УДК 004

Проектирование локальной вычислительной сети учреждения

Волков Виталий Александрович
Мордовский государственный университет им. Н.П.Огарева
студент

Аннотация
В современном мире у организаций есть потребность в обмене информацией между сотрудниками и другими учреждениями. Для предоставления таких возможностей строится локальная вычислительная сеть. В данной работе рассматриваются этапы проектирования такой сети. Способы построения подсетей организации. Методы обеспечения безопасности локальной вычислительной сети.
Ключевые слова: ЛВС; коммутатор; маршрутизатор; физическая топология; логическая топология; PacketTracer; VLAN; VLSM; NAT;ACL; топология; шлюз; адрес; сервер; TCP/IP; IP-адрес; IEEE 802.3u.

Local area network design agencies

Volkov Vitaliy Alexandrovich
Ogarev Mordovian State University
student

Abstract
In today's world, there is a need for organizations to exchange information between staff and other agencies. To provide such capabilities built local area network. This paper discusses the design stages of such a network. How to build an organization subnets. Security practices for local area network.
Key words: LAN; switch; router; physical topology; logical topology; Packet Tracer; VLAN; VLSM; NAT; ACL; topology; gateway; address; Server; TCP/IP; IP address; IEEE 802.3U.

В ходе работы организации зачастую возникает потребность передачи информации как между работниками одной организации, так и между различными предприятиями (связь между ними осуществляется либо через сеть Internet, либо через какую-либо другую транспортную сеть). Для предоставления таких возможностей коммуникации строится локальная вычислительная сеть учреждения (ЛВС). Проектируемая локальная вычислительная сеть разрабатывается с целью создания необходимых условий для работы организации среднего размера. Сеть должна соответствовать стандартам и всем заявленным в условии требованиям.

Условия проектирования ЛВС:

1. ЛВС должна соответствовать стандарту ISO/IEC 11801:2002;

2. Размещение рабочих станций следующее:
   - Отдел 1 (Комнаты 101 – 115) – 40 человек;
   - Отдел 2 (Комнаты 218-232) – 20 человек;
   - Отдел 3 (116-122) – 25 человек;
   - Отдел 4 (123 – 136, 201-217, 233 - 250) – 80 человек;

3. Имеется три внешних адреса из сети 194.54.65.32\28, шлюз 194.54.65.33, DNS 8.8.8.8;

4. Работники отделов имеют сетевой доступ только к компьютерам своего отдела, все работники (кроме отдела 4) имеют доступ в интернет, Работники отдела 2 имеют доступ к сетям всех отделов. В организации имеется Ftp сервер, имеющий свой внешний адрес, обеспечить доступ к нему извне.

Для начала спроектируем физическую топологию размещения оборудования согласно плану здания и выдвинутым условиям (см. рис. 1, 2). На первом этаже здания будет находятся 85 рабочих станций. На втором этаже расположим 80 персональных компьютеров. Общее количество узлов получим 165. Получим схему размещения оборудования, представленную ниже.

1. На первом этаже здания размещены 5 коммутаторов:
   1.1. №1 (коридор, стена кабинета №106) – в него включены 20 ПК 1-го отдела;
   1.2. №2 (коридор, стена кабинета №102) – включены 20 ПК 1-го отдела;
   1.3. №3 (коридор, напротив кабинета №118) – 13 ПК 3-го отдела;
   1.4. №4 (коридор, напротив кабинета №121) – 12 ПК 3-го отдела;
   1.5. №5 (коридор, стена кабинета №125) – 20 ПК 4-го отдела.
2. На втором этаже здания размещены также 5 коммутаторов:
   2.1. №1 (коридор, стена кабинета №210) – в него включены 15 ПК 4-го отдела;
   2.2. №2 (коридор, стена кабинета №203) – 15 ПК 4-го отдела;
   2.3. №3 (коридор, стена кабинета №227) – 20 ПК 2-го отдела;
   2.4. №4(коридор, стена кабинета №236) – 15 ПК 4-го отдела;
   2.5. №5(коридор, стена кабинета №239) – 15ПК 4-го отдела;

Помимо этого, на первом и втором этажах размещены центральные для них коммутаторы (напротив кабинета №119 и на стене кабинета №226 соответственно). В кабинете №123 на первом этаже предлагается разместить роутер, главный коммутатор предприятия и ftp-сервер.

Теперь нам нужно определиться с количеством и типом оборудования, которое будет использоваться в нашей ЛВС. Для данной сети мы будем использовать коммутаторы Cisco 2950, маршрутизатор Cisco 1841 и сервер Aquarius Server T50 D67.

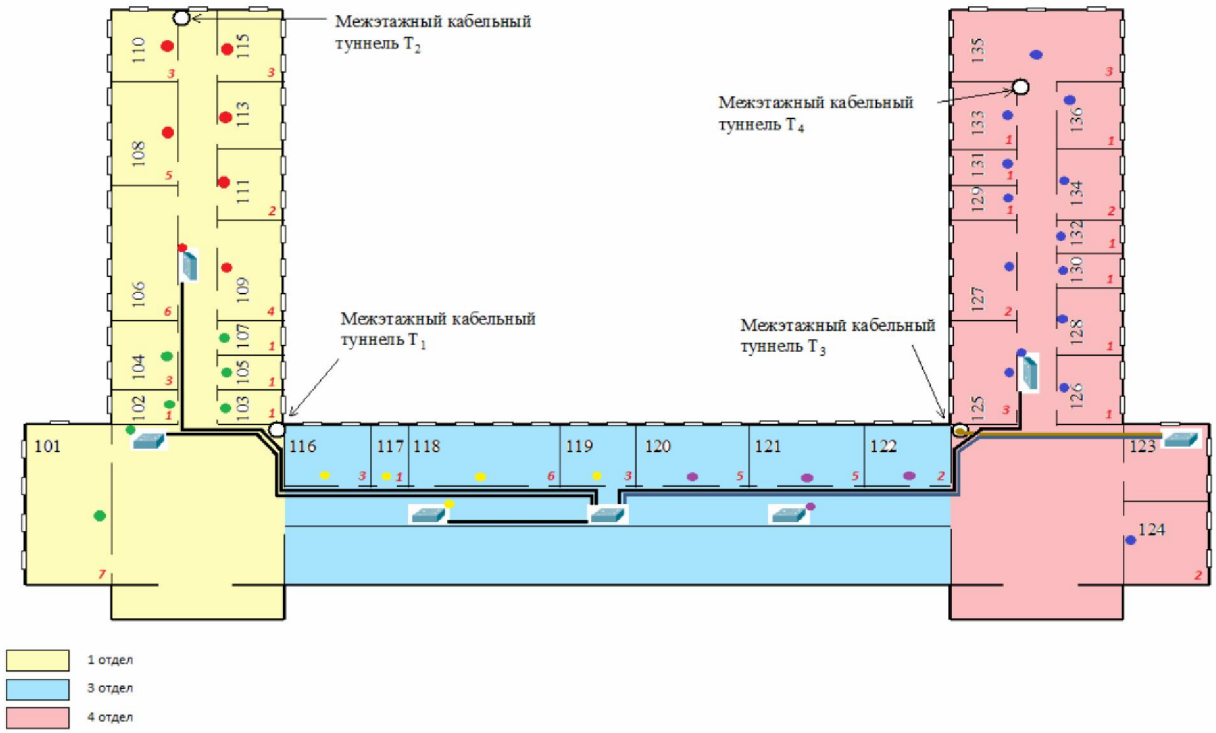

Рисунок 1 –Физическая топология (план прокладки кабеля, 1 этаж)

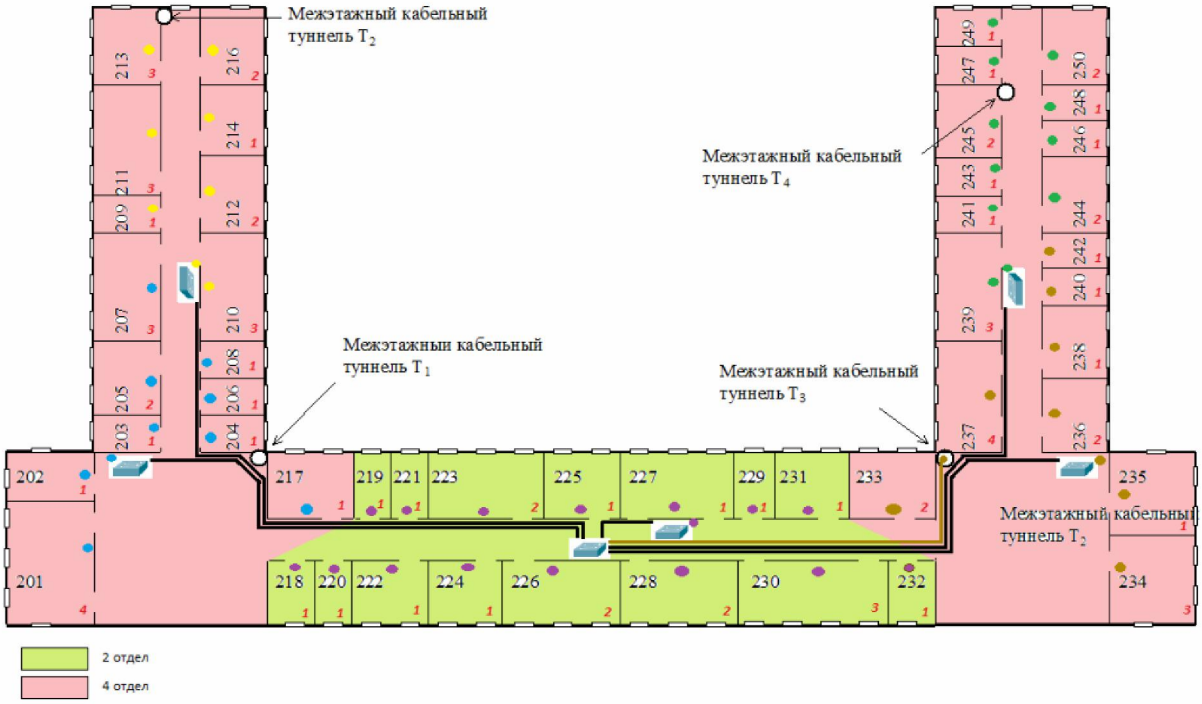

Рисунок 2 –Физическая топология (план прокладки кабеля, 2 этаж)

Полученная локальная вычислительная сеть построена по топологии расширенная звезда. В соответствии с ней, группы рабочих станций соединяются с коммутаторами, которые в свою очередь соединяются с центральным коммутатором (центральный узел), соединяющимся с роутером. Также к центральному коммутатору подключается ftp-сервер.

Топология «звезда» на технологии Ethernet является наиболее распространенной на сегодняшний момент. Она отвечает всем требованиям к современной локальной сети и довольно удобна в эксплуатации.

Достоинства данной топологии:

− выход из строя одной рабочей станции не отражается на работе всей сети в целом;
− хорошая масштабируемость сети;
− лёгкий поиск неисправностей и обрывов в сети;
− высокая производительность сети;
− гибкие возможности администрирования.

Недостатки выбранной топологии:

− выход из строя центрального концентратора оборачивается неработоспособностью сети;
− для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;
− конечное число рабочих станций в сети ограничено количеством портов в центральном концентраторе.

В центре каждой «звезды» располагается коммутатор, который непосредственно соединен с каждым отдельным узлом сети через тонкий гибкий кабель UTP, так же называемый «витой парой». Кабель соединяет сетевой адаптер ПК с коммутатором. Устанавливать сеть с топологией «звезда» просто и недорого. Число узлов, которые можно подключить к коммутатору, определяется возможным количеством портов самого коммутатора. Однако имеется ограничение по числу узлов: сеть может иметь максимум 1024 узла. Рабочая группа, созданная по схеме «звезда», может функционировать независимо или может быть связана с другими рабочими группами [1].

В качестве технологии доступа используется FastEthernet, который обеспечивает скорость обмена данными в 100 Мбит/с.

В качестве подвида данной технологии был выбран 100BASE-TX, IEEE 802.3u – развитие стандарта 10BASE-T для использования в сетях топологии «звезда». Задействована витая пара категории 5: CAT5e – скорость передач данных до 100 Мбит/спри использовании 2 пар. Кабель этой категории является самым распространённым и используется для построения компьютерных сетей. Его преимущества в более низкой себестоимости и меньшей толщине.

Далее нам надо собрать макет проектируемой сети (см. рис. 3). Для этого мы будем использовать программу CiscoPacketTracer. PacketTracer— это симулятор сети передачи данных, выпускаемый фирмой CiscoSystems. Позволяет делать работоспособные модели сети, настраивать маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями. Успешно позволяет создавать даже сложные макеты сетей, проверять на работоспособность топологии [3].

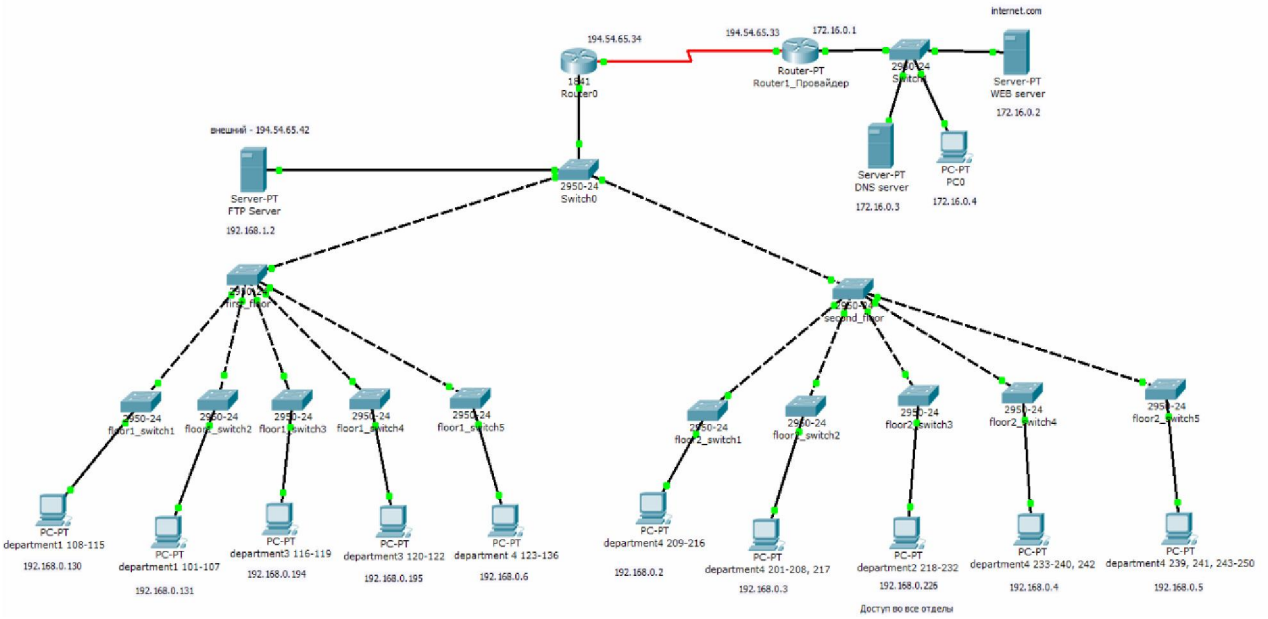

Рисунок 3 – Логическая топология

После составления макета сети необходимо настроить её согласно требованиям и проверить на работоспособность. Для построения подсетей организации мы будем использовать технологию VLAN [2]. Это дает такие преимущества как:

– облегченное перемещение, добавление устройств и изменение их соединений друг с другом;

– большая степень административного контроля вследствие наличия устройства, осуществляющего между сетями VLAN маршрутизацию на 3-м уровне;

– меньшее потребление полосы пропускания по сравнению с ситуацией одного широковещательного домена;

– сокращение непроизводственного использования CPU за счет сокращения пересылки широковещательных сообщений;

– предотвращение широковещательных штормов и предотвращение потерь.

Поскольку в организации 4 отдела, было решено использовать отдельный VLAN для каждого из них: VLAN 11 (для 1-го отдела), VLAN 12 (для 2-го отдела), VLAN 13 (для 3-го отдела), VLAN 14 (для 4-го отдела). Для ftp-сервера предусмотрена VLAN 15.

Порты коммутаторов, к которым подключаются непосредственно рабочие станции, находятся в режиме modeaccessдля соответствующей VLAN. Остальные порты коммутаторов служат магистральными портами, и находятся в режиме modetrunk.

Выбор адресного плана будет основан на технологии VLSM (технология бесклассовой адресации). Для построения ЛВС используется адресный план, представленный в таблице 1.

Таблица 1 – Адресный план

Название подсети	Размер	Адрес	Маска	Диапазон доступных адресов	Широковещание
Отдел 4 (80 чел.)	126	192.168.0.0/25	255.255.255.128	192.168.0.1 - 192.168.0.126	192.168.0.127
Отдел 1 (40 чел.)	62	192.168.0.128/26	255.255.255.192	192.168.0.129 - 192.168.0.190	192.168.0.191
Отдел 3 (25 чел.)	30	192.168.0.192/27	255.255.255.224	192.168.0.193 - 192.168.0.222	192.168.0.223
Отдел 2 (20 чел.)	30	192.168.0.224/27	255.255.255.224	192.168.0.225 - 192.168.0.254	192.168.0.255
Ftp-сервер	14	192.168.1.0/28	255.255.255.240	192.168.1.1 - 192.168.1.14	192.168.1.15

Уровень распределения (уровень рабочих групп) является связующим звеном между уровнями доступа и ядра. В зависимости от способа реализации, уровень распределения может выполнять следующие функции:

- обеспечение маршрутизации, качества обслуживания и безопасности сети и агрегирование адресов;
- переход от одной технологии к другой (например, от 100Base-TX к 1000Base-T);

EEE 802.1Q — открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN.

Так как 802.1Q не изменяет заголовки кадра, то сетевые устройства, которые не поддерживают этот стандарт, могут передавать трафик без учёта его принадлежности к VLAN.

802.1Q помещает внутрь фрейма тег, который передает информацию о принадлежности трафика к VLAN'у (рис. 4).

16 бит	**3 бита**	**1 бит**	**12 бит**
TagProtocolIdentifier (TPID)	**Priority**	**CanonicalFormatIndicator (CFI)**	**VLAN Identifier (VID)**

Рисунок 4 – Кадр стандарта EEE 802.1Q

Размер тега — 4 байта. Он состоит из полей:

− TagProtocolIdentifier (TPID) — Идентификатор протокола тегирования. Размер поля — 16 бит. Указывает, какой протокол используется для тегирования. Для 802.1q используется значение 0x8100.

− TagControlInformation (TCI)- поле, инкапсулирующее в себе поля приоритета, канонического формата и идентификатора VLAN:

- Priority — приоритет. Размер поля — 3 бита. Используется стандартом IEEE 802.1p для задания приоритета передаваемого трафика.

- CanonicalFormatIndicator (CFI) — Индикатор канонического формата. Размер поля — 1 бит. Указывает на формат MAC-адреса. 0 — канонический (Кадр Ethernet), 1 — не канонический (Кадр TokenRing,FDDI).
- VLAN Identifier (VID) — идентификатор VLAN'a. Размер поля — 12 бит. Указывает, какомуVLAN'у принадлежит фрейм. Диапазон возможных значений VID от 0 до 4094.

При использовании стандарта Ethernet II 802.1Q вставляет тег перед полем "Тип протокола" (рис. 5). Так как фрейм изменился, пересчитывается контрольная сумма.

Адрес приемника	**Адрес источника**	**Тег**	**Тип протокола/ Длина кадра**	**Данные**	**Новая контрольная сумма**

Рисунок 5 – Построение тегированного фрейма по стандарту IEEE 802.1Q

В проектируемой ЛВС используется маршрутизатор Cisco 1841. Для маршрутизации между VLAN на роутере пропишем субинтерфейсы.

```
interface FastEthernet0/0
noip address
duplex auto
speed auto
!
interface FastEthernet0/0.1
encapsulation dot1Q 11
ip address 192.168.0.129 255.255.255.192
ip access-group dep1_in in
ipnat inside
!
interface FastEthernet0/0.2
encapsulation dot1Q 12
ip address 192.168.0.225 255.255.255.224
ipnat inside
!
interface FastEthernet0/0.3
encapsulation dot1Q 13
ip address 192.168.0.193 255.255.255.224
ip access-group dep3_in in
ipnat inside
!
interface FastEthernet0/0.4
```

```
encapsulation dot1Q 14
ip address 192.168.0.1 255.255.255.128
ip access-group dep4_in in
ipnat inside
!
interface FastEthernet0/0.5
encapsulation dot1Q 15
ip address 192.168.1.1 255.255.255.240
ipnatinside
```

По требованиям к разрабатываемой ЛВС организация имеет три внешних адреса из сети 194.54.65.32\28.

Для трансляции сетевых адресов используется технология NAT – это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов [4].

NAT выполняет три важных функции:

1. Позволяет сэкономить IP-адреса (только в случае использования NAT в режиме PAT), транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 публичный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с приватными (внутренними) IP-адресами.

2. Позволяет предотвратить или ограничить обращение снаружи к внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются.

3. Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов.

```
ipnat pool public_address 194.54.65.40 194.54.65.40 netmask 255.255.255.240
ipnat inside source list nat-list pool public_address overload
ipnat inside source static 192.168.1.2 194.54.65.42
```

На роутере прописываем следующие маршруты:

```
iproute 0.0.0.0 0.0.0.0 194.54.65.33
iproute 172.16.0.0 255.255.255.0 194.54.65.33
```

Каждая корпоративная компьютерная сеть требует постоянного внимания к себе. Как бы хорошо она ни была настроена, насколько бы

надежное ПО не было установлено на серверах и клиентских компьютерах – нельзя полагаться лишь на внимание системного администратора. Необходимы автоматические и непрерывно действующие средства контроля состояния сети и своевременного оповещения о возможных проблемах.

Случайные сбои аппаратного или программного обеспечения могут привести к весьма неприятным последствиям. Существенное замедление функционирования сетевых сервисов и служб – еще наименее неприятное из них (хотя в худших случаях и может оставаться незамеченным в течение длительных промежутков времени). Гораздо хуже, когда критично важные службы или приложения полностью прекращают функционирование, и это остается незамеченным в течение длительного времени. Типы же «критичных» служб могут быть весьма разнообразны (и, соответственно, требовать различных методов мониторинга). От корректной работы веб-серверов и серверов базы данных может зависеть работоспособность внутрикорпоративных приложений и важных внешних сервисов для клиентов. Сбои и нарушения работы маршрутизаторов могут нарушать связь между различными частями корпорации и ее филиалами; серверы внутренней почты и сетевых мессенджеров, автоматических обновлений и резервного копирования, принт-серверы – любые из этих элементов могут страдать от программных и аппаратных сбоев.

И все же, непреднамеренные отказы оборудования и ПО – в большинстве случаев, разовые и легко исправляемые ситуации. Куда больше вреда может принести сознательные вредоносные действия изнутри или извне сети. Злоумышленники, обнаружившие «дыру» в безопасности системы, могут произвести множество деструктивных действий – начиная от простого вывода из строя серверов (что, как правило, легко обнаруживается и исправляется), и заканчивая заражением вирусами (последствия непредсказуемы) и кражей конфиденциальных данных (последствия плачевны).

Практически все из описанных выше сценариев (и множество аналогичных), в конечном итоге, ведут к серьезным материальным убыткам: нарушению схем взаимодействия между сотрудниками, безвозвратной утере данных, потере доверия клиентов, разглашению секретных сведений и т.п. Поскольку полностью исключить возможность отказа или некорректной работы техники невозможно, решение заключается в том, чтобы обнаруживать проблемы на наиболее ранних стадиях, и получать о них наиболее подробную информацию. Для этого, как правило, применяется различное программное обеспечение мониторинга и контроля сети, которое способно как своевременно оповещать технических специалистов об обнаруженной проблеме, так и накапливать статистические данные о стабильности и других параметрах работы серверов, сервисов и служб, доступные для подробного анализа.

Рассмотрим базовые методы мониторинга работы сети и контроля ее защищенности.

В проектируемой локальной вычислительной сети работники отделов имеют сетевой доступ только к компьютерам своего отдела и в сеть интернет (кроме отдела 4). Работники отдела 2 имеют доступ к сетям всех отделов. Также в организации имеется Ftp сервер.

Для реализации соответствующего доступа и необходимой безопасности создаём следующие ACL листы:

```
ip access-list extended dep4_in
permitip any host 192.168.1.2
permiticmp any any echo-reply
denyip any any
ip access-list extended dep1_in
permitip any host 192.168.1.2
permitip any 172.16.0.0 0.0.0.255
permitip any host 8.8.8.8
permiticmp any any echo-reply
denyip any any
ip access-list extended dep3_in
permitip any host 192.168.1.2
permitip any 172.16.0.0 0.0.0.255
permitip any host 8.8.8.8
permiticmp any any echo-reply
denyipanyany
```

Помимо этого, в ЛВС предусмотрен доступ к Ftp серверу извне. Для этого на роутере настраиваем NAT:

```
ipnat pool public_address 194.54.65.40 194.54.65.40 netmask 255.255.255.240
ipnat inside source list nat-list pool public_address overload
ipnat inside source static 192.168.1.2 194.54.65.42
```

После настройки локальной вычислительной сети нужно проверить её работоспособность.

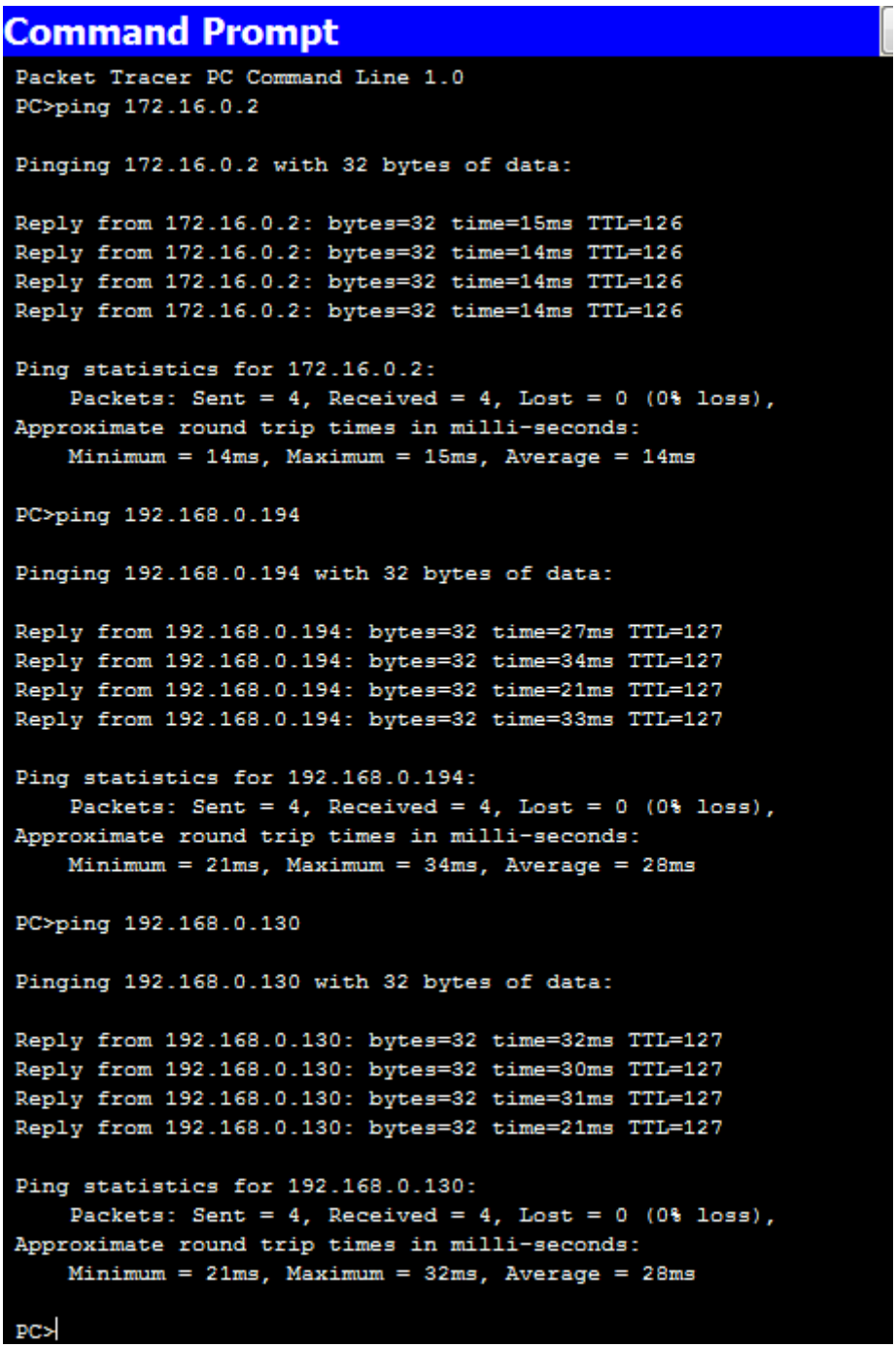

Рисунок 6 – Проверка работоспособности ЛВС

Из рисунка 6 мы видим, что спроектированная и настроенная нами локальная вычислительная сеть организации отлично работает.

В результате проделанной работы была построена ЛВС учреждения, удовлетворяющая всем заявленным требованиям. В состав сети входят 165 персональных компьютера и 1 сервер. Сеть работает по технологии IEEE 802.3u (FastEthernet).В процессе проектирования была заложена избыточность, для возможности расширения сети, подключения новых абонентов. Сеть организована по типу «звезда», так что все абоненты ЛВС имеют равный доступ к ресурсам сервера. Так как материалы, используемые при проектировании ЛВС, отвечают современным требованиям и являются

передовыми на рынке сетевых технологий, сеть останется актуальной продолжительное время.

Библиографический список

1. Новиков Ю.В. Локальные сети: Архитектура, алгоритмы, проектирование. М.: ЭКОМ, 2000. 312 с.
2. Одом У. Компьютерные сети. Первый шаг. М.: Вильямс, 2006.
3. Лещанкин К.А., Егунова А.И. Сети и телекоммуникации. Учебное пособие. Саранск, 2011.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. СПб., 2010. 484 с.