Akademia Techniczno-Humanistyczna
w Bielsku-Białej

Wydział Budowy Maszyn i Informatyki

Laboratorium z sieci komputerowych

Ćwiczenie numer:
5

Temat ćwiczenia:

Badanie protokołów rodziny TCP/IP

1. Wstęp teoretyczny.

Internet został zaprojektowany jako sieć łączności, która mogłaby działać także w okresie wojny. Chociaż Internet ewoluował w zupełnie innych kierunkach, niż wyobrażali to sobie jego twórcy, nadal jego podstawę stanowi zestaw protokołów TCP/IP. Architektura protokołów TCP/IP doskonale nadaje się do wykorzystania w zdecentralizowanej i odpornej na błędy sieci. Taką siecią jest Internet. Wiele z używanych aktualnie protokołów zostało opartych na modelu TCP/IP. TCP/IP nie jest pojedynczym protokołem, lecz pakietem protokołów. Model TCP/IP korzysta z czterowarstwowego modelu łączności, a nie jak w modelu OSI z siedmiowarstwowego. Modele odniesienia OSI i TCP/IP nie odpowiadają sobie w stosunku jeden do jednego. Każda warstwa modelu TCP/IP jest odwzorowana na jedną lub więcej warstw modelu OSI.

Model TCP/IP	Model OSI
Warstwa aplikacji	Warstwa aplikacji
	Warstwa prezentacji
	Warstwa sesji
Warstwa transportowa	Warstwa transportowa
Warstwa Internetu	Warstwa sieciowa
	Warstwa łącza danych
Warstwa dostępu do sieci	Warstwa fizyczna

Protokół IP

W modelu odniesienia TCP/IP podstawowym protokołem jest protokół IP. Pracuje on w warstwie Internetu. IP (*Internet Protocol*) jest bezpołączeniowym protokołem udostępniającym usługi adresowania, pakowania i przesyłania jednostek danych zwanych pakietami. IP identyfikuje hosty lokalne i zdalne. Gdy trasa do sieci docelowej wymaga innych rozmiarów pakietu, IP dzieli pakiet na fragmenty, co pozwala na ich transmisję bez błędów, a następnie składa razem fragmenty w pakiet w hoście docelowym. IP odrzuca też pakiety przeterminowane oraz przekazuje wyznaczone pakiety do protokołów w wyższych warstwach.

Budowa pakietu protokołu IP.

Pakiet IP składa się z dwóch części: nagłówka i ładunku. Nagłówek służy do sterowania zachowaniem w warstwie IP: trasowaniem, fragmentacją i tak dalej. Nagłówki i dane protokołów z wyższych warstw są zawarte w ładunku IP, czyli w obszarze danych.

<table>
<tr><td>4 bity</td><td>4 bity</td><td>4 bity</td><td>4 bity</td><td>4 bity</td><td>4 bity</td><td>4 bity</td><td>4 bity</td></tr>
<tr><td colspan="8"></td></tr>
<tr><td>Wersja</td><td>IHL</td><td colspan="2">Typ usługi (TOS)</td><td colspan="4">Całkowita długość</td></tr>
<tr><td colspan="4">Identyfikacja</td><td>Flagi</td><td colspan="3">Przesunięcie fragmentu</td></tr>
<tr><td colspan="2">Czas życia (TTL)</td><td colspan="2">Protokół</td><td colspan="4">Suma kontrolna nagłówka</td></tr>
<tr><td colspan="8">Adres IP nadawcy</td></tr>
<tr><td colspan="8">Adres IP odbiorcy</td></tr>
<tr><td colspan="6">Opcje IP</td><td colspan="2">Wypełnienie</td></tr>
<tr><td colspan="8">Dane</td></tr>
<tr><td colspan="8">...</td></tr>
</table>

Poszczególne pola oznaczają:

Wersja – określa format nagłówka pakietu IP. 4-bitowe pole wersji zawiera liczbę 4, jeśli jest to pakiet IPv4, a liczbę 6, jeśli jest to pakiet IPv6. Pole to nie jest jednak stosowane do rozróżniania pomiędzy pakietami IPv4 a IPv6 - taką rolę pełni pole typu protokołu obecne w ramce warstwy drugiej.

IHL (Internet Header Length) – określa długość nagłówka datagramu jako wielokrotność słów 32-bitowych. Jest to całkowita długość wszystkich informacji znajdujących się w nagłówku, obejmująca dwa pola nagłówka o zmiennych długościach.

Typ obsługi (TOS – Type Of Sernice) - określa poziom ważności, który został przypisany przez protokół wyższej warstwy; osiem bitów.

Całkowita długość – określa długość całego pakietu w bajtach z uwzględnieniem danych i nagłówka. Aby uzyskać długość pola danych, od długości całkowitej należy odjąć wartość IHL

Identyfikacja – zawiera liczbę całkowitą identyfikującą bieżący datagram. Jest to tak zwany numer sekwencyjny.

Flagi – pole o długości trzech bitów, w którym dwa mniej znaczące bity sterują fragmentacją. Jeden bit określa, czy pakiet może zostać podzielony na fragmenty, a drugi służy do oznaczenia ostatniego pakietu w serii podzielonych pakietów.

Przesunięcie fragmentu – pole pomocne przy składaniu fragmentów datagramu. Składa się z 13 bitów. Pole to pozwala na zakończenie poprzedniego pola na granicy 16 bitów.

Czas życia (TTL – Time To Live) – pole określające liczbę przeskoków, które może wykonać pakiet. Liczba ta jest zmniejszana o jeden za każdym razem, gdy pakiet przechodzi przez router. Gdy licznik osiągnie wartość zero, pakiet jest odrzucany. Zapobiega to przesyłaniu pakietu w nieskończonej pętli.

Protokół - pole wskazujące, który protokół wyższej warstwy, taki jak TCP lub UDP, odbiera pakiety przychodzące po zakończeniu przetwarzania IP. Wartości: 1 – ICMP, 6 – TCP, 17 – UDP

Suma kontrolna nagłówka – pole pomagające zapewnić integralność nagłówka. Matematyczna suma kontrolna, przeliczana w każdym ruterze z uwagi na zmiany informacji nagłówka

Adres IP nadawcy i odbiorcy – 32 bitowe numery IP nadawcy i odbiorcy danego pakietu.

Opcje – pole umożliwiające protokołowi IP obsługę różnych opcji, takich jak funkcje zabezpieczeń, wyboru trasy. Pole to ma zmienną długość.

Wypełnienie – zera dodane w celu zagwarantowania, że długość nagłówka jest wielokrotnością 32 bitów.

Dane – pole zawierające informacje wyższych warstw (np. segmenty TCP lub UDP). Zmienna długość do 64 kB.

Protokół ICMP

Sieci powinny działać poprawnie przez cały czas, lecz tak niestety nie jest. Gdy coś dzieje się nie tak w warstwie internetowej, rolę narzędzia do rozwiązywania problemów odgrywa protokół komunikacyjny zarządzania siecią Internet ICMP (*Internet Control Message Protocol*). ICMP jest protokołem serwisowym, który zgłasza błędy łączności między hostami. Protokół ICMP jest zestawem komunikatów, przesyłanych w datagramach IP i zdolnych do zgłaszania błędów w dostarczaniu innych datagramów IP. Komunikaty ICMP są narzędziami diagnostycznymi „wbudowanymi" w warstwę internetową. Jeśli dwa hosty nie są w stanie komunikować się ze sobą, komunikaty ICMP mogą pomóc w zdiagnozowaniu problemu.

Pakiet ICMP jest zawarty w samym datagramie IP i identyfikowany przez wartość w polu *Protokół* równą 1. Pakiet ICMP zawiera 8-bitowe pola *Typ* i *Kod* oraz 16-bitowe pole sumy kontrolnej.

8 bitów	8 bitów	16 bitów
Typ	**Kod**	**Suma kontrolna**

Pole **Typ** służy do identyfikacji typu komunikatu ICMP. Najbardziej znane typy to:
0 - *Echo Reply* (Odpowiedź echa) odpowiedź na komunikat *Żądanie echa*.
8 - *Echo Request* (Żądanie echa) służy do sprawdzenia łączności pomiędzy dwoma hostami. Narzędzie ping wysyła żądania echa ICMP.
11 - *Time Exceeded* (Przekroczony czas) gdy ruter otrzymuje pakiet o TTL równym 0, może wysłać ten komunikat do hosta źródłowego
Pole **Kod** zawiera bardziej szczegółowe informacje odnoszące się do typu komunikatu.
Pole **Suma kontrolna**, podobnie jak w innych rodzajach pakietów, służy do sprawdzenia integralności danych.

Protokół TCP

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.

Protokoły, które wykorzystują protokół TCP:
FTP (ang. File Transfer Protocol),
HTTP (ang. Hypertext Transfer Protocol),
SMTP (ang. Simple Mail Transfer Protocol),
Telnet.

Budowa segmentu protokołu TCP

Port źródłowy – 16 bitów		**Port docelowy – 16 bitów**	
Numer sekwencyjny – 32 bity			
Numer potwierdzenia – 32 bity			
Długość nagłówka (4 b)	**Zarezerwowane (6 b)**	**Bity kontrolne (6 b)**	**Okno (16 b)**
Suma kontrolna (16 b)		**Wskaźnik pilności (16 b)**	
Opcje (0 lub 32 bity)			
Dane			

Poszczególne pola oznaczają:

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

Długość nagłówka – 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 – określa koniec pilnych danych

Opcja – jedna obecnie definiowana opcja — maksymalny rozmiar segmentu TCP

Dane – dane protokołu wyższej warstwy.

Protokół UDP

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

Budowa datagramu UDP

Port źródłowy (16 b)	**Port docelowy (16 b)**
Długość (16 b)	**Suma kontrolna (16 b)**
Dane (jeśli istnieją)	

Poszczególne pola 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.

Protokół ARP

W przypadku sieci TCP/IP pakiet danych musi zawierać zarówno adres MAC, jak i adres IP urządzenia docelowego. Pakiet niezawierający jednego z nich nie zostanie przekazany z warstwy 3 do warstw wyższych.

Komputer potrzebujący pary adresów IP i MAC rozgłasza żądanie ARP. Wszystkie urządzenia w sieci analizują to żądanie. Jeżeli jedno z urządzeń lokalnych będzie miało pasujący do żądania adres IP, wyśle odpowiedź ARP zawierającą parę adresów IP-MAC. W wypadku, gdy adres IP należy do sieci lokalnej, a komputer nie istnieje lub jest wyłączony, nie pojawi się odpowiedź na żądanie ARP. W tej sytuacji urządzenie źródłowe zgłasza błąd.
Istnieje również odmiana RARP (Reverse ARP) jest on analogiczny do ARP z tą tylko różnicą, że mając adres MAC otrzymujemy adres IP.

Struktura komunikatu ARP

Rodzaj sprzętu (2 bajty)	**Rodzaj protokołu** (2 bajty)	**Rozmiar adresu MAC** (1 bajt)	**Rozmiar adresu protokołu** (1 bajt)	**Rodzaj operacji** (2 bajty)
Adres MAC stacji nadawczej (6 bajtów)	**Adres IP stacji nadawczej** (4 bajty)	**Adres MAC stacji odbiorczej** (6 bajtów)	**Adres IP stacji odbiorczej** (4 bajty)	

Poszczególne pola oznaczają:

Rodzaj sprzętu – definiuje rodzaj adresu używanego przez sprzęt. Dla Ethernetu wartość 1.

Rodzaj protokołu – określa protokół sieciowy, którego adresy są mapowane z adresami sprzętowymi przy użyciu protokołu ARP. Dla protokołu IP wartość tego pola wynosi: 0x0800

Rozmiar adresu MAC – określa rozmiar adresu sprzętowego (MAC) znajdowanego przez protokół ARP na podstawie adresu protokołu sieciowego. Dla sieci Ethernet wartość: 6

Rozmiar adresu protokołu – określa rozmiar adresu protokołu sieciowego na odstawie, którego protokół ARP znajduje adres sprzętowy. Dla sieci z protokołem IPv4 wartość: 4.

Rodzaj operacji – informacja czy dany komunikat jest zapytaniem ARP (wartość 1), odpowiedzią ARP (wartość 2), zapytaniem RARP (wartość 3), odpowiedzią RARP (wartość 4).

Adres MAC stacji nadawczej – adres sprzętowy komputera wysyłającego dany komunikat. W przypadku odpowiedzi to pole zawiera znaleziony adres MAC.

Adres IP stacji nadawczej – adres sieciowy komputera wysyłającego dany komunikat.

Adres MAC stacji odbiorczej – adres sprzętowy komputera dla którego przeznaczone jest dany komunikat. W przypadku zapytania ARP w tym polu umieszczane są zera.

Adres IP stacji odbiorczej – adres IP komputera, dla którego przeznaczony jest dany komunikat. W przypadku zapytania ARP pole to zawiera numer IP hosta, którego adres MAC ma być znaleziony.

2. Plan wykonania ćwiczenia

1. Zapoznać się z programem Anasil służącym do diagnostyki sieci komputerowych.
2. Przy użyciu programu Anasil przeanalizować pakiety związane w wymianą informacji generowanych poprzez rozkaz „ping”.
3. Przy użyciu programu Anasil przeanalizować pakiety związane w wymianą informacji generowanych poprzez rozkaz „tracert”.
4. Zaobserwować proces fragmentacji pakietu IP poprzez wysłanie pakietów IP z MTU większym niż 1500.
5. Zarejestrować komunikaty protokołu ARP wymieniane w czasie nawiązywania połączenia pomiędzy dwoma komputerami. W pierwszej kolejności należy usunąć z komputera obecną tablicę wpisów ARP – zastosować rozkaz „ arp –d * ”. Wykonać rozkaz „ping” do danego komputera.
6. Prześledzić wymianę segmentów TCP przy korzystaniu z usług WWW.
7. Napisać sprawozdanie zawierające fragmenty zarejestrowanych danych. Opisać ważniejsze pola i ich wartości w poszczególnych datagramach.

3. Literatura.

1. **TCP/IP. Biblia, Rob Scrimger, Paul LaSalle, Clay Leitzke, Mridula Parihar, Meeta Gupta, Tłumaczenie: Adam Jarczyk, Wydawnictwo Helion 2002.**
2. **Badanie protokołów rodziny TCP/IP, dr inż. Andrzej Zankiewicz.**
3. **TCP/IP dla każdego, Autor: Brian Komar, Tłumaczenie: Paweł Koronkiewicz, Wydawnictwo Helion 2002.**
4. **Akademia sieci Cisco. CCNA semestry 1 & 2 Wydawnictwo MIKOM 2003r.**