**Warstwa sieciowa.**

**1. Zadania:**

-znalezienie (najlepszej) drogi łączącej 2 hosty, które mogą się znajdować w oddzielnych sieciach lokalnych;

-zapewnienie adresacji logicznej;

-enkapsulacja i dekapsulacja pakietów.

**2.ICMP:**

-protokół IP nie sprawdza czy dane dotarły do adresata (jest zawodny);

-sprawdzanie, czy pakiety docierają do adresata pełnią protokoły wyższych warstw;

-protokół ICMP zajmuje się w ramach warstwy sieciowej sprawdzaniem dostępności sieci docelowej;

-zadaniem ICMP nie jest rozwiązywanie problemów z zawodnością IP, ale zgłaszanie braku łączności;

-protokół ICMP jest nieodzowną częścią IP i musi być realizowany przez każdą implementację IP;

-protokół ten został zdefiniowany w dokumencie RFC 792.

**3. Komunikaty ICMP:**

-wysyłają zwykle bramy lub hosty;

-przykłady wysyłanych komunikatów:

\*zbytnie obciążenie routera lub hosta – wysyłany jest komunikat ICMP, że należy zwolnić prędkość przesyłania komunikatów, bo host nie nadąża je przetwarzać;

\*router lub host znajduje lepszą trasę – może wtedy wysłać do źródła komunikat o lepszej trasie;

\*pole TTL pakietu jest równe 0 – wtedy router może wysłać komunikat ICMP do źródła i odrzuca pakiet;

\*host docelowy jest nieosiągalny – wtedy ostatnia brama wysyła komunikat ICMP o niedostępności adresata i przesyła do hosta źródłowego.

**4. Komunikat ICMP:**

-typ komunikatu identyfikuje komunikat;

-kod daje dalsze informacje na temat rodzaju komunikatu;

-suma kontrolna (odnosi się tylko do komunikatu ICMP) obliczana podobnie jak suma IP;

-identyfikator i numer sekwencyjny muszą mieć wartości unikalne;

-dane zawierają dodatkowe informacje potrzebne do zapytania i/lub odpowiedzi.

**5. Trasa datagramów ICMP:**

-trasy datagramów przenoszących komunikaty ICMP są wyznaczane tak samo, jak dla datagramów przenoszących informacje użytkowników;

-nie mają one żadnych dodatkowych priorytetów czy zabezpieczeń;

-gdy komunikaty o błędach zostaną zagubione albo zniszczone, to w przeciążonej sieci komunikat o błędzie może spowodować dodatkowe przeciążenia;

-zrobiono więc wyjątek w procedurach obsługi błędów: komunikaty o błędach nie są tworzone w przypadku gdy błąd został spowodowany przez datagram IP niosący komunikat ICMP.

**6. Ping:**

-program narzędziowy ping wykorzystuje komunikaty ICMP;

-program ten wysyła komunikat ICMP z wartością pola Typ ustawioną na wartość równą 8 – prośba o wysłanie komunikatu echo;

-w odpowiedzi na ten komunikat host, do którego jest adresowany ten komunikat, może odpowiedzieć komunikatem ICMP o wartości pola Typ równej 0.

**7. IGMP:**

-protokół zarządzania grupami internetowymi IGMP ułatwia komunikację urządzeń sieciowych przy pomocy transmisji grupowych;

-działanie tego protokołu jest podobne do komunikacji przy pomocy kanałów telewizyjnych lub radiowych (lub) krótkofalarskich. Klient decyduje, do którego kanału się podłącza (jaki program go interesuje) i tylko te informacje otrzymuje, jak również do tego samego kręgu zainteresowanych stacji kieruje swoje komunikaty;

-standard tego protokołu został opublikowany w dokumencie RFC 1112 pod koniec lat 90-tych XXw.;

-działanie protokołu opiera się na transmisjach grupowych;

-pakiety wysyłane są na adres grupowy IP;

-routery wiedzą, które komputery znajdują się w grupie obsługiwanej przez daną aplikację;

-pozwala to na jednokrotne wysłanie określonych danych do wszystkich hostów z danej grupy;

-jest to działanie bardziej efektywne niż transmisje kierowane (unicasting), czy też wysyłanie poprzez adres rozgłoszeni owy (broadcasting).

**8.Działanie IGMP:**

-Host Membership Report – komunikat IGMP, który wysyłają hosty, pragnące przyłączyć się do danej grupy;

-przyłączenie się klienta do danej grupy składa się z dwóch procesów:

\*host powiadamia router o tym, że chce się przyłączyć do danej grupy;

\*host wiąże w sposób dynamiczny IP z adresem grupowym, który jest zarezerwowany dla danej aplikacji oraz zarezerwowanym adresem Ethernetowym;

-Explicit Leave – komunikat IGMP, w którym host powiadamia lokalne routery o zamiarze opuszczenia grupy.

-routery okresowo sprawdzają czy kontynuować przesyłanie pakietów na adres grupowy;

-kontrolą jest wysłanie zapytania przy użyciu adresu grupowego przeznaczonego dla wszystkich hostów (244.0.0.1);

-pakiety wysyłane pod ten zarezerwowany numer IP mają ustawione pole TTL na wartość jeden, dzięki temu nie są rozsyłane dalej przez pierwszy router;

-w odpowiedzi hosty powinny przesłać pakiet raportu z adresem takim, jaki jest zarezerwowany dla tej grupy;

-po sprawdzeniu, które z grup jeszcze istnieją, routery będą przesyłać pakiety tylko do tych grup, natomiast pakiety z adresem grupowym będą odrzucane przez router.

**9.Protokoły współpracujące z IGMP:**

-protokół IGMP obsługuje rozsyłanie grupowe wewnątrz sieci lokalnych;

-przesyłaniem pakietów grupowych pomiędzy routerami zajmują się grupowe protokoły trasowania;

-wśród najczęściej spotykanych protokołów rozsyłania grupowego działających pomiędzy routerami są:

\*PIM (protokół adresowania grupowego niezależny od protokołów – RFC 2117);

\*MOSPF (rozszerzenie protokołu OSPF o adresowanie grupowe – RFC 1584);

\*DVMRP (protokół routingu grupowego na podstawie wektorów odległości).

**10. Segmentacja sieci (2 domeny: kolizyjna i rozgłoszeniowa):**

-domena kolizyjna to fragment sieci, w której może być prowadzona 1 i tylko 1 transmisja w danej chwili. Urządzenia warstwy 2 i 3 (?);

-domena rozgłoszeniowa to fragment sieci w obrębie którego rozgłaszane jest pewne … (skutek). Przyczyna to broad. (Wysyła ramki typu broadcast, zatrzymują się one na danym routerze). Granice dom. rozgłosz. Ograniczone są przez porty routera (lub sieci wirtualnej). Ramki multicast też muszą poruszać się w całości w obrębie takiej domeny.

**11. Sieci rozgłoszeniowe** zdominowane są domeną rozgłoszeniowa. Ramki obiegają całą stację, ale dochodzą tylko tam, gdzie zdefiniowany jest adres (chyba, że jest rozgłoszeniowy).

**12.** –regenerator sygnału:

\*zwiększa rozległość sieci;

\*zwiększa rozmiar domeny kolizyjnej.

-switch:

\*zwiększa rozległość sieci;

\*zmniejsza ruch w sieci przez filtrację ramek.

**13. Protokół ARP:**

-działa w warstwie sieciowej ISO/OSI i internetowej stosu IP/TCP;

-rozwiązywanie adresu jest procesem w którym adresy IP są mapowane dynamicznie na adresy MAC;

-dzięki adresowi MAC karta sieciowa jest w stanie sprawdzić czy przekazać dane do wyższej warstwy, w celu dalszego przetworzenia;

-podczas przygotowania pakietu do wysłania przez warstwę IP, dodawany jest źródłowy i docelowy adres MAC;

-protokół ARP zamyka komunikację wew. danego segmentu (jest używany tylko między komputerami wewnątrz jednej sieci).

**14. Pamięć podręczna ARP (zasada działania ARP):**

**a)**Host A ma do wysłania pakiet. Wysyła więc rozgłoszenie w domenie rozgłoszeniowej z żądaniem uzyskania adresu MAC od komputera z określonym adresem IP. Hosty inne niż C po odczytaniu żądania ignorują go.

**b)**Host C (ten z poprawnym IP) dodaje do własnej pamięci podręcznej adres MAC komputera inicjującego żądanie. Następnie odpowiada (bo zna adresy) wysyłając swój adres MAC.

**c)**Host A po odebraniu odp. ARP aktualizuje pamięć podręczną ARP nowymi informacjami. Pakiet zostaje wysłany na MAC adres uzyskany w ten sposób.

**d)**Jeśli pakiet adresowany jest do innego segmentu, czyli w części sieci posiada inny adres…