Глава 9. Транспортный уровень

Материалы для инструктора

CCNA Routing and Switching

Введение в сетевые технологии (v6.0)

Материалы для инструктора — руководство по планированию главы 9

- Эта презентация PowerPoint состоит из двух частей:
- Руководство по планированию для инструкторов
  - Ознакомительная информация по главе
  - Методические пособия
- Презентация перед классом для инструктора
  - Дополнительные слайды, которые можно использовать в классе
  - Начало на слайде № 13

- **Примечание.** Перед предоставлением общего доступа удалите руководство по планированию из данной презентации.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 9. Транспортный уровень

Introduction to Networks 6.0.
Руководство по планированию

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 9. Упражнения

Страница №	Тип упражнения	Название упражнения	Необязательно?
9.0.1.2	Работа в аудитории	Игра «Нам нужно поговорить»	Необязательно
9.1.2.10	Интерактивное упражнение	Сравнение характеристик протоколов TCP и UDP	Рекомендуется
9.2.1.5	Демонстрационный видеоролик	Трехэтапное квитирование TCP	Рекомендуется
9.2.1.6	Лабораторная работа	Наблюдение за процессом трехстороннего квитирования протокола TCP с помощью программы Wireshark	Рекомендуется
9.2.1.7	Интерактивное упражнение	Процесс установки подключения TCP и завершения сеанса	Рекомендуется
9.2.2.2	Демонстрационный видеоролик	Надежность TCP: порядковые номера и подтверждения	Рекомендуется
9.2.2.3	Демонстрационный видеоролик	Надежность TCP: потеря данных и повторная передача	Рекомендуется
9.2.3.5	Лабораторная работа	Изучение захваченных пакетов DNS и UDP с помощью программы Wireshark	Рекомендуется
9.2.4.3	Лабораторная работа	Изучение захваченных пакетов TCP и UDP с помощью программы Wireshark	Рекомендуется
9.2.4.4	Интерактивное упражнение	Протокол TCP или UDP	Рекомендуется

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 9. Упражнения

Страница №	Тип упражнения	Название упражнения	Необязательно?
9.3.1.1	Работа в аудитории	Игра «Нам снова нужно поговорить»	Необязательно
9.3.1.2	Packet Tracer	Обмен данными с использованием TCP и UDP	Необязательно

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 9. Проверочная работа

- После прохождения главы 9 учащиеся должны выполнить проверочную работу на знание материала главы 9.
- Для неформальной оценки успехов учащихся можно использовать контрольные работы, лабораторные работы, работу с симулятором Packet Tracer и другие упражнения.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 9. Практические рекомендации

Прежде, чем излагать материал главы 9, обратите внимание на следующее:

- Инструктор должен выполнить проверочную работу на знание материала главы 9.
- Цели этой главы:
  - Объяснить роль транспортного уровня в процессе передачи данных по сквозному каналу связи.
  - Объяснить характеристики протоколов TCP и UDP, включая номера портов и способы их применения.
  - Объяснить, каким образом процессы установления и завершения сеанса TCP позволяют обеспечить надежный обмен данными
  - Объяснить, каким образом передаются единицы данных протокола TCP и как подтверждается их гарантированная доставка
  - Описать клиентские процессы UDP для установления связи с сервером
  - Определить, какой вид передачи данных наиболее оптимален для распространённых приложений: высоконадёжная передача TCP или негарантированная передача UDP.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 9. Практические рекомендации (продолжение)

- Перед началом изучения этой главы повторите модель OSI и стек протоколов TCP/IP.
- Изучите процесс инкапсуляции, чтобы подготовиться к обзору этой главы.
- Опишите основные принципы сегментации и мультиплексирования (необходимые для сегментации передаваемых данных)
- Объясните предназначение двух протоколов транспортного уровня — UDP и TCP.
- Обсудите преимущества и недостатки протоколов TCP и UDP.
- Объясните необходимость идентификации сегментов с помощью порядковых номеров, чтобы в месте назначения их можно было собрать обратно в правильном порядке.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 9. Практические рекомендации (продолжение)

- Рассмотрите несколько одновременных сеансов обмена данными на хосте и хосте назначения, а также объясните необходимость сообщать верхним уровням, какое приложение использовать для обработки данных.
- Опишите процесс установки подключения и завершения сеанса связи, понятие надежности в отношении доставки, управление процессами и цель каждого из этих аспектов.
- Отдельно подчеркните такие процессы обеспечения надежности, как отслеживание сегментов, подтверждение и повторная передача.
- Объясните использование номеров портов, чтобы определить соответствующее приложение для каждого потока данных.
- Студенты должны запомнить наиболее часто используемые номера портов.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 9. Практические рекомендации (продолжение)

- Используйте программу Wireshark для проверки перехвата пакетов FTP и TFTP. В качестве демонстрации выполните лабораторную работу в разделе 9.2.4.3.
- Следующий видеоролик подходит для студентов средней школы и содержит объяснение различий между протоколами TCP и UDP: https://www.youtube.com/watch?v=KSJu5FqwEMM
- Обсудите, какие приложения и службы используют протокол UDP и/или TCP.
- Спросите студентов, какие службы и приложения они используют, и определите, используется ли в них протокол UDP, TCP или оба.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Глава 9. Дополнительные справочные материалы

- Дополнительные справочные материалы, содержащие различные стратегии обучения, в том числе планы занятий, описание аналогий для сложных понятий и темы обсуждений, доступны на веб-сайте сообщества сертифицированных сетевых специалистов (CCNA) по адресу https://www.netacad.com/group/communities/community-home.
- Практические рекомендации специалистов со всего мира для обучения по программе CCNA Routing and Switching. https://www.netacad.com/group/communities/ccna
- Если вы хотите поделиться с другими преподавателями планами занятий и другой полезной информацией, вы можете разместить её на сайте сообщества CCNA.
- Студенты могут записаться на курс **Introduction to Packet Tracer** (Введение в Packet Tracer) (для самостоятельного изучения)

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

CISCO

Глава 9. Транспортный уровень

CCNA Routing and Switching

Введение в сетевые технологии (v6.0)

Глава 9. Разделы и задачи

- 9.1. Протоколы транспортного уровня
  - Объяснить, каким образом протоколы и сервисы транспортного уровня реализуют коммуникацию в сетях передачи данных
    - Объяснить роль транспортного уровня в процессе передачи данных по сквозному каналу связи.
    - Объяснить характеристики протоколов TCP и UDP, включая номера портов и способы их применения.
- 9.2. Протоколы TCP и UDP
  - Сравнить операции протоколов транспортного уровня при поддержке сквозного канала связи
    - Объяснить, каким образом процессы установления и завершения сеанса TCP позволяют обеспечить надежный обмен данными
    - Объяснить, каким образом передаются единицы данных протокола TCP и как подтверждается их гарантированная доставка
    - Описать клиентские процессы UDP для установления связи с сервером
    - Определить, какой вид передачи данных наиболее оптимален для распространённых приложений: высоконадёжная передача TCP или негарантированная передача UDP.

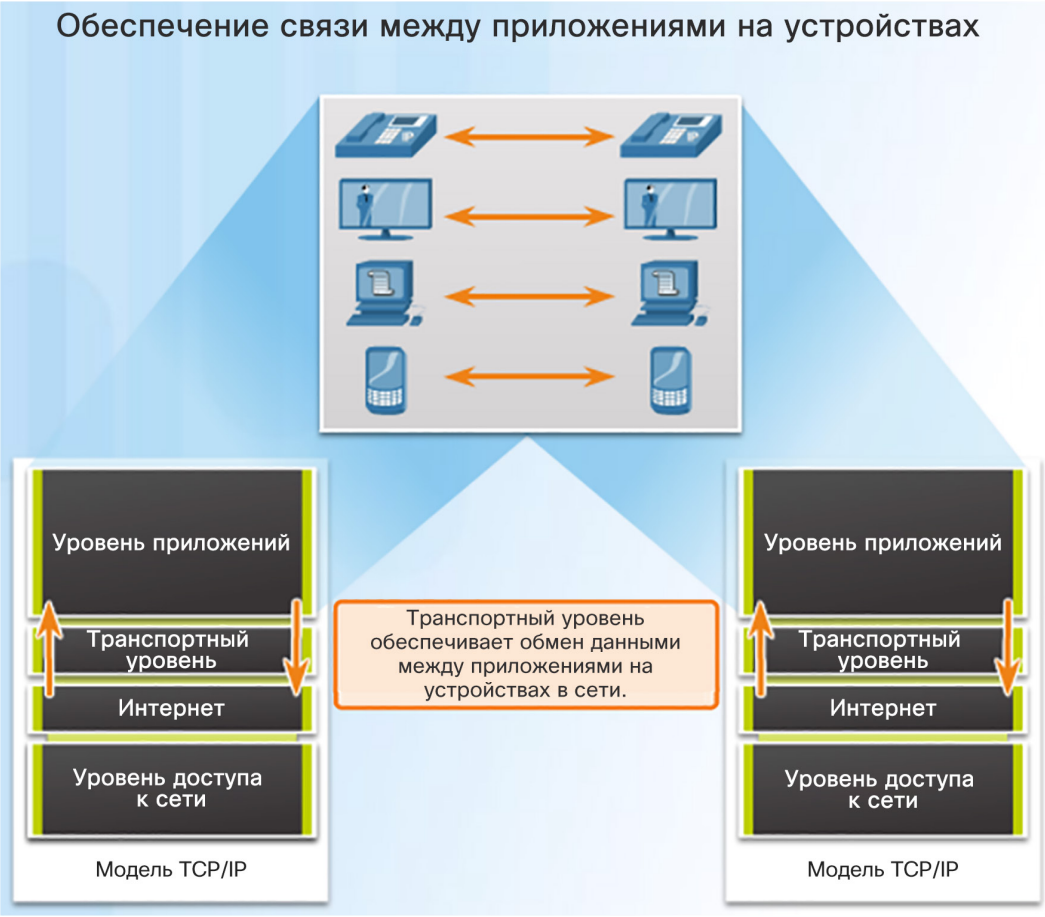
© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

9.1. Протоколы транспортного уровня

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

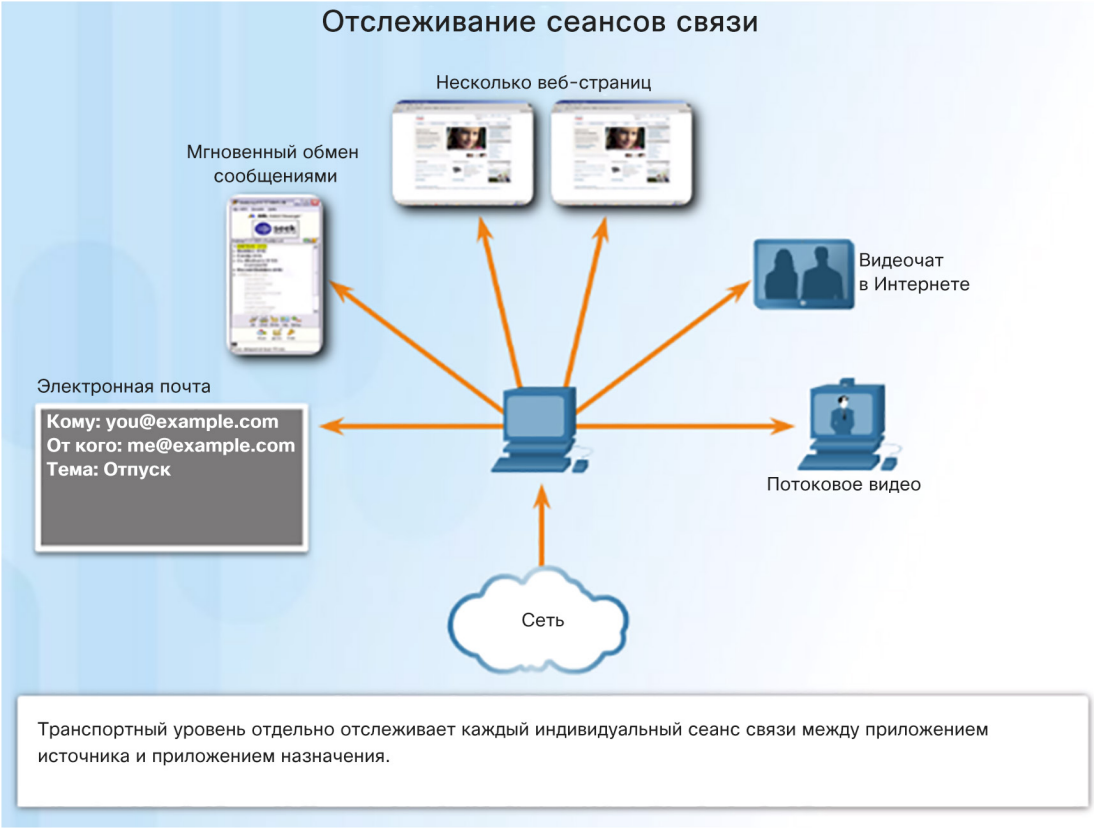
Роль транспортного уровня

- Выполняет установку временного сеанса связи между двумя приложениями и доставку данных между ними.
- Связь между уровнем приложений и нижними уровнями, которые отвечают за передачу данных по сети.



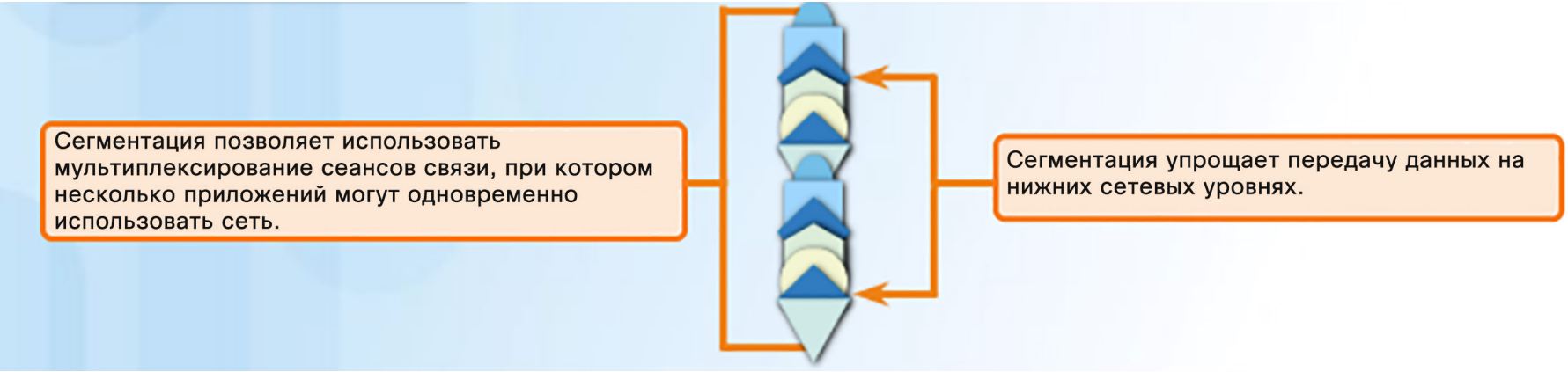
Функции транспортного уровня

- **Отслеживание сеансов связи.** Транспортный уровень отдельно отслеживает каждый индивидуальный сеанс связи между приложением источника и приложением назначения.
- **Сегментация**. Транспортный уровень разделяет данные на сегменты, которые проще контролировать и передавать. Заголовок, используемый для дефрагментации сегментов, используется для отслеживания.
- **Идентификация приложения**. Транспортный уровень гарантирует, что, даже если на устройстве запущено несколько приложений, все они получат правильные данные.



Мультиплексирование сеансов связи

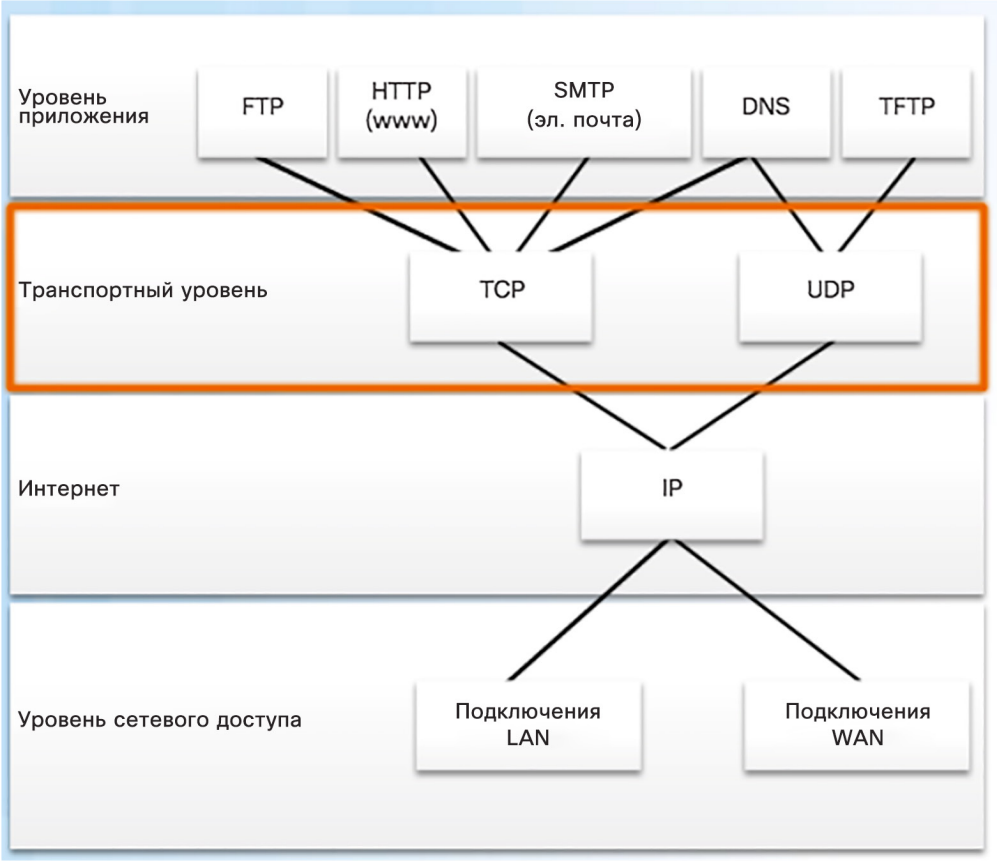
- Сегментация данных на более мелкие блоки позволяет осуществлять большое количество разных сеансов передачи данных в одной и той же сети.



© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

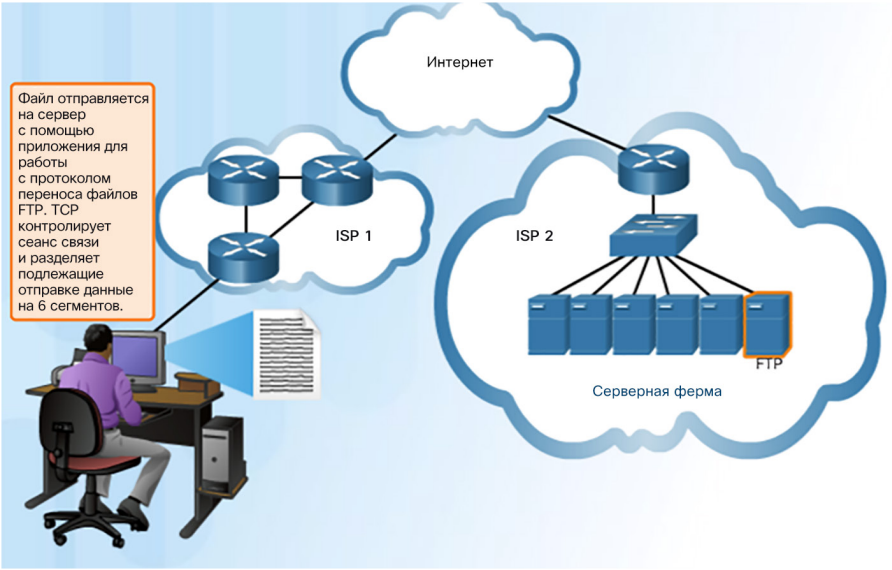
Надежность транспортного уровня

- TCP/IP предоставляет два протокола транспортного уровня:
  - Протокол управления передачей (TCP)
    - Считается надежным протоколом, гарантируя доставку всех данных к месту назначения.
    - Дополнительные поля, необходимые в заголовке, увеличивают размер и задержки.
  - Протокол пользовательских датаграмм (UDP)
    - Протокол не гарантирует надежности.
    - Он имеет меньше полей, поэтому быстрее, чем TCP.

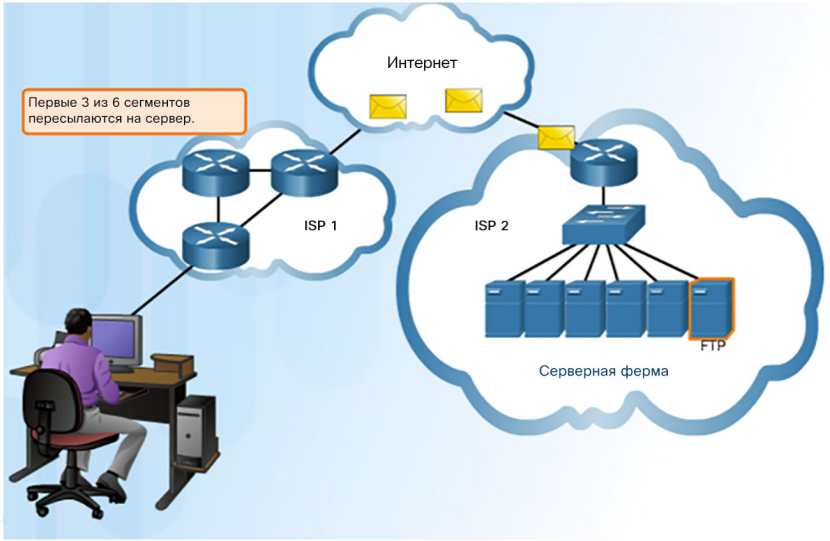


© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

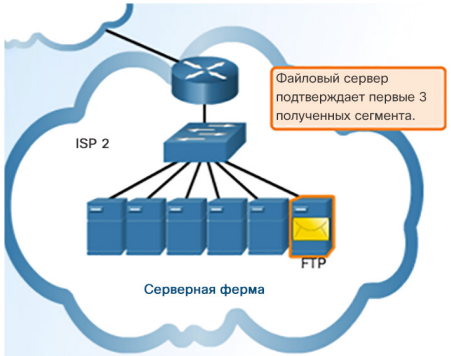
Протокол TCP

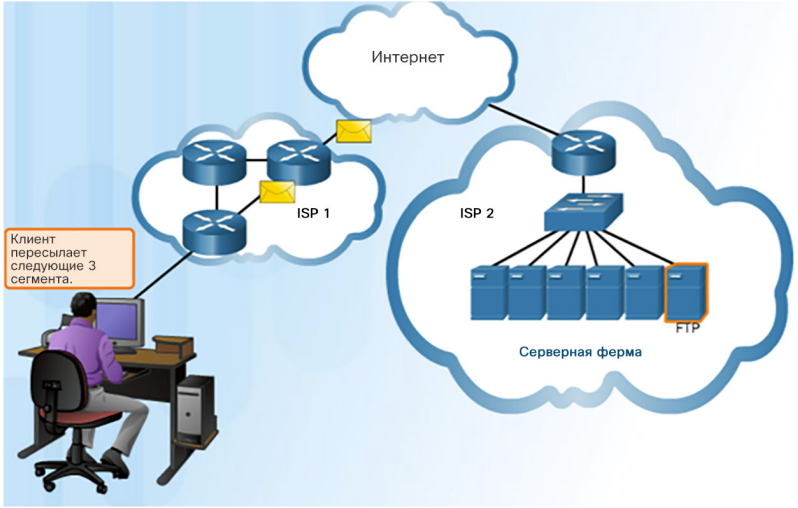


- Передача данных по протоколу TCP аналогична отправке отслеживаемых пакетов. Если заказ разбит на несколько частей, заказчик может зайти на веб-сайт транспортной компании и посмотреть порядок доставки.



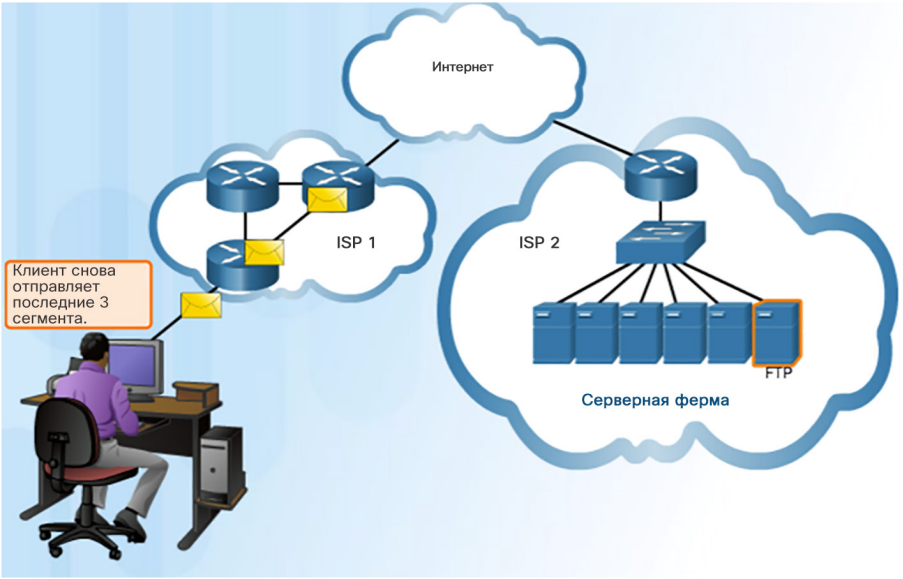
Протокол TCP (продолжение)





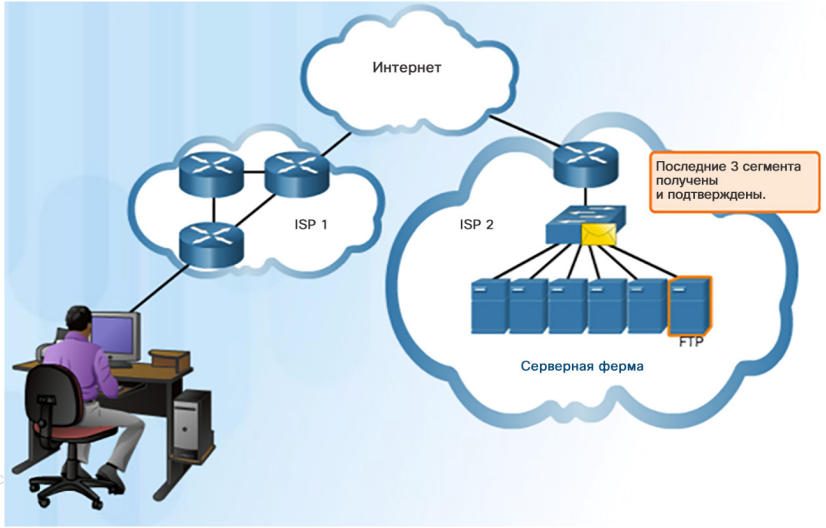
© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Протокол TCP (продолжение)



Три функции TCP:

- Нумерация и отслеживание сегментов данных
- Подтверждение полученных данных
- Повторная передача сегментов с неподтвержденными данными по истечении определенного времени ожидания.

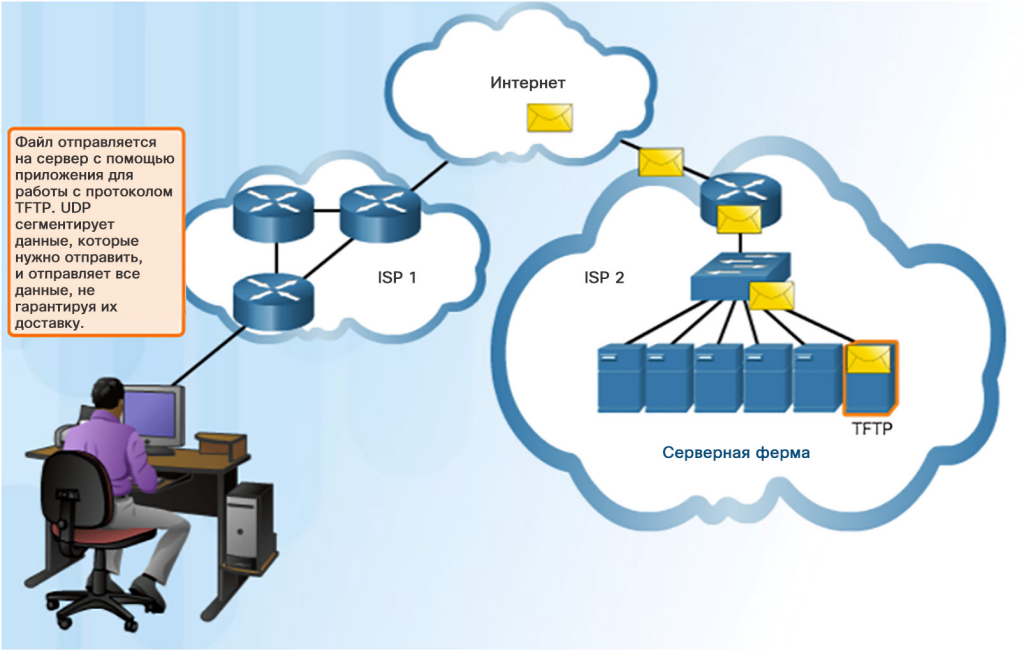


© Cisco

Протокол UDP

Протокол UDP создает меньшую нагрузку на сеть и сокращает возможные задержки.

- Негарантированная доставка (ненадежный протокол)
- Подтверждение не предоставляется
- Передача данных похожа на отправку простого письма



© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Соответствующий протокол транспортного уровня для соответствующего приложения

- Протокол TCP. Базам данных, веб-обозревателям и клиентским программам для работы с электронной почтой необходимо, чтобы все отправленные данные поступили на узел назначения в своем первоначальном состоянии.
- Протокол UDP. Если один или два сегмента потока видеоданных в реальном времени не будут доставлены или произойдет перебой в потоке, пользователь может этого не заметить.

UDP

IP-телефония

Видеотрансляция в реальном времени

Требования к протоколу:
- Высокая скорость
- Низкие накладные расходы
- Не требуются подтверждения
- Нет повторной отправки потерянных данных
- Обработка данных в том порядке, в каком они были получены

TCP

SMTP/POP (электронная почта)

HTTP

Требования к протоколу:
- Надежность
- Подтверждение данных
- Повторная отправка потерянных данных
- Доставка данных в порядке их отправки

Функции протокола TCP

- Установление сеанса связи
  - Является протоколом с установлением соединения
  - Проверяет, что приложение готово к получению данных
  - Согласует объем трафика, который можно переслать в заданное время
- Надежность доставки
  - Обеспечивает гарантированную доставку на узел назначения всех без исключения сегментов данных, отправленных источником
- Доставка в одинаковом порядке
  - Нумерация и определение последовательности сегментов гарантирует их повторную дефрагментацию в правильном порядке
- Управление потоком передачи данных
  - Регулирует объем данных, передаваемый источником

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Заголовок протокола TCP

- Порты источника и назначения используются для идентификации приложения
- Порядковый номер используется для повторной дефрагментации данных
- Номер подтверждения указывает, что данные были получены и порт назначения готов принять следующий байт из источника
- Длина заголовка — длина заголовка сегмента TCP
- Управляющие биты — назначение и функция сегмента TCP
- Размер окна — количество байтов, которые можно принять единовременно
- Контрольная сумма — используется для проверки ошибок заголовка и данных сегмента

Всего 20 байт

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Функции протокола UDP

Функции UDP

- Данные восстанавливаются в том порядке, в котором получены.
- Потерянные сегменты повторно не отправляются.
- Без установления сеанса связи.
- Без уведомления отправителя о доступности ресурса.

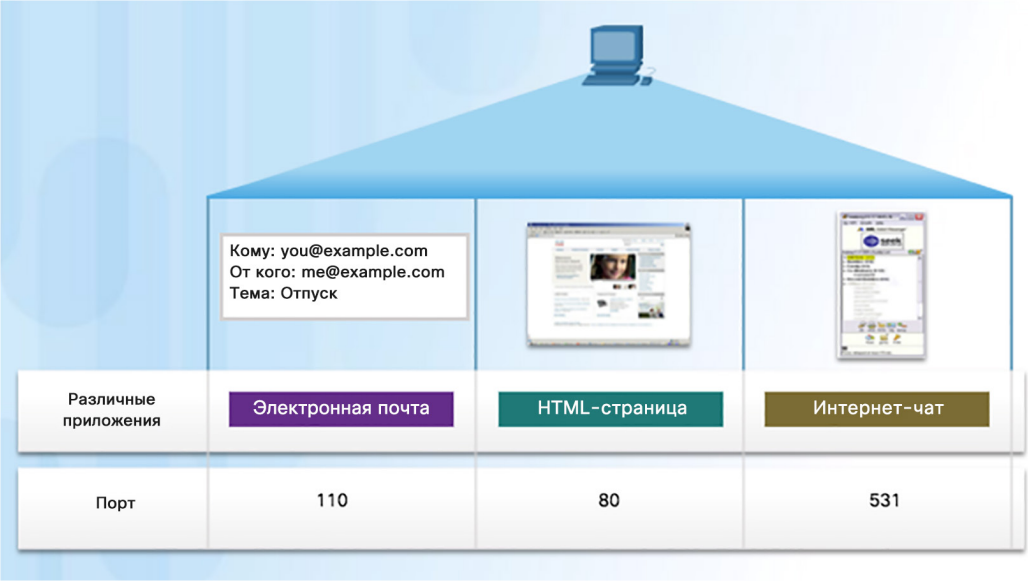
Заголовок протокола UDP

- UDP — это протокол без сохранения состояния (сегменты данных не отслеживаются)
- Надежность определяется приложением

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Несколько отдельных сеансов передачи данных

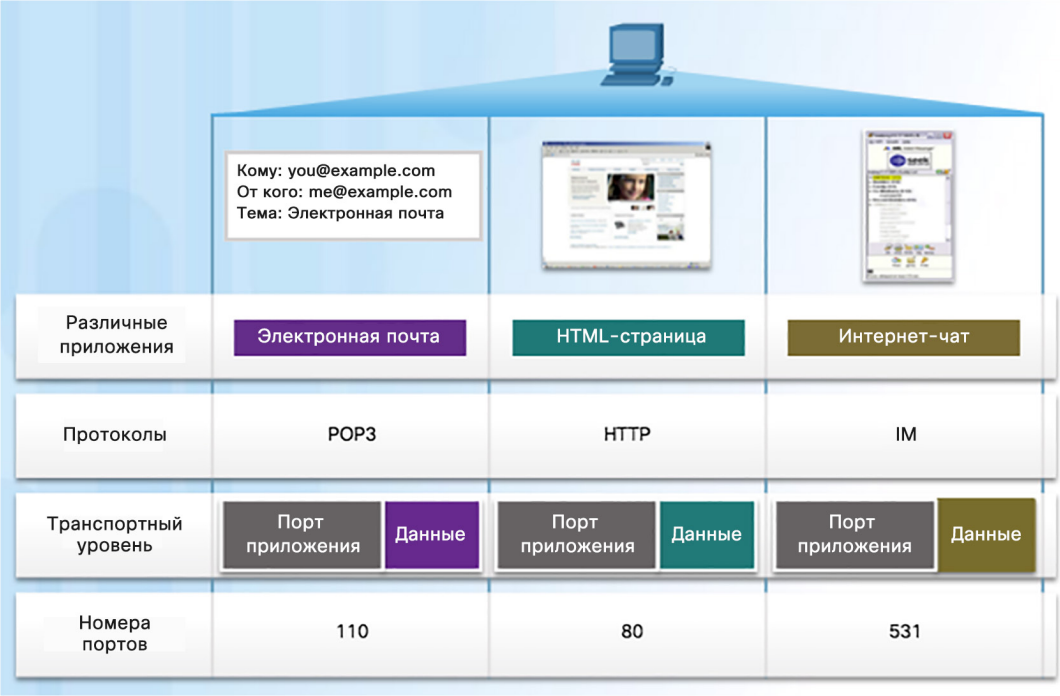
- Пользователи должны иметь возможность одновременно получать и отправлять электронные письма, просматривать веб-сайты и совершать звонки по телефону посредством VoIP.
- Протоколы TCP и UDP управляют несколькими сеансами передачи данных с помощью уникальных идентификаторов, которые называются номерами портов.



© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Номера портов

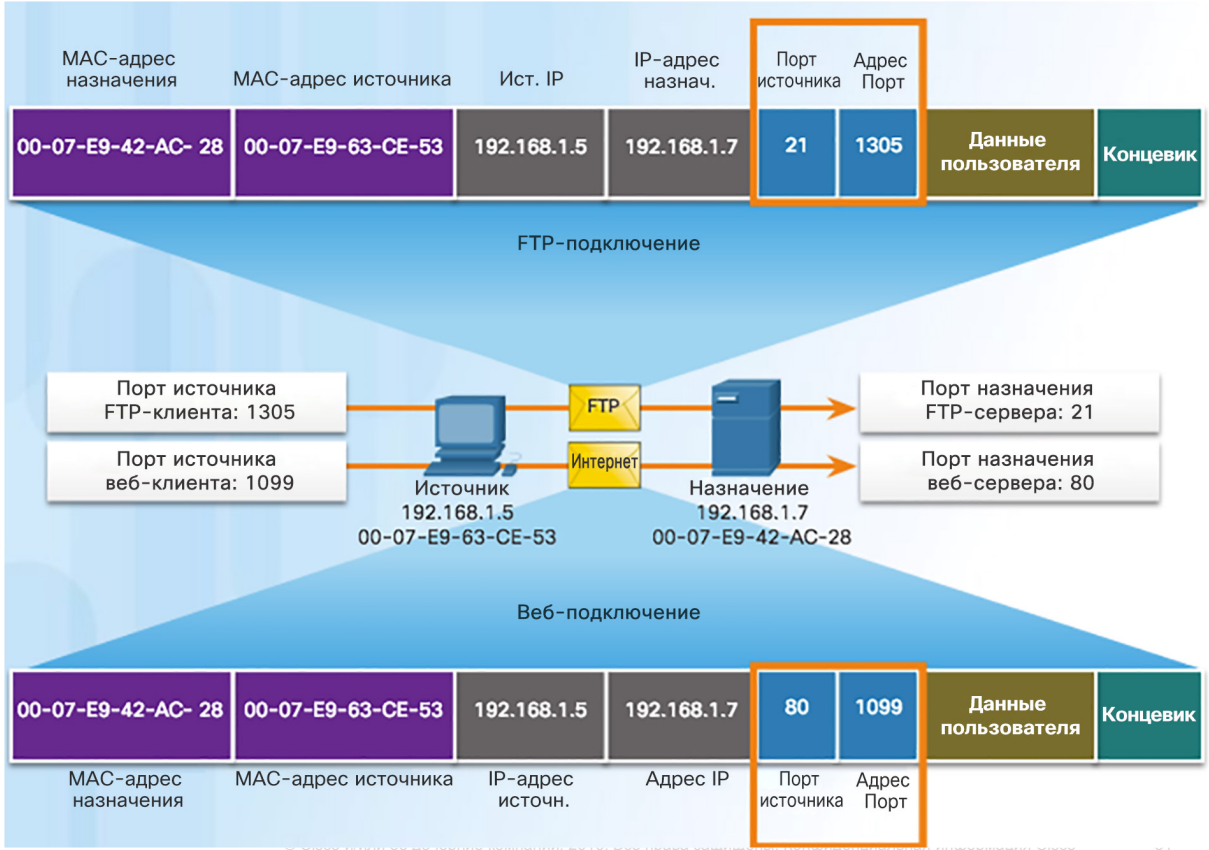
- Порт источника
  - Порт исходного приложения, который динамически создается устройством-отправителем.
  - Пример. Отдельные сеансы связи по протоколу HTTP отслеживаются по номерам портов источника.
- Порт назначения
  - Сообщает устройству назначения, какая служба запрашивается.
  - Пример. Порт 80 — запрашиваются веб-сервисы.



© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Пары сокетов

- Порты источника и назначения помещаются в сегмент
- Сегменты инкапсулируются в IP-пакет
- IP-адрес и номер порта = сокет
- Пример. 192.168.1.7:80
- Сокеты позволяют распознавать различные процессы
- Порт источника выступает в качестве обратного адреса



Группы номеров портов

Диапазон номеров портов	Группа портов
От 0 до 1023	Общеизвестные порты
От 1024 до 49151	Зарегистрированные порты
От 49152 до 65535	Частные и/или динамические порты

- Общеизвестные порты (номера от 0 до 1023). Эти номера зарезервированы для сервисов и приложений.
- Зарегистрированные порты (номера 1024–49151). IANA по запросу организаций присваивает данные порты для каких-либо специфичных процессов или приложений.
- Динамические или частные порты (номера от 49152 до 65535). Обычно динамически назначаются ОС клиента и используются для идентификации клиентского приложения во время сеанса связи.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Группы номеров портов (продолжение)

Общеизвестные номера портов

Номер порта	Протокол	Применение	Сокращение
20	TCP	File Transfer Protocol (Протокол передачи файлов) (данные)	FTP
21	TCP	File Transfer Protocol (Протокол передачи файлов) (управление)	FTP
22	TCP	Протокол Secure Shell	SSH
23	TCP	Telnet	–
25	TCP	Simple Mail Transfer Protocol (Протокол простого обмена электронной почтой)	SMTP
53	UDP, TCP	Domain Name Service (Служба доменных имен) (DNS)	DNS
67	UDP	Dynamic Host Configuration Protocol (Протокол динамической настройки узла) (сервер)	DHCP
68	UDP	Dynamic Host Configuration Protocol (Протокол динамической настройки узла) (клиент)	DHCP
69	UDP	Trivial File Transfer Protocol (Простейший протокол передачи файлов)	TFTP
80	TCP	Hypertext Transfer Protocol (Протокол передачи гипертекста)	HTTP
110	TCP	Post Office Protocol (Протокол почтового отделения) (версия 3)	POP3
143	TCP	Internet Message Access Protocol (Протокол доступа к сообщениям в Интернете)	IMAP
161	UDP	Simple Network Management Protocol (Простой протокол управления сетью)	SNMP
443	TCP	Hypertext Transfer Protocol Secure (Протокол защищенной передачи гипертекста)	HTTPS

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Команда netstat

- Сетевая утилита, которую можно использовать для проверки соединений.
- По умолчанию пытается разрешить IP-адреса в доменные имена, а номера портов — в названия общеизвестных приложений.
- Параметр -n используется для отображения IP-адресов и портов в числовой форме.

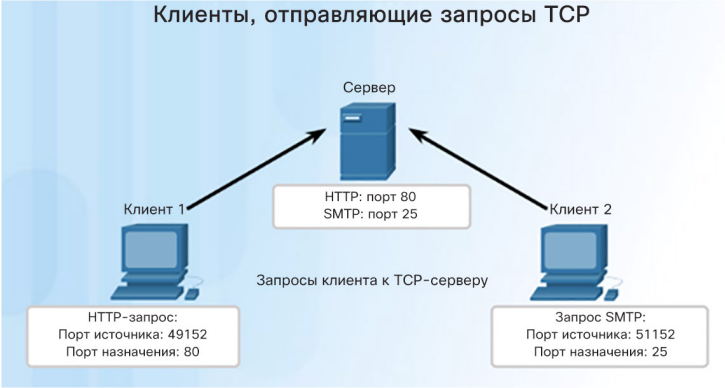
```
C:\> netstat

Active Connections

Proto  Local Address  Foreign Address          State
TCP    kenpc:3126     192.168.0.2:netbios-ssn  ESTABLISHED
TCP    kenpc:3158     207.138.126.152:http     ESTABLISHED
TCP    kenpc:3159     207.138.126.169:http     ESTABLISHED
TCP    kenpc:3160     207.138.126.169:http     ESTABLISHED
TCP    kenpc:3161     sc.msn.com:http          ESTABLISHED
TCP    kenpc:3166     www.cisco.com:http       ESTABLISHED

C:\>
```

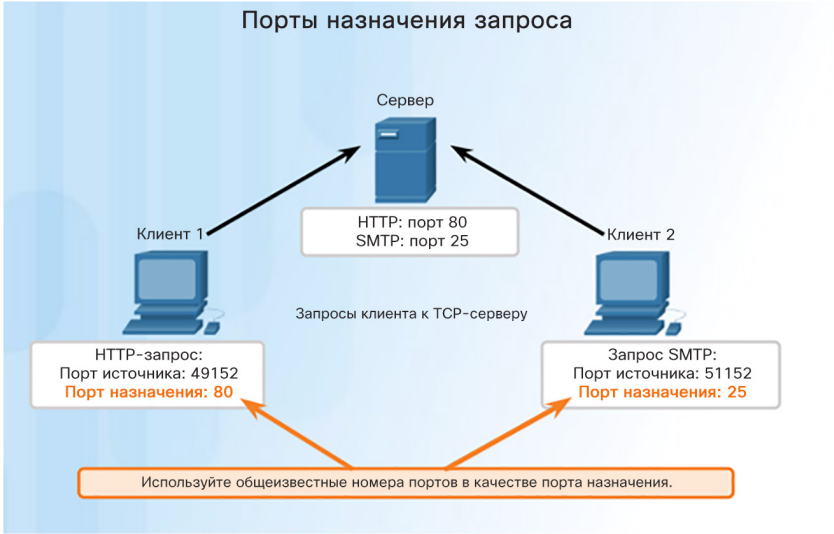
© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

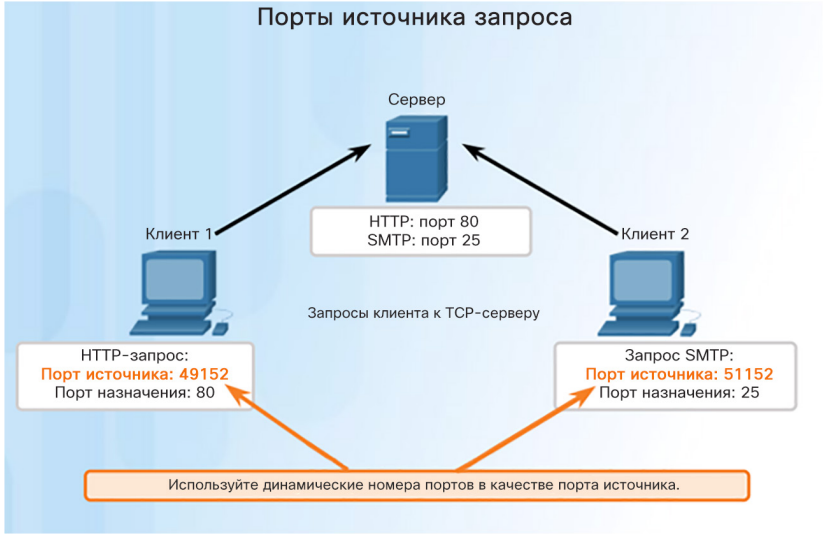
9.2. Протоколы TCP и UDP

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Процесс TCP-сервера

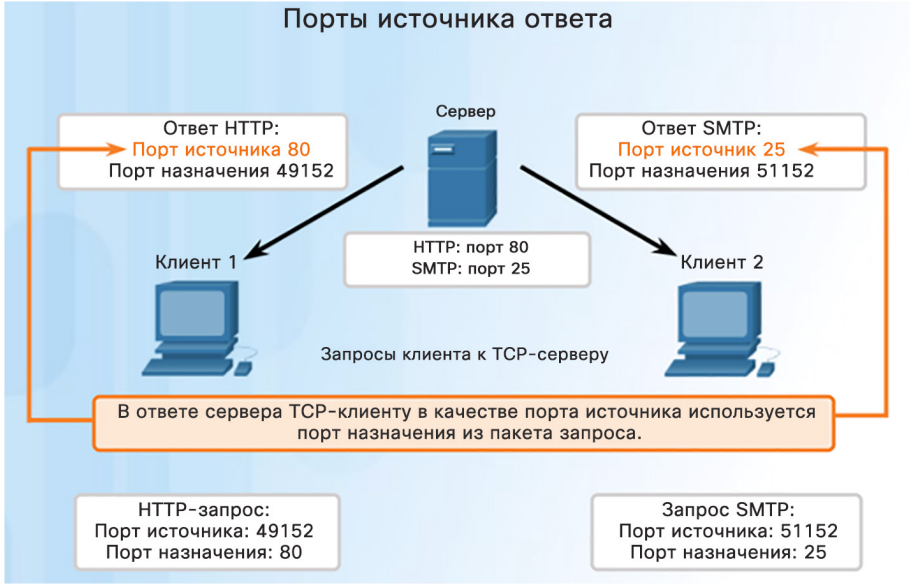






© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

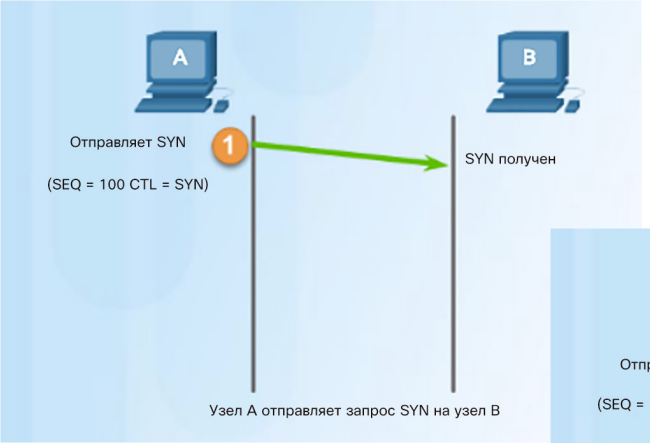
Процесс TCP-сервера (продолжение)



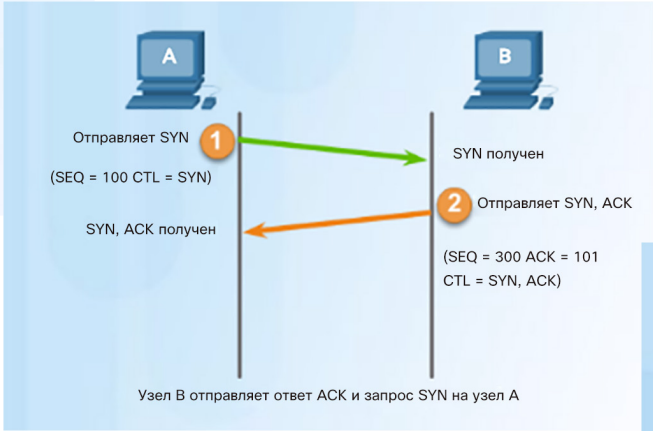
cisco
©

Процесс обмена данными по протоколу TCP

Установление TCP-соединения

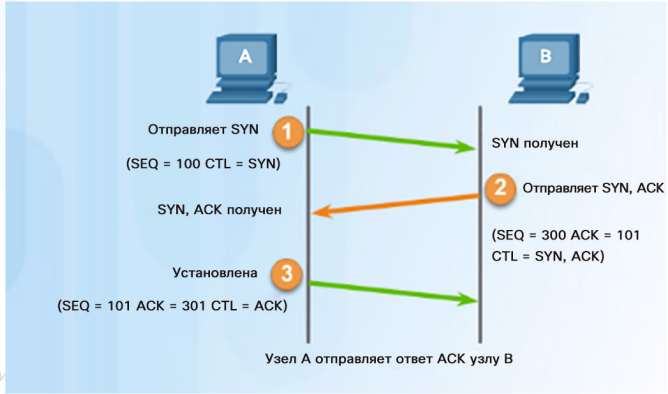


- Шаг 1. Инициирующий клиент запрашивает сеанс связи с сервером.



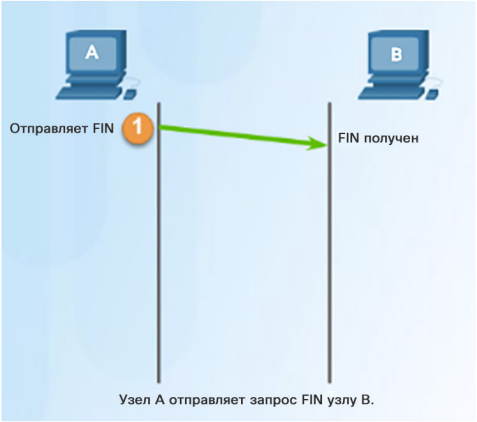
- Шаг 2. Сервер подтверждает и запрашивает сеанс связи с клиентом.

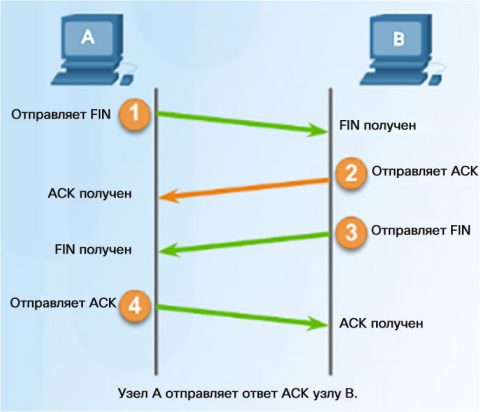
- Шаг 3. Клиент подтверждает сеанс связи с сервером.



© Cisco и/или ее дочерние компании

Прекращение TCP-соединения





- Для прекращения соединения в заголовке сегмента должен быть установлен управляющий флаг Finish (FIN).
- Для завершения каждого одностороннего TCP-сеанса используется двухстороннее квитирование (рукопожатие), которое состоит из сегмента FIN и сегмента ACK (подтверждение).
- Чтобы завершить один сеанс связи, поддерживаемый протоколом TCP, необходимы четыре операции обмена данными, которые завершат оба сеанса.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Анализ трехстороннего квитирования TCP

- Трехстороннее квитирование:
  - Сначала устанавливается, присутствует ли устройство назначения в сети
  - Затем проверяется, имеется ли на устройстве назначения активный сервис и принимает ли он запросы на номер порта назначения, который инициирующий клиент планирует использовать.
  - Далее устройству назначения сообщается, что клиент источника планирует установить сеанс связи на этом номере порта
- Шесть битов в поле битов управления в заголовке сегмента TCP называются флагами.
  - Флаг RST используется для сброса соединения при возникновении ошибки или в случае превышения времени ожидания.

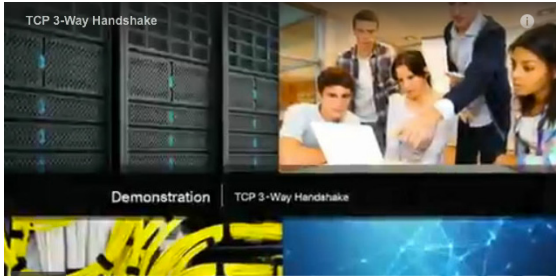
© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Демонстрационный видеоролик. Трехстороннее квитирование TCP

No.	Time	Source	Destination	Protocol	Info
10	16.303490	10.1.1.1	192.168.254.254	TCP	kiosk > http [SYN] Seq=0 W
11	16.304896	192.168.254.254	10.1.1.1	TCP	http > kiosk [SYN, ACK] Se
12	16.304925	10.1.1.1	192.168.254.254	TCP	kiosk > http [ACK] Seq=1 A
13	16.305153	10.1.1.1	192.168.254.254	HTTP	GET / HTTP/1.1
14	16.307875	192.168.254.254	10.1.1.1	TCP	http > kiosk [ACK] Seq=1 A

```
Frame 10: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: Vmware_be:62:88 (00:50:56:be:62:88), Dst: Cisco_63:74:a0 (00:0f:24:63:
Internet Protocol Version 4, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.254
Transmission Control Protocol, Src Port: kiosk (1061), Dst Port: http (80), Seq: 0, Len:
    Source port: kiosk (1061)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
    Flags: 0x02 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgement: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
```

SYN
SYN, ACK
ACK



© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

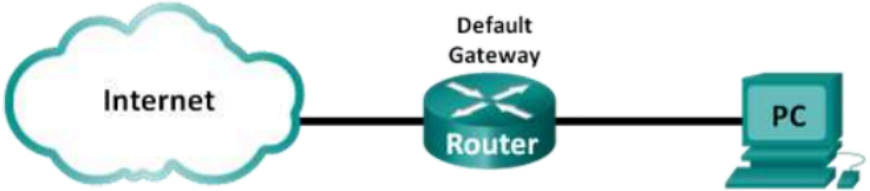
Лабораторная работа. Изучение процесса трехстороннего квитирования протокола TCP с помощью программы Wireshark

Cisco Networking Academy®

Mind Wide Open™

Lab - Using Wireshark to Observe the TCP 3-Way Handshake

Topology



Objectives

Part 1: Prepare Wireshark to Capture Packets

Part 2: Capture, Locate, and Examine Packets

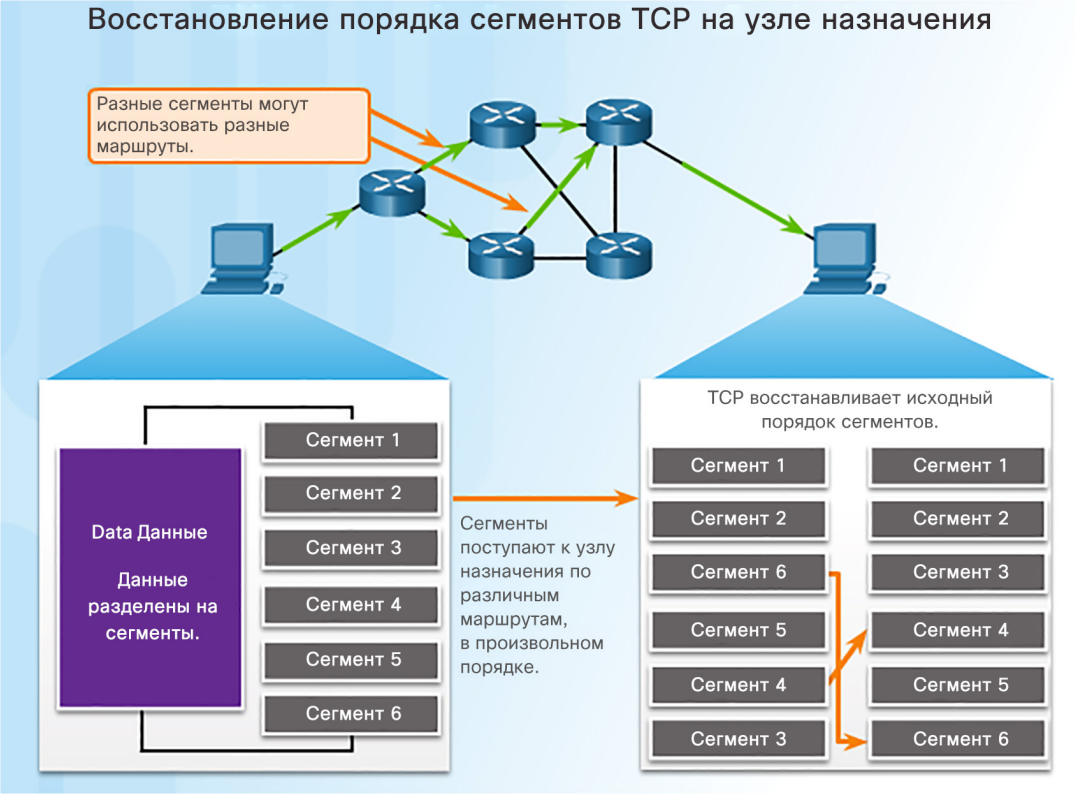
Background / Scenario

In this lab, you will use Wireshark to capture and examine packets generated between the PC browser using the HyperText Transfer Protocol (HTTP) and a web server, such as www.google.com. When an application, such as HTTP or File Transfer Protocol (FTP) first starts on a host, TCP uses the three-way handshake to establish a reliable TCP session between the two hosts. For example, when a PC uses a web browser to surf the Internet, a three-way handshake is initiated, and a session is established between the PC host and web server. A PC can have multiple, simultaneous, active TCP sessions with various web sites.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

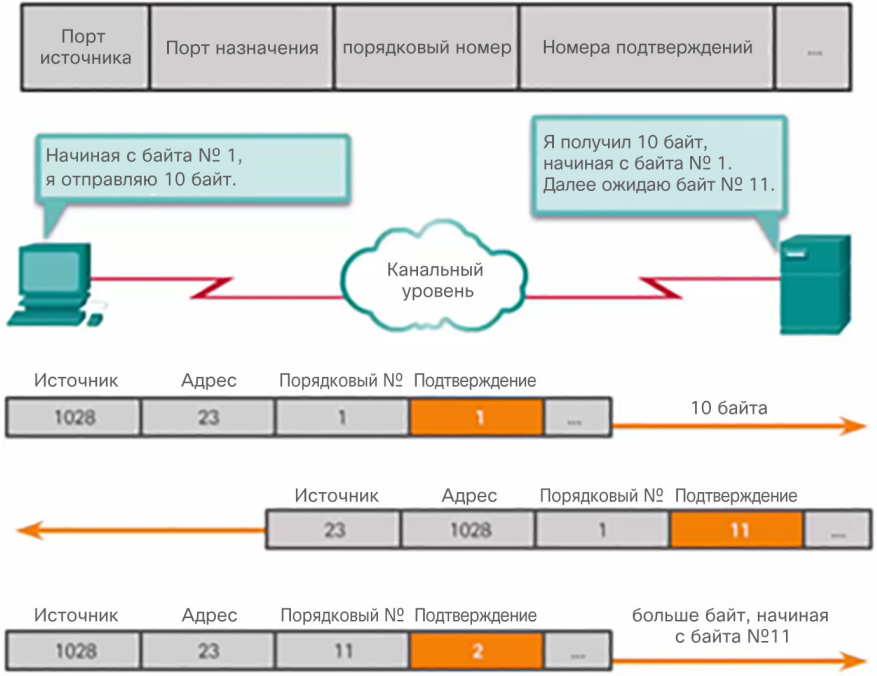
Надежность TCP: упорядоченная доставка

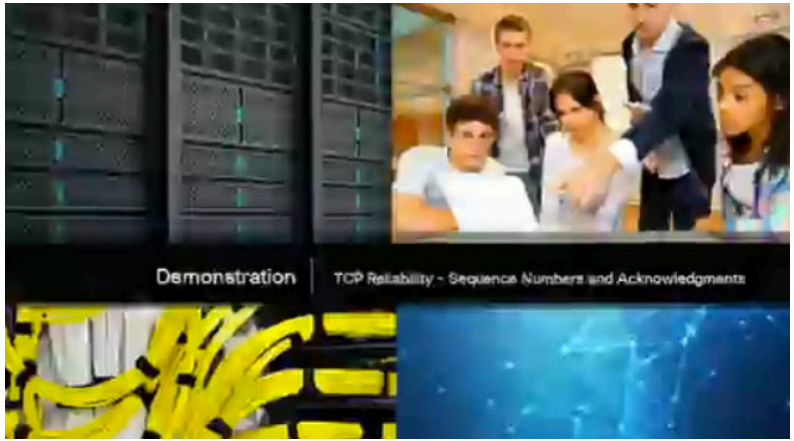
- В заголовке каждого пакета указываются порядковые номера.
- Порядковый номер представляет первый байт данных сегмента TCP.
- Во время настройки сеанса задается исходный номер последовательности (ISN) — представляет собой начальное значение байтов.
- По мере передачи данных во время сеанса порядковый номер увеличивается на число переданных байт.
- Можно выяснить, какие сегменты отсутствуют.



© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

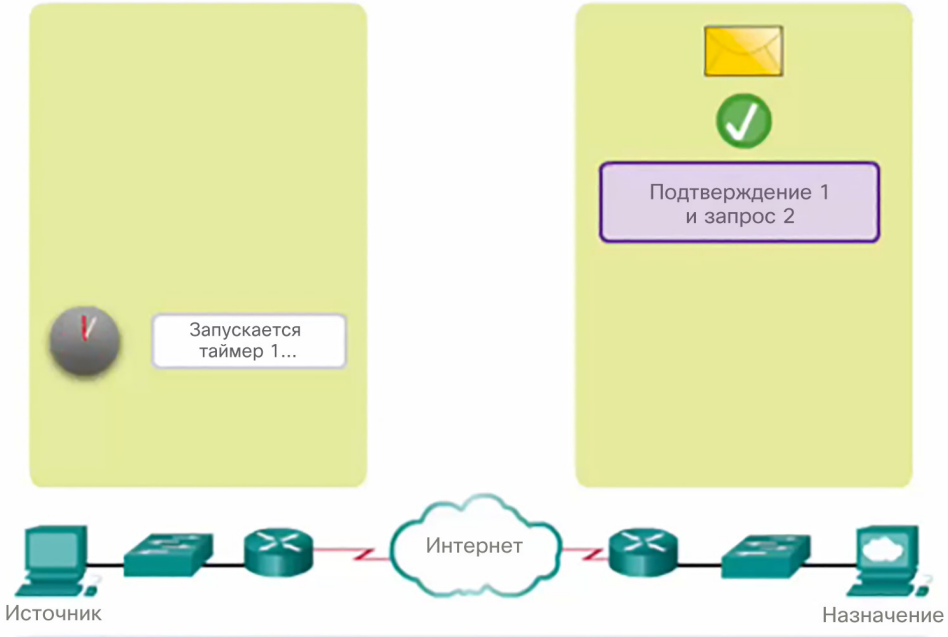
Демонстрационный видеоролик. Надежность TCP: порядковые номера и подтверждения

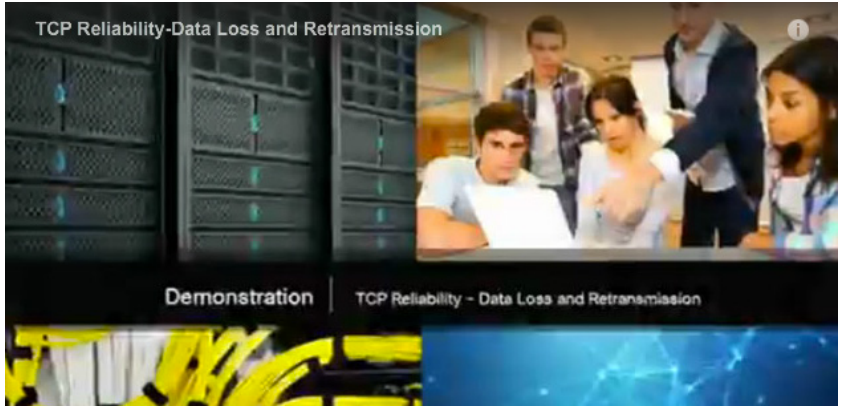




© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Демонстрационный видеоролик. Потеря данных и повторная передача





© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Управление потоком TCP: размер окна и подтверждения

- На рисунке источник передает 1460 байт данных в каждом сегменте.
- Размер окна согласован во время трехстороннего квитирования.
- Обычно компьютер PC B не дожидается получения 10 000 байт, чтобы отправить подтверждение.
- Компьютер PC A может изменить свое окно отправки при получении подтверждений от компьютера PC B.

Управление потоком TCP: предотвращение перегрузок

- Перегрузка приводит к повторной передачи потерянных сегментов TCP.
- Повторная передача сегментов можно усугубить перегрузку.
- Во избежание таких ситуаций и для предотвращения перегрузок сети в протоколе TCP предусмотрен ряд соответствующих механизмов, таймеров и алгоритмов
- Пример. Сократить число отправляемых байтов до получения подтверждения

UDP: низкая нагрузка или надежность

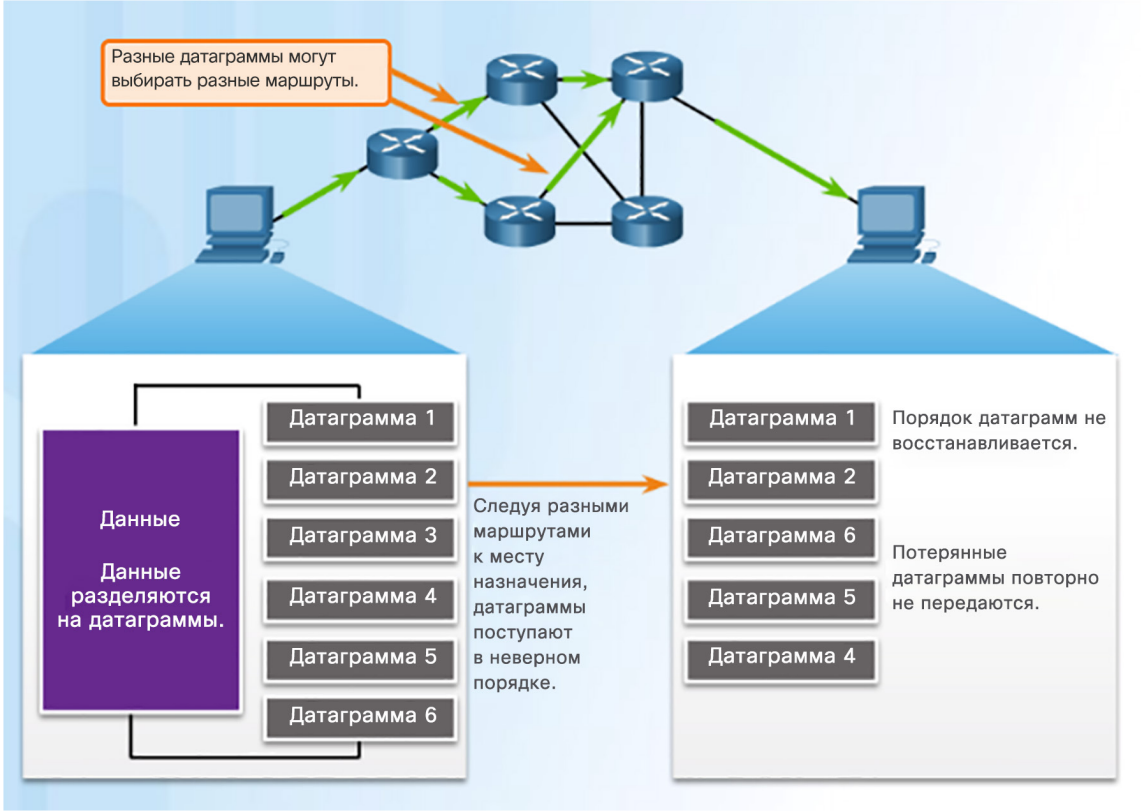
- Протокол UDP не ориентирован на установление соединения.
- Нет повторной отправки, определения последовательности и управления потоком.
- Функции не предоставляются транспортным уровнем, реализованным в другом месте.

Протокол UDP обеспечивает передачу данных с меньшими накладными расходами, поскольку он имеет небольшой заголовок датаграммы и не обменивается управляющим трафиком.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Повторная дефрагментация датаграммы UDP

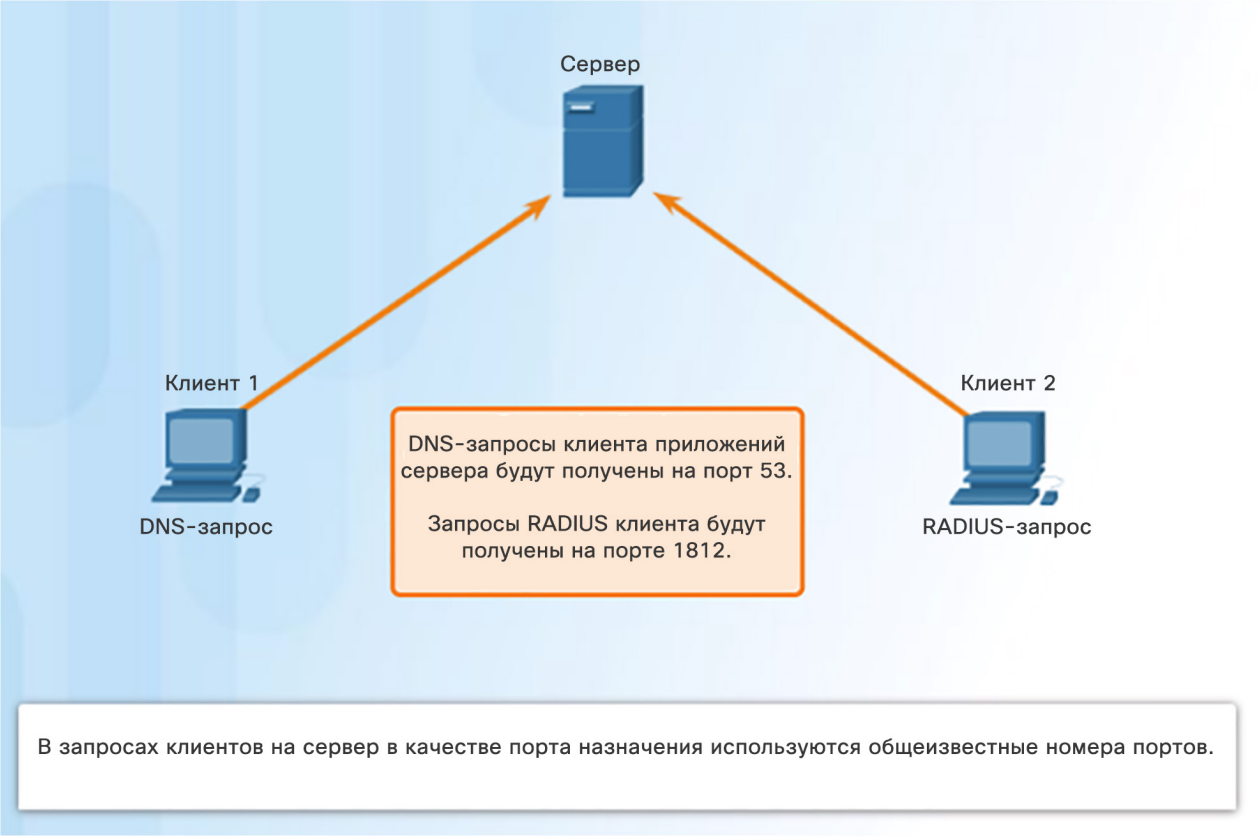
- Протокол UDP собирает данные в порядке получения и пересылает их приложению.
- Приложение должно определить правильную последовательность сегментов.



Протокол UDP: ненадежная доставка без установления соединения

Процессы и запросы UDP-сервера

Примечание. Сервер RADIUS (Remote Authentication Dial-in User Service), изображенный на рисунке, предоставляет службы аутентификации, авторизации и учета для управления доступом пользователей.



Процессы UDP-клиента

Клиенты, отправляющие запросы UDP

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Процессы UDP-клиента (продолжение)

Клиенты, отправляющие запросы UDP

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

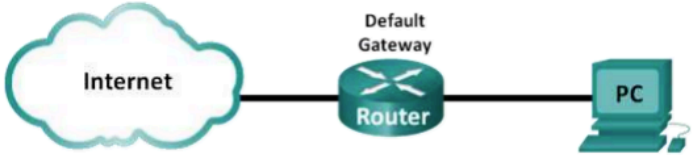
Лабораторная работа. Изучение захваченных пакетов DNS и UDP с помощью программы Wireshark

Cisco Networking Academy®

Mind Wide Open™

Lab - Using Wireshark to Examine a UDP DNS Capture

Topology



Objectives

Part 1: Record a PC's IP Configuration Information

Part 2: Use Wireshark to Capture DNS Queries and Responses

Part 3: Analyze Captured DNS or UDP Packets

Background / Scenario

If you have ever used the Internet, you have used the Domain Name System (DNS). DNS is a distributed network of servers that translates user-friendly domain names like www.google.com to an IP address. When you type a website URL into your browser, your PC performs a DNS query to the DNS server's IP address. Your PC's DNS server query and the DNS server's response make use of the User Datagram Protocol (UDP) as the transport layer protocol. UDP is connectionless and does not require a session setup as does TCP. DNS queries and responses are very small and do not require the overhead of TCP.

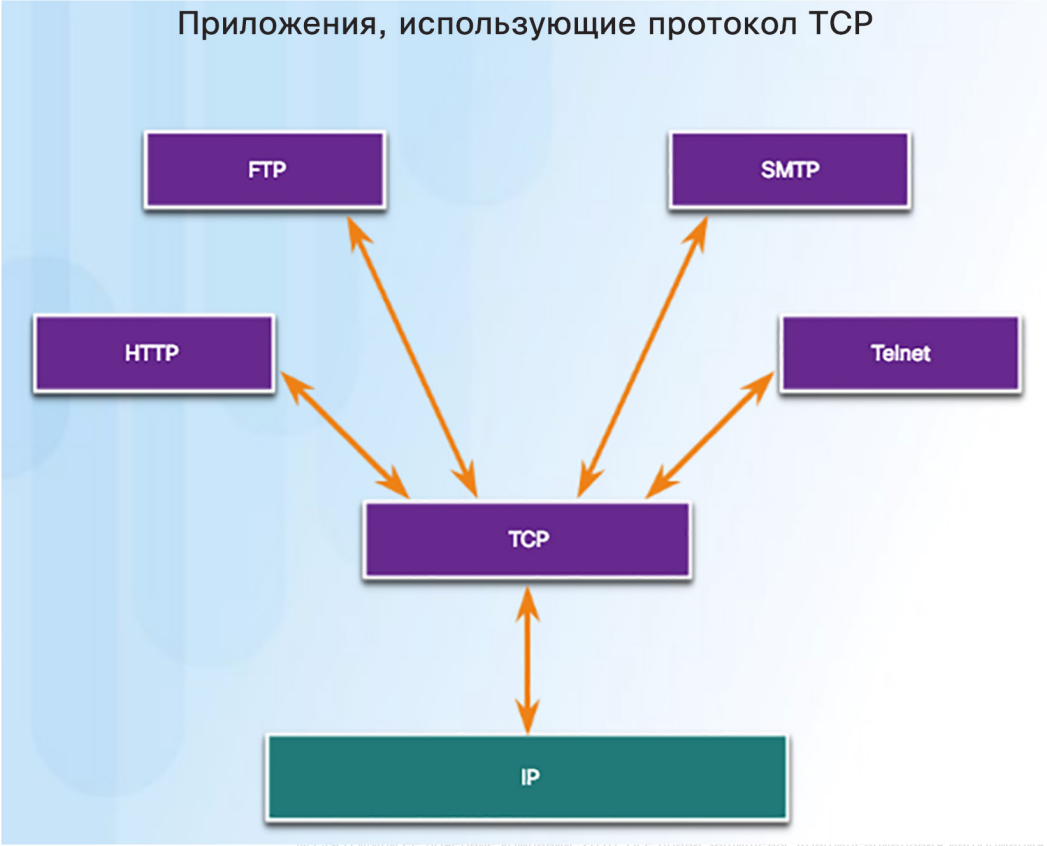
In this lab, you will communicate with a DNS server by sending a DNS query using the UDP transport protocol. You will use Wireshark to examine the DNS query and response exchanges with the same server.

Note: This lab cannot be completed using Netlab. This lab assumes that you have Internet access.

Required Resources

Приложения, использующие протокол TCP

Протокол TCP освобождает приложение от необходимости управления надежностью.

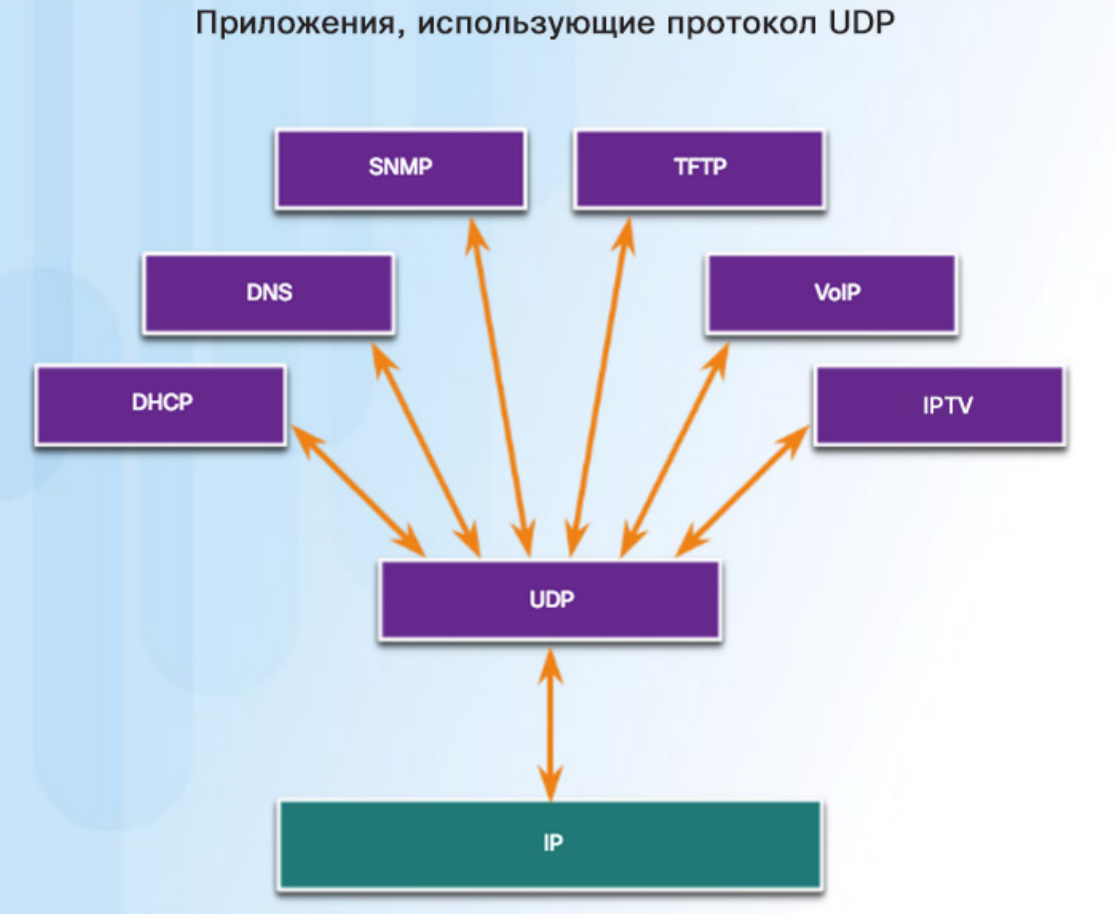


© Cisco или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Приложения, использующие протокол UDP

Для работы с протоколом UDP лучше всего подходят три типа приложений:

- Передача видео и мультимедиа в реальном времени
- Простой запрос и ответ
- Самостоятельно обеспе чивающие надежность



Лабораторная работа. Изучение захваченных пакетов TCP и UDP с помощью программы Wireshark

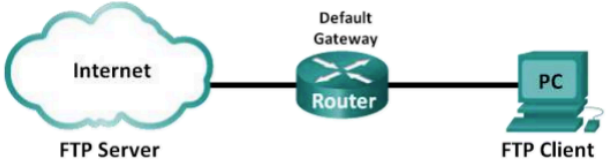
Cisco Networking Academy®

Mind Wide Open™

Lab - Using Wireshark to Examine TCP and UDP Captures

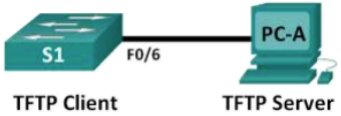
Topology – Part 1 (FTP)

Part 1 will highlight a TCP capture of an FTP session. This topology consists of a PC with Internet access.



Topology – Part 2 (TFTP)

Part 2 will highlight a UDP capture of a TFTP session. The PC must have both an Ethernet connection and a console connection to Switch S1.



Addressing Table (Part 2)

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Identify TCP Header Fields and Operation Using a Wireshark FTP Session Capture

Part 2: Identify UDP Header Fields and Operation Using a Wireshark TFTP Session Capture

9.3 Обзор по главе

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

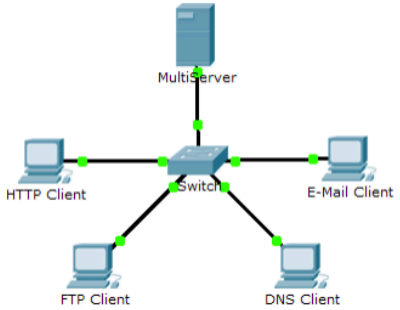
Packet Tracer. Обмен данными с использованием протоколов TCP и UDP

Cisco Networking Academy®

Mind Wide Open™

Packet Tracer Simulation - TCP and UDP Communications

Topology



Objectives

Part 1: Generate Network Traffic in Simulation Mode

Part 2: Examine the Functionality of the TCP and UDP Protocols

Background

This simulation activity is intended to provide a foundation for understanding the TCP and UDP in detail. Simulation mode provides the ability to view the functionality of the different protocols.

As data moves through the network, it is broken down into smaller pieces and identified in some fashion so that the pieces can be put back together. Each of these pieces is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer. Packet Tracer Simulation mode enables the user to view each of the protocols and the associated PDU. The steps outlined below lead the user through the process of requesting services using various applications available on a client PC.

This activity provides an opportunity to explore the functionality of the TCP and UDP protocols, multiplexing and the function of port numbers in determining which local application requested the data or is sending the data.

Глава 9. Транспортный уровень

- Объяснить, каким образом протоколы и сервисы транспортного уровня реализуют коммуникацию в сетях передачи данных
- Сравнить операции протоколов транспортного уровня при поддержке сквозного канала связи

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Новые термины и команды

• номер порта • мультиплексирование	• Протокол управления передачей (TCP) • Протокол пользовательских датаграмм (UDP)	• протокол с установлением соединения • с сохранением состояния • сокет

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

Новые термины и команды

• трехстороннее квитирование • начальный порядковый номер порта (ISN)	• подтверждение • выборочное подтверждение (SACK) • размер окна

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Конфиденциальная информация Cisco

CISCO