

МІНІСТЕРСТВО ОСВІТУ І НАУКИ УКРАЇНИ  
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ

ІНСТИТУТ КОМП'ЮТЕРНИХ СИСТЕМ

МАТЕРІАЛИ ДЕВ'ЯТОЇ  
МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ  
СТУДЕНТІВ ТА МОЛОДИХ ВЧЕНІХ



ПРИСВЯЧЕНА 55-РІЧЧЮ  
ІНСТИТУТУ КОМП'ЮТЕРНИХ СИСТЕМ

“Сучасні інформаційні технології 2019”

“Modern Information Technology 2019”



**NetCracker®**



23-24 травня

Одеса  
«Екологія»  
2019

УДК 004.77

**КОРПОРАТИВНАЯ СЕТЬ ОНПУ НА ОСНОВЕ ТЕХНОЛОГИЙ  
FAST ETHERNET, GIGABIT ETHERNET, FDDI**

Майборода В.О.

к. т. н., доцент Шапорин Р.О.

Одесский Национальный Политехнический Университет, УКРАИНА

**АННОТАЦИЯ.** Рассмотрена гибридная неоднородная ЛВС. Состоит из беспроводных и проводных сетей. Предложена стратегия улучшения сети за счет, изменения некоторых, основополагающих и высоконагруженных, узлов сети с Fast/ Gigabit Ethernet технологии на FDDI.

**Введение.** Технология[5] Fast Ethernet использует метод доступа CSMA/CD, такой же, как в технологии Ethernet, что обеспечивает согласованность технологий. Отличия Fast Ethernet от Ethernet наблюдаются только на физическом уровне. На канальном уровне изменений нет.

Технология Gigabit Ethernet

Поддержка полудуплексного режима метода доступа CSMA/CD сокращает диаметр сети до 25 м. Для увеличения диаметра сети до 200 м разработчики изменили размер минимального кадра с 64 до 512 байт. Для сокращения накладных расходов по передаче длинных кадров стандарт разрешает передавать несколько кадров подряд, не дополняя их до 512 байт и не передавая доступ к среде другому узлу.

Технология FDDI

Сеть[6] FDDI состоит из двух колец для повышения отказоустойчивости. Данные передаются по первичному кольцу сети в одном направлении, по вторичному кольцу - в противоположном. В обычном режиме используется только первичное кольцо. В случае отказа, когда часть первичного кольца не может передавать данные (например, обрыв кабеля или отказ узла), происходит процесс сворачивания колец, при котором первичное кольцо объединяется с вторичным, образуя новое кольцо. Сеть FDDI поддерживает скорость 100 Мбит/с. Диаметр сети - 100 км. Макс количество узлов - 500.

Wi-Fi является источником повышенного риска несанкционированного доступа. Проникнуть в беспроводную сеть значительно проще, чем в обычную, — не нужно подключаться к проводам, достаточно оказаться в зоне приема сигнала.

В защите Wi-Fi сетей применяются сложные алгоритмические и математические модели аутентификации и шифрования данных, контроля целостности их передачи, тем не менее, вероятность доступа к информации посторонних лиц является весьма существенной.

**Цель работы.**

1. Проектирование корпоративной сети для ОНПУ с использованием двух технологий
  - a. Спроектировать сеть на основе технологий Fast/ Gigabit Ethernet;
  - b. Определить высоконагруженные узлы и узлы, которые могут повлиять на отказоустойчивость, после чего перепроектировать вышеуказанные узлы при помощи технологии FDDI;
  - c. Убедится, что смена технологии не повлияет в худшую сторону на пропускную способность.
2. Обеспечение защиты беспроводной и проводной сети;
3. Обеспечить отказоустойчивость системы.

Основная часть работы.

Данная сеть гибридная, предполагает подключение, как по проводу, так и по WI-Fi. Обеспечивает взаимодействие стационарных ЭВМ и другой устройств при помощи доменной сети. Данные устройства подключаются по кабелю. Данное решение дает возможность гибкой настройки сети. Неоднородность сети обоснована возможностью подключения телефонов, планшетов, возможно IP-телефония и так далее.

Виртуализация ЛВС [1] являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы, несмотря на их физическое размещение в сети. Стоит заметить, что при использовании виртуальных локальных сетей уже не требуется подключать пользователей одного отдела к отдельному коммутатору. Данное решение даст возможность сократить количество используемых устройств и кабелей.

Для данного решения необходимо наличие коммутатор, программное обеспечение которого поддерживает функцию виртуальных локальных сетей, позволяет выполнять логическую сегментацию сети путем соответствующей программной настройки. Это дает возможность подключать пользователей, находящихся в разных сегментах, к одному коммутатору, а также сокращает количество необходимых физических интерфейсов на маршрутизаторе.

Интеллектуальная система управления сетью с использованием SNMP протокола[2]. В процессе функционирования сети возникает необходимость определить определенные параметры некоторого устройства, такие как, например, размер MTU (максимальный объём данных, который может быть передан протоколом за одну итерацию), количество принятых пакетов, открытые порты, установленную на машине операционную систему и ее версию и многое другое. Для осуществления этого как нельзя лучше подходят SNMP клиенты. Данное решение предоставляет возможность мониторинга всей сети и предотвращения возможных неполадок в сети и их своевременного устранения.

Бесшовный Wi-Fi. Контроллер, который своевременно "направляет" на ваше устройство сигнал с наиболее близко расположенной точки доступа. Данная сеть получила применение только как сеть общего пользования студентами и персоналом.

Защита беспроводной сети [4] обеспечивается трехфакторной аутентификацией: подтверждение MAC-адреса устройства, пароля от своего профиля и наличие устройства, с которого совершается подключение на территории покрытия Wi-Fi сети либо подключение к проводной сети.

**Выводы.** Данная модель ЛВС актуальна не только для университетов, школ, училищ, но и для крупных частных предприятий. Сеть предусматривает возможное развитие и увеличение вычислительных мощностей, высокую отказоустойчивость. Автоматизация сети обеспечивает: гибкую настройку под каждый из видов задач конечного пользователя, простоту в обслуживании благодаря возможности быстрого обнаружения неполадок и их скорой ликвидации, высокий уровень защиты сети. FDDI технология позволит в случае неполадки сегмента сети продолжать ее работоспособность, не смотря на неполадку одного из колец сети.

### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Виртуальные локальные сети [Электронной ресурс]. – Режим доступа: URL: <https://www.osp.ru/lan/2002/12/136942/>
2. SNMP протокол – принципы, безопасность, применение [Электронной ресурс]. – Режим доступа: URL: <http://www.codenet.ru/webmast/snmp/>
3. Биячурев Т.А. / под ред. Л. Г. Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.
4. Защита информационных в компьютерных сетях. /В. Ф. Шангин. Москва: ДМК Пресс, 2012. – 592с.: ил.
5. Качество обслуживания в сетях IP.; Пер. с англ. – М. ; Издательский дом «Вильямс», 2003. – 368 с. ; ил. – Парал. Тит. Англ.
6. Вишневецкий В.М. / Теоретические основы проектирования компьютерных сетей.; Москва: Техносфера, 2003, - 512с.