

Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś ^
- 1.0 Wprowadzenie v
- 1.1 Sieci wpływają na nasze życie v
- 1.2 Komponenty sieciowe v
- 1.3 Reprezentacja sieci i topologie v
- 1.4 Typowe rodzaje sieci v
- 1.5 Połączenie z Internetem v
- 1.6 Niezawodne sieci v
- 1.7 Trendy sieciowe v
- 1.8 Bezpieczeństwo sieci v
- 1.9 Profesjonalista IT v
- 1.10 Moduł ćwiczeń i quizu v
- 1.10.1 Czego się nauczyłem przerabiając ten moduł?

[🏠](#) / [Warstwa transportu](#) / [Niezawodność i kontrola przepływu](#)

Niezawodność i kontrola przepływu

14.6.1

Niezawodność w TCP - Gwarantowane i uporządkowane dostarczanie



Powodem, dla którego TCP jest lepszym protokołem dla niektórych aplikacji jest to, że w przeciwieństwie do UDP, ponownie wysyła porzucone pakiety i numeruje pakiety, aby wskazać ich prawidłową kolejność przed dostarczeniem. TCP może również pomóc w utrzymaniu przepływu pakietów, tak aby urządzenia nie zostały przeciążone. W tym temacie omówiono szczegółowo te cechy TCP.

Może zdarzyć się, że segmenty TCP nie docierają do miejsca przeznaczenia. Innym razem segmenty TCP mogą przychodzić nieuporządkowane. Aby odbiorca mógł zrozumieć oryginalną wiadomość, wszystkie dane muszą zostać odebrane, a dane w tych segmentach muszą zostać ponownie złożone w oryginalnej kolejności. Do tego celu używane są numery sekwencyjne, znajdujące się w nagłówku każdego segmentu. Numer sekwencyjny reprezentuje pierwszy bajt danych segmentu TCP.

Podczas nawiązywania sesji ustalany jest początkowy (inicjujący) numer sekwencyjny ISN. Ten numer ISN reprezentuje wartość początkową bajtów przesyłanych do aplikacji odbierającej. W miarę przesyłania danych, podczas sesji, numer sekwencyjny zwiększany jest o liczbę (bajtów), które zostały wysłane. Ten sposób nadzorowania ilości bajtów danych, umożliwia unikalną identyfikację i potwierdzenie każdego segmentu. Dzięki temu zaginione segmenty mogą być zidentyfikowane.

ISN nie rozpoczyna się od wartości jeden, ale jest w rzeczywistości liczbą losową. Ma to na celu zapobieganie niektórym typom złośliwych ataków. Dla uproszczenia, użyjemy ISN 1 w przykładach w tym module.

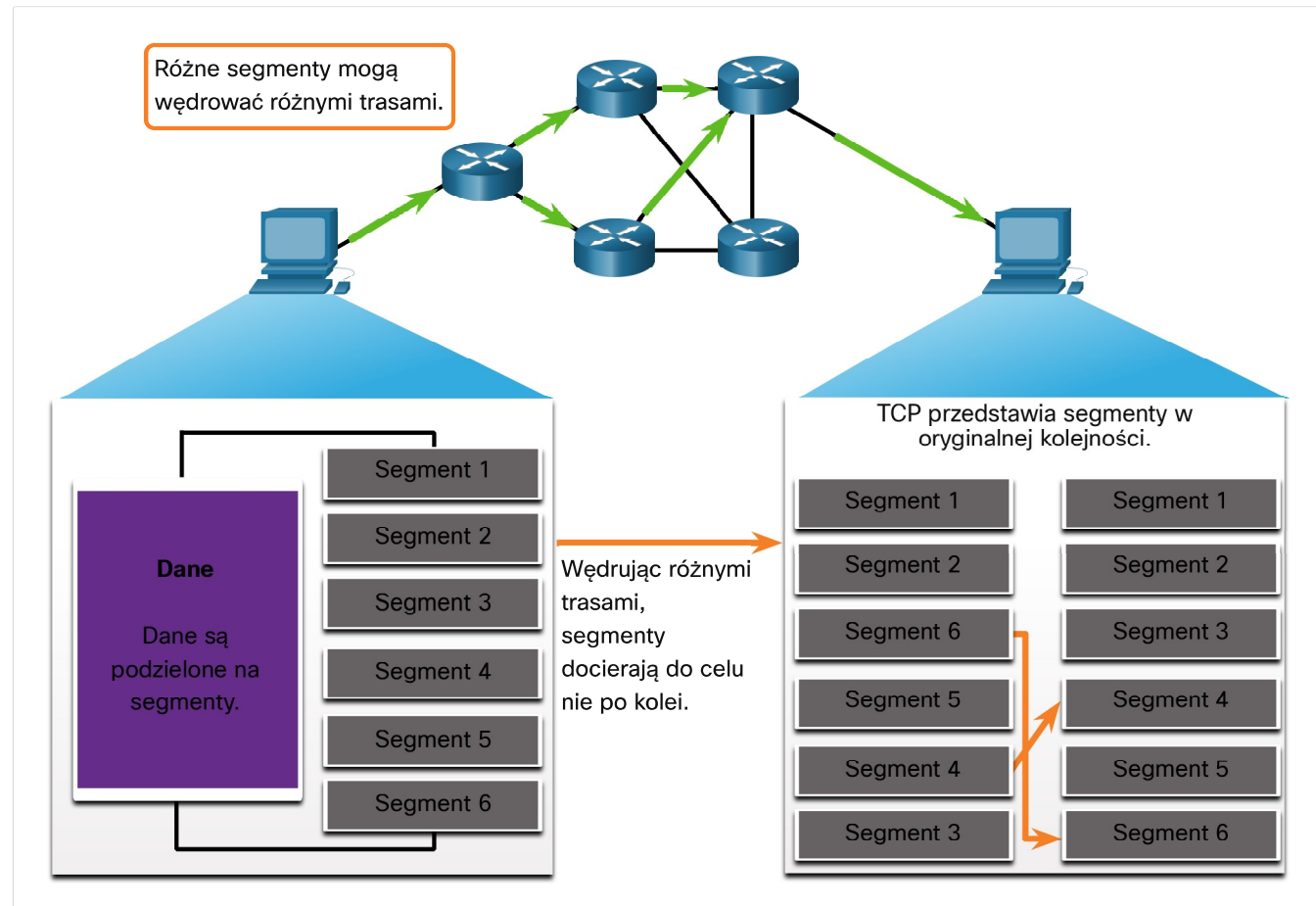
Numery sekwencyjne segmentów wskazują, jak ponownie złożyć i zmienić kolejność otrzymanych segmentów, jak pokazano na rysunku.

Kolejność segmentów TCP zostaje uporządkowana w miejscu

Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś ^
- 1.0 Wprowadzenie v
- 1.1 Sieci wpływają na nasze życie v
- 1.2 Komponenty sieciowe v
- 1.3 Reprezentacja sieci i topologie v
- 1.4 Typowe rodzaje sieci v
- 1.5 Połączenie z Internetem v
- 1.6 Niezawodne sieci v
- 1.7 Trendy sieciowe v
- 1.8 Bezpieczeństwo sieci v
- 1.9 Profesjonalista IT v
- 1.10 Moduł ćwiczeń i quizu v
- 1.10.1 Czego się nauczyłem przerabiając ten moduł?

przeznaczenia



Odbierający proces TCP, umieszcza dane z segmentu w buforze odbioru. Segmenty są składane we właściwej kolejności, wynikającej z numeru sekwencyjnego, a następnie przekazane aplikacji. Wszelkie segmenty przychodzące z numerami sekwencji, które są poza kolejnością, są przechowywane do późniejszego przetworzenia. Po otrzymaniu brakujących segmentów, dane zostają niezwłocznie ułożone we właściwej kolejności.

14.6.2



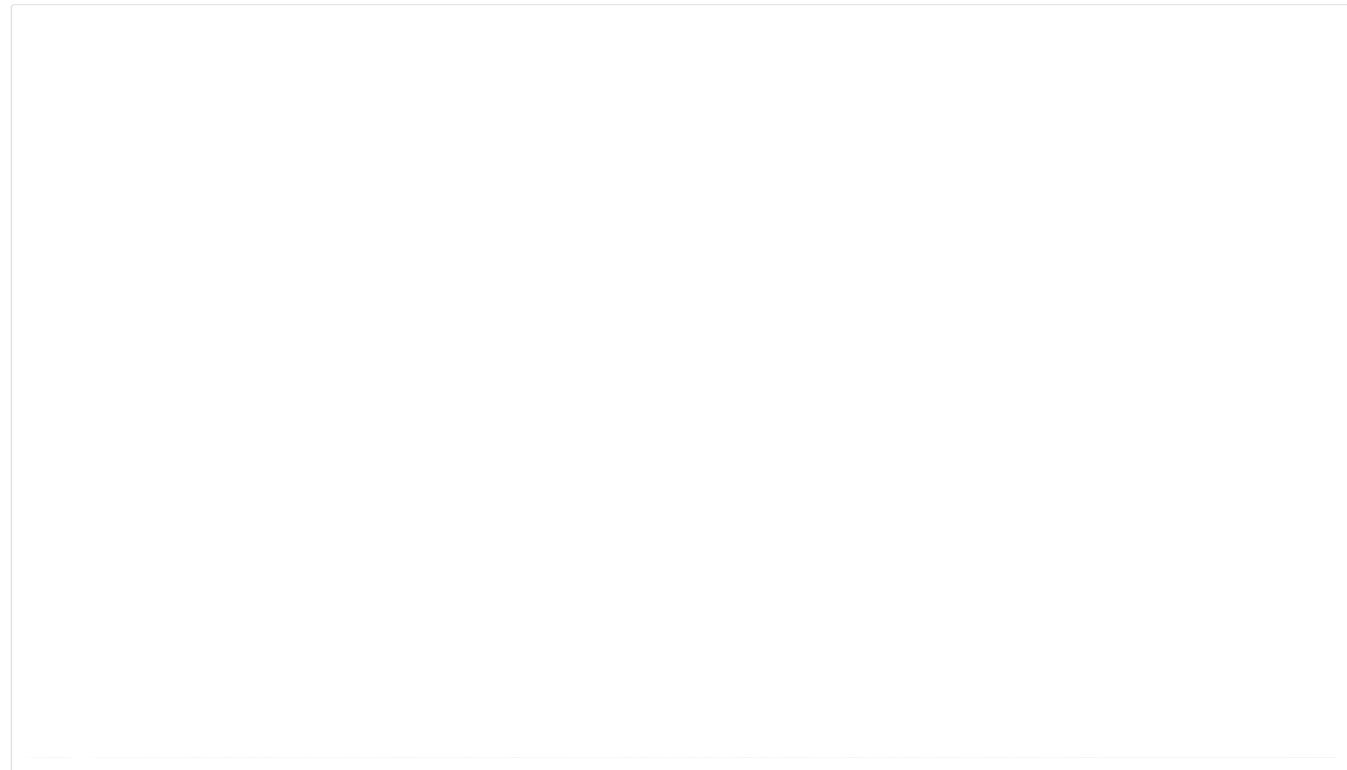
Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś ^
- 1.0 Wprowadzenie v
- 1.1 Sieci wpływają na nasze życie v
- 1.2 Komponenty sieciowe v
- 1.3 Reprezentacja sieci i topologie v
- 1.4 Typowe rodzaje sieci v
- 1.5 Połączenie z Internetem v
- 1.6 Niezawodne sieci v
- 1.7 Trendy sieciowe v
- 1.8 Bezpieczeństwo sieci v
- 1.9 Profesjonalista IT v
- 1.10 Moduł ćwiczeń i quizu v
- 1.10.1 Czego się nauczyłem przerabiając ten moduł?

Wideo - Niezawodność TCP - numery sekwencyjne i potwierdzenia

Jedną z funkcji TCP jest upewnienie się, że każdy wysłany segment dotarł do odbiorcy. Usługi TCP na hoście docelowym potwierdzają dostarczenie danych, wysłanych przez aplikację źródłową.

Kliknij przycisk Odtwórz na rysunku, aby wyświetlić lekcję na temat numerów sekwencyjnych i potwierdzeń w TCP.



14.6.3

Niezawodność w TCP - utrata danych i retransmisja

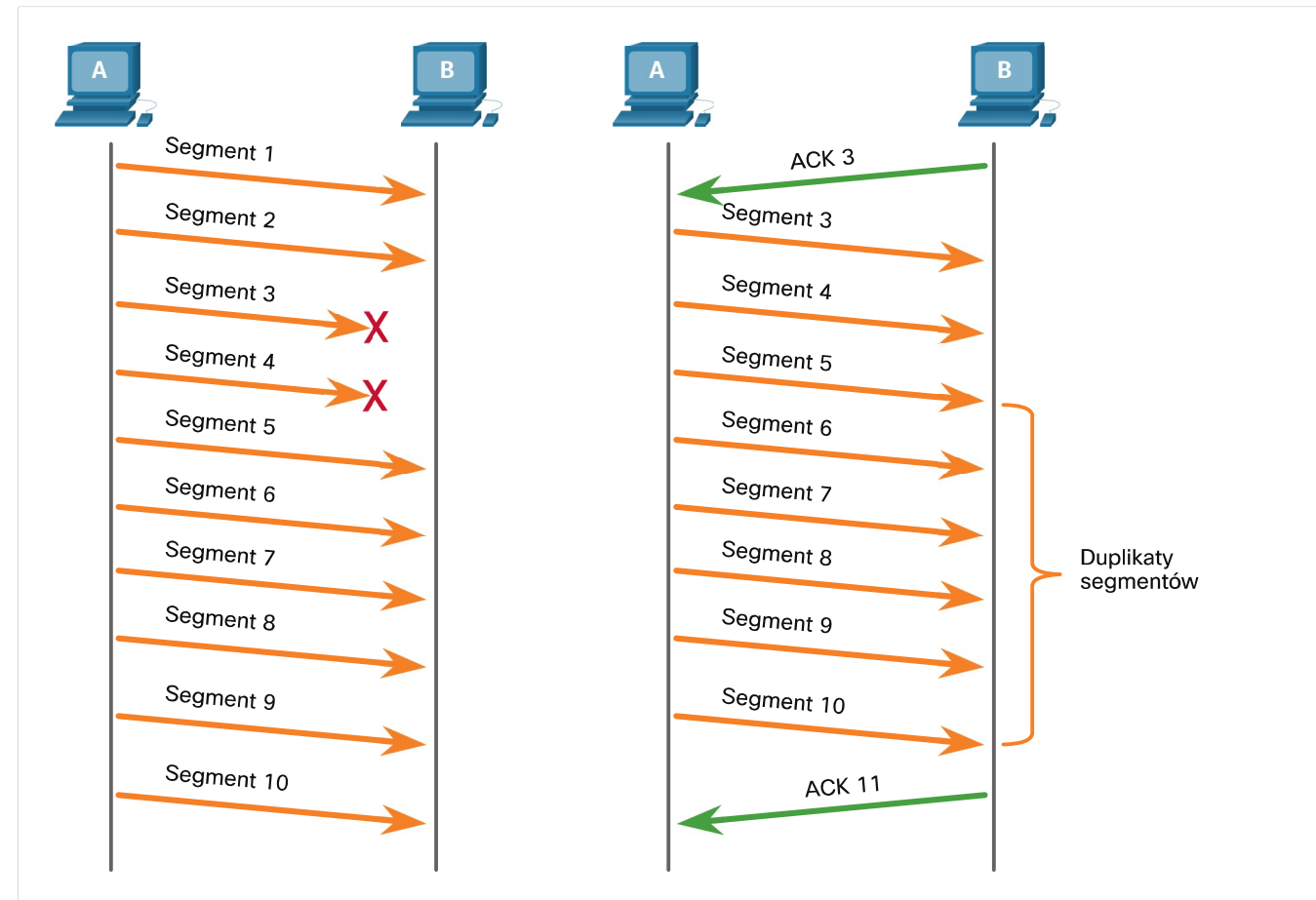


Wprowadzenie do sieci

1	Komunikacja sieciowa dziś	^
1.0	Wprowadzenie	v
1.1	Sieci wpływają na nasze życie	v
1.2	Komponenty sieciowe	v
1.3	Reprezentacja sieci i topologie	v
1.4	Typowe rodzaje sieci	v
1.5	Połączenie z Internetem	v
1.6	Niezawodne sieci	v
1.7	Trendy sieciowe	v
1.8	Bezpieczeństwo sieci	v
1.9	Profesjonalista IT	v
1.10	Moduł ćwiczeń i quizu	v
1.10.1	Czego się nauczyłem przerabiając ten moduł?	

Bez względu na to jak dobrze została zaprojektowana sieć, zawsze pojawi się sporadyczna utrata przesyłanych danych. Dlatego też TCP dostarcza metod zarządzania utraconymi segmentami. Jednym z nich jest mechanizm retransmisji segmentów niepotwierdzonych danych.

Przed późniejszymi ulepszeniami, TCP mógł potwierdzić tylko oczekiwany następny bajt. Na przykład, na rysunku, używając numerów segmentów dla uproszczenia, host A wysła segmenty od 1 do 10 do hosta B. Jeśli wszystkie segmenty dotrą z wyjątkiem segmentów 3 i 4, host B odpowiedziałby potwierdzeniem określającym, że następny oczekiwany segment to segment 3. Host A nie ma pojęcia, czy jakiegokolwiek inne segmenty dotarły, czy nie. Host A będzie zatem ponownie wysłać segmenty od 3 do 10. Jeśli wszystkie segmenty ponownie wysłane dotarły pomyślnie, segmenty od 5 do 10 będą zdublowane. Może to prowadzić do opóźnień, zatorów i nieefektywności.

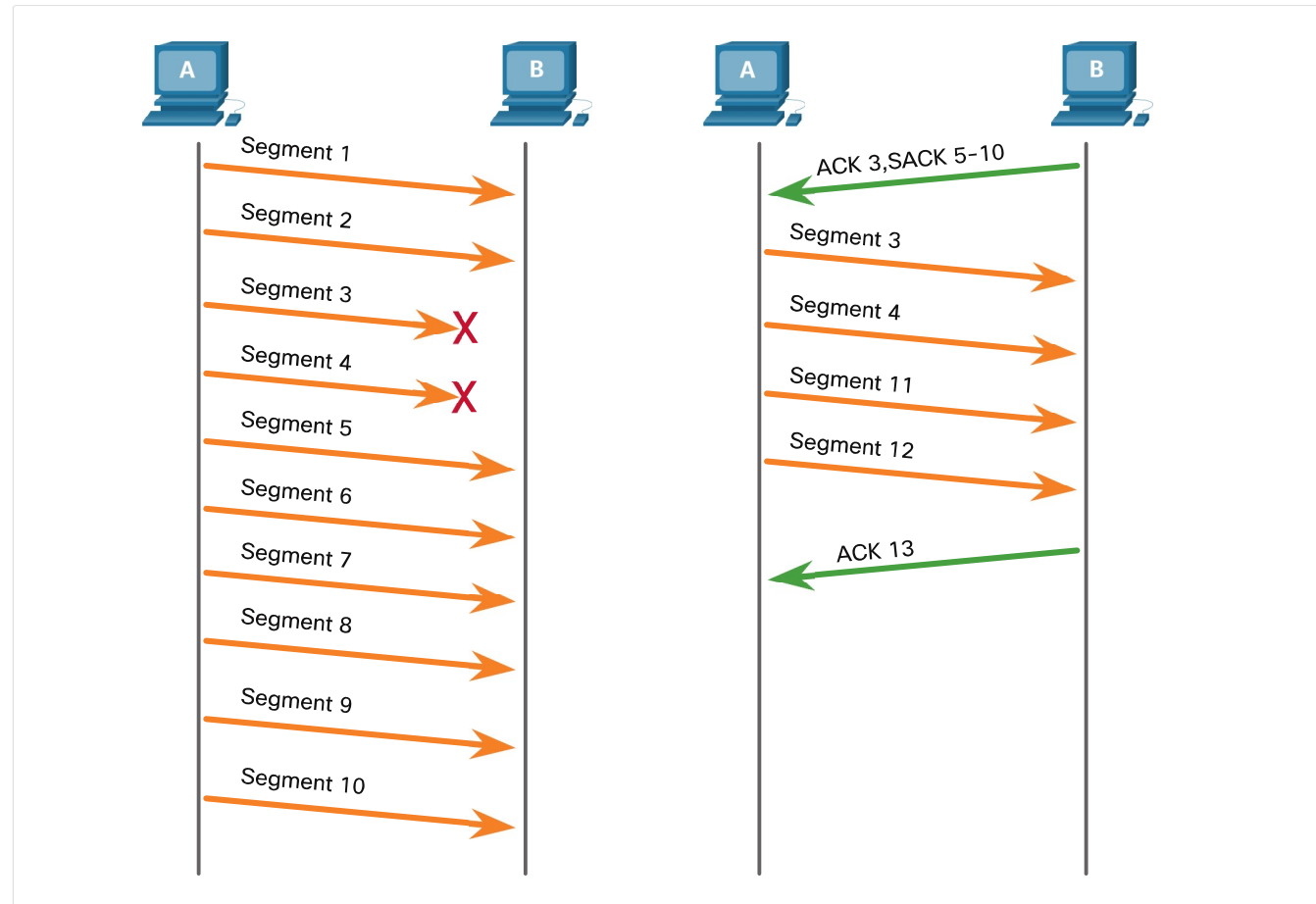


Systemy operacyjne hosta dziś zazwyczaj wykorzystują opcjonalną funkcję TCP o nazwie selektywne potwierdzenie (SACK),

Wprowadzenie do sieci

1	Komunikacja sieciowa dziś	^
1.0	Wprowadzenie	v
1.1	Sieci wpływają na nasze życie	v
1.2	Komponenty sieciowe	v
1.3	Reprezentacja sieci i topologie	v
1.4	Typowe rodzaje sieci	v
1.5	Połączenie z Internetem	v
1.6	Niezawodne sieci	v
1.7	Trendy sieciowe	v
1.8	Bezpieczeństwo sieci	v
1.9	Profesjonalista IT	v
1.10	Moduł ćwiczeń i quizu	v
1.10.1	Czego się nauczyłem przerabiając ten moduł?	

negocjowane podczas trójetapowego uzgadniania. Jeśli oba hosty obsługują SACK, odbiorca może jawnie potwierdzić, które segmenty (bajty) zostały odebrane w tym wszelkie segmenty nieciągłe. W związku z tym host wysyłający będzie musiał tylko ponownie przesłać brakujące dane. Na przykład na kolejnym rysunku, ponownie dla uproszczenia, używając numerów segmentów, host A wysła segmenty 1 do 10 do hosta B. Jeśli wszystkie segmenty dotrą z wyjątkiem segmentów 3 i 4, host B może potwierdzić, że otrzymał segmenty 1 i 2 (ACK 3) i selektywnie potwierdzić segmenty od 5 do 10 (SACK 5-10). Host A będzie musiał tylko ponownie wysłać segmenty 3 i 4.



Uwaga: TCP zazwyczaj wysła ACK dla każdego innego pakietu, ale inne czynniki wykraczające poza zakres tego tematu mogą zmienić to zachowanie.

TCP używa liczników czasu, aby wiedzieć, jak długo czekać przed ponownym wysłaniem segmentu. Na rysunku odtwórz film i kliknij link, aby pobrać plik PDF. Plik wideo i PDF dotyczy badania utraty danych TCP i retransmisji.

1.10.2 Moduł Quiz - Sieci dzisiaj

Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś ^
- 1.0 Wprowadzenie v
- 1.1 Sieci wpływają na nasze życie v
- 1.2 Komponenty sieciowe v
- 1.3 Reprezentacja sieci i topologie v
- 1.4 Typowe rodzaje sieci v
- 1.5 Połączenie z Internetem v
- 1.6 Niezawodne sieci v
- 1.7 Trendy sieciowe v
- 1.8 Bezpieczeństwo sieci v
- 1.9 Profesjonalista IT v
- 1.10 Moduł ćwiczeń i quizu v
- 1.10.1 Czego się nauczyłem przerabiając ten moduł?

14.6.4

Wideo - Niezawodność w TCP - utrata danych i retransmisja



Kliknij przycisk Odtwórz na rysunku, aby wyświetlić lekcję na temat retransmisji TCP.



14.6.5

Kontrola przepływu w TCP - rozmiar okna i



Wprowadzenie do sieci

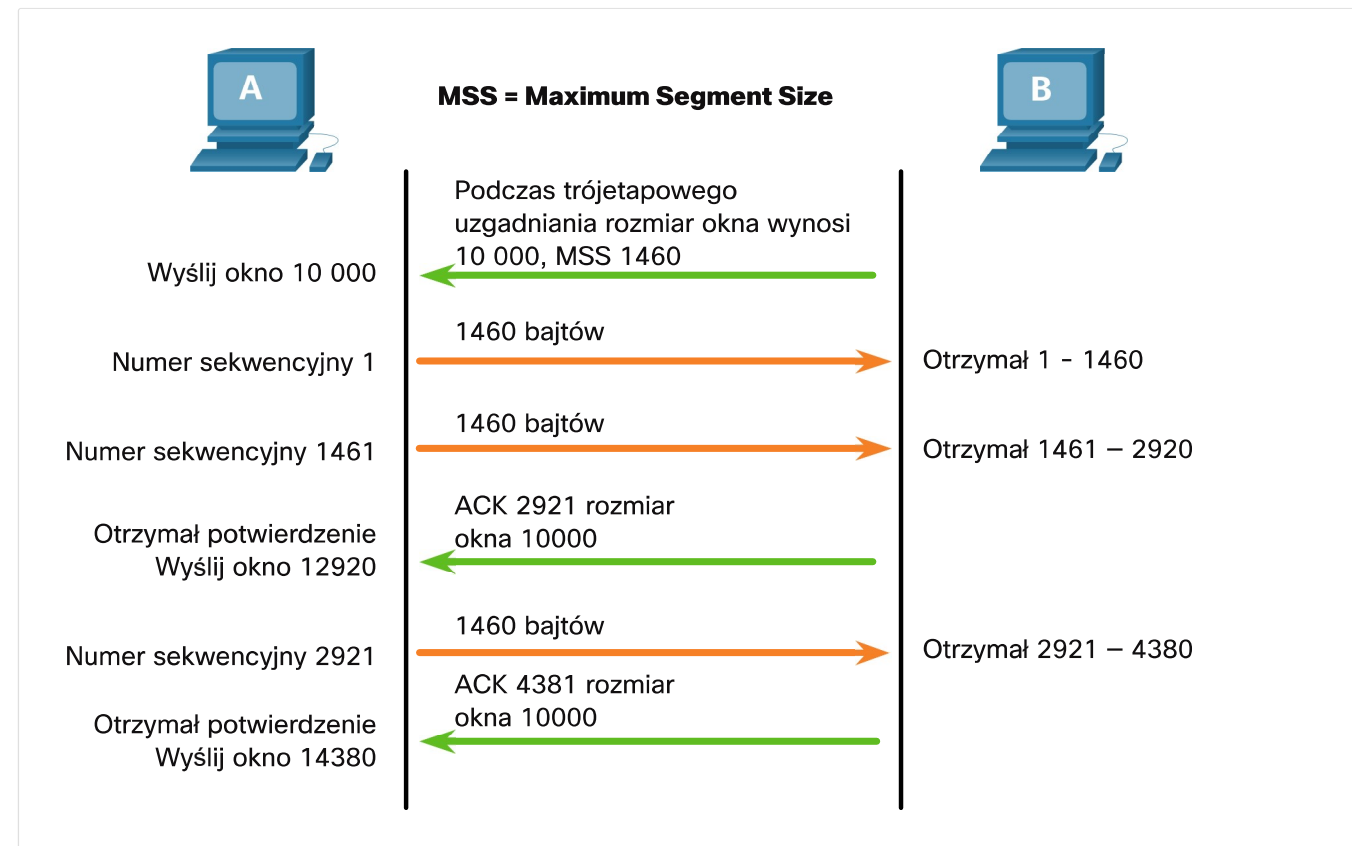
- 1 Komunikacja sieciowa dziś ^
- 1.0 Wprowadzenie v
- 1.1 Sieci wpływają na nasze życie v
- 1.2 Komponenty sieciowe v
- 1.3 Reprezentacja sieci i topologie v
- 1.4 Typowe rodzaje sieci v
- 1.5 Połączenie z Internetem v
- 1.6 Niezawodne sieci v
- 1.7 Trendy sieciowe v
- 1.8 Bezpieczeństwo sieci v
- 1.9 Profesjonalista IT v
- 1.10 Moduł ćwiczeń i quizu v
- 1.10.1 Czego się nauczyłem przerabiając ten moduł?

potwierdzenia

TCP zapewnia również mechanizmy kontroli przepływu. Kontrola przepływu to ilość danych, które odbiorca może odbierać i przetwarzać niezawodnie. Kontrola przepływu wspiera mechanizm zapewnienia niezawodności transmisji TCP, przez dostosowanie tempa przepływu danych między dwoma usługami w ustanowionej sesji. Aby to osiągnąć, nagłówek TCP zawiera 16-bitowe pole zwane rozmiarem okna.

Rysunek pokazuje przykład wielkości okna i potwierdzeń.

Przykład rozmiaru okna TCP



Rozmiar okna określa liczbę bajtów wysłanych zanim nadawca będzie oczekiwał na ich potwierdzenie. Wartość potwierdzenia jest numerem następnego spodziewanego bajtu.

Wprowadzenie do sieci

1	Komunikacja sieciowa dziś	⤴
1.0	Wprowadzenie	⤵
1.1	Sieci wpływają na nasze życie	⤵
1.2	Komponenty sieciowe	⤵
1.3	Reprezentacja sieci i topologie	⤵
1.4	Typowe rodzaje sieci	⤵
1.5	Połączenie z Internetem	⤵
1.6	Niezawodne sieci	⤵
1.7	Trendy sieciowe	⤵
1.8	Bezpieczeństwo sieci	⤵
1.9	Profesjonalista IT	⤵
1.10	Moduł ćwiczeń i quizu	⤵
1.10.1	Czego się nauczyłem przerabiając ten moduł?	

Rozmiar okna to liczba bajtów, którą urządzenie docelowe sesji TCP może zaakceptować i przetworzyć jednocześnie. W tym przykładzie początkowy rozmiar okna PC B dla sesji TCP wynosi 10000 bajtów. Począwszy od pierwszego bajtu, bajtu numer 1, ostatni bajt, który komputer A może wysłać bez potwierdzenia, ma wartość 10000. Nazywa się to oknem wysyłania komputera A. Rozmiar okna jest zawarty w każdym segmencie TCP, więc odbiorca może w dowolnym momencie zmodyfikować rozmiar okna w zależności od dostępności bufora.

Początkowy rozmiar okna jest uzgodniony, gdy sesja TCP jest ustalana podczas trójetapowego uzgadniania. Urządzenie źródłowe musi ograniczyć liczbę bajtów wysłanych do urządzenia docelowego na podstawie rozmiaru okna odbiorcy. Dopiero gdy urządzenie źródłowe otrzyma potwierdzenie, że bajty zostały odebrane, może kontynuować wysyłanie kolejnych danych dla sesji. Zazwyczaj miejsce docelowe nie czeka na odbiór wszystkich bajtów dla rozmiaru okna przed odpowiedzią z potwierdzeniem. Gdy bajty są odbierane i przetwarzane, odbiorca wyśle potwierdzenie informujące źródło, że może nadal wysłać dodatkowe bajty.

Na przykład typowe jest to, że komputer B nie czeka aż do odebrania wszystkich 10 000 bajtów przed wysłaniem potwierdzenia. Oznacza to, że PC A może dostosować swoje okno wysyłania, ponieważ odbiera potwierdzenia z PC B. Jak pokazano na rysunku, gdy PC A otrzymuje potwierdzenie z numerem potwierdzenia 2921, który jest następnym oczekiwanym bajtem. Okno wysyłania PC zwiększy się o 2920 bajtów. To zmienia okno wysyłania z 10 000 bajtów na 12 920. Komputer A może teraz wysłać do kolejnych 10 000 bajtów na komputer B, o ile nie wysła więcej niż nowe okno wysyłania o wartości 12 920.

Miejsce docelowe wysyłające potwierdzenia podczas przetwarzania odebranych bajtów oraz ciągle dostosowywanie źródłowego okna wysyłania nazywane jest oknem przesuwным. W poprzednim przykładzie okno wysyłania PC A zwiększa lub przesuwa się na kolejne 2921 bajtów z 10 000 do 12 920.

Jeśli dostępność miejsca buforowego odbiorcy maleje, może to zmniejszyć rozmiar okna, aby poinformować źródło, aby zmniejszyć liczbę bajtów, które powinien wysłać bez otrzymania potwierdzenia.

Uwaga: Urządzenia dziś korzystają z protokołu okien przesuwnych. Odbiorca zazwyczaj wysyła potwierdzenie po co dwa odbierane segmenty. Liczba segmentów otrzymanych przed potwierdzeniem może się różnić. Zaletą okien przesuwnych jest to, że pozwala nadawcy w sposób ciągły przysyłać segmenty, tak długo, jak odbiornik potwierdza poprzednie segmenty. Szczegóły okien przesuwnych są poza zakresem tego kursu.

14.6.6

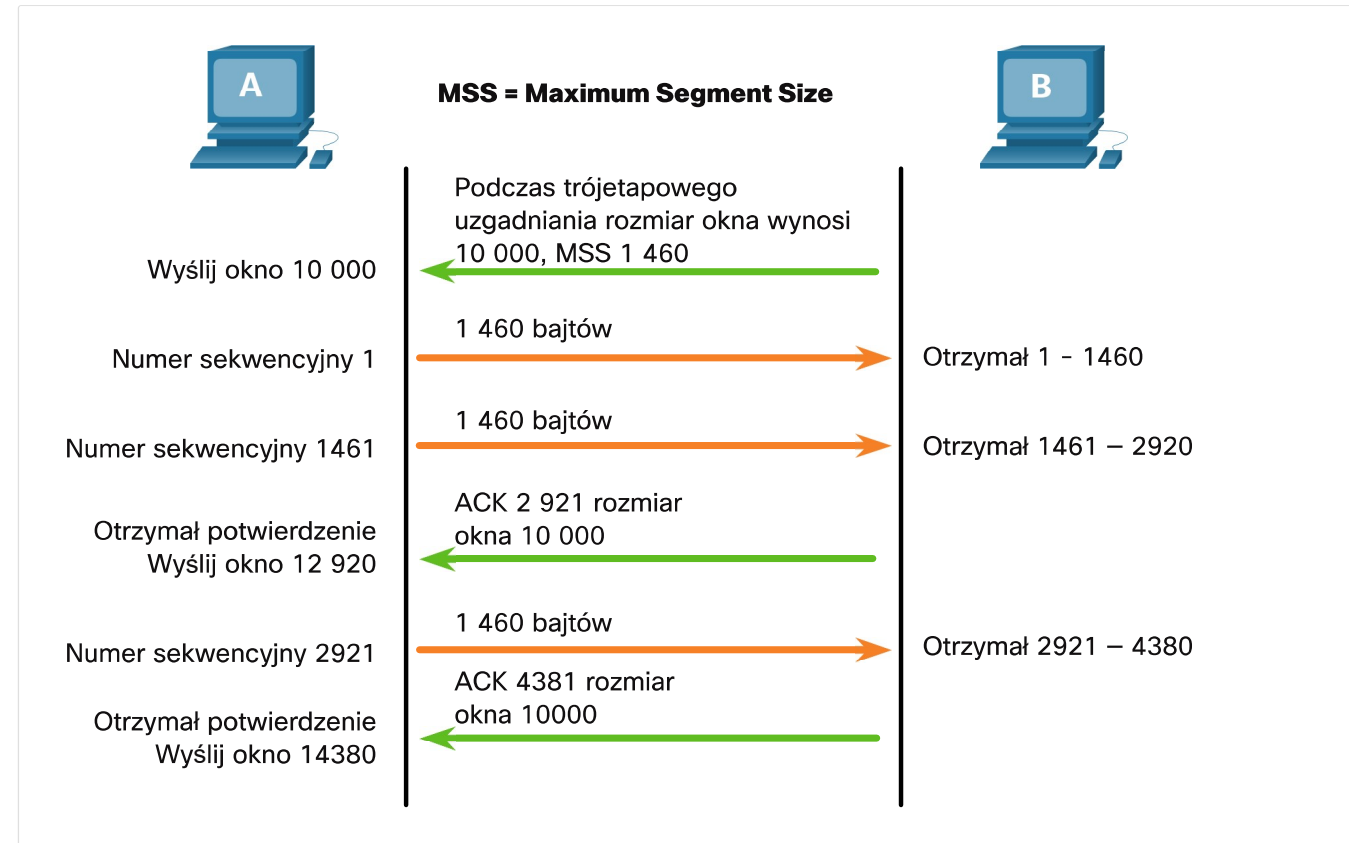
Kontrola przepływu TCP - maksymalny rozmiar segmentu (MSS)



Wprowadzenie do sieci

1	Komunikacja sieciowa dziś	^
1.0	Wprowadzenie	v
1.1	Sieci wpływają na nasze życie	v
1.2	Komponenty sieciowe	v
1.3	Reprezentacja sieci i topologie	v
1.4	Typowe rodzaje sieci	v
1.5	Połączenie z Internetem	v
1.6	Niezawodne sieci	v
1.7	Trendy sieciowe	v
1.8	Bezpieczeństwo sieci	v
1.9	Profesjonalista IT	v
1.10	Moduł ćwiczeń i quizu	v
1.10.1	Czego się nauczyłem przerabiając ten moduł?	

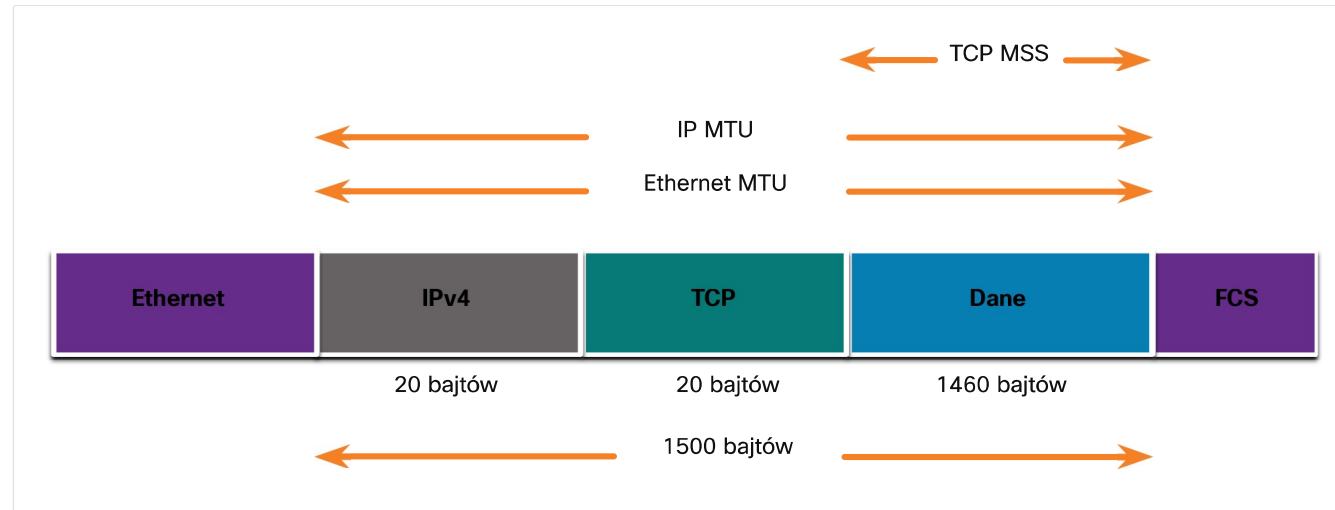
Na rysunku, źródło przesyła 1460 bajtów danych w każdym segmencie TCP. Zazwyczaj jest to maksymalny rozmiar segmentu (MSS), który może odbierać urządzenie docelowe. MSS jest częścią pola opcji w nagłówku TCP, który określa największą ilość danych w bajtach, jaką urządzenie może odbierać w jednym segmencie TCP. Rozmiar MSS nie zawiera nagłówka TCP. MSS jest zazwyczaj zawarte podczas trójetapowego uzgadniania.



Typowym MSS jest 1 460 bajtów podczas korzystania z protokołu IPv4. Host określa wartość pola MSS, odejmując nagłówki IP i TCP od maksymalnej jednostki transmisji Ethernet (MTU). Dla interfeju Ethernet domyślnym MTU jest 1500 bajtów. Odejmując nagłówek IPv4 20 bajtów i nagłówek TCP 20 bajtów, domyślny rozmiar MSS będzie wynosić 1460 bajtów, jak pokazano na rysunku.

Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś ^
- 1.0 Wprowadzenie v
- 1.1 Sieci wpływają na nasze życie v
- 1.2 Komponenty sieciowe v
- 1.3 Reprezentacja sieci i topologie v
- 1.4 Typowe rodzaje sieci v
- 1.5 Połączenie z Internetem v
- 1.6 Niezawodne sieci v
- 1.7 Trendy sieciowe v
- 1.8 Bezpieczeństwo sieci v
- 1.9 Profesjonalista IT v
- 1.10 Moduł ćwiczeń i quizu v
- 1.10.1 Czego się nauczyłem przerabiając ten moduł?



14.6.7

Kontrola przepływu w TCP - unikanie przeciążeń sieci



Gdy w sieci występuje przeciążenie, pakiety są odrzucane przez przeciążony router. Gdy pakiety zawierające segmenty TCP nie docierają do miejsca docelowego, pozostają niepotwierdzone. Określając szybkość, z jaką segmenty TCP są wysyłane, ale nie potwierdzone, źródło może przyjąć pewien poziom przeciążenia sieci.

Ileokroć występuje przekroczenie, nastąpi retransmisja utraconych segmentów TCP ze źródła. Jeśli retransmisja nie jest odpowiednio kontrolowana, dodatkowa retransmisja segmentów TCP może jeszcze pogorszyć zatory. Nie tylko nowe pakiety z segmentami TCP wprowadzane są do sieci, ale efekt sprzężenia zwrotnego utraconych segmentów TCP również zwiększy zator. Aby uniknąć i kontrolować przeciążenia, TCP wykorzystuje kilka mechanizmów obsługi zatorów, liczników czasu i algorytmów.

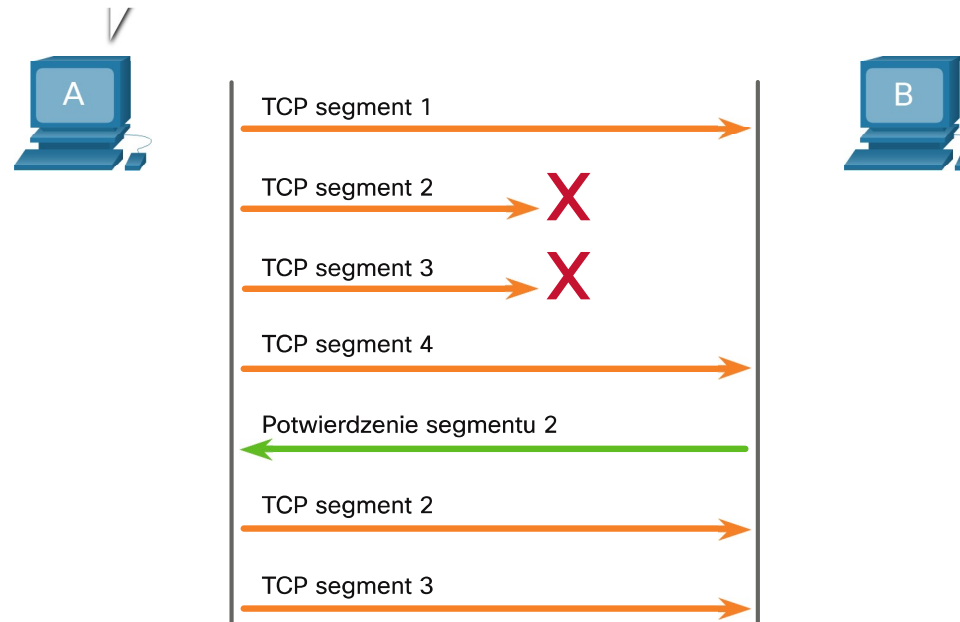
Jeśli źródło stwierdzi, że segmenty TCP nie są potwierdzone lub nie potwierdzone w odpowiednim czasie, to może zmniejszyć liczbę bajtów, które wysyła przed otrzymaniem potwierdzenia. Jak pokazano na rysunku, PC A wyczuwa, że jest zator, a zatem zmniejsza liczbę bajtów, które wysyła przed otrzymaniem potwierdzenia z PC B.

Sterowanie przeciążeniem w TCP

Wprowadzenie do sieci

1	Komunikacja sieciowa dziś	^
1.0	Wprowadzenie	v
1.1	Sieci wpływają na nasze życie	v
1.2	Komponenty sieciowe	v
1.3	Reprezentacja sieci i topologie	v
1.4	Typowe rodzaje sieci	v
1.5	Połączenie z Internetem	v
1.6	Niezawodne sieci	v
1.7	Trendy sieciowe	v
1.8	Bezpieczeństwo sieci	v
1.9	Profesjonalista IT	v
1.10	Moduł ćwiczeń i quizu	v
1.10.1	Czego się nauczyłem przerabiając ten moduł?	

Nie otrzymuję potwierdzeń, których oczekuję od PC B, więc zmniejszę liczbę bajtów, które wysłę przed otrzymaniem potwierdzenia.



Numery potwierdzenia dotyczą następnego oczekiwanego bajtu, a nie segmentu. Stosowane numery segmentów są uproszczone do celów ilustracyjnych.

Zauważ, że to źródło zmniejsza liczbę niepotwierdzonych bajtów, które wysyła, a nie rozmiar okna określony przez miejsce docelowe.

Uwaga: Wyjaśnienia rzeczywistych mechanizmów obsługi przeciążeń, liczników i algorytmów wykraczają poza zakres tego kursu.

14.6.8

Sprawdź, czy zrozumiałeś - Niezawodność i kontrola



Wprowadzenie do sieci

1	Komunikacja sieciowa dziś	^
1.0	Wprowadzenie	v
1.1	Sieci wpływają na nasze życie	v
1.2	Komponenty sieciowe	v
1.3	Reprezentacja sieci i topologie	v
1.4	Typowe rodzaje sieci	v
1.5	Połączenie z Internetem	v
1.6	Niezawodne sieci	v
1.7	Trendy sieciowe	v
1.8	Bezpieczeństwo sieci	v
1.9	Profesjonalista IT	v
1.10	Moduł ćwiczeń i quizu	v
1.10.1	Czego się nauczyłem przerabiając ten moduł?	

przepływu



Sprawdź swoją wiedzę na temat niezawodności i procesu kontroli przepływu TCP, wybierając NAJLEPSZĄ odpowiedź na poniższe pytania.

1. Jakie pole jest używane przez hosta docelowego do ponownego złożenia segmentów w oryginalnej kolejności?

- ☐ Bity kontrolne
- ☐ Port docelowy
- ☐ Numer sekwencyjny
- ☐ Port źródłowy
- ☐ Rozmiar okna

2. Jakie pole służy do zapewnienia kontroli przepływu?

- ☐ Bity kontrolne
- ☐ Port docelowy
- ☐ Numer sekwencyjny
- ☐ Port źródłowy
- ☐ Rozmiar okna

3. Co się stanie, gdy host wysyłający stwierdzi zatory?

- ☐ Host odbierający zwiększa liczbę bajtów, które wysyła przed otrzymaniem potwierdzenia z hosta wysyłającego.
- ☐ Host odbierający zmniejsza liczbę bajtów, które wysyła przed otrzymaniem potwierdzenia z hosta wysyłającego.
- ☐ Host wysyłający zwiększa liczbę bajtów, które wysyła przed otrzymaniem potwierdzenia z hosta docelowego.
- ☐ Host wysyłający zmniejsza liczbę bajtów, które wysyła przed otrzymaniem potwierdzenia z hosta docelowego.

[Sprawdź](#)[Rozwiązanie](#)

Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś ^
- 1.0 Wprowadzenie v
- 1.1 Sieci wpływają na nasze życie v
- 1.2 Komponenty sieciowe v
- 1.3 Reprezentacja sieci i topologie v
- 1.4 Typowe rodzaje sieci v
- 1.5 Połączenie z Internetem v
- 1.6 Niezawodne sieci v
- 1.7 Trendy sieciowe v
- 1.8 Bezpieczeństwo sieci v
- 1.9 Profesjonalista IT v
- 1.10 Moduł ćwiczeń i quizu v
- 1.10.1 Czego się nauczyłem przerabiając ten moduł?

Resetuj

< ^{14.5}
Proces komunikacji TCP

^{14.7}
Komunikacja z użyciem UDP >