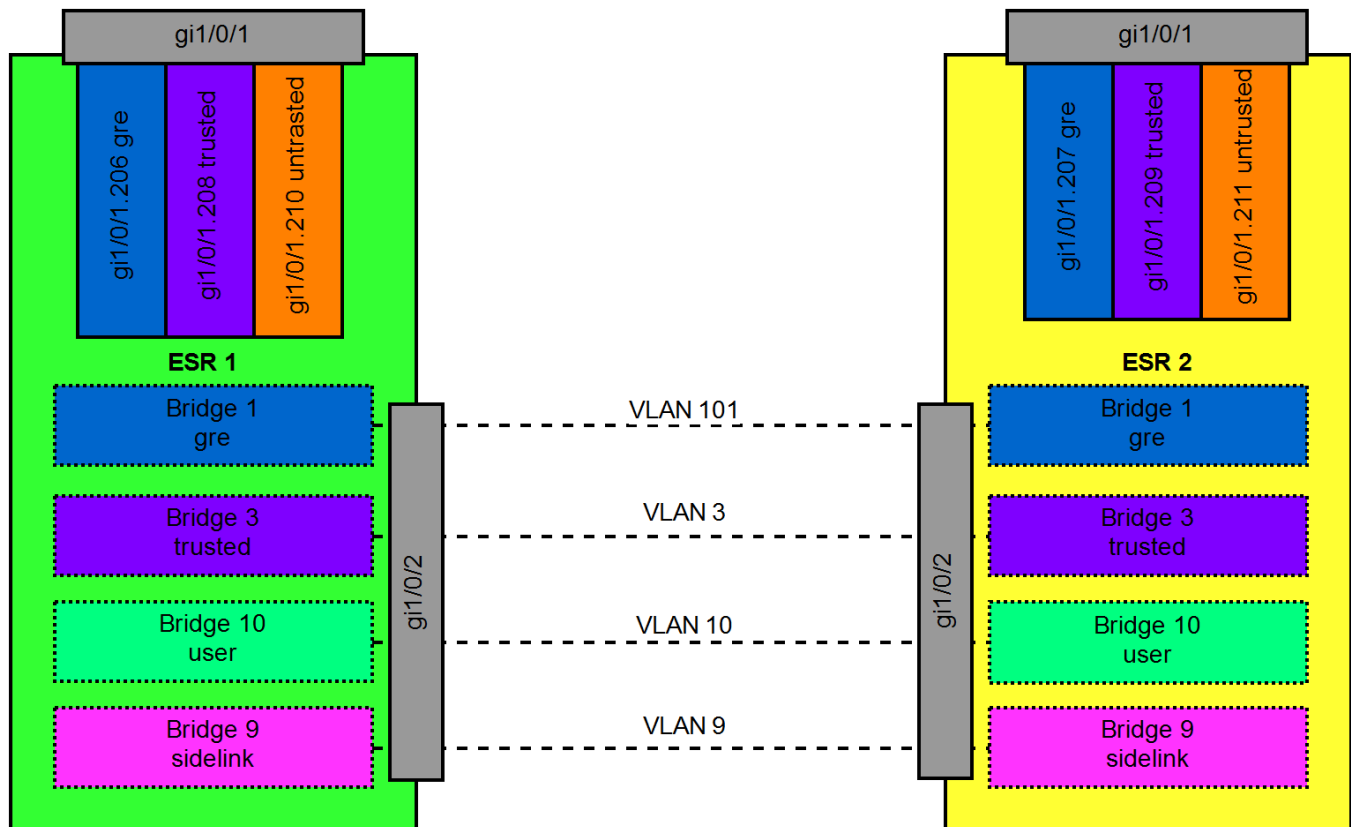
```

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

```

ESR

IP. . . 14 (,).



Обозначение зон безопасности:

	security zone gre
	security zone trusted
	security zone untrusted
	security zone user
	security zone sidelink

. 14.

:

1. trusted self trusted SoftWLC.
2. BGP self .
3. gre GRE ESR.
4. user trusted self DHCP (DNS).

5. user untrusted .
6. user neighbour DNS , (,).
7. neighbour self BGP.
8. neighbour untrusted .

ESR 1 2:

```
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 bgp
  port-range 179
exit
object-group service dns
  port-range 53
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

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 icmp
    enable
  exit
  rule 4
    action permit
    match protocol tcp
    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 5
    action permit
    match source-address SoftWLC
    enable
exit
rule 6
    action permit
    match protocol tcp
    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 udp
        match source-port dhcp_client
        match destination-port dhcp_server
        enable
    exit
    rule 2
        action permit
        match protocol vrrp
        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-port dns
        enable
    exit
exit
security zone-pair trusted user
    rule 1
        action permit
        enable
    exit
exit
security zone-pair trusted untrusted
    rule 1
        action permit
        enable
```

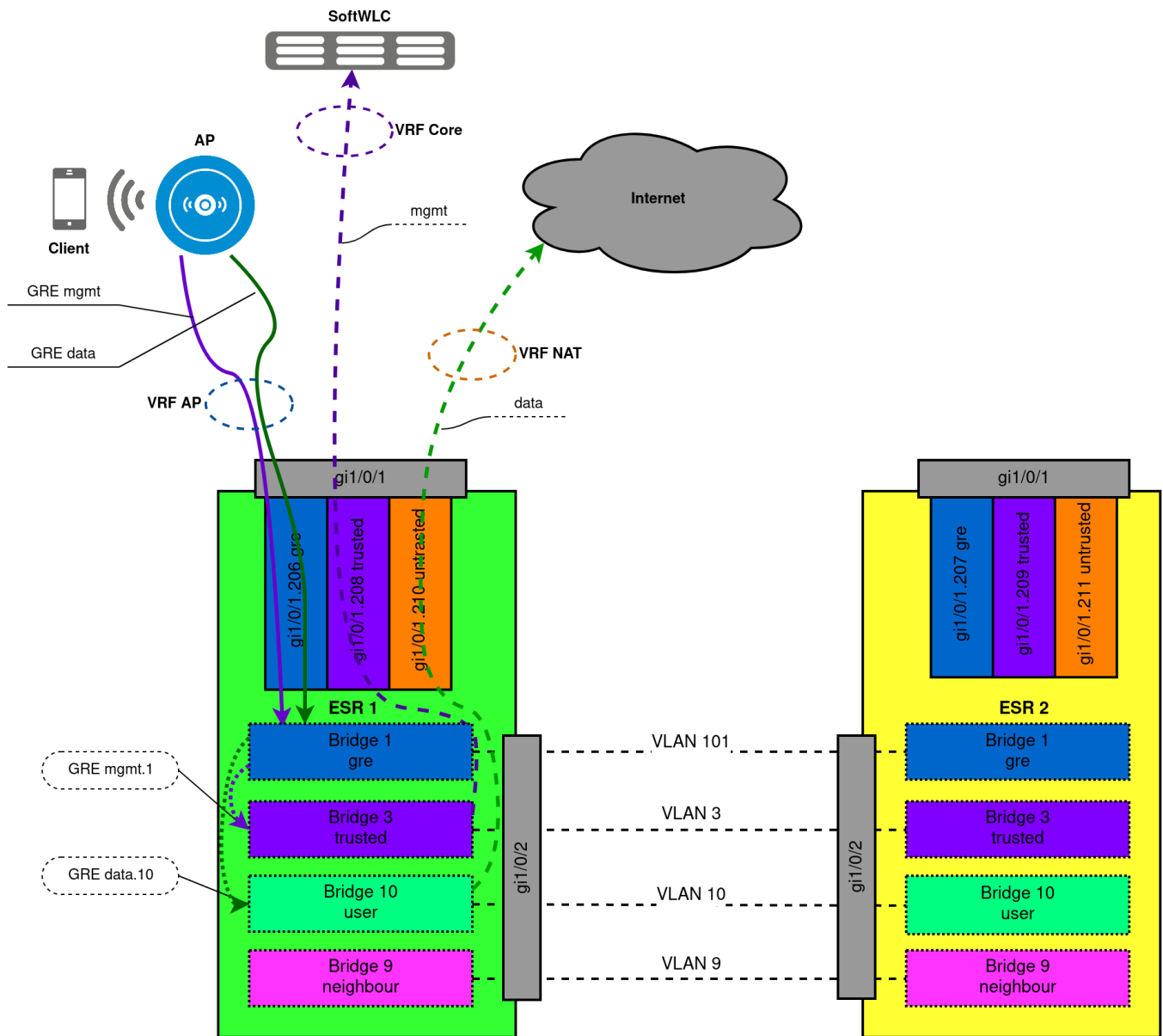
```
    exit
exit
security zone-pair gre gre
    rule 1
        action permit
        enable
    exit
exit
security zone-pair neighbour self
    rule 1
        action permit
        match protocol tcp
        match destination-port bgp
        enable
    exit
    rule 2
        action permit
        match protocol gre
        enable
    exit
    rule 3
        action permit
        match protocol icmp
        enable
    exit
    rule 4
        action permit
        match protocol udp
        match source-port dhcp_server
        match destination-port dhcp_server
        enable
    exit
    rule 5
        action permit
        match protocol udp
        match source-port dhcp_client
        match destination-port dhcp_server
        enable
    exit
    rule 6
        action permit
        match source-address SoftWLC
        enable
    exit
    rule 7
        action permit
        match protocol tcp
        match destination-port telnet
        enable
    exit
    rule 7
        action permit
        match protocol tcp
        match destination-port ssh
        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
        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 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-port dns
        enable
    exit
    rule 10
        action permit
        match not destination-address nets
        enable
    exit
exit
security zone-pair untrusted self
    rule 10
        action permit
        match protocol tcp
        match destination-port bgp
        enable
    exit
exit

```

firewall , no ip firewall disable.



. 15.

ESR **Bridge 3**, **gi1/0/1.208** (ESR 1 Alfa) **gi1/0/1.209** (ESR 2 Beta) VRF core.

, , **gi1/0/1.206** **Bridge1**. GRE :

- MNG GRE – 192.168.200.49 VLAN ID 3;

- DATA GRE – 192.168.200.50, VLAN ID, SSID.

Sub GRE , Bridge:

- **Bridge 3** – L3-, . Default Gateway . DHCP-relay, DHCP , VRF core.

- **Bridge 10** – L3-, SSID1, . Default Gateway Wi-Fi. DHCP-relay, DHCP , VRF core.

gi1/0/1.210 VRF NAT, .

- **Bridge 9** – L3-, ESR. ESR gi1/0/2. (, Port Channel (LACP).

VRRP ESR

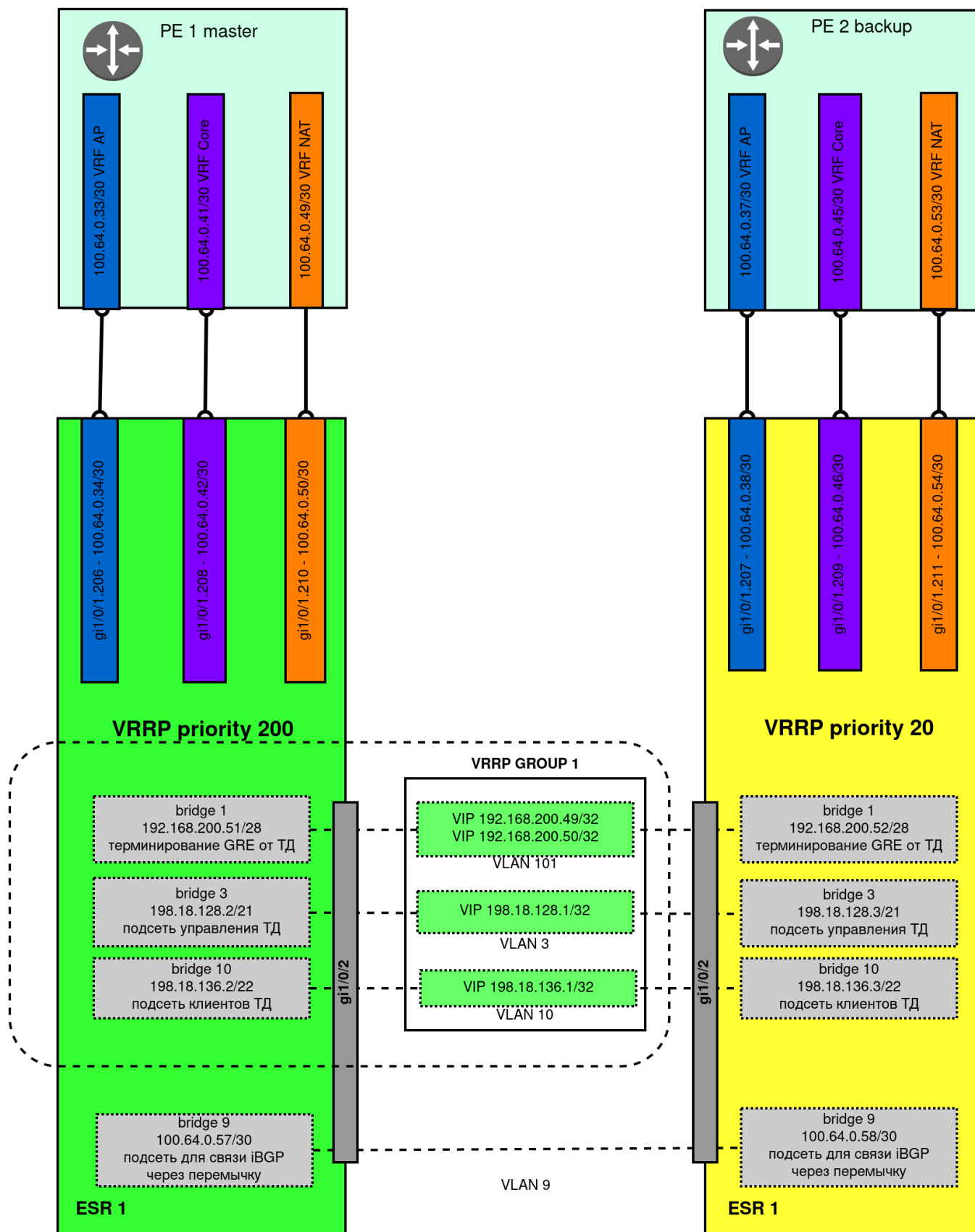
VRRP . 16. Bridge ESR, GRE VRRP, (vrrp group 1). ESR 1 Alfa ESR 2 Beta IP (Real IP) IP (Virtual IP -VIP). bridge vlan, gi1/0/2. ESR 1 Alfa 200, ESR 2 Beta – 20. ESR 1 Alfa vlan (101, 3, 10) – ESR 2 Beta, VIP.

bridge 3 bridge 10 VIP , . , , , IP .

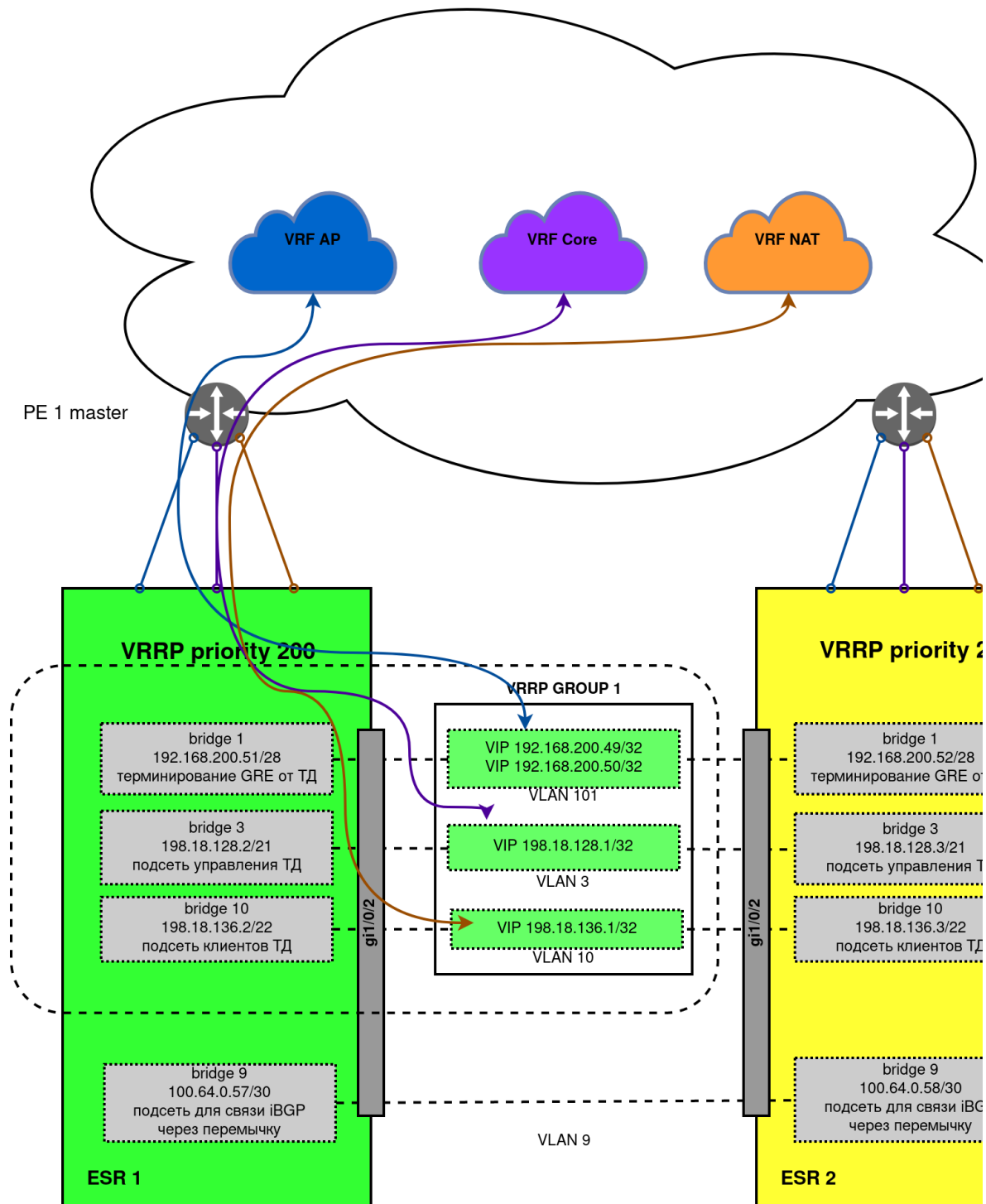
GRE 2 VIP bridge 1 .

bridge 9 . ESR 2 Beta, VRRP backup ESR 1 Alfa, .

, ESR, SoftGRE , IP ESR .

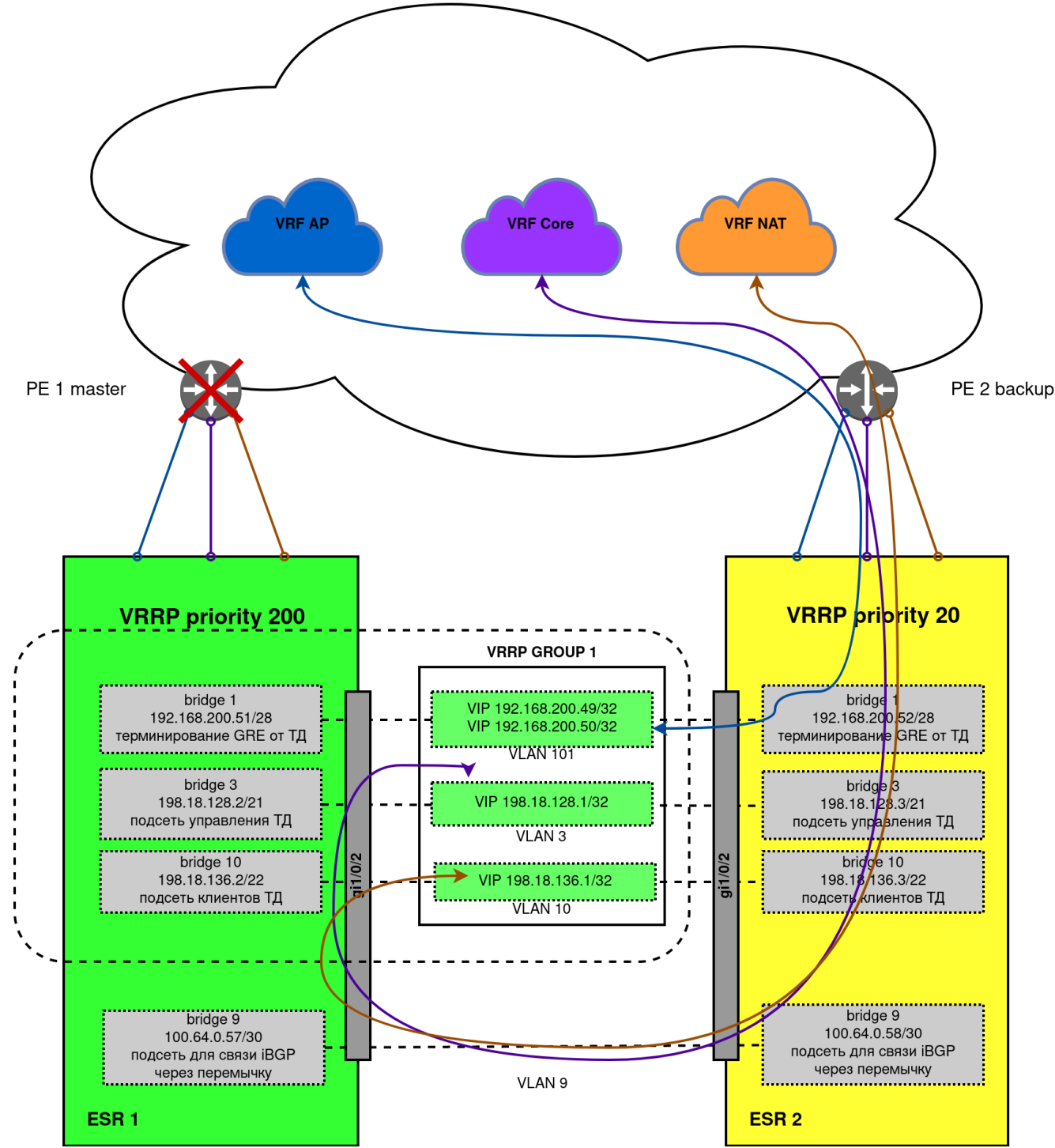


. 17 . VRF AP PE 1 master ESR 1. : VRF core, VRF NAT. PE 2 backup ESR 2 .
Operator network

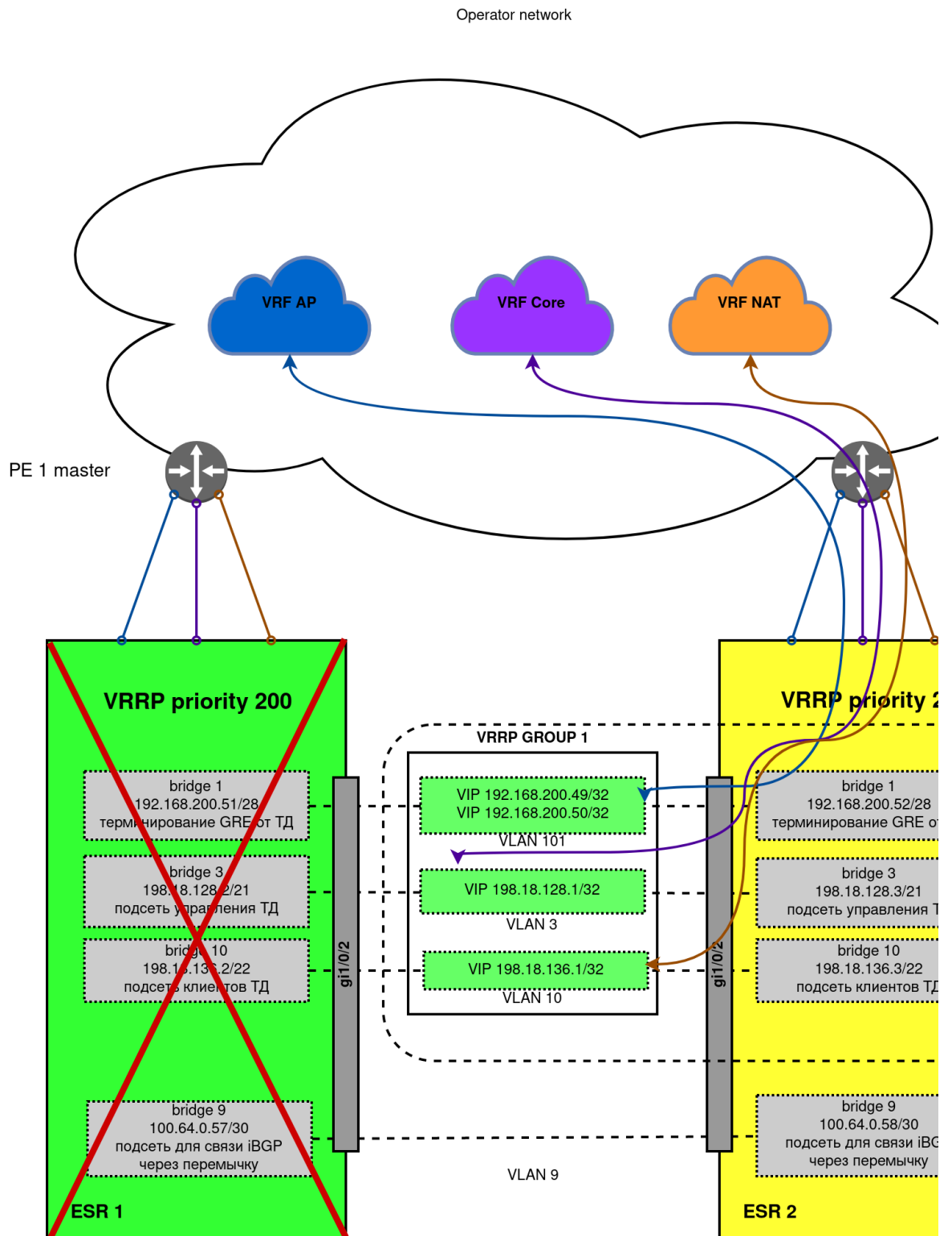


. 17.

PE 1 master



ESR 1



. 19.

ESR 1 VRRP. ESR 2 VRRP MASTER, VIP . VRF AP PE 2 backup ESR 2. : VRF core, VRF NAT. PE 1 master .

ESR 1

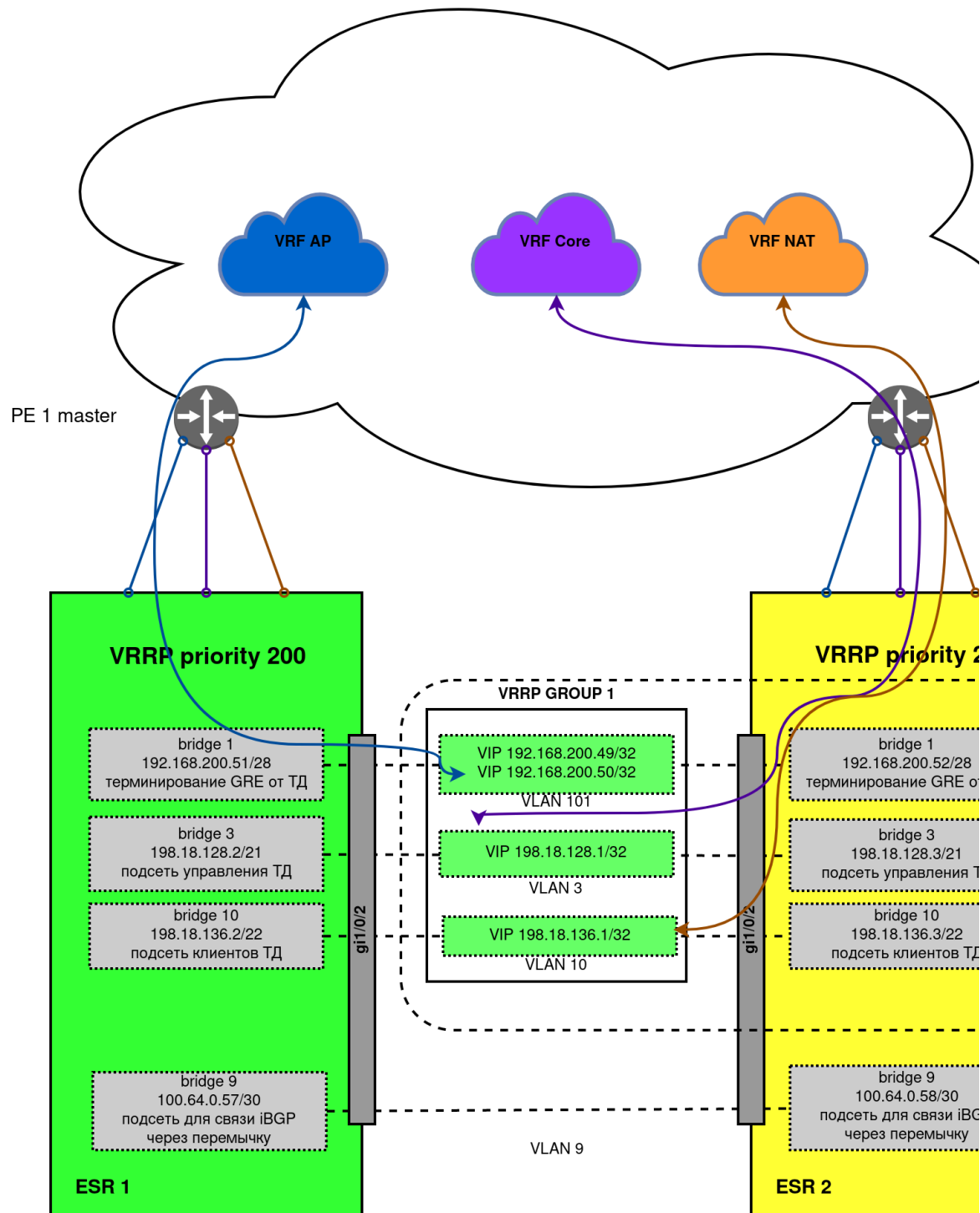
VRRP ESR 1 . ESR 1, VRRP. ,.. ESR 1 . VRRP :

1) vrrp preempt disable - VRRP, VRRP Master . ESR 2 VRRP master ESR 1.

2) vrrp preempt delay <> - VRRP, VRRP Master , . ESR 2 VRRP master . 420 - . VRRP Backup, ESR 1.

, 20, , ESR 1 , ESR 2 VRRP Master.

Operator network



. 20.

VRF AP PE 1 master ESR 1, ESR 2. PE 2 backup VRF.

, BGP VRRP, , : c VRRP+BGP

ESR 1 Alfa ESR 2 Beta

ESR 1.11.0

```
#!/usr/bin/clish
#18
#1.11.x
#07/05/2020
#20:46:29
hostname Alfa

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 bgp
  port-range 179
exit
object-group service dns
  port-range 53
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 100.64.0.56/30
exit
object-group network clients_AP
  ip prefix 198.18.136.0/22
exit
object-group network SoftWLC
  ip prefix 100.123.0.0/24
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

radius-server retransmit 2
radius-server host 100.123.0.2
  key ascii-text encrypted 88B11079B9014FAAF7B9
  timeout 5
  source-address 198.18.128.2
  auth-port 31812
  acct-port 31813
  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
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit
```

```
vlan 3
    force-up
exit
vlan 10
    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 set local-preference 20
        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 180
  vrrp
  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 180
  vrrp
  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 "data_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 180
vrrp
location data10
protected-ports local
protected-ports exclude vlan
ports vrrp filtering enable
ports vrrp filtering exclude vlan
enable
exit

interface gigabitethernet 1/0/1.206
description "VRF_AP"
security-zone gre
ip address 100.64.0.34/30
exit
interface gigabitethernet 1/0/1.208
description "VRF_CORE"
security-zone trusted
ip address 100.64.0.42/30
exit
interface gigabitethernet 1/0/1.210
description "VRF_NAT"
security-zone untrusted
ip address 100.64.0.50/30
exit
interface gigabitethernet 1/0/2
description "neighbour"
mode switchport
switchport general acceptable-frame-type tagged-only
switchport general allowed vlan add 3,9-10,101 tagged
exit
tunnel softgre 1
mode management
local address 192.168.200.49
default-profile
enable
exit
tunnel softgre 1.1
bridge-group 3
enable
exit
tunnel softgre 2
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 icmp
    enable
  exit
  rule 4
    action permit
    match protocol tcp
    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 5
    action permit
    match source-address SoftWLC
    enable
  exit
  rule 6
    action permit
    match protocol tcp
    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 udp
        match source-port dhcp_client
        match destination-port dhcp_server
        enable
    exit
    rule 2
        action permit
        match protocol vrrp
        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-port dns
        enable
    exit
exit
security zone-pair trusted user
    rule 1
        action permit
        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 1
        action permit
        match protocol tcp
        match destination-port bgp
        enable
    exit
    rule 2
        action permit
        match protocol gre
        enable
    exit
    rule 3
        action permit
        match protocol icmp
        enable
    exit
    rule 4
        action permit
        match protocol udp
        match source-port dhcp_server
        match destination-port dhcp_server
```

```
    enable
exit
rule 5
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
exit
rule 6
    action permit
    match source-address SoftWLC
    enable
exit
rule 7
    action permit
    match protocol tcp
    match destination-port ssh
    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
        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 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-port dns
        enable
    exit
```

```
rule 10
  action permit
  match not destination-address nets
  enable
exit
exit
security zone-pair untrusted self
  rule 10
    action permit
    match protocol tcp
    match destination-port bgp
    enable
  exit
exit

wireless-controller
  peer-address 100.64.0.58
  nas-ip-address 198.18.128.2
  vrrp-group 1
  data-tunnel configuration radius
  aaa das-profile COA
  aaa radius-profile PCRF
  enable
exit
ip telnet server
ip ssh server
```

```
#!/usr/bin/clish
#18
#1.11.x
#07/05/2020
#20:46:29
hostname Beta

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 bgp
  port-range 179
exit
object-group service dns
  port-range 53
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 100.64.0.56/30
exit
object-group network clients_AP
  ip prefix 198.18.136.0/22
exit
object-group network SoftWLC
  ip prefix 100.123.0.0/24
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

radius-server retransmit 2
radius-server host 100.123.0.2
  key ascii-text encrypted 88B11079B9014FAAF7B9
  timeout 5
  source-address 198.18.128.3
  auth-port 31812
  acct-port 31813
  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
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit

vlan 3
  force-up
exit
vlan 10
  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 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 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 192.168.200.52/28
vrrp id 1
vrrp ip 192.168.200.49/32
vrrp ip 192.168.200.50/32 secondary
vrrp priority 20
vrrp group 1
vrrp preempt disable
vrrp preempt delay 180
vrrp
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 20
vrrp group 1
vrrp preempt disable
vrrp preempt delay 180
vrrp
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 100.64.0.58/30
enable
exit
bridge 10
description "data_AP"
vlan 10
security-zone user
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 20
vrrp group 1
vrrp preempt disable
vrrp preempt delay 180
vrrp
location data10
protected-ports local
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 address 100.64.0.38/30
exit
interface gigabitethernet 1/0/1.209
description "VRF_CORE"
security-zone trusted
ip address 100.64.0.46/30
exit
interface gigabitethernet 1/0/1.211
```

```
description "VRF_NAT"
security-zone untrusted
ip address 100.64.0.54/30
exit
interface gigabitethernet 1/0/2
description "neighbour"
mode switchport
switchport general acceptable-frame-type tagged-only
switchport general allowed vlan add 3,9-10,101 tagged
exit
tunnel softgre 1
mode management
local address 192.168.200.49
default-profile
enable
exit
tunnel softgre 1.1
bridge-group 3
enable
exit
tunnel softgre 2
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 icmp
enable
exit
rule 4
action permit
match protocol tcp
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 5
    action permit
    match source-address SoftWLC
    enable
exit
rule 6
    action permit
    match protocol tcp
    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 udp
        match source-port dhcp_client
        match destination-port dhcp_server
        enable
    exit
    rule 2
        action permit
        match protocol vrrp
        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-port dns
        enable
    exit
exit
security zone-pair trusted user
    rule 1
        action permit
        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 1
        action permit
        match protocol tcp
        match destination-port bgp
        enable
    exit
    rule 2
        action permit
        match protocol gre
        enable
    exit
    rule 3
        action permit
        match protocol icmp
        enable
    exit
    rule 4
        action permit
        match protocol udp
        match source-port dhcp_server
        match destination-port dhcp_server
        enable
    exit
    rule 5
        action permit
        match protocol udp
        match source-port dhcp_client
        match destination-port dhcp_server
        enable
    exit
    rule 6
        action permit
        match source-address SoftWLC
        enable
    exit
    rule 7
        action permit
        match protocol tcp
        match destination-port ssh
        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
        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 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-port dns
    enable
  exit
  rule 10
    action permit
    match not destination-address nets
    enable
  exit
exit
security zone-pair untrusted self
  rule 10
    action permit
    match protocol tcp
    match destination-port bgp
    enable
  exit
exit

wireless-controller
  peer-address 100.64.0.57
  nas-ip-address 198.18.128.3
  vrrp-group 1
  data-tunnel configuration radius
  aaa das-profile COA
  aaa radius-profile PCRF
  enable
exit
ip telnet server
ip ssh server
```

DHCP

```

default-lease-time 86400;
max-lease-time 87000;

log-facility local7;

class "ELTEX-DEVICES" {
    match if (
        (substring (option vendor-class-identifier, 0, 14)="ELTEX_WEP-12AC") or
        (substring (option vendor-class-identifier, 0, 14)="ELTEX_WOP-12AC") or
        (substring (option vendor-class-identifier, 0, 14)="ELTX_WEP-12AC") or
        (substring (option vendor-class-identifier, 0, 14)="ELTX_WOP-12AC") or
        (substring (option vendor-class-identifier, 0, 13)="ELTEX_WEP-2AC") or
        (substring (option vendor-class-identifier, 0, 12)="ELTEX_WOP-2L") or
        (substring (option vendor-class-identifier, 0, 12)="ELTEX_WEP-2L") or
        (substring (option vendor-class-identifier, 0, 12)="ELTEX_WEP-1L") or
        (substring (option vendor-class-identifier, 0, 6)="ESR-10") or
        (substring (option vendor-class-identifier, 0, 6)="ESR-20")
    );
}

# , DHCP
subnet 100.123.0.0 netmask 255.255.255.0 {}

# , 43 11,12 , GRE
subnet 192.168.250.0 netmask 255.255.255.0 {
    pool {
        allow members of "ELTEX-DEVICES";
        option routers 192.168.250.1;
        range 192.168.250.100 192.168.250.254;
        option vendor-encapsulated-options 0b:0e:31:39:32:2e:31:36:38:2e:32:30:30:2e:34:39:0c:0e:31:39:32:2e:31:36:38:2e:32:30:30:2e:35:30;
    }
}

# , bridge 3 ESR
subnet 198.18.128.0 netmask 255.255.248.0 {
    pool {
        option routers 198.18.128.1;
        range 198.18.128.100 198.18.135.254;
        option vendor-encapsulated-options 0A:0B:31:30:30:2e:31:32:33:2e:30:2e:32;
        allow members of "ELTEX-DEVICES";
        option domain-name-servers 100.123.0.2;
    }
}

# , bridge 10 ESR
subnet 198.18.136.0 netmask 255.255.252.0 {
    pool {
        option routers 198.18.136.1;
        range 198.18.136.10 198.18.139.254;
        option domain-name-servers 100.123.0.2;
    }
}

```