

Базовые настройки безопасности на коммутаторах MES

Докладчик: Владимир Носов
presale-инженер



Сегодня мы рассмотрим



- Создание нового пользователя
- Безопасные и небезопасные службы (telnet и ssh, http и https)
- Management ACL
- DHCP Snooping
- Dynamic ARP Inspection
- Port Security;
- IP source Guard;
- RADIUS/TACACS авторизация для управления коммутатором
- NAICE

Создание нового пользователя



Подключение «из коробки»

```
Telnet 192.168.1.239 admin/admin
```

Создание нового пользователя

```
MES2300-24 (config)#username vladimir password pa$$w0rd privilege 15
```

```
MES2300-24 (config)#username vladimir password encrypted  
b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb9  
80b1d7785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86  
encryption-algorithm sha-512 privilege 15
```

Парольная политика



```
MES2300-24 (config) #passwords aging 30
```

```
MES2300-24 (config) #passwords complexity enable  
MES2300-24 (config) #passwords complexity min-classes 4  
MES2300-24 (config) #passwords complexity min-length 12  
MES2300-24 (config) #passwords complexity not-current  
MES2300-24 (config) #passwords complexity not-username  
MES2300-24 (config) #passwords complexity no-repeat 2
```

Безопасные и небезопасные службы (telnet и ssh, http и https)



	Telnet	SSH
Безопасность	Всё передается в открытом виде	Шифрует весь трафик

Telnet



```
Frame 16: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp1s0, id 0
Ethernet II, Src: EltexEnterpr_64:28:c0 (ec:b1:e0:64:28:c0), Dst: TPLink_f9:7f:0e (5c:e9:31:f9:7f:0e)
Internet Protocol Version 4, Src: 10.10.10.20, Dst: 10.10.10.10
Transmission Control Protocol, Src Port: 23, Dst Port: 52628, Seq: 53, Ack: 43, Len: 12
Telnet
  Data: \r\n
  Data: User Name:
```

```
Frame 18: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface enp1s0, id 0
Ethernet II, Src: TPLink_f9:7f:0e (5c:e9:31:f9:7f:0e), Dst: EltexEnterpr_64:28:c0 (ec:b1:e0:64:28:c0)
Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.10.10.20
Transmission Control Protocol, Src Port: 52628, Dst Port: 23, Seq: 43, Ack: 65, Len: 1
Telnet
  Data: a
```

```
Frame 32: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp1s0, id 0
Ethernet II, Src: EltexEnterpr_64:28:c0 (ec:b1:e0:64:28:c0), Dst: TPLink_f9:7f:0e (5c:e9:31:f9:7f:0e)
Internet Protocol Version 4, Src: 10.10.10.20, Dst: 10.10.10.10
Transmission Control Protocol, Src Port: 23, Dst Port: 60284, Seq: 41, Ack: 8, Len: 20
Telnet
  Data: show running-config
```

```
Frame 39: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface enp1s0, id 0
Ethernet II, Src: EltexEnterpr_64:28:c0 (ec:b1:e0:64:28:c0), Dst: TPLink_f9:7f:0e (5c:e9:31:f9:7f:0e)
Internet Protocol Version 4, Src: 10.10.10.20, Dst: 10.10.10.10
Transmission Control Protocol, Src Port: 23, Dst Port: 60284, Seq: 64, Ack: 10, Len: 16
Telnet
  Data: no spanning-tree
```

Отключение telnet и http



```
MES2300-24(config)#no ip telnet server  
MES2300-24(config)#no ip http server
```

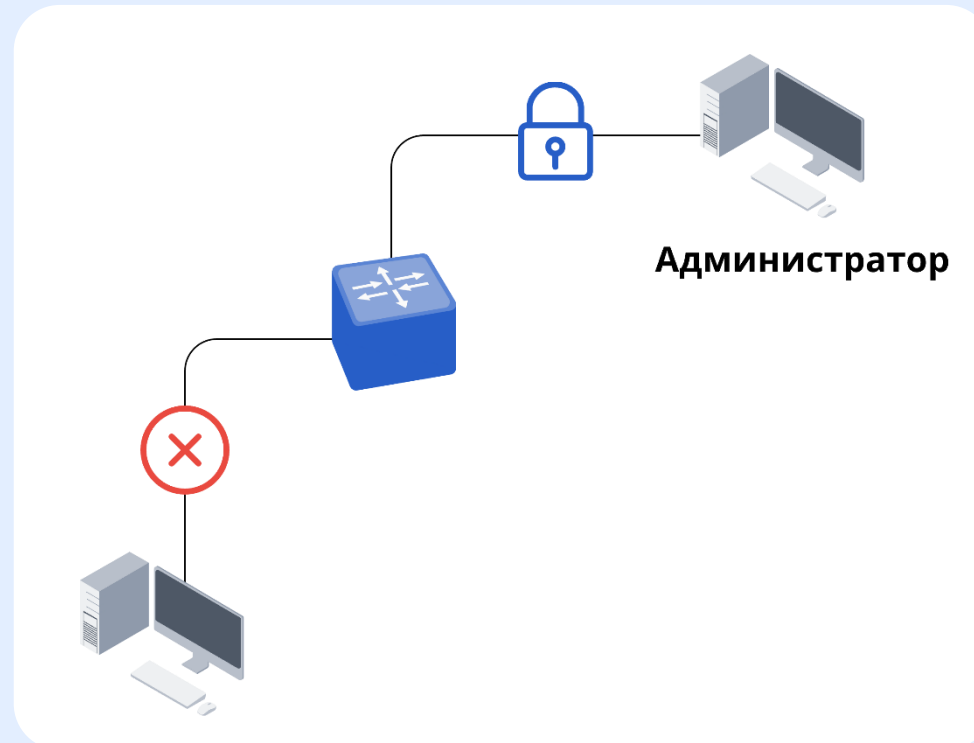
```
MES2300-24(config)#ip http secure-server  
MES2300-24(config)#ip ssh server
```

```
MES2300-24(config)#ip ssh cipher <...>  
MES2300-24(config)#ip ssh kex <...>
```

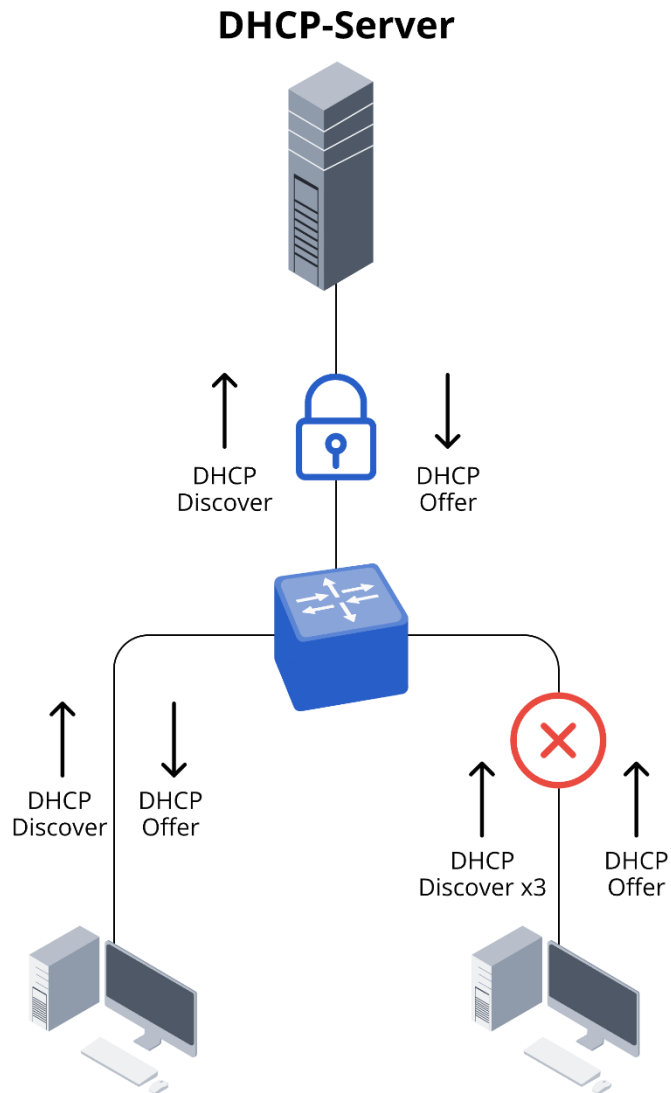
Management ACL



```
MES2300-24(config)#management access-list mgmt_list  
MES2300-24(config-macl)#permit ip-source 10.10.10.0 mask /24  
TenGigabitEthernet1/0/1  
MES2300-24(config-macl)#exit  
MES2300-24(config)#management access-class mgmt_list
```



DHCP Snooping



```
MES2300-24(config)#vlan 100 name clients_VLAN
MES2300-24(config)#interface vlan 100
MES2300-24(config-if)#ip address 10.10.10.10 /24
MES2300-24(config-if)#exit
MES2300-24(config)#ip dhcp snooping
MES2300-24(config)#ip dhcp snooping vlan 100
MES2300-24(config)#interface gigabitethernet1/0/1
MES2300-24(config-if)#switchport access vlan 100
MES2300-24(config-if)#ip dhcp snooping limit clients 2
MES2300-24(config)#interface TenGigabitEthernet1/0/1
MES2300-24(config-if)#switchport mode trunk
MES2300-24(config-if)#switchport trunk allowed vlan add 100
MES2300-24(config-if)#ip dhcp snooping trust
```

DHCP Snooping



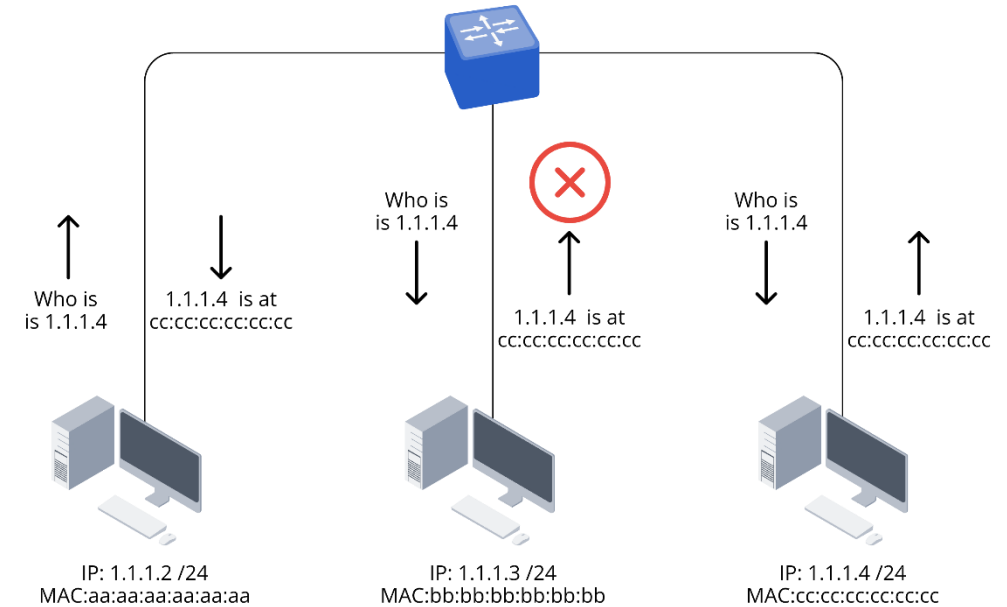
```
MES2300-24#show ip dhcp snooping binding
```

MAC Address	IP Address	Lease (sec)	Type	VLAN	Interface
ec:b1:e0:00:00:00	100.100.100.10	47	learned	100	gi1/0/1

Dynamic ARP Inspection



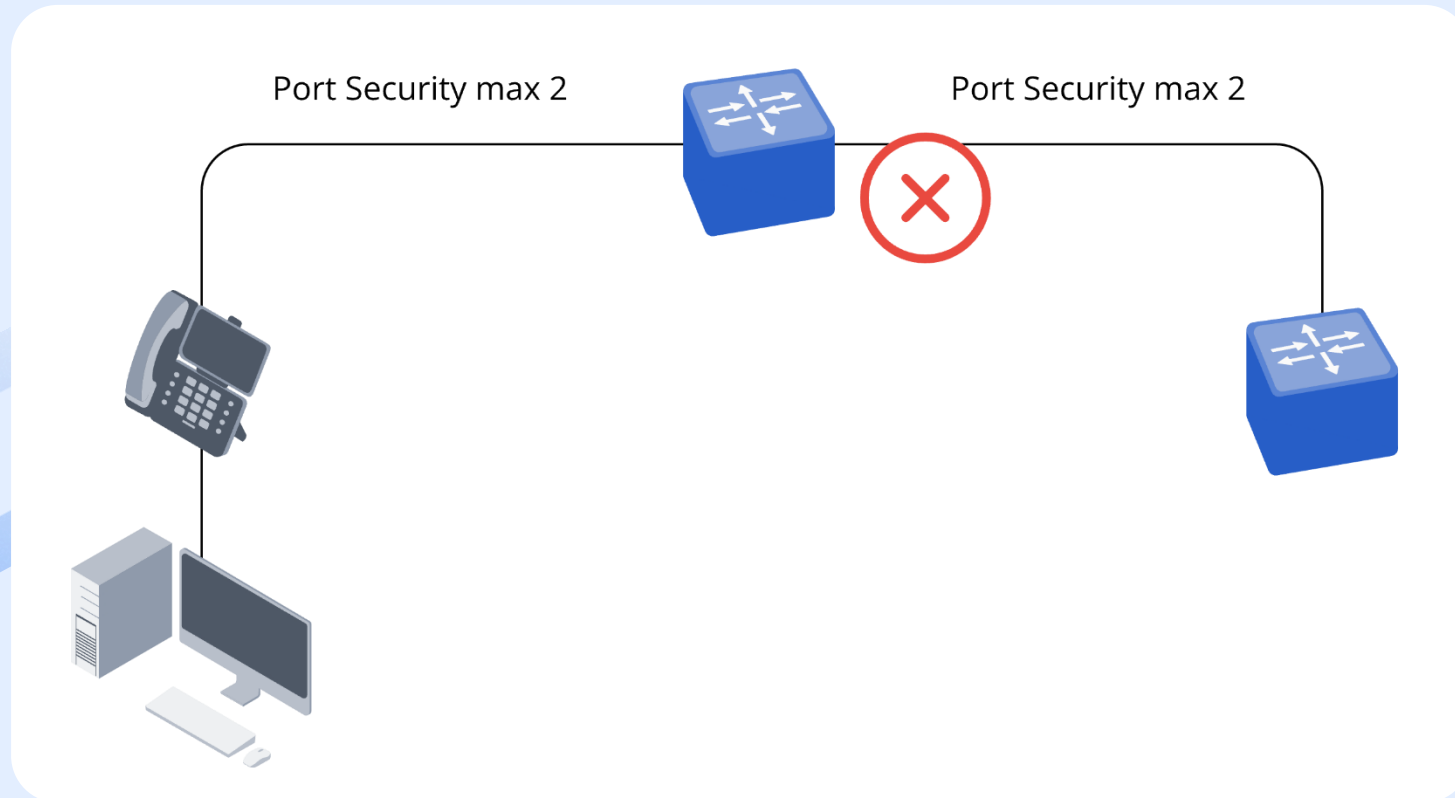
```
MES2300-24(config)#vlan 100 name clients_VLAN
MES2300-24(config)#interface vlan 100
MES2300-24(config-if)#ip address 10.10.10.10 /24
MES2300-24(config-if)#exit
MES2300-24(config)#ip dhcp snooping
MES2300-24(config)#ip dhcp snooping vlan 100
MES2300-24(config)#ip arp inspection
MES2300-24(config)#ip arp inspection vlan 100
MES2300-24(config)#interface range gigabitethernet1/0/1-3
MES2300-24(config-if)#switchport access vlan 100
MES2300-24(config)#interface TenGigabitEthernet1/0/1
MES2300-24(config-if)#switchport mode trunk
MES2300-24(config-if)#switchport trunk allowed vlan add 100
MES2300-24(config-if)#ip dhcp snooping trust
MES2300-24(config-if)#ip arp inspection trust
```



Port Security



```
MES2300-24 (config)#interface GigabitEthernet1/0/1  
MES2300-24 (config-if)#port security max 2  
MES2300-24 (config-if)#port security mode secure permanent  
MES2300-24 (config-if)#port security discard
```

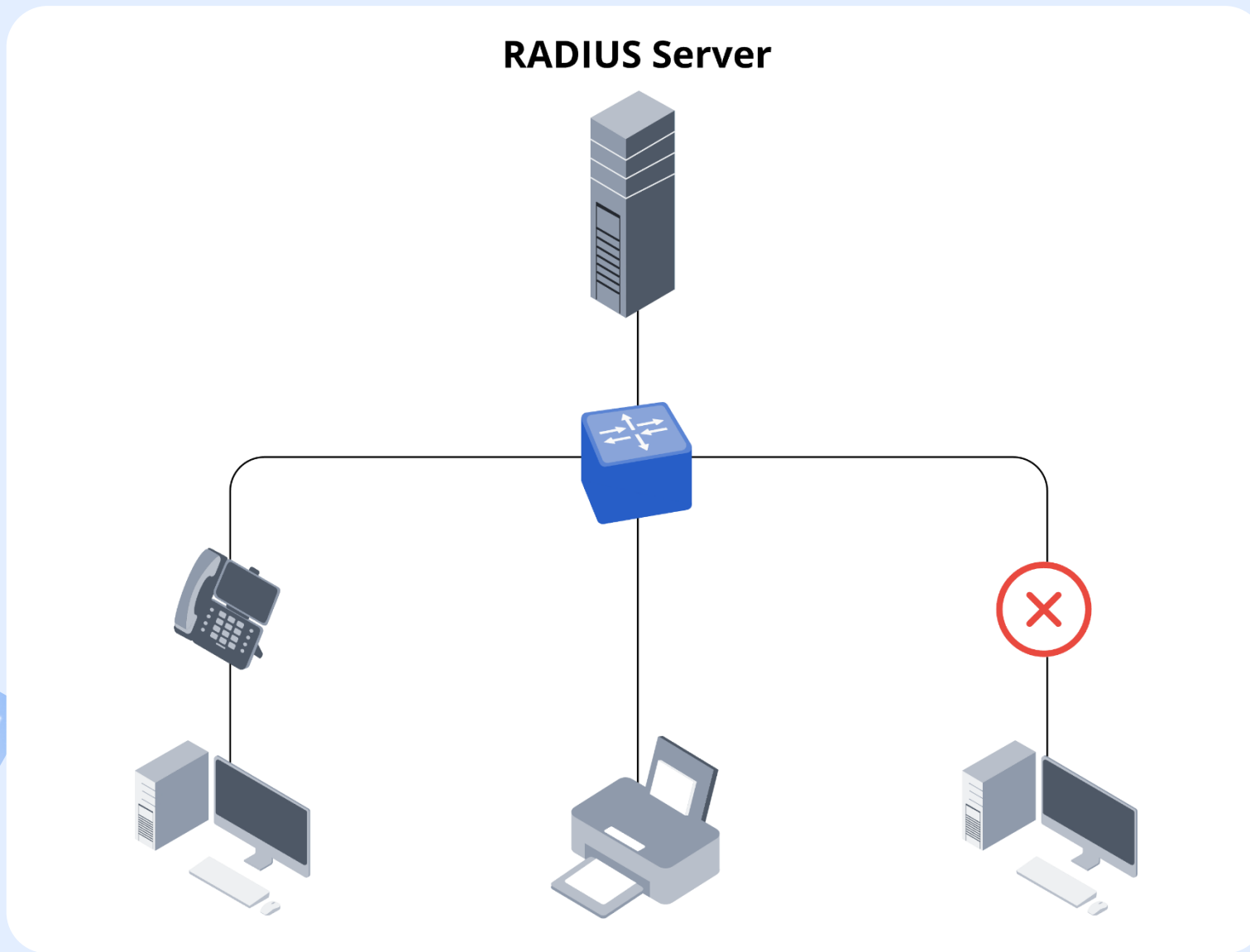


IP source Guard



```
MES2300-24(config)#vlan 100 name clients_VLAN
MES2300-24(config)#ip dhcp snooping
MES2300-24(config)#ip dhcp snooping vlan 100
MES2300-24(config)#ip source-guard
MES2300-24(config)#interface range gigabitethernet1/0/1-3
MES2300-24(config-if)#switchport access vlan 100
MES2300-24(config-if)#ip source-guard
MES2300-24(config-if)#ip source-guard mac-check
MES2300-24(config)#ip source-guard binding aa:aa:aa:aa:aa:aa
100 10.10.10.15 GigabitEthernet1/0/1
```

802.1x и RADIUS-авторизация клиентов



802.1x и RADIUS-авторизация клиентов



Глобальные настройки:

```
MES2300-24(config)#vlan 10 name clients_vlan
MES2300-24(config)#vlan 20 name voice
MES2300-24(config)#vlan 30 name printer
MES2300-24(config)#vlan 40 name guest_vlan
MES2300-24(config)#vlan 50 name critical_vlan
MES2300-24(config)#vlan 60 name RADIUS_vlan
MES2300-24(config)#interface vlan 60
MES2300-24(config-if)#ip address 192.168.1.10 /24
MES2300-24(config)#dot1x system-auth-control
MES2300-24(config)#radius-server host 192.168.1.150 key eltex
```

Глобальные VLAN:

```
MES2300-24(config)#interface vlan 40
MES2300-24(config-if)#dot1x guest-vlan
MES2300-24(config)#interface vlan 50
MES2300-24(config-if)#dot1x critical-vlan
```

802.1x и RADIUS-авторизация клиентов



Клиентский порт:

```
MES2300-24(config-if)#dot1x port-control auto
MES2300-24(config-if)#dot1x host-mode multi-sessions
MES2300-24(config-if)#dot1x reauthentication
MES2300-24(config-if)#dot1x authentication 802.1x mac
MES2300-24(config-if)#dot1x guest-vlan enable
MES2300-24(config-if)#dot1x critical-vlan enable
MES2300-24(config-if)#dot1x radius-attributes filter-id
MES2300-24(config-if)#dot1x radius-attributes vendor-specific data-filter
MES2300-24(config-if)#dot1x radius-attributes vlan static
MES2300-24(config-if)#switchport mode general
MES2300-24(config-if)#switchport general allowed vlan add 10 untagged
MES2300-24(config-if)#switchport general pvid 10
```

AAA TACACS+



```
MES2300-24(config)#enable password level 15 encrypted godemode
MES2300-24(config)#vlan 150 name tacacs_vlan
MES2300-24(config)#interface vlan 150
MES2300-24(config-if)#ip address 192.168.1.10 /24
MES2300-24(config-if)#exit
MES2300-24(config)#tacacs-server host 192.168.1.252 key Eltex
MES2300-24(config)#aaa authentication login authorization default tacacs local
MES2300-24(config)#aaa authentication enable default tacacs enable
MES2300-24(config)#aaa accounting login start-stop group tacacs+
MES2300-24(config)#aaa accounting commands stop-only group tacacs+
MES2300-24(config)#aaa authorization commands default group tacacs+ local
```



Network Access and Information Control Engine (NAICE)

программная система, предоставляющая централизованный контроль доступа пользователей к сети и обеспечивающая комплексное управление правами к её ресурсам



Добавление коммутатора



NAICE

Поиск Alt + S

Главная

Мониторинг

Администрирование

Пользователи системы

Сетевые ресурсы

Администрирование > Сетевые ресурсы > Устройства

Сетевые ресурсы

Устройства Группы устройств Профили устройств

+

🗑

↺

📌

📌

	Имя ↑	IPv4	Профиль	Протоколы	Местоположение	Тип устройства	Описание
--	-------	------	---------	-----------	----------------	----------------	----------



Добавление коммутатора



NAICE

Поиск Alt + S

Главная

Мониторинг

Администрирование

Пользователи системы

Сетевые ресурсы

Управление идентификацией

Политики

Элементы

Наборы политик

Профилирование

Гостевые порталы

Контроль сетевых устройств

Элементы политик

Политики сетевых устройств

СМС-шлюзы

Администрирование > Сетевые ресурсы > Устройства

← Добавление

Имя *

MES2300-24

Профиль *

DEFAULT

Модель

MES2300-24

Тип адреса

IPv4 адрес

Значение *

192.168.1.10

Описание

Введите описание

0 / 200

Профилирование

Гостевые порталы

Контроль сетевых устройств

Элементы политик

Политики сетевых устройств

СМС-шлюзы

Лицензирование

Документация

Оставить пожелания

Демонстрационный режим

ver 1.0

AD admin

Группы сетевых устройств

All Device Types *

All Device Types

All Locations *

All Locations

Mes-test *

Mes-test

Настройки аутентификации RADIUS

Секретный ключ *

eltex

Настройки аутентификации TACACS+

Секретный ключ

Введите текст

Добавление пользователя 802.1x



NAICE

Поиск Alt + S

Главная

Мониторинг

Администрирование

- Пользователи системы
- Сетевые ресурсы
- Управление идентификацией

Администрирование > Управление идентификацией > Пользователи

Управление идентификацией

Пользователи сети Группы пользователей сети Эндпоинты

+

🗑

↺

⬇

⬆

☐	Статус	Логин ↑
☐	✓ Включено	admin
☐	✓ Включено	naice



Добавление пользователя 802.1x



NAICE

Администрирование > Управление идентификаци...

Поиск Alt + S

Главная

Мониторинг

Администрирование

- Пользователи системы
- Сетевые ресурсы
- Управление идентификацией

Политики

- Элементы
- Наборы политик
- Профилирование

Гостевые порталы

Контроль сетевых устро...

- Элементы политик
- Политики сетевых устройств

← Добавление

☒ Включено

Логин *

user_1

Пароль *

user_1_password

Подтверждение пароля *

user_1_password

Имя

Введите имя

Фамилия

Введите фамилию

Email

Группы пользователя



☐	Имя ↑
☐	Internal DB users

Добавление устройства для tab-авторизации



NAICE

Поиск Alt + S

Главная

Мониторинг

Администрирование

- Пользователи системы
- Сетевые ресурсы
- Управление идентификацией

Администрирование > Управление идентификаци... > Эндпоинты

Управление идентификацией

Пользователи сети Группы пользователей сети **Эндпоинты** Группы эндпоинтов Внешн

+

↺

↻

🔍

🗑

⬇

⬆

☐	MAC адрес	Статус	Подробнее	Описание
☐	EC:08:6B:04:1A:08	✓ Подключено	📄	Discovered Endpoint
☐	68:13:E2:86:84:9C	✓ Подключено	📄	Discovered Endpoint

Добавление устройства для tab-авторизации



NAICE

Поиск Alt + S

Главная

Мониторинг

Администрирование

- Пользователи системы
- Сетевые ресурсы
- Управление идентификацией

Политики

- Элементы
- Наборы политик
- Профилирование

Гостевые порталы

Контроль сетевых устройств

- Элементы политик
- Политики сетевых устройств

СМС-шлюзы

Администрирование > Управление идентификаци...

← Добавление

MAC адрес

aa:aa:aa:aa:aa:aa

Описание

Введите описание

0 / 200

Общие атрибуты

☐ Ручное назначение политики

Политика профилирования *

Выберите политику

☒ Ручное назначение группы

Группа эндпоинта *

Endpoints

Добавление администратора для устройств



NAICE

Поиск Alt + S

Главная

Мониторинг

Администрирование

Политики

Гостевые порталы

Контроль сетевых устройств

Элементы политик

Политики сетевых устройств

СМС-шлюзы

Контроль сетевых устройств > Политики сетевых устройств

Политики сетевых устройств

Сбросить

Поиск

Политики выполняются в указанном порядке.

Вы можете изменить порядок перетаскиванием строки таблицы

Статус	Имя*	Описание	Условия*	Протокол	Количество срабатываний
По умолчанию	Default	Tacacs default policy set		PAP/ASCII	1703

Добавление администратора для устройств



Политика авторизации



	Статус	Имя*	Условия*	Профиль TACACS*	Набор команд TACACS*	Количество срабатываний
	Включено	Authorization rule	Добавить	Выберите профиль	Выберите набор	



Добавление администратора для устройств



Редактор

NEW

Атрибут *

Выберите значение

ⓘ Поле обязательно

Оператор *

Равно

☐ Is Not

Выбор атрибута для условия

Все

Device

Identity

LDAP

Network Access

TACACS+

Q username

x

Словарь

Выберите словарь

ID

ID

Атрибут

Словарь

ID

Username

Endpoint Identity

2

Guest endpoint username

Guest endpoints

2

Username

TACACS+

9

Добавление администратора для устройств



Редактор

NEW

Атрибут *

TACACS+·Username

Оператор *

Равно

Атрибут/значение *

admin_eltex

☐ Is Not

Дублировать

Сохранить

Добавление администратора для устройств



Политика авторизации

	Статус	Имя*	Условия*	Профиль TACACS*	Набор команд TACACS*	Количество срабатываний
	Включено	Authorization rule	TACACS+Username Равно admin_eltex	Maximum privilege	Allow all	





Design guide



Telegram-канал



**Мы всегда готовы к диалогу, разработке
и доработке решений под ваше техническое задание**



630020, г. Новосибирск, ул. Окружная, 29В
09:00 – 18:00 (GMT+7)
Понедельник – пятница



+7 (383) 274-10-01, 274-48-48
eltex@eltex-co.ru; eltex-co.ru

ООО «Предприятие «ЭЛТЕКС» | Российский разработчик и производитель телекоммуникационного оборудования