академия eltex
+7 (383) 274-48-01 +7 (383) 274-48-02 info@academy.eltex-co.ru

Использование маршрутизаторов Eltex ESR (продвинутый уровень) v.2

Длительность курса: 40 академических часов (5 дней)

Целевая аудитория:
- Системные администраторы;
- Специалисты технических и инженерных служб;
- Инженеры сопровождения и технической поддержки;
- Разработчики сетевого ПО.

Требования к участникам:
- Знание основ информационных технологий;
- Знание модели OSI и роли протоколов в передаче данных;
- Понимание базовых принципов маршрутизации;
- Знание основ построения сетей, протоколов TCP/IP и технологии Ethernet;
- Знание таких понятий как: коммутатор, маршрутизатор, IP-адрес, MAC-адрес, маска подсети и префикс, VLAN, режимы Trunk и Access, типы коннекторов, поля кадров Ethernet, инкапсуляция, деление IP-сетей на подсети и суммирование IP-сетей;
- Знание принципов работы основных протоколов и сервисов (DHCP, ACL, NAT, NTP, Syslog);
- Умение работать с CLI (без привязки к конкретному производителю).

Результаты обучения:

Уметь:
- соединять локальные сети с сетью Internet;
- внедрять технологии и сервисы QoS, VRRP, IPsec и DMVPN;
- расширять сети малого и среднего размера с помощью WAN-технологий;
- настраивать протоколы динамической маршрутизации (OSPF, BGP).

Знать:
- основы сетевых технологий: модели OSI, TCP/IP;
- основы работы протоколов IPv4;
- основные принципы обеспечения безопасности сетевых устройств;
- принципы построения избыточных сетей.

Владеть:
- навыками управления сетевыми устройствами;
- навыками настройки сетей среднего размера с использованием телекоммуникационного оборудования.

Учебно-тематический план

«Использование маршрутизаторов Eltex ESR (продвинутый уровень) v.2»

Наименование	Описание	Время
Тема:	**1. Обзор оборудования.**	**2 часа**
Описание:	1.1. Обзор маршрутизаторов ESR. 1.1.1. Модели ESR и их характеристики. 1.1.2. Функциональные возможности. 1.2. Устройство маршрутизатора. 1.2.1. Конструктивное исполнение. 1.2.2. Подключение маршрутизатора. 1.2.3. Загрузка маршрутизатора. 1.3. Командная строка. 1.3.1. Иерархия режимов и переходов между ними. 1.3.2. Конфигурационные файлы и commit/confirm. 1.3.3. Обновление ПО маршрутизатора. 1.4. Интерфейсы. 1.4.1. Режимы работы. 1.4.2. Возможности L2 функционала. 1.4.2.1. VLAN. 1.4.2.2. LLDP. 1.4.2.3. SPAN/RSPAN. 1.4.2.4. Private VLAN. 1.4.2.5. Dual-Homming. 1.4.3. Логические интерфейсы. 1.4.3.1. Loopback. 1.4.3.2. Sub. 1.4.3.3. Q-in-Q. 1.4.3.4. Bridge. 1.4.3.5. Port-channel. 1.4.4. Подключаемые интерфейсы. 1.4.4.1. USB-модем. 1.4.4.2. E1. 1.4.5. Диагностика интерфейсов. 1.5. Синхронизация времени. 1.5.1. Общие сведения. 1.5.2. Команды настройки.	1 час
Лабораторная:	1.Подключение и работа с CLI. 1.1. Переходы между режимами командной строки. 1.2. Очистка маршрутизатора.	1 час

Наименование	Описание	Время
Тема:	**2. Защита маршрутизатора.**	**2 часа**
Описание:	2.1. Базовая защита маршрутизатора.	1 час

	2.1.1. Аутентификация. 2.1.2. Пользователи. 2.1.3. Уровни привилегий. 2.1.4. Настройка паролей. 2.1.5. Учёт действий пользователей. 2.1.6. Консольный доступ. 2.1.7. Подключение к RADIUS-серверу. 2.1.8. Подключение к TACACS-серверу. 2.1.9. Подключение к LDAP-серверу. 2.2. Списки контроля доступа. 2.2.1. Общие сведения. 2.2.2. Принцип работы ACL. 2.2.3. Порядок настройки. 2.2.4. Поиск совпадений по параметрам. 2.2.5. Редактирование ACL-списка. 2.2.6. Диагностика. 2.2.7. Примеры настройки ACL. 2.3. Межсетевой экран ESR. 2.3.1. Общие сведения. 2.3.1.1. Межсетевой экран на основе зон безопасности. 2.3.1.2. Межсетевой экран с отслеживанием состояния сессий. 2.3.1.3. Порядок настройки межсетевого экрана. 2.3.2. Зоны безопасности. 2.3.3. Определение интерфейсов к зонам безопасности. 2.3.4. Создание списков object-group. 2.3.4.1. Object-group network. 2.3.4.2. Object-group service. 2.3.4.3. Object-group mac. 2.3.4.4. Object-group application. 2.3.4.5. Object-group url. 2.3.4.6. Object-group address-port. 2.3.5. Взаимодействие между зонами безопасности. 2.3.6. Правила межсетевого экрана. 2.3.6.1. Поиск совпадений по параметрам. 2.3.6.2. Порядок обработки правил. 2.3.6.3. Редактирование правил. 2.3.6.4. Логирование правил. 2.3.7. Диагностика. 2.3.8. Примеры настройки межсетевого экрана. 2.4. Преобразование сетевых адресов. 2.4.1. Общие сведения о NAT. 2.4.2. Source NAT. 2.4.3. Destination NAT. 2.4.4. Static NAT. 2.4.5. NAT ALG и firewall tracking. 2.5. Защита от сетевых атак. 2.5.1. DoS Defence. 2.5.2. Spy-Blocking. 2.5.3. Suspicious packets.	

	2.5.4. Пример настройки защиты от сетевых атак.	
Лабораторная:	2. Настройка защиты маршрутизатора. 2.1. Создание sub-интерфейса и настройка IP-адреса. 2.2. Создание и настройка пользователя. 2.3. Создание и настройка профиля аутентификации. 2.4. Аутентификация по RADIUS-серверу. 2.5. Аутентификация по TACACS-серверу. 2.6. Настройка межсетевого экрана ESR.	1 час

Наименование	**Описание**	**Время**
Тема:	**3. Туннелирование и удалённый доступ.**	**2 часа**
Описание:	3.1. Конфигурирование симметричных туннелей. 3.1.1. Общие сведения. 3.1.2. IP4IP4. 3.1.3. VTI. 3.1.4. GRE. 3.1.5. L2TPv3. 3.2. Сервисы удалённого доступа. 3.2.1. Общие сведения. 3.2.1.1. PPP. 3.2.1.2. PAP и CHAP. 3.2.1.3. MS-CHAP. 3.2.1.4.Multilink PPP (MLPPP). 3.2.2. PPPoE-клиент. 3.2.3. PPTP. 3.2.3.1. PPTP-сервер. 3.2.3.2. PPTP-клиент. 3.2.4. L2TP. 3.2.4.1. L2TP-сервер. 3.2.4.2. L2TP-клиент. 3.2.5. WireGuard. 3.2.5.1. WireGuard-сервер. 3.2.5.2. WireGuard-клиент. 3.2.6. OpenVPN. 3.2.6.1. OpenVPN-сервер. 3.2.6.2. OpenVPN-клиент.	1 час
Лабораторная:	3. Настройка туннелей. 3.1. Настройка IP4IP4-туннеля. 3.2. Настройка GRE-туннеля. 3.3. Настройка L2TPv3-туннеля.	1 час

Наименование	Описание	Время
Тема:	**4. Контроль маршрутизации.**	**2 часа**
Описание:	4.1. Общие сведения о маршрутизации. 4.1.1. Таблица маршрутизации. 4.1.2. Предпочтение маршрута (preference). 4.1.3. Метрика маршрута (cost). 4.1.4. Гибкость протоколов маршрутизации. 4.1.5. Порядок обработки пакетов на ESR. 4.2. Конфигурирование PBR. 4.2.1. Маршрутизация на основе политики. 4.2.2. Принцип работы и этапы конфигурирования. 4.2.3. Настройка PBR. 4.2.4. Пример настройки PBR. 4.3. Конфигурирование Multi-WAN. 4.3.1. Общие сведения о Multi-WAN. 4.3.2. Принцип работы и этапы конфигурирования. 4.3.3. Настройка Multi-WAN. 4.3.4. Настройка на интерфейсе. 4.3.5. Диагностика Multi-WAN. 4.3.6. Пример настройки Multi-WAN. 4.4. Конфигурирование VRF-lite. 4.4.1. Виртуальная маршрутизация. 4.4.2. Настройка VRF на ESR. 4.4.3. Диагностика VRF. 4.4.4. Пример настройки VRF. 4.5. Конфигурирование BFD. 4.5.1. Общая информация о BFD. 4.5.2. BFD для OSPF. 4.5.3. BFD для BGP. 4.5.4. Команды настройки. 4.5.5. Пример настройки BFD.	1 час
Лабораторная:	4. Настройка средств контроля маршрутизации. 4.1. Настройка PBR. 4.2. Настройка Multi-WAN. 4.3. Настройка VRF. 4.4. Настройка BFD.	1 час

Наименование	Описание	Время
Тема:	**5. Резервирование L3.**	**2 часа**
Описание:	5.1. Конфигурирование VRRP. 5.1.1. Общие сведения. 5.1.2. Команды настройки. 5.1.3. Примеры настройки VRRP.	1 час

	5.2. Конфигурирование Track-объектов. 5.2.1. Общие сведения. 5.2.2. Команды настройки. 5.2.3. Примеры настройки Track-объекта. 5.2.3.1. Изменение маршрутизации с помощью Track-объекта. 5.2.3.2. Статическое отслеживание маршрутов с помощью IP SLA. 5.2.3.3.Резервирование ESR с проверкой качества uplink-каналов. 5.3. Конфигурирование DHCP. 5.3.1. Общие сведения. 5.3.2. DHCP-клиент. 5.3.3. DHCP-сервер. 5.3.4. DHCP-ретранслятор. 5.4. Резервирование DHCP с помощью VRRP. 5.4.1. Команды настройки. 5.4.2. Пример настройки резервирования DHCP. 5.5. Резервирование сессий firewall с помощью VRRP. 5.5.1. Команды настройки. 5.5.2. Пример резервирования сессий firewall. 5.6. Создание кластера из ESR. 5.6.1. Общие сведения о кластеризации. 5.6.2. Пример настройки кластера.	
Лабораторная:	5. Настройка резервирования L3. 5.1. Настройка VRRP.	1 час

Наименование	**Описание**	**Время**
Тема:	**6. Конфигурирование OSPF.**	**2 часа**
Описание:	6.1. Общие сведения. 6.1.1. Создание процесса. 6.1.2. Включение OSPF на интерфейсе. 6.2. Компоненты OSPF. 6.2.1. Базы данных. 6.2.2. Типы пакетов. 6.2.3. Состояния OSPF. 6.2.4. Типы маршрутизаторов. 6.2.5. Типы областей. 6.2.6. Типы записей LSA. 6.2.7. Типы сетей. 6.2.8. Роли маршрутизаторов. 6.2.9. Выбор DR. 6.2.10. Стоимость канала. 6.3. Дополнительные настройки OSPF. 6.3.1. Типы соседства и аутентификация. 6.3.2. Виртуальный канал. 6.3.3. Пассивный интерфейс.	1 час

	6.3.4. Таймеры. 6.3.5. Суммирование межобластных маршрутов. 6.4. Диагностика. 6.5. Примеры настройки OSPF.	
Лабораторная:	6. Настройка OSPF. 6.1. Создание процесса OSPF и настройка области. 6.2. Настройка OSPF на интерфейсе. 6.3. Диагностика OSPF.	1 час

Наименование	**Описание**	**Время**
Тема:	**7. Конфигурирование BGP.**	**2 часа**
Описание:	7.1. Общие сведения. 7.1.1. Организации и регистраторы. 7.1.2. Автономные системы и уникальные номера. 7.1.3. Типы автономных систем. 7.1.4. Провайдеро-зависимые и провайдеро-независимые IP-адреса. 7.2. Основы BGP. 7.2.1. Маршрут BGP. 7.2.2. Выбор лучшего маршрута. 7.3. Настройка eBGP. 7.3.1. Дополнительные параметры eBGP. 7.3.2. eBGP Multihop. 7.4. Настройка iBGP. 7.4.1. Peer-group. 7.4.2. Next-hop-self. 7.4.3. Route-reflector. 7.4.4. Allow-local-as. 7.5. Диагностика BGP. 7.6. Пример настройки BGP.	1 час
Лабораторная:	7. Настройка BGP. 7.1. Настройка eBGP. 7.2. Настройка iBGP.	1 час

Наименование	**Описание**	**Время**
Тема:	**8. Анонсирование и фильтрация.**	**2 часа**
Описание:	8.1. Механизмы анонсирования маршрутов. 8.1.1. Анонсирование redistribute. 8.1.2. Анонсирование network. 8.1.3. Анонсирование default-information-originate. 8.1.4. Анонсирование с помощью route-map. 8.1.4.1. Анонсирование default-route из BGP в OSPF. 8.1.4.2. Анонсирование default-route через OSPF в	1 час

	normal/backbone areas. 8.1.5. Суммаризация маршрутов при анонсировании по BGP. 8.2. Механизмы фильтрации принимаемых маршрутов. 8.2.1. Фильтрация с prefix-list. 8.2.2. Фильтрация с route-map. 8.2.3. Фильтрация по router-id. 8.3. Фильтрация маршрутов при анонсировании. 8.3.1. Фильтрация при анонсировании с prefix-list. 8.3.2. Фильтрация при анонсировании с route-map. 8.3.3. Фильтрация маршрутов с route-map для BGP. 8.4. Модификация маршрутных атрибутов BGP. 8.4.1. Фильтрация по атрибутам BGP.	
Лабораторная:	8. Анонсирование и фильтрация. 8.1. Механизмы анонсирования маршрутов. 8.2. Механизмы фильтрации принимаемых маршрутов.	1 час

Наименование	**Описание**	**Время**
Тема:	**9. Конфигурирование QoS.**	**4 часа**
Описание:	9.1. Общие сведения о Quality of Service. 9.1.1. Модели QoS. 9.1.2. Механизмы DiffServ. 9.1.3. Принцип работы QoS. 9.1.4. TCP-трафик. 9.1.5. Голосовой и видео трафик. 9.1.6. Классификация и маркировка. 9.1.6.1. Классификация. 9.1.6.2. Классификация на разных уровнях. 9.1.6.3. Модели поведения при маркировке. 9.1.6.4. Требования к приложениям. 9.1.6.5. Классы AF. 9.1.6.6. Маркировка DSCP. 9.2. Инструменты и алгоритмы QoS. 9.2.1. Предотвращение перегрузок. 9.2.1.1. Tail drop и Head drop. 9.2.1.2. Случайное раннее обнаружение (RED). 9.2.1.3. Мягкое случайное раннее обнаружение (GRED). 9.2.2. Управление перегрузками. 9.2.2.1. «Первый пришёл — первый ушёл» (FIFO). 9.2.2.2. Приоритетная очередь (PQ или SP). 9.2.2.3. Стохастическая справедливая очередь (SFQ). 9.2.2.4. Взвешенная циклическая обработка (WRR). 9.2.3. Ограничение скорости. 9.2.3.1. Механизм «Дырявое ведро» (Leaky Bucket). 9.2.3.2. Механизм «Маркерное ведро» (Token Bucket). 9.3. Команды настройки базового режима QoS. 9.3.1. Пример настройки базового QoS. 9.4. Команды настройки расширенного режима QoS.	2 часа

	9.4.1. Пример настройки расширенного QoS.	
Лабораторная:	9. Настройка QoS. 9.1. Настройка базового QoS. 9.2. Настройка расширенного QoS.	2 часа

Наименование	**Описание**	**Время**
Тема:	**10. Конфигурирование IPsec.**	**4 часа**
Описание:	10.1. Общие сведения об IPsec. 10.1.1. Целостность и аутентификация данных. 10.1.2. Аутентификация удалённой стороны. 10.1.3. Конфиденциальность. 10.1.4. Алгоритм Диффи-Хеллмана. 10.1.5. Протоколы IPsec. 10.1.5.1. Протокол Authentication Header (AH). 10.1.5.2. Протокол Encapsulating Security Payload (ESP). 10.1.5.3. Транспортный и туннельный режимы. 10.1.5.4. Security Association (SA). 10.1.5.5. Internet Security Association and Key Management Protocol (ISAKMP). 10.1.5.6. IPsec с IKEv1. 10.1.5.7. IPsec с IKEv2. 10.1.6. Обнаружение неактивного соседа. 10.1.7. Порядок настройки IPsec. 10.1.8. Route-based IPsec VPN и Policy-based IPsec VPN. 10.2. Команды настройки. 10.2.1.Пример Route-based IPsec VPN. 10.2.2. Пример Policy-based IPsec VPN. 10.2.3. Пример GRE over IPsec. 10.3. Методы аутентификации. 10.3.1. PSK. 10.3.2. Список ключей. 10.3.3. XAUTH. 10.3.4. RSA. 10.3.5. EAP. 10.4. IPsec VPN в схеме с NAT. 10.5. Диагностика IPsec.	2 часа
Лабораторная:	10. Настройка IPsec. 10.1. Настройка Route-based IPsec VPN. 10.2. Настройка Policy-based IPsec VPN.	2 часа

Наименование	**Описание**	**Время**
Тема:	**11. Конфигурирование DMVPN.**	**4 часа**

Описание:	11.1. Общие сведения о DMVPN. 11.1.1. Использование mGRE. 11.1.2. Протокол NHRP. 11.1.3. Основные принципы работы NHRP. 11.1.3.1. Формирование GRE-пакета на базе таблицы NHRP. 11.1.3.2. Регистрация Spoke на Hub. 11.1.3.3. Разрешение адреса в сети DMVPN. 11.1.3.4. Уведомление Spoke о неоптимальной отправке трафика через Hub. 11.1.4. Фазы работы DMVPN. 11.1.4.1. 1 фаза DMVPN. 11.1.4.2. 2 фаза DMVPN. 11.1.4.3. 3 фаза DMVPN. 11.1.4.4. Отличия фазы 2 и 3. 11.1.5. Флаги. 11.1.6. Схемы применения. 11.1.6.1. Один Hub и два облака DMVPN. 11.1.6.2. Два Hub и одно облако DMVPN. 11.1.6.3. Два Hub и два облака DMVPN. 11.1.6.4. Резервирование DMVPN. 11.1.7. Ограничение DMVPN при использовании NAT. 11.2. Команды настройки DMVPN (mGRE+NHRP). 11.3. Порядок настройки DMVPN с OSPF. 11.3.1. Этап 1. Настройка mGRE и NHRP. 11.3.2. Этап 2. Настройка OSPF. 11.3.3. Этап 3. Настройка IPsec. 11.4. Примеры настройки DMVPN. 11.4.1. DMVPN с OSPF. 11.4.2. DMVPN с BGP. 11.4.3. DMVPN с динамическим IP-адресом на SPOKE. 11.4.4. DMVPN с внешним DHCP и DHCP relay на HUB.	2 часа
Лабораторная:	11. Настройка DMVPN. 11.1. Настройка DMVPN с OSPF. 11.2. Настройка DMVPN с BGP.	2 часа

Наименование	**Описание**	**Время**
Тема:	**12. Мониторинг и управление.**	**4 часа**
Описание:	12.1. Конфигурирование SNMP. 12.1.1. Общие сведения о SNMP. 12.1.1.1. Принцип работы SNMP. 12.1.1.2. Версии протокола SNMP. 12.1.2. Типы сообщений SNMP. 12.1.3. База MIB и идентификатор объекта. 12.1.4. Строка сообщества. 12.1.5. Безопасность SNMP.	2 часа

	12.1.6. Формат сообщения SNMP. 12.1.6.1. Заголовок SNMP. 12.1.6.2. Заголовок запросов GET/SET. 12.1.6.3. PDU GET-request, GET-next-request, SET-request, GET-bulk-request. 12.1.6.4. PDU GET-response. 12.1.6.5. Заголовок TRAP. 12.1.6.6. PDU TRAP. 12.1.6.7. Поля Variable Bindings. 12.1.6.8. Формат SNMPv3 с USM. 12.1.7. Команды настройки. 12.1.8. Пример настройки SNMP. 12.2. Конфигурирование NetFlow. 12.2.1. Общие сведения о NetFlow. 12.2.1.1. Возможности NetFlow. 12.2.1.2. Компоненты NetFlow. 12.2.1.3. Принцип работы NetFlow. 12.2.2. Общие сведения о sFlow. 12.2.3. Сравнение NetFlow и sFlow. 12.2.4. Формат сообщений NetFlow. 12.2.4.1. Формат заголовка NetFlow. 12.2.4.2. Формат шаблона Template Flow Set. 12.2.4.3. Формат шаблона Data Flow Set. 12.2.4.4. Формат шаблона Options Template FlowSet. 12.2.4.5. Формат набора Options Data в Data FlowSet. 12.2.5. Управление шаблонами. 12.2.6. Уязвимости в безопасности NetFlow. 12.2.7. Команды настройки NetFlow. 12.2.7.1. Пример настройки NetFlow. 12.2.8. Команды настройки sFlow. 12.2.8.1. Пример настройки sFlow. 12.3. Конфигурирование Zabbix-агента. 12.3.1. Общие сведения о Zabbix. 12.3.2. Принцип работы Zabbix. 12.3.3. Способы мониторинга Zabbix. 12.3.4. Команды настройки. 12.3.5. Пример настройки Zabbix-агента. 12.4. Конфигурированиие LLDP-MED. 12.4.1. Настройка LLDP-MED. 12.4.2. Диагностика. 12.4.3. Пример настройки Voice VLAN. 12.5. Обзор ECCM. 12.5.1.Возможности ECCM.	
Лабораторная:	12. Настройка мониторинга. 12.1. Настройка SNMP. 12.2. Настройка NetFlow. 12.3. Настройка sFlow. 12.4. Настройка Zabbix-агента.	2 часа

Промежуточные и итоговые формы контроля: 8 часов

В рамках данного курса предоставляется одна попытка прохождения сертификационного испытания, которая может быть использована в день завершения курса.
В случае неудачного завершения, можно обратиться в коммерческий отдел для приобретения платной дополнительной попытки.
Платной попыткой можно воспользоваться в течение одного календарного месяца после завершения обучения.