

Sieci komputerowe

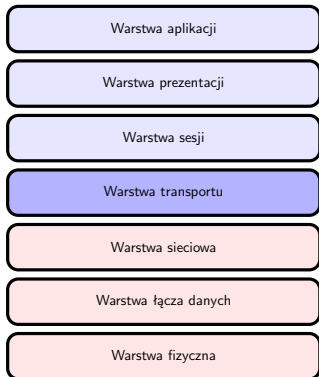
Warstwa transportu

R. Wojciechowski¹ Ł. Sturgulewski¹ M. Bąkała¹
A. Sierszeń¹ G. Nowak¹

¹Institut Informatyki Stosowanej Politechniki Łódzkiej
<http://www.iis.p.lodz.pl>

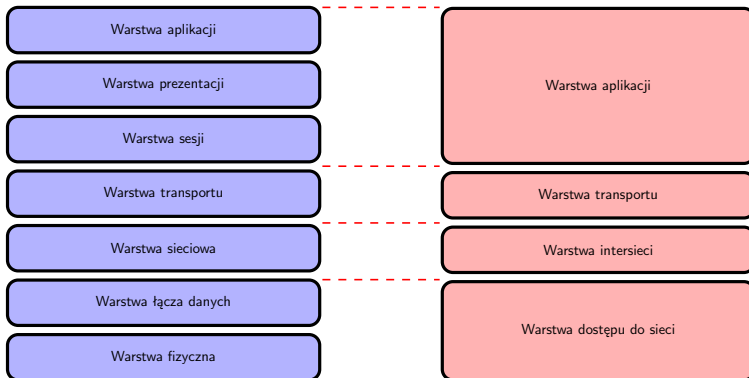
©2018, v2.0

Warstwa transportu

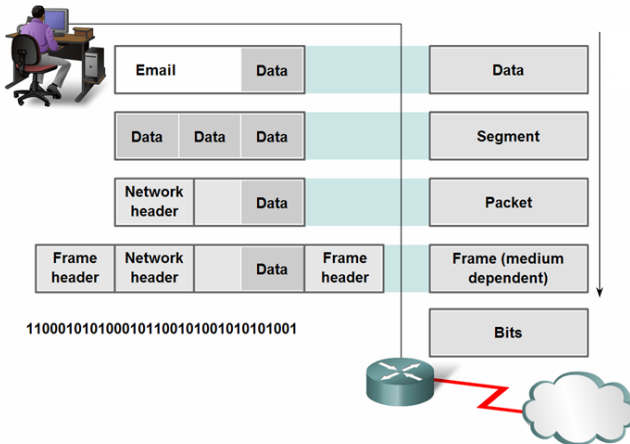


- Oddzielenie warstw fizycznych od aplikacyjnych
- Dostarczanie niezawodnych usług komunikacyjnych – ustanawianie, utrzymywanie i rozłączanie wirtualnych połączeń
- Podział informacji na mniejsze segmenty i składanie segmentów w całą, spójną informację
- Połączenie między stacjami

Model TCP/IP vs OSI



Enkapsulacja danych



Materiały szkoleniowe Cisco CCNA: <http://www.netacad.com>

Zadania warstwy transportowej

- Warstwa transportu wprowadza przezroczysty transfer danych pomiędzy użytkownikami docelowymi wprowadzając mechanizmy zapewniające niezawodność transmisji
- Strumień danych warstwy transportowej jest logicznym połączeniem pomiędzy punktami w sieci
- Kontrola nad strumieniem jest realizowana przy udziale warstw niższych i obejmuje szereg mechanizmów segmentacji, potwierdzeń, przesuwnego okna, ...

Zadania warstwy transportowej

- Realizacja funkcji transportu danych
- Niezawodne i precyzyjne regulowanie przepływu informacji ze źródła do celu
- *Quality of Service*
- Kontrola przepływu wspomagana przez niższe warstwy modelu OSI

Identyfikator portu

- Zamysłem wprowadzenia identyfikatorów portów było umożliwienie transmisji współbieżnej informacji pochodzących z różnych strumieni (źródeł danych) poprzez mechanizmy znakowania usług i odpowiedniej synchronizacji dialogu komunikacyjnego

Znakowanie usług

- Strumienie danych pochodzące od aplikacji klienckich i przekazywane do określonych usług zdalnych wykorzystują mechanizm portów do identyfikacji określonych sesji warstw wyższych
- Numeracja portów
 - 0 – 1023 → porty określone przydzielane przez IANA (*Internet Assigned Numbers Authority*)
 - 1024 – 65535 → porty dynamiczne
 - porty zarejestrowane dla określonych producentów (najczęściej również w zakresie 1024 – 65535)
- Identyfikacja toru nadawca \longleftrightarrow odbiorca: $[Adres\ IP] + [Numer\ portu]$

Numery portów

```
zly.kis.p.lodz.pl - PuTTY
#ident "@(#)services 1.32 01/11/21 SMI"
#
#
# Copyright (c) 1999-2001 by Sun Microsystems, Inc.
# All rights reserved.
#
# Network services, Internet style
#
tcpmux      1/tcp
echo        7/tcp
echo        7/udp
discard     9/tcp      sink null
discard     9/udp      sink null
sysstat     11/tcp
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
chargen     19/tcp      ttytst source
chargen     19/udp      ttytst source
ftp-data    20/tcp
ftp         21/tcp
ssh         22/tcp      # Secure Shell
telnet      23/tcp
/etc/services
```



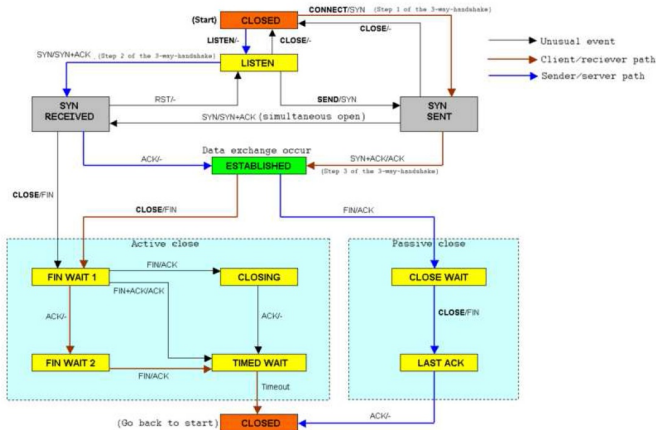
Stany portów

- Podczas komunikacji pomiędzy usługami na konkretnych portach, wyszczególnia się określone stany portów w zależności od sytuacji w sesji
- Możliwe stany portów: LISTEN, SYN-SENT, SYN-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, TIME-WAIT, CLOSED

Stany portów

- **LISTEN** - stan nasłuchiwania, oczekiwanie na połączenie ze zdalnego hosta (→ typowy stan w aplikacjach serwerowych)
- **SYN-SENT** - stan oczekiwania na odpowiedź zdalnej strony z ustawionymi flagami SYN oraz ACK (wysłano SYN, *3-way handshake*)
- **SYN-RECEIVED** - stan oczekiwania na odpowiedź zdalnej strony z potwierdzeniem ACK (wysłano SYN i ACK, *3-way handshake*)
- **ESTABLISHED** - stan gotowości do wymiany danych (sesja zestawiona)

Stany portów



Protokół zorientowany połączeniowo

Protokół zorientowany połączeniowo

Protokół zorientowany połączeniowo - mechanizm transmisji danych zakładający ustanowienie połączenia (negocjację ustawień połączenia) przed właściwą wymianą danych. Protokoły zorientowane połączeniowo zalicza się do grupy protokołów niezawodnych, gdyż gwarantują otrzymanie danych przez stronę zdalną we właściwej sekwencji

Materiały szkoleniowe Cisco CCNA: <http://www.netacad.com>

Protokół bezpołączeniowy

Protokół bezpołączeniowy

Protokół bezpołączeniowy - mechanizm transmisji danych umożliwiający wysłanie danych bez wcześniejszego ustanowienia połączenia (negocjacji ustawień). Protokoły bezpołączeniowe zalicza się do grupy protokołów zawodnych, gdyż nie gwarantują otrzymania danych przez stronę zdalną (brak mechanizmów potwierżeń)

Materiały szkoleniowe Cisco CCNA: <http://www.netacad.com>

Protokoły warstwy transportu

- TCP (*Transmission Control Protocol*)
- UDP (*User Datagram Protocol*)
- SCTP (*Stream Control Transmission Protocol*)

Protokół TCP, *Transmission Control Protocol*

- Protokół zorientowany połączeniowo (wirtualne obwody) → niezawodność
- Segmentyzacja danych / konsolidacja segmentów
- Retransmisja wszystkiego, co nie zostało odebrane

Nagłówek prokołu TCP

+	Bits 0–3	4–9	10–15	16–31
0	Source Port			Destination Port
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Reserved	Flags	Window
128	Checksum			Urgent Pointer
160	Options (optional)			
160/192+	Data			

Nagłówek prokołu IP oraz TCP

+	Bits 0–3	4–7	8–9	10–15	16–31
0	Source address				
32	Destination address				
64	Zeros		Protocol		TCP length
96	Source Port			Destination Port	
128	Sequence Number				
160	Acknowledgement Number				
192	Data Offset	Reserved	Flags		Window
224	Checksum			Urgent Pointer	
256	Options (optional)				
256/288+	Data				

Nagłówek prokołu TCP, flagi

- URG – informuje o istotności pola priorytetu
- ACK – informuje o istotności pola numeru potwierdzenia
- PSH – wymusza przesłanie pakietu
- RST – resetuje połączenie (wymagane ponowne uzgodnienie sekwencji)
- SYN – synchronizuje kolejne numery sekwencyjne
- FIN – oznacza zakończenie przekazu danych
- NS, CWR, ECE – obsługa przeciążeń

Kontrola przepływu

- Dostosowanie tempa transmisji poprzez wprowadzenie mechanizmów potwierdzeń umożliwiających spowolnienie tempa nadawania
- Transmisja określonych sekwencji danych poprzez wprowadzenie numerów sekwencyjnych i uwzględnienie ich w numerach potwierdzeń
- Wprowadzenie metod korekcji błędów - definicje sposobów wykrywania błędów transmisji (*Error Detection* → CRC16, CRC32, ...) oraz reakcji na nie (*Error Control* → ARQ)

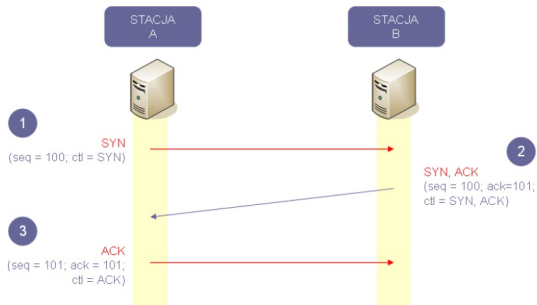
Metody kontroli przepływu TCP

- Potrójny uścisk ręki / Nawiązanie połączenia
- Wprowadzenie numerów sekwencyjnych transmitowanych danych
- Mechanizm potwierdzeń TCP
- Mechanizm przesuwnego okna

Potrójny uścisk ręki

- Procedura inicjalizacyjna przeprowadzana w celu synchronizacji początkowych numerów sekwencyjnych ramek nadawcy i odbiorcy
- Kontrola przepływu realizowana na podstawie numerów sekwencyjnych ramek
- Konieczność synchronizacji - brak powiązania między numerami sekwencyjnymi a innymi czynnikami mogącymi mieć wpływ na dobór numeru początkowego

Potrójny uścisk ręki



Potrójny uścisk ręki

```
* Frame 3 (62 bytes on wire, 62 bytes captured)
* Ethernet II, Src: 00:0d:9d:c8:8e:ad, Dst: 00:e0:18:b6:66:79
* Internet Protocol, Src Addr: 192.168.1.2 (192.168.1.2), Dst Addr: 192.168.1.2 (192.168.1.2)
* Transmission Control Protocol, Src Port: 3227 (3227), Dst Port: 3227 (3227)
  Source port: 3227 (3227)
  Destination port: ftp (21)
  Sequence number: 0 (relative sequence number)
  Header length: 28 bytes
  Flags: 0x0002 [SYN]
    0... .. = Congestion Window Reduced (CWR): Not set
    .0... .. = ECN-Echo: Not set
    ..0... .. = Urgent: Not set
    ...0... .. = Acknowledgment: Not set
    ....0... .. = Push: Not set
    .....0... .. = Reset: Not set
    .....1... .. = Syn: Set
    .....0... .. = Fin: Not set
  Window size: 25200
  Checksum: 0xc52f (correct)
  Options: (8 bytes)
```

```
* Frame 4 (62 bytes on wire, 62 bytes captured)
* Ethernet II, Src: 00:e0:18:b6:66:79, Dst: 00:0d:9d:c8:8e:ad
* Internet Protocol, Src Addr: 212.51.216.2 (212.51.216.2), Dst Addr: 212.51.216.2 (212.51.216.2)
* Transmission Control Protocol, Src Port: ftp (21), Dst Port: 3227 (3227)
  Source port: ftp (21)
  Destination port: 3227 (3227)
  Sequence number: 0 (relative sequence number)
  Acknowledgement number: 1 (relative ack number)
  Header length: 28 bytes
  Flags: 0x0012 [SYN, ACK]
    0... .. = Congestion Window Reduced (CWR): Not set
    .0... .. = ECN-Echo: Not set
    ..0... .. = Urgent: Not set
    ...1... .. = Acknowledgment: Set
    ....0... .. = Push: Not set
    .....0... .. = Reset: Not set
    .....1... .. = Syn: Set
    .....0... .. = Fin: Not set
  Window size: 17520
  Checksum: 0x05d6 (correct)
  Options: (8 bytes)
  SEQ/ACK analysis
```

```
* Frame 5 (54 bytes on wire, 54 bytes captured)
* Ethernet II, Src: 00:0d:9d:c8:8e:ad, Dst: 00:e0:18:b6:66:79
* Internet Protocol, Src Addr: 192.168.1.2 (192.168.1.2), Dst Addr: 192.168.1.2 (192.168.1.2)
* Transmission Control Protocol, Src Port: 3227 (3227), Dst Port: 3227 (3227)
  Source port: 3227 (3227)
  Destination port: ftp (21)
  Sequence number: 1 (relative sequence number)
  Acknowledgement number: 1 (relative ack number)
  Header length: 20 bytes
  Flags: 0x0010 [ACK]
    0... .. = Congestion Window Reduced (CWR): Not set
    .0... .. = ECN-Echo: Not set
    ..0... .. = Urgent: Not set
    ...1... .. = Acknowledgment: Set
    ....0... .. = Push: Not set
    .....0... .. = Reset: Not set
    .....0... .. = Syn: Not set
    .....0... .. = Fin: Not set
  Window size: 25200
  Checksum: 0x149a (correct)
  SEQ/ACK analysis
```


TCP, wymiana danych

- Bezbłędny transfer danych
- Transfer oczekiwanych danych (z zachowaniem kolejności)
- Retransmisja zagubionych pakietów
- Ignorowanie zduplikowanych pakietów
- Zapobieganie przeciążeniom

Protokół UDP, *User Datagram Protocol*

- Protokół bezpołączeniowy → zawodność
- Transmisja datagramów bez podziału ani konsolidacji przepływających informacji
- Brak mechanizmów sprawdzenia poprawności otrzymania informacji i kontroli przepływu (→ niezawodność może być realizowana przez protokoły warstw wyższych)

Nagłówek prokołu UDP

Packetsizer - [Capture Session]

File Edit Session Utilities Window Help

Decode Protocols Connections Statistics Wireless Capture Filter

Received 8 Parsed Filter: B Memory: 0.0%

Num	Source Address	Dest Address	Summary
1	0.0.0.0	255.255.255.255	DHCP: DHCP Discover - Transaction ID 0x...
2	192.168.1.1	255.255.255.255	DHCP: DHCP Offer - Transaction ID 0x...
3	0.0.0.0	255.255.255.255	DHCP: DHCP Request - Transaction ID 0x...
4	192.168.1.1	255.255.255.255	DHCP: DHCP ACK - Transaction ID 0x...
5	D-Link_a9:c7:dc	Broadcast	ARP: Who has 192.168.1.5? Gratuitous AR
6	D-Link_a9:c7:dc	Broadcast	ARP: Who has 192.168.1.5? Gratuitous AR
7	D-Link_a9:c7:dc	Broadcast	ARP: Who has 192.168.1.5? Gratuitous AR
8	192.168.1.5	239.255.255.230	SSDP: M-SEARCH * HTTP://1.1

Frame 1 (342 bytes on wire, 342 bytes captured)

Ethernet II, Src: 08:00:00:00:00:00, Dest: FF:FF:FF:FF:FF:FF

User Datagram Protocol, Src Port: bootpc (68), Dest Port: bootpc (67)

Source port: bootpc (68)

Destination port: bootpc (67)

Length: 308

Checksum: 0xaed6 (correct)

bootstrp Protocol

Display Filter: Apply Edit Reset

0000: ff ff ff ff ff 00 00 88 e9 c7 dc 08 00 41 00
 0010: 01 48 a1 15 00 00 80 11 98 72 00 00 00 ff ffH.S.....
 0020: ff ff 00 44 00 43 01 34 a6 40 01 01 08 00 87 13B.C.A.M.....
 0030: 77 06 00 00 00 00 00 00 00 00 00 00 00 00 00W.....
 0040: 00 00 00 00 00 00 00 00 88 e9 c7 dc 00 00 00 00
 0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0110: 00 00 00 00 00 00 63 82 53 63 35 01 01 74 01 01C.S.C.S.....

Porównanie protokołów warstwy transportu

	TCP	UDP
Rozmiar nagłówka	20 bajtów	8 bajtów
Treść pakietu	Segment	Datagram
Numer portu	Tak	Tak
Zorientowany połączeniowo	Tak	Nie
ARQ	Tak	Nie
Numeracja sekw. segmentu	Tak	Nie
Kontrola przepływu	Tak	Nie

TCP i UDP

Zastanów się, jakie następstwa wynikają z korzystania z TCP, a jakie z UDP.



Warstwa aplikacji i transportu

Zastanów się, które z poznanych protokołów warstwy aplikacji korzystają z TCP, które z UDP.



Weryfikacja portów komunikacyjnych

- Weryfikacja portów komunikacyjnych

Windows -> cmd -> netstat -a

Command Prompt

```
C:\Users\student>netstat -a
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	LAB309:0	LISTENING
TCP	0.0.0.0:445	LAB309:0	LISTENING
TCP	0.0.0.0:1025	LAB309:0	LISTENING
TCP	0.0.0.0:1026	LAB309:0	LISTENING
TCP	0.0.0.0:1027	LAB309:0	LISTENING
TCP	0.0.0.0:1028	LAB309:0	LISTENING
TCP	0.0.0.0:1037	LAB309:0	LISTENING
TCP	0.0.0.0:1051	LAB309:0	LISTENING
TCP	0.0.0.0:1093	LAB309:0	LISTENING
TCP	0.0.0.0:1307	LAB309:0	LISTENING
TCP	0.0.0.0:1309	LAB309:0	LISTENING
TCP	0.0.0.0:2179	LAB309:0	LISTENING
TCP	0.0.0.0:2343	LAB309:0	LISTENING
TCP	0.0.0.0:3500	LAB309:0	LISTENING
TCP	0.0.0.0:3502	LAB309:0	LISTENING
TCP	0.0.0.0:8080	LAB309:0	LISTENING
TCP	0.0.0.0:8834	LAB309:0	LISTENING
TCP	0.0.0.0:48080	LAB309:0	LISTENING
TCP	0.0.0.0:59110	LAB309:0	LISTENING
TCP	0.0.0.0:59111	LAB309:0	LISTENING
TCP	0.0.0.0:59112	LAB309:0	LISTENING
TCP	0.0.0.0:59113	LAB309:0	LISTENING
TCP	10.10.22.11:139	LAB309:0	LISTENING
TCP	10.10.22.11:1642	wav02s05-in-f14:https	ESTABLISHED
TCP	127.0.0.1:1029	LAB309:1030	ESTABLISHED



Metody skanowania portów

- TCP – connect
- TCP SYN
- TCP FIN
- TCP ACK
- ...

TCP - connect

- Test polega na przeprowadzeniu połączenia TCP: intruz wysyła na określony port pakiet SYN. Jeśli skanowany host odpowie pakietem SYN/ACK oznacza to, że port jest otwarty, jeśli RST/ACK – port jest zamknięty. Jeśli połączenie zostało nawiązane intruz zamyka je pakietem ACK
- Skanowanie TCP – connect jest łatwe do wykrycia

TCP SYN

- Modyfikacja TCP – connecta
- Polega na przeprowadzeniu połączenia TCP: intruz wysyła na określony port pakiet SYN. Jeśli skanowany host odpowie pakietem SYN/ACK oznacza to, że port jest otwarty, jeśli RST/ACK – port jest zamknięty. Jeśli połączenie zostało nawiązane intruz go NIE zamyka - połączenie nie trafia do logów systemowych
- Skanowanie TCP SYN jest trudniejsze do wykrycia niż TCP - connect

TCP FIN

- Technika ukrytego skanowania (*stealth scanning*)
- Celem jest ominięcie reguł filtrowania i ukrycie faktu skanowania
- Wykorzystanie własności stosu TCP polegającej na tym, że zamknięty port powinien na każdy błędny pakiet odpowiedzieć pakietem RST, otwarty zignoruje pakiet FIN
- Aby wykryć skanowanie FIN należy zastosować narzędzia IDS

Skanowanie sieci z wykorzystaniem nmap

- Różne typy skanowania (TCP SYN, Connect, ACK)

```
nmap [-sS | -sT | -sA] (...)
```

- Ograniczenie zakresu portów poddanych skanowaniu

```
nmap -p [Zakres portów] (...)
```

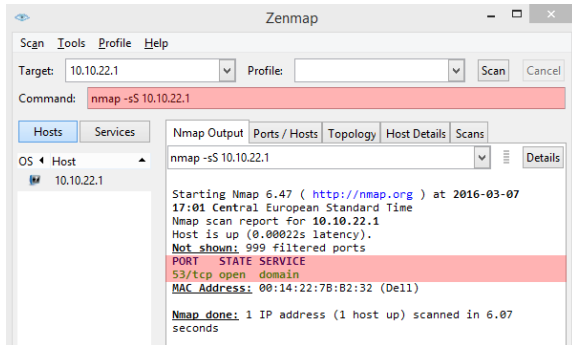
```
nmap -p 22, -p 1-10, -p U:53,T:100-200 (...)
```



Skanowanie sieci z wykorzystaniem nmap

- Skanowanie portów określonego hosta

`nmap -sS 10.10.22.1`



Koniec

Dziękuję za uwagę . . .