PROTOKOŁY TRANSPORTU
PORTY – krótki przegląd

1. Standardowe protokoły internetowe

1.1. TCP – Transmission Control Protocol

Aplikacje, dla których istotne jest, żeby dane niezawodnie dotarły do celu, wykorzystują protokół TCP. Zapewnia on prawidłowe przesyłanie danych we właściwej kolejności. Nie zastępuje on protokołu IP, lecz wykorzystuje jego właściwości do nadawania i odbioru.

TCP jest niezawodnym protokołem transmisyjnym, zorientowanym połączeniowo. Komputer po upływie określonego czasu wysyła dane ponownie aż do chwili, gdy otrzyma od odbiorcy potwierdzenie, że zostały poprawnie odebrane.

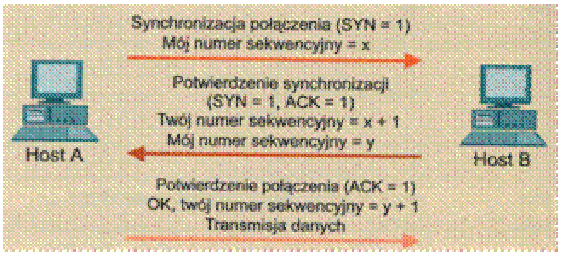
Jednostka czasu, którą posługują się we wzajemnej komunikacji moduły TCP, nosi nazwę segmentu. Każdy segment zawiera przy tym automatycznie sumę kontrolną, która podlega weryfikacji po stronie odbiorcy. W ten sposób sprawdza się, czy dane zostały odebrane poprawnie.

TCP jest zorientowany na połączenia. Protokół tworzy zatem połączenie logiczne komputer-komputer. W tym celu wysyła przed rozpoczęciem właściwej transmisji danych użytecznych pewną ilość informacji kontrolnych, nazywanych handshake.

Handshake wykorzystywany w TCP to 3-Way-Handshake, ponieważ w jego trakcie wymieniane są trzy bloki informacji. Nawiązywanie połączenia rozpoczyna się od tego, że oba komputery ustalają wartość początkową sekwencji numerycznej – Initial Sequence Number (ISN). Oba systemy TCP wymieniają między sobą i potwierdzają te wartości.

1.1.1. 3-Way-Handshake

Nawiązywanie połączenia za pomocą 3-Way-Handshake można przedstawić w postaci diagramu. Za pomocą odpowiedniego polecenia połączenie przechodzi w tryb Listen, w którym można nawiązać kontakt z innym systemem TCP.



Jeżeli system znajduje się w trybie Listen, czeka na nadejście znaku SYN, aby odpowiedzieć kolejnym znakiem SYN, a następnie przejść w tryb SYN Received. Jeżeli znak SYN został wysłany, połączenie przechodzi w tryb SYN Send. System TCP pozostaje w tym trybie aż do otrzymania od drugiego systemu znaku SYN w odpowiedzi. Jeżeli nadejdzie pozytywna odpowiedź na ten znak SYN, system TCP przechodzi w tryb SYN Received. Po pozytywnym potwierdzeniu znaku SYN (ACK w odpowiedzi na SYN) nadajnik i odbiornik przechodzą w tryb Established – może się rozpocząć transmisja danych między obydwoma komputerami. Po przesłaniu wszystkich danych komputery biorące udział w komunikacji kontynuują procedurę 3-Way-Handshake. W celu zakończenia połączenia wymieniane są segmenty z bitem No more data from sender.

1.2. UDP – User Datagram Protocol

Protokół UDP zapewnia protokołom wyższego rzędu zdefiniowaną usługę transmisji pakietów danych, zorientowanej transakcyjnie. Dysponuje minimalnymi mechanizmami transmisji danych i opiera się bezpośrednio na protokole IP. W przeciwieństwie do TCP nie gwarantuje kompleksowej kontroli skuteczności transmisji, a zatem nie ma pewności dostarczenia pakietu danych do odbiorcy, nie da się rozpoznać duplikatów, ani nie można zapewnić przekazu pakietów we właściwej kolejności.

Mimo to jest wiele istotnych powodów stosowania UDP jako protokołu transportowego. Gdy trzeba przesłać niewiele danych, nakłady administracyjne na nawiązanie połączenia i zapewnienie prawidłowej transmisji mogą być większe od nakładów niezbędnych do ponownej transmisji wszystkich danych.

2. Protokoły, porty i gniazda

Gdyby nie było portów, komunikacja za pośrednictwem standardowych protokołów internetowych TCP i UDP byłaby niemożliwa. To dzięki portom wiele aplikacji może jednocześnie wymieniać dane, wykorzystując jedno łącze internetowe.

2.1. Numery portów

Numery portów stanowią jeden z podstawowych elementów stosowania protokołów TCP i UDP. Gdy dane docierają do komputera docelowego, muszą jeszcze zostać dostarczone do właściwej aplikacji. Podczas transportu informacji przez warstwy sieci potrzebny jest mechanizm, który najpierw gwarantuje przekazanie danych do właściwego w danym wypadku protokołu.

Łączenie danych z wielu źródeł w jeden strumień danych nosi nazwę multipleksowania. Protokół internetowy (IP) musi zatem poddać dane nadchodzące z sieci procesowi demultipleksowania. W tym celu IP oznacza protokoły transportowe numerami protokołów. Same protokoły transportowe wykorzystują z kolei numery porów do identyfikacji aplikacji.

Numer protokołu IP zawarty jest w jednym bajcie w trzecim słowie nagłówka datagramu. Wartość ta determinuje przekazanie do odnośnego protokołu w warstwie transportowej; przykładowo 6 to TCP, 17 to UDP. Protokół transportowy musi przekazać otrzymane dane do właściwego procesu aplikacji.

Aplikacje identyfikowane są na podstawie numerów portów o długości 16 bitów, do których dane kierowane są po nadejściu do komputera docelowego. W pierwszym słowie każdego nagłówka TCP czy UDP zapisany jest też numer portu źródłowego i numer portu docelowego. Jeżeli aplikacja ma być dostępna pod określonym numerem portu, musi przekazać tę informację do stosu protokółu TCP/IP.

2.2. Gniazda

Kombinację adresu IP i numeru portu określa się jako gniazdo. To połączenie umożliwia jednoznaczną identyfikację poszczególnych procesów sieciowych w ramach całego Internetu.

Zapis ma następującą postać: adres IP:port, np. 62.96.227.70:80. Dwa gniazda definiują połączenie: jedno określa komputer źródłowy, drugie – docelowy.

TCP i UDP mogą nadawać te same numery portów. Dopiero połączenie protokołu i numeru portu jest jednoznaczne. Numer portu 53 w TCP nie jest identyczny z numerem portu 53 w UDP.

3. Porty – krótki przegląd

Microsoft Windows wykorzystuje kilka portów do realizacji swoich funkcji sieciowych. W starszych wersjach, do Windows Me/NT, były to porty 137, 138 i 139. Od Windows 2000 Server message lock wysyłane są przez port 445. Oczywiście, wersje Windows od 2000 są zgodne w dół, a więc obie procedury mogą funkcjonować równolegle.

- Port 137

  Obsługuje tzw. NetBIOS Name Service. Za jego pomocą Windows przyporządkowuje wzajemnie – podobnie jak w DNS – nazwy komputerów i adresy IP. W określonych wypadkach może to powodować następującą sytuację – jeżeli użytkownik surfuje na windowsowym serwerze WWW, ten ostatni wysyła zapytanie do portu 137 komputera użytkownika. Dzieje się tak, ponieważ serwer windowsowy wykorzystuje funkcję winsock gethostbyaddr() do odczytania nazwy odległego komputera. Funkcja ta jest jednak tak zaimplementowana w Windows, że najpierw następuje próba odczytu przez NetBIOS, a dopiero w razie niepowodzenia wykorzystywany jest odczyt przez DNS.

  Tego rodzaju ruch powinien być generalnie zabroniony, zarówno wchodzący, jak i wychodzący. Jeżeli dwie sieci windowsowe mają wymieniać dane przez Internet, generalnie należy zastosować VPN.

- Port 138

  Kryje się za nim usługa NetBIOS datagram service. Za jej pomocą Windows rozsyła głównie informacje o sieci Windows, najczęściej w formie rozgłaszania. Na przykład usługa Windows computerbrowser wykorzystuje informacje NetBIOS do sporządzenia aktualnej listy komputerów w sieci Windows, wyświetlanej w oknie Otoczenie sieciowe.

  Największe niebezpieczeństwo związane z usługą datagram service polega na tym, że haker może przekonać Windows za pomocą sfałszowanych pakietów, iż jego komputer należy do lokalnej sieci, a więc może w ten sposób obejść różnice zabezpieczeń odnoszących się do komputerów lokalnych i internetowych. Również i tu obowiązuje zasada, że port ten należy zamknąć w obu kierunkach

- Port 139

  Przez tę usługę NetBIOS Session Service odbywa się właściwa wymiana danych w sieciach Windows. Jeżeli port ten jest otwarty, haker może się połączyć z komputerem i próbować zhakować udostępnianie plików i drukarek. Najczęściej wykorzystywana metoda to atak siłowy, polegający na wypróbowaniu jak największej liczby prawdopodobnych haseł.

  Otwarty port 139 może powodować jeszcze inne problemy. Usługa Windows Messenger nasłuchuje tu w oczekiwaniu na wiadomości, przesyłane za pomocą net send, co często jest wykorzystywane do spamowania. W takim wypadku użytkownik nie otrzymuje e-mailu; od razu otwiera się okno z wiadomością nadesłaną przez spamera. Dlatego port ten powinien być zamknięty w obu kierunkach.

- Sieć Microsoft – port 135

  Nawet jeśli port 139 jest zamknięty, nie chroni nas to do końca przed spamem nadsyłanym z wykorzystaniem Messengera. Polecenie net send wykorzystuje nieudokumentowaną funkcje usługi Microsoft RPC, która w porcie 135 (epmap, endpoint mapper) nasłuchuje w oczekiwaniu na nadchodzące zapytania RPC. Usługa ta oferuje m.in. połączenie z Messengerem, a więc net send może wykorzystać tę drogę jako alternatywę, gdy normalny dostęp przez port 139 nie jest możliwy. Są już narzędzia do rozsyłania spamu, które wykorzystują tę metodę.

- Port 445

  W Windows 2000 Microsoft rozszerzył protokół SMB o możliwość wykonywania przez TCP/IP, z pominięciem okrężnej drogi „NetBIOS over TCP/IP". Windows używa w tym celu wyłącznie portu 445 (microsoft-ds).

  W otoczeniu składającym się wyłącznie z Windows 2000, XP i .NET Server 2003 można go wyłączyć, odznaczając NetBIOS over TCP/IP w opcjach karty sieciowej. Na skutek tego odczytywanie nazw w sieci LAN będzie się odbywało tylko przez DNS, ale już nie poprzez WINS lub rozgłaszanie NetBIOS. Potrzebny jest zatem albo serwer DNS w sieci LAN, który będzie zarządzał również lokalnymi komputerami (choćby Windows 2000 jako serwer DHCP i DNS), lub na każdym komputerze trzeba założyć listę hostów. Dla portu 445 obowiązuje zasada, że ruch SMB dozwolony jest tylko wewnątrz sieci LAN.

4. Literatura

4.1. Komar, B. (2002). TCP/IP dla każdego. Gliwice: Helion.

4.2. „PC World Komputer PRO”. Nr 2/2003.

4.3. „PC World Komputer PRO”. Nr 3/2003.