Packet Tracer - Badanie modeli TCP/IP i OSI w działaniu.

Cele

Część 1: Badanie ruchu internetowego HTTP

Część 2: Wyświetlenie elementów zestawu protokołów TCP/IP

Wprowadzenie

Prezentowana symulacja ma za zadanie dostarczyć podstaw do zrozumienia sposobu działania zestawu protokołów TCP/IP oraz ich relacji do modelu OSI. Praca w trybie symulacji pozwala przeglądać zawartość danych przesyłanych w sieci na poziomie każdej warstwy.

Kiedy dane przesyłane są przez sieć, to dzielone są na mniejsze części i oznaczane w sposób, który pozwoli na ich ponowne złożenie kiedy dotrą do celu. Każda część ma przyporządkowaną określoną nazwę (jednostka danych protokołu [PDU]) która jest związaną z określoną warstwą modeli TCP/IP i OSI. Przedstawiona symulacja programu Packet Tracer umożliwia obserwację poszczególnych warstw i związanych z nimi jednostkami PDU. Kolejne kroki prowadzą użytkownika przez proces żądania wyświetlania strony z serwera WWW za pomocą przeglądarki internetowej dostępnej na komputerze klienta.

Mimo, wyświetlenia dużej ilości informacji, które zostaną omówione bardziej szczegółowo w dalszej części kursu, teraz masz okazję poznać sposób działania programu Packet Tracer oraz zapoznać się możliwościami wizualizacji procesu enkapsulacji.

Instrukcje

Część 1: Zbadaj ruch internetowy HTTP

W części 1 tego ćwiczenia będziesz używał Packet Tracer (PT) w trybie symulacji do generowania ruchu w sieci i badania HTTP.

Krok 1: Przełącz się z trybu Realtime do trybu Simulation.

W prawym dolnym rogu interfejsu Packet Tracer znajdują się przyciski, które pozwalają przełączać się pomiędzy trybami czasu rzeczywistego (**Realtime**) i symulacji (**Simulation**). PT zawsze uruchamia się w trybie **Realtime**, w którym protokoły sieciowe pracują w realnym czasie z realną prędkością. Jednakże możliwości Packet Tracera pozwalają użytkownikowi "zatrzymanie czasu"; poprzez przełączenie się w tryb symulacji. W trybie symulacji pakiety są wyświetlane jako animowane koperty, czas jest zorientowany zdarzeniowo, a użytkownik może obserwować zdarzenia w sieci krok po kroku.

a. Kliknij ikonę **Simulation**, aby przełączyć się z trybu **Realtime** do trybu **Simulation**.

b. Wybierz **HTTP** z filtrów listy zdarzeń **Event List Filters**.

   1) HTTP może już być jedynym widocznym zdarzeniem. W razie potrzeby, kliknij przycisk **Edit Filters** u dołu panelu symulacji, aby wyświetlić dostępne widoczne zdarzenia. Zaznacz pole przycisku wyboru **Show All/None** i zauważ, jak pola wyboru przełączają się na odznaczone lub zaznaczone, w zależności od aktualnego stanu.

   2) Klikaj pole wyboru **Show All/None** dopóki wszystkie pola zostaną odznaczone, a następnie wybierz **HTTP** z zakładki Misc okna Edit Filters. Kliknij X w prawym górnym rogu okna, aby zamknąć okno **Edit Filters**. Pozycja Visible Events powinna pokazywać teraz tylko HTTP.

Krok 2: Wygeneruj ruch HTTP.

Obecnie panel Simulation jest pusty. W górnej części Event List panelu Simulation znajduje się pięć kolumn. Gdy ruch jest generowany i przemieszcza się krok po kroku, na liście zaczynają się wyświetlać zdarzenia.

Uwaga: serwer WWW (Web Server) i klient WWW (Web Client) wyświetlone są w lewym okienku. Panele mogą być dostosowane do odpowiedniego rozmiaru poprzez przesuwanie linii oddzielającej, która znajduje się obok paska przewijania, w lewo lub w prawo (gdy pojawi się strzałka z dwoma grotami).

a. Kliknij **Web Client**, który znajduje się w lewym okienku.

b. Następnie kliknij kolejno w zakładkę **Desktop** i ikonę **Web Browser**, aby ją otworzyć.

c. W polu URL wpisz **www.osi.local** i kliknij **Go**.

Ponieważ tryb symulacji jest zorientowany zdarzeniowo, po każdym zdarzeniu musisz kliknąć przycisk **Capture/Forward** aby przejść do kolejnego zdarzenia. Przycisk Capture/Forward znajduje się po lewej stronie niebieskiego pasma, który znajduje się poniżej okna topologii. Z trzech przycisków, to ten po prawej.

d. Kliknij cztery razy przycisk **Capture/Forward**. Powinny pojawić się cztery zdarzenia na liście zdarzeń.

Spójrz na stronę przeglądarki internetowej klienta WWW. Czy coś się zmieniło?

Krok 3: Zbadaj zawartość pakietu HTTP.

a. Kliknij pierwszy kolorowy kwadrat w kolumnie **Type** na liście **Event List**. Może okazać się konieczne, aby rozwinąć **panel symulacji** lub użyć paska przewijania poniżej **listy zdarzeń** .

Na ekranie pojawi się okno **PDU Information at Device: Web Client**. Ponieważ jest to początek transmisji, w oknie tym znajdują się tylko dwie zakładki (**OSI Model** i **Outbound PDU Details**). Gdy rozpatrywanych będzie więcej zdarzeń, to wyświetlone będą trzy zakładki - dojdzie dodatkowo zakładka **Inbound PDU Details**. Kiedy zdarzenie jest ostatnim zdarzeniem w strumieniu ruchu, to wyświetlane są tylko karty **OSI Model** i **Inbound PDU Details**.

b. Upewnij się, że wybrana jest zakładka **OSI Model**.

W kolumnie **Out Layers** kliknij **Layer 7**.

Jakie informacje wyświetlone są w ponumerowanych krokach bezpośrednio poniżej pól **In Layers** i **Out Layers** dla warstwy 7?

Jaka jest wartość **Dst Port** dla **Layer 4** w kolumnie **Out Layers** ?

Jaka jest wartość **Dest. IP** dla **Layer 3** w kolumnie **Out Layers** ?

Jakie informacje są wyświetlane w warstwie 2 w kolumnie **Out Layers**?

c. Kliknij na **Outbound PDU Details**.

Informacje wyświetlone pod **PDU Formats** odzwierciedlają warstwy modelu TCP/IP.

Uwaga: Informacje podane w sekcji **Ethernet II** zakładki Outbound PDU Details dostarczają jeszcze bardziej szczegółowych informacji niż te, które wyświetlone są poniżej warstwy 2 na zakładce **OSI Model**. Zakładka **Outbound PDU Details** zawiera informacje bardziej opisowe i szczegółowe. Wartości pod **DEST MAC** i **SRC MAC** w ramach szczegółów PDU (**PDU Details**) sekcji **Ethernet II** wyświetlane są w zakładce **OSI Model** pod warstwą 2, ale nie są oznaczone jako takie**.**

Jakie są wspólne informacje wymienione w sekcji **IP** szczegółów PDU (**PDU Details**) w porównaniu do informacji wymienionych w zakładce **OSI Model**? Z którą warstwą jest ona związana?

Jakie są wspólne informacje wymienione w sekcji **TCP** szczegółów PDU (**PDU Details**) w porównaniu do informacji wymienionych w zakładce **OSI Model**? Z którą warstwą jest to związane?

Co to jest **Host** wymienione w sekcji **HTTP PDU Datails** ? Z jaką warstwą te informacje byłyby powiązane w ramach zakładki **OSI Model**?

d. Kliknij następny kolorowy kwadrat w kolumnie **Type** na liście **Event List**. Tylko warstwa 1 jest aktywna (nie wyszarzona). Urządzenie przenosi ramkę z bufora i umieszcza ją w sieci.

e. Przejdź do następnego pola HTTP **Type** wewnątrz **Event List** i kliknij pole kolorowego kwadratu. Okno to zawiera zarówno warstwy **In Layers** i **Out Layers**. Zwróć uwagę na kierunek strzałki bezpośrednio pod kolumną **In Layers**; jest skierowana ku górze, wskazując kierunek, w którym informacja podróżuje. Przejrzyj te warstwy sporządzając notatki z przeglądanych pozycji. Na szczycie kolumny strzałka wskazuje w prawo. Oznacza to, że serwer wysyła właśnie informacje z powrotem do klienta.

Porównując informacje wyświetlane w kolumnie **In Layers** z tymi w kolumnie **Out Layers**, jakie są między nimi główne różnice?

f. Wybierz zakładkę **Inbound and Outbound PDU Details**. Przejrzyj szczegóły PDU.

g. Kliknij ostatni kolorowy kwadrat w kolumnie **Info**.

Ile zakładek zostało wyświetlonych w tym zdarzeniu? Wyjaśnij.

Część 2: Wyświetlenie elementów zestawu protokołów TCP/IP

W części 2 tego ćwiczenia używany będzie tryb symulacji Packet Tracer po to, aby zobaczyć i zbadać kilka innych protokołów zawartych w zestawie TCP/IP.

Krok 1: Zobacz dodatkowe zdarzenia

a. Zamknij wszystkie otwarte okna z informacją PDU.

b. W sekcji **Event List Filters** > **Visible Events** kliknij **Show All/None**.

Jakie dodatkowe typy zdarzeń są wyświetlane?

Te dodatkowe wpisy odgrywają różne role w ramach zestawu TCP/IP. Address Resolution Protocol (ARP) żąda adresów MAC dla hostów docelowych. DNS odpowiedzialny jest za konwersję nazwy (na przykład **www.osi.local**) na adres IP. Dodatkowe zdarzenia TCP odpowiedzialne są za połączenie, uzgadnianie parametrów komunikacji oraz za rozłączenie sesji komunikacji pomiędzy urządzeniami. O protokołach tych zostało wspomniane wcześniej i będą nadal omawiane w dalszej części kursu. Obecnie w ramach Packet Tracera istnieje ponad 35 możliwych protokołów (typów zdarzeń) dostępnych do przechwytywania.

c. Kliknij pierwsze zdarzenie DNS w kolumnie **Type**. Zapoznaj się z zakładkami **OSI Model** i **PDU Detail**, a następnie zwróć uwagę na proces enkapsulacji. Jak spojrzysz na zakładkę **OSI Model** z podświetloną **Layer 7**, to opis tego, co się tam dzieje wypisany jest bezpośrednio poniżej w **In Layers** i **Out Layers** ("1. Klient DNS wysyła zapytanie DNS do serwera DNS. "). Jest to bardzo przydatna informacja, która pomoże zrozumieć, co dzieje się podczas procesu komunikacji.

d. Kliknij na **Outbound PDU Details**.

Jakie informacje podane są w polu **NAME** sekcji DNS QUERY?

e. Kliknij ostatni kolorowy kwadrat DNS **Info** na liście zdarzeń.

Na którym urządzeniu został przechwycony PDU?

Jaka jest wartość wyświetlona obok **ADDRESS**: w sekcji DNS ANSWER zakładki (**Inbound PDU Details**)?

f. Znajdź pierwsze zdarzenie **HTTP** na liście i kliknij kolorowe pole kwadratu zdarzenia **TCP** bezpośrednio po tym zdarzeniu. Zaznacz **Layer 4** w zakładce **OSI Model** .

Na podstawie numerowanej listy bezpośrednio poniżej obszarów **In Layers** i **Out Layers**, jakie informacje wyświetlone są w punkcie 4 i 5?

TCP zarządza łączeniem i rozłączaniem kanału komunikacyjnego wraz z innymi obowiązkami. To określone zdarzenie pokazuje, że kanał komunikacyjny został ustanowiony (ESTABLISHED).

g. Kliknij ostatnie zdarzenie TCP. Zaznacz Layer 4 w zakładce **OSI Model** . Przeanalizuj kroki opisane bezpośrednio pod **In Layers** i **Out Layers**.

Jakie jest przeznaczenie tego zdarzenia, w oparciu o informacje zawarte w ostatniej pozycji na liście (powinna być to pozycja 4)?

Pytania - wyzwanie

Symulacja stanowi przykład sesji internetowej pomiędzy klientem a serwerem w sieci lokalnej (LAN). Klient generuje żądania do określonych usług działających na serwerze. Serwer musi być skonfigurowany do nasłuchiwania na określonych portach żądań klienta. (Podpowiedź: Spójrz na warstwę 4 zakładki **OSI Model** żeby zobaczyć informacje o porcie.)

Na podstawie informacji, która została sprawdzona podczas przechwytywania w Packet Tracer, jaki numer portu ma, nasłuchujący żądań stron WWW serwer (**Web Server**)?

Na jakim porcie **Web Server** nasłuchuje żądania DNS?