Moduł 11.Warstwa transportowa i aplikacji

Zadaniem warstwy transportowej TCP/IP jest, jak sugeruje jej nazwa, transport danych pomiędzy aplikacjami urządzenia źródłowego i docelowego. Dokładne poznanie działania warstwy transportowej jest niezbędne do zrozumienia zagadnień związanych z nowoczesnymi sieciami przesyłania danych. W module tym zostaną opisane funkcje i usługi tej krytycznej warstwy modelu sieciowego TCP/IP.

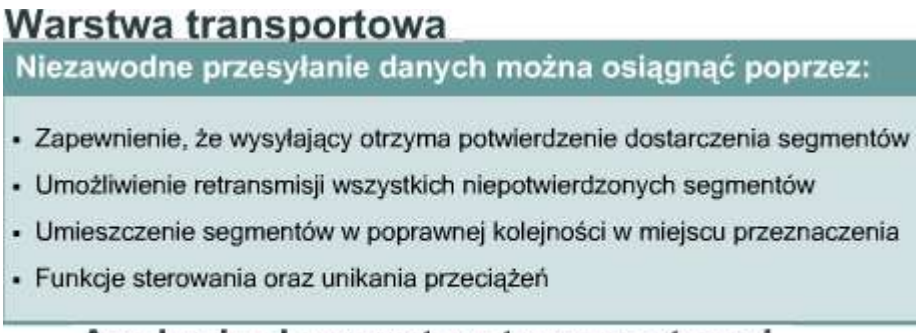
Wiele aplikacji sieciowych znajdujących się w warstwie aplikacji modelu TCP/IP jest dobrze znanych nawet sporadycznym użytkownikom sieci. Na przykład terminy HTTP, FTP i SMTP są akronimami często spotykanymi przez użytkowników przeglądarek WWW i klientów poczty elektronicznej. W module tym zostały również opisane funkcje tych oraz innych aplikacji modelu sieciowego TCP/IP.

11.1 Warstwa transportowa TCP/IP

11.1.1 Wprowadzenie do warstwy transportowej

Do podstawowych zadań warstwy transportowej, warstwy 4 modelu OSI, należą transportowanie informacji i sterowanie ich przepływem ze źródła do celu w sposób niezawodny i dokładny.

Kontrola typu end-to-end oraz niezawodność są zapewniane przez okna przesuwne, numery kolejne i potwierdzenia.



Aby zrozumieć niezawodność i kontrolę przepływu, można wyobrazić sobie kogoś, kto po rocznej nauce języka obcego odwiedza kraj, w którym ten język jest używany. Podczas rozmowy słowa muszą być wypowiadane powoli i dla pewności powtarzane, by nie zgubić sensu rozmowy. Tym właśnie jest kontrola przepływu.

Warstwa transportowa zapewnia usługi przesyłania danych z hosta źródłowego do hosta docelowego. Umożliwia ona nawiązanie połączenia logicznego pomiędzy punktami końcowymi sieci. Protokoły warstwy transportowej dzielą na segmenty i ponownie składają dane wysyłane przez aplikacje wyższej warstwy, przesyłając je w tym samym strumieniu danych warstwy transportowej. Strumień danych warstwy transportowej obsługuje transport typu end-to-end, czyli transport między punktami końcowymi.

Strumień ten jest logicznym połączeniem pomiędzy punktami końcowymi sieci. Do jego podstawowych zadań należy transportowanie informacji i sterowanie ich przepływem ze źródła do celu w sposób niezawodny i dokładny. Podstawowym zadaniem warstwy 4 jest zapewnienie kontroli typu end-to-end z wykorzystaniem metody okien przesuwnych oraz zapewnienie niezawodności za pomocą mechanizmów numerów kolejnych i potwierdzeń. Warstwa transportowa określa połączenia typu end-to-end pomiędzy aplikacjami na hostach.

Usługi transportowe obejmują następujące usługi podstawowe:

- segmentacja danych aplikacji wyższej warstwy,
- ustanawianie operacji typu end-to-end,
- transport segmentów między dwoma hostami końcowymi,
- kontrola przepływu zapewniana przez okna przesuwne,
- niezawodność zapewniana przez numery sekwencyjne i potwierdzenia.

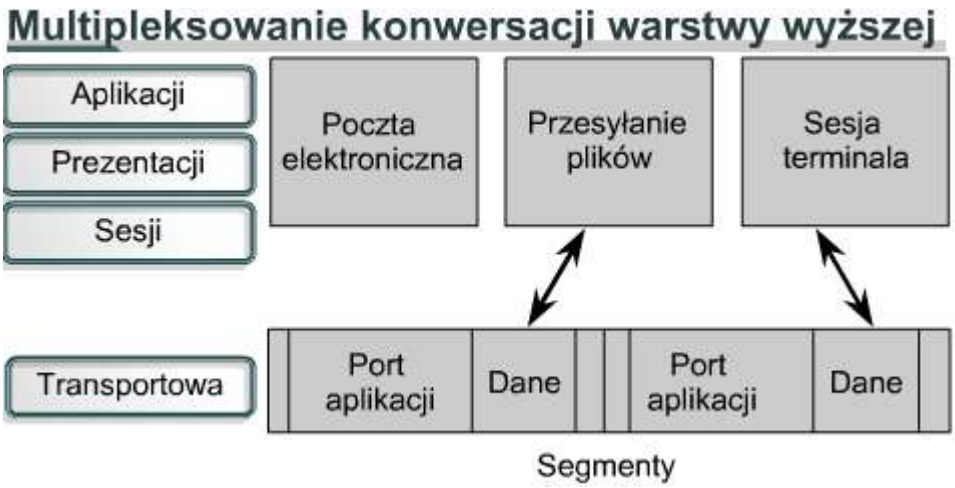
TCP/IP jest kombinacją dwóch oddzielnych protokołów. Protokół IP działa w warstwie 3 i jest protokołem bezpołączeniowym odpowiadającym za dostarczanie danych poprzez sieć z dołożeniem wszelkich starań. Protokół TCP działa w warstwie 4 i jest usługą zorientowaną połączeniowo odpowiedzialną za kontrolę przepływu i niezawodność. Połączenie tych protokołów w parę zapewnia szerszy zakres usług. Razem stanowią one podstawę dla całego zestawu protokołów, zwanego zestawem protokołów TCP/IP. Na jego podstawie powstał Internet.

11.1.2 Kontrola przepływu

Podczas przesyłania segmentów danych przez warstwę transportową podejmowane są starania, aby nie dopuścić do utraty danych. Przyczyną utraty danych może być sytuacja, w której host odbierający nie jest w stanie

przetwarzać danych z taką szybkością, z jaką one do niego docierają. Host odbierający jest wtedy zmuszony do ich odrzucenia. Kontrola przepływu zapobiega problemowi przepełnienia buforów hosta odbierającego. Protokół TCP zawiera mechanizm kontroli przepływu polegający na umożliwieniu komunikacji pomiędzy hostem wysyłającym i odbierającym. W ten sposób oba hosty ustalają prędkość transferu danych na wartość odpowiadającą każdemu z nich.

11.1.3 Przegląd operacji ustanawiania, obsługi i zakończenia sesji



W modelu odniesienia OSI wiele aplikacji może współdzielić to samo połączenie transportowe. Funkcje transportu danych są realizowane na zasadzie wysyłania segmentu za segmentem. Innymi słowy, różne aplikacje mogą wysyłać segmenty danych w oparciu o zasadę „pierwszy przychodzi, pierwszy obsłużony". Pierwszy odebrany segment będzie obsłużony jako pierwszy. Segmenty te mogą podlegać routingowi do tego samego lub różnych adresatów. Jest to nazywane zwielokrotnianiem (multipleksowaniem) konwersacji warstwy wyższej. Wiele równoczesnych konwersacji jednostek warstwy wyższej może być multipleksowanych na pojedynczym połączeniu.

Jedną z funkcji warstwy transportowej jest ustanowienie sesji zorientowanej połączeniowo pomiędzy podobnymi urządzeniami pracującymi w warstwie aplikacji. Aby rozpocząć transfer danych, obie aplikacje, zarówno wysyłająca jak i odbierająca, przekazują informację do swoich systemów operacyjnych, że zostanie zainicjowane połączenie. Połączenie zainicjowane przez jeden węzeł musi zostać zaakceptowane przez drugi węzeł. Moduły oprogramowania protokołu w dwóch systemach operacyjnych komunikują się ze sobą za pośrednictwem wysyłanych przez sieć wiadomości w celu zweryfikowania, czy transfer jest autoryzowany i czy obie strony są gotowe.

Zostaje ustanowione połączenie, a po zakończeniu wszystkich czynności synchronizacyjnych rozpoczyna się transfer danych. W czasie przesyłania oba urządzenia nadal się komunikują za pomocą oprogramowania protokołu w celu weryfikacji poprawności odbieranych danych.

Na rysunku zaprezentowane zostało typowe połączenie pomiędzy systemem wysyłającym i odbierającym. Pierwsze uzgodnienie jest żądaniem synchronizacji. Drugie i trzecie uzgodnienie potwierdzają początkowe żądanie synchronizacji, równocześnie synchronizując parametry połączenia w przeciwnym kierunku. Końcowy segment uzgodnienia jest potwierdzeniem służącym do poinformowania adresata, że obie strony są zgodne, iż zostało ustanowione połączenie. Po ustanowieniu połączenia rozpoczyna się transfer danych.

Przeciążenie podczas transferu danych może wystąpić z dwóch powodów:

- Po pierwsze, szybki komputer może być w stanie generować ruch szybciej, niż sieć może go przekazywać.
- Po drugie, jeśli wiele komputerów równocześnie wysyła datagramy do tego samego adresata, może on zostać przeciążony, mimo że problemu nie spowodował żaden pojedynczy komputer.

Gdy datagramy są odbierane przez bramę lub hosta szybciej niż mogą zostać przetworzone, są one tymczasowo przechowywane w pamięci. Jeśli ruch trwa dalej, w końcu zostaje wyczerpana pamięć hosta lub bramy, co powoduje odrzucanie kolejnych datagramów.

Zamiast dopuszczenia do utraty danych, proces TCP na odbierającym hoście może wysłać do nadawcy powiadomienie „nie gotowy". Wskaźnik ten, działający jak znak stopu, sygnalizuje wysyłającemu, żeby przerwał wysyłanie danych. Gdy odbierający może obsłużyć dalsze dane, wysyła wskaźnik transportowy „gotowy". Po odebraniu tego wskaźnika wysyłający może wznowić transmisję segmentów.

Na końcu transferu danych host nadający wysyła sygnał wskazujący koniec transmisji. Na końcu sekwencji danych host odbierający potwierdza koniec transmisji i połączenie jest zamykane.

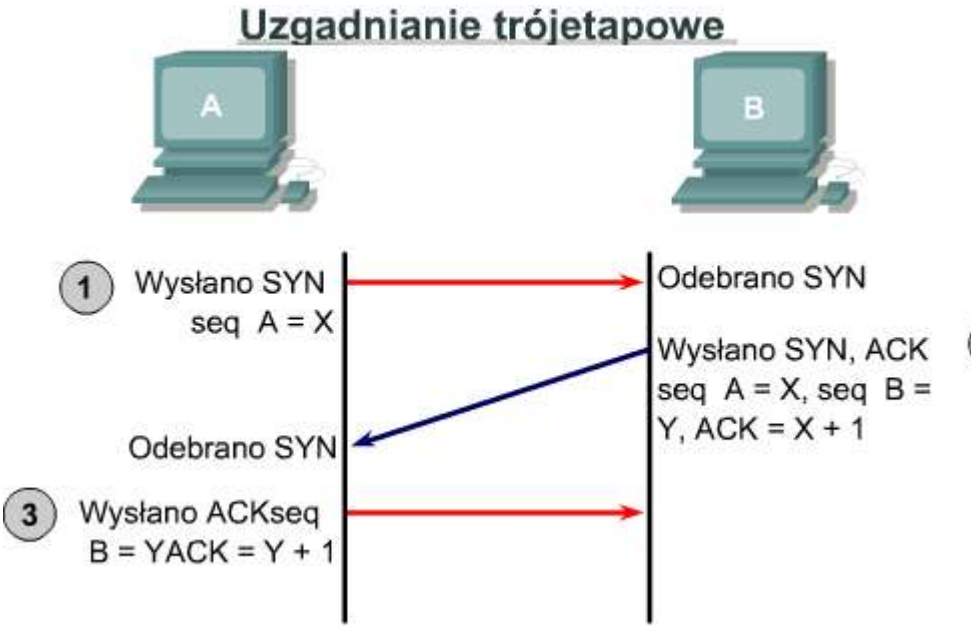
11.1.4 Uzgadnianie trójetapowe

Protokół TCP jest protokołem zorientowanym połączeniowo. Wymaga on ustanowienia połączenia przed rozpoczęciem przesyłania danych. Aby ustanowić lub zainicjować połączenie, muszą zostać zsynchronizowane początkowe numery sekwencyjne (ISN) obu hostów. Synchronizacja polega na wymianie ustanawiających połączenie segmentów zawierających bit kontrolny zwany SYN (synchronizacja) oraz numery ISN. Segmenty zawierające bit SYN są również nazywane segmentami „SYN". Rozwiązanie to wymaga odpowiedniego

mechanizmu wybierania początkowego numeru sekwencyjnego oraz procesu uzgadniania służącego do wymiany numerów ISN.
Synchronizacja wymusza wysłanie przez każdą ze stron własnego początkowego numeru sekwencyjnego i odbiór potwierdzenia wymiany (ACK) od strony przeciwnej. **Każda strona musi również odebrać od drugiej strony numer ISN i wysłać potwierdzenie ACK. Kolejność jest następująca:**

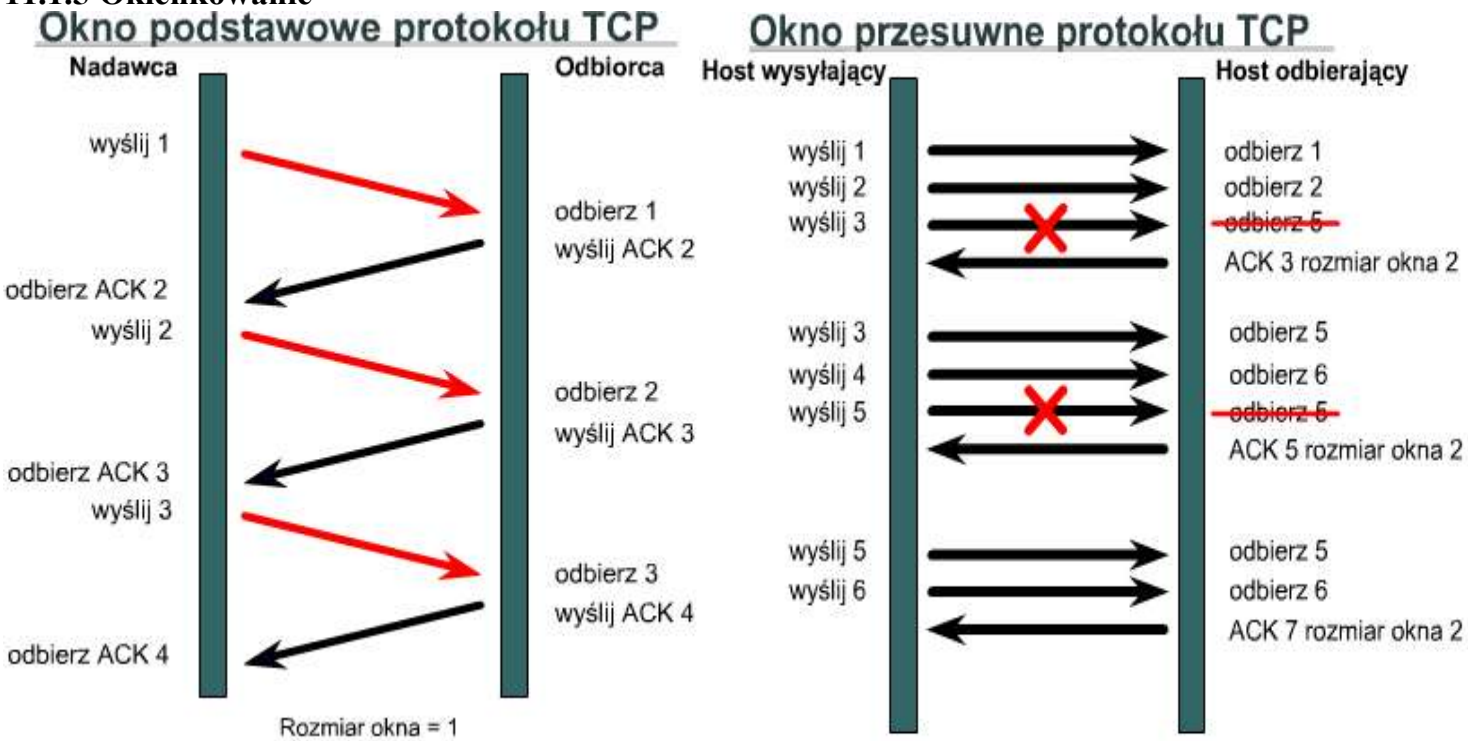
1. Wysyłający host (A) inicjuje połączenie przez wysłanie pakietu SYN do odbiorcy (hosta B) ze swoim numerem początkowym ISN = X: **A —> B SYN, seq A = X**
2. B otrzymuje pakiet, zapamiętuje, że numer sekwencyjny seq hosta A = X, odpowiada pakietem z ustawionym bitem ACK i numerem potwierdzenia X + 1, a także określa swój numer początkowy ISN = Y. Potwierdzenie ACK z numerem X + 1 oznacza, że host B otrzymał wszystkie oktety do oktetu X włącznie i będzie oczekiwał na oktet o numerze X + 1:
   B —> A ACK, seq A = X, SYN seq B = Y, ACK = X + 1
3. A otrzymuje pakiet od B, wie, że numer sekwencyjny seq hosta B = Y, i odpowiada pakietem z ustawionym bitem ACK i numerem potwierdzenia Y + 1, co kończy proces ustanawiania połączenia:
   A —> B ACK, seq B = Y, ACK = Y + 1

Wymiana ta jest zwana uzgadnianiem trójetapowym.



2 Uzgadnianie trójetapowe jest konieczne ze względu na to, że numery sekwencyjne nie są związane z globalnym zegarem w sieci i protokoły TCP mogą mieć różne mechanizmy wybierania numeru ISN. Odbiorca pierwszego segmentu SYN nie ma innego sposobu na rozpoznanie starego lub spóźnionego segmentu niż pamiętanie ostatniego numeru podczas kolejnego połączenia. Pamiętanie tego numeru nie zawsze jest możliwe. Dlatego odbiorca musi zwrócić się do wysyłającego o weryfikację segmentu SYN.

11.1.5 Okienkowanie

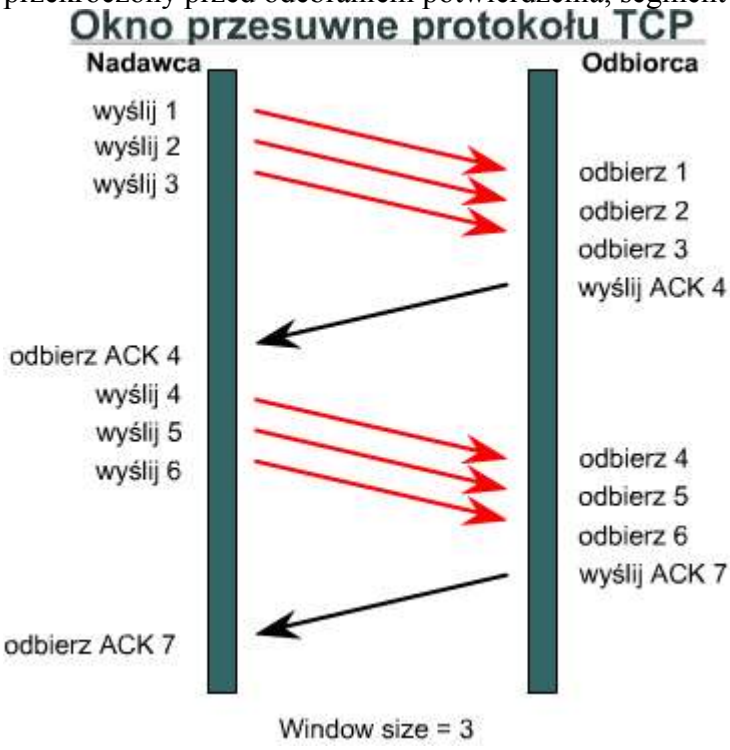


Aby zapewnić niezawodność zorientowanego połączeniowo transferu danych, pakiety danych muszą być dostarczane do odbiorcy w tej samej kolejności, w której zostały wysłane. Przesyłanie danych za pomocą danego protokołu nie powiedzie się, jeśli jakieś pakiety danych zostaną utracone, uszkodzone, powielone lub odebrane w

innej kolejności. Łatwym rozwiązaniem jest potwierdzanie przez odbiorcę odbioru każdego pakietu przed wysłaniem kolejnego.
Gdyby nadawca musiał czekać na potwierdzenie po wysłaniu każdego pakietu, przepustowość byłaby niska. Z tego powodu w przypadku większości niezawodnych protokołów zorientowanych połączeniowo dozwolone jest pozostawanie więcej niż jednego pakietu bez potwierdzenia w danym czasie. Czas pozostały po zakończeniu transmisji pakietu danych przez nadawcę i przed zakończeniem przetwarzania otrzymanego przez niego potwierdzenia jest wykorzystywany do przesłania większej ilości danych. Liczba pakietów danych, które nadawca może wysłać przed otrzymaniem potwierdzenia, jest określana jako rozmiar okna lub okno.
Protokół TCP wykorzystuje potwierdzenia typu expectational. Potwierdzenia typu expectational oznaczają, że numer potwierdzenia odnosi się do pakietu, który jest oczekiwany jako następny. Obrazowym pojęciem opisującym dynamiczną negocjację rozmiaru okna podczas sesji TCP jest okienkowanie. Okienkowanie to mechanizm kontroli przepływu. Wymaga ono, żeby urządzenie źródłowe otrzymywało od adresata potwierdzenie po wysłaniu określonej ilości danych. Odbierający proces TCP zgłasza „okno" do wysyłającego procesu TCP. Okno to określa liczbę pakietów, poczynając od numeru potwierdzenia, do których odebrania jest obecnie gotów odbierający proces TCP.
Przy rozmiarze okna równym 3 urządzenie źródłowe może wysłać do adresata trzy bajty. Urządzenie źródłowe musi następnie czekać na potwierdzenie. Gdy adresat otrzyma trzy bajty, wysyła potwierdzenie do urządzenia źródłowego, które teraz może wysłać kolejne trzy bajty. Jeśli adresat z powodu przepełnienia buforów nie otrzyma tych trzech bajtów, to nie wyśle potwierdzenia. Ponieważ źródło nie otrzyma potwierdzenia, będzie to oznaczało, że bajty powinny być wysłane ponownie, a szybkość transmisji powinna zostać zmniejszona.
Jak pokazano na rysunku , nadawca wysyła trzy pakiety przed rozpoczęciem oczekiwania na potwierdzenie ACK. Jeśli odbiorca może obsłużyć okno o rozmiarze tylko dwóch pakietów, z okna odrzucony zostaje pakiet trzeci, określa się go jako następny, a nowa wartość rozmiaru okna jest określana jako dwa. Nadawca wysyła kolejne dwa pakiety, lecz ma ciągle ustawiony rozmiar okna równy trzy. Oznacza to, że nadawca będzie nadal oczekiwał potwierdzenia od odbiorcy po wysłaniu trzech pakietów. Odbiorca odpowiada, żądając piątego pakietu i nadal określając rozmiar okna równy dwa.

11.1.6 Potwierdzenia

Niezawodne dostarczanie gwarantuje, że strumień danych wysłany z jednego urządzenia jest dostarczony przez łącze danych do innego urządzenia bez powielenia lub utraty danych. Potwierdzenie pozytywne wraz z retransmisją jest techniką, która gwarantuje niezawodne dostarczanie danych. Potwierdzenie pozytywne wymaga, by odbiorca po odebraniu danych skontaktował się ze źródłem i wysłał wiadomość potwierdzającą. Nadawca zachowuje zapis dotyczący każdego wysłanego pakietu danych (segmentu TCP) i oczekuje na potwierdzenie. W momencie wysłania segmentu zostaje również przez nadawcę uruchomiony zegar. Jeśli założony czas zostanie przekroczony przed odebraniem potwierdzenia, segment będzie ponownie wysłany.



Na rysunku został zaprezentowany nadawca wysyłający pakiety danych 1, 2 i 3. Odbiorca potwierdza odbiór pakietów przez żądanie pakietu 4. Po odbiorze potwierdzenia nadawca wysyła pakiety 4, 5 i 6. Jeśli pakiet 5 nie dotrze do celu, odbiorca wysyła potwierdzenie z żądaniem ponownego wysłania pakietu 5. Nadawca wysyła ponownie pakiet 5, po czym odbiera potwierdzenie z żądaniem kontynuacji transmisji począwszy od pakietu 7.
Protokół TCP zapewnia kolejność segmentów poprzez potwierdzenia odnoszące się do następnego w kolejności segmentu. Przed wysłaniem każdy segment jest numerowany. Po stronie stacji odbierającej protokół TCP ponownie składa segmenty w całą wiadomość. Jeśli numer sekwencyjny w szeregu został opuszczony, segment ten jest transmitowany ponownie. Segmenty, które nie zostały potwierdzone w zadanym czasie, zostaną wysłane ponownie

11.1.7 Protokół TCP (ang. Transmission Control Protocol)

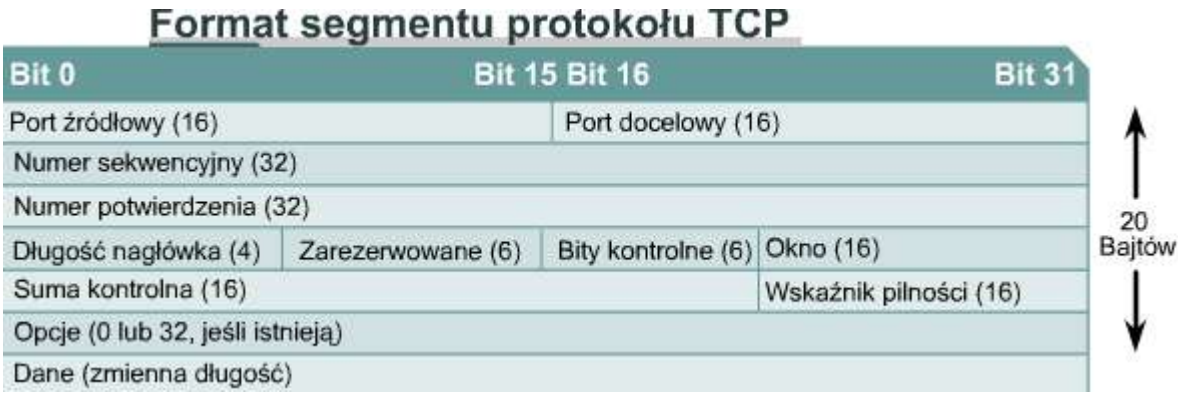
Protokół TCP jest należącym do warstwy 4 protokołem zorientowanym połączeniowo, który zapewnia niezawodną transmisję danych w trybie pełnego dupleksu. TCP jest częścią stosu protokołów TCP/IP. W środowisku zorientowanym połączeniowo przed rozpoczęciem transferu informacji musi zostać ustanowione połączenie między dwoma stacjami końcowymi. Protokół TCP jest odpowiedzialny za podział wiadomości na segmenty, ponowne złożenie ich na stacji docelowej, ponowne wysłanie wszystkich nieodebranych informacji i scalenie wiadomości z segmentów. Zapewnia on obwód wirtualny pomiędzy aplikacjami użytkowników końcowych.

Protokoły, które wykorzystują protokół TCP:

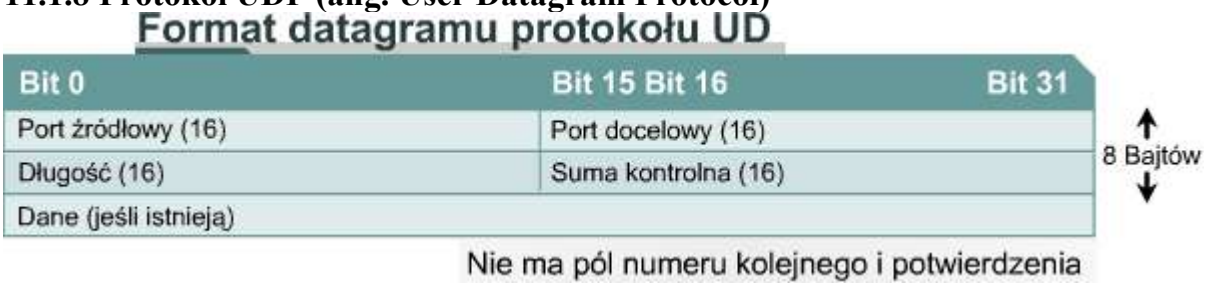
- protokół FTP (ang. *File Transfer Protocol*),
- protokół HTTP (ang. *Hypertext Transfer Protocol*),
- protokół SMTP (ang. *Simple Mail Transfer Protocol*),
- protokół Telnet.

Poniżej podano definicje pól segmentu TCP:

- **port źródłowy:** numer portu nadającego,
- **port odbiorcy:** numer wywoływanego portu,
- **numery sekwencyjne:** numery używane do zapewnienia prawidłowej kolejności nadchodzących danych,
- **numer potwierdzenia:** następny oczekiwany oktet TCP,
- **HLEN:** liczba 32-bitowych słów w nagłówku,
- **zarezerwowane:** pole ustawione na wartość zero,
- **bity kodowe:** funkcje sterujące (na przykład nawiązywanie i kończenie sesji),
- **okno:** liczba oktetów, którą zaakceptuje nadawca,
- **suma kontrolna:** suma kontrolna obliczona na podstawie pól nagłówka i danych,
- **wskaźnik pilności:** (ang. *Urgent Pointer*) określa koniec pilnych danych,
- **opcja:** jedna obecnie definiowana opcja — maksymalny rozmiar segmentu TCP,
- **dane:** dane protokołu wyższej warstwy.



11.1.8 Protokół UDP (ang. User Datagram Protocol)



Protokół UDP jest bezpołączeniowym protokołem transportowym należącym do stosu protokołów TCP/IP. Protokół UDP to prosty protokół wymiany datagramów bez potwierdzania czy gwarancji ich dostarczenia. Przetwarzanie błędów i retransmisja muszą być obsłużone przez protokoły wyższych warstw.

Protokół UDP nie wykorzystuje mechanizmów okienkowania ani potwierdzeń, więc niezawodność, jeśli jest wymagana, musi być zapewniana przez protokoły warstwy aplikacji. Protokół UDP jest zaprojektowany dla aplikacji, które nie mają potrzeby składania sekwencji segmentów.

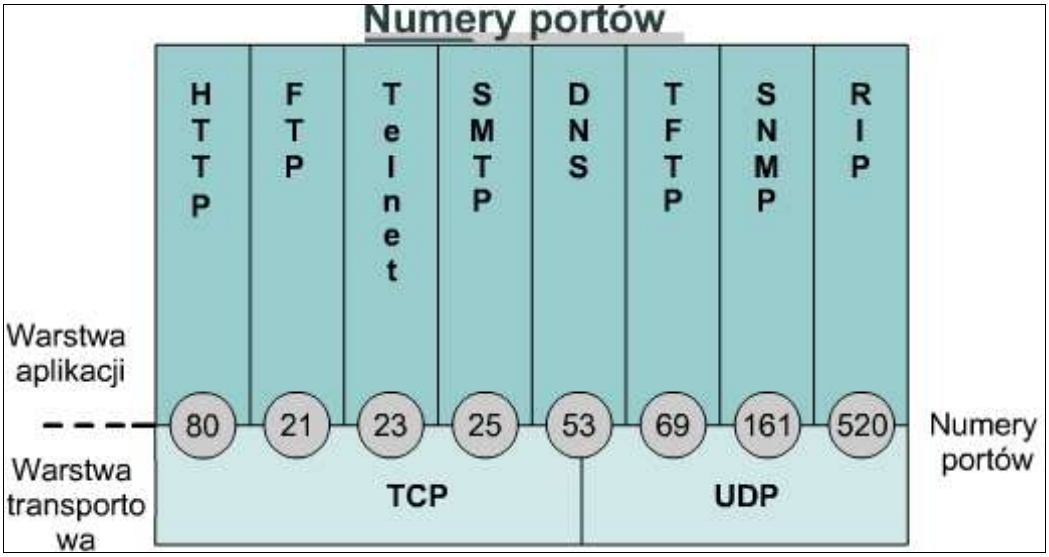
Protokoły, które wykorzystują protokół UDP:

- protokół TFTP (ang. *Trivial File Transfer Protocol*),
- protokół SNMP (ang. *Simple Network Management Protocol*),
- protokół DHCP (ang. *Dynamic Host Control Protocol*),
- protokół DNS (ang. *Domain Name System*).

Poniżej podano definicje pól segmentu UDP:

- **port źródłowy:** numer portu nadającego,
- **port odbiorcy:** numer wywoływanego portu,
- **długość:** liczba bajtów nagłówka i danych,
- **suma kontrolna:** suma kontrolna obliczona na podstawie pól nagłówka i danych,
- **dane:** dane protokołu wyższej warstwy.

11.1.9 Numery portów wykorzystywanych w protokołach TCP i UDP



W protokołach TCP i UDP numery portów (gniazd) są wykorzystywane do przekazywania informacji do wyższych warstw. Numery portów służą do rozróżniania rozmaitych konwersacji odbywających się w tym samym czasie w sieci. Projektanci aplikacji uzgodnili korzystanie z dobrze znanych numerów portów wydanych przez komitet Internet Assigned Numbers Authority (IANA). W każdym dialogu między aplikacjami FTP są wykorzystywane standardowe numery portów 20 i 21. Port 20 jest przeznaczony dla transmisji danych, zaś port 21 jest używany do sterowania. Do konwersacji, które nie dotyczą aplikacji z przypisanym dobrze znanym numerem portu, numery portów są przydzielane losowo z określonego zakresu powyżej numeru 1023. Niektóre porty są zarezerwowane zarówno w protokole TCP, jak i UDP, lecz aplikacje mogą ich nie obsługiwać. **Numery portów mają przydzielone następujące zakresy:**

- Numery poniżej 1024 są uważane za dobrze znane numery portów.
- Numery portów powyżej 1023 są przydzielane dynamicznie.
- Zarejestrowane numery portów to takie, które zostały zarejestrowane dla określonych aplikacji producenta. Większość z nich znajduje się powyżej numeru 1024.

Numery portów są wykorzystywane przez systemy końcowe do wyboru właściwej aplikacji. Host źródłowy dynamicznie przydziela numery portów źródła rozpoczynającego transmisję. Numery te są zawsze większe od 1023.

11.2 Warstwa aplikacji

11.2.1 Wprowadzenie do warstwy aplikacji modelu TCP/IP

W procesie projektowania modelu TCP/IP w jego warstwie aplikacji zostały zawarte warstwy sesji i prezentacji modelu OSI. Oznacza to, że reprezentacja danych, kodowanie i sterowanie konwersacją są obsługiwane w warstwie aplikacji zamiast w osobnych, niższych warstwach, jak to ma miejsce w modelu OSI. Taki projekt zapewnia projektantom oprogramowania maksymalną elastyczność na poziomie warstwy aplikacji modelu TCP/IP.

Protokoły TCP/IP, obsługujące przesyłanie plików, pocztę elektroniczną i zdalne logowanie, są prawdopodobnie najlepiej znane użytkownikom Internetu. Protokoły te obejmują następujące aplikacje:

- protokół DNS (ang. *Domain Name System*),
- protokół FTP (ang. *File Transfer Protocol*),
- protokół HTTP (ang. *Hypertext Transfer Protocol*),
- protokół SMTP (ang. *Simple Mail Transfer Protocol*),
- protokół SNMP (ang. *Simple Network Management Protocol*),
- protokół Telnet

11.2.2 System DNS Internet bazuje na hierarchicznym schemacie adresowania. Umożliwia on oparcie routingu na klasach adresów zamiast na pojedynczych adresach. Problemem, jaki wywołuje to po stronie użytkownika, jest skojarzenie poprawnego adresu z daną witryną internetową. Bardzo łatwo zapomnieć adres IP danej witryny, gdyż nie zawiera on nic, co mogłoby się kojarzyć z jej treścią. Można sobie wyobrazić trudność zapamiętania adresów IP dziesiątek, setek czy nawet tysięcy witryn internetowych. System nazw domen został zaprojektowany po to, by skojarzyć treść witryny z jej adresem. System nazw domen (DNS) to system używany w Internecie do tłumaczenia nazw domen i ich publicznie ogłoszonych węzłów sieciowych na adresy IP. Domena jest grupą komputerów, które są ze sobą powiązane poprzez ich geograficzną lokalizację lub typ prowadzonej działalności. Nazwa domeny jest łańcuchem znaków, cyfr lub kombinacją obu. Zwykle nazwa domeny będzie nazwą lub skrótem reprezentującym adres numeryczny witryny internetowej. W Internecie istnieje ponad 200 domen górnego poziomu, których przykładami są:

- **.us:** Stany Zjednoczone (United States),
- **.uk:** Wielka Brytania (United Kingdom).

Warstwa aplikacji

Światowe domeny ogólne

COM - Domena ta jest przeznaczona dla jednostek komercyjnych, tzn. dla przedsiębiorstw. Ze względu na wielki rozrost tej domeny istnieje obawa o obciążenie administracyjne i wydajność systemu, jeśli przyrost utrzyma się na obecnym poziomie. Rozważa się podział domeny COM i pozwolenie na przyszłą rejestrację jednostek komercyjnych w domenach podrzędnych.

EDU - Domena ta była pierwotnie przeznaczona dla wszystkich instytucji edukacyjnych. Zostało tu zarejestrowanych wiele uniwersytetów, szkół, college'ów, organizacji oferujących usługi edukacyjne oraz konsorcjów edukacyjnych. Ostatnio została podjęta decyzja o ograniczeniu dalszej rejestracji do czteroletnich college'ów i uniwersytetów. Szkoły i college'e dwuletnie mają być rejestrowane w domenach krajowych (zob. poniżej fragment dot. domeny US, szczególnie K-12 oraz CC).

NET - Domena ta przeznaczona jest tylko dla komputerów dostawców usług sieciowych, to jest komputerów NIC i NOC, komputerów administracyjnych oraz komputerów węzłów sieciowych. Klienci dostawców usług sieciowych będą mieli własne nazwy domen (nie w domenie nadrzędnej NET ang. Top Level Domain, TLD).

ORG - Domena ta jest przeznaczona jako ogólna domena TLD dla organizacji, których profil nie odpowiada innym jednostkom. Mogą tu znaleźć swoje miejsce niektóre organizacje pozarządowe.

INT - Domena ta jest przeznaczona dla organizacji ustanowionych na mocy umów międzynarodowych lub dla międzynarodowych baz danych.

Ogólne domeny dotyczące tylko Stanów Zjednoczonych

GOV - Domena ta była pierwotnie przeznaczona dla wszelkiego rodzaju biur i agencji rządowych. Ostatnio została podjęta decyzja o tym, żeby rejestrować w tej domenie tylko agencje federalne rządu USA. Agencje stanowe i lokalne są rejestrowane w domenie krajowej.

MIL - Domena ta jest używana przez wojsko USA.

Przykład kodu domeny krajowej

US - Domena US, jako przykład domeny krajowej, umożliwia rejestrację wszelkiego rodzaju jednostek w Stanach Zjednoczonych na podstawie podziału polityczno-administracyjnego, tzn. ma następującą hierarchię: <nazwa_jednostki>.<region>. <kod stanu>. US. Na przykład: IBM.Armonk.NY.US. Co więcej, gałęzie domeny US w ramach każdego stanu zawierają kody dla szkół (K12), college'ów społecznych (CC), szkół technicznych (TEC), stanowych agencji rządowych (STATE), rad samorządowych (COG), bibliotek (LIB), muzeów (MUS) oraz kilku innych ogólnych typów jednostek.

Istnieją również nazwy ogólne, których przykładami są:

- **.edu:** witryny edukacyjne,
- **.com:** witryny komercyjne,
- **.gov:** witryny rządowe,
- **.org:** witryny organizacji non-profit,
- **.net:** usługi sieciowe.

11.2.3 FTP i TFTP

Protokół FTP jest niezawodną usługą zorientowaną połączeniowo, która wykorzystuje protokół TCP do przesyłania plików pomiędzy systemami obsługującymi protokół FTP. Głównym zadaniem protokołu FTP jest przesyłanie plików poprzez kopiowanie i przenoszenie ich pomiędzy serwerami i klientami. W przypadku kopiowania plików z serwera protokół FTP najpierw ustanawia połączenie sterujące między klientem i serwerem. Następnie między komputerami zostaje ustanowione drugie połączenie, za pośrednictwem którego są przesyłane dane. Transfer danych może się odbywać w trybie ASCII lub w trybie binarnym. Tryby te określają sposób kodowania dla plików danych, co w modelu OSI jest zadaniem warstwy prezentacji. Po zakończeniu przesyłania plików połączenie danych zostaje automatycznie zakończone. Gdy cała sesja kopiowania i przenoszenia plików jest zakończona, po wylogowaniu się i zakończeniu sesji przez użytkownika zostaje zamknięte połączenie sterujące służące do przesyłania poleceń.

Protokół TFTP jest usługą bezpołączeniową wykorzystującą protokół UDP (ang. *User Datagram Protocol*). Protokół TFTP jest używany przez router do przesyłania plików konfiguracyjnych oraz obrazów systemu Cisco IOS, a także do przesyłania plików pomiędzy systemami korzystającymi z TFTP. Protokół TFTP został zaprojektowany jako niewielki i prosty w implementacji. Dlatego też brak mu większości funkcji protokołu FTP. Protokół TFTP pozwala na odczyt i zapis plików do lub ze zdalnego serwera, lecz nie umożliwia wyświetlania zawartości katalogów i nie ma obecnie żadnych funkcji związanych z uwierzytelnianiem użytkownika. Protokół ten jest przydatny w niektórych sieciach LAN, gdyż działa on szybciej niż protokół FTP i w stabilnym środowisku pracuje niezawodnie

11.2.4 Protokół http

Adres URL

http://	www.	cisco.com	/edu/
Określa protokół, jaki ma być użyty przez przeglądarkę.	Identyfikuje nazwę hosta lub nazwę określonego komputera.	Reprezentuje jednostkę domeny witryny WWW.	Identyfikuje folder, w którym strona WWW jest zlokalizowana na serwerze. Ponieważ nazwa strony nie jest podana, przeglądarka załaduje domyślną stronę określoną przez serwer.

Elementy standardowego adresu URL (ang. Uniform Resource Locator).

Protokół HTTP (ang. *Hypertext Transfer Protocol*) działa w sieci WWW, która jest najszybciej rozwijającą się i najczęściej używaną częścią Internetu. Jednym z głównych powodów niezwykłego rozwoju sieci WWW jest związana z nią łatwość dostępu do informacji. Przeglądarka WWW jest aplikacją typu klient-serwer, co oznacza, że do funkcjonowania wymaga zarówno komponentów klienta, jak i serwera. Dane są prezentowane przez przeglądarkę WWW w formie multimedialnej na stronach WWW, które wykorzystują tekst, grafikę, dźwięk i pliki wideo. Strony WWW są tworzone za pomocą języka służącego do formatowania zwanego HTML (ang. *Hypertext Markup Language*). Polecenia języka HTML tak kierują pracą przeglądarki WWW na danej stronie WWW, by przedstawiła ona wygląd tej strony w określony sposób. Co więcej, język HTML określa miejsca umieszczenia tekstu, plików i obiektów, które mają być przesłane z serwera WWW do przeglądarki. Hiperłącza sprawiają, iż poruszanie się po sieci WWW jest proste. Hiperłącze jest obiektem, wyrazem, frazą lub obrazkiem na stronie WWW. Po jego kliknięciu przeglądarka zostaje przekierowana na inną stronę WWW. Strona WWW zawiera (przeważnie ukryty w opisie HTML) adres lokalizacji znany jako adres URL (ang. *Uniform Resource Locator*).

W adresie URL http://www.cisco.com/edu/, część „http://” informuje przeglądarkę o tym, jakiego protokołu należy użyć. Druga część, „www” jest nazwą hosta lub nazwą określonej maszyny o danym adresie IP. Ostatnia część, „/edu/”, identyfikuje położenie na serwerze określonego folderu zawierającego domyślną stronę WWW. Zwykle przeglądarka WWW otwiera się na stronie początkowej lub „domowej" (ang. *home*). Adres URL strony domowej został wcześniej zapisany w obszarze konfiguracji przeglądarki WWW i może być zmieniony w dowolnym momencie. Na stronie startowej można kliknąć jedno z hiperłączy do stron WWW lub wpisać adres URL na pasku adresu przeglądarki. Przeglądarka WWW sprawdza protokół pod kątem potrzeby otwarcia innego programu, a następnie za pomocą systemu DNS określa adres IP serwera WWW. Następnie warstwy transportowa, sieci, łącza danych i fizyczna współdziałają w celu zainicjowania sesji z serwerem WWW. Dane przesyłane do serwera HTTP zawierają nazwę katalogu z lokalizacją strony WWW. Dane mogą również zawierać nazwę konkretnego pliku ze stroną HTML. Jeśli żadna nazwa nie została podana, zostaje użyta nazwa domyślna określona w konfiguracji serwera.

Serwer w odpowiedzi na żądanie wysyła do klienta WWW cały tekst, pliki audio i wideo oraz grafikę, zgodnie z instrukcjami HTML. Wszystkie te pliki zostają ponownie złożone przez przeglądarkę po stronie klienta w celu

utworzenia widoku strony WWW, a następnie sesja zostaje zakończona. Po kliknięciu innej strony znajdującej się na tym samym lub innym serwerze cały proces zaczyna się od nowa.

11.2.5 Protokół SMTP

Serwery poczty elektronicznej w celu wysyłania i odbioru poczty komunikują się ze sobą za pomocą protokołu SMTP (ang. *Simple Mail Transfer Protocol*). Protokół SMTP przesyła wiadomości e-mail w formacie ASCII, wykorzystując do tego protokół TCP.

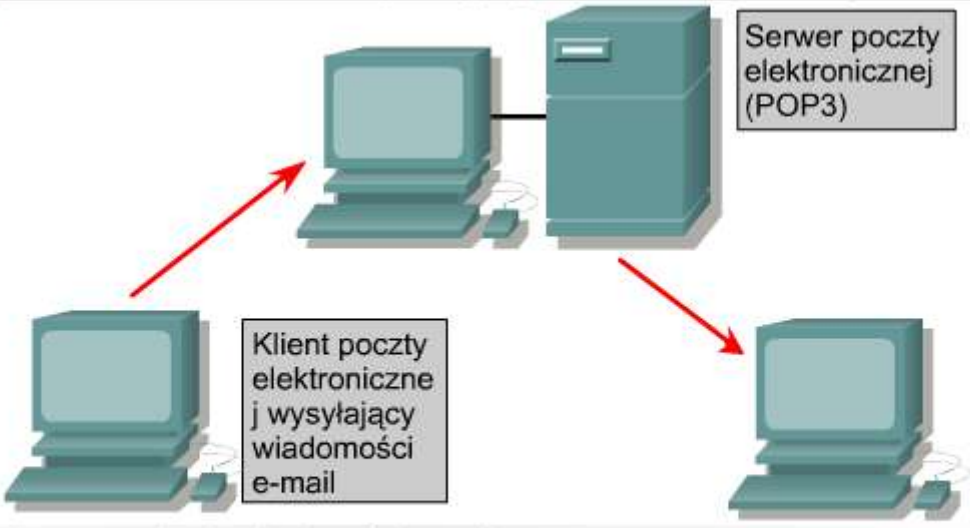
Gdy serwer poczty elektronicznej otrzymuje wiadomość przeznaczoną dla klienta lokalnego, przechowuje ją i oczekuje, aż klient pobierze pocztę. Klienci poczty elektronicznej mogą pobierać przeznaczone dla nich wiadomości na kilka sposobów. Mogą użyć programów, które uzyskują bezpośredni dostęp do plików serwera pocztowego, lub ściągnąć pocztę za pomocą jednego z wielu protokołów sieciowych. Najbardziej popularnymi protokołami klientów poczty elektronicznej są POP3 oraz IMAP4, oba wykorzystują do transportu danych protokół TCP. Pomimo że klienci poczty elektronicznej wykorzystują do pobierania poczty takie specjalne protokoły, to prawie zawsze do jej wysyłania używają protokołu SMTP. Ponieważ do wysyłania i odbierania poczty są używane dwa różne protokoły i prawdopodobnie dwa różne serwery, zdarza się, że klienci pocztowi mogą wykonywać tylko jedno z tych zadań. Dlatego zwykle dobrze jest osobno rozwiązywać problemy dotyczące wysyłania i odbierania poczty elektronicznej.

Podczas sprawdzania konfiguracji klienta pocztowego należy upewnić się, że ustawienia protokołów SMTP i POP lub IMAP są poprawnie skonfigurowane. Dobrym sposobem sprawdzenia osiągalności serwera pocztowego jest próba nawiązania połączenia Telnet z portem SMTP (25) lub POP3 (110). Aby przetestować możliwość skontaktowania się z usługą SMTP na serwerze pocztowym o adresie IP 192.168.10.5, można w wierszu poleceń systemu Windows użyć następującego polecenia:

C:\>telnet 192.168.10.5 25

Protokół SMTP nie oferuje wielu możliwości zabezpieczeń i nie wymaga żadnego uwierzytelniania. Administratorzy często nie zezwalają hostom spoza sieci wewnętrznej na wykorzystywanie ich serwera SMTP do wysyłania lub przekazywania poczty. Robią tak, aby uniemożliwić nieautoryzowanym użytkownikom wykorzystanie ich serwerów jako przekaźników poczty (ang. *mail relay*)

Przesyłanie wiadomości e-mail pomiędzy serwerem pocztowym a klientem



Podczas wysyłania wiadomości e-mail zaprezentowany proces ma za zadanie wysłać tę wiadomość do serwera pocztowego obsługującego danego użytkownika. Użytkownik ten następnie pobiera wiadomość z serwera pocztowego.

11.2.6 Protokół SNMP

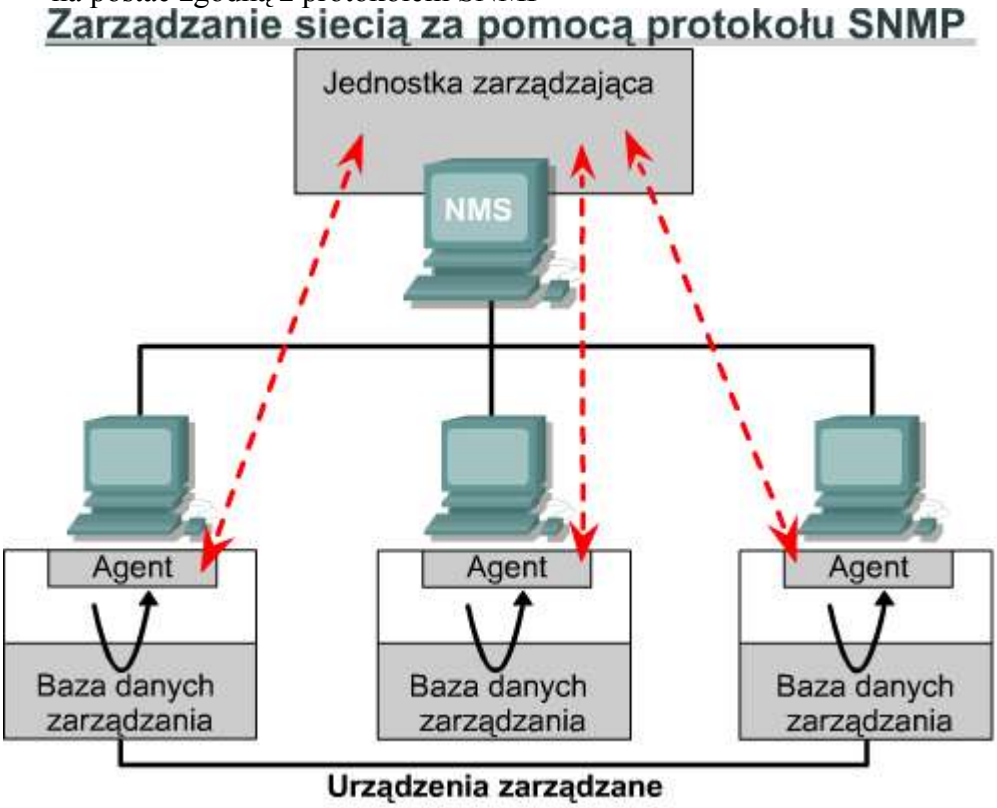
Protokół SNMP (ang. *Simple Network Management Protocol*) jest protokołem warstwy aplikacji ułatwiającym wymianę pomiędzy urządzeniami sieciowymi informacji związanych z zarządzaniem.

Protokół SNMP umożliwia administratorom sieci zarządzanie wydajnością sieci, odnajdywanie i rozwiązywanie problemów sieciowych oraz planowanie rozwoju sieci. Protokołem warstwy transportowej w ramach SNMP jest protokół UDP.

Sieć zarządzana za pomocą protokołu SNMP składa się z trzech następujących elementów kluczowych:

- **System zarządzania siecią (NMS):** system NMS uruchamia aplikacje, które monitorują i sterują urządzeniami zarządzanymi. Większość funkcji przetwarzania i zasobów pamięci wymaganych do zarządzania siecią jest zapewniana przez system NMS. W każdej zarządzanej sieci musi istnieć przynajmniej jeden system NMS.

- **Urządzenia zarządzane:** urządzenia zarządzane to węzły sieci, które zawierają agenta SNMP i są elementami zarządzanej sieci. Urządzenia zarządzane zbierają i przechowują informacje dotyczące zarządzania oraz udostępniają je systemom NMS za pomocą protokołu SNMP. Urządzeniami zarządzanymi, zwanymi czasem elementami sieci, mogą być routery, serwery dostępowe, przełączniki, mosty, koncentratory, komputery lub drukarki.
- **Agenci:** agenci to moduły oprogramowania do zarządzania siecią znajdujące się w zarządzanych urządzeniach. Agent ma lokalną wiedzę na temat informacji dotyczących zarządzania i tłumaczy te informacje na postać zgodną z protokołem SNMP



11.2.7 Protokół Telnet

Oprogramowanie klienckie Telnet zapewnia możliwość zalogowania się do zdalnych hostów internetowych z uruchomionym serwerem Telnet, a następnie wykonywanie poleceń przy użyciu wiersza poleceń. Klient usługi Telnet jest nazywany hostem lokalnym. Serwer Telnet, wykorzystujący specjalne oprogramowanie zwane demonem, jest nazywany hostem zdalnym.

Aby nawiązać połączenie z klienta Telnet, musi zostać wybrana opcja połączenia. Zwykle pojawia się okienko dialogowe z zapytaniem o nazwę hosta i typ terminala. Nazwa hosta to adres IP lub nazwa DNS zdalnego komputera. Typ terminala opisuje rodzaj emulacji, jaką powinien realizować klient Telnet. Operacje realizowane za pomocą protokołu Telnet nie wykorzystują mocy obliczeniowej komputera transmitującego. Zamiast tego, do zdalnego hosta transmitowane są naciśnięcia klawiszy, a ekran wynikowy jest przesyłany z powrotem na lokalny monitor. Całe przetwarzanie i zapis wyników są realizowane po stronie komputera zdalnego.

Telnet pracuje na poziomie warstwy aplikacji modelu TCP/IP. Zatem protokół Telnet funkcjonuje w trzech górnych warstwach modelu OSI. Warstwa aplikacji realizuje polecenia. Warstwa prezentacji obsługuje formatowanie, zwykle w kodzie ASCII. Zadaniem warstwy sesji jest transmisja. W modelu TCP/IP wszystkie te funkcje należą do warstwy aplikacji.