

ВВЕДЕНИЕ

Компьютерные сети давно стали неотъемлемой частью нашей жизни. Сети предоставляют пользователям широкий спектр возможностей для доступа к различной информации и коммуникации, а локальные сети позволяют совместно пользоваться общими устройствами и ресурсами.

Основными преимуществами локальных сетей являются возможность доступа к общим устройствам, например, к принтерам и сканерам, общим ресурсам, например, базы данных, вычислительные мощности, возможность корпоративной работы и обмена данными.

Локальные компьютерные сети были разработаны в 1960-х годах для использования в колледжах, университетах и исследовательских центрах, в первую очередь для соединения нескольких вычислительных машин. Широко применяться локальные сети стали после того, как была разработана и стандартизирована технология Ethernet. Возможность беспроводного соединения значительно расширила количество разных типов устройств, которые могут соединяться с локальной сетью. Типичные примеры мест, где используются такие сети: школы, заводы, предприятия, научные лаборатории.

Помимо многих преимуществ, локальные компьютерные сети имеют и проблемы, такие как проектирование и необходимость обслуживания. Непредвиденные ситуации могут вывести из строя оборудование, что приведёт к остановке работы организации и огромным убыткам. Также опасность представляет возможность хищения данных посредством компьютерной сети. Несмотря на это, локальные компьютерные сети получают всё большее распространение и всё глубже проникают во многие сферы деятельности человека.

В современном мире, использование компьютерных сетей является необходимостью в любой сфере деятельности для того, чтобы успешно конкурировать с другими организациями, действующими в этой области.

Целью данной курсовой работы является проектирование локальной компьютерной сети для организации, занимающейся торговлей овощами и фруктами.

Задачами курсовой работы являются:

- разработка логической топологии сети;
- выбор и настройка сетевого оборудования;
- проектирование физической топологии сети.

1. ОБЗОР ЛИТЕРАТУРЫ

Книга Эндрю Таненбаума «Компьютерные сети» [3] предоставила подробный разбор всех аспектов и уровней организации сетей.

На сайте производителя сетевого оборудования Allied Telesis [1] я ознакомился со списком актуальных моделей маршрутизаторов, коммутаторов и точек беспроводного доступа, подходящими для финансов, которые организация готова выделить на создание локальной сети, и с документацией, прилагающейся к оборудованию. Также на этом сайте доступны руководства по установке и настройке оборудования.

Из источника [2] мной была почёрпнута информация об управлении локальными сетями для малого и крупного бизнеса. Также я подробнее узнал о функциях, которые выполняют прокси-серверы, о том, как клиенты должны взаимодействовать с прокси, и о вариантах размещения прокси-сервера в сети.

На сайте [8] я ознакомился со списком наиболее популярных и актуальных прокси-серверов для Linux. Более подробную информацию об особенностях и настройке некоторых из этих серверов я узнал в источниках [9 – 11].

Источник [12] предоставил информацию о различиях между DVR и NVR видеорегистраторами. В источнике [7] содержится информация о подключении NVR-камер видеонаблюдения к локальной сети и особенностях их работы. Из источника [13] я узнал о том, как подключать DVR-видеорегистраторы к локальной сети и взаимодействовать с ними.

2. СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе будет рассмотрена структура локальной сети.

Чертёж структурной схемы СКС представлен в приложении А.

Для того, чтобы спроектировать структуру сети, нужно рассмотреть планировку здания, в котором располагается организация.

По заданию организация размещается в здании квадратной формы на трёх этажах: нулевой, первый и второй. Общая площадь помещений, занимаемых организацией, составляет 430 метров квадратных.

На нулевом этаже находится складское помещение и кабинет заведующего складом. В кабинете находятся две пользовательские станции и принтер. В складском помещении установлены две камеры видеонаблюдения, в коридоре – одна камера.

На первом этаже располагаются торговый зал, пост охраны и комната с сетевым оборудованием. Единственная пользовательская станция, находящаяся на этом этаже, располагается в комнате охранника. В комнате с сетевым оборудованием находится маршрутизатор, коммутатор, прокси-сервер, web-сервер, сетевой видеорегистратор. В торговом зале находятся три камеры видеонаблюдения.

На втором этаже находится кабинет отдела кадров, комната администратора сети, кабинет начальника организации и его приёмная, бухгалтерия, кабинет маркетолога. В кабинетах начальника организации, администратора сети, маркетолога, отделе кадров и приёмной находится по одной пользовательской станции. В бухгалтерии находятся 2 пользовательские станции. В коридоре этажа установлены две камеры видеонаблюдения.

На нулевом и втором этажах находится по одному коммутатору, к которым подключается оконечное оборудование этих этажей.

На первом этаже находится корневой коммутатор, к которому подключены коммутаторы нулевого и второго этажей, а также оконечное оборудование первого этажа.

В задании указано, что для обеспечения безопасности требуется использовать прокси. Это значит, что внутренняя сеть организации должна иметь доступ к сети Internet только через прокси-сервер. Прокси сервер находится между маршрутизатором и корневым коммутатором.

3. ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

В рамках данного проекта сеть предприятия будет разделена на 5 виртуальные сети:

1. Виртуальная сеть для стационарных подключений;
2. Виртуальная сеть для мобильных подключений;
3. Виртуальная сеть для администрирования;
4. Виртуальная сеть для web-сервера;
5. Виртуальная сеть для системы видеонаблюдения.

Связь маршрутизатора, коммутаторов, точки беспроводного доступа, web-сервера, принтера, компьютеров и компонентов системы видеонаблюдения будет произведена с помощью кабелей Ethernet.

Для соединения посредством Gigabit Ethernet будет использоваться стандарт 802.3ab 1000BASE-T, определяющий работу передачи данных по неэкранированной витой паре 5е категории.

Оптимальным стандартом для беспроводной сети будет IEEE 802.11n, который имеет значительные преимущества в максимальной скорости передачи данных (до 150 Мбит/с) по сравнению с стандартами 802.11a/g. Данный стандарт имеет обширную зону распространения радиоволн в 100 м. Также стандарт обеспечивает обратную совместимость с устройствами, работающими по стандартам 802.11a/b/g.

Данный раздел сопровождает чертеж схемы СКС функциональной (приложение «Б»).

3.1 Обоснование выбора пользовательской операционной системы.

В качестве операционной системы для пользовательских станций выбрана ОС Windows 10. На сегодняшний день, Windows 10 является самой популярной операционной системой и достаточно проста в использовании для обычного пользователя, поэтому большинству сотрудников будет удобнее и привычнее работать с этой операционной системой.

3.2 Обоснование выбора операционной системы серверов.

Для прокси-сервера и web-сервера была выбрана операционная система Debian, т.к. она потребляет меньше аппаратных ресурсов, чем современные Windows, и отлично подходит для использования на сервере.

В качестве web-сервера был выбран сервер Apache. Apache является популярным и проверенным web-сервером, а также обладает хорошей документацией.

По аналогичным причинам, для прокси-сервера был выбран Squid – популярное, производительное и хорошо задокументированное решение, обладающее всем необходимым организации функционалом.

3.3 Обоснование выбора пользовательских станций.

Так как организация, для которой разрабатывается сеть, занимается торговлей овощами и фруктами, и её сотрудники используют офисное программное обеспечение, которое не требует большого количества оперативной памяти, высокопроизводительных процессора и видеокарты, можно выделить следующие требования для пользовательских станций:

1. Шестиядерный процессор intel core i5 8400 является оптимальным выбором для офисного компьютера в бюджетном ценовом сегменте. Характеристики процессора хватает для производительной работы сотрудников организации;

2. 8 ГБ DDR4 оперативной памяти и накопителя HDD 1000 ГБ достаточно для комфортной работы сотрудников;

При изучении готовых сборок, представленных на рынке, была выбрана модель Jet Office 5i8400D8HD1VGALW50. Компьютер удовлетворяет всем вышеперечисленным условиям и имеет среднюю цену порядка 1200 рублей, что приемлемо для бюджетной организации.

Станция обладает следующими характеристиками:

- процессор intel core i5 8400;
- оперативная память DDR4 8 ГБ;
- накопитель HDD 1000 ГБ;
- графический адаптер Intel UHD Graphics 630.

3.4 Обоснование выбора web-сервера и прокси сервера

Требования организации к производительности web-сервера и прокси-сервера схожи, поэтому было решено использовать для них одинаковое аппаратное обеспечение.

Для сервера важно иметь ECC RAM, поэтому в первую очередь нужно выбрать процессор, поддерживающий работу с таким типом памяти. Популярными серверными процессорами с поддержкой ECC RAM являются процессоры Intel Xeon. Для целей организации подойдёт любой процессор из этой серии.

8 ГБ DDR4 оперативной памяти хватит для стабильной работы сервера при ожидаемых нагрузках. HDD накопителя на 1000 ГБ достаточно для хранения необходимых данных.

При сравнении готовых серверов, представленных на рынке, была выбрана модель Dell POWEREDGE T40.

Станция POWEREDGE T40 обладает следующими характеристиками:

- процессор Intel Xeon E-2224G;
- оперативная память DDR4 ECC 8 ГБ;

- накопитель HDD 1000 ГБ;
- графический адаптер Intel UHD Graphics P630.

3.5 Обоснование выбора чёрно-белого принтера А4

После исследования рынка принтеров выбор пал на Pantum P3010DW. Он имеет среднюю стоимость \$150. Pantum P3010DW является лазерным цветным принтером, печатающим формат А4, что отлично подходит для нужд нашей организации.

Для подключения принтер имеет порт Ethernet, что даёт возможность подключать принтер не к компьютеру, а к сети, предоставляя доступ для удалённого использования всем рабочим станциям внутри сети.

Также имеется возможность подключения по беспроводному интерфейсу WiFi 802.11 b/g/n.

3.6 Обоснование выбора системы видеонаблюдения

При изучении рынка систем видеонаблюдения стало понятно, что с одинаковым успехом можно использовать как систему типа DVR, так и систему типа NVR. При использовании системы любого из этих типов можно добиться одинакового результата, однако NVR камеры значительно дороже как в установке, так и при обслуживании. С учётом того, что сеть по заданию характеризуется как бюджетная, такую значительную разницу в цене стоит учесть и использовать DVR камеры. Была выбрана система Swann SWDVK-845808V, состоящая из 8 проводных камер. Накопитель может хранить до 1TB видео-данных. Камеры могут вести запись в качестве 720p или 1080p.

3.7 Обоснование выбора активного сетевого оборудования

Полный перечень оборудования представлен в приложении «В».

3.7.1 Маршрутизатор AT-AR2050V

Так как по условию задания технология, посредством которой осуществляется выход в интернет, не определена, требуется по своему усмотрению выбрать маршрутизатор производителя Allied Telesis. При этом следует учитывать, что проектируемая сеть в задании характеризуется как бюджетная. В результате изучения каталога имеющегося в продаже оборудования был выбран маршрутизатор AT-AR2050V.

Маршрутизатор AR2050V-10 поддерживает Gigabit Ethernet. Данное устройство обладает следующими основными характеристиками:

1. 4 Gigabit Ethernet LAN-порта;

- 2. 1 Gigabit Ethernet WAN-порт;
- 3. 1 USB-порт и 1 порт для консоли;
- 4. Поддержка стандарта 802.1Q

Данное устройство будет являться мостом между коммутатором и сетью провайдера. На нём будет выполняться маршрутизация между виртуальными подсетями организации.

3.7.2 Коммутатор AT-GS950/16

Одним из важнейших критериев для выбора была управляемость коммутатора. AT-GS950/16 является управляемым коммутатором второго уровня, а значит он нам подходит.

Технические характеристики:

- основные порты: 16 Ethernet 10/100/1000 PoE+;
- порты каскадирования: 2 Small Form-Factor Pluggable (SFP) Gigabit Ethernet;
- максимальный размер пакета (MTU): до 10000 байт;
- скорость передачи трафика: 1488 mpps;
- память DRAM: 64 Мб;
- флэш-память: 16 Мб;
- MAC addresses: 8000;
- Available PoE Power: 15.4W PoE.

3.7.3 Точка беспроводного доступа TQ5403

Точка доступа TQ5403 отлично подходит для использования в сетях небольшого и среднего размера.

Технические характеристики:

- протоколы WiFi: 802.11a/b/g/n/ac Wave 2;
- технология MIMO: 2x2 MU-MIMO;
- антенны: 2.4GHz 18.79dBi 3.95dBi/ 5GHz 22.13dBm 4.20dBi/ 5GHz 28dBm 4.83dBi;
- протоколы аутентификации WiFi: WPA/WPA2/WPA3;
- память FLASH: 256 Мб;
- объем ОЗУ: 1 Гб;
- габариты: 215 x 215 x 48 мм.

Также TQ5403 имеет два GigabitEthernet интерфейса.

3.8 Обоснование выбора пассивного сетевого оборудования

Для коммутаторов, находящихся на нулевом и втором этажах, невозможно выделить отдельную комнату, поэтому из соображений безопасности было решено разместить сетевое оборудование в телекоммуникационные шкафы. Шкаф модели “LANMASTER Next TWT-CBWNG-6U-6X4-BK” высотой 6U подойдет для размещения этих коммутаторов.

Оборудование первого этажа, находящееся в отдельной комнате, также было решено поместить в шкаф модели, указанной выше, для удобства и дополнительной защиты.

3.9 Схема адресации

В задании выдана подсеть 201.68.7.0/25.

Исходя из перечня оборудования, а также ролей пользователей, которые имеют к нему доступ, следует разделить подсеть на 5 подсетей. Одна будет для принтера и стационарных компьютеров сотрудников предприятия. Вторая – для мобильных подключений. Третья подсеть нужна для сервера, четвертая для администрирования, а пятая для системы видеонаблюдения. При этом запретим выход сервера в интернет, а также доступ мобильных подключений к ресурсам предприятия.

Подсеть 201.68.7.0/25 разбита с учетом количества устройств, приходящихся на каждый vlan. Адреса подсетей представлены в таблице 3.1

Для стационарных устройств (8 ПК и 6 принтеров) выбрана подсеть IPv4 201.68.7.0/28, и подсеть fc00::/8 для IPv6.

В беспроводной сети 5 мобильных устройств. Для нее выделена подсеть 201.68.7.16/28.

Для системы видеонаблюдения выделена подсеть 201.68.7.32/28.

Для администрирования нужно выделить подсеть, которая будет включать 5 устройств: центральный маршрутизатор, три коммутатора и компьютер администратора. Была выбрана подсеть 201.68.7.48/29.

И для Web-сервера берем подсеть 201.68.7.56/29.

Таблица 3.1 – Схема адресации сетей

Назначение	VLAN	Адрес подсети	Маска подсети
Стационарные подключения	10	201.68.7.0	255.255.255.240
		fc00::	/64
Беспроводная	20	201.68.7.16	255.255.255.240
Видеонаблюдения	30	201.68.7.32	255.255.255.240
Административная	40	201.68.7.48	255.255.255.248
Сервер	50	201.68.7.56	255.255.255.248

3.10 Настройка маршрутизатора

```
Awplus>enable
Awplus#conf terminal
Awplus (config) #hostname Router
Настроим подинтерфейсы для VLAN:
Router (config) #in eth1
Router (config-subif) #encapsulation 10 dot1q
Router (config-subif) #encapsulation 20 dot1q
Router (config-subif) #encapsulation 30 dot1q
Router (config-subif) #encapsulation 40 dot1q
Router (config-subif) #encapsulation 50 dot1q
Router (config-subif) #in eth 1.10
Router (config-subif) #ip address 201.68.7.1/28
Router (config-subif) #in eth 1.20
Router (config-subif) #ip address 201.68.7.17/28
Router (config-subif) #in eth 1.30
Router (config-subif) #ip address 201.68.7.33/28
Router (config-subif) #in eth 1.40
Router (config-subif) #ip address 201.68.7.49/29
Router (config-subif) #in eth 1.50
Router (config-subif) #ip address 201.68.7.57/29
Router (config-subif) #exit
```

IPv4 адреса роутера и маски для каждой из подсетей представлены в таблице 3.2.

Таблица 3.2 – Схема адресации центрального роутера

Назначение	IP адрес	Маска подсети
Стационарные подключения	201.68.7.1	255.255.255.240
Беспроводная	201.68.7.17	255.255.255.240
Видеонаблюдения	201.68.7.33	255.255.255.240
Административная	201.68.7.49	255.255.255.248
Сервер	201.68.7.57	255.255.255.248

В рамках нашей задачи пользовательская подсеть, беспроводная подсеть и подсеть web-сервера не должны пересекаться с подсетью видеонаблюдения. Также подсети пользователей, web-сервера и беспроводная подсеть должны иметь доступ в интернет. Поэтому для разграничения взаимодействия между подсетями настроим firewall.

Настроим firewall для ограничения доступа к некоторым административной подсети:

```
Router (config) #firewall
Router (config-firewall) #rule 1 deny any from public to vlan 30
Router (config-firewall) #rule 2 deny any from vlan 10 to vlan 30
```

```
Router (config-firewall)#rule 3 deny any from vlan 20 to vlan 30
Router (config-firewall)#rule 4 deny any from vlan 50 to vlan 30
Router (config-firewall)#enable
```

Сохраняем текущую конфигурацию в загрузочную:

```
Router#copy running-config startup-config
```

Административная подсеть должна иметь возможность взаимодействовать с устройствами из любой подсети, поэтому для неё правил в firewall не создаём.

3.11 Настройка коммутаторов

Выдадим адреса устройствам в соответствии с таблицей 3.3.

Таблица 3.3 – Адреса устройств для административной подсети.

Устройство	IP адрес	Маска подсети
Router	201.68.7.49	255.255.255.248
Switch0	201.68.7.50	255.255.255.248
Switch1	201.68.7.51	255.255.255.248
Switch2	201.68.7.52	255.255.255.248
Admin-PC	201.68.7.53	255.255.255.248

Для начала подключим коммутаторы через консольный порт и зададим им имена по аналогии с маршрутизатором.

Конфигурация коммутатора нулевого этажа:

```
Awplus>enable
Awplus#conf terminal
Awplus(config)#hostname Switch0
```

Создаем VLAN:

```
Switch0(config)#vlan database
Switch0(config-vlan)#vlan 10 name user state enable
Switch0(config-vlan)#vlan 20 name wireless state enable
Switch0(config-vlan)#vlan 40 name management state enable
Switch0(config-vlan)#vlan 50 name web-server state enable
Switch0(config-vlan)#exit
```

Настраиваем IP-адреса для VLAN:

```
Switch0 (config-subif)#in vlan 40
Switch0 (config-subif)#ip address 201.68.7.50/29
```

Настраиваем интерфейсы:

```
Switch0(config)#in p 1
Switch0(config-if)# switchport mode trunk
Switch0(config-if)# switchport trunk allowed vlan add 10, 20, 40, 50
Switch0(config)#in p 2
Switch0(config-if)# switchport mode access
Switch0(config-if)# switchport access vlan 10
Switch0(config)#in p 3
```

```
Switch0(config-if)# switchport mode access
Switch0(config-if)# switchport access vlan 10
Switch0(config)#in p 4
Switch0(config-if)# switchport mode access
Switch0(config-if)# switchport access vlan 20
Switch0(config)#in p 5
Switch0(config-if)# switchport mode access
Switch0(config-if)# switchport access vlan 10
```

Сохраняем текущую конфигурацию в загрузочную:

```
Switch0#copy running-config startup-config
```

Конфигурация коммутатора первого этажа:

```
Awplus>enable
```

```
Awplus#conf terminal
```

```
Awplus(config)#hostname Switch1
```

Создаем VLAN:

```
Switch1(config)#vlan database
```

```
Switch1(config-vlan)#vlan 10 name user state enable
```

```
Switch1(config-vlan)#vlan 20 name wireless state enable
```

```
Switch1(config-vlan)#vlan 30 name cctv state enable
```

```
Switch1(config-vlan)#vlan 40 name management state enable
```

```
Switch1(config-vlan)#vlan 50 name web-server state enable
```

```
Switch1(config-vlan)#vlan 60 name intr state enable
```

```
Switch1(config-vlan)#exit
```

Настраиваем IP-адреса для VLAN:

```
Switch1 (config-subif)#in vlan 40
```

```
Switch1 (config-subif)#ip address 201.68.7.51/29
```

Настраиваем интерфейсы:

```
Switch1(config)#in p 1
```

```
Switch1(config-if)# switchport mode access
```

```
Switch1(config-if)# switchport access vlan 60
```

```
Switch1(config)#in p 2
```

```
Switch1(config-if)# switchport mode access
```

```
Switch1(config-if)# switchport access vlan 20
```

```
Switch1(config)#in p 3
```

```
Switch1(config-if)# switchport mode access
```

```
Switch1(config-if)# switchport access vlan 30
```

```
Switch1(config)#in p 4
```

```
Switch1(config-if)# switchport mode access
```

```
Switch1(config-if)# switchport access vlan 30
```

```
Switch1(config)#in p 5
```

```
Switch1(config-if)# switchport mode access
```

```
Switch1(config-if)# switchport access vlan 50
```

```
Switch0(config)#in p 6-7
```

```
Switch0(config-if)# switchport mode trunk
```

```
Switch0(config-if)# switchport trunk allowed vlan add 10, 20, 40, 50
```

Сохраняем текущую конфигурацию в загрузочную:

```
Switch1#copy running-config startup-config
```

Конфигурация коммутатора второго этажа:

```
Awplus>enable
Awplus#conf terminal
Awplus(config)#hostname Switch2
```

Создаем VLAN:

```
Switch2(config)#vlan database
Switch2(config-vlan)#vlan 10 name user state enable
Switch2(config-vlan)#vlan 20 name wireless state enable
Switch2(config-vlan)#vlan 40 name management state enable
Switch2(config-vlan)#vlan 50 name web-server state enable
Switch2(config-vlan)#exit
```

Настраиваем IP-адреса для VLAN:

```
Switch2 (config-subif)#in vlan 40
Switch2 (config-subif)#ip address 201.68.7.53/29
```

Настраиваем интерфейсы:

```
Switch2(config)#in p 1
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# switchport trunk allowed vlan add 10, 20, 40, 50
Switch2(config)#in p 2-12
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 10
Switch2(config)#in p 13
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 20
Switch2(config)#in p 14
Switch2(config-if)# switchport mode access
Switch2(config-if)# switchport access vlan 40
```

Сохраняем текущую конфигурацию в загрузочную:

```
Switch2#copy running-config startup-config
```

3.12 Настройка ПК и маршрутизации между ними

Для ПК требуется настроить статическую IPv4 и IPv6 маршрутизацию. Адреса ПК представлены в таблице 3.3. Сперва включим ipv6 на центральном роутере и зададим ему ipv6 адрес:

```
Router (config)#in eth1
Router (config-subif)#in eth 1.10
Router (config-subif)#ipv6 enable
Router (config-subif)#ipv6 address fc00::1/8
```

Таблица 3.4 – Адреса ПК.

Устройство	IP адрес	Маска подсети
Stk-PC1	201.68.7.2	255.255.255.240
	fc00::2	/64
Stk-PC2	201.68.7.3	255.255.255.240
	fc00::3	/64
Sec-PC	80.94.11.34	255.255.255.240
	fc00::4	/64
User-PC1	201.68.7.4	255.255.255.240
	fc00::5	/64
User-PC2	201.68.7.5	255.255.255.240
	fc00::6	/64
User-PC3	201.68.7.6	255.255.255.240
	fc00::7	/64
User-PC4	201.68.7.7	255.255.255.240
	fc00::8	/64
User-PC5	201.68.7.8	255.255.255.240
	fc00::9	/64
User-PC6	201.68.7.9	255.255.255.240
	fc00::10	/64
Admin-PC	201.68.7.53	255.255.255.248
	fc00::11	/64

Настройка адресов IPv4 и IPv6 на ПК с Windows производится по следующему алгоритму:

1. Заходим в свойства Ethernet.

2. Выбираем IP версии 4 (TCP/IP), нажимаем кнопку «Свойства». Делаем поле «Использовать следующий IP-адрес», заполняем поля «IP-адрес» и «Маска подсети» соответствующими адресами из таблицы 3.5.

В поле «Основной шлюз» вводим IPv4 адрес центрального маршрутизатора. Окна настройки представлены на рисунке 3.1.

3. Настройка IPv6 аналогична IPv4, только нужно выбрать IP версии 6 (TCP/IP), и в окне настройки ввести IPv6 адреса ПК и маршрутизатора. Окна настройки представлены на рисунке 3.2.

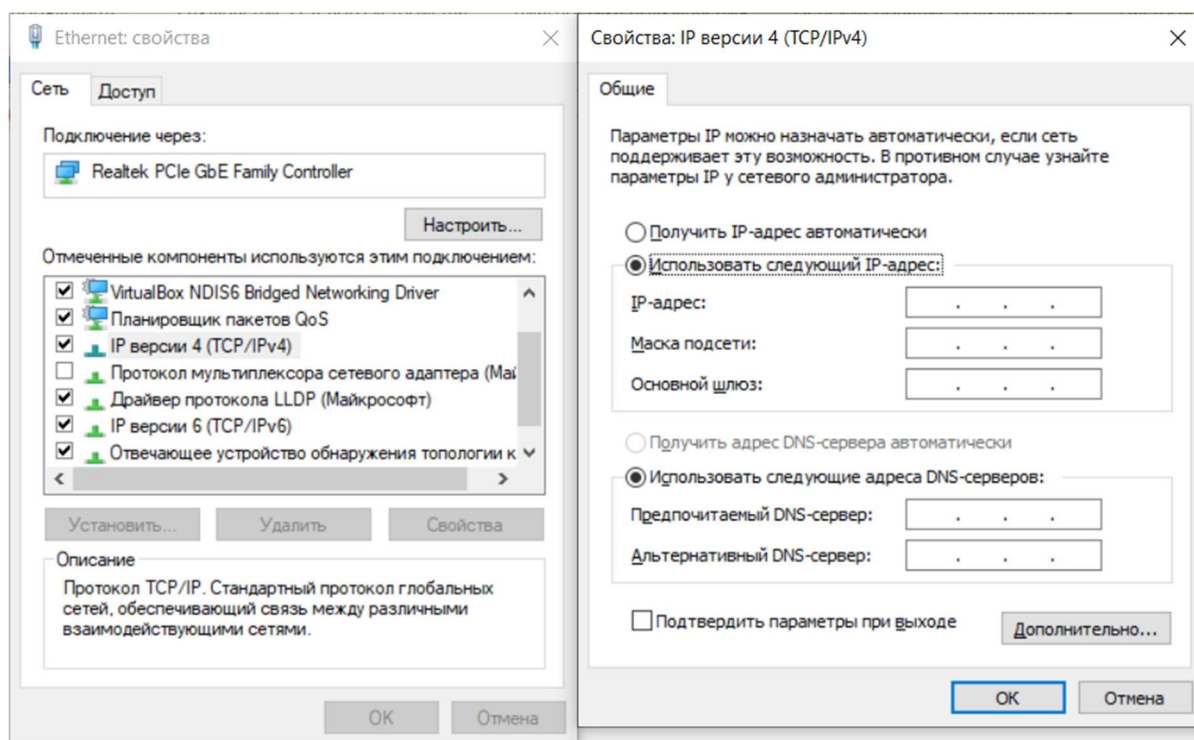


Рисунок 3.1 – Настройка IPv4 на ПК

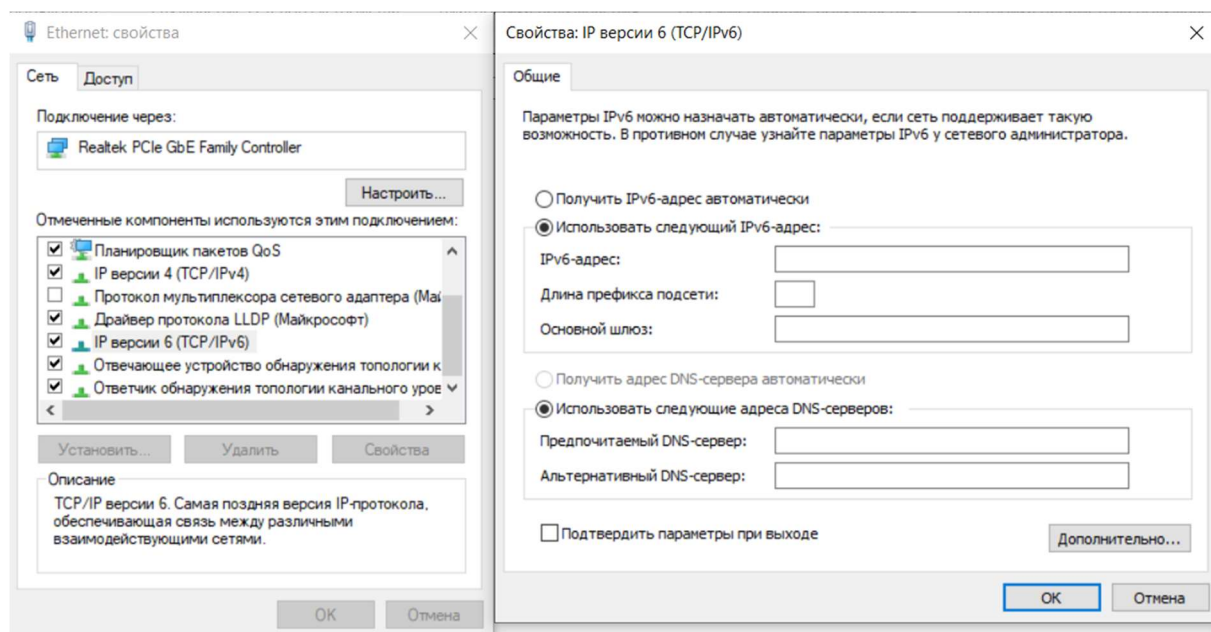


Рисунок 3.2 – Настройка IPv6 на ПК

3.13 Настройка принтера

Для того, чтобы принтер можно было использовать, его необходимо подключить к локальной сети, а после этого установить драйвер с прилагающегося диска.

Подключение принтера к локальной сети состоит в физическом его подключении посредством Ethernet кабеля и настройке IP адреса. Настроить IP адрес можно с помощью встроенной в принтер консоли, показанной на рисунке 3.3.



Рисунок 3.3 – Консоль принтера

Сначала нужно нажать кнопку «Menu», затем стрелками выбрать раздел «Network Set» и нажать кнопку «OK». После этого таким же образом выбираем раздел «Wired network setting». Задаём IP адрес и маску подсети. Для этого стрелками выбираем цифры от 0 до 9 и подтверждаем выбор кнопкой «OK». После того, как последняя цифра маски была введена, ещё раз нажимаем кнопку «OK» для сохранения и кнопку «Return», чтобы вернуться в предыдущий раздел меню.

Теперь необходимо установить на принтер драйверы, поставляемые в комплекте с принтером на диске. Для этого вставляем диск в дисковод компьютера. После этого на экране появится окно, показанное на рисунке 3.4.

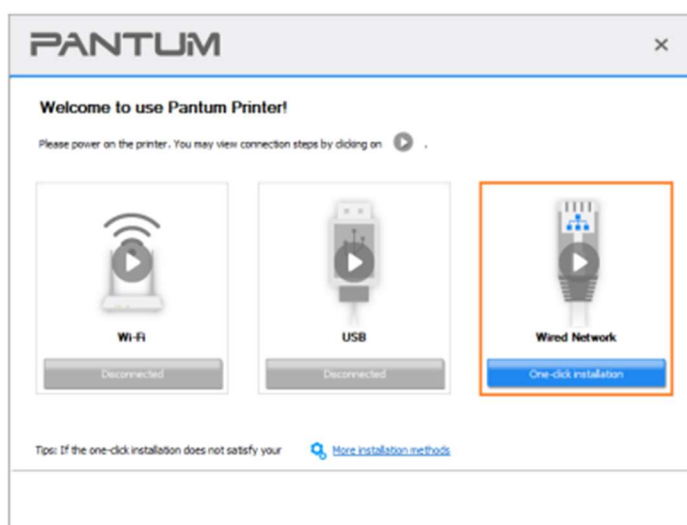


Рисунок 3.4 – Поиск ПО для принтера

Нажимаем на кнопку One-click installation под Wired Network. После этого мы увидим окно со списком всех принтеров в сети. Выбираем IP адрес нужного принтера, после чего начнётся установка драйвера. По завершении установки появится окно, показанное на рисунке 3.5. Нажимаем кнопку «Done» для выхода из программы установки. Принтер готов к использованию.



Рисунок 3.5 – Окно завершения установки драйвера

3.14 Настройка web-сервера

На компьютере для web-сервера нужно будет указать адрес 201.68.7.58 и маску 255.255.255.248. В качестве шлюза указать ip роутера 201.68.7.57.

Web-сервер Apache не требует настройки, его можно использовать сразу же после установки. Все настройки зависят от конкретных потребностей организации и того, как сервер будет использоваться.

3.15 Настройка Прокси-сервера

Настройка прокси-сервера Squid осуществляется путём изменения его конфигурационных файлов. Он предоставляет такие функции, как кэширование, обратный прокси и другие.

Распространённым применением прокси является ограничение доступа сотрудников организации к определённым сайтам. Ниже приведён пример конфигурации, который запретит сотрудникам посещать youtube, twitter и instagram.

Откроем конфигурационный файл:

```
$sudo nano /etc/squid/blocked_sites
```

Добавим в него сайты, доступ к которым нужно ограничить. Файл должен выглядеть так:

```
youtube.com
```

```
twitter.com
```

```
instagram.com
```

После этого добавляем в прокси access list:

```
acl blocked_sites dstdomain "/etc//squid/blocked_sites"
```

```
http_access deny blocked_sites
```

Перезапускаем сервер:

```
$sudo systemctl restart squid
```

После этого изменённая конфигурация вступит в силу.

3.16 Настройка точки беспроводного доступа

Для удалённого подключения к точке доступа необходимо ввести адрес 192.168.1.230 в адресной строке браузера.

После этого появится следующее окно, показанное на рисунке 3.6 – потом напишу.



Рисунок 3.6 – Окно ввода пароля

При первом подключении нужно ввести имя пользователя manager и пароль friend.

Тогда появится окно, показанное на рисунке 3.7.

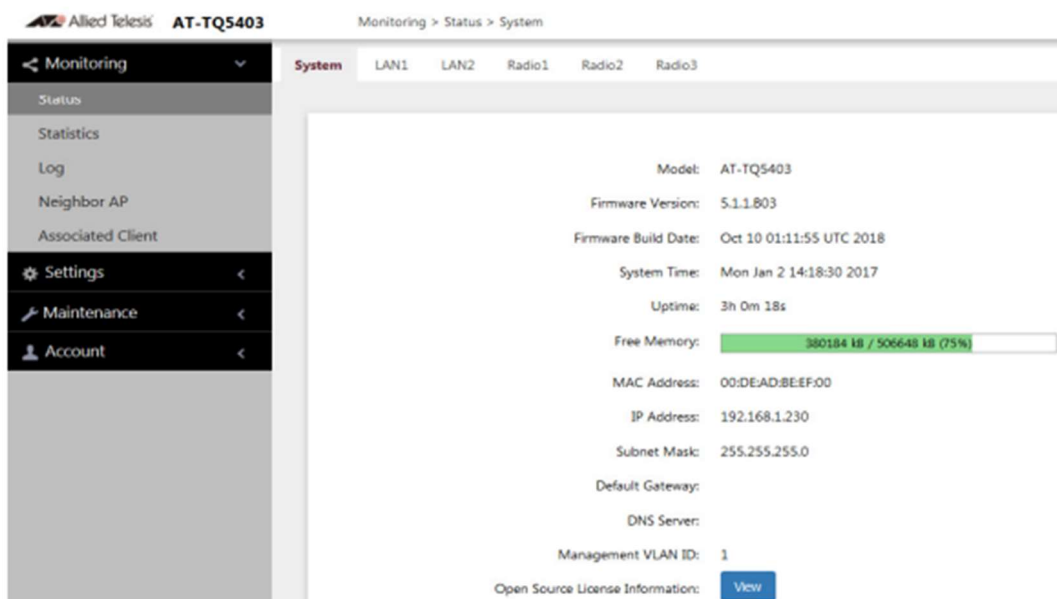


Рисунок 3.7 – окно настройки точки доступа

Перейдём во вкладку Settings>System>Network. На рисунках 3.8, 3.9, 3.10 показано, как после конфигурации IP адресов и масок подсетей для всех трёх точек доступа будет выглядеть эта вкладка для каждой из них.

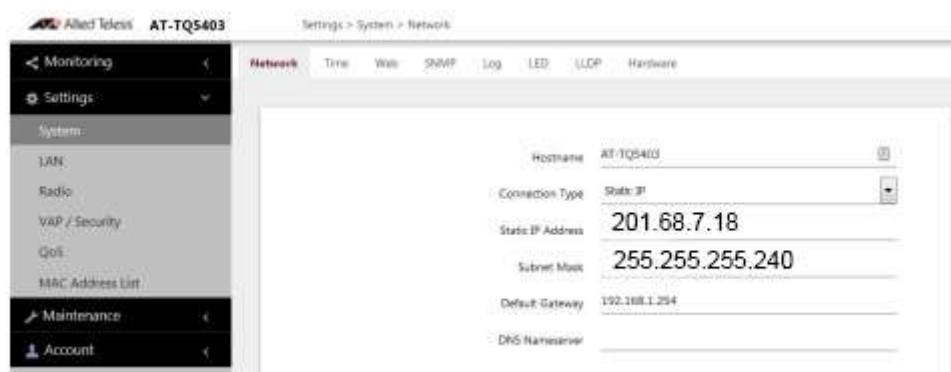


Рисунок 3.8 – Точка доступа нулевого этажа

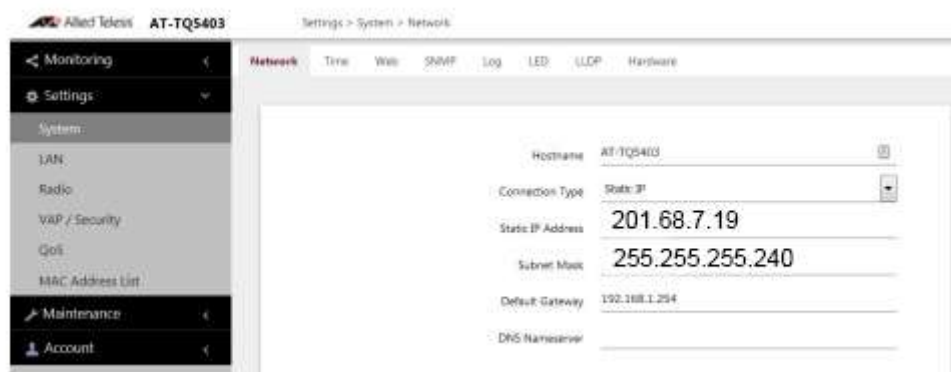


Рисунок 3.9 – Точка доступа первого этажа

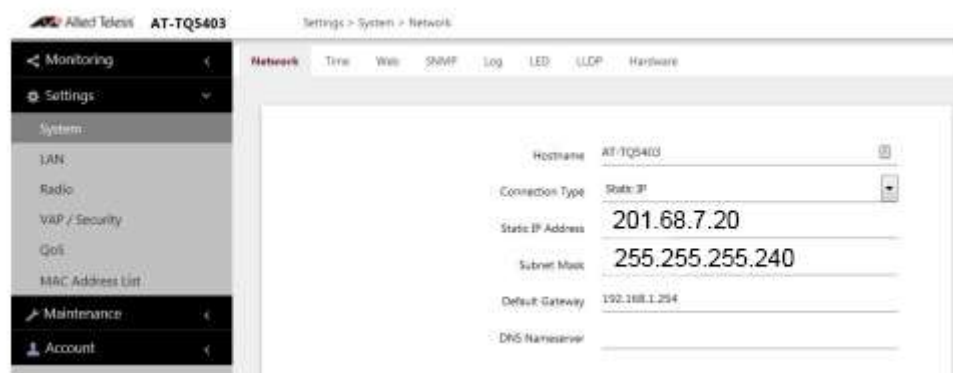


Рисунок 3.10 – Точка доступа второго этажа

Настроим протокол безопасности WPA Personal. Для этого перейдём во вкладку Settings>VAP>Security>Radio1 и напишем пароль в поле Key. Вкладка после выбора пароля показана на рисунке 3.11.



Рисунок 3.11 – Конфигурация WPA точек доступа

4 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

В проектируемой локальной компьютерной сети кабельная система реализована с помощью прокладки витой пары за подвесным потолком. От потолка к информационным розеткам кабель протягивается по стенам, в кабельном коробе. Информационные розетки расположены у пола, в близости от конечных устройств. Между этажами кабели проходят по кабельным шахтам. Кабели системы видеонаблюдения проложены по зданию аналогичным образом.

Центральный маршрутизатор, коммутатор и сервер находятся в служебном помещении. Коммутатор и маршрутизатор расположены в телекоммуникационном шкафу, сервер и сетевой видеорегистратор стоят на столе. Точки беспроводного доступа вынесены в коридор и закреплены на потолке, для обеспечения лучшей связи в помещении. Коммутаторы, расположенные на нулевом и втором этажах, помещены в подвесные телекоммуникационные шкафы для того, чтобы обезопасить их от физического воздействия.

В плане здания можно увидеть месторасположение информационных розеток и сетевого оборудования, прокладку кабелей.

С планами этажей можно ознакомиться в приложениях Г, Д, Е.

4.1 Обоснование выбора кабельного короба

Особых требований к кабельным каналам нет, поэтому был выбран кабель-канал Bylectrica КДК40х25.

4.2 Обоснование выбора информационных розеток

Для подключения устройств к сети необходимо обеспечить доступность устройств к кабелю. Удобно и эстетично организовать доступ позволяет монтаж информационных розеток RJ-45. Хорошим вариантом информационных розеток являются французские SCHNEIDER ELECTRIC AtlasDesign, обеспечивающие доступ к сети.

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы была разработана локальная компьютерная сеть для организации, занимающейся торговлей овощами и фруктами. Также были получены практические и теоретические знания, и навыки проектирования локальной вычислительной сети.

Был исследован рынок сетевого оборудования, стандарты и требования к создаваемой системе.

Результатами проектирования являются структурная, функциональная схемы, план этажей здания организации, перечень оборудования и материалов, необходимых для построения и реализации сети. Сюда вошли маршрутизатор, коммутаторы, рабочие станции, принтеры, серверы и пассивное сетевое оборудование. Оборудование, выбранное в данной работе, удовлетворяет всем стандартам качества, надежности.

Полученная компьютерная сеть будет проста в обслуживании, а также при необходимости ее можно будет масштабировать.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- [1] Сайт производителя сетевого оборудования Allied Telesis [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.alliedtelesis.com/us/en> – Дата доступа: 27.09.2022
- [2] Олифер, В. Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер – СПб: Питер, 2019. – 992 с.
- [3] Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – 5-е издание – Санкт-Петербург [и другие]: Питер, Питер Пресс, 2017. – 955 с.
- [4] Спецификация маршрутизатора AR2050V [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.alliedtelesis.com/by/en/products/security-appliances/secure-vpn-routers/ar2050v#description-tab> – Дата доступа: 13.10.2022
- [5] Спецификация точки беспроводного доступа TQ5403 [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.alliedtelesis.com/sites/default/files/documents/datasheets/ati-tq5403-ds.pdf> – Дата доступа: 13.10.2022
- [6] Указания по монтажу точки беспроводного доступа TQ5403 [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.alliedtelesis.com/sites/default/files/documents/installation-guides/ati-tq5403series-ig.pdf> – Дата доступа: 13.10.2022
- [7] Информация о подключении камер видеонаблюдения к локальной сети [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.versitron.com/blog/how-to-configure-nvr-for-ip-camera-on-a-network> – Дата доступа: 13.10.2022
- [8] Список популярных прокси-серверов для Linux [Электронный ресурс] – Электронные данные. – Режим доступа: <https://losst.pro/luchshie-proksi-servery-linux> – Дата доступа: 13.10.2022
- [9] Информация о прокси-сервере Squid [Электронный ресурс] – Электронные данные. – Режим доступа: <http://www.squid-cache.org/> – Дата доступа: 13.10.2022
- [10] Информация о прокси-сервере Privoxy [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.privoxy.org/> – Дата доступа: 13.10.2022
- [11] Информация о прокси-сервере Tinyproxy [Электронный ресурс] – Электронные данные. – Режим доступа: <http://tinyproxy.github.io/> – Дата доступа: 13.10.2022
- [12] Различия между DVR и NVR видеорегистраторами [Электронный ресурс] – Электронные данные. – Режим доступа: <https://info.verkada.com/compare/dvr-vs-nvr/#:~:text=A%20DVR%20converts%20analog%20footage,for%20storage%20and%20remote%20viewing.> – Дата доступа: 13.10.2022
- [13] Информация о подключении DVR видеорегистраторов к локальной сети [Электронный ресурс] – Электронные данные. – Режим доступа:

<https://www.cctvcore.com/connect-dvr-lan-basic-network-connection.aspx>– Дата доступа: 13.10.2022

[14] Пользовательское руководство для системы видеонаблюдения Swann SWDVK-845808V [Электронный ресурс] – Электронные данные. – Режим доступа: <https://www.manua.ls/swann/swdvk-845808v/manual>– Дата доступа: 04.12.2022

[15] Документация по использованию веб-интерфейса коммутатора AT-GS950/16 [Электронный ресурс] – Электронные данные. – Режим доступа: https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/gs950_16webs114v110a.pdf– Дата доступа: 04.12.2022