Учреждение образования
«Гомельский государственный университет
имени Франциска Скорины»

Факультет физики и информационных технологий
Кафедра автоматизированных систем обработки информации

СОГЛАСОВАНО
Заведующий кафедрой
автоматизированных систем
обработки информации
А.В.Воруев
__ _____ 2023 г.

СОГЛАСОВАНО
Декан
факультета физики и
информационных технологий
Д.Л.Коваленко
__ _____ 2023 г.

ЭЛЕКТРОННЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ПРОТОКОЛЫ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ

для учащихся второй ступени высшего образования (магистратура)
специальности 1-45 80 01 Системы и сети инфокоммуникаций

составители: заведующий кафедрой АСОИ, к.т.н., доцент, Воруев А.В.
старший преподаватель Кулинченко В.Н.
старший преподаватель Кучеров А.И.

Рассмотрено и утверждено
на заседании кафедры АСОИ
__14 марта___ 2023 г., протокол № _8_

Рассмотрено и утверждено
на заседании научно-методического
совета университета
30.03. 2023 г., протокол № 7

Гомель 2023

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Электронный учебно-методический комплекс (ЭУМК) по дисциплине «Протоколы дистанционного управления» представляет собой комплекс систематизированных учебных, методических и вспомогательных материалов, предназначенных для использования в образовательном процессе специальности 1-45 80 01 Системы и сети инфокоммуникаций.

ЭУМК разработан в соответствии со следующими нормативными документами:

1. Положением об учебно-методическом комплексе на уровне высшего образования, утвержденном постановлением Министерства образования Республики Беларусь от 26.07.2011 №167.

2. Учебного плана УВО специальности высшего образования второй ступени (магистратура) 1-45 80 01 Системы и сети инфокоммуникаций регистрационный № I 45-2-01/Д-19 от 09.04.2019 г.

3. Учебной программой по учебной дисциплине «Протоколы дистанционного управления» для специальности 1-45 80 01 Системы и сети инфокоммуникаций, утвержденной 22.05.2019, регистрационный номер УД-31-2019-191/уч.

Целью дисциплины «Протоколы дистанционного управления» является изучение технологий построения транспортных сетей инфокоммуникаций; протоколов распределения информации физического, канального, сетевого и транспортного уровней базовой эталонной модели взаимодействия открытых систем; способов организации управляемой работы сетевых сред в составе группировки физических и виртуальных устройств; освоение принципов предотвращения несанкционированного доступа к операционным системам сетевых устройств и принципов построения и технической эксплуатации транспортных сетей телекоммуникаций.

ЭУМК направлен на всестороннюю подготовку учащихся теоретическим основам и практическим навыками по решению новых инженерных задач, возникающих при освоении и внедрении в сетевых стандартов и методов организации вычислительного процесса в сетевых структурах. Организация изучения дисциплины на основе ЭУМК предполагает продуктивную образовательную деятельность, позволяющую сформировать социально-личностные и профессиональные компетенции будущих специалистов.

ЭУМК способствует успешному осуществлению учебной деятельности, дает возможность планировать и осуществлять самостоятельную управляемую работу учащихся, обеспечивает рациональное распределение учебного времени по темам учебной дисциплины и совершенствование методики проведения занятий.

ЭУМК состоит из теоретического, практического и вспомогательного разделов. Теоретический раздел содержит тексты лекций. Практический раздел содержит методические рекомендации к лабораторным работам,

тестовые задания и вопросы для самоконтроля. Вспомогательный раздел содержит учебную программу и список литературы.

Теоретический раздел содержит лекционный материал по всем темам учебной программы, включая и темы, вынесенные на самостоятельное изучение. В разделе так же содержатся рекомендации по организации и выполнению управляемой самостоятельной работы по трем уровням сложности.

Практический раздел включает в себя темы лабораторных занятий и задания с краткими методическими указаниями по выполнению лабораторных работ. В разделе так же приводятся некоторый набор тестовых заданий и к каждой теми указаны вопросы для самоконтроля.

Вспомогательный раздел содержит необходимые элементы учебно-программной документации по дисциплине с указанием рекомендуемой литературы (основной, дополнительной, вспомогательной).

Все разделы ЭУМК в полной мере соответствуют содержанию учебной программы и объему учебного плана.

Дисциплина учреждения высшего образования «Протоколы дистанционного управления» изучается магистрантами1 года обучения (1семестр) дневной формы обучения для специальности: 1-45 80 01 Системы и сети инфокоммуникаций.

Общее количество часов –230.

Дневная форма обучения: аудиторное количество часов – 72; из них: лекционных занятий – 32 (в том числе УСР – 14), практических занятий – 16, лабораторных работ – 24.

Форма отчётности – экзамен.

Заочная форма обучения: аудиторное количество часов – 18; из них: лекционных занятий – 8, практических занятий – 4, лабораторных работ – 6.

Форма отчётности – экзамен.

2 ТЕКСТЫ ЛЕКЦИЙ

Раздел 1 Ключевые принципы программно-определяемых сетей

В алгоритмическом плане пересылка пакетов в сети проста, и основной задачей является достижение необходимой скорости передачи данных. Отправителями и получателями пакетов являются интерфейсы маршрутизатора, а определение адресата осуществляется с помощью т.н. таблицы передачи -ForwardingInformationBase (FIB).

Задачей же маршрутизации является построение собственной таблицы, таблицы маршрутизации (RoutingInformationBase, RIB), которая потом транслируется в таблицу FIB. Для построения этой таблицы и используются протоколы маршрутизации, которые на основе информации, полученной от соседних маршрутизаторов, и собственной конфигурации (например, статических маршрутов и ограничений, наложенных сетевой политикой маршрутизации), формируют представление о сети и ее топологии.

В контексте данной темы важным в этой модели является то, что каждый маршрутизатор принимает решения самостоятельно и относительно независимо.

Такая модель работает замечательно в простых сетях, особенно когда основной задачей является обеспечение связности. Она проста и надежна. Однако по мере усложнения сетевой архитектуры и политики внутренней и внешней маршрутизации, ограничения модели становятся все более заметны.

Новые функции и возможности неимоверно увеличивают сложность системы, их тестирование трудоемко, а внедрение дорогостояще и рискованно. Поэтому большие надежды возлагают на сетевую парадигму, получившую название SDN (Software Defined Networking) или Программно-Конфигурируемая Сеть.

Раздел 2 Протоколы доступа к операционной системе

Тема 2.1 Протокол прикладного уровня TELNET

TELNET (teletypenetwork) - сетевой протокол для реализации текстового терминального интерфейса по сети (в современной форме - при помощи транспорта TCP). Название «telnet» имеют также некоторые утилиты, реализующие клиентскую часть протокола. Современный стандарт протокола описан в RFC 854.

Для каждого интерфейса TELNET переводит символы (данные или команды), которые получает от местного терминала, в NVT(NetworkVirtualTerminal)-форму и доставляет их в сеть. С другой стороны, сервер TELNET переводит команды из формы NVT в форму, доступную удаленному компьютеру.

Всю информацию Telnet посылает в незашифрованном виде, поэтому сейчас он рассматривается как один из самых небезопасных сервисов в Интернет. Telnet безопасен только в том случае, когда безопасны все машины и сети на пути от компьютера-клиента к компьютеру-серверу.

Тема 2.2 Протокол SSH

SSH (secureshell- безопасная оболочка) это набор программ, которые позволяют регистрироваться на компьютере по сети, удаленно выполнять на нем команды, а также копировать и перемещать файлы между компьютерами. SSH организует защищенное безопасное соединение поверх небезопасных каналов связи. Спецификация протокола SSH-2 содержится в RFC 4251.

SSH предоставляет замены традиционным r-командам удаленного доступа с тем отличием, что они обладают повышенной безопасностью. Они выполняются поверх защищенных зашифрованных соединений, которые не позволяет прослушивать или подменять трафик. Кроме того, SSH может обеспечивать безопасное соединение для передачи любого другого трафика: например, почтовых сообщений или файлов.

Тема 2.3 Концепция Internet Standard Management Framework

SNMP (SimpleNetworkManagementProtocol- простой протокол сетевого управления) - стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для контроля подключённых к сети устройств на предмет условий, которые требуют внимания администратора. SNMP определён Инженерным советом интернета (IETF) как компонент TCP/IP.

Базовая структура InternetStandardManagementFramework состоит из основных компонентов (для всех версий концепции - для SNMPv1, SNMPv2, SNMPv3): SNMP-сущность (SNMPentity), MIB (managementinformationbase, база данных, которая используется для управления устройствами в сети), NMS (NetworkManagementStation, станция управления сетью).

Спецификация RFC 1155, RFC 1212, RFC 1213, RFC 1157, RFC 3411.

Тема 2.4 Протокол управления процессом обработки данных Openflow

Протокол используется для управления сетевыми коммутаторами и маршрутизаторами с центрального устройства - контроллера сети (например, с сервера или даже персонального компьютера). Это управление заменяет или дополняет работающую на коммутаторе (маршрутизаторе) встроенную программу, осуществляющую построение маршрута, создание карты коммутации и т. д.. Контроллер используется для управления таблицами потоков коммутаторов, на основании которых принимается решение о передаче принятого пакета на конкретный порт коммутатора. Таким образом в сети формируются прямые сетевые соединения с минимальными задержками передачи данных и необходимыми параметрами.

Версии микропрограмм с поддержкой Openflow разработаны для устройств многих производителей, включая ExtremeNetworks, Juniper, Cisco, HP, IBM, NEC.

Раздел 3 Протоколы автоматического согласования параметров связи

Тема 3.1 Протоколы согласования канального уровня

Коммутатор и протоколы, которые используют коммутаторы могут быть целью атак. Более того, некоторые настройки коммутаторов (как правило, это настройки по умолчанию) позволяют выполнить ряд атак и получить несанкционированный доступ к сети или вывести из строя сетевые устройства. Однако, коммутатор может быть и достаточно мощным средством защиты. Так как через него происходит всё взаимодействие в сети, то логично контролировать это на нем.

Безопасностьпротоколов, которыеиспользуюткоммутаторы: Spanning Tree Protocol (STP); 802.1Q (VLAN); Link Layer Discovery Protocol (LLDP); Cisco Discovery Protocol (CDP); Extreme Discovery Protocol; Foundry Discovery Protocol; Nortel Discovery Protocol; MikroTik Neighbor Discovery Protocol (MNDP); VLAN Trunking Protocol (VTP); Dynamic Trunking Protocol (DTP); Hot Standby Router Protocol (HSRP).

Тема 3.2 Протоколы маршрутизации

Маршрутизация - процесс определения лучшего пути, по которому пакет может быть доставлен получателю. Возможные пути передачи пакетов называются маршрутами. Лучшие маршруты к известным получателям хранятся в таблице маршрутизации. В

зависимости от способа заполнения таблицы маршрутизации, различают два вида маршрутизации: статическая маршрутизация и динамическая маршрутизация

Устройство, выполняющее маршрутизацию, именуется маршрутизатором. В качестве маршрутизатора могут использоваться специализированные устройства, такие, например, как Cisco Router, или это могут быть обычные компьютеры, оснащённые несколькими сетевыми картами (или принимающие тегированный трафик) и работающие под управлением универсальной операционной системы, такой как FreeBSD или GNU/Linux.

В зависимости от алгоритма маршрутизации протоколы делятся на два вида: дистанционно-векторные протоколы (основаны на алгоритме DVA-distancevectoralgorithm) и протоколы состояния каналов связи (основаны на алгоритме LSA-linkstatealgorithm).

По области применения выделяют протоколы: для междоменной маршрутизации и для внутридоменной маршрутизации.

Тема 3.3 Синхронизация событий и сбор сетевых статистик

NetworkTimeProtocol (NTP) - сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью. NTP использует для своей работы протокол UDP 123 порт. Система NTP чрезвычайно устойчива к изменениям латентности среды передачи. NTP использует алгоритм Марзулло (предложен КейтомМарзулло (KeithMarzullo) из Университета Калифорнии, Сан-Диего), включая такую особенность, как учёт времени передачи. В версии 4 способен достигать точности 10 мс (1/100 с) при работе через Интернет, и до 0.2 мс (1/5000 с) и лучше внутри локальных сетей.

Раздел 4 Ограничение доступа к управлению узлами сети

Тема 4.1 Межсетевая фильтрация трафика

Межсетевой экран, сетевой экран - программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Список контроля доступа (ACL) - это последовательный список разрешающих или запрещающих операторов, называемых записями списка контроля доступа (ACE). Записи списка контроля доступа обычно называют утверждениями списка контроля доступа. При прохождении сетевого трафика через интерфейс, где действует список контроля доступа (ACL), маршрутизатор последовательно сопоставляет информацию из пакета с каждой записью в списке контроля доступа на предмет соответствия. Это называется фильтрацией пакетов.

Тема 4.2Внутрисетевая фильтрация трафика

Частная VLAN (PVLAN), также известная как изоляция портов, представляет собой метод в компьютерных сетях, где VLAN содержит порты коммутатора, которые ограничены так, что они могут взаимодействовать только с данной «восходящей линией связи». Ограниченные порты называются «частными портами». Каждая частная VLAN обычно содержит много частных портов и одну восходящую линию связи. В качестве восходящей линии связи обычно используется порт (или группа агрегации каналов), подключенный к маршрутизатору, брандмауэру, серверу, сети провайдера или подобному центральному ресурсу.

Коммутатор перенаправляет все кадры, полученные от частного порта, на порт восходящей линии связи, независимо от идентификатора VLAN или MAC-адреса назначения. Кадры, принятые от порта восходящей линии связи, пересылаются обычным

способом (то есть на порт, содержащий MAC-адрес назначения, или на все порты VLAN для широковещательных кадров или для неизвестных MAC-адресов назначения). В результате прямой одноранговый трафик между одноранговыми узлами через коммутатор блокируется, и любая такая связь должна проходить через восходящую линию связи. Хотя частные VLAN обеспечивают изоляцию между узлами на канальном уровне, связь на более высоких уровнях все еще может быть возможной в зависимости от дальнейшей конфигурации сети.

Типичное приложение для частной VLAN - это гостиница или Ethernet для домашней сети, где в каждой комнате или квартире есть порт для доступа в Интернет. Подобная изоляция порта используется в ADSL DSLAM на основе Ethernet. Разрешение прямого обмена данными на канальном уровне между узлами клиента может подвергнуть локальную сеть различным атакам безопасности, таким как подмена ARP, а также увеличить вероятность повреждения из-за неправильной конфигурации.

RADIUS (RemoteAuthenticationDialInUserService, служба удалённой аутентификации дозванивающихся пользователей) - сетевой протокол, предназначенный для обеспечения централизованной аутентификации, авторизации и учёта (Authentication, Authorization, andAccounting, AAA) пользователей, подключающихся к различным сетевым службам. Используется, например, при аутентификации пользователей WiFi, VPN, в прошлом, dialup-подключений, и других подобных случаях. Описан в стандартах RFC 2865 и RFC 2866.

Тема 4.3 Системы централизованного управления доступом

Для решения вопросов управления необходимо получать информацию обо всех событиях сети. Дляэтогосуществуют SIEM-решения (Security Information and Event Management).

Данные решения включают в себя средства автоматизированного сбора событий, их нормализации, то есть приведения текста события к некоторому общему виду (например, выделение из события имени пользователя, его IP-адреса, порта соединения и т.д.). Также, классический SIEM осуществляет сохранение всех событий в единой БД и позволяет составлять правила корреляции различных событий. С помощью этих правил специалист по безопасности может существенно автоматизировать свою работу по обнаружению и предотвращению атак. Опционально решение может также содержать средства генерации отчетов и автоматизации расследования инцидентов. Как правило, присутствует возможность реагирования на события и интеграции с системами IPS.

Тема 4.4 Понятие Zone-Based Policy Firewall

В основе Zone-BasedPolicyFirewall лежит распределение интерфейсов маршрутизатора по зонам безопасности. После этого все правила настраиваются для взаимодействий между зонами. Такой подход облегчает настройки правил межсетевого экрана. Кроме того в Zone-BasedPolicyFirewall используется Cisco PolicyLanguage (CPL), которая позволяет более гибко, чем в предыдущих версиях межсетевого экрана, настраивать правила фильтрации трафика. Zone-BasedPolicyFirewall появился в IOS 12.4(6)T.

Раздел 5 Автоматизация операций по обслуживанию сети

Тема 5.1 Понятие сетевого контура

Термин FogComputing («туманные вычисления») был введен в оборот вице-президентом компании Cisco ФлавиоБономи (FlavioBonomi) в 2011 году. Он предложил концепцию FogComputing по аналогии с «облачными вычислениями» (CloudComputing), как расширение «облака» до границ сети. Технологически, концепция FogComputing тесно

связана с распределёнными (облачными) дата-центрами, в которых серверы дата-центров могут располагаться во многих местоположениях, вплоть до границы сети. Дата-центры могут быть небольшими (контейнерного, модульного или мобильного исполнения), являясь фактически «выносами» крупных дата-центров. Таким образом, отличительная черта FogComputing- приближенность к конечным пользователям и поддержка их мобильности.

Развитие интернета вещей (IoT, InternetofThings) потребовало поддержки мобильности устройств IoT для различных местоположений с геолокацией и с небольшой задержкой на обработку данных. Поэтому была предложена новая платформа для удовлетворения таких требований, которая и получила название Fogcomputing – «туманные вычисления». Её основной особенностью является обработка данных в непосредственной близости от источников их получения, без необходимости их передачи в крупные дата-центры только для того, чтобы их там обработать и передать назад результаты.

Тема 5.2 Балансировка сетевых сервисов

Цель балансировки нагрузки - оптимизация использования ресурсов, максимизация пропускной способности, уменьшение времени отклика и предотвращение перегрузки какого-либо одного ресурса. Использование нескольких компонентов балансировки нагрузки вместо одного может повысить надежность и доступность за счет резервирования. Балансировка нагрузки предполагает обычно наличие специального программного обеспечения или аппаратных средств, таких как многоуровневый коммутатор или система доменных имен, как серверный процесс.

В масштабах вычислительного процесса решения по балансировке нагрузки часто разделяются на две категории: L4 и L7. Они относятся к уровням 4 и 7 модели OSI. Модель OSI представляет очень плохое приближение к сложности решений балансировки нагрузки, которые включают традиционные протоколы уровня 4, такие как TCP и UDP, но часто заканчиваются включением битов и частей протоколов на разных уровнях OSI.

Тема 5.3 Визуализация взаимодействия сетевых устройств

Для эффективного извлечения ценной информации важно, чтобы коллектор потоков мог нормализовать данные телеметрии из различных источников, не теряя при этом исходной информации, содержащейся в ненормализованных данных. Это позволит анализировать весь объем собранных данных с использованием единого подхода, при этом имея возможность пользоваться преимуществами отдельных протоколов (например, счетчиками выборки sFlow).

Zabbix- это полномасштабный инструмент для сетевого и системного мониторинга сети, который объединяет несколько функций в одной веб-консоли. Он может быть сконфигурирован для мониторинга и сбора данных с самых разных серверов и сетевых устройств, обеспечивая обслуживание и мониторинг производительности каждого объекта.

Тема 5.4 Программирование взаимодействия сетевых устройств

Архитектура цифровых сетей Cisco DigitalNetworkArchitecture (Cisco DNA) предлагает заказчикам набор программного и аппаратного обеспечения для работы:

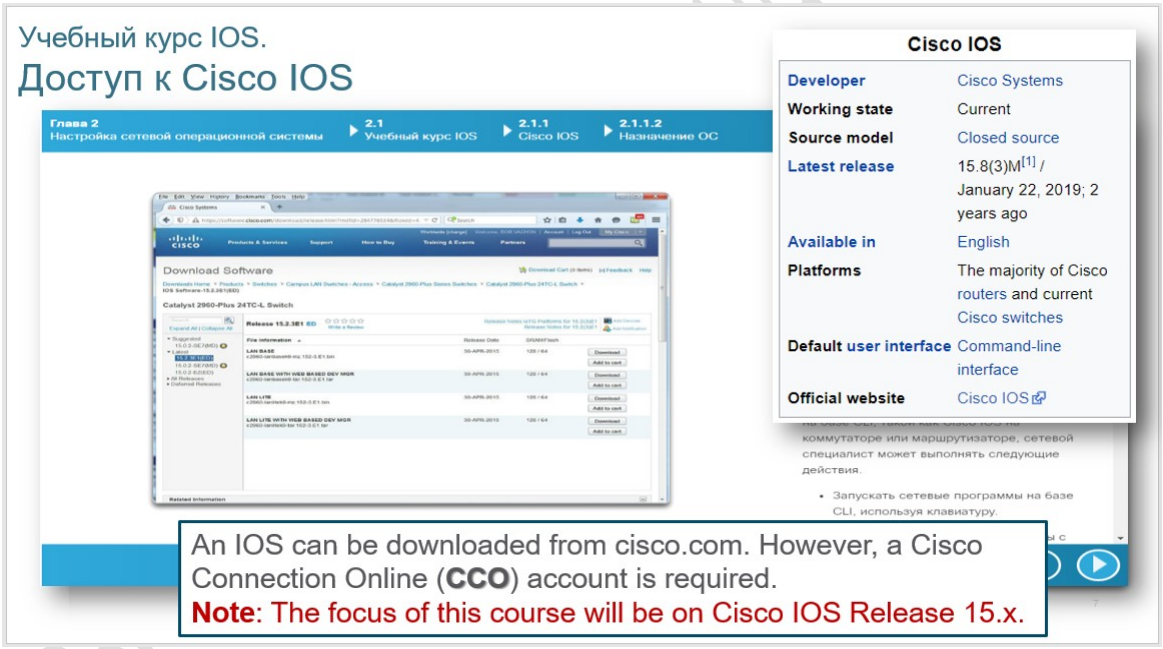
Cisco DNA Center- интуитивная, централизованная система управления, основанная на интенционном принципе и охватывающая процессы, связанные с проектированием, конфигурированием, политиками и обеспечением исполнения (assurance). Получая от Cisco DNA Center полный обзор и контекстную информацию по всей сети, ИТ-специалисты могут централизовано управлять всеми сетевыми функциями.

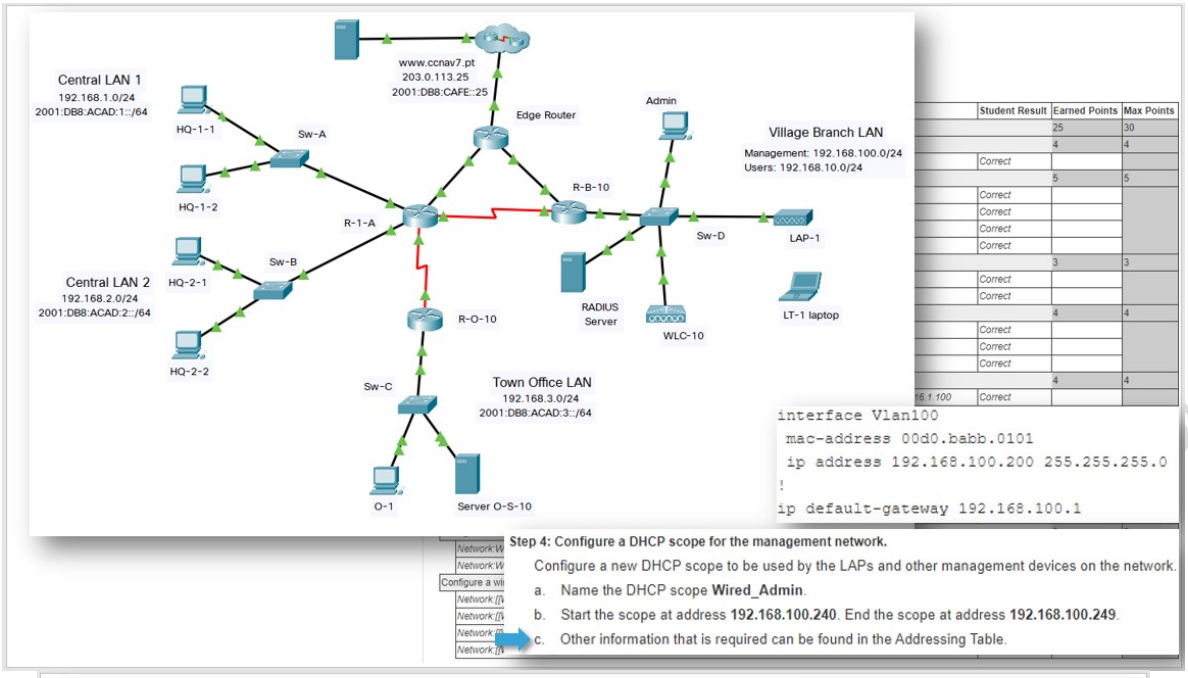
Программноопределяемыйдоступ (Software-Defined Access, SD-Access). В технологии SD-Access автоматизация применения политик и сегментации сети используется для существенного упрощения доступа к сети со стороны пользователей, устройств и объектов. Автоматизируя такие повседневные рутинные операции, как настройка, конфигурирование и отладка, SD-Access резко уменьшает время, необходимое для адаптации сети, сокращает сроки устранения проблем с нескольких недель и месяцев до нескольких часов, а также существенно ослабляет последствия взлома систем безопасности.

Платформа сетевых данных и обеспечение исполнения (NetworkDataPlatformandAssurance). Новая мощная аналитическая платформа оперативно выполняет классификацию и корреляцию больших объемов передаваемых по сети данных и с помощью машинного обучения трансформирует их в проактивную аналитику, бизнес-информацию и оперативную информацию, выдавая результаты с помощью сервиса Cisco DNA CenterAssurance.

Анализ зашифрованного трафика (EncryptedTrafficAnalytics). Почти половина кибератак сегодня маскируются в зашифрованном трафике, и их число постоянно растет. Используя для анализа потоков данных интеллектуальные средства Cisco Talos и машинное обучение, сеть способна определять сигнатуры известных атак даже в зашифрованном трафике, не расшифровывая его и сохраняя конфиденциальность данных.

Пример презентационного материала для проведения занятия





Различия между IOS и IOS XE

Cisco IOS - это монолитная операционная система, работающая непосредственно на оборудовании, в то время как IOS XE представляет собой комбинацию ядра Linux и (монолитного) приложения (IOSd), которое работает поверх этого ядра. С другой стороны, IOS XR основан на QNX (начиная с версии 5.0 он также основан на Linux), где приложение IOSd было разделено на множество различных приложений. В то время как IOS XE (IOSd) и IOS используют один и тот же код, IOS XR - это совершенно другая кодовая база.

Поскольку в IOS XE IOSd работает как приложение поверх Linux, становится возможным запускать различные приложения на аппаратном обеспечении, хорошим примером этого является запуск Wireshark на коммутаторе. [9] Другой пример - контейнеры открытых служб Cisco IOS XE. [10]

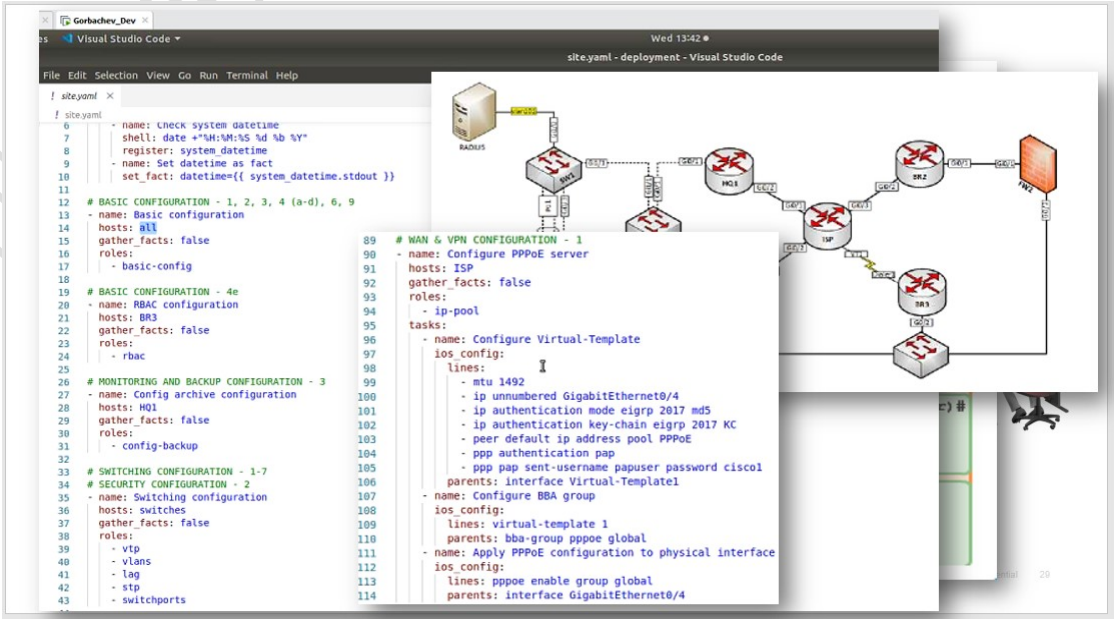
НУЖНО ЛИ ЗАНОВО ОБУЧАТЬСЯ РАБОТЕ С IOS XE?

Нет, Cisco IOS XE выглядит так же, как и традиционное программное обеспечение Cisco IOS. Изменены только несколько команд, такие как «show processor» и «show memory», которые были расширены для учета многоядерных процессоров, которые теперь поддерживает Cisco IOS XE. В целом, если вы знаете, как управлять программным обеспечением Cisco IOS, то вы знаете, как управлять Cisco IOS XE.

Существует несколько преимуществ перехода от IOS к IOS XE, которым будут пользоваться конечные пользователи. IOS XE поможет снизить общую стоимость владения многими решениями Cisco, предлагая расширенную интеграцию служб для повышения функциональности в сети. Кроме того, она поддерживает несколько ядер процессора, плоскость управления и разделение плоскости данных, и абстракцию платформы. Cisco IOS XE содержит Cisco IOS Release 15 внутри себя. Программное обеспечение Cisco IOS работает как процесс в Cisco IOS XE в так называемых демонах (daemon) IOS или **IOSd**.

Differences between IOS and IOS XR

```
! Cisco IOS
!
router bgp 109
  no synchronization
  bgp log-neighbor-changes
  neighbor 203.0.113.1 remote-as 109
  neighbor 203.0.113.1 update-source Loopback0
  no auto-summary
!
! Cisco IOS XR
!
router bgp 109
  neighbor 203.0.113.1
    remote-as 109
    update-source Loopback0
  !
```



Обнаружение устройств с помощью протокола CDP

Настройка и проверка протокола CDP

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
```

Проверка состояния и вывод информации

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# cdp enable
```

Включает протокол CDP на интерфейсе (отключает команда **no CDP enable**)

```
Router(config)# no cdp run
Router(config)# exit
Router# show cdp
% CDP is not enabled
Router# conf t
Router(config)# cdp run
```

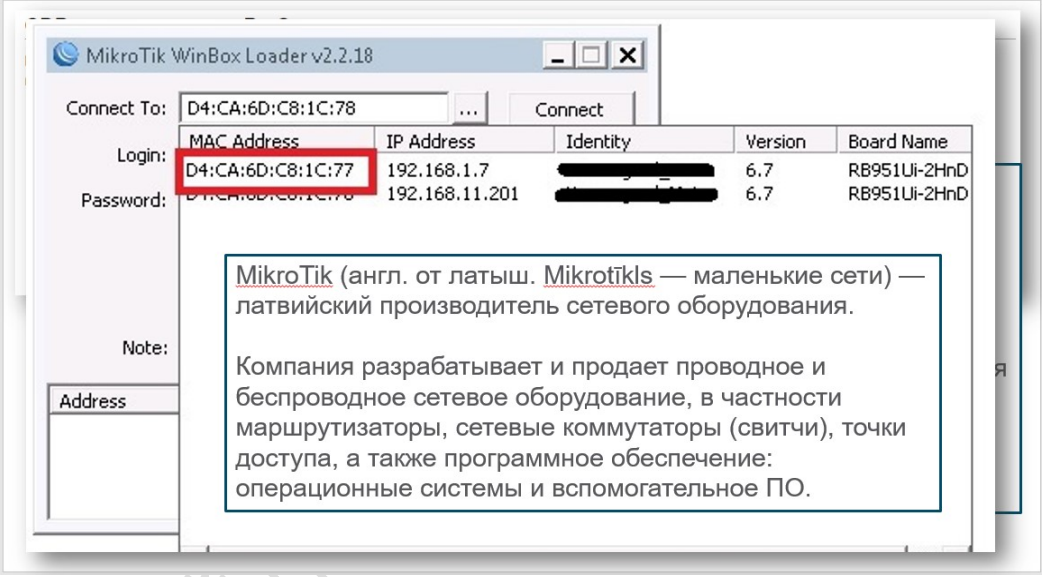
Глобально отключает команда **no cdp run** (включает команда **cdp run**)

```
Router# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Total cdp entries displayed : 0
```

Соседние устройства не обнаружены

```
Router# show cdp interface
Embedded-Service-Engine0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/0/0 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/0/1 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

Указывает интерфейсы с включенным протоколом CDP



MikroTik (англ. от латыш. Mikrotīkls — маленькие сети) — латвийский производитель сетевого оборудования.

Компания разрабатывает и продает проводное и беспроводное сетевое оборудование, в частности маршрутизаторы, сетевые коммутаторы (свитчи), точки доступа, а также программное обеспечение: операционные системы и вспомогательное ПО.

Протокол NTP

Настройка системных часов

```
R1# clock set 20:36:00 dec 11 2015
R1#
*Dec 11 20:36:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 21:32:31
UTC Fri Dec 11 2015 to 20:36:00 UTC Fri Dec 11 2015, configured from console by
console.
```

Для управления, обеспечения безопасности, поиска и устранения неполадок, а также планирования сетей требуются точные метки времени

Настроить дату и время на маршрутизаторе или коммутаторе можно одним из двух способов:

- вручную настройте дату и время, как показано на рисунке;
- настройте протокол сетевого времени (NTP).
  - Протокол NTP использует порт UDP 123
  - Клиенты NTP получают время и дату из одного источника

NTP — один из старейших используемых протоколов. NTP разработан Дэвидом Л. Миллсом (David L. Mills) из университета Дэлавера в 1985 году и в настоящее время продолжает совершенствование.
Текущая версия — NTP 4.

NTP использует алгоритм Марзулло (предложен Кейтом Марзулло (Keith Marzullo) из Университета Калифорнии, Сан-Диего), включая такую особенность, как учёт времени передачи.
NTP 4 способен достигать точности 10 мс (1/100 с) при работе через Интернет, и до 0.2 мс (1/5000 с) или меньше внутри локальных сетей.

Принципы работы системного журнала

Принципы работы системного журнала

- Протокол системного журнала (syslog) начинает с отправки системных сообщений и выходных данных команд **debug** в локальный процесс ведения журналов соответствующего устройства.
- Каким образом процесс ведения журналов управляет этими сообщениями и выводом, зависит от настроек устройства.
- Сообщения системного журнала могут отправляться по сети на внешний сервер системного журнала. Могут включаться в различные отчеты.
- Сообщения системного журнала могут отправляться во внутренний буфер. Просматривать эти сообщения можно только через интерфейс командной строки устройства.

- Получателями сообщений системного журнала могут быть:
  - буфер ведения журналов (ОЗУ в маршрутизаторе или коммутаторе);
  - порт консоли;
  - линия терминала;
  - Сервер Syslog.

3ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1. Теория
    1. История создания и развития программно-определяемых сетей и структур
    2. Самоорганизация работы сетевых устройств на разных уровнях модели ISO/OSI
    3. Устойчивость связи и балансировка трафика в режиме ONLINE
    4. Структура сетевых примитивов и сообщений telnet
    5. Виды устройств, поддерживающих управление по протоколу telnet
    6. Программные оболочки telnet-соединений
    7. Обеспечение безопасности SSH
    8. Аутентификация в SSH с помощью открытых ключей
    9. Туннели SSH
    10. Архитектура InternetStandardManagementFramework
    11. Сообщения протокола SNMP
    12. Настройка SNMP на сетевых устройствах
    13. Путь прохождения данных (datapath)
    14. Таблицы потоков (flowtable) и действий
    15. Контроллеры Openflow
    16. Протоколы для междоменной и межсетевой маршрутизации
    17. OnDemandRouting
    18. Иерархическая система «часовых уровней» NTP
    19. Гостевые сети
    20. Сети резервного копирования
    21. Уязвимости операционных систем узлов сети
    22. Разделение функций controlplan и dataplan
    23. Сетевой протокол централизованной аутентификации, авторизации и учёта RADIUS
    24. Доступность и безопасность данных
    25. Развитие интернета вещей
    26. Технологическая концепция FogComputing
    27. Сценарии использования FogComputing и балансировка точки обработки данных
    28. Балансировка трафика сетевыми устройствами L2 и L3
    29. Базовая балансировка нагрузки TCP L4
    30. Базовая балансировка нагрузки TCP L7

2. Практика.
    1. Дистанционно-векторный протокол RIP
    2. Дистанционно-векторный протокол EGRP
    3. Протокол на базе состояния каналов связиOSPF
    4. Концепция и принципы работы DTP
    5. Концепция и принципы работы VTP
    6. Концепция и принципы работы STP
    7. Концепция и принципы работы RSTP
    8. Концепция и принципы работы MSTP
    9. Концепция и принципы работы SPB
    10. Протокол сетевого времени NTP
    11. Стандартные списки ACL
    12. Расширенные списки ACLIPv4
    13. Расширенные списки ACLIPv6
    14. Фильтрация трафика на уровне L2
    15. Базовая настройка ZBFW

16. Базовая настройка DMZ

4 ЗАДАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

Лабораторная работа №1 Создание сеанса управления Telnet.

Задание: Изучить подходы внедренияконцепций сетевого виртуального терминала (NetworkVirtualTerminal) или NVT, принципов договорных опций (согласование параметров взаимодействия), симметрии связи "терминал-процесс"..

Лабораторная работа №2 Создание сеанса управления SSH.

Задание: Научиться конфигурировать защищенный протокол удаленного управления SSH на оборудовании Cisco и Mikrotik, а также давать доступ оборудованию в интернет.

Лабораторная работа №3 Настройка системы SNMP-мониторинга с использованием оборудования Cisco уровней L2 и L3.

Задание: Создание сети и настройка базовых параметров устройств. Настройка диспетчера и агентов SNMP. Преобразование кодов OID с использованием Cisco SNMP ObjectNavigator.

Лабораторная работа №4 Пример реализации OpenFlowConfiguration.

Задание: Организация контроля состояния канала связи. Измерение накладных расходов на организацию мониторинга

Лабораторная работа №5 Настройка модели многодоменной сетевой архитектуры с автосогласованием каналов связи и маршрутов.

Задание: Получение практических навыков конфигурирования оборудования для работыс протоколом динамической маршрутизации OSPF.Выполнение настройки сети с несколькими зонами.

Лабораторная работа №6 Построение многоуровневой системы синхронизации сетевых узлов с централизованным методом сбора статистик работы системы

Задание: Сообщения Syslog могут сопровождаться метками времени для анализа последовательности сетевых событий; поэтому важно синхронизировать часы всех сетевых устройств с помощью сервера NTP..

Лабораторная работа №7Использование ACL списков в структуре модели информационной безопасности узла сети

Задание: Обеспечение сетевой безопасности является важным аспектом при разработке и управлении IPсетями. Применение соответствующих правил для фильтрации пакетов на основе установленной политики безопасности.

Лабораторная работа №8Использование инструмента системного мониторинга Zabbix

Задание: Составление карты сети и серверов, которые должны быть охвачены мониторингам. Отражение текущего состояния серверов и узлов сети.

5 ТЕСТОВЫЕ ЗАДАНИЯ (примеры)

Какой из видов клиентских лицензий соответствует предлагаемому определению:
"Это специальный вид лицензии, предназначенный для подключения удаленных пользователей к корпоративному серверу терминалов. Данная лицензия не налагает ограничений на количество подключений, однако, согласно пользовательскому соглашению (EULA), сервер терминалов для таких подключений должен быть выделенным, что не допускает его использования для обслуживания сессий от локальных пользователей."

Выберите один ответ.

- ○ лицензия «на пользователя» (User Terminal Server CAL)
- ○ лицензия для внешних пользователей (External Terminal Server Connector)
- ○ нет верного варианта ответа
- ○ временная лицензия (Temporary Terminal Server CAL)
- ○ лицензия «на устройство» (Device Terminal Server CAL)

Какой из терминов соответствует предлагаемому определению:
"... объединяет в себе сеть (для управления трафиком), ресурсы (для управления рабочими нагрузками) и хранилище (для управления данными)."

Выберите один ответ.

- ○ Software Defined Data Center
- ○ Software Defined Networks
- ○ Software Defined Process
- ○ Software Defined Perimeter
- ○ Software Defined Storage

В чем состоит основное назначение преобразования NAT?

Выберите один ответ.

- ○ увеличение временной задержки при продвижении данных в глобальной сети
- ○ обеспечение обмена файлами между одноранговыми устройствами
- ○ повышение безопасности сети
- ○ повышение производительности сети
- ○ экономия IPv4-адресов

Определите среду, в рамках которой команда по копированию всего содержимого папки в другой каталог выглядит следующим образом:

Copy-Item -Path C:\New.Directory -Destination C:\temp -Recurse -Force -Passthru

Выберите один ответ.

- ○ Python
- ○ VBScript
- ○ Perl
- ○ PowerShell
- ○ Bash

Для какого из RIR зарезервирован диапазон IPv6 адресов **2800:0000::/12** ?

Выберите один ответ.

- ○ RIPE NCC
- ○ ARIN
- ○ APNIC
- ○ AFRINIC
- ○ LACNIC

Какой протокол позволяет защищать удаленные подключения?

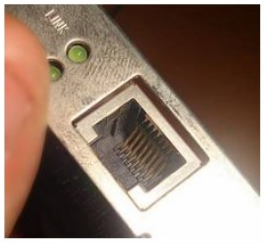
Выберите один ответ.

- ○ POP
- ○ SSH
- ○ FTP
- ○ NetBEUI
- ○ HTTP

При работе с удаленной системой по протоколу SSH часто возникает необходимость запуска команды, на выполнение которой требуется много времени. При этом известно, что после закрытия соединения SSH все выполняющиеся задания будут прерваны.
Какая из утилит позволит продолжить выполнение сеанса в фоне и вернуться в сеанс после переподключения?

Выберите один ответ.

- ○ terminal
- ○ freeze
- ○ sleep
- ○ tmux
- ○ нет верного варианта ответа



Выберите один ответ.

- RJ-45
- BNC
- Serial
- 110 тип
- RJ-11
- ST

Посмотрите на изображение. Укажите тип оборудования, к которому относится рисунок.

Выберите один ответ.

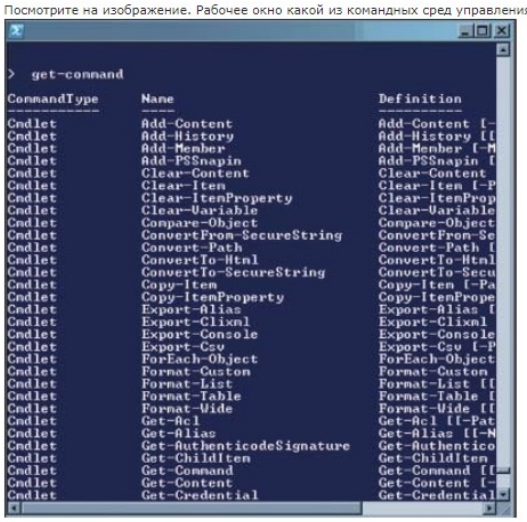
- Модем
- Коммутатор
- Концентратор
- Медиаконвертор
- Маршрутизатор

Многие современные компании оставляют за собой право контроля кода управления устройством, переданного во владению пользователю. Какой из вендоров получил репутационные потери после примера, описанного далее:
Закрытые в апреле 2020 года специалистами компании уязвимости нулевого дня были обнаружены ранее экспертами по ИБ из Google Project Zero и Threat Analysis Group. В том числе, CVE-2020-1027 — уязвимость ядра ОС ПК, позволяющая злоумышленникам запускать код с повышенными привилегиями и получить полный доступ к ядру системы.

Выберите один ответ.

- Tesla
- Cisco
- MicroSoft
- Samsung
- Apple

Посмотрите на изображение. Рабочее окно какой из командных сред управления на нем показано.



Выберите один ответ.

- NETSH
- SSH
- BASH
- Telnet
- PowerShell

Если один конец Ethernet-подключения настроен на полнодуплексный, а другой — на полудуплексный режим, где можно наблюдать возникновение поздних конфликтов?

Выберите один ответ.

- на обоих концах подключения
- только на последовательных интерфейсах
- на полнодуплексном конце подключения
- на полудуплексном конце подключения

Какому их видов облачных вычислений соответствует определение "... бизнес-модель предоставления услуг, при которой все физические ресурсы дата-центра, такие как вычислительные мощности, диски и сети, объединяются в большие пулы виртуальных ресурсов. Пул физических ресурсов (физический сервер или сервера) будет предоставляться только одному арендатору/организации..."?

Выберите один ответ.

- Публичное облако
- Локальное публичное облако
- Частное или приватное облако
- Гибридное облако
- Облачное сообщество

Какова значительная разница между концентратором и коммутатором локальной сети уровня 2?

Выберите один ответ.

- Каждый порт концентратора является доменом коллизии, а каждый порт коммутатора является доменом широковещательной рассылки.
- Концентратор пересылает кадры, а коммутатор пересылает только пакеты.
- Концентратор делит домены коллизий, а коммутатор делит домены широковещательной рассылки.
- Нет верного варианта ответа
- Концентратор расширяет домен коллизий, а коммутатор делит домен коллизий.

На рисунке представлен пример настройки текстового сообщения на устройствах под управлением Cisco IOS.

```
Router(config)#banner login ^
Enter TEXT message.  End with the character '^'
##########################################
#  This is a Login banner used to show   #
#    legal and privacy information.      #
#                                        #
#     Unauthorized users prohibited      #
##########################################
^
Router(config)#end
Router#exit
```

Для какого режима взаимодействия с оператором он предназначен?

Выберите один ответ.

- Сообщение входа в пользовательский режим (Сессия подключения установлена)
- Сообщение входящей линии терминала
- Сообщение для тайм-аута сессии управления
- Message of the Day
- Сообщение входа в привилегированный режим

7

Учреждение образования
«Гомельский государственный университет имени Франциска Скорины»

УТВЕРЖДАЮ
Проректор по учебной работе
ГГУ имени Ф. Скорины

_____ И.В. Семченко
_____
(дата утверждения)
Регистрационный № УД-_____/
уч.

ПРОТОКОЛЫ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ

Учебная программа учреждения высшего образования
для специальности1-45 80 01 Системы и сети инфокоммуникаций

2019

Учебная программа составлена на основе: образовательного стандарта ОСВО
1-45 80 01-2019 и учебного плана по специальности высшего образования второй ступени (магистратура) 1-45 80 01 Системы и сети инфокоммуникаций регистрационный № I 45-2-01/Д-19 от 09.04.2019 г.

СОСТАВИТЕЛЬ:
А.В.Воруев, доцент кафедры АСОИ

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой автоматизированных систем обработки информации
(протокол № ___от _____)

Научно-методическим советом Учреждения образования «Гомельский государственный университет имени Франциска Скорины».
(протокол № _8_от _17.05.2019_)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дисциплинакомпонента учреждения высшего образования «Протоколы дистанционного управления»специальности1-45 80 01 Системы и сети инфокоммуникацийявляется дисциплиной компонента учреждения высшего образованияи изучается магистрантами первого года обучения.

Актуальность изучения данной дисциплины продиктована практической необходимостью использования протоколов дистанционного управления при решении задач контроля, обслуживания и модернизации операционных систем сетевых устройств, а также построения современных сетевых сред, соответствующих стандартам программируемых сетевых архитектур.

Необходимость дисциплины «Протоколы дистанционного управления» связана с решением новых инженерных задач, возникающих при освоении и внедрении в сетевых стандартов и методов организации вычислительного процесса в сетевых структурах.

В изложении дисциплины используется комплексный подход по изучению современных проблем дистанционного управления: от разработки теоретических основ до формулировки практических рекомендаций по эффективному использованию протоколов промышленного управления.

ЦЕЛЬ, ЗАДАЧИ, РОЛЬ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью дисциплины «Протоколы дистанционного управления» является овладение магистрантами основами дистанционного управления и защиты от несанкционированного доступа операционных систем сетевых устройств.

Задачами дисциплины являются:

– изучение технологий построения транспортных сетей инфокоммуникаций;

– изучение протоколов распределения информации физического, канального, сетевого и транспортного уровней базовой эталонной модели взаимодействия открытых систем;

– изучение способов организации управляемой работы сетевых сред в составе группировки физических и виртуальных устройств;

– освоение принципов предотвращения несанкционированного доступа к операционным системам сетевых устройств;

– освоение принципов построения и технической эксплуатации транспортных сетей телекоммуникаций.

В результате изучения дисциплины магистрант должен:

знать:

– базовые технологии транспортных сетей инфокоммуникаций;

– протоколы физического, канального, сетевого и транспортного уровней модели OSI;

– протоколы внутренней и внешней маршрутизации;

– протоколы удаленного доступа к управлению сетевыми устройствами.

уметь:

– получать доступ к сетевому устройству с открытым и авторизованным доступом;

– проводить базовую настройку сетевых устройств с использованием протоколов Telnet, SSH, SNMP;

– настраивать протоколы маршрутизации;

– применять протоколы автоматического согласования параметров сетевых каналов и самоорганизации сетевых структур;

– организовывать централизованный сбор статистики по работе сетевых устройств;

– измерять и анализировать трафик в транспортных сетях;

– моделировать сетевое взаимодействие и активность пользователей;

должен владеть:

– представлениями о проектировании и управлении транспортными сетями.

ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ СОДЕРЖАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В результате изучения учебной дисциплины «Протоколы дистанционного управления» формируются следующие компетенции:

СК-2 Выполнение научно-исследовательские и опытно-конструкторские работ в области систем и сетей инфокоммуникаций.

СК-3 Владение технологиями проектирования и разработки инфокоммуникационных систем.

МЕТОДЫ (ТЕХНОЛОГИИ) ОБУЧЕНИЯ

Основными методами (технологии) обучения являются:

– словесные, наглядные, практические (по источнику изложения учебного материала);

– репродуктивные, объяснительно-иллюстрированные, поисковые, исследовательские, проблемные и др. (по характеру учебно-познавательной деятельности);

– индуктивные и дедуктивные (по логике изложения и восприятия учебного материала).

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ МАГИСТРАНТОВ

При изучении учебной дисциплины рекомендуется использовать

следующие формы самостоятельной работы:

– проработка конспекта лекций и учебной литературы;

– самостоятельная подготовка к лабораторным и практическим работам;

– изучение материала, вынесенного на самостоятельную проработку;

– самостоятельная работа в виде решения индивидуальных задач в аудитории во время проведения лабораторных занятий под контролем преподавателя;

– самостоятельное решение во внеурочное время контрольных задач, получаемых на лекциях.

ДИАГНОСТИКА КОМПЕТЕНЦИИ МАГИСТРАНТА

Учебным планом специальности в качестве формы итогового контроля по дисциплине «Протоколы дистанционного управления»предусмотрен экзамен.

Для текущего контроля и самоконтроля знаний и умений учащихся по данной дисциплине используется: выполнение лабораторных работ с их защитой.

Дисциплина учреждения высшего образования «Протоколы дистанционного управления» изучается магистрантами1 года обучения (1семестр) дневной формы обучения для специальности: 1-45 80 01 Системы и сети инфокоммуникаций.

Общее количество часов –230.

Дневная форма обучения: аудиторное количество часов – 72; из них: лекционных занятий – 32 (в том числе УСР – 14), практических занятий – 16, лабораторных работ – 24.

Форма отчётности – экзамен.

Заочная форма обучения: аудиторное количество часов – 18; из них: лекционных занятий – 8, практических занятий – 4, лабораторных работ – 6.

Форма отчётности – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1 Ключевые принципы программно-определяемых сетей

В алгоритмическом плане пересылка пакетов в сети проста, и основной задачей является достижение необходимой скорости передачи данных. Отправителями и получателями пакетов являются интерфейсы маршрутизатора, а определение адресата осуществляется с помощью т.н. таблицы передачи -ForwardingInformationBase (FIB).

Задачей же маршрутизации является построение собственной таблицы, таблицы маршрутизации (RoutingInformationBase, RIB), которая потом транслируется в таблицу FIB. Для построения этой таблицы и используются протоколы маршрутизации, которые на основе информации, полученной от соседних маршрутизаторов, и собственной конфигурации (например, статических маршрутов и ограничений, наложенных сетевой политикой маршрутизации), формируют представление о сети и ее топологии.

В контексте данной темы важным в этой модели является то, что каждый маршрутизатор принимает решения самостоятельно и относительно независимо.

Такая модель работает замечательно в простых сетях, особенно когда основной задачей является обеспечение связности. Она проста и надежна. Однако по мере усложнения сетевой архитектуры и политики внутренней и внешней маршрутизации, ограничения модели становятся все более заметны.

Новые функции и возможности неимоверно увеличивают сложность системы, их тестирование трудоемко, а внедрение дорогостояще и рискованно. Поэтому большие надежды возлагают на сетевую парадигму, получившую название SDN (Software Defined Networking) или Программно-Конфигурируемая Сеть.

Раздел 2 Протоколы доступа к операционной системе

Тема 2.1Протокол прикладного уровня TELNET

TELNET (teletypenetwork) - сетевой протокол для реализации текстового терминального интерфейса по сети (в современной форме - при помощи транспорта TCP). Название «telnet» имеют также некоторые утилиты, реализующие клиентскую часть протокола. Современный стандарт протокола описан в RFC 854.

Для каждого интерфейса TELNET переводит символы (данные или команды), которые получает от местного терминала, в NVT(NetworkVirtualTerminal)-форму и доставляет их в сеть. С другой стороны, сервер TELNET переводит команды из формы NVT в форму, доступную удаленному компьютеру.

Всю информацию Telnet посылает в незашифрованном виде, поэтому сейчас он рассматривается как один из самых небезопасных сервисов в

Интернет. Telnet безопасен только в том случае, когда безопасны все машины и сети на пути от компьютера-клиента к компьютеру-серверу.

Тема 2.2 Протокол SSH

SSH (secureshell- безопасная оболочка) это набор программ, которые позволяют регистрироваться на компьютере по сети, удаленно выполнять на нем команды, а также копировать и перемещать файлы между компьютерами. SSH организует защищенное безопасное соединение поверх небезопасных каналов связи. Спецификация протокола SSH-2 содержится в RFC 4251.

SSH предоставляет замены традиционным r-командам удаленного доступа с тем отличием, что они обладают повышенной безопасностью. Они выполняются поверх защищенных зашифрованных соединений, которые не позволяет прослушивать или подменять трафик. Кроме того, SSH может обеспечивать безопасное соединение для передачи любого другого трафика: например, почтовых сообщений или файлов.

Тема 2.3КонцепцияInternet Standard Management Framework

SNMP (SimpleNetworkManagementProtocol- простой протокол сетевого управления) - стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для контроля подключённых к сети устройств на предмет условий, которые требуют внимания администратора. SNMP определён Инженерным советом интернета (IETF) как компонент TCP/IP.

Базовая структура InternetStandardManagementFramework состоит из основных компонентов (для всех версий концепции - для SNMPv1, SNMPv2, SNMPv3): SNMP-сущность (SNMPentity), MIB (managementinformationbase, базаданных, котораяиспользуетсядляуправленияустройствамивсети), NMS (NetworkManagementStation, станция управления сетью).

Спецификация RFC 1155, RFC 1212, RFC 1213, RFC 1157, RFC 3411.

Тема 2.4 Протокол управления процессом обработки данных Openflow

Протокол используется для управления сетевыми коммутаторами и маршрутизаторами с центрального устройства - контроллера сети (например, с сервера или даже персонального компьютера). Это управление заменяет или дополняет работающую на коммутаторе (маршрутизаторе) встроенную программу, осуществляющую построение маршрута, создание карты коммутации и т. д.. Контроллер используется для управления таблицами потоков коммутаторов, на основании которых принимается решение о передаче принятого пакета на конкретный порт коммутатора. Таким образом

в сети формируются прямые сетевые соединения с минимальными задержками передачи данных и необходимыми параметрами.

Версии микропрограмм с поддержкой Openflow разработаны для устройств многих производителей, включая ExtremeNetworks, Juniper, Cisco, HP, IBM, NEC.

Раздел 3 Протоколы автоматического согласования параметров связи

Тема 3.1Протоколы согласованияканального уровня

Коммутатор и протоколы, которые используют коммутаторы могут быть целью атак. Более того, некоторые настройки коммутаторов (как правило, это настройки по умолчанию) позволяют выполнить ряд атак и получить несанкционированный доступ к сети или вывести из строя сетевые устройства. Однако, коммутатор может быть и достаточно мощным средством защиты. Так как через него происходит всё взаимодействие в сети, то логично контролировать это на нем.

Безопасностьпротоколов, которыеиспользуюткоммутаторы: Spanning Tree Protocol (STP); 802.1Q (VLAN); Link Layer Discovery Protocol (LLDP); Cisco Discovery Protocol (CDP); Extreme Discovery Protocol; Foundry Discovery Protocol; Nortel Discovery Protocol; MikroTik Neighbor Discovery Protocol (MNDP); VLAN Trunking Protocol (VTP); Dynamic Trunking Protocol (DTP); Hot Standby Router Protocol (HSRP).

Тема 3.2Протоколымаршрутизации

Маршрутизация - процесс определения лучшего пути, по которому пакет может быть доставлен получателю.Возможные пути передачи пакетов называются маршрутами. Лучшие маршруты к известным получателям хранятся в таблице маршрутизации.В зависимости от способа заполнения таблицы маршрутизации, различают два вида маршрутизации: статическая маршрутизация и динамическая маршрутизация

Устройство, выполняющее маршрутизацию, именуется маршрутизатором. В качестве маршрутизатора могут использоваться специализированные устройства, такие, например, как Cisco Router, или это могут быть обычные компьютеры, оснащённые несколькими сетевыми картами (или принимающие тегированный трафик) и работающие под управлением универсальной операционной системы, такой как FreeBSD или GNU/Linux.

В зависимости от алгоритма маршрутизации протоколы делятся на два вида: дистанционно-векторные протоколы (основаны на алгоритме DVA-distancevectoralgorithm) и протоколы состояния каналов связи (основаны на алгоритме LSA-linkstatealgorithm).

По области применения выделяют протоколы:для междоменной маршрутизации и для внутридоменной маршрутизации.

Тема 3.3 Синхронизация событий и сбор сетевых статистик

NetworkTimeProtocol (NTP) - сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью. NTP использует для своей работы протокол UDP 123 порт. Система NTP чрезвычайно устойчива к изменениям латентности среды передачи. NTP использует алгоритм Марзулло (предложен КейтомМарзулло (KeithMarzullo) из Университета Калифорнии, Сан-Диего), включая такую особенность, как учёт времени передачи. В версии 4 способен достигать точности 10 мс (1/100 с) при работе через Интернет, и до 0.2 мс (1/5000 с) и лучше внутри локальных сетей.

Раздел 4Ограничение доступа к управлению узлами сети

Тема 4.1Межсетевая фильтрация трафика

Межсетевой экран, сетевой экран - программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.Список контроля доступа (ACL)- это последовательный список разрешающих или запрещающих операторов, называемых записями списка контроля доступа (ACE). Записи списка контроля доступа обычно называют утверждениями списка контроля доступа. При прохождении сетевого трафика через интерфейс, где действует список контроля доступа (ACL), маршрутизатор последовательно сопоставляет информацию из пакета с каждой записью в списке контроля доступа на предмет соответствия. Это называется фильтрацией пакетов.

Тема 4.2Внутрисетевая фильтрация трафика

Частная VLAN (PVLAN), также известная как изоляция портов, представляет собой метод в компьютерных сетях, где VLAN содержит порты коммутатора, которые ограничены так, что они могут взаимодействовать только с данной «восходящей линией связи». Ограниченные порты называются «частными портами». Каждая частная VLAN обычно содержит много частных портов и одну восходящую линию связи. В качестве восходящей линии связи обычно используется порт (или группа агрегации каналов), подключенный к маршрутизатору, брандмауэру, серверу, сети провайдера или подобному центральному ресурсу.

Коммутатор перенаправляет все кадры, полученные от частного порта, на порт восходящей линии связи, независимо от идентификатора VLAN или MAC-адреса назначения. Кадры, принятые от порта восходящей линии связи,

пересылаются обычным способом (то есть на порт, содержащий MAC-адрес назначения, или на все порты VLAN для широковещательных кадров или для неизвестных MAC-адресов назначения). В результате прямой одноранговый трафик между одноранговыми узлами через коммутатор блокируется, и любая такая связь должна проходить через восходящую линию связи. Хотя частные VLAN обеспечивают изоляцию между узлами на канальном уровне, связь на более высоких уровнях все еще может быть возможной в зависимости от дальнейшей конфигурации сети.

Типичное приложение для частной VLAN - это гостиница или Ethernet для домашней сети, где в каждой комнате или квартире есть порт для доступа в Интернет. Подобная изоляция порта используется в ADSL DSLAM на основе Ethernet. Разрешение прямого обмена данными на канальном уровне между узлами клиента может подвергнуть локальную сеть различным атакам безопасности, таким как подмена ARP, а также увеличить вероятность повреждения из-за неправильной конфигурации.

RADIUS (RemoteAuthenticationDialInUserService, служба удалённой аутентификации дозванивающихся пользователей) - сетевой протокол, предназначенный для обеспечения централизованной аутентификации, авторизации и учёта (Authentication, Authorization, andAccounting, AAA) пользователей, подключающихся к различным сетевым службам. Используется, например, при аутентификации пользователей WiFi, VPN, в прошлом, dialup-подключений, и других подобных случаях. Описан в стандартах RFC 2865 и RFC 2866.

Тема 4.3 Системы централизованного управления доступом

Для решения вопросов управления необходимо получать информацию обо всех событиях сети. Дляэтогосуществуют SIEM-решения (Security Information and Event Management).

Данные решения включают в себя средства автоматизированного сбора событий, их нормализации, то есть приведения текста события к некоторому общему виду (например, выделение из события имени пользователя, его IP-адреса, порта соединения и т.д.). Также, классический SIEM осуществляет сохранение всех событий в единой БД и позволяет составлять правила корреляции различных событий. С помощью этих правил специалист по безопасности может существенно автоматизировать свою работу по обнаружению и предотвращению атак. Опционально решение может также содержать средства генерации отчетов и автоматизации расследования инцидентов. Как правило, присутствует возможность реагирования на события и интеграции с системами IPS.

Тема 4.4 Понятие Zone-Based Policy Firewall

В основе Zone-BasedPolicyFirewall лежит распределение интерфейсов маршрутизатора по зонам безопасности. После этого все правила настраиваются для взаимодействий между зонами.Такой подход облегчает

настройки правил межсетевого экрана. Кроме того в Zone-BasedPolicyFirewall используется Cisco PolicyLanguage (CPL), которая позволяет более гибко, чем в предыдущих версиях межсетевого экрана, настраивать правила фильтрации трафика.Zone-BasedPolicyFirewallпоявилсявIOS 12.4(6)T.

Раздел 5 Автоматизация операций по обслуживанию сети

Тема 5.1 Понятие сетевого контура

Термин FogComputing («туманные вычисления») был введен в оборот вице-президентом компании Cisco ФлавиоБономи (FlavioBonomi) в 2011 году. Он предложил концепцию FogComputing по аналогии с «облачными вычислениями» (CloudComputing), как расширение «облака» до границ сети. Технологически, концепция FogComputing тесно связана с распределёнными (облачными) дата-центрами, в которых серверы дата-центров могут располагаться во многих местоположениях, вплоть до границы сети. Дата-центры могут быть небольшими (контейнерного, модульного или мобильного исполнения), являясь фактически «выносами» крупных дата-центров. Таким образом, отличительная черта FogComputing-приближенность к конечным пользователям и поддержка их мобильности.

Развитие интернета вещей (IoT, InternetofThings) потребовало поддержки мобильности устройств IoT для различных местоположений с геолокацией и с небольшой задержкой на обработку данных. Поэтому была предложена новая платформа для удовлетворения таких требований, которая и получила название Fogcomputing – «туманные вычисления». Её основной особенностью является обработка данных в непосредственной близости от источников их получения, без необходимости их передачи в крупные дата-центры только для того, чтобы их там обработать и передать назад результаты.

Тема 5.2 Балансировка сетевых сервисов

Цель балансировки нагрузки - оптимизация использования ресурсов, максимизация пропускной способности, уменьшение времени отклика и предотвращение перегрузки какого-либо одного ресурса. Использование нескольких компонентов балансировки нагрузки вместо одного может повысить надежность и доступность за счет резервирования. Балансировка нагрузки предполагает обычно наличие специального программного обеспечения или аппаратных средств, таких как многоуровневый коммутатор или система доменных имен, как серверный процесс.

В масштабах вычислительного процесса решения по балансировке нагрузки часто разделяются на две категории: L4 и L7. Они относятся к уровням 4 и 7 модели OSI. Модель OSI представляет очень плохое приближение к сложности решений балансировки нагрузки, которые включают традиционные протоколы уровня 4, такие как TCP и UDP, но часто

заканчиваются включением битов и частей протоколов на разных уровнях OSI.

Тема 5.3 Визуализация взаимодействия сетевых устройств

Для эффективного извлечения ценной информации важно, чтобы коллектор потоков мог нормализовать данные телеметрии из различных источников, не теряя при этом исходной информации, содержащейся в ненормализованных данных. Это позволит анализировать весь объем собранных данных с использованием единого подхода, при этом имея возможность пользоваться преимуществами отдельных протоколов (например, счетчиками выборки sFlow).

Zabbix- это полномасштабный инструмент для сетевого и системного мониторинга сети, который объединяет несколько функций в одной веб-консоли. Он может быть сконфигурирован для мониторинга и сбора данных с самых разных серверов и сетевых устройств, обеспечивая обслуживание и мониторинг производительности каждого объекта.

Тема 5.4 Программирование взаимодействия сетевых устройств

Архитектура цифровых сетей Cisco DigitalNetworkArchitecture (Cisco DNA) предлагает заказчикам набор программного и аппаратного обеспечения для работы. Cisco DNA Center- интуитивная, централизованная система управления, основанная на интенционном принципе и охватывающая процессы, связанные с проектированием, конфигурированием, политиками и обеспечением исполнения (assurance). Получая от Cisco DNA Center полный обзор и контекстную информацию по всей сети, ИТ-специалисты могут централизовано управлять всеми сетевыми функциями.

Программноопределяемыйдоступ (Software-Defined Access, SD-Access). В технологии SD-Access автоматизация применения политик и сегментации сети используется для существенного упрощения доступа к сети со стороны пользователей, устройств и объектов. Автоматизируя такие повседневные рутинные операции, как настройка, конфигурирование и отладка, SD-Access резко уменьшает время, необходимое для адаптации сети, сокращает сроки устранения проблем с нескольких недель и месяцев до нескольких часов, а также существенно ослабляет последствия взлома систем безопасности.

Платформа сетевых данных и обеспечение исполнения (NetworkDataPlatformandAssurance). Новая мощная аналитическая платформа оперативно выполняет классификацию и корреляцию больших объемов передаваемых по сети данных и с помощью машинного обучения трансформирует их в проактивную аналитику, бизнес-информацию и оперативную информацию, выдавая результаты с помощью сервиса Cisco DNA CenterAssurance.

Анализ зашифрованного трафика (EncryptedTrafficAnalytics). Почти половина кибератак сегодня маскируются в зашифрованном трафике, и их число постоянно растет. Используя для анализа потоков данных интеллектуальные средства Cisco Talos и машинное обучение, сеть способна

определять сигнатуры известных атак даже в зашифрованном трафике, не расшифровывая его и сохраняя конфиденциальность данных.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА (дневная форма обучения)

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов					Кол-во часов УСР	Формы контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	**ВВЕДЕНИЕ В ДИСЦИПЛИНУ (2 Ч.)**	**2**						
1.1	Ключевые принципы программно-определяемых сетей 1. История создания и развития программно-определяемых сетей и структур. 2. Самоорганизация работы сетевых устройств на разных уровнях модели ISO/OSI. 3. Устойчивость связи и балансировка трафика в режиме ONLINE.	**2**						
2.	**ПРОТОКОЛЫ ДОСТУПА К ОПЕРАЦИОННОЙ СИСТЕМЕ (20 Ч.)**	**4**	**4**		**8**		**4**	
2.1.	Протокол прикладного уровня TELNET 1. Структура сетевых примитивов и сообщений telnet 2. Виды устройств, поддерживающих управление по протоколу telnet 3. Программные оболочки telnet-соединений	**2**			**2**			отчет по лабораторной работе
2.2	Протокол SSH 1. Обеспечение безопасности SSH 2. Аутентификация в SSH с помощью открытых ключей 3. Туннели SSH		**4**		**4**			отчет по лабораторной работе
2.3	Концепция Internet Standard Management Framework 1. Архитектура Internet Standard Management Framework 2. MIB 3.Сообщения протокола SNMP 4. Настройка SNMP на сетевых устройствах.	**2**			**2**		**2**	отчет по лабораторной работе
2.4	Протокол управления процессом обработки данных Openflow 1. Путь прохождения данных (datapath). 2. Таблицы потоков (flowtable) и действий. 3. Контроллеры Openflow.						**2**	

1	2	3	4	5	6	7	8	9
3.	**ПРОТОКОЛЫ АВТОМАТИЧЕСКОГО СОГЛАСОВАНИЯ ПАРАМЕТРОВ СВЯЗИ (14 Ч.)**	**2**	**4**		**4**		**4**	
3.1	Протоколы согласования канального уровня 1. Концепция и принципы работы DTP 2. Концепция и принципы работы VTP 3. Концепция и принципы работы STP 4. Протокол сетевого времени NTP		**4**				**2**	
3.2	Протоколы маршрутизации 1. Дистанционно-векторные протоколы 2. Протоколы состояния каналов связи 3. Протоколы для междоменной и межсетевой маршрутизации 4. On Demand Routing						**2**	
3.3	Синхронизация событий и сбор сетевых статистик 1. Иерархическая система «часовых уровней» NTP 2. Системный журнал (Syslog) 3. Формат сообщений системного журнала 4. Сервер системного журнала	**2**			**4**			отчет по лабораторной работе
4.	**ОГРАНИЧЕНИЕ ДОСТУПА К УПРАВЛЕНИЮ УЗЛАМИ СЕТИ (22 Ч.)**	**6**	**4**		**8**		**4**	
4.1	Межсетевая фильтрация трафика 1. Стандартные списки ACL 2. Расширенные списки ACL 3. Фильтрация трафика на уровне L2	**2**			**4**		**2**	отчет по лабораторной работе
4.2	Внутрисетевая фильтрация трафика 1. Сетевая сегрегация 2. Гостевые сети 3. Сети резервного копирования	**2**						
4.3	Системы централизованного управления доступом 1. Уязвимости операционных систем узлов сети 2. Разделение функций controlplan и dataplan 3. Сетевой протокол централизованной аутентификации, авторизации и учёта RADIUS		**4**				**2**	
4.4	Понятие Zone-BasedPolicyFirewall 1. Базовая настройка ZBFW. 2. Доступность и безопасность. 3. Туннелированние соединений.	**2**			**4**			отчет по лабораторной работе
5.	**АВТОМАТИЗАЦИЯ ОПЕРАЦИЙ ПО ОБСЛУЖИВАНИЮ СЕТИ (14 Ч.)**	**4**	**4**		**4**		**2**	
5.1	Понятие сетевого контура 1. Развитие интернета вещей 2. Технологическая концепция FogComputing 3. Сценариев использования FogComputing и балансировка точки обработки данных	**2**						

1	2	3	4	5	6	7	8	9
5.2	Балансировка сетевых сервисов 1. Балансировка трафика сетевыми устройствами L2 и L3 2. Базовая балансировка нагрузки TCP L4 3. Базовая балансировка нагрузки TCP L7		**2**					
5.3	Визуализация взаимодействия сетевых устройств 1. Утилита NeDi. 2. Инструмент для анализа пакетов Ntop. 3. Инструмент системного мониторинга Zabbix.	**2**			**4**		**2**	отчет по лабораторной работе
5.4	Программирование взаимодействия сетевых устройств 1. Software-DefinedAccess 2. Network Data Platform and Assurance 3. Encrypted Traffic Analytics		**2**					
	Всего по дисциплине	**18**	**16**		**24**		**14**	**экзамен**

Доцент кафедры АСОИ А.В.Воруев

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА (заочная форма обучения, заочная интегрированная форма обучения на основе среднего специального образования, дистанционная форма обучения)

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов					Кол-во часов УСР	Формы контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	**ВВЕДЕНИЕ В ДИСЦИПЛИНУ (2 Ч.)**	**2**						
1.1	Ключевые принципы программно-определяемых сетей 1. История создания и развития программно-определяемых сетей и структур. 2. Самоорганизация работы сетевых устройств на разных уровнях модели ISO/OSI. 3. Устойчивость связи и балансировка трафика в режиме ONLINE.	**2**						
2.	**ПРОТОКОЛЫ ДОСТУПА К ОПЕРАЦИОННОЙ СИСТЕМЕ (4 Ч.)**	**2**			**2**			
2.1.	Протокол прикладного уровня TELNET 1. Структура сетевых примитивов и сообщений telnet 2. Виды устройств, поддерживающих управление по протоколу telnet 3. Программные оболочки telnet-соединений	**Самостоятельное изучение**						
2.2	Протокол SSH 1. Обеспечение безопасности SSH 2. Аутентификация в SSH с помощью открытых ключей 3. Туннели SSH	**Самостоятельное изучение**						
2.3	Концепция Internet Standard Management Framework 1. Архитектура Internet Standard Management Framework 2. MIB 3.Сообщения протокола SNMP 4. Настройка SNMP на сетевых устройствах.	**2**			**2**			отчет по лаборатор-ной работе
2.4	Протокол управления процессом обработки данных Openflow 1. Путь прохождения данных (datapath). 2. Таблицы потоков (flowtable) и действий. 3. Контроллеры Openflow.	**Самостоятельное изучение**						

1	2	3	4	5	6	7	8	9
3.	**ПРОТОКОЛЫ АВТОМАТИЧЕСКОГО СОГЛАСОВАНИЯ ПАРАМЕТРОВ СВЯЗИ (8 Ч.)**	**2**	**2**		**4**			
3.1	Протоколы согласования канального уровня 1. Концепция и принципы работы DTP 2. Концепция и принципы работы VTP 3. Концепция и принципы работы DTP 4. Протокол сетевого времени NTP		**2**					
3.2	Протоколы маршрутизации 1. Дистанционно-векторные протоколы 2. Протоколы состояния каналов связи 3. Протоколы для междоменной и межсетевой маршрутизации 4. On Demand Routing	**Самостоятельное изучение**						
3.3	Синхронизация событий и сбор сетевых статистик 1. Иерархическая система «часовых уровней» NTP 2. Системный журнал (Syslog) 3. Формат сообщений системного журнала 4. Сервер системного журнала	**2**			**4**			отчет по лабораторной работе
4.	**ОГРАНИЧЕНИЕ ДОСТУПА К УПРАВЛЕНИЮ УЗЛАМИ СЕТИ (2 Ч.)**	**2**						
4.1	Межсетевая фильтрация трафика 1. Стандартные списки ACL 2. Расширенные списки ACL 3. Фильтрация трафика на уровне L2	**2**						
4.2	Внутрисетевая фильтрация трафика 1. Сетевая сегрегация 2. Гостевые сети 3. Сети резервного копирования	**Самостоятельное изучение**						
4.3	Системы централизованного управления доступом 1. Уязвимости операционных систем узлов сети 2. Разделение функций controlplan и dataplan 3. Сетевой протокол централизованной аутентификации, авторизации и учёта RADIUS	**Самостоятельное изучение**						
4.4	Понятие Zone-BasedPolicyFirewall 1. Базовая настройка ZBFW. 2. Доступность и безопасность. 3. Туннелированние соединений.	**Самостоятельное изучение**						
5.	**АВТОМАТИЗАЦИЯ ОПЕРАЦИЙ ПО ОБСЛУЖИВАНИЮ СЕТИ (2 Ч.)**		**2**					
5.1	Понятие сетевого контура 1. Развитие интернета вещей 2. Технологическая концепция FogComputing 3. Сценариев использования FogComputing и балансировка точки обработки данных	**Самостоятельное изучение**						

1	2	3	4	5	6	7	8	9
5.2	Балансировка сетевых сервисов 1. Балансировка трафика сетевыми устройствами L2 и L3 2. Базовая балансировка нагрузки TCP L4 3. Базовая балансировка нагрузки TCP L7	**Самостоятельное изучение**						
5.3	Визуализация взаимодействия сетевых устройств 1. Утилита NeDi. 2. Инструмент для анализа пакетов Ntop. 3. Инструмент системного мониторинга Zabbix.	**Самостоятельное изучение**						
5.4	Программирование взаимодействия сетевых устройств 1. Software-DefinedAccess 2. Network Data Platform and Assurance 3. Encrypted Traffic Analytics		**2**					
	Всего по дисциплине	**8**	**4**		**6**			**экзамен**

Доцент кафедры АСОИ А.В.Воруев

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

1. Организация доступа к сетевому устройству по протоколу TELNET по консольному и удаленному способам подключения.
2. Организация доступа к сетевому устройству по протоколу SSH.
3. Организация доступа к сетевому устройству с использованием семейства протоколов SNMP.
4. Организация доступа к сетевому устройству с использованием семейства протоколов HTTP.
5. Уязвимости и защита операционных систем сетевых устройств.
6. APIдоступа к сетевому оборудованию.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

1. Создание сеанса управления Telnet. Анализ сетевого трафика протокола средствами Wireshark.
2. Создание сеанса управления SSH. Анализ сетевого трафика протокола средствами Wireshark.
3. Настройка системы SNMP-мониторинга с использованием оборудования Cisco уровней L2 и L3.
4. ПримерреализацииOpenFlow Configuration.
5. Настройка модели многодоменной сетевой архитектуры с автосогласованием каналов связи и маршрутов.
6. Построение многоуровневой системы синхронизации сетевых узлов с централизованным методом сбора статистик работы системы
7. Использование ACL списков в структуре модели информационной безопасности узла сети
8. Использование инструмента системного мониторинга Zabbix

ФОРМЫ КОНТРОЛЯ ЗНАНИЙ

1 Отчеты по лабораторным работам.

2 Тестирование.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ НЕОБХОДИМОГО ОБОРУДОВАНИЯ И КОМПЬЮТЕРНЫХ ПРОГРАММ

1 Класс современных персональных ЭВМ.

2 Материалы электронного курса «CCNARoutingandSwitching» международного образовательного проекта CiscoNetworkingAcademy.

4 Программное средство моделирование сетевых сред CiscoPacketTracer.

5 Сетевой стенд, средства виртуализации сетевых узлов.

РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ УСР

Для самостоятельного изучения выделяются следующие темы:
- концепция Internet Standard Management Framework;
- протокол управления процессом обработки данных Openflow;
- протоколы согласования канального уровня;
- протоколы маршрутизации;
- межсетевая фильтрация трафика;
- системы централизованного управления доступом;
- визуализация взаимодействия сетевых устройств.

Тема2.3 КонцепцияInternetStandardManagementFramework – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в применении концепции InternetStandardManagementFramework.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие знания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.
2. Исправьте ошибки в определениях.
3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты, лабораторная работа.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.
2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.
3. Объясните принципы разбираемой темы.

Форма выполнения заданий – индивидуальная.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Опишите принципы управления устройствами в IP-сетях на основе архитектур TCP/UDP.
2. Определите различия в подходах к управлению устройств различного уровня модели ISO/OSI.
3. Рассмотрите функциональную модель SNMP рекомендованную Инженерным советом интернета (IETF).

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – реферат.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.
2) Конспект лекций по дисциплине.
3) Информация в сети Интернет.

Тема 2.4 Протокол управления процессом обработки данных Openflow – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в применении протокола управления процессом обработки данных Openflow.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие знания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.
2. Исправьте ошибки в определениях.
3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты, лабораторная работа.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.
2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.
3. Объясните принципы разбираемой темы.

Форма выполнения заданий – индивидуальная.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Опишите принципы построения пути прохождения данных.
2. Определите различия в подходах к управлению устройств различного уровня модели ISO/OSI.
3. Рассмотрите таблицы потоков (flowtable) и действий.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – реферат.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.
2) Конспект лекций по дисциплине.
3) Информация в сети Интернет.

Тема3.1 Протоколы согласования канального уровня – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в применении протоколов согласования канального уровня.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие знания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.
2. Исправьте ошибки в определениях.
3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты, лабораторная работа.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.

2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.

3. Объясните принципы разбираемой темы.

Форма выполнения заданий – индивидуальная.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Рассмотрите функциональную модель протокола DTPи его основные настройки.

2. Рассмотрите функциональную модель протокола VTPи его основные настройки.

3. Рассмотрите функциональную модель протокола STPи его основные настройки.

4. Рассмотрите функциональную модель протокола NTPи его основные настройки.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – реферат.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.

2) Конспект лекций по дисциплине.

3) Информация в сети Интернет.

Тема3.2Протоколы маршрутизации – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в применении протоколовдинамической маршрутизации.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие знания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.

2. Исправьте ошибки в определениях.

3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты, лабораторная работа.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.

2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.

3. Объясните принципы разбираемой темы.

Форма выполнения заданий – индивидуальная.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Рассмотрите функциональную модель дистанционно-векторных протоколов маршрутизациии их основные настройки.

2. Рассмотрите функциональную модель протоколов маршрутизациипо состоянию каналов связи и их основные настройки.

3. Рассмотрите функциональную модель междоменных и межсетевых протоколов маршрутизациии их основные настройки.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – реферат.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.

2) Конспект лекций по дисциплине.

3) Информация в сети Интернет.

Тема4.1Межсетевая фильтрация трафика – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в применении межсетевой фильтрации трафика.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие знания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.

2. Исправьте ошибки в определениях.

3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты, лабораторная работа.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.

2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.

3. Объясните принципы разбираемой темы.

Форма выполнения заданий – индивидуальная.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Опишите принципы построения стандартных списков ACL.

2. Опишите принципы построения расширенных списков ACL.

3. Опишите принципы построения системы фильрацииL2-трафика.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – реферат.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.

2) Конспект лекций по дисциплине.

3) Информация в сети Интернет.

Тема4.3 Системы централизованного управления доступом – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в применении концепции систем централизованного управления доступом.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие знания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.
2. Исправьте ошибки в определениях.
3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты, лабораторная работа.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.
2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.
3. Объясните принципы разбираемой темы.

Форма выполнения заданий – индивидуальная.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Опишите принципы управления устройствами в IP-сетях на основе SecurityInformationandEventManagement.
2. Определите различия в подходах к управлению устройств различного уровня модели ISO/OSI.
3. Рассмотрите функциональную модель реагирования на события в сети и способы интеграции с системами IPS.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – реферат.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.
2) Конспект лекций по дисциплине.
3) Информация в сети Интернет.

Тема5.3 Визуализация взаимодействия сетевых устройств – 2 часа

Цели: 1) овладеть знаниями по данной теме, терминологией и методологией; 2) сформировать компетенцию в применении систем визуализации взаимодействия сетевых устройств.

Виды заданий УСР по теме с учетом модулей сложности:

А) Задания, формирующие знания по учебному материалу на уровне узнавания:

1. Соотнесите термины с определениями.
2. Исправьте ошибки в определениях.

3. Вставьте в определение соответствующий термин.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – тесты, лабораторная работа.

Б) Задания, формирующие компетенции на уровне воспроизведения:

1. Дайте определения терминам.

2. Приведите примеры, подтверждающие или опровергающие правильность утверждений.

3. Объясните принципы разбираемой темы.

Форма выполнения заданий – индивидуальная.

Форма контроля выполнения заданий – тесты, контрольные вопросы.

В) Задания, формирующие компетенции на уровне применения полученных знаний:

1. Опишите принципы работы утилитыNeDi.

2. Опишите принципы работы инструмента для анализа пакетов Ntop.

3. Опишите принципы работы инструмента системного мониторинга Zabbix.

Форма выполнения заданий - индивидуальная.

Форма контроля выполнения заданий – реферат.

Учебно-методическое обеспечение:

1) Рекомендуемая основная и дополнительная литература.

2) Конспект лекций по дисциплине.

3) Информация в сети Интернет.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

ОСНОВНАЯ

1 Семенов, Ю. Алгоритмы телекоммуникационных сетей. Часть 3. Процедуры, диагностика, безопасность / Ю. Семенов // Учебное пособие – Бином. Лаборатория знаний, 2017. – 511 с

2 Семенов, Ю. А. Алгоритмы телекоммуникационных сетей : учебное пособие : для студентов по телекоммуникационным спец. Ч.2 : Протоколы и алгоритмы маршрутизации в Internet / Юрий Алексеевич Семенов. – Москва : Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2014. – 829 с.

3 Максимов, Н. В. Компьютерные сети : учебное пособие для студентов ссузов и вузов специальности "Информатика и вычислительная техника" / Николай Вениаминович Максимов, И.И. Попов, Министерство образования Российской Федерации. – 3-е изд., перер. – Москва : ФОРУМ, 2008. – 448 с.

4 Таненбаум, Э. Компьютерные сети: учебно-методическое издание / Э.Таненбаум; Д. Уэзеролл. 5-е изд. – 5-е изд. – Москва [и др.]: ПИТЕР, 2012. – 955 с.

5 Оливер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Оливер. – г. Санкт-Петербург : Питер, 2020. – 1008 с.

6 Олифер, В. Г. Сетевые операционные системы: учебник для вузов / В.Г.Олифер, Н.А.Олифер. – СПб. и др.: Питер, 2006. – 538 с. : ил.

7 Гук, М. Аппаратные средства локальных сетей: энциклопедия / М.Гук. – СПб. и др.: Питер, 2000. – 572 с. : ил.

ДОПОЛНИТЕЛЬНАЯ

8 Олифер, В. Г. Новые технологии и оборудование IP-сетей / В.Г. Олифер, Н.А. Олифер. – СПб.: БХВ. СПб., 2000. – 512 с.

9 Власов, Юрий Владимирович. Администрирование сетей на платформе MS WindowsServer : учебное пособие / Юрий Владимирович Власов, Татьяна Игоревна Рицкова. – Москва : Интернет-ун-т Информационных Технологий : БИНОМ. Лаборатория знаний, 2014. – 384 с.

ЭЛЕКТРОННЫЕ РЕСУРСЫ

10 Свободная энциклопедия ВикипедиЯ [Электронный ресурс]. – 2020. – Режим доступа: http://ru.wikipedia.org. – Дата доступа: 12.03.2020.

11 Интернет университет информационных технологий [Электронный ресурс]. – 2020. – Режим доступа: http://www.intuit.ru. – Дата доступа: 12.03.2020.

12 Информационно-справочный портал технической информации Хабрахабр [Электронный ресурс]. – 2020. – Режим доступа: http://habr.com. – Дата доступа: 12.03.2020.

13 Материалы электронного курса «CCNARoutingandSwitching» международного образовательного проекта CiscoNetworkingAcademy [Электронный ресурс]. – 2020. – Режим доступа: http://netacad.com/. – Дата доступа: 12.03.2020.