



ESR Series Routers

**ESR-10, ESR-12V, ESR-12VF, ESR-14VF, ESR-100,
ESR-200, ESR-1000, ESR-1200, ESR-1700**

Operation Manual

Firmware Version 1.4.4

Document version	Issue date	Revisions
Version 1.14	31 January 2019	Changes in sections: <ul style="list-style-type: none"> - 7.31 Configuring remote access client via PPPoE - 7.32 Configuring remote access client via PPTP - 7.33 Configuring remote access client via L2TP
Version 1.13	11 November 2018	Synchronization with firmware version 1.4.1
Version 1.12	17 April 2018	Synchronization with firmware version 1.4.0
Version 1.11	20 December 2017	Synchronization with firmware version 1.3.0
Version 1.10	4 September 2017	Synchronization with firmware version 1.2.1
Version 1.9	3 May 2017	Chapters added: <ul style="list-style-type: none"> - 7.19.2 Policy-based IPsec VPN configuration - 7.35 BRAS (Broadband Remote Access Server) configuration Changes in sections: <ul style="list-style-type: none"> - 2.3 Main specifications - 2.4 Design - 2.5 Delivery package - 3.3 ESR-1000, ESR-1200 power module installation - 5.1 ESR router factory settings
Version 1.8	14 December 2016	Chapters added: <ul style="list-style-type: none"> - 7.2 Q-in-Q termination configuration - 7.20 LT-tunnels configuration - 7.31 VRRP tracking configuration
Version 1.7	3 March 2016	Chapters added: <ul style="list-style-type: none"> - 8 FAQ
Version 1.6	24 February 2016	Chapters added: <ul style="list-style-type: none"> - 7.15.1 Configuring Route-map for BGP - 7.21 Configuring remote access to corporate network via OpenVPN protocol - 7.31 SNMP configuration Changes in sections: <ul style="list-style-type: none"> - 7.15 PBR routing policy configuration - 7.19 Configuring remote access to corporate network via PPTP protocol
Version 1.5	6 August 2015	Added description for ESR-100, ESR-200 Chapters added: <ul style="list-style-type: none"> - 2.4.2 ESR-100, ESR-200 design Changes in sections: <ul style="list-style-type: none"> - 2.4 Design - 2.5 Delivery package - 3 Installation and connection - 7.1 VLAN configuration - 7.6 Source NAT configuration - 7.16 L2TPv3 tunnel configuration - 7.24 Netflow configuration - 7.25 sFlow configuration - 7.26 LACP configuration
Version 1.4	9 June 2015	Chapters added: <ul style="list-style-type: none"> - 6.1 AAA configuration - 6.1 User privileges configuration - 6.7 Access list (ACL) configuration - 6.9 MLPPP configuration - 6.14 Route-map configuration - 6.21.2 Advanced QoS - 6.24 VRF Lite configuration Changes in sections: <ul style="list-style-type: none"> - 2.4.4 Light indication

Version 1.3	5 March 2015	<p>Chapters added:</p> <ul style="list-style-type: none"> - 6.15 Dual-Homing configuration - 6.16 QoS configuration - 6.17 Mirroring configuration - 6.18 VRRP configuration - 6.19 MultiWAN configuration <p>Changes in sections:</p> <ul style="list-style-type: none"> - 6.4 Firewall configuration - 6.5 Static routes configuration - 6.6 Bridge configuration - 6.7 RIP configuration - 6.8 OSPF configuration - 6.9 BGP configuration - 6.10 GRE tunnel configuration - 6.11 L2TPv3 tunnel configuration - 6.12 Route-based IPsec VPN configuration - 6.13 Configuring remote access to corporate network via PPTP protocol - 6.14 Configuring remote access to corporate network via L2TP/IPsec protocol - 7.1 Updating firmware via system resources - 7.2 Updating firmware via bootloader
Version 1.2	2 December 2014	<p>Chapters added:</p> <ul style="list-style-type: none"> - 6.6 Bridge configuration - 6.7 RIP configuration - 6.8 OSPF configuration - 6.9 BGP configuration - 6.10 L3 tunnel (GRE) configuration - 6.11 L2TPv3 tunnel (L2TPv3) configuration
Version 1.1	3 June 2014	<p>Chapters added:</p> <ul style="list-style-type: none"> - 6 Router configuration
Version 1.0	25 April 2014	First issue.
Firmware version	1.4.4	

CONTENTS

1	INTRODUCTION.....	9
1.1	Abstract.....	9
1.2	Target Audience.....	9
1.3	Symbols.....	9
2	PRODUCT DESCRIPTION.....	10
2.1	Purpose.....	10
2.2	Functions.....	10
2.2.1	Interface functions.....	10
2.2.2	Functions for MAC address processing.....	10
2.2.3	Second-layer functions of OSI model.....	11
2.2.4	Third-layer functions of OSI model.....	11
2.2.5	Traffic tunnelling functions.....	12
2.2.6	Management and configuration functions.....	12
2.2.7	Network security functions.....	13
2.3	Main specifications.....	13
2.4	Design.....	16
2.4.1	ESR-1700 design.....	16
2.4.2	ESR-1000, ESR-1200 design.....	18
2.4.3	ESR-100, ESR-200 design.....	21
2.4.4	ESR-12VF, ESR-14VF design.....	23
2.4.5	ESR-12V design.....	25
2.4.6	ESR-10 design.....	27
2.4.7	Light Indication.....	28
2.5	Delivery Package.....	32
3	INSTALLATION AND CONNECTION.....	34
3.1	Support brackets mounting.....	34
3.2	Device rack installation.....	35
3.3	ESR-1000, ESR-1200, ESR-1700 power module installation.....	36
3.4	Connection to Power Supply.....	36
3.5	SFP transceiver installation and removal.....	37
3.5.1	Transceiver installation.....	37
3.5.2	Transceiver removal.....	37
4	MANAGEMENT INTERFACES.....	38
4.1	Command line interface (CLI).....	38
4.2	Types and naming procedure of router interfaces.....	38
4.3	Types and naming procedure of router tunnels.....	40
5	INITIAL ROUTER CONFIGURATION.....	41
5.1	ESR router factory settings.....	41
5.1.1	Description of factory settings.....	41
5.2	Router connection and configuration.....	42
5.2.1	Connection to the router.....	42
5.2.2	Applying the configuration change.....	43
5.2.3	Basic router configuration.....	43
6	FIRMWARE UPDATE.....	47
6.1	Updating firmware via system resources.....	47
6.2	Updating firmware via bootloader.....	48

6.3	Secondary bootloader update (U-Boot)	49
7	ROUTER CONFIGURATION EXAMPLES.....	51
7.1	VLAN Configuration.....	51
7.1.1	Configuration algorithm	51
7.1.2	Configuration example 1. VLAN removal from the interface.....	52
7.1.3	Configuration example 2. Enabling VLAN processing in tagged mode	52
7.1.4	Configuration example 3. Enabling VLAN processing in tagged and untagged modes	53
7.2	LLDP configuration	53
7.2.1	Configuration algorithm	54
7.2.2	Configuration example	54
7.3	LLDP MED configuration	55
7.3.1	Configuration algorithm	55
7.3.2	Voice VLAN configuration example.....	56
7.4	Sub-interface termination configuration.....	57
7.4.1	Configuration algorithm	57
7.4.2	Sub-interface configuration example.....	58
7.5	QinQ termination configuration	58
7.5.1	Configuration algorithm	58
7.5.2	Q-in-q configuration example	59
7.6	USB modems configuration	60
7.6.1	USB modems configuration algorithm	60
7.6.2	Configuration example	61
7.7	AAA Configuration	62
7.7.1	Local authentication configuration algorithm	62
7.7.2	AAA configuration algorithm via RADIUS.....	64
7.7.3	AAA configuration algorithm via TACACS	66
7.7.4	AAA configuration algorithm via LDAP.....	68
7.7.5	Example of authentication configuration using telnet via RADIUS server.....	70
7.8	Command privilege configuration	71
7.8.1	Configuration algorithm	71
7.8.2	Example of command privilege configuration	71
7.9	DHCP server configuration.....	71
7.9.1	Configuration algorithm	72
7.9.2	DHCP server configuration example	74
7.10	Destination NAT configuration	75
7.10.1	Configuration algorithm.....	75
7.10.2	Destination NAT configuration example.....	77
7.11	Source NAT configuration	79
7.11.1	Configuration algorithm.....	79
7.11.2	Configuration example 1.....	81
7.11.3	Configuration example 2.....	82
7.12	Static NAT configuration	84
7.12.1	Configuration algorithm.....	84
7.12.1	Static NAT configuration example	84
7.12.1	85
7.12.2	85
7.12.3	Configuration example of application filtration (DPI).....	85

7.13	Configuration of logging and protection against network attacks	87
7.13.1	Configuration algorithm	87
7.13.2	Description of attack protection mechanisms	89
7.13.3	Configuration example of logging and protection against network attacks.....	92
7.14	Firewall configuration	94
7.14.1	Configuration algorithm	94
7.14.2	Firewall configuration example.....	98
7.15	Access list (ACL) configuration	100
7.15.1	Configuration algorithm	100
7.15.2	Access list configuration example	101
7.16	Static routes configuration.....	102
7.16.1	Configuration process	102
7.16.2	Static routes configuration example	103
7.17	MLPPP Configuration	105
7.17.1	Configuration algorithm	105
7.17.2	Configuration example.....	107
7.18	Bridge configuration.....	107
7.18.1	Configuration algorithm	108
7.18.2	Example of bridge configuration for VLAN and L2TPv3 tunnel.....	109
7.18.3	Example of bridge configuration for VLAN	110
7.18.4	Configuration example of the second VLAN tag adding/removing	111
7.19	RIP Configuration	112
7.19.1	Configuration algorithm	112
7.19.2	RIP configuration example	115
7.20	OSFP configuration.....	116
7.20.1	Configuration algorithm	116
7.20.2	OSPF configuration example	122
7.20.3	OSPF stub area configuration example	123
7.20.4	Virtual link configuration example	123
7.21	BGP configuration	125
7.21.1	Configuration algorithm	125
7.21.2	Configuration example.....	130
7.22	BFD configuration.....	131
7.22.1	Configuration algorithm	131
7.22.2	Configuration example of BFD with BGP	133
7.23	PBR routing policy configuration.....	134
7.23.1	Configuring Route-map for BGP.....	134
7.23.2	Route-map based on access control lists (Policy-based routing).....	139
7.24	GRE tunnel configuration	141
7.24.1	Configuration algorithm	141
7.24.2	IP-GRE tunnel configuration example.....	143
7.25	L2TPv3 tunnel configuration	145
7.25.1	Configuration algorithm	145
7.25.2	L2TPv3 tunnel configuration example	146
7.26	IPsec VPN configuration	148
7.26.1	Route-based IPsec VPN configuration	148
7.26.2	Policy-based IPsec VPN configuration.....	156

7.27	LT tunnels configuration	163
7.27.1	Configuration algorithm.....	163
7.27.2	Configuration example.....	164
7.28	Configuring remote access to corporate network via PPTP protocol.....	165
7.28.1	Configuration algorithm.....	165
7.28.2	PPTP server configuration example	166
7.29	Configuring remote access to corporate network via L2TP/IPsec protocol	168
7.29.1	Configuration algorithm.....	168
7.29.2	Configuration example.....	170
7.30	Configuring remote access to corporate network via OpenVPN protocol	172
7.30.1	Configuration algorithm.....	172
7.30.2	Configuration example.....	174
7.31	Configuring remote access client via PPPoE	175
7.31.1	Configuration algorithm.....	176
7.31.2	PPPoE client configuration example	177
7.32	Configuring remote access client via PPTP	178
7.32.1	Configuration algorithm.....	178
7.32.2	Example of remote connection configuration via PPTP	179
7.33	Configuring remote access client via L2TP.....	180
7.33.1	Configuration algorithm.....	180
7.33.2	Example of remote connection configuration via L2TP	181
7.34	Dual-Homing configuration.....	182
7.34.1	Configuration algorithm.....	182
7.34.2	Configuration example.....	183
7.35	QoS configuration	184
7.35.1	Basic QoS.....	184
7.35.2	Advanced QoS.....	187
7.36	Mirroring configuration	191
7.36.1	Configuration algorithm.....	191
7.36.2	Configuration example.....	192
7.37	Netflow configuration.....	193
7.37.1	Configuration algorithm.....	193
7.37.2	Configuration example.....	193
7.38	sFlow configuration.....	194
7.38.1	Configuration algorithm.....	194
7.38.2	Configuration example.....	195
7.39	LACP configuration.....	196
7.39.1	Configuration algorithm.....	196
7.39.2	Configuration example.....	197
7.40	VRRP configuration	197
7.40.1	Configuration algorithm.....	198
7.40.2	Configuration example 1.....	200
7.40.3	Configuration example 2.....	201
7.41	VRRP tracking configuration	202
7.41.1	Configuration algorithm.....	202
7.41.2	Configuration example.....	203
7.42	VRF Lite configuration.....	205

7.42.1	Configuration algorithm.....	206
7.42.2	Configuration example.....	206
7.43	MultiWAN configuration.....	207
7.43.1	Configuration algorithm.....	207
7.43.2	Configuration example.....	210
7.44	SNMP configuration.....	211
7.44.1	Configuration algorithm.....	211
7.44.2	Configuration example.....	213
7.45	BRAS (Broadband Remote Access Server) configuration.....	215
7.45.1	Configuration algorithm.....	215
7.45.2	Example of configuration with SoftWLC.....	218
7.45.3	Example of configuration without SoftWLC.....	223
7.46	VoIP configuration.....	228
7.46.1	SIP profile configuration process.....	228
7.46.2	FXS/FXO ports configuration process.....	229
7.46.3	Dial plan configuration process.....	230
7.46.4	VoIP configuration example.....	230
7.46.5	Dial plan configuration example.....	232
7.46.6	FXO port configuration.....	235
8	FREQUENTLY ASKED QUESTIONS.....	237

1 INTRODUCTION

1.1 Abstract

Today, large-scale communication network development projects are becoming increasingly common. One of the main tasks in implementation of large multiservice networks is the creation of reliable high-performance transport network that will serve as a backbone in multilayer architecture of next-generation networks.

ESR series routers could be used in large enterprise networks, SMB networks and operator's networks. Devices provide high performance and bandwidth, and feature protection of transmitted data.

This operation manual describes intended use, specifications, features, design, installation, first time setup, and firmware update guidelines for the ESR series router (next, the device).

1.2 Target Audience

This user manual is intended for technical personnel that performs device installation, configuration and monitoring via command line interface (CLI) as well as the system maintenance and firmware update procedures. Qualified technical personnel should be familiar with the operation basics of TCP/IP protocol stacks and Ethernet networks design concepts.

1.3 Symbols

Designation	Description
<i>Calibri italic</i>	Variables and parameters that should be replaced with the appropriate word or string are written in Calibri Italic.
Semibold font	Notes and warnings are written in semibold font.
<Semibold italic>	Keyboard keys are enclosed in angle brackets.
Courier New	Examples of command entry are written in Courier New semibold.
Courier New	Results of command execution are written in Courier New font in a frame with the shadow border.
[]	In the command line, optional parameters are shown in square brackets; when entered, they provide additional options.
{ }	In the command line, mandatory parameters are shown in curly braces. Choose one of the following:
	In the description of the command, this sign means 'or'.

Notes and warnings



Notes contain important information, tips or recommendations on device operation and setup.



Warnings are used to inform the user about harmful situations for the device and the user alike, which could cause malfunction or data loss.

2 PRODUCT DESCRIPTION

2.1 Purpose

ESR series devices are the high performance multi-purpose network routers. Device combines traditional network features with a complex multi-tier approach to routing security, and ensures robust corporate environment protection.

Device has a built-in firewall that enables protection of your network environment and supports latest data security, encryption, authentication and anti-intrusion features.

Device contains software and hardware means of data processing. Top performance is achieved through optimal distribution of data processing tasks between different subsets of the device.

2.2 Functions

2.2.1 Interface functions

Table 1 lists interface functions of the device.

Table 1 – Device interface functions

Cable connection polarity detection (Auto MDI/MDIX)	Automatic cable type detection—crossed or straight. <ul style="list-style-type: none"> – MDI (Medium Dependent Interface – straight) – cable standard for connection of terminal devices – MDIX (Medium Dependent Interface with Crossover – crossed) – cable standard for connection of hubs and switches
Back pressure routing support (Back pressure)	The backpressure routing method is utilized in half-duplex connections for management of data streams, coming from the opposite devices, by means of collisions. This method allows to avoid buffer overruns and the loss of data.
Flow control (IEEE 802.3X)	Flow control allows to interconnect the low-speed and the high-speed devices. To avoid buffer overrun, the low-speed device gains the ability to send PAUSE packets that will force the high-speed device to pause the packet transmission.
Link aggregation (LAG)	Link aggregation allows to increase the communication link bandwidth and robustness. Router supports static and dynamic link aggregation. For dynamic aggregation, link group management is performed via LACP protocol.

2.2.2 Functions for MAC address processing

Table 2 lists MAC address processing functions of the device.

Table 2 – MAC address processing functions

MAC address table	MAC address table sets the correspondence between MAC addresses and device interfaces and is used for data packet routing. Routers support table capacity up to 16K of MAC addresses and reserve specific MAC addresses for the system use.
--------------------------	---

Learning mode	<p>MAC address table may contain either static addresses or addresses learnt during data packet transition through the device.</p> <p>Learning involves registration of packet source MAC addresses with their binding to ports and VLANs. Afterwards, this data is used for incoming packet routing. Registered MAC address lifetime is limited. Administrator may adjust this setting. If destination MAC address specified in the packet that was received by the device is not listed in the table, this packet will be sent further as a broadcast packet within L2 segment of the network.</p>
----------------------	--

2.2.3 Second-layer functions of OSI model

Table 3 lists second-layer functions and special aspects (OSI Layer 2).

Table 3 – Second-layer functions description (OSI Layer 2)

VLAN support	<p>VLAN (Virtual Local Area Network) is a solution used for splitting a network into separate segments on L2 level. VLAN utilization allows to increase the operation stability for large networks by splitting them into smaller networks, isolate diversified data traffic by type and solve many other tasks.</p> <p>Routers support various VLAN management methods:</p> <ul style="list-style-type: none"> – VLAN based on data packet tagging according to IEEE802.1Q – VLAN based on device ports (port-based) – VLAN based on utilization of data classification policies (policy-based)
Spanning Tree Protocol (STP)¹	<p>The main task of Spanning Tree Protocol is to exclude redundant network links and convert network topology into the tree-like structure. Common areas of protocol application involve the prevention of network traffic loops and establishing of redundant communication links.</p>

2.2.4 Third-layer functions of OSI model

Table 4 lists third-layer functions (OSI Layer 3).

Table 4 – Third-layer functions description (OSI Layer 3)

Static IP routes	<p>Administrator of the router can add or remove static entries into/from the routing table.</p>
Dynamic routing	<p>With dynamic routing protocols, the device will be able to exchange the routing information with neighbouring routers and automatically create a routing table. Router supports the following protocols: RIP, OSPFv2, OSPFv3, BGP.</p>
ARP table	<p>ARP (Address Resolution Protocol) is a protocol used for resolution of the network and data-link layer addresses. ARP table contains information on the established correspondence.</p> <p>Correspondence is established on the basis of the network device response analysis; device addresses are requested with broadcast packets.</p>
DHCP client	<p>DHCP (Dynamic Host Configuration Protocol) protocol enables automation of the network device management process.</p> <p>DHCP client allows the router to obtain the network address and additional settings from the external DHCP server. As a rule, this method is used for obtaining network settings of a public network operator (WAN).</p>
DHCP server	<p>DHCP server enables automation and centralization of the network device configuration process.</p>

¹ In the current firmware version, this functionality is supported only by ESR-1000 router

	<p>DHCP server allocated on a router allows for a complete solution for the local area network support.</p> <p>DHCP server integrated into the router assigns IP addresses to network devices and transfers additional network settings, e.g. server addresses, network gateway addresses and other necessary settings.</p>
Network Address Translation (NAT)	<p>Network address translation is a mechanism that translates IP addresses and port numbers for transit packets.</p> <p>NAT function allows to minimize the quantity of IP address used through translation of multiple internal network IP addresses into a single external public IP address. NAT conceals local area network internal structure and allows to enhance its security.</p> <p>Routers support the following NAT options:</p> <ul style="list-style-type: none"> – Source NAT (SNAT) – the network address and the source port number will be replaced, when packet is transferred forth, and the destination address will be replaced in the response packet. – Destination NAT (DNAT) – external access is translated by the firewall to the user computer in LAN that has an internal address and thus directly inaccessible from outside the network.

2.2.5 Traffic tunnelling functions

Table 5 – Traffic tunneling functions

Tunneling protocols	<p>Tunneling is a method of packet conversion during their network transfer that involves the replacement, modification and addition of a new packet network header. This method may be used for negotiation of transport protocols when the data is transferred through the transit network as well as for creation of secured connections where tunnelled data is being encrypted.</p> <p>Routers support the following types of tunnels:</p> <ul style="list-style-type: none"> – GRE – IP packet is encapsulated into another IP packet with GRE (General Routing Encapsulation) header – IPv4-IPv4 – tunnel that encapsulates source IP packets into IP packets with alternative network parameters – L2TPv3 – tunnel for L2 traffic transmission using IP packets – IPsec – tunnel with the encryption of transmitted data – L2TP, PPTP – tunnels used for establishing a remote 'client-sever' access
----------------------------	---

2.2.6 Management and configuration functions

Table 6 – Basic management and configuration functions

Configuration file download and upload	<p>Device parameters are saved into the configuration file that contains configuration data for the specific device ports as well as for the whole system. The following protocols may be used for file transfers: TFTP, FTP, and SCP.</p>
Command line interface (CLI)	<p>CLI management is performed locally via serial port RS-232, or remotely via Telnet, SSH. Console command line interface (CLI) is the industrial standard. CLI interpreter contains the list of commands and keywords that will help the user and reduce the amount of input data.</p>
Syslog	<p>Syslog protocol is designed for transmission of system event messages and event logging.</p>
Network utilities: ping, traceroute	<p><i>ping and traceroute utilities</i> allow you to check the availability of network devices and identify data transfer routes in IP networks.</p>
Controlled access management–privilege levels	<p>Routers support system access level management for users. Access levels enable responsibility areas management for device administrators. Access levels are numbered from 1 to 15; Level 15 stands for full access to device management features.</p>

Authentication	Authentication is a user identity check procedure. Routers support the following authentication methods: <ul style="list-style-type: none"> – local–local user database stored on the device is used for authentication – group–user database is located on the authentication server RADIUS and TACACS protocols are user for server interactions.
SSH server Telnet server	SSH and Telnet server features allow you to establish connection to the device and perform device management.
Automatic configuration restore	Device features automatic configuration restore system designed to prevent remote access loss after re-configuration. If the configuration change is not confirmed in the specified time, configuration will be rolled back to the last known state.

2.2.7 Network security functions

The table lists network security functions of the device.

Table 7 – Network security functions

Security zones	All router interfaces are distributed by security areas. For each zone pair, you can set the rules that determine the possibility of data transmission between zones, data traffic filtering rules.
Data filtering	For each zone pair, you can specify the rule set that manages the filtering process for data transmitted through the router. Device command interface provides appropriate means for detailed configuration of the traffic classification rules and to apply the resulting solution for traffic transmission.

2.3 Main specifications

Table 8 lists main specifications of the router.

Table 8 – Main specifications

General parameters		
Packet processor	ESR-1700	Broadcom XLP780
	ESR-1200 ESR-1000	Broadcom XLP316L
	ESR-200	Broadcom XLP204
	ESR-100	Broadcom XLP104
	ESR-14VF ESR-12V(F) ESR-10	Broadcom NS+ (BCM58625)
Interfaces	ESR-1700	4 x Ethernet 10/100/1000BASE-T/1000BASE-X Combo 8 x 10GBASE-R/1000BASE-X (SFP+/SFP)
	ESR-1200	12 x Ethernet 10/100/1000BASE-T/1000BASE-X Combo 4 x Ethernet 10/100/1000Base/1000BASE-X Combo 8 x 10GBASE-R/1000BASE-X (SFP+/SFP)
	ESR-1000	24 x Ethernet 10/100/1000BASE-T/1000BASE-X Combo 2 x 10GBASE-R/1000BASE-X (SFP+/SFP)
	ESR-200	4 x Ethernet 10/100/1000BASE-T/1000BASE-X Combo 4 x Ethernet 10/100/1000BASE-T/1000BASE-X Combo
	ESR-100	4 x Ethernet 10/100/1000BASE-T/1000BASE-X Combo
	ESR-14VF	8 x Ethernet 10/100/1000BASE-T/1000BASE-X Combo

		1 x 1000BASE-X (SFP), 4xFXS
	ESR-12VF	8 x Ethernet 10/100/1000BASE-T, 1 x 1000BASE-X (SFP), 3xFXS, 1xFXO
	ESR-12V	8 x Ethernet 10/100/1000BASE-T, 3xFXS, 1xFXO
	ESR-10	4 x Ethernet 10/100/1000BASE-T, 2 x 1000BASE-X
Types of optical transceivers	ESR-1700 ESR-1200 ESR-1000	1000BASE-X SFP, 10GBASE-R SFP+
	ESR-200 ESR-100 ESR-14VF ESR-12V(F) ESR-10	1000BASE-X SFP
Duplex or half-duplex interface modes		- duplex and half-duplex modes for electric ports - duplex mode for optical ports
Maximum bandwidth (hardware switching)	ESR-1700 ESR-1200	160 Gbps
	ESR-1000	88 Gbps
Data transfer rate	ESR-1700 ESR-1200 ESR-1000	- electric interfaces 10/100/1000Mbps - optical interfaces 1/10Gbps
	ESR-200 ESR-100 ESR-14VF ESR-12V(F) ESR-10	- electric interfaces 10/100/1000Mbps - optical interfaces 1Gbps
MAC address table	ESR-1700 ESR-1200	128k entries
	ESR-1000	16k entries
	ESR-200 ESR-100 ESR-14VF ESR-12V(F) ESR-10	2k bridge entries
VLAN support		up to 4k active VLANs according to 802.1Q
Quantity of L3 interfaces	ESR-1700 ESR-1200 ESR-1000 ESR-200 ESR-100	2000
	ESR-14VF ESR-12V(F) ESR-10	200
Quantity of BGP routes	ESR-1700 ESR-1200 ESR-1000	2.8M
	ESR-200 ESR-100	1.4M
	ESR-14VF ESR-12V(F) ESR-10	800k
Quantity of OSPF routes	ESR-1700 ESR-1200 ESR-1000	500k
	ESR-200 ESR-100	300k

	ESR-14VF ESR-12V(F) ESR-10	
Quantity of RIP routes		10k
Quantity of static routes		11k
FIB size	ESR-1700 ESR-1200 ESR-1000	1.7M
	ESR-200 ESR-100	1.4M
	ESR-14VF ESR-12V(F) ESR-10	800k
Compliance		IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet ANSI/IEEE 802.3 Speed autodetection IEEE 802.3x Data flow control IEEE 802.3ad LACP link aggregation IEEE 802.1q VLAN virtual local networks IEEE 802.1v IEEE 802.3ac IEEE 802.3ae IEEE 802.1D IEEE 802.1w IEEE 802.1s
Control		
Local control		CLI
Remote control		TELNET, SSH
Physical specifications and ambient conditions		
Power supply	ESR-1700 ESR-1200 ESR-1000	AC: 220V+20%, 50Hz DC: -36 .. - 72V Power options: - Single AC or DC power supply - Two AC or DC power supplies with hot swapping
	ESR-200 ESR-100 ESR-14VF ESR-12V(F)	AC: 220V+20%, 50Hz
	ESR-10	AC: 220V
Maximum consumption: power	ESR-1700	250 W
	ESR-1200	85 W
	ESR-1000	75 W
	ESR-200	25 W
	ESR-100	20 W
	ESR-14VF ESR-12V(F)	27 W
	ESR-10	9 W
Weight	ESR-1700	12 kg max
	ESR-1200	5.5 kg max
	ESR-1000	3.6 kg max
	ESR-200 ESR-100	2.5 kg max
	ESR-14VF	1 kg max

	ESR-12V(F) ESR-10	
Dimensions	ESR-1700	440x490x88 mm
	ESR-1200 ESR-1000	430x352x44 mm
	ESR-200 ESR-100	310x240x44 mm
	ESR-14VF ESR-12V(F)	267x160.5x43.6 mm
	ESR-10	430x352x44 mm
Operating temperature range	ESR-1700 ESR-1200 ESR-1000 ESR-200 ESR-100	-10 to +45°C
	ESR-14VF ESR-12V(F) ESR-10	0 to +40 °C
Storage temperature range		-40 to +70°C
Operation relative humidity (non-condensing)		up to 80%
Storage relative humidity (non-condensing)		from 10% to 95%
Average lifetime		10 years

2.4 Design

This section describes the design of the device. Depicted front, rear, and side panels of the device, connectors, LED indicators and controls.

The device has a metal housing available for 19" form-factor rack mount; housing size is 1U.

2.4.1 ESR-1700 design

2.4.1.1 ESR-1700 front panel

The front panel of ESR-1700 is shown in Figure 1.

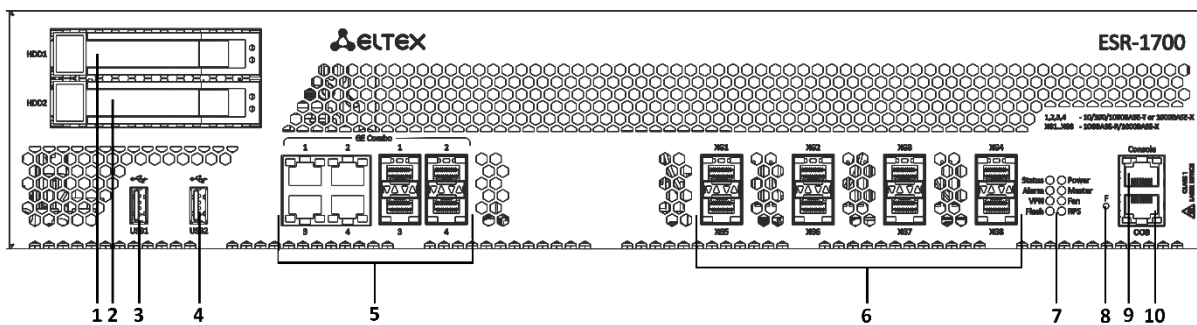


Figure 1 – ESR-1700 front panel

Table 9 lists connectors, LEDs and controls located on the front panel of ESR-1700.

Table 9 – Description of ESR-1700 connectors, LEDs and front panel controls

No	Front panel element	Description
1	HDD1	Connector for HDD installation.
2	HDD2	Connector for HDD installation.
3	USB1	Port for USB device connection.
4	USB2	Port for USB device connection.
5	Combo Ports [1 .. 4]	4 x Gigabit Ethernet 10/100/1000BASE-X (SFP) ports
6	XG1 - XG8	Slots for installation of 10G SFP+/1G SFP transceivers.
7	Status	Current device status LED.
	Alarm	Alarm LED.
	VPN	HA operation mode indicator. Not supported in the current firmware version.
	Flash	Activity of exchange with data storage – SD card or USB Flash.
	Power	Device power LED.
	Master	Indicator of failover modes operation. Not supported in the current firmware version.
	Fan	Fan operation LED.
	RPS	Redundant power supply LED.
8	F	Functional key that reboots the device and resets it to factory settings: <ul style="list-style-type: none"> – Pressing the key for less than 10 seconds reboots the device; – Pressing the key for more than 10 seconds resets the terminal to factory settings.
9	Console	Console port RS-232 for local management of the device.
10	OoB	Ethernet port for router management.

2.4.1.2 ESR-1700 rear panel

The rear panel of ESR-1700 is depicted in Figure 2¹.

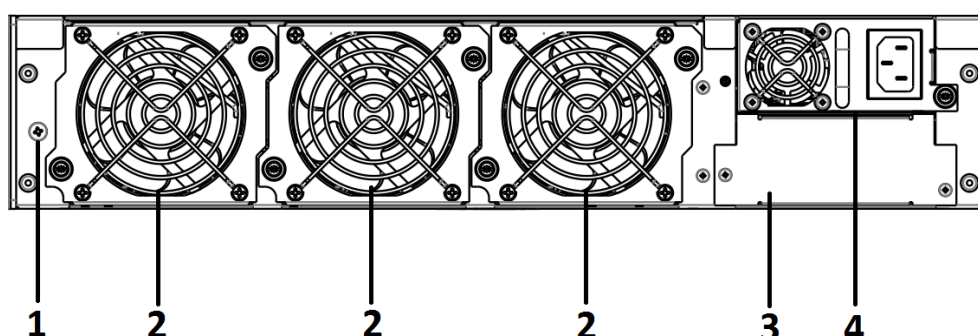


Figure 2 – ESR-1700 rear panel

¹ The figure shows the router delivery package with a single AC power supply.

Table 10 lists connectors located on the rear panel of ESR-1700.

Table 10 – Description of ESR-1700 rear panel connectors

No	Description
1	Earth bonding point of the device.
2	Hot-swappable removable ventilation modules.
3	Main power supply.
4	Place for installation of a redundant power supply.

2.4.1.3 Side panels of the device

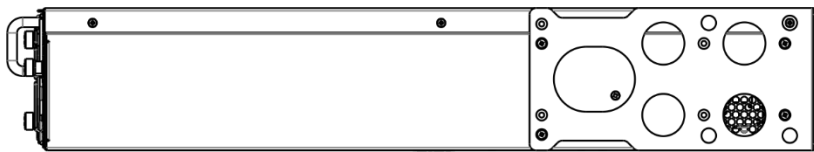


Figure 3 – ESR-1700 right side panel

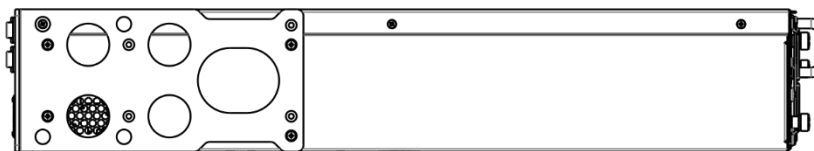


Figure 4 – ESR-1700 left side panel

Side panels of the device have air vents for heat removal. Do not block air vents. This may cause the components to overheat, which may result in device malfunction. For recommendations on device installation, see section 'Installation and connection'.

2.4.2 ESR-1000, ESR-1200 design

2.4.2.1 ESR-1200 front panel

The front panel of ESR-1700 is shown in Figure 5.

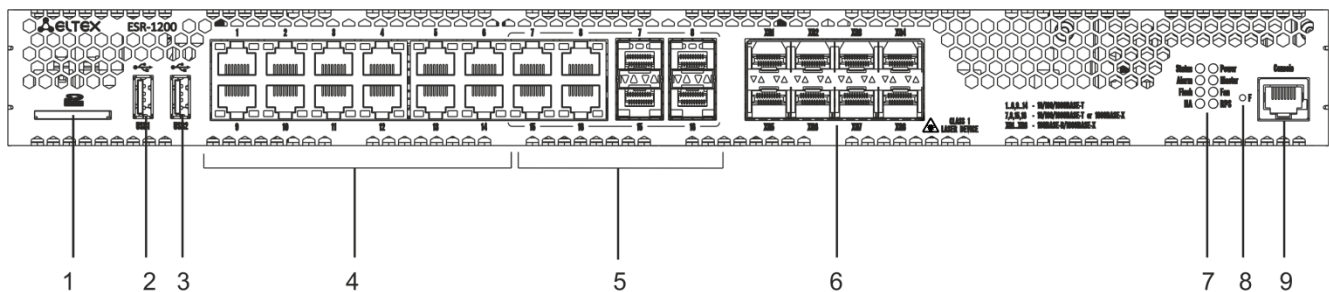


Figure 5 – ESR-1200 front panel

Table 11 lists connectors, LEDs and controls located on the front panel of ESR-1200.

Table 11 – Description of connectors, LEDs and controls located on the front panel of ESR-1200

No	Front panel element	Description
1	SD	SD-card connector.
2	USB1	Port for USB device connection.
3	USB2	Port for USB device connection.
4	[1 .. 12]	12 x Gigabit Ethernet 10/100/1000BASE-T (RJ-45) ports.
5	Combo Ports	4 x Gigabit Ethernet 10/100/1000BASE-X (SFP) ports
6	XG1 - XG8	Slots for installation of 10G SFP+/1G SFP transceivers.
7	Status	Current device status LED.
	Alarm	Alarm LED.
	HA	HA operation mode indicator.
	Flash	Activity indicator of exchange with data storages (SD-card or USB Flash).
	Power	Device power LED.
	Master	Indicator of failover modes operation.
	Fan	Fan operation LED.
7	RPS	Redundant power supply LED.
	RPS	Redundant power supply LED.
8	F	Functional key that reboots the device and resets it to factory settings: <ul style="list-style-type: none"> – Pressing the key for less than 10 seconds reboots the device; – Pressing the key for more than 10 seconds resets the terminal to factory settings.
9	Console	Console port RS-232 for local management of the device.

2.4.2.2 ESR-1000 front panel

The front panel of ESR-1700 is shown in Figure 6.

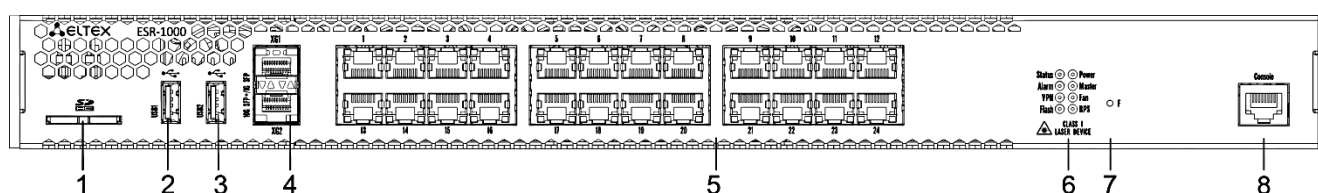


Figure 6 – ESR-1000 front panel

Table 12 lists connectors, LEDs and controls located on the front panel of ESR-1000.

Table 12 – Description of ESR-1000 connectors, LEDs and front panel controls

No	Front panel element	Description
1	SD	SD-card connector.
2	USB1	Port for USB device connection.
3	USB2	Port for USB device connection.
4	XG1, XG2	Slots for installation of 10G SFP+/1G SFP transceivers.
5	[1 .. 24]	24 x Gigabit Ethernet 10/100/1000BASE-T (RJ-45) ports.

6	Status	Current device status LED.
	Alarm	Alarm LED.
	VPN	Active VPN sessions indicator.
	Flash	Activity indicator of exchange with data storages (SD-card or USB Flash).
	Power	Device power LED.
	Master	Indicator of failover modes operation.
	Fan	Fan operation LED.
	RPS	Redundant power supply LED.
7	F	Functional key that reboots the device and resets it to factory settings: <ul style="list-style-type: none"> – Pressing the key for less than 10 seconds reboots the device; – Pressing the key for more than 10 seconds resets the terminal to factory settings.
8	Console	Console port RS-232 for local management of the device.

2.4.2.3 ESR-1000, ESR-1200 rear panel

The rear panel layout of ESR-1000, ESR-1200 is depicted in Figure 7¹.

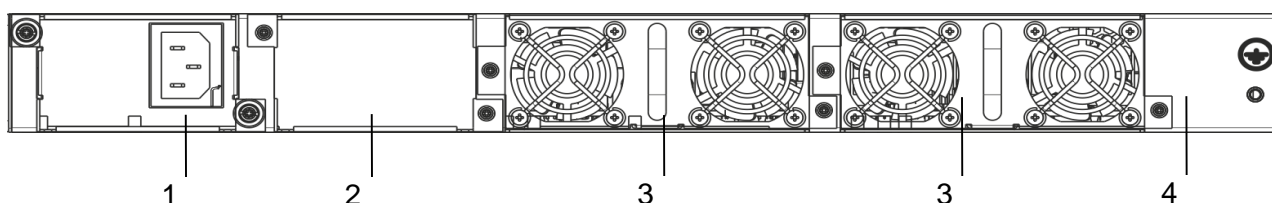


Figure 7 – ESR-1000, ESR-1200 rear panel

Table 13 lists connectors located on the rear panel of ESR-1700.

Table 13 – Description of ESR-1700 rear panel connectors

No	Description
1	Main power supply.
2	Place for installation of a redundant power supply.
3	Hot-swappable removable ventilation modules.
4	Earth bonding point of the device.

2.4.2.4 Side panels of the device

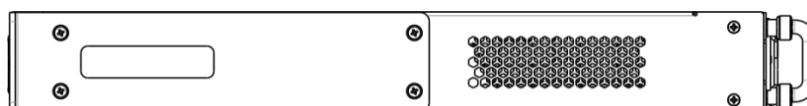


Figure 8 – ESR-1000, ESR-1200 right-side panel

¹ The figure shows the router delivery package with a single AC power supply.

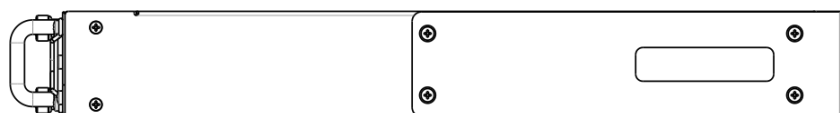


Figure 9 – ESR-1000, ESR-1200 left-side panel

Side panels of the device have air vents for heat removal. Do not block air vents. This may cause the components to overheat, which may result in device malfunction. For recommendations on device installation, see section 'Installation and connection'.

2.4.3 ESR-100, ESR-200 design

2.4.3.1 ESR-100, ESR-200 front panel

The front panel layout of ESR-100 is depicted in Figure 10.

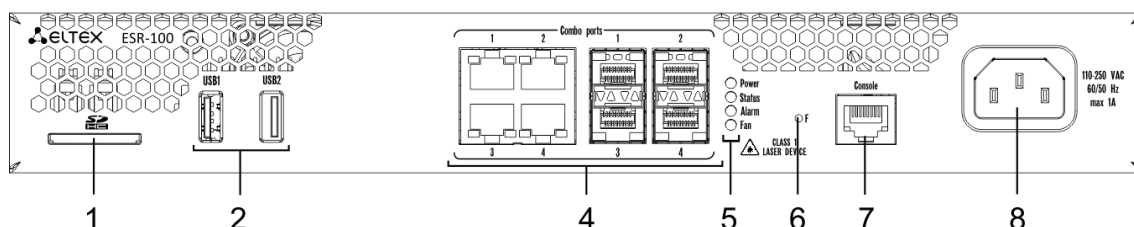


Figure 10 – ESR-100 front panel

The front panel layout of ESR-200 is depicted in Figure 11.

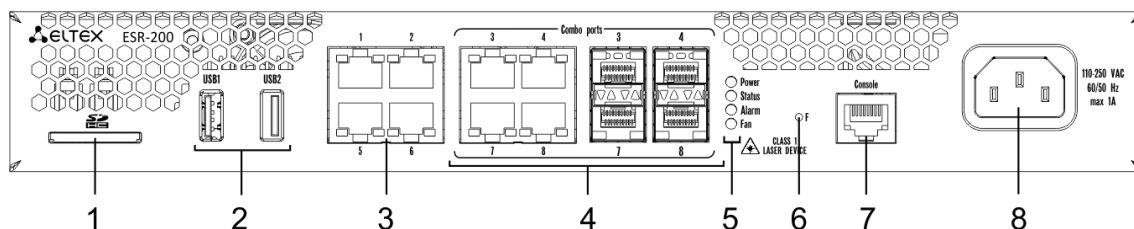


Figure 11 – ESR-200 front panel

Table 14 lists connectors, LEDs and controls located on the front panel of ESR-100 and ESR-200 routers.

Table 14 – Description of connectors, LEDs and controls located on the front panel

No	Front panel element	Description
1	SD	SD-card connector.
2	USB1, USB2	2 x USB-enabled devices connection port.
3	[1 .. 4]	4 x Gigabit Ethernet 10/100/1000BASE-T (RJ-45) ports.
4	Combo Ports	4 x Gigabit Ethernet 10/100/1000BASE-X (SFP) ports
5	Power	Device power LED.
	Status	Current device status LED.
	Alarm	Alarm LED.

	Fan	Fan operation LED.
6	F	Functional key that reboots the device and resets it to factory settings: <ul style="list-style-type: none"> – Pressing the key for less than 10 seconds reboots the device; – Pressing the key for more than 10 seconds resets the terminal to factory settings.
7	Console	Console port RS-232 for local management of the device.
8	110-250VAC 60/50Hz max 1A	Power supply.

2.4.3.2 ESR-100, ESR-200 rear panel

The rear panel layout of ESR-100, ESR-200 is depicted in Figure 12.

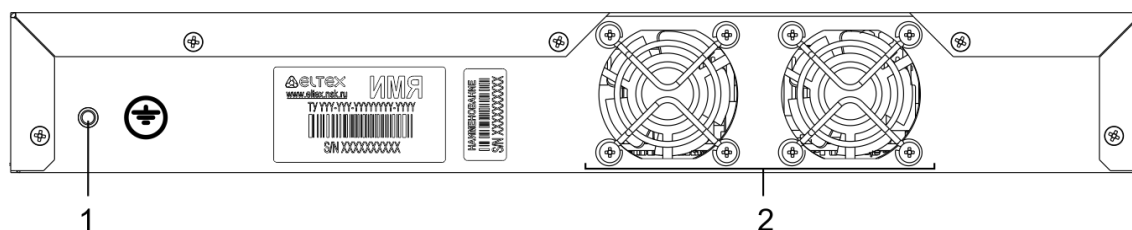


Figure 12 – ESR-1000, rear panel

Table 15 lists connectors located on the rear panel of ESR-1700.

Table 15 – Description of ESR-1700 rear panel connectors

No	Description
1	Earth bonding point of the device.
2	Ventilation module.

2.4.3.3 ESR-100, ESR-200 side panels



Figure 13 – ESR-100 and ESR-200 right-side panel



Figure 14 – ESR-100 and ESR-200 left-side panel

2.4.4 ESR-12VF, ESR-14VF design

The device has a metal housing available for 19" form-factor rack mount; housing size is 1U.

2.4.4.1 ESR-12VF, ESR-14VF front panel

The front panel of ESR-1700 is shown in Figure 15.

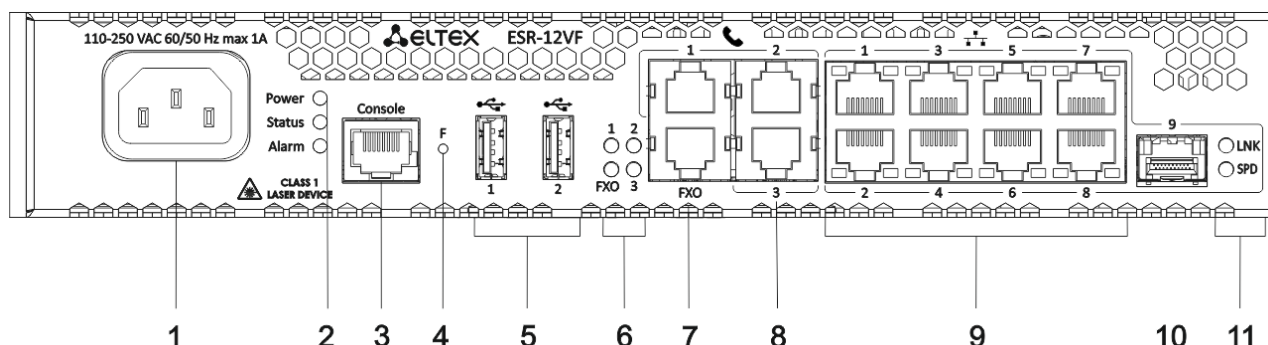


Figure 15 – ESR-12VF, ESR-14VF front panel

Table 16 lists connectors, LEDs and controls located on the front panel of ESR-12VF and ESR-14VF routers.

Table 16 – Description of connectors, LEDs and controls located on ESR-12VF, ESR-14VF front panel

No	Front panel element	Description
1	220V AC	Power supply.
2	Power	Device power LED.
3	Console	Console port RS-232 for local management of the device.
4	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory default configuration.
5	USB1, USB2	2 USB connectors for connecting external USB devices.
6	FXO	PSTN external subscriber line LED.
	1,2,3	Internal subscriber terminals LED.
7	FXO	1 FXO connector for connection PSTN external subscriber line (only for ESR-12VF).
8	FXS 1, FXS 2, FXS 3	3 connectors for internal subscriber terminals (for ESR-12VF).
	FXS 1, FXS 2, FXS 3	4 connectors for internal subscriber terminals (for ESR-14VF).
9	[1 .. 8]	8 ports of Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
10	Optical Port	1 port of Gigabit Ethernet-100/1000BASE-X (SFP)
11	1,2	Optical interfaces LED.

2.4.4.2 ESR-12VF, ESR-14VF rear panel

The rear panel layout of ESR-12VF, ESR-14VF is depicted in Figure 16.

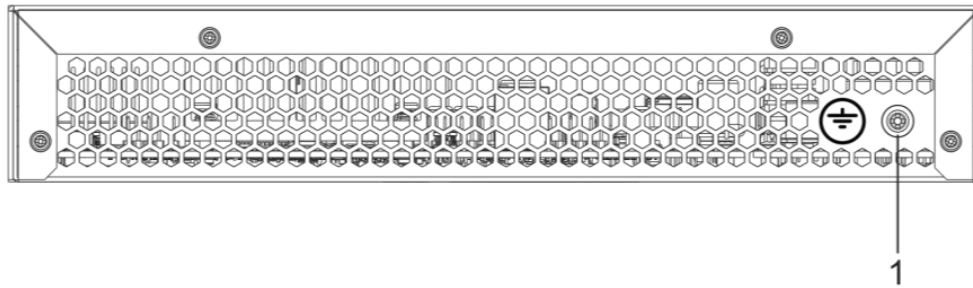


Figure 16 – ESR-12VF, ESR-14VF rear panel

Table 17 lists connectors located on the rear panel of ESR-1700.

Table 17 – Description of ESR-1700 rear panel connectors

№	Description
1	Earth bonding point of the device.

2.4.4.3 ESR-12VF, ESR-14VF side panels

The side panel layout of ESR-12VF, ESR-14VF is depicted in Figures 17 and 18.

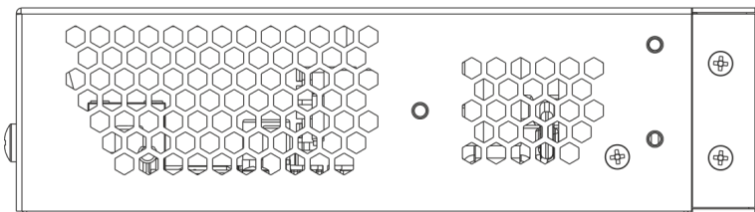


Figure 17 – ESR-12VF, ESR-14VF left-side panel

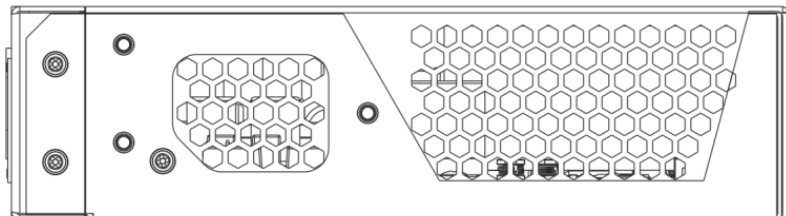


Figure 18 – ESR-12VF, ESR-14VF right-side panel

2.4.5 ESR-12V design

The device has a metal housing available for 19" form-factor rack mount; housing size is 1U.

2.4.5.1 ESR-12V front panel

The front panel of ESR-1700 is shown in Figure 19.

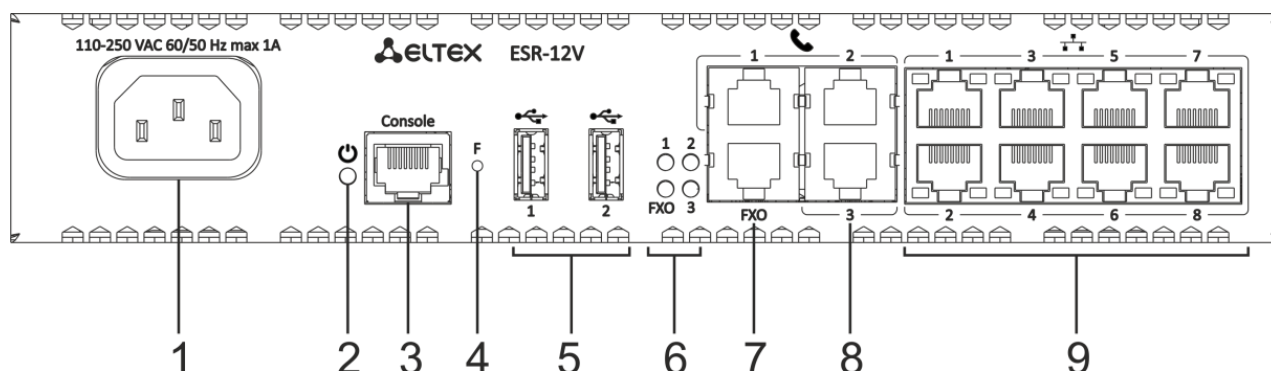


Figure 19 – ESR-12V front panel

Table 18 lists connectors, LEDs and controls located on the front panel of ESR-12V.

Table 18 – Description of connectors, LEDs and controls located on the front panel of ESR-12V

Nº	Front panel element	Description
1	220V AC	Power supply.
2	Power	Device power LED.
3	Console	Console port RS-232 for local management of the device.
4	F	Functional key that reboots the device and resets it to factory default configuration: - pressing the key for less than 10 seconds reboots the device. - pressing the key for more than 10 seconds resets the device to factory default configuration.
5	USB1, USB2	2 USB connectors for connecting external USB devices.
6	FXO	PSTN external subscriber line LED.
	1,2,3	Internal subscriber terminals LED.
7	FXO	1 FXO connector for connection PSTN external subscriber line.
8	FXS 1, FXS 2, FXS 3	3 connectors for internal subscriber terminals.
9	[1 .. 8]	8 x Gigabit Ethernet 10/100/1000BASE-T (RJ-45) ports.

2.4.5.2 ESR-12V rear panel

The rear panel layout of ESR-12V is depicted in Figure 20.

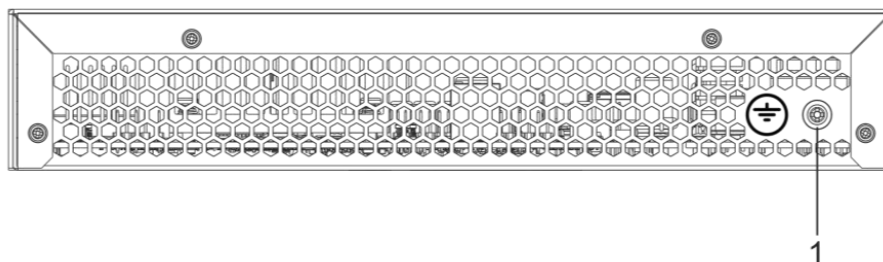


Figure 20 – ESR-12V rear panel

Table 19 lists connectors located on the rear panel of ESR-1700.

Table 19 – Description of ESR-1700 rear panel connectors

No	Description
1	Earth bonding point of the device.

2.4.5.3 ESR-12V side panels

The side panel layout of ESR-12V is depicted in Figures 21 and 22.

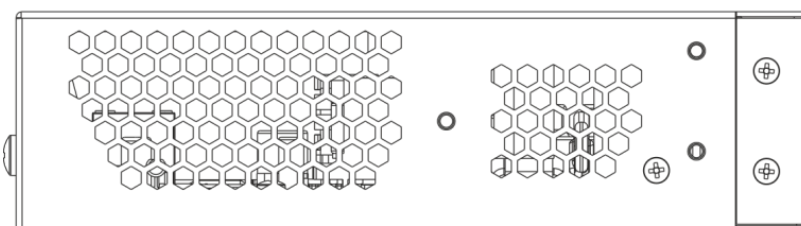


Figure 21 – ESR-12V left-side panel

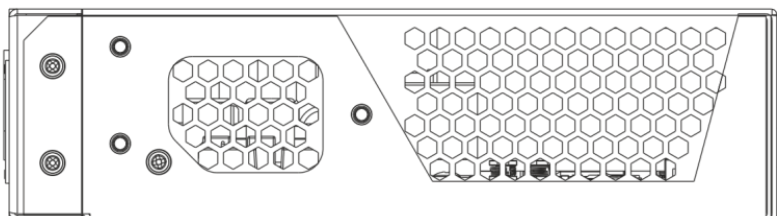


Figure 22 – ESR-12V right-side panel

2.4.6 ESR-10 design

2.4.6.1 ESR-10 rear panel

The rear panel layout of ESR-10 is depicted in Figure 23.

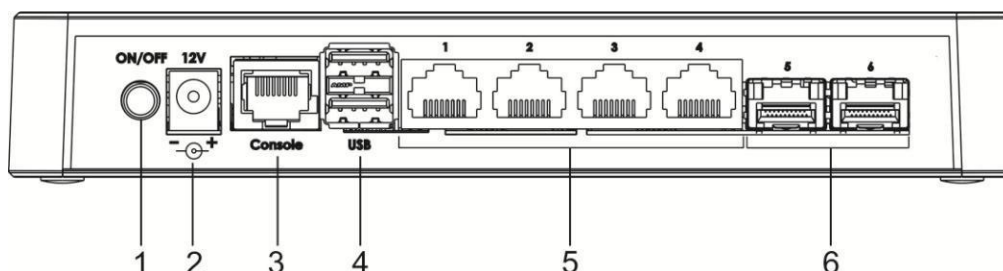


Figure 23 – ESR-10 rear panel

Table 20 lists connectors, LEDs and controls located on the rear panel of ESR-10.

Table 20 – Description of connectors, LEDs and controls located on the front panel of ESR-10

No	Front panel element	Description
1	ON/OFF	Power on/off button
2	12V DC	Connector for power adapter connection
3	Console	Console port RS-232 for local management of the device.
4	USB1, USB2	2 USB connectors for connecting external USB devices
5	[1 .. 4]	4 ports of Gigabit Ethernet 10/100/1000BASE-T (RJ-45)
6	Optical Ports	2 ports of Gigabit Ethernet 100/1000BASE-X (SFP)

2.4.6.2 ESR-10 side panels

The side panel layout of ESR-10 is depicted in Figure 24.

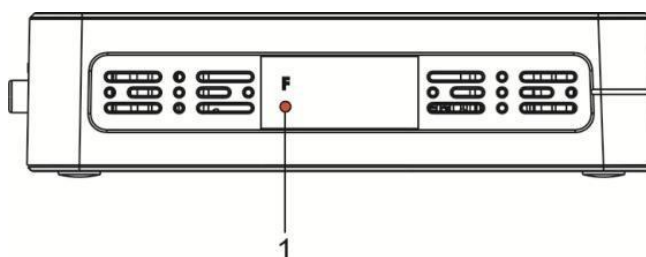


Figure 24 – ESR-10 side panel

Table 21 lists connectors located on the rear panel of ESR-1700.

Table 21 – Description of ESR-1700 rear panel connectors

No	Side panel element	Description
1	F	Functional key that reboots the device and resets it to factory settings: <ul style="list-style-type: none"> – pressing the key for less than 10 seconds reboots the device. – pressing the key for more than 10 seconds resets the device to factory default configuration.

2.4.6.3 ESR-10 top panel

The top panel layout of ESR-10 is depicted in Figure 25.

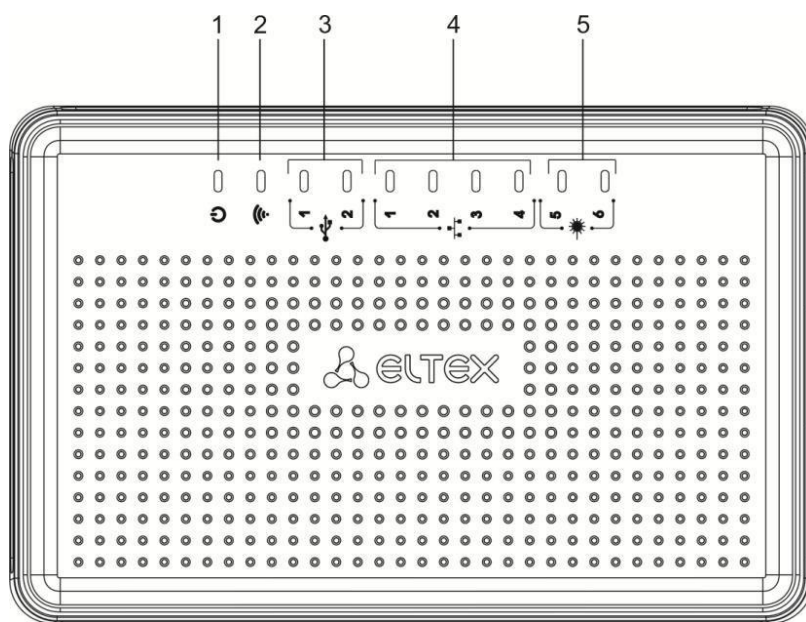


Figure 25 – ESR-10 top panel

Table 22 lists LEDs located on ESR-10 top panel.

Table 22 – Description of top panel LEDs

No	Top panel element	Description
1	Power	Device power and operation status LED
2	-	The LED is not used
3	USB1, USB2	External USB devices LED
4	[1 .. 4]	Ethernet ports LED
5	[5 .. 6]	Optical interfaces LED.

2.4.7 Light Indication

2.4.7.1 ESR-1000, ESR-1200 light indication

Gigabit Ethernet copper interface status is represented by two LEDs—green *LINK/ACT* LED and amber *SPEED* LED. Location of the copper interface LEDs is depicted in Figure 26. SFP interface status is represented by two LEDs – *RX/ACT* and *TX/ACT* – depicted in Figure 27. For light indication meaning, see Tables 23 and 24.

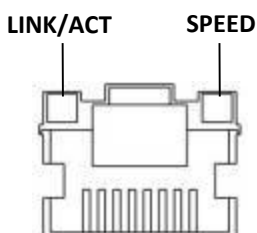
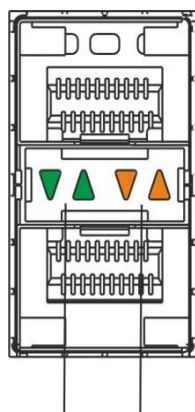


Figure 26 – Location of RJ-45 connector indicators



RX/ACT TX/ACT

Figure 27 – Location of optical interface indicators

Table 23 – Light indication of copper interface status

SPEED indicator is lit	LINK/ACT indicator is lit	Ethernet interface state
Off	Off	Port is disabled or connection is not established
Off	Solid on	10Mbps or 100Mbps connection is established
Solid on	Solid on	1000Mbps connection is established
X	Flashes	Data transfer is in progress

Table 24 – Light indication of SFP/SFP+ interface status

RX/ACT indicator is lit	TX/ACT indicator is lit	Ethernet interface state
Off	Off	Port is disabled or connection is not established
Solid on	Solid on	Connection established
Flashes	X	Data reception in progress
X	Flashes	Data transfer in progress

The following table lists description of system indicator statuses and meanings.

Table 25 – Status of system indicators

Indicator name	Indicator function	LED state	Device state
<i>Status</i>	Current device status LED.	Green	Device is in normal operation state.
		Orange	Device is booting up the software.
<i>Alarm</i>	Alarm LED.	-	-
<i>VPN</i>	Active VPN sessions indicator.	-	-
<i>Flash</i>	Data storage activity indicator: SD card or USB Flash.	Orange	Read/write operation execution with 'copy' command
<i>Power</i>	Device power LED.	Green	Device power is OK. Main power supply, if installed, is operational.

		Orange	Main power supply failure or fault, or the primary main is missing.
		Off	Device internal power supply failure.
Master	Indicator of failover modes operation.	-	-
Fan	Cooling fan status.	Off	All fans are operational.
		Red	One or more fans has failed. Possible cause of failure: at least one of the fans has stopped or is working at lower rpm.
RPS	Backup power supply operation mode.	Green	Backup power supply is installed and operational.
		Off	Backup power supply is not installed.
		Red	Backup power supply is missing or failed. ESR-100/ESR-200 light indication

2.4.7.2 ESR-100, ESR-200 light indication

Gigabit Ethernet copper interface and SFP interface statuses are represented by two LEDs—green LINK/ACT LED and amber SPEED LED. Location of the copper interface LEDs is depicted in Figure 28. SFP interface status is depicted in Figure 29. For light indication meaning, see Table 26.

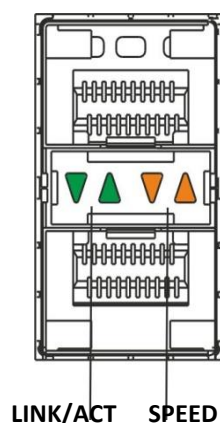


Figure 28 – Location of optical interface indicators

Table 26 – Light indication of copper and SFP interface status

SPEED indicator is lit	LINK/ACT indicator is lit	Ethernet interface state
Off	Off	Port is disabled or connection is not established
Off	Solid on	10Mbps or 100Mbps connection is established
Solid on	Solid on	1000Mbps connection is established
X	Flashes	Data transfer in progress

The following table lists description of system indicator statuses and meanings.

Table 27 – Status of system indicators

Indicator name	Indicator function	LED state	Device state
Status	Current device status LED.	Green	Device is in normal operation state.
		Orange	Device is booting up the software.
Alarm	Alarm LED.	-	-
Power	Device power LED.	Green	Device power is OK. Main power supply, if installed, is operational.
		Orange	Main power supply failure or fault, or the primary main is missing.
		Off	Device internal power supply failure.
Fan	Cooling fan status.	Off	All fans are operational.
		Red	One or more fans has failed. Possible cause of failure: at least one of the fans has stopped or is working at lower rpm.

2.4.7.3 ESR-10 light indication

Gigabit Ethernet copper interfaces statuses are represented by amber SPEED LED.

Table 28 – Light indication of copper interface status

SPEED indicator is lit	Ethernet interface state
Off	Port is disabled or connection is not established
Solid on	1000Mbps connection is established
Flashes	Data transfer in progress

2.4.7.4 ESR-12V(F) light indication

Gigabit Ethernet copper interface statuses are represented by two LEDs – green LINK/ACT LED and amber SPEED LED.

Table 29 – Light indication of copper and SFP interface status

SPEED indicator is lit	LINK/ACT indicator is lit	Ethernet interface state
Off	Off	Port is disabled or connection is not established
Off	Solid on	10Mbps or 100Mbps connection is established
Solid on	Solid on	1000Mbps connection is established
X	Flashes	Data transfer in progress

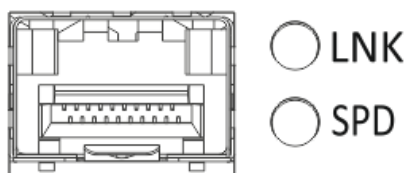


Figure 29 – Location of SFP connector indicators (only for ESR-12VF, ESR-14VF)

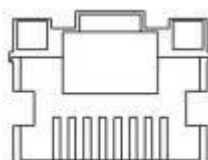


Figure 30 – Location of RJ-45 connector indicators

The following table lists description of system indicator statuses and meanings.

Table 30 – Status of system indicators

Indicator name	Indicator function	LED state	Device state
<i>Power</i>	Device power LED.	Green	Device power is OK. Main power supply, if installed, is operational. The main software is uploaded.
		Red	The main software is not uploaded.
		Off	Device internal power supply failure.

2.5 Delivery Package

ESR-10 standard delivery package includes:

- ESR-10 router;
- External 12V power block;
- Documentation.

ESR-12V standard delivery package includes:

- ESR-12V router;
- Power cable;
- 19" rack mounting kit;
- Documentation.

ESR-12VF standard delivery package includes:

- ESR-12VF router;
- Power cable;
- 19" rack mounting kit;
- Documentation.

ESR-14VF standard delivery package includes:

- ESR-14VF router;
- Power cable;
- 19" rack mounting kit;
- Documentation.

ESR-100 standard delivery package includes:

- ESR-100 router;
- Power cable;
- 19" rack mounting kit;
- Documentation.

ESR-200 standard delivery package includes:

- ESR-200 router;
- Power cable;
- 19" rack mounting kit;
- Documentation.

ESR-1000 standard delivery package includes:

- ESR-1000 router;
- Power cable;
- Console port connection cable (RJ-45 – DB9F);
- 19" rack mounting kit;
- Documentation.

ESR-1200 standard delivery package includes:

- ESR-1200 router;
- Power cable;
- 19" rack mounting kit;
- Documentation.

ESR-1700 standard delivery package includes:

- ESR-1700 router;
- 19" rack mounting kit;
- Documentation.



Power module (PM-160-220/12 or PM-75-48/12) may be included in the ESR-1000, ESR-1200 delivery package on the customer's request.



Power module (PM350-220/12 or PM-35048/12) may be included in the ESR-1700 delivery package on the customer's request.



SFP/SFP+ transceivers may be included in the delivery package on the customer's request.

3 INSTALLATION AND CONNECTION

This section describes installation of the device into a rack and connection to a power supply.

3.1 Support brackets mounting

The delivery package includes support brackets for rack installation and mounting screws to fix the device case on the brackets. To install the support brackets:

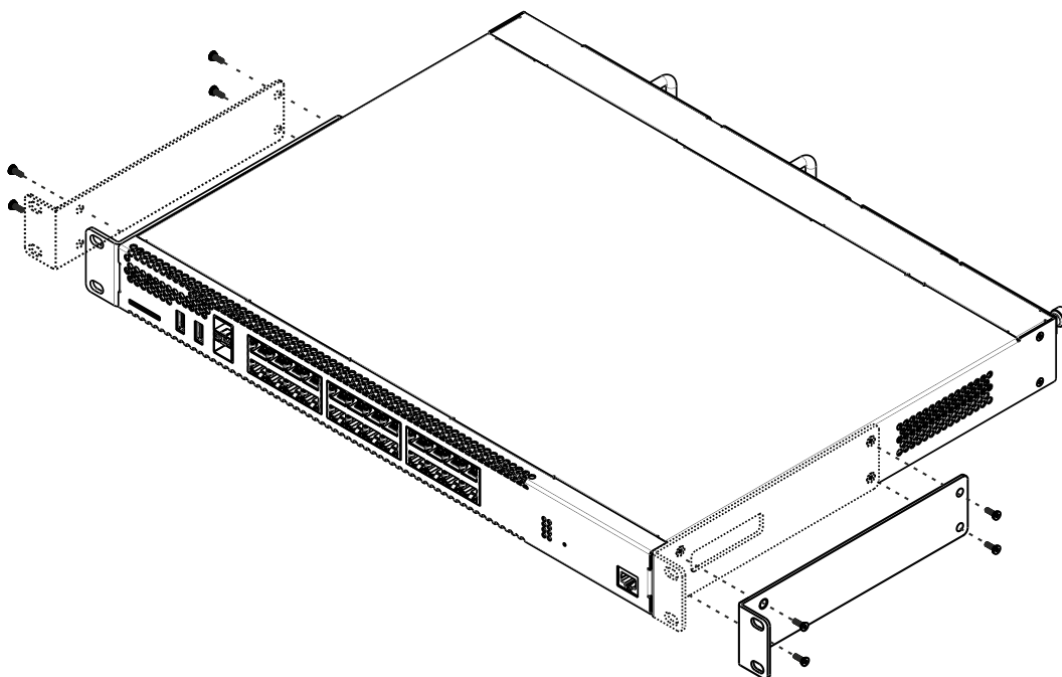


Figure 31 – Support brackets mounting

1. Align four mounting holes in the support bracket with the corresponding holes in the side panel of the device.
2. Use a screwdriver to screw the support bracket to the case.
3. Repeat steps 1 and 2 for the second support bracket.

3.2 Device rack installation

To install the device to the rack:

1. Attach the device to the vertical guides of the rack.
2. Align mounting holes in the support bracket with the corresponding holes in the rack guides. Use the holes of the same level on both sides of the guides to ensure the device horizontal installation.
3. Use a screwdriver to screw the router to the rack.

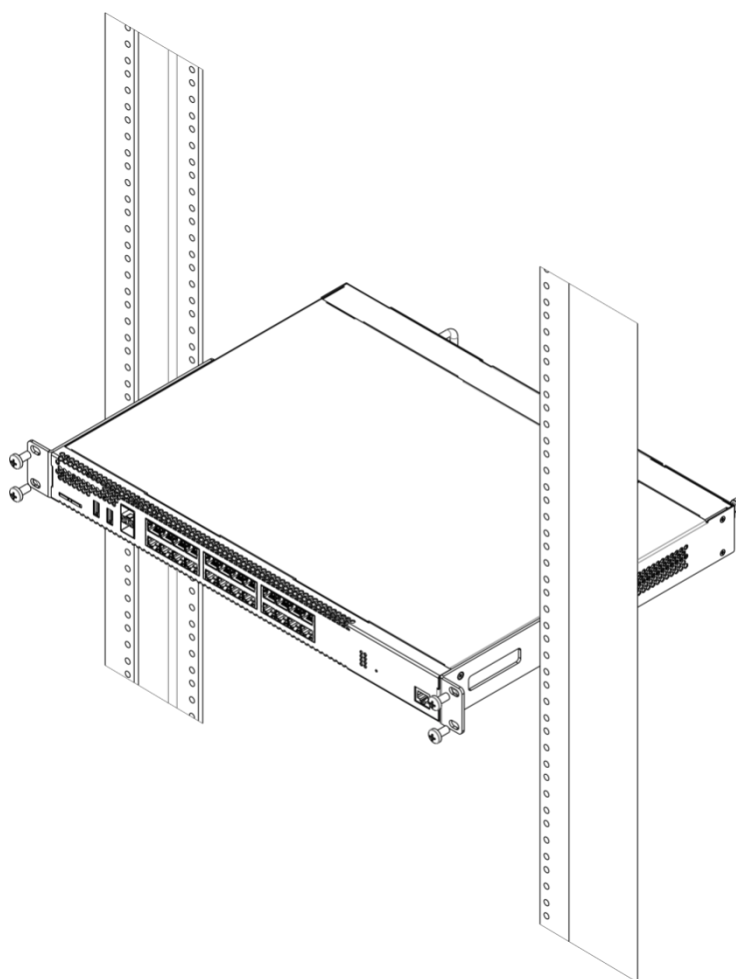


Figure 32 – Device rack installation



Device ventilation system is implemented using 'front-rear' layout. Vents are located on the front and side panels of the device; ventilation modules are located at the rear. Do not block air inlet and outlet vents to avoid components overheating and subsequent device malfunction.

3.3 ESR-1000, ESR-1200, ESR-1700 power module installation

ESR-1000/ESR-1200/ESR-1700 router can operate with one or two power modules. The second power module installation is necessary when the device operates under strict reliability requirements.

From the electric point of view, both places for power module installation are identical. In the context of device operation, the power module located closer to the edge is considered as the main module, and the one closer to the centre – as the backup module. Power modules can be inserted and removed without powering the device off. When additional power module is inserted or removed, the router continues operation without reboot.

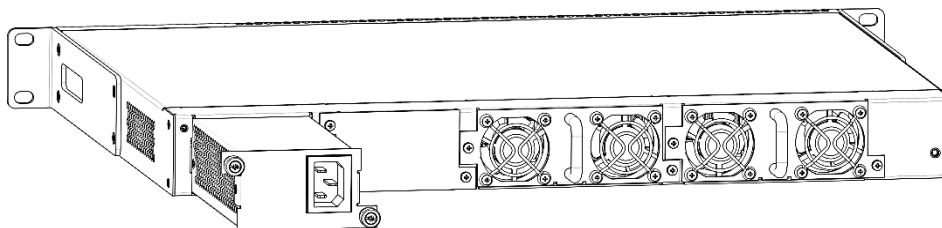


Figure 33 – Power module installation

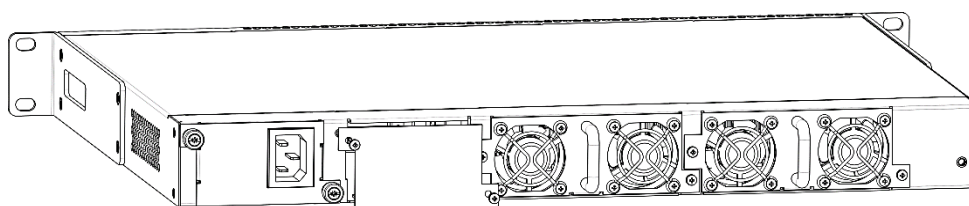


Figure 34 – Cover installation



Power module fault indication may be caused not only by the module failure, but also by the absence of the primary power supply.

You can check the state of power modules by the indication on the front panel of the router (see Section 2.4.7) or by diagnostics, available through the router management interfaces.

3.4 Connection to Power Supply

1. Ground the case of the device prior to connecting it to the power supply. An insulated multiconductor wire should be used for earthing. The device grounding and the earthing wire cross-section should comply with Electric Installation Code.
2. If a PC or another device is supposed to be connected to the router console port, the device should be also securely grounded.
3. Connect the power supply cable to the device. Depending on the delivery package, the device can be powered by AC or DC electrical network. To connect the device to AC power supply, use the cable from the delivery package. To connect the device to DC power supply, use the cable with cross-section not less than 1mm².
4. Turn the device on and check the front panel LEDs to make sure the terminal is in normal operating conditions.

3.5 SFP transceiver installation and removal



Optical modules can be installed when the terminal is turned on or off.

3.5.1 Transceiver installation

1. Insert the top SFP module into a slot with its open side down, and the bottom SFP module with its open side up.

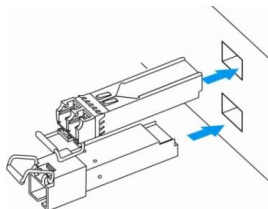


Figure 35 – SFP transceiver installation

2. Push the module into the device housing until it is secured with a clicking sound.

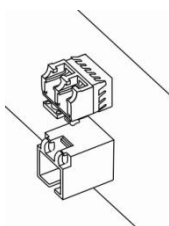


Figure 36 – Installed SFP transceivers

3.5.2 Transceiver removal

1. Flip the module handle to unlock the latch.

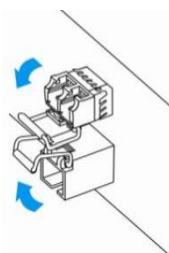


Figure 37 – Opening the Latch of SFP Transceivers

2. Remove the module from the slot.

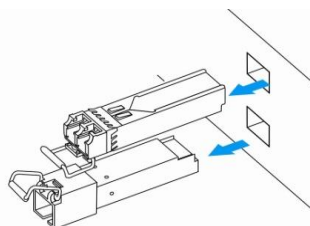


Figure 38 – SFP transceiver removal

4 MANAGEMENT INTERFACES

You may use various management interfaces in order to control and monitor the device.

To access the device, you may use network connection via Telnet or SSH as well as direct connection via RS-232 compliant console port. For Telnet, SSH or console port connections, the command line interface is used for device management.



Factory settings contain trusted zone description and IP address for device management access—192.168.1.1/24.

Trusted zone includes the following interfaces:

For ESR-10: GigabitEthernet 1/0/2-5;

For ESR-12V(F): GigabitEthernet 1/0/2-8;

For ESR-100: GigabitEthernet 1/0/2-4;

For ESR-200: GigabitEthernet 1/0/2-8;

For ESR-1000: GigabitEthernet 1/0/2-24;

For ESR-1200: GigabitEthernet 1/0/2-16, TengigabitEthernet 1/0/3-8.

For ESR-1700: GigabitEthernet 1/0/2-4, TengigabitEthernet 1/0/3-12.

By default, the user 'admin' with the password 'password' is defined in factory settings.

For each management interface provided, there are unified configuration operating principles. When modifying and applying the configuration, you should follow the specific sequence described herein that is intended to protect the device from misconfiguration.

4.1 Command line interface (CLI)

Command Line Interface (CLI) allows to perform the device management and monitor its operation and status. You will require the PC application supporting Telnet or SSH protocol operation or direct connection via the console port (e.g. HyperTerminal).

Command line interface enables user authorization and restricts access to commands depending on their access level, provided by the administrator.

You can create as many users as you like, access rights will be assigned individually to each user.


To ensure command line interface security, all commands are divided into 2 categories—privileged and unprivileged. Privileged commands basically include configuration commands. Unprivileged commands include monitoring commands.

The system allows multiple users to connect to the device simultaneously.

4.2 Types and naming procedure of router interfaces

Network interfaces of various types and purposes are used for the router operation. The naming system allows you to uniquely address the interfaces by their functional purpose and location in the system. The following table contains the list of interfaces types.

Table 31 – Types and naming procedure of router interfaces

Interface type	Designation
<p>Physical interfaces</p> <p>1Gbps ports</p> <p>10Gbps ports</p>	<p>Designation of physical interface includes its type and identifier. The identifier of physical interfaces is as follows: <UNIT>/<SLOT>/<PORT>, where</p> <ul style="list-style-type: none"> - <UNIT> – number of a device in a device group, - <SLOT> – device module number or “0” if the device does not consist of modules, - <PORT> – port sequence number. <p>gigabitethernet <UNIT>/<SLOT>/<PORT> Designation example: gigabitethernet 1/0/12 Note: It is permitted to use short name, for example, gi1/0/12.</p> <p>tengigabitethernet <UNIT>/<SLOT>/<PORT> Designation example: tengigabitethernet 1/0/2 Note: It is permitted to use short name, for example, te1/0/2.</p>
<p>Channel aggregation groups</p>	<p>Designation of channel aggregation group includes its type and identifier: port-channel <CHANNEL_ID> Designation example: port-channel 6</p> <p> It is permitted to use short name, for example, po1.</p>
<p>Sub-interfaces</p>	<p>Designation of sub-interface is generated from the designation of basic interface and sub-interface identifier (VLAN) separated by a dot. Designation example: gigabitethernet 1/0/12.100 tengigabitethernet 1/0/2.123 port-channel 1.6 Note: Sub-interface identifier may take values of [1..4094].</p>
<p>Q-in-Q interfaces</p>	<p>Designation of Q-in-Q interface is generated from the designation of basic interface, service VLAN identifier and user VLAN identifier separated by a dot. Designation example: gigabitethernet 1/0/12.100.10 tengigabitethernet 1/0/2.45.12 port-channel 1.6.34 Note: Service and user VLAN identifier may take values of [1..4094].</p>
<p>E1 interfaces</p>	<p>Designation of E1 interface includes its type and identifier. E1 interfaces identifier is as follows: <UNIT>/<SLOT>/<STREAM>, where</p> <ul style="list-style-type: none"> - <UNIT> – number of a device in a device group, - <SLOT> – number of device E1 module, - <STREAM> – E1 flow sequence number. <p>Designation example: e1 1/0/1</p>
<p>E1 channels aggregation groups</p>	<p>Designation of E1 channels aggregation group includes its type and interface sequence number: multilink <CHANNEL_ID> Designation example: multilink <CHANNEL_ID></p>
<p>Logical interfaces</p>	<p>Designation of logical interface is the interface sequence number: Designation example: loopback 4 bridge 60 service-port 1</p>



1. Number of interfaces of each type depends on the router model.
2. The current firmware does not support for devices stacking. A device number in unit device group can only take the value of 1.
3. Some commands support for simultaneous operation with the interface group. To specify the interface group, you may use a comma-separated list or specify a range of identifiers using a hyphen “-”.

Examples of interface groups specifying:

`interface gigabitethernet 1/0/1, gigabitethernet 1/0/5`

`interface tengigabitethernet 1/0/1-2`

`interface gi1/0/1-3,gi1/0/7,te1/0/1`

4.3 Types and naming procedure of router tunnels

Network tunnels of various types and purposes are used for the router operation. The naming system allows you to uniquely address the tunnels by their functional purpose. The following table contains the list of tunnels types.

Table 32 – Types and naming procedure of router tunnels

Tunnel type	Designation
L2TPv3 tunnel	Designation of L2TPv3 tunnel includes the type and sequence number of a tunnel: l2tpv3 <L2TPV3_ID> Designation example: l2tpv3 1/0/1
GRE tunnel	Designation of GRE tunnel includes the type and sequence number of a tunnel: gre <GRE_ID> Designation example: gre 1
SoftGRE tunnel	Designation of SoftGRE tunnel includes the type and sequence number of a tunnel and, optionally, a virtual interface VLAN ID: softgre <GRE_ID>[.<VLAN>] Designation example: e1 1/1/10
IPv4-over-IPv4 tunnel	Designation of IPv4-over-IPv4 tunnel includes the type and sequence number of a tunnel: ip4ip4 <IPIP_ID> Designation example: ip4ip4 1/0/1
IPsec tunnel	Designation of IPsec tunnel includes the type and sequence number of a tunnel: vti <VTI_ID> Designation example: vti 1
Logical tunnel (tunnel between VRF)	Designation of logical tunnel includes the type and sequence number of a tunnel: lt <LT_ID> Designation example: lt 1



Number of tunnels of each type depends on the router model and firmware version.

5 INITIAL ROUTER CONFIGURATION

5.1 ESR router factory settings

The device is shipped to the consumer with the factory configuration installed that includes essential basic settings. Factory configuration allows you to use the router as a gateway with SNAT without applying any additional settings. Also, factory configuration contains settings that allow you to obtain network access to the device for advanced configuration.

5.1.1 Description of factory settings

To establish network connection, the configuration features 2 security zones named 'Trusted' for local area network and 'Untrusted' for public network. All interfaces are divided between two security zones:

1. 'Untrusted' zone is meant for a public network (WAN) connection. In this zone, DHCP ports are open in order to obtain dynamic IP address from the provider. All incoming connections from this zone to the router are blocked.

This security zone includes the following interfaces:

For ESR-10/12V: GigabitEthernet 1/0/1;

For ESR-12VF, ESR-14VF: GigabitEthernet 1/0/1; GigabitEthernet 1/0/9;

For ESR-100/200: GigabitEthernet 1/0/1;

For ESR-1000/1200/1700: GigabitEthernet1/0/1, TengigabitEthernet1/0/1, TengigabitEthernet1/0/2.

Zone interfaces are grouped into a single L2 segment via *Bridge 2* network bridge.

2. 'Trusted' zone is meant for a local area network (LAN) connection. In this zone, the following ports are open: Telnet and SSH ports for remote access, ICMP ports for router availability test, DHCP ports for clients obtaining IP addresses from the router. Outgoing connections from this zone into the Untrusted zone are allowed.

This security zone includes the following interfaces:

For ESR-10: GigabitEthernet 1/0/2-6;

For ESR-12V(F): GigabitEthernet 1/0/2-8;

For ESR-100: GigabitEthernet 1/0/2-4;

For ESR-200: GigabitEthernet1/0/2-8;

For ESR-1000: GigabitEthernet1/0/2-24;

For ESR-1200: GigabitEthernet1/0/2-16, TengigabitEthernet1/0/3-8;

For ESR-1700: GigabitEthernet1/0/2-4, TengigabitEthernet1/0/3-12.

Zone interfaces are grouped into a single L2 segment via *Bridge 1* network bridge.

On the *Bridge 2* interface, DHCP client is enabled to obtain dynamic IP address from the provider. On *Bridge 1* interface, static IP address 192.168.1.1/24 is configured. Created IP address acts as a gateway for LAN clients. For LAN clients, DHCP address pool 192.168.1.2-192.168.1.254 is configured with the mask 255.255.255.0. For clients in order to access the Internet, the router should have Source NAT service enabled.

Security zone policies have the following configuration:

Table 33 – Security zone policy description

Traffic origin zone	Traffic destination zone	Traffic type	Action
Trusted	Untrusted	TCP, UDP, ICMP	enabled
Trusted	Trusted	TCP, UDP, ICMP	enabled
Trusted	self	TCP/23(Telnet), TCP/22(SSH), ICMP, UDP/67(DHCP Server), UDP/123(NTP)	enabled
Untrusted	self	UDP/68(DHCP Client),	enabled



To enable device configuration on the first startup, 'admin' account has been created in the router configuration. We strongly recommend to change administrator password during the initial configuration of the router.



To enable network access to the router on the first startup, static IP address 192.168.1.1/24 has been configured on *Bridge 1* interface.

5.2 Router connection and configuration

ESR series routers are intended to perform border gateway functions and securing the user network when it is connected to public data networks.

Basic router configuration should include:

- Assigning IP addresses (static or dynamic) to the interfaces that participate in data routing;
- Creation of security zones and distribution of interfaces between these zones;
- Creation of policies governing data transfer through these zones;
- Configuration of services that accompany the data routing (NAT, Firewall, etc.).

Advanced settings depend on the requirements of the specific device application pattern and may be easily added or modified with the existing management interfaces.

5.2.1 Connection to the router

There are several device connection options:

5.2.1.1 Ethernet LAN connection



Upon the initial startup, the router starts with the factory configuration. For factory configuration description, see Section 5.1 *ESR router factory settings* of this Manual.

Connect the network data cable (patch cord) to any port within the **'Trusted'** zone and to the PC intended for management tasks.

In the router factory configuration, DHCP server is enabled with IP address pool in **192.168.1.0/24** subnet.

When network interface is connected to the management computer, the latter should obtain the network address from the server.

If IP address is not obtained for some reason, assign the interface address manually using any address except for 192.168.1.1 in 192.168.1.0/24 subnet.

5.2.1.2 RS-232 console port connection

Using RJ-45/DBF9 cable included into device delivery package, connect the router **'Console'** port to the computer RS-232 port.

Launch terminal application (e.g. HyperTerminal or Minicom) and create a new connection. VT100 terminal emulation mode should be used.

Specify the following settings for RS-232 interface:

Bit rate: 115200bps
Data bits: 8bit
Parity: no
Stop bits: 1
Flow control: none

5.2.2 Applying the configuration change

Any changes made in the configuration will take effect only after applying the command:

```
esr# commit  
Configuration has been successfully committed
```

After applying the command above, the configuration rollback timer is started. To stop the timer and rollback mechanism, use the following command:

```
esr# confirm  
Configuration has been successfully confirmed
```

The default value of rollback timer is 600 seconds. To change the timer settings, use the following command:

```
esr(config)# system config-confirm timeout <TIME>
```

<TIME> – time period of configuration confirmation pending, takes value in seconds [120..86400].

5.2.3 Basic router configuration

Upon the first startup, the router configuration procedure includes the following steps:

- Changing password for "admin" user.
- Creation of new users.
- Assigning device name (Hostname).

- Setting parameters for public network connection in accordance with the provider requirements.
- Configuring remote connection to router.
- Applying basic settings.

5.2.3.1 Changing password for "admin" user.

To ensure the secure system access, you should change the password for the privileged 'admin' user.



'techsupport' account ('eltex' up to version 1.0.7) is required for service centre specialist remote access.

'remote' account – RADIUS, TACACS+, LDAP authentication.

'admin', 'techsupport', 'remote' users cannot be deleted. You may only change passwords and a privilege level.

Username and password are required for login during the device administration sessions.

To change 'admin' password, use the following commands:

```
esr# configure
esr(config)# username admin
esr(config-user)# password <new-password>
esr(config-user)# exit
```

5.2.3.2 Creation of new users

Use the following commands to create a new system user or configure the username, password, or privilege level:

```
esr(config)# username <name>
esr(config-user)# password <password>
esr(config-user)# privilege <privilege>
esr(config-user)# exit
```



Privilege levels 1–9 allow you to access the device and view its operation status, but the device configuration is disabled. Privilege levels 10–14 allow both the access to the device and configuration of majority of its functions. Privilege level 15 allows both the access to the device and configuration of all its functions.

Example of commands, that allow you to create user 'fedor' with password '12345678' and privilege level 15 and create user 'ivan' with password 'password' and privilege level '1':

```
esr# configure
esr(config)# username fedor
esr(config-user)# password 12345678
esr(config-user)# privilege 15
esr(config-user)# exit
esr(config)# username ivan
esr(config-user)# password password
esr(config-user)# privilege 1
esr(config-user)# exit
```

5.2.3.3 Assigning device name

To assign the device name, use the following commands:

```
esr# configure
esr(config)# hostname <new-name>
```

When a new configuration is applied, command prompt will change to the value specified by **<new-name>** parameter.

5.2.3.4 Configuration of public network parameters

To configure router network interface in the public network, you should assign parameters defined by the network provider – default IP address, subnet mask and gateway address – to the device.

Example of static IP address configuration commands for **GigabitEthernet 1/0/2.150** sub-interface used for obtaining access to the router via **VLAN 150**.

Interface parameters:

- IP address: 192.168.16.144;
- Subnet mask: 255.255.255.0;
- Default gateway IP address: 192.168.16.1.

```
esr# configure
esr(config)# interface gigabitethernet 1/0/2.150
esr(config-subif)# ip address 192.168.16.144/24
esr(config-subif)# exit
esr(config)# ip route 0.0.0.0/0 192.168.16.1
```

To ensure the correct IP address assigning for the interface, enter the following command when the configuration is applied:

```
esr# show ip interfaces
```

IP address	Interface	Type
192.168.16.144/24	gigabitethernet 1/0/2.150	static

Provider may use dynamically assigned addresses in their network. If there is DHCP server in the network, you can obtain the IP address via DHCP protocol.

Configuration example for obtaining dynamic IP address from DHCP server on **GigabitEthernet 1/0/10** interface:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/10
esr(config-if)# ip address dhcp
esr(config-if)# exit
```

To ensure the correct IP address assigning for the interface, enter the following command when the configuration is applied:

```
esr# show ip interfaces
```

IP address	Interface	Type
------------	-----------	------

192.168.11.5/25

gigabitethernet 1/0/10

DHCP

5.2.3.5 Configuring remote connection to router.

In the factory configuration, remote access to the router may be established via Telnet or SSH from the **'trusted'** zone. To enable remote access to the router from other zones, e.g. from the public network, you should create the respective rules in the firewall.

When configuring access to the router, rules should be created for the following pair of zones:

- **source-zone** – zone that the remote access will originate from;
- **self** – zone which includes router management interface.

Use the following commands to create the allowing rule:

```
esr# configure
esr(config)# security zone-pair <source-zone> self
esr(config-zone-pair)# rule <number>
esr(config-zone-rule)# action permit
esr(config-zone-rule)# match protocol tcp
esr(config-zone-rule)# match source-address <network object-group>
esr(config-zone-rule)# match destination-address <network object-group>
esr(config-zone-rule)# match source-port any
esr(config-zone-rule)# match destination-port <service object-group>
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# exit
```

Example of commands that allow users from **'untrusted'** zone with IP addresses in range **132.16.0.5-132.16.0.10** to connect to the router with IP address **40.13.1.22** via SSH:

```
esr# configure
esr(config)# object-group network clients
esr(config-addr-set)# ip address-range 132.16.0.5-132.16.0.10
esr(config-addr-set)# exit
esr(config)# object-group network gateway
esr(config-addr-set)# ip address-range 40.13.1.22
esr(config-addr-set)# exit
esr(config)# object-group service ssh
esr(config-port-set)# port-range 22
esr(config-port-set)# exit
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 10
esr(config-zone-rule)# action permit
esr(config-zone-rule)# match protocol tcp
esr(config-zone-rule)# match source-address clients
esr(config-zone-rule)# match destination-address gateway
esr(config-zone-rule)# match source-port any
esr(config-zone-rule)# match destination-port ssh
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# exit
```

6 FIRMWARE UPDATE

6.1 Updating firmware via system resources



To update the firmware, use any of the following servers: TFTP, FTP, SCP. Router firmware files obtained from the manufacturer should be allocated on the server.

The router stores two copies of the firmware. To ensure the reliability of the firmware update procedure, only the copy that was not used for the last device startup is available for the update.



When update the firmware, the router configuration is converted according to a new version.

When loading a router with an older software version than the previously loaded configuration, the configuration is not converted and is subsequently deleted.



Update via system resources is available in version 1.0.3.69 and later. You may update the firmware from the earlier versions using the instructions located in Section 6.2.

To update the firmware for the device running the operating system, follow procedure described below.

1. Prepare the selected server for operation. You should know the server address; also firmware distributive file should be loaded onto the server.
2. The router should be prepared for operation according to the documentary requirements. Router configuration should allow for data exchange with the server via TFTP/FTP/SCP and ICMP protocols. At that, you should take into account the server inherence to the router security zones.
3. Connect to the router locally via Console port or remotely via Telnet or SSH.

Check the server availability for the router using *ping* command on the router. If the server is not available, check the router settings and the status of the server network interfaces.

4. To update the router firmware, enter the following command. Specify IP address of the server being used as *<server>* parameter. For updates that utilize FTP or SCP server, you should enter a username (*<user>* parameter) and a password (*<password>* parameter). Specify the name of the firmware file loaded onto the server as *<file_name>* parameter. When the command is executed, router will copy the file into its internal memory, perform data integrity check and save it into non-volatile memory.

TFTP:

```
esr# copy tftp://<server>:<file_name> system:firmware
```

FTP:

```
esr# copy ftp://[<user>[:<password>]@]<server>:<file_name>
system:firmware
```

SCP:

```
esr# copy scp://[<user>[:<password>]@]<server>://<folder>/<file_name>
system:firmware
```

For example, let's update basic firmware via SCP:

```
esr# copy scp://adm:password123@192.168.16.168://home/tftp/firmware
system:firmware
```

- To start the device with the new firmware version, you have to switch the active image. With *show bootvar* command, locate the image number, containing updated firmware.

```
esr# show bootvar
Image  Version                               Date                               Status  After
reboot
-----
----
1      1.0.4 build 141[f812808]               date 18/02/2015 time               Active  *
16:12:54
2      1.0.4 build 141[f812808]               date 18/02/2015 time               Not Active
16:12:54
```

Use the following command to select the image:

```
esr# boot system image-[1|2]
```

- To update the secondary bootloader (U-Boot), enter the following command: Specify IP address of the server being used as *<server>* parameter. For updates that utilize FTP or SCP server, you should enter a username (*<user>* parameter) and a password (*<password>* parameter). Specify the name of the secondary bootloader onto the server as *<file_name>* parameter (when using SCP, you should specify a full pathname – *<folder>* parameter). When the command is executed, router will copy the file into its internal memory, perform data integrity check and save it into non-volatile memory.

TFTP:

```
esr# copy tftp://<server>:/<file_name> system:boot
```

FTP:

```
esr# copy ftp://<server>:/<file_name> system:boot
```

SCP:

```
esr# copy scp://[<user>[:<password>]@]<server>://<folder>/<file_name>
system:boot
```

6.2 Updating firmware via bootloader

Router firmware may be updated via the bootloader as follows:

- When U-Boot finishes the router initialization, break the device startup with the **<Esc>** key.

```
Configuring PoE...
distribution 1 dest_threshold 0xa drop_timer 0x0
Configuring POE in bypass mode
```



```

NAE configuration done!
initializing port 0, type 2.
initializing port 1, type 2.
SMC Endian Test:b81fb81f
nae-0, nae-1
=====Skip: Load SYS UCORE for old 8xxB1/3xxB0 revision on default.
Hit any key to stop autoboot: 2

```

2. Specify TFTP server address:

```
BRCM.XLP316Lite Rev B0.u-boot# setenv serverip 10.100.100.1
```

3. Specify router IP address:

```
BRCM.XLP316Lite Rev B0.u-boot# setenv ipaddr 10.100.100.2
```

4. You may save the environment using 'saveenv' command for future updates.

5. Launch firmware update procedure:

```
BRCM.XLP316Lite Rev B0.u-boot# run tftp_update_image1
BRCM.XLP316Lite Rev B0.u-boot# run set_bootpart_1
```

```

Using nae-0-3 device
TFTP from server 10.100.100.1; our IP address is 10.100.100.2
Filename 'esr1000/firmware'.
Load address: 0xa800000060000000
Loading: TftpStart:TftpTimeoutMsecs = 10000, TftpTimeoutCountMax = 6
#####
#####
#####
#####
#####
#####
done
Bytes transferred = 64453909 (3d77d15 hex)
Device 0: MT29F8G08ABBCAH4 ... is now current device

NAND erase: device 0 offset 0x1440000, size 0x6400000
Bad block table found at page 262080, version 0x01
Bad block table found at page 262016, version 0x01
Erasing at 0x7800000 -- 1895825408% complete..
OK

NAND write: device 0 offset 0x1440000, size 0x6400000
104857600 bytes written: OK

```

6. Run the downloaded software:

```
BRCM.XLP316Lite Rev B0.u-boot# reset
```

6.3 Secondary bootloader update (U-Boot)

Secondary bootloader initializes NAND and the router. During the update, a new file of the secondary bootloader is saved to the flash

To view the current version of the load file operating on the device, execute 'version' command in U-Boot CLI. Also, the version is displayed during the router startup:

```
BRCM.XLP316Lite Rev B0.u-boot# version  
BRCM.XLP.U-Boot:1.1.0.47 (29/11/2016 - 19:00:24)
```

Firmware update procedure:

1. When U-Boot finishes the router initialization, break the device startup with the <Esc> key.

```
Configuring PoE...  
distribution 1 dest_threshold 0xa drop_timer 0x0  
Configuring POE in bypass mode  
NAE configuration done!  
initializing port 0, type 2.  
initializing port 1, type 2.  
SMC Endian Test:b81fb81f  
nae-0, nae-1  
=====Skip: Load SYS UCORE for old 8xxB1/3xxB0 revision on default.  
Hit any key to stop autoboot: 2
```

2. Specify TFTP server address:

```
BRCM.XLP316Lite Rev B0.u-boot# setenv serverip 10.100.100.1
```

3. Specify router IP address:

```
BRCM.XLP316Lite Rev B0.u-boot# setenv ipaddr 10.100.100.2
```

4. You may save the environment using 'saveenv' command for future updates.

5. Launch firmware update procedure:

```
BRCM.XLP316Lite Rev B0.u-boot# run upd_uboot or BRCM.XLP316LiteRevB0.u-boot#  
runtftp_update_uboot, depends on the bootloader version
```

```
Using nae-1 device  
TFTP from server 10.100.100.1; our IP address is 10.100.100.2  
Filename 'esr1000/u-boot.bin'.  
Load address: 0xa800000078020000  
Loading: #####  
done  
Bytes transferred = 852648 (d02a8 hex)  
SF: Detected MX25L12805D with page size 256, total 16777216 bytes  
16384 KiB MX25L12805D at 0:0 is now current device
```

6. Reboot the router:

```
BRCM.XLP316Lite Rev B0.u-boot# reset
```

7 ROUTER CONFIGURATION EXAMPLES

7.1 VLAN Configuration

VLAN (Virtual Local Area Network) is a logical (virtual) local area network that represents a group of devices, which communicate on channel level regardless of their physical location. VLAN operation is based on the use of additional Ethernet header fields according to 802.1q standard. In fact, VLAN isolates the broadcast domain by limiting the switching of only those Ethernet frames which have the same VLAN-ID in the Ethernet header.

7.1.1 Configuration algorithm

Step	Description	Command	Keys
1	Create VLAN	<code>esr(config)# vlan <VID></code>	<VID> – VLAN identifier, set in the range of [2..4094]. It is also possible to create multiple vlan (with a comma) or vlan range (with a hyphen).
2	Specify vlan name (optionally)	<code>esr(config-vlan)# name <vlan-name></code>	<vlan-name> – up to 255 characters.
3	Disable monitoring of the status of interfaces on which processing of the given VLAN Ethernet frames is allowed (optionally)	<code>esr(config-vlan)# force-up</code>	
4	Disable the processing of incoming untagged Ethernet frames based on the default VLAN's switching table (VLAN-ID – 1) (optionally)	<code>esr(config-if-gi)# no switchport forbidden default-vlan</code>	
5	Set L2 interface operation mode	<code>esr(config-if-gi)# switchport access</code>	Only for ESR-10/12V(F)/14VF/100/200. This mode is the default mode and is not displayed in the configuration.
		<code>esr(config-if-gi)# switchport trunk</code>	Only for ESR-10/12V(F)/14VF/100/200.
		<code>esr(config-gi)# switchport general</code>	Only for ESR-1000/1200/1700. This mode is the default mode and is not displayed in the configuration.
6	Configure VLAN list on the interface in tagged mode	<code>esr(config-if-gi)# switchport trunk allowed vlan add <VID></code>	For ESR-10/12V(F)/14VF/100/200. <VID> – VLAN identifier, set in the range of [2..4094]. It is also possible to create multiple vlan (with a comma) or vlan range (with a hyphen).
		<code>esr(config-if-gi)# switchport general allowed vlan add <VID> tagged</code>	For ESR-1000/1200/1700. <VID> – VLAN identifier, set in the range of [2..4094]. It is also possible to create multiple vlan (with a comma) or vlan range (with a hyphen).
7	Configure VLAN on the interface in tagged mode (optionally)	<code>esr(config-if-gi)# switchport trunk native-vlan <VID></code>	For ESR-10/12V(F)/14VF/100/200. <VID> – VLAN identifier, set in the range of [2..4094].

		<code>esr(config-if-gi)# switchport general allowed vlan add <VID> untagged</code>	For ESR-1000/1200/1700. <VID> – VLAN identifier, set in the range of [2..4094].
8	Enable the processing of Ethernet frames of all created VLANs on the interface (optionally)	<code>esr(config-if-gi)# switchport trunk allowed vlan auto-all</code>	Only for ESR-10/12V(F)/14VF/100/200.
		<code>esr(config-if-gi)# switchport general allowed vlan auto-all</code>	Only for ESR-1000/1200/1700.

7.1.2 Configuration example 1. VLAN removal from the interface

Objective:

On the basis of the factory configuration, remove gi1/0/1 port from VLAN 2.

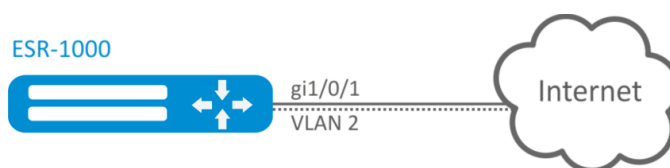


Figure 39 – Network structure

Solution:

Remove VLAN2 from gi1/0/1 port:

```
esr(config)# interface gi 1/0/1
esr(config-if-gi)# switchport general allowed vlan remove 2 untagged
esr(config-if-gi)# no switchport general pvid
```

7.1.3 Configuration example 2. Enabling VLAN processing in tagged mode

Objective:

Configure gi1/0/1 and gi1/0/2 ports for packet transmission and reception in VLAN 2, VLAN 64, VLAN 2000.

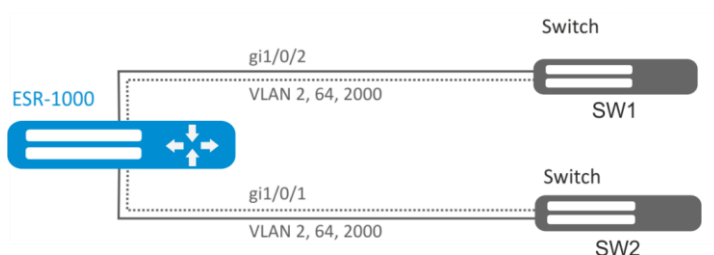


Figure 40 – Network structure

Solution:

Create VLAN 2, VLAN 64, VLAN 2000 on ESR-1000:

```
esr-1000(config)# vlan 2,64,2000
```

Specify VLAN 2, VLAN 64, VLAN 2000 for gi1/0/1-2 port:

```
esr-1000(config)# interface gi1/0/1
esr-1000(config-if-gi)# switchport forbidden default-vlan
esr-1000(config-if-gi)# switchport general allowed vlan add 2,64,2000 tagged
```

7.1.4 Configuration example 3. Enabling VLAN processing in tagged and untagged modes

Objective:

Configure gi1/0/1 ports for packet transmission and reception in VLAN 2, VLAN 64, VLAN 2000 in trunk mode, configure gi1/0/2 port in access mode for VLAN 2 on ESR-100/ESR -200.

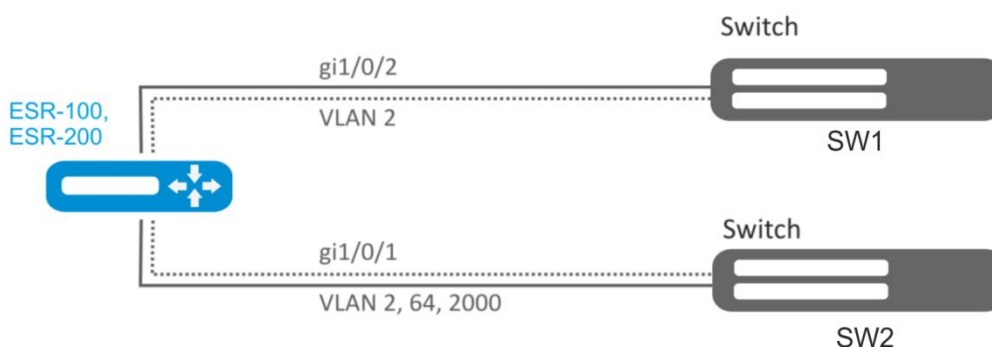


Figure 41 – Network structure

Solution:

Create VLAN 2, VLAN 64, VLAN 2000 on ESR-100/ ESR-200:

```
esr(config)# vlan 2,64,2000
```

Specify VLAN 2, VLAN 64, VLAN 2000 for gi1/0/1 port:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# switchport forbidden default-vlan
esr(config-if-gi)# switchport mode trunk
esr(config-if-gi)# switchport trunk allowed vlan add 2,64,2000
```

Specify VLAN2 to gi1/0/2 port:

```
esr(config)# interface gi1/0/2
esr(config-if-gi)# switchport access vlan 2
```

7.2 LLDP configuration

Link Layer Discovery Protocol (LLDP) is a data link layer protocol allowing network equipment to notify the devices operating in a local network of its existence and to transmit parameters to it as well as to receive similar information.

7.2.1 Configuration algorithm

Step	Description	Command	Keys
1	Enable LLDP on the router	<code>esr(config)# lldp enable</code>	
2	Set the period during which the router keeps the information received via LLDP (optionally)	<code>esr(config)# lldp hold-multiplier <SEC></code>	<SEC> – time interval in seconds, takes values of [1..10].
3	Set IP address which will be transmitted to LLDP TLV as the management-address (optionally)	<code>esr(config)# lldp management-address <ADDR></code>	<ADDR> – IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]. One of the existent is set by default
4	Set the system-description field which will be transmitted to LLDP TLV as the system-description. (optionally)	<code>esr(config)# lldp system-description <DESCRIPTION></code>	<DESCRIPTION> – system description, set by the string of up to 255 characters. By default contains the information of the router model and firmware version.
5	Set the system-name field which will be transmitted to LLDP TLV as the system-name. (optionally)	<code>esr(config)# lldp system-name <NAME></code>	<NAME> – system name, set by the string of up to 255 characters. By default coincides with the specified hostname
6	Set the LLDPDU sending period (optionally)	<code>esr(config)# lldp timer <SEC></code>	<SEC> – time interval in seconds, takes values of [1..32768].
7	Enable the LLDPDU receiving and proceeding on the physical interface.	<code>esr(config-if-gi)# lldp receive</code>	
8	Enable the LLDPDU sending on the physical interface.	<code>esr(config-if-gi)# lldp transmit</code>	

7.2.2 Configuration example

Objective:

Organize the LLDPDU exchange and proceeding between ESR-1 and ESR-2 routers.

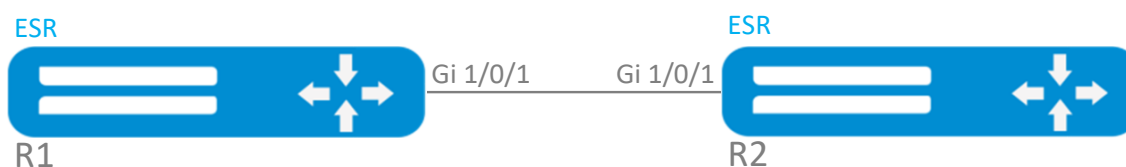


Figure 42 – Network structure

Solution:

1. R1 configuration

Enable LLDP globally on the router:

```
esr(config)# lldp enable
```

Enable the receiving and transmission of LLDPDU on the gi 1/0/1 interface.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# lldp receive
```

```
esr(config-if-gi)# lldp transmit
```

2. R2 configuration

Enable LLDP globally on the router:

```
esr(config)# lldp enable
```

Enable the receiving and transmission of LLDPDU on the gi 1/0/1 interface.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# lldp receive
esr(config-if-gi)# lldp transmit
```

To view LLDP neighbors information, use the following command:

```
esr# show lldp neighbors
```

To view more detailed information on the certain interface neighbor, use the following command:

```
esr# show lldp neighbors gigabitethernet 1/0/1
```

To view LLDP statistics, use the following command:

```
esr# show lldp statistics
```

7.3 LLDP MED configuration

LLDP MED — LLDP standard enhancement which allows to transmit network policies: VLAN ID, DSCP, priority.

7.3.1 Configuration algorithm

Step	Description	Command	Keys
1	Enable LLDP on the router	<code>esr(config)# lldp enable</code>	
2	Enable MED LLDP enhancement on the router	<code>esr(config)# lldp med fast-start enable</code>	
3	Create network policy	<code>esr(config)# network-policy <NAME></code>	<NAME> – network-policy name, set by the string of up to 31 characters.
4	Specify the application type	<code>esr(config-net-policy)# application <APP_TYPE></code>	<APP-TYPE> – type of the application for which network-policy will be enabled. Takes the following values: voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling.
5	Set DSCP value	<code>esr(config-net-policy)# dscp <DSCP></code>	<DSCP> – DSCP code value, takes values in the range of [0..63].

6	Set COS value	<code>esr(config-net-policy)# priority <PRIORITY></code>	<COS> – priority value, takes the following values: best-effort – COS0; background – COS1; excellent-effort – COS2; critical-applications – COS3; video – COS4; voice – COS5; internetwork-control – COS6; network-control – COS7.
7	Set VLAN ID value	<code>esr(config-net-policy)# vlan <VID> [tagged]</code>	<VID> – VLAN ID, takes values of [1..4094]; tagged – key, during the installation of which, the subscriber device will send Ethernet frames of the specified application in a tagged form.
8	Set a network policy on the interface	<code>esr(config-if-gi)# lldp network-policy <NAME></code>	<NAME> – network-policy name, set by the string of up to 31 characters.
9	Enable LLDPDU transmission on the physical interface.	<code>esr(config-if-gi)# lldp transmit</code>	

7.3.2 Voice VLAN configuration example

Voice VLAN — VLAN ID, in receiving of which an IP phone switches to the trunk mode with the specified VLAN ID for VoIP traffic reception and transmission. VLAN ID transmission is performed by LLDP MED enhancement.

Objective:

VoIP traffic and data traffic should be grouped in different VLANs - vid 10 for data and vid 20 for VoIP - and the sending of Voice VLAN from the gi 1/0/1 ESR port should be configured. Voice VLAN should be supported and enabled on the IP phone.



Figure 43 – Network structure

Solution:

Use ESR-12V as an example

First create VLAN 10 and 20 and configure the gi 1/0/1 interface in the trunk mode:

```
esr(config)# vlan 10,20
esr(config-vlan)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# switchport mode trunk
esr(config-if-gi)# switchport trunk allowed vlan add 10,30
esr(config-if-gi)# exit
```


Enable LLDP and MED capability in LLDP globally on the router:

```
esr(config)# lldp enable
esr(config)# lldp med fast-start enable
```

Create and configure network policy in the way that VLAN ID 20 is specified for the voice application:

```
esr(config)# network-policy VOICE_VLAN
esr(config-net-policy)# application voice
esr(config-net-policy)# vlan 20 tagged
esr(config-net-policy)# exit
```

Configure LLDP on the interface and set a network policy:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# lldp transmit
esr(config-if-gi)# lldp receive
esr(config-if-gi)# lldp network-policy VOICE_VLAN
esr(config-if-gi)# exit
```

7.4 Sub-interface termination configuration

To terminate Ethernet frames of a certain VLAN on a specific physical interface, you need to create a sub-interface with the number of VLAN, frames of which will be terminated. When creating two sub-interfaces having the same VLAN but located on different physical/aggregated interfaces, switching of Ethernet frames between these sub-interfaces will not be possible as external segments will be separate broadcast domains. For data exchange between subscribers of different sub-interfaces (even with the same VLAN-ID) routing will be used, i.e. data exchange will occur at the third level of the OSI model.

7.4.1 Configuration algorithm

Step	Description	Command	Keys
1	Create a sub-interface of a physical interface.	<code>esr(config)# interface gigabitethernet <PORT>.<S-VLAN></code> or <code>interface tengigabitethernet <PORT>.<S-VLAN></code> or <code>interface port-channel <CH>.<S-VLAN></code>	<PORT> – physical interface number. <CH> – aggregated interface number. <S-VLAN> – identifier of created S-VLAN. If a physical interface is included in bridge-group, it will be impossible to create sub-interface.
2	Specify sub-interface description (optionally).	<code>esr(config-subif)# description <DESCRIPTION></code>	<DESCRIPTION> – interface description, set by the string of up to 255 characters.
3	Specify VRF instance, in which the given sub-interface will operate (optionally).	<code>esr(config-subif)# ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.
4	Set the time interval during which statistics on the sub-interface load is collected. (optionally).	<code>esr(config-subif)# load-average <TIME></code>	<TIME> – interval in seconds, takes values of [5..150].
5	Enable bridge-group sub-interface (optionally).	<code>esr(config-subif)#bridge-group <BRIDGE-ID></code>	<BRIDGE-ID> – bridge identifying number.

6	Set the lifetime of IPv4/IPv6 entries in the ARP table studied on the given interface (optionally).	<pre>esr(config-subif)# ip arp reachable-time <TIME> or ipv6 nd reachable-time <TIME></pre>	<TIME> – lifetime of dynamic MAC addresses, in milliseconds. Allowed values are from 5000 to 100000000 milliseconds. Real time of the entry update varies from [0,5;1,5]*<TIME>.
---	---	---	--

7.4.2 Sub-interface configuration example

Objective:

Configure 192.168.3.1/24 network termination in VLAN: 828 on gigabitethernet 1/0/1 physical interface.

Solution:

Create sub-interface for VLAN: 828

```
esr(config)# interface gigabitethernet 1/0/1.828
```

Configure IP address from necessary subnet.

```
esr(config)# interface gigabitethernet 1/0/1.828
esr(config-subif)# ip address 192.168.3.1/24
esr(config-subif)# exit
```



In addition to assigning an IP address, you must either disable the firewall or configure the corresponding security zone on the sub interface.

7.5 QinQ termination configuration

QinQ is a technology of packet transmission with two 802.1q tags. The technology is used for extending quantity of VLANs in data networks. 802.1q header, which is closer to payload, is an Inner Tag also known as C-VLAN (Customer VLAN). 802.1q header, which is comes before C-VLAN, is an Outer Tag also known as S-VLAN (Service VLAN). Using of double tags in Ethernet frames is describing by 802.1ad protocol.

7.5.1 Configuration algorithm

Step	Description	Command	Keys
1	Create a sub-interface of a physical interface.	<pre>esr(config)# interface gigabitethernet <PORT>.<S-VLAN> or interface tengigabitethernet <PORT>.<S-VLAN> or interface port-channel <CH>.<S-VLAN></pre>	<PORT> – physical interface number. <CH> – aggregated interface number. <S-VLAN> – identifier of created S-VLAN.
2	Create q-in-q interface	<pre>esr(config)# interface gigabitethernet <PORT>.<S-VLAN>.<C-VLAN> or esr(config)# interface</pre>	<PORT> – physical interface number. <CH> – aggregated interface number. <S-VLAN> – identifier of created S-VLAN.

		<code>tengigabitethernet <PORT>.<S-VLAN>.<C-VLAN></code> or <code>esr(config)# interface port-channel <CH>.<S-VLAN>.<C-VLAN></code>	<C-VLAN> – identifier of created C-VLAN. If a physical interface or a sub-interface is included in bridge-group, it will be impossible to create sub-interface.
3	Specify q-in-q interface description (optionally).	<code>esr(config-qinq-if) # description <DESCRIPTION></code>	<DESCRIPTION> – interface description, set by the string of up to 255 characters.
4	Specify VRF instance, in which the given q-in-q interface will operate (optionally).	<code>esr(config-qinq-if) # ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.
5	Set the time interval during which statistics on the q-in-q interface load is collected. (optionally).	<code>esr(config-qinq-if) # load-average <TIME></code>	<TIME> – interval in seconds, takes values of [5..150].
6	Enable bridge-group q-in-q interface (optionally).	<code>esr(config-qinq-if) #bridge-group <BRIDGE-ID></code>	<BRIDGE-ID> – bridge identifying number.
7	Set the lifetime of IPv4/IPv6 entries in the ARP table studied on the given q-in-q interface (optionally).	<code>esr(config-qinq-if) # ip arp reachable-time <TIME></code> or <code>ipv6 nd reachable-time <TIME></code>	<TIME> – lifetime of dynamic MAC addresses, in milliseconds. Allowed values are from 5000 to 100000000 milliseconds. Real time of the entry update varies from [0,5;1,5]*<TIME>.

7.5.2 Q-in-q configuration example

Objective:

Configure 192.168.1.1/24 subnet termination (Combinations C-VLAN: 741, S-VLAN: 828 on gigabitethernet 1/0/1 physical interface.

Solution:

Create sub-interface for S-VLAN: 828

```
esr(config)# interface gigabitethernet 1/0/1.828
esr(config-subif)# exit
```

Create QinQ sub-interface for C-VLAN: 741 and configure IP address from necessary subnet.

```
esr(config)# interface gigabitethernet 1/0/1.828.741
esr(config-qinq-if)# ip address 192.168.1.1/24
esr(config-qinq-if)# exit
```



Besides assigning IP address, it is necessary to disable firewall or to configure corresponding security zone on qinq interface.

7.6 USB modems configuration

The use of USB modems allows organizing additional link channel for router operation. When connecting USB modems, you may use USB hubs. Up to 10 USB modems can be configured in the system at the same time.

7.6.1 USB modems configuration algorithm

Step	Description	Command	Keys
1	After USB modem connection, wait until the system detects the connected device		
2	Define which number of the device is allocated to the connected USB modem	<code>esr# show cellulars status modem</code>	The connected device identifier will be specified in "USB port" field
3	Create parameter profile for USB modem and switch to the profile configuration mode	<code>esr(config)# cellular profile <ID></code>	<ID> – parameter profile identifier for USB modem in the system [1..10].
4	Specify parameter profile description (optionally).	<code>esr(config-cellular-profile)# description <DESCRIPTION></code>	<DESCRIPTION> – interface description, set by the string of up to 255 characters.
5	Set mobile network access point	<code>esr(config-cellular-profile)# apn <NAME></code>	<NAME> – mobile network access point, set by the string of up to 31 characters.
6	Set the name of mobile network user (if required by cellular carrier)	<code>esr(config-cellular-profile)# user <NAME></code>	<NAME> – user name, set by the string of up to 31 characters.
7	Set the password of mobile network user (if required by cellular carrier)	<code>esr(config-cellular-profile)# password ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }</code>	<CLEAR-TEXT> – unencrypted password, set by the string of [8 .. 64] characters, may include characters [0-9a-fA-F]; <ENCRYPTED-TEXT> – unencrypted password, set by the string of [16..128] characters.
8	Set the dial-up number for connection to the mobile network	<code>esr(config-cellular-profile)# number <WORD></code>	<WORD> – dial-up number for connection to the mobile network, set by the string of up to 15 characters.
9	Set the method of user authentication in the mobile network (optionally)	<code>esr(config-cellular-profile)# allowed-auth <TYPE></code>	<TYPE> - method of user authentication in the mobile network [none, PAP, CHAP, MSCHAP, MSCHAPv2, EAP].
10	Limit the possibility of the use of IP addresses in mobile network.	<code>esr(config-cellular-profile)# ip-version { ipv4 ipv6 }</code>	ipv4 – IPv4 range; ipv6 – IPv6 range;
11	Create USB modem in the router configuration and switch to the modem configuration mode	<code>esr(config)# cellular modem <ID></code>	<ID> – USB modem identifier in the system [1..10].

12	Specify VRF instance, in which the given modem will operate (optionally).	<code>esr(config-cellular-modem)# ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.
13	Set USB modem identifier allocated by the system (specified in item 2)	<code>esr(config-cellular-modem)# device <WORD></code>	<WORD> – identifier of the connected modem USB port [1..12].
14	Set the previously established parameter profile to the USB modem	<code>esr(config-cellular-modem)# profile <ID></code>	<ID> – parameter profile identifier for USB modem in the system [1..10].
15	Set SIM card unlock code (if necessary)	<code>esr(config-cellular-modem)# pin <WORD></code>	<WORD> - SIM card unlock code [4..8]. Only figures are supported for usage.
16	Allow the use of any USB modem operation mode (optionally)	<code>esr(config-cellular-modem)# allowed-mode <MODE></code>	<MODE> – acceptable USB modem operation mode [2g, 3g, 4g]. By default: all modes supported by the modem are allowed
17	Set the size of the largest received packet (optionally)	<code>esr(config-cellular-modem)# mru { <MRU> }</code>	<MRU> – MRU value, takes values in the range of [128..16383].
18	Set the preferable USB modem operation mode in the mobile network (optionally)	<code>esr(config-cellular-modem)# preferred-mode { <MODE> }</code>	<MODE> – preferable USB modem operation mode [2g, 3g, 4g].
19	Activate USB modem	<code>esr(config-cellular-modem)# enable</code>	

7.6.2 Configuration example

Objective:

Configure connection to the Internet by using USB modem.

Solution:

For example, consider the connection to the cellular operator MTS.

After modem connection, wait until the system detects the device Determine the port of the device that was assigned to the connected USB modem:

```
esr# show cellular status modem
```

Number device	USB port	Manufacturer	Model	Current state	Interface	Link state
1	1-2	huawei	E3372	Disabled	--	Down

Create the parameter profile for USB modem

```
esr(config)# cellular profile 1
```

Specify the required APN or any other necessary address. Below you can see the example of connection to MTS APN:

```
esr(config-cellular-profile)# apn internet.mts.ru
```

If necessary, create user name, password, dial-up number and authentication number

```
esr(config-cellular-profile)# user mts
esr(config-cellular-profile)# password ascii-text mts
esr(config-cellular-profile)# number *99#
esr(config-cellular-profile)# allowed-auth PAP
```

Let us proceed to configuring the USB modem and set the identifier corresponding to the device port that was defined at the beginning:

```
esr(config)# cellular modem 1
esr(config-cellular-modem)# device 1-2
```

Set the corresponding parameter profile and activate the modem:

```
esr(config-cellular-modem)# profile 1
esr(config-cellular-modem)# enable
```

7.7 AAA Configuration

AAA (Authentication, Authorization, Accounting) is used for description of access provisioning and control.

- Authentication is a matching of a person (request) for the existing account in the security system. Performed by the login and password.
- Authorization (authorization, privilege verification, access level verification) is a matching of the existing account in the system (passed authentication) and specific privileges.
- Accounting (accounting) is a monitoring of user connection or changes made by the user.

7.7.1 Local authentication configuration algorithm

Step	Description	Command	Keys
1	Set local as authentication method.	<pre>esr(config)# aaa authentication login { default <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]</pre>	<NAME> – list name, set by the string of up to 31 characters. Authentication methods: local – authentication by local user database; tacacs – authentication by TACACS servers list; radius – authentication by RADIUS servers list; ldap – authentication by LDAP servers list;
2	Set enable as authentication method of user privileges elevation.	<pre>esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]</pre>	<NAME> – list name, set by the string of up to 31 characters. Authentication methods: local – authentication by local user database; tacacs – authentication by TACACS servers list; radius – authentication by RADIUS servers list; ldap – authentication by LDAP servers list;

3	Set the method for iterating over authentication methods (optionally).	<code>esr(config)# aaa authentication mode <MODE></code>	<MODE> – options of iterating over methods: chain - if the server returned FAIL , proceed to the following authentication method in the chain; break - if the server returned FAIL , abandon authentication attempts. If the server is unavailable, continue authentication attempts by the following methods in the chain. Default value: chain.
4	Specify the number of failed authentication attempts to block the user login and time of the lock (optionally)	<code>esr(config)# aaa authentication attempts max-fail <COUNT> <TIME></code>	<COUNT> – number of failed authentication attempts leading to the user blocking, takes values of [1..65535]; <TIME> – the time interval in minutes for which the user will be blocked, takes values [1..65535]. Default value: <COUNT> - 5; <TIME> - 300
5	Enable request for change the default password for the 'admin' user (optionally)	<code>esr(config)# security passwords default-expired</code>	
6	Enable the inhibit mode on the use of previously set local user passwords (optionally)	<code>esr(config)# security passwords history <COUNT></code>	<COUNT> – number of passwords saved in the router memory. Takes values in the range of [1..15]. Default value: 0
7	Set the lifetime of local user password (optionally)	<code>esr(config)# security passwords lifetime <TIME></code>	<TIME> – password lifetime in days. Takes values in the range of [1..365]. By default: The lifetime of local user password is unlimited.
8	Set a limit on the minimum length of local user password and ENABLE password (optionally)	<code>esr(config)# security passwords min-length <NUM></code>	<NUM> – minimum number of characters in the password. Takes values in the range of [8..128]. Default value: 0
9	Set a limit on the maximum length of local user password and ENABLE password (optionally)	<code>esr(config)# security passwords max-length <NUM></code>	<NUM> – maximum number of characters in the password. Takes values in the range of [8..128]. Default value: not limited.
10	Set the minimum number of character types that must be present in the local user password and ENABLE password (optionally)	<code>esr(config)# security passwords symbol-types <COUNT></code>	<COUNT> – minimum number of character types in the password. Takes values in the range of [1..4]. Default value: 1
11	Set the minimum number of lower case letters in the local user password and ENABLE password (optionally)	<code>esr(config)# security passwords lower-case <COUNT></code>	<COUNT> – minimum number of lower case letters in the local user password and ENABLE password (optionally) Takes values in the range of [0..128]. Default value: 0
12	Set the minimum number of upper case letters in the local user password and ENABLE password (optionally)	<code>esr(config)# security passwords upper-case <COUNT></code>	<COUNT> – minimum number of upper case letters in the password. Takes values in the range of [0..128]. Default value: 0
13	Set the minimum number of digits in the local user	<code>esr(config)# security passwords numeric-count <COUNT></code>	<COUNT> – minimum number of digits in the password. Takes values in the range of [0..128].

	password and ENABLE password (optionally)		Default value: 0
14	Set the minimum number of special characters in the local user password and ENABLE password (optionally)	<code>esr(config)# security passwords special-case <COUNT></code>	<COUNT> – minimum number of special characters in the password. Takes values in the range of [0..128]. Default value: 0
15	Add user in the local database and switch to the user parameters configuration mode	<code>esr(config)# username <NAME></code>	<NAME> – user name, set by the string of up to 31 characters.
16	Set user password	<code>esr(config-user)# password { <CLEAR-TEXT> encrypted <HASH_SHA512> }</code>	<CLEAR-TEXT> – password, set by the string of [8 .. 31] characters, may include characters [0-9a-fA-F]; <HASH_SHA512> – password hash by sha512 algorithm, set by the string of 110 characters.
17	Set user privileges level	<code>esr(config-user)# privilege <PRIV></code>	<PRIV> – required privilege level. Takes values in the range of [1..15].
18	Switch to the corresponding terminal configuration mode	<code>esr(config)# line console</code> <code>or</code> <code>esr(config)# line telnet</code> <code>or</code> <code>esr(config)# line ssh</code>	
19	Activate user login authentication list	<code>esr(config-line-ssh)# login authentication <NAME></code>	<NAME> – list name, set by the string of up to 31 characters.
20	Activate authentication list of user privileges elevation	<code>esr(config-line-ssh)# enable authentication <NAME></code>	<NAME> – list name, set by the string of up to 31 characters.
21	Set the interval after which the idle session will be terminated	<code>esr(config-line-ssh)# exec-timeout <SEC></code>	<SEC> – time interval in minutes, takes values of [1..65535].

7.7.2 AAA configuration algorithm via RADIUS

Step	Description	Command	Keys
1	Set the DSCP code global value for the use in IP headers of RADIUS server egress packets (optionally).	<code>esr(config)# radius-server dscp <DSCP></code>	<DSCP> – DSCP code value, takes values in the range of [0..63]. Default value: 63.
2	Set the global number of iterative queries to the last active RADIUS server (optionally).	<code>esr(config)# radius-server retransmit <COUNT></code>	<COUNT> – number of iterative queries to the RADIUS server, takes values of [1..10]. Default value: 1.
3	Set the global value of the interval after which the router assumes that the RADIUS server is not available (optional).	<code>esr(config)# radius-server timeout <SEC></code>	<SEC> – time interval in seconds, takes values of [1..30]. Default value: 3 seconds.
4	Add RADIUS server to the list of used servers and switch to its configuration mode.	<code>esr(config)# radius-server host { <IP-ADDR> <IPV6-ADDR> } [vrf <VRF>]</code> <code>esr(config-radius-server)#</code>	<IP-ADDR> – RADIUS server IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <IPV6-ADDR> – RADIUS server IPv6 address, defined as X:X:X:X:X, where each part takes values in hexadecimal format [0..FFFF]

			<VRF> – VRF item name, set by the string of up to 31 characters.
5	Specify the number of failed authentication attempts to block the user login and time of the lock (optionally)	<code>aaa authentication attempts max-fail <COUNT> <TIME></code>	<COUNT> – number of failed authentication attempts leading to the user blocking, takes values of [1..65535]; <TIME> – the time interval in seconds for which the user will be blocked, takes values [1..65535]. Default value: <COUNT> - 5; <TIME> - 300
6	Set the password for authentication on remote RADIUS server.	<code>esr(config-radius-server)# key ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> }</code>	<TEXT> – string [8..16] ASCII characters; <ENCRYPTED-TEXT> – unencrypted password, [8..16] bytes size, set by the string of [16..32] characters.
7	Prioritize the use of a remote RADIUS server (optionally).	<code>esr(config-radius-server)# priority <PRIORITY></code>	<PRIORITY> – priority of using a remote server, takes values of [1..65535]. The lower value, the more prioritized server. Default value: 1.
8	Set the interval after which the router assumes that the RADIUS server is not available (optionally).	<code>esr(config-radius-server)# timeout <SEC></code>	<SEC> – time interval in seconds, takes values of [1..30]. Default value: global timer value is used.
9	Set IPv4/IPv6 address that will be used as source IPv4/IPv6 address in transmitted RADIUS packets.	<code>esr(config-radius-server)# source-address { <ADDR> <IPV6-ADDR> }</code>	<ADDR> – source IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <IPV6-ADDR> – source IPv6 address, defined as X:X:X:X where each part takes values in hexadecimal format [0..FFFF].
10	Set radius as authentication method.	<code>esr(config)# aaa authentication login { default <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]</code>	<NAME> – list name, set by the string of up to 31 characters. Authentication methods: local – authentication by local user database; tacacs – authentication by TACACS servers list; radius – authentication by RADIUS servers list; ldap – authentication by LDAP servers list;
11	Set radius as authentication method of user privileges elevation.	<code>esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]</code>	<NAME> – list name, set by the string of up to 31 characters. default – default list name. <METHOD> – authentication methods: enable – authentication by enable passwords; tacacs – authentication by TACACS; radius – authentication by RADIUS; ldap – authentication by LDAP;

12	Set the method for iterating over authentication methods (optionally).	<code>esr(config)# aaa authentication mode <MODE></code>	<MODE> – options of iterating over methods: chain - if the server returned FAIL , proceed to the following authentication method in the chain; break - if the server returned FAIL , abandon authentication attempts. If the server is unavailable, continue authentication attempts by the following methods in the chain. Default value: chain.
13	Configure radius in the list of user session accounting methods (optionally).	<code>esr(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>]</code>	<METHOD> – accounting methods: tacacs – session accounting by TACACS; radius – session accounting by RADIUS;
14	Switch to the corresponding terminal configuration mode	<code>esr(config)# line <TYPE></code>	<TYPE> – console type: console – local console; ssh – secure remote console;
15	Activate user login authentication list	<code>esr(config-line-console)# login authentication <NAME></code>	<NAME> – list name, set by the string of up to 31 characters. Created in step 8.
16	Activate authentication list of user privileges elevation	<code>esr(config-line-console)# enable authentication <NAME></code>	<NAME> – list name, set by the string of up to 31 characters. Created in step 9.

7.7.3 AAA configuration algorithm via TACACS

Step	Description	Command	Keys
1	Set the DSCP code global value for the use in IP headers of TACACS server egress packets (optionally).	<code>esr(config)# tacacs-server dscp <DSCP></code>	<DSCP> – DSCP code value, takes values in the range of [0..63]. Default value: 63.
2	Set the global value of the interval after which the router assumes that the TACACS server is not available (optionally).	<code>esr(config)# tacacs-server timeout <SEC></code>	<SEC> – time interval in seconds, takes values of [1..30]. Default value: 3 seconds.
3	Add TACACS server to the list of used servers and switch to its configuration mode.	<code>esr(config)# tacacs-server host { <IP-ADDR> <IPV6-ADDR> } [vrf <VRF>]</code> <code>esr(config-tacacs-server)#</code>	<IP-ADDR> – TACACS server IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <IPV6-ADDR> – TACACS server IPv6 address, defined as X:X:X:X::X, where each part takes values in hexadecimal format [0..FFFF] <VRF> – VRF item name, set by the string of up to 31 characters.
4	Specify the number of failed authentication attempts to block the user login and time of the lock (optionally)	<code>aaa authentication attempts max-fail <COUNT> <TIME></code>	<COUNT> – number of failed authentication attempts leading to the user blocking, takes values of [1..65535]; <TIME> – the time interval in minutes for which the user will be blocked, takes values [1..65535]. Default value: <COUNT> - 5; <TIME> - 300
5	Set the password for authentication on remote TACACS server.	<code>esr(config-tacacs-server)# key ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> }</code>	<TEXT> – string [8..16] ASCII characters;

			<ENCRYPTED-TEXT> – unencrypted password, [8..16] bytes size, set by the string of [16..32] characters.
6	Set the port number to communicate with remote TACACS server (optionally).	<code>esr(config-tacacs-server)# port <PORT></code>	<PORT> – TCP port number for communication with remote server, takes values of [1..65535]. Default value: 49 for TACACS server.
7	Prioritize the use of a remote TACACS server (optionally).	<code>esr(config-tacacs-server)# priority <PRIORITY></code>	<PRIORITY> – priority of using a remote server, takes values of [1..65535]. The lower value, the more prioritized server. Default value: 1.
8	Set IPv4/IPv6 address that will be used as source IPv4/IPv6 address in transmitted TACACS packets.	<code>esr(config-radius-tacacs)# source-address { <ADDR> <IPV6-ADDR> }</code>	<ADDR> – source IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255];
9	Set TACACS as authentication method of user privileges elevation.	<code>esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]</code>	<NAME> – list name, set by the string of up to 31 characters. default – default list name. <METHOD> – authentication methods: enable – authentication by enable passwords; tacacs – authentication by TACACS; radius – authentication by RADIUS; ldap – authentication by LDAP;
10	Set the method for iterating over authentication methods (optionally).	<code>esr(config)# aaa authentication mode <MODE></code>	<MODE> – options of iterating over methods: chain - if the server returned FAIL, proceed to the following authentication method in the chain; break - if the server returned FAIL , abandon authentication attempts. If the server is unavailable, continue authentication attempts by the following methods in the chain. Default value: chain.
11	Configure the list of CLI commands accounting methods (optionally).	<code>esr(config)# aaa accounting commands stop-only tacacs</code>	
12	Configure tacacs in the list of user session accounting methods (optionally).	<code>esr(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>]</code>	<METHOD> – accounting methods: tacacs – session accounting by TACACS; radius – session accounting by RADIUS;
13	Switch to the corresponding terminal configuration mode	<code>esr(config)# line <TYPE></code>	<TYPE> – console type: console – local console; ssh – secure remote console;
14	Activate user login authentication list	<code>esr(config-line-console)# login authentication <NAME></code>	<NAME> – list name, set by the string of up to 31 characters. Created in step 7.
15	Activate authentication list of user privileges elevation	<code>esr(config-line-console)# enable authentication <NAME></code>	<NAME> – list name, set by the string of up to 31 characters. Created in step 8.

7.7.4 AAA configuration algorithm via LDAP

Step	Description	Command	Keys
1	Specify basic DN (Distinguished name) that will be used when searching for users.	<code>esr(config)# ldap-server base-dn <NAME></code>	<NAME> – basic DN, set by the string of up to 255 characters.
2	Set the interval after which the router assumes that the LDAP server is not available (optionally).	<code>esr(config)# ldap-server bind timeout <SEC></code>	<SEC> – time interval in seconds, takes values of [1..30]. Default value: 3 seconds.
3	Specify the DN (Distinguished name) of a user with administrator rights, under which authorization will take place on the LDAP server when searching for users.	<code>esr(config)# ldap-server bind authenticate root-dn <NAME></code>	<NAME> – DN of a user with administrator rights, set by the string of up to 255 characters.
4	Specify the password of a user with administrator rights, under which authorization will take place on the LDAP server when searching for users.	<code>esr(config)# ldap-server bind authenticate root-password ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> }</code>	<TEXT> – string [8..16] ASCII characters; <ENCRYPTED-TEXT> – unencrypted password, [8..16] bytes size, set by the string of [16..32] characters.
5	Specify a class name of the objects among which it is necessary to search for users on LDAP server (optionally).	<code>esr(config)# ldap-server search filter user-object-class <NAME></code>	<NAME> – object class name, set by the string of up to 127 characters. Default value: posixAccount.
6	Specify the user search scope in LDAP server tree (optionally).	<code>esr(config)# ldap-server search scope <SCOPE></code>	<SCOPE> – user search scope on LDAP server, takes the following values: onelevel – search through the objects on the level following the basic DN in LDAP server tree; subtree – search through the basic DN subtree objects in LDAP server tree. Default value: subtree.
7	Specify the interval after which the device assumes that LDAP server has not found users entries satisfying the search condition (optionally).	<code>esr(config)# ldap-server search timeout <SEC></code>	<SEC> – time interval in seconds, takes values of [0..30]. Default value: 0 – device is waiting for search completion and responses from LDAP server.
8	Specify an attribute name of the object which is compared with the name of the desired user on LDAP server (optional).	<code>esr(config)# ldap-server naming-attribute <NAME></code>	<NAME> – object attribute name, set by the string of up to 127 characters. Default value: uid.
9	Specify the object attribute name which is compared with the name of a desired user on LDAP server (optionally).	<code>esr(config)# ldap-server privilege-level-attribute <NAME></code>	<NAME> – object attribute name, set by the string of up to 127 characters. Default value: priv-lvl
10	Set the DSCP code global value for the use in IP headers of LDAP server egress packets (optionally).	<code>esr(config)# ldap-server dscp <DSCP></code>	<DSCP> – DSCP code value, takes values in the range of [0..63]. Default value: 63

11	Add LDAP server to the list of used servers and switch to its configuration mode.	<code>esr(config)# ldap-server host { <IP-ADDR> <IPV6-ADDR> } [vrf <VRF>] esr(config-ldap-server)#</code>	<IP-ADDR> – LDAP server IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <IPV6-ADDR> – LDAP server IPv6 address, defined as X:X:X:X::X, where each part takes values in hexadecimal format [0..FFFF] <VRF> – VRF item name, set by the string of up to 31 characters.
12	Specify the number of failed authentication attempts to block the user login and time of the lock (optionally)	<code>aaa authentication attempts max-fail <COUNT> <TIME></code>	<COUNT> – number of failed authentication attempts leading to the user blocking, takes values of [1..65535]; <TIME> – the time interval in minutes for which the user will be blocked, takes values [1..65535]. Default value: <COUNT> - 5; <TIME> - 300
13	Set the port number to communicate with remote LDAP server (optionally).	<code>esr(config-ldap-server)# port <PORT></code>	<PORT> – TCP port number for communication with remote server, takes values of [1..65535]. Default value: 389 for LDAP server.
14	Prioritize the use of a remote LDAP server (optionally).	<code>esr(config-ldap-server)# priority <PRIORITY></code>	<PRIORITY> – priority of using a remote server, takes values of [1..65535]. The lower value, the more prioritized server. Default value: 1.
15	Set IPv4/IPv6 address that will be used as source IPv4/IPv6 address in transmitted LDAP packets.	<code>esr(config-ldap-server)# source-address { <ADDR> <IPV6-ADDR> }</code>	<ADDR> – source IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <IPV6-ADDR> – source IPv6 address, defined as X:X:X:X::X where each part takes values in hexadecimal format [0..FFFF].
16	Set LDAP as authentication method.	<code>esr(config)# aaa authentication login { default <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]</code>	<NAME> – list name, set by the string of up to 31 characters. Authentication methods: local – authentication by local user database; tacacs – authentication by TACACS servers list; radius – authentication by RADIUS servers list; ldap – authentication by LDAP servers list;
17	Set LDAP as authentication method of user privileges elevation.	<code>esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]</code>	<NAME> – list name, set by the string of up to 31 characters. default – default list name. <METHOD> – authentication methods: enable – authentication by enable passwords; tacacs – authentication by TACACS; radius – authentication by RADIUS; ldap – authentication by LDAP;

18	Set the method for iterating over authentication methods in case of failure (optionally).	<code>esr(config)# aaa authentication mode <MODE></code>	<MODE> – options of iterating over methods: chain - if the server returned FAIL, proceed to the following authentication method in the chain; break - if the server returned FAIL , abandon authentication attempts. If the server is unavailable, continue authentication attempts by the following methods in the chain. Default value: chain.
19	Switch to the corresponding terminal configuration mode	<code>esr(config)# line <TYPE></code>	<TYPE> – console type: console – local console; ssh – secure remote console;
20	Activate user login authentication list	<code>esr(config-line-console)# login authentication <NAME></code>	<NAME> – list name, set by the string of up to 31 characters. Created in step 14.
21	Activate authentication list of user privileges elevation	<code>esr(config-line-console)# enable authentication <NAME></code>	<NAME> – list name, set by the string of up to 31 characters. Created in step 15.

7.7.5 Example of authentication configuration using telnet via RADIUS server

Objective:

Configure authentication for users being connected via Telnet and RADIUS (192.168.16.1/24).

Solution:

Configure connection to RADIUS server and specify the key (password):

```
esr# configure
esr(config)# radius-server host 192.168.16.1
esr(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-radius-server)# exit
```

Create authentication profile:

```
esr(config)# aaa authentication login log radius
```

Specify authentication mode used for Telnet protocol connection:

```
esr(config)# line telnet
esr(config-line-telnet)# login authentication log
esr(config-line-telnet)# exit
esr(config)# exit
```

To view the information on RADIUS server connection settings, use the following command:

```
esr# show aaa radius-servers
```

To view the authentication profiles, use the following command:

```
esr# show aaa authentication
```

7.8 Command privilege configuration

Command privilege configuration is a flexible tool that allows you to assign baseline user privilege level (1–15) to a command set. In future, you may specify privilege level during user creation which will define a command set available to them.

- *Levels 1-9* enable all monitoring commands (show ...).
- *Levels 10-14* enable all commands except for device reboot, user management and other specific commands.
- *Level 15* enables all monitoring commands.

7.8.1 Configuration algorithm

To change minimum privilege level required for CLI command execution, use the following command:

```
esr(config)# privilege <COMMAND-MODE> level <PRIV><COMMAND>
```

<COMMAND-MODE> – command mode;

<PRIV> – required privilege level of command subtree, takes value of [1..15];

<COMMAND> – command subtree, set by the string of up to 255 characters.

7.8.2 Example of command privilege configuration

Objective:

Transfer all interface information display commands to the privilege level 10 except for 'show interfaces bridges' command. Transfer 'show interfaces bridges' command to the privilege level 3.

Solution:

In configuration mode, identify commands enabled for operation under privilege level 10 and privilege level 3.

```
esr(config)# privilege root level 3 "show interfaces bridge"
esr(config)# privilege root level 10 "show interfaces"
```

7.9 DHCP server configuration

Integrated DHCP server of the router allows you to configure LAN device network settings. Router DHCP server is able to send additional options to network devices, for example:

- *default-router* – IP address of the router used as default gateway.
- *domain-name* – domain name which will be used by client while solving host names via domain name system (DNS).
- *dns-server* – list of domain name server addresses for the current network that should be known by the client. Server addresses are listed in descending order of their preference.

7.9.1 Configuration algorithm

Step	Description	Command	Keys
1	Enable IPv4/IPv6 DHCP server.	<code>esr(config)# ip dhcp-server [vrf <VRF>]</code>	<VRF> – VRF item name within which DHCP server will operate. Set by the string of up to 31 characters.
		<code>esr(config)# ipv6 dhcp-server [vrf <VRF>]</code>	
2	Set the DSCP code global value for the use in IP headers of DHCP server egress packets (optionally).	<code>esr(config)# ip dhcp-server dscp <DSCP></code>	<DSCP> – DSCP code value, takes values in the range of [0..63]. Default value: 61.
3	Create pool of DHCP server IPv4/IPv6 addresses and switch to its configuration mode.	<code>esr(config)# ip dhcp-server pool <NAME> [vrf <VRF>]</code>	<NAME> – name of the pool of DHCP server IPv4/IPv6 addresses, set by the string of up to 31 characters. <VRF> – VRF item name within which the given pool of DHCP server IP addresses will operate. Set by the string of up to 31 characters.
		<code>esr(config)# ipv6 dhcp-server pool <NAME> [vrf <VRF>]</code>	
4	Specify IPv4/IPv6 address and mask for the subnet from which IPv4/IPv6 addresses pool will be allocated.	<code>esr(config-dhcp-server)# network <ADDR/LEN></code>	<ADDR/LEN> – IP address and prefix of a subnet, defined as AAA.BBB.CCC.DDD/EE where each part AAA-DDD takes values of [0..255] and EE takes values of [1..32].
		<code>esr(config-ipv6-dhcp-server)# network <IPV6-ADDR/LEN></code>	<IPV6-ADDR/LEN> – IP address and prefix of a subnet, defined as X:X:X:X:X/EE where each X part takes values in hexadecimal format [0..FFFF] and EE takes values of [1..128].
5	Add IPv4/IPv6 addresses range to the address pool of configurable DHCP server.	<code>esr(config-dhcp-server)# address-range <FROM-ADDR>-<TO-ADDR></code>	<FROM-ADDR> – range starting IP address; <TO-ADDR> – range ending IP address, The addresses are defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]. You can specify up to 32 IP addresses ranges, the list should be comma-separated.
		<code>esr(config-ipv6-dhcp-server)# address-range <FROM-ADDR>-<TO-ADDR></code>	<FROM-ADDR> – range starting IP address; <TO-ADDR> – range ending IP address; The addresses are defined as X:X:X:X:X where each part takes values in hexadecimal format [0..FFFF].
6	Add IPv4/IPv6 address for a specific physical address to the address pool of configurable DHCP server (optionally).	<code>esr(config-dhcp-server)# address <ADDR> {mac-address <MAC> client-identifier <CI>}</code>	<ADDR> – client IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <MAC> – MAC address of the client, which will be given the IP address, is defined as XX: XX: XX: XX: XX: XX where each part takes the values of [00..FF]. <CI> – client identifier according to DHCP Option 61. Can be specified as follows: HH:HH:HH:HH:HH:HH:HH: - client identifier in hexadecimal format and client MAC address; STRING – text string from 1 to 64 characters.

		<code>esr(config-ipv6-dhcp-server)# address <ADDR> mac-address <MAC></code>	<IPV6-ADDR> – client IPv6 address, defined as X:X:X:X where each part takes values in hexadecimal format [0..FFFF]; <MAC> – MAC address of the client, which will be given the IP address, defined as XX: XX: XX: XX: XX: XX where each part takes the values of [00..FF].
7	Specify the list of default gateway IPv4 addresses which will be transmitted by DHCP server to clients through DHCP option 3.	<code>esr(config-dhcp-server)# default-router <ADDR></code>	<ADDR> – default gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; You can specify up to 8 IP addresses, the list should be comma-separated.
8	Specify network domain DNS name. Domain name is transmitted to clients as part of DHCP option 15 (optionally).	<code>esr(config-dhcp-server)# domain-name <NAME></code> <code>esr(config-ipv6-dhcp-server)# domain-name <NAME></code>	<NAME> – client domain DNS name, set by the string of up to 255 characters.
9	Specify DNS server IPv4/IPv6 addresses list. The list is transmitted to clients as part of DHCP option 6 (optionally).	<code>esr(config-dhcp-server)# dns-server <ADDR></code>	<ADDR> – DNS server IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]. You can specify up to 8 IP addresses, the list should be comma-separated.
		<code>esr(config-ipv6-dhcp-server)# dns-server <IPV6-ADDR></code>	<IPV6-ADDR> – DNS server IPv6 address, defined as X:X:X:X:X where each part takes values in hexadecimal format [0..FFFF]. You can specify up to 8 IPv6 addresses, the list should be comma-separated.
10	Specify maximum IP addresses lease time (optionally). If DHCP client requests the lease time that exceeds a maximum value, the time specified by the command will be set.	<code>esr(config-dhcp-server)# max-lease-time <TIME></code>	<TIME> – maximum IP address lease time, defined as DD:HH:MM, where: DD – amount of days, takes values of [0..364]; HH – amount of hours, takes values of [0..23]; MM – amount of minutes, takes values of [0..59] Default value: 1 day
		<code>esr(config-ipv6-dhcp-server)# max-lease-time <TIME></code>	
11	Specify the lease time for which a client will be given IP address (optionally). This time will be used if a client did not request the certain lease time.	<code>esr(config-dhcp-server)# default-lease-time <TIME></code>	<TIME> – maximum IP address lease time, defined as DD:HH:MM, where: DD – amount of days, takes values of [0..364]; HH – amount of hours, takes values of [0..23]; MM – amount of minutes, takes values of [0..59] Default value: 12 hours.
		<code>esr(config-ipv6-dhcp-server)# default-lease-time <TIME></code>	
12	Create supplier class identifier (DHCP Option 60) (optionally).	<code>esr(config)# ip dhcp-server vendor-class-id <NAME></code>	<NAME> – supplier class identifier, set by the string of up to 31 characters.
		<code>esr(config)# ipv6 dhcp-server vendor-class-id <NAME></code>	
13	Specify specific supplier information (DHCP Option 43).	<code>esr(config-dhcp-vendor-id)# vendor-specific-options <HEX></code>	<HEX> – specific supplier information, specified in hexadecimal format of up to 128 characters.
		<code>esr(config-ipv6-dhcp-vendor-id)# vendor-specific-options <HEX></code>	

14	Specify NetBIOS server IP address (DHCP option 44) (optionally).	<code>esr (config-dhcp-server) # netbios-name-server <ADDR></code>	<ADDR> – NetBIOS server IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]. You can specify up to 4 IP addresses.
15	Specify tftp server IP address (DHCP option 150) (optionally).	<code>esr (config-dhcp-server) # tftp-server <ADDR></code>	<ADDR> – DNS server IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].

7.9.2 DHCP server configuration example

Objective:

Configure DHCP server operation in a local network that belongs to the 'trusted' security zone. Specify IP address pool from 192.168.1.0/24 subnet for distribution to clients. Specify address lease time equal to 1 day. Configure transmission of the default route, domain name and DNS server addresses to clients using DHCP options.

Solution:

Create 'trusted' security zone and determine the inheritance of the network interfaces being used to zones:

```
esr# configure
esr(config)# security zone trusted
esr(config-zone)# exit
```

Create address pool named 'Simple' and add IP address range intended for server clients lease into this pool. Specify parameters of the subnet that the pool belongs to, and the lease time for addresses:

```
esr# configure
esr(config)# ip dhcp-server pool Simple
esr(config-dhcp-server)# network 192.168.1.0/24
esr(config-dhcp-server)# address-range 192.168.1.100-192.168.1.125
esr(config-dhcp-server)# default-lease-time 1:00:00
```

Configure transfer of additional network parameters to clients:

- default route: 192.168.1.1;
- domain name: eltex.loc;
- DNS server list: DNS1: 172.16.0.1, DNS2: 8.8.8.8;

```
esr(config-dhcp-server)# domain-name "eltex.loc"
esr(config-dhcp-server)# default-router 192.168.1.1
esr(config-dhcp-server)# dns-server 172.16.0.1 8.8.8.8
esr(config-dhcp-server)# exit
```

To enable IP address distribution from the configurable pool by DHCP server, IP interface should be created on the router that belongs to the same subnet as the pool addresses.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone trusted
esr(config-if-gi)# ip address 192.168.1.1/24
esr(config-if-gi)# exit
```

To enable DHCP protocol message transmission to the server, you should create the respective port profiles including source port 68 and destination port 67 used by DHCP protocol and create the allowing rule in the security policy for UDP protocol packet transmission:

```
esr(config)# object-group service dhcp_server
esr(config-object-group-service)# port-range 67
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_client
esr(config-object-group-service)# port-range 68
esr(config-object-group-service)# exit
esr(config)# security zone-pair trusted self
esr(config-zone-pair)# rule 30
esr(config-zone-rule)# match protocol udp
esr(config-zone-rule)# match source-address any
esr(config-zone-rule)# match destination-address any
esr(config-zone-rule)# match source-port dhcp_client
esr(config-zone-rule)# match destination-port dhcp_server
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# exit
```

Enable server operation:

```
esr(config)# ip dhcp-server
esr(config)# exit
```

To view the list of leased addresses, use the following command:

```
esr# show ip dhcp binding
```

To view the configured address pools, use the following commands:

```
esr# show ip dhcp server pool
esr# show ip dhcp server pool Simple
```



Configuration of settings for IPv6 is performed by analogy to IPv4.

7.10 Destination NAT configuration

Destination NAT (DNAT) function includes destination IP address translation for packets transferred through the network gateway.

DNAT is used for redirection of traffic, coming to a specific 'virtual' address in a public network, to a 'real' server in LAN located behind the network gateway. This function may be used for establishing a public access to servers located within the private network without any public network address.

7.10.1 Configuration algorithm

Step	Description	Command	Keys
1	Switch to the configuration mode of destination address translation service.	<code>esr(config)# nat destination</code>	
2	Create a pool of IP addresses and/or TCP/UDP ports with a specific name (optionally).	<code>esr(config-dnat)# pool <NAME></code>	<NAME> – NAT addresses pool name, set by the string of up to 31 characters.

3	Set the internal IP address which will replace a destination IP address.	<code>esr(config-dnat-pool)# ip address <ADDR></code>	<ADDR> – IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
4	Set the internal TCP/UDP port which will replace a destination TCP/UDP port.	<code>esr(config-dnat-pool)# ip port <PORT></code>	<PORT> – TCP/UDP port, takes values of [1..65535].
5	Create a rule group with a specific name.	<code>esr(config-dnat)# ruleset <NAME></code>	<NAME> – rule group name, set by the string of up to 31 characters.
6	Specify VRF instance, in which the given rule group will operate (optionally).	<code>esr(config-dnat-ruleset)# ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.
7	Set the rule group scope. The rules will be applied only to traffic coming from a certain zone or interface.	<code>esr(config-dnat-ruleset)# from { zone <NAME> interface <IF> tunnel <TUN> default }</code>	<NAME> – isolation zone name; <IF> – device interface name; <TUN> – device tunnel name; default – defines a rule group for all traffic, the source of which does not meet the requirements of other rule groups.
8	Specify a rule with a certain number. The rules are proceeded in ascending order.	<code>esr(config-dnat-ruleset)# rule <ORDER></code>	<ORDER> – rule number, takes values of [1..10000].
9	Specify the profile of IP addresses {sender recipient} for which the rule should work.	<code>esr(config-dnat-rule)# match [not]¹ {source destination}-address <OBJ-GROUP-NETWORK-NAME></code>	<OBJ-GROUP-NETWORK-NAME> – IP addresses profile name, set by the string of up to 31 characters. “Any” value points at any source IP address.
10	Specify the profile of services (tcp/udp ports) {sender recipient} for which the rule should work (optionally).	<code>esr(config-dnat-rule)# match [not]¹ {source destination}-port <PORT-SET-NAME></code>	<PORT-SET-NAME> – port profile name, set by the string of up to 31 characters. “Any” value points at any source TCP/UDP port.
11	Set name or number of IP for which the rule should work (optionally).	<code>esr(config-dnat-rule)# match [not]¹ {protocol <TYPE> protocol-id <ID> }</code>	<TYPE> – protocol type, takes the following values: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. “Any” value points at any protocol type. <ID> – IP identification number, takes values of [0x00-0xFF].
12	Specify the type and code of ICMP messages for which the rule should work (if ICMP is selected as protocol) (optionally).	<code>esr(config-dnat-rule)# match [not]¹ icmp {<ICMP_TYPE><ICMP_CODE> <TYPE-NAME>}</code>	<ICMP_TYPE> – ICMP message type, takes values of [0..255]. <ICMP_CODE> – ICMP message code, takes values of [0..255]. “Any” value points at any message code. <TYPE-NAME> – ICMP message type name.
13	Specify the action “translation of source address and port” for the traffic meeting the requirements of “match” commands.	<code>esr(config-dnat-rule)# action destination-nat { off pool <NAME> netmap <ADDR/LEN> }</code>	off – translation is disabled; pool<NAME> – name of the pool that contains IP addresses and/or TCP/UDP ports set; netmap <ADDR/LEN> – subnet IP address and mask used during translation. The parameter is defined as AAA.BBB.CCC.DDD/EE where each part AAA-DDD takes values of [0..255] and EE takes values of [1..32].

¹ When using *not* command, the rule will work for the values that are not included in the specified profile

14	Activate a configured rule.	<code>esr(config-dnat-rule)# enable</code>	
----	-----------------------------	--	--

Each “match” command may contain “not” key. When using the key, packets that do not meet the given requirement will fall under the rule.

You can obtain more detail information about firewall configuration in “CLI command reference guide”.

7.10.2 Destination NAT configuration example

Objective:

Establish access from the public network that belongs to the ‘UNTRUST’ zone to LAN server in ‘TRUST’ zone. Server address in LAN - 10.1.1.100. Server should be accessible from outside the network—address 1.2.3.4, access port 80.

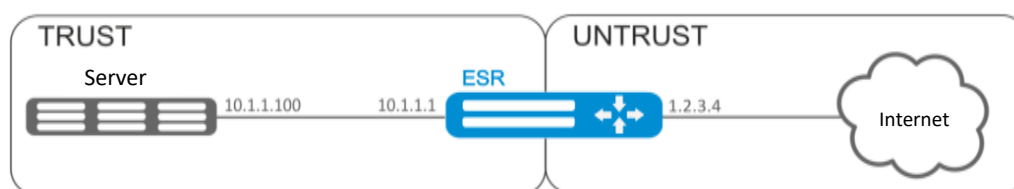


Figure 44 – Network structure

Solution:

Create 'UNTRUST' and 'TRUST' security zones. Specify the inheritance of the network interfaces being used to zones. Assign IP addresses to interfaces simultaneously.

```
esr# configure
esr(config)# security zone UNTRUST
esr(config-zone)# exit
esr(config)# security zone TRUST
esr(config-zone)# exit

esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone TRUST
esr(config-if-gi)# ip address 10.1.1.1/25
esr(config-if-gi)# exit

esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 1.2.3.4/29
esr(config-if-te)# security-zone UNTRUST
esr(config-if-te)# exit
```

Create IP address and port profiles required for configuration of the Firewall and DNAT rules.

- NET_UPLINK – public network address profile;
- SERVER_IP – local area network address profile;
- SRV_HTTP – port profile.

```
esr(config)# object-group network NET_UPLINK
esr(config-object-group-network)# ip address 1.2.3.4
```

```
esr(config-object-group-network) # exit

esr(config) # object-group service SRV_HTTP
esr(config-object-group-service) # port 80
esr(config-object-group-service) # exit

esr(config) # object-group network SERVER_IP
esr(config-object-group-network) # ip address 10.1.1.100
esr(config-object-group-network) # exit
```

Proceed to DNAT configuration mode and create destination address and port pool that will be used for translation of packet addresses coming to address 1.2.3.4 from the external network.

```
esr(config) # nat destination
esr(config-dnat) # pool SERVER_POOL
esr(config-dnat-pool) # ip address 10.1.1.100
esr(config-dnat-pool) # ip port 80
esr(config-dnat-pool) # exit
```

Create 'DNAT' rule set which will be used for address translation. In the set attributes, specify that the rules are applying only to packets coming from the 'UNTRUST' zone. Rule set includes data matching requirements for destination address and port (match destination-address, match destination-port) and for the protocol. Also, the set includes an action that applies to the data that satisfy all of the rules (action destination-nat). The rule set is applied with 'enable' command.

```
esr(config-dnat) # ruleset DNAT
esr(config-dnat-ruleset) # from zone UNTRUST
esr(config-dnat-ruleset) # rule 1
esr(config-dnat-rule) # match destination-address NET_UPLINK
esr(config-dnat-rule) # match protocol tcp
esr(config-dnat-rule) # match destination-port SRV_HTTP
esr(config-dnat-rule) # action destination-nat pool SERVER_POOL
esr(config-dnat-rule) # enable
esr(config-dnat-rule) # exit
esr(config-dnat-ruleset) # exit
esr(config-dnat) # exit
```

To transfer the traffic coming from 'UNTRUST' zone into 'TRUST' zone, create the respective pair of zones. Only DNAT-translated traffic with the destination address matching the 'SERVER_IP' specified in the profile should be transferred.

```
esr(config) # security zone-pair UNTRUST TRUST
esr(config-zone-pair) # rule 1
esr(config-zone-pair-rule) # match source-address any
esr(config-zone-pair-rule) # match destination-address SERVER_IP
esr(config-zone-pair-rule) # match protocol any
esr(config-zone-pair-rule) # match destination-nat
esr(config-zone-pair-rule) # action permit
esr(config-zone-pair-rule) # enable
esr(config-zone-pair-rule) # exit
esr(config-zone-pair) # exit
esr(config) # exit
```

Configuration changes will take effect when the configuration is applied:

```
esr# show ip nat destination pools
esr# show ip nat destination rulesets
esr# show ip nat proxy-arp
```

```
esr# show ip nat translations
```

7.11 Source NAT configuration

Source NAT (SNAT) function substitutes source address for packets transferred through the network gateway. When packets are transferred from LAN into public network, source address is substituted to one of the gateway public addresses. Additionally, source port substitution may be added to the source address. When packets are transferred back from public network to LAN, address and port are reverted to their original values.

SNAT function enables Internet access for computers located in LAN. At that, there is no need in assigning public IP addresses for these computers.

7.11.1 Configuration algorithm

Step	Description	Command	Keys
1	Switch to the configuration mode of source address translation service.	<code>esr(config)# nat source</code>	
2	Create a pool of IP addresses and/or TCP/UDP ports with a specific name (optionally).	<code>esr(config-snat)# pool <NAME></code>	<NAME> – NAT addresses pool name, set by the string of up to 31 characters.
3	Set the range of IP addresses which will replace a source IP address.	<code>esr(config-snat-pool)# ip address-range <IP>[-<ENDIP>]</code>	<IP> – IP address of the beginning of the range, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <ENDIP> – IP address of the end of the range, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]. If IP address of the end of the range is not specified, only IP address of the beginning of the range is used as IP address for translation.
4	Specify the range of external TCP/UDP ports which will replace a source TCP/UDP port.	<code>esr(config-snat-pool)# ip port-range <PORT>[-<ENDPORT>]</code>	<PORT> – TCP/UDP port of the beginning of range, takes values of [1..65535]. <ENDPORT> – TCP/UDP port of the end of range, takes values of [1..65535]. If TCP/UDP port of the end of the range is not specified, only TCP/UDP port of the beginning of the range is used as TCP/UDP port for translation.
5	Set the internal TCP/UDP port which will replace a source TCP/UDP port.	<code>esr(config-snat-pool)# ip port <PORT></code>	<PORT> – TCP/UDP port, takes values of [1..65535].
6	Enable NAT persistent functions.	<code>esr(config-snat-pool)# persistent</code>	
7	Create a rule group with a specific name.	<code>esr(config-snat)# ruleset <NAME></code>	<NAME> – rule group name, set by the string of up to 31 characters.
8	Specify VRF instance, in which the given rule group will operate (optionally).	<code>esr(config-snat-ruleset)# ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.

9	Set the rule group scope. The rules will be applied only to traffic coming to a certain zone or interface.	<code>esr(config-snat-ruleset)# to { zone <NAME> interface <IF> tunnel <TUN> default }</code>	<NAME> – isolation zone name; <IF> – device interface name; <TUN> – device tunnel name; default – defines a rule group for all traffic, the source of which does not meet the requirements of other rule groups.
10	Specify a rule with a certain number. The rules are proceeded in ascending order.	<code>esr(config-snat-ruleset)# rule <ORDER></code>	<ORDER> – rule number, takes values of [1..10000].
11	Specify the profile of IP addresses {sender recipient} for which the rule should work.	<code>esr(config-snat-rule)# match [not]¹ {source destination}-address <OBJ-GROUP-NETWORK-NAME></code>	<OBJ-GROUP-NETWORK-NAME> – IP addresses profile name, set by the string of up to 31 characters. “Any” value points at any source IP address.
12	Specify the profile of IP addresses {sender recipient} for which the rule should work (optionally).	<code>esr(config-snat-rule)# match [not]¹ {source destination}-port <PORT-SET-NAME></code>	<PORT-SET-NAME> – port profile name, set by the string of up to 31 characters. “Any” value points at any source TCP/UDP port.
13	Set name or number of IP for which the rule should work (optionally).	<code>esr(config-snat-rule)# match [not]¹{protocol protocol-id} <TYPE></code>	<TYPE> – protocol type, takes the following values: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. “Any” value points at any protocol type. <ID> – IP identification number, takes values of [0x00-0xFF].
14	Specify the type and code of ICMP messages for which the rule should work (optionally).	<code>esr(config-snat-rule)# match [not] icmp {<ICMP_TYPE><ICMP_CODE> <TYPE-NAME>}</code>	<ICMP_TYPE> – ICMP message type, takes values of [0..255]. <ICMP_CODE> – ICMP message code, takes values of [0..255]. “Any” value points at any message code. <TYPE-NAME> – ICMP message type name.
15	Specify the action “translation of source address and port” for the traffic meeting the requirements of “match” command.	<code>esr(config-snat-rule)# action source-nat { off pool <NAME> netmap <ADDR/LEN> [static] interface [FIRST_PORT – LAST_PORT] }</code>	off – translation is disabled; pool<NAME> – name of the pool that contains IP addresses and/or TCP/UDP ports set; netmap <ADDR/LEN> – subnet IP address and mask used during translation; static – option for static NAT organization. The parameter is defined as AAA.BBB.CCC.DDD/EE where each part AAA-DDD takes values of [0..255] and EE takes values of [1..32]. interface [FIRST_PORT – LAST_PORT] – specify the translation to the interface IP address. If the range of TCP/UDP ports is additionally specified, the translation will occur only for the sender TCP/UDP ports included in the specified range.
16	Activate a configured rule.	<code>esr(config-snat-rule)# enable</code>	

Each “match” command may contain “not” key. When using the key, packets that do not meet the given requirement will fall under the rule.

You can obtain more detail information about firewall configuration in “CLI command reference guide”.

7.11.2 Configuration example 1

Objective:

Configure access for users in LAN 10.1.2.0/24 to public network using Source NAT function. Specify public network address range for SNAT 100.0.0.100-100.0.0.249.

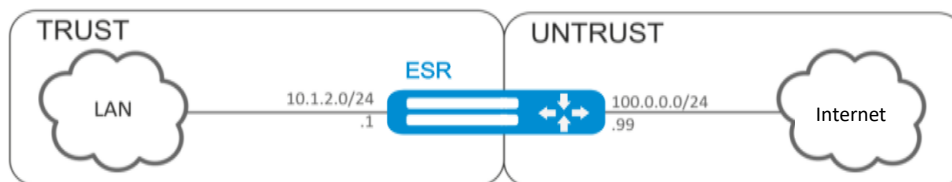


Figure 45 – Network structure

Solution:

Begin configuration with creation of security zones, configuration of network interfaces and their inheritance to security zones. Create 'TRUST' zone for LAN and 'UNTRUST' zone for public network.

```
esr# configure
esr(config)# security zone UNTRUST
esr(config-zone)# exit
esr(config)# security zone TRUST
esr(config-zone)# exit

esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 10.1.2.1/24
esr(config-if-gi)# security-zone TRUST
esr(config-if-gi)# exit

esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 100.0.0.99/24
esr(config-if-te)# security-zone UNTRUST
esr(config-if-te)# exit
```

For SNAT function configuration and definition of rules for security zones, create 'LOCAL_NET' LAN address profile that includes addresses which are allowed to access the public network and 'PUBLIC_POOL' public network address profile.

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip address-range 10.1.2.2-10.1.2.254
esr(config-object-group-network)# exit

esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip address-range 100.0.0.100-100.0.0.249
esr(config-object-group-network)# exit
```

To transfer traffic from 'TRUST' zone into 'UNTRUST' zone, create a pair of zones and add rules allowing traffic transfer in this direction. Additionally, there is a check in place to ensure that data source address belongs to 'LOCAL_NET' address range in order to limit the access to public network. Rules are applied with enable command.

```
esr(config)# security zone-pair TRUST UNTRUST
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# match source-address LOCAL_NET
esr(config-zone-pair-rule)# match destination-address any
```

```

esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

Configure SNAT service. First step is to create public network address pool for use with SNAT.

```

esr(config)# nat source
esr(config-snat)# pool TRANSLATE_ADDRESS
esr(config-snat-pool)# ip address-range 100.0.0.100-100.0.0.249
esr(config-snat-pool)# exit

```

Second step is to create SNAT rule set. In the set attributes, specify that the rules are applying only to packets transferred to public network—into the 'UNTRUST' zone. Rules include a check which ensures that data source address belongs to 'LOCAL_NET' pool.

```

esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to zone UNTRUST
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit

```

In order the router could response to the ARP requests for addresses from the public pool, you should launch ARP Proxy service. ARP Proxy service is configured on the interface that IP address from 'PUBLIC_POOL' public network address profile subnet belongs to.

```

esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PUBLIC_POOL

```

To enable public network access for LAN devices, they should be configured for routing—10.1.2.1 should be defined as a gateway address.

On the router, you should create the route for public network. Specify this route as a default using the following command.

```

esr(config)# ip route 0.0.0.0/0 100.0.0.1
esr(config)# exit

```

7.11.3 Configuration example 2

Objective:

Configure access for users in LAN 21.12.2.0/24 to public network using Source NAT function without the firewall. Public network address range for SNAT 200.10.0.100-200.10.0.249.



Figure 46 – Network structure

Solution:

Begin configuration with network interface configuration and disabling the firewall:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 21.12.2.1/24
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# exit

esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 200.10.0.1/24
esr(config-if-te)# ip firewall disable
esr(config-if-te)# exit
```

For SNAT function configuration, create 'LOCAL_NET' LAN address profile that includes addresses which are allowed to access the public network and 'PUBLIC_POOL' public network address profile.

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip address-range 21.12.2.2-21.12.2.254
esr(config-object-group-network)# exit

esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip address-range 200.10.0.100-200.10.0.249
esr(config-object-group-network)# exit
```

Configure SNAT service.

First step is to create public network address pool for use with SNAT:

```
esr(config)# nat source
esr(config-snat)# pool TRANSLATE_ADDRESS
esr(config-snat-pool)# ip address-range 200.10.0.100-200.10.0.249
esr(config-snat-pool)# exit
```

Second step is to create SNAT rule set. In the set attributes, specify that the rules are applying only to packets transferred to public network through te1/0/1 port. Rules include a check which ensures that data source address belongs to 'LOCAL_NET' pool:

```
esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to interface te1/0/1
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
```

In order the router could response to the ARP requests for addresses from the public pool, you should launch ARP Proxy service. ARP Proxy service is configured on the interface that IP address from 'PUBLIC_POOL' public network address profile subnet belongs to:

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PUBLIC_POOL
```

To enable public network access for LAN devices, they should be configured for routing – 21.12.2.1 should be defined as a gateway address.

On the router, you should create the route for public network. Specify this route as a default using the following command:

```
esr(config)# ip route 0.0.0.0/0 200.10.0.254
```

```
esr(config)# exit
```

7.12 Static NAT configuration

Static NAT — static NAT sets a unique match between two addresses. In other words, when passing through the router the address is changed to another strictly specified one, one-to-one. The record about this translation is kept indefinitely until NAT reconfiguration is carried out on the router.

7.12.1 Configuration algorithm

Static NAT configuration is carried out by Source NAT means, the configuration algorithm is described in Section 7.11.1 of the manual.

7.12.1 Static NAT configuration example

Objective:

Configure two-way and continuous translation from LAN for the addresses range of 21.12.2.100-21.12.2.150 to the public network 200.10.0.0/24. Public network address range for translation use – 200.10.0.100-200.10.0.150.



Figure 47 – Network structure

Solution:

Begin configuration with network interface configuration and disabling the firewall:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 21.12.2.1/24
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# exit

esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 200.10.0.1/24
esr(config-if-te)# ip firewall disable
esr(config-if-te)# exit
```

For Static NAT configuration, create 'LOCAL_NET' LAN address profile that includes local subnet and 'PUBLIC_POOL' public network address profile.

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip prefix 21.12.2.0/24
esr(config-object-group-network)# exit

esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip prefix 200.10.0.0/24
esr(config-object-group-network)# exit
```

The range of public network addresses for Static NAT use is specified in “PROXY” profile:

```
esr(config)# object-group network PROXY
esr(config-object-group-network)# ip address-range 200.10.0.100-200.10.0.150
esr(config-object-group-network)# exit
```

Configure Static NAT service in SNAT configuration mode. In the set attributes, specify that the rules are applying only to packets transferred to public network through te1/0/1 port. The rules include data source address test for belonging to “LOCAL_NET” pool and destination addresses test for belonging to “PUBLIC_POOL” pool.

```
esr(config)# nat source
esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to interface te1/0/1
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# match destination-address PUBLIC_POOL
esr(config-snat-rule)# action source-nat netmap 200.10.0.0/24 static
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
```

In order the router could response to the ARP requests for addresses from the “PROXY” translation pool, you should launch ARP Proxy service. ARP Proxy service is configured on the interface that IP address from 'PROXY' address profile subnet belongs to:

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PROXY
```

To enable 200.10.0.0/24 network access for LAN devices, they should be configured for routing – 21.12.2.1 should be defined as a gateway address.

The configuration changes come into effect after applying the following commands:

```
esr# commit
Configuration has been successfully committed
esr# confirm
Configuration has been successfully confirmed
```

You can display active translations by using the following command:

```
esr# show ip nat translations
```

7.12.3 Configuration example of application filtration (DPI)



Attention! The use of application filtering mechanism reduces by several times the router performance because of the need to check each packet. The performance decreases with an increase in amount of the selected for filtration applications.

Objective:

Block access to such resources as youtube, bittorrent and facebook.



Figure 48 – Network structure

Solution:

Create a security zone for each ESR network:

```
esr# configure
esr(config)# security zone LAN
esr(config-zone)# exit
esr(config)# security zone WAN
esr(config-zone)# exit
```

Configure network interfaces and identify their inheritance to security zones:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# ip address 10.0.0.1/24
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# exit
esr(config)# interface gi1/0/2
esr(config-if-te)# ip address 192.168.0.1/24
esr(config-if-te)# security-zone LAN
esr(config-if-te)# exit
```

To configure security zones rules, you should create profile of the applications that should be blocked.

```
esr(config)# object-group application APP
esr(config-object-group-application)# application youtube
esr(config-object-group-application)# application bittorrent
esr(config-object-group-application)# application facebook
esr(config-object-group-application)# exit
```

To set the rules of traffic passing from “WAN” zone to “LAN” zone, create a couple of zones and add a rule prohibiting the application traffic from passing and a rule allowing the rest of traffic to pass. Rules are applied with *enable* command.

```
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action deny
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match application APP
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-pair)# exit
```

To set the rules of traffic passing from “LAN” zone to “WAN” zone, create a couple of zones and add a rule allowing all traffic to pass. Rules are applied with *enable* command.

```
esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-pair)# exit
```

To view port membership in zones, use the following command:

```
esr# show security zone
```

To view zone pairs and their configuration, use the following commands:

```
esr# show security zone-pair
esr# show security zone-pair configuration
```

To view active sessions, use the following commands:

```
esr# show ip firewall sessions
```

7.13 Configuration of logging and protection against network attacks

7.13.1 Configuration algorithm

Step	Description	Command	Keys
1	Enable protection against ICMP flood attacks.	<code>esr(config)# ip firewall screen dos- defense icmp- threshold { <NUM> }</code>	<NUM> – amount of ICMP packets per second, set in the range of [1..10000]
2	Enable protection against land attacks	<code>esr(config)# firewall screen dos-defense land</code>	
3	Enable the limitation on amount of simultaneous sessions based on the destination address	<code>esr(config)# ip firewall screen dos- defense limit- session-destination { <NUM> }</code>	<NUM> – limitation on amount of IP sessions, set in the range of [1..10000].
4	Enable the limitation on the amount of simultaneous sessions, based on the source address, that mitigates DoS attacks	<code>esr(config)# ip firewall screen dos- defense limit- session-source { <NUM> }</code>	<NUM> – limitation on amount of IP sessions, set in the range of [1..10000].
5	Enable protection against SYN flood attacks.	<code>esr(config)# ip firewall screen dos- defense syn-flood { <NUM> } [src-dsr]</code>	<NUM> – maximum amount of TCP packets with the set SYN flag per second, set in the range of [1..10000]. src-dst – limitation on the amount of TCP packets with the SYN flag set, based on the source and destination addresses.

6	Enable protection against UDP flood attacks.	<code>esr(config)# ip firewall screen dos- defense udp-threshold { <NUM> }</code>	<NUM> – maximum amount of UDP packets per second, set in the range of [1..10000].
7	Enable protection against winnuke attacks	<code>esr(config)# ip firewall screen dos- defense winnuke</code>	
8	Enable the blocking of TCP packets with the FIN flag set and the ACK flag not set.	<code>esr(config)# ip firewall screen spy- blocking fin-no-ack</code>	
9	Enable the blocking of various type ICMP packets	<code>esr(config)# ip firewall screen spy- blocking icmp-type</code>	<TYPE> – ICMP type, may take the following values: destination-unreachable echo-request reserved source-quench time-exceeded
10	Enable the protection against IP-sweep attacks.	<code>esr(config)# ip firewall screen spy- blocking ip-sweep { <NUM> }</code>	<NUM> – ip sweep attack detection time, set in milliseconds [1..1000000].
11	Enable protection against port scan attacks.	<code>esr(config)# ip firewall screen spy- blocking port-scan { <threshold> } [<TIME>]</code>	<threshold> – interval in milliseconds during which the port scan attack will be recorded [1..1000000]. <TIME> – blocking time in milliseconds [1..1000000].
12	Enable the protection against IP spoofing attacks.	<code>esr(config)# ip firewall screen spy- blocking spoofing</code>	
13	Enable the blocking of TCP packets, with the SYN and FIN flags set	<code>esr(config)# ip firewall screen spy- blocking syn-fin</code>	
14	Enable the blocking of TCP packets, with all flags or with the set of flags: FIN,PSH,URG. The given command provides the protection against XMAS attack	<code>esr(config)# ip firewall screen spy- blocking tcp-all-flag</code>	
15	Enable the blocking of TCP packets, with the zero "flags" field.	<code>esr(config)# ip firewall screen spy- blocking tcp-no-flag</code>	
16	Enable the blocking of fragmented ICMP packets	<code>esr(config)# ip firewall screen suspicious-packets icmp-fragment</code>	
17	Enable the blocking of fragmented IP packets.	<code>esr(config)# ip firewall screen suspicious-packets ip-fragment</code>	
18	Enable the blocking of ICMP packets more than 1024 bytes.	<code>esr(config)# ip firewall screen suspicious-packets icmp-fragment</code>	
19	Enable the blocking of fragmented TCP packets, with the SYN flag	<code>esr(config)# ip firewall screen suspicious-packets syn-fragment</code>	
20	Enable the blocking of fragmented UDP packets	<code>esr(config)# ip firewall screen suspicious-packets udp-fragment</code>	

21	Enable the blocking of packets, with the protocol ID contained in IP header equal to 137 and more	<code>esr(config)# ip firewall screen suspicious-packets unknown-protocols</code>	
22	Set the frequency of notification (via SNMP, syslog and in CLI) of detected and blocked network attacks	<code>esr(config)# ip firewall logging interval <NUM></code>	<NUM> – time interval in seconds [30 .. 2147483647]
23	Enable more detailed message output about detected and blocked network attacks in the CLI.	<code>esr(config)# ip firewall logging screen detailed</code>	
24	Enable mechanism of DoS attacks detection and logging via CLI, syslog and SNMP.	<code>esr(config)# ip firewall logging screen dos-defense <ATTACK_TYPE></code>	<ATTACK_TYPE> – DoS attack type, takes the following values: icmp-threshold, land, limit-session-destination, limit-session-source, syn-flood, udp-threshold, winnuke.
25	Enable mechanism of espionage activity detection and logging via CLI, syslog and SNMP.	<code>esr(config)# ip firewall logging screen spy-blocking { <ATTACK_TYPE> icmp-type <ICMP_TYPE> }</code>	<ATTACK_TYPE> – espionage activity type, takes the following values: fin-no-ack, ip-sweep, port-scan, spoofing, syn-fin, tcp-all-flag, tcp-no-flag. <ICMP_TYPE> – ICMP type, takes the following values: destination-unreachable, echo-request, reserved, source-quench, time-exceeded.
26	Enable mechanism of specialized packets detection and logging via CLI, syslog and SNMP.	<code>esr(config)# ip firewall logging screen suspicious- packets <PACKET_TYPE></code>	<PACKET_TYPE> – specialized packets type, takes the following values: icmp-fragment, ip-fragment, large-icmp, syn-fragment, udp-fragment, unknown-protocols.

7.13.2 Description of attack protection mechanisms

ip firewall screen dos-defense icmp-threshold

The given command enables the protection against ICMP flood attacks. When the protection is enabled, the amount of all types ICMP packets per second for one destination address is limited. The attack leads to the host reboot and its failure due to the necessity to process each query and respond to it.

ip firewall screen dos-defense land

The given command enables the protection against land attacks. When the protection is enabled, the packets with the same source and destination IP addresses and with SYN flag in TCP header are blocked. The attack leads to the host reboot and its failure due to the necessity to process each TCP SYN packet and the attempts of the host to establish a TCP session with itself.

ip firewall screen dos-defense limit-session-destination

When the host IP sessions table is overfilled, the host is unable to establish new sessions and it drops the queries (this may happen during various attacks: SYN flood, UDP flood, ICMP flood and etc.). The command enables the limitation on the amount of simultaneous sessions, based on the source address, that mitigates DoS attacks.

ip firewall screen dos-defense limit-session-source

When the host IP sessions table is overfilled, the host is unable to establish new sessions and it drops the queries (this may happen during various DoS attacks: SYN flood, UDP flood, ICMP flood and etc.). The command enables the limitation on the amount of simultaneous sessions, based on the source address, that mitigates DoS attacks.

ip firewall screen dos-defense syn-flood

The given command enables the protection against SYN flood attacks. When the protection is enabled, the amount of TCP packets with the SYN flag set per second for one destination address is limited. The attack leads to the host reboot and its failure due to the necessity to process each TCP SYN packet and the attempts to establish a TCP session.

ip firewall screen dos-defense udp-threshold

The given command enables the protection against UDP flood attacks. When the protection is enabled, the amount of UDP packets per second for one destination address is limited. The attack lead to the host reboot and its failure due to the massive UDP traffic.

ip firewall screen dos-defense winnuke

The given command enables the protection against winnuke attacks. When the protection is enabled, TCP packets with the URG flag set and 139 destination port are blocked. The attack leads to the older Windows versions (up to 95 version) failure.

ip firewall screen spy-blocking fin-no-ack

The given command enables the blocking of TCP packets with the FIN flag set and the ACK flag not set. These packets are specialized and it is possible to determine a victim operational system by the respond.

ip firewall screen spy-blocking icmp-type destination-unreachable

The given command enables the blocking of all 3 type ICMP packets (destination-unreachable) including the packets generated by the router itself. The protection prevents an attacker from learning about network topology and hosts availability

ip firewall screen spy-blocking icmp-type echo-request

The given command enables the blocking of all 8 type ICMP packets (echo-request) including the packets generated by the router itself. The protection prevents an attacker from learning about network topology and hosts availability

ip firewall screen spy-blocking icmp-type reserved

The given command enables the blocking of all 2 and 7 type ICMP packets (reserved) including the packets generated by the router itself. The protection prevents an attacker from learning about network topology and hosts availability

ip firewall screen spy-blocking icmp-type source-quench

The given command enables the blocking of all 4 type ICMP packets (source quench) including the packets generated by the router itself. The protection prevents an attacker from learning about network topology and hosts availability

ip firewall screen spy-blocking icmp-type time-exceeded

The given command enables the blocking of all 11 type ICMP packets (time exceeded) including the packets generated by the router itself. The protection prevents an attacker from learning about network topology and hosts availability

ip firewall screen spy-blocking ip-sweep

The given command enables the protection against IP-sweep attacks. When the protection is enabled, if more than 10 ICMP queries from one source arrive within the specified interval, the first 10 queries are dropped by the router and 11th with the following ones are discarded for the remaining interval time. The protection prevents an attacker from learning about network topology and hosts availability.

ip firewall screen spy-blocking port-scan

The given command enables the protection against port scan attacks. If more than 10 TCP packets with the SYN flag arrive to one source within the first specified interval (<THRESHOLD>), then this behaviour is recorded as port scan attack and all the following packets of that type are blocked for the second specified time interval (<TIME>). An attacker will not be able to scan the device open ports quickly.

ip firewall screen spy-blocking spoofing

The given command enables the protection against ip spoofing attacks. When the protection is enabled, the router checks packets for matching the source address and routing table entries, and in case of mismatch the packet is dropped. For example, if a packet with source address 10.0.0.1/24 arrives to the Gi1/0/1 interface and the given subnet is located after the Gi1/0/2 interface in the routing table, it is considered that the source address has been replaced. Protects from network intrusions with replaced source IP addresses.

ip firewall screen spy-blocking syn-fin

The given command enables the blocking of TCP packets, with the SYN and FIN flags set. These packets are specialized and it is possible to determine a victim operational system by the respond.

ip firewall screen spy-blocking tcp-all-flag

Enable the blocking of TCP packets, with all flags or with the set of flags: FIN, PSH, URG. The protection against XMAS attack is provided.

ip firewall screen spy-blocking tcp-no-flag

The given command enables the blocking of TCP packets, with the zero “flags” field. These packets are specialized and it is possible to determine a victim operational system by the respond.

ip firewall screen suspicious-packets icmp-fragment

The given command enables the blocking of fragmented ICMP packets. ICMP packets are usually small and there is no need to fragment them.

ip firewall screen suspicious-packets ip-fragment

The given command enables the blocking of fragmented packets.

ip firewall screen suspicious-packets large-icmp

The given command enables the blocking of ICMP packets more than 1024 bytes.

ip firewall screen suspicious-packets syn-fragment

The given command enables the blocking of fragmented TCP packets, with the SYN flag. TCP packets with the SYN flag are usually small and there is no need to fragment them. The protection prevents concentration of fragmented packets in a buffer.

ip firewall screen suspicious-packets udp-fragment

The given command enables the blocking of fragmented UDP packets.

ip firewall screen suspicious-packets unknown-protocols

The given command enables the blocking of packets, with the protocol ID contained in IP header equal to 137 and more.

7.13.3 Configuration example of logging and protection against network attacks

Objective:

Protect LAN and ESR router from land, syn-flood, ICMP flood network attacks and configure the notification of attacks by SNMP to SNMP server 192.168.0.10

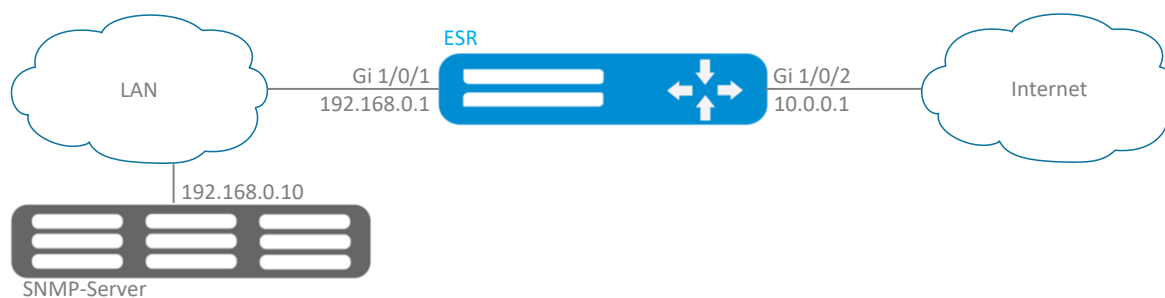


Figure 49 – Network structure

Solution:

You should first configure interfaces and firewall (firewall configuration or its absence will not influence on the operation of network attacks protection):

```

esr(config)# security zone LAN
esr(config-zone)# exit
esr(config)# security zone WAN
esr(config-zone)# exit
esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 100
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# ex
esr(config-zone-pair)# exit
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 100
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# ip address 10.0.0.1/24
esr(config-if-gi)# exit

```

Enable the protection against land, syn-flood, ICMP flood attacks:

```

esr(config)# ip firewall screen dos-defense land
esr(config)# ip firewall screen dos-defense syn-flood 100 src-dst
esr(config)# ip firewall screen dos-defense icmp-threshold 100

```

Configure the logging of detected attacks:

```

esr(config)# ip firewall logging screen dos-defense land
esr(config)# ip firewall logging screen dos-defense syn-flood
esr(config)# ip firewall logging screen dos-defense icmp-threshold

```

Configure SNMP server to which the traps will be sent

```

esr(config)# snmp-server
esr(config)# snmp-server host 192.168.0.10

```

To view the statistics on recorded network attacks, use the following command:

```

esr# show ip firewall screen counters

```

7.14 Firewall configuration

Firewall is a package of hardware or software tools that allows for control and filtering of transmitted network packets in accordance with the defined rules.

7.14.1 Configuration algorithm

Step	Description	Command	Keys
1	Create security zones.	<code>esr(config)# security zone <zone-name1></code> <code>esr(config)# security zone <zone-name2></code>	<zone-name> – up to 12 characters.
2	Specify a security zone description.	<code>esr(config-zone)# description <description></code>	<description> - up to 255 characters.
3	Specify VRF instance, in which the given security zone will operate (optionally).	<code>esr(config-zone)# ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.
4	Enable session counters for NAT and Firewall (optionally, may reduce the performance).	<code>esr(config)# ip firewall sessions counters</code>	
5	Disable filtration of packets for which it was not possible to determine belonging to any known connection and which are not the beginning of a new connection (optionally, may reduce the performance).	<code>esr(config)# ip firewall sessions allow-unknown</code>	
6	Select firewall operation mode (optionally)	<code>esr(config)# ip firewall mode <MODE></code>	<MODE> – firewall operation mode, may take the following values: stateful, stateless. Default value: stateful
7	Determine the session lifetime for unsupported protocols (optionally).	<code>esr(config)# ip firewall sessions generic-timeout <TIME></code>	<TIME> – session lifetime for unsupported protocols, takes values in seconds [1..8553600]. By default: 60 seconds.
8	Determine ICMP session lifetime after which it is considered to be outdated (optionally).	<code>esr(config)# ip firewall sessions icmp-timeout <TIME></code>	<TIME> – ICMP session lifetime, takes values in seconds [1..8553600]. By default: 30 seconds.
9	Determine ICMPv6 session lifetime after which it is considered to be outdated (optionally).	<code>esr(config)# ip firewall sessions icmpv6-timeout <TIME></code>	<TIME> – ICMP session lifetime, takes values in seconds [1..8553600]. By default: 30 seconds.
10	Determine the size of outstanding sessions table (optionally).	<code>esr(config)# ip firewall sessions max-expect <COUNT></code>	<COUNT> – table size, takes values of [1..8553600]. By default: 256.
11	Determine the size of trackable sessions table (optionally).	<code>esr(config)# ip firewall sessions max-tracking <COUNT></code>	<COUNT> – table size, takes values of [1..8553600]. By default: 512000.
12	Determine the lifetime of TCP session in “connection is being established” state after which it is considered to be outdated (optionally).	<code>esr(config)# ip firewall sessions tcp-connect-timeout <TIME></code>	<TIME> – lifetime of TCP session in “connection is being established” state, takes values in seconds [1..8553600]. By default: 60 seconds.

13	Determine the lifetime of TCP session in “connection is being closed” state after which it is considered to be outdated (optionally).	<code>esr(config)# ip firewall sessions tcp-disconnect- timeout <TIME></code>	<TIME> – lifetime of TCP session in “connection is being closed” state, takes values in seconds [1..8553600]. By default: 30 seconds.
14	Determine the lifetime of TCP session in “connection is being established” state after which it is considered to be outdated (optionally).	<code>esr(config)# ip firewall sessions tcp-established- timeout <TIME></code>	<TIME> – lifetime of TCP session in “connection is being established” state, takes values in seconds [1..8553600]. By default: 120 seconds.
15	Determine the timeout after which the closed TCP session is actually deleted from the table of trackable sessions (optionally).	<code>esr(config)# ip firewall sessions tcp-latecome-timeout <TIME></code>	<TIME> – timeout, takes value in seconds [1..8553600]. By default: 120 seconds.
16	Enable application-level session tracking for certain protocols (optionally).	<code>esr(config)# ip firewall sessions tracking { <PROTOCOL> sip [<OBJECT-GROUP- SERVICE>] }</code>	<PROTOCOL> – application-level protocol [ftp, h323, pptp, netbios-ns, tftp] sessions of which should be tracked. <OBJECT-GROUP-SERVICE> – profile name of SIP session TCP/UDP ports, set by the string of up to 31 characters. If the group is not specified, SIP session tracking will be carried out for 5060 port. Instead of a certain protocol you can use the “all” key that enables application-level session tracking for all available protocols. By default - disabled for all protocols
17	Determine the lifetime of UDP session in “connection is confirmed” state after which it is considered to be outdated (optionally).	<code>esr(config)# ip firewall sessions udp-assured-timeout <TIME></code>	<TIME> – lifetime of UDP session in “connection is confirmed” state, takes values in seconds [1..8553600]. By default: 180 seconds.
18	Determine the lifetime of UDP session in “connection is not confirmed” state after which it is considered to be outdated (optionally).	<code>esr(config)# ip firewall sessions udp-wait-timeout <TIME></code>	<TIME> – lifetime of UDP session in “connection is not confirmed” state, takes values in seconds [1..8553600]. By default: 30 seconds.
19	Create IP addresses lists which will be used during filtration.	<code>esr(config)# object- group network <obj- group-name></code>	<obj-group-name> – up to 31 characters.
20	Specify IP addresses list description (optionally).	<code>esr(config-object- group-network) # description <description></code>	<DESCRIPTION> – profile description, set by the string of up to 255 characters.
21	Add necessary IPv4/IPv6 addresses to the list.	<code>esr(config-object- group-network) # ip prefix <ADDR/LEN></code>	<ADDR/LEN> – subnet, defined as AAA.BBB.CCC.DDD/EE where each part AAA- DDD takes values of [0..255] and EE takes values of [1..32].
		<code>esr(config-object- group-network) # ip address-range <FROM- ADDR>-<TO-ADDR></code>	<FROM-ADDR> – range starting IP address; <TO-ADDR> – range ending IP address, optional parameter; If the parameter is not specified, a single IP address is set by the command. The addresses are defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].

		<code>esr (config-object-group-network) # ipv6 prefix <IPV6-ADDR/LEN></code>	<IPV6-ADDR/LEN> – IP address and mask of a subnet, defined as X:X:X:X/EE where each X part takes values in hexadecimal format [0..FFFF] and EE takes values of [1..128].
		<code>esr (config-object-group-network) # ipv6 address-range <FROM-ADDR>-<TO-ADDR></code>	<FROM-ADDR> – range starting IPv6 address; <TO-ADDR> – range ending IPv6 address, optional parameter. If the parameter is not specified, a single IPv6 address is set by the command. The addresses are defined as X:X:X:X where each part takes values in hexadecimal format [0..FFFF].
22	Create services lists which will be used during filtration.	<code>esr (config) # object-group service <obj-group-name></code>	<obj-group-name> – service profile name, set by the string of up to 31 characters.
23	Specify services list description (optionally).	<code>esr (config-object-group-service) # description <description></code>	<description> – profile description, set by the string of up to 255 characters.
24	Add necessary services (tcp/udp ports) to the list.	<code>esr (config-object-group-service) # port-range <port></code>	<port> – takes values in the range of [1..65535]. You can specify several ports separated by commas “,” or you can specify the range of ports with “-”.
25	Create applications lists which will be used in DPI mechanism.	<code>esr (config) # object-group application <NAME></code>	<NAME> – application profile name, set by the string of up to 31 characters.
26	Specify applications list description (optionally).	<code>esr (config-object-group-application) # description <description></code>	<description> – profile description, set by the string of up to 255 characters.
27	Add necessary applications to the lists.	<code>esr (config-object-group-application) # application <APPLICATION ></code>	<APPLICATION> – specifies the application covered by the given profile
28	Add interfaces (physical, logical, E1/Multilink and connected), remote-access server (l2tp, openvpn, pptp) or tunnels (gre, ip4ip4, l2tp, lt, pppoe, pptp) into security zones (optionally).	<code>esr (config-if-gi) # security-zone <zone-name></code>	<zone-name> – up to 12 characters.
	Disable Firewall functions on the network interface (physical, logical, E1/Multilink and connected), remote-access server (l2tp, openvpn, pptp) or tunnels (gre, ip4ip4, l2tp, lt, pppoe, pptp) (optionally).	<code>esr (config-if-gi) # ip firewall disable</code>	
29	Create an interzone interaction rule set.	<code>esr (config) # security zone-pair <src-zone-name1> <dst-zone-name2></code>	<src-zone-name> – up to 12 characters. <dst-zone-name> – up to 12 characters.
30	Create an interzone interaction rule set.	<code>esr (config-zone-pair) # rule <rule-number></code>	<rule-number> - 1..10000.
31	Specify rule description (optionally).	<code>esr (config-zone-rule) # description <description></code>	<description> - up to 255 characters.

32	Specify the given rule force.	<code>esr(config-zone-rule)# action <action> [log]</code>	<action> - permit/deny/reject/netflow-sample/sflow-sample log – activation key for logging of sessions established according to the given rule.
33	Set name or number of IP for which the rule should work.	<code>esr(config-zone-rule)# match [not]¹ protocol <protocol-type></code>	<protocol-type> – protocol type, takes the following values: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. When specifying the “any” value, the rule will work for any protocols.
		<code>esr(config-zone-rule)# match [not]¹ protocol-id <protocol-id></code>	<protocol-id> – IP identification number, takes values of [0x00-0xFF].
34	Specify the profile of transmitter IP addresses for which the rule should work.	<code>esr(config-zone-rule)# match [not]¹ source-address <OBJ-GROUP-NETWORK-NAME></code>	<OBJ-GROUP-NETWORK-NAME> – IP addresses profile name, set by the string of up to 31 characters. When specifying the “any” value, the rule will work for sender/recipient IP address.
35	Set the profile of destination IP addresses for which the rule should work.	<code>esr(config-zone-rule)# match [not]¹ destination-address <OBJ-GROUP-NETWORK-NAME></code>	
36	Set source MAC address for which the rule should work (optionally).	<code>esr(config-zone-rule)# match [not]¹ source-mac <mac-addr></code>	<mac-addr> – defined as XX:XX:XX:XX:XX:XX where each part takes the values of [00..FF].
37	Set sender MAC address for which the rule should work (optionally).	<code>esr(config-zone-rule)# match [not]¹ destination-mac <mac-addr></code>	
38	Set TCP/UDP ports profile for which the rule should work (if the protocol is specified).	<code>esr(config-zone-rule)# match [not]¹ source-port <PORT-SET-NAME></code>	<PORT-SET-NAME> – set by the string of up to 31 characters. When specifying the “any” value, the rule will work for any sender/recipient TCP/UDP port.
39	Set the destination TCP/UDP ports profile for which the rule should work (if the protocol is specified).	<code>esr(config-zone-rule)# match [not]¹ destination-port <PORT-SET-NAME></code>	
40	Specify the type and code of ICMP messages for which the rule should work (if ICMP is selected as protocol).	<code>esr(config-zone-rule)# match [not]¹ icmp <ICMP_TYPE> <ICMP_CODE></code>	<ICMP_TYPE> – ICMP message type, takes values of [0..255]. <ICMP_CODE> – ICMP message code, takes values of [0..255]. When specifying the “any” value, the rule will work for any ICMP message code.
41	Set the limitation under which the rule will only work for traffic modified by the IP address and destination ports translation service.	<code>esr(config-zone-rule)# match [not]¹ destination-nat</code>	
42	Set the maximum packet rate (optionally, available only for zone-pair any self and zone-pair <zone-name> any).	<code>esr(config-zone-pair-rule)# rate-limit pps <rate-pps></code>	<rate-pps> - maximum amount of packets that can be transmitted. Takes values in the range of [1..10000].
43	Set the filtration only for fragmented IP packets (optionally, available only for zone-pair any self and zone-pair <zone-name> any).	<code>esr(config-zone-pair-rule)# match [not]¹ fragment</code>	

44	Set the filtration only for IP packets including ip-option (optionally, available only for zone-pair any self and zone-pair <zone-name> any).	<code>esr(config-zone-pair-rule)# match [not]¹ ip-option</code>	
45	Create an interzone interaction rule.	<code>esr(config-zone-rule)# enable</code>	
46	Enable the filtration and session tracking mode while packets are transmitted between one Bridge group participants (optionally, available only for ESR-1000/1200/1700)	<code>esr(config-bridge)# ports firewall enable</code>	

Each “match” command may contain “not” key. When using the key, packets that do not meet the given requirement will fall under the rule.

You can obtain more detail information about firewall configuration in “CLI command reference guide”.

7.14.2 Firewall configuration example

Objective:

Enable message passage via ICMP between PC1, PC2 and ESR router.

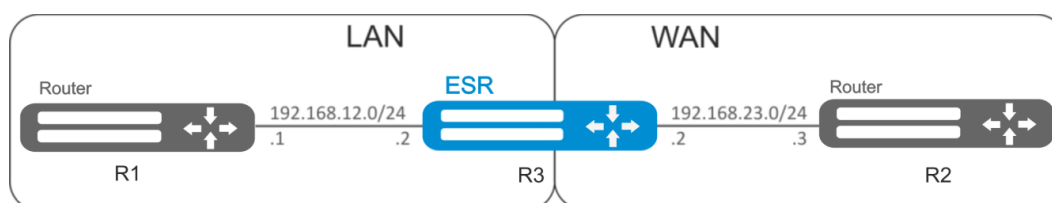


Figure 50 – Network structure

Solution:

Create a security zone for each ESR network:

```
esr# configure
esr(config)# security zone LAN
esr(config-zone)# exit
esr(config)# security zone WAN
esr(config-zone)# exit
```

Configure network interfaces and identify their inheritance to security zones:

```
esr(config)# interface gi1/0/2
esr(config-if-gi)# ip address 192.168.12.2/24
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# exit
esr(config)# interface gi1/0/3
esr(config-if-gi)# ip address 192.168.23.2/24
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# exit
```

To configure the rules for security zones, create 'LAN' address profile that includes addresses which are allowed to access WAN network and 'WAN' network address profile.

```
esr(config)# object-group network WAN
esr(config-object-group-network)# ip address-range 192.168.23.2
esr(config-object-group-network)# exit
esr(config)# object-group network LAN
esr(config-object-group-network)# ip address-range 192.168.12.2
esr(config-object-group-network)# exit
esr(config)# object-group network LAN_GATEWAY
esr(config-object-group-network)# ip address-range 192.168.12.1
esr(config-object-group-network)# exit
esr(config)# object-group network WAN_GATEWAY
esr(config-object-group-network)# ip address-range 192.168.23.3
esr(config-object-group-network)# exit
```

To transfer traffic from 'LAN' zone into 'WAN' zone, create a pair of zones and add a rule allowing ICMP traffic transfer from PC1 to PC2. Rules are applied with *enable* command.

```
esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address WAN_GATEWAY
esr(config-zone-pair-rule)# match source-address LAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

To transfer traffic from 'WAN' zone into 'LAN' zone, create a pair of zones and add a rule allowing ICMP traffic transfer from PC2 to PC1. Rules are applied with *enable* command: Rules are applied with *enable* command.

```
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address LAN_GATEWAY
esr(config-zone-pair-rule)# match source-address WAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

Router always has a security zone named 'self'. When the traffic recipient is the router itself, i.e. traffic is not transit, pass 'self' zone as a parameter. Create a pair of zones for traffic coming from 'WAN' zone into 'self' zone. In order the router could response to the ICMP requests from 'WAN' zone, add a rule allowing ICMP traffic transfer from PC2 to ESR router:

```
esr(config)# security zone-pair WAN self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address WAN
esr(config-zone-pair-rule)# match source-address WAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

Create a pair of zones for traffic coming from 'LAN' zone into 'self' zone. In order the router could response to the ICMP requests from 'LAN' zone, add a rule allowing ICMP traffic transfer from PC1 to ESR:

```

esr(config)# security zone-pair LAN self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address LAN
esr(config-zone-pair-rule)# match source-address LAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# exit

```

To view port membership in zones, use the following command:

```
esr# show security zone
```

To view zone pairs and their configuration, use the following commands:

```

esr# show security zone-pair
esr# show security zone-pair configuration

```

To view active sessions, use the following commands:

```
esr# show ip firewall sessions
```

7.15 Access list (ACL) configuration

Access Control List or ACL is a list that contains rules defining traffic transmission through the interface.

7.15.1 Configuration algorithm

Step	Description	Command	Keys
1	Create access control list and switch to its configuration mode.	<code>esr(config)# ip access-list extended <NAME></code>	<NAME> – access control list name, set by the string of up to 31 characters.
2	Specify the description of a configurable access control list (optionally).	<code>esr(config-acl)# description <DESCRIPTION></code>	<DESCRIPTION> – access control list description, set by the string of up to 255 characters.
3	Create a rule and switch to its configuration mode. The rules are proceeded by the router in number ascending order.	<code>esr(config-acl)# rule <ORDER></code>	<ORDER> – rule number, takes values of [1..4094].
4	Specify the action that should be applied for the traffic meeting the given requirements.	<code>esr(config-acl-rule)# action <ACT></code>	<ACT> – allocated action: permit – traffic transfer is permitted; deny – traffic transfer is denied.
5	Set name or number of protocol for which the rule should work.	<code>esr(config-acl-rule)# match protocol <TYPE></code>	<TYPE> – protocol type, takes the following values: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. When specifying the “any” value, the rule will work for any protocols.
		<code>esr(config-acl-rule)# match protocol-id <ID></code>	<ID> – IP identification number, takes values of [0x00-0xFF].

6	Set sender IP addresses for which the rule should work.	<code>esr(config-acl-rule)# match source-address { <ADDR> <MASK> any }</code>	<ADDR> – sender IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255];
7	Set destination IP addresses for which the rule should work.	<code>esr(config-acl-rule)# match destination- address { <ADDR> <MASK> any }</code>	<MASK> – IP address mask, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]. Mask bits, set to zero, specify IP address bits excluded from the comparison when searching. When specifying the “any” value, the rule will work for any sender/recipient IP address.
8	Set sender MAC addresses for which the rule should work (optionally).	<code>esr(config-acl-rule)# match source-mac <ADDR><WILDCARD></code>	<ADDR> – sender MAC address, defined as XX:XX:XX:XX:XX:XX where each part takes the values of [00..FF].
9	Set destination MAC addresses for which the rule should work (optionally).	<code>esr(config-acl-rule)# match destination-mac <ADDR><WILDCARD></code>	<WILDCARD> – MAC address mask, defined as XX:XX:XX:XX:XX:XX where each part takes the values of [00..FF]. Mask bits, set to zero, specify MAC address bits excluded from the comparison when searching.
10	Set the number of sender TCP/UDP ports for which the rule should work (if the protocol is specified).	<code>esr(config-acl-rule)# match source-port { <PORT> any }</code>	<PORT> – number of sender TCP/UDP port, takes values of [1..65535]. When specifying the “any” value, the rule will work for any sender TCP/UDP port.
11	Set the destination TCP/UDP ports number for which the rule should work (if the protocol is specified).	<code>esr(config-acl-rule)# match destination- port { <PORT> any }</code>	
12	Set priority 802.1p value for which the rule should work (optionally).	<code>esr(config-acl-rule)# match cos <COS></code>	<COS> – priority 802.1p value, takes values of [0..7].
13	Set DSCP code value for which the rule should work (optionally). Can not be used with IP Precedence.	<code>esr(config-acl-rule)# match dscp <DSCP></code>	<DSCP> – DSCP code value, takes values in the range of [0..63].
14	Set IP Precedence code for which the rule should work (optionally). Can not be used with DSCP.	<code>esr(config-acl-rule)# match ip-precedence <IPP></code>	<IPP> – IP Precedence code value, takes values in the range of [0..7].
15	Set VLAN ID for which the rule should work (optionally).	<code>esr(config-acl-rule)# match vlan <VID></code>	<VID> – VLAN ID, takes values of [1..4094].
16	Activate a rule.	<code>esr(config-acl-rule)# enable</code>	
17	Specify access control list for the configured interface to filtrate incoming traffic.	<code>esr(config-if-gi)# service-acl input <NAME></code>	<NAME> – access control list name, set by the string of up to 31 characters.

Also the access lists can be used to organize QoS policy.

7.15.2 Access list configuration example

Objective:

Allow traffic transmission from 192.168.20.0/24 subnet only.

Solution:

Configure access control list for filtering by a subnet:

```
esr# configure
esr(config)# ip access-list extended white
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address 192.168.20.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
```

Apply access list to Gi1/0/19 interface for inbound traffic:

```
esr(config)# interface gigabitethernet 1/0/19
esr(config-if-gi)# service-acl input white
```

To view the detailed information on access control list, use the following command:

```
esr# show ip access-list white
```

7.16 Static routes configuration

Static routing is a type of routing in which routes are defined explicitly during the router configuration without dynamic routing protocols.

7.16.1 Configuration process

You can add a static route by using the following command in global configuration mode:

```
esr(config)# ip route [ vrf <VRF> ] <SUBNET> { <NEXTHOP> | interface <IF> | tunnel
<TUN> | wan load-balance rule <RULE> [<METRIC>] | blackhole | unreachable |
prohibit } [ <METRIC> ] [ track <TRACK-ID> ] [ bfd ]
```

- <VRF> – VRF name, set by the string of up to 31 characters.
- <SUBNET> – destination address, can be specified in the following format:
 - AAA.BBB.CCC.DDD – host IP address, where each part takes values of [0..255].
 - AAA.BBB.CCC.DDD/NN – network IP address with prefix mask, where AAA-
DDD take values of [0..255] and NN takes values of [1..32].
- <NEXTHOP> – gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255];
- <IF> – IP interface name, specified in the form which is described in Section 3.3;
- <TUN> – tunnel name, specified in the form which is described in Section 4.3;
- <RULE> – wan rule number, set in the range of [1..50];
- blackhole – when specifying the command, the packets to this subnet will be removed by the device without sending notifications to a sender;
- unreachable – when specifying the command, the packets to this subnet will be removed by the device, a sender will receive in response ICMP Destination unreachable (Host unreachable, code 1);
- prohibit – when specifying the command, the packets to this subnet will be removed by the device, a sender will receive in response ICMP Destination unreachable (Communication administratively prohibited, code 13);
- bfd – when specifying the given key, the removal of static route in case of next-hop unavailability is activated.

To add static IPv6 route to the given subnet, use the following command:

```
ipv6 route [ vrf <VRF> ] <SUBNET> { <NEXTHOP> [ resolve ] | interface <IF> | wan
load-balance rule <RULE> | blackhole | unreachable | prohibit } [ <METRIC> ]
[ bfd ]
```

- <VRF> – VRF name, set by the string of up to 31 characters.
- <SUBNET> – destination address, can be specified in the following formats:
 - The addresses are defined as X:X:X::X where each part takes values in hexadecimal format [0..FFFF].
 - <IPV6-ADDR/LEN> – IP address and mask of a subnet, defined as X:X:X::X/EE where each X part takes values in hexadecimal format [0..FFFF] and EE takes values of [1..128].
- <IPV6-ADDR> – client IPv6 address, defined as X:X:X::X where each part takes values in hexadecimal format [0..FFFF];
- resolve – when specifying the given parameter, gateway IPv6 address will be recursively calculated through the routing table. If the recursive calculation fails to find a gateway from a directly connected subnet, then this route will not be installed into the system;
- <IF> – IP interface name, specified in the form which is described in Section 3.3;
- blackhole – when specifying the command, the packets to this subnet will be removed by the device without sending notifications to a sender;
- unreachable – when specifying the command, the packets to this subnet will be removed by the device, a sender will receive in response ICMP Destination unreachable (Host unreachable, code 1);
- prohibit – when specifying the command, the packets to this subnet will be removed by the device, a sender will receive in response ICMP Destination unreachable (Communication administratively prohibited, code 13);
- <METRIC> – route metric, takes values of [0..255].
- bfd – when specifying the given key, the removal of static route in case of next-hop unavailability is activated.

7.16.2 Static routes configuration example

Objective:

Configure Internet access for users in LAN 192.168.1.0/24 and 10.0.0.0/8 using the static routing. On R1 device, create gateway for Internet access. Traffic within LAN should be routed within LAN zone, traffic from the Internet should belong to WAN zone.

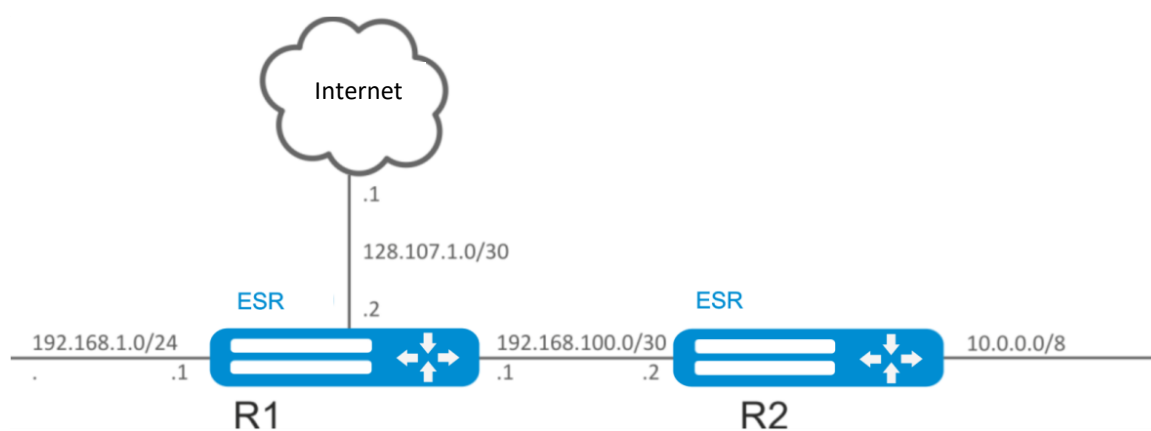


Figure 51 – Network structure

Solution:

Specify the device name for R1 router:

```
esr# hostname R1
```

Specify 192.168.1.1/24 address and the “LAN” zone for the gi1/0/1 interface. R1 interface will be connected to 192.168.1.0/24 network via this interface:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.1.1/24
esr(config-if-gi)# exit
```

Specify 192.168.100.1/30 address and the “LAN” zone for the gi1/0/2 interface. R1 will be connected to R2 device via the given interface for the further traffic routing:

```
esr(config)# interface gi1/0/2
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.100.1/30
esr(config-if-gi)# exit
```

Specify 128.107.1.2/30 address and the “WAN” zone for the gi1/0/3 interface. R1 interface will be connected to the Internet via this interface:

```
esr(config)# interface gi1/0/3
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# ip address 128.107.1.2/30
esr(config-if-gi)# exit
```

Create a route for interaction with 10.0.0.0/8 network using R2 device as a gateway (192.168.100.2):

```
esr(config)# ip route 10.0.0.0/8 192.168.100.2
```

Create a route for interaction with the Internet using the provider gateway as a nexthop (128.107.1.1):

```
esr(config)# ip route 0.0.0.0/0 128.107.1.1
```

Specify the device name for R2 router:

```
esr# hostname R2
```

Specify 10.0.0.1/8 address and the “LAN” zone for the gi1/0/1 interface. R2 interface will be connected to 10.0.0.0/8 network via this interface:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 10.0.0.1/8
esr(config-if-gi)# exit
```

Specify 192.168.100.2/30 address and the “LAN” zone for the gi1/0/2 interface. R2 will be connected to R1 device via the given interface for the further traffic routing:

```
esr(config)# interface gi1/0/2
```



```
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.100.2/30
esr(config-if-gi)# exit
```

Create a default route by specifying the IP address of R1 router gi1/0/2 interface (192.168.100.1) as a nexthop:

```
esr(config)# ip route 0.0.0.0/0 192.168.100.1
```

You can use the following command to check the routing table:

```
esr# show ip route
```

7.17 MLPPP Configuration

Multilink PPP (MLPPP) is an aggregated channel that encompasses methods of traffic transition via multiple physical channels while having a single logical connection. This option allows to enhance bandwidth and enables load balancing.



Figure 52 – Network structure

7.17.1 Configuration algorithm

Step	Description	Command	Keys
1	Configure aggregation group.	<code>esr(config)# interface multilink <IF></code>	<IF> – interface name.
2	Specify the description of configured aggregation group (optionally).	<code>esr(config-multilink)# description <DESCRIPTION></code>	<DESCRIPTION> – aggregation group description, set by the string of up to 255 characters.
3	Specify the time interval during which the statistics on the aggregation group load is averaged (optionally).	<code>esr(config-multilink)# load-average <TIME></code>	<TIME> – interval in seconds, takes values of [5..150]. Default value: 5.
4	Specify MTU (Maximum Transmission Unit) size for the aggregation group (optionally). MTU above 1500 will be active only when using the "system jumbo-frames" command.	<code>esr(config-multilink)# mtu <MTU></code>	<MTU> – MTU value, takes values in the range of [1280..1500]. Default value: 1500.
6	Enable CHAP authentication.	<code>esr(config-multilink)# ppp authentication chap</code>	
7	Enable authentication override (optionally).	<code>esr(config-multilink)# ppp chap refuse</code>	

8	Specify the router name that is sent to a remote party for CHAP authentication.	<code>esr(config-multilink)# ppp chap hostname <NAME></code>	<NAME> – router name, set by the string of up to 31 characters.
9	Specify the password that is sent with the router name to a remote party for CHAP authentication.	<code>esr(config-multilink)# ppp chap password ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }</code>	<CLEAR-TEXT> – unencrypted password, set by the string of [8..64] characters, may include [0-9a-fA-F] characters. <ENCRYPTED-TEXT> – unencrypted password, set by the string of [16..128] characters.
10	Allow any non-null IP address to be accepted as a local IP address from the neighbour (optionally).	<code>esr(config-multilink)# ppp ipcp accept-address</code>	
11	Set IP address that is sent to a remote party for the further allocation.	<code>esr(config-multilink)# ppp iccp remote-address <ADDR></code>	<ADDR> – IP address of a remote gateway.
12	Specify a user for remote party authentication and switch to the specified user configuration mode	<code>esr(config-multilink)# chap username <NAME></code>	<NAME> – user name, set by the string of up to 31 characters.
13	Set encrypted or unencrypted password for a specific user to authenticate the remote party.	<code>esr(config-ppp-user)# password ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }</code>	<CLEAR-TEXT> – unencrypted password, set by the string of [8..64] characters, may include [0-9a-fA-F] characters. <ENCRYPTED-TEXT> – unencrypted password, set by the string of [16..128] characters.
14	Set the amount of attempts to send Configure-Request packets before the remote peer is found to be unable to respond (optionally).	<code>esr(config-multilink)# ppp max-configure <VALUE></code>	<VALUE> – time in seconds, takes values of [1..255]. Default value: 10.
15	Set the amount of attempts to send Configure-NAK packets before all options are confirmed (optionally).	<code>esr(config-multilink)# ppp max-failure <VALUE></code>	<VALUE> – time in seconds, takes values of [1..255].
16	Set the amount of attempts to send Terminate-Request packets before the session is aborted (optionally).	<code>esr(config-multilink)# ppp max-terminate <VALUE></code>	<VALUE> – time in seconds, takes values of [1..255]. Default value: 2.
17	Set MRU (Maximum Receive Unit) size for the interface.	<code>esr(config-multilink)# ppp mru <MRU></code>	<MRU> – MRU value, takes values in the range of [128..1485]. Default value: 1500.
18	Specify the time interval in seconds after which the router sends a keepalive message (optionally).	<code>esr(config-multilink)# ppp timeout keepalive <TIME></code>	<TIME> – time in seconds, takes values of [1..32767]. Default value: 10.
19	Specify the time interval in seconds after which the router sends a keepalive message (optionally).	<code>esr(config-multilink)# ppp timeout retry <TIME></code>	<TIME> – time in seconds, takes values of [1..255]. Default value: 3.
20	Specify the maximum packet size for MLPP interface.	<code>esr(config-multilink)# mrru <MRRU></code>	<MRRU> – maximum size of a received packet for MLPP interface, takes value in the range of [1500..10000].

21	Bind e1 port to the physical interface.	<code>esr(config-if-gi)# switchport e1 <SLOT></code>	<SLOT> – slot identifier, takes values in the range of [0..3].
22	Put the physical port into SFPe1 module operation mode.	<code>esr(config-if-gi)# switchport mode e1</code>	
23	Enable MLPPP mode on E1 interface.	<code>esr(config-e1)# ppp multilink</code>	
24	Include E1 interface in the aggregation group.	<code>esr(config-e1)# ppp multilink-group <GROUP-ID></code>	<GROUP-ID> – group identifier, takes values in the range of [1..4].

7.17.2 Configuration example

Objective:

Configure MLPPP connection to the opposite side with IP address 10.77.0.1/24 via MXE device.



Figure 53 – Network structure

Solution:

Switch gigabitethernet 1/0/10 interface into E1 operation mode:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/10
esr(config-if-gi)# description "*** MXE ***"
esr(config-if-gi)# switchport mode e1
esr(config-if-gi)# switchport e1 slot 0
esr(config-if-gi)# exit
```

Configure MLPPP 3:

```
esr(config)# interface multilink 3
esr(config-multilink)# ip address 10.77.0.2/24
esr(config-multilink)# security-zone trusted
esr(config-multilink)# exit
esr(config)# exit
```

Enable interface e1 1/0/1, interface e1 1/0/4 into MLPPP 3 aggregation group:

```
esr(config)# interface e1 1/0/1
esr(config-e1)# ppp multilink
esr(config-e1)# ppp multilink-group 3
esr(config-e1)# exit
esr(config)# interface e1 1/0/4
esr(config-e1)# ppp multilink
esr(config-e1)# ppp multilink-group 3
esr(config-e1)# exit
```

7.18 Bridge configuration

Bridge is a method of connection for two Ethernet segments on data-link level without any higher level protocols, such as IP. Packet transmission is based on Ethernet addresses, not on IP addresses. Given that the transmission is performed on data-link level (Level 2 of the OSI model), higher level protocol traffic passes through the bridge transparently.

7.18.1 Configuration algorithm

Step	Description	Command	Keys
1	Add a network bridge to the system and switch to its configuration mode.	<code>esr (config) # bridge <BRIDGE-ID></code>	<BRIDGE-ID> – bridge identification number, takes values in the range of: for esr10/12V(F)/14VF – [1..50]; for esr100/200 – [1..250]; for esr1000/1200 – [1..500].
2	Enable network bridge.	<code>esr (config-bridge) # enable</code>	
3	Specify VRF instance, in which the given modem will operate (optionally).	<code>esr (config-bridge) # ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.
4	Specify the configured network bridge description (optionally).	<code>esr (config-bridge) # description <DESCRIPTION></code>	<DESCRIPTION> – network bridge description, set by the string of up to 255 characters.
5	Specify the size of MTU packets that can be passed by the bridge (optionally; possible if only VLAN is included in the bridge). MTU above 1500 will be active only when using the "system jumbo-frames" command.	<code>esr (config-bridge) # mtu <MTU></code>	<MTU> – MTU value, takes values in the range of: for esr10/12V(F)/14VF – [552..9600] for esr-100/200/1000/1200/1700 – [552..10000].
6	Specify the time interval during which the statistics on the bridge load is averaged (optionally).	<code>esr (config-bridge) # load-average <TIME></code>	<TIME> – interval in seconds, takes values of [5..150]. Default value: 5
7	Connect the current network bridge with VLAN. All interfaces and L2 tunnels that are members of the assigned VLAN are automatically included in the network bridge and become members of the shared L2 domain (optionally)	<code>esr (config-bridge) # vlan <VID></code>	<VID> – VLAN identifier, set in the range of [1..4094].
8	Specify the network bridge MAC address different from a system one (optionally).	<code>esr (config-bridge) # mac-address <ADDR></code>	<ADDR> – network bridge MAC address, defined as XX:XX:XX:XX:XX:XX where each part takes the values of [00..FF].
9	Connect sub interface, qinq interface, L2GRE tunnel or L2TPv3 tunnel with the network bridge. Connected interfaces/tunnels and network bridges automatically become participants of the shared L2 domain (optionally).	<code>esr (config-if-gi) # bridge-group <BRIDGE-ID></code> <code>esr (config-if-l2tpv3) # bridge-group <BRIDGE-ID></code>	<BRIDGE-ID> – bridge identification number, takes values in the range of: for esr10/12V(F)/12VF – [1..50]; for esr100/200 – [1..250]; for esr1000/1200 – [1..500].

10	Enable interface isolation mode on the bridge. In this mode, the traffic exchange between members of the network bridge is prohibited. (Optionally; relevant only for ESR-1000/1200/1700)	<code>esr(config-bridge)# protected-ports [exclude vlan]</code>	exclude vlan – when specifying the given key, VLAN (connected with bridge) is excluded from the isolated interfaces list.
11	Prohibit unknown-unicast traffic switching (when a destination MAC address is not included in the switching table) in the given bridge. (optionally; relevant only for ESR-1000/1200/1700)	<code>esr(config-bridge)# unknown-unicast- forwarding disable</code>	
12	Set the lifetime of IPv4/IPv6 entries in the ARP table studied on the given bridge (optionally).	<code>esr(config- bridge)# ip arp reachable-time <TIME> or ipv6 nd reachable- time <TIME></code>	<TIME> – lifetime of dynamic MAC addresses, in milliseconds. Allowed values are from 5000 to 100000000 milliseconds. Real time of the entry update varies from [0,5;1,5]*<TIME>.

7.18.2 Example of bridge configuration for VLAN and L2TPv3 tunnel

Objective:

Combine router interfaces related to LAN and L2TPv3 tunnel passing through the public network into a single L2 domain. For combining, use VLAN 333.

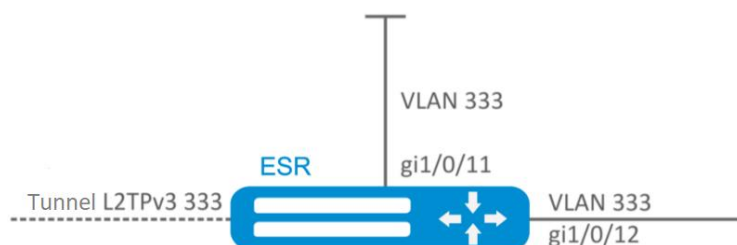


Figure 54 – Network structure

Solution:

Create VLAN 333:

```
esr(config)# vlan 333
esr(config-vlan)# exit
```

Create 'trusted' security zone:

```
esr(config)# security-zone trusted
esr(config-zone)# exit
```

Add gi1/0/11, gi1/0/12 interfaces to VLAN 333:

```
esr(config)# interface gigabitethernet 1/0/11-12
```

```
esr(config-if) # switchport general allowed vlan add 333 tagged
```

Create bridge 333, map VLAN 333 to it and specify membership in 'trusted' zone:

```
esr(config) # bridge 333
esr(config-bridge) # vlan 333
esr(config-bridge) # security-zone trusted
esr(config-bridge) # enable
```

Specify the inheritance of L2TPv3 tunnel to bridge mapped to LAN (for L2TPv3 tunnel configuration, see Section 7.25). In general, bridge and tunnel identifiers should not match the VID, unlike this example.

```
esr(config) # tunnel l2tpv3 333
esr(config-l2tpv3) # bridge-group 333
```

7.18.3 Example of bridge configuration for VLAN

Objective:

Configure routing between VLAN 50 (10.0.50.0/24) and VLAN 60 (10.0.60.0/24). VLAN 50 should belong to 'LAN1', VLAN 60 – to 'LAN2', enable free traffic transmission between zones.

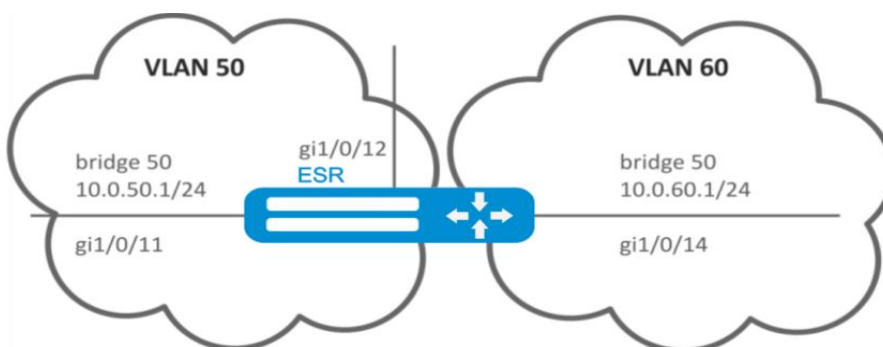


Figure 55 – Network structure

Solution:

Create VLAN 50, 60:

```
esr(config) # vlan 50.60
esr(config-vlan) # exit
```

Create 'LAN1' and 'LAN2' security zones:

```
esr(config) # security-zone LAN1
esr(config-zone) # exit
esr(config) # security-zone LAN2
esr(config-zone) # exit
```

Map VLAN 50 to gi1/0/11, gi1/0/12 interfaces:

```
esr(config) # interface gigabitethernet 1/0/11-12
esr(config-if-gi) # switchport general allowed vlan add 50 tagged
```

Map VLAN 60 to gi1/0/14 interface:

```
esr(config)# interface gigabitethernet 1/0/14
esr(config-if-gi)# switchport general allowed vlan add 60 tagged
```

Create bridge 50, map VLAN 50, define IP address 10.0.50.1/24 and membership in 'LAN1' zone:

```
esr(config)# bridge 50
esr(config-bridge)# vlan 50
esr(config-bridge)# ip address 10.0.50.1/24
esr(config-bridge)# security-zone LAN1
esr(config-bridge)# enable
```

Create bridge 60, map VLAN 60, define IP address 10.0.60.1/24 and membership in 'LAN2' zone:

```
esr(config)# bridge 60
esr(config-bridge)# vlan 60
esr(config-bridge)# ip address 10.0.60.1/24
esr(config-bridge)# security-zone LAN2
esr(config-bridge)# enable
```

Create firewall rules that enable free traffic transmission between zones:

```
esr(config)# security zone-pair LAN1 LAN2
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair LAN2 LAN1
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# exit
```

To view an interface membership in a bridge, use the following command:

```
esr# show interfaces bridge
```

7.18.4 Configuration example of the second VLAN tag adding/removing

Objective:

The gigabitethernet 1/0/1 interface receives Ethernet frames with various VLAN tags. It is necessary to redirect them to the gigabitethernet 1/0/2 interface, adding the second VLAN-ID 828. When Ethernet frames with VLAN-ID 828 come on the gigabitethernet 1/0/2, this tag must be removed and sent to the gigabitethernet 1/0/1 interface.

Solution:

Create the bridge without VLAN and IP address on the route.

```
esr(config)# bridge 1
esr(config-bridge)# enable
esr(config-bridge)# exit
```

Include the gigabitethernet 1/0/1 interface in bridge 1.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# bridge-group 1
esr(config-if-gi)# exit
```

Include the gigabitethernet 1/0/2.828 sub interface in bridge 1.

```
esr(config)# interface gigabitethernet 1/0/2.828
esr(config-subif)# bridge-group 1
esr(config-subif)# exit
```



When adding the second VLAN tag to an Ethernet frame, its size is increased by 4 bytes. MTU must be increased by 4 bytes or more on the gigabitethernet 1/0/2 router interface and on all equipment transmitting q-in-q-frames.

7.19 RIP Configuration

RIP is a distance-vector dynamic routing protocol that uses hop count as a routing metric. The maximum amount of hops allowed for RIP is 15. By default, each RIP router transmits full routing table into the network every 30 seconds. RIP operates at 3rd level of TCP/IP stack via UDP port 520.

7.19.1 Configuration algorithm

Step	Description	Command	Keys
1	Configure RIP precedence for the main routing table (optionally).	<code>esr(config)# ip protocols rip preference <VALUE></code>	<VALUE> – protocol precedence, takes values in the range of [1..255]. Default value: RIP (100).
2	Configure RIP routing tables' capacity (optionally).	<code>esr(config)# ip protocols rip max-routes <VALUE></code>	<VALUE> – amount of RIP routes in the routing table, takes values in the range of: for esr-100/200/1000/1200/1700 - [1..10000]; for esr-10/12V(F)/14VF - [1..1000]. Default value: for esr-100/200/1000/1200/1700 - (10000), for esr-10/12V(F)/14VF - (1000).
3	Create IP subnets lists that will be used for further filtration of advertised and received IP routes.	<code>esr(config)# ip prefix-list <NAME></code>	<NAME> – name of a subnet list being configured, set by the string of up to 31 characters.
4	Permit or deny the prefixes lists.	<code>esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route}</code>	<OBJ-GROUP-NETWORK-NAME> – IP addresses profile name, set by the string of up to 31 characters; <LEN> – prefix length, takes values of [1..32] in prefix IP lists;

		<pre>esr(config-pl)# deny {object-group <OBJ- GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route}</pre>	<p>eq – when specifying the command, the prefix length must match the specified one;</p> <p>le – when specifying the command, the prefix length must be less than or match the specified one;</p> <p>ge – when specifying the command, the prefix length must be more than or match the specified one;</p> <p>default-route – default route filtration.</p>
5	Switch to the RIP process configuration mode.	<pre>esr(config)# router rip esr(config-rip)#</pre>	
6	Enable RIP.	<pre>esr(config-rip)# enable</pre>	
7	Specify RIP authentication algorithm (optionally).	<pre>esr(config-rip)# authentication algorithm { cleartext md5 }</pre>	<p>cleartext – unencrypted password;</p> <p>md5 – password is hashed by md5 algorithm.</p>
8	Set the password for neighbour authentication (optionally).	<pre>esr(config-rip)# authentication key ascii-text { <CLEAR- TEXT> encrypted <ENCRYPTED-TEXT> }</pre>	<p><CLEAR-TEXT> – password, set by the string of 8 to 16 characters;</p> <p><ENCRYPTED-TEXT> – encrypted password of 8 to 16 bytes (from 16 to 32 characters) in hexadecimal format (0xYYYY ...) or (YYYY ...).</p>
9	Specify the list of passwords for authentication via md5 hashing algorithm (optionally).	<pre>esr(config-rip)# authentication key- chain <KEYCHAIN></pre>	<p><KEYCHAIN> – key list identifier, set by the string of up to 16 characters.</p>
10	Disable routes advertising on the interfaces/tunnels/bridge where it is not necessary (optionally).	<pre>esr(config-rip)# passive-interface {<IF> <TUN> }</pre>	<p><IF> – interface and identifier;</p> <p><TUN> – tunnel name and number.</p>
11	Set time interval after which the advertising is carried out (optionally).	<pre>esr(config-rip)# timers update <TIME></pre>	<p><TIME> – time in seconds, takes values of [1..65535].</p> <p>Default value: 180 seconds.</p>
12	Set time interval of route entry correctness without updating (optionally).	<pre>esr(config-rip)# timers invalid <TIME></pre>	<p><TIME> – time in seconds, takes values of [1..65535].</p> <p>Default value: 180 seconds.</p>
13	Set time interval after which the route removing is carried out (optionally).	<pre>esr(config-rip)# timers flush <TIME></pre>	<p><TIME> – time in seconds, takes values of [1..65535].</p> <p>When setting the value, consider the following rule: «timersinvalid + 60»</p> <p>Default value: 240 seconds.</p>
14	Enable subnets advertising.	<pre>esr(config-rip)# network <ADDR/LEN></pre>	<p><ADDR/LEN> – subnet address, set in the following format:</p> <p>AAA.BBB.CCC.DDD/NN – network IP address with prefix mask, where AAA-DDD take values of [0..255] and NN takes values of [1..32].</p>
15	Add subnets filtration in incoming or outgoing updates (optionally).	<pre>esr(config-rip)# prefix-list <PREFIX- LIST-NAME> { in out }</pre>	<p><PREFIX-LIST-NAME> – name of a subnet list being configured, set by the string of up to 31 characters.</p> <p>in – incoming routes filtration;</p> <p>out – advertised routes filtration.</p>
16	Enable advertising of routes received in an alternative way (optionally).	<pre>esr(config-rip)# redistribute static [route-map <NAME>]</pre>	<p><NAME> – name of the route map that will be used for advertised static routes filtration and modification, set by the string of up to 31 characters.</p>

		<pre>esr(config-rip)# redistribute connected [route-map <NAME>]</pre>	<p><NAME> – name of the route map that will be used for filtration and modification of advertised directly connected subnets, set by the string of up to 31 characters.</p>
		<pre>esr(config-rip)# redistribute ospf <ID><ROUTE-TYPE> [route-map <NAME>]</pre>	<p><ID> – process number, takes values of [1..65535]. <ROUTE-TYPE> – route type: intra-area – OSPF process routes advertising within a zone; inter-area – OSPF process routes advertising between zones; external1 – OSPF format 1 external routes advertising; external2 – OSPF format 2 external routes advertising; <NAME> – name of the route map that will be used for advertised OSPF routes filtration and modification, set by the string of up to 31 characters.</p>
		<pre>esr(config-rip)# redistribute bgp <AS> [route-map <NAME>]</pre>	<p><AS> – stand alone system number, takes values of [1..4294967295]. <NAME> – name of the route map that will be used for advertised BGP routes filtration and modification, set by the string of up to 31 characters.</p>
17	Switch to the interface/tunnel/network bridge configuration mode.	<pre>esr(config)# interface <IF- TYPE><IF-NUM></pre>	<p><IF-TYPE> – interface type; <IF-NUM> - F/S/P – F frame (1), S – slot (0), P – port.</p>
		<pre>esr(config)# tunnel <TUN-TYPE><TUN-NUM></pre>	<p><TUN-TYPE> – tunnel type; <TUN-NUM> – tunnel number.</p>
		<pre>esr(config)# bridge <BR-NUM></pre>	<p><BR-NUM> – bridge number.</p>
18	Set RIP routes metric value on the interface (optionally).	<pre>esr(config-if-gi)# ip rip metric <VALUE></pre>	<p><VALUE> – metric size, takes values of [0..32767]. Default value: 5.</p>
19	Set the routes advertising mode via RIP (optionally).	<pre>esr(config-if-gi)# ip rip mode <MODE></pre>	<p><MODE> – routes advertising mode: multicast – routes are advertised in multicast mode; broadcast – routes are advertised in broadcast mode; unicast – routes are advertised to the neighbours in unicast mode; Default value: multicast.</p>
20	Specify a neighbour's IP address for establishment of a relation in routes advertising unicast mode (optionally).	<pre>esr(config-if-gi)# ip rip neighbor <ADDR></pre>	<p><ADDR> – IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].</p>
21	Enable subnet summarization (optionally).	<pre>esr(config-if-gi)# ip rip summary-address <ADDR/LEN></pre>	<p><ADDR/LEN> – IP address and subnet mask, defined as AAA.BBB.CCC.DDD/EE where each part AAA-DDD takes values of [0..255] and EE takes values of [1..32].</p>

7.19.2 RIP configuration example

Objective:

Configure RIP on the router in order to exchange the routing information with neighbouring routers. The router should advertise static routes and subnets 115.0.0.0/24, 14.0.0.0/24, 10.0.0.0/24. Routes should be advertised each 25 seconds.

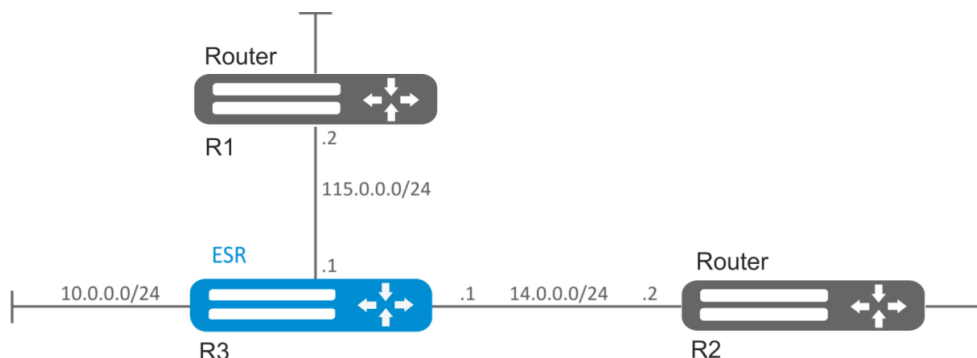


Figure 56 – Network structure

Solution:

Pre-configure IP addresses on interfaces according to the network structure shown in Figure 56.

Switch to the RIP configuration mode:

```
esr(config)# router rip
```

Define subnets that will be advertised by the protocol: 115.0.0.0/24, 14.0.0.0/24 and 10.0.0.0/24:

```
esr(config-rip)# network 115.0.0.0/24
esr(config-rip)# network 14.0.0.0/24
esr(config-rip)# network 10.0.0.0/24
```

To advertise static routes by the protocol, execute the following command:

```
esr(config-rip)# redistribute static
```

Configure timer, responsible for routing information transmission:

```
esr(config-rip)# timers update 25
```

When all required settings are done, enable the protocol:

```
esr(config-rip)# enable
```

To view the RIP routing table, use the following command:

```
esr# show ip rip
```



In addition to RIP protocol configuration, open UDP port 520 in the firewall.

7.20 OSPF configuration

OSPF is a dynamic routing protocol, based on link-state technology and using shortest path first Dijkstra algorithm.

7.20.1 Configuration algorithm

Step	Description	Command	Keys
1	Configure OSPF precedence for the main routing table (optionally).	<code>esr(config)# ip protocols ospf preference <VALUE></code>	<VALUE> – protocol precedence, takes values in the range of [1..255]. Default value: 150.
		<code>esr(config-vrf)# ip protocols ospf preference <VALUE></code>	
2	Configure OSPF routing tables' capacity (optionally).	<code>esr(config)# ip protocols ospf max-routes <VALUE></code>	<VALUE> – amount of OSPF routes in the routing table, takes values in the range of: for esr-1000/1200/1700 [1..500000]; for esr-100/200 [1..300000]; for esr-10/12V(F)/14VF [1..30000]. Default value for the global mode: for esr-1000/1200/1700 – (500000); for esr-100/200 – (300000); for esr-10/12V(F)/14VF – (30000). Default value for the global mode: 0
		<code>esr(config)# ipv6 protocols ospf max-routes <VALUE></code>	
3	Enable the output of OSPF neighbor state information (optionally).	<code>esr(config)# router ospf log-adjacency-changes</code>	
		<code>esr(config)# ipv6 router ospf log-adjacency-changes</code>	
4	Create IP subnets lists that will be used for further filtration of advertised and received IP routes.	<code>esr(config)# ip prefix-list <NAME></code>	<NAME> – name of a subnet list being configured, set by the string of up to 31 characters.
		<code>esr(config)# ipv6 prefix-list <NAME></code>	
5	Permit or deny the prefixes lists.	<code>esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route}</code>	<OBJ-GROUP-NETWORK-NAME> – IP addresses profile name, set by the string of up to 31 characters; <LEN> – prefix length, takes values of [1..32] in prefix IP lists; eq – when specifying the command, the prefix length must match the specified one; le – when specifying the command, the prefix length must be less than or match the specified one; ge – when specifying the command, the prefix length must be more than or match the specified one; default-route – default route filtration.
		<code>esr(config-pl)# deny {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route}</code>	
		<code>esr(config-ipv6-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-</code>	

		<pre>route} esr(config-ipv6-pl)# deny object-group <OBJ-GROUP-NETWORK- NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route}</pre>	
6	Add OSPF process to the system and switch to the OSPF process parameters configuration mode.	<pre>esr(config)# router ospf <ID> [vrf <VRF>] esr(config)# ipv6 router ospf <ID> [vrf <VRF>]</pre>	<p><ID> – stand alone system number, takes values of [1..65535].</p> <p><VRF> – VRF instance name, set by the string of up to 31 characters, within which the routing protocol will operate.</p>
7	Set the router identifier for the given OSPF process.	<pre>esr(config-ospf)# router-id <ID> esr(config-ipv6- ospf)# router-id <ID></pre>	<p><ID> – router identifier, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].</p>
8	Define OSPF process routes precedence.	<pre>esr(config-ospf)# preference <VALUE> esr(config-ipv6- ospf)# preference <VALUE></pre>	<p><VALUE> – OSPF process routes precedence, takes values in the range of [1..255].</p> <p>Default value: 10.</p>
9	Enable compatibility with RFC 1583 (optionally).	<pre>esr(config-ospf)# compatible rfc1583 esr(config-ipv6- ospf)# compatible rfc1583</pre>	
11	Add subnets filtration in incoming or outgoing updates (optionally).	<pre>esr(config-ospf)# prefix-list <PREFIX- LIST-NAME> { in out } esr(config-ipv6- ospf)# prefix-list <PREFIX-LIST-NAME> { in out }</pre>	<p><PREFIX-LIST-NAME> – name of a subnet list being configured, set by the string of up to 31 characters.</p> <p>in – incoming routes filtration; out – advertised routes filtration.</p>
12	Enable advertising of routes received in an alternative way (optionally).	<pre>esr(config-ospf)# redistribute static [route-map <NAME>] esr(config-ipv6- ospf)# redistribute static [route-map <NAME>] esr(config-ospf)# redistribute connected [route-map <NAME>] esr(config-ipv6- ospf)# redistribute connected [route-map <NAME>] esr(config-ospf)# redistribute rip [route-map <NAME>] esr(config-ospf)# redistribute bgp <AS> [route-map <NAME>] esr(config-ipv6- ospf)# redistribute bgp <AS> [route-map <NAME>]</pre>	<p><NAME> – name of the route map that will be used for advertised static routes filtration and modification, set by the string of up to 31 characters.</p> <p><NAME> – name of the route map that will be used for filtration and modification of advertised directly connected subnets, set by the string of up to 31 characters.</p> <p><NAME> – name of the route map that will be used for advertised RIP routes filtration and modification, set by the string of up to 31 characters.</p> <p><AS> – stand alone system number, takes values of [1..4294967295].</p> <p><NAME> – name of the route map that will be used for advertised BGP routes filtration and modification, set by the string of up to 31 characters.</p>
13	Enable OSPF process.	<pre>esr(config-ospf)# enable esr(config-ipv6- ospf)# enable</pre>	
14		<pre>esr(config-ospf)# area <AREA_ID></pre>	

	Create OSPF area and switch to the scope configuration mode.	<code>esr(config-ipv6-ospf)# area <AREA_ID></code>	<AREA_ID> – area identifier, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
15	Enable subnets advertising.	<code>esr(config-ospf-area)# network <ADDR/LEN></code>	<ADDR/LEN> – subnet address, set in the following format: AAA.BBB.CCC.DDD/NN – network IP address with prefix mask, where AAA-DDD take values of [0..255] and NN takes values of [1..32].
		<code>esr(config-ipv6-ospf-area)# network <IPV6-ADDR/LEN></code>	<IPV6-ADDR/LEN> – IPv6 address and mask of a subnet, defined as X:X:X::X/EE where each X part takes values in hexadecimal format [0..FFFF] and EE takes values of [1..128].
16	Specify the area type	<code>esr(config-ospf-area)# area-type <TYPE> [no-summary]</code>	<TYPE> – area type: stub – set the stub value (stub area); no-summary – command in conjunction with the “stub” parameter forms the “totallystubby” area (only the default route is used to transfer information outside the area).
		<code>esr(config-ipv6-ospf-area)# area-type <TYPE> [no-summary]</code>	nssa – set the nssa value (NSSA area); no-summary – command in conjunction with the “nssa” parameter forms the “totallynssa” area (by default the route is generated as an inter-place one).
17	Enable the default route generation for NSSA area and its advertising as NSSA-LSA.	<code>esr(config-ospf-area)# default-information-originate</code>	
		<code>esr(config-ipv6-ospf-area)# default-information-originate</code>	
18	Enable the subnet summarization or hiding.	<code>esr(config-ospf-area)# summary-address <ADDR/LEN> { advertise not-advertise }</code>	<ADDR/LEN> – IP address and subnet mask, defined as AAA.BBB.CCC.DDD/EE where each part AAA-DDD takes values of [0..255] and EE takes values of [1..32]; advertise – when specifying the command, a total subnet will be advertised instead of subnets specified; not-advertise – when specifying the command, the subnets included in a subnet specified will not be advertised.
		<code>esr(config-ipv6-ospf-area)# summary-address <IPV6-ADDR/LEN> { advertise not-advertise }</code>	<IPV6-ADDR/LEN> – IPv6 address and mask of a subnet, defined as X:X:X::X/EE where each X part takes values in hexadecimal format [0..FFFF] and EE takes values of [1..128]; advertise – when specifying the command instead of the subnets included in a subnet specified, a total subnet will be advertised; not-advertise – the subnets included in a subnet specified will not be advertised.
19	Enable OSPF area.	<code>esr(config-ospf-area)# enable</code>	
		<code>esr(config-ipv6-ospf-area)# enable</code>	
20	Establish a virtual connection between the	<code>esr(config-ospf-area)# virtual-link <ID></code>	<ID> – identifier of the router with which the virtual connection is established,

	main and remote areas having several areas between them.	<code>esr(config-ipv6-ospf-area)# virtual-link <ID></code>	defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
21	Set the time interval in seconds after which the router re-sends a packet that has not received a delivery confirmation (for example, a DatabaseDescription packet or LinkStateRequest packets).	<code>esr(config-ospf-vlink)# retransmit-interval <TIME></code>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 5 seconds.
		<code>esr(config-ipv6-ospf-vlink)# retransmit-interval <TIME></code>	
22	Set the time interval in seconds after which the router sends the next hello packet.	<code>esr(config-ospf-vlink)# hello-interval <TIME></code>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 10 seconds.
		<code>esr(config-ipv6-ospf-vlink)# hello-interval <TIME></code>	
23	Set the time interval in seconds after which the neighbor is considered to be idle. This interval should be a multiple of the 'hello interval' value.	<code>esr(config-ospf-vlink)# dead-interval <TIME></code>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 40 seconds.
		<code>esr(config-ipv6-ospf-vlink)# dead-interval <TIME></code>	
24	Set the time interval in seconds after which the router selects DR in the network.	<code>esr(config-ospf-vlink)# wait-interval <TIME></code>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 40 seconds
		<code>esr(config-ipv6-ospf-vlink)# wait-interval <TIME></code>	
25	Define authentication algorithm.	<code>esr(config-ospf-vlink)# authentication algorithm <ALGORITHM></code>	<ALGORITHM> – authentication algorithm: cleartext – password, transmitted in unencrypted form (available only for RIP and OSPF-VLINK); md5 – password is hashed by md5 algorithm.
26	Set the password for neighbour authentication.	<code>esr(config-ospf-vlink)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }</code>	<CLEAR-TEXT> – password, set by the string of 8 to 16 characters; <ENCRYPTED-TEXT> – encrypted password of 8 to 16 bytes (from 16 to 32 characters) in hexadecimal format (0xYYYY ...) or (YYYY ...).
27	Specify the list of passwords for authentication via md5 hashing algorithm.	<code>esr(config-ospf-vlink)# authentication key chain <KEYCHAIN></code>	<KEYCHAIN> – key list identifier, set by the string of up to 16 characters.
28	Enable virtual connection.	<code>esr(config-ospf-vlink)# enable</code>	
29	Switch to the interface/tunnel/network bridge configuration mode.	<code>esr(config)# interface <IF-TYPE><IF-NUM></code>	<IF-TYPE> – interface type; <IF-NUM> - F/S/P – F frame (1), S – slot (0), P – port.
		<code>esr(config)# tunnel <TUN-TYPE><TUN-NUM></code>	<TUN-TYPE> – tunnel type; <TUN-NUM> – tunnel number.
		<code>esr(config)# bridge <BR-NUM></code>	<BR-NUM> – bridge number.
30	Define the interface / tunnel / network bridge inheritance to a specific OSPF process.	<code>esr(config-if-gi)# ip ospf instance <ID></code>	<ID> – process number, takes values of [1..65535].
		<code>esr(config-if-gi)# ipv6 ospf instance <ID></code>	

31	Define the interface inheritance to a specific OSPF process area.	<pre>esr(config-if-gi)# ip ospf area <AREA_ID></pre> <pre>esr(config-if-gi)# ipv6 ospf area <AREA_ID></pre>	<AREA_ID> – area identifier, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
32	Enable the routing via OSPF on the interface.	<pre>esr(config-if-gi)# ip ospf</pre> <pre>esr(config-if-gi)# ipv6 ospf</pre>	
33	Enable the mode in which the OSPF process will ignore MTU interface value in incoming Database Description packets.	<pre>esr(config-if-gi)# ip ospf mtu-ignore</pre> <pre>esr(config-if-gi)# ipv6 ospf mtu-ignore</pre>	
34	Specify OSPF authentication algorithm.	<pre>esr(config-if-gi)# ip ospf authentication algorithm <ALGORITHM></pre>	<ALGORITHM> – authentication algorithm: cleartext – unencrypted password; md5 – password is hashed by md5 algorithm.
35	Set the password for OSPF neighbor authentication when transmitting an unencrypted password.	<pre>esr(config-if-gi)# ip ospf authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED- TEXT> }</pre>	<CLEAR-TEXT> – password, set by the string of 8 to 16 characters; <ENCRYPTED-TEXT> – encrypted password of 8 to 16 bytes (from 16 to 32 characters) in hexadecimal format (0xYYYY ...) or (YYYY ...).
36	Specify the list of passwords for neighbor authentication via md5 hashing algorithm.	<pre>esr(config-if-gi)# ip ospf authentication key-chain <KEYCHAIN></pre>	<KEYCHAIN> – key list identifier, set by the string of up to 16 characters.
37	Set the time interval in seconds after which the router selects DR in the network.	<pre>esr(config-if-gi)# ip ospf wait-interval <TIME></pre> <pre>esr(config-if-gi)# ipv6 ospf wait- interval <TIME></pre>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 40 seconds.
38	Set the time interval in seconds after which the router re-sends a packet that has not received a delivery confirmation (for example, a DatabaseDescription packet or LinkStateRequest packets).	<pre>esr(config-if-gi)# ip ospf retransmit- interval <TIME></pre> <pre>esr(config-if-gi)# ipv6 ospf retransmit-interval <TIME></pre>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 5 seconds.
39	Set the time interval in seconds after which the router sends the next hello packet.	<pre>esr(config-if-gi)# ip ospf hello-interval <TIME></pre> <pre>esr(config-if-gi)# ipv6 ospf hello- interval <TIME></pre>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 10 seconds.
40	Set the time interval in seconds after which the neighbor is considered to be idle. This interval should be a multiple of the 'hello interval' value.	<pre>esr(config-if-gi)# ip dead-interval <TIME></pre> <pre>esr(config-if-gi)# ipv6 dead-interval <TIME></pre>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 40 seconds.
41	Set the time interval during which NBMA interface waits before sending a HELLO packet to a neighbor, even if the neighbor is idle.	<pre>esr(config-if-gi)# ip poll-interval <TIME></pre> <pre>esr(config-if-gi)# ipv6 poll-interval <TIME></pre>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 120 seconds.

42	Set static IP address of a neighbor to establish a relation in NMBA and P2MP (Point-to-MultiPoint) networks.	<pre>esr(config-if-gi)# ip ospf neighbor <IP> [eligible]</pre>	<p><IP> – neighbor’s IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].</p> <p>eligible – optional parameter, allows the device to take part in DR selection process in NMBA networks. The interface priority should be greater than zero.</p>
		<pre>esr(config-if-gi)# ip ospf neighbor <IP> [eligible]</pre>	<p><IPV6-ADDR> – neighbor’s IPv6 address, defined as X:X:X::X where each part takes values in hexadecimal format [0..FFFF];</p> <p>eligible – optional parameter, allows the device to take part in DR selection process in NMBA networks. The interface priority should be greater than zero.</p>
43	Define the network type for OSPF neighborhood establishment.	<pre>esr(config-if-gi)# ip ospf network <TYPE></pre>	<p><TYPE> – network type:</p> <p>broadcast – broadcast connection type;</p> <p>non-broadcast – NBMA connection type;</p> <p>point-to-multipoint – point-to-multipoint connection type;</p> <p>point-to-multipoint non-broadcast – point-to-multipoint NBMA connection type;</p> <p>point-to-point – point-to-point connection type.</p> <p>Default value: broadcast.</p>
		<pre>esr(config-if-gi)# ipv6 ospf network <TYPE></pre>	
44	Set the router priority that is used for DR and BDR selection.	<pre>esr(config-if-gi)# ip ospf priority <VALUE></pre>	<p><VALUE> – interface priority, takes values of [1..65535].</p> <p>Default value: 120.</p>
		<pre>esr(config-if-gi)# ipv6 ospf priority <VALUE></pre>	
45	Set the metric size on the interface or tunnel.	<pre>esr(config-if-gi)# ip ospf cost <VALUE></pre>	<p><VALUE> – metric size, takes values of [0..32767].</p> <p>Default value: 150.</p>
		<pre>esr(config-if-gi)# ipv6 ospf cost <VALUE></pre>	
47	Enable BFD protocol for OSPF protocol.	<pre>esr(config-if-gi)# ip ospf bfd-enable</pre>	
		<pre>esr(config-if-gi)# ipv6 ospf bfd-enable</pre>	

7.20.2 OSPF configuration example

Objective:

Configure OSPF protocol on the router in order to exchange the routing information with neighbouring routers. The router should be in 1.1.1.1 identifier area and announce routes received via RIP.

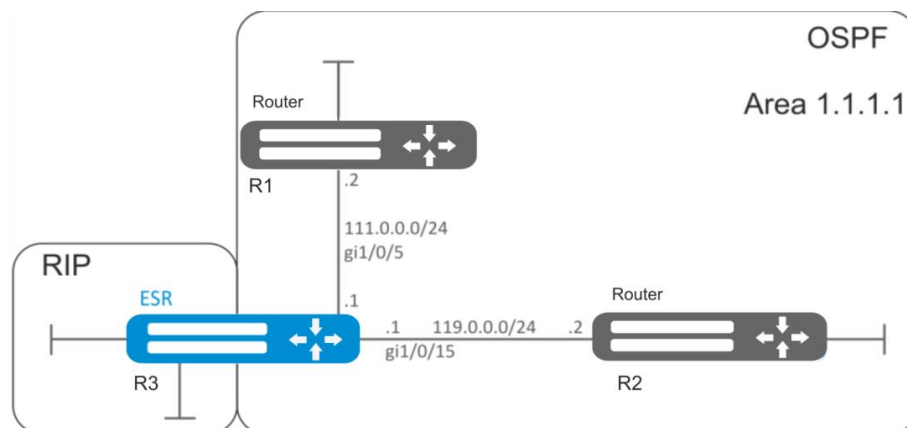


Figure 57 – Network structure

Solution:

Pre-configure IP addresses on interfaces according to the network structure shown in Figure 57.

Create OSPF process with identifier 10 and proceed to the OSPF protocol configuration mode:

```
esr(config)# router ospf 10
```

Create and enable the required area:

```
esr(config-ospf)# area 1.1.1.1
esr(config-ospf-area)# enable
esr(config-ospf-area)# exit
```

Enable advertising of the routing information from RIP:

```
esr(config-ospf)# redistribute rip
```

Enable OSPF process:

```
esr(config-ospf)# enable
esr(config-ospf)# exit
```

Neighbouring routers are connected to gi1/0/5 and gi1/0/15 interfaces. To establish the neighbouring with other routers, map them to OSPF process and the area. Next, enable OSPF routing for the interface.

```
esr(config)# interface gigabitethernet 1/0/5
esr(config-if-gi)# ip ospf instance 10
esr(config-if-gi)# ip ospf area 1.1.1.1
esr(config-if-gi)# ip ospf
esr(config-if-gi)# exit
```

```

esr(config)# interface gigabitethernet 1/0/15
esr(config-if-gi)# ip ospf instance 10
esr(config-if-gi)# ip ospf area 1.1.1.1
esr(config-if-gi)# ip ospf
esr(config-if-gi)# exit
esr(config)# exit

```

7.20.3 OSPF stub area configuration example

Objective:

Change 1.1.1.1 area type, area should be stub. Stub router should advertise routes received via RIP.

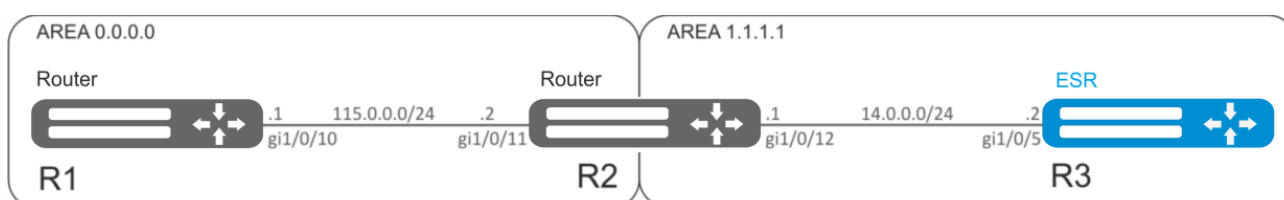


Figure 58 – Network structure

Solution:

Pre-configure OSPF protocol and IP addresses on interfaces according to the network structure shown in Figure 58.

Change area type to stub. For each router from 1.1.1.1 area, execute the following command in the configuration mode:

```

esr(config-ospf-area)# area-type stub

```

For R3 stub router, enable advertising of the routing information from RIP:

```

esr(config-ospf)# redistribute rip

```

7.20.4 Virtual link configuration example

Objective:

Merge two backbone areas using virtual link.

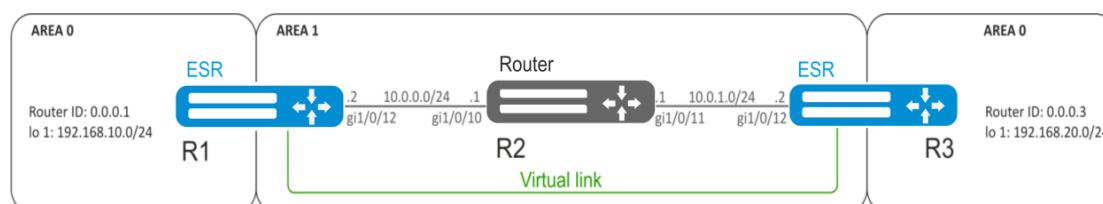


Figure 59 – Network structure

Solution:

Virtual link is a specialized connection that allows you to merge a split zone or connect a zone to the backbone zone through the third zone. Virtual link is configured between two Area Border Routers (ABR).

Pre-configure OSPF protocol and IP addresses on interfaces according to the network structure shown in Figure 59.

For R1 router, proceed to 1.1.1.1 area configuration mode:

```
esr(config-ospf) # area 1.1.1.1
```

Create and enable virtual link with the identifier 0.0.0.3:

```
esr(config-ospf-area) # virtual-link 0.0.0.3
esr(config-ospf-vlink) # enable
```

For R3 router, proceed to 1.1.1.1 area configuration mode:

```
esr(config-ospf) # area 1.1.1.1
```

Create and enable virtual link with the identifier 0.0.0.1:

```
esr(config-ospf-area) # virtual-link 0.0.0.1
esr(config-ospf-vlink) # enable
```

Review the routing table on R1 router:

```
esr# show ip route
```

C	* 10.0.0.0/24	[0/0]	dev gil/0/12,	[direct 00:49:34]
O	* 10.0.1.0/24	[150/20]	via 10.0.0.1 on gil/0/12,	[ospf1 00:49:53] (0.0.0.3)
O	* 192.168.20.0/24	[150/30]	via 10.0.0.1 on gil/0/12,	[ospf1 00:50:15] (0.0.0.3)
C	* 192.168.10.0/24	[0/0]	dev lo1,	[direct 21:32:01]

Review the routing table on R3 router:

```
esr# show ip route
```

O	* 10.0.0.0/24	[150/20]	via 10.0.1.1 on gil/0/12,	[ospf1 14:38:35] (0.0.0.2)
C	* 10.0.1.0/24	[0/0]	dev gil/0/12,	[direct 14:35:34]
C	* 192.168.20.0/24	[0/0]	dev lo1,	[direct 14:32:58]
O	* 192.168.10.0/24	[150/30]	via 10.0.1.1 on gil/0/12,	[ospf1 14:39:54] (0.0.0.1)

Since OSPF considers virtual link as the part of the area, R1 routes received from R3 are marked as an intrazone and vice versa.

To view the neighbors, use the following command:

```
esr# show ip ospf neighbors 10
```

To view OSPF routing table, use the following command:

```
esr# show ip ospf 10
```



In the firewall, you should enable OSPF protocol (89).

7.21 BGP configuration

BGP protocol is designed to exchange subnet reachability information among autonomous systems (AS), i.e. router groups united under a single technical control that uses interdomain routing protocol for defining packet delivery routes to other AS. Transmitted information includes a list of AS that are accessible through this system. Selection of the optimal routes is based on effective rules for the network.

7.21.1 Configuration algorithm

Step	Description	Command	Keys
1	Configure BGP precedence for the main routing table (optionally).	<code>esr(config)# ip protocols bgp preference <VALUE></code>	<VALUE> – protocol precedence, takes values in the range of [1..255]. Default value: BGP (170).
2	Configure BGP routing tables' capacity (optionally).	<code>esr(config)# ip protocols bgp max-routes <VALUE></code> <code>esr(config)# ipv6 protocols bgp max-routes <VALUE></code> <code>esr(config-vrf)# ip protocols bgp max-routes <VALUE></code> <code>esr(config-vrf)# ipv6 protocols bgp max-routes <VALUE></code>	<VALUE> – amount of BGP routes in the routing table, takes values in the range of: for esr-1000/1200/1700 [1..2800000]; for esr-100/200 [1..1500000]; for esr-10/12V(F)/14VF [1..800000]. Default value: BGP (2600000).
3	Enable the output of BGP neighbor state information (optionally).	<code>esr(config)# router bgp log-neighbor-changes</code> <code>esr(config)# ipv6 router bgp log-neighbor-changes</code>	
4	Enable ECMP and define the maximum amount of equal routes to a destination point.	<code>esr(config)# router bgp maximum-paths <VALUE></code>	<VALUE> – amount of valid equal routes to the target, takes the values of [1..16].
5	Create IP subnets lists that will be used for further filtration of advertised and received IP routes.	<code>esr(config)# ip prefix-list <NAME></code> <code>esr(config)# ipv6 prefix-list <NAME></code>	<NAME> – name of a subnet list being configured, set by the string of up to 31 characters.
6	Permit or deny the prefixes lists.	<code>esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route}</code> <code>esr(config-pl)# deny {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] default-route}</code>	<OBJ-GROUP-NETWORK-NAME> – IP addresses profile name, set by the string of up to 31 characters; <LEN> – prefix length, takes values of [1..32] in prefix IP lists; eq – when specifying the command, the prefix length must match the specified one; le – when specifying the command, the prefix length must be less than or match the specified one; ge – when specifying the command, the prefix length must be more than or match the specified one; default-route – default route filtration.
7	Add BGP process to the system and switch to the BGP process parameters configuration mode.	<code>esr(config)# router bgp <AS></code>	<AS> – stand alone system number, takes values of [1..4294967295].

8	Define the type of configured routing information and switch to this configuration mode.	<code>esr(config-bgp) # address-family { ipv4 ipv6 } [vrf <VRF>]</code>	ipv4 – IPv4 family; ipv6 – IPv6 family; <VRF> – VRF instance name, set by the string of up to 31 characters, within which the routing protocol will operate.
9	Set the router identifier.	<code>esr(config-bgp-af) # router-id <ID></code> <code>esr(config-ipv6-bgp-af) # router-id <ID></code>	<ID> – router identifier, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
10	Set the time interval after which the connection with the opposing party is checked.	<code>esr(config-bgp-af) # timers keepalive <TIME></code> <code>esr(config-ipv6-bgp-af) # timers keepalive <TIME></code>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 60 seconds.
11	Set time interval after which the opposing party is considered to be unavailable.	<code>esr(config-bgp-af) # timers holdtime <TIME></code> <code>esr(config-ipv6-bgp-af) # timers holdtime <TIME></code>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 180 seconds.
12	Set the time of minimum and maximum delay during which it is prohibited to establish a connection in order to prevent frequent disconnections.	<code>esr(config-bgp-af) # timers error-wait <TIME1> <TIME2></code> <code>esr(config-ipv6-bgp-af) # timers error-wait <TIME1> <TIME2></code>	<TIME1> – minimum delay time in seconds, takes values of [1..65535]. <TIME2> – maximum delay time in seconds, takes values of [1..65535].
13	Set the Route-Reflector identifier of the cluster to which the router BGP process belongs.	<code>esr(config-bgp-af) # cluster-id <ID></code> <code>esr(config-ipv6-bgp-af) # cluster-id <ID></code>	<ID> – Route-Reflector cluster identifier, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
14	Define the global algorithm of neighbor authentication.	<code>esr(config-bgp-af) # authentication algorithm <ALGORITHM></code> <code>esr(config-ipv6-bgp-af) # authentication algorithm <ALGORITHM></code>	<ALGORITHM> – encryption algorithm: md5 – password is encrypted by md5 algorithm.
15	Set the global password for neighbour authentication.	<code>esr(config-bgp-af) # authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }</code> <code>esr(config-ipv6-bgp-af) # authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }</code>	<CLEAR-TEXT> – password, set by the string of 8 to 16 characters; <ENCRYPTED-TEXT> – encrypted password of 8 to 16 bytes (from 16 to 32 characters) in hexadecimal format (0xYYYY ...) or (YYYY ...).
16	Enable BGP process.	<code>esr(config-bgp-af) # enable</code> <code>esr(config-ipv6-bgp-af) # enable</code>	
17	Enable the advertising of static routes received in an alternative way.	<code>esr(config-bgp-af) # redistribute static [route-map <NAME>]</code> <code>esr(config-ipv6-bgp-af) # redistribute static [route-map <NAME>]</code>	<NAME> – name of the route map that will be used for advertised static routes filtration and modification, set by the string of up to 31 characters.

		<pre>esr(config-bgp-af) # redistribute connected [route-map <NAME>]</pre>	<p><NAME> – name of the route map that will be used for filtration and modification of advertised directly connected subnets, set by the string of up to 31 characters.</p>
		<pre>esr(config-ipv6-bgp- af) # redistribute connected [route-map <NAME>]</pre>	
		<pre>esr(config-bgp-af) # redistribute rip [route-map <NAME>]</pre>	<p><NAME> – name of the route map that will be used for advertised RIP routes filtration and modification, set by the string of up to 31 characters.</p>
		<pre>esr(config-ipv6-bgp- af) # redistribute rip [route-map <NAME>]</pre>	
		<pre>esr(config-bgp-af) # redistribute ospf <ID> <ROUTE-TYPE> [route-map <NAME>]</pre>	<p><ID> – process number, takes values of [1..65535]. <ROUTE-TYPE> – route type: intra-area – OSPF process routes advertising within a zone; inter-area – OSPF process routes advertising between zones; external1 – OSPF format 1 external routes advertising; external2 – OSPF format 2 external routes advertising;</p>
		<pre>esr(config-ipv6-bgp- af) # redistribute ospf <ID> <ROUTE- TYPE> [route-map <NAME>]</pre>	<p><NAME> – name of the route map that will be used for advertised OSPF routes filtration and modification, set by the string of up to 31 characters.</p>
		<pre>esr(config-bgp-af) # redistribute bgp <AS> [route-map <NAME>]</pre>	<p><AS> – stand alone system number, takes values of [1..4294967295]. <NAME> – name of the route map that will be used for advertised BGP routes filtration and modification, set by the string of up to 31 characters.</p>
		<pre>esr(config-ipv6-bgp- af) # redistribute bgp <AS> [route-map <NAME>]</pre>	
18	Enable subnets advertising.	<pre>esr(config-bgp-af) # network <ADDR/LEN></pre>	<p><ADDR/LEN> – subnet address, set in the following format: AAA.BBB.CCC.DDD/NN – network IP address with prefix mask, where AAA-DDD take values of [0..255] and EE takes values of [1..32].</p>
		<pre>esr(config-ipv6-bgp- af) # network <ADDR/LEN></pre>	<p>X:X:X:X::X/EE – IPv6 address and mask of a subnet, where each X part takes values in hexadecimal format [0..FFFF] and EE takes values of [1..128].</p>
19	Add subnets filtration in incoming or outgoing updates (optionally).	<pre>esr(config-bgp-af) # prefix-list <PREFIX- LIST-NAME> { in out }</pre>	<p><PREFIX-LIST-NAME> – name of a subnet list being configured, set by the string of up to 31 characters. in – incoming routes filtration; out – advertised routes filtration.</p>
20	Add BGP neighbor and switch to the BGP process parameters configuration mode.	<pre>esr(config-bgp-af) # neighbor <ADDR></pre>	<p><ADDR> – neighbor's IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].</p>
		<pre>esr(config-ipv6-bgp- af) # neighbor <IPV6- ADDR></pre>	<p><IPV6-ADDR> – client IPv6 address, defined as X:X:X:X::X where each part takes values in hexadecimal format [0..FFFF].</p>

21	Specify the neighbor description. (optionally).	<pre>esr (config-bgp-neighbor) # description <DESCRIPTION> esr (config-ipv6-bgp-neighbor) # description <DESCRIPTION></pre>	<DESCRIPTION> – neighbor description, set by the string of up to 255 characters.
22	Set the time interval after which the connection with the opposing party is checked. (optionally)	<pre>esr (config-bgp-neighbor) # timers keepalive <TIME> esr (config-ipv6-bgp-neighbor) # timers keepalive <TIME></pre>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 60 seconds.
23	Set time interval after which the opposing party is considered to be unavailable. (optionally)	<pre>esr (config-bgp-neighbor) # timers holdtime <TIME> esr (config-ipv6-bgp-neighbor) # timers holdtime <TIME></pre>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 180 seconds.
24	Set the time of minimum and maximum delay during which it is prohibited to establish a connection in order to prevent frequent disconnections. (optionally)	<pre>esr (config-bgp-af) # timers error-wait <TIME1> <TIME2> esr (config-ipv6-bgp-af) # timers error-wait <TIME1> <TIME2></pre>	<TIME1> – minimum delay time in seconds, takes values of [1..65535]. <TIME2> – maximum delay time in seconds, takes values of [1..65535]. Default value: 60 and 300 seconds
25	Set the number of BGP neighbor stand alone system.	<pre>esr (config-bgp-neighbor) # remote-as <AS> esr (config-ipv6-bgp-neighbor) # remote-as <AS></pre>	<AS> – stand alone system number, takes values of [1..4294967295].
26	Allow connections to neighbors that are located not in directly connected subnets. (optionally)	<pre>esr (config-bgp-neighbor) # ebgp- multihop <NUM> esr (config-ipv6-bgp-neighbor) # ebgp- multihop <NUM></pre>	<NUM> – maximum amount of hops when installing EBGP (used for TTL).
27	Set the mode in which all updates are sent to BGP neighbor with the IP address of a local router outgoing interface as the next-hop. (optionally)	<pre>esr (config-bgp-neighbor) # next-hop- self esr (config-ipv6-bgp-neighbor) # next-hop- self</pre>	
28	Set the mode in which private numbers of autonomous systems are removed from the AS Path routes BGP attribute before sending an update (in accordance with RFC 6996). (optionally)	<pre>esr (config-bgp-neighbor) # remove- private-as esr (config-ipv6-bgp-neighbor) # remove- private-as</pre>	
29	Set the mode in which the default route is always sent to the BGP neighbor in the update along with other routes. (optionally)	<pre>esr (config-bgp-neighbor) # default- originate esr (config-ipv6-bgp-neighbor) # default- originate</pre>	
30	Enable generation and sending of a default route, if the default route is in the	<pre>esr (config-bgp-af) # default-information- originate</pre>	

	FIB routing table. (optionally)		
31	Specify BGP neighbor as a Route-Reflector client. (optionally)	<pre>esr(config-bgp-neighbor)# route-reflector-client</pre> <pre>esr(config-ipv6-bgp-neighbor)# route-reflector-client</pre>	
32	Define the precedence of the routes received from a neighbor. (optionally)	<pre>esr(config-bgp-neighbor)# preference <VALUE></pre> <pre>esr(config-ipv6-bgp-neighbor)# preference <VALUE></pre>	<VALUE> – neighbor routes precedence, takes values in the range of [1..255]. Default value: 170.
33	Set IP/IPv6 router address that will be used as source IP/IPv6 address in transmitted BGP route information updates. (optionally)	<pre>esr(config-bgp-neighbor)# update-source { <ADDR> <IPV6-ADDR> }</pre> <pre>esr(config-ipv6-bgp-neighbor)# update-source <ADDR></pre>	<p><ADDR> – source IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255];</p> <p><IPV6-ADDR> – source IPv6 address, defined as X:X:X:X:X where each part takes values in hexadecimal format [0..FFFF].</p>
34	Enable the mode in which the reception of routes in the BGP attribute, AS Path of which includes the numbers of process stand alone system, is allowed. (optionally)	<pre>esr(config-bgp-neighbor)# allow-local-as <NUMBER></pre> <pre>esr(config-bgp-neighbor)# allow-local-as <NUMBER></pre>	<NUMBER> – threshold amount of instances of autonomous system number in the AS Path attribute at which the route will be accepted, the range of acceptable values [1..10].
35	Enable BFD protocol on the BGP neighbor being configured (optionally).	<pre>esr(config-bgp-neighbor)# bfd-enable</pre> <pre>esr(config-ipv6-bgp-neighbor)# bfd-enable</pre>	
36	Specify neighbor authentication algorithm. (optionally)	<pre>esr(config-bgp-neighbor)# authentication algorithm <ALGORITHM></pre> <pre>esr(config-ipv6-bgp-neighbor)# authentication algorithm <ALGORITHM></pre>	<ALGORITHM> – encryption algorithm: md5 – password is encrypted by md5 algorithm.
37	Set the password for neighbour authentication. (optionally)	<pre>esr(config-bgp-neighbor)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }</pre> <pre>esr(config-ipv6-bgp-neighbor)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }</pre>	<p><CLEAR-TEXT> – password, set by the string of 8 to 16 characters;</p> <p><ENCRYPTED-TEXT> – encrypted password of 8 to 16 bytes (from 16 to 32 characters) in hexadecimal format (0xYYYY ...) or (YYYY ...).</p>

It often happens, especially when configuring iBGP, that in one bgp address-family you need to configure several bgp neighbor with the same parameters. To avoid configuration redundancy, it is recommended to use bgp peer-group in which you can describe common parameters and it is easy to identify the bgp peer-group membership in the bgp neighbor configuration.

7.21.2 Configuration example

Objective:

Configure BGP on the router with the following parameters:

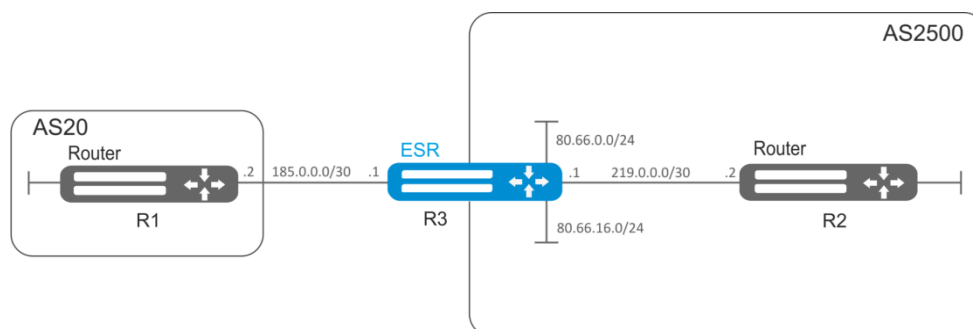


Figure 60 – Network structure

- proprietary subnets: 80.66.0.0/24, 80.66.16.0/24;
- advertising of directly connected subnets;
- proprietary AS 2500;
- first neighbouring-subnet 219.0.0.0/30, proprietary IP address 219.0.0.1, neighbour IP address 219.0.0.2, AS 2500;
- second neighbouring-subnet 185.0.0.0/30, proprietary IP address 185.0.0.1, neighbour IP address 185.0.0.2, AS 20.

Solution:

Configure required network parameters:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 185.0.0.1/30
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# ip address 219.0.0.1/30
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/3
esr(config-if-gi)# ip address 80.66.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/4
esr(config-if-gi)# ip address 80.66.16.1/24
esr(config-if-gi)# exit
```

Create BGP process for AS 2500 and enter process parameters' configuration mode:

```
esr(config)# router bgp 2500
```

Enter routing information configuration mode for IPv4:

```
esr(config-bgp)# address-family ipv4
```

Advertise directly connected subnets:

```
esr(config-bgp-af) # redistribute connected
```

Create neighboring with 185.0.0.2, 219.0.0.2 specifying AS and enable them:

```
esr(config-bgp-af) # neighbor 185.0.0.2
esr(config-bgp-neighbor) # remote-as 20
esr(config-bgp-neighbor) # enable
esr(config-bgp-neighbor) # exit
esr(config-bgp-af) # neighbor 219.0.0.2
esr(config-bgp-neighbor) # remote-as 2500
esr(config-bgp-neighbor) # enable
esr(config-bgp-neighbor) # exit
```

Enable protocol operation:

```
esr(config-bgp-af) # enable
esr(config-bgp-af) # exit
esr(config) # exit
```

To view BGP peers information, use the following command:

```
esr# show ip bgp 2500 neighbors
```

To view BGP routing table, use the following command:

```
esr# show ip bgp
```



You should open TCP port 179 in the firewall.

7.22 BFD configuration

BFD (Bidirectional Forwarding Detection) is a protocol operating over other protocols and allowing to reduce the problem detection time to 50 msec. BFD is two-party protocol, it requires the configuration of both routers (both routers generate BFD packets and respond to each other).

7.22.1 Configuration algorithm

Step	Description	Command	Keys
1	Enable BFD for OSPF on the interface	<code>esr(config-if-gi) # ip ospf bfd-enable</code>	
2	Enable BFD for BGP neighbor on the interface	<code>esr(config-bgp-neighbor) # bfd-enable</code>	
3	Set the interval after which the BFD message is sent to the neighbor. Globally (optionally)	<code>esr(config) # ip bfd idle-tx-interval <TIMEOUT></code>	<TIMEOUT> – interval after which the BFD packet should be sent, takes values in milliseconds in the range of [200..65535] for ESR-1000/1200/1700 and [300..65535] for ERS-10/12V(F)/100/200 By default, 1 second
4	Enable the logging of BFD protocol state changes (optionally)	<code>esr(config) # ip bfd log-adjacency-changes</code>	

5	Set the minimum interval after which the neighbor should generate BFD message. Globally (optionally)	<code>esr(config)# ip bfd min-rx-interval <TIMEOUT></code>	<TIMEOUT> – interval after which the BFD message should be sent by the neighbor, takes values in milliseconds in the range of [200..65535] for ESR-1000/1200/1700 and [300..65535] for ESR-10/12V(F)/100/200 By default: 300 milliseconds for ESR-10, ESR-12V(F), ESR-14VF, ESR-100 and ESR-200 200 milliseconds for ESR-1000, ESR-1200 and ESR-1700
6	Set the minimum interval after which the BFD message is sent to the neighbor. Globally (optionally)	<code>esr(config)# ip bfd min-tx-interval <TIMEOUT></code>	<TIMEOUT> – interval after which the BFD message should be sent by the neighbor, takes values in milliseconds in the range of [200..65535] for ESR-1000/1200/1700 and [300..65535] for ESR-10/12V(F)/100/200 By default: 300 milliseconds for ESR-10, ESR-12V(F), ESR-14VF, ESR-100 and ESR-200 200 milliseconds for ESR-1000, ESR-1200 and ESR-1700
7	Set the amount of dropped packets, at which the BFD neighbor is considered to be unavailable. Globally	<code>esr(config)# ip bfd multiplier <COUNT></code>	<COUNT> – amount of dropped packets, at which the neighbor is considered to be unavailable, takes values in the range of [1..100]. By default: 5
8	Put BFD mechanism with the specified IP address into operation.	<code>esr(config)# ip bfd neighbor <ADDR> [{ interface <IF> tunnel <TUN> }] [local-address <ADDR> [multihop]] [vrf <VRF>]</code>	<ADDR> – gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <IF> – interface or interface group; <TUN> – tunnel type and number. <VRF> – VRF name, set by the string of up to 31 characters. multihop – key for setting TTL=255, for BFD mechanism operation through the routed network.
9	Switch BFD session to the passive mode, so that BFD messages will not be sent until the messages from BFD neighbor are received. Globally (optionally)	<code>esr(config)# ip bfd passive</code>	
10	Set the interval after which the BFD message is sent to the neighbor. On the interface (optionally)	<code>esr(config-if-gi)# ip bfd idle-tx-interval <TIMEOUT></code>	<TIMEOUT> – interval after which the BFD packet should be sent, takes values in milliseconds in the range of [200..65535] for ESR-1000/1200/1700 and [300..65535] for ERS-10/12V(F)/100/200. By default: 1 second

11	Set the minimum interval after which the neighbor should generate BFD message. On the interface (optionally)	<code>esr(config-if-gi)# ip bfd min-rx-interval <TIMEOUT></code>	<TIMEOUT> – interval after which the BFD message should be sent by the neighbor, takes values in milliseconds in the range of [200..65535] for ESR-1000/1200/1700 and [300..65535] for ESR-10/12V(F)/100/200 By default: 300 milliseconds for ESR-10, ESR-12V(F), ESR-14VF, ESR-100 and ESR-200 200 milliseconds for ESR-1000, ESR-1200 and ESR-1700
12	Set the minimum interval after which the BFD message is sent to the neighbor. On the interface (optionally)	<code>esr(config-if-gi)# ip bfd min-tx-interval <TIMEOUT></code>	<TIMEOUT> – interval after which the BFD message should be sent by the neighbor, takes values in milliseconds in the range of [200..65535] for ESR-1000/1200/1700 and [300..65535] for ESR-10/12V(F)/100/200 By default: 300 milliseconds for ESR-10, ESR-12V(F), ESR-14VF, ESR-100 and ESR-200 200 milliseconds for ESR-1000, ESR-1200 and ESR-1700
13	Set the amount of dropped packets, at which the BFD neighbor is considered to be unavailable. On the interface (optionally)	<code>esr(config-if-gi)# ip bfd multiplier <COUNT></code>	<COUNT> – amount of dropped packets, at which the neighbor is considered to be unavailable, takes values in the range of [1..100]. By default: 5
14	Switch BFD session to the passive mode, so that BFD messages will not be sent until the messages from BFD neighbor are received. On the interface (optionally)	<code>esr(config-if-gi)# ip bfd passive</code>	

7.22.2 Configuration example of BFD with BGP

Objective:

Configure eBGP between ESR R1 and R2 and enable BFD.



Figure 61 – Network structure

Solution:

1. R1 configuration

Preconfigure Gi1/0/1 interface:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# ip address 10.0.0.1/24
```

Configure eBGP with BFD:

```
esr(config)# router bgp 100
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.0.0.2
esr(config-bgp-neighbor)# remote-as 200
esr(config-bgp-neighbor)# update-source 10.0.0.1
esr(config-bgp-neighbor)# bfd-enable
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# ex
esr(config-bgp-af)# enable
esr(config-bgp-af)# exit
```

2. R2 configuration

Preconfigure Gi1/0/1 interface:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# ip address 10.0.0.2/24
```

Configure eBGP with BFD:

```
esr(config)# router bgp 200
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.0.0.1
esr(config-bgp-neighbor)# remote-as 100
esr(config-bgp-neighbor)# update-source 10.0.0.2
esr(config-bgp-neighbor)# bfd-enable
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# ex
esr(config-bgp-af)# enable
esr(config-bgp-af)# exit
```

7.23 PBR routing policy configuration

7.23.1 Configuring Route-map for BGP

Route-maps may serve as filters processing routing information when it is received from or sent to the neighbouring device. Processing may include filtering based on various route criteria and setting attributes (MED, AS-PATH, community, LocalPreference, etc.) for the respective routes.

Also, Route-map may assign routes based on access control lists (ACL).

7.23.1.1 Configuration algorithm

Step	Description	Command	Keys
1	Create a route map for IP routes filtration and modification.	<code>esr(config)# route-map <NAME></code>	<NAME> – router map name, set by the string of up to 31 characters.

2	Create a route map rule.	<code>esr (config-route-map)# rule <ORDER></code>	<ORDER> – rule number, takes values of [1..10000].
3	Specify the action that should be applied for routing information.	<code>esr (config-route-map-rule)# action <ACT></code>	<ACT> – allocated action: permit – routing information reception or advertising is permitted; deny – denied.
4	Set BGPAS-Path attribute value in the route for which the rule should work (optionally).	<code>esr (config-route-map-rule)# match as-path [begin end contain] <AS-PATH></code>	<AS-PATH> – list of stand alone system numbers, defined as AS,AS,AS, takes values of [1..4294967295]. Optional parameters: begin – attribute value begins with the specified AS numbers; end – attribute value ends with the specified AS numbers; contain – attribute value includes the specified AS numbers list.
5	Set BGPCommunity attribute value for which the rule should work (optionally).	<code>esr (config-route-map-rule)# match community <COMMUNITY-LIST></code>	<COMMUNITY-LIST> – community list, defined as AS:N,AS:N, takes values of [1..4294967295]. You can specify up to 64 community.
6	BGPExtendedCommunity attribute value for which the rule should work (optionally).	<code>esr (config-route-map-rule)# match extcommunity <EXTCOMMUNITY-LIST></code>	<EXTCOMMUNITY-LIST> – extcommunity list, defined as KIND:AS:N, KIND:AS:N, where KIND – extcommunity type: - RT (Route Target); - RO (Route Origin); N – extcommunity number, takes values of [1..65535].
7	Set IP addresses profile including destination subnet values in the route (optionally).	<code>esr (config-route-map-rule)# match ip address object-group <OBJ-GROUP- NETWORK - NAME></code> <code>esr (config-route-map-rule)# match ipv6 address object-group <OBJ-GROUP- NETWORK - NAME></code>	<OBJ-GROUP-NETWORK-NAME> – name of the IP addresses profile that includes destination subnets prefixes, set by the string of up to 31 characters.
8	Set IP addresses profile that includes BGPNext-Hop attribute value in the route for which the rule should work (optionally).	<code>esr (config-route-map-rule)# match ip next-hop object-group <OBJ-GROUP- NETWORK - NAME></code> <code>esr (config-route-map-rule)# match ipv6 next-hop object-group <OBJ-GROUP- NETWORK - NAME></code>	<OBJ-GROUP-NETWORK-NAME> – name of the IP addresses profile that includes destination subnets prefixes, set by the string of up to 31 characters.
9	Set the profile that includes IP addresses of the router having advertised the route for which the rule should work (optionally).	<code>esr (config-route-map-rule)# match ip route-source object-group <OBJ-GROUP-NETWORK -NAME></code> <code>esr (config-route-map-rule)# match ipv6 route-source object-group <OBJ-GROUP-NETWORK -NAME></code>	<OBJ-GROUP-NETWORK-NAME> – name of the IP addresses profile that includes destination subnets prefixes, set by the string of up to 31 characters.
10	Specify ACL group for which the rule should work.	<code>esr (config-route-map-rule)# match access-group <NAME></code>	<NAME> – access control list name, set by the string of up to 31 characters.
11	Set BGP MED attribute value in the route for which the rule should work (optionally).	<code>esr (config-route-map-rule)# match metric bgp <METRIC></code>	<METRIC> – BGP MED attribute value, takes values in the range of [0..4294967295].

12	Set OSPF Metric attribute value in the route for which the rule should work.	<code>esr (config-route-map-rule)# match metric ospf <TYPE> <METRIC></code>	<TYPE> – OSPF Metric attribute type, takes values type-1 and type-2; <METRIC> – OSPF Metric attribute value, takes values in the range of [0..65535].
13	Set RIP Metric attribute value in the route for which the rule should work.	<code>esr (config-route-map-rule)# match metric rip <METRIC></code>	<METRIC> – RIP Metric attribute value, takes values in the range of [0..16].
14	Set OSPF Tag attribute value in the route for which the rule should work.	<code>esr (config-route-map-rule)# match tag ospf <TAG></code>	<TAG> – OSPF Tag attribute value, takes values in the range of [0..4294967295].
15	Set RIP Tag attribute value in the route for which the rule should work.	<code>esr (config-route-map-rule)# match tag rip <TAG></code>	<RIP> – RIP Tag attribute value, takes values in the range of [0..65535].
16	Set BGP AS-Path attribute value that will be added to the beginning of AS-Path list (optionally).	<code>esr (config-route-map-rule)# action set as-path prepend <AS-PATH> {track <TRACK-ID>}</code>	<AS-PATH> – stand alone systems number list that will be added to the current value in the route. Set as AS, AS, AS, takes values of [1..4294967295]. <TRACK-ID> – vrrp-tracking identifier that provides the specified action execution. Changes in the range of [1..60].
17	Set BGP Community attribute value that will be specified in the route (optionally).	<code>esr (config-route-map-rule)# action set community {COMMUNITY-LIST} no-advertise no-export }</code>	<COMMUNITY-LIST> – community list, defined as AS:N,AS:N, where each part takes values of [1..65535]. no-advertise – routes transmitted with the given community should not be advertised to other BGP neighbors; no-export – routes transmitted with the given community should not be advertised to eBGP neighbors but can be advertised to external neighbors in the confederation.
18	Set BGP ExtCommunity attribute value that will be specified in the route (optionally).	<code>esr (config-route-map-rule)# action set extcommunity <EXTCOMMUNITY-LIST></code>	<EXTCOMMUNITY-LIST> – extcommunity list, defined as KIND:AS:N, KIND:AS:N, where KIND – extcommunity type: - RT (Route Target); - RO (Route Origin); N – extcommunity number, takes values of [1..65535].
19	Specify BGP Next-Hop attribute that will be set in the route when advertising (optionally).	<code>esr (config-route-map-rule)# action set ip bgp-next-hop <ADDR></code>	<ADDR> – gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
		<code>esr (config-route-map-rule)# action set ipv6 bgp-next-hop <IPV6-ADDR></code>	<IPV6-ADDR> – gateway IPv6 address, defined as X:X:X::X where each part takes values in hexadecimal format [0..FFFF].

20	Specify Next-Hop value that will be set in the route received by BGP (optionally).	<pre>esr(config-route-map-rule)# action set ip next-hop {NEXTHOP} blackhole unreachable prohibit}</pre>	<p><NEXTHOP> – gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255];</p> <p>blackhole – packets to this subnet will be removed without sending notifications to a sender;</p> <p>unreachable – packets to this subnet will be removed, a sender will receive in response ICMP Destination unreachable (Host unreachable, code 1);</p> <p>prohibit – packets to this subnet will be removed by the device, a sender will receive in response ICMPDestinationunreachable (Communication administratively prohibited code 13).</p>
		<pre>esr(config-route-map-rule)# action set ipv6 next-hop <IPV6-NEXTHOP></pre>	<p><IPV6-NEXTHOP> – gateway IPv6 address, defined as X:X:X:X where each part takes values in hexadecimal format [0..FFFF].</p>
21	Specify BGP Local Preference attribute value that will be set in the route (optionally).	<pre>esr(config-route-map-rule)# action set local-preference <PREFERENCE></pre>	<p><PREFERENCE> – BGP Local Preference attribute value, takes values in the range of [0..255].</p>
22	Specify BGP Origin attribute value that will be set in the route (optionally).	<pre>esr(config-route-map-rule)# action set origin <ORIGIN></pre>	<p><ORIGIN> – BGP Origin attribute value:</p> <p>egp – route is learnt by EGP;</p> <p>igp – route is received inside the initial AS;</p> <p>incomplete – route is learnt in another way.</p>
23	Specify BGP MED value that will be set in the route (optionally).	<pre>esr(config-route-map-rule)# action set metric bgp <METRIC></pre>	<p><METRIC> – BGP MED attribute value, takes values in the range of [0..4294967295].</p>
24	Add filtration and modification of routes in incoming or outgoing directions.	<pre>esr(config-bgp-neighbor)# route-map <NAME><DIRECTION></pre>	<p><NAME> – name of the route map having been configured;</p> <p><DIRECTION> – direction:</p> <p>in – filtration and modification of received routes;</p> <p>out – filtration and modification of advertised routes.</p>
		<pre>esr(config-ipv6-bgp-neighbor)# route-map <NAME><DIRECTION></pre>	

7.23.1.2 Configuration example 1

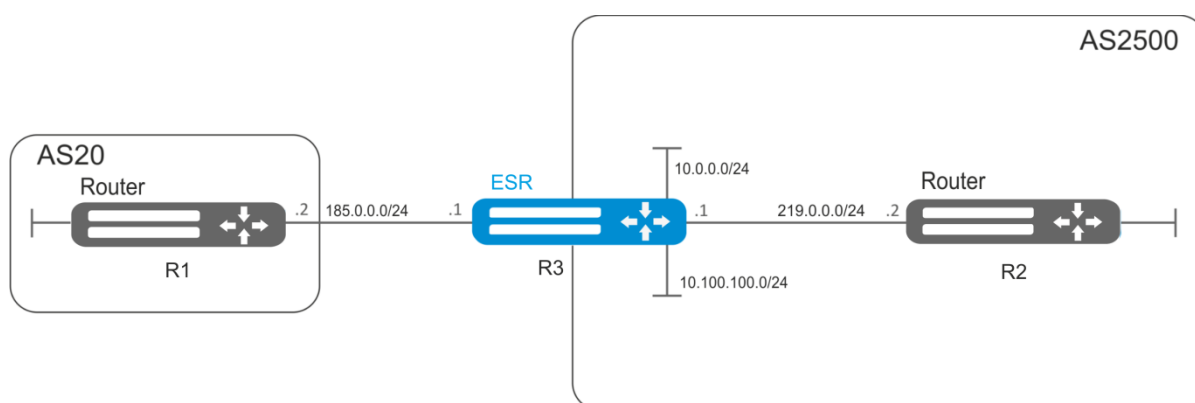


Figure 62 – Network structure

Objective:

Assign community for routing information coming from AS 20:

First, do the following:

- Configure BGP with AS 2500 on ESR router;
- Establish neighbouring with AS20.

Solution:

Create a policy:

```
esr# configure  
esr(config)# route-map from-as20
```

Create rule 1:

```
esr(config-route-map)# rule 1
```

If AS PATH contains AS 20, assign community 20:2020 to it and exit:

```
esr(config-route-map-rule)# match as-path contain 20  
esr(config-route-map-rule)# action set community 20:2020  
esr(config-route-map-rule)# exit  
esr(config-route-map)# exit
```

In AS 2500 BGP process, enter neighbour parameter configuration:

```
esr(config)# router bgp 2500  
  
esr(config-bgp)# address-family ipv4  
  
esr(config-bgp-af)# neighbor 185.0.0.2
```

Map the policy to routing information:

```
esr(config-bgp-neighbor)# route-map from-as20 in
```

7.23.1.3 Configuration example 2

Objective:

For the whole transmitted routing information (from community 2500:25), assign MED equal to 240 and define EGP routing information source:

First:

Configure BGP with AS 2500 on ESR

Solution:

Create a policy:

```
esr(config)# route-map to-as20
```

Create a rule:

```
esr(config-route-map) # rule 1
```

If community contains 2500:25, assign MED 240 and Origin EGP to it:

```
esr(config-route-map-rule) # match community 2500:25
esr(config-route-map-rule) # action set metric bgp 240
esr(config-route-map-rule) # action set origin egp
esr(config-route-map-rule) # exit
esr(config-route-map) # exit
```

In AS 2500 BGP process, enter neighbour parameter configuration:

```
esr(config) # router bgp 2500

esr(config-bgp) # address-family ipv4

esr(config-bgp-af) # neighbor 185.0.0.2
```

Map the policy to routing information being advertised:

```
esr(config-bgp-neighbor) # route-map to-as20 out

esr(config-bgp-neighbor) # exit
esr(config-bgp) # exit
esr(config) # exit
```

7.23.2 Route-map based on access control lists (Policy-based routing)

7.23.2.1 Configuration algorithm

Step	Description	Command	Keys
1	Create a route map for IP routes filtration and modification.	<code>esr(config)# route-map <NAME></code>	<NAME> – router map name, set by the string of up to 31 characters.
2	Create a route map rule	<code>esr(config-route-map)# rule <ORDER></code>	<ORDER> – rule number, takes values of [1..10000].
3	Specify the action that should be applied for routing information.	<code>esr(config-route-map-rule)# action <ACT></code>	<ACT> – allocated action: permit – routing information reception or advertising is permitted; deny – denied.
4	Set ACL for which the rule should work (optionally).	<code>esr(config-route-map-rule)# match ip access-group <NAME></code>	<NAME> – access control list name, set by the string of up to 31 characters.
5	Set Next-Hop for the packets that meet the requirements of the specified ACL (optionally).	<code>esr(config-route-map-rule)# action set ip next-hop verify-availability <NEXTHOP><METRIC></code>	<NEXTHOP> – gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <METRIC> – route metric, takes values of [0..255].
6	Specify ACL-based routing policy.	<code>esr(config-if-gi)# ip policy route-map <NAME></code>	<NAME> – configured routing policy name, set by the string of up to 31 characters.

7.23.2.2 Configuration example

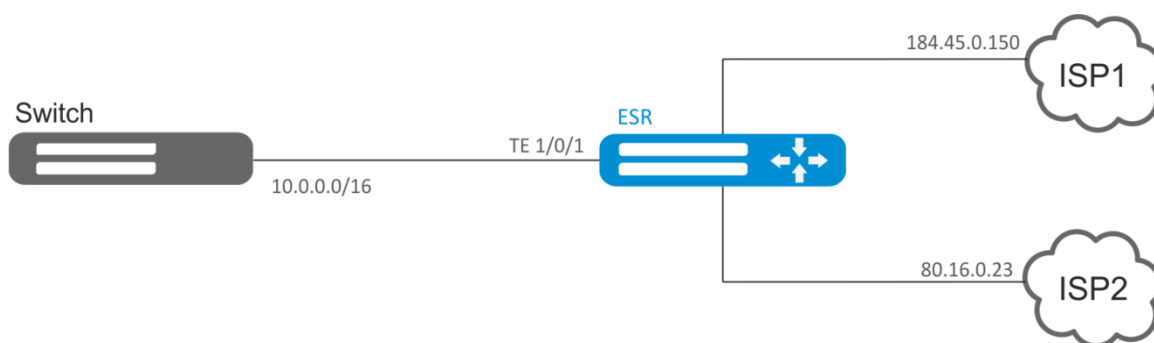


Figure 63 – Network structure

Objective:

Distribute traffic between Internet service providers based on user subnets.

First, assign IP address to interfaces.

Route traffic from addresses 10.0.20.0/24 through ISP1 (184.45.0.150), and traffic from addresses 10.0.30.0/24 – through ISP2 (80.16.0.23). You should monitor availability of ISP addresses (ISP connection operational capability), and if one the connections goes down, redirect all the traffic from malfunctioning connection to the operational one.

Solution:

Create ACL:

```

esr# configure
esr(config)# ip access-list extended sub20
esr(config-acl)# rule 1
esr(config-acl-rule)# match source-address 10.0.20.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# action permit
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
esr(config)# ip access-list extended sub30
esr(config-acl)# rule 1
esr(config-acl-rule)# match source-address 10.0.30.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# action permit
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
  
```

Create a policy:

```

esr(config)# route-map PBR
  
```

Create rule 1:

```

esr(config-route-map)# rule 1
  
```

Specify ACL as a filter:

```
esr(config-route-map-rule) # match ip access-group sub20
```

Specify nexthop for sub20:

```
esr(config-route-map-rule) # action set ip next-hop verify-availability 184.45.0.150 10
esr(config-route-map-rule) # action set ip next-hop verify-availability 80.16.0.23 30
esr(config-route-map-rule) # exit
esr(config-route-map) # exit
```

Rule 1 should provide traffic routing from the network 10.0.20.0/24 to address 184.45.0.150, and in case of its failure, to address 80.16.0.23. Gateway precedence is defined by metrics values – 10 and 30.

Create rule 2:

```
esr(config-route-map) # rule 2
```

Specify ACL as a filter:

```
esr(config-route-map-rule) # match ip access-group sub30
```

Specify nexthop for sub30 and exit:

```
esr(config-route-map-rule) # action set ip next-hop verify-availability 80.16.0.23 10
esr(config-route-map-rule) # action set ip next-hop verify-availability 184.45.0.150 30
esr(config-route-map-rule) # exit
esr(config-route-map) # exit
```

Rule 2 should provide traffic routing from the network 10.0.30.0/24 to address 80.16.0.23, and in case of its failure, to address 184.45.0.150. Precedence is defined by metrics values.

Proceed to TE 1/0/1 interface:

```
esr(config) # interface tengigabitethernet 1/0/1
```

Map the policy the respective interface:

```
esr(config-if-te) # ip policy route-map PBR
```

7.24 GRE tunnel configuration

GRE (Generic Routing Encapsulation) is a network packet tunneling protocol. Its main purpose is to encapsulate packets of the OSI model network layer into IP packets. GRE may be used for VPN establishment on 3rd level of OSI model. In ESR router implemented static unmanageable GRE tunnels, i.e. tunnels are created manually via configuration on local and remote hosts. Tunnel parameters for each side should be mutually agreeable, otherwise transferred data will not be decapsulated by the partner.

7.24.1 Configuration algorithm

Step	Description	Command	Keys
1	Configure L3 interface from which a GRE tunnel will be built.		

2	Create a GRE tunnel and switch to its configuration mode.	<code>esr(config)# tunnel gre <INDEX></code>	<INDEX> – tunnel identifier in the range of: for esr10/12V(F) – [1..10], esr100/200 – [1..250], for esr1000/1200/1700 - [1..500]
3	Specify VRF instance, in which the given GRE tunnel will operate (optionally).	<code>esr(config-bridge)# ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.
4	Specify the description of the configured tunnel (optionally).	<code>esr(config-gre)# description <DESCRIPTION></code>	<DESCRIPTION> – tunnel description, set by the string of up to 255 characters.
5	Set local IP address for tunnel installation.	<code>esr(config-gre)# local address <ADDR></code>	<ADDR> – gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
		<code>esr(config-gre)# interface <IF></code>	<IF> – interface IP address of which is used for the tunnel installation.
6	Set remote IP address for tunnel installation.	<code>esr(config-gre)# remote address <ADDR></code>	<ADDR> – gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
7	Specify the GRE tunnel encapsulation mode.	<code>esr(config-gre)# mode <MODE></code>	<MODE> – specify the GRE tunnel encapsulation mode: ip – encapsulation of IP in GRE; ethernet – encapsulation of Ethernet frames in GRE. Default value: ip
8	Set the IP address of a tunnel local side (only in ip mode).	<code>esr(config-gre)# ip address <ADDR/LEN></code>	<ADDR/LEN> – IP address and prefix of a subnet, defined as AAA.BBB.CCC.DDD/EE where each part AAA-DDD takes values of [0..255] and EE takes values of [1..32]. You can specify up to 8 IP addresses separated by commas.
9	Assign the broadcast domain for encapsulation in the tunnel's GRE packets (only in ethernet mode).	<code>esr(config-gre)# bridge-group <BRIDGE-ID></code>	<BRIDGE-ID> – bridge identifier, takes values in the range of: for esr10/12V(F) – [1..50], esr100/200 – [1..250], for esr1000/1200 - [1..500]
10	Specify MTU size (MaximumTransmissionUnit) for the tunnel (optionally). MTU above 1500 will be active only when using the "system jumbo-frames" command.	<code>esr(config-gre)# mtu <MTU></code>	<MTU> – MTU value, takes values in the range of: for esr-10/12V(F)/14VF [1280..9600]; for esr-100/200/1000/1200/1700 [1280..10000]. Default value: 1500.
11	Specify the TTL lifetime for tunnel packets (optionally).	<code>esr(config-gre)# ttl <TTL></code>	<TTL> – TTL value, takes values in the range of [1..255]. Default value: Inherited from encapsulated packet.
12	Specify DSCP for the use in IP header of encapsulated packet (optionally).	<code>esr(config-gre)# dscp <DSCP></code>	<DSCP> – DSCP code value, takes values in the range of [0..63]. Default value: inherited from encapsulated packet.
13	Enable key transmitting in GRE tunnel header (according to RFC 2890) and set the key value. Configured on the both tunnel sides. (optionally).	<code>esr(config-gre)# key <KEY></code>	<KEY> – KEY value, takes values in the range of [1..2000000]. Default value: key is not transmitted.

14	Enable the calculation of the checksum and entry it to the GRE header of the packets to be sent. Also it is necessary to enable verifying of the checksum on the remote side. (optionally)	<code>esr(config-gre)# local checksum</code>	
15	Enable verification of the presence and consistency of checksum values in the headers of GRE packets being received. Also it is necessary to enable calculation of the checksum on the remote side. (optionally)	<code>esr(config-gre)# remote checksum</code>	
16	Enable the check for tunnel remote gateway availability (optionally)	<code>esr(config-gre)# keepalive enable</code>	
17	Specify the keepalive packets timeout from the opposing party (optionally)	<code>esr(config-gre)# keepalive timeout <TIME></code>	<TIME> – time in seconds, takes values of [1..32767]. Default value: 10
18	Set the number of attempts to check the availability of a tunnel remote gateway (optionally)	<code>esr(config-gre)# keepalive retries <VALUE></code>	<VALUE> – number of attempts, takes values in the range of [1..255]. Default value: 5
19	Specify the time interval during which the statistics on the tunnel load is averaged (optionally)	<code>esr(config-gre)# load-average <TIME></code>	<TIME> – interval in seconds, takes values of [5..150]. Default value: 5
20	Enable sending snmp-trap about tunnel enabling/disabling.	<code>esr(config-gre)# snmp init-trap</code>	
21	Enable the mechanism of IP addresses iterative query using DHCP on the specified interfaces when the GRE tunnel is disconnected via keepalive (optionally)	<code>esr(config-gre)# keepalive dhcp dependent-interface <IF></code>	<IF> – physical/logical interface on which IP address obtaining via DHCP is enabled.
22	Specify the time interval between GRE tunnel disabling and IP address iterative query on the interface/interfaces specified by the keepalive dhcp dependent-interface command (optionally)	<code>esr(config-gre)# keepalive dhcp link- timeout <SEC></code>	<SEC> – time interval between GRE tunnel disabling and IP address requery via DHCP on the interfaces
23	Enable the tunnel.	<code>esr(config-gre)# enable</code>	

7.24.2 IP-GRE tunnel configuration example

Objective:

Establish L3-VPN for company offices using IP network with GRE protocol for traffic tunneling.

- IP address 115.0.0.1 is used as a local gateway for the tunnel;
- IP address 114.0.0.10 is used as a remote gateway for the tunnel;
- IP address of the tunnel at the local side is 25.0.0.1/24.

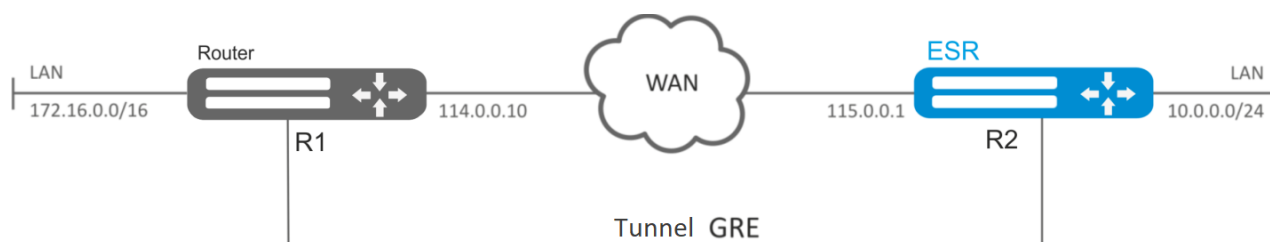


Figure 64 – Network structure

Solution:

Pre-configure interfaces on the routers for connection with WAN, enable GRE packets reception from a security zone where WAN connected interfaces operate.

Create GRE 10 tunnel:

```
esr(config)# tunnel gre 10
```

Specify local and remote gateways (IP addresses of WAN border interfaces):

```
esr(config-gre)# local address 115.0.0.1
esr(config-gre)# remote address 114.0.0.10
```

Specify tunnel IP address 25.0.0.1/24:

```
esr(config-gre)# ip address 25.0.0.1/24
```

Also, the tunnel should belong to the security zone in order to create rules that allow traffic to pass through the firewall. To define the tunnel inheritance to a zone, use the following command:

```
esr(config-gre)# security-zone untrusted
```

Enable tunnel:

```
esr(config-gre)# enable
esr(config-gre)# exit
```

Create route to the partner's local area network on the router. Specify previously created GRE tunnel as a destination interface.

```
esr(config)# ip route 172.16.0.0/16 tunnel gre 10
```

When settings are applied, traffic will be encapsulated into the tunnel and sent to the partner regardless of their GRE tunnel existence and settings validity.

Alternatively, you may specify the following parameters for GRE tunnel:

- Enable GRE header checksum calculation and inclusion into a packet with encapsulated packet for outbound traffic:


```
esr(config-gre)# local checksum
```
- Enable check for GRE checksum presence and validity for inbound traffic:


```
esr(config-gre)# remote checksum
```


- Specify a unique identifier:

```
esr(config-gre)# key 15808
```
- Specify DSCP, MTU, TTL values:

```
esr(config-gre)# dscp 44
esr(config-gre)# mtu 1426
esr(config-gre)# ttl 18
```
- Enable and configure keepalive mechanism:

```
esr(config-gre)# keepalive enable
esr(config-gre)# keepalive timeout <TIME>
esr(config-gre)# keepalive retries <VALUE>
```

To view the tunnel status, use the following command:

```
esr# show tunnels status gre 10
```

To view sent and received packet counters, use the following command:

```
esr# show tunnels counters gre 10
```

To view the tunnel configuration, use the following command:

```
esr# show tunnels configuration gre 10
```

IPv4-over-IPv4 tunnel configuration is performed in the same manner.



During tunnel creation, you should enable GRE protocol (47) in the firewall.

7.25 L2TPv3 tunnel configuration

L2TPv3 (Layer 2 Tunneling Protocol Version 3) is a protocol used for tunneling of 2nd level OSI model packets between two IP nodes. IP or UDP is used as an encapsulation protocol. L2TPv3 may be used as an alternative to MPLS P2P L2VPN (VLL) for L2 VPN establishment. In ESR router implemented static unmanageable L2TPv3 tunnels, i.e. tunnels are created manually via configuration on local and remote hosts. Tunnel parameters for each side should be mutually agreeable, otherwise transferred data will not be decapsulated by the partner.

7.25.1 Configuration algorithm

Step	Description	Command	Keys
1	Configure L3 interface from which a L2TPv3 tunnel will be built.		
2	Create a L2TPv3 tunnel and switch to its configuration mode.	<pre>esr(config)# tunnel l2tpv3 <INDEX></pre>	<INDEX> – tunnel identifier in the range of: for esr100/200 – [1..250], for esr1000/1200/1700 - [1..500]
3	Specify the description of the configured tunnel (optionally).	<pre>esr(config-l2tpv3)# description <DESCRIPTION></pre>	<DESCRIPTION> – tunnel description, set by the string of up to 255 characters.
4	Specify VRF instance, in which the given L2TPV3 tunnel will operate (optionally).	<pre>esr(config-l2tpv3)# ip vrf forwarding <VRF></pre>	<VRF> – VRF name, set by the string of up to 31 characters.

5	Set local IP address for tunnel installation.	<code>esr(config-l2tpv3)# local address <ADDR></code>	<ADDR> – gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
6	Set remote IP address for tunnel installation.	<code>esr(config-l2tpv3)# remote address <ADDR></code>	<ADDR> – gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
7	Select encapsulation method for L2TPv3 tunnel.	<code>esr(config-l2tpv3)# protocol <TYPE></code>	<TYPE> – encapsulation type, possible values: Ip-encapsulation -encapsulation in an IP packet; Udp-encapsulation -encapsulation in UDP datagrams.
8	Set local session identifier.	<code>esr(config-l2tpv3)# local session-id <SESSION-ID></code>	<SESSION-ID> – session identifier, takes values in the range of [1..200000].
9	Set remote session identifier.	<code>esr(config-l2tpv3)# remote session-id <SESSION-ID></code>	<SESSION-ID> – session identifier, takes values in the range of [1..200000].
10	Define local UDP port (if UDP was selected as encapsulation method).	<code>esr(config-l2tpv3)# local port <UDP></code>	<UDP> – UDP port number in the range of [1..65535].
11	Define remote UDP port (if UDP was selected as encapsulation method).	<code>esr(config-l2tpv3)# remote port <UDP></code>	<UDP> – UDP port number in the range of [1..65535].
12	Assign the broadcast domain for encapsulation in the tunnel's L2TPV3 packets.	<code>esr(config-l2tpv3)# bridge-group <BRIDGE-ID></code>	<BRIDGE-ID> – bridge identifier, takes values in the range of: for esr10/12V(F) – [1..50], esr100/200 – [1..250], for esr1000/1200 – [1..500]
13	Enable the tunnel.	<code>esr(config-l2tpv3)# enable</code>	
14	Specify MTU size (MaximumTransmissionUnit) for the tunnels (optionally). MTU above 1500 will be active only when using the "system jumbo-frames" command.	<code>esr(config-l2tpv3)# mtu <MTU></code>	<MTU> – MTU value, takes values in the range of: for esr10/12V(F)/14VF – [1280..9600]; for esr100/200/1000/1200/1700 – [1280..10000]. Default value: 1500.
15	Define the local cookie value to check the conformance of data being transmitted and session (optionally).	<code>esr(config-l2tpv3)# local cookie <COOKIE></code>	<COOKIE> – COOKIE value, the parameter takes values of 8 or 16 characters in hexadecimal form.
16	Define the remote cookie value to check the conformance of data being transmitted and session (optionally).	<code>esr(config-l2tpv3)# remote cookie <COOKIE></code>	<COOKIE> – COOKIE value, the parameter takes values of 8 or 16 characters in hexadecimal form.
17	Specify the time interval during which the statistics on the tunnel load is averaged (optionally)	<code>esr(config-l2tpv3)# load-average <TIME></code>	<TIME> – interval in seconds, takes values of [5..150]. Default value: 5.

7.25.2 L2TPv3 tunnel configuration example

Objective:

Establish L2 VPN for company offices using IP network with L2TPv3 protocol for traffic tunneling.

- UDP is used as an encapsulation protocol, port number at the local side and port number at the partner's side is 519;

- IP address 21.0.0.1 is used as a local gateway for the tunnel;
- IP address 183.0.0.10 is used as a remote gateway for the tunnel;
- Tunnel identifier at the local side equals 2, at the partner's side - 3;
- Tunnel identifier inside the tunnel equals 100, at the partner's side - 200;
- Forward traffic into the tunnel from the bridge with identifier 333.

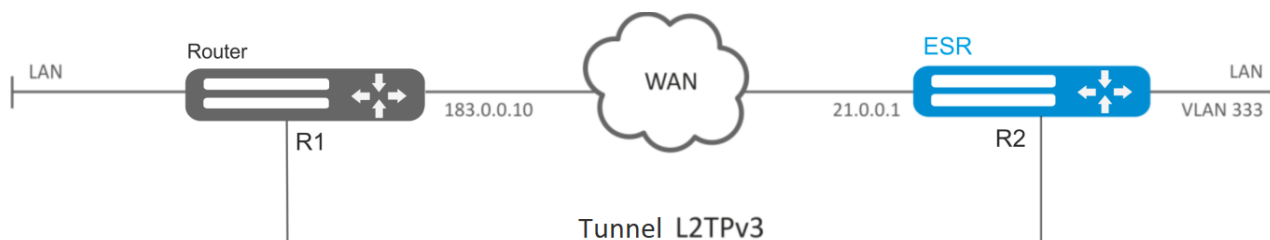


Figure 65 – Network structure

Solution:

Create L2TPv3 333 tunnel:

```
esr# configure
esr(config)# tunnel l2tpv3 333
```

Specify local and remote gateways (IP addresses of WAN border interfaces):

```
esr(config-l2tpv3)# local address 21.0.0.1
esr(config-l2tpv3)# remote address 183.0.0.10
```

Specify identifiers for session inside the tunnel for local and remote sides:

```
esr(config-l2tpv3)# protocol udp
esr(config-l2tpv3)# local port 519
esr(config-l2tpv3)# remote port 519
```

Specify tunnel identifiers for local and remote sides:

```
esr(config-l2tpv3)# local session-id 100
esr(config-l2tpv3)# remote session-id 200
```

Define the inheritance of L2TPv3 tunnel to a bridge that should be mapped to remote office network (for bridge configuration, see Section 7.18.2):

```
esr(config-l2tpv3)# bridge-group 333
```

Enable previously created tunnel and exit:

```
esr(config-l2tpv3)# enable
esr(config-l2tpv3)# exit
```

Create sub-interface for switching of traffic coming from the tunnel into LAN with VLAN id 333:

```
esr(config)# interface gi 1/0/2.333
```

Define the inheritance of sub-interface to a bridge that should be mapped to LAN (for bridge configuration, see Section 7.17):

```
esr(config-subif)# bridge-group 333
```

```
esr(config-subif)# exit
```

When settings are applied, traffic will be encapsulated into the tunnel and sent to the partner regardless of their L2TPv3 tunnel existence and settings validity.

Tunnel settings for the remote office should mirror local ones. IP address 183.0.0.10 should be used as a local gateway. IP address 21.0.0.1 should be used as a remote gateway for the tunnel. Encapsulation protocol port number at the local side should be 520, at the partner's side – 519. Session identifier inside the tunnel should be equal to 200, at the partner's side – 100. Also, the tunnel should belong to a bridge that should be connected with the partner's network.

To view the tunnel status, use the following command:

```
esr# show tunnels status l2tpv3 333
```

To view sent and received packet counters, use the following command:

```
esr# show tunnels counters l2tpv3 333
```

To view the tunnel configuration, use the following command:

```
esr# show tunnels configuration l2tpv3 333
```



In addition to tunnel creation, you should enable UDP inbound traffic in the firewall with source port 519 and destination port 519.

7.26 IPsec VPN configuration

IPsec is a set of protocols that enable security features for data transferred via IP protocol. This set of protocols allows for identity validation (authentication), IP packet integrity check and encryption, and also includes protocols for secure key exchange over the Internet.

7.26.1 Route-based IPsec VPN configuration

7.26.1.1 Configuration algorithm

Step	Description	Command	Keys
1	Create a VTI tunnel and switch to its configuration mode.	<code>esr(config)# tunnel vti <TUN></code>	<TUN> – device tunnel name.
2	Specify the local IP address of the VTI tunnel.	<code>esr(config-vti)#local address <ADDR></code>	<ADDR> – IP address of a local gateway.
3	Specify the remote IP address of the VTI tunnel.	<code>esr(config-vti)#remote address <ADDR></code>	<ADDR> – IP address of a remote gateway.
4	Specify the IP address of the VTI tunnel local side.	<code>esr(config-vti)# ip address <ADDR/LEN></code>	<ADDR/LEN> – IP address and prefix of a subnet, defined as AAA.BBB.CCC.DDD/EE where each part AAA-DDD takes values of [0..255] and EE takes values of [1..32].
5	Include the VTI tunnel in a security zone and configure interaction rules	<code>esr(config-vti)# security-zone<NAME></code>	<NAME> – security zone name, set by the string of up to 12 characters.

	between zones or disable firewall for VTI tunnel.	<code>esr(config-vti)# ip firewall disable</code>	
6	Enable the tunnel.	<code>esr(config- vti)#enable</code>	
7	Create an IKE profile and switch to its configuration mode.	<code>esr(config)# security ike proposal <NAME></code>	<NAME> – IKE protocol name, set by the string of up to 31 characters.
8	Specify the description of the configured IKE profile (optionally).	<code>esr(config-ike- proposal)# description<DESCRIPT ION></code>	<DESCRIPTION> – tunnel description, set by the string of up to 255 characters.
9	Specify IKE authentication algorithm. (optionally)	<code>esr(config-ike- proposal)# authentication algorithm <ALGORITHM></code>	<ALGORITHM> – authentication algorithm, takes values of: md5, sha1, sha2-256, sha2-384, sha2-512. Default value: sha1
10	Specify IKE encryption algorithm. (optionally)	<code>esr(config-ike- proposal)# encryption algorithm <ALGORITHM></code>	<ALGORITHM> – encryption protocol, takes the following values: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. Default value: 3des
10	Define Diffie-Hellman group number. (optionally)	<code>esr(config-ike- proposal)# dh-group <DH-GROUP></code>	<DH-GROUP> – Diffie-Hellman group number, takes values of [1, 2, 5, 14, 15, 16, 17, 18]. Default value: 1
11	Specify IKE authentication mode. (optionally)	<code>esr(config-ike- proposal)# authentication method <METHOD></code>	<METHOD> – key authentication method. May take the following values: pre-shared-key – authentication method using pre-received encryption keys; rsa-public-key – authentication method using RSA certificate. Default value: pre-shared-key
12	Create an IKE policy and switch to its configuration mode.	<code>esr(config)# security ike policy <NAME></code>	<NAME> – IKE policy name, set by the string of up to 31 characters.
13	Specify the lifetime of IKE protocol connection (optionally).	<code>esr(config-ike- proposal)# lifetime seconds <SEC></code>	<SEC> – time interval, takes values of [4..86400] seconds. Default value: 3600
14	Bind IKE profile to IKE policy.	<code>esr(config-ike- policy)# proposal <NAME></code>	<NAME> – IKE protocol name, set by the string of up to 31 characters.
15	Specify authentication key. (mandatorily if pre-shared-key is selected as authentication mode)	<code>esr(config-ike- policy)# pre-shared- key ascii-text<TEXT></code>	<TEXT> – string [1..64] ASCII characters.
16	Create an IKE gateway and switch to its configuration mode.	<code>esr(config)# security ike gateway <NAME></code>	<NAME> – IKE protocol gateway name, set by the string of up to 31 characters.
17	Bind IKE policy to IKE gateway.	<code>esr(config-ike-gw)# ike-policy <NAME></code>	<NAME> – IKE protocol policy name, set by the string of up to 31 characters.
18	Specify IKE version (optionally).	<code>esr(config-ike-gw)# version <VERSION></code>	<version> – IKE protocol version: v1-only or v2-only. Default value: v1-only
19	Set the route-based mode.	<code>esr(config-ike-gw)# mode - route-based</code>	

20	Specify the action for DPD (optionally).	<code>esr(config-ike-gw)# dead-peer-detection action <MODE></code>	<MODE> – DPD operation mode: restart – connection is being restarted; clear – connection is being cleared; hold – connection is being held; none – mechanism is disabled, no actions are taken. Default value: none
21	Specify the interval between sending messages via DPD mechanism (optionally).	<code>esr(config-ike-gw)# dead-peer-detection interval <SEC></code>	<SEC> – interval between sending messages via DPD mechanism, takes values of [1..180] seconds. Default value: 2
22	Specify the time period of response to DPD mechanism messages (optionally).	<code>esr(config-ike-gw)# dead-peer-detection timeout <SEC></code>	<SEC> – time interval of response to DPD mechanism messages, takes values of [1..180] seconds. Default value: 30 seconds
23	Bind VTI tunnel to IKE gateway.	<code>esr(config-ike-gw)# bind-interface vti <VTI></code>	<VTI> – VTI ID.
24	Create IPsec profile.	<code>esr(config)# security ipsec proposal <NAME></code>	<NAME> – IPsec protocol profile name, set by the string of up to 31 characters.
25	Specify IPsec authentication algorithm. (optionally)	<code>esr(config-ipsec- proposal)# authentication algorithm <ALGORITHM></code>	<ALGORITHM> – authentication algorithm, takes values of: md5, sha1, sha2-256, sha2-384, sha2-512. Default value: sha1
26	Specify IPsec encryption algorithm. (optionally)	<code>esr(config-ipsec- proposal)# encryption algorithm <ALGORITHM></code>	<ALGORITHM> – encryption protocol, takes the following values: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. Default value: 3des
27	Specify encapsulation protocol for IPsec (optionally).	<code>esr(config-ipsec- proposal)# protocol <PROTOCOL></code>	<PROTOCOL> – encapsulation protocol, takes the following values: esp, ah Default value: esp
28	Create an IPsec policy and switch to its configuration mode.	<code>esr(config)# security ipsec policy <NAME></code>	<NAME> – IPsec policy name, set by the string of up to 31 characters.
29	Bind IPsec profile to IPsec policy.	<code>esr(config-ipsec- policy)# proposal <NAME></code>	<NAME> – IPsec protocol profile name, set by the string of up to 31 characters.

30	Specify the lifetime of IPsec tunnel (optionally).	<code>esr(config-ipsec-policy)# lifetime { seconds <SEC> packets <PACKETS> kilobytes <KB> }</code>	<p><SEC> – IPsec tunnel lifetime after which the re-approval is carried out. Takes values in the range of [1140..86400] seconds.</p> <p><PACKETS> – number of packets after transmitting of which the IPsec tunnel re-approval is carried out. Takes values in the range of [4..86400].</p> <p><KB> – traffic amount after transmitting of which the IPsec tunnel re-approval is carried out. Takes values in the range of [4..86400] seconds. Default value: 28800 seconds</p>
31	Create IPsec VPN policy and switch to its configuration mode.	<code>esr(config)# security ipsecvpn <NAME></code>	<NAME> – VPN name, set by the string of up to 31 characters.
32	Define the matching mode of data required for VPN enabling.	<code>esr(config-ipsec-vpn)# mode <MODE></code>	<MODE> – VPN operation mode.
33	Bind IPsec policy to IPsec VPN.	<code>esr(config-ipsec-vpn)# ike ipsec-policy <NAME></code>	<NAME> – IPsec policy name, set by the string of up to 31 characters.
34	Set the DSCP value for the use in IP headers of IKE outgoing packets (optionally).	<code>esr(config-ipsec-vpn)# ike dscp <DSCP></code>	<DSCP> – DSCP code value, takes values in the range of [0..63]. Default value: 63
34	Set VPN activation mode.	<code>esr(config-ipsec-vpn)# ike establish-tunnel <MODE></code>	<p><MODE> – VPN activation mode:</p> <ul style="list-style-type: none"> by-request – connection is enabled by an opposing party; route – connection is enabled when there is traffic routed to the tunnel; immediate – tunnel is enabled automatically after applying the configuration.
36	Bind IKE gateway to IPsec VPN.	<code>esr(config-ipsec-vpn)# ike gateway <NAME></code>	<NAME> – IKE gateway name, set by the string of up to 31 characters.
37	Set the time interval value in seconds after which the connection is closed, if no packet has been received or sent via SA (optionally).	<code>esr(config-ipsec-vpn)# ike idle-time <TIME></code>	<TIME> – interval in seconds, takes values of [4..86400].
38	Disable key re-approval before the IKE connection is lost due to the timeout, the number of transmitted packets or bytes (optionally).	<code>esr(config-ipsec-vpn)# ike rekey disable</code>	

39	Configure the start of IKE connection keys re-approval before the expiration of the lifetime (optionally).	<code>esr(config-ipsec-vpn)# ike rekey margin { seconds <SEC> packets <PACKETS> kilobytes <KB> }</code>	<p><SEC> – time interval in seconds remaining before the connection release (set by the <code>lifetimeseconds</code> command, see 22.2.13). Takes values in the range of [4..86400].</p> <p><PACKETS> – number of packets remaining before the connection release (set by the <code>lifetimepackets</code> command). Takes values in the range of [4..86400].</p> <p><KB> – traffic volume in kilobytes remaining before the connection release (set by the <code>lifetimekilobytes</code> command). Takes values in the range of [4..86400].</p> <p>Default value:</p> <ul style="list-style-type: none"> - Keys re-approval before the expire of time – 540 seconds before. - Keys re-approval before the expire of traffic volume and amount of packets – disabled.
40	Set the level of margin seconds, margin packets, margin kilobytes values random spread (optionally).	<code>esr(config-ipsec-vpn)# ike rekey randomization <VALUE></code>	<p><VALUE> – maximum ratio of values spread, takes values of [1..100].</p> <p>Default value: 100%</p>
41	Specify the description for IPsec-VPN (optionally).	<code>esr(config-ipsec-vpn)# description <DESCRIPTION></code>	<p><DESCRIPTION> – profile description, set by the string of up to 255 characters.</p>
42	Enable IPsec VPN.	<code>esr(config-ipsec-vpn)# enable</code>	

7.26.1.2 Configuration example

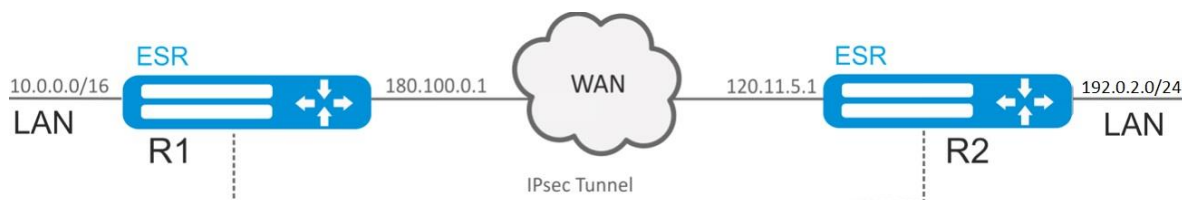


Figure 66 – Network structure

Objective:

Configure IPsec tunnel between R1 and R2.

- R1 IP address: 120.11.5.1;
- R2 IP address: 180.100.0.1;

IKE:

- Diffie-Hellman group: 2;
- encryption algorithm: AES 128 bit;
- authentication algorithm: MD5.

IPsec:

- encryption algorithm: AES 128 bit;

- authentication algorithm: MD5.

Solution:

1. R1 configuration

Configure external network interface and identify its inheritance to a security zone:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if-gi)# ip address 180.100.0.1/24
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# exit
```

Create VTI tunnel. Traffic will be routed via VTI into IPsec tunnel. Specify IP addresses of WAN border interfaces as local and remote gateways:

```
esr(config)# tunnel vti 1
esr(config-vti)# local address 180.100.0.1
esr(config-vti)# remote address 120.11.5.1
esr(config-vti)# enable
esr(config-vti)# exit
```

To configure security zones rules, you should create ISAKMP port profile:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# exit
```

Create a static route to the remote LAN. For each subnet located beyond the Ipsec tunnel, specify a route via VTI tunnel:

```
esr(config)# ip route 192.0.2.0/24 tunnel vti 1
```

Create IKE protocol profile. Select Diffie-Hellman group 2, AES 128 bit encryption algorithm and MD5 authentication algorithm in the profile. The given security parameters are used for IKE connection protection:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
```

Create IKE protocol policy. For the policy, specify the list of IKE protocol profiles that may be used for node and authentication key negotiation:

```
esr(config)# security ike policy ike_poll1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Create IKE protocol gateway. For this profile, specify VTI tunnel, policy, protocol version and mode of traffic redirection into the tunnel.

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_poll1
esr(config-ike-gw)# mode route-based
esr(config-ike-gw)# bind-interface vti 1
esr(config-ike-gw)# version v2-only
```

```
esr(config-ike-gw)# exit
```

Create security parameters profile for IPsec tunnel. For the profile, select Diffie-Hellman group 2, AES 128 bit encryption algorithm and MD5 authentication algorithm. Use the following parameters to secure IPsec tunnel:

```
esr(config)# security ipsec proposal ipsec_prop1  
esr(config-ipsec-proposal)# authentication algorithm md5  
esr(config-ipsec-proposal)# encryption algorithm aes128  
esr(config-ipsec-proposal)# exit
```

Create a policy for IPsec tunnel. For the policy, specify the list of IPsec tunnel profiles that may be used for node negotiation:

```
esr(config)# security ipsec policy ipsec_poll  
esr(config-ipsec-policy)# proposal ipsec_prop1  
esr(config-ipsec-policy)# exit
```

Create IPsec VPN. For VPN, specify IKE protocol gateway, IPsec tunnel policy, key exchange mode and connection establishment method. When all parameters are entered, enable tunnel using enable command.

```
esr(config)# security ipsec vpn ipsec1  
esr(config-ipsec-vpn)# mode ike  
esr(config-ipsec-vpn)# ike establish-tunnel immediate  
esr(config-ipsec-vpn)# ike gateway ike_gw1  
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_poll  
esr(config-ipsec-vpn)# enable  
esr(config-ipsec-vpn)# exit  
esr(config)# exit
```

2. R2 configuration

Configure external network interface and identify its inheritance to a security zone:

```
esr# configure  
esr(config)# interface gi 1/0/1  
esr(config-if)# ip address 120.11.5.1/24  
esr(config-if)# security-zone untrusted  
esr(config-if)# exit
```

Create VTI tunnel. The traffic will be redirected through VTI to IPsec tunnel. Specify IP addresses of WAN border interfaces as local and remote gateways:

```
esr(config)# tunnel vti 1  
esr(config-vti)# remote address 180.100.0.1  
esr(config-vti)# local address 120.11.5.1  
esr(config-vti)# enable  
esr(config-vti)# exit
```

To configure security zones rules, create ISAKMP port profile:

```
esr(config)# object-group service ISAKMP  
esr(config-object-group-service)# port-range 500  
esr(config-object-group-service)# exit
```

Create a static route to a remote LAN. For each subnet located beyond the IPsec tunnel, specify a route via VTI tunnel:

```
esr(config)# ip route 10.0.0.0/16 tunnel vti 1
```

Create IKE protocol profile. Select Diffie-Hellman group 2, AES 128 bit encryption algorithm and MD5 authentication algorithm in the profile. The given security parameters are used for IKE connection protection:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
esr(config)#
```

Create IKE protocol policy. For the policy, specify the list of IKE protocol profiles that may be used for node and authentication key negotiation:

```
esr(config)# security ike policy ike_poll
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Create IKE protocol gateway. For this profile, specify VTI tunnel, policy, protocol version and mode of traffic redirection into the tunnel.

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_poll
esr(config-ike-gw)# mode route-based
esr(config-ike-gw)# bind-interface vti 1
esr(config-ike-gw)# version v2-only
esr(config-ike-gw)# exit
```

Create security parameters profile for IPsec tunnel. For the profile, select Diffie-Hellman group 2, AES 128 bit encryption algorithm and MD5 authentication algorithm. Use the following parameters to secure IPsec tunnel:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Create a policy for IPsec tunnel. For the policy, specify the list of IPsec tunnel profiles that may be used for node negotiation:

```
esr(config)# security ipsec policy ipsec_poll
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit
```

Create IPsec VPN. For VPN, specify IKE protocol gateway, IPsec tunnel policy, key exchange mode and connection establishment method. When all parameters are entered, enable tunnel using enable command.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
```

```

esr(config-ipsec-vpn) # ike establish-tunnel immediate
esr(config-ipsec-vpn) # ike gateway ike_gw1
esr(config-ipsec-vpn) # ike ipsec-policy ipsec_poll
esr(config-ipsec-vpn) # enable
esr(config-ipsec-vpn) # exit
esr(config) # exit

```

To view the tunnel status, use the following command:

```
esr# show security ipsec vpn status ipsec1
```

To view the tunnel configuration, use the following command:

```
esr# show security ipsec vpn configuration ipsec1
```



In the firewall, you should enable ESP and ISAKMP protocol (UDP port 500).

7.26.2 Policy-based IPsec VPN configuration

7.26.2.1 Configuration algorithm

Step	Description	Command	Keys
1	Create an IKE instance and switch to its configuration mode.	<code>esr(config)# security ike proposal <NAME></code>	<NAME> – IKE protocol name, set by the string of up to 31 characters.
2	Specify the description of the configured tunnel (optionally).	<code>esr(config-ike-proposal)# description<DESCRIPTION></code>	<DESCRIPTION> – tunnel description, set by the string of up to 255 characters.
3	Specify IKE authentication algorithm.	<code>esr(config-ike-proposal)# authentication algorithm <ALGORITHM></code>	<ALGORITHM> – authentication algorithm, takes values of: md5, sha1, sha2-256, sha2-384, sha2-512.
4	Specify IKE encryption algorithm.	<code>esr(config-ike-proposal)# encryption algorithm <ALGORITHM></code>	<ALGORITHM> – encryption protocol, takes the following values: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.
5	Define Diffie-Hellman group number.	<code>esr(config-ike-proposal)# dh-group <DH-GROUP></code>	<DH-GROUP> – Diffie-Hellman group number, takes values of [1, 2, 5, 14, 15, 16, 17, 18].
6	Specify the authentication mode.	<code>esr(config-ike-proposal)# authentication method <METHOD></code>	<METHOD> – key authentication method. May take the following values: pre-shared-key – authentication method using pre-received encryption keys; rsa-public-key – authentication method using RSA certificate.
7	Create an IKE profile policy and switch to its configuration mode.	<code>esr(config)# security ike policy <NAME></code>	<NAME> – IKE policy name, set by the string of up to 31 characters.

8	Specify the lifetime of IKE protocol connection (optionally).	<code>esr(config-ike-proposal)# lifetime seconds <SEC></code>	<SEC> – time interval, takes values of [4..86400] seconds.
9	Bind the policy to profile.	<code>esr(config-ike-policy)# proposal <NAME></code>	<NAME> – IKE protocol name, set by the string of up to 31 characters.
10	Specify authentication key.	<code>esr(config-ike-policy)# pre-shared-key ascii-text<TEXT></code>	<TEXT> – string [1..64] ASCII characters.
11	Create an IKE gateway and switch to its configuration mode.	<code>esr(config)# security ike gateway <NAME></code>	<NAME> – IKE protocol gateway name, set by the string of up to 31 characters.
12	Bind IKE policy.	<code>esr(config-ike-gw)# ike-policy <NAME></code>	<NAME> – IKE protocol policy name, set by the string of up to 31 characters.
13	Specify IKE version (optionally).	<code>esr(config-ike-gw)# version <VERSION></code>	<version> – IKE protocol version: v1-only or v2-only .
14	Set the mode of traffic redirection into the tunnel.	<code>esr(config-ike-gw)# mode<MODE></code>	<MODE> – mode of traffic redirection into the tunnel, takes the following values: policy-based – traffic is redirected on the basis of its inherence to the subnets specified in policies; route-based – traffic is redirected on the basis of the routes with tunnel interface as a gateway.
15	Specify the action for DPD (optionally).	<code>esr(config-ike-gw)# dead-peer-detection action <MODE></code>	<MODE> – DPD operation mode: restart – connection is being restarted; clear – connection is being cleared; hold – connection is being held; none – mechanism is disabled, no actions are taken.
16	Specify the interval between sending messages via DPD mechanism (optionally).	<code>esr(config-ike-gw)# dead-peer-detection interval <SEC></code>	<SEC> – interval between sending messages via DPD mechanism, takes values of [1..180] seconds.
17	Specify the time period of response to DPD mechanism messages (optionally).	<code>esr(config-ike-gw)# dead-peer-detection timeout <SEC></code>	<SEC> – time interval of response to DPD mechanism messages, takes values of [1..180] seconds.
18	Specify IKE version (optionally).	<code>esr(config-ike-gw)# version <VERSION></code>	<version> – IKE protocol version: v1-only or v2-only .

19	Set sender's IP subnets.	<code>esr(config-ike-gw)# local network <ADDR/LEN> [protocol { <TYPE> <ID> } [port <PORT>]]</code>	<ADDR/LEN> – subnet IP address and mask of a sender. The parameter is defined as AAA.BBB.CCC.DDD/EE where each part AAA-DDD takes values of [0..255] and EE takes values of [1..32]; <TYPE> – protocol type, takes the following values: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre; <ID> – IP ID, takes values of [0x00-0xFF]; <PORT> – TCP/UDP port, takes values of [1..65535].
20	Specify the IP address of IPsec tunnel local gateway.	<code>esr(config-ike-gw)#local address <ADDR></code>	<ADDR> – IP address of a local gateway.
21	Specify the IP address of IPsec tunnel remote gateway.	<code>esr(config-ike-gw)#remote address <ADDR></code>	<ADDR> – IP address of a remote gateway.
22	Set receiver's subnet IP address as well as IP and port.	<code>esr(config-ike-gw)# remote network <ADDR/LEN> [protocol { <TYPE> <ID> } [port <PORT>]]</code>	<ADDR/LEN> – subnet IP address and mask of a sender. The parameter is defined as AAA.BBB.CCC.DDD/EE, where each part AAA – DDD takes values of [0..255] and EE takes values of [1..32]; <TYPE> – protocol type, takes the following values: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre; <ID> – IP ID, takes values of [0x00-0xFF]; <PORT> – TCP/UDP port, takes values of [1..65535].
23	Create IPsec profile.	<code>esr(config)# security ipsec proposal <NAME></code>	<NAME> – IPsec protocol profile name, set by the string of up to 31 characters.
24	Specify IPsec authentication algorithm.	<code>esr(config-ipsec- proposal)# authentication algorithm <ALGORITHM></code>	<ALGORITHM> – authentication algorithm, takes values of: md5, sha1, sha2-256, sha2-384, sha2-512.
26	Specify IPsec encryption algorithm.	<code>esr(config-ipsec- proposal)# encryption algorithm <ALGORITHM></code>	<ALGORITHM> – encryption protocol, takes the following values: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.
26	Specify protocol (optionally).	<code>esr(config-ipsec- proposal)# protocol <PROTOCOL></code>	<PROTOCOL> – encapsulation protocol, takes the following values: esp, ah
27	Create an IPsec profile policy and switch to its configuration mode.	<code>esr(config)# security ipsec policy <NAME></code>	<NAME> – IPsec policy name, set by the string of up to 31 characters.
28	Bind the policy to profile.	<code>esr(config-ipsec- policy)# proposal <NAME></code>	<NAME> – IPsec protocol profile name, set by the string of up to 31 characters.

29	Specify the lifetime of IPsec tunnel (optionally).	<code>esr(config-ipsec-policy)# lifetime { seconds <SEC> packets <PACKETS> kilobytes <KB> }</code>	<SEC> – IPsec tunnel lifetime after which the re-approval is carried out. Takes values in the range of [1140..86400] seconds. <PACKETS> – number of packets after transmitting of which the IPsec tunnel re-approval is carried out. Takes values in the range of [4..86400]. <KB> – traffic amount after transmitting of which the IPsec tunnel re-approval is carried out. Takes values in the range of [4..86400] seconds.
30	Create IPsec VPN policy and switch to its configuration mode.	<code>esr(config)# security ipsecvpn <NAME></code>	<NAME> – VPN name, set by the string of up to 31 characters.
31	Define the matching mode of data required for VPN enabling.	<code>esr(config-ipsec-vpn)# mode <MODE></code>	<MODE> – VPN operation mode.
32	Bind IPsec policy to VPN.	<code>esr(config-ipsec-vpn)#ike ipsec-policy <NAME></code>	<NAME> – IPsec policy name, set by the string of up to 31 characters.
33	Set the DSCP value for the use in IP headers of IKE outgoing packets (optionally).	<code>esr(config-ipsec-vpn)#ike dscp <DSCP></code>	<DSCP> – DSCP code value, takes values in the range of [0..63].
34	Set VPN activation mode.	<code>esr(config-ipsec-vpn)#ike establish-tunnel <MODE></code>	<MODE> – VPN activation mode: by-request – connection is enabled by an opposing party; route – connection is enabled when there is traffic routed to the tunnel; immediate – tunnel is enabled automatically after applying the configuration.
35	Bind IKE gateway to VPN.	<code>esr(config-ipsec-vpn)# ike gateway <NAME></code>	<NAME> – IKE gateway name, set by the string of up to 31 characters.
36	Set the time interval value in seconds after which the connection is closed, if no packet has been received or sent via SA (optionally).	<code>esr(config-ipsec-vpn)# ike idle-time <TIME></code>	<TIME> – interval in seconds, takes values of [4..86400].
37	Disable key re-approval before the IKE connection is lost due to the timeout, the number of transmitted packets or bytes (optionally).	<code>esr(config-ipsec-vpn)# ike rekey disable</code>	
38	Configure the start of IKE connection keys re-approval before the expiration of the lifetime (optionally).	<code>esr(config-ipsec-vpn)# ike rekey margin { seconds <SEC> packets <PACKETS> kilobytes <KB> }</code>	<SEC> – time interval in seconds remaining before the connection release (set by the <code>lifetimeseconds</code> command). Takes values in the range of [4..86400]. <PACKETS> – number of packets remaining before the connection release (set by the <code>lifetimepackets</code> command). Takes values in the range of [4..86400]. <KB> – traffic volume in kilobytes remaining before the connection release (set by the <code>lifetimekilobytes</code> command). Takes values in the range of [4..86400].

39	Set the level of margin seconds, margin packets, margin kilobytes values random spread (optionally).	<code>esr(config-ipsec-vpn)# ike rekey randomization <VALUE></code>	<VALUE> – maximum ratio of values spread, takes values of [1..100].
40	Describe VPN (optionally).	<code>esr(config-ipsec-vpn)# description <DESCRIPTION></code>	<DESCRIPTION> – profile description, set by the string of up to 255 characters.
41	Enable IPsec VPN.	<code>esr(config-ipsec-vpn)# enable</code>	

7.26.2.2 Configuration example

Objective:

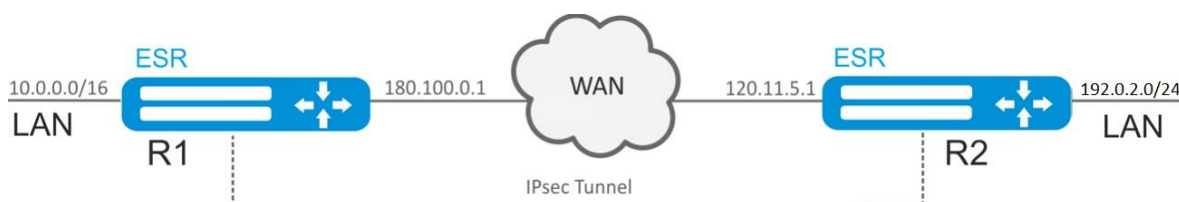


Figure 67 – Network structure

Configure IPsec tunnel between R1 and R2.

R1 IP address: 120.11.5.1;

R2 IP address: 180.100.0.1;

IKE:

- Diffie-Hellman group: 2;
- encryption algorithm: AES 128 bit;
- authentication algorithm: MD5.

IPsec:

- encryption algorithm: AES 128 bit;
- authentication algorithm: MD5.

Solution:

1. R1 configuration

Configure external network interface and identify its inheritance to a security zone:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 120.11.5.1/24
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# exit
```

To configure security zones rules, you should create ISAKMP port profile:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# exit
```


Create IKE protocol profile. Select Diffie-Hellman group 2, AES 128 bit encryption algorithm and MD5 authentication algorithm in the profile. The given security parameters are used for IKE connection protection:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
```

Create IKE protocol policy. For the policy, specify the list of IKE protocol profiles that may be used for node and authentication key negotiation:

```
esr(config)# security ike policy ike_poll
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Create IKE protocol gateway. For this profile, specify VTI tunnel, policy, protocol version and mode of traffic redirection into the tunnel.

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_poll
esr(config-ike-gw)# local address 180.100.0.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address 120.11.5.1
esr(config-ike-gw)# remote network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

Create security parameters profile for IPsec tunnel. For the profile, select Diffie-Hellman group 2, AES 128 bit encryption algorithm and MD5 authentication algorithm. Use the following parameters to secure IPsec tunnel:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Create a policy for IPsec tunnel. For the policy, specify the list of IPsec tunnel profiles that may be used for node negotiation:

```
esr(config)# security ipsec policy ipsec_poll
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit
```

Create IPsec VPN. For VPN, specify IKE protocol gateway, IPsec tunnel policy, key exchange mode and connection establishment method. When all parameters are entered, enable tunnel using enable command.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel immediate
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_poll
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

2. R2 configuration

Configure external network interface and identify its inheritance to a security zone:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit
```

To configure security zones rules, you should create ISAKMP port profile:

```
esr(config)# object-group service ISAKMP
esr(config-addr-set)# port-range 500
esr(config-addr-set)# exit
```

Create IKE protocol profile. Select Diffie-Hellman group 2, AES 128 bit encryption algorithm and MD5 authentication algorithm in the profile. The given security parameters are used for IKE connection protection:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
esr(config)#
```

Create IKE protocol policy. For the policy, specify the list of IKE protocol profiles that may be used for node and authentication key negotiation:

```
esr(config)# security ike policy ike_poll
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Create IKE protocol gateway. For this profile, specify VTI tunnel, policy, protocol version and mode of traffic redirection into the tunnel.

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_poll
esr(config-ike-gw)# remote address 180.100.0.1
esr(config-ike-gw)# remote network 10.0.0.0/16
esr(config-ike-gw)# local address 120.11.5.1
esr(config-ike-gw)# local network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

Create security parameters profile for IPsec tunnel. For the profile, select Diffie-Hellman group 2, AES 128 bit encryption algorithm and MD5 authentication algorithm. Use the following parameters to secure IPsec tunnel:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Create a policy for IPsec tunnel. For the policy, specify the list of IPsec tunnel profiles that may be used for node negotiation:

```
esr(config)# security ipsec policy ipsec_poll
esr(config-ipsec-policy)# proposal ipsec_prop1
```

```
esr(config-ipsec-policy)# exit
```

Create IPsec VPN. For VPN, specify IKE protocol gateway, IPsec tunnel policy, key exchange mode and connection establishment method. When all parameters are entered, enable tunnel using enable command.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel immediate
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

To view the tunnel status, use the following command:

```
esr# show security ipsec vpn status ipsec1
```

To view the tunnel configuration, use the following command:

```
esr# show security ipsec vpn configuration ipsec1
```



In the firewall, you should enable ESP and ISAKMP protocol (UDP port 500).

7.27 LT tunnels configuration

LT (logical tunnel) is a type of tunnels dedicated for transmission of routing information and traffic between different virtual routers (VRF Lite) configured on a router. LT-tunnel might be used for organization of interaction between two or more VRF using firewall restrictions.

7.27.1 Configuration algorithm

Step	Description	Command	Keys
1	Create LT tunnels for each of existing VRF.	<code>esr(config)# tunnel lt <ID></code>	<ID> – tunnel identifier, set in the range of [1..128].
2	Specify the description of the configured tunnels (optionally).	<code>esr(config-lt)# description <DESCRIPTION></code>	<DESCRIPTION> – tunnel description, set by the string of up to 255 characters.
3	Include each LT tunnel in the corresponding VFR.	<code>esr(config-lt)# ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.
4	Include each LT tunnel in a security zone and configure interaction rules between zones or disable firewall for LT tunnel.	<code>esr(config-lt)# security-zone<NAME></code>	<NAME> – security zone name, set by the string of up to 12 characters.
		<code>esr(config-lt)# ip firewall disable</code>	
5	For each LT tunnel, set the opposite LT tunnel number (in another VRF).	<code>esr(config-lt)# peer lt <ID></code>	<ID> – tunnel identifier, set in the range of [1..128].
6	For each LT tunnel, specify IP address for packets routing. For interacting LT tunnels, IP addresses should locate in one IP subnet.	<code>esr(config-lt)# ip address <ADDR/LEN></code>	<ADDR/LEN> – IP address and prefix of a subnet, defined as AAA.BBB.CCC.DDD/EE where each part AAA-DDD takes values of [0..255] and EE takes values of [1..32].

7	Enable the tunnels.	<code>esr(config-lt)#enable</code>	
8	For each VRF configure required routing protocols via LT tunnel.		
9	Specify the time interval during which the statistics on the tunnel load is averaged (optionally)	<code>esr(config-lt)# load-average <TIME></code>	<TIME> – interval in seconds, takes values of [5..150]. Default value: 5
10	Specify the size of MTU packets that can be passed by the bridge (optionally; possible if only VLAN is included in the bridge). MTU above 1500 will be active only when using the "system jumbo-frames" command.	<code>esr(config-lt)# mtu <MTU></code>	<MTU> – MTU value, takes values in the range of: for esr-10/12V(F)/14VF [552..9600]; for esr-100/200/1000/1200/1700 – [552..10000].

7.27.2 Configuration example

Objective: Organize interaction between hosts terminated in two VRF vrf_1 and vrf_2.

Initial configuration:

```
hostname esr
ip vrf vrf_1
exit
ip vrf vrf_2
exit

interface gigabitethernet 1/0/1
  ip vrf forwarding vrf_1
  ip firewall disable
  ip address 10.0.0.1/24
exit
interface gigabitethernet 1/0/2
  ip vrf forwarding vrf_2
  ip firewall disable
  ip address 10.0.1.1/24
exit
```

Solution:

Create LT tunnels for each VRF, specifying IP address from one subnet:

```
esr(config)# tunnel lt 1
esr(config-lt)# ip vrf forwarding vrf_1
esr(config-lt)# ip firewall disable
esr(config-lt)# ip address 192.168.0.1/30
esr(config-lt)# exit
esr(config)# tunnel lt 2
esr(config-lt)# ip vrf forwarding vrf_2
esr(config-lt)# ip firewall disable
esr(config-lt)# ip address 192.168.0.2/30
esr(config-lt)# exit
```

Designate LT tunnel from VRF, which is necessary to establish link with, for each LT tunnel and activate them.

```
esr(config)# tunnel lt 1
esr(config-lt)# peer lt 2
```

```

esr(config-lt)# enable
esr(config-lt)# exit
esr(config)# tunnel lt 2
esr(config-lt)# peer lt 1
esr(config-lt)# enable
esr(config-lt)# exit

```



If NONE of dynamic routing protocols works in VRF, specify static routes for each VRF:

```

esr(config)# ip route vrf vrf_1 0.0.0.0/0 192.168.0.2
esr(config)# ip route vrf vrf_2 0.0.0.0/0 192.168.0.1

```

7.28 Configuring remote access to corporate network via PPTP protocol

PPTP (Point-to-Point Tunneling Protocol) is a point-to-point tunneling protocol that allows a computer to establish secure connection with a server by creating a special tunnel in a common unsecured network. PPTP encapsulates PPP frames into IP packets for transmission via global IP network, e.g. the Internet. PPTP may be used for tunnel establishment between two local area networks. PPTP uses an additional TCP connection for tunnel handling.

7.28.1 Configuration algorithm

Step	Description	Command	Keys
1	Create PPTP server profile.	<code>esr(config)# remote-access pptp <NAME></code>	<NAME> – PPTP server profile name, set by the string of up to 31 characters.
2	Select PPTP clients authentication mode.	<code>esr(config-pptp-server)# authentication mode { local radius }</code>	local – user authentication by local base radius – user authentication by RADIUS server base.
3	Specify the description of the configured server (optionally).	<code>esr(config-pptp-server)# description <DESCRIPTION></code>	<DESCRIPTION> – PPTP server description, set by the string of up to 255 characters.
4	Define the list of DNS servers that will be used by remote users (optionally).	<code>esr(config-pptp-server)# dns-servers object-group <OBJ-GROUP-NETWORK-NAME></code>	<OBJ-GROUP-NETWORK-NAME> – name of the IP addresses profile that includes required DNS servers addresses, set by the string of up to 31 characters.
5	Specify outgoing packets DSCP priority (optionally).	<code>esr(config-pptp-server)# dscp <DSCP></code>	<DSCP> – outgoing packets dscp priority [0..63].
6	Enable MPPE encryption for PPTP connections (optionally).	<code>esr(config-pptp-server)# encryption mppe</code>	
7	IP address of a local gateway.	<code>esr(config-pptp-server)# local-address object-group <OBJ-GROUP-NETWORK-NAME> ip-address <ADDR></code>	<OBJ-GROUP-NETWORK-NAME> – name of the IP addresses profile that includes local gateway IP address, set by the string of up to 31 characters; <ADDR> – range starting IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].

8	Specify MTU size (MaximumTransmissionUnit) for the server (optionally). MTU above 1500 will be active only when using the "system jumbo-frames" command.	<code>esr (config-pptp-server) mtu <MTU></code>	<MTU> – MTU value, takes values in the range of [1280..1500]. Default value: 1500.
9	Specify IP address that should be proceeded by PPTP server.	<code>esr (config-pptp-server) # outside-address { object-group <OBJ-GROUP-NETWORK-NAME> ip-address <ADDR> }</code>	<OBJ-GROUP-NETWORK-NAME> – name of the profile having IP address that should listened by PPTP server, set by the string of up to 31 characters; <ADDR> – range starting IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
10	Specify IP addresses list from which dynamic IP addresses are leased to remote users by PPTP.	<code>esr (config-pptp-server) # remote-address { object-group <OBJ-GROUP-NETWORK-NAME> address-range <FROM-ADDR>-<TO-ADDR> }</code>	<OBJ-GROUP-NETWORK-NAME> – name of the IP addresses profile that includes remote users IP addresses list, set by the string of up to 31 characters; <FROM-ADDR> – range starting IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <TO-ADDR> – range ending IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
11	Include the PPTP server in a security zone and configure interaction rules between zones or disable firewall.	<code>esr (config-pptp-server) # security-zone <NAME></code>	<NAME> – security zone name, set by the string of up to 31 characters.
12	Specify user name (when using local user authentication).	<code>esr (config-pptp-server) username <NAME></code>	<NAME> – user name, set by the string of up to 12 characters.
13	Set user password.	<code>esr (config-pptp-user) password ascii-text { <PASSWORD> encrypted <PASSWORD> }</code>	<PASSWORD> – user password, set by the string of up to 32 characters.
14	Enable user.	<code>esr (config-pptp-user) enable</code>	
17	Define the list of WINS servers that will be used by remote users (optionally).	<code>esr (config-pptp-server) # wins-servers object-group <OBJ-GROUP-NETWORK-NAME></code>	<OBJ-GROUP-NETWORK-NAME> – name of the IP addresses profile that includes required WINS servers addresses, set by the string of up to 31 characters.

7.28.2 PPTP server configuration example

Objective:

Configure PPTP server on a router.

- PPTP server address: 120.11.5.1;
- Gateway inside the tunnel for connecting clients: 10.10.10.1;
- IP address pool for lease: 10.10.10.5-10.10.10.25;
- DNS servers: 8.8.8.8, 8.8.8.4;
- Accounts for connection: fedor, ivan.

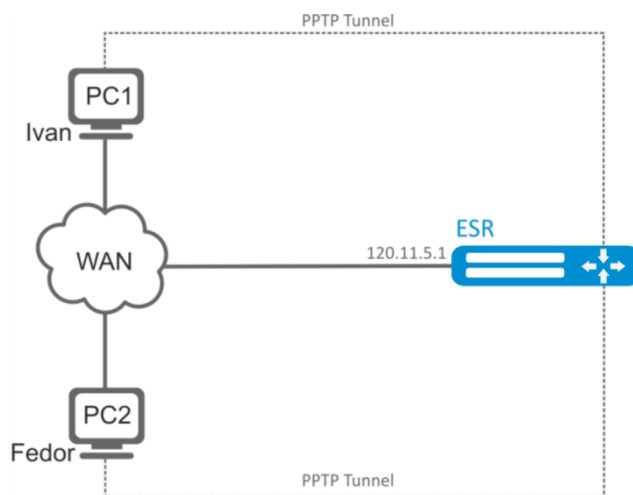


Figure 68 – Network structure

Solution:

Create an address profile that contains an address to be listened by the server:

```
esr# configure
esr(config)# object-group network pptp_outside
esr(config-object-group-network)# ip address-range 120.11.5.1
esr(config-object-group-network)# exit
```

Create address profile that contains local gateway address:

```
esr(config)# object-group network pptp_local
esr(config-object-group-network)# ip address-range 10.10.10.1
esr(config-object-group-network)# exit
```

Create address profile that contains client addresses:

```
esr(config)# object-group network pptp_remote
esr(config-object-group-network)# ip address-range 10.10.10.5-10.10.10.25
esr(config-object-group-network)# exit
```

Create address profile that contains DNS servers:

```
esr(config)# object-group network pptp_dns
esr(config-object-group-network)# ip address-range 8.8.8.8
esr(config-object-group-network)# ip address-range 8.8.4.4
esr(config-object-group-network)# exit
```

Create PPTP server and map profiles listed above:

```
esr(config)# remote-access pptp remote-workers
esr(config-pptp)# local-address object-group pptp_local
esr(config-pptp)# remote-address object-group pptp_remote
esr(config-pptp)# outside-address object-group pptp_outside
esr(config-pptp)# dns-servers object-group pptp_dns
```

Select authentication method for PPTP server users:

```
esr(config-pptp)# authentication mode local
```

Specify security zone that user sessions will be related to:

```
esr(config-pptp)# security-zone VPN
```

Create PPTP users *Ivan* and *Fedor* for PPTP server:

```
esr(config-pptp)# username ivan
esr(config-pptp-user)# password ascii-text password1
esr(config-pptp-user)# enable
esr(config-pptp-user)# exit
esr(config-pptp)# username fedor
esr(config-pptp-user)# password ascii-text password2
esr(config-pptp-user)# enable
esr(config-pptp-user)# exit
esr(config-pptp)# exit
```

Enable PPTP server:

```
esr(config-pptp)# enable
```

When a new configuration is applied, the router will listen to 120.11.5.1:1723. To view PPTP server session status, use the following command:

```
esr# show remote-access status pptp server remote-workers
```

To view PPTP server session counters, use the following command:

```
esr# show remote-access counters pptp server remote-workers
```

To clear PPTP server session counters, use the following command:

```
esr# clear remote-access counters pptp server remote-workers
```

To end PPTP server session for user 'fedor', use one of the following commands:

```
esr# clear remote-access session pptp username fedor
esr# clear remote-access session pptp server remote-workers username fedor
```

To view PPTP server configuration, use the following command:

```
esr# show remote-access configuration pptp remote-workers
```



In addition to PPTP server creation, you should open TCP port 1723 designed for connection handling and enable GRE protocol (47) for the tunnel traffic in the firewall.

7.29 Configuring remote access to corporate network via L2TP/IPsec protocol

L2TP (Layer 2 Tunneling Protocol) is a sophisticated tunneling protocol used to support virtual private networks. L2TP encapsulates PPP frames into IP packets for transmission via global IP network, e.g. the Internet. L2TP may be used for tunnel establishment between two local area networks. L2TP uses an additional UDP connection for tunnel handling. L2TP protocol does not provide data encryption, therefore it is usually combined with an IPsec protocol group that provides security on a packet level.

7.29.1 Configuration algorithm

Step	Description	Command	Keys
1	Create L2TP server profile.	<code>esr(config)# remote-access l2tp <NAME></code>	<NAME> – L2TP server profile name, set by the string of up to 31 characters.
2	Select L2TP clients authentication mode.	<code>esr(config-l2tp-server)# authentication mode</code>	local – user authentication by local base.

		{ local radius }	radius – user authentication by RADIUS server base.
3	Specify the description of the configured server (optionally).	<code>esr(config-l2tp-server)# description <DESCRIPTION></code>	<DESCRIPTION> – L2TP server description, set by the string of up to 255 characters.
4	Define the list of DNS servers that will be used by remote users (optionally).	<code>esr(config-l2tp-server)# dns-servers object-group <OBJ-GROUP-NETWORK-NAME></code>	<OBJ-GROUP-NETWORK-NAME> – name of the IP addresses profile that includes required DNS servers addresses, set by the string of up to 31 characters.
5	Specify outgoing packets DSCP priority.	<code>esr(config-l2tp-server)# dscp <DSCP></code>	<DSCP> – outgoing packets dscp priority [0..63].
6	Enable server.	<code>esr(config-l2tp-server)# enable</code>	
7	Select a key authentication method for IKE connection.	<code>esr(config-l2tp-server)# ipsec authentication method pre-shared-key</code>	
8	Specify a shared secret authentication key that should be the same for both parties of the tunnel.	<code>esr(config-l2tp-server)# ipsec authentication pre-shared-key { ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> } hexadecimal { <HEX> encrypted <ENCRYPTED-HEX> } }</code>	<TEXT> – string [1..64] ASCII characters; <HEX> – number, [1..32] bytes size, set by the string of [2..128] characters in hexadecimal format (0xYYYY ...) or (YYYY ...). <ENCRYPTED-TEXT> – encrypted password, [1..32] bytes size, set by the string of [2..128] characters. <ENCRYPTED-TEXT> – encrypted number, [2..64] bytes size, set by the string of [2..256] characters.
8	IP address of a local gateway.	<code>esr(config-l2tp-server)# local-address object-group <OBJ-GROUP-NETWORK-NAME> ip-address <ADDR></code>	<OBJ-GROUP-NETWORK-NAME> – name of the IP addresses profile that includes local gateway IP address, set by the string of up to 31 characters; <ADDR> – range starting IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
9	Specify MTU size (MaximumTransmissionUnit) for the server (optionally). MTU above 1500 will be active only when using the "system jumbo-frames" command.	<code>esr(config-l2tp-server) mtu <MTU></code>	<MTU> – MTU value, takes values in the range of [1280..1500]. Default value: 1500.
10	Specify IP address that should be listened by L2TP server.	<code>esr(config-l2tp-server)# outside-address object-group <OBJ-GROUP-NETWORK-NAME> ip-address <ADDR></code>	<OBJ-GROUP-NETWORK-NAME> – name of the profile having IP address that should be listened by L2TP server, set by the string of up to 31 characters; <ADDR> – range starting IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
11	Specify IP addresses list from which dynamic IP addresses are leased to remote users by L2TP.	<code>esr(config-l2tp-server)# remote-address { object-group <OBJ-GROUP-NETWORK-NAME> address-range <FROM-ADDR>-<TO-ADDR> }</code>	<OBJ-GROUP-NETWORK-NAME> – name of the IP addresses profile that includes remote users IP addresses list, set by the string of up to 31 characters; <FROM-ADDR> – range starting IP address, defined as

			AAA.BBB.CCC.DDD where each part takes values of [0..255]; <TO-ADDR> – range ending IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
12	Include the L2TP server in a security zone and configure interaction rules between zones.	<code>esr(config-l2tp-server)# security-zone <NAME></code>	<NAME> – security zone name, set by the string of up to 31 characters.
13	Specify user name (when using local authentication base).	<code>esr(config-l2tp-server) username <NAME></code>	<NAME> – user name, set by the string of up to 12 characters.
14	Specify user password (when using local authentication base).	<code>esr(config-l2tp-user) password ascii-text { <PASSWORD> encrypted <PASSWORD> }</code>	<PASSWORD> – user password, set by the string of up to 32 characters.
15	Enable user.	<code>esr(config-l2tp-user) enable</code>	
16	Define the list of WINS servers that will be used by remote users (optionally).	<code>esr(config-l2tp-server)# wins-servers object-group <OBJ-GROUP-NETWORK-NAME></code>	<OBJ-GROUP-NETWORK-NAME> – name of the IP addresses profile that includes required WINS servers addresses, set by the string of up to 31 characters.

7.29.2 Configuration example

Objective:

Configure L2TP server on a router for remote user connection to LAN. Authentication is performed on RADIUS server.

- L2TP server address: 120.11.5.1;
- Gateway inside the tunnel: 10.10.10.1;
- Radius server address: 192.168.1.4;

For IPsec, key authentication method is used: key-'password'.

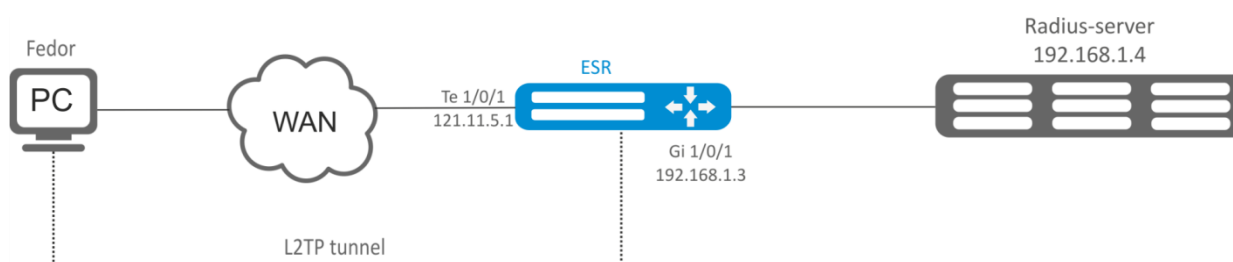


Figure 69 – Network structure

Solution:

First, do the following:

- Configure RADIUS server connection;
- Configure zones for te1/0/1 and gi1/0/1 interfaces.
- Specify IP addresses for te1/0/1 and te1/0/1 interfaces.

Create address profile that contains local gateway address:

```
esr(config)# object-group network l2tp_local
esr(config-object-group-network)# ip address-range 10.10.10.1
esr(config-object-group-network)# exit
```

Create address profile that contains DNS servers:

```
esr(config)# object-group network pptp_dns
esr(config-object-group-network)# ip address-range 8.8.8.8
esr(config-object-group-network)# ip address-range 8.8.4.4
esr(config-object-group-network)# exit
```

Create L2TP server and map profiles listed above:

```
esr(config)# remote-access l2tp remote-workers
esr(config-l2tp)# local-address ip-address 10.10.10.1
esr(config-l2tp)# remote-address address-range 10.10.10.5-10.10.10.15
esr(config-l2tp)# outside-address ip-address 120.11.5.1
esr(config-l2tp)# dns-server object-group l2tp_dns
```

Select authentication method for L2TP server users:

```
esr(config-l2tp)# authentication mode radius
```

Specify security zone that user sessions will be related to:

```
esr(config-l2tp)# security-zone VPN
```

Specify authentication method for IKE phase 1 and define an authentication key.

```
esr(config-l2tp)# ipsec authentication method psk
esr(config-l2tp)# ipsec authentication pre-shared-key ascii-text password
```

Enable L2TP server:

```
esr(config-l2tp)# enable
```

When a new configuration is applied, the router will listen to IP address 120.11.5.1 and port 1701. To view L2TP server session status, use the following command:

```
esr# show remote-access status l2tp server remote-workers
```

To view L2TP server session counters, use the following command:

```
esr# show remote-access counters l2tp server remote-workers
```

To clear L2TP server session counters, use the following command:

```
esr# clear remote-access counters l2tp server remote-workers
```

To end L2TP server session for user 'fedor', use one of the following commands:

```
esr# clear remote-access session l2tp username fedor
esr# clear remote-access session l2tp server remote-workers username fedor
```

To view L2TP server configuration, use the following command:

```
esr# show remote-access configuration l2tp remote-workers
```



In addition to L2TP server creation, you should open UDP port 500, 1701, 4500 designed for connection handling and enable ESP (50) and GRE protocol (47) for the tunnel traffic in the firewall.

7.30 Configuring remote access to corporate network via OpenVPN protocol

OpenVPN is a sophisticated tool based on SSL that implements Virtual Private Networks (VPN), enables remote access and solves many different tasks related to data transmission security.

7.30.1 Configuration algorithm

Step	Description	Command	Keys
1	Create OpenVPN server profile.	<code>esr(config)# remote-access openvpn <NAME></code>	<NAME> – OpenVPN server profile name, set by the string of up to 31 characters.
2	Specify IP addresses list from which dynamic IP addresses are leased to remote users in L2 mode by OpenVPN server. (only for tunnel ethernet)	<code>esr(config-openvpn-server)# address-range <FROM-ADDR>-<TO-ADDR></code>	<FROM-ADDR> – range starting IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <TO-ADDR> – range ending IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
3	Include client connections via OpenVPN in L2 domain (only for tunnel ethernet).	<code>esr(config-openvpn-server)# bridge-group <BRIDGE-ID></code>	<BRIDGE-ID> – bridge identifying number.
4	Specify certificates and keys.	<code>esr(config-openvpn-server)# certificate <CERTIFICATE-TYPE><NAME></code>	<CERTIFICATE-TYPE> – certificate or key type, may take the following values: ca – Certificate Authority; crl – Certificate Revocation List; dh – Diffie-Hellman key; server-crt – public server certificate; server-key – private server key; ta – HMAC key. <NAME> – certificate or key name, set by the string of up to 31 characters.
5	Enable data transmission blocking between clients (optionally).	<code>esr(config-openvpn-server)# client-isolation</code>	
6	Set the maximum amount of simultaneous user sessions (optionally).	<code>esr(config-openvpn-server)# client-max <VALUE></code>	<VALUE> – maximum amount of users, takes values of [1..65535].
7	The mechanism of transmitted data compression between clients and the OpenVPN server is enabled (optionally).	<code>esr(config-openvpn-server)# compression</code>	
8	Specify the description of the configured server (optionally).	<code>esr(config-openvpn-server)# description <DESCRIPTION></code>	<DESCRIPTION> – OpenVPN server description, set by the string of up to 255 characters.
9	Define the list of DNS servers that will be used by remote users (optionally).	<code>esr(config-openvpn-server)# dns-server <ADDR></code>	<ADDR> – DNS server IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].

10	Select encryption algorithm used when data transmission.	<code>esr(config-openvpn-server)# encryption algorithm <ALGORITHM></code>	<ALGORITHM> – encryption protocol identifier, takes the following values: 3des, blowfish128, aes128.
11	Define the subnet from which IP addresses are leased to users. (only for tunnel ip)	<code>esr(config-openvpn-server)# network <ADDR/LEN></code>	<ADDR/LEN> – subnet address, set in the following format: AAA.BBB.CCC.DDD/EE – network IP address with prefix mask, where AAA-DDD take values of [0..255] and EE takes values of [1..32].
12	Specify TCP/UDP port that will be listened by OpenVPN server (optionally).	<code>esr(config-openvpn-server)# port <PORT></code>	<PORT> – TCP/UDP port, takes values of [1..65535].
13	Specify an encapsulated protocol.	<code>esr(config-openvpn-server)# protocol <PROTOCOL></code>	<PROTOCOL> – encapsulation type, possible values: TCP encapsulation in TCP segments; Udp encapsulation in UDP datagrams.
14	Enable the default route advertising for OpenVPN connections, which leads to the replacement of the default route on the client side (optionally).	<code>esr(config-openvpn-server)# redirect-gateway</code>	
16	Enable the advertising of specified subnets, the gateway is OpenVPN server IP address (optionally).	<code>esr(config-openvpn-server)# route <ADDR/LEN></code>	<ADDR/LEN> – subnet address, set in the following format: AAA.BBB.CCC.DDD/EE – network IP address with prefix mask, where AAA-DDD take values of [0..255] and EE takes values of [1..32].
17	Include the OpenVPN server in a security zone and configure interaction rules between zones.	<code>esr(config-openvpn-server)# security-zone <NAME></code>	<NAME> – security zone name, set by the string of up to 31 characters.
18	Set time interval after which the opposing party is considered to be unavailable (optionally).	<code>esr(config-openvpn-server)# timers holdtime <TIME></code>	<TIME> – time in seconds, takes values of [1..65535].
19	Set the time interval after which the connection with the opposing party is checked (optionally).	<code>esr(config-openvpn-server)# timers keepalive <TIME></code>	<TIME> – time in seconds, takes values of [1..65535].
20	Define type of connection with a private network via OpenVPN server.	<code>esr(config-openvpn-server)# tunnel <TYPE></code>	<TYPE> – encapsulation protocol, takes the following values: ip – point-to-point connection; ethernet – L2 domain connection.
21	Define the subnet for a specified OpenVPN server user (when using a local base for user authentication).	<code>esr(config-openvpn-server)# username <NAME>subnet <ADDR/LEN></code>	<NAME> – user name, set by the string of up to 31 characters. <ADDR/LEN> – subnet address, set in the following format: AAA.BBB.CCC.DDD/NN – network IP address with prefix mask, where AAA-DDD take values of [0..255] and EE takes values of [1..32].
22	Define the list of WINS servers that will be used by remote users (optionally).	<code>esr(config-openvpn-server)# wins-server <ADDR></code>	<ADDR> – WINS server IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
23	Enable OpenVPN server profile.	<code>esr(config-openvpn-server)# enable</code>	

7.30.2 Configuration example

Objective: Configure OpenVPN server in L3 mode on a router for remote user connection to LAN.

- OpenVPN server subnet: 10.10.100.0/24;
- Mode: L3;
- Authentication based on certificates.

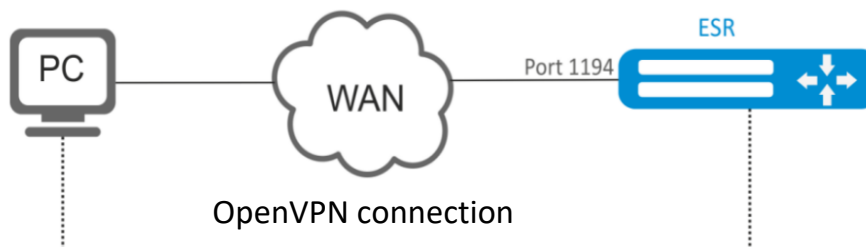


Figure 70 – Network structure

Solution:

First, do the following:

- Prepare certificates and keys:
 - CA certificate
 - OpenVPN server key and certificate
 - Diffie-Hellman and HMAC key for TLS
- Configure zone for te1/0/1 interface
- Specify IP address for te1/0/1 interface

Import certificates and keys via tftp

```
esr# copy tftp://192.168.16.10:/ca.crt certificate:ca/ca.crt
esr# copy tftp://192.168.16.10:/dh.pem certificate:dh/dh.pem
esr# copy tftp://192.168.16.10:/server.key certificate:server-key/server.key
esr# copy tftp://192.168.16.10:/server.crt certificate:server-crt/server.crt
esr# copy tftp://192.168.16.10:/ta.key certificate:ta/ta.key
```

Create OpenVPN server and a subnet for its operation:

```
esr(config)# remote-access openvpn AP
esr(config-openvpn)# network 10.10.100.0/24
```

Specify L3 connection type and encapsulation protocol.

```
esr(config-openvpn)# tunnel ip
esr(config-openvpn)# protocol tcp
```

Announce LAN subnets that will be available via OpenVPN connection and define DNS server

```
esr(config-)# route 10.10.0.0/20
esr(config-openvpn)# dns-server 10.10.1.1
```

Specify previously imported certificates and keys that will be used with OpenVPN server:

```

esr(config-openvpn)# certificate ca ca.crt
esr(config-openvpn)# certificate dh dh.pem
esr(config-openvpn)# certificate server-key server.key
esr(config-openvpn)# certificate server-crt server.crt
esr(config-openvpn)# certificate ta ta.key

```

Specify security zone that user sessions will be related to:

```

esr(config-openvpn)# security-zone VPN

```

Select aes128 encryption algorithm:

```

esr(config-openvpn)# encryption algorithm aes128

```

Enable OpenVPN server:

```

esr(config-openvpn)# enable

```

When a new configuration is applied, the router will listen to port 1194 (used by default).

To view OpenVPN server session status, use the following command:

```

esr# show remote-access status openvpn server AP

```

To view OpenVPN server session counters, use the following command:

```

esr# show remote-access counters openvpn server AP

```

To clear OpenVPN server session counters, use the following command:

```

esr# clear remote-access counters openvpn server AP

```

To end OpenVPN server session for user 'fedor', use one of the following commands:

```

esr# clear remote-access session openvpn username fedor
esr# clear remote-access session openvpn server AP username fedor

```

To view OpenVPN server configuration, use the following command:

```

esr# show remote-access configuration openvpn AP

```



In addition to OpenVPN server creation, you should open TCP port 1194 in the firewall.

7.31 Configuring remote access client via PPPoE

PPPoE is a tunneling protocol that allows encapsulating IP PPP over Ethernet connections and has PPP connection software capabilities, which allows using it to establish virtual connections to a neighbouring Ethernet device or a point-to-point connection that is used to transmit IP packets, and also works with PPP features. This allows applying conventional PPP-oriented software to configure the connection that uses not serial communication link but packet-oriented network (for example, Ethernet) to organize a classical connection with login and password for Internet connections. In addition, IP address on

the opposite side of connection is assigned only when PPPoE connection is open, allowing the dynamic reuse of IP addresses.

7.31.1 Configuration algorithm

Step	Description	Command	Keys
1	Create a PPPoE tunnel and switch to its configuration mode.	<code>esr (config) # tunnel pppoe <PPPoE></code>	<PPPoE> – tunnel sequence number from 1 to 10.
2	Specify the description of the configured client (optionally).	<code>esr (config- pppoe) # description <DESCRIPTION></code>	<DESCRIPTION> – PPPoE server description, set by the string of up to 255 characters.
3	Specify authentication method (optionally).	<code>esr (config-ppptp) # authentication method <METHOD></code>	<METHOD> – authentication method, possible values: chap, mschap, mschap-v2, eap, pap Default value: chap
4	Enable the opt-out of receiving the default route from PPPoE server (optionally).	<code>esr (config- pppoe) # ignore- default-route</code>	
5	Specify the interface through which the PPPoE connection will be established.	<code>esr (config- pppoe) # interface <IF></code>	<IF> – interface or interface group.
6	Specify the time interval during which the statistics on the load is averaged (optionally).	<code>esr (config- pppoe) # load- average <TIME></code>	<TIME> – time interval in seconds from 5 to 150 (5 seconds by default)
7	Specify MTU size (MaximumTransmissionUnit) for PPPoE tunnel. MTU above 1500 will be active only when using the "system jumbo-frames" command (optionally).	<code>esr (config- pppoe) # mtu <MTU></code>	<MTU> – MTU value, takes values in the range of: ESR-10, ESR-12V(F), ESR-14VF – [1280..9600]; ESR-100, ESR-200, ESR-1000, ESR-1200, ESR-1700 – [1280..10000]. _x000B_ For LT tunnels: ESR-10, ESR-12V(F), ESR-14VF – [552..9600]; ESR-100, ESR-200, ESR-1000, ESR-1200, ESR-1700 – [552-10000]. Default value: 1500
8	Specify user name and password for connection to PPPoE server	<code>esr (config- pppoe) # username <NAME> password ascii- text { <CLEAR- TEXT> encrypted <ENCRYPTED- TEXT> }</code>	<NAME> – user name, set by the string of up to 31 characters; <CLEAR-TEXT> – password, set by the string of 8 to 16 characters; <ENCRYPTED-TEXT> – encrypted password, set by the string of [16..128] characters.
9	Specify the name of VRF instance in which the specified network interface, bridge, security zone, dynamic authorization server (DAS) or NAT rules group will be used. (optionally)	<code>esr (config- pppoe) # ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.
10	Disable Firewall function on a network interface (optionally)	<code>esr (config- pppoe) # ip firewall disable</code>	
	Configure a security zone.	<code>esr (config- pppoe) #security- zone <NAME></code>	<NAME> – security zone name, set by the string of up to 31 characters.

11	Enable a configured profile.	<code>esr(config-pppoe)# enable</code>	
----	------------------------------	--	--

7.31.2 PPPoE client configuration example

Objective:

Configure PPPoE client on the router.

- Accounts for connection – tester;
- Account passwords – password;
- The connection should be established from the gigabitethernet 1/0/7 interface.

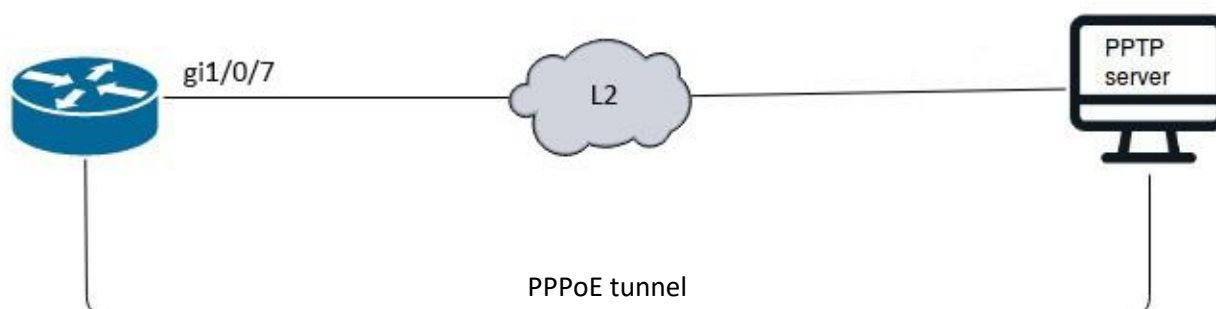


Figure 71 – Network structure

Solution:

Pre-configure PPPoE server with the accounts.

Enter the PPPoE client configuration mode and disable the firewall:

```
esr# configure
esr(config)# tunnel pppoe 1
esr(config-pppoe)# ip firewall disable
```

Specify user name and password for connection to PPPoE server:

```
esr(config-pppoe)# username tester password ascii-text password
```

Specify the interface through which the PPPoE connection will be established:

```
esr(config-pppoe)# interface gigabitethernet 1/0/7
esr(config-pptp)# enable
```

To view the tunnel status, use the following command:

```
esr# show tunnels configuration pppoe 1
```

To view PPPoE client session counters, use the following command:

```
esr# show tunnels counters pppoe 1
```

7.32 Configuring remote access client via PPTP

PPTP (Point-to-Point Tunneling Protocol) is a point-to-point tunneling protocol that allows establishing secure connection with a server by creating a special tunnel in a common unsecured network. PPTP encapsulates PPP frames into IP packets for transmission via global IP network, e.g. the Internet. PPTP may be used for tunnel establishment between two local area networks. PPTP uses an additional TCP connection for tunnel handling.

7.32.1 Configuration algorithm

Step	Description	Command	Keys
1	Create a PPTP tunnel and switch to its configuration mode.	<code>esr(config)# tunnel pptp <INDEX></code>	<INDEX> – tunnel identifier, set in the range of: [1..10].
2	Specify authentication method (optionally).	<code>esr(config-pptp)# authentication method <METHOD></code>	<METHOD> – authentication method, possible values: chap, mschap, mschap-v2, eap, pap Default value: chap
3	Specify VRF instance, in which the given PPTP tunnel will operate (optionally).	<code>esr(config-pptp)# ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.
4	Specify the description of the configured tunnel (optionally).	<code>esr(config-pptp)# description <DESCRIPTION></code>	<DESCRIPTION> – tunnel description, set by the string of up to 255 characters.
5	Set remote IP address for tunnel installation.	<code>esr(config-pptp)# remote address <ADDR></code>	<ADDR> – local gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
6	Specify MTU size (MaximumTransmissionUnit) for the tunnel (optionally).	<code>esr(config-pptp)# mtu <MTU></code>	<MTU> – MTU value takes value in the following range: for esr10/12V/ – [552..9600], for esr100/200/1000/1200/1700 – [552..10000]. Default value: 1500
7	Ignore the default route via the given PPTP tunnel (optionally)	<code>esr(config-pptp)# ignore-default-route</code>	
8	Specify the time interval during which the statistics on the tunnel load is averaged (optionally).	<code>esr(config-pptp)# load-average <TIME></code>	<TIME> – interval in seconds, takes values of [5..150]. Default value: 5
9	Specify the user and set an encrypted or unencrypted password to authenticate the remote party.	<code>esr(config-pptp)# username <NAME> password ascii-text { <WORD> encrypted <HEX> }</code>	<NAME> – user name, set by the string of up to 31 characters. <WORD> – unencrypted password, set by the string of [8..64] characters, may include [0-9a-fA-F] characters. <HEX> – encrypted password, set by the string of [16..128] characters.
10	Include the PPTP tunnel in a security zone and configure interaction rules between zones or disable firewall (optionally).	<code>esr(config-pptp)# security-zone <NAME></code>	<NAME> – security zone name, set by the string of up to 31 characters.
11	Disable the incoming traffic processing in Firewall (optionally).	<code>esr(config-pptp)# ip firewall disable</code>	
12	Enable the tunnel.	<code>esr(config-pptp)# enable</code>	

7.32.2 Example of remote connection configuration via PPTP

Objective:

Configure PPTP tunnel on a router:

- PPTP server address: 20.20.0.1;
- account for connection – login: ivan, password: simplepass.

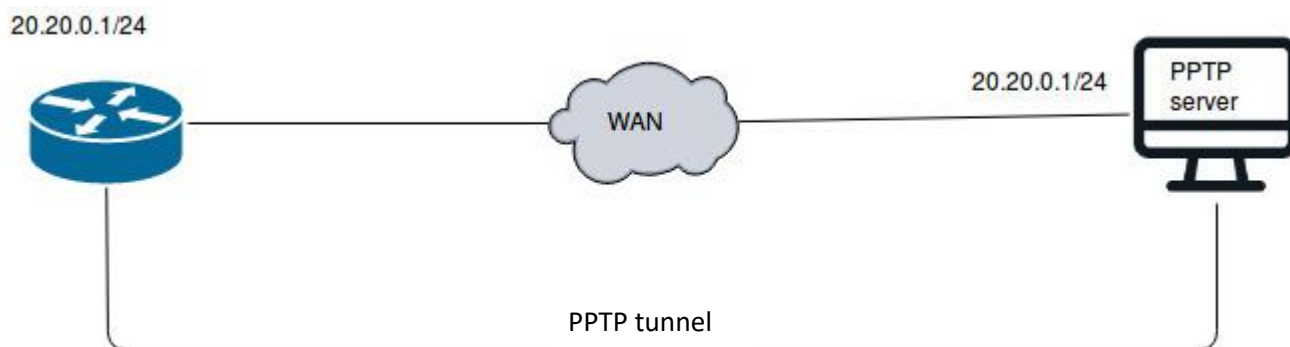


Figure 72 – Network structure

Solution:

Create PPTP tunnel:

```
esr(config)# tunnel pptp 1
```

Specify the account (Ivan user) to connect to the server:

```
esr(config-pptp)# username ivan password ascii-text simplepass
```

Specify the remote gateway:

```
esr(config-pptp)# remote address 20.20.0.1
```

Create a security zone:

```
esr(config-pptp)# security-zone VPN
```

Enable PPTP tunnel:

```
esr(config-pptp)# enable
```

To view the tunnel status, use the following command:

```
esr# show tunnels status pptp
```

To view sent and received packet counters, use the following command:

```
esr# show tunnels counters pptp
```

To view the tunnel configuration, use the following command:

```
esr# show tunnels configuration pptp
```

7.33 Configuring remote access client via L2TP

L2TP (Layer 2 Tunneling Protocol) is a sophisticated tunneling protocol used to support virtual private networks. L2TP encapsulates PPP frames into IP packets for transmission via global IP network, e.g. the Internet. L2TP may be used for tunnel establishment between two local area networks. L2TP uses an additional UDP connection for tunnel handling. L2TP protocol does not provide data encryption, therefore it is usually combined with an IPsec protocol group that provides security on a packet level.

7.33.1 Configuration algorithm

Step	Description	Command	Keys
1	Create a L2TP tunnel and switch to its configuration mode.	<code>esr(config)# tunnel l2tp <INDEX></code>	<INDEX> – tunnel identifier, set in the range of: [1..10].
2	Specify authentication method (optionally).	<code>esr(config-pptp)# authentication method <METHOD></code>	<METHOD> – authentication method, possible values: chap, mschap, mschap-v2, eap, pap Default value: chap
3	Specify VRF instance, in which the given L2TP tunnel will operate (optionally).	<code>esr(config-l2tp)# ip vrf forwarding <VRF></code>	<VRF> – VRF name, set by the string of up to 31 characters.
4	Specify the description of the configured tunnel (optionally).	<code>esr(config-l2tp)# description <DESCRIPTION></code>	<DESCRIPTION> – tunnel description, set by the string of up to 255 characters.
5	Set remote IP address for tunnel installation.	<code>esr(config-l2tp)# remote address <ADDR></code>	<ADDR> – local gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
6	Specify MTU size (MaximumTransmissionUnit) for the tunnel (optionally)	<code>esr(config-l2tp)# mtu <MTU></code>	<MTU> – MTU value takes value in the following range: for esr10/12V/ – [552..9600], for esr100/200/1000/1200/1700 – [552..10000]. Default value: 1500
7	Ignore the default route via the given L2TP tunnel (optionally)	<code>esr(config-l2tp)# ignore-default-route</code>	
8	Specify the time interval during which the statistics on the tunnel load is averaged (optionally).	<code>esr(config-l2tp)# load-average <TIME></code>	<TIME> – interval in seconds, takes values of [5..150]. Default value: 5
9	Specify the user and set an encrypted or unencrypted password to authenticate the remote party.	<code>esr(config-l2tp)# username <NAME> password ascii-text { <WORD> encrypted <HEX> }</code>	<NAME> – user name, set by the string of up to 31 characters. <WORD> – unencrypted password, set by the string of [8..64] characters, may include [0-9a-fA-F] characters. <HEX> – encrypted password, set by the string of [16..128] characters.
10	Select a key authentication method for IKE connection.	<code>esr(config-l2tp-server)# ipsec authentication method pre-shared-key</code>	

11	Specify a shared secret authentication key that should be the same for both parties of the tunnel.	<code>esr(config-l2tp-server)# ipsec authentication pre-shared-key { ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> } hexadecimal {<HEX> encrypted <ENCRYPTED-HEX> } }</code>	<TEXT> – string [1..64] ASCII characters; <HEX> – number, [1..32] bytes size, set by the string of [2..128] characters in hexadecimal format (0xYYYY ...) or (YYYY ...). <ENCRYPTED-TEXT> – encrypted password, [1..32] bytes size, set by the string of [2..128] characters. <ENCRYPTED-TEXT> – encrypted number, [2..64] bytes size, set by the string of [2..256] characters.
12	Include the L2TP tunnel in a security zone and configure interaction rules between zones or disable firewall (optionally).	<code>esr(config-l2tp)# security-zone <NAME></code>	<NAME> – security zone name, set by the string of up to 31 characters.
13	Disable the incoming traffic processing in Firewall (optionally).	<code>esr(config-l2tp)# ip firewall disable</code>	
14	Enable the tunnel	<code>esr(config-l2tp)# enable</code>	

7.33.2 Example of remote connection configuration via L2TP

Objective:

Configure PPTP tunnel on a router:

- PPTP server address: 20.20.0.1;
- account for connection – login: ivan, password: simplepass

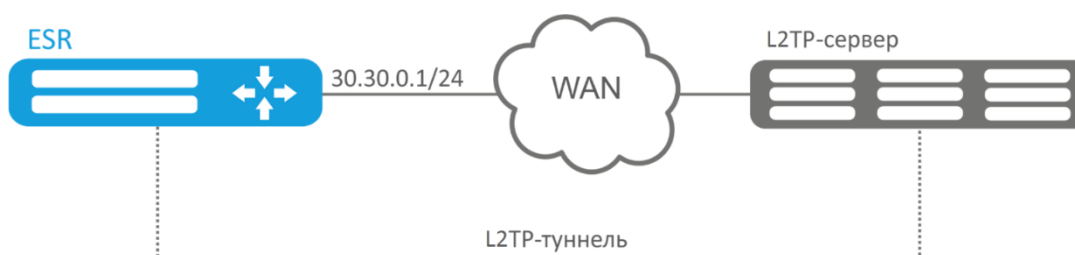


Figure 73 – Network structure

Solution:

Create L2TP tunnel:

```
esr(config)# tunnel l2tp 1
```

Specify the account (Ivan user) to connect to the server:

```
esr(config-l2tp)# username ivan password ascii-text simplepass
```

Specify the remote gateway:

```
esr(config-l2tp)# remote address 20.20.0.1
```

Specify a security zone:

```
esr(config-l2tp)# security-zone VPN
```

Specify ipsec authentication method:

```
esr(config-l2tp)# ipsec authentication method pre-shared-key
```

Specify ipsec security key:

```
esr(config-l2tp)# ipsec authentication pre-shared-key ascii-text password
```

Enable L2TP tunnel:

```
esr(config-l2tp)# enable
```

To view the tunnel status, use the following command:

```
esr# show tunnels status l2tp
```

To view sent and received packet counters, use the following command:

```
esr# show tunnels counters l2tp
```

To view the tunnel configuration, use the following command:

```
esr# show tunnels configuration l2tp
```

7.34 Dual-Homing configuration¹

Dual-Homing is a technology based on redundant links that creates a secure connection in order to prevent failures of the key network resources.

7.34.1 Configuration algorithm

Step	Description	Command	Keys
1	Specify a redundant interface to which the switching will occur when the connection is lost on a primary one.	<pre>esr(config-if-gi)# backup interface<IF> vlan <VID></pre>	<IF> – interface to which the switching will occur <VID> – VLAN ID, set in the range of [2..4094]. You can also specify it by the range with “-” or by comma-separated list..
2	Specify the number of packet copies with the same MAC address that will be sent to an active interface when switching (optionally).	<pre>esr(config)# backup- interface mac-duplicate <COUNT></pre>	<COUNT> – amount of packets copies, takes values of [1..4].
3	Specify the number of packet per second that will be sent to an active interface when switching (optionally).	<pre>esr(config)# backup- interfacemac-per- second<COUNT></pre>	<COUNT> – amount of MAC addresses per second, takes value of [50..400].
4	Specify that it is necessary to carry out the switching to the primary interface when restoring the communication (optionally).	<pre>esr(config)# backup- interface preemption</pre>	

¹ Supported only for ESR-1000 in the current firmware version

7.34.2 Configuration example

Objective:

Establish redundancy of the ESR router L2 connections for VLAN 50-55 using SW1 and SW2 devices.

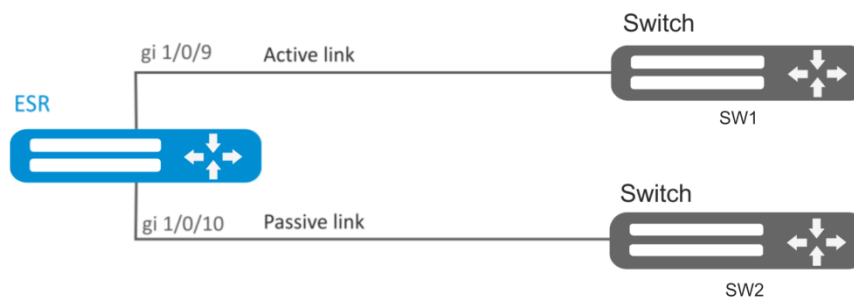


Figure 74 – Network structure

Solution:

First, do the following:

Create VLAN 50, -55:

```
esr(config)# vlan 50-55
```

You should disable STP for gigabitethernet 1/0/9 and gigabitethernet 1/0/10 interfaces, i.e. these protocols cannot operate simultaneously:

```
esr(config)# interface gigabitethernet 1/0/9-10
```

```
esr(config-if-gi)# spanning-tree disable
```

Add gigabitethernet 1/0/9 and gigabitethernet 1/0/10 interfaces into VLAN 50-55 in 'general' mode.

```
esr(config-if-gi)# switchport general allowed vlan add 50-55
```

```
esr(config-if-gi)# exit
```

Main configuration step:

Make gigabitethernet 1/0/10 redundant for gigabitethernet 1/0/9:

```
esr(config)# interface gigabitethernet 1/0/9
```

```
esr(config-if-gi)# backup interface gigabitethernet 1/0/10 vlan 50-55
```

To view information on redundant interfaces, use the following command:

```
esr# show interfaces backup
```

7.35 QoS configuration

QoS (Quality of Service) is a technology that provides various traffic classes with various service priorities. QoS service allows network applications to co-exist in a single network without altering the bandwidth of other applications.

7.35.1 Basic QoS

7.35.1.1 Configuration algorithm

Step	Description	Command	Keys
1	Enable QoS on the interface/ Tunnel/network bridge. If QoS policy is not assigned on the interface, the interface operates in BasicQoS mode.	<code>esr(config-if-gi)# qos enable</code>	
2	Set the trust mode for 802.1p and DSCP codes values in incoming packets. (optionally)	<code>esr(config)# qos trust <MODE></code>	<MODE> – trust mode for 802.1p and DSCP codes values, takes one of the following values: dscp – trust mode for DSCP codes values in IP header. Not IP packets will be sent to the default queue. cos – trust mode for 802.1p codes values in 802.1q tag. Untagged packets will be sent to the default queue. cos-dscp – trust mode for DSCP codes values in IP packets and for 802.1p codes values in other packets.
3	Set the match between DSCP codes values of incoming packets and outgoing queues. The given match works for incoming interfaces/tunnels/bridge on which QoS is enabled. (optionally)	<code>esr(config)# qos map dscp-queue <DSCP> to <QUEUE></code>	<DSCP> – service classifier in a packet IP header, takes values in the range of [0..63]; <QUEUE> – queue identifier, takes values in the range of [1..8]. Default values: DSCP: (0-7), queue 1 DSCP: (8-15), queue 2 DSCP: (16-23), queue 3 DSCP: (24-31), queue 4 DSCP: (32-39), queue 5 DSCP: (40-47), queue 6 DSCP: (48-55), queue 7 DSCP: (56-63), queue 8
4	Set the match between 802.1p codes values of incoming packets and outgoing queues. The given match works for incoming interfaces/tunnels/bridge on which QoS is enabled. (optionally)	<code>esr(config)# qos map cos-queue <COS> to <QUEUE></code>	<COS> – service classifier in 802.1q packet tag, takes values in the range of [0..7]; <QUEUE> – queue identifier, takes values in the range of [1..8]. Default values: CoS: (0), queue 1 CoS: (1), queue 2 CoS: (2), queue 3 CoS: (3), queue 4 CoS: (4), queue 5 CoS: (5), queue 6 CoS: (6), queue 7 CoS: (7), queue 8

5	Set the match between DSCP codes values of incoming packets and outgoing DSCP codes. (if remarking is required) The given match works for incoming interfaces/tunnels/bridge on which QoS is enabled.	<code>esr(config)# qos map dscp-queue <DSCP> to <DSCP></code>	<DSCP> – service classifier in a packet IP header, takes values in the range of [0..63].
6	Enable DSCP codes changes according to the DSCP-Mutation table. (if remarking is required)	<code>esr(config)# qos dscp mutation</code>	
7	Set the number of the default queue to which all traffic except IP falls into the trust mode for DSCP priorities.	<code>esr(config)# qos queue default <QUEUE></code>	<QUEUE> – queue identifier, takes values in the range of [1..8].
8	Set the amount of priority queues. The remaining queues are weighted. (optionally)	<code>esr(config)# priority-queue out num-of-queues <VALUE></code>	<VALUE> – amount of queues, takes values of [0..8], where: 0 – all queues take part in WRR (WRR – weight-based queue processing mechanism); 8 – all queues are served as «strictpriority» (strictpriority – priority queue is served as soon as the packets appear). The priority queues are allocated, starting from the 8th one, decreasing the queue number. Default value: 8
9	Define the weights for corresponding weighted queues.	<code>esr(config)# qos wrr-queue <QUEUE> bandwidth <WEIGHT></code>	<QUEUE> – queue identifier, takes values in the range of [1..8]; <WEIGHT> – weight value, takes values in the range of [1..255]. The default value: weight 1 for all queues.
10	Set the outgoing traffic rate limiting for a certain queue or interface in total. The command is relevant only for BasicQoS mode of the interface. If the incoming traffic was classified by advanced QoS, the limiting will not work. (if the incoming rate limiting is required)	<code>esr(config-if-gi)# traffic-shape { <BANDWIDTH> [BURST] queue <QUEUE><BANDWIDTH> [BURST] }</code>	<QUEUE> – queue identifier, takes values in the range of [1..8]. <BANDWIDTH> – average traffic rate in Kbps, takes the value of [3000..1000000] for TengigabitEthernet interfaces and [64..1000000] for other interfaces and tunnels; <BURST> – size of the restrictive threshold in KB, takes the value [4..16000]. 128 KB. Default value: Disabled.
11	Set the incoming traffic rate limiting. (if the outgoing rate limiting is required)	<code>esr(config-if-gi)# rate-limit <BANDWIDTH> [BURST]</code>	<BANDWIDTH> – average traffic rate in Kbps, takes the value of [3000..1000000] for TengigabitEthernet interfaces and [64..1000000] for other interfaces and tunnels; <BURST> – size of the restrictive threshold in KB, takes the value [4..16000]. 128 KB. Default value: Disabled.

7.35.1.2 Configuration example

Objective:

Configure the following restrictions on gigabitethernet 1/0/8 interface: transfer DSCP 22 traffic into 8th priority queue, DSCP 14 traffic into 7th weighted queue, limit transfer rate to 60Mbps for 7th queue.

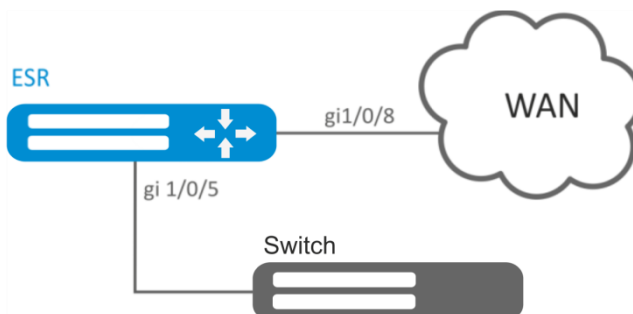


Figure 75 – Network structure

Solution:

In order to make 8th queue a priority queue, and 2nd to 8th queues weighted ones, limit the quantity of priority queues to 1:

```
esr(config)# priority-queue out num-of-queues 1
```

Redirect DSCP 22 traffic into 1st priority queue:

```
esr(config)# qos map dscp-queue 22 to 1
```

Redirect DSCP 14 traffic into 7th priority queue:

```
esr(config)# qos map dscp-queue 14 to 7
```

Enable QoS on the inbound interface from LAN side:

```
esr(config)# interface gigabitethernet 1/0/5
esr(config-if-gi)# qos enable
esr(config-if-gi)# exit
```

Enable QoS on the inbound interface from WAN side:

```
esr(config)# interface gigabitethernet 1/0/8
esr(config-if-gi)# qos enable
```

Limit transfer rate to 60Mbps for 7th queue:

```
esr(config-if)# traffic-shape queue 7 60000
esr(config-if)# exit
```

To view QoS statistics, use the following command:

```
esr# show qos statistics gigabitethernet 1/0/8
```

7.35.2 Advanced QoS

7.35.2.1 Configuration algorithm

Step	Description	Command	Keys
1	Create access lists to define the traffic to which the advanced QoS should be applied.		See Section Access list (ACL) configuration
2	Create QoS class and switch to the class parameters configuration mode.	<code>esr(config)# class-map <NAME></code>	<NAME> – name of the class being created, set by the string of up to 31 characters.
3	Specify the description of QoS class. (optionally)	<code>esr(config-class-map)# description <description></code>	<description> - up to 255 characters.
4	Specify the traffic related to the configured class by access control list (ACL).	<code>esr(config-class-map)# match access-group <NAME></code>	<NAME> – access control list name, set by the string of up to 31 characters.
5	Specify DSCP code value which will be set in IP packets corresponding to the class being configured. (cannot be assigned simultaneously with IP Precedence and CoS fields). (if remarking is required)	<code>esr(config-class-map)# set dscp <DSCP></code>	<DSCP> – DSCP code value, takes values in the range of [0..63].
6	Specify IP Precedence code value which will be set in IP packets corresponding to the class being configured (cannot be assigned simultaneously with DSCP and CoS fields). (if remarking is required)	<code>esr(config-class-map)# set ip-precedence <IPP></code>	<IPP> – IP Precedence code value, takes values in the range of [0..7].
7	Specify 802.1p priority value which will be set in packets corresponding to the class being configured (cannot be assigned simultaneously with DSCP and IP Precedence fields). (if remarking is required)	<code>esr(config-class-map)# set cos <COS></code>	<COS> – priority 802.1p value, takes values of [0..7].
8	Create QoS policy and switch to the policy parameters configuration mode.	<code>esr(config)# policy-map <NAME></code> <code>esr(config-policy-map)#</code>	<NAME> – name of the policy being created, set by the string of up to 31 characters.
9	Specify the description of QoS policy. (optionally)	<code>esr(config-policy-map)# description <description></code>	<description> - up to 255 characters.
10	Set the committed outgoing bandwidth for the policy in total.	<code>esr(config-policy-map)# shape average <BANDWIDTH> [BURST]</code>	<BANDWIDTH> – committed bandwidth in Kbps, takes the value of [64..1000000]; <BURST> – size of the restrictive threshold in KB, takes the value [4..16000]. 128 KB.

11	Enable automatic bandwidth allocation between classes without bandwidth configuration, including the default class. (if required)	<code>esr(config-policy-map)# shape auto-distribution</code>	
12	Include the specified QoS class in the policy and switch to the class parameters configuration mode within the policy.	<code>esr(config-policy-map)# class <NAME></code> <code>esr(config-class-policy-map)#</code>	<NAME> – name of the class being bound, set by the string of up to 31 characters. When specifying the “class-default” value, the incoming unclassified traffic falls into the given class.
13	Include QoS policy in QoS class to create hierarchical QoS.	<code>esr(config-class-policy-map)# service-policy <NAME></code>	<NAME> – policy name, set by the string of up to 31 characters. Inserted policy must already be created.
14	Set the committed outgoing bandwidth for the class within the policy. (if required)	<code>esr(config-class-policy-map)# shape average <BANDWIDTH> [BURST]</code>	<BANDWIDTH> – committed bandwidth in Kbps, takes the value of [64..1000000]; <BURST> – size of the restrictive threshold in KB, takes the value [4..16000]. 128 KB.
15	Set the shared outgoing bandwidth for a specific class. The class may occupy the bandwidth if a lower priority class has not occupied its committed bandwidth. (if required)	<code>esr(config-class-policy-map)# shape peak <BANDWIDTH> [BURST]</code>	
16	Specify the class operation mode. (optionally)	<code>esr(config-class-policy-map)# mode <MODE></code>	<MODE> – class mode: fifo – FIFO mode (First In, First Out); gred – GRED mode (Generalized RED); red – RED mode (Random Early Detection); sfq – SFQ mode (SFQ queue allocates flow-based packets transmission). Default value: FIFO .
17	Specify the class priority in WRR process. (if required)	<code>esr(config-class-policy-map)# priority class <PRIORITY></code>	<PRIORITY> – priority of class in WRR process, takes values of [1..8]. Classes with the highest priority are proceeded first.
18	Switch the class to the StrictPriority mode and specify the class priority. (if required)	<code>esr(config-class-policy-map)# priority level <PRIORITY></code>	<PRIORITY> – priority level in StrictPriority process, takes values of [1..8]. Classes with the highest priority are proceeded first. The default value: the class operates in WRR mode, the priority is not specified.
19	Specify the limited number of virtual queues. (optionally)	<code>esr(config-class-policy-map)# fair-queue <QUEUE-LIMIT></code>	<QUEUE-LIMIT> – limited number of virtual queues, takes values in the range of [16..4096]. Default value: 16.
20	Specify the limited number of packets for a virtual queue. (optionally)	<code>esr(config-class-policy-map)# queue-limit <QUEUE-LIMIT></code>	<QUEUE-LIMIT> – limited number of packets in a virtual queue, takes values in the range of [2..4096]. Default value: 127.

21	Specify RED (Random Early Detection) parameters. (if required)	<pre>esr(config-class-policy-map)# random-detect <LIMIT><MAX><MIN><PROBABILITY></pre>	<p><LIMIT> – limited size of a queue in bytes, takes values of in the range of [1..1000000];</p> <p><MAX> – maximum size of a queue in bytes, takes value in the range of [1..1000000];</p> <p><MIN> – minimum size of a queue in bytes, takes value in the range of [1..1000000];</p> <p><PROBABILITY> – probability of packet drop, takes values of [0..100].</p> <p>When specifying the values, the following rules should be fulfilled:</p> <p><MAX>> 2 * <MIN></p> <p><LIMIT>> 3 * <MAX></p>
22	Specify GRED (Generalized Random Early Detection) parameters. (if required)	<pre>esr(config-class-policy-map)# random-detect precedence <PRECEDENCE><LIMIT><MAX><MIN><PROBABILITY></pre>	<p><PRECEDENCE> – IPPrecedence value [0..7];</p> <p><LIMIT> – limited size of a queue in bytes, takes values of in the range of [1..1000000];</p> <p><MAX> – maximum size of a queue in bytes, takes value in the range of [1..1000000];</p> <p><MIN> – minimum size of a queue in bytes, takes value in the range of [1..1000000];</p> <p><PROBABILITY> – probability of packet drop, takes values of [0..100].</p> <p>When specifying the values, the following rules should be fulfilled:</p> <p><MAX>> 2 * <MIN></p> <p><LIMIT>> 3 * <MAX></p>
23	Enable tcp headers compression protocol for the certain class traffic. (if required)	<pre>esr(config-class-policy-map)# compression header ip tcp</pre>	
24	Enable QoS on the interface/tunnel/network bridge.	<pre>esr(config-if-gi)# qos enable</pre>	
25	Define the QoS policy on a configured interface/tunnel/network bridge to classify input and output traffic.	<pre>esr(config-if-gi)# service-policy { input output } <NAME></pre>	<p><NAME> – QoS policy name, set by the string of up to 31 characters.</p>

7.35.2.2 Configuration example

Objective: Classify incoming traffic by a subnet (10.0.11.0/24, 10.0.12.0/24), label it by DSCP (38 and 42) and segregate by a subnet (40Mbps and 60Mbps), limit general bandwidth to 250Mbps, process the rest of traffic using SFQ mechanism.

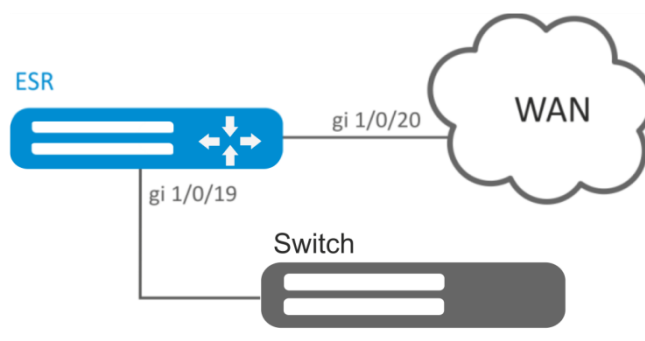


Figure 76 – Network structure

Solution:

Configure access control lists for filtering by a subnet, proceed to global configuration mode:

```

esr(config)# ip access-list extended f11
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address 10.0.11.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
esr(config)# ip access-list extended f12
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address 10.0.12.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit

```

Create classes f11 and f12, specify the respective access control lists, configure labelling:

```

esr(config)# class-map f11
esr(config-class-map)# set dscp 38
esr(config-class-map)# match access-group f11
esr(config-class-map)# exit
esr(config)# class-map f12
esr(config-class-map)# set dscp 42
esr(config-class-map)# match access-group f12
esr(config-class-map)# exit

```

Create policy and define general bandwidth limits:

```

esr(config)# policy-map fl
esr(config-policy-map)# shape average 250000

```

Map class to policy, configure bandwidth limit and exit:

```
esr(config-policy-map)# class fl1
esr(config-class-policy-map)# shape average 40000
esr(config-class-policy-map)# exit
esr(config-policy-map)# class fl2
esr(config-class-policy-map)# shape average 60000
esr(config-class-policy-map)# exit
```

For the rest of traffic, configure a class with SFQ mode:

```
esr(config-policy-map)# class class-default
esr(config-class-policy-map)# mode sfq
esr(config-class-policy-map)# fair-queue 800
esr(config-class-policy-map)# exit
esr(config-policy-map)# exit
```

Enable QoS on the interfaces, policy on gi 1/0/19 interface ingress for classification purposes and gi1/0/20 egress for applying restrictions and SFQ mode for default class:

```
esr(config)# interface gigabitethernet 1/0/19
esr(config-if-gi)# qos enable
esr(config-if-gi)# service-policy input fl
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/20
esr(config-if-gi)# qos enable
esr(config-if-gi)# service-policy output fl
esr(config-if-gi)# exit
```

To view the statistics, use the following command:

```
esr# do show qos policy statistics gigabitethernet 1/0/20
```

7.36 Mirroring configuration¹

Traffic mirroring is a feature of the router that allows for redirection of traffic from a specific port of the router to another port of the same router (local mirroring) or to a remote device (remote mirroring).

7.36.1 Configuration algorithm

Step	Description	Command	Keys
1	Define VLAN over which the mirrored traffic will be transmitted (in case of using remote mirroring).	<code>esr(config)# port monitor remote vlan <VID><DIRECTION></code>	<VID> – VLAN ID, set in the range of [2..4094]; <DIRECTION> – traffic direction: tx – mirroring only output traffic to the specified VLAN; rx – mirroring only input traffic to the specified VLAN.
2	Enable the remote mirroring mode (in case of using remote mirroring).	<code>esr(config)# port monitor remote</code>	
3	Define the mode of the port transmitting mirrored traffic.	<code>esr(config)# port monitor mode <MODE></code>	<MODE> – mode: network – combined data transmission mode and mirroring;

¹ In the current firmware version, this functionality is supported only by ESR-1000 router.

			monitor-only – only mirroring.
4	Enable mirroring in the interface configuration mode.	<code>esr (config-if-gi) # port monitor interface <IF><DIRECTION></code>	<IF> – interface to which the mirroring will occur; <DIRECTION> – traffic direction: tx – mirroring only output traffic; rx – mirroring only input traffic;

7.36.2 Configuration example

Objective:

Establish remote mirroring of traffic through VLAN 50 from gi1/0/11 interface to be sent to server for processing purposes.

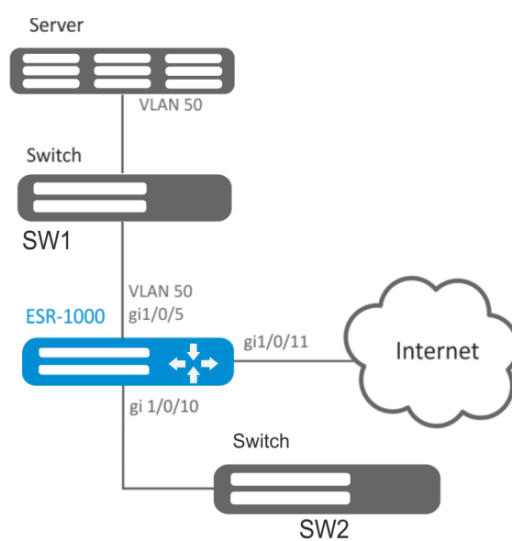


Figure 77 – Network structure

Solution:

First, do the following:

- Create VLAN 50:
- On gi 1/0/5 interface, add VLAN 50 in 'general' mode.

Main configuration step:

Specify VLAN that will be used for transmission of mirrored traffic:

```
esr1000 (config) # port monitor remote vlan 50
```

For gi 1/0/5 interface, specify a port for mirroring:

```
esr1000 (config) # interface gigabitethernet 1/0/5  
esr1000 (config-if-gi) # port monitor interface gigabitethernet 1/0/11
```

For gi 1/0/5 interface, specify the remote mirroring mode:

```
esr1000 (config-if-gi) # port monitor remote
```


7.37 Netflow configuration

Netflow is a network protocol designed for traffic accounting and analysis. Netflow allows transmitting traffic information (source and destination address, port, quantity of information) from the network equipment (sensor) to the collector. Common server may serve as a collector.

7.37.1 Configuration algorithm

Step	Description	Command	Keys
1	Specify Netflow protocol version.	<code>esr(config)# netflow version <VERSION></code>	<VERSION> – Netflow protocol version: 5, 9 and 10.
2	Set the maximum amount of observed sessions.	<code>esr(config)# netflow max-flows <COUNT></code>	<COUNT> – amount of observed sessions, takes values of [10000..2000000]. Default value: 512000.
3	Set the interval after which the information on outdated sessions is exported to the collector.	<code>esr(config)# netflow inactive-timeout <TIMEOUT></code>	<TIMEOUT> – delay before sending outdated sessions information, set in seconds, takes the value of [0..240]. Default value: 15 seconds.
4	Set the rate of the statistics sending to a Netflow collector.	<code>esr(config)# netflow refresh-rate <RATE></code>	<RATE> – rate of the statistics sending, set in packets/flow, takes the value of [1..10000]. Default value: 10.
5	Enable Netflow on the router.	<code>esr(config)# netflow enable</code>	
6	Create the Netflow collector and switch to its configuration mode.	<code>esr(config)# netflow collector <ADDR></code>	<ADDR> – collector IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
7	Set the Netflow service port on the statistics collection server.	<code>esr(config-netflow-host)# port <PORT></code>	<PORT> – UDP port number in the range of [1..65535]. Default value: 2055.
8	Enable statistics sending to the Netflow server in the interface/tunnel/network bridge configuration mode.	<code>esr(config-if-gi)# ip netflow export</code>	

7.37.2 Configuration example

Objective:

Establish accounting for traffic from gi1/0/1 interface to be sent to the server via gi1/0/8 interface for processing purposes.

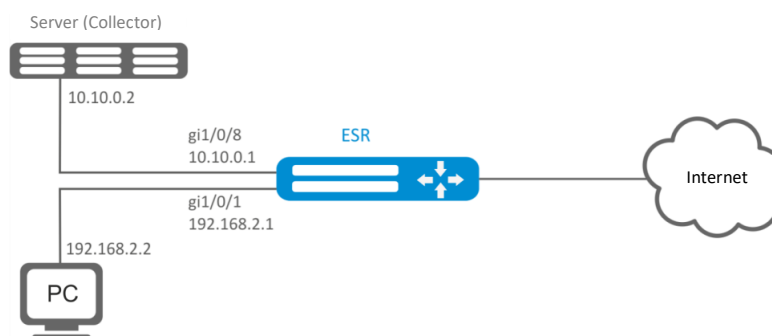


Figure 78 – Network structure

Solution:

First, do the following:

- For gi1/0/1, gi1/0/8 interfaces disable firewall with 'ip firewall disable' command.
- Assign IP address to ports.

Main configuration step:

Specify collector IP address:

```
esr(config)# netflow collector 10.10.0.2
```

Enable netflow statistics export collection for gi1/0/1 network interface:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip netflow export
```

Enable netflow on the router:

```
esr(config)# netflow enable
```

To view the Netflow statistics, use the following command:

```
esr# show netflow statistics
```

Netflow configuration for traffic accounting between zones is performed by analogy to sFlow configuration; for description, see Section 7.38 sFlow configuration.

7.38 sFlow configuration

sFlow is a computer network, wireless network and network device monitoring standard designed for traffic accounting and analysis.

7.38.1 Configuration algorithm

Step	Description	Command	Keys
1	Set the rate of sending the unchanged user traffic packets to sFlow collector.	<code>esr(config)# sflow sampling-rate <RATE></code>	<RATE> – rate of sending the user traffic packets to the collector, takes the value of [1..10000000]. If the rate value is 10, one of ten packets will be sent to the collector. Default value: 1000.
2	Set the interval after which the information on the network interface counters is obtained	<code>esr(config)# sflow poll-interval <TIMEOUT></code>	<TIMEOUT> – interval after which the information on the network interface counters is obtained, takes values of [1..10000]. Default value: 10 seconds.
3	Enable sFlow on the router.	<code>esr(config)# sflow enable</code>	
4	Create the sFlow collector and switch to its configuration mode.	<code>esr(config)# sflow collector <ADDR></code>	<ADDR> – collector IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].

5	Enable statistics sending to the sFlow server in the interface/tunnel/network bridge configuration mode.	<code>esr(config-if-gi)# ip sflow export</code>	
---	--	---	--

7.38.2 Configuration example

Objective:

Establish accounting for traffic between 'trusted' and 'untrusted' zones.

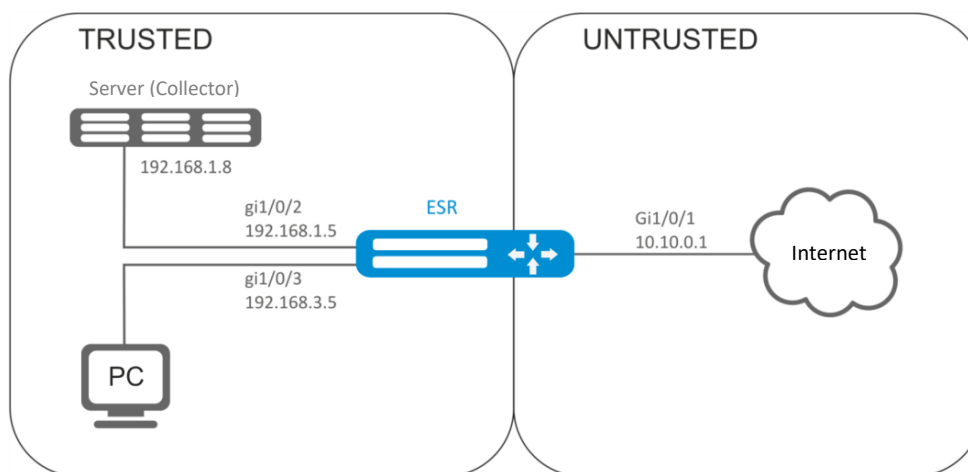


Figure 79 – Network structure

Solution:

Create two security zones for ESR networks:

```
esr# configure
esr(config)# security zone TRUSTED
esr(config-zone)# exit
esr(config)# security zone UNTRUSTED
esr(config-zone)# exit
```

Configure network interfaces and identify their inheritance to security zones:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# security-zone UNTRUSTED
esr(config-if-gi)# ip address 10.10.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gi1/0/2-3
esr(config-if-gi)# security-zone TRUSTED
esr(config-if-gi)# exit
esr(config)# interface gi1/0/2
esr(config-if-gi)# ip address 192.168.1.5/24
esr(config-if-gi)# exit
esr(config)# interface gi1/0/3
esr(config-if-gi)# ip address 192.168.3.5/24
esr(config-if-gi)# exit
```

Specify collector IP address:

```
esr(config)# sflow collector 192.168.1.8
```

Enable sFlow protocol statistics export for all traffic within 'rule1' for TRUSTED-UNTRUSTED direction:

```
esr(config)# security zone-pair TRUSTED UNTRUSTED
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action sflow-sample
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
```

Enable sFlow on the router:

```
esr(config)# sflow enable
```

sFlow configuration for traffic accounting from the interface is performed by analogy to 7.37 Netflow configuration.

7.39 LACP configuration

LACP is a link aggregation protocol that allows multiple physical links to be combined into a single logical link. This process allows to increase the communication link bandwidth and robustness.

7.39.1 Configuration algorithm

Step	Description	Command	Keys
1	Set the system priority for LACP.	<code>esr(config)# lacp system-priority <PRIORITY></code>	<PRIORITY> – priority, set in the range of [1..65535]. Default value: 1.
2	Set the load balancing mechanism for channel aggregation groups.	<code>esr(config)# port-channel load-balance {src-dst-mac-ip src-dst-mac src-dst-ip src-dst-mac-ip-port}</code>	– src-dst-mac-ip – balancing mechanism is based on the MAC address and IP address of a sender and receiver; – src-dst-mac – balancing mechanism is based on the MAC address of a sender and receiver; – src-dst-ip – balancing mechanism is based on the IP address of a sender and receiver; – src-dst-mac-ip-port – balancing mechanism is based on the MAC address, IP address and port of a sender and receiver.
3	Set LACP administration timeout.	<code>esr(config)# lacp timeout { short long }</code>	- long – long timeout; - short – short timeout. Default value: long.
4	Create and switch to the aggregated interface configuration mode.	<code>esr(config)# interface port-channel <ID></code>	<ID> – sequence number of a channel aggregation group, takes values of [1..12].
5	Configure the required parameters of aggregated channel.		
6	Switch to the physical interface configuration mode.	<code>esr(config)# interface <IF-TYPE><IF-NUM></code>	<IF-TYPE> interface type (gigabitethernet or tengigabitethernet). <IF-NUM> – F/S/P – F frame (1), S – slot (0), P – port.

7	Include a physical interface in the channel aggregation group specifying the mode of the channel aggregation group formation.	<code>esr(config-if-gi) # channel-group <ID> mode <MODE></code>	<ID> – sequence number of a channel aggregation group, takes values of [1..12]. <MODE> – mode of the channel aggregation group formation: – auto – add interface to the dynamic aggregation group with the support of LACP; – on – add interface to the static aggregation group.
8	Set the Ethernet interface LACP priority.	<code>esr(config-if-gi) # lacp port-priority <PRIORITY></code>	<PRIORITY> – priority, set in the range of [1..65535]. Default value: 1.

7.39.2 Configuration example

Objective:

Configure aggregated link between ESR router and the switch.



Figure 80 – Network structure

Solution:

First, do the following settings:

For gi1/0/1, gi1/0/2 interfaces disable security zone with 'no security-zone' command.

Main configuration step:

Create port-channel 2 interface:

```
esr(config) # interface port-channel 2
```

Add gi1/0/1, gi1/0/2 physical interfaces into the created link aggregation group:

```
esr(config) # interface gigabitethernet 1/0/1-2  
esr(config-if-gi) # channel-group 2 mode auto
```

Further port-channel configuration is performed by analogy to the common physical interface.

7.40 VRRP configuration

VRRP (Virtual Router Redundancy Protocol) is a network protocol designed for increased availability of routers, acting as a default gateway. This is performed by aggregation of a router group into a single virtual router and assigning a shared IP address, that will be used as a default gateway for computers in the network.

7.40.1 Configuration algorithm

Step	Description	Command	Keys
1	Switch to the interface/tunnel/network bridge configuration mode for which it is necessary to configure VRRP	<code>esr (config) # interface <IF-TYPE><IF-NUM></code>	<IF-TYPE> – interface type; <IF-NUM> - F/S/P – F frame (1), S – slot (0), P – port.
		<code>esr (config) # tunnel <TUN-TYPE><TUN-NUM></code>	<TUN-TYPE> – tunnel type; <TUN-NUM> – tunnel number.
		<code>esr (config) # bridge <BR-NUM></code>	<BR-NUM> – bridge number.
2	Configure the required parameters on the interface/tunnel/network bridge including IP address		
3	Enable VRRP process on IP interface.	<code>esr (config-if-gi) # vrrp</code>	
		<code>esr (config-if-gi) # ipv6 vrrp</code>	
4	Set virtual IP address of VRRP router.	<code>esr (config-if-gi) # vrrp ip <ADDR/LEN></code>	<ADDR/LEN> – virtual IP address, defined as AAA.BBB.CCC.DDD/EE where each part AAA-DDD takes values of [0..255] and EE takes values of [1..32]. You can specify several IP addresses separated by commas. Up to 4 IP addresses can be assigned to the interface.
		<code>esr (config-if-gi) # ipv6 vrrp ip <IPV6-ADDR></code>	<IPV6-ADDR> – virtual IPv6 address, defined as X:X:X:X where each part takes values in hexadecimal format [0..FFFF]. You can specify up to 8 IPv6 addresses separated by commas.
5	Set the VRRP router identifier.	<code>esr (config-if-gi) # vrrp id <VRID></code>	<VRID> – VRRP router identifier, takes values in the range of [1..255].
		<code>esr (config-if-gi) # ipv6 vrrp id <VRID></code>	
6	Set the VRRP router priority.	<code>esr (config-if-gi) # vrrp priority <PR></code>	<PR> – VRRP router priority, takes values in the range of [1..254].
		<code>esr (config-if-gi) # ipv6 vrrp priority <PR></code>	Default value: 100.
7	Identify the VRRP router's inherence to a group. The group provides with an opportunity to synchronize several VRRP processes, so if in one of the processes there is a change of master, then in another process the roles will also be changed.	<code>esr (config-if-gi) # vrrp group <GRID></code>	<GRID> – VRRP router group identifier, takes values in the range of [1..32].
		<code>esr (config-if-gi) # ipv6 vrrp group <GRID></code>	
8	Set the IP address that will be used as a source IP address for VRRP messages.	<code>esr (config-if-gi) # vrrp source-ip <IP></code>	<ADDR> – sender IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255];
		<code>esr (config-if-gi) # ipv6 vrrp source-ip <IPV6></code>	<IPV6> – source IPv6 address, defined as X:X:X:X where each part takes values in hexadecimal format [0..FFFF].
9	Set the interval between sending VRRP messages	<code>esr (config-if-gi) # vrrp timers advertise <TIME></code>	<TIME> – time in seconds, takes values of [1..40].
		<code>esr (config-if-gi) # ipv6 vrrp timers advertise <TIME></code>	Default value: 1 second.

10	Set the interval after which GratuitousARP messages are sent when switching the router to the Master status.	<code>esr(config-if-gi) # vrrp timers garp delay <TIME></code>	<TIME> – time in seconds, takes values of [1..60]. Default value: 5 seconds.
11	Set the amount of GratuitousARP messages that will be sent when switching the router to the Master status.	<code>esr(config-if-gi) # vrrp timers garp repeat <COUNT></code>	<COUNT> – amount of messages, takes values of [1..60]. Default value: 5.
12	Set the interval after which GratuitousARP messages will be sent periodically while the router is in the Master status.	<code>esr(config-if-gi) # vrrp timers garp refresh <TIME></code>	<TIME> – time in seconds, takes values of [1..65535]. Default value: Periodic sending is disabled.
13	Set the amount of GratuitousARP messages that will be sent with the garprefresh period while the router is in the Master status.	<code>esr(config-if-gi) # vrrp timers garp refresh-repeat <COUNT></code>	<COUNT> – amount of messages, takes values of [1..60]. Default value: 1.
14	Specify whether the higher priority Backup router would try to take the Master role from the current lower priority Master router.	<code>esr(config-if-gi) # vrrp preemption disable</code> <code>esr(config-if-gi) # ipv6 vrrp preemption disable</code>	
15	Set the time interval after which the higher priority Backup route will try to take the Master role from the current lower priority Master router.	<code>esr(config-if-gi) # vrrp preemption delay <TIME></code> <code>esr(config-if-gi) # ipv6 vrrp preemption delay <TIME></code>	<TIME> – timeout, takes value in seconds [1..1000]. Default value: 0
16	Set the password for neighbour authentication.	<code>esr(config-if-gi) # vrrp authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }</code>	<CLEAR-TEXT> – password, set by the string of 8 to 16 characters; <ENCRYPTED-TEXT> – encrypted password of 8 to 16 bytes (from 16 to 32 characters) in hexadecimal format (0xYYYY ...) or (YYYY ...).
17	Define authentication algorithm.	<code>esr(config-if-gi) # vrrp authentication algorithm <ALGORITHM></code>	<ALGORITHM> – authentication algorithm: cleartext – unencrypted password; md5 – password is hashed by md5 algorithm.
18	Specify VRRP version.	<code>esr(config-if-gi) # vrrp version <VERSION></code>	<VERSION> – VRRP version: 2, 3.
19	Set the mode when vrrp IP address remains in the UP status regardless of the status of the interface itself. (optionally)	<code>esr(config-if-gi) # vrrp force-up</code>	
20	Specify the delay between the assignment of MASTER status to ipv6 vrrp and the start of ND messages distribution.	<code>esr(config-if-gi) # ipv6 vrrp timers nd delay <TIME></code>	<TIME> – time in seconds, takes values of [1..60]. Default value: 5
21	Specify the period of ND protocol information update for ipv6 vrrp in MASTER status.	<code>esr(config-if-gi) # ipv6 vrrp timers nd refresh <TIME></code>	<TIME> – time in seconds, takes values of [1..65535]. Default value: 5

22	Specify the amount of ND messages sent in the update period for ipv6 vrrp in MASTER status.	<code>esr(config-if-gi)# ipv6 vrrp timers nd refresh-repeat <NUM></code>	<NUM> – amount, takes values of [1..60]. Default value: 0
23	Specify the amount of ND packets sendings after setting ipv6 vrrp to the MASTER status.	<code>esr(config-if-gi)# ipv6 vrrp timers nd repeat <NUM></code>	<NUM> – amount, takes values of [1..60]. Default value: 1

7.40.2 Configuration example 1

Objective: Establish LAN virtual gateway in VLAN 50 using VRRP. IP address 192.168.1.1 is used as a local virtual gateway.

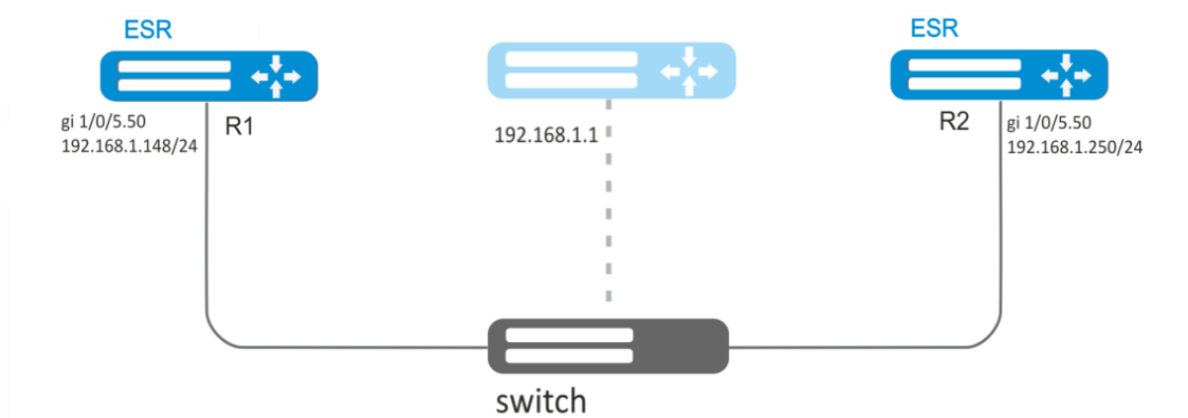


Figure 81 – Network structure

Solution:

First, do the following:

- create a correspond sub interface;
- configure a zone for the sub-interface;
- specify IP address for the sub-interface.

Main configuration step:

Configure R1 router.

Configure VRRP in the created sub-interface. Specify unique VRRP identifier:

```
R1(config)#interface gi 1/0/5.50
```

```
R1(config-subif)# vrrp id 10
```

Specify virtual gateway IP address 192.168.1.1/24:

```
R1(config-subif)# vrrp ip 192.168.1.1
```

Enable VRRP:

```
R1(config-subif)# vrrp
```

```
R1(config-subif)# exit
```


Configure R2 in the same manner.

7.40.3 Configuration example 2

Objective: Establish virtual gateways for 192.168.20.0/24 subnet in VLAN 50 and 192.168.1.0/24 in VLAN 60 using VRRP with Master sync feature. To do this, you have to group VRRP processes. IP addresses 192.168.1.1 and 192.168.20.1 are used as virtual gateways.

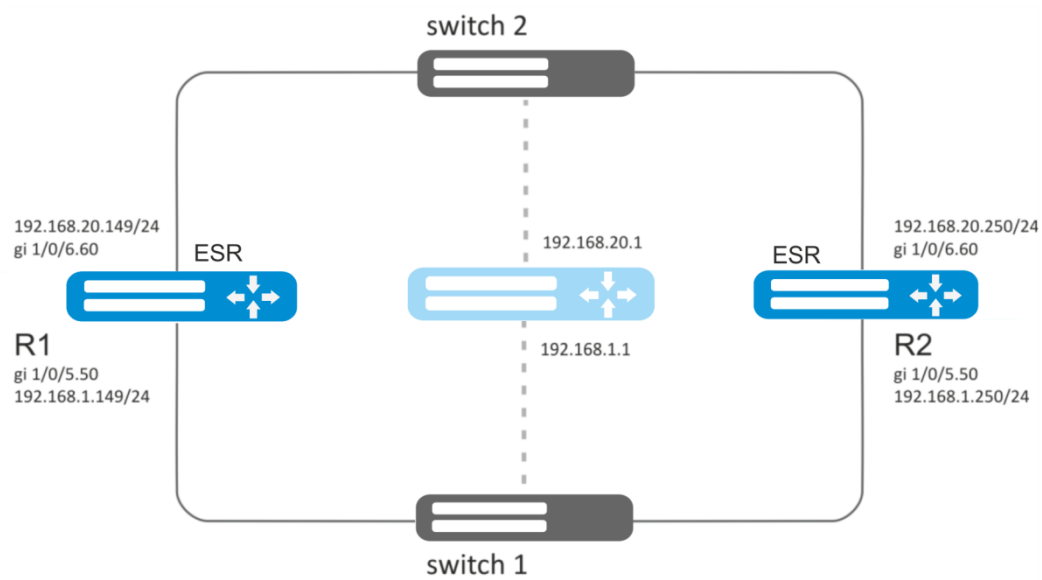


Figure 82 – Network structure

Solution:

First, do the following:

- create correspond sub interfaces;
- configure a zone for the sub-interfaces;
- specify IP addresses for the sub-interfaces.

Main configuration step:

Configure R1 router.

Configure VRRP for 192.168.1.0/24 subnet in the created sub-interface.

Specify unique VRRP identifier:

```
R1 (config-sub) # interface gi 1/0/5.50
R1 (config-subif) # vrrp id 10
```

Specify virtual gateway IP address 192.168.1.1:

```
R1 (config-subif) # vrrp ip 192.168.1.1
```

Specify VRRP group identifier:

```
R1 (config-subif) # vrrp group 5
```

Enable VRRP:

```
R1(config-subif)# vrrp
R1(config-subif)# exit
```

Configure VRRP for 192.168.20.0/24 subnet in the created sub-interface.

Specify unique VRRP identifier:

```
R1(config-sub)#interface gi 1/0/6.60
R1(config-subif)# vrrp id 20
```

Specify virtual gateway IP address 192.168.20.1:

```
R1(config-subif)# vrrp ip 192.168.20.1
```

Specify VRRP group identifier:

```
R1(config-subif)# vrrp group 5
```

Enable VRRP:

```
R1(config-subif)# vrrp
R1(config-subif)# exit
```

Configure R2 in the same manner.



In addition to tunnel creation, you should enable VRRP protocol (112) in the firewall.

7.41 VRRP tracking configuration

VRRP tracking is a mechanism, which allows activating static routes, depending on VRRP state.

7.41.1 Configuration algorithm

Step	Description	Command	Keys
1	Configure VRRP according to the Section 7.6.1.		
2	Add Tracking object to the system and switch to the Tracking object parameters configuration mode.	<code>esr(config)#tracking <ID></code>	<ID> – Tracking object number, takes values of [1..60].
3	Specify a rule for keeping track of VRRP process status.	<code>esr(config-tracking)# vrrp <VRID> [not] state { master backup fault }</code>	<VRID> – trackable VRRP router identifier, takes values in the range of [1..255].
4	Enable Tracking object.	<code>esr(config-tracking)#enable</code>	

5	Create a static IP route to the specified subnet indicating the Tracking object.	<pre> esr(config)# ip route [vrf <VRF>] <SUBNET> { <NEXTHOP> [resolve] interface <IF> tunnel <TUN> wan load-balance rule <RULE> blackhole unreachable prohibit } [<METRIC>] [track <TRACK-ID>] </pre>	<p><VRF> – VRF name, set by the string of up to 31 characters.</p> <p><SUBNET> – destination address, can be specified in the following formats: AAA.BBB.CCC.DDD – host IP address, where each part takes values of [0..255]. AAA.BBB.CCC.DDD/NN – network IP address with prefix mask, where AAA- DDD take values of [0..255] and NN takes values of [1..32].</p> <p><NEXTHOP> – gateway IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255];</p> <p>resolve – when specifying the given parameter, gateway IP address will be recursively calculated through the routing table. If the recursive calculation fails to find a gateway from a directly connected subnet, then this route will not be installed into the system;</p> <p><IF> – IP interface name, specified in the form which is described in Section 4.2;</p> <p><TUN> – tunnel name, specified in the form which is described in Section 4.3;</p> <p><RULE> – wan rule number, set in the range of [1..50];</p> <p>blackhole – when specifying the command, the packets to this subnet will be removed by the device without sending notifications to a sender;</p> <p>unreachable – when specifying the command, the packets to this subnet will be removed by the device, a sender will receive in response ICMP Destination unreachable (Host unreachable, code 1);</p> <p>prohibit – when specifying the command, the packets to this subnet will be removed by the device, a sender will receive in response ICMP Destination unreachable (Communication administratively prohibited, code 13);</p> <p><METRIC> – route metric, takes values of [0..255];</p> <p><TRACK-ID> – Tracking object identifier. If the router is bound to the Tracking object, it will appear in the system only after meeting all requirements specified in the object.</p>
---	--	---	---

7.41.2 Configuration example

Objective:

Virtual gateway 192.168.0.1/24 is organized for 192.168.0.0/24 subnet, using VRRP protocol and routers R1 and R2. There is a link with a singular subnet 192.168.1.0/30 between R1 and R2 routers. Subnet 10.0.1.0/24 is terminated only on R2 router. PC has IP address - 192.168.0.4/24 and default gateway 192.168.1.1.

When router R1 is in vrrp backup state, traffic from PC will be transmitted without any additional settings. When router R1 is in vrrp master state, additional route is necessary for subnet 10.0.1.0/24 through interface 192.168.1.2.

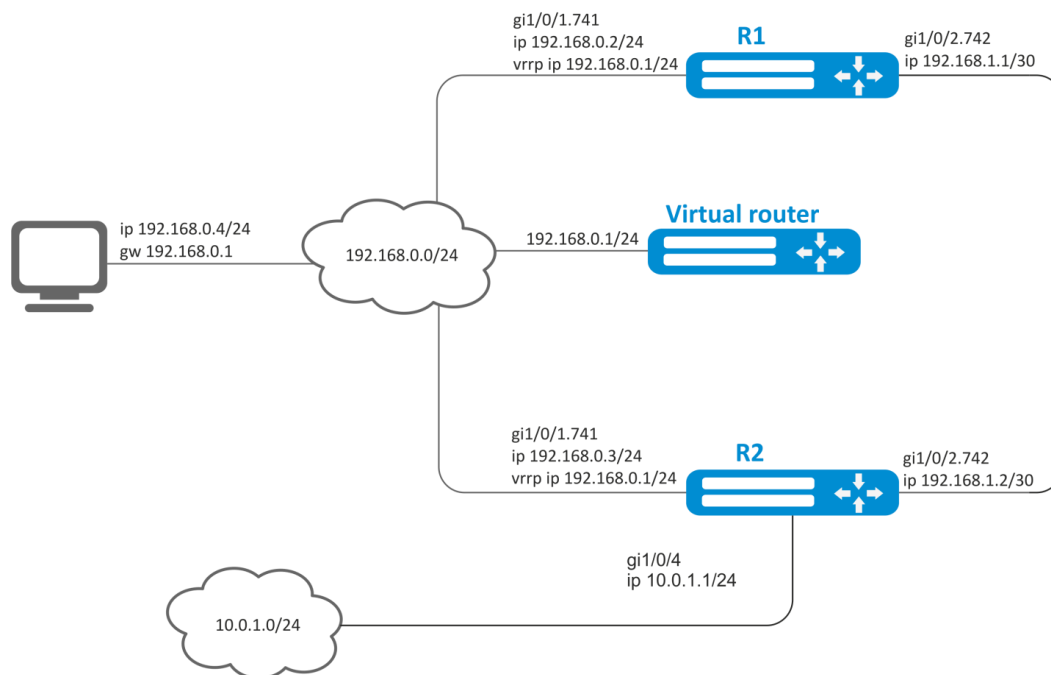


Figure 83 – Network structure

Initial configurations of the routers:

R1 router

```
hostname R1
interface gigabitethernet 1/0/1
    switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/1.741
    ip firewall disable
    ip address 192.168.0.2/24
    vrrp id 10
    vrrp ip 192.168.0.1/24
    vrrp
exit
interface gigabitethernet 1/0/2
    switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/2.742
    ip firewall disable
    ip address 192.168.1.1/30
exit
```

R2 router

```
hostname R2
interface gigabitethernet 1/0/1
    switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/1.741
```

```

ip firewall disable
ip address 192.168.0.3/24
vrrp id 10
vrrp ip 192.168.0.1/24
vrrp
exit
interface gigabitethernet 1/0/2
switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/2.742
ip firewall disable
ip address 192.168.1.2/30
exit
interface gigabitethernet 1/0/4
ip firewall disable
ip address 10.0.1.1/24
exit

```

Solution:

There is no need in any changes in router R2, since subnet 10.0.1.0/24 is terminated on it and as soon as router R2 is vrrp master, packets will be transmitted to corresponding interface. As soon as R1 becomes vrrp master, route for packets must be created with destination IP address from network 10.0.1.0/24.

Create tracking-object with corresponding condition:

```

R1(config)# tracking 1
R1(config-tracking)# vrrp 10 state master
R1(config-tracking)# enable
R1(config-tracking)# exit

```

Create static route to subnet 10.0.1.0/24 through 192.168.1.2, which will work in case of satisfying of tracking 1 condition:

```

R1(config)# ip route 10.0.1.0/24 192.168.1.2 track 1

```

7.42 VRF Lite configuration

VRF (Virtual Routing and Forwarding) is a technology designed for isolation of routing information that belongs to different classes (e.g., routes of a specific client).

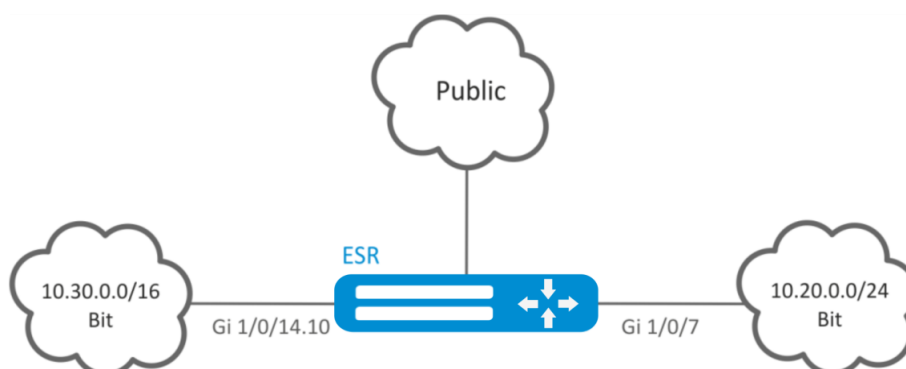


Figure 84 – Network structure

7.42.1 Configuration algorithm

Step	Description	Command	Keys
1	Create VRF instance and switch to the VRF instance parameters configuration mode.	<code>esr(config)# ip vrf <VRF></code>	<VRF> – VRF instance name, set by the string of up to 31 characters.
2	Assign the description of the configured VRF instance.	<code>esr(config-vrf)# description <DESCRIPTION></code>	<DESCRIPTION> – VRF instance description, set by the string of up to 255 characters.
3	Set the capacity of routing tables in configured VRF for IPv4/IPv6 (optionally).	<code>esr(config-vrf)# ip protocols <PROTOCOL> max-routes <VALUE></code> <code>esr(config-vrf)# ipv6 protocols <PROTOCOL> max-routes <VALUE></code>	<PROTOCOL> – protocol type, takes the following values: ospf, bgp; <VALUE> – amount of routes in the routing table, takes values in the range of: OSPF ESR-1000/1200/1700 [1..500000], ESR-100/200 [1..300000], ESR-10/12V(F)/14VF [1..30000]; BGP ESR-1000/1200/1700 [1..2800000], ESR-100/200 [1..1400000], ESR-10/12V(F)/14VF [1..800000]. Default value: 0
4	Enable and configure dynamic traffic routing protocols (Static/OSPF/BGP) in VRF instance (optionally). See corresponding sections 7.16, 7.20 and 7.21.		
5	In the configuration mode of physical/logical interface, tunnel, DNAT/SNAT rule, DAS server or SNMPv3 user, specify the name of VRF instance for which the mode will be used (optionally).	<code>esr(config-snat-ruleset)# ip vrf forwarding <VRF></code>	<VRF> – VRF instance name, set by the string of up to 31 characters.
6	Configure LT tunnel to transmit traffic to global mode or to other VRFs (if required).		

7.42.2 Configuration example

Objective:

ESR series router features 2 connected networks that should be isolated from other networks.

Solution:

Create VRF:

```
esr(config)# ip vrf bit
esr(config-vrf)# exit
```

Create a security zone:

```
esr(config)# security zone vrf-sec
esr(config-zone)# ip vrf forwarding bit
esr(config-zone)# exit
```

Create rule for a pair of zones and allow all TCP/UDP traffic:

```

esr(config)# security zone-pair vrf-sec vrf-sec
esr(config-zone-pair)# rule 1
esr(config-zone-rule)# match source-address any
esr(config-zone-rule)# match destination-address any
esr(config-zone-rule)# match protocol udp
esr(config-zone-rule)# match source-port any
esr(config-zone-rule)# match destination-port any
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-rule)# match source-address any
esr(config-zone-rule)# match destination-address any
esr(config-zone-rule)# match protocol tcp
esr(config-zone-rule)# match source-port any
esr(config-zone-rule)# match destination-port any
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit

```

Create interface mapping, assign IP addresses, specify an inheritance to a security zone:

```

esr(config)# interface gigabitethernet 1/0/7
esr(config-if-gi)# ip vrf forwarding bit
esr(config-if-gi)# ip address 10.20.0.1/24
esr(config-if-gi)# security-zone vrf-sec
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/14.10
esr(config-subif)# ip vrf forwarding bit
esr(config-subif)# ip address 10.30.0.1/16
esr(config-subif)# security-zone vrf-sec
esr(config-subif)# exit
esr(config)# exit

```

To view information on interfaces mapped to VRF, use the following command:

```
esr# show ip vrf
```

To view VRF routing table, use the following command:

```
esr# show ip route vrf bit
```

7.43 MultiWAN configuration

MultiWAN technology establishes a fail-safe connection with redundancy of links from multiple providers and solves the problem involving traffic balancing between redundant links.

7.43.1 Configuration algorithm

Step	Description	Command	Keys
1	Configure interfaces through which MultiWAN will operate: set ip addresses and specify security zone.		

2	Write static routes through WAN (if required).	<code>esr(config)# ip route <SUBNET> wan load-balance rule <ID> [<METRIC>]</code>	<ID> – identifier of the rule being created (see item 2). <METRIC> – route metric, takes values of [0..255].
3	Create WAN rule and switch to the rule parameters configuration mode.	<code>esr(config)# wan load-balance rule <ID></code>	<ID> – identifier of the rule being created, takes values in the range of [1..50].
4	Specify interfaces or tunnels which are gateways in the route created by MultiWAN service.	<code>esr(config-wan-rule)# outbound { interface <IF> tunnel <TUN> } [WEIGHT]</code>	<IF> – device interface name; <TUN> – tunnel name; [WEIGHT] – tunnel or interface weight, defined in the range of [1..255]. If the value is equal 2, than 2 times more traffic will be transmit via the given interface than via the interface with the default value. A route with the highest weight will be active in the redundancy mode. Default value: 1
5	Describe the rules (optionally).	<code>esr(config-wan-rule)# description <DESCRIPTION></code>	<DESCRIPTION> – wan rule description, set by the string of up to 255 characters.
6	You can use this command to switch from the balancing mode to the redundancy mode.	<code>esr(config-wan-rule)# failover</code>	
7	Enable wan rule.	<code>esr(config-wan-rule)# enable</code>	
8	Create a list of IP addresses to check the connection integrity and perform the switching to the list parameters configuration mode.	<code>esr(config)# wan load-balance target-list <NAME></code>	<NAME> – list name, set by the string of up to 31 characters.
9	Specify the check target and switch to the target parameters configuration mode.	<code>esr(config-target-list)# target <ID></code>	<ID> – target identifier, set in the range of [1..50]. If the “all” parameter value is used when removing, all targets for the configured target list will be removed.
10	Describe target (optionally).	<code>esr(config-wan-target)# description <DESCRIPTION></code>	<DESCRIPTION> – target description, set by the string of up to 255 characters.
11	Specify the standby time via ICMP (optionally).	<code>esr(config-wan-target)# resp-time <TIME></code>	<TIME> – timeout, takes value in seconds [1..30].
12	Specify IP address of the check.	<code>esr(config-wan-target)# ip address <ADDR></code>	<ADDR> – destination IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
		<code>esr(config-wan-target)# ipv6 address <IPV6-ADDR></code>	<IPV6-ADDR> – destination IPv6 address, defined as X:X:X:X where each part takes values in hexadecimal format [0..FFFF].
13	Enable the target check.	<code>esr(config-wan-target)# enable</code>	
Commands for 13-17 items should be applied on interfaces/tunnels in MultiWAN.			
14	Enable WAN mode on the interface for IPv4/IPv6 stack.	<code>esr(config-if-gi)# wan load-balance enable</code>	
		<code>esr(config-if-gi)# ipv6 wan load-balance enable</code>	
15	Set the amount of ineffective attempts to	<code>esr(config-if-gi)# wan load-balance failure-count <VALUE></code>	<VALUE> – number of attempts, takes values in the range of [1..10].

	check the connection, after which, if there is not response from the opposing side, the connection is considered to be inactive (optionally).	<code>esr(config-if-gi)# ipv6 wan load-balance failure-count <VALUE></code>	Default value: 1
16	Set the amount of successful attempts to check the connection, after which, if successful, the connection is considered to be active again. (optionally).	<code>esr(config-if-gi)# wan load-balance success-count <VALUE></code> <code>esr(config-if-gi)# ipv6 wan load-balance success-count <VALUE></code>	<VALUE> – number of attempts, takes values in the range of [1..10]. Default value: 1
17	Set a neighbour's IP address that will be indicated as one of the gateways in a static route created by MultiWAN service.	<code>esr(config-if-gi)# wan load-balance nexthop { <IP> dhcp enable tunnel enable }</code>	<IP> – destination IP address (gateway), defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]. dhcp enable – if IP address on the interface is obtained via DHCP client, a gateway from DHCP server is used. tunnel enable – use a destination address as nexthop - p-t-p. Applicable for the interfaced being connected that operate via ppp.
		<code>esr(config-if-gi)# ipv6 wan load-balance nexthop { <IPV6> }</code>	<IPV6> – destination IPv6 address (gateway), defined as X:X:X:X::X where each part takes values in hexadecimal format [0..FFFF].
18	This command will be checking the IP addresses from the integrity check list. If one of the nodes being checked is unavailable, the gateway will be considered to be unavailable.	<code>esr(config-if-gi)# wan load-balance target-list { check- all <NAME> }</code>	<NAME> – run check on the basis of a certain target list (specified in item 7). check-all – run check on the basis of all targets in the list.
		<code>esr(config-if-gi)# ipv6 wan load-balance target-list { check- all <NAME> }</code>	
19	Write static routes through WAN (if required).	<code>esr(config)# ip route <SUBNET> wan load- balance rule <ID> [<METRIC>]</code>	<ID> – identifier of the rule being created (see item 2). <METRIC> – route metric, takes values of [0..255].
		<code>esr(config)# ipv6 route <SUBNET> wan load-balance rule <ID> [<METRIC>]</code>	

7.43.2 Configuration example

Objective:

Configure route to the server (108.16.0.1/28) with the load balancing option.

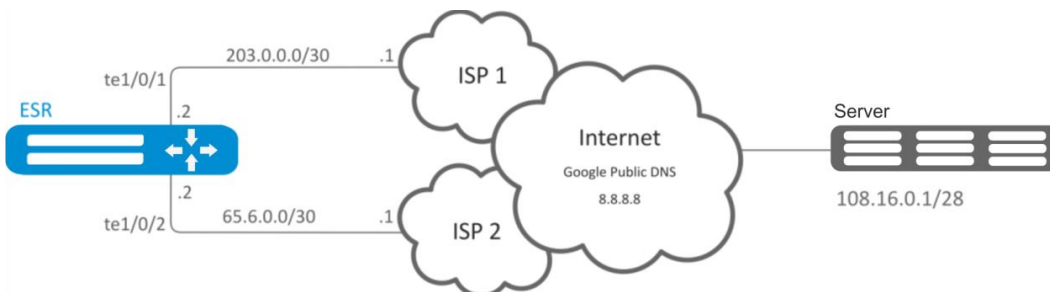


Figure 85 – Network structure

Solution:

First, do the following:

- Configure zones for te1/0/1 and te1/0/2 interfaces.
- Specify IP addresses for te1/0/1 and te1/0/2 interfaces.

Main configuration step:

Configure routing:

```
esr(config)# ip route 108.16.0.0/28 wan load-balance rule 1
```

Create WAN rule:

```
esr(config)# wan load-balance rule 1
```

Specify affected interfaces:

```
esr(config-wan-rule)# outbound interface tengigabitethernet 1/0/2
esr(config-wan-rule)# outbound interface tengigabitethernet 1/0/1
```

Enable the created balancing rule and exit the rule configuration mode:

```
esr(config-wan-rule)# enable
esr(config-wan-rule)# exit
```

Create a list for the connection integrity check:

```
esr(config)# wan load-balance target-list google
```

Create integrity check target:

```
esr(config-target-list)# target 1
```

Specify address to be checked, enable check for the specified address and exit:

```
esr(config-wan-target)# ip address 8.8.8.8
esr(config-wan-target)# enable
esr(config-wan-target)# exit
```

Configure interfaces. In te1/0/1 interface configuration mode, specify nexthop:

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if)# wan load-balance nexthop 203.0.0.1
```

In te1/0/1 interface configuration mode, specify a list of targets for connection check:

```
esr(config-if)# wan load-balance target-list google
```

In te1/0/1 interface configuration mode, enable WAN mode and exit:

```
esr(config-if)# wan load-balance enable
esr(config-if)# exit
```

In te1/0/2 interface configuration mode, specify nexthop:

```
esr(config)# interface tengigabitethernet 1/0/2
esr(config-if)# wan load-balance nexthop 65.6.0.1
```

In te1/0/2 interface configuration mode, specify a list of targets for connection check:

```
esr(config-if)# wan load-balance target-list google
```

In te1/0/2 interface configuration mode, enable WAN mode and exit:

```
esr(config-if)# wan load-balance enable
esr(config-if)# exit
```

To switch into redundancy mode, configure the following:

Proceed to WAN rule configuration mode:

```
esr(config)# wan load-balance rule 1
```

MultiWAN function may also work in redundancy mode when traffic is directed to the active interface with the highest weight. To enable this mode, use the following command:

```
esr(config-wan-rule)# failover
```

7.44 SNMP configuration

SNMP (Simple Network Management Protocol) is a protocol designed for device management in IP networks featuring TCP/UDP architecture. SNMP provides management data as variables that describe the configuration of a system being managed.

7.44.1 Configuration algorithm

Step	Description	Command	Keys
1	Enable SNMP server	<code>esr(config)# snmp-server</code>	
2	Specify community for the access via SNMPv2c.	<code>esr(config)# snmp-server community</code>	<COMMUNITY> – community for the access via SNMP;

		<pre><COMMUNITY> [<TYPE>] [{ <IP-ADDR> <IPV6- ADDR> } [view <VIEW- NAME>] [vrf <VRF>]</pre>	<p><TYPE> – access level: ro – read-only access; rw – read and write access. <IP-ADDR> – IP address of the client provided with the access, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]. <IPV6-ADDR> – client IPv6 address, defined as X:X:X:X where each part takes values in hexadecimal format [0..FFFF]; <VIEW-NAME> – SNMP view profile name, set by the string of up to 31 characters; <VRF> – name of a VRF instance from which the access will be allowed, set by the string of up to 31 characters.</p>
3	Set the value of SNMP variable that contains contact information	<pre>esr(config)# snmp- server contact <CONTACT></pre>	<CONTACT> – contact information, set by the string of up to 255 characters.
4	Set the DSCP code value for the use in IP headers of SNMP server egress packets (optionally).	<pre>esr(config)# snmp- server dscp <DSCP></pre>	<DSCP> – DSCP code value, takes values in the range of [0..63]. Default value: 63.
5	Enable router reboot by using snmp messages (optionally)	<pre>esr(config)# snmp- server system-shutdown</pre>	
6	Create SNMPv3 user.	<pre>esr(config)# snmp- server user <NAME></pre>	<NAME> – user name, set by the string of up to 31 characters.
7	Set the value of SNMP value that contains the information on the device location	<pre>esr(config)# snmp- server location <LOCATION></pre>	<LOCATION> – information on the device location, set by the string of up to 255 characters.
8	Specify user access level via SNMPv3.	<pre>esr(config-snmp-user) # access <TYPE></pre>	<TYPE> – access level: ro – read-only access; rw – read and write access.
9	Specify user security mode via SNMPv3.	<pre>esr(config-snmp-user) # authentication access <TYPE></pre>	<TYPE> – security mode: auth – used only for authentication; priv – both authentication and data encryption are used.
10	Specify SNMPv3 queries authentication algorithm.	<pre>esr(config-snmp-user) # authentication algorithm <ALGORITHM></pre>	<ALGORITHM> – encryption algorithm: md5 – password is encrypted by md5 algorithm; sha1 – password is encrypted by sha1 algorithm.
11	Set the password for SNMPv3 queries authentication.	<pre>esr(config-snmp-user) # authentication key ascii-text { <CLEAR- TEXT> encrypted <ENCRYPTED-TEXT> }</pre>	<CLEAR-TEXT> – password, set by the string of 8 to 16 characters; encrypted – when specifying a command, an encrypted password is set: <ENCRYPTED-TEXT> – encrypted password of 8 to 16 bytes (from 16 to 32 characters) in hexadecimal format (0xYYYY ...) or (YYYY ...).
12	Enable filtration and set the profile of IP addresses from which SNMPv3 packets with the given SNMPv3 user name can be received.	<pre>esr(config-snmp-user) # client-list <NAME></pre>	<NAME> – name of a previously created object-group, set by the string of up to 31 characters.

13	Enable filtration and set IPv4/IPv6 address which is provided with the access to the router as the given SNMPv3 user.	<code>esr(config-snmp-user)# ip address <ADDR></code>	<ADDR> – IP address of the client provided with the access, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255].
		<code>esr(config-snmp-user)# ipv6 address <ADDR></code>	<IPV6-ADDR> – client IPv6 address, defined as X:X:X:X where each part takes values in hexadecimal format [0..FFFF].
14	Enable SNMPv3 user.	<code>esr(config-snmp-user)# enable</code>	Default value: process is disabled.
15	Specify the transmitted data encryption algorithm.	<code>esr(config-snmp-user)# privacy algorithm <ALGORITHM></code>	<ALGORITHM> – encryption algorithm: aes128 – use AES-128 encryption algorithm; des – use DES encryption algorithm.
16	Set password for the transmitted data encryption.	<code>esr(config-snmp-user)# privacy key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }</code>	<CLEAR-TEXT> – password, set by the string of 8 to 16 characters; <ENCRYPTED-TEXT> – encrypted password of 8 to 16 bytes (from 16 to 32 characters) in hexadecimal format (0xYYYY ...) or (YYYY ...).
17	Set the snmp view profile permitting or denying the access to one or another OID for user.	<code>esr(config-snmp-user)# view <VIEW-NAME></code>	<VIEW-NAME> – SNMP view profile name on the basis of which the access to OID is provided, set by the string of up to 31 characters.
18	Enable SNMP notifications transmission to the specified IP address and switch to SNMP notifications configuration mode.	<code>esr(config)# snmp-server host { <IP-ADDR> <IPV6-ADDR> } [vrf <VRF>]</code>	<IP-ADDR> – IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]. <IPV6-ADDR> – IPv6 address, defined as X:X:X:X where each part takes values in hexadecimal format [0..FFFF]; <VRF> – name of a VRF instance where the SNMP notifications collector is located, set by the string of up to 31 characters.
19	Define the port of SNMP notifications collector on the remote server (optionally).	<code>esr(config-snmp-host)# port <PORT></code>	<PORT> – UDP port number in the range of [1..65535]. Default value: 162.
20	Set the filtration of SNMP notifications being sent.	<code>esr(config)# snmp-server filter <TYPE></code>	<TYPE> – type of filtered messages. May take the following values: bras, config, environment, files-operations, interfaces, links. Additional parameters depend on the filter type. See CLI command reference guide.
21	Create snmp view profile permitting or denying the access to one of another OID for community (SNMPv2) and user (SNMPv3).	<code>esr(config)# snmp-server view <VIEW-NAME></code>	<VIEW-NAME> – SNMP view profile name, set by the string of up to 31 characters.

7.44.2 Configuration example

Objective:

Configure SNMPv3 server with authentication and data encryption for 'admin' user. ESR router IP address: 192.168.52.41, server IP address: 192.168.52.8.



Figure 86 – Network structure

Solution:

First, do the following:

- Specify zone for gi1/0/1 interface;
- Configure IP address for gi1/0/1 interface.

Main configuration step:

Enable SNMP server:

```
esr(config) # snmp-server
```

Create SNMPv3 user:

```
esr(config) # snmp-server user admin
```

Specify security mode:

```
esr(snmp-user) # authentication access priv
```

Specify authentication algorithm for SNMPv3 requests:

```
esr(snmp-user) # authentication algorithm md5
```

Set the password for SNMPv3 request authentication:

```
esr(snmp-user) # authentication key ascii-text 123456789
```

Specify the transmitted data encryption algorithm:

```
esr(snmp-user) # privacy algorithm aes128
```

Set password for the transmitted data encryption:

```
esr(snmp-user) # privacy key ascii-text 123456789
```

Enable SNMPv3 user:

```
esr(snmp-user) # enable
```

Define receiver-server of Trap-PDU messages:

```
esr(config) # snmp-server host 192.168.52.41
```

7.45 BRAS (Broadband Remote Access Server) configuration

7.45.1 Configuration algorithm

Step	Description	Command	Keys
1	Add RADIUS server to the list of used servers and switch to its configuration mode.	<code>esr(config)# radius - server host { <IP- ADDR> <IPV6-ADDR> } [vrf <VRF>]esr(config- radius-server)#</code>	<IP-ADDR> – RADIUS server IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <IPV6-ADDR> – RADIUS server IPv6 address, defined as X:X:X::X where each part takes values in hexadecimal format [0..FFFF]. <VRF> – VRF instance name, set by the string of up to 31 characters.
2	Set the password for authentication on remote RADIUS server.	<code>esr(config-radius- server)# key ascii- text { <TEXT> encrypted <ENCRYPTED- TEXT> }</code>	<TEXT> – string of [8..16] ASCII characters; <ENCRYPTED-TEXT> – encrypted password, [8..16] bytes size, set by the string of [16..32] characters.
3	Create AAA profile.	<code>esr(config)# aaa radius-profile <NAME></code>	<NAME> – server profile name, set by the string of up to 31 characters.
4	Specify RADIUS server in AAA profile.	<code>esr(config-aaa-radius- profile)# radius- server host { <IP- ADDR> <IPV6-ADDR> }</code>	<IP-ADDR> – RADIUS server IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255]; <IPV6-ADDR> – RADIUS server IPv6 address, defined as X:X:X::X where each part takes values in hexadecimal format [0..FFFF].
5	Create DAS server.	<code>esr(config)# das-server <NAME></code>	<NAME> – DAS server name, set by the string of up to 31 characters.
6	Set the password for authentication on remote DAS server.	<code>esr(config-das- server)# key ascii-text {<TEXT> encrypted <ENCRYPTED-TEXT> }</code>	<TEXT> – string of [8..16] ASCII characters; <ENCRYPTED-TEXT> – encrypted password, [8..16] bytes size, set by the string of [16..32] characters.
7	Create AAA DAS profile.	<code>esr(config)# aaa das- profile <NAME></code>	<NAME> – DAS profile name, set by the string of up to 31 characters.
8	Specify DAS server in DAS profile.	<code>esr(config-aaa-das- profile)# das-server <NAME></code>	<NAME> – DAS server name, set by the string of up to 31 characters.
9	Configure BRAS.	<code>esr(config)# subscriber-control [vrf <VRF>]</code>	<VRF> – VRF instance name, set by the string of up to 31 characters, within which the user control will operate.
10	Select the profile of dynamic authorization servers to which CoS queries from PCRF will be sent.	<code>esr(config-subscriber- control)# aaa das- profile <NAME></code>	<NAME> – DAS profile name, set by the string of up to 31 characters.
11	Select RADIUS server profile to obtain the user service parameters.	<code>esr(config-subscriber- control)# aaa services-radius- profile <NAME></code>	<NAME> – RADIUS server profile name, set by the string of up to 31 characters.
12	Select RADIUS server profile to obtain the user session parameters.	<code>esr(config-subscriber- control)# aaa sessions-radius- profile <NAME></code>	<NAME> – RADIUS server profile name, set by the string of up to 31 characters.
13	Set router IP address that will be used as source IP	<code>esr(config-subscriber- control)# nas-ip- address <ADDR></code>	<ADDR> – source IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255];

	address in transmitted RADIUS packets.		
14	Enable session authentication by MAC address (optionally).	<code>esr(config-subscriber-control)# session mac-authentication</code>	
15	Organize transparent filter-based transmission of administrative traffic (DHCP, DNS and etc.).	<code>esr(config-subscriber-control)# bypass-traffic-acl <NAME></code>	<NAME> – name of the ACL being bound, set by the string of up to 31 characters.
16	Switch to the default service configuration mode.	<code>esr(config-subscriber-control)# default-service</code>	
17	Bind the specified QoS class to the default service.	<code>esr(config-subscriber-default-service)# class-map <NAME></code>	<NAME> – name of the class being bound, set by the string of up to 31 characters.
18	Specify a name of the URL list that will be used to filtrate HTTP/HTTPS traffic of non-authenticated users.	<code>esr(config-subscriber-default-service)# filter-name { local<LOCAL-NAME> remote<REMOTE-NAME> }</code>	<LOCAL-NAME> – URL profile name, set by the string of up to 31 characters; <REMOTE-NAME> – remote server URL list name, set by the string of up to 31 characters.
19	Specify the actions that should be applied for HTTP/HTTPS packets, whose URL is included in the list of URL assigned by the “filter-name” command.	<code>esr(config-subscriber-default-service)# filter-action<ACT></code>	<ACT> – allocated action: permit – traffic transfer is permitted; deny – traffic transfer is denied. redirect <URL> – redirect to the specified URL will be carried out, set by the string of up to 255 characters.
20	Specify the actions that should be applied for HTTP/HTTPS packets, whose URL is not included in the list of URL assigned by the “filter-name” command.	<code>esr(config-subscriber-default-service)# default-action<ACT></code>	<ACT> – allocated action: permit – traffic transfer is permitted; deny – traffic transfer is denied. redirect <URL> – redirect to the specified URL will be carried out, set by the string of up to 255 characters.
21	Enable user control profile.	<code>esr(config-subscriber-control)# enable</code>	
22	Change the identifier of a network interface (physical, sub interface or network bridge) (optionally).	<code>esr(config-if)# location <ID></code>	<ID> – network interface identifier, set by the string of up to 220 characters.
23	Enable user control on the interface.	<code>esr(config-if-gi)# service-subscriber-control {any object-group <NAME>}</code>	<NAME> – IP addresses profile name, set by the string of up to 31 characters.
24	Enable iterative query of quota value when it expires for user services with a configured restriction on the amount of traffic or time (optionally).	<code>esr(config-subscriber-control)# quota-expired-reauth</code>	
25	Enable session authentication by IP address (optionally).	<code>esr(config-subscriber-control)# session ip-authentication</code>	
26	Enable transparent transmission of backup traffic for BRAS (optionally).	<code>esr(config-subscriber-control)# backup traffic-processing transparent</code>	

27	Specify the interval after which currently unused URL lists will be removed (optionally).	<code>esr(config)# subscriber-control unused-filters-remove- delay <DELAY></code>	<DELAY> – time interval in seconds, takes values of [10800..86400].
28	Specify the interval after which, if a user has not sent any packets, the session is considered to be outdated and is removed from the device (optionally).	<code>esr(config-subscriber- default- service)#session- timeout <SEC></code>	<SEC> – time interval in seconds, takes values of [120..3600].
29	Specify the VRRP group on the basis of which user control service status is determined (primary/redundant) (optionally).	<code>esr(config-subscriber- control)# vrrp-group <GRID></code>	<GRID> – VRRP router group identifier, takes values in the range of [1..32].
30	Define destination TCP ports from which the traffic will be redirected to the router HTTP Proxy server (optionally).	<code>esr(config-subscriber- control)# ip proxy http listen-ports <NAME></code>	<NAME> – TCP/UDP ports profile name, set by the string of up to 31 characters.
31	Define HTTP Proxy server port on the router (optionally).	<code>esr(config-subscriber- control)# ip proxy http redirect-port <PORT></code>	<PORT> – port number, set in the range of [1..65535].
32	Define destination TCP ports from which the traffic will be redirected to the router HTTPS Proxy server (optionally).	<code>esr(config-subscriber- control)# ip proxy https listen-ports <NAME></code>	<NAME> – TCP/UDP ports profile name, set by the string of up to 31 characters.
33	Define HTTPS Proxy server port on the router (optionally).	<code>esr(config-subscriber- control)# ip proxy https redirect-port <PORT></code>	<PORT> – port number, set in the range of [1..65535].
34	Set router IP address that will be used as source IP address in HTTP/HTTPS packets transmitted by Proxy server (optionally).	<code>esr(config-subscriber- control)# ip proxy source-address <ADDR></code>	<ADDR> – source IP address, defined as AAA.BBB.CCC.DDD where each part takes values of [0..255];
35	Specify URL address of the server providing lists of traffic filtration applications (optionally)	<code>esr(config)# subscriber-control apps-server-url <URL></code>	<URL> – reference address, set by the string from 8 to 255 characters.
36	Enable the application control on the interface (optionally).	<code>esr(config-if-gi)# subscriber-control application-filter <NAME></code>	<NAME> – application profile name, set by the string of up to 31 characters.
37	Set/clear the upper bound of BRAS sessions amount (optionally).	<code>esr(config-subscriber- control)# thresholds sessions-number high <Threshold></code>	<Threshold> – BRAS sessions amount, [0-50000] – for ESR-1700 [0-10000] – for ESR-1200/1000 [0-1000] – for ESR-100/200
38	Set/clear the lower bound of BRAS sessions amount (optionally).	<code>esr(config-subscriber- control)# thresholds sessions-number low <Threshold></code>	<Threshold> – BRAS sessions amount, [0-50000] – for ESR-1700 [0-10000] – for ESR-1200/1000 [0-1000] – for ESR-100/200

7.45.2 Example of configuration with SoftWLC

Objective: Provide access to the Internet only to authorized users.

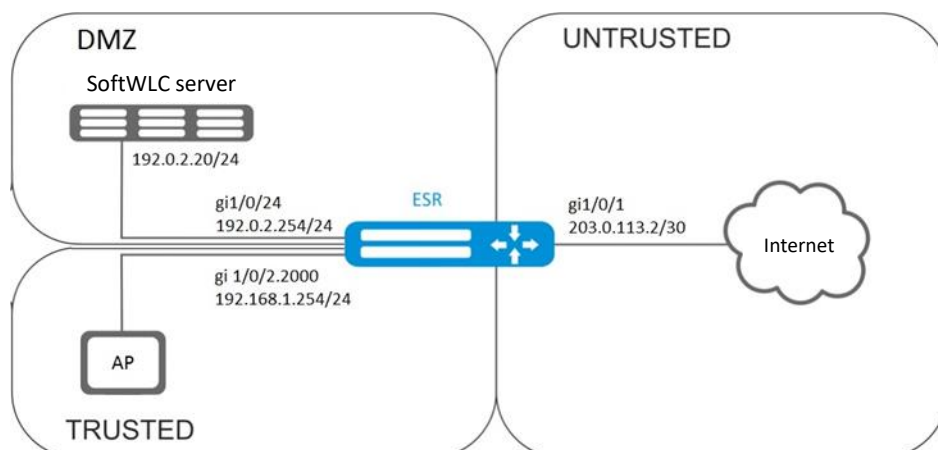


Figure 87 – Network structure

Solution:

SoftWLC server keeps accounts data and tariff plan parameters. You can obtain more detailed information on installation and configuring SoftWLC server using following links:

<http://kcs.eltex.nsk.ru/articles/960> – general article of SoftWLC;

<http://kcs.eltex.nsk.ru/articles/474> – SoftWLC installation from repositories.

The BRAS license is obligatory for router, after its activation you can start device configuring.

Create 3 security zones, according to the network structure depicted in Figure 87:

```
esr# configure
esr(config)# security zone trusted
esr(config-zone)# exit
esr(config)# security zone untrusted
esr(config-zone)# exit
esr(config)# security zone dmz
esr(config-zone)# exit
```

Configure public port parameters and assign its default gateway:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# ip address 203.0.113.2/30
esr(config-if-gi)# service-policy dynamic upstream
esr(config-if-gi)# exit
esr(config)# ip route 0.0.0.0/0 203.0.113.1
```

Configure port in direction to the SoftWLC server:

```
esr (config)# interface gigabitethernet 1/0/24
esr (config-if-gi)# security-zone dmz
esr (config-if-gi)# ip address 192.0.2.1/24
esr (config-if-gi)# exit
```

Configure port for Wi-Fi access point connection:

```

esr(config)# bridge 2
esr(config-bridge)# security-zone trusted
esr(config-bridge)# ip address 192.168.0.254/24
esr(config-bridge)# ip helper-address 192.0.2.20
esr(config-bridge)# service-subscriber-control object-group users
esr(config-bridge)# location ssid1
esr(config-bridge)# enable
esr(config-bridge)# exit
esr(config)# interface gigabitethernet 1/0/2.2000
esr(config-subif)# bridge-group 1
esr(config-subif)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# service-policy dynamic downstream
esr(config-if-gi)# exit

```



Customer connection must be implemented through sub-interfaces to bridges. Selection of tariff plan depends on Location parameter (see bridge 2 configuration).

The module which is responsible for AAA operations is based on eltex-radius and available by SoftWLC IP address. Numbers of ports for authentication and accounting in the example below are the default values for SoftWLC.

Define parameters for interaction with the module:

```

esr(config)# radius-server host 192.0.2.20
esr(config-radius-server)# key ascii-text password
esr(config-radius-server)# auth-port 31812
esr(config-radius-server)# acct-port 31813
esr(config-radius-server)# exit

```

Create AAA profile:

```

esr(config)# aaa radius-profile RADIUS
esr(config-aaa-radius-profile)# radius-server host 192.0.2.20
esr(config-aaa-radius-profile)# exit

```

Specify parameters for access to DAS (Direct-attached storage) server:

```

esr(config)# object-group network server
esr(config-object-group-network)# ip address-range 192.0.2.20
esr(config-object-group-network)# exit
esr(config)# das-server CoA
esr(config-das-server)# key ascii-text password
esr(config-das-server)# port 3799
esr(config-das-server)# clients object-group server
esr(config-das-server)# exit
esr(config)# aaa das-profile CoA
esr(config-aaa-das-profile)# das-server CoA
esr(config-aaa-das-profile)# exit

```

The traffic from trusted zone is blocked before authentication as well as DHCP and DNS requests. You need to configure allowing rules in order to pass DHCP and DNS requests:

```

esr(config)# ip access-list extended DHCP
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any

```

```
esr(config-acl-rule)# match source-port 68
esr(config-acl-rule)# match destination-port 67
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 11
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 53
esr(config-acl-rule)# enable
esr(config-acl-rule)#exit
esr(config-acl)# exit
```

Then, create rules for redirecting to portal and passing traffic to the Internet:

```
esr(config)# ip access-list extended WELCOME
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
esr (config)# ip access-list extended INTERNET
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
```

Specify web resources which are available without authorization:

```
esr(config)# object-group url defaultservice
esr(config-object-group-url)# url http://eltex.nsk.ru
esr(config-object-group-url)# exit
```

The URL filtering lists are kept on SoftWLC server (you need to change only IP address of SoftWLC server, if addressing is different from the example. Leave the rest of URL without changes):

```
esr(config)# subscriber-control filters-server-url
http://192.0.2.20:7070/Filters/file/
```

Configure and enable BRAS, define NAS IP as address of the interface interacting with SoftWLC (gigabitethernet 1/0/24 in the example):

```
esr(config)# subscriber-control
esr(config-subscriber-control)# aaa das-profile CoA
esr(config-subscriber-control)# aaa sessions-radius-profile RADIUS
esr(config-subscriber-control)# nas-ip-address 192.0.2.1
esr(config-subscriber-control)# session mac-authentication
esr(config-subscriber-control)# bypass-traffic-acl DHCP
esr(config-subscriber-control)# default-service
esr(config-subscriber-default-service)# class-map INTERNET
esr(config-subscriber-default-service)# filter-name local defaultservice
esr(config-subscriber-default-service)# filter-action permit
```

```

esr(config-subscriber-default-service)# default-action redirect
http://192.0.2.20:8080/eltex_portal/
esr(config-subscriber-default-service)# session-timeout 3600
esr(config-subscriber-default-service)# exit
esr(config-subscriber-control)# enable
esr(config-subscriber-control)# exit

```

Configure rules for transition between security zones.

```

esr(config)# object-group service telnet
esr(config-object-group-service)# port-range 23
esr(config-object-group-service)# exit
esr(config)# object-group service ssh
esr(config-object-group-service)# port-range 22
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_server
esr(config-object-group-service)# port-range 67
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_client
esr(config-object-group-service)# port-range 68
esr(config-object-group-service)# exit
esr(config)# object-group service ntp
esr(config-object-group-service)# port-range 123
esr(config-object-group-service)# exit

```

Enable access to the Internet from trusted and dmz zones:

```

esr(config)# security zone-pair trusted untrusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair dmz untrusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair dmz trusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit

```

Enable DHCP transmitting from trusted to dmz:

```

esr (config)# security zone-pair trusted dmz
esr (config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp

```

```
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match source-port dhcp_client
esr(config-zone-pair-rule)# match destination-port dhcp_server
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

Enable ICMP transmission to the device. For BRAS operation you need to open ports for web proxying - TCP 3129/3128 (NetPortDiscovery Port/Active API Server port:

```
esr(config)# object-group service bras
esr(config-object-group-service)# port-range 3129
esr(config-object-group-service)# port-range 3128
esr(config-object-group-service)# exit
esr(config)# security zone-pair trusted self
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol tcp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match source-port any
esr(config-zone-pair-rule)# match destination-port bras
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
esr(config)# security zone-pair dmz self
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
```

Activate DHCP-Relay:

```
esr(config)# ip dhcp-relay
```

Configure SNAT for gigabitethernet 1/0/1 port:

```
esr(config)# nat source
esr(config-snat)# ruleset inet
esr(config-snat-ruleset)# to interface gigabitethernet 1/0/1
```

```

esr(config-snat-ruleset)# rule 10
esr(config-snat-rule)# match source-address any
esr(config-snat-rule)# action source-nat interface
esr(config-snat-rule)# enable
esr(config-snat-rule)# end

```

7.45.3 Example of configuration without SoftWLC

Objective: Configure BRAS without SoftWLC support.

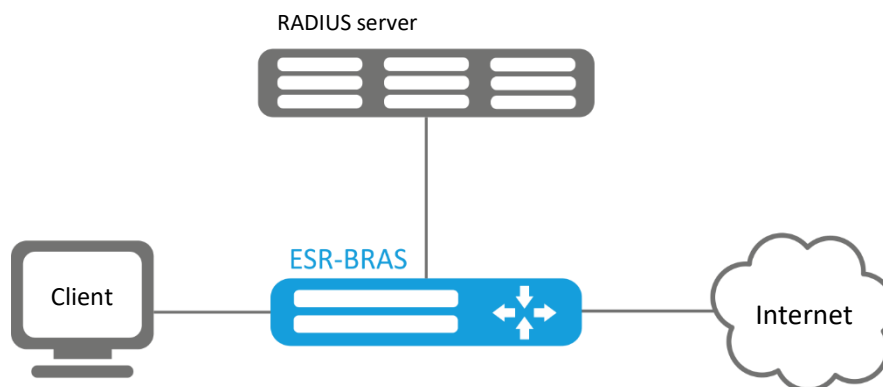


Figure 88 – Network structure

Given: Subnet with clients 10.10.0.0/16, subnet for working with FreeRADIUS server 192.168.1.1/24

Solution:

Step 1: RADIUS server configuration.

For FreeRADIUS server, you need to specify the subnet that can send the queries and add a user list. To do this, add the following to the users file in the directory with FreeRADIUS server configuration files:

User profile:

```
<MACADDR> Cleartext-Password := <MACADDR>
```

#User name

```
User-Name = <USER_NAME>,
```

#Maximum session lifetime

```
Session-Timeout = <SECONDS>,
```

#Maximum session lifetime when the system is idle

```
Idle-Timeout = <SECONDS>,
```

#Session statistics update time

```
Acct-Interim-Interval = <SECONDS>,
```

#Service name for a session (A - the service is enabled, N - the service is disabled)

```
Cisco-Account-Info = "{A|N}<SERVICE_NAME>"
```

Service profile:

```
<SERVICE_NAME> Cleartext-Password := <MACADDR>
```

Matches class-map name in ESR settings

```
Cisco-AVPair = "subscriber:traffic-class=<CLASS_MAP>",
```

Action that is applied to the traffic by ESR (permit, deny, redirect)

```
Cisco-AVPair = "subscriber:filter-default-action=<ACTION>",
```

The ability of IP flows passing (enabled-uplink, enabled-downlink, enabled, disabled)

```
Cisco-AVPair = "subscriber:flow-status=<STATUS>"
```

Add a subnet, in which ESR is located, to the clients.conf file:

```
client ESR {  
    ipaddr = <SUBNET>  
    secret = <RADIUS_KEY>  
}
```

In this case the RADIUS server configuration will be as follows:

Add the following strings to the “clients.conf” file:

```
client BRAS {  
    ipaddr = 192.168.1.1  
    secret = password  
}
```

Add the following strings to the “users” file (specify a client MAC address instead of <MAC>):

```
"54-E1-AD-8F-37-35" Cleartext-Password := "54-E1-AD-8F-37-35"  
User-Name = <Bras_user>,  
Session-Timeout = 259200,  
Idle-Timeout = 259200,  
Cisco-AVPair += "subscriber:policer-rate-in=1000",  
Cisco-AVPair += "subscriber:policer-rate-out=1000",  
Cisco-AVPair += "subscriber:policer-burst-in=188",  
Cisco-AVPair += "subscriber:policer-burst-out=188",  
Cisco-Account-Info = "AINTERNET"  
  
INTERNET Cleartext-Password := "INTERNET"  
User-Name = "INTERNET",  
Cisco-AVPair = "subscriber:traffic-class=INTERNET",  
Cisco-AVPair += "subscriber:filter-default-action=permit"
```

Step 2: ESR configuration.

BRAS functional configuration requires the BRAS licence:

```
esr(config)# do sh licence
```


Licence information

Name: Eltex

Version: 1.0

Type: ESR-X

S/N: NP00000000

MAC: XX:XX:XX:XX:XX:XX

Features:

BRAS - Broadband Remote Access Server

Configuration of parameters for the interaction with RADIUS server:

```
esr(config)# radius-server host 192.168.1.2
esr(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-radius-server)# source-address 192.168.1.1
esr(config-radius-server)# exit
```

Create AAA profile:

```
esr(config)# aaa radius-profile bras_radius
esr(config-aaa-radius-profile)# radius-server host 192.168.1.2
esr(config-aaa-radius-profile)# exit
esr(config)# aaa radius-profile bras_radius_servers
esr(config-aaa-radius-profile)# radius-server host 192.168.1.2
esr(config-aaa-radius-profile)# exit
```

Specify parameters for the DAS server:

```
esr(config)# das-server das
esr(config-das-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-das-server)# exit
esr(config)# aaa das-profile bras_das
esr(config-aaa-das-profile)# das-server das
esr(config-aaa-das-profile)# exit
```

```
esr(config)# vlan 10
esr(config-vlan)# exit
```

Then, create rules for redirecting to portal and passing traffic to the Internet:

```
esr(config)# ip access-list extended BYPASS
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port 68
esr(config-acl-rule)# match destination-port 67
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 2
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
```

```
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 53
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config)# ip access-list extended INTERNET
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config)# ip access-list extended WELCOME
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 443
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 20
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 8443
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 30
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 80
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 40
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 8080
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
```

! Configuration of filtration by URL is obligatory. It is necessary to configure http-proxy filtration on BRAS for non-authorized users:

```
esr(config)# object-group url defaultserv
esr(config-object-group-url)# url http://eltex.nsk.ru
esr(config-object-group-url)# url http://ya.ru
esr(config-object-group-url)# url https://ya.ru
esr(config-object-group-url)# exit
```

Configure and enable BRAS, define NAS IP as address of the interface interacting with RADIUS server (gigabitethernet 1/0/2 in the example):

```

esr(config)# subscriber-control
esr(config-subscriber-control)# aaa das-profile bras_das
esr(config-subscriber-control)# aaa sessions-radius-profile bras_radius
esr(config-subscriber-control)# aaa services-radius-profile bras_radius_servers
esr(config-subscriber-control)# nas-ip-address 192.168.1.1
esr(config-subscriber-control)# session mac-authentication
esr(config-subscriber-control)# bypass-traffic-acl BYPASS
esr(config-subscriber-control)# default-service
esr(config-subscriber-default-service)# class-map BYPASS
esr(config-subscriber-default-service)# filter-name local defaultserv
esr(config-subscriber-default-service)# filter-action permit
esr(config-subscriber-default-service)# default-action redirect http://192.168.1.2:8080/eltex_portal
esr(config-subscriber-default-service)# session-timeout 121
esr(config-subscriber-default-service)# exit
esr(config-subscriber-control)# enable
esr(config-subscriber-control)# exit

```

Perform the following settings on the interfaces that require BRAS operation (minimum one interface is required for the successful start):

```

esr(config)# bridge 10
esr(config-bridge)# vlan 10
esr(config-bridge)# ip firewall disable
esr(config-bridge)# ip address 10.10.0.1/16
esr(config-bridge)# ip helper-address 192.168.1.2
esr(config-bridge)# service-subscriber-control any
esr(config-bridge)# location USER
esr(config-bridge)# protected-ports
esr(config-bridge)# protected-ports exclude vlan
esr(config-bridge)# enable
esr(config-bridge)# exit

```

Configure port towards the SoftWLC server:

```

esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# ip address 192.168.1.1/24
esr(config-if-gi)# exit

```

Port towards the Client:

```

esr(config)# interface gigabitethernet 1/0/3.10
esr(config-subif)# bridge-group 10
esr(config-subif)# ip firewall disable
esr(config-subif)# exit

```

Configure SNAT for gigabitethernet 1/0/2 port:

```

esr(config)# nat source
esr(config-snat)# ruleset factory
esr(config-snat-ruleset)# to interface gigabitethernet 1/0/2
esr(config-snat-ruleset)# rule 10
esr(config-snat-rule)# description "replace 'source ip' by outgoing interface ip address"
esr(config-snat-rule)# match protocol any
esr(config-snat-rule)# match source-address any
esr(config-snat-rule)# match destination-address any
esr(config-snat-rule)# action source-nat interface
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
esr(config-snat)# exit

```

```
esr(config)# ip route 0.0.0.0/0 192.168.1.2
```

The configuration changes come into effect after applying the following commands:

```
esr(config) # do commit
esr(config) # do confirm
```

To view the information and statistics on the user control sessions, use the following command:

```
esr # sh subscriber-control sessions status
```

Session id	User name	IP address	MAC address	Interface	Domain
1729382256910270473	Bras_user	10.10.0.3	54:e1:ad:8f:37:35	gi1/0/3.10	--

7.46 VoIP configuration

VoIP is a set of protocols that allow to transmit voice data via IP networks. Within the given device, VoIP is used to connect analogue telephones to an IP network with the possibility to make phone calls.

7.46.1 SIP profile configuration process

Step	Description	Command	Keys
1	Configure a SIP profile	<code>esr(config)# sip profile <NUM></code>	<NUM> – SIP profile number, set in the form of a digit from 1 to 5.
2	Configure a primary SIP proxy server and registration server	<code>esr(config-sip-profile)# proxy primary</code>	
3	Configure a SIP proxy server	<code>esr(config-voip-sip-proxy)# ip address proxy-server <IP></code>	<IP> – proxy server IP address
4	Configure a SIP proxy server port	<code>esr(config-voip-sip-proxy)# ip port proxy-server <PORT></code>	<PORT> – number of proxy server UDP port, takes values of [1..65535]. If standard 5060 port is used, you do not need to specify it.
5	Configure a registration server address	<code>esr(config-voip-sip-proxy)# ip address registration-server <IP></code>	<IP> – registration server IP address.
6	Configure a registration server port:	<code>esr(config-voip-sip-proxy)# ip port registration-server <PORT></code>	<PORT> – number of registration server UDP port, takes values of [1..65535]. If standard 5060 port is used, you do not need to specify it.
7	Enable registration	<code>esr(config-voip-sip-proxy)# registration</code>	
8	Enable proxy server and registration server:	<code>esr(config-voip-sip-proxy)# enable</code>	
9	Configure a registration server address	<code>esr(config-voip-sip-proxy)# ip address registration-server <IP></code>	<IP> – registration server IP address.
10	Configure a registration server port:	<code>esr(config-voip-sip-proxy)# ip port registration-server <PORT></code>	<PORT> – number of registration server UDP port, takes values of [1..65535]. If standard 5060 port is used, you do not need to specify it.
11	Specify SIP domain in which the device is located	<code>esr(config-sip-profile)# sip-domain address <ADDRESS></code>	<ADDRESS> – SIP domain in which the device is located, set by ipv4 address or domain name.
12	Enable the use of SIP domain when registering	<code>esr(config-sip-profile)# sip-domain</code>	

		<code>registration enable</code>	
13	SIP profile configuration	<code>esr(config)# sip profile <NUM></code>	<NUM> – SIP profile number, set in the form of a digit from 1 to 5.
14	Assign a dial plan to the current SIP profile	<code>esr(config-sip-profile)# dialplan pattern <DNAME></code>	<DNAME> – name of the dial plan, set by the string of up to 31 characters.
15	Enable SIP profile	<code>esr(config-sip-profile)# enable</code>	

7.46.2 FXS/FXO ports configuration process

Step	Description	Command	Keys
1	Switch to the FXO/FXS ports configuration mode	<code>esr(config)# interface voice-port <NUM></code>	<NUM> – port number, takes values of [1..4].
2	Assign a subscriber number reserved for a telephone port	<code>esr(config-voice-port-fxs)# sip user phone <PHONE></code>	<PHONE> – subscriber number reserved for a telephone port, set by the string of up to 50 characters.
3	Assign the user name matched with the port	<code>esr-12v(config-voice-port-fxs)# sip user display-name <LOGIN></code>	<LOGIN> – user name displayed in the Display-Name field, set by the string of up to 31 characters.
4	Select SIP profile for a certain port.	<code>esr(config-voice-port-fxs)# profile sip <PROFILE></code>	<PROFILE> – SIP profile number, set in the form of a digit from 1 to 5.
5	Configure a login for authentication	<code>esr(config-voice-port-fxs)# authentication name <LOGIN></code>	<LOGIN> – login for authentication, set by the string of up to 31 characters
6	Configure a password for authentication	<code>esr(config-voice-port-fxs)# authentication password <PASS></code>	<PASS> – authentication password, set by the string of up to 16 characters.
7	Enable FXO port	<code>esr(config)# interface voice-port <NUM></code>	<NUM> – FXO port number, takes values of [1..4].
8	Assign a subscriber number reserved for a telephone port	<code>esr(config-voice-port-fxo)# sip user phone <PHONE></code>	<PHONE> – subscriber number reserved for a telephone port.
9	Specify UDP port from which and to which the FXO set will send and receive SIP messages	<code>esr(config-voice-port-fxo)# sip port <PORT></code>	<PORT> – UDP port number.
10	Assign the user name matched with the port	<code>esr(config-voice-port-fxo)# sip user display-name <LOGIN></code>	<LOGIN> – user name displayed in the Display-Name field, set by the string of up to 31 characters.
11	Configure a login for authentication	<code>esr(config-voice-port-fxo)# authentication name <LOGIN></code>	<LOGIN> – login for authentication, set by the string of up to 31 characters.
12	Configure a password for authentication	<code>esr(config-voice-port-fxo)# authentication password <PASS></code>	<PASS> – authentication password, set by the string of up to 16 characters.
13	Enable the number transmission to PSTN	<code>esr(config-voice-port-fxo)# pstn transmit-number</code>	
14	Disable prefix transmission	<code>esr(config-voice-port-fxo)# no pstn transmit-prefix</code>	
15	Enable the “Hotline PSTN to IP” service	<code>esr(config-voice-port-fxo)# hotline ipt</code>	
16	Number of the subscriber that will receive calls from PSTN	<code>esr(config-voice-port-fxo)# hotline number ipt <PHONE></code>	<PHONE> – phone number that calls are made to when using the service, takes the value from 1 to 50. “Hot/Warm line” in the direction from analogue telephone line to VoIP.

7.46.3 Dial plan configuration process

Step	Description	Command	Keys
1	Create a dial plan	<code>esr(config)# dialplan pattern <DNAME></code>	<DNAME> – name of the dial plan, set by the string of up to 31 characters.
2	Add dial rules	<code>esr(config-dial-ruleset)# pattern <REGEXP></code>	<REGEXP> - regular expression specifying the dial plan. Set by the string of up to 1024 characters. Regular expression rules are described in Section 7.46.5
3	Enable the dial plan	<code>esr(config-dial-ruleset)# enable</code>	

7.46.4 VoIP configuration example

Objective:

Connect analogue telephones and fax modems to the IP network via ESR router. SIP server, located on the ESR, functions as proxy server and registration server.

Solution:



Figure 89 – Network structure

Configure a SIP profile:

```
esr(config)# sip profile 1
```

Configure a primary SIP proxy server and registration server:

```
esr(config-sip-profile)# proxy primary
```

Configure SIP proxy server address (use an embedded SIP server as SIP proxy server):

```
esr(config-voip-sip-proxy)# ip address proxy-server 192.0.2.5
```

Configure a SIP proxy server port:

```
esr(config-voip-sip-proxy)# ip port proxy-server 5080
```

If standard 5060 port is used, you do not need to specify it.

If it is necessary to use the registration, you should perform the following steps:

Configure registration server address (use an embedded SIP server as registration server):

```
esr(config-voip-sip-proxy)# ip address registration-server 192.0.2.5
```

Configure a registration server port:

```
esr(config-voip-sip-proxy)# ip port registration-server 5080
```

If standard 5060 port is used, you do not need to specify it.

Enable registration:

```
esr(config-voip-sip-proxy)# registration
```

Enable proxy server and registration server:

```
esr(config-voip-sip-proxy)# enable
```

This completes the configuration of SIP proxy server and registration server:

```
esr(config-voip-sip-proxy)# exit
```

The next step is to continue SIP profile configuration.



If the embedded SIP server is used as SIP proxy and registration server, you should perform its configuration according to the manual “SIP server configuration on ESR series routers: ESR-12V, ESR-12VF, ESR-14VF».

Configure a SIP domain:

```
esr(config-sip-profile)# sip-domain address sipdomain.com
```

If it is necessary to use SIP Domain for the registration, use the following command:

```
esr(config-sip-profile)# sip-domain registration enable
```

In this configuration all calls will be directed to SIP proxy server. If it is necessary to specify another direction for outgoing calls, you should perform the following:

Create a dial plan, see Section 7.46.5.

Next, assign the created dial plan to the SIP profile:

```
esr(config)# sip profile 1
```

```
esr(config-sip-profile)# dialplan pattern firstDialplan
```

This completes the configuration of a dial plan for SIP profile.

Enable SIP profile:

```
esr-12v(config-sip-profile)# enable
```

This completes the baseline configuration of SIP profile:

```
esr(config-sip-profile)# exit
```

The next step is to configure subscriber ports:

```
esr(config)# interface voice-port 1
```

Specify a subscriber number:

```
esr(config-voice-port-fxs)# sip user phone 4101
```

Specify a displayed name:

```
esr(config-voice-port-fxs)# sip user display-name user-one
```

Used SIP profile:

```
esr(config-voice-port-fxs)# profile sip 1
```

Configure login and password for authentication

```
esr(config-voice-port-fxs)# authentication name login-4101
```

```
esr(config-voice-port-fxs)# authentication password superpassword
```

This completes the baseline configuration of a subscriber port:

```
esr(config-voice-port-fxs)# exit
```

7.46.5 Dial plan configuration example

Objective:

Configure a dial plan in such a manner that calls to local numbers (connected to the given ESR-12V) are switched locally and calls to all other directions – through SIP proxy.

Solution:

Create a dial plan:

```
esr(config)# dialplan pattern firstDialplan
```

Dial plan is specified by regular expressions:

```
esr(config-dial-ruleset)# pattern "<regular expressions>"
```

For the objective mentioned above, the "<regular expressions>" is given by:

"S5, L5 (410[1-3]@{local} | [xABCD*#].S)"

where:

410[1-3]@{local} – calls to 4101, 4102, 4103 numbers will be switched locally;

[xABCD*#].S – calls to all other numbers will be directed to SIP proxy.

Enable the dial plan:


```
esr(config-dial-ruleset)# enable
```

Dial plan configuration is finished.

```
esr(config-dial-ruleset)# exit
```

Regular expression structure:

Sxx, Lxx (),

where:

xx – S and L timers arbitrary values;

() – dial plan boundaries.

The basis is designators for dialled digits sequence to be written. Sequence of digits is written by several designators: digits dialled from a phone keyboard: 0, 1, 2, 3, ..., 9, # and *.



The use of # character in dial plan can block the completion of dialling with this key!

Bracketed sequence of digits corresponds to any bracketed character.

- Example: ([1239]) – corresponds to any of 1, 2, 3 or 9 digits.

You may specify the hyphenated range of characters. Usually it is used inside the square brackets.

- Example 1: (1-5) – any digit from 1 to 5.
- Example 2: ([1-39]) – example from the previous item with another recording format.

'X' character corresponds to any digit from 0 to 9.

- Example: (1XX) – any three-digit number starting with 1.

«.» – repeating the previous character from 0 to infinity number of times.

«+» – repeating the previous character from 1 to infinity number of times.

{a,b} – repeating the previous character from a to b times;

{a,} – repeating the previous character equal to or more than a times;

{,b} – repeating the previous character equal to or less than b times.

- Example: (810X.) – international number with any amount of digits.

Settings influencing on the dial plan processing:

- Interdigit Long Timer (letter "L" in dial plan entry) – timeout to enter the next digit if there are no templates matching the dialled combination;
- Interdigit Short Timer (letter "S" in dial plan entry) – timeout to enter the next digit if at least one pattern completely matches the dialled combination and there is at least one more pattern before matching with that it is necessary to perform the extension dialling.

Additional features:

1. Replacement of a dialled sequence

Syntaxes: `<arg1:arg2>`

This feature allows to replace a dialled sequence to any sequence of dialled characters. In this case, the second argument must be specified with a certain value, both arguments may be empty.

- Example: (`<83812:> XXXXXX`) – this entry will correspond to dialled digits 83812 but the sequence will be omitted and will not be transmitted to the SIP server.

2. Insert a tone in the set

When connecting the intercity (in office stations – a city), you may usually hear a station's response that can be implemented by inserting a comma into the desired position of the numbers sequence.

- Example: (`8, 770`) – when dialling 8770 number, the 8 digit will be followed by a continuous tone.

3. Disable number dialling

If you add an exclamation sign '!' to the end of number template, the number set corresponding to the template will be blocked.

- Example: (`8 10X xxxxxxx ! | 8 xxx xxxxxxx`) – expression allows to dial only between long-distance call numbers and excludes international calls.

4. Replace the values of number dialling timers

Timers values can be assigned both to a whole dial plan and to a certain template. "S" is responsible for the «*Interdigit Short Timer*» setup and "L" – for the «*Interdigit Long Timer*» setup. Timers values can be specified for all templates in a dial plan if the values are listed before the opening parenthesis.

- Example: `S4 (8XXX.)` or `S4,L8 (XXX)`

If these values are specified only in one of the sequences, then they are valid only for it. Also, in this case it is not necessary to put a colon between the key and the timeout value, the value can be located anywhere in the template.

- Example: (`S4 8XXX. | XXX`) or (`[1-5] XX S0`) – entry generates an instant call forwarding when dialling a three-digit number starting with 1,2, ... ,5.

5. Dialling via direct address (IP Dialing)

"@" character put after the number means that the address of the server, to which the dialled number call will be sent, will be specified. It is recommended to use «*IP Dialing*» as well as receiving and transmission of calls without registration («*Call Without Reg*», «*Answer Without Reg*»). This can help in case of server failure.

In addition, the format of address with IP Dialing can be used in numbers intended to forward calls.

- Example 1: (`8 xxx xxxxxxx`) – 11-digit number, starting with 8.
- Example 2: (`8 xxx xxxxxxx | <:8495> xxxxxxx`) – 11-digit number, starting with 8; if 7-digit number was entered, add 8495 to the number being transmitted.
- Example 3: (`0[123] | 8 [2-9]xx [2-9]xxxxx`) – emergency service numbers dialling as well as unusual dialling of long-distance call numbers.

- Example 4: (S0 <:82125551234>) – shortcut dialling of a specified number, analogy of the «Hotline» mode on other gateways.
- Example 5: (S5 <:1000> | xxxx) – the given dial plan allows to dial any number consisting of digits; if nothing is entered during 5 seconds, call number 1000 (let it be a secretary).
- Example 6: (8, 10x. | 1xx@10.110.60.51:5060) – the given dial plan allows to dial numbers starting with 810 and containing at least one digit after “810”. After entering 8, the “station response” signal will be returned. Also a set of three-digit numbers starting with “1”, the Invite of which will be sent to 10.110.60.51 IP address and 5060 port, will be returned.
- Example 7: (S3 *xx# | #xx# | #xx# | *xx*x+#) – management and the use of VAS.

Local calls inside the device may be required in some cases. If the device’s IP address is not known or is periodically changed, it is convenient to use the reserved word {local} as the server address, which means sending the corresponding sequence of digits to the device’s own address.

- Example: (123@{local}) – call to 123 will be proceeded locally inside the device.

7.46.6 FXO port configuration

Objective:

Add the ability to make a call to PSTN subscriber through the ESR-12V FXO port.

Solution:

Enable FXO port:

```
esr(config)# interface voice-port 4
```

Specify FXO port number same as PSTN access prefix:

```
esr(config-voice-port-fxo)# sip user phone 9
```

Specify UDP port from which and to which the FXO set will send and receive SIP messages:

```
esr(config-voice-port-fxo)# sip port 5064
```

Specify a displayed name:

```
esr(config-voice-port-fxo)# sip user display-name user-one
```

Configure login and password for authentication

```
esr(config-voice-port-fxo)# authentication name login-9
```

```
esr(config-voice-port-fxo)# authentication password superpassword
```

Assign SIP profile to FXO port:

```
esr(config-voice-port-fxo)# profile sip 1
```

Enable the number transmission to PSTN:

```
esr(config-voice-port-fxo) # pstn transmit-number
```

Disable prefix transmission:

```
esr(config-voice-port-fxo) # no pstn transmit-prefix
```

For outgoing calls to work, you need to specify the following rule in the dial plan settings, which means that outgoing calls to numbers with prefix 9 are routed locally to the FXO set:

```
9x. @ {local} :5064
```

This completes the baseline configuration of outgoing calls to PSTN. To make a call to PSTN, you should dial the callee number with the specified prefix (FXO set phone number).

To receive calls from PSTN, you should select the subscriber that will receive all calls from PSTN, let it be a subscriber with number 305.

Enable the “Hotline PSTN to IP” service:

```
esr(config-voice-port-fxo) # hotline ipt
```

Number of the subscriber that will receive calls from PSTN:

```
esr(config-voice-port-fxo) # hotline number ipt 305
```

This completes the baseline configuration of FXO port.

8 FREQUENTLY ASKED QUESTIONS

- **Receiving of routes, which are configured in VRF via BGP or/and OSPF, failed. The neighbouring is successfully installed, but record of routes in RIB is denied:
%ROUTING-W-KERNEL: Can not install route. Reached the maximum number of BGP routes in the RIB**

Allocate RIB resource for VRF (0 by default). Do it in VRF configuration mode:

```
esr(config)# ip vrf <NAME>
esr(config-vrf)# ip protocols ospf max-routes 12000
esr(config-vrf)# ip protocols bgp max-routes 1200000
esr(config-vrf)# end
```

- **SSH/Telnet sessions, which go through ESR router, are closing.**

Configure transmission of keepalive packets in order to keep session active. Keepalive transmission option is configured on SSH client, for instance, section "Connection" for PuTTY client.

It is possible to set time to closing inactive TCP sessions (1 hour in example):

```
esr(config)# ip firewall sessions tcp-established-timeout 3600
```

- **Firewall was disabled on interface. However access for active sessions from the port was not closed, according to security zone-pair rules, after including this interface to security zone, removing from 'ip firewall disable' configuration and applying changes.**

Changes in Firewall configuration will be active only for new sessions. The reset of Firewall active sessions does not occur. You can clear active sessions in firewall, using following command:

```
esr# clear ip firewall session
```

- **LACP does not launch on XG ports of ESR-1000/1200/1700**

Port-channel has speed 1000M mode by default. Enable speed 10G mode:

```
esr(config)# interface port-channel 1
esr(config-port-channel)# speed 10G
```

- **How to clear ESR configuration completely and reset it to factory default?**

Copy blank configuration in candidate-config and apply it in running-config.

```
esr# copy system:default-config system:candidate-config
```

Reset to factory default is similar.

```
esr# copy system:factory-config system:candidate-config
```

- **How to attach sub-interface to created VLAN?**

While sub-interface creation, VLAN is created and attached automatically (direct correlation index sub-VID).

```
esr(config)# interface gigabitethernet 1/0/1.100
```

Information messages are shown after applying:

```
2016-07-14T012:46:24+00:00 %VLAN: creating VLAN 100
```

- **Do the ESR-series routers have features for traffic analysis?**

Opportunity of analysing traffic through CLI interfaces is realized on ESR-series routers. A packet sniffer is launched by *monitor* command.

```
esr# monitor gigabitethernet 1/0/1
```

- **How to configure ip-prefix-list 0.0.0.0/0?**

Example of prefix-list configuration is shown below. The configuration allows route reception by default.

```
esr(config)# ip prefix-list eltex  
esr(config-pl)# permit default-route
```

- **Problem of asynchronous traffic transmission is occurred**

In case of asynchronous routing, Firewall will forbid "incorrect" ingress traffic (which does not open new connection and does not belong any established connection) for security reasons.

Allowing rule in Firewall does not solve the problem.

Firewall should be disabled on the ingress interface.

```
esr(config-if-gi)# ip firewall disable
```

TECHNICAL SUPPORT

For technical assistance in issues related to handling of ELTEXALATAU Ltd. equipment please address to Service Centre of the company:

Republic of Kazakhstan, 050032, Medeu district, microdistrict Alatau, 9 st. Ibragimova, 9

Phone:

+7(727) 220-76-10

+7(727) 220-76-07

E-mail: post@eltexalatau.kz

In official website of the ELTEXALATAU Ltd. you can find technical documentation and software for products, refer to knowledge base, consult with engineers of Service center in our technical forum:

<http://www.eltexalatau.kz/en/>