

Основы компьютерных сетей.

5. Транспортный уровень.

Протоколы с гарантированной и негарантированной доставкой данных: TCP и UDP. Форматы TCP-сегмента и UDP-дейтаграммы. Сокеты. Технология перегруженного NAT(PAT).
Диагностика транспортного уровня.

План занятия:

Как работают протоколы
транспортного уровня и чем они
отличаются TCP/UDP;

понятия сессии и сокета;

какие протоколы прикладного уровня
используются и для чего Сетевой
уровень предоставляет сервис по
передаче пакетов между сетями,
обеспечивая прозрачный доступ в
сеть для верхних протоколов.

Какие задачи решает транспортный
уровень?



Транспортный уровень:

Транспортный уровень



Транспортный уровень:

Функционирование транспортного уровня



Транспортный уровень:

1. Появляется новая сущность – Порт
2. Решает вопрос гарантированной доставки (если нужно)
3. Доставляет сообщение до конкретного приложения

Транспортный уровень:

1. Появляется новая сущность – Порт
2. Решает вопрос гарантированной доставки (если нужно)
3. Доставляет сообщение до конкретного приложения

TCP - гарантированная доставка

UDP - негарантированная доставка

UDP :

UDP :



User Datagram Protocol (UDP) – протокол передачи дейтаграмм пользователя.

UDP:

- без установления соединения
- используется служебными протоколами в локальных сетях RIP, SNMP, DHCP, TFTP и потоковыми приложениями.

UDP :

Протокол работает без установления соединения, кроме того не используется подтверждение о доставки, что приводит к тому что передаваемые дейтаграммами могут быть потеряны и как следствие это не гарантирует доставку данных.

Дейтаграммы могут поступать не в любой последовательности повторяться и не доходить до адреса назначения.

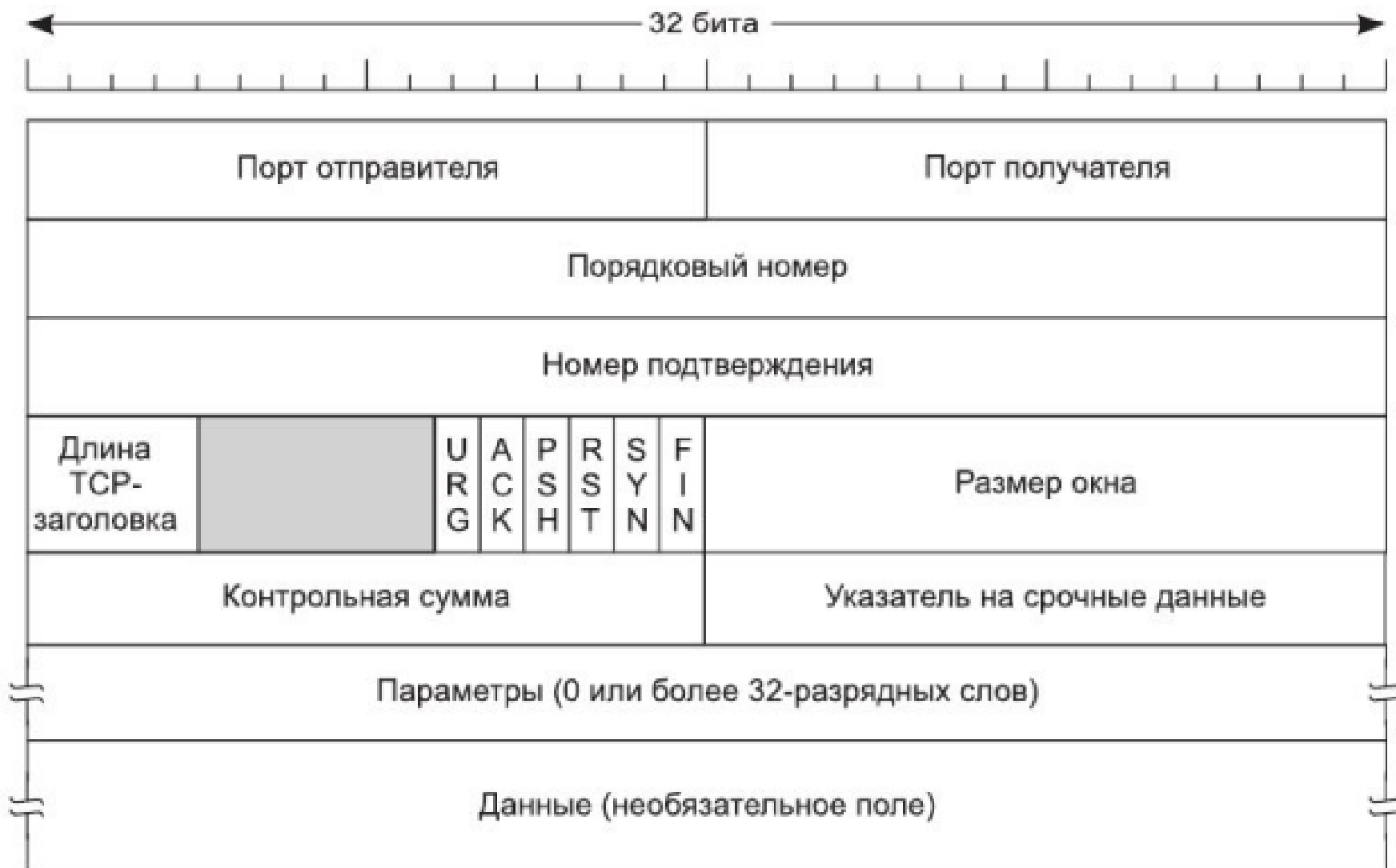
Это все можно отнести к минусам в отличие от протокола TCP. Плюсом является возможность начать передачу данных без установления соединения.

Пространство адресов протокола UDP, отделено от TCP-портов.

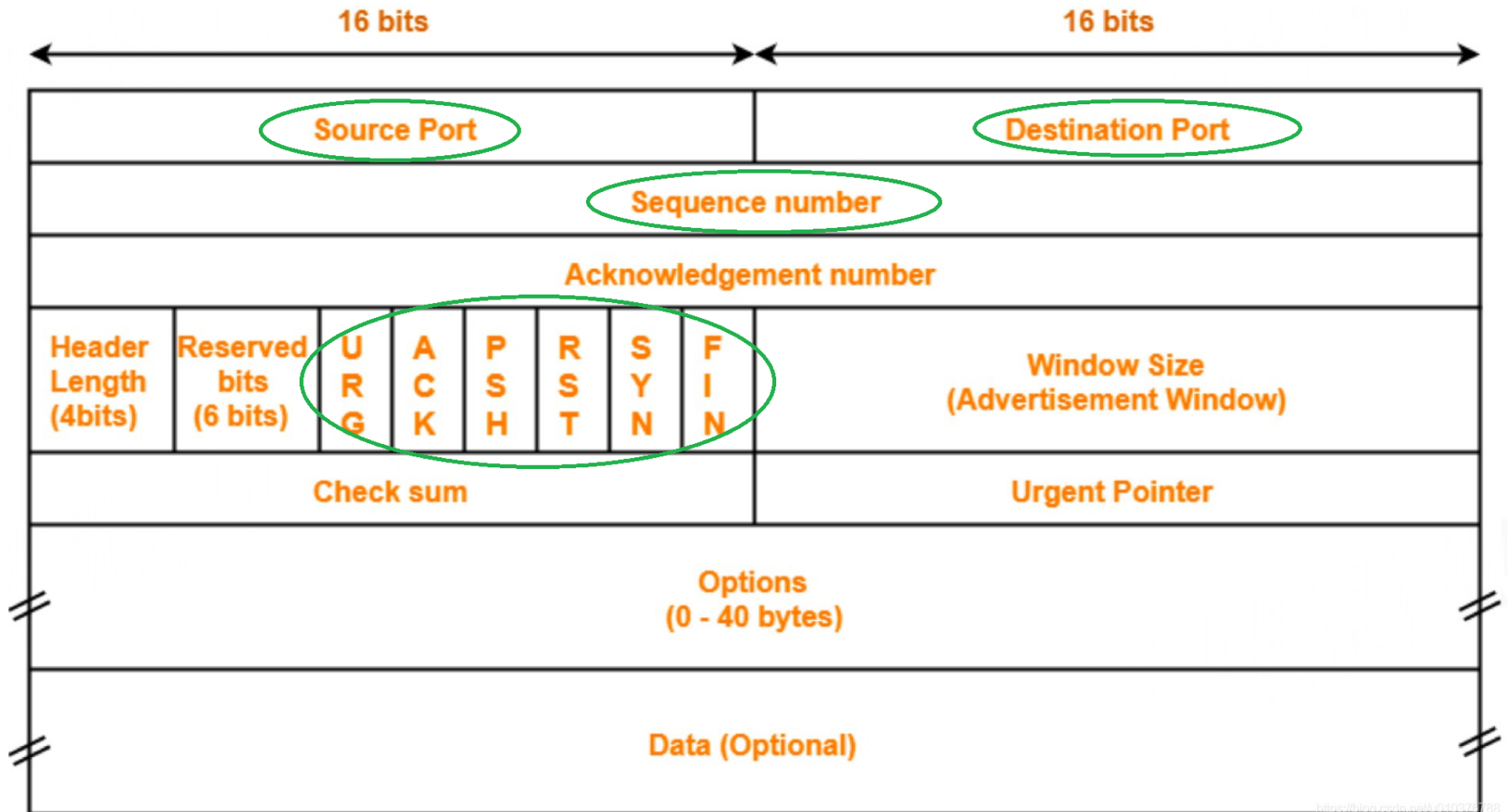
TCP:

- Ориентирован на соединение.
- Надежная передача.
- Управление потоком.
- Сегментирование данных полученных от протоколов прикладного уровня на дейтаграммы, для передачи по сети.
- Нумерация и упорядочивание дейтаграмм.
- Буферизация дейтаграмм.
- Сопоставление и адресация процессов (приложение) и сетевых запросов (создание сокетов).
- Управление интенсивностью передачи.

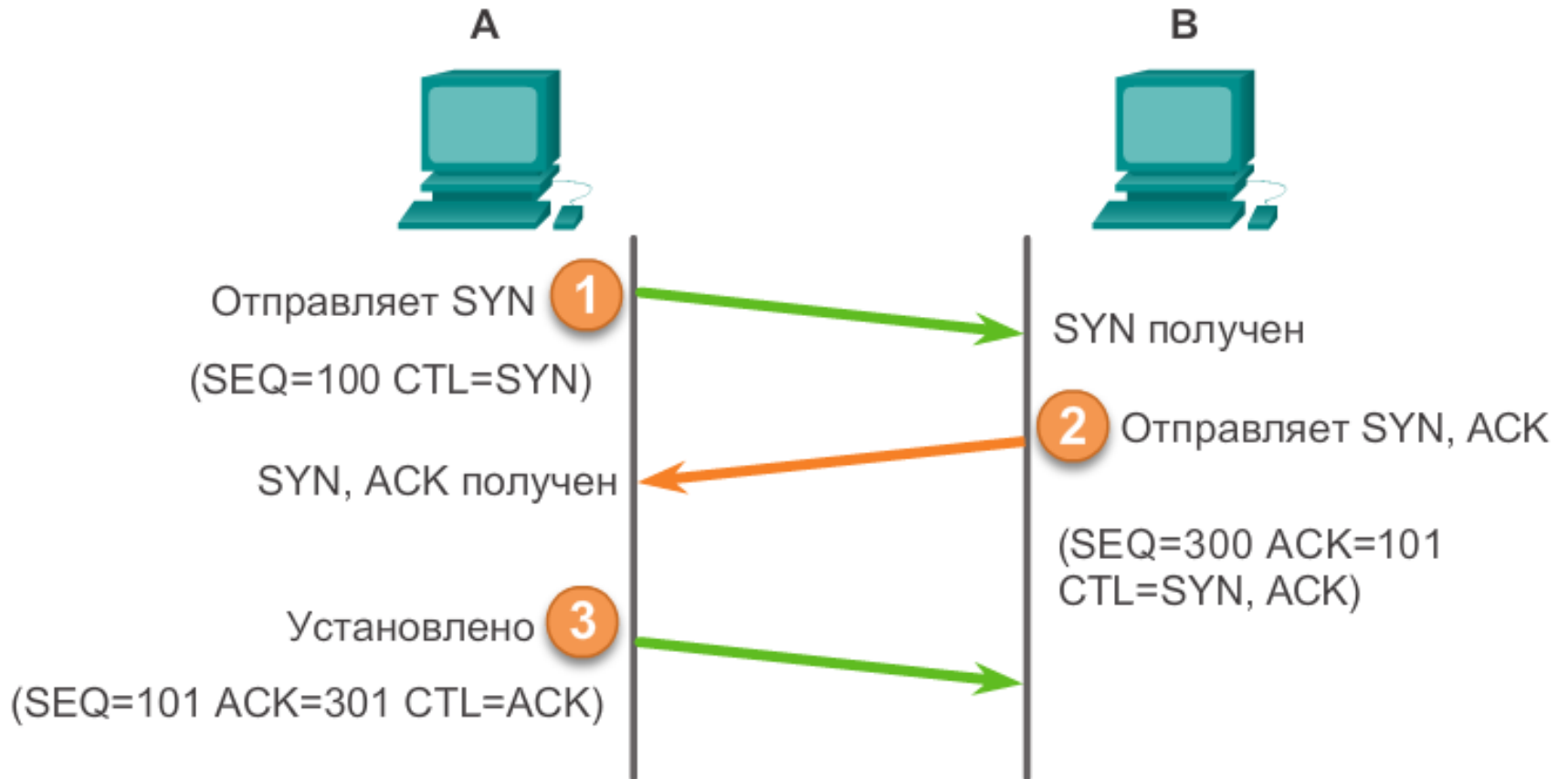
TCP:



TCP:



TCP:

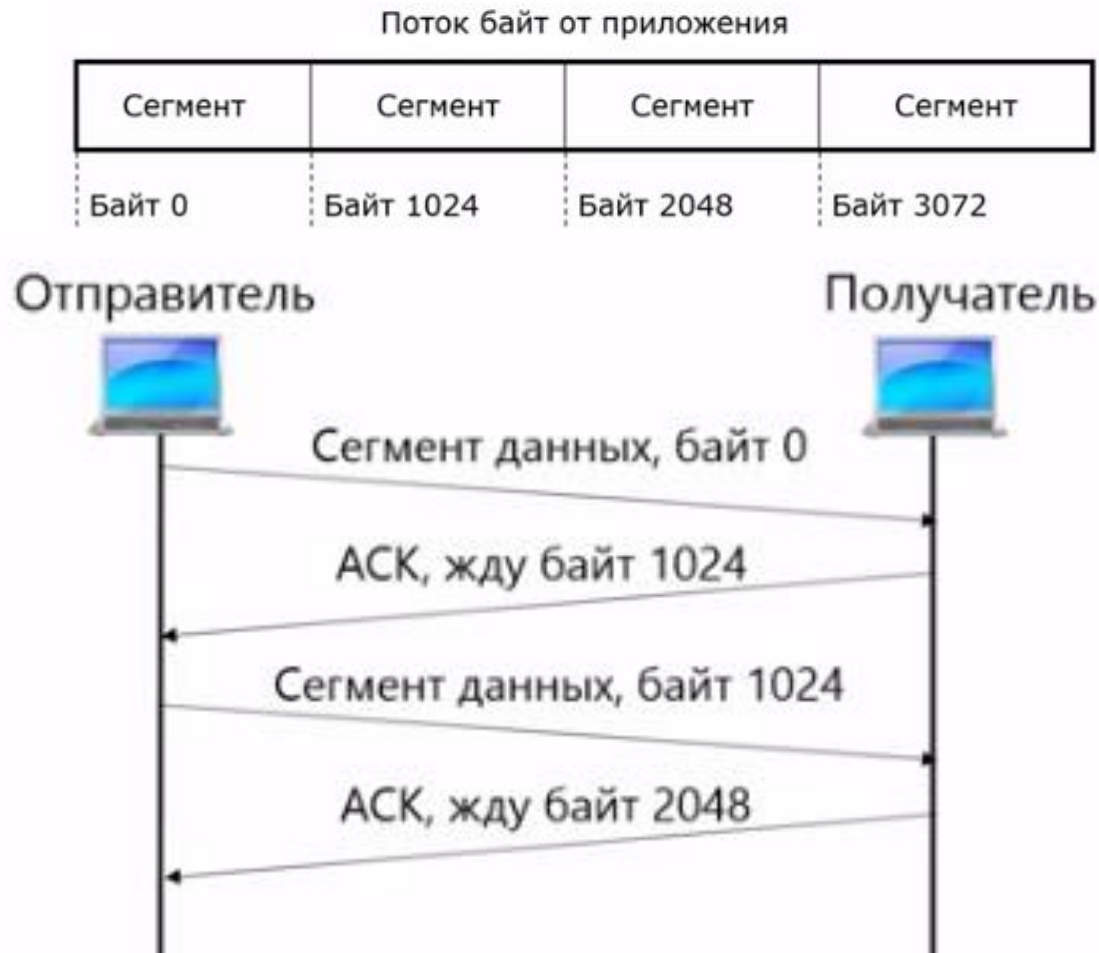


CTL: какие биты управления в TCP-заголовке заданы в значении 1
Узел А отправляет ACK-ответ узлу В.

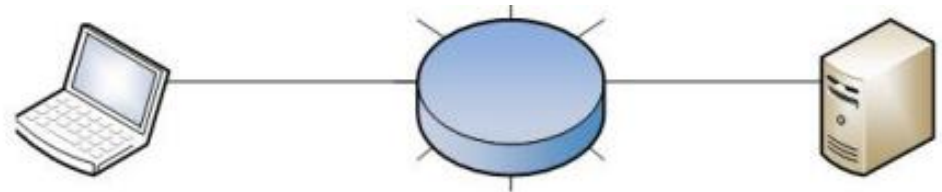
TCP:

Механизм обеспечения сохранения порядка следования сообщений

- Нумерация сообщений



ТСР. Метод скользящего окна:

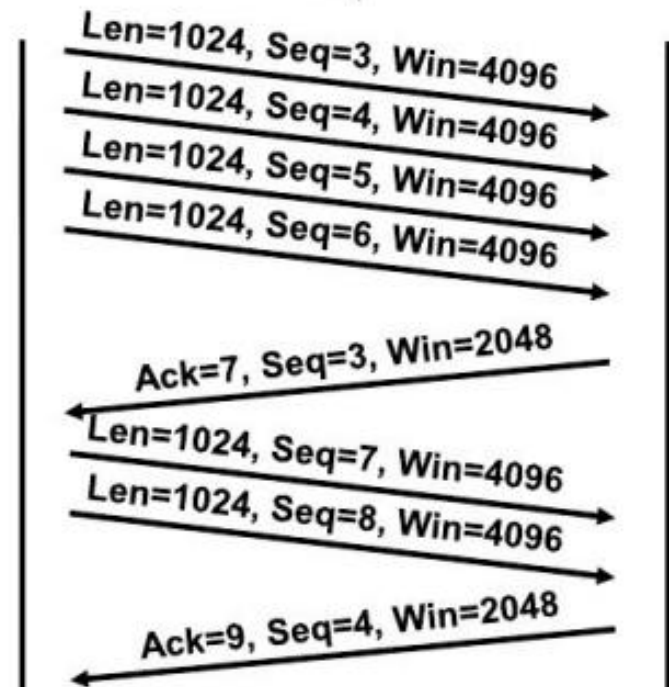


Len= length (длина)

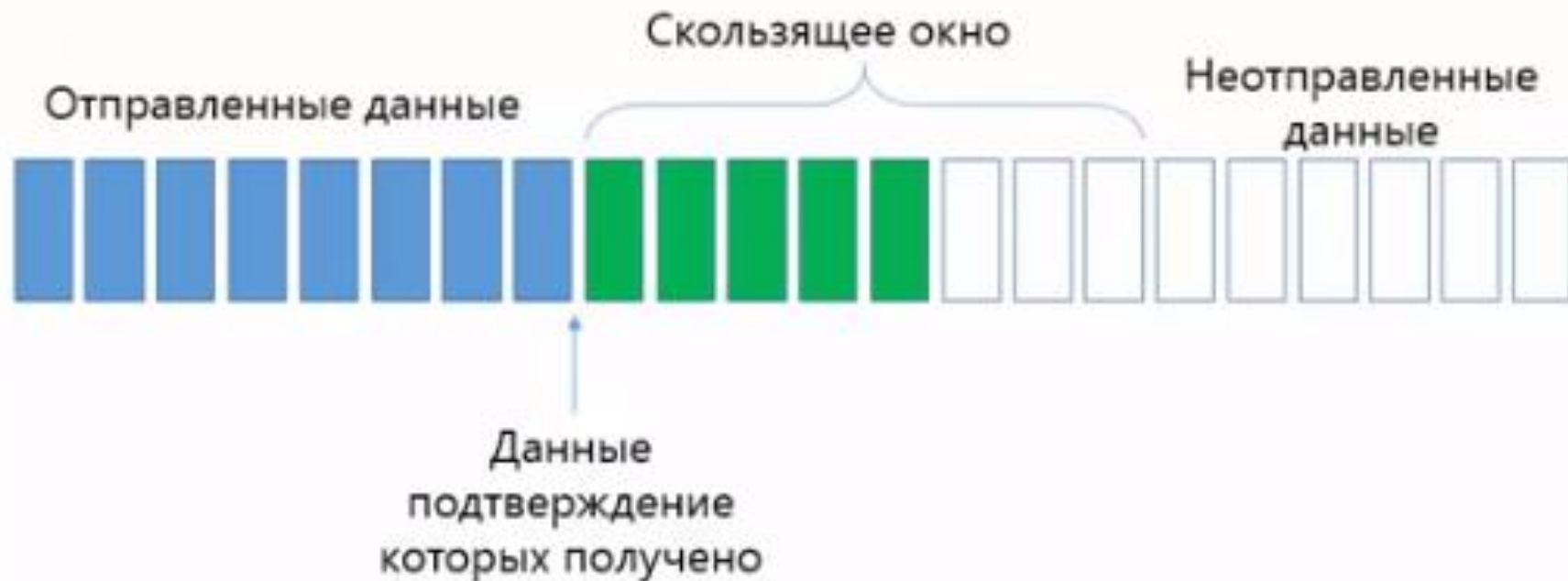
Seq= sequence

(номер сообщения в
последовательности)

Win=window (размер окна)



ТСР. Метод скользящего окна:



Сокет (программный интерфейс):

Интерфейс сокета Беркли используется для взаимодействия между компьютерами в сети или процессами запущенными на компьютере.

Сокеты – это стандарт интерфейсов для транспортных подсистем.

Различные варианты сокетов могут быть реализованы в разных ОС и языках программирования.

Операция SOCKET создает новый сокет и записывает его в таблицу транспортной подсистемы.

Параметры вызова задают тип используемого формата адресации, тип применяемого сервиса (например, надежный поток байтов) и протокол.

Сокет – логическая конструкция, уровень абстракции, для удобства взаимодействия приложения по сети.

(protocol, dst IP, src IP, dst PORT, src PORT) - 5-tuple или Socket

Уникальный набор для конкретной сессии.

Список портов по умолчанию для популярных протоколов:

21 – ftp

22 – ssh

23 – telnet

25 – smtp

43 – whois

53 – dns

68 – dhcp

80 – http

110 – pop3

115 – sftp

119 – nntp

123 – ntp

139 – netbios

143 – imap

161 – snmp

179 – bgp

220 – imap3

389 – ldap

443 – https

993 – imaps

Базовые операции сокетов для TCP

SOCKET (СОКЕТ) Создание нового сокета

BIND (СВЯЗАТЬ) Привязать локальный адрес и сокет

LISTEN (ОЖИДАТЬ) Слушать входящие соединения; указав размер очереди (ESTABLISHED - установлено)

ACCEPT (ПРИНЯТЬ) Подтвердить установление входящего соединения

CONNECT (СОЕДИНИТЬ) Инициировать процесс установления соединения

SEND (ПОСЛАТЬ) Передать информацию по установленному соединению

RECEIVE (ПОЛУЧИТЬ) Принять информацию по установленному соединению

CLOSE (ЗАКРЫТЬ) Закрывать сеанс связи и отправить сообщение о завершение соединения

Технология NAT

NAT (Network Address Translation) — трансляция сетевых адресов.

Процедура по изменению адресов в заголовках IP-пакетов при их прохождении через маршрутизатор или другое устройство.

Типы NAT:

- Статический NAT.
- Динамический NAT.
- Перегруженный NAT.

Технология NAT

Локальные сети, не маршрутизируются в Интернете:

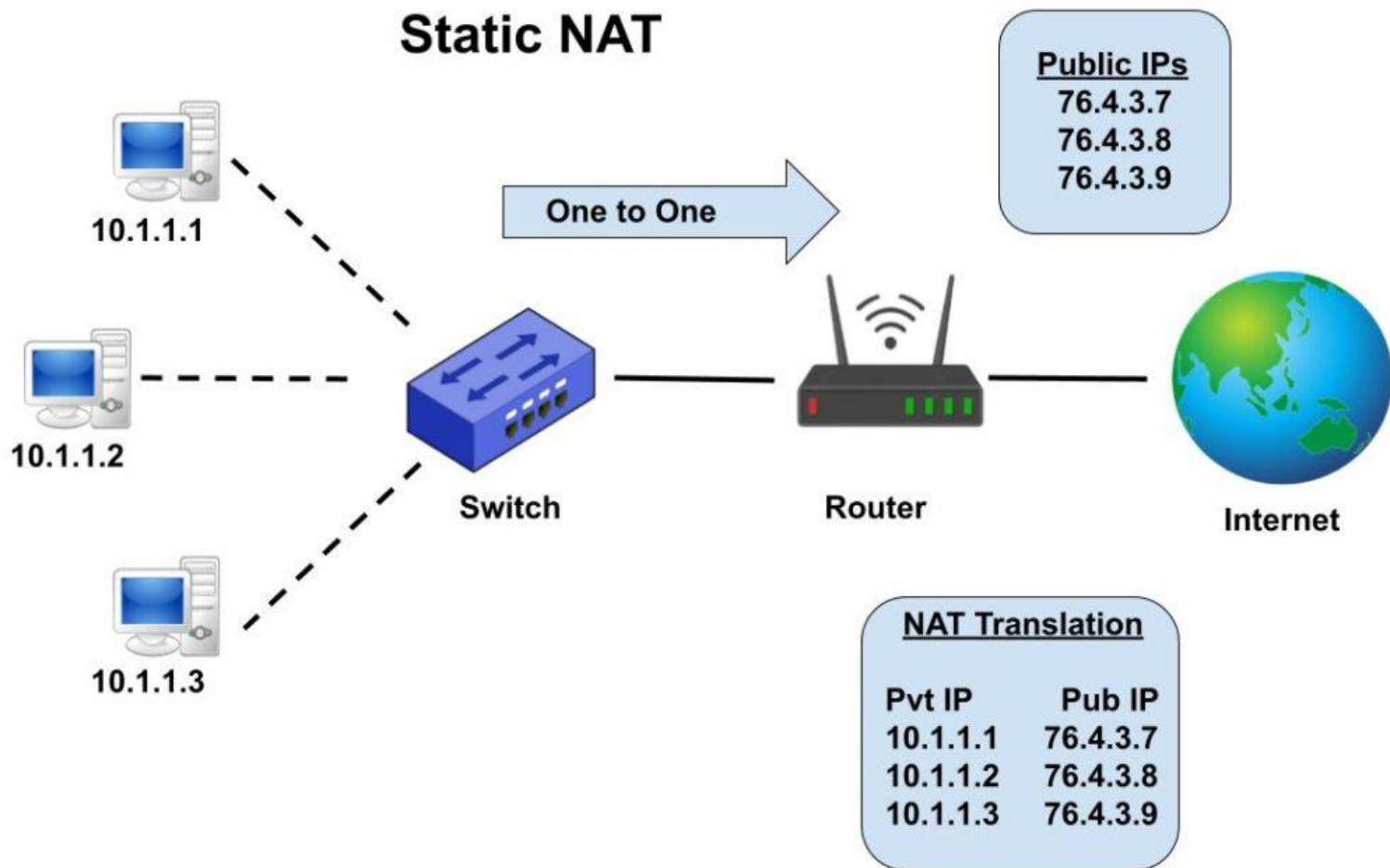
10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

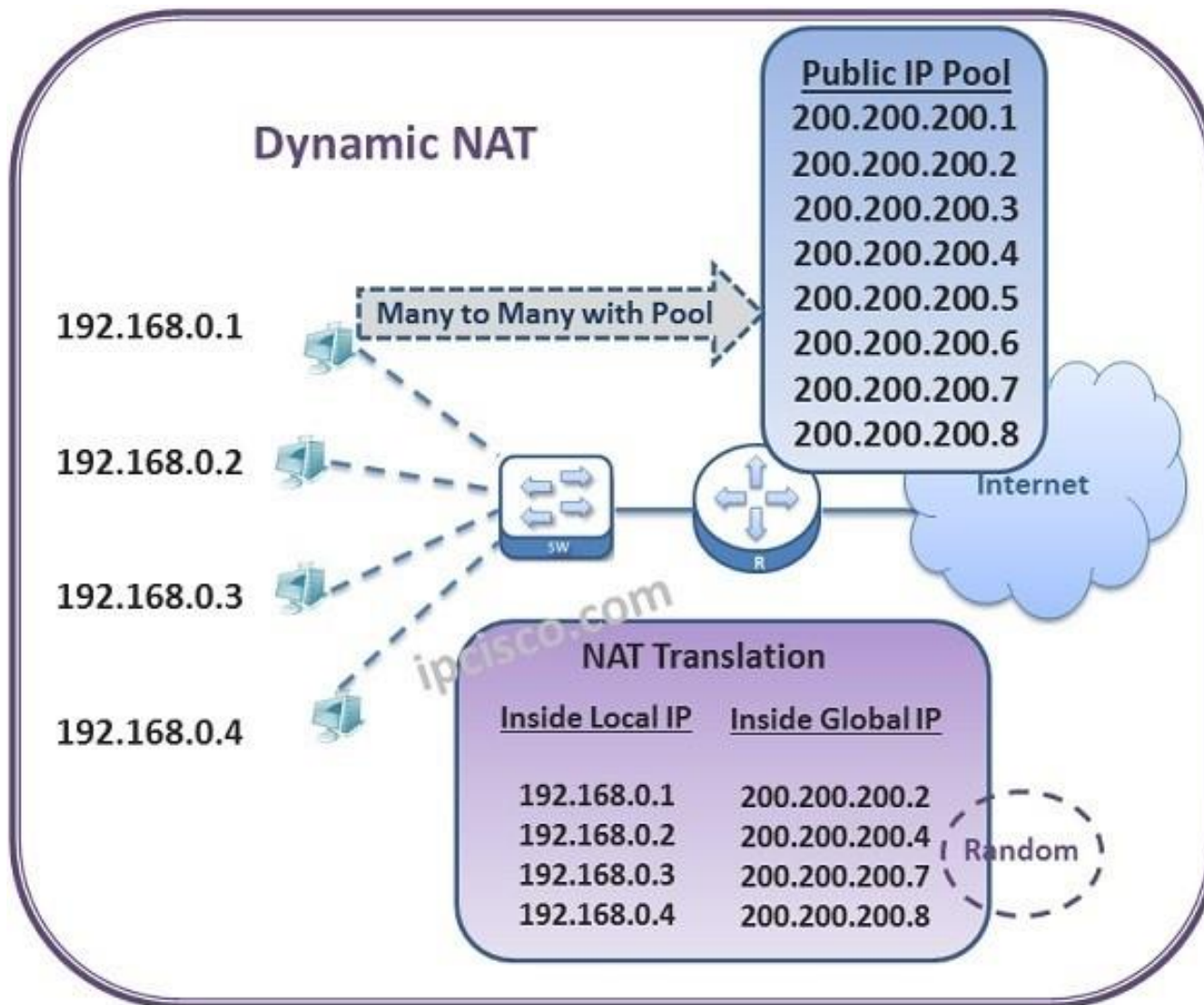
Статический NAT

Технология статического NAT позволяет организовать сокрытие внутренних адресов и доступ к Интернет на сетевом уровне.

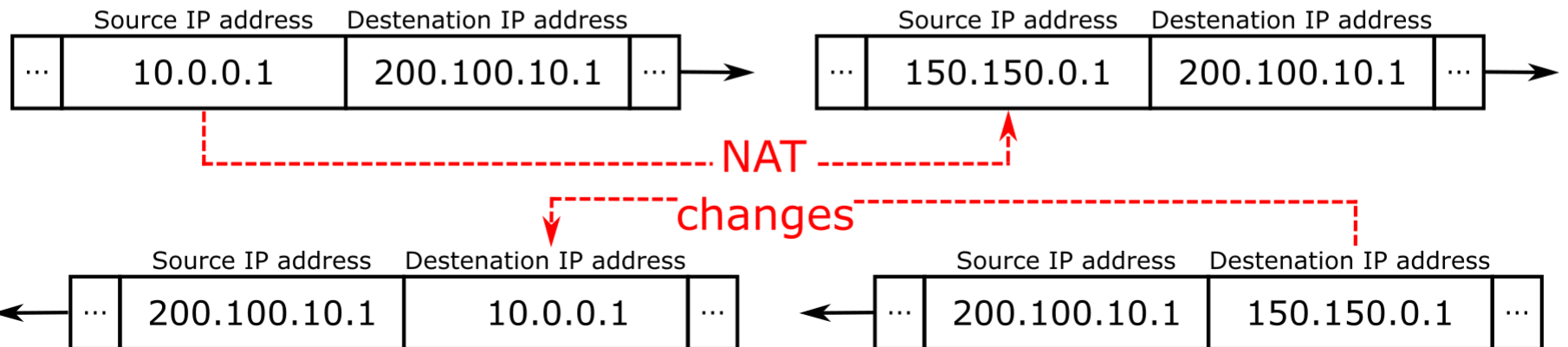
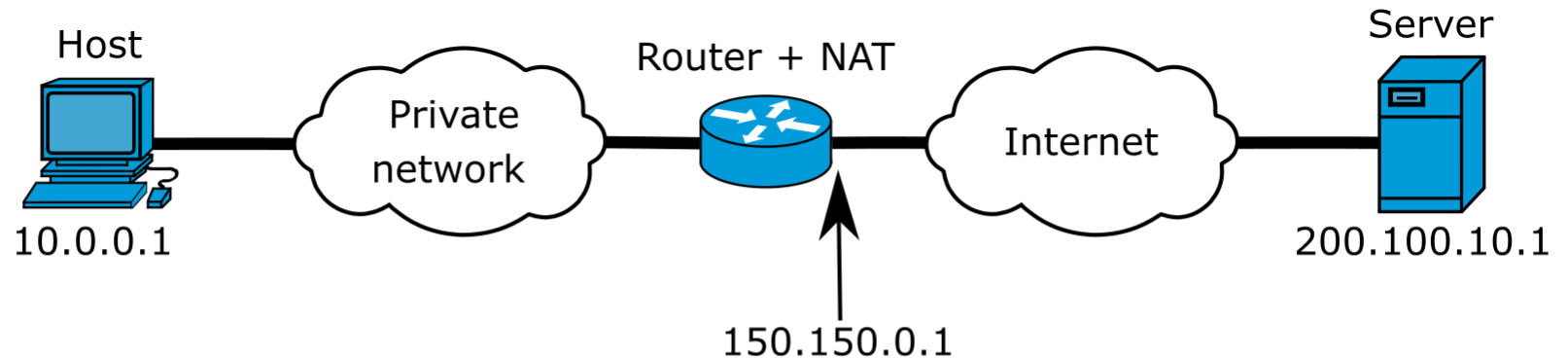


Динамический NAT

Если же количество машин больше, чем белых IP-адресов, и используются они не слишком часто, может использоваться динамический NAT.



Destination NAT. Source NAT.



Технология NAT

Различия между NAT и PAT

7

NAT

Пул внутренних глобальных адресов	Внутренний локальный адрес
-----------------------------------	----------------------------

209.165.200.226	192.168.10.10
-----------------	---------------

209.165.200.227	192.168.10.11
-----------------	---------------

209.165.200.228	192.168.10.12
-----------------	---------------

209.165.200.229	192.168.10.13
-----------------	---------------

Пул внутренних глобальных адресов	Внутренний локальный адрес
-----------------------------------	----------------------------

209.165.200.226	192.168.10.10
-----------------	---------------

209.165.200.227	192.168.10.11
-----------------	---------------

209.165.200.228	192.168.10.12
-----------------	---------------

209.165.200.229	192.168.10.13
-----------------	---------------

PAT

Внутренний глобальный адрес	Внутренний локальный адрес
-----------------------------	----------------------------

209.165.200.226:1444	192.168.10.10:1444
----------------------	--------------------

209.165.200.226:1445	192.168.10.11:1444
----------------------	--------------------

209.165.200.226:1555	192.168.10.12:1555
----------------------	--------------------

209.165.200.226:1556	192.168.10.13:1555
----------------------	--------------------

Внутренний глобальный адрес	Внутренний локальный адрес
-----------------------------	----------------------------

209.165.200.226:1444	192.168.10.10:1444
----------------------	--------------------

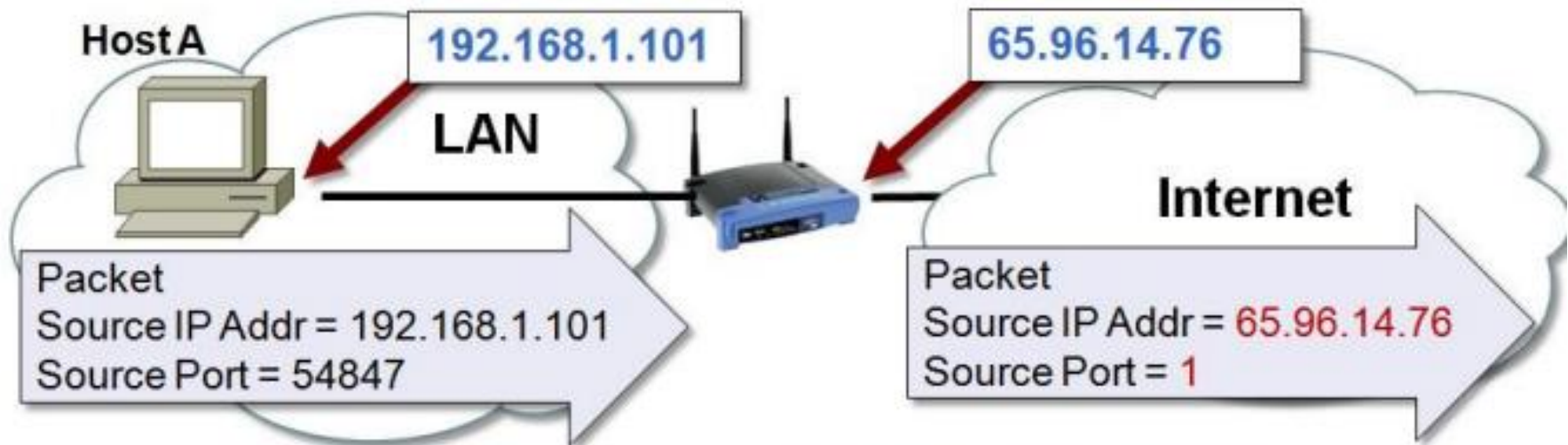
209.165.200.226:1445	192.168.10.11:1444
----------------------	--------------------

209.165.200.226:1555	192.168.10.12:1555
----------------------	--------------------

209.165.200.226:1556	192.168.10.13:1555
----------------------	--------------------

Как показано на рисунке, NAT преобразует IPv4-адреса, исходя из схемы 1:1 для частных IPv4-адресов и публичных IPv4-адресов. В то же время, PAT меняет и адрес, и номер порта.

Перегруженный NAT (PAT, NAPT)

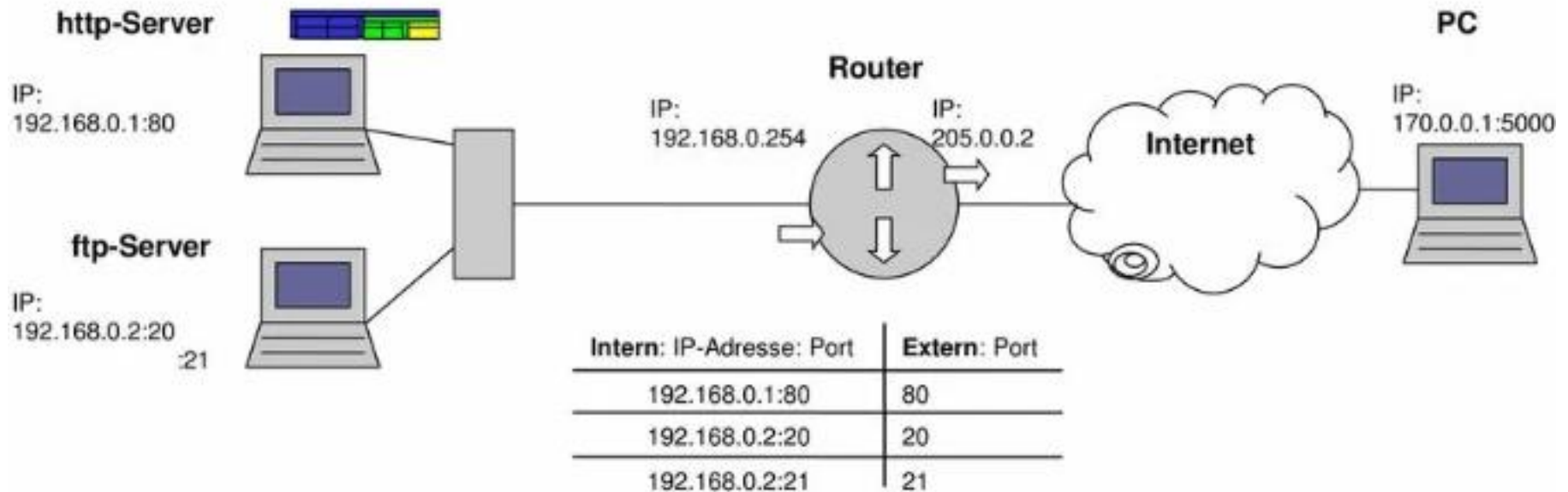


NAT Translation Table				
	Local IP Address	Source Port #	Internet IP Address	Source Port #
process X, Host A →	192.168.1.101	54,847	= 65.96.14.76	1
Host B →	192.168.1.103	24,123	= 65.96.14.76	2
process Y, Host A →	192.168.1.101	42,156	= 65.96.14.76	3
Host C →	192.168.1.102	33,543	= 65.96.14.76	4

Port Forwarding

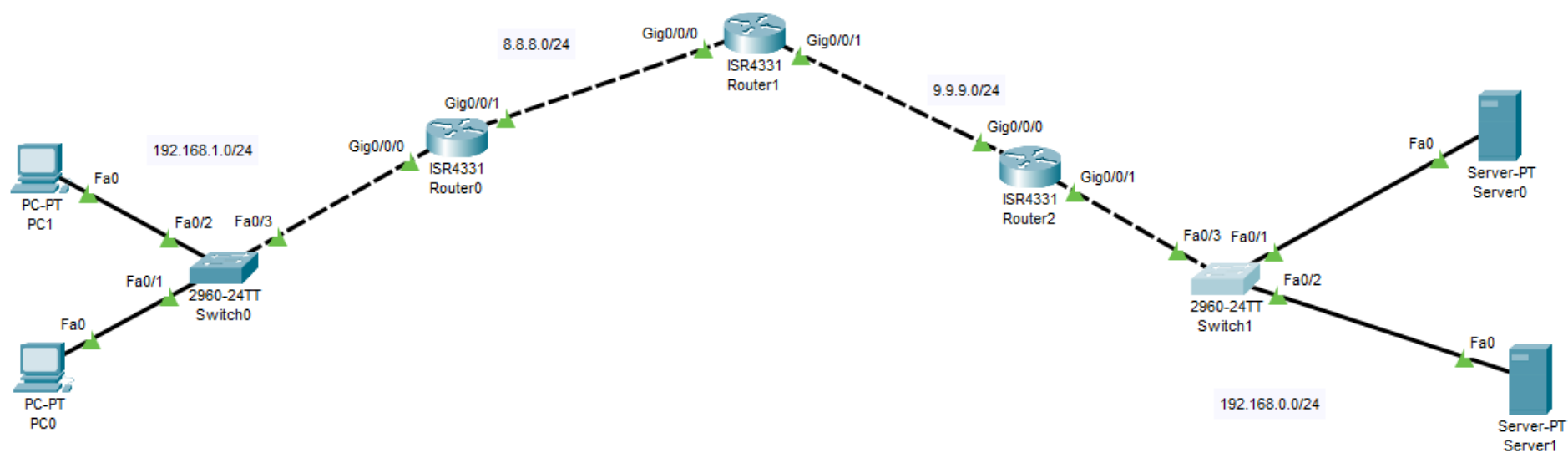
Port Forwarding - это технология, которая позволяет обращаться из Интернет к компьютеру во внутренней сети за маршрутизатором, использующим NAT. Доступ осуществляется при помощи перенаправления трафика определенных портов с внешнего адреса маршрутизатора на адрес выбранного компьютера в локальной сети.

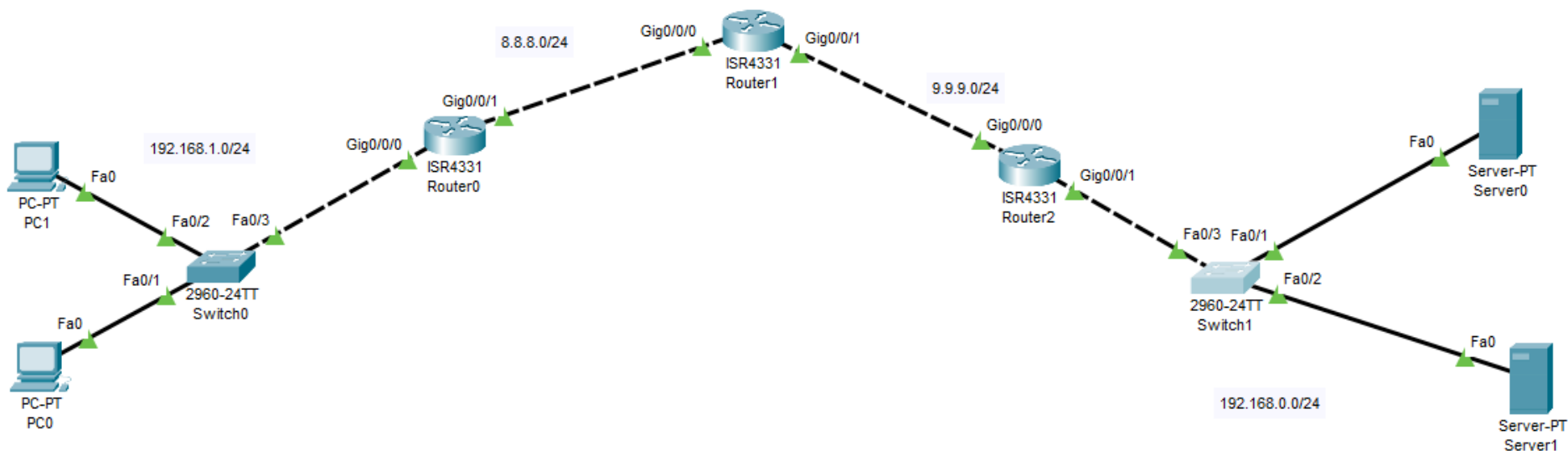
Port Forwarding



IP - Paket						
.	Quell - IP	Ziel - IP	.	TCP - Segment		
				Quell-Port	Ziel-Port	Daten
.	170.0.0.1	192.168.0.1	.	5000	80	

Практика





NAT

//1. Направление трансляции

```
Router#conf t
```

```
Router(config)#int gigabitEthernet 0/0/0 //выбираем интерфейс, входящие пакеты  
которого будем транслировать
```

```
Router(config-if)#ip nat ?
```

inside Inside interface for address translation

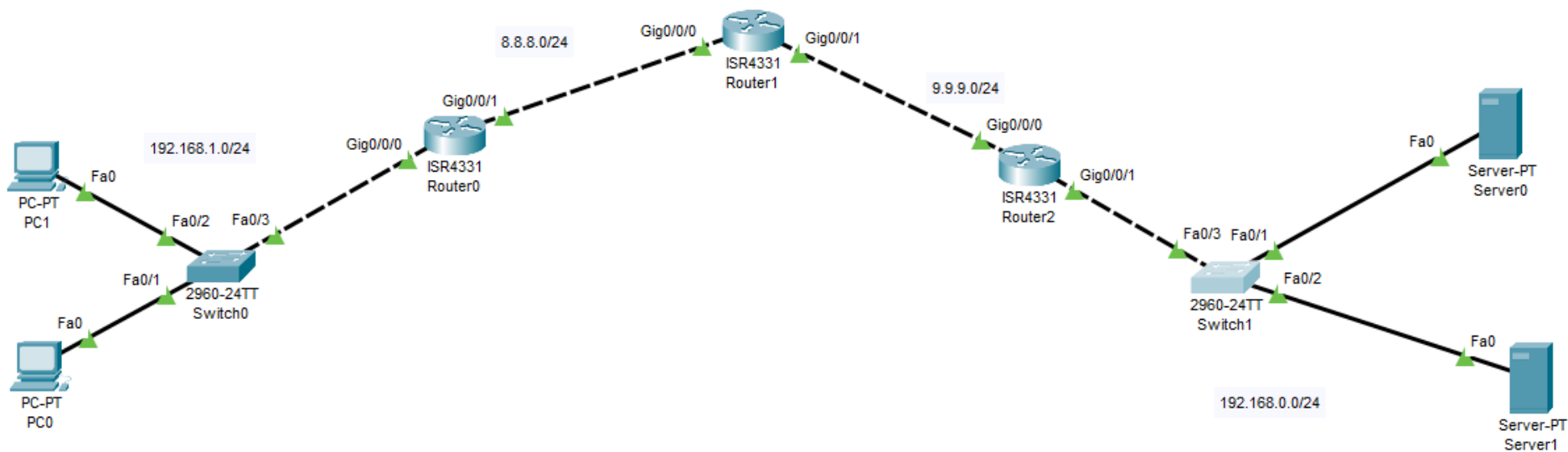
outside Outside interface for address translation

```
Router(config-if)#ip nat inside // указываем сторону (внутренняя)
```

```
Router(config-if)#exit
```

```
Router(config)#int gigabitEthernet 0/0/1
```

```
Router(config-if)#ip nat outside // внешняя
```



NAT

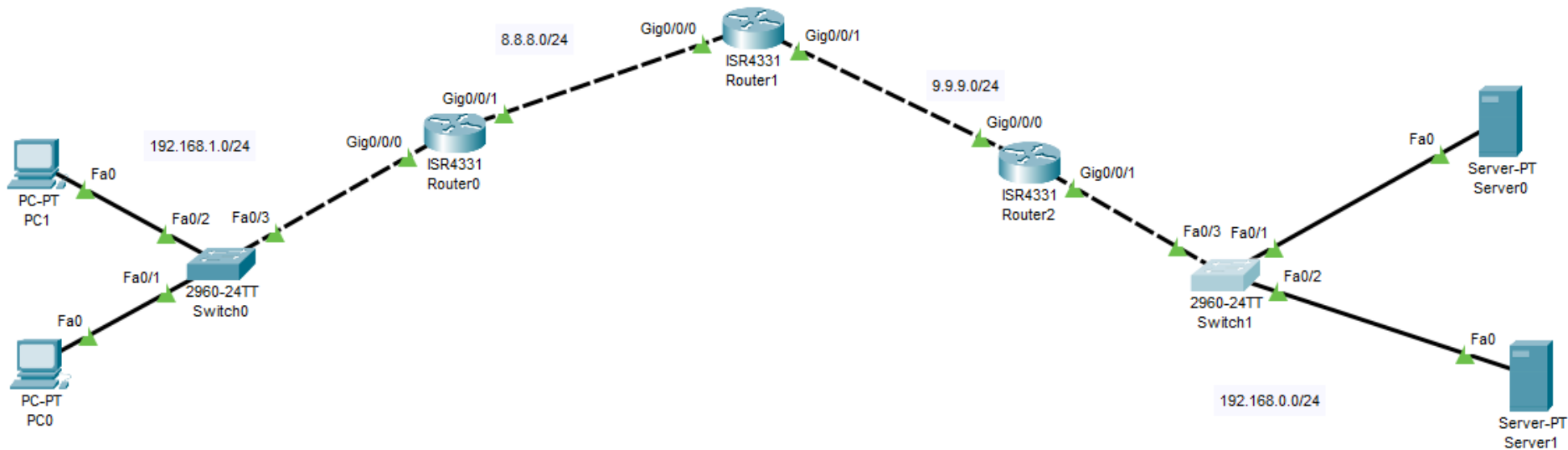
//2 выбрать трафик

Router(config)#ip access-list ?

extended Extended Access List

standard Standard Access List

Router(config)#ip access-list standard NAME-ACL



NAT

// 3 Настройка NAT

Router(config)# ip nat inside ?

source Source address translation

Router(config)# ip nat inside source ?

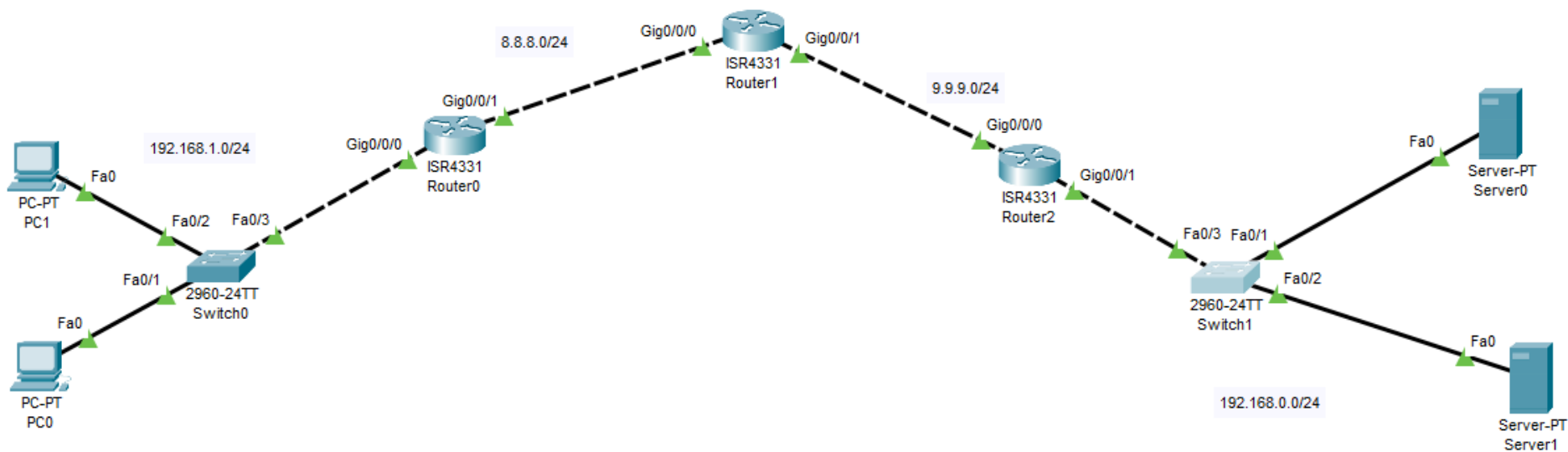
list Specify access list describing local addresses

static Specify static local->global mapping

Router(config)# ip nat inside source list NAME-ACL interface
gigabitEthernet 0/0/1 overload

Router(config)#exit

Router#show ip nat translations



//static port forwarding: 9.9.9.2:80 => 192.168.0.100:80

```
Router(config)#int gigabitEthernet 0/0/0
```

```
Router(config-if)#ip nat outside
```

```
Router(config-if)#exit
```

```
Router(config)#int gigabitEthernet 0/0/1
```

```
Router(config-if)#ip nat inside
```

```
Router(config-if)#exit
```

```
Router(config)#ip nat inside source static tcp 192.168.0.100 80 9.9.9.2 80
```

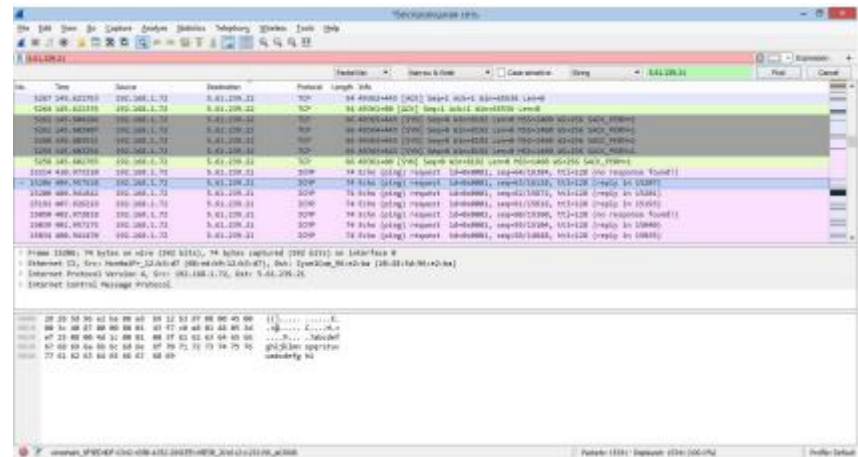
```
Router(config)#exit
```

```
Router#show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
tcp	9.9.9.2:80	192.168.0.100:80	---	

Практика

1. Анализатор сетевого трафика Wireshark.
2. Анализатор трафика в Cisco RT.



Домашнее задание:

1. Изучить методичку.