

Sieci komputerowe

Wykład 8 — Warstwa aplikacyjna

Marta Szarmach
Zakład Telekomunikacji Morskiej
Wydział Elektryczny
Uniwersytet Morski w Gdyni

04.2022

Plan prezentacji

- 1 Przesył zawartości stron internetowych
 - HTTP
 - HTTPS
- 2 Przesył plików
 - FTP
 - TFTP
- 3 Poczta elektroniczna
 - SMTP
 - POP3 i IMAP
- 4 Przesył informacji sieciowych
 - DHCP
 - DNS
 - NTP

Warstwa aplikacyjna

Warstwa aplikacyjna — przypomnienie:

Rola

Udostępnianie
użytkownikom/aplikacjom
interfejsu do wprowadzania
danych do sieci:

- tworzenie wiadomości
- przekazywanie wiadomości do niższych warstw.

Protokoły

- Klientkie:
 - Przesył zawartości stron internetowych: HTTP i HTTPS
 - Przesył plików: FTP, TFTP
 - Poczta elektroniczna: SMTP, POP3, IMAP
 - Zdalny dostęp: telnet, SSH
- Sieciowo-kontrolne: DHCP, DNS, NTP, SNMP

1. Przesył zawartości stron internetowych

HTTP i HTTPS

1.1 Przesył zawartości stron internetowych. HTTP

HTTP (ang. *Hypertext Transfer Protocol*):

- Umożliwia przesył zawartości stron WWW
- Wykorzystuje port 80 TCP
- W oryginalnej wersji przesyłane dane nie są szyfrowane
- Protokół bezstanowy — dane wymienione pomiędzy urządzeniami nie są zapamiętywane (w tym celu na kliencie musi zostać zapisany plik *cookie*)
- Wymieniane są dane dotyczące m.in. wykorzystywanej przeglądarki internetowej, języka, kodowania znaków

1.2 Przesył zawartości stron internetowych. HTTPS

Rodzaje metod użytkownika w HTTP:

- GET — prośba o udostępnienie zasobu
- PUT — przesłanie danych na serwer (pod konkretną lokalizację)
- POST — przesłanie danych na serwer (np. danych z formularza)
- DELETE — żądanie usunięcia zasobu
- HEAD — sprawdzenie dostępności zasobu

5275	50.885743	192.168.1.9	153.19.112.229	HTTP	564 GET / HTTP/1.1
5279	50.905428	153.19.112.229	192.168.1.9	HTTP	586 HTTP/1.1 302 Found (text/html)
9187	85.696516	192.168.1.9	213.216.76.24	HTTP	136 GET /ncc.txt HTTP/1.1
9189	85.726370	213.216.76.24	192.168.1.9	HTTP	205 HTTP/1.1 200 OK (text/html)

1.2 Przesył zawartości stron internetowych. HTTPS

Przykładowe komunikaty od serwera:

- 200 — OK
- 201 — Created
- 302 — Found (dane są chwilowo pod innym adresem)
- 304 — Not modified

- 404 — Not Found
- 110 — Connection time out
- 111 — Connection refused
- 503 — Service unavailable (chwilowe przeciążenie)

1.2 Przesył zawartości stron internetowych. HTTPS

HTTPS (ang. *Hypertext Transfer Protocol Secure*):

- Bardziej bezpieczna wersja HTTP, w której dane są szyfrowane
- Wykorzystuje port 443 TCP na warstwie transportowej
- Na warstwie prezentacji wykorzystuje protokół TLS (ang. *Transport Layer Security*), który zapewnia szyfrowanie danych czy uwierzytelnianie serwerów

2. Przesył plików

FTP i TFTP

2.1 Przesył plików. FTP

FTP (ang. *File Transfer Protocol*):

- Umożliwia pobranie pliku z serwera lub jego wysłanie na serwer
- Umożliwia takie dodatkowe funkcjonalności jak:
uwierzytelnianie użytkownika (ale też i dostęp anonimowy),
praca na folderach
- Wykorzystuje 2 porty TCP: jeden do przesyłu informacji sterujących (uwierzytelnianie, wskazanie pliku), a inny do przesyłu faktycznych danych
- Może pracować w dwóch trybach: aktywnym oraz pasywnym

2.1 Przesył plików. FTP

Tryby pracy FTP:

Tryb aktywny

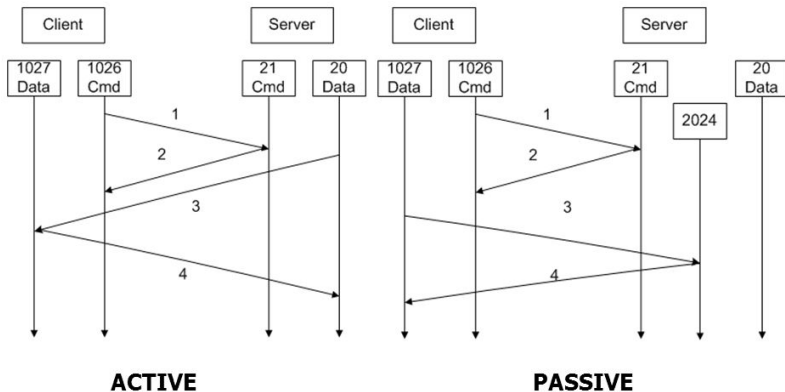
- Klient z portu prywatnego X nawiązuje z serwerem połączenie kontrolne na porcie 21, a serwer inicjuje powstanie sesji do przesyłu danych (na serwerze na porcie 20, u klienta $X+1$)
- Problemem może być blokowanie portu $X+1$ przez firewall klienta dla połączeń z zewnątrz

Tryb pasywny

- Klient z portu prywatnego X nawiązuje z serwerem połączenie kontrolne na porcie 21, a następnie inicjuje powstanie sesji do przesyłu danych (na serwerze na porcie prywatnym Y, u siebie $X+1$)
- Problem blokowania portu przez firewall nie występuje (ruch zainicjowano z wewnątrz sieci)

2.1 Przesył plików. FTP

Tryby pracy FTP:



Grafika: medium.com

2.2 Przesył plików. TFTP

TFTP (ang. *Trivial File Transfer Protocol*):

- Jest uproszczoną wersją FTP — nie umożliwia uwierzytelniania użytkowników, obsługi folderów
- Wykorzystuje port 69 UDP
- Posiada wbudowany mechanizm potwierdzania otrzymania porcji danych
- Dane wysyłane są w 512-bajtowych blokach (otrzymanie mniejszego bloku oznacza koniec transmisji)

2.2 Przesył plików. TFTP

Przykładowy przebieg komunikacji 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	29.571124	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

3. Poczta elektroniczna

SMTP, IMAP i POP3

3.1 Poczta elektroniczna. SMTP

SMTP (ang. *Simple Mail Transfer Protocol*):

- Umożliwia wysyłanie poczty elektronicznej (stanowi serwer poczty wychodzącej)
- Wykorzystuje port 25 TCP
- Proces wysyłania poczty:
 1. Rozpoczęcie połączenia (EHLO)
 2. Przekazanie adresu nadawcy (MAIL From)
 3. Przekazanie adresu odbiorcy (RCPT To)
 4. Przekazanie treści wiadomości (DATA)
 5. Zakończenie połączenia (QUIT)

3.1 Poczta elektroniczna. SMTP

Przykładowa sesja SMTP:

```
C:\>telnet eagle-server.example.com 25
220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Sun, 28 Jan
2007 20:41:0
3 +1000
HELO eagle-server.example.com
250 localhost.localdomain Hello [172.16.1.2], pleased to meet you
MAIL From: ccna2@example.com
250 2.1.0 ccna2@example.com... Sender ok
RCPT To: instructor@example.com
250 2.1.5 instructor@example.com... Recipient ok
DATA
354 Please start mail input.
Test e-mail serwera SMTP...
.
250 Mail queued for delivery.
QUIT
221 Closing connection. Good bye.
Połączenie z hostem przerwane.
C:\>
```

3.2 Poczta elektroniczna. POP3 i IMAP

Protokoły obsługujące pocztę przychodzącą:

POP3

- *Post Office Protocol ver. 3*
- Wykorzystuje port 110 TCP
- Umożliwia pobieranie i kasowanie poczty, tworząc kopię u klienta

IMAP

- *Internet Message Access Protocol*
- Wykorzystuje port 143 TCP
- Umożliwia zdalny dostęp do folderów z pocztą na serwerze

4. Przesył informacji sieciowych

DHCP, DNS, NTP

4.1 Przesył informacji sieciowych. DHCP

DHCP (ang. *Dynamic Host Configuration Protocol*):

- Umożliwia automatycznie przydzielanie hostom adresacji IP (administrator nie musi tego robić statycznie)
- Wykorzystuje porty 67 (u serwera) i 68 (u klienta) UDP
- Przekazuje klientowi (hostowi) takie informacje, jak:
 - Adres IP
 - Maskę sieciową
 - Adres IP bramy domyślnej
 - Adres IP serwera DNS
 - i inne

4.1 Przesył informacji sieciowych. DHCP

Proces otrzymania adresu dzięki DHCP:

1. Klient poszukuje obecnego w sieci serwera DHCP (komunikat DHCPDISCOVER).
2. Serwer odpowiada na wołanie 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.

4.1 Przesył informacji sieciowych. DHCP

Proces otrzymania adresu dzięki DHCP:

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

- Klient co jakiś czas wysyła DHCPREQUEST, aby odnowić dzierżawę adresu IP (w połowie czasu).
- Klient może zrezygnować z dzierżawy, wysyłając DHCPRELEASE.

4.2 Przesył informacji sieciowych. DNS

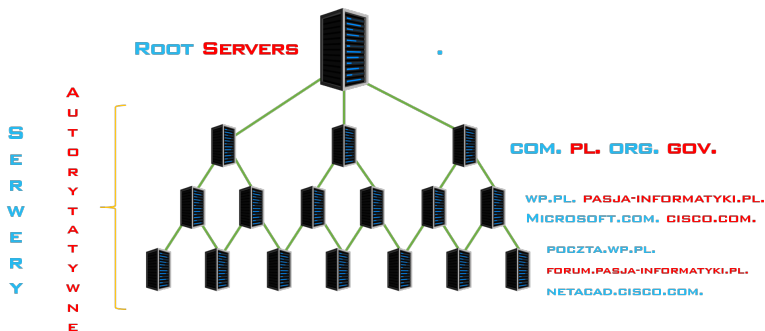
DNS (ang. *Domain Name System*):

- 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 UDP

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

4.2 Przesył informacji sieciowych. DNS

Hierarchia systemu DNS:

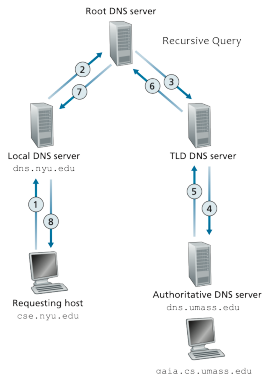
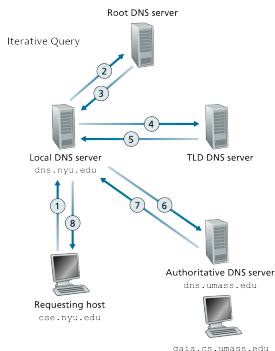


Grafika: pasja-informatyki.pl

4.2 Przesył informacji sieciowych. DNS

Rodzaje odpowiedzi DNS:

- **Iteracyjne** — serwer musi dać odpowiedź
- **Rekurencyjne** — serwer może odesłać do innych



4.2 Przesył informacji sieciowych. DNS

Rodzaje odpowiedzi DNS:

- **Autorytatywne** — otrzymana od serwera posiadającego bezpośrednią informację o domenie
- **Nieautorytatywne** — otrzymana od serwera niezaufanego

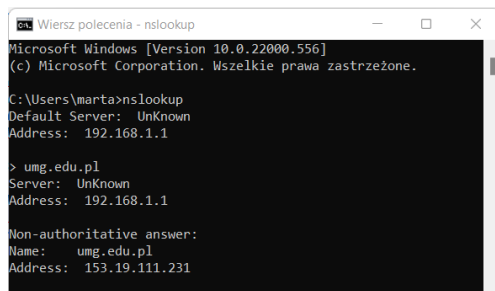
Rekordy DNS:

- A — adres IPv4 domeny
- AAAA — adres IPv6 domeny
- CNAME — nazwa kanoniczna domeny
- MX — adres serwera pocztowego domeny
- NS — adres serwera DNS domeny

4.2 Przesył informacji sieciowych. DNS

Komendy obsługujące DNS w systemie Windows:

- **ipconfig/displaydns** — wyświetla powiązania DNS z pamięci podręcznej
- **nslookup** — umożliwia wydawanie zapytań DNS



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

C:\Users\marta>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
```

4.3 Przesył informacji sieciowych. NTP

NTP (ang. *Network Time Protocol*):

- Umożliwia synchronizację czasu na urządzeniach sieciowych: klienci odpytują serwer o czas i modyfikują wskazania swoich zegarów systemowych (uwzględniając czas propagacji pakietu)
- Wykorzystuje 123 port UDP
- Hierarchia urządzeń:
 - STRATUM0 — pierwotne wzorce czasu UTC (zegary atomowe)
 - STRATUM1 — wysokiej jakości serwery mające bezpośredni dostęp do wzorców czasu
 - STRATUM2 — serwery odpytujące serwery STRATUM1
 - STRATUM3 — serwery lokalne, odpytujące serwery STRATUM2
 - STRATUM4 — komputery odpytujące serwery STRATUM3