ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СТЕРЛИТАМАКСКИЙ МНОГОПРОФИЛЬНЫЙ ПРОФЕССИОНАЛЬНЫЙ КОЛЛЕДЖ
(ГАПОУ СМПК)

КУРСОВАЯ РАБОТА

«МОДЕЛИРОВАНИЕ ЭТАПОВ АДМИНИСТРИРОВАНИЯ И НАСТРОЙКИ УДАЛЕННОГО ДОСТУПА К РЕСУРСАМ ЛОКАЛЬНОЙ СЕТИ»

Выполнил:
студент III курса группы ССА-39
специальности 09.02.06 Системное
и сетевое администрирование
Бойкив Михаил Орестович

Руководитель:
Шарафиев Ринат Расимович.

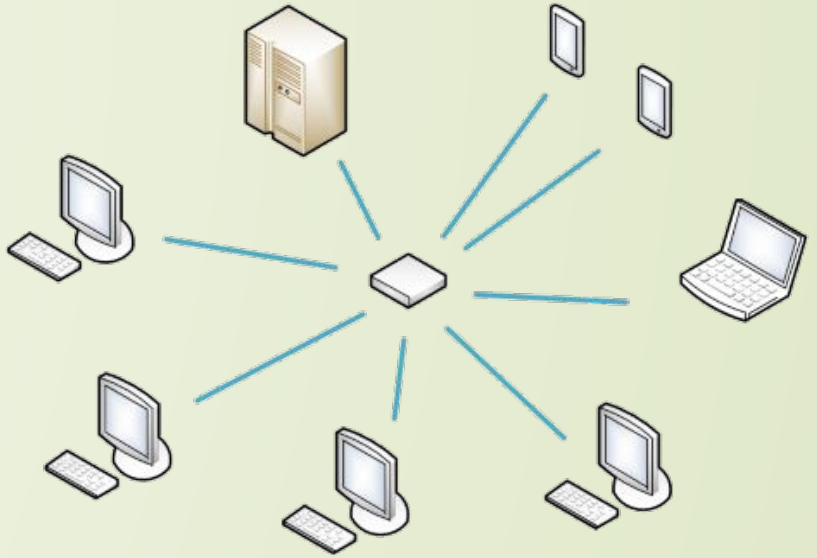
Стерлитамак, 2020

Цель проекта: смоделировать этапы настройки удаленного доступа средствами Windows Server 2016, а также Cisco IOS.

Задачи проекта:

- 1. Рассмотреть учебно-техническую литературу по теме курсовой работы.
- 2. Раскрыть понятие, назначение, а также некоторые принципы работы локальной сети, рассмотреть назначение удаленного доступа к ресурсам локальной сети.
- 3. Описать средства Windows Server 2016 и Cisco IOS для настройки удаленного доступа.
- 4. Смоделировать объекты сетевой инфраструктуры локальной сети.
- 5. Описать этапы моделирования настройки удаленного доступа средствами Windows Server 2016 и Cisco IOS.

Некоторые пояснения

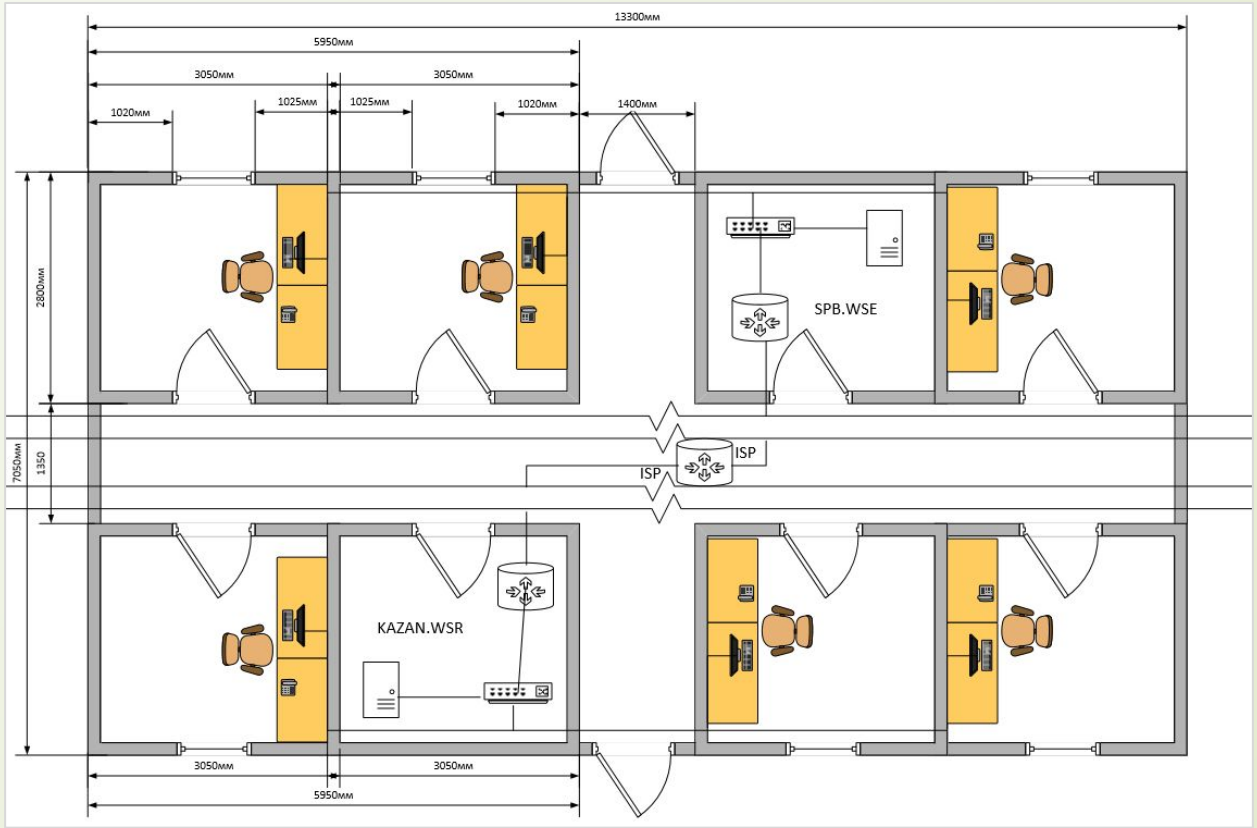


Ресурс локальной сети – это все, чем располагают объединенные в сеть компьютеры, то есть по сути это элементы сетевой инфраструктуры, а именно устройства: сетевые принтеры, сервера, коммутаторы, маршрутизаторы и другие.

Удалённый доступ — программы или функции операционных систем, позволяющие получить удалённый доступ к компьютеру через Интернет или посредством локальной вычислительной (ЛВС) сети для просмотра экрана, а также программы удалённого администрирования

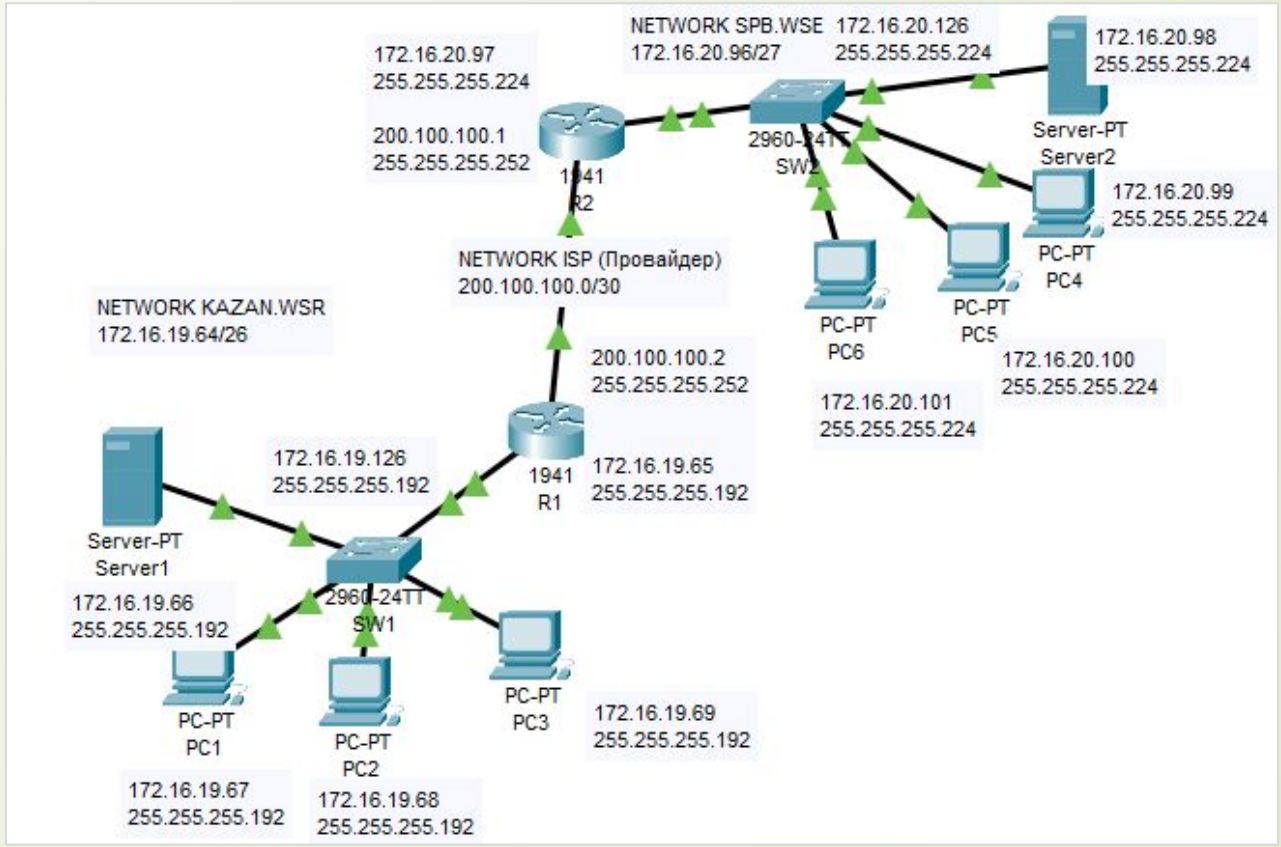
Проектирование локальной сети

Построена физическая топология локальной сети центрального офиса и его филиала



Проектирование локальной сети

Построена логическая топология локальной сети центрального офиса и его филиала



Проведение базовой настройки

Были настроены сетевые устройства некоторым списком команд, а также назначены IP-адреса на порты этих самых устройств в соответствии с таблицей адресации.

Устройство	Интерфейс	IP-адрес	Subnet mask (Маска подсети)	Основной шлюз
R1	G0/0	200.100.100.2	255.255.255.252	–
	G0/1	172.16.19.65	255.255.255.192	–
R2	G0/0	200.100.100.1	255.255.255.252	–
	G0/1	172.16.20.97	255.255.255.224	–
SW1	VLAN 1	172.16.19.126	255.255.255.192	172.16.19.65
SW2	VLAN 1	172.16.20.126	255.255.255.224	172.16.20.97
PC1	NIC	172.16.19.67	255.255.255.192	172.16.19.65
PC2	NIC	172.16.19.68	255.255.255.192	172.16.19.65
PC3	NIC	172.16.19.69	255.255.255.192	172.16.19.65
PC4	NIC	172.16.20.99	255.255.255.224	172.16.20.97
PC5	NIC	172.16.20.100	255.255.255.224	172.16.20.97
PC6	NIC	172.16.20.101	255.255.255.224	172.16.20.97
Server1	NIC	172.16.19.66	255.255.255.192	172.16.19.65
Server2	NIC	172.16.20.98	255.255.255.224	172.16.20.97

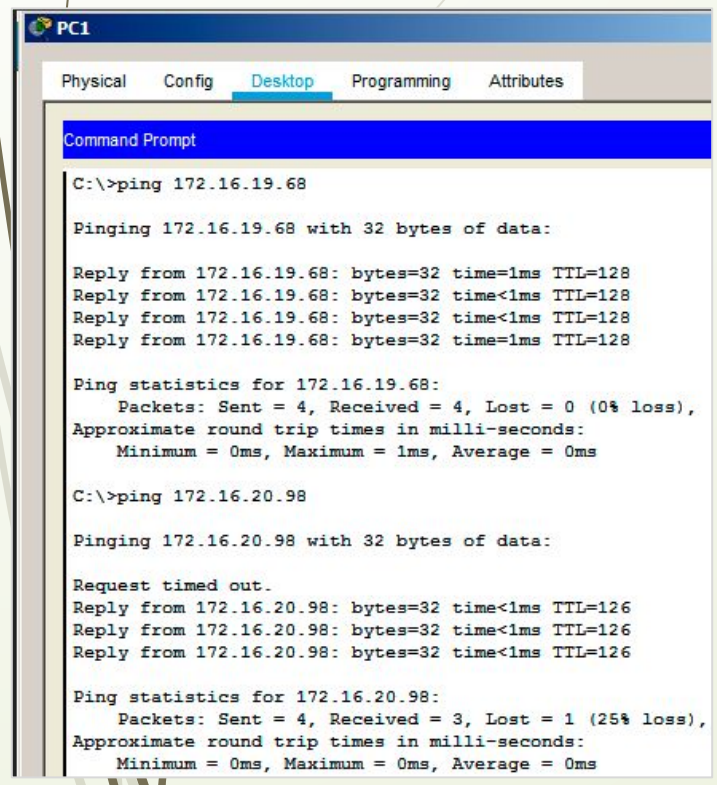
Таблица адресации устройств

```
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#service password-encryption
R1(config)#enable secret class
R1(config)#banner motd # Unauthorized access is strictly prohibited. #
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#int g0/1
R1(config-if)#ip address 172.16.19.65 255.255.255.192
R1(config-if)#no sh
R1(config-if)#int g0/0
R1(config-if)#ip address 200.100.100.2 255.255.255.252
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 g0/0
```

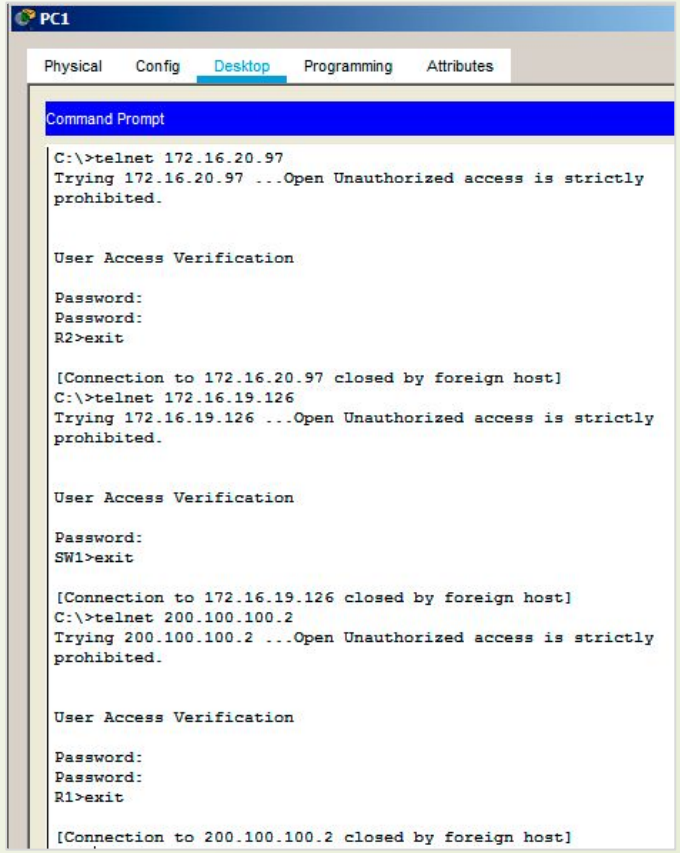
Команды базовой настройки на примере R1

Проведение базовой настройки

После проведенных манипуляций по базовой настройки должны успешно отправляться эхо-запросы (ping) и должен быть рабочий telnet.



Успешные эхо-запросы ко всем устройствам в сети



Установленный telnet на всех промежуточных устройствах в сети

Switch(config)#hostname SW1

SW1(config)#no ip domain-lookup

SW1(config)#service password-encryption

SW1(config)#enable secret class

SW1(config)#banner motd # Unauthorized access is strictly prohibited. #

SW1(config)#line con 0

SW1(config-line)#password cisco

SW1(config-line)#login

SW1(config-line)#logging synchronous

SW1(config-line)#line vty 0 15

SW1(config-line)#password cisco

SW1(config-line)#login

SW1(config-line)#exit

SW1(config)#int vlan 1

SW1(config-if)#ip address 172.16.19.126 255.255.255.192

SW1(config-if)#no sh

SW1(config-if)#exit

SW1(config)#ip default-gateway 172.16.19.65

Команды базовой настройки коммутатора на примере SW1

Настройка SSH на сетевом оборудовании Cisco

```
R2#enable
R2#clock set 11:34:23 14 Jun 2020
R2#conf t
R2(config)#ip domain name spb.wse
R2(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
R2(config)#username admin privilege 15 secret Pa$$w0rd
R2(config)#aaa new-model
R2(config)#ip ssh version 2
R2(config)#line vty 0 4
R2(config-line)#transport input ssh
R2(config-line)#logging synchronous
R2(config-line)#privilege level 15
R2(config-line)#exec-timeout 60 0
R2(config-line)#exit
R2(config)#exit
R2#copy run start
```

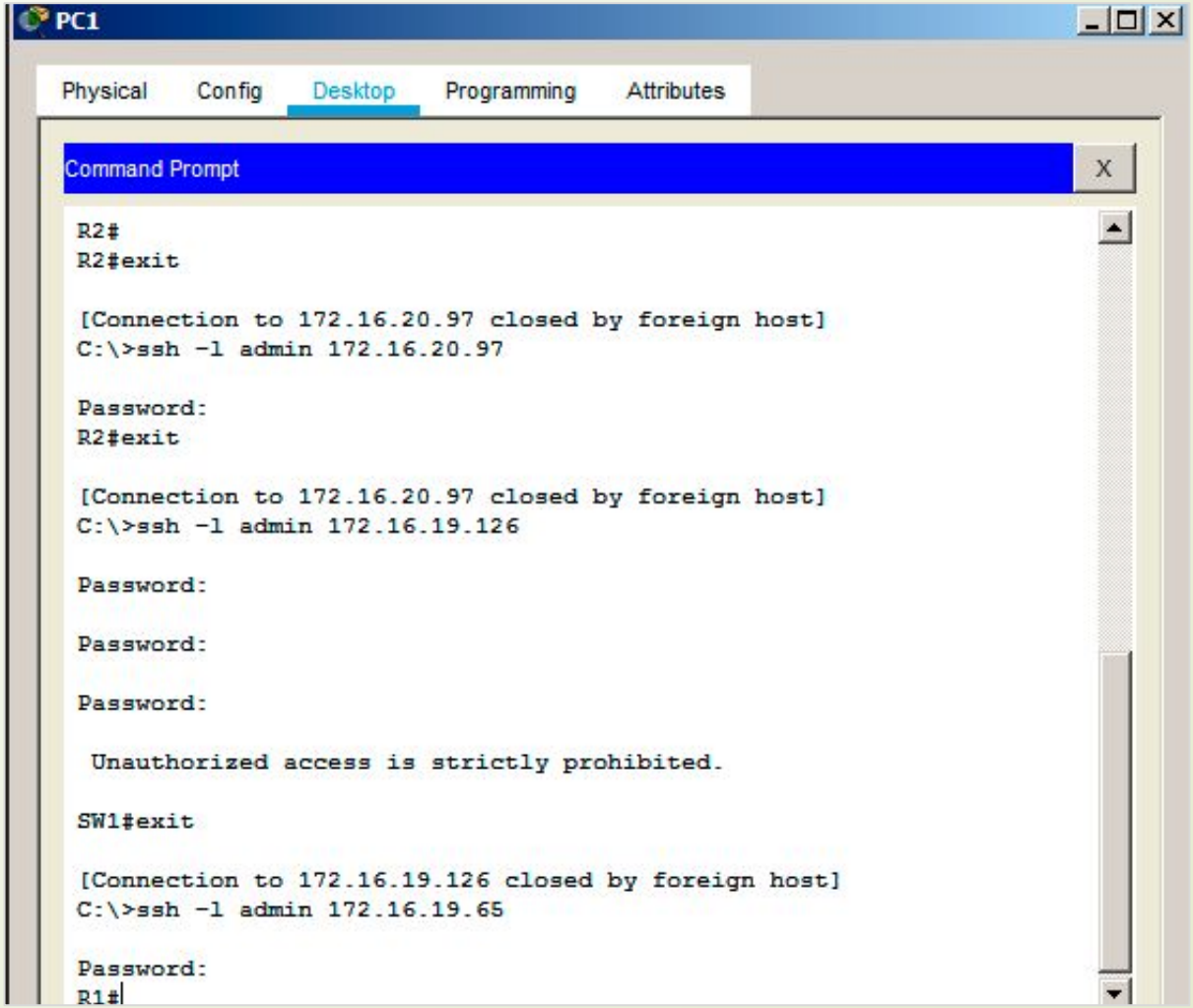
Команды для настройки SSH на примере R2

```
SW2#enable
SW2#clock set 11:34:43 14 Jun 2020
SW2#conf t
SW2(config)#ip domain name spb.wse
SW2(config)#hostname SW2
SW2(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
SW2(config)#username admin privilege 15 secret Pa$$w0rd
SW2(config)#ip ssh version 2
SW2(config)#line vty 0 4
SW2(config-line)#transport input ssh
SW2(config-line)#logging synchronous
SW2(config-line)#privilege level 15
SW2(config-line)#exec-timeout 60 0
SW2(config-line)#exit
SW2(config)#exit
SW2#copy run start
```

Команды для настройки SSH на примере SW2

Настройка SSH на сетевом оборудовании Cisco

Подключение по SSH с PC1 к SW1 и R2, для демонстрации правильной настройки SSH



Настройка удалённого доступа в среде Windows

Для начала необходимо создать модель сети Сервер–Клиент в среде виртуализации Vmware Workstation. После создания виртуальных машин на ПК сервера необходимо установить Windows Server 2016, а на ПК клиентов Windows 10. Далее идёт проведение базовой настройки оборудования, куда входит:

- Назначение IP-адресов на сетевые адаптеры.
- Переименование ПК.
- Настройка FireWall для прохождения ICMPv4 трафика.

Device	Summary
Memory	8 GB
Processors	4
Hard Disk (SCSI)	20 GB
Network Adapter	Custom (VMnet12)
USB Controller	Present
Display	Auto detect

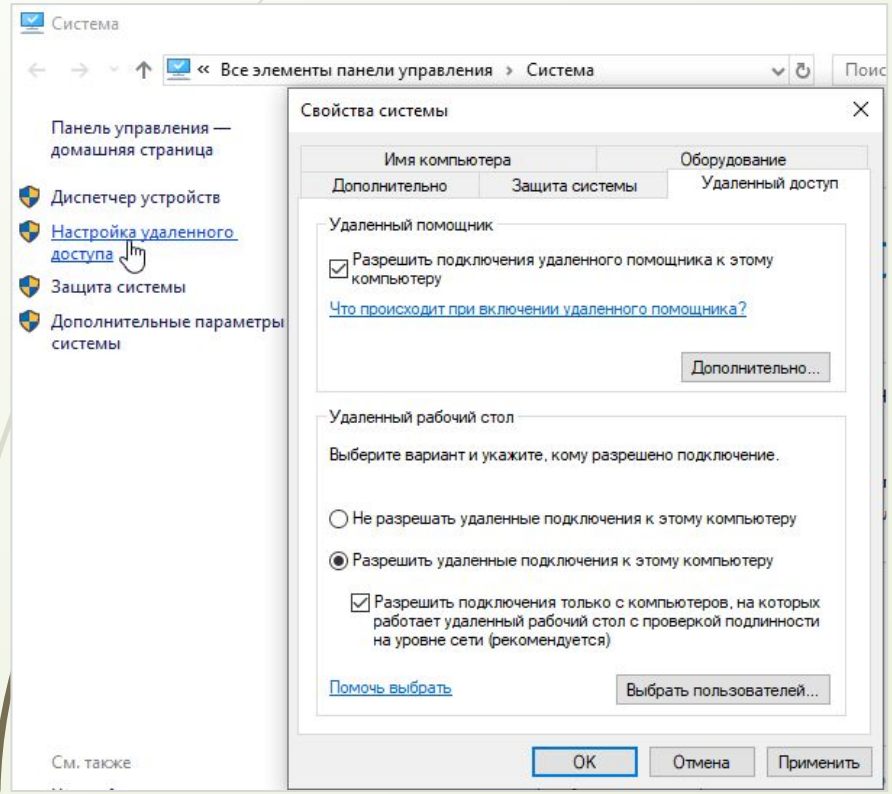
Технические характеристики сервера

Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	20 GB
Network Adapter	Custom (VMnet12)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Технические характеристики клиентских компьютеров

Настройка удалённого доступа в среде Windows

После этого необходимо произвести включение протокола RDP, чтобы к тому или иному устройству можно было подключиться удалённо.

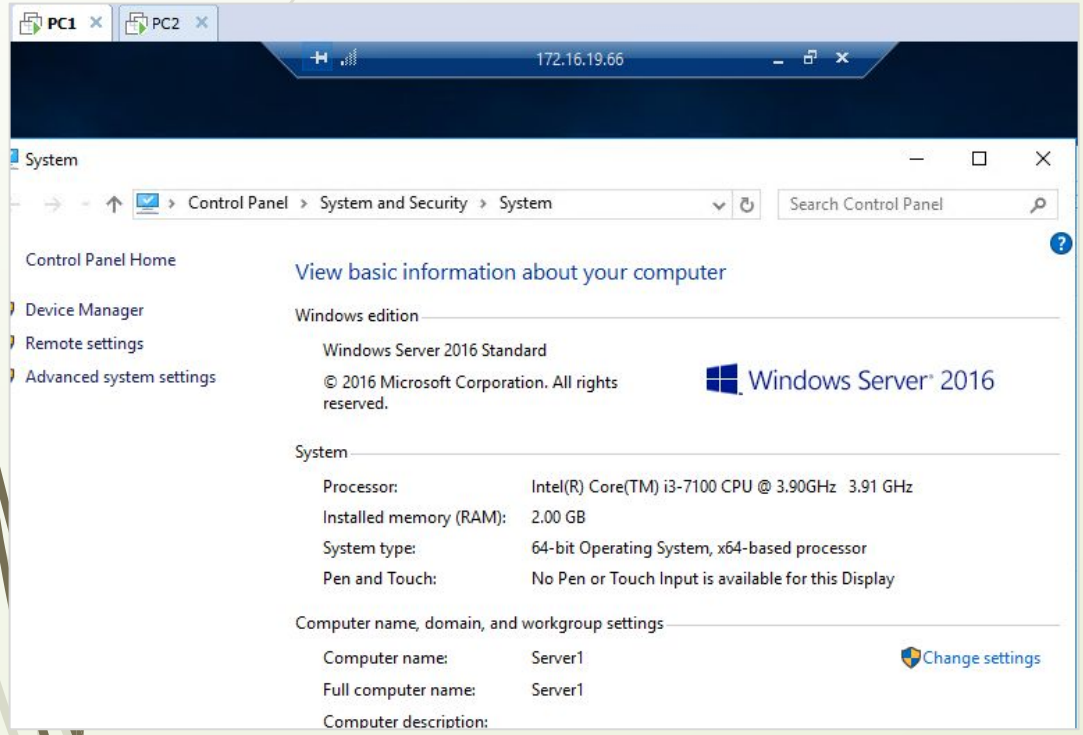


Включение удалённого доступа к компьютеру

Во вкладке «Система» в Панели Управления перейти во вкладку «Настройка удалённого доступа» и выставить «Разрешить удалённые подключения к этому компьютеру».

Настройка удалённого доступа в среде Windows

Далее необходимо протестировать удалённое подключение. Для этого необходимо в командной строке «Выполнить» ввести команду: mstsc



Удалённый рабочий стол сервера Server1 с подключением к нему с PC1

В появившемся окне «Подключение к удалённому рабочему столу» необходимо ввести либо IP-адрес ПК, к которому необходимо подключиться, либо имя компьютера в сети, после чего жмём кнопку подключить, принимаем сертификацию, вводим данные учётной записи и можем видеть рабочий стол удалённого компьютера.

Выводы

Таким образом после рассмотрения учебно-технической литературы были проведены такие мероприятия:

- Раскрытие некоторых теоретических понятий.
- Проведён ряд действий направленных на проектирование локальной сети.
- Выполнена базовая настройка сетевой инфраструктуры локальной сети.
- Была проверена работоспособность Telnet.
- Выполнена настройка SSH.
- Осуществлена настройка удалённого доступа в среде Windows.

В соответствии с вышеизложенным, цель курсового проекта достигнута путем решения поставленных задач, смоделированы этапы администрирования и настройки удаленного доступа к ресурсам локальной сети.

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СТЕРЛИТАМАКСКИЙ МНОГОПРОФИЛЬНЫЙ ПРОФЕССИОНАЛЬНЫЙ КОЛЛЕДЖ
(ГАПОУ СМПК)

КУРСОВАЯ РАБОТА

«МОДЕЛИРОВАНИЕ ЭТАПОВ АДМИНИСТРИРОВАНИЯ И НАСТРОЙКИ УДАЛЕННОГО ДОСТУПА К РЕСУРСАМ ЛОКАЛЬНОЙ СЕТИ»

Выполнил:
студент III курса группы ССА-39
специальности 09.02.06 Системное
и сетевое администрирование
Бойкив Михаил Орестович

Руководитель:
Шарафиев Ринат Расимович.

Стерлитамак, 2020