

Packet Tracer - Изучение моделей TCP/IP и OSI в действии

Задачи

Часть 1. Изучение HTTP-трафика

Часть 2. Отображение элементов семейства протоколов TCP/IP

Общие сведения

Данное упражнение по моделированию — первый шаг на пути к пониманию принципов работы пакета протоколов TCP/IP и его взаимосвязи с моделью OSI. Режим моделирования позволяет просматривать содержимое пересылаемых по сети данных на каждом из уровней.

По мере продвижения данных по сети они разбиваются на более мелкие фрагменты и идентифицируются таким образом, чтобы их можно было воссоединить по прибытию в пункт назначения. Каждый фрагмент получает собственное имя (единица данных протокола — PDU) и ассоциируется с конкретным уровнем моделей TCP/IP и OSI. Режим моделирования программы Packet Tracer позволяет просматривать все уровни и относящиеся к ним PDU. Ниже описана последовательность шагов пользователя для запроса веб-страницы с веб-сервера с помощью установленного на клиентском ПК веб-браузера.

Хотя большая часть показанной на экране информации будет подробнее рассмотрена далее, это даст вам возможность ознакомиться с возможностями программы Packet Tracer, а также наглядно рассмотреть процесс инкапсуляции.

Инструкции

Часть 1. Изучение HTTP-трафика

В части 1 данного упражнения вы будете использовать программу Packet Tracer (PT) в режиме моделирования для генерирования веб-трафика и изучения протокола HTTP.

Шаг 1. Перейдите из режима реального времени в режим моделирования.

В правом нижнем углу интерфейса Packet Tracer находятся вкладки для переключения между режимами **Realtime** (режим реального времени) и **Simulation** (режим моделирования). PT всегда запускается в режиме **реального времени**, в котором сетевые протоколы работают с реалистичными значениями времени. Однако широкие возможности Packet Tracer позволяют пользователю «остановить время», переключившись в режим моделирования. В режиме моделирования пакеты отображаются как анимированные конверты, временем управляют события и пользователи могут пошагово переходить от одного сетевого события к другому.

- a. Щелкните значок режима **Simulation** для переключения из режима **реального времени** в режим **моделирования**.
- b. Выберите в списке **Event List Filters** (Фильтры списка событий) пункт **HTTP**.
 - 1) HTTP в этот момент уже может быть единственным видимым событием. При необходимости нажмите кнопку **«Редактировать фильтры»** в нижней части панели моделирования, чтобы отобразить доступные видимые события. Установите или снимите флажок **Show All/None** (Показать все/ничего) и обратите внимание на то, как изменится состояние установленных и снятых флажков.

- 2) Щелкните флажок **Show All/None** до тех пор, пока все флажки не будут сняты, а затем выберите **HTTP**. Щелкните X в правом верхнем углу окна, чтобы закрыть окно «**Редактировать фильтры**». В разделе видимых событий теперь отображается только HTTP.

Шаг 2. Сгенерируйте веб-трафик (HTTP).

На данный момент панель моделирования пуста. В верхней части панели моделирования видны наименования шести столбцов списка событий. По мере генерации и продвижения трафика в списке будут появляться события.

Примечание. Веб-сервер и веб-клиент показаны на левой панели. Размер панели можно изменить, если навести указатель на полосу прокрутки и, когда он примет вид двунаправленной стрелки, перетащить его влево или вправо.

- a. Щелкните **Web Client** (Веб-клиент) на крайней левой панели.
- b. Щелкните вкладку **Desktop** (Рабочий стол), затем щелкните значок **Web Browser** (Веб-браузер), чтобы открыть веб-браузер.
- c. В поле URL введите адрес **www.osi.local** и нажмите кнопку **Go**.

Поскольку время в режиме моделирования привязано к событиям, для отображения событий в сети необходимо использовать кнопку **Capture/Forward** (Захват/вперед). Кнопка движения вперед по захваченным пакетам расположена в левой части синей полосы, которая находится под окном топологии. Из трех кнопок, эта самая правая.

- d. Нажмите кнопку **Capture/Forward** четыре раза. В списке событий должны быть четыре события.

Посмотрите на страницу веб-клиента в веб-браузере. Что-нибудь изменилось? Да

Шаг 3. Изучите содержимое HTTP-пакета.

- a. Щелкните первый цветной квадрат в столбце **Type** списка событий **Event List**. Вам может понадобиться развернуть **панель моделирования** или использовать полосу прокрутки непосредственно под списком событий **Event List**.

Откроется окно **PDU Information at Device: Web Client** (Информация о PDU на устройстве: веб-клиент). В этом окне есть только две вкладки: **OSI Model** (Модель OSI) и **Outbound PDU Details** (Сведения об исходящей PDU), поскольку это только начало передачи. По мере изучения новых событий станут видны три вкладки, включая новую вкладку **Inbound PDU Details** (Сведения о входящей PDU). Когда событие является последним в потоке трафика, отображаются только вкладки **OSI Model** и **Inbound PDU Details**.

- b. Убедитесь, что выбрана вкладка **OSI Model**.

В столбце **Out Layers** нажмите **Layer 7**.

Какая информация перечислена в пронумерованных шагах непосредственно под полями **In Layers** (Входящие уровни) и **Out Layers** (Исходящие уровни)? In layers: -, out Layers: Type, TCP Src Port, Dst Port, Ip Header Src. IP, Dest IP, Ethernet II, Port(s)

Какое значение столбца **Dst Port** на **Уровне 4** в столбце **Out Layers** ? 80

Какое значение имеет параметр **Dest**. Значение IP для **Layer 3** в столбце **Out Layers**? 192.168.1.254

Какая информация отображается на слое 2 в столбце **Out Layers**?

Ethernet II Header 0060.47CA.4DE
>> 0001.96A9.401D

Заголовок Ethernet II уровня 2 и входящие и исходящие MAC-адреса.

- с. Щелкните вкладку **Outbound PDU Details** (Сведения об исходящей PDU).

Сведения на вкладке **PDU Details** (Сведения о PDU) отражают уровни модели TCP/IP.

Примечание. Сведения в разделе Ethernet II представляют собой еще более подробные данные, чем показанные в разделе уровня 2 на вкладке OSI Model. Вкладка **Outbound PDU Details** содержит более описательные и подробные сведения. Значения **DEST MAC** (MAC-адрес назначения) и **SRC MAC** (MAC-адрес источника) в разделе Ethernet II на вкладке **PDU Details** отображаются на вкладке **OSI Model** в разделе Layer 2, но не указаны в качестве таковых.

Если сравнить сведения в разделе **IP** вкладки **PDU Details** со сведениями на вкладке **OSI Model**, какая информация является для них общей? К какому уровню она относится? Layer 3

Если сравнить сведения в разделе **TCP** вкладки **PDU Details** со сведениями на вкладке **OSI Model**, какая информация является для них общей и к какому уровню она относится? Layer 4

Какой **Host** (узел) указан в разделе **HTTP** вкладки **PDU Details**? С каким уровнем будут связаны эти сведения на вкладке **OSI Model**? www.osi.local, layer7

- d. Щелкните первый цветной квадрат в столбце **Type** списка событий **Event List**. Активен только уровень 1 (не отображается серым цветом). Устройство перемещает кадр из буфера и помещает его в сеть.

- e. Перейдите к следующему полю **HTTP Info** в списке событий **Event List** и щелкните цветной квадрат. В этом окне есть два столбца: **In Layers** и **Out Layers**. Обратите внимание на направление стрелки непосредственно под столбцом **In Layers**. Она смотрит вверх, показывая направление перемещения данных. Прокрутите эти уровни, обращая внимание на просмотренные ранее элементы. В верхней части столбца стрелка указывает вправо. Это означает, что сервер теперь отправляет данные обратно клиенту.

Сравните данные в столбце **In Layers** с данными в столбце **Out Layers** и скажите, в чем заключается основное отличие между ними.

In Layers обращение от 192.168.1.1 к 192.168.1.254, в Out layers наоборот

- f. Откройте вкладку **Inbound PDU Details** (Сведения о входящей PDU). просмотр сведений о PDU.
g. Щелкните последний цветной квадрат в столбце **Info**.

Сколько вкладок отображается с этим событием и почему? Дайте пояснение.

Только две (одна — OSI Model, а вторая — Inbound PDU Details, поскольку это принимающее устройство).

Часть 2. Отображение элементов семейства протоколов TCP/IP

В части 2 данного упражнения вы будете использовать режим моделирования Packet Tracer для наблюдения и изучения работы некоторых других протоколов, входящих в семейство TCP/IP.

Шаг 1. Просмотрите дополнительные события

- a. Закройте все окна со сведениями о PDU.
b. В разделе **Event List Filters > Visible Events** (Фильтры списка событий > Видимые события) нажмите кнопку **Show All/None**.

Какие дополнительные типы событий показаны?

Event List Filters - Visible Events
ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Эти дополнительные записи играют различные роли в семействе протоколов TCP/IP. Протокол разрешения адресов (ARP) запрашивает MAC-адреса для узлов назначения. Протокол DNS отвечает за преобразование имен (например, **www.osi.local**) в IP-адреса. Дополнительные события TCP связаны с установлением соединений, согласованием параметров связи и разъединением сеансов связи между устройствами. Эти протоколы упоминались ранее и будут рассмотрены более подробно в ходе изучения курса. В настоящее время Packet Tracer позволяет захватывать более 35 протоколов (типов событий).

- c. Щелкните первое событие DNS в столбце **Type**. Просмотрите вкладки **OSI Model** и **PDU Detail** и обратите внимание на процесс инкапсуляции. На вкладке **OSI Model** с выделенным полем **Layer 7** непосредственно под столбцами **In Layers** и **Out Layers** отображается описание того, что происходит. ("1. The DNS client sends a DNS query to the DNS server." [DNS-клиент отправляет DNS-запрос на DNS-сервер]) Это очень полезная информация, которая помогает понять, что происходит во время процесса связи.

- d. Щелкните вкладку **Outbound PDU Details** (Сведения об исходящей PDU).

Какие сведения показаны в поле **NAME**: в разделе DNS QUERY? www.osi.local

- e. Щелкните последний цветной квадрат DNS **Info** в списке событий.

На каком устройстве был захвачен PDU? web server

Какое значение показано рядом с полем **ADDRESS**: в разделе DNS ANSWER на вкладке **Inbound PDU Details**? 192.168.1.254

- f. Найдите первое событие **HTTP** в списке и щелкните цветной квадрат события **TCP** сразу после этого события. Выделите **Layer 4** на вкладке **OSI Model**.

Какие сведения отображаются под пунктами 4 и 5 в пронумерованном списке непосредственно под столбцами **In Layers** и **Out Layers**?

The TCP connection is successful
The device sets the connection state to ESTABLISHED

TCP, наряду с другими функциями, управляет подключением и отключением канала связи. Данное конкретное событие указывает на то, что канал связи был установлен (ESTABLISHED).

- g. Щелкните последнее событие TCP. Выделите Layer 4 на вкладке **OSI Model**. Проверьте действия, перечисленные непосредственно под столбцами **In Layers** и **Out Layers**.

Расскажите, для чего предназначено событие, используя информацию, предоставленную в последнем пункте списка (это должен быть пункт 4).

The TCP connection was reset
The device sets the connection state to CLOSED

Сложные вопросы

В этом упражнении по моделированию рассмотрен пример сеанса веб-связи между клиентом и сервером в локальной сети (LAN). Клиент делает запросы к определенным службам, функционирующим на сервере. Сервер должен быть настроен на прослушивание определенных портов для получения запросов клиентов. (Совет. Для получения информации о порте см. Layer 4 на вкладке **OSI Model**.)

Взяв за основу сведения, которые проверялись в ходе захвата данных в Packet Tracer, ответьте: «Какой порт прослушивает **веб-сервер** для получения веб-запросов?». 80

Какой порт прослушивает **веб-сервер** для получения DNS-запросов?

53