

Ваша команда является интегратором сетевых решений. Вас нанял УРТК им. А.С. Попова для развертывания удаленных филиалов в галактике «Звездных войн». Филиал УРТК в городе Корусант будет основным филиалом и разместит основное оборудование. Филиал в городе Мос-Эйсли будет вторым филиалом и будет использовать ресурсы основного филиала.

Ваша задача развернуть ЛВС филиалов в минимальной конфигурации. Настроить связь между филиалами и УРТК им. А.С. Попова. Произвести монтаж и настройку сетевого оборудования, развертывание и настройку основных сервисов.

Всё, что не охватывает данное задание, что не вредит оборудованию и другим участникам может быть Вами использовано.

Для работы будет выделено:

1 день – 7 часов

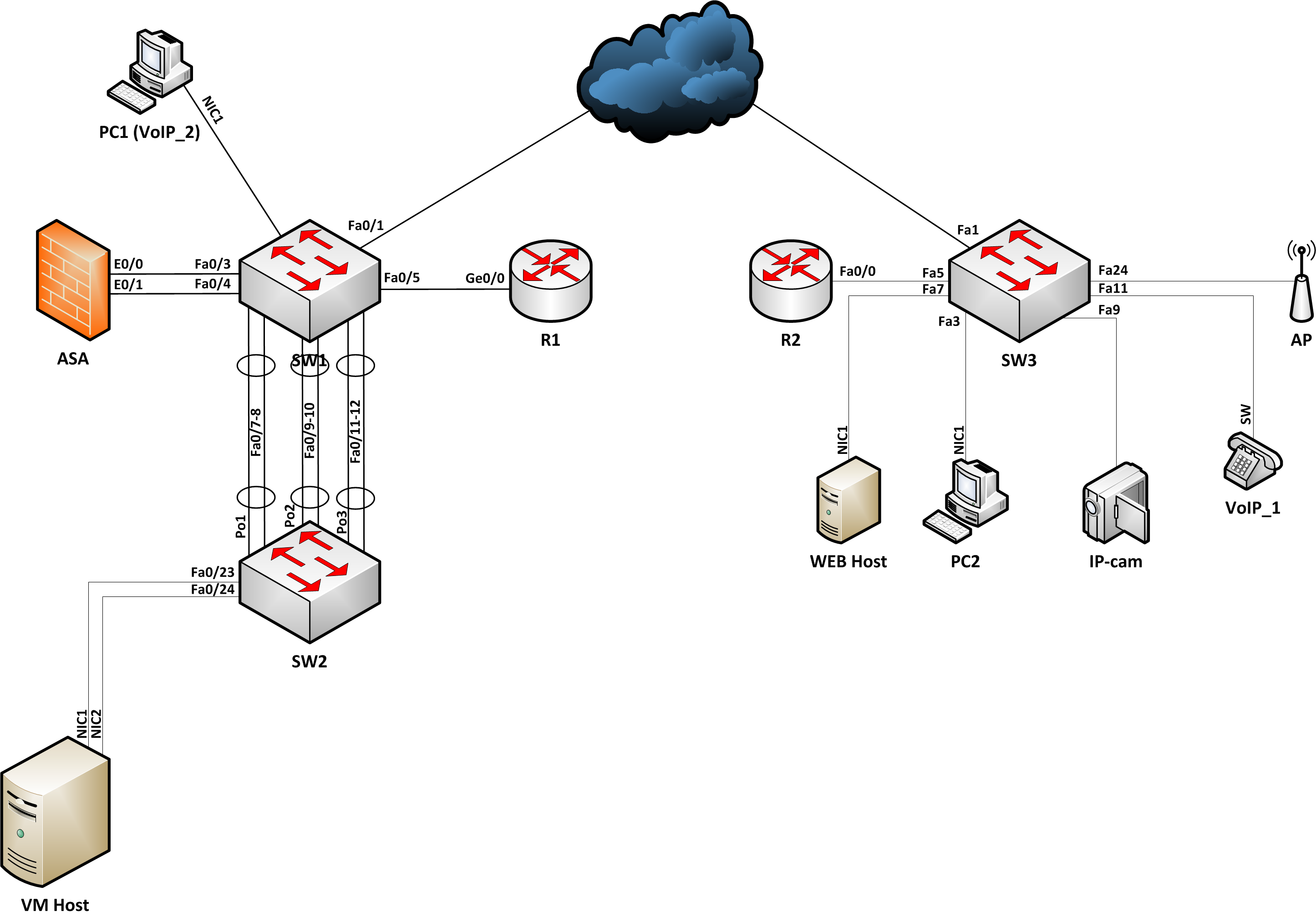
2 день – 5 часов

3 день – 2 часа работы команды + 1 час подготовки капитана к защите проекта + защита капитанов (20 мин на команду).

Внимание! Сборка PC2 будет проверяться в первый день.

Внимание! Все устройства и ОС перед проверкой будут перезагружаться!

Филиал в городе Корусант обслуживают два специалиста команды. Они территориально располагаются в одном месте – лаборатория 104. Филиал в городе Мос-Эйсли обслуживает один специалист – лаборатория 305.



Физическая топология сети

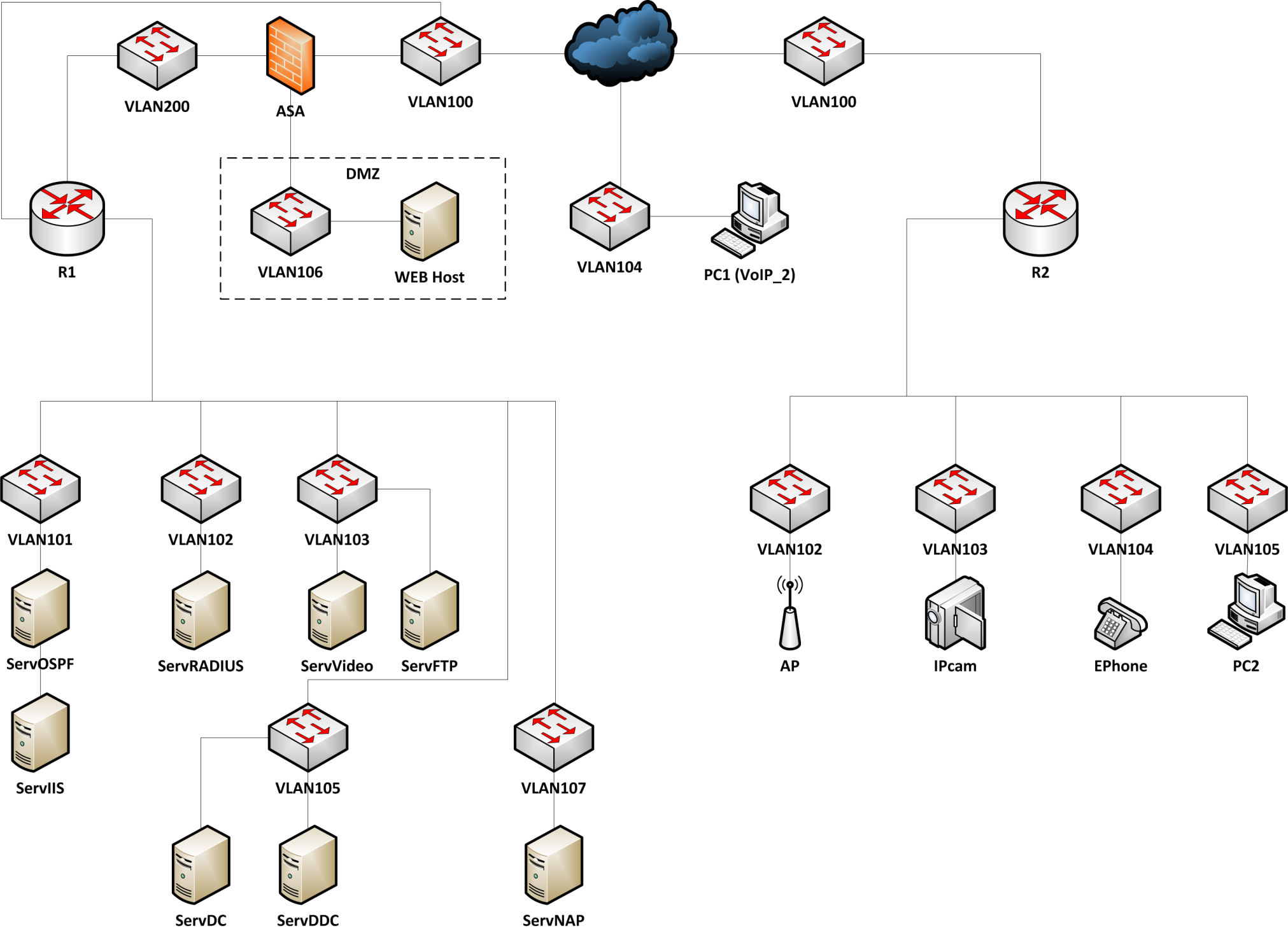


Схема канального уровня сети

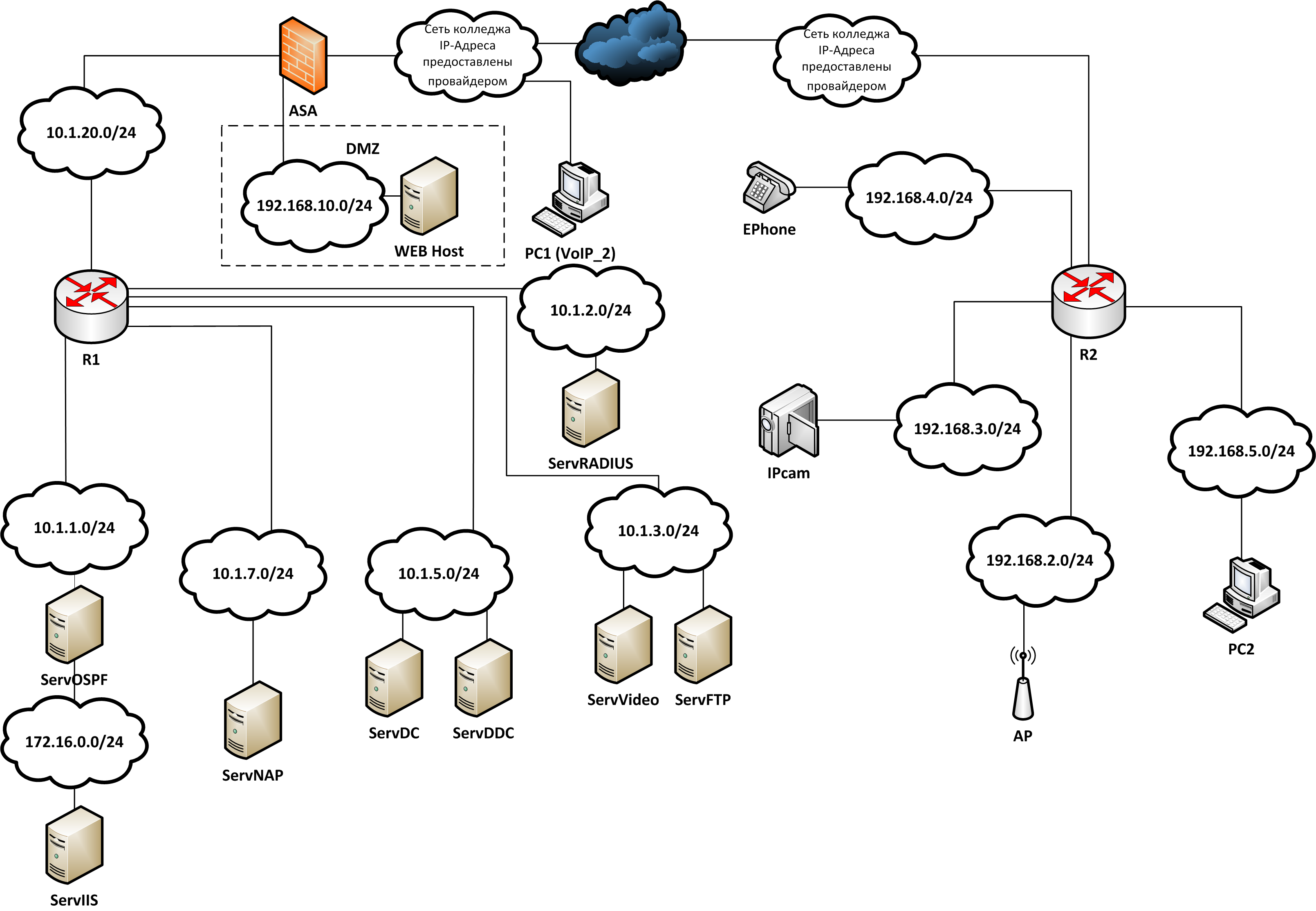


Схема сетевого уровня

Заказчик предоставил Вам все необходимое оборудование, инструменты, системное программное обеспечение и обеспечил доступ в Интернет.

Проверьте, не испортили ли ситхи преднастройки ваших систем.

В третий день Интернет, предоставляемый заказчиком, в филиал города Мос-Эйсли будет отключен. Надеемся, что филиал в городе Корусант «раздаст» интернет по настроенной сети.

Здесь и далее **XX** – номер команды (рабочего места). Например, команде и рабочему месту с номером 3 соответствуют значения **XX**=03. Будьте внимательны и не запутайтесь с числовыми значениями – это может привести к неработоспособности итоговой конфигурации и потере баллов!

Жюри будет оценивать выполнение задания по окончанию всех работ, в форме защиты проекта капитаном команды. Капитан должен иметь возможность подключения на ВСЕ устройства сети и ко ВСЕМ операционным системам.

На площадке присутствует технический специалист, который осуществляет помощь членам жюри. Без указания членов жюри он не может осуществлять техническую поддержку участников.

Недопустимо во время выполнения заданий использовать сотовые телефоны, планшеты и любые другие устройства (инструменты), не предоставленных организаторами. В случае нахождения устройства (инструмента), которое, по мнению жюри, может дать преимущество определенному участнику, данное устройство (инструмент) должно быть исключено из использования участником.

Организаторы предполагают, что квалификация участников позволяет корректно вводить выданные организаторами сетевые реквизиты и не организовывать «шторм». В противном случае участник может помешать выполнению задания другими участниками, при этом возможно снятие баллов.

Внимание! У Вас есть доступ к сети Интернет, настройте себе связь между участниками команды и организуйте работу именно «в команде» задачи должны решаться параллельно.

Недопустимо копирование или вынос задания во время Олимпиады за пределы конкурсной площадки.

Внимание! Необходимо явно разрешить ответы на «эхо-запросы» на всех узлах сети, так же капитан должен иметь возможность трассировать маршруты всей своей сети и за её пределы.

Внимание! Должен быть организован доступ с PC1 до сетевого коммутационного оборудования по протоколу SSH v2, до ОС на базе Linux – по протоколу SSH, до ОС на базе Windows – по протоколу RDP.

Установка операционных систем должна быть произведена с сервера сетевой установки. При корректном физическом подключении с внешней сети и соответствующих настройках на оборудовании, сервер сетевой установки раздаст IP адрес из Вашей подсети. По этому IP-адресу будет доступ в сеть Интернет. Вам потребуется самостоятельно, по выданному IP, определить свою сеть и использовать её в дальнейшем.

|  |  |  |
| --- | --- | --- |
| Наименование | Филиал Корусант | Филиал Мос-Эйсли |
| VM\_Host\_XX (сервер виртуализации) | Windows Server 2012 r2 | - |
| PC1 (в сборе) | Windows 8.1 | - |
| PC2 (отдельные комплектующие для сборки) | - | Windows 8.1 |
| WEB\_Host | - | Debian 7.8 |
| IP-телефон VoIP\_1 | - | Cisco 7962G (или аналог) |
| IP-телефон VoIP\_2 (программное на PC1+гарнитура) | IP Communicator | - |
| Маршрутизатор R1 | Cisco 2801 | - |
| Маршрутизатор R2 | - | Cisco 2801 |
| Коммутатор Sw1 | Cisco Catalyst 2960 | - |
| Коммутатор Sw2 | Cisco Catalyst 2960 | **-** |
| Коммутатор Sw3 | - | Cisco SF-300 24P |
| IP\_Cam | - | Dahua DH-IPC-HFW4300EP-0360B |
| AP | - | Cisco AIR-CAP1702I-R-K9 |
| ASA | Cisco ASA5505 | - |
| Инструмент обжима | 1 шт | 1 шт |
| Отвертка крестовая | - | 1 шт |
| Коннекторы 8P8C | N шт | N шт |
| Кабель UTP 5e | M м | M м |

Внимание! На момент настройки требуется соблюдать следующую политику паролей:

|  |  |  |
| --- | --- | --- |
| Узел сети | Имя | Пароль |
| Все локальные администраторы Windows | LocalAdmin | P@ssw0rd\_XX |
| Все локальные администраторы Windows | DomainAdmin | P@ssw0rd\_XX |
| Администратор Linux | root | P@ssw0rd\_XX |
| Привилегированный доступ на маршрутизатор | - | urtc\_XX |
| Привилегированный доступ на коммутатор | - | cisco\_XX |
| Использование любых других пользователей и паролей, явно неопределенных в задании, является ошибкой! | | |

***Задачи филиала в городе Корусант:***

1. Осуществите подключение сетевого оборудования, PC1 и сервера согласно схеме. Использование интерфейсов отличных от предложенных в схеме считается ошибкой.
2. На PC1 разверните ОС Windows 8.1. Установите недостающие драйвера на оборудование (в том числе и на монитор). Использование стандартных драйверов или WDDM драйверов считается ошибкой.
3. Пока идет установка ОС, как истинные приверженцы силы соберите фигурку Йоды.
4. Восстановите доступ до активного сетевого оборудования.
5. Задайте имена в соответствии с топологией.
6. Обновите прошивку коммутатора SW2 Cisco WS-C2960-24TC-L на прошивку с флешки
7. Настройте баннер MOTD: URALOLIMP\_2015\_XX.
8. На коммутаторах SW1 и SW2 создайте виртуальные локальные сети в соответствии с таблицей:

|  |  |  |
| --- | --- | --- |
| №VLAN | Имя VLAN | Примечание |
| 1 | default | не используется |
| 100 | Internet | Для сети Интернет |
| 101 | Quagga | Для Quagga |
| 102 | Wi-Fi | Для Wi-Fi |
| 103 | Video | Для Video |
| 104 | VoIP | Для VoIP |
| 105 | AD | Для AD |
| 106 | DMZ | Для DMZ |
| 107 | NAP | Для NAP |
| 200 | ASA | Для ASA |
| 300 | Manage | Для управления |

1. На коммутаторах настройте объявление о VLAN по протоколу VTP (SW2 – Сервер, SW1 – клиент).
2. Настройте на коммутаторах агрегированные каналы согласно таблице:

|  |  |  |  |
| --- | --- | --- | --- |
| Оборудование | Порт | Имя | Протокол |
| SW1-SW2 | Fa0/7, Fa0/8 | Po1 | LACP (Активный SW1) |
| SW1-SW2 | Fa0/9, Fa0/10 | Po2 | PAGP(Активный SW2) |
| SW1-SW2 | Fa0/11, Fa0/12 | Po3 | Static |

Используйте инкапсуляцию IEEE 802.1Q. Максимально ограничьте перечень VLAN, трафик которых разрешен для передачи через транковый интерфейс.

1. На коммутаторах используйте версию протокола остовного дерева, основанную на стандарте IEEE 802.1w. SW1 должен быть корнем STP-дерева во всех VLAN, кроме VLAN 107 и VLAN 300.
2. Настройте порты доступа коммутаторов таким образом, чтобы они сразу же переходили в режим пересылки.
3. Настройте на всех устройствах и виртуальных машинах синхронизацию времени с NTP-сервером (в роли NTP-сервера выступает R1). Установите часовой пояс Екатеринбурга.
4. Настройте на R1 DHCP сервер, который обеспечит раздачу сетевых реквизитов во все VLAN.
5. На межсетевом экране выполните действия:
   1. Задайте виртуальные локальные сети в соответствии с таблицей:

|  |  |  |
| --- | --- | --- |
| №VLAN | Имя VLAN | Security Level |
| 100 | WAN | 10 |
| 200 | LAN | 90 |
| 600 | DMZ | 50 |

* 1. Настройте центр сертификации для организации защищенных соединений

1. На участке R1-R2 настройте IPSec over GRE-RSA с шифрованием 3DES.
2. PC1 после начального конфигурирования должен располагаться во внешней сети (сеть УРТК). На участке PC1-ASA необходимо организовать L2TP/IPSec PSK.
3. Необходимо развернуть сервер виртуализации с операционной системой (ОС) Windows Server 2012 R2 Standard и ролью Hyper-V. Сервер виртуализации (хост) должен иметь имя ***VM Host***. Ключ установки написан на аудиторной доске.
4. На VM Host:
   1. Настройте виртуальные коммутаторы в соответствии со схемой
   2. Установите виртуальные машины с настройкой системных требований в соответствии с таблицей

|  |  |  |  |
| --- | --- | --- | --- |
| Имя | ОС | Системные требования | Примечание |
| ServDC | Windows Server 2012 R2 | Одно ядро, 2 ГБ ОЗУ, 40 ГБ НЖМД |  |
| ServDDC | Windows Server 2012 R2 | Одно ядро, 2 ГБ ОЗУ, 40 ГБ НЖМД | Недопустимо использование GUI |
| ServOSPF | Debian 7 | Одно ядро, 512 МБ ОЗУ, 20 ГБ НЖМД | Недопустимо использование GUI |
| ServIIS | Windows Server 2012 R2 | Одно ядро, 2 ГБ ОЗУ, 40 ГБ НЖМД |  |
| ServRADIUS | Debian 7 | Одно ядро, 512 МБ ОЗУ, 20 ГБ НЖМД | Недопустимо использование GUI |
| ServVideo | Windows Server 2012 R2 | Одно ядро, 2 ГБ ОЗУ, 40 ГБ НЖМД для системы, RAID5 из дисков емкостью по 40 ГБ для хранения видео |  |
| ServFTP | Debian 7 | Одно ядро, 512 МБ ОЗУ, 30 ГБ НЖМД для системы, RAID5 из дисков емкостью по 40 ГБ для хранения видео | Недопустимо использование GUI |
| ServNAP | Windows Server 2012 R2 | Одно ядро, 2 ГБ ОЗУ, 40 ГБ НЖМД |  |

1. Настройте протокол динамической маршрутизации OSPF. Филиал в городе Корусант Area1, кроме ServIIS, филиал в городе Мос-Эйсли Area2, а ServIIS располагается Area3 для подсетей всех VLAN. На всех маршрутизаторах настройте аутентификацию для протокола OSPF с ключом ospfauth. Ключ должен передаваться в виде хеша. Area0 является магистральной зоной.
2. Настройка ServDС (основной контроллер домена), ServDDC (резервный контроллер домена):
   1. Настройки Контроллера домена. Имя домена - urtc\_XX.rus. Все PC с операционной системой Windows и все виртуальные машины с операционной системой Windows входят в домен.
   2. В развернутом Вами домене, создайте пользователей и группы в соответствии со следующей таблицей:

|  |  |  |  |
| --- | --- | --- | --- |
| Группа пользователей | Тип группы | Количество членов группы | Полное имя пользователей группы |
| Контрабандисты | Глобальная | 2 | Джабба Хатт  Джанго Фетт |
| Millennium Falcon | Глобальная | 2 | Хан Соло  Чубакка |
| Республика | Глобальная | 2 | Лея Органа  Мейс Винду |

* 1. Расписание входа в систему

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Полное имя пользователя | Имя пользователя для входа в систему | Членство в группах | Когда пользователю разрешен вход в систему | С каких компьютеров пользователю разрешен вход в систему |
| Лея Органа | Organa\_L | Domain Admins, Respublica | В любое время | Все компьютеры домена |
| Хан Соло | Solo\_H | Domain Users, Millennium Falcon | В любое время | Все компьютеры, кроме контроллера домена |
| Чубакка | Chubakka | Domain Users, Millennium Falcon | Рабочие дни  7.00 – 21.00  Запрет – воскресенье | PC1 |
| Мейс Винду | Windu\_M | Domain Users, Respublica | Рабочие дни  7.00 – 21.00  Запрет – воскресенье | PC2 |
| Джанго Фетт | Fett\_D | Domain Users, Kontr | Рабочие дни  7.00 – 18.00  Запрет – суббота, воскресенье | PC1 |
| Джабба Хатт | Hatt\_D | Domain Users, Kontr | Рабочие дни  7.00 – 18.00  Запрет – суббота, воскресенье | PC2 |

* 1. Планирование паролей

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Имя входа пользователя | Пользователь должен сменить пароль при следующем входе в систему | Возможность изменять свой пароль | Срок действия пароля | Пароль |
| Organa\_L | Нет | Да | Не ограничен | P@ssw0rd |
| Solo\_H | Нет | Да | 60 дней | P@ssw0rd |
| Chubakka | Да | Да | 30 дней | содержит не менее 6 символов, букв, спец. символов и цифр |
| Windu\_M | Да | Да | 30 дней |
| Fett\_D | Да | Да | 30 дней |
| Hatt\_D\_ | Да | Да | 30 дней |

Укажите путь до политики, ограничивающий срок действия паролей

|  |
| --- |
|  |
|  |
|  |
|  |

Укажите путь до политики, ограничивающей длину и состав пароля

|  |
| --- |
|  |
|  |
|  |
|  |

* 1. Задайте политику на уровне всего домена, выполняющую блокировку учетных записей на 5 минут в том случае, если подряд было сделано не менее трех ошибок входа в систему.

Укажите путь до политики

|  |
| --- |
|  |
|  |
|  |
|  |

* 1. Создайте организационное подразделение Picture. Поместите в организационное подразделение учетную запись сотрудников Windu\_M, Fett\_D, Hatt\_D. Задайте политику на уровне организационного подразделения, запрещающую менять картинку рабочего стола и загружающую общую для всех картинку с номером Вашей команды и логотипом учебного заведения.

Укажите путь до политики

|  |
| --- |
|  |
|  |
|  |
|  |

1. Необходимо развернуть ServVideo, представляющий собой программный квадратер Macroscope, с использованием аппаратного ключа. Проброс аппаратного ключа в виртуальную машину мы рекомендуем осуществить средствами USB over Network (<http://www.fabulatech.com/usb-over-network-download.html>), в триальном режиме. Дистрибутив USB over Network и файл лицензии Macroscop на флешке. Необходимо настроить:
   1. Запись только по движению с максимальным разрешением и 10 кадрами в секунду. Ролики по 10 минут. Возможность просмотра видеопотока непривилегированному пользователю (пользователь security, пароль urtk\_XX)
   2. Обеспечить запись на локальный диск. Укажите используемые настройки:

|  |
| --- |
|  |
|  |
|  |
|  |

* 1. Необходимо на ServVideo настроить систему резервного копирования. Средства резервного копирования выбираются участником самостоятельно. Архивируется только видеоданные: первая копия полная, затем делаются копии только изменившихся данных каждый час. Копии именуются: <XX\_Дата\_Время>. Все резервные копии записываются на ServFTP. Укажите выбранный инструмент и используемые настройки

|  |
| --- |
|  |
|  |
|  |
|  |

1. Необходимо развернуть ServFTP. Выбор FTP сервера возлагается на участника. Доступ на чтение для пользователя read\_XX пароль XX, доступ на запись без права на удаление write пароль XX. Укажите выбранное ПО

|  |
| --- |
|  |
|  |
|  |
|  |

1. ServNAP должен обеспечивать проверку обновлений ОС и наличия антивирусных средств и антивирусных баз на компьютерах под управлением ОС Windows и для мобильных устройств.
2. В разворачиваемой сети должна быть обеспечена антивирусная защита средствами ESET NOD32 Antivirus Business Edition (смотри Приложение 1, файл лицензии на флешке). Необходимо обеспечить своевременное обновление антивирусных средств, централизованное управление и сбор статистики. Компоненты антивируса должны быть установлены в соответствии с таблицей:

|  |  |
| --- | --- |
| Узел сети | Компоненты антивируса |
| PC1 | Клиентская часть, средства администрирования |
| PC2 | Клиентская часть |
| ServDC | Клиентская часть |
| ServDDC | Клиентская часть |
| ServIIS | Клиентская часть |
| ServFTP | Клиентская часть |
| ServNAP | Сервер мониторинга и обновлений |

1. На ServIIS необходимо развернуть WEB сервер, работающий только по протоколу HTTPS. Доступ до сайта возможен только по сертификатам. Сертификаты должны быть интегрированы в браузер PC1 и PC2. Сайт должен состоять из одной страницы с логотипом учебной организации.

Укажите, чем были сгенерированы сертификаты:

|  |
| --- |
|  |
|  |
|  |
|  |

Укажите браузер, в который интегрированы сертификаты:

|  |
| --- |
|  |
|  |
|  |
|  |

1. ServOSPF должен представлять собой программный маршрутизатор. Маршрутизация должна обеспечиваться пакетом Quagga.

Укажите путь до настроек:

|  |
| --- |
|  |
|  |
|  |
|  |

1. ServRADIUS должен быть реализован посредством пакета FreeRADIUS и обеспечивать модель AAA на всех сетевых устройствах.
2. На PC1 установите IP Communicator, подключите и настройте гарнитуру. IP Communicator должен получать настройки с Call Manager Express (R2). Должна быть обеспечена телефонная связь с филиалом в городе Мос-Эйсли.

***Задачи филиала в городе Мос-Эйсли:***

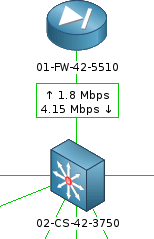
1. Осуществите сборку PC2 из предоставленных компонентов. Левую стенку не закручивать на болты.
2. Осуществите подключение сетевого оборудования, PC2 и WEB Host согласно схеме. Использование интерфейсов отличных от предложенных в схеме считается ошибкой.
3. На PC2 разверните ОС Windows 8.1. Установите недостающие драйвера на оборудование (в том числе и на монитор). Использование стандартных драйверов или WDDM драйверов считается ошибкой.
4. Пока идет установка ОС, как истинные приверженцы силы, соберите фигурку мастера Йоды.
5. На WEB Host разверните Debian 7.8. Установка графического интерфейса считается ошибкой.
6. Восстановите доступ до активного сетевого оборудования.
7. Задайте имена в соответствии с топологией.
8. Настройте баннер MOTD: URALOLIMP\_2015\_XX.
9. На коммутаторе SW3 создайте виртуальные локальные сети в соответствии с таблицей:

|  |  |  |
| --- | --- | --- |
| №VLAN | Имя VLAN | Примечание |
| 1 | default | не используется |
| 100 | Internet | Для сети Интернет |
| 101 | Quagga | Для Quagga |
| 102 | Wi-Fi | Для Wi-Fi |
| 103 | Video | Для Video |
| 104 | VoIP | Для VoIP |
| 105 | AD | Для AD |
| 106 | DMZ | Для DMZ |
| 107 | NAP | Для NAP |
| 200 | ASA | Для ASA |
| 300 | Manage | Для управления |

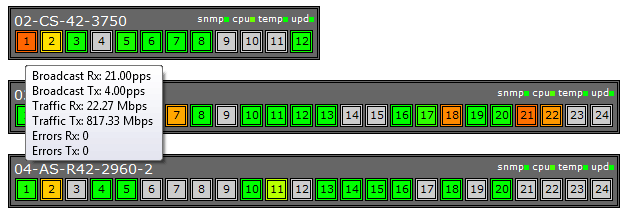
1. На коммутаторах используйте версию протокола остовного дерева, основанную на стандарте IEEE 802.1w.
2. Настройте порты доступа коммутатора таким образом, чтобы они сразу же переходили в режим пересылки.
3. Настройте на всех устройствах и виртуальных машинах синхронизацию времени с NTP-сервером (в роли NTP-сервера выступает R1). Установите часовой пояс Екатеринбурга.
4. Подготовьте WEB Host для размещения его в DMZ
5. На участке R1-R2 настройте IPSec over GRE-RSA с шифрованием 3DES.
6. На маршрутизаторе R2 настройте Call Manager Express. Телефония должна работать по протоколу SCCP. Настройте максимальное количество имен каталога и телефонов равное 2. Запрещено использовать автоматическую регистрацию телефонов. Присвойте телефону VoIP1 DN1 с номером XX1, VoIP2 DN2 с номером XX2. В качестве рисунка приветствия телефона должен использоваться логотип учебной организации (псевдографика), а в качестве звонка должна быть использована мелодия «Имперский Марш» (файл на флешке)
7. Для IP\_Cam, VoIP1 и AP настройте PoE на коммутаторе
8. AP должна работать в автономном режиме и получать настройки с ServRADIUS. Точка должна работать только по стандарту IEEE 802.11n. Канал должен соответствовать номеру команды.
9. Подготовьте IP\_Cam для передачи видео на ServVideo
10. На WEB Host необходимо развернуть сервер Zabbix. Сервер должен обеспечивать мониторинг состояния устройств в соответствии с таблицей:

|  |  |
| --- | --- |
| Узел сети | Мониторинг параметра |
| PC1 | Загрузка оперативной памяти |
| PC2 | Загрузка процессора |
| WEB Host | Загрузка процессора |
| VM Host | Загрузка процессора, Загрузка оперативной памяти, объем дискового пространства |
| SW1 | Загрузка процессора, Загрузка оперативной памяти, Нагрузка на активные интерфейсы |
| SW2 | Загрузка процессора, Загрузка оперативной памяти, Нагрузка на активные интерфейсы |
| SW3 | Загрузка процессора, Загрузка оперативной памяти, Нагрузка на активные интерфейсы |
| R1 | Загрузка процессора, Загрузка оперативной памяти, Нагрузка на активные интерфейсы |
| R2 | Загрузка процессора, Загрузка оперативной памяти, Нагрузка на активные интерфейсы |
| ASA | Загрузка процессора, Загрузка оперативной памяти, Нагрузка на активные интерфейсы |

Постройте карту сети (либо L1, либо L2), с указанием скоростей соединений. Пример на рисунке:



1. Настройте мониторинг состояния портов SW1, SW2, SW3.



Серый цвет порта обозначает, то, что он находится в down. Цвет от зеленого до красного меняется в зависимости от загрузки порта. Гигабитные порты выделены рамочкой.

1. Настройка нагрузки:
   1. На PC2 установите серверную часть iperf и обеспечьте её автоматический запуск в фоновом режиме после старта системы. На ServFTP установите клиентскую часть iperf и обеспечьте её автоматический запуск в фоновом режиме после старта системы с подключением к серверу. Обеспечьте непрерывную передачу трафика с максимальной нагрузкой на канал. Запрещается менять имя iperf в исполняемом файле.

Укажите путь до настроек сервера и клиента

|  |
| --- |
|  |
|  |
|  |
|  |

* 1. На WEB Host установите серверную часть iperf3 и обеспечьте её автоматический запуск в фоновом режиме после старта системы. На ServIIS установите клиентскую часть iperf3 и обеспечьте её автоматический запуск в фоновом режиме после старта системы с подключением к серверу. Обеспечьте непрерывную передачу трафика с максимальной нагрузкой на канал. Запрещается менять имя iperf3 в исполняемом файле.

Укажите путь до настроек сервера и клиента:

|  |
| --- |
|  |
|  |
|  |
|  |

* 1. Обеспечьте непрерывную передачу трафика между серверными и клиентскими частями iperf, iperf3 для набора статистики Zabbix и нагрузки на коммутаторы. Скриншот статистики за 5 и 15 минут работы сохраните на рабочий стол

Приложение 1

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | [ESET NOD32](http://www.esetnod32.ru/) |  | | |
|  | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **Уважаемый клиент!**  Благодарим Вас за интерес к комплексному решению **ESET NOD32 Antivirus Business Edition**.  **Внимание!** [Ознакомьтесь с изменениями в лицензировании и активации продуктов ESET](http://www.esetnod32.ru/business/licensing/).   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  |  | | --- | --- | |  | | | **Лицензионные данные для активации продуктов:** | | | Лицензионный ключ: **BFR9-X8G5-3PBB-M9SS-H7MG** Публичный ключ лицензии: **33C-CCH-GKB** Наименование компании: **УРТК** | | |  | | |  | | | A: Endpoint Products Family | **Защита рабочих станций, мобильных устройств и файловых серверов**  Вы можете использовать следующие продукты:  ESET Endpoint Antivirus для Microsoft Windows  ESET Endpoint Antivirus для Mac OS X  ESET NOD32 Antivirus Business Edition для Linux Desktop  ESET Endpoint Security для Android  ESET Mobile Security Business Edition для Microsoft Windows Mobile/Symbian  ESET File Security для Microsoft Windows Server  ESET File Security для Microsoft Windows Server Core  ESET File Security для Linux/BSD/Solaris  ESET Remote Administrator  **Имя пользователя (логин):** **EAV-0135514850**  **Пароль:** **d9n3xsfufd**  **Количество пользователей:** **15**  **Дата окончания действия лицензии:** **24/06/15** | |  | Срок действия лицензии указан в формате день/месяц/год. Лицензионный файл **ERA-Endpoint.lic** необходим для активации централизованного управления продуктами через ESET Remote Administrator. | |  | | |  |   Скачать дистрибутивы антивирусных продуктов ESET можно на официальном сайте в разделе «[Скачать – Для бизнеса](http://www.esetnod32.ru/download/business/commercial/)», а документация к продуктам размещена в разделе «[Скачать – Документация – Для корпоративных пользователей](http://www.esetnod32.ru/download/manuals/business/)».  **Конфиденциальность**  Сохраняйте конфиденциальность лицензионных данных! Если они попадут в руки третьих лиц, это может привести к деактивации лицензии. | | |