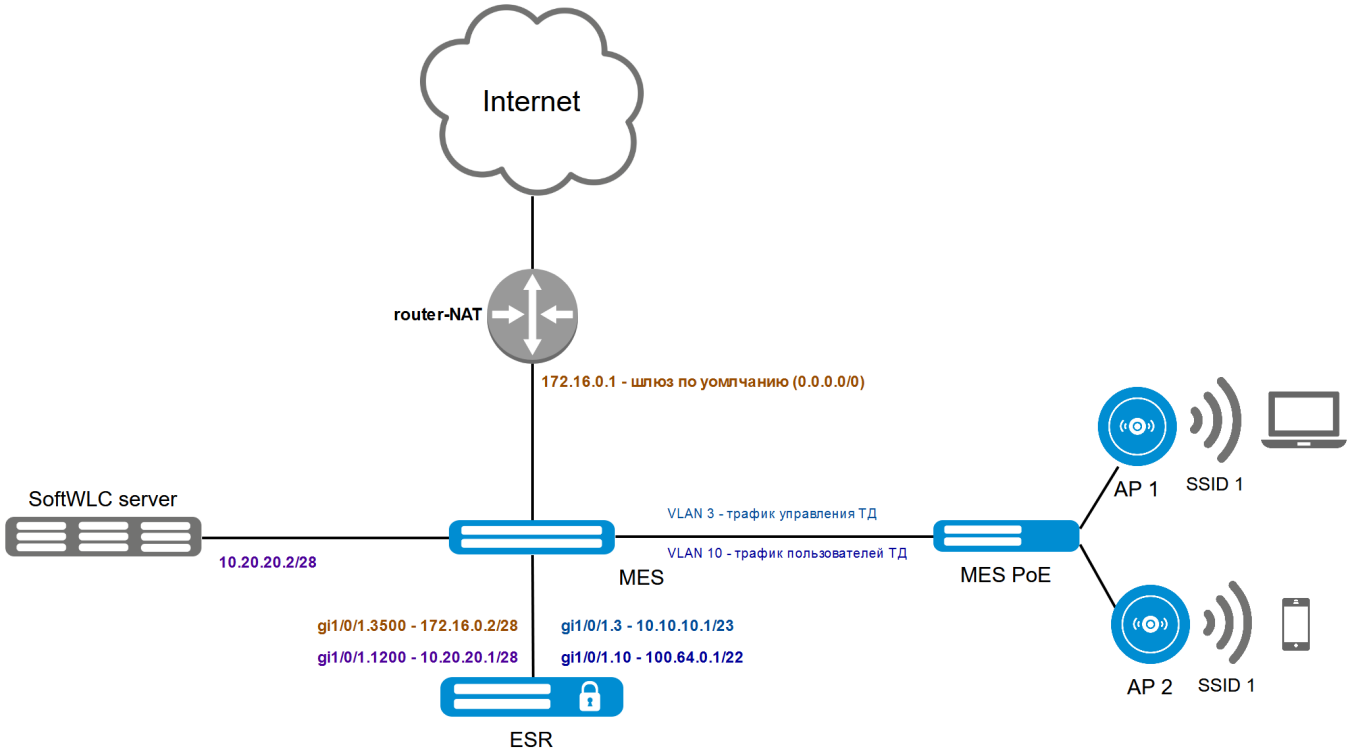
ESR L2 (WiFi L2)

, ( ) L2, , vlan vlan SSID. SSID vlan. vlan ESR. **WiFi L2**. , . 1. , SoftWLC .

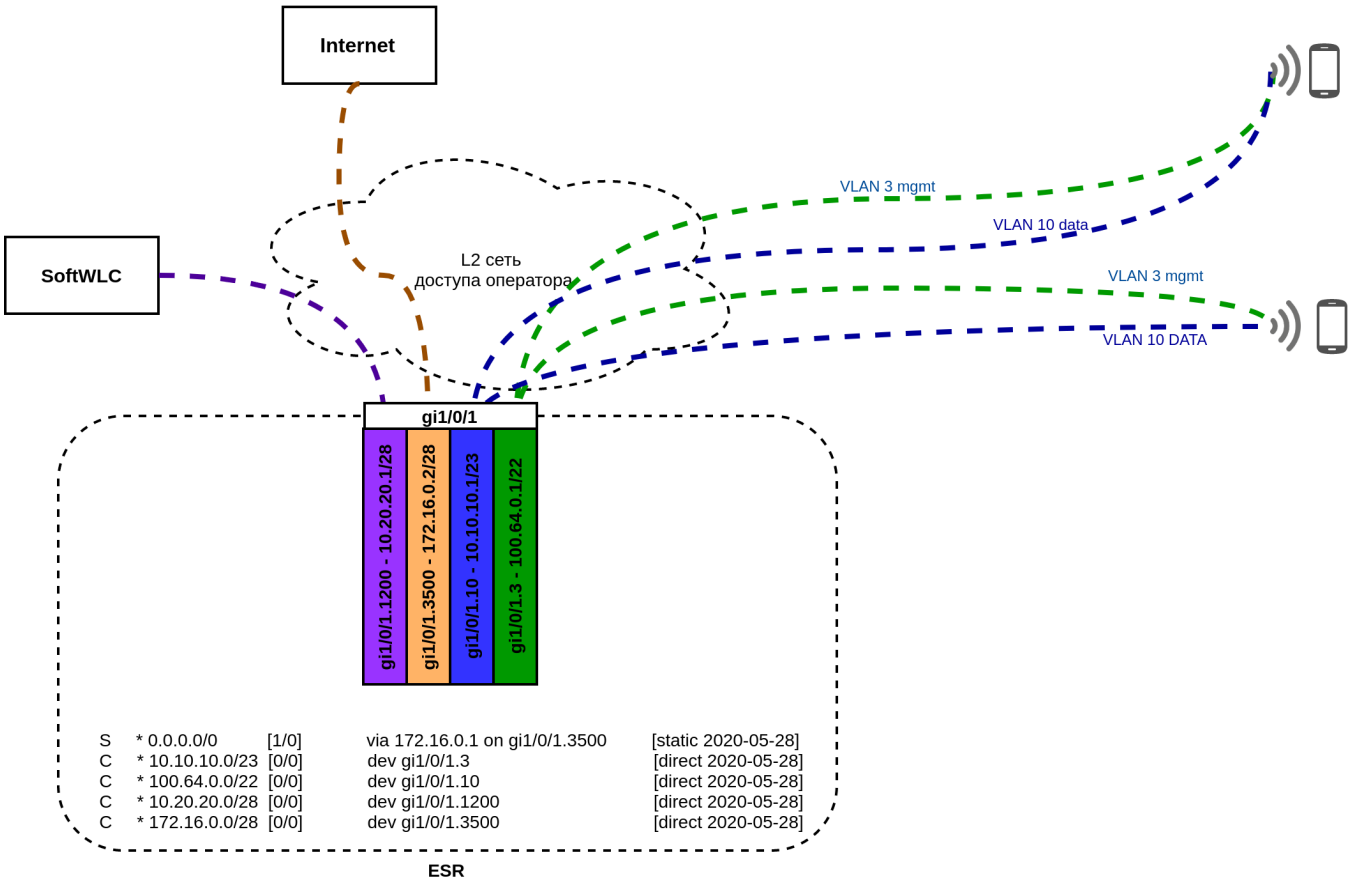


. 1 ( ) L2 .

:

vlan			ESR	SoftWLC
3	10.10.10.0/23		10.10.10.1	
10	100.64.0.0/22	SSID	100.64.0.1	
1200	10.20.20.0/28	SoftWLC	10.20.20.1	10.20.20.2
3500	172.16.0.0/28		172.16.0.2	

, . 2, ESR.



. 2 ESR, L2 .

1. vlan 3500, 172.16.0.1 (router-NAT). router-NAT, NAT .
2. ESR vlan 1200, 10.20.20.0/28, SoftWLC.
3. IP vlan 3 c DHCP , SoftWLC, 10.10.10.0/23. 43, SoftWLC- (. v1.16_ 43 DHCP). vlan-, , vlan ID 3. vlan 3 ESR, - gi1/0/1.3, (10.10.10.1) .
4. SSID, vlan ID 10. SSID 10, , vlan 10 ESR. ESR vlan 10 - gi1/0/1.10, 100.64.0.1 SSID.
5. c vlan 10 ESR. DHCP , DHCP-relay ESR SoftWLC.

vlan. vlan , . MES:

```
interface gigabitethernet1/0/1
 description AP_1
 switchport mode trunk
 switchport trunk allowed vlan add 10
 switchport trunk native vlan 3
 switchport forbidden default-vlan
!
```

ESR

(L2/L3 WiFi -). ESR 1.11.0.

telnet, SSH:

```
ip telnet server
ip ssh server
```

tcp/udp , :

```
object-group service dhcp_server
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group network MGMT
  ip prefix 10.10.10.0/23
  ip prefix 10.20.20.0/28
exit
```

ESR10/20/100/200/1000 spanning-tree, . . :

```
no spanning-tree
```

:

```
security zone trusted
exit
security zone untrusted
exit
security zone user
exit
```

SNMP, SoftWLC:

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

snmp-server host 10.20.20.2
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 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 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
```

SSID , SoftWLC, :

```
interface gigabitethernet 1/0/1.3
  description "AP_MANAGMENT"
  security-zone trusted
  ip address 10.10.10.1/23
  ip helper-address 10.20.20.2
exit
interface gigabitethernet 1/0/1.10
  description "AP_SSID_USERS"
  security-zone user
  ip address 100.64.0.1/22
  ip helper-address 10.20.20.2
exit
interface gigabitethernet 1/0/1.1200
  description "MANAGMENT"
  security-zone trusted
  ip address 10.20.20.1/28
exit
interface gigabitethernet 1/0/1.3500
  description "INTERNET"
  security-zone untrusted
  ip address 172.16.0.2/28
exit
```

DHCP :

```
ip dhcp-relay
```

:

```
ip route 0.0.0.0/0 172.16.0.1
```

:

```
#        MGMT:
security zone-pair trusted self
  rule 1
    action permit
    match source-address MGMT
    enable
  exit
exit

#     trusted    :
security zone-pair trusted trusted
  rule 1
    action permit
    match source-address MGMT
    enable
  exit
exit

#      trusted   :
security zone-pair trusted user
  rule 1
    action permit
    enable
  exit
exi

#      DHCP,      :
security zone-pair user self
  rule 1
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
exit

#   ,   DHCP:
security zone-pair user trusted
  rule 1
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
exit

#       :
security zone-pair user untrusted
  rule 1
    action permit
    enable
  exit
exit
```

ESR

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

object-group service dhcp_server
  port-range 67
exit
```

```
object-group service dhcp_client
  port-range 68
exit

object-group network MGMT
  ip prefix 10.10.10.0/23
  ip prefix 10.20.20.0/28
exit

no spanning-tree

security zone trusted
exit
security zone untrusted
exit
security zone user
exit


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

snmp-server host 10.20.20.2
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 ports
snmp-server enable traps ports port-counters-errors
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

interface gigabitethernet 1/0/1.3
  description "AP_MANAGMENT"
  security-zone trusted
  ip address 10.10.10.1/23
  ip helper-address 10.20.20.2
exit
interface gigabitethernet 1/0/1.10
  description "AP_SSID_USERS"
  security-zone user
  ip address 100.64.0.1/22
  ip helper-address 10.20.20.2
exit
interface gigabitethernet 1/0/1.1200
  description "MANAGMENT"
  security-zone trusted
  ip address 10.20.20.1/28
exit
interface gigabitethernet 1/0/1.3500
  description "INTERNET"
  security-zone untrusted
  ip address 172.16.0.2/28
exit
security zone-pair trusted self
  rule 1
    action permit
    match source-address MGMT
    enable
  exit
exit
security zone-pair trusted trusted
  rule 1
    action permit
```

```
    match source-address MGMT
    enable
  exit
exit
security zone-pair trusted user
  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
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
exit
security zone-pair user untrusted
  rule 1
    action permit
    enable
  exit
exit


ip dhcp-relay

ip route 0.0.0.0/0 172.16.0.1

ip telnet server
ip ssh server
```

DHCP

DHCP , . DHCP ISC-DHCP-SERVER.

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

log-facility local7;

#listening subnet
subnet 10.20.20.0 netmask 255.255.255.240 {}

#  ,
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")
        );
}

#    vlan 3
subnet 10.10.10.0 netmask 255.255.254.0 {
        pool {
                option routers 10.10.10.1;
                range 10.10.10.2 10.10.11.254;
                option vendor-encapsulated-options 0A:0A:31:30:2e:32:30:2e:32:30:2e:32;
                allow members of "ELTEX-DEVICES";
                option domain-name-servers 172.16.0.254;
        }
}

#   SSID vlan 10
subnet 100.64.0.0 netmask 255.255.252.0 {
        default-lease-time 3600;
        max-lease-time 3700;
        pool {
                option routers 100.64.0.1;
                range 10.64.0.2 100.64.3.254;
                option domain-name-servers 172.16.0.254;
        }
}
```

NAT ESR

- NAT ESR. :

```
object-group network nat
  ip prefix 100.64.0.0/22
exit

nat source
  ruleset NAT
    to zone untrusted
    rule 1
      match source-address nat
      action source-nat interface
      enable
    exit
  exit
exit
```

Bridge

- vlan SSID, vlan . , vlan "Bridge". "Bridge", -, vlan . , vlan 10 11:

```
#   -   vlan 10
no interface gigabitethernet 1/0/1.10

#   "Bridge"
bridge 10
  description "AP_SSID_USERS"
  security-zone user
  ip address 100.64.0.1/22
  ip helper-address 10.20.20.2
  protected-ports local
  enable
exit

interface gigabitethernet 1/0/1.10
  bridge-group 10
exit
interface gigabitethernet 1/0/1.11
  bridge-group 10
exit
```