

Instrukcja laboratoryjna z przedmiotu: Sieci komputerowe

Ćwiczenie 8: Warstwa aplikacyjna. Działanie protokołów HTTP, TFTP, DHCP i DNS

Marta Szarmach
Zakład Telekomunikacji Morskiej
Wydział Elektryczny
Uniwersytet Morski w Gdyni

04.2022

I. Wprowadzenie

Warstwa 7. modelu OSI — aplikacyjna — ma za zadanie udostępnić użytkownikom/aplikacjom interfejs do wprowadzania danych do sieci: tworzenie wiadomości i przekazywanie ich do niższych warstw. To na warstwie aplikacyjnej działają protokoły do przesyłu zawartości stron internetowych (HTTP), plików (FTP i TFTP), poczty elektronicznej (wychodzącej SMTP oraz przychodzącej: POP3 i IMAP), czy służące do wymiany pomiędzy urządzeniami informacji niezbędnych do poprawnego działania sieci komputerowych (DNS, DHCP czy NTP).

HTTP (ang. *Hypertext Transfer Protocol*) umożliwia przesył zawartości stron WWW. Serwer WWW nasłuchuje na porcie 80 TCP. Klient wysyła żądania do serwera, wykonując różne metody, takie jak GET (prośba o udostępnienie zasobu), PUT i POST (przesłanie danych na serwer), DELETE (żądanie usunięcia zasobu) albo HEAD (sprawdzenie dostępności zasobu). Serwer odpowiada komunikatami zawierającymi status żądania, przykładowo, 200 (OK) czy 404 (Not Found). W wiadomościach HTTP wymieniane są dane dotyczące m.in. wykorzystywanej przeglądarki internetowej, języka, kodowania znaków.

TFTP (ang. *Trivial File Transfer Protocol*) jest prostym protokołem umożliwiającym przesył plików. W przeciwieństwie do swojego bardziej rozbudowanego odpowiednika, FTP, nie obsługuje pracy na folderach ani uwierzytelniania użytkownika, ma jednak zaimplementowany mechanizm potwierdzania odbioru każdego bloku danych (zawierającego domyślnie 512 bajtów),

jako że na warstwie transportowej wykorzystuje protokół UDP, który sam w sobie tego nie zapewnia.

DHCP (ang. *Dynamic Host Configuration Protocol*) umożliwia automatyczne przydzielanie hostom adresacji IP (adresu IP, maski sieciowej, adresu IP bramy domyślnej czy serwera DNS), dzięki czemu administrator nie musi tego robić statycznie. Wykorzystuje porty UDP: 67 (u serwera) i 68 (u klienta). Proces uzyskiwania informacji o adresacji poprzez DHCP wygląda następująco:

1. Klient poszukuje obecnego w sieci serwera DHCP (wysyłając komunikat DHCPDISCOVER).
2. Serwer odpowiada na żądanie klienta i proponuje mu pewien adres IP (DHCPOFFER).
3. Klient prosi o zarezerwowanie proponowanego przez serwer adresu, godząc się na jego przyjęcie (DHCPREQUEST).
4. Serwer potwierdza zarezerwowanie adresu dla klienta, następuje jego ostateczne przypisanie (DHCPACK). Jeśli adres z jakichś przyczyn jest już zajęty, serwer odmawia (DHCPNAK) i procedura musi się zacząć od początku.

Klient co jakiś czas musi odnawiać dzierżawę (wysyłając ponownie DHCPREQUEST), może też ją w każdej chwili zakończyć (DHCPRELEASE).

DNS (ang. *Domain Name System*) umożliwia tłumaczenie nazw mnemonicznych (zrozumiałych dla człowieka, np. umg.edu.pl) odwiedzanych stron internetowych na adresy IP serwerów WWW (zrozumiałych dla maszyny, np. 153.19.111.231). Wykorzystuje port 53. Jest to system silnie hierarchiczny, opierający się na serwerach zawierających informacje o powiązaniu nazwy domeny i adresu IP serwera WWW. Serwer posiadający bezpośrednio informację o danej domenie, jeśli jest o nią zapytany, udzieli odpowiedzi autorytatywnej („z pierwszej ręki”), a jeśli posiada informację pochodzącą od innego serwera, będzie to odpowiedź nieautorytatywna. W ramach informacji o domenach przechowywane są takie dane, jak:

- adres IPv4 domeny (rekord A),
- adres IPv6 domeny (rekord AAAA),
- nazwa kanoniczna domeny (rekord CNAME),
- adres serwera pocztowego domeny (rekord MX),
- adres serwera DNS domeny (NS).

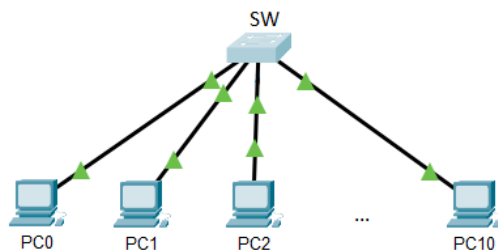
II. Cel ćwiczenia

Celem niniejszego ćwiczenia jest zapoznanie się z funkcjonowaniem warstwy aplikacyjnej modelu OSI w sieciach komputerowych poprzez:

- zapoznanie się z konfiguracją serwera HTTP Apache,
- przechwycenie w programie Wireshark ruchu protokołów: HTTP, TFTP, DHCP oraz DNS i zaobserwowanie ich działania,
- użycie komendy *nslookup* do wydawania zapytań o konkretne rekordy DNS.

III. Stanowisko laboratoryjne

Do wykonania ćwiczenia niezbędne jest stanowisko laboratoryjne składające się z komputerów klasy PC z zainstalowanym systemem Windows oraz oprogramowaniem Wireshark, połączonych w sieć za pomocą przełącznika sieciowego Cisco.



Przed przystąpieniem do ćwiczenia:

- Włącz komputer do lokalnej sieci laboratoryjnej, uruchamiając na nim kartę sieciową o nazwie *LAB*. Kliknij *Start* \Rightarrow *Ustawienia* \Rightarrow *Połączenia sieciowe*. Prawym klawiszem wybierz kartę sieciową *LAB* i kliknij *Włącz*, podobnie wybierz kartę sieciową *Internet* i wybierz *Wyłącz* (od tego momentu komputer straci połączenie z internetem na rzecz sieci laboratoryjnej).
- Ustaw statycznie adres IP według schematu:
IP: 172.16.1.*numer_Twojego_stanowiska*
Maska podsieci: 255.255.255.0

W drugiej części zajęć do wykonania ćwiczenia wystarczy komputer klasy PC z dostępem do Internetu.

IV. Przebieg ćwiczenia

1 Analiza ruchu HTTP

1.1 Przechwyć ruch HTTP wygenerowany podczas otwierania strony internetowej.

- Otwórz program Wireshark i rozpocznij przechwytywanie ruchu sieciowego na karcie sieciowej Realtek. Włącz filtrowanie przechwyconego ruchu, tak, by widoczne były tylko wiadomości HTTP.
- Wygeneruj ruch sieciowy: poproś sąsiada o adres IP jego komputera i wpisz go w pasku adresu w przeglądarce internetowej. Przejdiesz w ten sposób na prostą stronę WWW, która jest przechowywana na komputerze sąsiada: **It works!** (przypomnij sobie, że na każdym z komputerów w laboratorium zainstalowane jest oprogramowanie Apache, dzięki któremu każdy z komputerów staje się serwerem WWW).
- Sprawdź, czy w programie Wireshark pojawiły się przechwycone wiadomości HTTP. Zatrzymaj przechwytywanie danych.

1.2 Przyjrzyj się informacjom przesyłanym w wiadomościach HTTP.

- Zaznacz pierwszą przechwyconą wiadomość. Jaka metoda została wykonana? Odczytaj informacje o przeglądarce klienta i zestawie znaków.

No. -	Time	Source	Destination	Protocol	Info
24	24.313687	172.16.1.1	172.16.1.7	HTTP	GET / HTTP/1.1
25	24.314248	172.16.1.7	172.16.1.1	HTTP	HTTP/1.1 200 OK (text/html)
26	24.359594	172.16.1.1	172.16.1.7	HTTP	GET /favicon.ico HTTP/1.1
27	24.360225	172.16.1.7	172.16.1.1	HTTP	HTTP/1.1 404 Not Found (text/html)
28	24.370832	172.16.1.1	172.16.1.7	HTTP	GET /favicon.ico HTTP/1.1
29	24.371449	172.16.1.7	172.16.1.1	HTTP	HTTP/1.1 404 Not Found (text/html)

Frame 25 (379 bytes on wire, 379 bytes captured)
Ethernet II, Src: 00:1a:92:32:3f:ac (00:1a:92:32:3f:ac), Dst: 00:1a:92:32:3f:a9 (00:1a:92:32:3f:a9)
Internet Protocol, Src: 172.16.1.7 (172.16.1.7), Dst: 172.16.1.1 (172.16.1.1)
Transmission Control Protocol, Src Port: http (80), Dst Port: 1122 (1122), Seq: 1, Ack: 325, Len: 325
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Request Version: HTTP/1.1
Response Code: 200
Date: Tue, 12 Apr 2022 11:04:14 GMT\r\n
Server: Apache/2.2.4 (win32)\r\n
Last-Modified: Sat, 20 Nov 2004 13:16:24 GMT\r\n
ETag: "2db3-2c-6e1a3a00"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 44
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html\r\n
\r\n
Line-based text data: text/html
<html><body><h1>It works!</h1></body></html>

- b) Zaznacz drugą przechwyconą wiadomość i przyjrzyj się niektórym przenoszonym informacjom:

- wersji HTTP,
- kodowi odpowiedzi (czy żądanie się powiodło),
- oprogramowaniu serwera,
- informacji o czasie ostatniej modyfikacji dokumentu.

Otwórz sekcję *Line-based text data*, aby zobaczyć kod html żądanej strony, przesłany w sposób nieszyfrowany (jawnym tekstem).

1.3 Przyjrzyj się konfiguracji serwera WWW.

Na każdym z komputerów w laboratorium zainstalowane jest oprogramowanie Apache, które sprawia, że komputer staje się serwerem WWW: przechowuje kod html strony internetowej, której inne komputery mogą żądać, nasłuchuje (domyślnie na porcie 80 TCP), czy nikt nie zgłasza się z takim żądaniem.

- a) Znajdź na komputerze pliki konfiguracyjne serwera WWW: kliknij w *Mój komputer* \Rightarrow *Dysk lokalny (C:)* \Rightarrow *Program Files* \Rightarrow *Apache Software Foundation* \Rightarrow *Apache 2.2*.
- b) W katalogu conf odszukaj plik *httpd.txt* — jest to plik zawierający konfigurację Twojego serwera WWW. Przyjrzyj się jego zawartości, aby zlokalizować miejsca, w których można skonfigurować:
- ścieżkę do plików programu Apache,
 - port TCP, na których serwer WWW nasłuchuje żądań,
 - listę zainstalowanych modułów,
 - adres e-mail do webmastera,
 - nazwę serwera WWW,
 - miejsce przechowywania plików z logami i wiele innych.
- c) Zmień port TCP, na którym Twój serwer WWW nasłuchuje żądań HTTP.
- W przeglądarce internetowej w pasku adresu wpisz swój adres IP, aby przekonać się, że obecnie serwer WWW działa na domyślnym porcie powiązanym z HTTP (80): powinna wyświetlić się prosta strona internetowa.
 - W pliku *httpd.txt* znajdź sekcję Listen i zmień port nasłuchiwania z 80 na 8080. Zrestartuj serwer WWW (kliknij ikonę Apache w prawym dolnym rogu i wybierz *Restart*).

- Po ponownym wpisaniu w przeglądarce swojego adresu IP, powinien pojawić się komunikat o niepowodzeniu otwarcia strony. Dopiero wpisanie pełnych danych gniazda: 172.16.1.X:8080 (gdzie X to ostatni oktet adresu IP Twojego komputera), przeglądarka wie, że ma zwrócić się do serwera na nowozmienionym porcie 8080.
- Do dokonania tejże zmiany u sąsiada, wpisz adres IP jego komputera w przeglądarce. Zobacz, że znów musisz jeszcze doprecyzować port, aby poprawnie wyświetlić jego stronę internetową.

d) Zmodyfikuj swoją domyślną stronę internetową.

- Znajdź plik *index.html* znajdujący się w katalogu *htdocs*, otwórz go za pomocą Notatnika.
- Zmodyfikuj jego zawartość w prosty sposób (zmień napis, kolor czcionki itp.).
- W przeglądarce internetowej wpisz znów swój adres IP i port 8080. Zobacz, jak modyfikując plik *index.html*, wpływasz na wygląd swojej strony internetowej.
- Po dokonaniu modyfikacji przez sąsiada, odwiedź jego stronę internetową.

2 Analiza ruchu TFTP

Wiesz już z poprzedniego ćwiczenia, że na Twoim komputerze zainstalowany jest program `tftpd32`, za pomocą którego Twój komputer staje się serwerem TFTP. Spróbuj wysłać na ten serwer plik tekstowy z konfiguracją laboratoryjnego przełącznika, a w programie Wireshark zaobserwuj, jak wygląda ruch TFTP podczas takiego przesyłu plików.

2.1 Przechwyć ruch TFTP.

- Uruchom program `tftpd32` (*Start* \Rightarrow *Programy* \Rightarrow *tftpd32*).
- Włącz program Wireshark i uruchom przechwytywanie danych (filtruj po TFTP).
- Zaloguj się na laboratoryjny switch (*telnet* 172.16.1.253 w cmd, hasło *cisco*). Przejdź komendą *enable* do trybu uprzywilejowanego (ponownie podaj hasło *cisco*).
- Uruchom przechwytywanie ruchu sieciowego w programie Wireshark, filtruj po TFTP.
- Wydadź przełącznikowi polecenie przekopiowania pliku z konfiguracją bieżącą (*running-config*) na serwer TFTP:

```
Switch# copy running-config tftp:
```

Doprecyzuj adres serwera TFTP, na który chcesz wysłać plik (podaj adres IP swojego komputera) oraz zostaw domyślną nazwę pliku po wysłaniu. Powinieneś zaobserwować, że plik pojawił się na pulpicie Twojego komputera.

- Zatrzymaj przechwytywanie danych w Wiresharku.

2.2 Przyjrzyj się przechwyconemu ruchowi TFTP.

99	29.564414	172.16.1.253	172.16.1.1	TFTP	write Request, File: switch-config, Transfer type: octet
100	29.566982	172.16.1.1	172.16.1.253	TFTP	Acknowledgement, Block: 0
102	29.571041	172.16.1.253	172.16.1.1	TFTP	Data Packet, Block: 1
103	29.572824	172.16.1.1	172.16.1.253	TFTP	Acknowledgement, Block: 1
106	29.572412	172.16.1.253	172.16.1.1	TFTP	Data Packet, Block: 2
107	29.572526	172.16.1.1	172.16.1.253	TFTP	Acknowledgement, Block: 2
108	29.575340	172.16.1.253	172.16.1.1	TFTP	Data Packet, Block: 3 (last)
109	29.575383	172.16.1.1	172.16.1.253	TFTP	Acknowledgement, Block: 3

- Zwróć uwagę na mechanizm potwierdzania odbioru stosowany w tym protokole.
- Przyjrzyj się podziałowi przesyłanych danych na równe bloki.

3 Analiza ruchu DHCP

3.1 Przechwycić ruch wygenerowany podczas wysyłania żądania i odbierania odpowiedzi DHCP.

- a) Wyłącz kartę sieciową LAB, włącz kartę o nazwie Internet, aby odzyskać dostęp do internetu. Upewnij się (we właściwościach TCP/IP karty sieciowej), że Twój komputer na karcie Internet ma uruchomione Pobieranie adresu IP automatycznie.
- b) Uruchom ponownie program Wireshark. Włącz przechwytywanie danych w Wiresharku, filtrując po DHCP (udp.port==68).
- c) Wymuś pobranie adresu poprzez DHCP, wpisując w Wierszu polecenia komendę *ipconfig/release* (zwolnienie dzierżawy) i *ipconfig/renew* (odświeżenie dzierżawy).

ipconfig/release

ipconfig/renew

- d) Zatrzymaj przechwytywanie danych w Wiresharku.

3.2 Przeanalizuj przechwycony ruch DHCP.

- a) Przyjrzyj się przechwyconemu ruchowi sieciowemu — rozwiń ostatnią sekcję w Wiresharku.

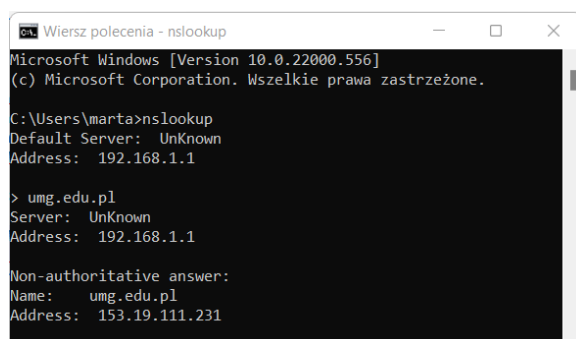
60 6.370257	192.168.1.9	192.168.1.1	DHCP	342 DHCP Release
93 12.005291	0.0.0.0	255.255.255.255	DHCP	344 DHCP Discover
102 13.039426	192.168.1.1	192.168.1.9	DHCP	344 DHCP Offer
103 13.040561	0.0.0.0	255.255.255.255	DHCP	370 DHCP Request
104 13.048074	192.168.1.1	192.168.1.9	DHCP	362 DHCP ACK

- b) Zaobserwuj, jak wyglądają wiadomości DHCP w trakcie negocjacji dzierżawy adresu IP:
 - wiadomość DHCPRELEASE od Ciebie, wymuszająca zwolnienie dzierżawy,
 - wiadomość DHCPDISCOVER od Ciebie, wysłana na adres rozgłoszeniowy w wyniku poszukiwania aktywnego serwera DHCP,
 - wiadomość DHCPOFFER z proponowanym adresem IP dla Twojego komputera,
 - wiadomość DHCPREQUEST od Ciebie, oznaczająca zgodę na przyjęcie proponowanego przez serwer adresu,
 - wiadomość DHCPACK, potwierdzającą dzierżawę.

4 Analiza ruchu DNS

4.1 Przechwycić ruch wygenerowany podczas wysyłania zapytania i odbierania odpowiedzi DNS.

- Otwórz program Wireshark i rozpocznij przechwytywanie ruchu sieciowego na karcie sieciowej Realtek. Włącz filtrowanie przechwyconego ruchu, tak, by widoczne były tylko wiadomości DNS.
- W Wierszu polecenia systemu Windows wydaj polecenie *nslookup*. Zadać serwerowi DNS zapytanie o adres IP jakiegokolwiek strony internetowej, np. umg.edu.pl.



```
Wiersz polecenia - nslookup
Microsoft Windows [Version 10.0.22000.556]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\martas>nslookup
Default Server:  UnKnown
Address:  192.168.1.1

> umg.edu.pl
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    umg.edu.pl
Address: 153.19.111.231
```

- Sprawdź, czy w programie Wireshark pojawiły się przechwycone dane, po czym zatrzymaj przechwytywanie danych.

4.2 Przeanalizuj przechwycony ruch DNS.

- Przyjrzyj się przechwyconym wiadomościom DNS.

1 0.000000	192.168.1.9	192.168.1.1	DNS	70 Standard query 0x0004 A umg.edu.pl
2 0.006196	192.168.1.1	192.168.1.9	DNS	86 Standard query response 0x0004 A umg.edu.pl A 153.19.111.231
3 0.007516	192.168.1.9	192.168.1.1	DNS	70 Standard query 0x0005 AAAA umg.edu.pl
4 0.020765	192.168.1.1	192.168.1.9	DNS	117 Standard query response 0x0005 AAAA umg.edu.pl SOA dns1.umg.edu.pl

- Zobacz, jak zbudowane jest zapytanie DNS, a jak odpowiedź. Jakiego typu odpowiedź uzyskał Twój komputer — autorytatywną czy nie? O jaki rekord pytał? Co jest w nim przechowywane?

4.3 Wyślij zapytania o inne niż A/AAAA rekordy DNS.

- Zmień typ poszukiwanych rekordów na MX i dowiedz się, jaki serwer pocztowy związany jest z domeną umg.edu.pl.

```
>set type=MX
>umg.edu.pl
```

- b) Zmień typ poszukiwanych rekordów na NS i dowiedz się, jaki serwer DNS związany jest z domeną umg.edu.pl.

```
>set type=NS
```

```
>umg.edu.pl
```

- c) Wyjdź z programu *nslookup* (poleceniem *exit*), po czym wyświetl przechowywane w pamięci Twojego komputera powiązania DNS (adresu mnemonicznego z IP).

```
ipconfig/displaydns
```

V. Pytania kontrolne

1. Jaka jest rola warstwy aplikacyjnej modelu OSI?
2. Do czego służy protokół HTTP i jak działa?
3. Do czego służy protokół TFTP i czym różni się od FTP?
4. Do czego służy protokół DHCP i jak działa?
5. Do czego służy protokół DNS i jakich informacji dostarcza?