Лабораторная установка по исследованию функционирования корпоративных сетей передачи данных(КСПД)

Щербин П.В., группа КЗИ-106
Научный руководитель: Мишин Д.В.

Проблематика

Проблема:

Проведение натурных экспериментов требует наличия значительных финансовых и технических ресурсов, а это недопустимо при создании лабораторных установок(ЛУ).

Моделирование сопряжено с рядом трудностей связанных со сложностью топологии КСПД, большим числом структурных элементов (СЭ).

Задачи

Задачи:

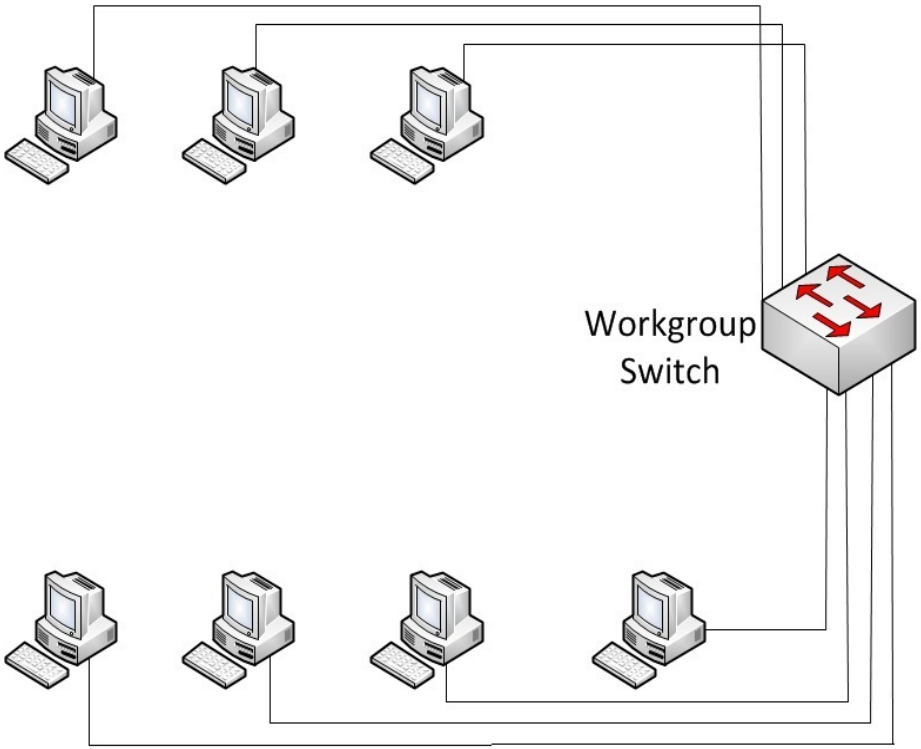
- *разработать схемы лабораторной установки(ЛУ);*
- *собрать ЛУ;*
- *развернуть систему сбора статистической информации о трафике;*
- *провести ряд экспериментов.*

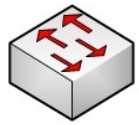
Определение

КСПД:

это распределенная техническая инфраструктура, представляющая собой организованную совокупность структурных элементов (СЭ) - оконечных узлов, телекоммуникационного оборудования и каналов электросвязи.

Схема ЛВС аудитории 427б-2




- Коммутатор Cisco Catalyst


- Рабочие станции (ПК)

Схема лабораторной установки

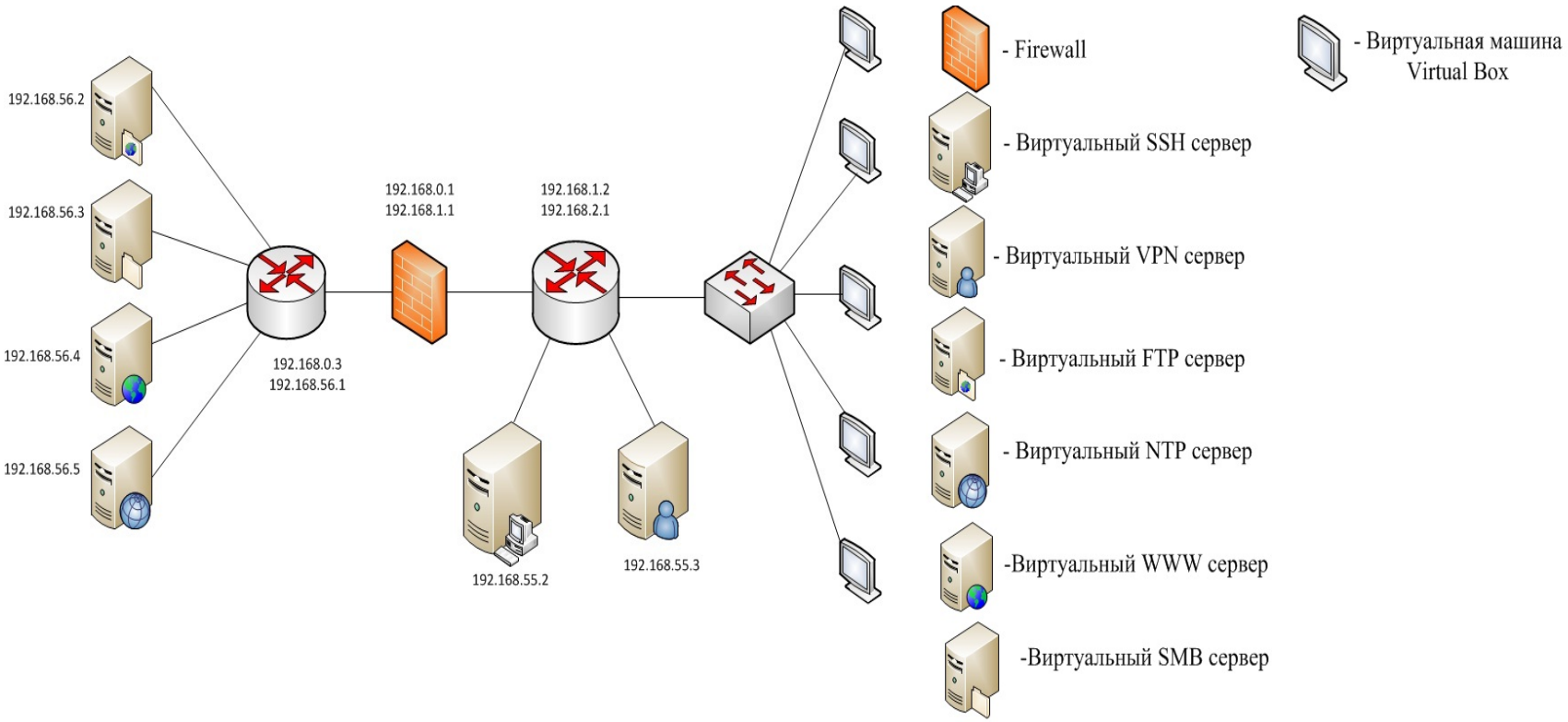
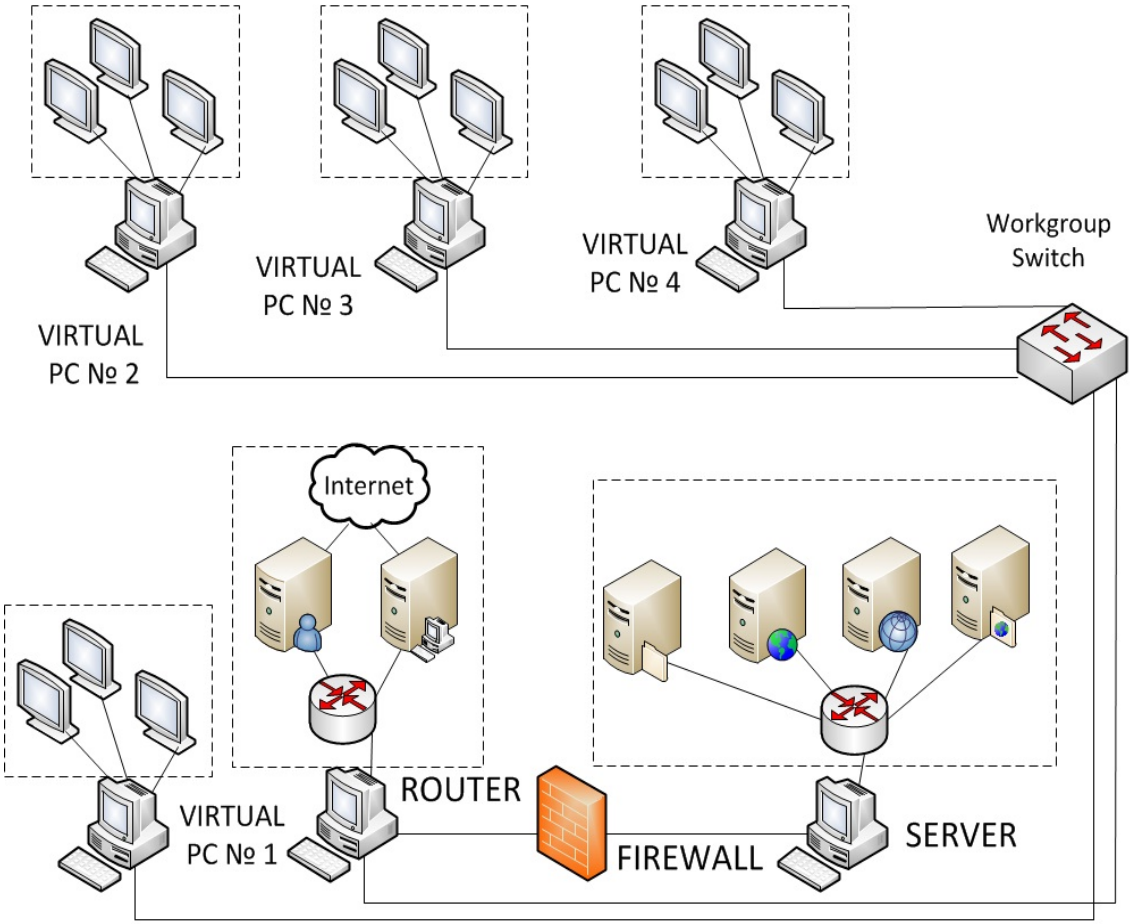


Схема лабораторной установки



- Firewall
- Сегмент сети, который виртуализируется
- Виртуальная машина Virtual Box
- Виртуальный FTP сервер
- Виртуальный NTP -сервер
- Виртуальный WWW сервер
- Виртуальный SMB сервер

Структурные элементы лабораторной установки:

Лабораторная установка состоит из четырех элементов:

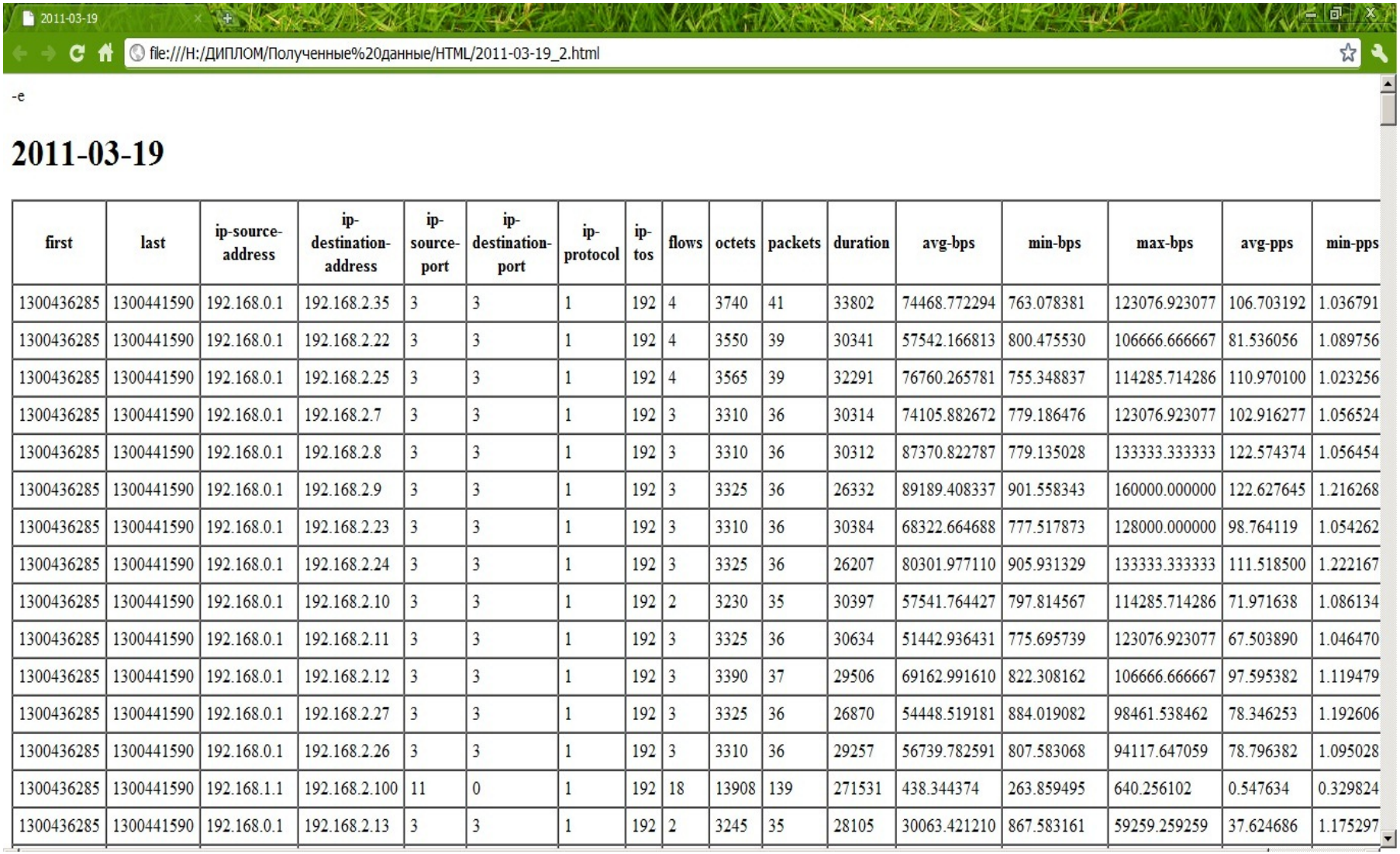
- ПК с именем «SERVER» – реализует маршрутизатор Cisco(GNS3) и подключенные к нему сервера на VirtualBox;
- ПК с именем «FIREWALL» – фаерволл на Iptables;
- ПК с именем «ROUTER» – маршрутизатор Cisco(GNS3) и сервера на VirtualBox;
- множество ПК с именами «VIRTUAL PC No» - реализуют оконечные узлы (рабочие станции).

Необходимые характеристики:

Характеристики,которые чаще всего нужны для различного рода исследований(экспериментов):

1. средний размер пакета;
2. средний размер потока;
3. среднее число пакетов в потоке;
4. среднее число потоков в секунду реального времени;
5. средний размер пакета в потоке;
6. время начала потока в ЮНИКС тайм;
7. время конца потока в ЮНИКС тайм;
8. общее число байтов(октетов);
9. общее число пакетов;
10. средняя пропускная способность Бит/Сек;
11. средняя пропускная способность Пакет/Сек;

Статистический отчет



2011-03-19

first	last	ip-source-address	ip-destination-address	ip-source-port	ip-destination-port	ip-protocol	ip-tos	flows	octets	packets	duration	avg-bps	min-bps	max-bps	avg-pps	min-pps
1300436285	1300441590	192.168.0.1	192.168.2.35	3	3	1	192	4	3740	41	33802	74468.772294	763.078381	123076.923077	106.703192	1.036791
1300436285	1300441590	192.168.0.1	192.168.2.22	3	3	1	192	4	3550	39	30341	57542.166813	800.475530	106666.666667	81.536056	1.089756
1300436285	1300441590	192.168.0.1	192.168.2.25	3	3	1	192	4	3565	39	32291	76760.265781	755.348837	114285.714286	110.970100	1.023256
1300436285	1300441590	192.168.0.1	192.168.2.7	3	3	1	192	3	3310	36	30314	74105.882672	779.186476	123076.923077	102.916277	1.056524
1300436285	1300441590	192.168.0.1	192.168.2.8	3	3	1	192	3	3310	36	30312	87370.822787	779.135028	133333.333333	122.574374	1.056454
1300436285	1300441590	192.168.0.1	192.168.2.9	3	3	1	192	3	3325	36	26332	89189.408337	901.558343	160000.000000	122.627645	1.216268
1300436285	1300441590	192.168.0.1	192.168.2.23	3	3	1	192	3	3310	36	30384	68322.664688	777.517873	128000.000000	98.764119	1.054262
1300436285	1300441590	192.168.0.1	192.168.2.24	3	3	1	192	3	3325	36	26207	80301.977110	905.931329	133333.333333	111.518500	1.222167
1300436285	1300441590	192.168.0.1	192.168.2.10	3	3	1	192	2	3230	35	30397	57541.764427	797.814567	114285.714286	71.971638	1.086134
1300436285	1300441590	192.168.0.1	192.168.2.11	3	3	1	192	3	3325	36	30634	51442.936431	775.695739	123076.923077	67.503890	1.046470
1300436285	1300441590	192.168.0.1	192.168.2.12	3	3	1	192	3	3390	37	29506	69162.991610	822.308162	106666.666667	97.595382	1.119479
1300436285	1300441590	192.168.0.1	192.168.2.27	3	3	1	192	3	3325	36	26870	54448.519181	884.019082	98461.538462	78.346253	1.192606
1300436285	1300441590	192.168.0.1	192.168.2.26	3	3	1	192	3	3310	36	29257	56739.782591	807.583068	94117.647059	78.796382	1.095028
1300436285	1300441590	192.168.1.1	192.168.2.100	11	0	1	192	18	13908	139	271531	438.344374	263.859495	640.256102	0.547634	0.329824
1300436285	1300441590	192.168.0.1	192.168.2.13	3	3	1	192	2	3245	35	28105	30063.421210	867.583161	59259.259259	37.624686	1.175297

Вывод

Вывод:

созданная ЛУ полностью соответствует требованиям, предъявляемых к КСПД, что позволяет проводить ряд экспериментов. На данной установке возможно проведение следующие опытов:

- *имитация пользовательской активности в КСПД (скачивание файла с WWW сервера, просмотр Web-страниц и тому подобное), сбор статистической информации о трафике и последующий анализ;*
- *изучение механизма несанкционированного доступа в КСПД;*
- *практическое испытание различных систем обнаружения вторжений;*
- *проведение различного рода атак на сервера.*

Инструменты

Инструменты:

- Graphical Network Simulator 3 -виртуализация сетевых устройств;
- модуль Apache2 - mod status - мониторинг сервера и его нагрузки;
- fprobe - программный сенсор NetFlow,flow-tools - программный коллектор;
- VirtualBox - виртуализация конечных рабочих станции;
- vboxwebsrv+phpvirtualbox - управление VirtualBox через Web интерфейс;
- ClusterSSH - управление конечными рабочими станциями через SSH;
- lynx - консольный браузер;
- hping3 - генерация пакетов;