МИШИН Д.В., ЩЕРБИН П.В.

ЛАБОРАТОРНАЯ УСТАНОВКА ДЛЯ ИССЛЕДОВАНИЯ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК КОРПОРАТИВНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Владимирский государственный университет им. А.Г. и Н.Г. Столетовых

В процессе исследования функциональных характеристик корпоративных сетей передачи данных (КСПД) исследователь сталкивается с необходимостью моделирования процессов исследуемой КСПД предприятия в лабораторных условиях (проведение натурных экспериментов требует значительных финансовых и технических ресурсов).

Под КСПД мы будем понимать распределенную техническую инфраструктуру, представляющую собой организованную совокупность структурных элементов (СЭ) - оконечных узлов, телекоммуникационного оборудования и каналов электросвязи [5,6]. КСПД объединяет множество сегментов ЛВС (филиалов, офисов) в мультисервисную гетерогенную сеть, предназначенную для предоставления единого защищенного сетевого пространства ограниченному рамками предприятия кругу пользователей и предоставляющую прикладные сервисы (FTP, Web, SMB, SMTP, POP3, Proxy и т.д.). Структуру КСПД представим в виде схемы (рисунок 1):

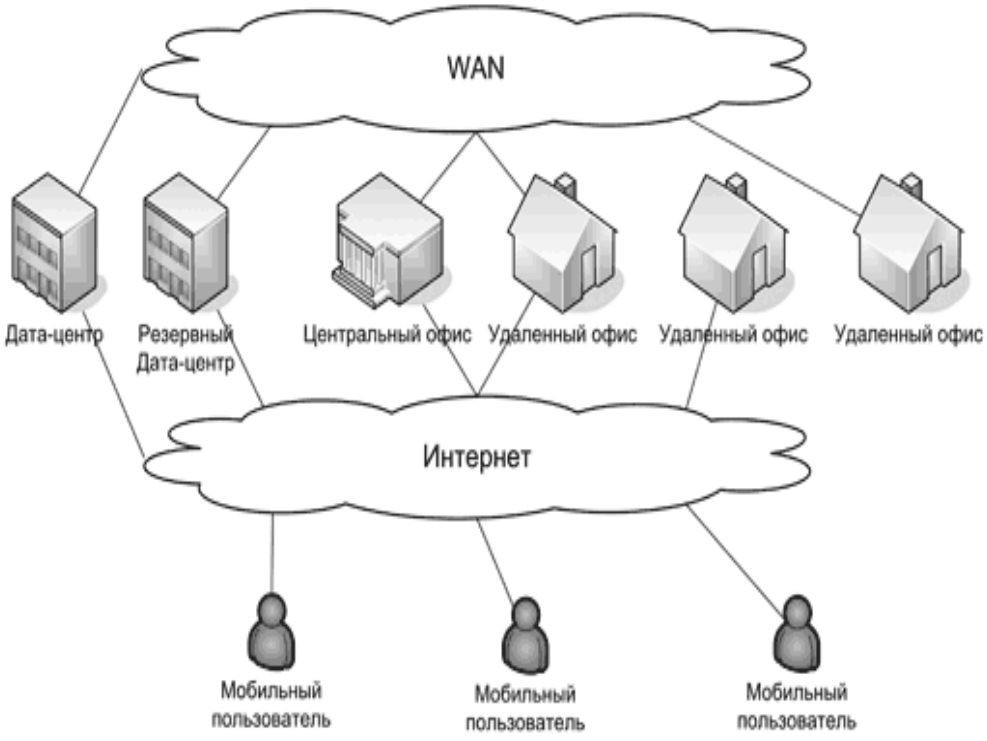

Рис. 1. – Структура КСПД

Среди множества решений реализующих экспериментальную установку (ЭУ), авторами выбрано решение на основе виртуализации, как наименее затратное. В докладе описывается экспериментальная установка по исследованию функциональных характеристик КСПД на основе продукта Graphical Network Simulator 3 (GNS3).

На основе имеющейся сети лаборатории (схема ее представлена на рисунке 2) необходимо построить сеть, схема которой представлена на рисунке 3.

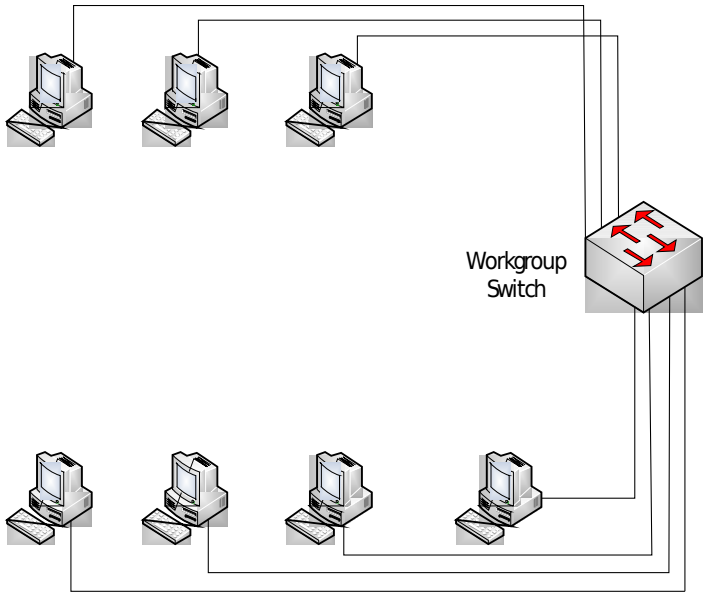

Рис.2. – Схема ЛВС лаборатории

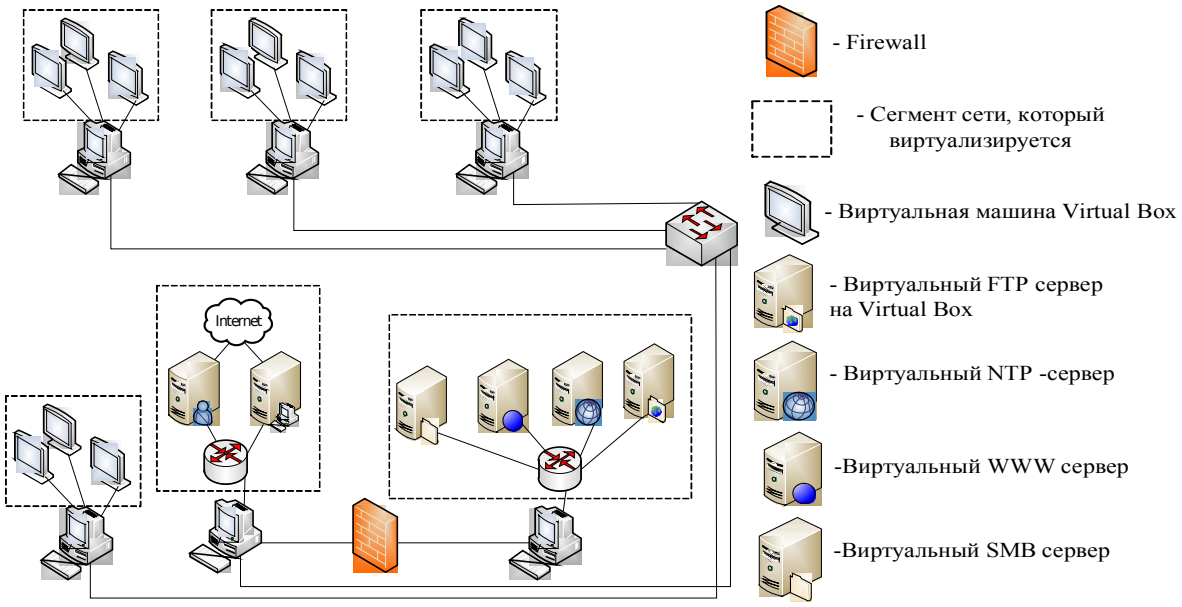

Рис. 3. – Схема лабораторной установки КСПД

Лабораторная установка состоит из четырех основных компонентов: два персональных компьютера (ПК) моделирующих сервера (ПК – виртуальные сервер удаленного доступа SSH и VPN; ПК – виртуальные FTP, NTP, WWW, SMB сервера), одного ПК – файрволла и остальных ПК - конечных рабочих станций. Компоненты подключаются друг к другу через реальный коммутатор, а также при помощи соединительных кабелей. Роль серверов и конечных узлов выполняют виртуальные машины на основе системы управления виртуальными машинами (СУВМ) VirtualBox, файрволл построен на базе Iptables, сервера связаны между собой через виртуальные маршрутизаторы Cisco, которые созданы в GNS3.

На обоих виртуальных маршрутизаторах настраивается механизм преобразования адресов – NAT. На центральном устройстве, к которому подключаются серверы удаленного доступа, конфигурируется система сбора статистической информации о трафике NetFlow. Netflow — протокол 5 (сеансового) уровня сетевой модели OSI, разработанный компанией Cisco и предназначенный для сбора информации об IP-трафике внутри сети. Данная технология поможет в процессе исследования процессов и функциональных характеристик КСПД.

NAT необходимо настроить, так как реально существующая КСПД состоит из нескольких подсетей, а значит в лабораторной установке они также должны быть. Собранная модель КСПД представляет собой следующие подсети (Рисунок 4):

- 192.168.56.2 – 192.168.56.6 – внутренний адрес маршрутизатора и адреса виртуальных серверов
- 192.168.0.1 - 192.168.0.3 – адреса двух реальных ПК и внешний адрес маршрутизатора;
- 192.168.1.1-192.168.1.3 – адреса двух реальных ПК и внешний адрес маршрутизатора;
- 192.168.2.1 – 192.168.2.65 – внутренний адрес маршрутизатора и адреса конечных виртуальных машин.

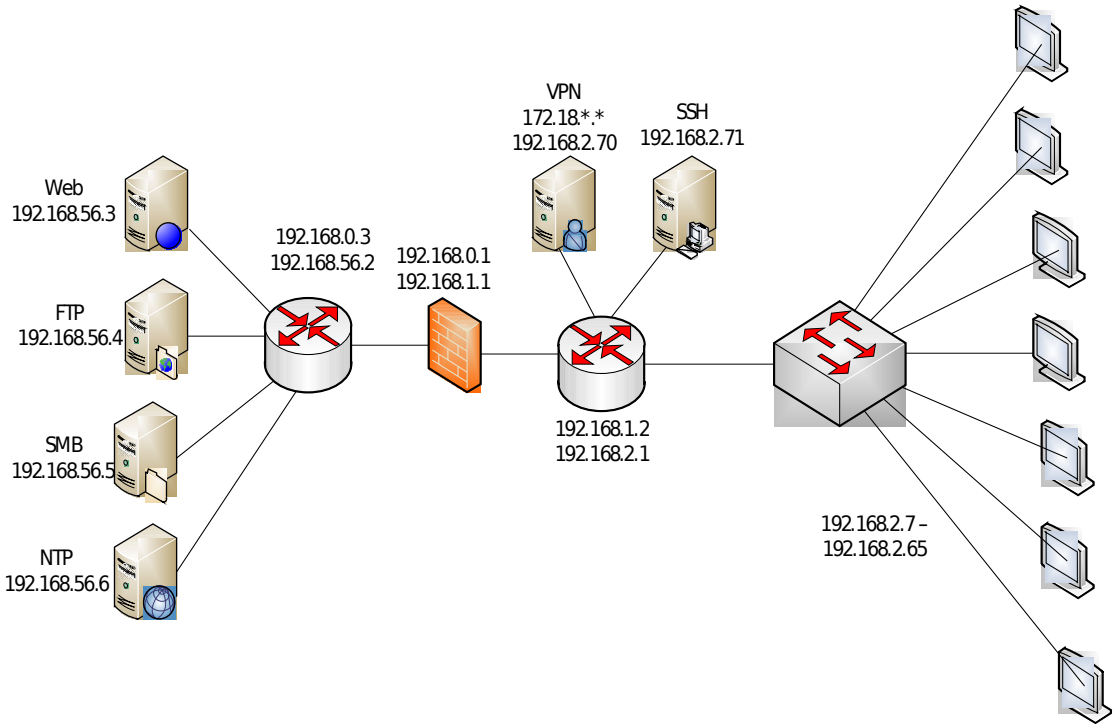

Рис. 4. – Схема лабораторной установки КСПД

Конфигурирование GNS3: Graphical Network Simulator сводится к указанию двух путей к файлам: путь и выбор образа, используемого для сетевых устройств (это образ специальной операционной системы маршрутизаторов – Cisco IOS) и путь к программе – эмулятору Dynamips.

Следующим шагом будет расстановка в рабочей области программы 3 элементов: маршрутизатор и двух «облаков» сетевых интерфейсов. Все это осуществляется при помощи Drag&Drop. Каждое «облако» это своеобразный сетевой мост между интерфейсом сетевого устройства и реальным сетевым подключением ПК.

Маршрутизатор, который подключается к серверам, настраивается таким образом, что внешний интерфейс подключается к сетевой карте ПК, а внутренний к «виртуальному» подключению, созданному VirtualBox.

Таким образом, с помощью GNS3: Graphical Network Simulator удалось создать сложные по топологии сети и объединять реальную сеть с виртуальным оборудованием, которое полностью как программно, так и аппаратно виртуализируется. Стоит также отметить, что необходимо использовать максимально эффективно имеющиеся вычислительные

ресурсы. Поэтому было принято решение о установке минимальной операционной системы (ОС) Ubuntu Server на ПК, которые виртуализируют конечные рабочие станции. Данная ОС не имеет графического интерфейса и управляется только из режима командной строки, а так как VirtualBox работает в графическом режиме при установке данного программного продукта требуется установить множества зависимых пакетов. Но ОС по прежнему будет работать только с командной строкой. Для управления VirtualBox надо инсталлировать Web сервер Apache2 с поддержкой языка PHP и два специальных модуля: vboxwebsrv и phpvirtualbox. После этого будет достаточно запустить команду вида: /usr/bin/vboxwebsrv -b --logfile /dev/null >/dev/null. Данная команда запустит web интерфейс, к которому мы можем подключиться из любого браузера. В установке для подключения к виртуальным машинам применяется SSH доступ.

На каждую виртуальную машину установлен следующий набор программного обеспечения: Debian, hping3, nmap, lynx, wget, mc, ssh. ОС Debian установлена в минимальном виде без графического интерфейса.

Выше было сказано про применение технологии NetFlow. Она заключается в том, что сетевое оборудование, в нашем случае маршрутизатор, собирает информацию о трафике с определенного интерфейса и затем через определенный промежуток времени отсылает его на компьютер-коллектор.

На данном ПК установлены две специальные программы: сенсор и коллектор. Сенсор собирает статистическую информацию, присланную с определенного сетевого интерфейса, в файлы. Коллектор же представляет собой набор утилит, которые позволяют проанализировать статистику и создать отчет.

Наиболее распространенными являются fprobe – сенсор и набор утилит flow-tools. Настройки анализа и составления отчета выполняются в виде текстовых конфигурационных файлов. Существует множество опций и видов отчетов. Приведем список некоторых из них.

Таблица 1. – Список опций

first	Время начала потока в UNIX time
last	Время конца потока в UNIX time
flows	Общее число потоков
octets	Общее число байтов
packets	Общее число пакетов
duration	Время конца потока-Время начала потока
avg-bps	Средняя пропускная способность Бит/Сек
min-bps	Минимальная пропускная способность Бит/Сек
max-bps	Максимальная пропускная способность Бит/Сек
avg-pps	Средняя пропускная способность Пакет/Сек
min-pps	Минимальная пропускная способность Пакет/Сек
max-pps	Максимальная пропускная способность Пакет/Сек

Отчеты создаются в виде html страницы с таблицей, столбцы которой и изменяются в зависимости от опций и вида отчета.

Таким образом, создав лабораторную установку и применив в ней технологию NetFlow, можно изучать процессы функционирования, взаимодействия серверов и клиентов, исследовать устойчивость, живучесть и надежность КСПД.

Таблица.2. – Виды отчетов

summary-detail	Общий отчет
packet-size	Средний размер пакета
octets	Байты
packets	Пакеты
ip-source/destination-port	Порт источника /Порт получателя
bps	Пропускная способность Бит/Сек
pps	Пропускная способность Пакет/Сек
ip-protocol	Протокол(его номер в соответствии с /etc/protocols)
ip-source/destination-address	IP адреса источника/ IP адрес получателя
ip-exporter-address	IP адрес экспортера
input/output-interface	Входящий интерфейс/ Исходящий интерфейс
ip-source-address/input-interface	IP адреса источника/входящий интерфейс
ip-source-address/output-interface	IP адреса источника/исходящий интерфейс
ip-destination-address/output-interface	IP адрес получателя/исходящий интерфейс
ip-source/destination-address/input/output-interface	IP адреса источника/ IP адрес получателя / входящий интерфейс /исходящий интерфейс
ip-source/destination-address/ip-source/destination-port	IP адреса источника/ IP адреса получателя/Порт источника/Порт получателя
ip-source-address/input/output-interface	IP адреса источника /Входящий интерфейс/Исходящий интерфейс
ip-destination-address/input/output-interface	IP адреса получателя /Входящий интерфейс/Исходящий интерфейс
first	Время начала потока
last	Время конца потока
ip-source/destination-address/ip-protocol/ip-tos/ip-source/destination-port	IP адреса источника/ IP адреса получателя/IP протокол/IP сервис/ Порт источника/Порт получателя

Подход, описанный в статье, можно предложить в качестве типового для создания ЭУ исследования КСПД.

ЛИТЕРАТУРА

1. http://xgu.ru/wiki/Xentaur
2. http://www.gns3.net/
3. «HACKING EXPOSED 6: NETWORK SECURITY SECRETS & SOLUTIONS» *STUART MCCLURE, JOEL SCAMBRAY, GEORGE KURTZ*. ISBN: 978-0-07-161375-0. P – 655
4. http://citforum.ru/nets/articles/ent_network_services/
5. *Кульгин М.* Технологии корпоративных сетей/ Энциклопедия.- СПб.:Питер, 1999.- 704с.
6. *Олифер В.Г., Олифер Н.А.* Стратегическое планирование сетей масштаба предприятия.– М.: Центр Информационных Технологий, 2000. 680 с.

Сведения об авторах

Щербин Павел Владимирович
Владимирский Государственный Университет им. А.Г. и Н.Г. Столетовых
Студент
tur89106@yandex.ru

Мишин Денис Вячеславович
Владимирский Государственный Университет им. А.Г. и Н.Г. Столетовых, кафедра Информатики и Защиты Информации
Заведующий лабораториями, ассистент кафедры ИЗИ
mishin@izi.vlsu.ru