1.6.2 ESR 1.4.1 1.6.2

clish

, ftp/tftp clish, 1.6.2 14.

```
#!/usr/bin/clish
#14
```

, running-config candidate-config: show configuration changes.

```
esr1000# show configuration changes
bridge 1
- vlan 3500
- mac-address a8:f9:4b:aa:23:b2
- security-zone untrusted
- ip address 192.168.48.52/20
- ip helper-address vrrp-group 1
- vrrp id 35
- vrrp ip 192.168.48.55/32
+ vlan 2308
+ security-zone GRE
+ ip address 192.168.200.19/28
+ vrrp id 1
+ vrrp ip 192.168.200.17/32
+ vrrp ip 192.168.200.18/32 secondary
- protected-ports
- protected-ports exclude vlan
- ports vrrp filtering enable
- ports vrrp filtering exclude vlan
```

"+" , candidate-config running-config. "-" , candidate-config, running-config.

BGP

, (route-map, prefix-list) (RIP, OSPF, BGP). .

:

- Route-map (in)
- Prefix-list (in)
- Route-map (in) + Prefix-list (in)
- Redistribute + route-map

, , , .

:

1) IGP - , ;

2) EGP - .

:

- Route-map (out)
- Prefix-list (out)
- Route-map (out) + Prefix-list (out)

iBGP . .

eBGP . .

BGP ESR :

```
router bgp 65252
  address-family ipv4
     router-id 10.203.195.153
     neighbor 10.203.195.129
      remote-as 65001
      prefix-list AP_GRE out
      route-map INPREF in
      route-map OUTPREFGRE out
      enable
    exit
    neighbor 10.203.195.137
      remote-as 65001
      prefix-list MNG out
      route-map INPREF in
      route-map OUTPREFMNG out
      enable
    exit
    neighbor 10.203.195.145
      remote-as 65001
      prefix-list INTERNET out
      route-map INPREF in
      enable
    exit
    neighbor 10.203.195.154
      remote-as 65252
      next-hop-self
     enable
    exit
    enable
  exit
exit
```

BGP redistribute connected, connected BGP. (, OSPF, RIP, static BGP) - redistribute.

:

```
router bgp 65252
  address-family ipv4
    router-id 10.203.195.153
    redistribute connected              #
    neighbor 10.203.195.129
      remote-as 65001
      prefix-list AP_GRE out
      route-map INPREF in
      route-map OUTPREFGRE out
      enable
    exit
    neighbor 10.203.195.137
      remote-as 65001
      prefix-list MNG out
      route-map INPREF in
      route-map OUTPREFMNG out
      enable
    exit
    neighbor 10.203.195.145
      remote-as 65001
      prefix-list INTERNET out
      route-map INPREF in
      enable
    exit
    neighbor 10.203.195.154
      remote-as 65252
      next-hop-self
      enable
    exit
    enable
  exit
exit
```

1.4.1, 1.6.2, .. ESR connected eBGP .

.

port-channel

- routerport - L3
- switchport - L2
- hybrid - L2+L3

mode switchport :

backup	*Configure interface as part of dual homing pair*
port-security	*Configure port security parameters*
spanning-tree	*Configure Spanning Tree Subsystem*
switchport	*Configure switch port parameters*
bridge-group	*Add interface to bridge*
port	*Perform switch port configuration*
switchport	*Configure switch port parameters*
threshold	*Configure alarms thresholds parameters*
channel-group	*Add interface to port channel*
lacp	*Configure interface IEEE 802.3 link aggregation parameters*

mode routerport ( ):

ip	*Configure IP interface parameters*
ipv6	*Configure IPv6 interface parameters*
subscriber-control	*Configure subscriber control parameters*
service-subscriber-control	*Enable a subscriber control service policy on the interface*
vrrp	*Enable VRRP on interface*
wan	*Configure WAN*

ESR low (ESR-10, ESR-12v, ESR-100, ESR-200) routerport/switchport. ESR middle (ESR-1000, ESR-1200, ESR-1700) . 1.6.0 , . :

```
interface gigabitethernet 1/0/1
  ip firewall disable
  switchport access vlan 2
exit
interface gigabitethernet 1/0/1.1000
  ip address dhcp
  ip firewall disable
  ip dhcp client ignore router
exit
```

:

```
interface gigabitethernet 1/0/1
  switchport access vlan 2
exit
```

- gigabitethernet 1/0/1.1000 .

, "any" , . 1.4.1 1.6.2 .

, 1.4.1 :

```
security zone-pair trusted trusted
  rule 1
    action permit
    match protocol any
    match source-address any
    match destination-address any
    enable
  exit
exit
```

1.6.2 :

```
security zone-pair trusted trusted
  rule 1
    action permit
    enable
  exit
exit
```

, "any" . 1.4.1 1.6.2 .

admin, root, techsupport.

admin, root, techsupport . 8 32 .

factory-config admin:

```
esr-10 login: admin
Password:
You are required to change your password immediately!!!


****************************************

*            Welcome to ESR-1000            *

****************************************


esr-1000(change-expired-password)#
esr-1000(change-expired-password)# password
  encrypted   Configure user's password sha512
  WORD(8-32)  User's password

esr-1000(change-expired-password)# password 12345678
esr-1000(change-expired-password)# commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes will be
reverted in 600 seconds.
2019-04-23T09:00:02+00:00 %CLI-I-CRIT: user admin from console  input: commit
esr-1000(change-expired-password)# confirm
Configuration has been confirmed. Commit timer canceled.
2019-04-23T09:00:05+00:00 %CLI-I-CRIT: user admin from console  input: confirm
esr-1000#
```

techsupport, root :

```
esr-1000# config
esr-1000(config)# root login enable
error - check root-enable: Couldn't enable root user - default password is set. Change the password and try
again
esr-1000(config)# tech-support login enable
error - check techsupport-enable: Couldn't enable techsupport user - default password is set. Change the
password and try again
esr-1000(config)# username root
esr-1000(config-user)# password 12345678
esr-1000(config-user)# exit
esr-1000(config)# username techsupport
esr-1000(config-user)# password 12345678
esr-1000(config-user)# exit
esr-1000(config)# root login enable
esr-1000(config)# tech-support login enable
esr-1000(config)# exit
esr-1000# comm
Configuration has been successfully applied and saved to flash. Commit timer started, changes will be
reverted in 600 seconds.
2019-04-23T09:02:49+00:00 %CLI-I-CRIT: user admin from console  input: commit
esr-1000# confirm
Configuration has been confirmed. Commit timer canceled.
2019-04-23T09:02:52+00:00 %CLI-I-CRIT: user admin from console  input: confirm
esr-1000#
```

security passwords history. 1 15. . 1.6.2 1, *no security passwords history*. ,

```
esr-1000(config)# security passwords history 0
```

1.4.1, , security passwords history 0. , tftp, .. , ESR security passwords history , .

, ESR-10, OTT EMS: "Wireless" " " "OTT .".

child SA IPsec VPN

child SA IPsec VPN. :

show security ipsec vpn authentication vrf < IPSEC VPN> show security ipsec vpn authentication vrf < VRF> < IPSEC VPN> . VRF , , VRF IPsec VPN.

```
1700-ipsec# show security ipsec vpn authentication vrf ipsec1 XAUTH_IPSEC_VPN

Local host        Remote host       Local subnet          Remote
subnet         Authentication                              State

---------------   ---------------   -------------------   -------------------   ------------------------------
------------   -----------

10.12.20.3        192.168.255.19    192.168.200.32/28     172.31.0.1/32         Xauth PSK, login: a8:f9:4b:
ac:97:5b         Established

10.12.20.3        192.168.255.40    192.168.200.32/28     172.31.0.2/32         Xauth PSK, login: e0:d9:e3:
50:71:e0         Established

10.12.20.3        192.168.255.4     192.168.200.32/28     172.31.0.3/32         Xauth PSK, login: e0:d9:e3:
70:59:20         Established
```

:

1) IP (nat - "" IP, nat), Remote host;

2) mode-cfg - Remote subnet;

3) XAUTH - Authentication. authentication method pre-shared-key rsa-public-key .

child SA - Local subnet/Remote subnet no child SA. , .

```
1700-ipsec# show security ipsec vpn authentication vrf ipsec1 XAUTH_IPSEC_VPN

Local host        Remote host       Local subnet          Remote
subnet         Authentication                              State

---------------   ---------------   -------------------   -------------------   ------------------------------
------------   -----------

10.12.20.3        192.168.255.19    no child SA           no child SA           Xauth PSK, login: a8:f9:4b:
ac:97:5b         Established

10.12.20.3        192.168.255.40    192.168.200.32/28     172.31.0.2/32         Xauth PSK, login: e0:d9:e3:
50:71:e0         Established

10.12.20.3        192.168.255.4     192.168.200.32/28     172.31.0.3/32         Xauth PSK, login: e0:d9:e3:
70:59:20         Established
```

ESR10-OTT-BR-2# show security ipsec vpn authentication ipsec_vpn

Local host Remote host Local subnet Remote subnet Authentication State

--- --- --- --- --- ---

192.168.255.19 10.12.20.3 172.31.0.1/32 192.168.200.32/28 Xauth PSK, login: a8:f9:4b:ac:97:5b Established

Ansible

Ansible SFTP. , SFTP ESR : *ip sftp enable*

:

```
username sftp
  password password
  ip sftp enable
exit
```

, *ip sftp enable* radius/tacacs .

: ESR Ansible

SNMP - source-address source-interface

SNMP source-address source-interface. SNMP . , source-address source-interface . :

source-address:

```
snmp-server host 100.123.0.2
  source-address 100.123.0.174
exit
```

source-interface:

```
snmp-server host 100.123.0.2
  source-interface bridge 23
exit
```

SNMP - , .

. 1.6.2 . , . 1.4.1 .

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

snmp-server host 100.123.0.2
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-dp-critical-temp
snmp-server enable traps environment cpu-dp-overheat-temp
snmp-server enable traps environment cpu-dp-supercooling-temp
snmp-server enable traps environment cpu-mgmt-critical-temp
snmp-server enable traps environment cpu-mgmt-overheat-temp
snmp-server enable traps environment cpu-mgmt-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 - ,

, BRIDGE, ESR1000/1200/1700.

```
bridge <>
rate-limit arp-broadcast                              #        .
rate-limit arp-broadcast pps <>  #          .    100,    1-65535.
```

bridge softgre, - , arp- . , - ( ), CPU , arp .

rate-limit arp-broadcast , . , . , 100. rate-limit arp-broadcast pps 1-65535. bridge.

? , bridge 250 softgre. , , softgre, 1000 . , -, -, (1000), 250 softgre-, , , 250000 , softgre 1000 . , , 100 , 100 , 900 . , 25000 , softgre 100 , .

EoGRE

EoGRE, wireless-controller, : clear tunnels softgre all. debug:

```
esr1000(debug)# clear tunnels softgre all
```

EoGRE . , . VRRP - EoGRE VRRP MASTER, VRRP BACKUP , .. VRRP MASTER, .

ESR1200/1700 - FBD

ESR1200/1700 FBD. debug:

```
esr1700(debug)#
```

ESR syslog monitor debug (syslog console debug,).

:

```
esr1700(debug)# show mac status
2019-06-19T17:58:30+07:00 %SW-D-DBG: FDB size: 131072
2019-06-19T17:58:30+07:00 %SW-D-DBG: FDB used entries: 12 (static 1/dynamic 11)
2019-06-19T17:58:30+07:00 %SW-D-DBG: FDB free entries: 131060
2019-06-19T17:58:30+07:00 %SW-D-DBG: Hash chain length: 4
2019-06-19T17:58:30+07:00 %SW-D-DBG: FDB hash function: crc
2019-06-19T17:58:30+07:00 %SW-D-DBG: Aging time: 300 seconds
2019-06-19T17:58:30+07:00 %SW-D-DBG: VLAN Lookup mode: Independent VLAN Learning
2019-06-19T17:58:30+07:00 %SW-D-DBG: Global configuration for FID 16 bits: disable
2019-06-19T17:58:30+07:00 %SW-D-DBG: Address update queue: no full 0 end 0
2019-06-19T17:58:30+07:00 %SW-D-DBG: FDB upload queue: no full 0 end 0
2019-06-19T17:58:30+07:00 %SW-D-DBG: Sending NA messages to the CPU (bucket is full): disable
```

Downgrade ESR 1.6.2 1.4.1

1.6.2 1.4.1.

!!! 1.6.2 , 1.6.2 (IPsec XAUTH , source-interface wireless-controller, radius, snmp, QoS) - .

1) , , image:

```
Beta-1700# copy tftp://100.110.0.150:/esr1700-1.4.1-build185.firmware system:firmware
|****************************************| 100% (81286kB) Firmware updated successfully.
Beta-1700#
```

2) debug downgrade configuration 1.4.1:

```
Beta-1700# debug
Beta-1700(debug)# downgrade
  configuration  Downgrade configuration version
Beta-1700(debug)# downgrade configuration 1.4.1
Configuration has been successful downgraded!
Beta-1700(debug)# exit
```

3) image 1.4.1:

```
Beta-1700# sh bootvar
Image   Version                     Date                   Status         After reboot
-----   -------------------------   --------------------   ------------   ------------
1       1.4.1 build 185[1665ee7]    date 19/11/2018 time   Not Active
                                    14:52:03

2       1.6.x build 47[b72537e9]    date 12/04/2019 time   Active         *
                                    11:02:37

Beta-1700# boot system image-1
Do you really want to set boot system image? (y/N): y
Beta-1700# sh bootvar
Image   Version                     Date                   Status         After reboot
-----   -------------------------   --------------------   ------------   ------------
1       1.4.1 build 185[1665ee7]    date 19/11/2018 time   Not Active     *
                                    14:52:03

2       1.6.x build 47[b72537e9]    date 12/04/2019 time   Active
                                    11:02:37
```

4) ESR：

```
Beta-1700# reload system
Do you really want to reload system ? (y/N): y
Beta-1700# Connection closed by foreign host.
```