I. Algorytmy zapewniające niezawodność sieci w warstwie 2 i 3.

a) Routing - jest to algorytm zapewniający przesyłanie pakietów z komputera źródłowego do docelowego. Routery po otrzymaniu pakietu forwardują go zgodnie z ustaloną zasadą z tablicy routingu.

Wyróżnia się routing statyczny, w którym administrator może wybrać alternatywną drogę w razie awarii oraz routing dynamiczny, w którym routery same odnajdują trasę alternatywną(dzięki periodycznym dzieleniu się tablicami routingu)

b) Spanning tree - jest to algorytm, który przeciwdziała pętleniu się ramek. Działa poprzez wybór jednego węzła jako korzenia drzewa, a następnie usuwa krawędzie w celu utworzenia struktury hierarchicznej. Z punktu widzenia niezawodności istotnie jest, że mechanizm ten zakłada okresowe rozsyłanie ramek BPDU, co umożliwia wykrycie awarii, w przypadku gdy, któraś ze stacji się nie odezwie. Rekonfiguracja polega na przebudowaniu drzewa(około 50s). Zamiast tego można użyć Rapid Spanning Tree (około 6s),który szybciej rozsyła ramki BPDU. Multiple Spinning Tree umożliwia tworzenie drzewa dla każdego Vlana

c) Agregacja łączy - mechanizm polega na realizacji wysokoprzepustowego połączenia full-duplex dwóch przełączników łącząc ze sobą kilka ich portów. Agregacja łączy wspiera mechanizm load balancing, czyli podział obciązenie między nadmiarowe łącza. Agregacja łączy umozliwia zwiększenie przepustowości łącza oraz zapewnia redundancje, aby w przypadku awarii jednego łącza, pozostałe wciąż utrzymywały połączenie.Trwa to do kilkudziesięciu-kilkuset mikrosekund.

II. Jakie znasz kodowania transmisyjne? Dlaczego nie używa się prostego kodowania Manchester lub zerojedynkowego w prostych rozwiązaniach Ethernetu?
Dlaczego wprowadzono kodowanie xb-yb?

a) Kodowania trasmisyjne

* Manchester(narzut 100%, dwupoziomowe, 1 jest kodowana przez przejscie z ze stanu niskiego do wysokiego, 0 jest kodowane przez przejscie ze stanu wyoskiego na niski)

* MLT-3 (kodowanie 4b/5b, 1 -> zmiana stanu, 0 -> brak zmiany stanu)

* PAM-5 (kodowanie 8b/10b)

* PAM-16 (kodowanie 64b/66b i 8b/10b)

* kodowania xb/yb (4b/5b w 100M internecie, 8b/10b w 1G internecie, 64b/66b w 10 G internecie. W 64b/66b narzut wynosi 3%, a nie jak w 8b/10b 20%)

b) Dlaczego nie uzywa się kodowania Manchester oraz dlaczego wprowadzono kodowanie xb-yb

Dla kodowania Manchester potrzeba pasma przesyłającego dane dwa razy szybciej niż prędkość transmisji. Jest to nieopłacalene, ponieważ jest 100% narzutu(na każdy bit trzeba wyemitować 2 wartości). Dlatego zamiast tego stosuje się kodowanie xb/yb, które ma mniejszy narzut oraz pozwala dostosować wolniejsze pasmo !!!!!!

Przyczyny stosowania kodowania xb/yb:
1.Poukładanie 0 i 1 tak, żeby się zmieniały(ze względu na zrównoważenie pradowe)
2.Stosuje się go żeby uniknąć długich ciągów 0 i 1(można podejrzewać, ze kabel został uszkodzony, „ukradli kabel :)”)
3.Zapobieżenie przegrzania się układów nadających

DOKOŃCZYĆ !!!

III. Nazewnictwo

10 - 10 gigabit CZY TO NA PEWNO GIGABIT?

DŁUGOŚCI FALI:
S => short, L => long, E => extra long

WARSTWA FIZYCZNA:
R => LAN PHY, W => WAN PHY

KODOWANIE:
X => X-8b/10b, W => W-64B/66B

K - backplane (łączenie modułów przełącznika/ routera)
C - copper
T - skrętka
Base - baseband signaling

Przykłady:

SR - dlugosc fali -> Short, warstwa fizyczna -> LAN PHY

LR - dlugosc fali -> Long, warstwa fizyczna -> LAN PHY

ER - dlugosc fali -> Extra Long, LAN PHY

LX4 - dlugosc fali -> Long, kodowanie X-8b/10b, 4 tory trasmisji

LRM - dlugosc fali -> Long, wartstwa fizyczna -> LAN PHY, Multimode(wielomodowy) WAZNE !!!

SW - dlugosc fali -> short, warstwa fizyczna -> WAN PHY,kodowanie 64b/66b

LW - dlugosc fali -> long, warstwa fizyczna -> WAN PHY, kodowanie 64b/66b

EW - dlugosc fali -> extra long, warstwa fizyczna -> WAN PHY, kodowanie 64b/66b

CX4 - cooper(miedz), czyli kabel miedziany, 'X' -> to kodowanie X-8b/10b, 4 tory transmisji WAZNE !!!

T - skrętka

TYCH NIE JESTEM PEWNY:

KX4 - K-backplane, 4 tory transmisji, kodowanie to X-8b/10b

KR - K-backplane, warstwa fizyczna - LAN PHY

IV. Kiedy stosować/ użyję koncentratora:

a) dla sieci zamkniętych(ze względu na rozgłaszanie na wszystkie porty)

b) dla małych obciążeń sieci(małe prawdopodobieństwo kolizji)

c) gdy buduję sieć w topologii gwiazdy

d) dla łączenia sieci homogenicznych

V. Kiedy stosować/ użyję przełącznika:

a) chcę podzielić domenę kolizyjną na poddomeny !!!

b) chce zwiększyć przepustowość sieci

c) w rozproszonych oraz centralizowanych sieciach szkieletowych !!!

d) muszę skorzystać z mechanizmu Spanning Tree

VII.Kiedy stosować/ użyję routera:

a) chce rozdzielić domenę rozgłoszeniową

b) chce połączyć sieć z siecią WAN

VIII. Rodzaje rekordów DNS:

a) rekord "A"

Rekord "A" jest używany do mapowania nazwy domenowej na adres IPv4. Dzięki temu możliwe jest rozwiązanie nazwy domenowej na odpowiadający jej adres IP, umożliwiając komunikację między hostami w sieci na podstawie nazw domenowych. Rekord "A" może mieć różny TTL(Time To Live), czyli czas życia, który określa jak długo rekord powinien być przechowywany w pamięci podręcznej systemów DNS. TTL jest istotny, ponieważ pozwala na aktualizację rekordu w przypadku zmiany adresu IP lub przeniesieniu zasobu na inny serwer.

b) rekord MX (mail exchange)

Rekord jest używany do określania serwera poczty odpowiedzialnego za odbieranie wiadomości e-mail dla danej domeny.Rekord MX zawiera informacje o priorytetach różnych serwerów poczty, gdzie niższa wartość priorytetu oznacza wyższy priorytet. Gdy jest wysyłana wiadomość e-mail na adres związany z daną domeną, system DNS używa rekordu MX, aby przekierować wiadomość do serwera poczty o najniższym priorytecie. Serwer ten odiera wiadomość i dostaracza ją do odpowiedniego odbiorcy.

c) AAAA - adres IPv6 hosta

d) NS - wskazuje na autorytatywny serwer nazw danej domeny

e) SOA - ogólne informacje o domenie

f) CNAME - alias

g) PTR - stosowane do wyszukiwania wstecznego

h) HINFO - informacje o sprzęcie obsługującym daną domenę

i) SRV - identyfikacja usług

Czym jest DNS:

DNS służy do przekrzstałcania ludzkich nazw na adresy IP. Dzięki DNS nie trzeba znac adresu IP i maski, żeby odnaleźć daną stronę
DNS może działać w dwóch trybach:

* Rekursji - serwer wysyła zapytania do serwerów wyższych w imieniu klienta
* Iteracji - odpytujemy po kolei wszystkie znane nam serwery.

Występuję ograniczenie do 13 serwerów DNS ze względu na to, że wielkość pakietu UDP nie pomieści więcej informacji niż o 13 serwerach.

Za DNS w Polsce odpowiada NASK, w trójmieście TASK.

NAZWA DOMENOWA:

* Nazwę domeny wyznacza się poprzez poprowadzenie ścieżki do korzenia i połączenie poszczególnych członów kropkami.

* Cała przestrzeń nazw podzielona jest na rozłączne strefy

* Serwery DNS mają adresy anycastowe - zapytanie idzie do najbliższego względem hopów

* Serwery używają rund - Robin do dzielenia obciążenia zasobów sieciowych

Typy serwerów nazw:

a) root server (informacje o wszystkich domenach)
b) slave server (kopie)
c) coaching server
d) forwarding server

Struktura drzewa DNS:

a) jest to struktura drzewiasta - tworzy obszar nazw domen

b) ma "root"

c) dzieci roota to TLD

d) domena -> poddrzewo w wielkim drzewie

e) poddomena -> poddrzewo danej domeny

f) żeby stworzyć nową domenę potrzeba zgody od właściciela domeny

IX. Dlaczego należy minimalizować liczbę urządzeń sieciowych?

Przy koncentratorach im więcej urządzeń tym mniejszy zasięg. Przy

przełącznikach i ruterach zmienia się opóźnienie przechodzenia ramek przez takie urządzenie. Każdy przełącznik i każdy router to zbiór buforów.
Jeżeli trafimy na taki moment, że w buforze jest dużo danych (to z ramką czekamy długo), a jeżeli jest mało danych(to z ramką czekamy krótko) i im więcej urządzeń po drodze tym więcej buforów i zmienność opóźnienia może być bardzo duża.

X. Jakie są tryby pracy przełączników i typy metod przełaczania

Tryby pracy:

* Przełączanie w trybie przezroczystym

Jak dostaje wiadomość(tablica jest pusta lub niepełna albo jest pełna ale nie ma pewnego urządzenia) to wówczas taki przełącznik wysyła te wiadomość na wszystkie porty, oprócz na port, z którego to przyszło.
Powoduje to to, że taka wiadomość (pod nieznany adres) zalewa sieć.

* Przełączanie w trybie ekspresowym (lub szybkim)

Wiadomość przychodząca pod nieznany adres jest wysyłana na dedykowane porty. Porty może dedykować firma lub supervisor. Wtedy mamy pewność, że gdy wysyłamy na porty parzyste to nie pójdzie to na wszystkie porty, tylko na połowę portów.
Można je stosować w aplikacjach czasu rzeczywistego !!!

* Metoda cut through(fast forward)

Jest bardzo szybkie. Wprowadza kilkudziesięcio-bitowe opóźnienie. Istnieje groźba, że wystąpią błędy to aplikacja dostanie błędne dane. Jeżeli aplikacje nie tolerują przekłamań(np. Aplikacje za którymi stoją pieniądze lub podejmowanie decyzji) nie wolno wtedy stosować cut through. Może zostać użyte np. podczas transmitowania mowy(przekłamanie pojedynczej wiadomości nie jest kluczowe).

* Odrazu nadajemy na port, na którym jest odbiorca ???

* Metoda store and forward

Cała ramka jest wczytywana do przełącznika. Stosujemy wtedy, gdy wiemy, że aplikacje muszą dostawać poprawne dane. Używana w aplikacjach, które nie tolerują błędnych danych np. Aplikacje bankowe (czy na pewno???)

* wolniejsze i tańsze niż cut through

XI. Dlaczego ramka ma mniej niż 2 kB, ale więcej niż 64B?

Więcej niż 64B, ponieważ 64 jest minimalną długościa ramki. Wynika to z historii. Ethernet kiedyś nie był full-duplex, a detekcja kolizji mogła zachodzić, gdy nadawca sam nadaje jeszcze swoją ramkę. Kolizja jest wykrywalna dla 51.2 us * 10 Mb/s = 512 b => 64B

Ma mniej niż 2 kB ze względu na kompatybilność wsteczną. Węzły w Ethernecie muszą móc pomieścić cała ramkę w RAMie.

XII. 10 Bb/s - ile/jakie rozwiazania i które generują dokładnie 10 Gb/s

Jest 7 takich rozwiązań, żaden nie pracuje/generuje ze względu na kodowanie xb/yb

Rozwiązania :

SR, LR, ER, SW, LW, EW, LX4

XIV. PCF vs DCF (kiedy, który / unikanie kolizji)

DCF - dostęp rywalizacyjny. Opiera się na CSMA/CA oraz wysyłaniu ramek rts/cts w celu rezerwacji metdium. Jeśli zostanie wykryte, że medium jest wolne, to stacja oczekuje DIFS i zaczyna nadawanie. Potwierdzenie odbioru ramki sygnalizowane jest ramką ACK.

PCF - opcjonalna(przepytywanie) metoda dostępu(bez potrzeby rywalizacji).Istnieją w niej wymagania co do czasu dostępu. Point Corridor wskazuje, która stacja ma prawo do wysyłania ramki. Zapobiega problemowi stacji ukrytej.

XIII. Wady IPv4 wynikające z nagłowka:

a) wersja protokołu - niepotrzebnie 4b. Mogłoby być 1, skoro tylko 2 stany

b) typ usługi - ignorowane przez wiele urządzeń, rzadko stosowane, 2b nieużywane

c) długość całkowita datagramu - maksymalny rozmiar datagramu może być za mały

d) identyfikacja - umożliwia identyfikacje wiadomości wraz z adresem IP, co zmniejsza prywatność, pole może być za małe na długie połączenia

e) przesunięcie fragmentacji - "klęska internetu" -> trzeba czekać, aż cała wiadomość do nas dojdzie. Zanim otrzymamy zgubioną część to możemy już

usunąć resztę tamtej wiadomości. Duża fragmentacja = duże opóźnienia, większy narzut

f) czas życia datagramu:

kryminogenny -> trudno wykryć atakującego
zmniejszenie prywatności -> systemy operacyjne mają charakterystyczne wartości, za małe pole (czasem potrzeba większej ilości hopów)

g) protokół przesyłający dane - za małe pole (jest więcej protokołów niż 256), nieustandaryzowane

h) suma kontrolna - za krótka i niepotrzebna(większość routerów nigdy nie wykryje błędów ze względu na niską stopę błędu ~ 10^-12), wykrywa nieparzystą ilość błędów

i) adres źrodłowy/docelowy - za małe pola, niewystarczające w skali świata

j) opcje nagłówka - rzadko używane, datagramy przechodzą przez zbyt wiele routerów jak na 40B

XIV. Kryteria wyboru przełącznika

a) standardowość (czy ma wbudowane wsparcie dla IEEE 802.1/802.3)

b) elastyczność (automatyczne ustalanie prędkości transmisji między portami, wsparcie nowych technologii)

c) przepustowość (liczona w bps)

d) pojemność tablic adresów MAC (odpowiednia by zmiejszyć podatność na atak przez zalewanie)

e) dedykowany port do zarządzania (odporny na zalewanie przełącznika)

f) VLany (powienien umożliwiać budowanie Vlanów)

g) szybkość przetwarzania ramek (jak nie ma podane jakie ramki to zakładamy, że najmniejsze)

h) możliwość kontrolowania przeływu pakietów (sterowanie ruchem pakietów rozgłoszeniowych, blokowanie medium)

i) możliwość budowania wysokoprzepustowych połączeń między przełącznikami (agregacja łączy, load balancing)

XV. Prównaj przełącznik z routerem

Metody przełączania:

przełącznik -> STORE AND FORWARD, CUT THROUG

Koncentrator -> brak

router -> STORE AND FORWARD

Realizowane algorytmy:

przełącznik -> STP

koncentrator -> brak

router -> routing,forwading

Vlany:

przełącznik -> tak

Koncentrator -> nie

router -> nie

Filtracja ruchu:

przełącznik -> tak(uczenie się)

Koncentrator -> nie

router -> tak(blokada rozgłoszeń)

Ilość protokołów:

przełącznik -> kilkanaście-kilkadziesią

Koncentrator -> kilka

router -> kilka

Opóźnienie:

przełącznik -> rzędu mikrosekund

Koncentrator -> setki nanosekund

router -> do kilku milisekund

Bezpieczeństwo:

przełącznik -> filtrowanie, zabezpieczenie przeciw zalewaniu, ogarniczenie adresów MAC

Koncentrator -> niebezpiecznie (ruch rozgłoszeniowy)

router -> Vlany, układy odpwiedzialne za firewall, blokowanie ruchu rozgłoszeniowego

Warstwa:

przełącznik -> 2 i 3

koncentrator -> 1

router -> 3

Zależność od protokołów:

przełącznik -> zależne od warstwy łącza danych

Koncentrator -> niezależne

router -> zależne od warstwy sieciowej

Domena rozgłoszeniowa:

przełącznik -> powiększa

Koncentrator -> powiększa

router -> dzieli

Buforowanie:

przełącznik -> tak

Koncentrator -> nie

router -> tak

XVI. Opisz działanie systemów pocztowych(w tym podstawowe protokoły)

Wyróżniamy:

* lokalny system poczty - serwer pocztowy znajduje się w sieci lokalnej

* web based email system - serwer pocztowy znajduje się w internecie

Schemat działania:

1) Użytkownik pisze treść, załączniki, adresata
2) Mail jest przerabiany przez agenta użytkownika -> UA(user agent), dodaje nagłówek MIME, nadawcę (UA header)
3) UA wysyła maila do MTA (Mail Transfer Agent) 1
4) MTA 1 dorzuca swój header
5) Mail dzięki SMTP lata po internecie, aż trafi do MTA 2
6) MTA 2 dorzuca swój header

* Protokół SMTP (Simple Mail Transfer Protocol) - odpowiada za przesyłanie wiadomości między serwerami MTA.

* Protokół POP3 - komunikacja jednostronna, przy pobieraniu maili z serwera ściąga wiadomości na urządzenie, po czym usuwa wiadomość z serwera.
* Protokół IMAP4 - komunikacja dwustronna, przy pobieraniu maila z serwera kopiuje wiadomości na urządzenie i zostawia dane na serwerze w spokoju.

XVII. Analiza różnych typów adresów w sieciach IP

1. Adres IP

a) Służy do identyfikacji elementów w 3 warstwie sieciowej
b) Nie musi jednoznacznie identyfikować urządzenia jak MAC
c) IPv6 - 128 bitów
d) IPv4 - 34 bity
e) W zależności od NET ID adres należy do klas (A-E)

2. Adres MAC

a) Służy do identyfikacji elementów w 2 warstwie łącza danych
b) 48 bitów - unikatowy dla urządzen w skali świata

Istnieją zarezerwowane adresy MAC np. do testów

3. Adres Portu

a) numery portów 0 - 2^16 -1(65535)
b) 0-1023 - ogólnie znane i przypisane do usług
c) 1024 - 49151 - używane przez aplikacje do komunikacji w sieci
d) 49152 - (2^16 -1) -> prywatne

Numery portów powinny być unikatowe dla każdej usługi w obrębie jednego protokołu

Numery przydziela IANA

4. Odwzorowanie IP <-> MAC

a) Odwzorowanie dokonuje ARP
b) Zapewnia dynamiczne odwzorowanie
c) Nie wymaga przechowywania tablicy przekształcania adresowego przez komputer

Komputery przechowywają ostatnio używane odwzorowania
Przekształcenia odwrotnego dokonuje protokół RARP (MAC <-> IP)

a) rozsyła zapytanie
b) Urządzenie uprawnione (demon RARP) odpowiada adresem IP, a jak nie zna odwzorowania to milczy
c) Zwykle komputer wysyłający zapytanie nie zna adresu IP i chce go poznać

Najprostszy sposób statycznego przydzielania adresów IP (demon RARP ma statyczną tablicę odwzorowań)

Obecnie do przydzielania IP służy DHCP.

WOŹNIAK

Porównaj znane Ci rozwiązania sieci LAN …..

ETHERNET

priorytety - brak

czas dostępu - niedeterministyczny

Token Bus

priorytety - wewnetrzne

czas dostępu - deterministyczny

Token Ring

priorytety - tak

czas dostępu - deterministyczny

WIFI

priorytety - w 802.11e

czas dostępu - niedeterministyczny

Standardy jakości:

PSTN/ISDN/GSM - sieć zorientowana połączeniowo

BISDN/ATM - stratne systemu kolejkowania

IP/ VolP - stopień satysfakcji użytkownika

Organizacje takie jak ITU-T oraz IETF formułują wymagania funkcjonalne i jakościowe dla produktów telekomunikacyjnych.

ITU-T - skupia się na znalezieniu równowagi między oczekiwaniami użytkowników, a ofertą usługodawców.

IETF - koncentruje się na rozwoju protokołów sieciowych.

ETSI - szczegółowo rozpatruje kategorie i grupy parametrów jakości. Bada takie atrybuty jakości jak: dostępność, dokładność,szybkość, wydajność, niezawodność, elastyczność, użyteczność i bezpieczeństwo.

3GPP - opracowuje standardy dla systemów komunikacji mobilnej. Skupia się na punkcie widzenia użytkownika

W przypadku usług internetowych jakość jest rozumiana jako koszt wykonania, koszt wytworzenia czy łatwość obsługi.

Ocena jakości usług uwzględnia jakość interfejsu użytkownika, jakość dostarczanej strony oraz szybkość realizacji usługi.

W celu zapewnienia jakości platformy usługowej można ocenić jej użyteczność, wiarygodność i innowacyjność.