

Л.Н. Васильева, И.И. Ильина

(г. Чебоксары, Чувашский государственный университет им. И.Н. Ульянова)

L.N. Vasilieva, I.I. Ilyina (Cheboksary, Chuvash State University
named after I.N. Ulyanova)

МОДЕЛИРОВАНИЕ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ НА ОСНОВЕ ПЛАТФОРМЫ CISCO PACKET TRACER

MODELING INFOCOMMUNICATION NETWORKS BASED ON THE CISCO PACKET TRACER PLATFORM

В статье рассмотрен симулятор визуального инструмента сетевого моделирования Cisco Packet Tracer, а также пример его применения в качестве среды для моделирования сетей, обнаружения и устранения неисправностей.

This article discusses the Cisco Packet Tracer simulator of a visual network modeling tool, as well as an example of its application as a medium for network modeling, troubleshooting and troubleshooting.

Ключевые слова: инфокоммуникационная сеть, компьютерная сеть предприятия, Cisco Packet Tracer, vlan, NAT.

Keywords: infocommunication network; computer network of the enterprise; Cisco Packet Tracer, vlan, NAT.

В настоящее время симуляция становится все более актуальной темой, наряду с применением методов моделирования. Для облегчения процесса обучения студентов проектированию сетей и систем связи можно использовать визуальные инструменты. Cisco Packet Tracer - инновационный и мощный инструмент сетевого моделирования, используемый для практики, обнаружения и устранения неисправностей. Это программное обеспечение предоставляет широкий спектр сетевых устройств, таких как коммутаторы и маршрутизаторы Cisco, работающие на IOS 12 и IOS 15, беспроводные устройства от Linksys, конечные устройства, такие как персональные компьютеры и серверы с командной строкой.

Cisco Packet Tracer больше, чем просто симулятор, он обеспечивает моделирование сетей, а также позволяет осуществлять эксперименты с поведением сети и оценивать возможные сценарии развития событий. Предоставленное симулятором физическое рабочее пространство можно использовать для определения ассортимента устройств.

Программное обеспечение Cisco Packet Tracer имеет дружелюбный пользовательский интерфейс: позволяет эмулировать и изучать основные процессы функционирования реальных компьютерных сетей [1], моделировать некоторые атаки и типичные угрозы безопасности компьютерных сетей [2], [3]. При этом отсутствует необходимость использования дорогостоящих устройств реального сетевого оборудования и программного обеспечения.

Рассмотрим задачу проектирования и разработки безопасной корпоративной сети (рис 1), выполняемой студентами в рамках расчетно-графической работы.

Корпоративная сеть предприятия состоит из информационных систем и каналов связи и является вариантом сотрудничества людей и компьютеров, обеспечивающих скорость доставки и обработки данных.

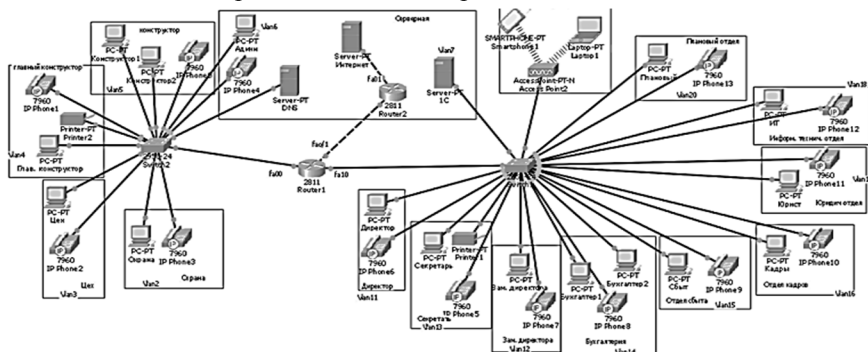


Рис. 1 Общая схема сети

Для проектирования сети использована технология VLAN (рис 2). Взаимодействие узлов настроено таким образом, что оно не зависит от их физического места локации. К данной сети были применены меры защиты информации как передаваемых, так и получаемых пакетов данных.

Технология преобразования сетевых адресов NAT позволяет преобразовать IP-адреса транзитных пакетов. С помощью данной технологии возможно скрыть внутреннюю структуру корпоративной сети, также она позволяет использовать один IP-адрес для доступа в Интернет с нескольких конечных устройств.

Одним из механизмов, позволяющих поддерживать сетевую безопасность, является список управления доступом Access control list, на основании которого назначаются правила доступа потока пакетов внутри сети.

На основе использования среды Cisco Packet Tracer обучающие могут спроектировать защищенную корпоративную сеть с помощью настроек VLAN, маршрутизации и NAT протокола. Платформа Cisco позволяет студентам наглядно изучить процессы функционирования сетевых устройств.



Рис. 2. Просмотр информации о VLAN на коммутаторе

Список литературы

1. Ремнев, П.Ю. Проектирование защищенной сети предприятия / П.Ю. Ремнев, Л.Н. Васильева // Информационные технологии в электротехнике и электроэнергетике: материалы XI Всерос. науч.-техн. конф. – Чебоксары: Изд-во Чуваш. ун-та – 2018. – С. 494-496.
2. Чумаров, С.Г. Моделирование угроз для сетей IP-телефонии/ С.Г. Чумаров, Г.В. Сидоров // Информационные технологии в электротехнике и электроэнергетике: материалы XI Всерос. науч.-техн. конф. – Чебоксары: Изд-во Чуваш. ун-та. – 2018. – С. 491-494.
3. Чумаров, С.Г. Информационная безопасность сетей IP-телефонии в образовательной среде // Современный университет в цифровой образовательной среде: ориентиры на опережающее развитие: материалы X Междунар. учеб.-метод. конф. – Чебоксары, 2018. – С. 41-45.