

## **ПРОЕКТИРОВАНИЕ КОРПОРАТИВНОЙ ИНФОКОММУНИКАЦИОННОЙ СЕТИ**

***Аннотация:** Целью данной статьи является описание разработки локальной вычислительной сети учреждения. Сеть должна соответствовать стандартам и всем заявленным в условии требованиям.*

***Ключевые слова:** Вычислительная сеть, топология сети, архитектура сети.*

***Annotation:** The purpose of this article is to describe the development of the local computer network of the institution. The network must comply with the standards and all the requirements stated in the condition..*

***Key words:** Computing network, network topology, network architecture.*

Проектируемая локальная вычислительная сеть разрабатывается с целью создания необходимых условий для работы организации среднего размера. 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 и строится локальная вычислительная сеть учреждения.

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.

В качестве технологии доступа используется Fast Ethernet, 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/с при использовании 2 пар. Кабель этой категории является самым распространённым и используется для построения компьютерных сетей. Его преимущества в более низкой себестоимости и меньшей толщине.

В работе для построения подсетей организации используется технология VLAN. 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 непроизводительного использования CPU за счет сокращения пересылки широковещательных сообщений;
- предотвращение широковещательных штормов и предотвращение потерь.

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 замедления 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 БД 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.

Ниже рассматриваются базовые методы мониторинга работы сети и контроля ее защищенности.

Сеть работает по технологии IEEE 802.3u (Fast Ethernet).

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.

#### **Использованные источники:**

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. – 3-е издание, Санкт-Петербург, 2010. – 484 с.
2. «Локальные сети: Архитектура, алгоритмы, проектирование» Новиков Ю. В. – М.: Издательство ЭКОМ, 2000. – 312 с.
3. Уендел Одом. Компьютерные сети. Первый шаг: М. : Издательский - дом "Вильяме", 2006.