Pomiary pasywne polegają na obserwowaniu pakietów danych w określonych punktach pomiarowych oraz analizie otrzymanych wyników

sniffer – program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i analizowanie danych przepływających w sieci.

Sniffery – wykorzystywane są do analizowania ruchu w sieci przez administratorów jak i hakerów z tego powodu podczas pracy w sieci nie wolno bez powodu uruchamiać tego typu programów. Administrator sieci o wykryciu uruchomionego sniffera na komputerze może potraktować użytkownika jako potencjalnego intruza i odłączyć jego komputer od sieci.

Wireshark – popularny program typu sniffer. Jest dostępny w wersji na platformę Windows Linux i MacOS

8

Rodzaje testów i pomiarów aktywnych

Pomiary aktywne polegają na inicjowaniu ruchu sieci tzw. Pakietów pomiarowych. Wprowadzone są do sieci dodatkowe dane, które ułatwiają wykonywanie pomiarów lub diagnozowanie sieci.

Pomiary aktywne pozwalają na określenie jakości usług sieciowych QoS – quality of service

QoS określa poziom gwarantowanych wartości parametrów sieciowych w celu osiągnięcia satysfakcji użytkownika

Szafy typu rack:

- 19”

- 23”

- 10”

- 24”

1U – 1 ¾ cala

Funkcje urządzeń sieciowych:

1. Zabezpieczenia portów
2. Obsługa sieci VLAN

Lekcja

Temat: Metody i zasady pomiaru okablowania strukturalnego

1. Urządzenia do sprawdzania instalacji:
   * tester prosty – tester sieci LAN służy do pomiaru ciągłości okablowania sieci LAN i sieci telefonicznych. Pozwala na wykrycie błędnych połączeń złączki, zwarć oraz przerw. Przy jego pomocy można testować połączenia wykonane skrętką UTP, FTP zakończonych wtykami RJ45 (8P8C). Oraz przewodem telefonicznym zakończonym złączem RJ11. Tester składa się z dwóch części: zasadniczej i końcówki montowanych na dwóch końcach testowanej skrętki
   * Tester sieci z szukaczem par – Tester MT-7059 jest uniwersalnym przyrządem, która umożliwia: sprawdzanie poprawności połączeń przewodów opartych o skrętkę komputerową zakończonym złączem RJ45. Sprawdzanie poprawności połączeń przewodów oparty o wtyk RJ11 i 12, sprawdzanie poprawności BNC oraz sprawdzanie poprawności połączeń opartych o złącza USB
   * Tester sieci z mapą połączeń – tester sieci internetowej UTP/STP. Urządzenie wyposażone jest w wyświetlacz LCD. Pozwala na sprawdzenie wiązki przewodów

obsługa QoS (jakości)

stosowanie zaawansowanych zasad zapewniających bezpieczeństwo ruchu w sieci (Access Control List)

Lekcja

Temat: Komunikacja w sieci

1. Użytkownicy i urządzenia w sieci komputerowej komunikują się ze sobą i wymieniają informacje. Wymiana informacji musi przebiegać w ściśle określony sposób, umożliwiający przesyłanie danych. Każde z komunikacyjnych się urządzeń musi przestrzegać pewnych ustalonych zasad i reguł postępowania. Zbiór zasad i norm, których muszą przestrzegać komunikujące się ze sobą urządzenia jest nazywany protokołem komunikacyjnym. Komunikacja między urządzeniami może przebiegać w trybie połączeniowym (connection oriented) lub bezpołączeniowym (connetcionless oriented)
2. Tryb połączeniowy – polega na ustanowieniu logicznego połączenia pomiędzy dwoma komunikującymi się ze sobą urządzeniami. Aby rozpocząć komunikację należy najpierw nawiązać połączenie. Z trybu połączeniowego korzysta się wtedy, gdy
3. Tryb bezpołączeniowy – w trybie bezpołączeniowym komunikaty przekazywane są niezależnie np. przy przekazywaniu wiadomości za pomocą poczty elektronicznej. W komunikacji biorą udział przynajmniej dwa urządzenia.
4. Tryb jednostkowy – jeżeli jedno urządzenie wysyła dane do dokładnie jednego urządzenia to taki tryb transmisji nazywamy jednostkowym (unicast). W sieciach rozwiązane jest to w ten sposób, że każde urządzenie posiada swój unikatowy adres. Dane wysyłane przez nadawcę docierają do wielu urządzeń ale odbierane są tylko przez to urządzenie którego adres jest adresem docelowy (pozostałe urządzenia ignorują dane które nie są przeznaczone dla nich)
5. Tryb rozgłoszeniowy – urządzenie nadawcze możę wysyłać informacje do wszystkich urządzeń. W takim przypadku adresem docelowym jest specjalny adres naywany rozgłoszeniowym (broadcast). Urządzenia traktują transmisję na adres rozgłoszeniowy tak, jakby były adresowane na ich adres jednostkowy.
6. Tryb grupowy – w rozgłaszaniu grupowym (multicast) dane przeznczone są tylko dla wybranej grupy urządzeń. Adres docelowy jest specjalnym adresem, określającym wybrane urządzenia z dane j sieci. W transmisji grupowej unika się wielokrotnego wysyłania tego samego komunikatu do wielu nadawców po każdym łączu sieciowym informacja jest przekazywana jednokrotnie.
7. Transmisja jednokierunkowa

Transmisja w której odbiornik nie może przesłać odpowiedzi ani innych danych. Przykładem takiego typu transmisji jest emisja audycji radiowych, gdzie słuchacz przy odbiorniku radiowym może tylko odbierać informacje pochodzące z nadajnika. Tego typu transmisje nie są stosowane w sieciach komputerowych.

1. Półduplex (half-duplex)

Transmisja dwukierunkowa, naprzemienna. W danym momencie jest ustalony tylko jeden kierunek transmisji, a urządzenie może albo nadawać, albo odbierać informacje. Do odwrócenia kierunku transmisji jest potrzebny system sygnalizacji, wskazujący, że urządzenie ukończyło nadawanie i może odbierać informacje.

1. Duplex (full-duplex)

To transmisja jednoczesna i dwukierunkowa. Wymaga zazwyczaj dwóch par przewodów dla sieci cyfrowych. Dla połączeń analogowych dla jednej pary przewodów szerokość pasma jest dzielona na dwie części.

1. Działanie usług i aplikacji

Niektóre usługi sieciowe takie jak poczta elektroniczna, transfer plików pobieranie stron internetowych itp., wymagają niezawodnego przesyłania danych Nadawca i odbiorca komunikują się miedzy sobą, aby się upewnić że wszystkie dane dotarły bez błędów i w odpowiedniej kolejności. W przypadku błędów protokoły te żądają retransmisji uszkodzonych lub zagubionych danych. Dla tych usług stosowane są protokoły zagubionych danych. Dla tych usług stosowane są protokoły zapewniające niezawodny transport danych.

Inne usługi takie jak przesyłanie dźwięku bul obrazu na żywo tolerują utratę pewnej ilości danych, W ich przypadku niewielkie zakłócenia spowodowane brakiem części danych są mniej uciążliwe dla odbiorcę niż przerwy w odtwarzaniu spowodowane retransmisją.

W tym przypadku stosowane są protokoły zawodnego transferu danych. Nie oznacza to, że dane nie dotrą do miejsca przeznaczenia, lecz tylko to że protokoły nie gwarantują nie bezbłędnego dostarczenia danych.

Aby działać bez zakłóceń, niektóre aplikacje muszą być w stanie transmitować lub odbierać dane z określoną prędkością, Na przykład aplikacja odtwarzająca pliki multimedialne musi odbierać taką ilość danych która jest niezbędna do wyświetlenia filmu lub odtworzenia muzyki. Aplikacja taka wymaga określonej przepustowości, Leżeli warunek ten nie będzie spełniony to aplikacja nie będzie działała prawidłowo (lub w ogóle nie uruchomi) albo będzie zmuszona pracować przy innych parametrach np., niższej rozdzielczości obrazu lub jakości dźwięku.

1. Czas i opóźnienia

Istnieje pewna grupa aplikacji pracujących w ez, czasie rzeczywistym, które dopuszczają niewielkie czasy opóźnienia przesyłąnych danych. Przykładem może być telekonferencj, w której opóźnienia w transmisji dancy hpowodująprzerwy w rozmowie. W grach sieciowych czas między wykonaniem czynności, np. kliknięciem musząm a rekcją na to zdarzenie musi być krótki, avy zapenić płynność gry.

1. Protokoły

Protokoły internetowe to podzbiór protokołów komunikacyjnych stosowanych w sieci internet, Komuptery w internecie komunikują się ze sobąza pomocą protokołu IP (internet protocol), działającego w warstwie sieciowej i TCP (Transmission Control Protocol) lub UDP(User Datageam Protocol), działających w warsrwie tranprotowej. Inne protokoły , takie jak http (Hypertext Transfer Protocol) są wykorzystywane w warstwie aplikacji

Rodzaje s

Wyróżniamy dwa typy podstawowe rodzaje sieci:

* Sieci równorzędne
* W sieciach o architekturze równorzędnej każdy komputer może być klientem (korzystać z usług oferowanych przez inne urządzenia) serwerem udostępniać usługi lub być jednocześnie klientem i serwerem. Wszystkie urządzenia w sieci mają taki sam priorytet – żadne z nich nie hest podporządkowany.
* Sieć p2p charakteryzuję się zmiennością struktury węzłów sieci która spowodowana jest zmiennością liczby i lokalizacji sieciowej aktualnie aktywnych hostów
* Zmienna struktura sieci p2p uzależniona od liczby podłączonych użytkowników niesie ze sobą ryzyko odcięcia od sieci w momencie gdy wszyscy „sąsiedzi” rozłączą się w tym samym czasie
* Ze względu na zachowanie się węzłów po utracie „sąsiada” można wydzielić dwa modele sieci:

- model pasywny – sieci nie podejmuje żadnych działań

- model aktywny – sieć próbuje zastąpić utracone połączenie nowym, wybieranym w oparciu o specjalne protokoły

* Najpopularniejsze sieci P2P służą do współdzielenia plików w Internecie, Można wyróżnić dwie odmiany:

- sieci bez centralnego serwera które nie mają centralnej bazy o zasobach

- sieci z centralnymi serwerami które przechowują informacje o użytkownikach podłączonych w danej chwili do sieci oraz w niektórych wypadkach o udostępnianych zasobach

* Sieci wyposażone w centralny serwer są znacznie bardziej efektywne, gdyż nowy użytkownik podłączający się do sieci otrzymuje na wstępie listę wszystkich użytkowników podłączonych do danego serwera ma także dostęp (najczęściej) do indeksu dostępnych plików, który może błyskawicznie przeszukać.
* Centralne serwery oferują czasami także dodatkowe usługi jak np. czat czy system przesyłania wiadomości
* Sieci klient – serwer:

Przykładami sieci typu klient -serwer jest Novell Netware lub Windows Serwer

W każdej z tych sieci do przechowywania informacji o obiektach np. użytkownikach, udostępnianych zasadach, uprawnieniach, służy usługa katalogowa.

W przypadku sieci NetWare usługa ta nazywana jest eDirectory lub we wcześniejszych wersjach Novell Directory Services (NDS). Usługa katalogowa w środowisku Windows nosi nazwę Active Directory.

Zalety sieci klient -serwer:

* sieci klient – serwer są dużo bardziej bezpieczne niż sieci peer-to-peer
* Serwer przetwarza wszystkie żądania przez co stacje robocze są odciążone
* Administrowanie siecią z jednego miejsca
* Bezpieczeństwo sieci

Wady sieci klient – serwer:

* Wysokie koszty budowy oraz eksploatacji (serwer, oprogramowanie, administrator)
* Awaria głównego komputera jakim jest serwer unieruchomi całą sieć

Lekcja

Temat: Model warstwowy ISO/OSI

1. Po co stworzono model warstwowy sieci:
   1. Ponieważ protokoły mogą być skomplikowane, nadaje się im strukturę warstwową
   2. Został stworzony w celu umożliwienia tworzenia urządzeń zdolnych do komunikacji między sobą
   3. Ze względu na ustandaryzowanie elementów sieci
   4. Z myślą o inżynierach administratorach i użytkownikach
2. Model odniesienia OSI jest traktowany jako wzorzec transmisji danych dla protokołów komunikacyjnych w sieciach komputerowych. Podstawowym założeniem modelu jest podział systemów sieciowych na 7 warstw, współpracujących ze sobą w ściśle określony sposób.

Został o przyjęty przez międzynarodową Organizację Standaryzującą ISO w 1984 roku

1. Model sieci ISO/OSI (aplikacji, to tam gdzie my):
   1. Aplikacji (7):
      1. Zapewnia dostęp do sieci aplikacjom użytkownika.
      2. Zajmuje się specyfikacją interfejsu użytkownika.
      3. Świadczy usługi końcowe dla aplikacji
   2. Prezentacji (6):
      1. Obsługuje znaki narodowe, formaty graficzne.
      2. Odpowiada za szyfrowanie i kompresję

GATEWAY – BRAMA

* 1. Sesji (5):
     1. Zapewnia komunikację między różnymi systemami.
     2. Zarządza sesjami transmisyjnymi.
  2. Transportowa (4):
     1. Zapewnia połączenie między aplikacjami na różnych systemach
     2. Kontroluje poprawność przesyłanych danych.
     3. Dzieli dane na segmenty,
  3. Sieciowa (3) - router:
     1. Ustanawia, utrzymuje i rozłącza połączenie sieciowe.
     2. Obsługuje routing i adresację logiczną.
     3. Dzieli na pakiety.
     4. Jako jedyna posiada informacje na temat fizycznej topologii sieci.
     5. Tutaj dostajemy adres IP.
  4. Łącza danych (2) – MAC (bridge itp.):
     1. Nadzoruje warstwę fizyczną
     2. Dba o poprawność danych.
     3. Zapewnia łączność między dwoma bezpośrednio połączonymi urządzeniami.
     4. Dzieli na ramki. Zapisuje dane w postaci bitowej.
     5. Logical Link Control (LLC) – kontroluje poprawność przesyłania ramek
  5. Fizyczna (1) - medium:
     1. Odbiera dane i przesyła je jako sygnał fizyczny – reprezentowane w skonkretyzowany sposób

1. Na przykładzie komunikacji mailowej:
   1. Sporządzenie maila w programie pocztowym
   2. Zamiana wiadomość na uniwersalny strumień danych
   3. Ukierunkowane strumienia wysyłki
   4. Podział strumienia na segmenty i nadanie każdemu z nich nagłówku
   5. Podział segmentu na pakiety i przypisanie nagłówka z adresami IP
   6. Podział segmentów na ramki i przypisanie nagłówka z adresami fizycznymi (MAC) i stopki zawierającej sumę kontrolną. Zapis ramek w postaci bitowej.
   7. Zamiana bitów na sygnał i transport do adresata
2. Proces podziału strumienia danych na jednostki danych i opatrywania ich nagłówkami nazywany jest enkapsulacją.
3. Podsumowanie:
   1. Pozwala podzielić zadanie sieciowe na łatwiejsze do analizy części
   2. Umożliwia łatwiejsze zastępowanie z jednego rozwiązania innym bez konieczności wprowadzania zmian w innych warstwach
   3. Wprowadza niezależność poszczególnych rodzajów nośników danych wykorzystywanych w sieciach – jedne zastępują (bądź uzupełniają) drugie

HISSSS

INKWIZYCJA TEMAT 15 – OGLNIE NIE TYLKO HISZPAŃSKA

Lekcja

Temat: Model TCP/IP

* 1. Oprócz modelu OSI istnieją także inne modele sieci z których najpopularniejszy stos protokołów TCP/IP, powstał na zamówienie Departamenty Obrony USA (stąd druga nazwa to stos DOD)
  2. Warstwa aplikacji – obejmuje funkcje trzech najwyższych warstw modelu OSI (aplikacji, prezentacji, sesji). Użytkownicy uruchamiają programy, które uzyskują dostęp do usług za pośrednictwem protokołu na poziomie warstwy transportu i wysyłają lub odbierają dane w postaci pojedynczych komunikatów lub rumienia bajtów. Programy użytkowe przekazują do warstwy transportowej dane w wymaganym formacie aby mogły one zostać dostarczone w odpowiednie miejsce.

W warstwie tej działa wiele protokołów aplikacji.

* 1. Podstawowym zadaniem warstwy transportowej jest zapewnienie komunikacji między programami użytkownika. Warstwa ta może zarządzać przepływem informacji oraz zapewniać niezawodność przesyłania przez porządkowanie segmentów danych i retransmisję uszkodzonych lub zagubionych segmentów.

W komputerze może działać wiele aplikacji wymieniających dane w sieci pry wykorzystaniu portów określonych dla każdego połączenia i nie nastąpi wymieszanie się przesyłanych przez nie danych.

* 1. Warstwa internetowa przyjmuje segmenty z warstwy transportowej razem z informacjami identyfikującymi odbiorcę. Zadaniem jej jest wysyłanie pakietów i dostarczenie ich do miejsca przeznaczenia niezależnie od trasy po której będą przesyłane, niezależnie od trasy, po której będą przesyłane. Protokołem zarządzającym tą warstwą jest protokół IP

Warstwa dzieli dane na pakiety dodając nagłówek zawierający między innymi adres IP nadawcy i odbiorcy

Proces ten jest określany jako rooting

* 1. Warstwa dostępu do sieci odbiera pakiety IP i przesyła je przez daną sieć

Zapewnia interfejs z siecią fizyczną i zajmuje się przekazywaniem danych rzez fizyczne połączenia między urządzeniami sieciowymi,

Najczęściej są to karty sieciowe lub modemy

Formatuje dane do transmisji przez nośnik oraz adresuje dane do podsieci opierając się na adresach fizycznych

Zapewnia sprawdzanie błędów przesyłu danych za pomocą sumy kontrolnej ramki.

* 1. Porównanie modelu OSI i TCP/IP:
     1. aplikacji = aplikacji, prezentacji, sesji:
* http, DNS, DHCP, FTP
  + 1. transportowa = transportowa:
* TCP, UTP
  + 1. Internetu = sieciowa:
* IP, ICMP, IGMP, RIP, OSPF, BGP
  + 1. dostępu do sieci = łącza danych, fizyczna:
* BLUETOOTH, ETHERNET, DSL, ISDN, 802.11 WIFI
  1. Do ustalenia adresu MAC jest wykorzystywany protokół ARP. Gdy komputer chce skorzystać z protokoły ARP przygotowuje specjalny pakiet zapytania ARP, który jest wysyłany na adres rozgłoszeniowy dzięki czemu dociera do wszystkich urządzeń w sieci lokalnej.

Urządzenie o szukanym adresie sieciowym odpowiada przesyłając pakiet z odpowiednią zawierającą adres sprzętowy MAC. Komputer dysponuje już wszystkimi adresami i może przygotować ramkę. Aby uniknąć konieczności wysyłania kolejnego zapytania ARP, komputer zapisuje sobie w specjalnej tablicy informację o adresach urządzeń z którymi się komunikował.

Przed następnym wysłaniem zapytania ARP sprawdzi w tablicy, czy nie ma zapisanego poszukiwanego adresu. Komputery mogą się ze sobą komunikować za pośrednictwem adresy fizycznego tylko w obrębie danej sieci (w warstwie drugiej modelu OSI) Jeśli jakieś informacje moją być przesłane do innej sieci to protokół ARP jest wykorzystywany do uzyskania informacji o adresie bramy sieciowej.

* 1. Mechanizmy odwzorowania adresów przez wymianę komunikatów z wykorzystaniem protokoły ARP przebiega następująco:
     1. Komputer A, który chce wysłać pakiet z danymi sprawdza czy w jego tablicy ARP jest szukany adres IP komputera B, jeśli taki adres jest w tablicy to wykonywany jest punkt 5. Jeśli nie to punkt 2
     2. Komputer A, który chce wysłać pakiet z danymi wysyła najpierw zapytanie ARP do wszystkich komputerów w sieci w którym pyta: Kto na potrzebny mi adres IP?
     3. Komputer B, który pozytywnie odpowiada na to pytanie dopisuje do swojej tablicy ARP adres IP i MAC komputera A i odsyła odpowiedź ze swoim adresem MAC
     4. Komputer A który wysłał zapytanie w pkt 1, odbiera odpowiedź, dopisuje adres IP i MAC komputera B do swojej tablicy ARP
     5. Komputer A, wysyła pakiet IP z danymi do komputera B
  2. Zawartość tablicy ARP komputera, który komunikował się z innymi urządzeniami

Protokół odwrotny RARP (reverse address resolution protocol)

Arp -a

PPP

Lekcja

Temat: Biznesplan – plan działania przedsiębiorstwa

* + 1. Czym jest bizneslan?
    2. Zasady sporządzania biznesplnu
    3. Jak napisać biznesplan? – elementy biznesplanu
    4. Uproszczony biznesplan – str. 145

Lekcja

Temat: Protokoły warstwy łącza danych

1. Druga warstwa modelu ISO/OSI
2. 1 ramka zapakowuje 1 datagram z wyższej warstwy (kapsulacja)
3. Uwzględnia:
   1. Detekcję błędów
   2. Retransmisję
   3. Kontrola przepływu
   4. Losowy dostęp
4. Stadard Ethernet IEEE 802.3:
   1. Podstawowym standardem wykorzystywanym w budowie sieci lokalnych Ethernet  
      podstawowe kategorie Ethernet:
      1. 10Mb/s
      2. 100Mb/s
      3. 1Gb/s
5. Przemieszczanie segmentów – warstwy jedna po drugiej
6. 1 datagram może być przetwarzany przez różne protokoły
7. TCP/IP:
   1. Aplikacji- http, DNS, DHCP, FTP
   2. Trasportowa – TCP, UDP
   3. Internet – Ipv4, IPv6, ICMP
8. Ramkowanie -dane przesyłane w sieci Ethernet są podzielane na fragmenty nazywane ramkami.
9. Ramka:
   1. Preambuła – 7 bajtów złożnoych z naprzemiennych jedynek i zer pozwalający na szybka synchronizację odbiorników
   2. SFD – znacznik początkowy
   3. Adres MAC odbiorcy (6 bajtów)
   4. Adres MAC nadawcy (6 bajtów)  
      **adres MAC ma 48 bitów (czyli 6BAJTÓW)**
   5. Typ ramki / długość (2 bajty) – jeżeli jego wartość jest mniejsza niż 1500 to oznacza długość ramki, jeżeli większa – typ pakietu
   6. Przesyłane Dane (46-1500 bajtów) – jeżeli dane są mniejsze od 46 bajtów to są uzupełniane ramkami
   7. Suma kontrolna FCS (frame check sequences) – pozwala na wykrycie błędów transmisji (4 bajty)
10. Standard Ethernet:
    1. W sieci Ethernet każda stacja widzi wszystkie przepływające ramki danych i sprawdza czy przepływająca ramka nie jest adresowana do niej. Sprawdzenie ramki polega na porównaniu adresu MAC karty sieciowej i adresu zapisanego w polu „adres MAC odbiorcy”. Jeżeli adresy są identyczne to ramka jest odbierana w innym przypadku ramka i jest odrzucana
    2. Model przesyłania danych składa się z:
       1. Prędkość przesyłania danych wyrażona w Mb/s np. 10, 100, 1000
       2. Rodzaj transmisji:
          1. Base – transmisja w paśmie podstawowym (baseband)
          2. Broad – transmisja przy wykorzystaniu częstotliwości nośnej (broadband)
    3. Rodzaj astosowanego medium:
       1. 2 – cienki kabel koncentryczny (thin Ethernet)
       2. 5 – gruby Ethernet (thick Ethernet)
       3. T – skrętka
       4. F – światłowód
11. Koncentrator:
    1. CSMA/CD- protokół odpowiedzialny za unikanie kolizji
    2. Tworzy domeny kolizyjne (od koncetratora włącznie w dół)
    3. Domeny kolizyjne:  
       Urządzenia sieciowe pierwszej warstwy modelu OSI retransmitują sygnał do wszystkich portów, z wyjątkiem tego, za którego pomocą otrzymały sygnał. Wszystkie urządzenia otrzymują sygnał i rywalizują o dostęp do nośnika. Na skutek jednoczesnej transmisji przez dwa lub więcej urządzeń za pomocą współdzielonego medium transmisyjnego może dojść do kolizji. (max.1024 użądzenia)
12. Przełącznik:
    1. Switch ma tablicę par adres MAC-port w której zapamiętuje adresy źródłowe wyciągnięte z ramek. Jeśli docelowy adres MAC nie jest zapisany, ramka jest wysyłana na wszystkie porty (oprócz źródłowego) pod adres rozgłoszeniowy (ff-ff-ff-ff-ff-ff). Przestarzałe adresy są usuwane.  
       Urządzenia połączone switchem są w jednej domenie rozgłoszeniowej, ponieważ wiadomość wysyłana pod adres rozgłoszeniowy MAC trafi do każdego z nich. Natomiast switch separuje domeny kolizyjne, ponieważ switch nie stanowi jednego segmentu sieci (jednego pasma transmisyjnego) i nie zachodzą na nim kolizje.
    2. Domena rozgłoszeniowa jest tworzona od switcha w dół (włącznie)
    3. Switch też może rodzielić sieci rozgłoszeniowe poprzez vlan
13. Protokoły w warstwie sieci
    1. IPv4
    2. IPv6
    3. Novell IPX
    4. AppleTalk
    5. CLNS?DECNet
14. Protokół IP:
    1. Odpowiedzialny za przesyłanie pakietów użytkownika sieci niezależnie od używanego medium transmisyjnego
    2. Jest protokołem bezpołączeniowym – przed wysłaniem danych nie jest zestawiane żadne połączenie co oznacza że w trakcie transmisji nie sprawdza się poprawności pakietów przesłanych przez sieć nie ma zatem gwarancji ich dostarczenia ponieważ mogą zostać one po drodze zagubione
    3. Podstawowe funkcje:
       1. Określanie i tworzenie struktury pakietu
       2. Określenie schematu adresowania logicznego IP
       3. Kierowanie ruchem pakietów w sieci
    4. Budowa ramki:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 bajt | | | 2 bajt | 3 bajt | | 4 bajt | |
| Wersja | Długość nagłówka | | Typ usługi | Całkowita długość pakietu (16bit) | | | |
| Identyfikacja | | | | Flagi | Przesunięcie fragmentu | | |
| Czas życia TTL | | Protokół | | Suma kontrolna | | | |
| Adres źródłowy | | | | | | | |
| Adres docelowy | | | | | | | |
| Opcje | | | | | | | Uzupełnienie |
| Dane | | | | | | | |

Przesunięcie fragmentu (13 bitów) – używany do odpowiedniego poukładania pakietów; żeby miały taki sam układ przed fragmentacją

Czas życia TTL (8 bitów) – każde przejście przez router to zmniejszenie o 1; określa maksymalną ilość przeskoków (255 routerów); żeby pakiety nie krążyły bez końca

Protokół (8 bitów) – odpowiada za przekazanie do odpowiedniego protokołu pakietu

Suma kontrolna – sprawdza czy wszystkie dane zostały przetransmitowane

Adres źródłowy/Adres docelowy (po 4B=32b na sztukę)

Opcje – miejsce do obsługi innych usług

Uzupełnienie – uzupełnienie zerami

* 1. Warstwa sieciowa   
     odpowiada za wybranie optymalnej trasy, po jakiej będzie przesyłany każdy pakiet. Jeżeli odbiorca znajduje się w tej samej sieci, pakiet będzie wysłany bezpośrednio do niego. W przeciwnym razie musi być przekazany do bramy łączącej sieci.

Decyzje o wyborze trasy podejmuje router na podstawie adresu IP urządzenia docelowego, umieszczonego w nagłówku pakietu oraz na podstawie informacji posiadanych w tablic routingu.

* 1. Tablica routingu
  2. Protokoły routingu

Informacje o trasach w tablicac routingu mogą być wprowadzane statycznie przez administratora. Routery mogą również uczyć się tras w sposób dynamiczny:

* + 1. RIP (Routing Information Protocol):
    2. Opierając się na protocole RIP routery podejmują astępujące działania:
       1. Żądają aktualnych informacji o routingu od innych routerów i na ich podstawie aktualizują swoją tablicę routingu
       2. Odpowiadają a podobne ządanie innych routerów
       3. W ściśle określonych przedziałach czasu rozsyłają informacje o swojej obecności, inforując inne routery o aktualnej konfiguracji połączeń międzysieciowych
       4. W przypadku wykrycia zmian w konfiguracji sieci rozsyłają stosowną informację
    3. Uaktualnienie routingu:
       1. Protokół RIP wysyła komunikaty uaktualniające w określonych, stałych przedziałach czasu, na przykład co 30s, lub w przypadku pojawienia się zmian w topologii sieci. Router po przyjęciu uaktualnionego routingu, które dotyczy zmian jednego z wejść, uaktualnia tablicę routingu (routing table) by odzwierciedlić nową trasę. Wartość miary przypisanej danej ścieżce wzrasta o jeden i jako następny skok jest wskazany nadawca. Routery RIP utrzymują do miejsca przeznaczenia tylko najlepszą trasę, to jest trasę z najmniejszą liczbą skoków. Router niezwłocznie po uaktualnieniu swojej tablicy routingu wysyła informacje o zmianie do pozostałych routerów w sieci. Są one wysyłane niezależnie od regularnie wysyłanych uaktualnień.
       2. Miara routingu protokołu RIP – jedyną miarą używaną przez protokół RIP do mierzenia odległości pomiędzy źródłem a miejscem przeznaczenia jest zliczanie skoków (hop-count) Każdemy skokowi na drodze od źródła do miejsca przeznaczenia zostaje przypisana wartość, najczęściej 1
       3. Gdy router przyjmie uaktualnienie tablicy routingu, które zawiera nowe lub zmienione wejście sieciowego miejsca przeznaczenia to dodaje jedynkę do wartości miary wskazanej w uaktualnieniu i wpisuje zmianę do tablicy routingu. Adresem następnego skoku jest adres IP nadawcy.
       4. Protokół RIP, dzięki ograniczeniu liczby skoków, które mogą pojawić się pomiędzy źródłem a miejscem przeznaczenia, zapobiega przesyłaniu strumienia danych bez końca w pętli. Maksymalna liczba skoków na ścieżce wynosi 15. Jeśli router przyjmie uaktualnienie
       5. Stabilność protokołu RIP

W celu dostosowania się do szybkich zmian topologii sieci protokół RIP wyposażono, podobnie jak i inne protokoły routingujące, w mechanizmy stabilizujące. Na przykład, by zapobiec skutkom błędnej informacji o routingu, w protokole RIP zaimplementowano mechanizmy split-horizon i hold-down. Powstaniu pętli zapobiega ograniczenie – na trasie pomiędzy źródłem a miejscem przeznaczenia – liczby skoków (do 15)

* + - 1. Czasomierze protokołu RIP
      2. W celu dostosowania do potrzeb wydajności routingu, protokół RIP wyposażono w kilka czasomierzy (timers). Wśród nich są:
         1. Czasomierz uaktualnienia routingu (routing-upgrade timer)
         2. Limitu czasu trasy (route time timer)
         3. Czasomierz uaktualnienia routingu wyznacza przedziały czasu pomiędzy kolejnymi okresami ualtualnienia , Lest to stały przedział nie przekraczający 30s. Do każdego wejścia do tablicy routingu jest przypisany czasomierz limitu czasu trasy; w przypadku jego wyczerpania trasa zostaje oznaczona jako nieważna. Mimo tego jest nadal utrzymywania w tablicy rotingu ażdo momentu gdy zostanie wyczerpany czasomierz czyszczenia trasy
    1. OSPF (Open Shortest Path First):
       1. Jest protokołem routingu **stanu łącza** (link state), wykorzystującym **algorytm SPF** do obliczania najkrótszych ścieżek. Metryką w tym protokole jest koszt, który jest powiązany z przepustowością łączy (im większa przepustowość, tym niższy koszt)
       2. Przeznaczenie do dużych sieci, która może być podzielona na obszary. Routery wymieniają się komunikatami LSA (Link State Advertisement) i na podstawie tego każdy router zbiera informację o całej topologii obszaru, a następnie na podstawie algorytmu SPF oblicza najlepsze trasy do wszystkich sieci.
    2. IGRP(Interior-Gateway Routing Protocol) i EIGRP (następca IGRP):
       1. IGRP opracowane przez CISCO i podobne jak RIP, jest protokołem typu dystans-wektor, ale wykorzystuje jako metrykę rożne kombinacje czterech miar:
          1. Opóźnienia
          2. Szerokość pasma (przepustowości)
          3. Obciążenia
          4. Niezawodności
       2. EIGRP posiada cechy algorytmów routingu z wykorzystaniem wektora odległości i według stany łącza. Ten protokół do wyznaczenia tras stosuje algorytm DUAL (Difusing-Update Algorithm). Zalecany do stosowania przez CISCO
  1. Hierarchia routingu:
     1. AS – system autonomiczny – zbiór sieci pod wspólną administracją z ustaloną wspólną strategią routingu. Możemy podzielić na pewną liczbę obszarów (areas), które są grupami sąsiednich sieci i przyłączonych hostów. Poszczególne obszary sprzęgają routery graniczne obszaru. Router graniczny otrzymuje oddzielną dla każdego obszaru bazę danych o topologii.
  2. Routing wewnętrzny:
     1. Do niego zaliczamy protokoły:
        1. RIP
        2. OSPF
        3. IGRP
        4. EIGRP

Te protokoły mogą działać wewnątrz systemu autonomicznego. Do ustalania tras miedzy systemami autonomicznymi wykorzystywane są zewnętrzne protokoły routingu EPG czy BGP.

* 1. Rozsyłanie grupowe:
     1. Rozgłaszanie grupowe (multicasting), zasady:
        1. Gdy w sieci znaj duje się przynajmniej jeden członek konkretnej grupy multicastowej
        2. Hosty zgłaszają za pomocą IGMP swoje członkostwo w grupie multicastowej do dowolnego sąsiadującego router a multicastowego
        3. Komputery mogą być odbiorcami, nadawcami lub pełnić obie te funkcje jednocześnie w danej grupie multicastowej.
        4. Multicastowe adresy IP mieszczą się od 244.0.0.0 do 239.255.255.255

Zakres ten określa tylko grupę odbiorców nadawcy posiadają zawsze adres unicastowy.

* + - 1. Zakres adresów od 244.0.0.0 do 224.0.0.255 zarezerwowany jest dla protokołów w sieciach lokalnych i nie mogą być przekazywane przez routery.
      2. Zakres adresów od 244.0.1.0 do 238.255.255.255 jest zakresem adresów globalnych, które mogą być wykorzystywane do multicastingu między organizacjami oraz przez Internet.
      3. Przyłączanie hosta do grupy obejmuje dwa procesy:
         1. Host powiadamia router, że chce przyłączyć się do odpowiedniej grupy,
         2. Host wiąże dynamicznie IP z adresem grupowym zarezerwowanym dla danej aplikacji oraz zarezerwowanym adresem Ethernet.
  1. Protokoł IPMC
     1. Protokół IP nie gwarantuje niezawodnej transmisji danycm ake hest niezwykle ważne żęby w przpadku wystąpienia problemów nadawca otrzymał jakieś powiadomienie. To właśnie ICMP (Internet Control Message Protocol) jest mechanizmem używanym do przesyłania informacji zwrotnych o problemach z sieci, które uniemożliwiają dostarczenie pakietów do odbiorcy. Protokoły wyższych warstw, jak TCP, są w tanie rozpoznać, że pakiet dotarł do celu ale ICMP udostępnia sposoby wykrywania bardziej poważnych problemów jak wyczerpanie się wartości TTL (TTL exceed)

ICMP informuje o występujących problemach ale nie dla każdego możliwego błędu wyszczególnia środki zaradcze. Gdy pakiet spowoduje błąd, ICMP może jedynie powiadomić nadawcę o przyczynie, nadawca musi tę informację przekazać danemu programowi użytkownika albo podjąć inne działania mające na celu wyeliminowanie problemu.

* + 1. Protokół ICMP – komunikaty i kody

ICMP jest skomplikowanym protokołem. Każdy komunikat ICM określany jako major type na dodatkowo własne kody tzw, minor codes. ICMP działa w warstwie trzeciej (warstwie sieci) więc może być routowany przez Internet. Pakiet ICMP to w rzeczywustości pakiet IP przenoszący

* + 1. Najczęstsze typy komunikatów ICMP
       1. Echo Replay (typ 0) oraz echo request (typ 8) - ping
       2. Destination unreachable (3)
       3. Source quench (4)
       4. Redirect (5)
       5. Time exceeded (11)
    2. Zastosowania ICMP
       1. Ping i tracert

Lekcja

Temat: Adresowanie w sieci komputerowej

1. Typy adresów używanych w sieciach:
   1. Fizyczne – nazywane również adresami MAC (Media Access Control):

Adres fizyczny jest nadawany w każdej karcie sieciowej NIC (Network Interface Card) podczas jej wytwarzania. Adres ten jest niepowtarzalny i umieszczony w pamięci ROM kart. Długość adresu fizycznego wynosi 48 bitów, lecz jest przedstawiany w zapisie heksadecymalnym (szesnastkowym)

* 1. Logiczne – adresy IP (Internet Protocol):

Adres logiczny wskazuje punkt przyłączenia do sieci, który jest nazywany interfejsem. Adres taki może określać urządzenie, np. komputer, grupę urządzeń (adres grupowy) lub całą sieć (adres sieci).

Obecnie funkcjonują dwie wersje adresów logicznych:

* + 1. Adres IPv4:
       1. Adres IPv4 ma zawsze długość 32 bitów. /jest on podzielony na cztery 8-bitowe bloki, zwane oktetami. Administratorzy najczęściej przedstawiają adresy w postaci dziesiętnej (notacja dziesiętna z kropkami)
    2. Adres IPv6 – ma 128 - bitów

1. Klasy adresów IP:
   1. Mając do dyspozycji 32 bity można wygenerować 2^32
   2. Adresy IP ozstały podzielony na klasy A, B, C, D:
      1. Klasa A zawsze się zaczyna od 0 (pierwszy bit IP):
         1. Ma 126 sieci
         2. Może mieć 16 777 214 komputerów sieci
         3. Pierwszy oktet 1-126
      2. Klasa B zawsze zaczyna się od 10:
         1. Ilość sieci: 16 384
         2. Ilość komputerów w sieci 65 534
         3. Pierwszy oktet 128-191
      3. Klasa C zaczyna się od 110:
         1. Ilość sieci: 2 097 152
         2. Ilość komputerów w sieci: 254
         3. Pierwszy oktet 192 – 223
      4. Klasa D służy do multisesji (multicast) w sieciach IP Adres multi sesji jest niepowtarzalnym adresem sieciowym kierującym pakiety do zdefiniowanych z góry grup adresów IP. Jedna. Stacja może przesyłać strumień kierowany do wielu odbiorców jednocześnie. Przestrzeń adresowa klasy D obejmuje zakres od 224.0.0.0 do 239.255.255.255

Adresy klasy E zespół IANA (Internet Assigned Numbers Authority) zarezerwował sobie do własnych bada. Nie możne z nich korzystać w Internecie zakres prawidłowych adresów klasy E to 240.0.0.0 – 255.255.255.255

1. Adresy specjalne
2. Zakresy adresów prywatnych
3. Sposób reprezentowania adresów w sieci

Lekcja

Temat: Adresowanie bezklasowe – VLSM – maska o zmiennej długości

1. Istnieje wiele metod zapobiegania wyczerpywaniu się adresów. Należą do nich m.in.:
   1. Wykorzystanie adresów prywatnych
   2. Adresowanie bezklasowe
   3. Adresowanie IPv6
2. Adresowanie bezklasowe:
   1. W celu zapewnienia większej elastyczności w przydzielaniu adresów IP wprowadzono pojęcie maski podsieci (Subnetwork Mask), oznaczającej skrótem SM. Maska podsieci określa, ile bitów w adresie przeznaczonych jest do identyfikacji siedzi i podsieci (ID network) a ile bitów do identyfikacji hosta (ID host). Maska podsieci składa się z tej samej liczby bitów co adres IP. W masce w części sieci (ID network) i podsieci (ID subnetwork) występują same jedynki (w systemie dwójkowym) a w części hosta (ID host) same zera.
   2. Reprezentacja krótka maski podsieci, zwana również CIDR (Classless Inter-Domain Routing), informuje o ilości jedynek występujących w zapisie dwójkowym maski. Dzięki masce podsieci można wydzielić podsieci z mniejszą liczbą komputerów niż wynikałoby to z użycia pełnej klasy adresów. Aby utworzyć podsieć należy wykorzystać bity z części przeznaczonej na hosta, Jeśli zostaną wykorzystane bity z części przeznaczonej na hosta. Jeśli zostaną wykorzystane trzy bity z części przeznaczonej na hosta to otrzyma się przydział bitów na poszczególne części i wartości maski podsieci.
   3. Nef=2s-2  
      Nef – liczba efektywnych sieci
   4. Liczba możliwych hostów:  
      nh=2^h-2  
      gdzie:  
      nh – liczba hostów w podsieci  
      h – liczba bitów w części hosta
   5. Wyznaczanie

11000000.10101000.00000000.00000000

11111111.11111111.11111111.11100000

192.168.

Lekcja

Temat: Adresowanie IPv6

1. Co to jest IPv6?
   1. Mechanizm przekazywania pakietów danych w Internecie
   2. Nowa wersja powszechnie używanego dziś w Internecie Pv4
2. Adresowanie IPv6 wprowadzono ze względu na wyczerpanie się dostępnej puli adresów IPv4. Adresy IPv6 mają długość 128 bitów, co pozwala na uzyskanie 2^128 adresów  
   Protokół obsługuje zarówno konfigurację adresów przy wykorzystaniu serwera DHCP jak i bez tego serwera. Do IPv6 dodano nową wersję protokołu dynamicznej konfiguracji hostów DHCPv6 (Dynamic Host Configuration Protocol for IPv6) umożliwiającego komputerom uzyskanie do serwera danych konfiguracyjnych no adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski podsieci. Jego specyfikacja została opisana w RFC 3315
3. Pula adresów IPv4 a IPv6
   1. IPv4 – 32 bity  
      ok. 4 miliardy adresów
   2. IPv6 – 128 bitów  
      ok. 10^30 adresów na każdą osobę na Ziemi
   3. Zasada przyznawania adresów IPv6
      1. Nowa hierarchia przyznawania adresów
      2. Każdy dostaje jedną pulę adresów
      3. Pula jest na tyle duża, że wystarcza „na zawsze”
      4. Nie ma konieczności występować o nowe przydziały
   4. Nowe zastosowania – „nieskończona” ilość adresów IPv6 dla każdego pozwoli wykorzystywać je swobodnie na wiele nowych sposobów:
      1. Wiele urządzeń w gospodarstwach domowych będzie mogło być w prosty sposób widocznych w Internecie (dostęp do komputera domowego z biura, dostęp do muzyki, filmów, plików, kamer, systemów alarmowych itp.)
      2. Urządzenia mobilne (komórki, odtwarzacze mp3 i inne) będą mogły komunikować się bezpośrednio bez przeszkód przez Internet
4. Porównanie nagłówka IPv4 a IPv6
   1. Budowa datagramu IPv6:
      1. Wersja – 0-3 bity
      2. Priorytet – 4-11 bity
      3. Etykieta przepływu – 12 – 31 bitów
      4. Długość danych – 0 – 15 bitów
      5. Następny nagłówek – 16 – 23 bitów
      6. Limit przeskoków – 24 – 31 bitów
      7. Adres źródłowy (128 bitów) – 0 – 32 bitów – 4 linie
      8. Adres Docelowy (128 bitów) – 0 – 32 bitów – 4 linie
5. Adresowanie IPv6
   1. Hosty podłączone do tego samego łącza mogą automatycznie konfigurować dla siebie adresy lokalne dla łącza i komunikować się bez konfiguracji ręcznej. Adres IPv6 składa się z 128 bitów podzielonych na 16 bitowe fragmenty, oddzielone dwukropkami. Każdy 16 – bitowy blok reprezentowany jest za pomocą 4 -cyfrowej liczby szesnastkowej.
   2. Reprezentacja IPv6 może zostać uproszczona poprze usunięcie poprzedzających zer z każdego 16 – bitowego bloku. W tym uproszczeniu każdy blok musi posiadać przynajmniej jeden znak. Po pominięciu poprzedzających zer reprezentacja adresu wygląda następujco:  
      21DA:D3:0:2F3B:2AA:FF:FE28:9C5A
   3. Dozwolone jest pominiecie ciągu bloków składających się wyłącznie z zer. Pomijając blok zer, wprowadza się separator bloków :: (podwójny dwukropek)  
      Dopusczalny jest tylko jeden podwójny dwukropek w adresie.  
      Poniższe adresy są równoznaczne:  
      2001:0DB8:0000:0000:0000:0000:1234:ABCD  
      2001:0DB8:0:0:0:0:1234:ABCD  
      2001:0DB8:0:0::1234:ABCD  
      2001:0DB8::1234:ABCD  
      2001:DB8::1234:ABCD
   4. W adresacji wykorzystywanej w protokole IPv6 używane są trzy typy adresów:
      1. Unicast – identyfikujący pojedynczy interfejs
      2. Multicast – identyfikujące grupę interfejsów (mogą one należeć do różnych węzłów)
      3. Anycast – podobnie jak adresy multicast, identyfikują one grupę interfejsów, jednak pakiet wysyłany na adres anycast jest dostarczany do najbliższego węzła, np. najbliższego serwera DNS
   5. W IPv6 rozróżniane są zakresy adresów:
      1. Adresy lokalne dla łącza (link-lokal address) – wykorzystywane tylko o komunikacji w jednym segmencie sieci lokalnej lub przy połączeniu typu point-to-point. Routery nie przekazują pakietów z adresami lokalnymi.  
         Adresy te mają prefiks FE80/10. Każdy interfejs musi mieć przydzielony co najmniej jeden adres dla łącza nawet jeżeli posiada adres globalny lub unikalny adres lokalny.  
         Zakres ten odpowiada zakresowi APIPA w IPv4 (169.254.0.0/16)
      2. Unikalne adresy lokalne (unique local adress) – adresy będące odpowiednikami adresów prywatnych z protokołu IPv4. Adresy te mają prefiks FC00/7
      3. Adresy globalne (global unicast address) – adresy będące odpowiednikami adresów publicznych z protokołu IPv4. Adresy te to wszystkie inne nie wymienione we wcześniejszych punktach. (jeden do jednego z wielu)
      4. Adresy specjalne:

* ::/128 – adres nieokreślony (zawierający same zera – odpowiednik 0.0.0.0)
* ::1/128 – pętla zwrotna (loopback) – adres wskazujący na hosta lokalnego (odpowiednik 127.0.0.1)
* 2001::db8::/32 – pula wykorzystywana w przykładach i dokumentacji – nigdy nie będzie wykorzystywana produkcyjnie
* F00::/8 – pula multicastowa używana do komunikacji multicast
  1. Przykłady rozwoju i wdrożeń IPv6 w Polsce:
     1. PIONIER – Polski Internet Optyczny – ogólnopolska sieć akademicka i naukowa PIONIER
     2. Sieć IPv6 w Poznańskim Centrum Superkomputerowo – sieciowym (PCSS) w sieci Poznań
     3. Sieć europejska GEANT2
  2. Polska grupa Robocza IPv6:
     1. Inicjatywa non profit skupiająca uczestników zainteresowanych rozwojem IPv6 w Polsce:
        1. Firmy komercyjne
        2. Operatorów telekomunikacyjnych
        3. Dostawców usług
        4. Ośrodki naukowe
        5. Rządowe
        6. Przemysłowe
        7. Edukacyjne
  3. Wnioski:
     1. Pożądanie jest wdrażanie sieci IPv6 w skali krajowej:
        1. Pobudzanie postępu technicznego
        2. Nadążanie za światowym rozwojem technicznym
        3. Pobudzanie rozwoju przedsiębiorstw sektora ICT (technik informacyjno – komunikacyjnych)
        4. Podniesienie poziomu życia obywateli
        5. Nadzieją na wdrożenie są nowopowstający operatorzy sieci transmisji danych
        6. Istniejący operatorzy muszą mieć bodźce ekonomiczne aby zdecydować się na inwestycje modernizacyjne
     2. Wdrażanie IPv6:
        1. Nabardziej zaawansowany wdrożeń istnieje w sieciach akademicko-naukowych
        2. Brak wystarczającej moywacji u operatorów i dostawców komercyjnych
        3. Stopniowe wdrażanie jest potrzebne dla uniknięcia efektu „zderzenia ze ścianą” w przyszłości
     3. Świadomość IPv6:
        1. Rosnąca znajomość zagadnień IPv6 wśród kadry technicznej
        2. Małe motywacje wśród kadry menadżerskiej
        3. Konieczne kształtowanie świadomości o IPv6 jako jedynej drogi do budowania dobrych aplikacji w publicznym Internecie
     4. Zastosowania IPv6:
        1. Brak rewolucyjnych aplikacji i zastosowań dzięki którym IPv6 zyskałoby zainteresowanie użytkowników końcowych
        2. Olbrzymi rynek do zastosowań
     5. IPv4 vs IPv6:

|  |  |
| --- | --- |
| **IPv4** | **IPv6** |
| Adres długości 32 – bity | Adres długości 128 – bitów |
| Maska sieciowa | Brak maski sieciowej |
| Wsparcie dla IPSec opcjonalne | Wsparcie dla IPSec obowiązkowe |
| Suma kontrolna w nagłówku | Brak sumy kontrolnej w nagłówku |
| Dodatkowe opcje w nagłówku | Dodatkowe opcje przeniesione do pola Następny nagłówek |
| Musi być skonfigurowany ręcznie bądź przez DHCP | Nie musi być konfigurowany ręcznie ani przez DHCP |

Lekcja

Temat: Protokoły warstwy transportowej TCP i UDP

1. 4 w ISO, 3 TCP/IP
2. Warstwa transportowa – zapewnia usługi przesyłania danych z hosta źródłowego do hosta docelowego. Ustanawia logiczne połączenie między hostem wysyłającym i odbierającym. Protokoły transportowe dzielą i scalają dane wysyłane przez aplikacje wyższej warstwy w jednej strumień danych przepływający między punktami końcowymi
3. Protokoły warstwy transportowej to TCP i UDP
4. Protokół TCP (jest odpowiedzialny za bezbłędne dostarczanie informacji:
   1. Jest zorientowany na połączenie: oznacza to że program użytkowy który chce skorzystać z protokołu TCP musi najpierw zwrócić się do odbiorcy z prośbą o uzyskanie połączenia i uzyskać zgodę
   2. Jest protokołem typu punkt-punkt: oznacza to że każde połączenie TCP ma dokładnie dwa końce
   3. Zapewnia niezawodność: oznacza to że protokół TCP i zapewnia pełna niezawodność w dostarczaniu pakietów
   4. Zapewnia dwukierunkową komunikację oznacza to że komunikacja w połączeniu TCP odbywa się w dwóch kierunkach czyli zarówno od nadawcy do odbiorcy jak i od odbiorcy do nadawcy
   5. Zapewnia strumieniowy interfejs: oznacza to że program może wysłać połączeniem całą sekwencję bajtów w konsekwencji prowadzi to do tego, że dane nie muszą być dostarczane do odbiorcy w kawałkach tych samych wielkości w których zostały wysłane
   6. Zapewnia łagodne kończenie połączenia: oznacza to że protokół gwarantuje niezawodne dostarczenie pakietów przed zamknięciem połączenia
   7. Nagłówek TCP:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 bajt | 2 bajt | | 3 bajt | 4 bajt |
| Port źródłowy | | | Port docelowy | |
| Numer sekwencyjny | | | | |
| Numer potwierdzenia | | | | |
| Długość nagrania | Rezerwa | Znaczniki | Okno | |
| Suma kontrolna | | | Wskaźnik pilności | |
| Opcje | | | |  |
| Dane | | | | |

* 1. Ponieważ na komputerze posiadającym jeden adres IP może jednocześnie działać wiele aplikacji, to do ich identyfikacji wykorzystuje się porty. Porty reprezentowane są przez liczby naturalne z zakresu od 0 do 65535. Numery portów od 0 do 1023 są ogólnie znane (well-known port numbers) i zarezerwowane dla usług, np. WWW korzysta z portu 80, a telnet z portu 23. Dzięki portom możemy określić, dla jakiej aplikacji jest przeznaczony segment danych (port docelowy) lub z którego portu wysłano dane (port źródłowy)
  2. Komunikacja między aplikacjami może się odbywać za pomocą gniazd (socket). Gniazdo to kombinacja adresu IP i adresu portu. Jednoznacznie określa się proces w sieci lub zakończenie logicznego łącza komunikacyjnego między dwoma aplikacjami. Jeśli aplikacje uruchomione są na dwóch różnych komputerach, to para odpowiadających im gniazd definiuje połączenie.
  3. Każdy przesyłany segment danych jest oznaczony kolejnym numerem sekwencyjnym. Przed rozpoczęciem transmisji nadawca i odbiorca wymianiają między sobą te numery. Odbiorca wiadomości na podstawie numeru sekwencyjnego ustala kolejność segmentów oraz sprawdza czy wszystkie segmenty dotarły do mijsca przeznaczenia. Potwierdzienie odebrania segmentu polega na wysłaniu przez odbiorcę numeru kolejnego segmentu, który powinien być przesłany.
  4. Na przykład, jeżeli ostatni poprawnie odebrany segment miał numer 123, to odbiorca wyśle numer potwierdzenia 124(numer następnego segmentu), który ma być przesłany). Potwierdzenie jest wysyłane po odebraniu pewnej liczby danych, określonych w polu okno:
     1. Jeżeli w sieci występuje dużo błędów to wielkość okna jest zmniejszana aby częściej otrzymywać potwierdzenia i przez to zmniejszyć liczbę segmentów danych wymagających retransmisji. Jeżeli liczba błędów się zmniejsza to rozmiar okna jest powiększany, aby zapewnić większą przepustowość sieci.

1. Protokół UDP (User Datagram Protocol) – działa w warstwie transportowej w trybie bezpołączeniowym. Protokół ten nie gwarantuje dostarczenia danych do odbiorcy. Jeżeli pakiet nie dotrze do odbiorcy lub dotrze uszkodzony UDP nie podejmie żadnych działań zmierzających do retransmisji danych a zapewnienie niezawodności pozostawi warstwie wyższej. Nagłówek protokoły UDP jest prostszy niż TCP. Protokół jest wykorzystywany do szybkiego przesyłania danych w niezawodnych sieciach.

|  |  |  |  |
| --- | --- | --- | --- |
| 1 bajt | 2 bajt | 3 bajt | 4 bajt |
| Port źródłowy | | Port docelowy | |
| Długość | | Suma kontrolna | |
| dane | | | |

1. Wyobraźmy sobie na przykład, że musimy przesłać dane do 10000 odbiorców. Wykorzystując do tego protokół TCP musimy otworzyć, kontrolować a następnie zamknąć 10000 połączeń. Koszt tych operacji jest stosunkowo wysoki. Wykorzystanie natomiast protokołu UDP nie wymaga wykonania tych wszystkich czynności.

Lekcja

Temat: Protokoły warstwy aplikacji

1. Formy różnych technologii przesyłania danych
2. Aplikacji nie interesuje jaką drogą są przesyłane aplikacji
3. Protokoły warstwy aplikacji (aplikacji prezentacji sesji):
   1. http
   2. DNS
   3. DHCP
   4. FTP
4. http – port 80 – protokół używany do przesyłania plików tworzących strony www, komunikacja w ramach protokołu http oparta jest na wysyłaniu danych pomiędzy klientem i serwerem (odpowiadającym). Klient wysyła zapytanie – serwer wysyła odpowiednie dane. Trzeba jednak pamiętać, że protokół http zaliczany jest do protokołów bezstanowych, czyli takich, które nie przechowują danych.  
   Z jednej strony pozwala to na zmniejszenie obciążenia serwera danymi, z drugiej może okazać się kłopotliwe przy kilkurazowym korzystaniu ze strony. Dlatego też praktycznie do każdego serwisu opartego na protokole http wprowadzany jest mechanizm ciasteczek, które zapamiętują dane sesji na stronie odwiedzanego serwera (dane zapisane dzięki ciasteczkom mogą być później wykorzystywane przez właściciela serwera do różnych celów – np. kampania marketingowa).  
   Kody:
   1. kody 1xx (np. 110 connection timed out)
   2. kody 2xx (np. 200 ok)
   3. kody 3xx (np. 301 moved permamently)
   4. kody 4xx (p. 404 not found)
   5. kody 5xx (np. 502 bad Gateway)
5. smtp – port 25 – protokół używany do przesyłania wiadomości poczty elektronicznej wraz z załącznikami, RFC 2821, protokół niezawodnego przesyłania wiadomości tekstowych (e-mail) za pomocą prostych komend tekstowych

Przykład:

* 1. 220 serwer ESMTP Exim 4.43 Wed, 12 Jan 2005 23:14:13 +0100
  2. **helo** serwer.email.com
  3. 250 użytkownik.internet.com **hello**  użytkownik at użytkownik.internet.com [1.1.1.1]
  4. Mail from [nadawca@example.com](mailto:nadawca@example.com)
  5. 250 OK
  6. Rcpt to: [odbiorca@example.org](mailto:odbiorca@example.org)
  7. 250 accepted
  8. Data
  9. 354 Enter message, ending with „.” On line by itself
  10. Date: 03 jan 07 21:21:21
  11. From: nadawca@example.org
  12. To: [odbiorca@example.org](mailto:odbiorca@example.org)
  13. Subject: temat wiadomości
  14. Treści wiadomości
  15. .
  16. 250 OK id=1Coql6-0003Qi-MP
  17. Quit
  18. 221 serwer.email.com cloing connection

1. Komendy smtp:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ESMTP | | | SMTP | | |
|  |  | |  | |  |
| Auth | | Autoryzacja | Data | Przesłanie treści listu | |
| Dsn | | Powiadomienie ostatusie doręczenia | Helo | Nawiązanie połączenia SMTP | |
| Ehlo | | Spis obsługiwanych komend ESMTP | Help | Wypis dostępnych komend | |
| Etrn | | Przesłanie kolejki listów przeznaczonych do podłączającego się serwera | Mail | Nadawca listu | |
| Pipeling | | Protokołowe przesyłanie wiadomości | Noop | Podtrzymywanie połączenia | |
| Size | | Określanie wielkości przesyłanej wiadomości | Quit | Zakończenie sesji smtp | |
| 8bitmime | | Wsparcie dla 8bitowego kodowania wiadomości | Rcpt | Odbiorca listu | |
| Restart | | Wznowienie przesyłania wiadomości przy rozłączeniu sesji | Rset | Przerwanie sesji smtp | |
|  | |  | Vrfy | Sprawdzanie obecności skrzynki pocztowej o podanej nazwie | |

1. POP3 – port 110 – protokół używany do odbioru poczty elektronicznej  
   ograniczenia protokołu POP:
   1. Połączenie jest realizowane tylko na czas kiedy użytkownik pobiera pocztę, nie może zostać uśpione
   2. Każdy list musi być pobrany razem z załącznikami i żadnej jego części nie można w łatwy sposób pominąć – istnieje co prawda komenda top, ale pozwala ona jedynie określić przesyłaną liczbę linii od początku wiadomości
   3. Wszystkie odbierane listy trafiają do jednej skrzynki, nie da się utworzyć ich kilku
   4. Serwer POP3 nie potrafi sam przeszukiwać czekających w kolejce listów
2. Komputer – wysyłanie smtp – isp mail serwer – internet – pop3 – komputer
3. IMAP – port: 143 – protokół używany do odbioru poczty elektronicznej, oprócz POP3, pozwala również na zarządzanie zdalnymi folderami znajdującymi się na serwerze.  
   Jest następcą tradycyjnego protokołu POP3 służącego do komunikacji programów pocztowych z serwerem pocztowym. W stosunku do swojego poprzednika protokół IMAP jest bardziej rozbudowany i posiada większe możliwości zarządzania kontem e-mail
4. Najważniejsze cechy protokołu IMAP:
   1. Umożliwia operowanie na wiadomościach i folderach (tworzenie, usuwanie, przenoszenie) bezpośrednio na serwerze. Dane dla konta pocztowego, widoczne w kliencie pocztowym zainstalowanym na dowolnym komputerze oraz w programie Active Office są zawsze synchronizowane
   2. W przeciwieństwie do protokołu pop3, protokół IMAP umożliwia pobieranie nagłówki w wiadomości bez konieczności pobierania na lokalny komputer kompletnej zawartości wszystkich maili wraz z załącznikami. Pobieranie jedynie nagłówków wiadomości e-mail znacznie ogranicza objętość transferowanych danych, dlatego protokół IMAP doskonale sprawdza się w obsłudze poczty na urządzeniach mobilnych.
   3. Umożliwia dostęp do jednego konta pocztowego wielu użytkownikom jednocześnie
   4. Wiadomości odczytane przy użyciu protokołu IMAP nadal są przechowywane na serwerze. Na komputer lokalny mogą być pobierane jedynie nagłówki wiadomości. Dzięki temu kompletne wiadomości można usuwać oraz przenosić bez uprzedniego pobierania ich na lokalny komputer.
5. Elementy systemu pocztowego:
   1. MUA (Mail User Agent) – program używany przez odbiorcę końcowego do wysyłania, odbierania, filtrowania, czytania, pisania listów itp. (MS Outlook)
   2. MTA (Mail Transfer Agent) – część systemu pocztowego zajmująca się odbiorem poczty i/lub jej dalszym przekazaniem do innych serwerów (Postfix)
   3. MDA (Mail Delivery Agent) – część systemu pocztowego zajmująca się dostarczaniem poczty do lokalnego użytkownika
6. Telet – protokół używany do emulacji terminala umożliwiający komunikację ze zdalnym urządzeniem:
   1. Do korzystania z tej usługi niezbędne jest posiadanie na serwerze konta typu shell. Na niektórych serwerach administratorzy zakładają konta gościnne, które nie wymagają podania hasła lub hasła te są publicznie oddawane. Jednakże ze względów nadmiernego wykorzystywania takich kont, administratorzy wprowadzili możliwość używania tylko potrzebnych aplikacji, które mogą być wykorzystane na danym serwerze. Po połączeniu się z serwerem, na którym posiadamy konto shell, program zapyta nas o identyfikator użytkownika (login) i hasło dostępu (password). Usługa telnet umożliwia zatem pracę na zdalnym komputerze bez konieczności siedzenia bezpośrednio przed nim.
7. Połączenie FTP (File transfer protocol) – port 20, 21 (port danych i port poleceń) – protokół używany do interaktywnego przesyłania plików pomiędzy systemami:
   1. Aktywny tryb FTP  
      W trybie aktywnym klient FTP łączy się przez dowolny por nieuprzywilejowany (N>1024) z portem poleceń serwera FTP o numerze 21. Następnie klient rozpoczyna nasłuchiwanie na porcie N+1 i wysyła do serwera FTP polecenie PORT N+1. Serwer łączy się wówczas z określonym przez klienta portem przez własny port danych, czyli port 20.  
      Patrząc z punktu widzenia firewalla po stronie serwera transmisja FTP w trybie aktywnym wymaga, by możliwe było następujące połączenia:
      1. Do portu 21 serwera FTP skądkolwiek (klient nawiązuje połączenie)
      2. Od portu 21 serwera FTP do portu > 1024 (serwer wysyła odpowiedź do portu poleceń klienta)
      3. Od portu 20 serwera FTP do portu > 1024 (serwer przesyła dane do portu danych klienta)
      4. Do portu 20 serwera FTP do portu > 1024 (klient wysyła potwierdzenie ACK do portu danych serwera)
   2. Pasywny tryb FTP – nawiązuje oba połączenia z serwerem unikając w en sposób problemu firewalla blokującego połączenie z portem danych klienta nawiązywane przez serwer. Rozpoczynając połączenie FTP, klient otwiera dwa dowolne porty nie uprzywilejowane (N>1024 oraz N+1). Pierwszy port wykorzystywany jest do połączenia z portem 21 serwera, jednak zamiast wysłania polecenia PORT i oczekiwanie na połączenia od serwera, klient wysyła polecenie PASV. Serwer otwiera wówczas dowolny port nieuprzywilejowany (P>1024) i wysyła do klienta polecenie PORT P. Klient nawiązuje następnie połączenie między swoim portem N+1 a portem serwera P w celu transmisji danych.  
      Patrząc z punktu widzenia firewalla po stronie serwera, transmisja FTP w trybie pasywnym wymaga, by możliwe były następujące połączenia:
      1. Do portu 21 serwera FTP skądkolwiek (klient nawiązuje połączenie)
      2. Od portu 21 serwera FTP do portu > 1024 (serwer wysyła odpowiedź do portu poleceń klienta)
      3. Od portu > 1024 serwera FTP skądkolwiek (klient nawiązuje połączenie z portem danych określonym przez serwer)
      4. od portu > 1024 serwera FTP do portu > 1024 (serwer wysyła potwierdzenie ACK oraz dane do portu danych klienta)
8. Protokół TFTP (Trival File Transfer Protocol) – uproszczona wersja protokołu FTP (np. nie może wyświetlać katalogów , ani uwierzytelniać użytkowników, a jego jedynym zadaniem jest odczytywanie plików z komputera zdalnego i transmitowanie do niego plików), wykorzystywana do np. instalacji systemów operacyjnych w urządzeniach sieciowych, takich jak routery lub przełączniki
9. DHCP (Dynamic Host Configuration Protocol, port: 67) – protokół używany do dynamicznej konfiguracji urządzeń, a dokładniej odpowiedzialny jest za przydzielenie adresów IP, adresu domyślnej bramy i adresów serwerów DNS  
   Trzy techniki:
   1. Przydzielanie ręczne oparte na tablicy adresów MAC oraz odpowiednich dla nich adresów IP. Jest ona tworzona przez administratora serwera DHCP. W takiej sytuacji prawo do pracy w sieci mają tylko komputery zarejestrowane wcześniej przez obsługę systemu.
   2. Przydzielanie automatyczne, gdzie wolne adresy IP z zakresu ustalonego przez administratora są prydzielane kolejnym zgłaszającym się po nie klientom
   3. Przydzielanie dynamiczne pozwalające na ponowne użycie adresów IP Administrator sieci nadaje zakres adresów IP do rozdzielenia. Wszyscy klienci mają tak skonfigurowane interfejsy sieciowe że po starcie systemu automatycznie pobierają swoje adresy. Każdy adres przydzielany jest na pewien czas. Taka konfiguracja powoduje, że zwykły użytkownik ma ułatwioną pracę z siecią

Niektóre serwery DHCP dodatkowo przydzielają każdemu klientowi własny adres DNS, przekazywany na serwer nazw protokołem zgodnym ze specyfikacją RFC 2136

1. DHCP nagłówek:

|  |  |  |  |
| --- | --- | --- | --- |
| 00-07 | 08-15 | 16-23 | 24-31 |
| Operacja | Typ sprzętu | Długość adresu sprzętowego | Liczba skoków |
| xid (identyfikator transakcji) | | | |
| Liczba sekund | | Flagi | |
| Adres IP klienta | | | |
| Przydzielony adres IP klienta | | | |
| Adres IP serwera | | | |
| Adres IP bramki (routera) | | | |
| Adres sprzętowy klienta (16 oktetów) | | | |
| Nazwa serwera (64 oktety) | | | |
| Plik startowy (128 oktetów) | | | |
| Opcje producenta (długość zmienna) | | | |

1. NFS (network file system port: 2049) – protokół używany do udostępniania systemów plików (dysków sieciowych):
   1. Żądanie zostaje wysłane przez klienta
   2. Żądanie zostaje odebrane przez serwer
   3. Operacja zostaje wykonana
   4. Potwierdzenie zostaje wysłane przez serwer
   5. Potwierdzenie zostaje odebrane przez klienta
2. SNMP (simple network menager protocol, port: 161) -