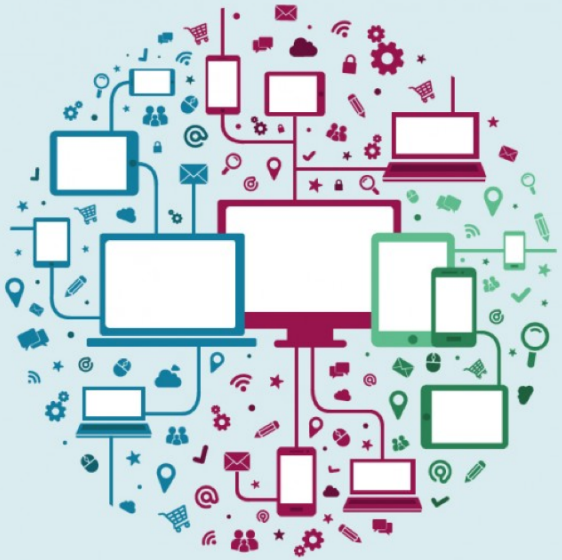
Компьютерные сети

Транспортный уровень

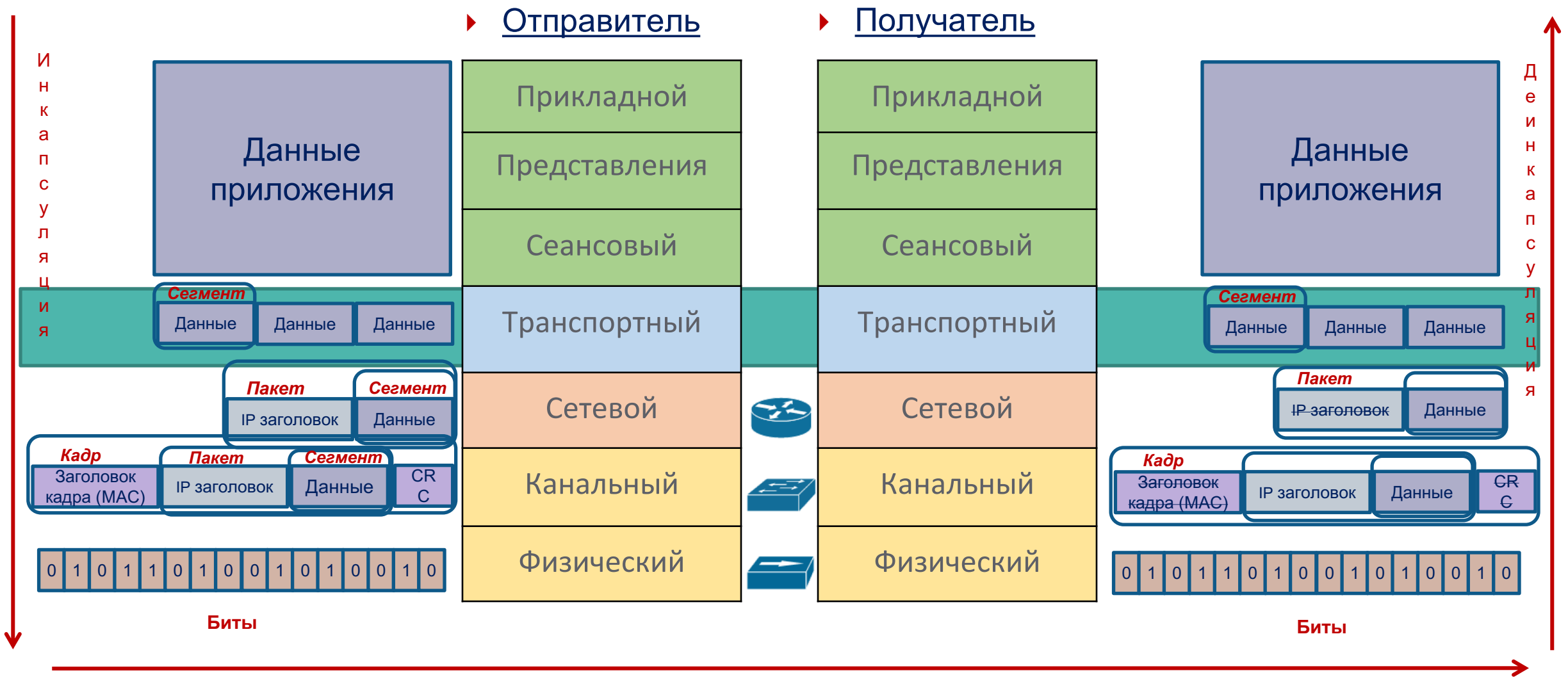
Протоколы с гарантированной и негарантированной доставкой данных: TCP и UDP. Форматы TCP-сегмента и UDP-дейтаграммы. Сокеты. Технология перегруженного NAT(PAT). Диагностика транспортного уровня.

Вопросы к аудитории



1. Проверка практических работ.
2. Есть ли проблемы?

Модель OSI. Транспортный уровень



Транспортный уровень

•сегментирование данных полученных от протоколов прикладного уровня на дейтаграммы, для передачи по сети

•нумерация и упорядочивание дейтаграмм

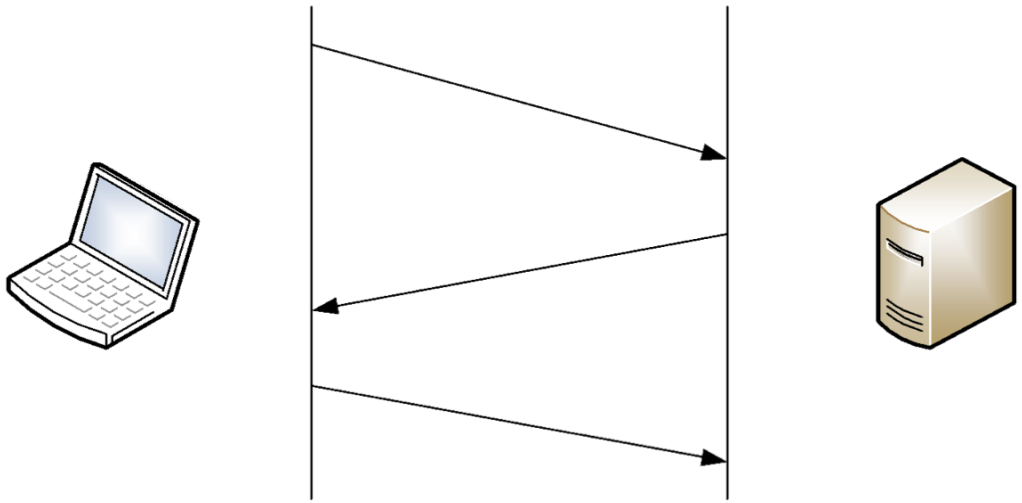
•буферизация дейтаграмм

•сопоставление и адресация процессов (приложение) и сетевых запросов (создание сокетов)

•управление интенсивностью передачи

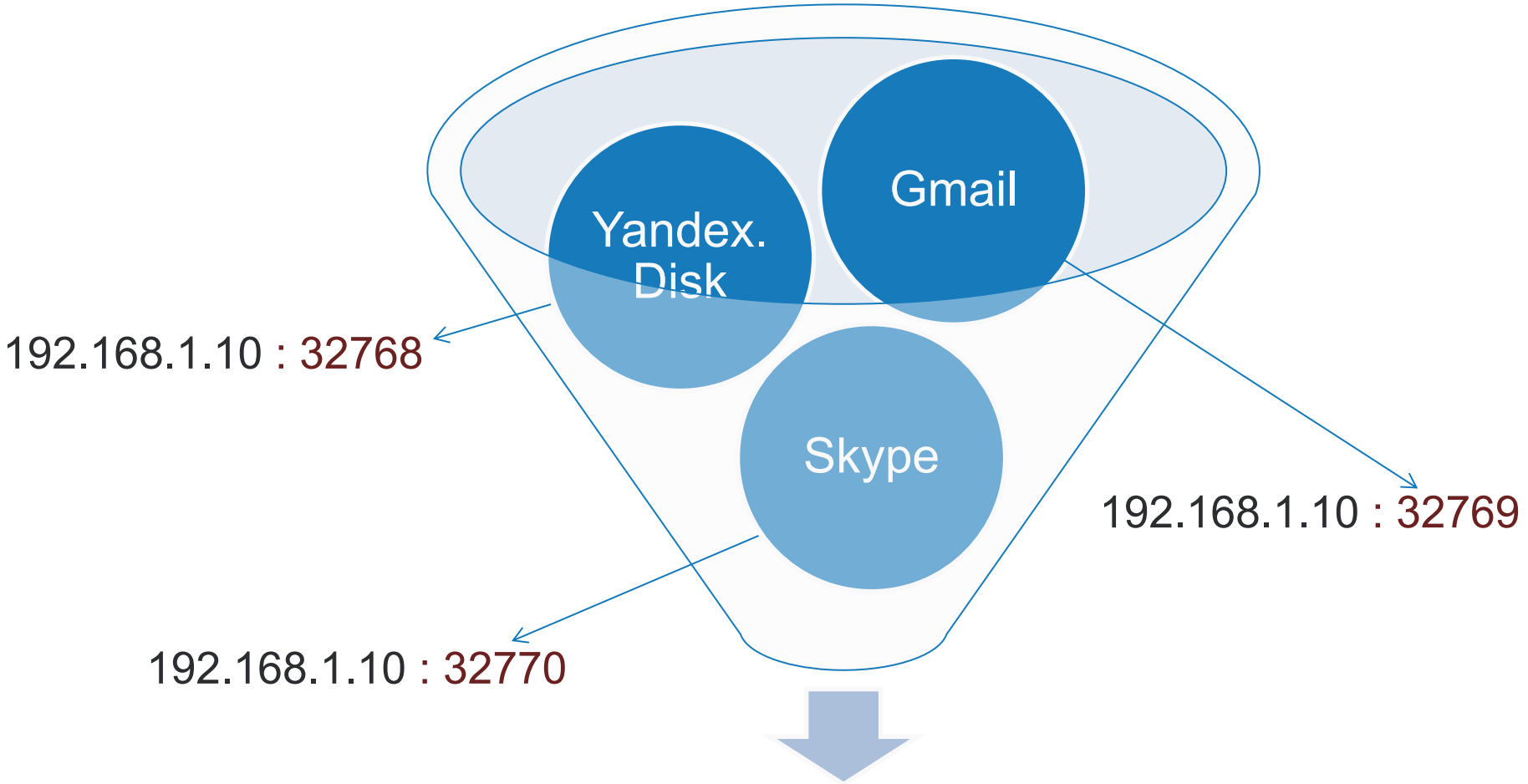
Протоколы:

- TCP
- UDP



Транспортный уровень

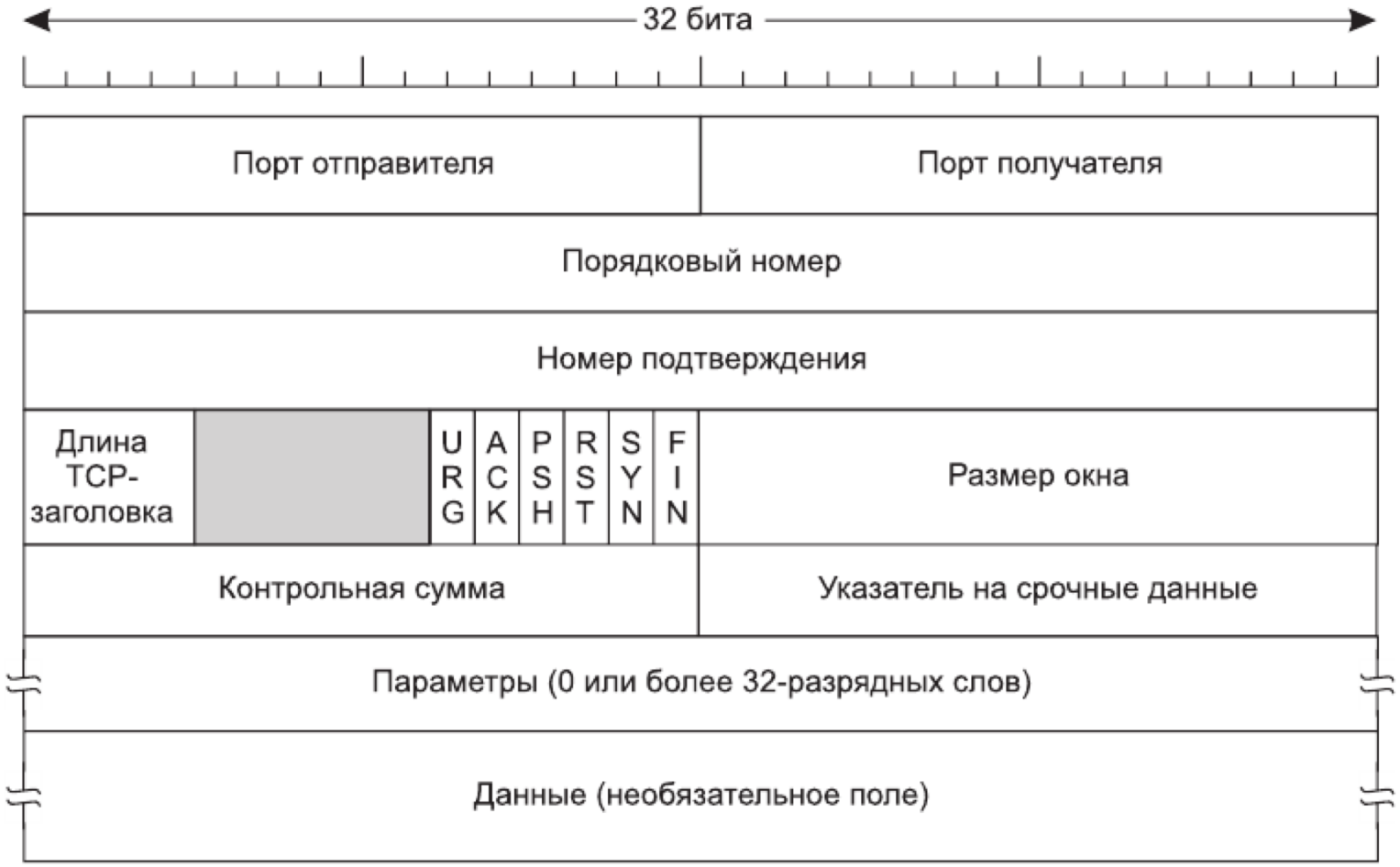
- сопоставление и адресация процессов (приложение) и сетевых запросов (создание сокетов)



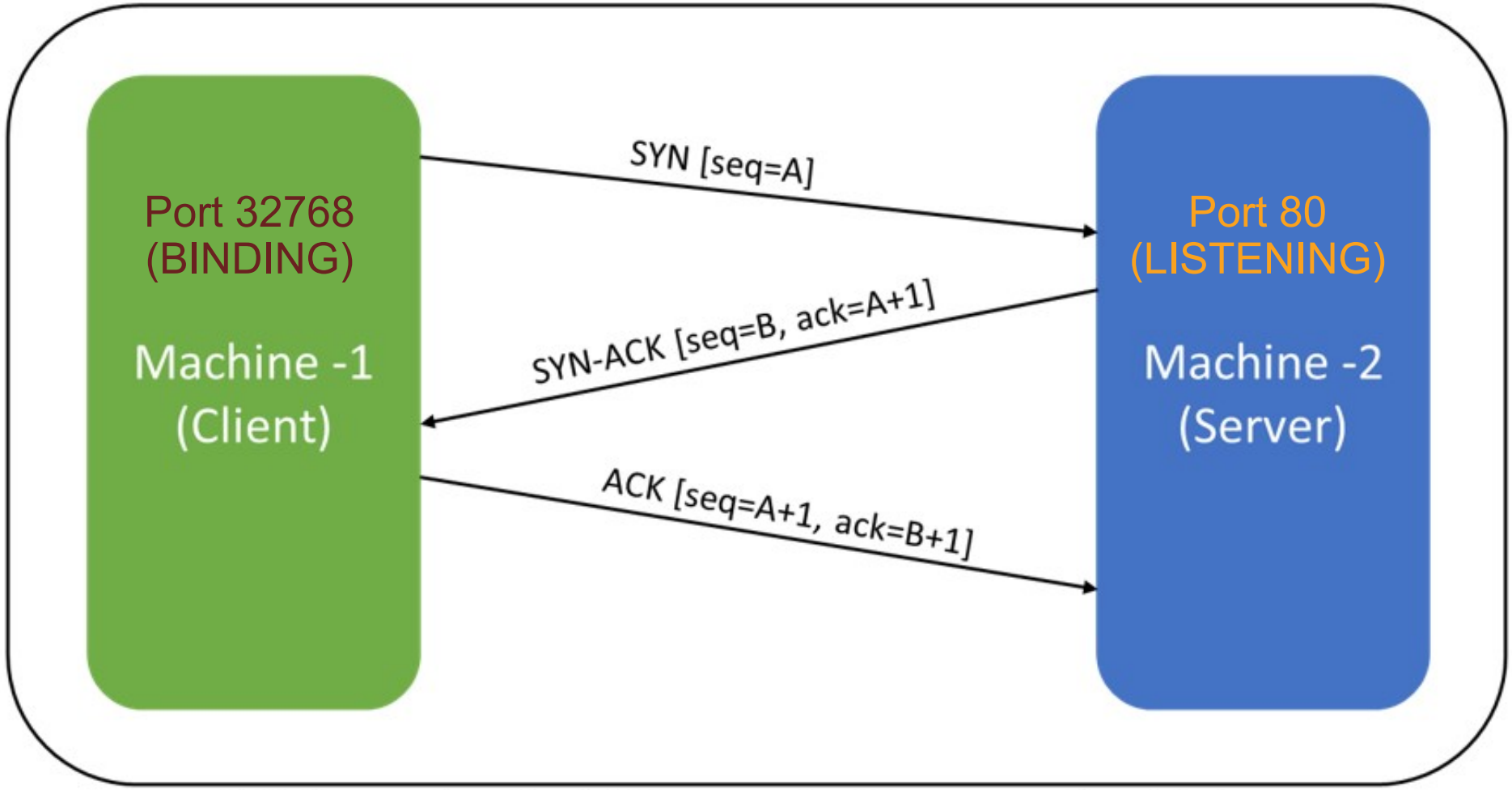
TCP

TCP:

- ориентирован на соединение
- надежная передача
- управление потоком



Установка соединения



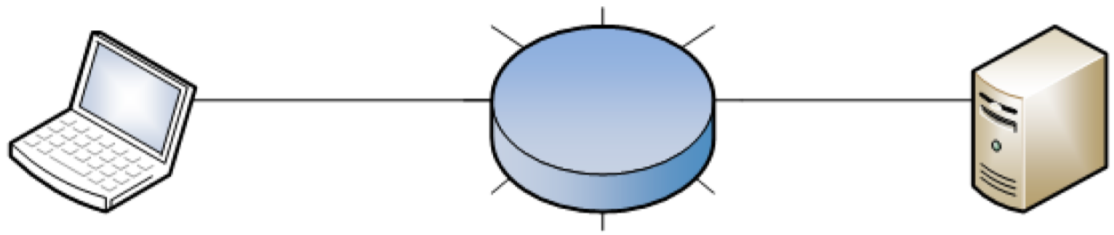
Технология подтверждений

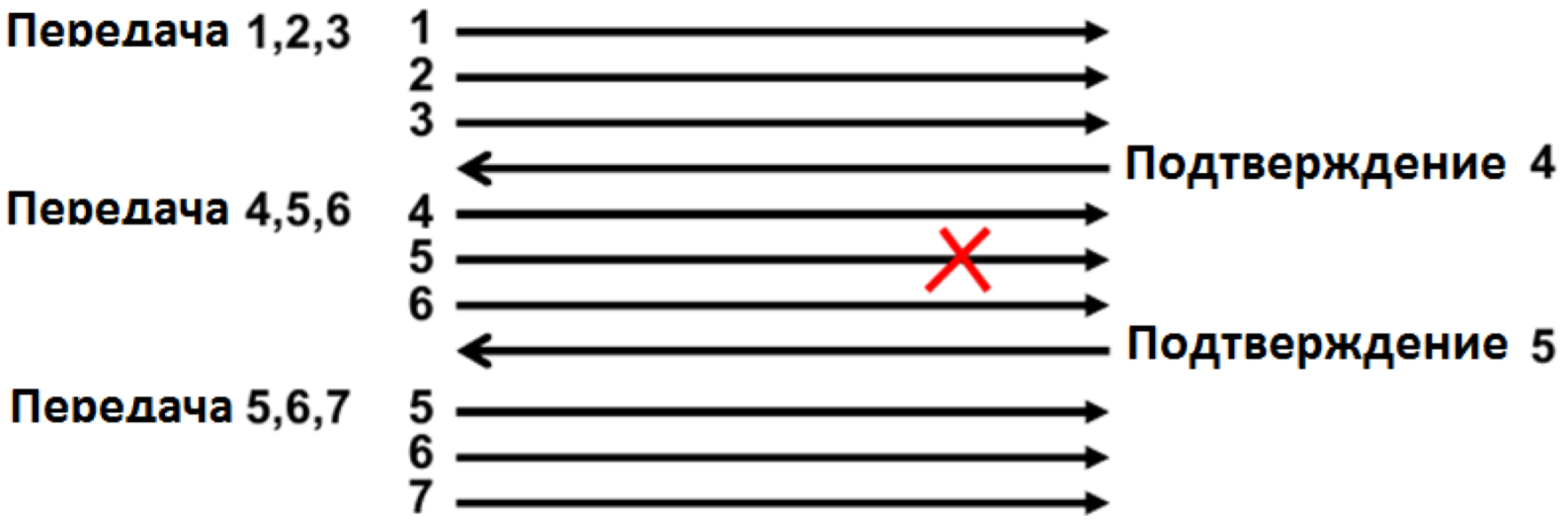
Synchronize (syn)

Синхронизировать

Acknowledge (ack)

Подтверждение





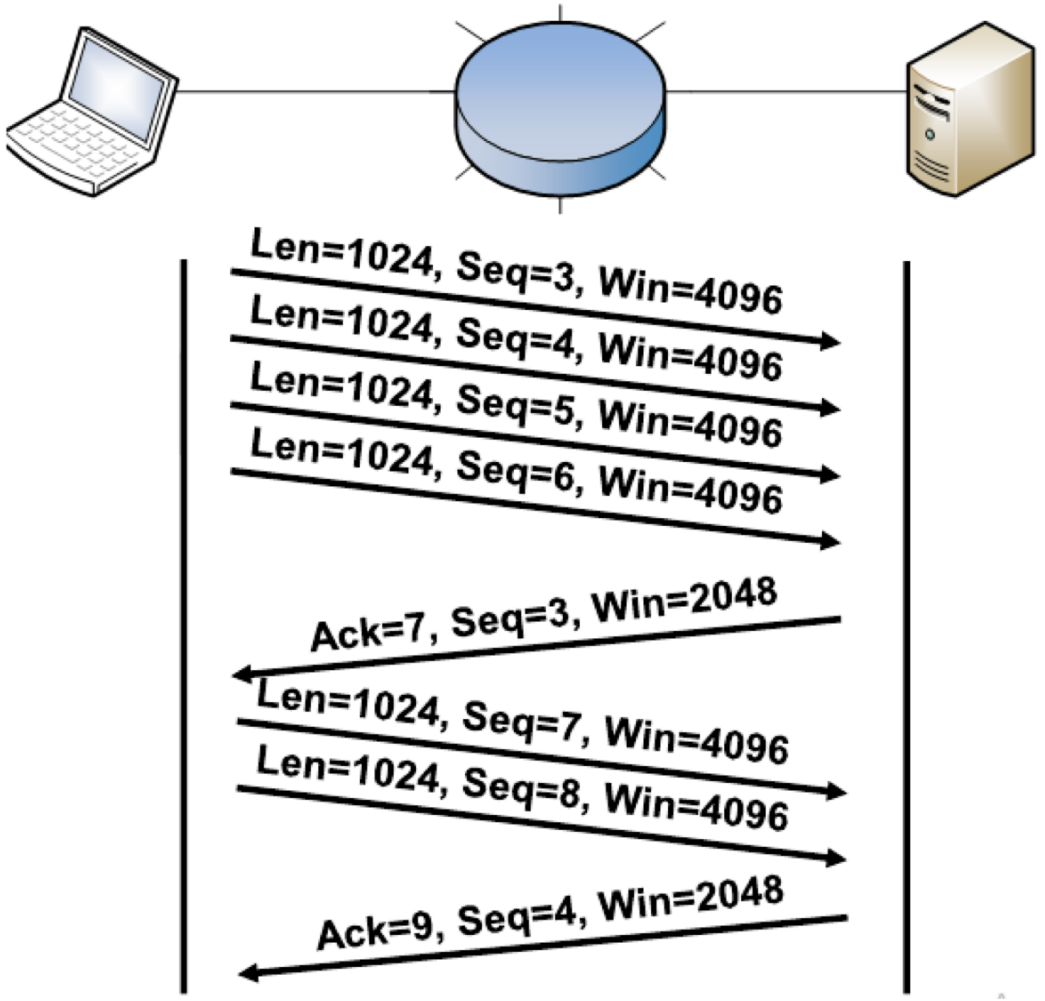
Изменение размера окна

Len= length (длина)

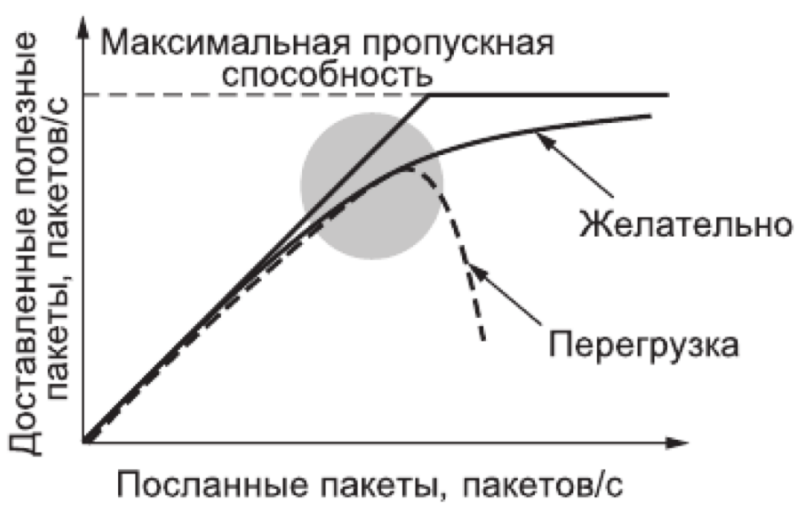
Seq= sequence

(номер сообщения в последовательности)

Win=window (размер окна)



Управление потоком



Методы управления потоком:

- Буферизация: поток данных буферизируется в ожидание паузы;
- Останавливающее сообщение: передача источником сообщения о снижение скорости передачи с помощью ICMP;
- Метод скользящего окна: управление кол-вом передаваемых данных в единицу времени.

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.

Например, при обращении к серверу geekbrains.ru на HTTP порт сокет будет выглядеть так: 5.61.239.21:80, а ответ будет поступать на mmm.nnn.ppp.qqq: xxxxx.

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

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) Закрыть сеанс связи и отправить сообщение о завершение соединения

SCTP

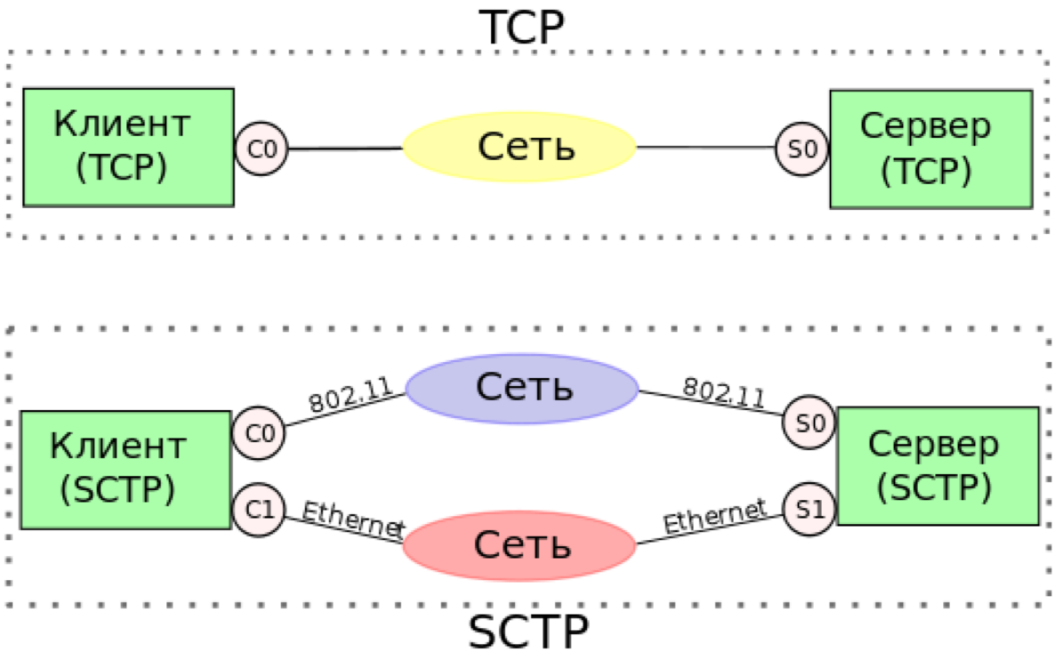
Транспортный протоколы развиваются, и встают новые задачи обработки групповых связанных потоков. Например, браузер может запрашивать с сервера несколько страниц, в этом случае создаются отдельные сокеты для каждого соединения.

SCTP (Stream Control Transmission Protocol — протокол передачи с управлением потоками), описанный в RFC 4960.

Протокол работает по аналогии с TCP. Из нововведений нужно выделить использование многопоточности и встроенную защиту от DDoS атак, в отличие от TCP.

SCTP

Протокол может использовать синхронное соединение хостов по нескольким независимым физическим каналам (multi-homing) например беспроводную и проводную сеть одновременно.



Процедура установления соединения (трехэтапное квитирование) в протоколе TCP

Процедура установления соединения (четырехэтапное квитирование) в протоколе SCTP

UDP

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

UDP:

- без установления соединения
- надежная передача.
- 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.

DCCP

Является усовершенствованным протоколом UDP, в который добавили механизм управления перегрузкой. Более подробную информацию по данному протоколу можно посмотреть в RFC 4340.

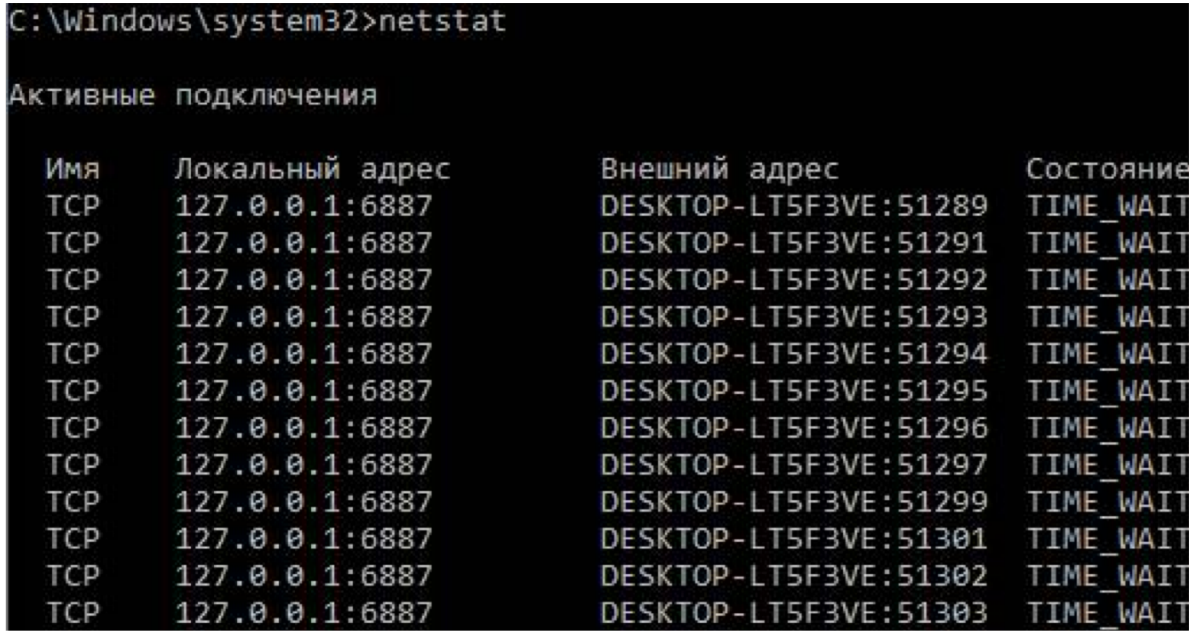
DCCP отличается следующими пунктами:

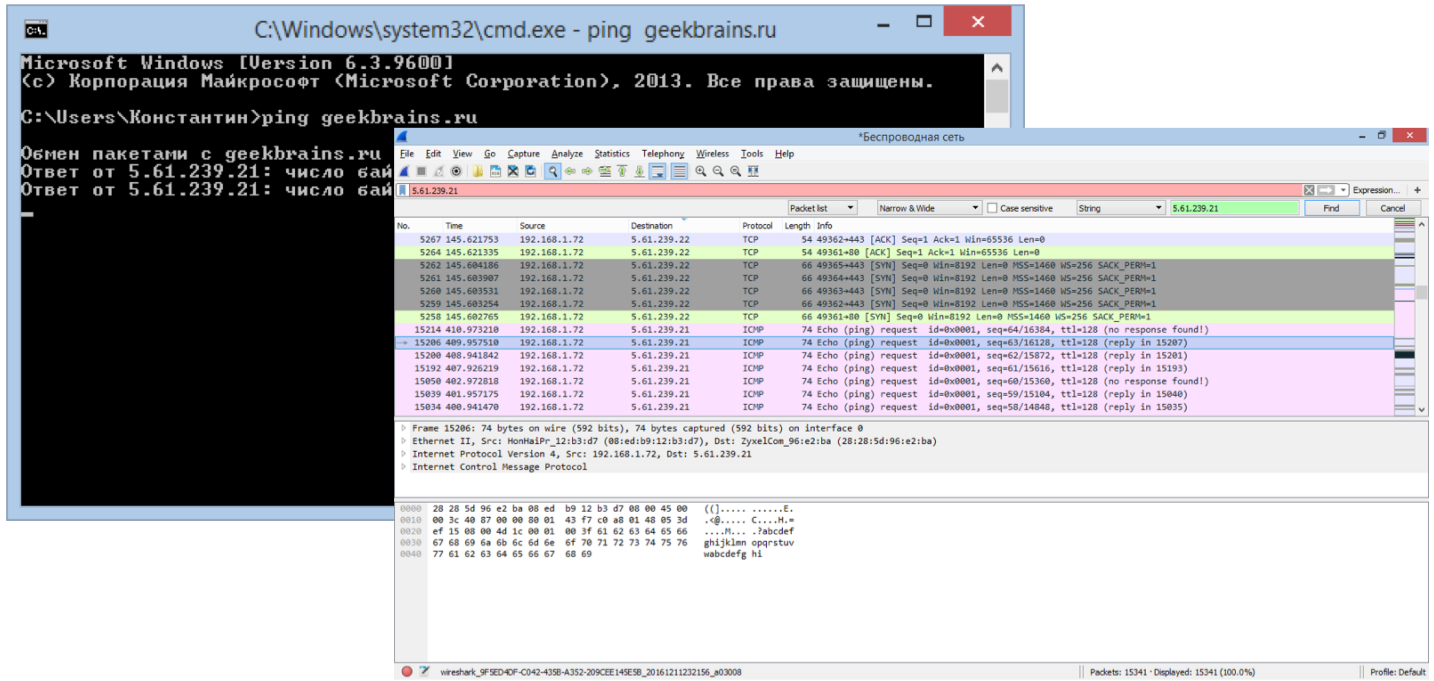
- поток дейтаграмм реализован с механизмом подтверждения получения данных, но без повторной отправки в случае потери данных;
- ненадежный алгоритм установления и закрытия соединения;
- согласование параметров передачи данных при установление соединения.

Практика

Утилита Netstat

Отслеживание установки соединения через анализатор сетевого трафика Wireshark





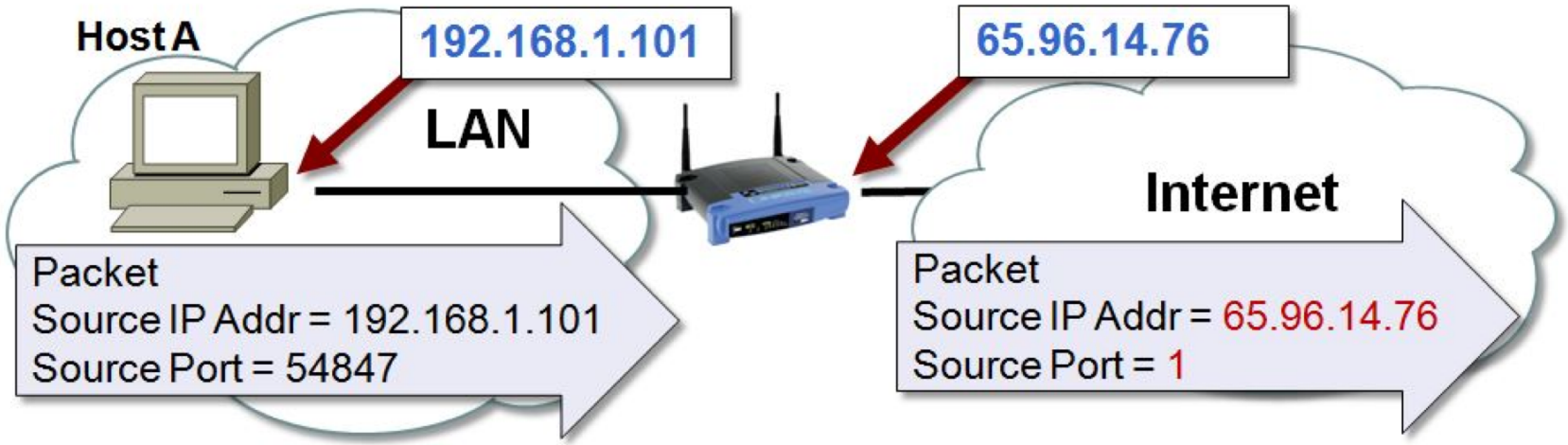
Технология NAT

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.

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

Destination NAT

Виртуальные серверы

ID	Порт сервиса	Внутренний порт	IP-Адрес	Протокол	Состояние	Изменить
1	8080	80	192.168.0.200	Все	Включено	Редактировать Удалить
2	8088	80	192.168.0.201	Все	Включено	Редактировать Удалить
3	8000	80	192.168.0.202	Все	Включено	Редактировать Удалить

Добавить новую... | Включить все | Отключить все | Удалить все

Практика

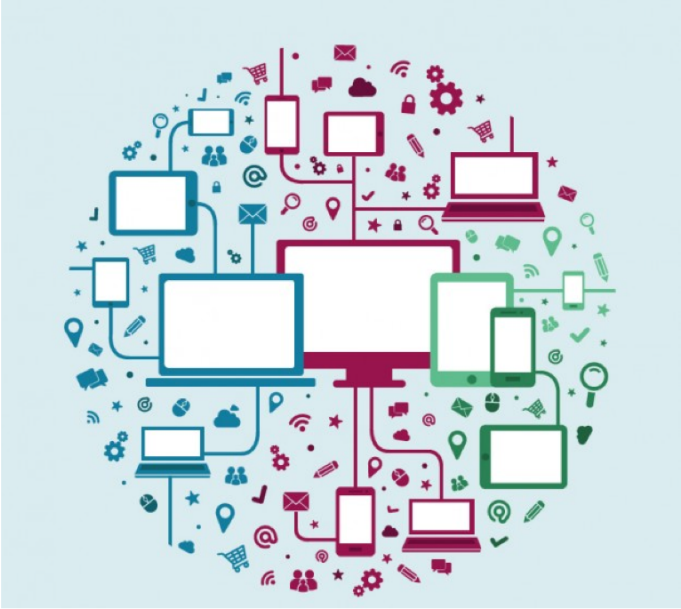
Настройка NAT/PAT в Cisco PT.

Анализ трафика в Cisco PT

Практическое задание

1. Работа с Wireshark. Изучение протоколов TCP, UDP
2. Настройка перегруженного NAT в Cisco Packet Tracer

Вопросы?



На следующем занятии…

Углубленное изучение сетевых технологий. Часть 1