Тестовый проект

АДМИНИСТРИРОВАНИЕ СЕТЕВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Разработчик:
Ильющенко Сергей Леонидович

Основной текст тестового проекта для конкурсанта:

Вы являетесь сотрудником одной из компаний “Новый Готхэм”, предоставляющую услуги по проектированию сетевых инфраструктур для различного рода заказчиков, интеграторскую деятельность и доступ в сеть Интернет. Менеджер вашей компании сообщил вам о том, что поступил новый заказ на проектирование сетевой инфраструктуры и по решению руководителя проектами его реализация легло полностью на Вас. Окинув взором требования Вы решили собрать и смоделировать данный проект у себя в тестовой лаборатории, но для полной реализации поставленных задач в лаборатории не нашлось нужного кол-ва сетевого и серверного оборудования. Поразмышляв, вы набросали физическую и логическую схему, которая в полной мере отражает все необходимые для реализации и проверки компоненты проекта (Рисунок 1 и Рисунок 2).

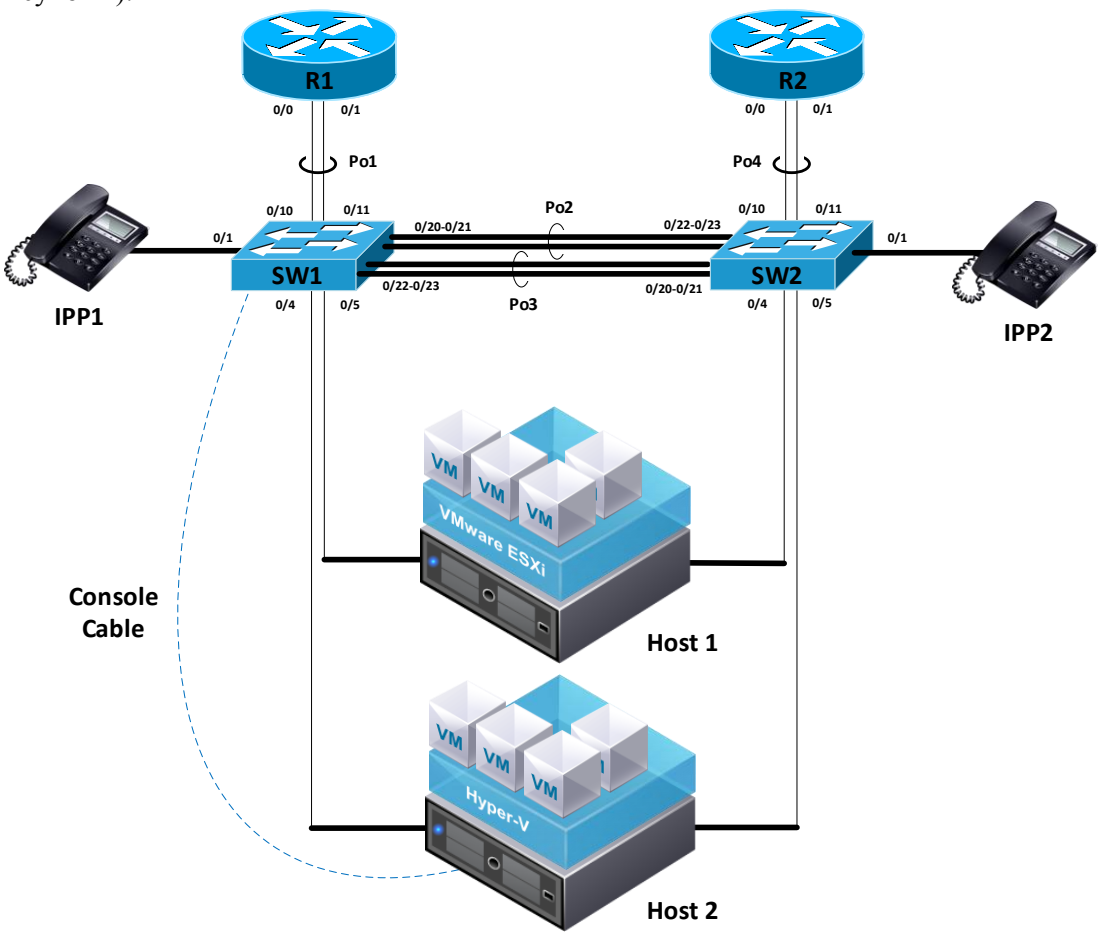

Рисунок 1 – Физическая топология тестового стенда.

Описание тестового стенда:

В схему входит два физических маршрутизатора (R1 и R2), два коммутатора (SW1 и SW2), два IP-телефона (IPP1 и IPP2), два сервера с функцией виртуализации (Host1 и Host2), один на базе продуктов Microsoft, другой на базе продуктов VMware. Такая необходимость обусловлена неопределенностью заказчика в выборе гипервизора в качестве основного для виртуализации центра обработки данных.

Связь между сетевым оборудованием обеспечивается по агрегированным каналам, согласно рисунку. Создание агрегированных каналов позволит избежать проблем, связанных с пропускной способностью каналов и возникновению узких мест между сетевым оборудованием в физической сети заказчика. Два отдельных агрегированных каналов между коммутаторами (SW1 и SW2) обусловлена логической схемой проектируемой сети заказчика.

На узел виртуализации Host 2 предустановлена операционная система Microsoft Windows Server 2012 R2 и все необходимые программные компоненты для управления сетевым оборудованием (Putty) и узлом виртуализации Host1 (VMware vSphere Client). Весь доступ к консолям сетевых устройств осуществляется через переходник USB-COM (или USB-miniUSB) с узла Host 2.

На узел виртуализации Host1 в качестве операционной системы предустановлен гипервизор VMware ESXi.

Задание I:

1. Соберите физический стенд согласно рисунку.
2. Задайте имена устройствам.
3. Установите пароль на привилегированный режим **CiscoEnaPa**. Пароль должен храниться в зашифрованном виде. Используйте более криптостойкий алгоритм, где это возможно.
4. Настройте систему AAA для доступа по консоли и протоколу SSH используя отдельные локальные базы данных пользователей на сетевых устройствах. Заведите двух пользователей: Admin (**AdminPa**), View (**ViewPa**). Все пароли должны храниться в зашифрованном виде.
5. Настройте агрегированные L2-каналы связи между сетевыми устройствами. Идентификаторы агрегированных каналов используйте согласно рисунку 1. Все агрегированные каналы должны работать в режиме trunk по протоколу 802.1q. Канал Po2 должен согласовываться по протоколу LACP, а Po3 по PAgP. Все агрегированные каналы должны иметь соответствующее описание.
6. На устройствах настройте протокол удаленного доступа SSH (Telnet так же разрешен за меньшее кол-во балов). В качестве интерфейса удаленного доступа для коммутаторов SW1 и SW2 используйте SVI интерфейс с идентификатором MNGM VLAN согласно таблице 1. На маршрутизаторах настройте соответствующий интерфейс для удаленного управления. Адресацию для данных интерфейсов используйте согласно таблице 1. Проверьте удаленный доступ к устройствам. Удаленный доступ должен происходить только из сети MGMT VLAN.
7. Установите актуальное время на маршрутизаторе R1 и используйте его в качестве источника времени для других сетевых устройств.
8. Порты коммутатора, к которым подключаются IP-телефоны, должны относится к сетям согласно логической топологии (Рисунок 2). Включите поддержку голосового VLAN Voice1 для коммутатора SW1 и Voice2 для коммутатора SW2 с идентификаторами согласно таблице 1. Телефоны должны получать питание через PoE. (Через блок питания за меньшее кол-во балов);
9. Установите имя компьютера Host 2 – Datacenter-2
10. Настройте узел Host 2 для поддержки виртуализации.
11. Настройте сетевые интерфейсы серверов и порты коммутаторов для работы виртуальных машин. Сами физические сервера должен относится к MGMT VLAN через интерфейс, смотрящий в сторону SW1.
12. Установите имя компьютера Host1 - Datacenter-1
13. Настройте Host1, таким образом, чтобы получить доступ через предустановленный на Host2 VMware vSphere Client к консоли управления ESXi.
14. На серверах подготовьте из шаблона необходимые виртуальные машины согласно логической схемы (Рисунок 2). Сами шаблоны хранятся в корне диска в папке VM_Template.
15. Настройте виртуальные коммутаторы на узлах виртуализации и обеспечьте доступ VM к необходимым сетям согласно логической топологии (Рисунок 2). Идентификаторы VLAN представлены в таблице 1.
16. На коммутаторах создайте VLAN согласно логической топологии. Настройте имена виртуальным локальным сетям согласно таблицы 1.
17. Через агрегированные каналы Po2 разрешите только те VLAN, которые маршрутизируются маршрутизатором R1, а Po2 – R2 соответственно. MGMT VLAN разрешен как на одном, так и на втором Po.
18. Настройте протокол STP таким образом, чтобы SW1 был основным корневым для виртуальных локальных сетей, которые маршрутизируются на R1, а SW2 резервным. Для виртуальных локальных сетей, маршрутизируемых на R2, наоборот соответственно. Для MGMT VLAN - SW1 является корневым.
19. Обеспечьте маршрутизацию VLAN, согласно рисунку, на маршрутизаторах R1 и R2. Адресацию для интерфейсов рассчитайте исходя из требований, представленных в таблице 1.

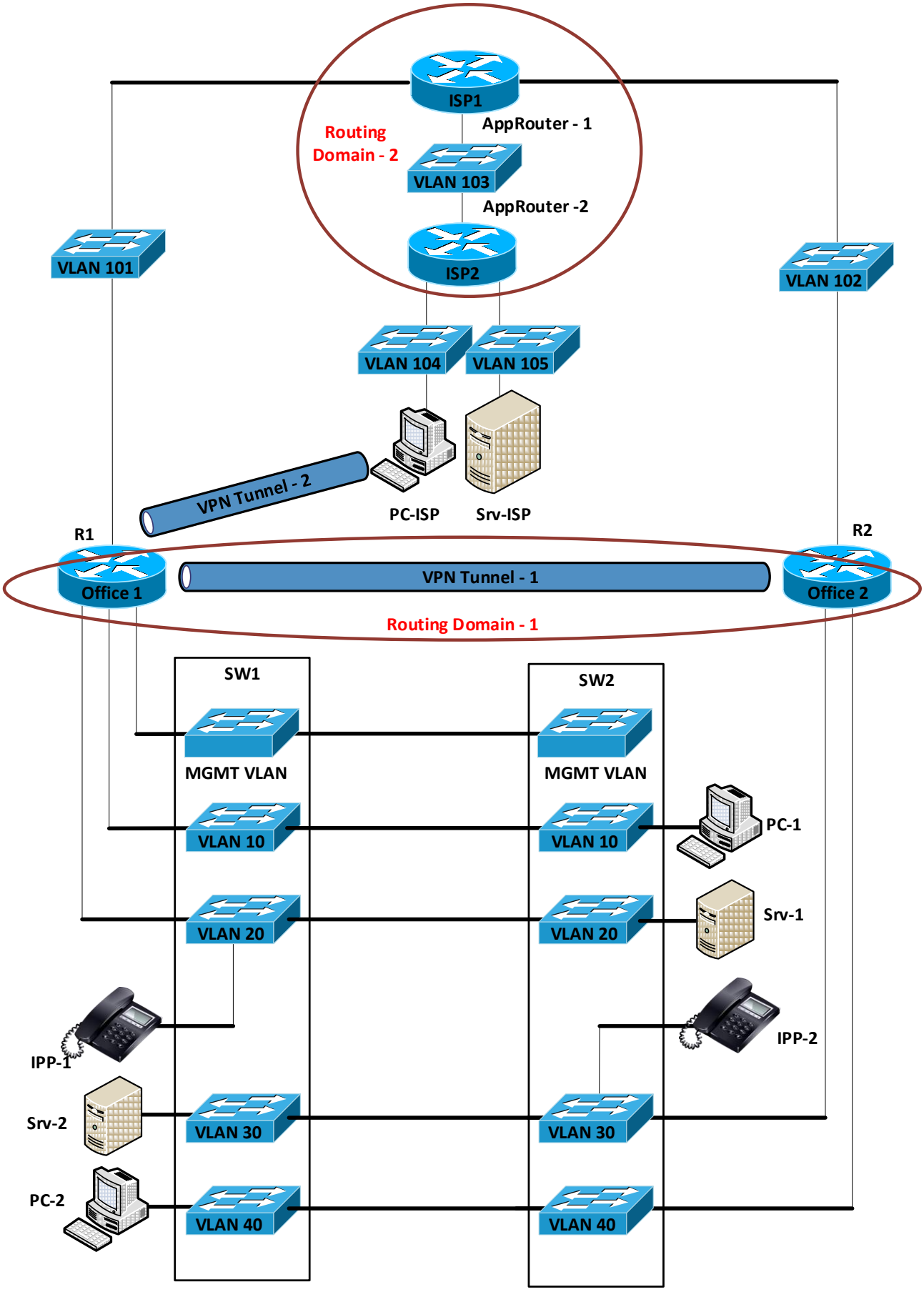

Рисунок 2 – Логическая топология реализуемого проекта на физическом стенде.

Описание логической схемы:

Заказчик имеет два территориально разнесённых офиса (Office 1 и Office 2). В каждом офисе имеется коммутируемая инфраструктура, смоделированная физическими коммутаторами SW1 и SW2 на вашем лабораторном стенде, согласно логической топологии (Рисунок 2). Вся маршрутизация между отделами выполняется физическими маршрутизаторами. Офисы соединены между собой VPN каналом. Маршрутизатор R1 выступает в качестве концентратора для site-to-site и remote-access VPN.

Доступ в Интернет смоделирован посредством физических маршрутизаторов R1 и R2. Поставщик услуг Интернета промоделирован в виде виртуальных машин на одном из физических серверов посредством технологии виртуализации. Виртуальные машины имеют имена согласно топологии: AppRouter-1, AppRouter-2, PCISP и SrvISP.

<u>Задание II</u>:

1. На физических узлах Host1 и Host2, включите виртуальные машины. Проведите дополнительные настройки для виртуальных машин для обеспечения связности согласно логической схемы. Назначьте IP адреса на интерфейсы согласно таблице 2 из соответствующих диапазонов таблицы 1.
2. Промоделируйте сеть провайдера услуг Интернет, установив службу маршрутизации на соответствующе виртуальные машины (AppRouter-1 и AppRouter-2). Используйте адресацию, исходя из таблицы 1 и 2.
3. Подымите сервис DHCP на виртуальных машинах и маршрутизаторах, настройте на них соответствующие диапазоны адресов по следующему принципу: Srv1 обслуживает сеть PC-1; Srv2 – PC2; SrvISP – PCISP; R1 - IPP1; R2 – IPP2. Сделайте все необходимое, чтобы клиенты и телефоны получали IP-адреса из соответствующих сетей через протокол DHCP.
4. Настройте маршрутизацию в сети провайдера (Routing Domain-2) согласно таблице 3.
5. На виртуальной машине SrvISP установите службу CA. Данный сервер будет выполнять роль автономного корневого центра сертификации. Сгенерируйте корневой сертификат. Хранение сертификатов организуйте в папке /ca_certs. Используйте ключ 2048 бит.
6. Запустите на виртуальной машине SrvISP службу FTP. Опубликуйте папку с сертификатом корневого центра с анонимным доступом. Скопируете сертификат на все виртуальные машины, через службу FTP. Установите данный сертификат на все виртуальные машины в качестве доверенного корневого центра сертификации (приемлем любой метод передайте сертификат).
7. На виртуальной машине SrvISP запустите web сервис по протоколу HTTP. Выпишете данной службе сертификат безопасности и организуйте работу протокола HTTPS. Создайте простейшую Web-страничку с текстом “Web-Server-ISP Hello world!!”
8. Установите на SrvISP службу DNS и, согласно таблицы 5, создайте соответствующие записи.
9. На ISP2 с помощью iptables запретите доступ к любым сервисам кроме тех, которые подняты на данном сервере. Сам сервер не должен иметь доступ ни к одному сервису извне (включая ICMP). Правила должны сохраняться после перезапуска ISP2.
10. Используя Web-обозреватель на компьютере PCISP проверьте работоспособность Web-веб сервера.
11. Настройте NAT на маршрутизаторах и обеспечьте выход клиентов внутри моделируемых филиалов компании к серверу SrvISP. Разрешите проходить функцию NAT только клиентским компьютерам.
12. Подымите VPN туннель между маршрутизаторами R1 и R2 по протоколу согласно таблице 4. Настройте маршрутизацию (Routing Domain-1) согласно таблице 2. Сделайте все необходимое для обеспечения полной связности между офисами моделируемого предприятия.
13. На виртуальной машине Srv1 установите роль контроллера домена. Уровень леса и домена должен быть не ниже, чем Server 2008. Именование компьютеров в домене идет в пределах зоны office1.local. Все зоны DNS должны быть интегрированы со службой AD.
14. Присвойте учетной записи администратора предприятия следующий пароль **Pa$$word.** Любыми средствами заведите в домене 60 пользователей с именами UserX, где X-эта номер по порядку. Создайте группу Office_user к которой должны относится все созданные пользователи.
15. Все оконечные станции, работающие под управлением ОС Windows в пределах организации, введите в домен. Именование станций должно соответствовать именованию на логической схеме.
16. Создайте несколько организационных единиц (OU) с именами: “Office_User”; “Office_Comp”; “Office_Group”. Эти OU должны находиться внутри еще одной созданной OU “Office_Main”. Распределите соответствующие объекты, созданные вами, по соответствующим OU.

17. Создайте групповую политику (GPO) с именем Office_GPO_Main и присвойте область действия в пределах OU “Office_Main”. Создайте внутри OU “Office_User” несколько OU с именами Staff-1, Staff-2 и Staff-3. Создайте для них отдельные GPO с соответствующими имена. Распределите пользователей поровну между OU Staff-1, Staff-2 и Staff-3.
18. В GPO для пользователей отдела Staff-2 настройте разрешение на конфигурацию времени и параметров рабочего стола. Для всех остальных запретите изменять параметры рабочего стола.
19. Запустите сервис VoIP через CME и обеспечьте регистрацию телефонов на маршрутизаторах R1для Office1 и R2 для Office2. Организуйте связь CME между собой. Для телефонов назначьте следующие номера: IPP1 – 101, IPP2 - 201. Сделайте все необходимое, чтобы телефоны могли связаться между собой. Установите на компьютеры PC1, PC2 программный клиент для службы VoIP. Назначьте им номер 102 и 202 соответственно. Обеспечьте связь между всеми клиентами сервиса VoIP.
20. Присоедините к PC2 два диск по 10 Гб. Поместите оба диска в одну группу томов (volume group) LVM. На данной группе создайте логический том (logical volume) объемом 15 Гб и отформатируйте его в ext4. Полученный том смонтируйте в каталог /mnt/data".
21. На PC2 установите графическую оболочку.
22. На сервере Srv2 запустите Web-службу. Создайте страницу, на которой продемонстрируйте работоспособность модуля PHP. Веб-сайт должен работать по протоколу https с сертификатом, подписанным SrvISP (самоподписанный сертификат за меньшее количество баллов, без сертификата – минимум баллов).
23. На сервере Srv2 установите сервис FTP. Настройте аутентификацию через Active Directory. Настройте соединение по протоколу ftps. В качестве корневого каталога используйте /rdmas/ftp_root. Создайте папку admin внутри данного каталога. Разрешите пользователю User1 чтение и запись файлов в данном каталоге. Пользователям User2 и User3 разрешите только чтение файлов из данного каталога. Для всех остальных пользователей запретите доступ к данному каталогу.
24. Опубликуйте сервисы web и ftp через службу NAT для интернет на соответствующим устройстве, который ближе всего находиться к публикуемому серверу. Используйте для служб IP адреса согласно таблице 5.
25. На сервере Srv2 установите сервис samba. В качестве домашнего каталога используйте /rdmas/smb_share. Настроить авторизацию через AD (User10-User15) (локальная авторизация за меньшее кол-во баллов). Для каждого пользователя создать отдельную папку с именем FolUserX, где X – номер пользователя. Каждый пользователь должен иметь привилегии RW для своей папки, и запрет доступа к чужим папкам. Создать папку public, каждый пользователь должен иметь привилегии RO для данной папки.
26. На сервере Srv2 установите службу DNS и, согласно таблицы 5, создайте соответствующие записи.
27. На серверах Srv1 и Srv2 должна осуществляться переадресация DNS-запросов на сервер SrvISP. Клиенты должны обращаться к своим DNS серверам.
28. Между серверами Srv1 и Srv2 необходимо настроить репликацию DNS-записей.
29. С компьютера PCISP установите соответствующего типа remote-access VPN (таблица 4) к маршрутизатору R1 и сделайте все необходимые настройки для доступа внутрь корпоративной среды. Должны быть доступны по протоколу ICMP все устройства, а также соответствующие сервисы и общие папки.

Таблица 1 – Исходные данные

<table>
<tr><th rowspan="2">VLAN ID</th><th rowspan="2">VLAN Name</th><th colspan="2">Subnet №</th><th rowspan="2">Кол-во адр. IPv4 (не менее)</th><th rowspan="2">Scope IPv4</th><th rowspan="2">Scope IPv6</th></tr>
<tr><th>IPv4</th><th>IPv6</th></tr>
<tr><td>5</td><td>MGMT</td><td>0</td><td>0</td><td>60</td><td>Использовать диапазон 192.168.0.0/26..</td><td rowspan="8">Разбить диапазон FC01::/48 на подсети используя nibble subnetting. В качестве шлюза по умолчанию использовать Link-local адрес FE80::1.</td></tr>
<tr><td>6</td><td>Voice1</td><td>0</td><td>1</td><td>30</td><td rowspan="2">Разбить диапазон 192.168.24.128/26 на подсети.</td></tr>
<tr><td>7</td><td>Voice2</td><td>1</td><td>4</td><td>30</td></tr>
<tr><td>10</td><td>LAN1</td><td>0</td><td>2</td><td>60</td><td rowspan="4">Разбить диапазон 192.168.24.0/25 на подсети используя VLSM.</td></tr>
<tr><td>20</td><td>SRV1</td><td>1</td><td>3</td><td>20</td></tr>
<tr><td>30</td><td>LAN2</td><td>2</td><td>5</td><td>10</td></tr>
<tr><td>40</td><td>SRV2</td><td>3</td><td>6</td><td>7</td></tr>
<tr><td>101</td><td>L1ISP1</td><td>0</td><td rowspan="2">-</td><td rowspan="2">5</td><td rowspan="2">Разбить диапазон 82.209.242.0/25 на подсети.</td><td rowspan="2">-</td></tr>
<tr><td>102</td><td>L2ISP1</td><td>1</td></tr>
</table>

103	L3ISP	2				
104	PCISP	5				
105	SrvISP	6				

Таблица 2 – Interfaces and IP addresses.

Device	Interface	IP Address	Note (IP Addresses scope)
Srv1	NIC	First	
PC1	NIC	DHCP	
Srv2	NIC	First	
PC2	NIC	DHCP	
IPP1	NIC	DHCP	
IPP2	NIC	DHCP	
PCISP	NIC	DHCP	
SrvISP	NIC	First	
ISP1	Link to R1	Last	
	Link to R2	First	
	Link to ISP2	First	
ISP2	Link to ISP1	Last	
	Link to PCISP	Last	
	Link to SrvISP	Last	
R1	Link to ISP1	First	
	Link to LAN1	Last	
	Link to SRV1	Last	
	Link to Voice1	Last	
	Link to MGMT VLAN	Last	
R2	Link to ISP1	Last	
	Link to LAN2	First	
	Link to SRV2	First	
	Link to Voice2	First	
SW1	MGMT SVI	First	
SW2	MGMT SVI	Second	

Таблица 3 – Type of routing.

Область	Routing IPv4	Routing IPv6
Routing Domain - 1	RIP	OSPF
Routing Domain - 2	OSPF	-

Таблица 4 – VPN.

Область	Protocol	Addressing IPv4	Addressing IPv6
VPN Tunnel - 1	GRE	192.168.1.0/24	-
VPN Tunnel - 2	AnyConnect	192.168.2.0/24	FC02:ABCD::/64

Таблица 5 – Domain names for DNS.

Domain name	IPv4 address	IPv6 address
DNS на SrvISP		
web.contora.com	82.209.242.2	-
ftp.contora.com	82.209.242.3	-
DNS Srv1		
Srv1.office1.local	Назначенный согласно заданию	Назначенный согласно заданию

ad.office1.local	Назначенный согласно заданию	Назначенный согласно заданию
DNS Srv2		
Srv2.office2.local	Назначенный согласно заданию	Назначенный согласно заданию
ftp.office2.local	Назначенный согласно заданию	Назначенный согласно заданию
Web.office2.loca	Назначенный согласно заданию	Назначенный согласно заданию

Таблица 6 – Программное обеспечение.

Оборудование	Операционная система	Сервисы
R1	Cisco IOS	CME DHCP Site-to-site VPN Remote VPN
R2	Cisco IOS	CME DHCP Site-to-site VPN
SW1	Cisco IOS	
SW2	Cisco IOS	
Srv1	Windows Server 2012R2 Datacenter	LDAP DHCP DNS
PC1	Windows 8.1	Telnet client SIP-client (Phonerlite)
Srv2	Ubuntu Server 14.04.4	DHCP DNS FTPS HTTPS SMB
PC2	Ubuntu Desktop 14.04.4	SSH-client SIP-client (Ekiga)
PCISP	Windows 8.1	
SrvISP	Windows Server 2012R2 Datacenter	DNS HTTPS FTPS CA DHCP
ISP1	Ubuntu Server 14.04.4	Routing
ISP2	Ubuntu Server 14.04.4	Routing Firewall

Таблица 7 – Пакеты ПО, службы и утилиты.

Службы	Windows	Linux
DHCP	Интегрированное	ISC DHCP
DNS	Интегрированное	Bind9
FTP	Интегрированное	ProFTPd
HTTP	IIS + PHP + MySQL	LAMP
LDAP	Интегрированное	OpenLDAP
SMB	Интегрированное	Samba
Firewall	Интегрированное	Интегрированное (IPtables)
Routing	Интегрированное	Quagga
CA	Интегрированное	OpenSSL

		NFS
		TFTP
		Syslog
		Radius