Sieci Komputerowe 2

16 czerwca 2008

Spis treści

1. Projektowanie protokołów

Podaj definicję protokołu komunikacyjnego. System realizujący zbiór reguł współpracy pomiędzy autonomicznymi jednostkami.

Realizacja protokołu jest systemem:
— rozproszonym,
— współbieżnym,
— reaktywnym,
— tolerującym błędy,
— dużym oraz
— trudnym do projektowania i realizacji.

Atrybuty protokołów:
— poprawność – dostarcza oczekiwanych usług,
— wytrzymałość – toleruje błędy i nieoczekiwane zachowania otoczenia,
— bezpieczeństwo – właściwe dla oferowanych usług,
— wygoda – łatwy do zrozumienia,
— łatwość rozbudowy – przyszłe potrzeby,
— wydajność – duża szybkość przy niskim koszcie oraz
— skalowalność – ze względu na liczbę użytkowników.

Wymień języki stosowane do projektowania protokołów SDL, Estelle, LOTOS, Promella.

Na czym polega rozszerzony model automatów skończonych? Polega on na tym, iż w stosunku do zwykłego automatu skończonego, rozszerzony automat skończony ma również zmienne i zegary, przekazywane komunikaty mają parametry i jest możliwe spontaniczne wykonanie jakiegoś przejścia (niezależnie od odbioru komunikaty).

Czym różni się walidacja od weryfikacji? Walidujemy wymagania (czy wiemy co chcemy), a weryfikujemy specyfikację projektu (czy nasz produkt jest zgodny z opisem).

Na czym polega walidacja statyczna a na czym dynamiczna? W walidacji statycznej specyfikacja jest sprawdzana przy zastosowaniu systemów automatycznego dowodzenia twierdzeń itp. Przy walidacji dynamicznej przeprowadzana jest symulacja działania protokołu.

Jakie błędy projektowe wykrywamy dzięki analizie formalnych modeli protokołów? Pozwalają wykryć następujące błędy:
— niekompletność,
— brak wyspecyfikowanych zdarzeń,
— zdarzenia niemożliwe,
— zastoje (deadlock) oraz
— martwe pętle (livelock).

Jaki wpływ na czas testowania ma fakt napisania specyfikacji systemu i analiza tej specyfikacji? W zasadzie nie wpływa. Może jedynie ułatwić generowanie testów.

2. Estelle

Omów model komunikacyjny oferowany przez język Estelle. Język oferuję mechanizm kanałów komunikacyjnych, które posiadają punkty interakcji, podłączane do konkretnych automatów. Podłączenie to może być dynamicznie zmieniane w czasie działania systemu. Komunikaty przechowywane są w kolejce FIFO, gdzie każde zadanie może mieć jedną lub więcej kolejek (tj. kolejka może obsługiwać dowolną liczbę punktów interakcji). Kolejki FIFO nigdy się nie przepełniają.

Język umożliwia również, aby zadanie mogło udostępnić zmienne do zapisu i odczytu dla rodzica.

Gdzie w specyfikacji można wprowadzić niedeterminizm i w jakim celu można do używać? Niedeterminizm można wprowadzić przy obsłudze komunikatów, tzn. można podać losowy czas po jakim zdarzenie zostanie obsłużone. Mechanizm można stosować np. do symulowania opóźnień sieci.

Omów istotę synchronizacji pomiędzy instancjami. Ojciec ma wyższy priorytet względem dziecka, tj. nie ma wyścigu w dostępie do zmiennych eksportowanych.

Jeżeli rodzic ma atrybut process to dzieci działają niezależnie względem siebie. Jeżeli rodzic ma atrybut activity tylko jedno dziecko może działać i dodatkowo, każde dziecko również musi mieć ten atrybut.

Jakie mogą być warunki zezwalające na wybór przejścia do wykonania?
— stan automatu,
— obecność komunikatu na szycie kolejki związanym z danym IP.
— wartość zmiennych lub parametrów,
— upłynięcie określonego czasu,
— priorytet.

Jakie akcje mogą być wykonane w efekcie odpalenia przejścia?
— wysłanie komunikatu,
— zmiana wartości zmiennych,
— utworzenie/zlikwidowanie potomnej instancji oraz
— utworzenie/zlikwidowanie połączeń pomiędzy IP.

Co znaczy stwierdzenie, że przejście jest atomem? Oznacza ono, iż przejście jest albo w pełni wykonane albo nie wykonane wcale.

Co stanowi stan zadania? Stan automatu, wartości zmiennych, stan połączeń wewnętrznych, zadania potomne i ich stany.

Jakie przejście nazywamy odblokowanym? Jest to przejście dla której spełnione są warunki do wykonania (tj. automat jest w odpowiednim stanie, na szczycie kolejki jest odpowiedni komunikat, zmienne i parametry mają odpowiednie wartości). Jeżeli dodatkowo ma timer $DELAY(e_1, e_2)$ i upłynął czas e_1, ale nie upłynął czas e_2 to przejście jest opcjonalnie gotowe. Jeżeli przejście jest odblokowane i jeżeli ma timer $DELAY(e_1, e_2)$, upłynął czas e_2 oraz ma najwyższy priorytet spośród przejść spełniających ten warunek to jest przejściem gotowym (fireable).

Jakie przejście może być wybrane do wykonania. Przejście gotowe oraz te opcjonalnie gotowe dla których minął losowy czas z zakresu e_1-e_2 z najwyższym priorytetem.

Wyjaśnij pojęcie globalnej sytuacji systemu (specyfikacji). Globalną sytuację systemu definiuje ciąg $(GID_{SP}, A_1, A_2, ...A_n)$, gdzie GID_{SP} to stan wszystkich zadań należących do drzewa SP, a A_i to zbiór przejść wykonywanych w $i$tym podsystemie (liczba podsystemów jest statyczna). Inicjalna sytuacja globalna to taka, gdy $GID_{SP} = inicjalnyGID_{SP}$ i $\forall_i A_i = \emptyset$.

Następną sytuacją globalną jest: (i) jeżeli istnieje i takie, że $A_i = \emptyset$, sytuacja, w której $A_i := AS(GID_{SPi})$ czyli zbiór przejść wybranych do wykonania w $i$tym podsystemie lub (ii) wpp. sytuacja globalna, w której $GID_{SP} := t(GID_{SP})$.

Jak powstaje graf stanów osiągalnych. Powstaje on na skutek rozrysowania wszystkich możliwych stanów globalnych jakie system może osiągnąć, tj. rozpoczęcie od stanu inicjującego i na podstawie wyżej opisanych reguł przechodzenie do kolejnych stanów.

3. Metody dzielenia dostępu do medium

Jaką funkcjonalność pełni warstwa LLC? Warstwa LLC (Logical Link Control) daje i umożliwia:
— jednolity interfejs niezależny od typu MAC,
— sterowanie przepływem,
— obsługę zgubionych i powielonych ramek,
— obsługę L-SAP (wiele użytkowników w wyższych warstwach) oraz
— multipleksowanie strumieni danych od różnych użytkowników.

Jaką funkcjonalność pełni warstwa MAC? Warstw MAC (Medium Access Control) umożliwia podział wspólnego medium (w tym adresowanie w ramach medium) oraz rozproszenie sterowania.

Do czego używane są bity w polu sterującym nagłówka MAC?
— Informacje sterujące,
— adresy nadawcy i odbiorcy,
— CRC.

Czy i dlaczego w sieciach lokalnych stosuje się przydział stały do medium? Nie stosuje się go, gdyż przepustowość medium jest marnowana w sytuacji, gdy tylko niewielka liczba urządzeń obecnych w sieci nadaje.

Zdefiniuj istotę współdzielenia medium z:

przydziałem losowym. W momencie, gdy urządzenie wykryje sposobność do nadania komunikatu (m.in. cisza na łączu) zaczyna nadawać i dopiero potem stara się naprawić sytuację kolizji.

przydziałem na żądanie. Urządzenie może nadawać dopiero, gdy otrzyma do tego prawo.

W jakich warunkach wymienione metody dostępu są optymalne? Przydział losowy sprawuje się dobrze, gdy jest małe nasycenie sieci, jednak źle, gdy nasycenie jest duże (duża liczba kolizji znacznie spowalnia transmisję), natomiast przydział na żądanie nie jest podatny na duże

nasycenie sieci (nie występują kolizje), ale działa wolniej przy małym nasyceniu sieci.

Ponadto, przydział na żądanie jest konieczny, gdy nie można zapewnić, iż dwa urządzenia, które mogą nadawać w tym samym czasie będą siebie słyszeć jak to jest w sieciach radiowych.

Jaka jest istota przydziału adaptacyjnego? Polega on na tym, iż sposób przydzielania medium wybierany jest w zależności od nasycenia ruchu. Jeżeli ruch jest niewielki stosowany jest przydział losowy, a jeżeli duży przydział na żądanie.

Na czym polega działanie sieci:

token ring Urządzenia połączone w pierścień, posiadanie znacznika daje prawo do nadawania, ale można odpowiadać bez znacznika.

slotted ring

register insertion ring W momencie, gdy na łączu jest cisza przez odpowiedni okres czasu urządzenie "podmienia" tę ciszę na swoją ramkę.

token bus Jak token ring, ale pierścień jest realizowany logicznie na szynie. Dołączanie nowych urządzeń powoduje możliwość zaistnienia kolizji. Brak ograniczeń na długość ramki.

Wyjaśnij istotę rozpraszania z kluczem bezpośrednim. Metoda ta polega na mnożeniu sygnału modulowanego przez sekwencję kodów zwaną sygnałem kluczującym. Umożliwia ona przez wielu nadawców jednoczenie w tym samym paśmie. Sygnał modulowany metod rozpraszania z kluczowaniem bezpośrednim zajmuje więcej pasma ni sygnał modulowany. Aby odczytać zakodowany sygnał, odbiorca musi dysponować układem deszyfrującym z tym samym i jednocześnie zsynchronizowanym ciągiem kodowym co nadawca.

Jakie są zalety nadawania w paśmie z poszerzonym widmem?
— Dużą odporność na zakłócenia.
— Zamiast przydziału częstotliwości lub czasu przydział ziarna generatora pseudolosowego.
— Pojemność sieci dobierana dynamicznie.

Jaki skutek daje zastosowanie taktów zezwalających w sieci Slotted Aloha? Powodują one, iż jeżeli nastąpi kolizja to na całej ramce. W efekcie wykorzystanie łącza podwaja się.

Wymień stosowane modyfikacje sieci Aloha.
— Slotted Aloha – urządzenie można rozpocząć nadawanie tylko w określonych chwilach czasowych.
— MOBITEX – pakiet wysyłany jest w czasie zależnym od jego priorytetu. Przy retransmisji priorytet pakietu jest zwiększany.
— Binder (1975) – (dla stałej, znanej liczby stacji) okres nasłuchiwania podzielony na przedziały, każdy przedział ma właściciela, w przypadku konfliktu tylko właściciel ma prawo reemisji.
— Crowther (1973) – (dla dużej i zmiennej liczby stacji) okres nasłuchiwania podzielony na przedziały, pusty przedział -¿ w następnym okresie można próbować go zająć, pomyślna emisja -¿ rezerwacja przedziału.
— Roberts (1973) – (dla dużej i zmiennej liczby stacji) okres nasłuchiwania podzielony na przedziały, ostatni przedział podzielony na N kwantów rezerwacji, losowy wybór kwantu na emisję żądania rezerwacji, potwierdzenie rezerwacji -¿ przydział przedziału.
— BTMA (Busy Tone Multiple Access) – kanał zajętości: CSMA (ton), kanał danych; efektywność 70
— SRMA (Slot Reservation Multiple Access) – kanał zajętości: CSMA (żadanie i odpowiedzi), kanał danych
— MACA (Mullllltiple Access with Collision Avoidance) – ramki: RTS, CTS, (DS, ACK, RRTS), dane

Omów przeznaczenie ramek sterujących w sieci typu MACA.
— RTS (Request To Send) – żądanie prawda do wysłania danych, ramka zawiera długość danych do wysłania;
— CTS (Clear To Send) – nadanie prawa do wysłania danych, ramka zawiera długość danych do odbioru;
— DS ?
— ACK (Acknowledgement) – potwierdzenie odbioru;
— RRTS ?

Czy w sieci Token Bus mogą nadawać stacje nienależące do pierścienia? Mogą, gdy zostają do niego dopiero podłączone.

Omów funkcję monitora w sieciach pierścieniowych.
— wyznaczanie taktów zegara,
— obsługa ramek awaryjnych,
— inicjalizacja pierścienia,
— wspomaganie rozgładzania,
— usuwanie zgubionych ramek.

Kiedy i dlaczego ramkę powinna poprzedzać preambuła? Preambuła jest stosowana w transmisji synchronicznej i dokonuje zsynchronizowania zegarów nadawcy i odbiorcy. Preambuła ta jest ciągiem impulsów zero-jedynkowych o ściśle określonym czasie trwania i ilości. (Preambuła w transmisji synchronicznej nie przekracza 25 impulsów). Wysyłana jest raz na początku przesyłu danych, a później powtarzana tylko wtedy, gdy nastąpi rozsynchronizowanie

(system śledzi ilość pojawiających się błędów, i na tej podstawie określa czy rozsynchronizowanie nastąpiło). Synchronizacja jest podtrzymywana przez zegary systemowe.

Wymień podstawowe typy sieci pierścieniowych i omów istotę ich działania. Patrz wyżej.

Wymień standardy szybkich sieci izochronicznych. (Izochroniczne–gwarancja pasma).
FDDI II, Iso-Ethernet, Fibre Channel, ATM

Wymień zalety i wady rozwiązań EPON. Zalety:
— minimalizacja włókien światłowodowych,
— minimalizacja liczby portów optycznych,
— splittery optyczny nie wymaga zasilania,
— łatwiejsze zarządzanie (splliter nie wymaga konfiguracji),
— niskie koszty utrzymania,
— istnieją rozwiązania z oknem dla telewizji kablowej.
Wady:
— brak redundantnych dróg,
— mniejsze pasmo (stały przydział),
— uniemożliwia przyszłe zwiększenie przepustowości - DWDM,
— ograniczenia w rozbudowie i skalowaniu,
— wiązanie się z jednym dostawcą (urządzenia różnych producentów mogą być ze sobą niekompatybilne),
— rozwiązanie ciągle drogie.

4. Media transmisyjne

Czy szybkość modulacji i prędkość transmisji są sobie równe? Nie. Szybkość modulacji określe szybkość z jaką zmieniają się stany na łączu. Prędkość transmisji uzależniona jest od szybkości modulacji oraz zastosowanego kodowania.

Jakie są zalety łącz światłowodywych?
— od 10 do 100 km bez regeneracji,
— przepustowość teoretycznei nawet do 50 Tbps,
— niewrażliwość na zakłócenia elektromagnetyczne,
— odporny chemicznie,
— trudny do podsłuchania oraz
— lekki (1000 skrętek na 1 km – 8 ton, 2 światłowody (większa pojemność) – 100 kg).

Porównaj cechy użytkowe kabli miedzianych i kabli światłowodowych. Patrz wyżej.

Scharakteryzuj podstawowe topologie sieci pod względem niezawodności, skalowalności i łatwości rozgłaszania.

Topologia gwiazdy rozmiar ograniczony wydajnością węzła centralnego, łatwe zarządzanie, wymaga niezawodności węzła cętralnego, drogie rozgłaszanie.

Topologia oczkowa (większa liczba łuków łączących węzły) dobra niezawodność, odporna na nasycenie transmisji, problem wyboru drogi.

Topologia szyny rozmiar ograniczony przepustowością szyny, łatwe rozgłaszanie.

Topologia pierścieniowa (węzły emitują odbierany strumień danych) odporna na nasycenie transmisjami, łatwe zarządzanie, uszkodzenie węzła unieruchamia sieć.

Topologia drzewiasta (przodek nadzoruje komunikację pomiędzy swoimi potomkami) względnie łatwe zarządzanie, ryzyko nasycenia transmisjami węzła(ów) centralnego(ych).

Jaki ma wpływ fizyczna topologia torów kablowych na topologię połączeń? Mały, tzn. można realizować różne topologie połączenia niezależnie od torów kablowych jednak dopasowanie torów kablowych do topologii sieci może ułatwić jej realizację.

Jakie topologie połączeń fizycznych można poprowadzić w kanalizacji o topologii gwiazdy? Dowolne, patrz wyżej.

Jakie są stosowane rozwiązanai zwiększające niezawodność topologii:

gwiazdy? Stosuje się redundantne urządzenie centralne,

szyny? Zapasowa, druga szyna.

pierścienia? W momencie zaniku prądu/awarii urządzenia wejście i wyjście interfejsu jest zwierane. Stosuje się dwa pierscienie działające w przeciwnych kierunkach i w momencie awarii urządzenia oba pierscienie u sąsiadów są zwierane.

5. Podstawy okablowania strukturalnego

Jakie są cele budowy okablowania strukturalnego?
— Eliminacja różnoroności okablowania,
— okablowanie niezależne od aplikacji,
— niezawodność infrastruktury kablowej,
— niższa cena oraz
— większa estetyka

Co to są pigtaile? Jest to krótki kawałek łącza światłowodowego, zakończony z jednej strony odpowiednią końcówką (stykiem). Zamontowanie końcówki do łącza jest trudne, gdy połączenie dwóch

kabli światłowodowych może wykonać byle technik z odpowiednim sprzętem.

Co to są patchcordy? Krótkie kable o ustandaryzowanej długości do bezpośredniego łączenia urządzeń.

Podaj podstawowe wymagania na zasilanie energetyczne urządzeń sieciowych.
— Wydzielone obwody zasilania energetycznego dla sieci komputerowej,
— UPS-y,
— agregaty prądotwórcze,
— konieczność separacji kabli elektrycznych od kabli sieci komputerowej,
— wspólny punkt uziemienia dla całego budynku,
— koooonieczność ochrony gniazd zasilania komputerów przed dołączeniem innych urządzeń,
— wyłączniki różnicowoprądowe oraz
— uziemienie ekranów okablowanai i ekranów urządzeń.

Jakie testy prowadzone są w instalacjach okablowania strukturalnego?
— lokalizacja kabli,
— weryfikacja długości kabli,
— integralność skrętek (wykrywanie błędów montażu),
— wykrywanie zwarć i przerw oraz
— pomiary zakłóceń elektromagnetycznych.

Dla łącz miedzianych: przesłuchy, stosunek sygnału do szumu, opóźnienia propagacji, współczynnik odbicia, tłumienność, impedancja charakterystycznej, pojemność elektryczna, oporność.

Dla łącz światłowodowych: tłumienność.

6. Transmisja danych

Dlaczego stosuje się transmisję asynchroniczn mimo jej niskiej efektywności względem transmisji synchronicznej? Względy historyczne (?), a ponadto nie wymaga ona synchronizacji zegarów urządzeń i wypełniania ciszy sygnałem, gdy tymczasem w wielu zastosowaniach wolniejsza transmisja w zupełności wystarcza, a jest prostsza do zaimplementowania.

Wymień co najmniej 3 metody synchronizacji ramkowej stosowane w transmisji asynchronicznej/synchronicznej. Niestety nie do końca mam pojęcie, które są synchroniczne, a które asynchroniczne.

— DDCMP (DEC) – transmisja bajtowa, nagłówek o stałej długości zawiera dłguość danych.
— BISYNC (IBM) – transmisja znakowa, cisza wypełniona przez SYNC, nagłówek rozpoczynany przez SOH (Start Of Header) i różne inne kody sterujące tj. STX (Start of TeXt), ETX (End of TeXt).
— SDLC (IBM) – transmisja bajtowa, unikalny bajt synchronizacji 01111110 (6 jedynek), cisza wypełnioana przez 11111111 (8 jedynek), znak zwolnienia pętli 11111110 (7 jedynek), po 5 jedynkach wstawwiany/usuwany bit 0.
— Technika naruszania kodu.
— Dodatkowe medium dla synchronizacji.

Wymień metody detekcji błędów binarnych. Echo, powtórzenie, kody detekcyjne (np. CRC, bit parzystości poprzecznej/poprzecznej i podłużnej), kody korekcyjne (np. kod Hamminga).

Jak wykrywane są błędy seryjne? Stosowane jest rozpraszanie (scrambling).

Jakie są zalety stosowania CRC w detekcji błędów? Umożliwiają one wykrywanie większej liczby błędów niż bity parzystości przy mniejszej nadmiarowości.

Jaki jest konieczny narzut bitowy dla korekcji pojedynczych bitów? $m + r < 2^r$, gdzie m liczba bitów danych, r liczba bitów parzystości (transmitowane słowo ma długość $m + r$ bitów).

Jakie są zalety i wady stosowania potwierdzeń pozytywnych ACK i negatywnych NAK? ACK: wiadomo na pewno, które pakiety dotarly do odbiorcy, ale istnieje konieczność wysyłania wielu zbędnych potwierdze przy transmisji poprawnej.

NAK: wysyłamy tylko informację o tych pakietach, które nie dotarły, ale nadawca musi trzymać wszystkie pakiety od początku transmisji.

Kiedy lepiej stosowa potwierdzenia negatywne (NAK) niż pozytywne (ACK)? Zależnie od tego jak dużo pakietów jest gubionych i czy połączenia są krótkie czy długie. Jeśli pakiety nie są gubione i połączenia są krótkie–NAK, wpp.–ACK.

Jak powinien być dobierany poziom niskiej i wysokiej wody w mechanizmie sterowania przepływem? Tak, aby urządzenie miało jeszcze miejsce na przyjęcia danych wysłanych przez drugą stronę, gdy ta nie odebrała jeszcze informacji o tym, aby przestać wysyłać dane oraz tak, aby po wysłaniu informacji, że można juz przesyłać dane, zanim druga strona zacznie to robić mieć jeszcze coś w buforze, aby móc te dane analizować.

Co to jest protokól XON / XOFF? Jest to protokół sterowania przepływem polegający na tym, iż gdy bufor odbiorcy jest pełny wysyła informacje do nadawcy, żeby przestał nadawać, a gdy już jest miejsce w buforze, aby znowu zaczął nadawać.

Oznaką tego protokołu jest działanie klawiszy Ctrl+S/Ctrl+Q pod różnej maści uniksami.

Dlaczego w protokole Bit Alternate konieczne jest numerowanie ramek danych? Gdyż nadawca może wysłać drugi raz tę samą ramkę, gdyż potwierdzenie jeszcze do niego nie dotarło lub zostało zgubione.

Dlaczego w protokole Bit Alternate konieczne jest numerowanie ramek potwierdzeń? Gdyż jak powyżej nadawca może wysłać dwa razy ramkę D0, a odbiorca dwa razy ACK, tyle że po odebraniu pierwszego ACK nadawca wyśle D1 i odbierze drugie ACK (przeznaczone dla ramki D0).

Czy mechanizm okna przesuwnego mona stosowa w transmisji znakowej czy datagramowej? W obu. W przypadku transmisji znakowej mamy po prostu bardzo dużą ziarnistość okna. W przypadku transmisji datagramowej ziarnistość jest taka jak największy możliwy datagram, ale za to jest mniej „slotów".

Kiedy w protokole warstwy N można nie realizować sterowania przepływem? Kiedy jest to zrealizowane w niższej warstwie.

Jakie są wady i zalety retransmisji selektywnej względem retransmisji seryjnej? Mniejsza ilość retransmitowaych danych, ale trudniejsza obsługa (konieczność rekonstrukcji ciągłych serii ramek) oraz buforowania zarówno po stronie nadawcy, jak i odbiorcy (przy retransmisji seryjnej tylko po stronie nadawcy),

Na czym polega zaleta kodowania Huffmana? Nie wymaga separatora, działa „nieźle" dla różnych rodzajów danych (optymalny w swojej klasie).

Jaki rodzaj komutacji jest najbardziej efektywny przy wysyłaniu bardzo krótkich a jaki przy wysyłaniu bardzo długich komunikatów? Przy wysyłaniu bardzo krótkich komunikatów najlepsza jest komutacja pakietów. Przy wysyłaniu bardzo długich komunikatów lepsza może być komutacja obwodów lub komunikatów.

Na czym polega zaleta komutacji pakietów wzgldem komutacji komunikatów? Komutacja pakietów jest szybsza względem komutacji komunikatów.

7. Aspekty bezpieczeństwa sieciowego

Wymień podstawowe usługi kryptograficzne. Poufność, integralność, uwierzytelnianie, niezaprzeczalność, dyspozycyjność, kontrola dostępu. (?)

Porównaj własciwości szyfrowania strumieniowego względem blokowego.

Porównaj właściwości szyfrowania asymetrycznego względem szyfrowania symetrycznego. Odpowiadając na to pytanie obrażać będę inteligencję czytelnika.

Na czym polega mechanizm uwierzytelniania z użyciem szyfrowania asymetrycznego? Strona uwierzytelniająca posiada klucz publiczny strony uwierzytelnianej, losuje jakieś dane i zaszyfrowane wysyła drugiej stronie. Jeżeli w odpowiedzi otrzyma dane pierwotne to znaczy, że druga strona posiada odpowiedni klucz prywatny.

Ewentualnie strona uwierzytelniająca może wysłać drugiej dane niezaszyfrowane i oczekiwać na dane zaszyfrowane kluczem prywatnym–czy faktycznie są to te dane sprawdza deszyfrując je kluczem publicznym.

Jakie funkcje pełni zaufana trzecia strona?

Czym różnią się certyfikaty kwalifikowane od niekwalifikowanych? Kwalifikowany zawiera dane biometryczne osoby fizycznej i dane o wydającym i jego podpis/ (?)

8. Protokoł ISO HDLC

Czy HDLC stosowany jest w łączach synchronicznych czy w asynchronicznych? Synchronicznych.

Wymień protokoły pochodne od HDLC i podaj ich zastosowanie.
- SDLC (Synchronous Data Link Control): HDLC bazuje na SDLC,
- LAP (Link Access Procedure): CCITT, X.25
- LAPB (Link Access Procedure Balanced): X.25
- LAPD (Link Access Procedure, D-channel): ISDN,
- LAPX (LAPB extended): teletex,
- LAPM (ITU V.24): modemy,
- LLC (Logical Link Control): IEEE 802

Na czym polega istota trybów pracy HDLC, tj. NRM, ARM i ABM?
- NRM (normal responce mode)–stacja główna przepytuje podrzędne,
- ARM (asynchronous responce mode)–stacje podrzędne mogą się same zgłaszać, kolizje gdy wielopunkt,
- ABM (asynchronous balanced mode)–każda stacja pełni funkcję mastera i slave'a (punkt-punkt).

9. Protokół ISO TP

Jakie funkcje pełni protokół ISO TP?
— Adresowanie użytkowników,
— spójność niesionych danych, niezależnie od „środka transportu”,
— przezroczystość dla niesionych danych,
— wybór jakości komunikacji.

Co oznaczają klasy jakości usług świadczonych przez warstwę sieci? Określają usługi, które dana sieć zapewnia lub innymi słowy poziom niezawodności sieci–na ich podstawie dobiera się odpowiednie strategie działania protokołu.

Na czym polega rozłączanie explicite? Aby połączenie zostało uznane za zakończone, strona kończąca musi wysłać odpowiedni komunikat–nie uznaje się połączenia za zakończone po przesłaniu wszystkich danych.

Kiedy dana warstwa protokołu nie musi obslugiwa sterowania przepływem? Kiedy warstwa niższa to robi.

Czy jedna/o...

instancja transportu może używa wiele instancji sieci? Może.

instancja transportu może obsługiwać wiele instancji sesji? Może.

połączenie transportowe może wykorzystywać wiele połączeń sieciowych? Może.

Jakie nowe, względem ISO TP i TCP, funkcjonalności oferuje XTP? XTP umożliwia:
— multicast,
— zarządzanie grupami,
— priorytety,
— „rate and burst control”,
— optymalne otwieranie / zamykanie połączeń,
— 3 typy obsługi błędów: TCP, UDP, fast NAK,
— „out of band data”.
które są nowe nie wiem.

10. Protokół ISO SP

Jakie uslugi wiadczy protokól ISO SP?
— nawiązanie połączenia z innym uytkownikiem warstwy sieciowej,
— wymiana danych, zamknięcie połączenia,
— zerwanie połączenia,
— rozmieszczanie punktów synchronizacji w trakcie dialogu i w razie błędu wznowienie go od zadanego punktu,
— zerwanie dialogu i wznowienie od zadanego punktu synchronizacji,
— negocjacja stosowania żetonów w celu: (i) umieszczania punktów synchronizacji, (ii) zwalniania połączenia oraz (iii) wyboru transmisji dupleksowej i półdupleksowej.

Dlaczego ISO SP nie używa zegarów? Bo szczęśliwi czasu nie liczą?

Podaj przyklady zastosowania usług (protokołu ISO SP) wymiany danych:

zwykłych przesyłanie danych, np. stron w teletekście.

typowych tekst wprowadzany przez operatora w teletekście.

potencjałowych uzgadnianie możliwości urządzeń końcowych transmisja właściwości dokumentu w teletekście.

ekspresowych sygnalizowanie przerwań.

Podaj przykłady zastosowania małej i dużej synchronizacji w protokole ISO SP. Duża synchronizacja rozdziela jednostki dialogu (np. pliki przesyłane), a mała strukturalizuje dane wewnątrz nich (np. dzieli pliki na strony).

11. Protokoły ISO: PP, ASN.1

Czym jest składnia:

abstrakcyjna? Reprezentacja niezależna od rzeczywistej formy w jakimkolwiek środowisku.

transferu? Sposób zakodowania składni abstrakcyjnej w ciąg przesyłanych bitów; jednej składni abstrakcyjnej odpowiada wiele składni transferu oraz jednej składni transferu–wiele składni abstrakcyjnych.

Wymień co najmniej 3 składnie transferu. BER (Basic Encoding Rules), CER (Canonical ER), DER (Distinguished ER), PER (Packing ER), XER (XML ER), ECN (Encoding Control Notification).

Jaka jest podstawowa funkcjonalność protokołu ISO PP? Reprezentacja informacji i transfer jej między systemami otwartymi.

Do czego służy ASN.1? Do definiowania abstrakcyjnych struktur danych.

Zdefiniuj w ASN.1 przykladowy obiekt będący rekordem bibliograficznym.
— Wpis ::= SEQUENCE { autorzy SET OF Autor, tłumacze SET OF Autor OPTIONAL, tytuł PRINTABLE STRING, tytuł-oryginału PRINTABLE STRING OPTIONAL, Rok-Wydania INTEGER }

— Autor ::= SEQUENCE { imię PRINTABLE STRING, nazwisko PRINTABLE STRING }

Czemu służy i jak jest reprezentowany Object Identifier? Służy on do reprezentowania konkretnych obiektów urządzenia. Jest reprezentowany jako ciąg liczb całkowitych określających numery gałęzi w drzewie zdefiniowanych obiektów.

Jaka jest struktura kodowania BER?
— Wartość o określonej długości: etykieta - długość - wartość.
— Wartość ze znacznikiem końca: etykieta - 0x80 - wartość - 0x00 0x00.

Czy kodowanie BER umożliwia bezpośredni przesył liczb rzeczywistych kodowanych tak jak w popularnych koprocesorach zmiennoprzecinkowych? Tak, umożliwia to typ REAL (etykieta UNIVERSAL 9).

W jakim celu zdefiniowano tzw. wspólne elementy warstwy aplikacji? Wymień je. Wynik wspólnych potrzeb:
— ustalenie kontekstu współpracy–ACSE (Association Control Service Element),
— wykonywanie oddalonych operacji–ROSE (Remote Operation Service Element),
— niezawodne przekazywanie dużych obiektów danych–RTSE (Reliable Transfer Service Element),
— zapewnienie spójności rozproszonych danych–CCR (Commitment Concurrency and Recovery).

Czy standard ROSE rozwizuje problem operacji nieidempotentnych? Nie, operacja nieidempotentne stanowią problem przy używaniu standardu ROSE. (operacja idempotentna–taka, którą można cofnąć bez konsekwencji)

Na czym polega istotna różnica pomiędzy FTP i RTSE? RTSE eliminuje uszkodzenia w trakcie konsumpcji danych.

Na czym polega dwufazowe wykonanie transakcji? W pierwszej fazie serwer przyjmuje opis transakcji i przygotowuje się do jej wykonania oraz komunikuje zerwanie lub przyjęcie, a w drugiej żadna ze stron nie może zaproponować zerwania, serwer kończy wykonywanie transakcji lub (w razie awarii) przywraca stan początkowy.

Czy jedna transakcja może polegać na wykonaniu akcji przez kilka autonomicznych jednostek? Nie.

Zaproponuj sposób wykonywania transakcji z uwzględnieniem:

zegarów eliminujących zastój w przypadku padu serwera lub klienta.
— serwer przyjmuje transakcję,
— klient i serwer uruchamiają zegary,
— serwer rozpoczyna wykonywanie transakcji.
— serwer potwierdza wykonanie/wycofanie transakcji lub klient wycofuje transakcję.

Jeżeli od momentu uruchomienia zegara upłynie zbyt dużo czasu i nie przyjdzie potwierdzenie obydwie strony uznają transakcję za niewykonaną (i w takim stanie pozostawiany jest zasób).

jedno fazowego glosowania zakresu transakcji.

Co zawiera ISODE? Biblioteki implementujące ASC, ROS, RTS, PP, SP, TP. Ponadto FTAM, VT, generator stubs dla ROS, kompilator ASN.1. (zawierają wspólne API sieciowe, które może być zrealizowane zarówno na protokołach ISO OSI, jak i lekkiej wersji na TCP/IP.)

12. Standardy ITU-T: MSC, TTCN

Do czego jest używany MSC? Message Sequence Chart służy do opisu sekwencji wymiany komunikatów, jest używany do:
— definicji wymagań,
— specyfikacji pobudzeń wejściowych dla walidacji i weryfikacji,
— dokumentacji rezultatów symulacji,
— testów regresyjnych,
— specyfikacji niedozwolonych scenariuszy.

Czy MSC ma zdefiniowaną formalną semantykę? Ma formalną semantykę–algebrę procesów.

Do czego służy TTCN? Tree and Tabular Combined Notation służy do opisu testowania systemów reakcyjnych (protokołów, usług, systemów opartych na CORBA, API): testowania zgodności ze specyfikacją, wytrzymałości, nieregresji, integracji.

Co oznaczają akronimy PICS i PIXIT? PICS–Protocol Implementation Conformance Statements (restrykcje/uzupełnienia dotyczące protokołu).

PIXIT–Protocol Implementation eXtra InformaTion (np. konfiguracje sprzętu, rodzaje połączeń)

Z jakich części składa się specyfikacja TTCN?
— charakterystyka,
— deklaracje,
— uściślenia,
— zachowanie.

Jaki werdykt może dać test? Wynik pozytywny (pass), negatywny (fail) lub nie da sie okreslić (inconclusive).

Czy opis testu może być niedeterministyczny? Nie może być.

Jakimi wyrażeniami opisujemy zachowanie testera? W postaci drzewa decyzyjnego. (?) Zapisujemy czynności wykonywane przez testera, a następnie na podstawie rezultatów przechodzi się do kolejnych węzłów lub kończy test z określonym werdyktem.

Jakie obiekty mogą być parametrami w definicji testu?
— wartości zmiennych,
— odwołania do zmiennych,
— nazwy punktów dostępu,
— nazwy zegarów.

Do czego służą testy predefiniowanych zachowań? Określają akcje wykonywane niezależnie od bieżącej pozycji (np. opis sytuacji wyjątkowych).

Czy w TTCN jest możliwy opis testu rozproszonego? Nie, (?) a przynajmniej są w tym trudności.

13. Sieci X.25, FrameRelay i ATM

Kiedy pojawiły się pierwsze sieci X.25?
— USA–1976,
— Europa–1978 (Francja),
— Polska–1992 (CUPAK, POLPAK, NASK).

Jakie są podstawowe różnice między sieciami Internet i X.25? Sieci X.25 zapewniają jakość transmisji oraz dostarczenie pakietów i są połączeniowe. Sieci Internet nie.

Co rozumiemy przez pojęcie sieci X.25? Jest to sieć zbudowana wg standardów opisujących warstwę sieci, fizyczną i łącza:
— warstwa 1: protokoły X.21, X.21 bis, V.24 (RS232C),
— warstwa 2: HDLC, LAPB,
— warstwa 3: PLP (procedury połączeń wirtualnych).

Do czego służą urządzenia PAD? Packet Assembly/Disassembly umożliwiają dostęp do sieci X.25 urządzeniom działającym wg innych standardów, np. korzystając z połączenia telefonicznego (modem). (?)

Jakie są maksymalne przepustowości w sieciach X.25:

w (a)synchronicznym łączu dostępowym? w łączu dostępowym jest do 64kbps, ale jak to jest konkretnie w a/synchronicznych to nie wiem.

w łączu międzywęzłowym? do 2Mbps

Dlaczego wymiana clear confirmation pomiędzy DTE i DCE nie pociąga za sobą przesyłu pakietu poprzez sieć?

Na czym polega i do czego jest używane połączenie skrócone? Polega na przesyłaniu danych wraz z pakietem otwierającym i/lub zamykającym połączenie. Służy do przyśpieszenia transmisji szczególnie, gdy chcemy odebrać/wysłać tylko jeden pakiet danych po czym zerwać połączenie.

Co to są udogodnienia w sieciach pakietowych? Dodatkowe usługi oferowane przez operatorów. (?)

Wymień podstawowe różnice między X.25, FrameRelay i ATM.
— szybkość: X.25 do 2 Mbps, FR do 45 Mbps, ATM do 2,5 Gbps,
— koszt (od najtańszego): X.25, FR, ATM,
— różnice w opóźnieniach komutacji (od największych): X.25, FR, ATM,
— ATM: transmisja asynchroniczna, możliwość zmiany prędkości w trakcie połączenia,
— ATM: gwarancje QoS w mocno przeciążonych łączach,
— FR: prosty protokół, tanie wdrożenia na istniejących liniach telefonicznych (cyfrowych) i komputerach terminalnych.

Jakie mechanizmy obsługi przeciążeń są stosowane we FR?
— BECN (Backward Explicit Congestion Notification),
— FECN (Forward Explicit Congestion Notification),
— CLLM (Consolidated Link Layer Management)–zarządzanie w wydzielonym obwodzie o numerze 1023,
— Simple Control Flow–XON/XOFF.

Ile bajtów danych przenoszą komórki ATM? 48

Dlaczego wprowadzono kanały wirtualne w ATM?

Jakie funkcje pełni AAL?
— dzielenie pakietów na komórki i ewentualne ich wydłużanie,
— obsługa błędów,
— sterowanie przepływem,

Scharakteryzuj klasy usług w sieciach ATM.
— CBR (Constant Bit Rate)–emulacja komutacji z przełączaniem obwodów (np. dla telefonii, wideokonferencji, telewizji–bez kompresji),

— rt-VBR (real time Variable Bit Rate)–zmienna przepustowość, stały jitter (np. dla interaktywnego wideo, kompresowanego obrazu i głosu),
— nrt-VBR (non-real time Variable Bit Rate)–przepustowość zmienna, statyczne multipleksowanie służy optymalnemu wykorzystaniu sieci (np. dla transakcji bankowych, systemów nadzoru).
— ABR (Available Bit Rate)–przepustowość sterowana dla minimalizacji opóźnień i liczby gubionych pakietów,
— UBR (Unspecified Bit Rate)–np. dla TCP/IP
— UBR+-UBR z obsługą biru znakowania ruchu nadmiarowego.

Def. parametry					
Cell Loss Ratio	+	+	+	+	
Cell Transfer Delay	+		+		
Cell Delay Variation	+	+	+		
Peak Cell Rate	+	+	+		+
Sustained Cell Rate		+	+		
Burst Tolerance		+	+		
flow control				+	

Jakie są zalety i wady sieci ATM? Zalety:
— uniwersalność zastosowań,
— QoS,
— dopracowane zarządzanie ruchem,
— efektywne dla małych i średnich sieci.
Wady:
— narzut na sygnalizację–ponad 10%, dla IP 20-25%,
— czasochłonne składanie i rozkładanie pakietów–dla IP nawet bardzo wydajny procesor nie wygeneruje szybszego strumienia niż 622Mbps,
— nieskalowalne dla bardzo dużych sieci–w praktyce bez znaczenia, bo jest to problem tylko dla dużych sieci, których w praktyce się nie buduje.

14. Zarzędzanie sieciami

Wymień warstwy zarządzania TMN. Warstwy zarządzania (podział horyzontalny):
— biznesem (BML–Business ML),
— usługami (SML–Service ML),
— siecią (NML–Network ML),
— elementami sieci (NEML–Network Element ML).

Wymień obszary zarządzania wg ISO. Obszary funkcjonalne ISO (podział wertykalny):
— zarządzanie zachowaniem,
— zarządzanie uszkodzeniami,
— zarządzanie konfiguracją,
— zarządzanie sprawozdawczością, np. rozliczeniami,
— zarządzanie bezpieczeństwem.

Jakie są istotne różnice między wersjami protokołu SNMP?
— SNMPv2 wprowadza (i) szyfrowanie haseł oraz (ii) komunikację pomiędzy stacjami zarządzającymi,
— SNMPv3 wprowadza (i) złożone mechanizmy identyfikacji, prywatności, autoryzacji i kontroli dostępu, (ii) strukturę zarządzania–nazewnictwo jednostek, społeczności, polityk, użytkowników, zarządzania kluczem oraz (iii) język definiowania danych–odziedziczony z v2

Jaką funkcje pełni agent SNMP? Odpowiada na zapytania zarządcy, raportuje wyjątki/pułapki.

Jak są definiowane obiekty dla SNMP? ASN.1.

Co oznaczają pojęcia:

wspólnoty SNMP? Agent + zbiór stacji zarządzających; identyfikowani dla wspólnego zarządzania.

widok MIB? Podzbiór danych udostępnianych wspólnotom.

Jakie komunikaty obsługuje SNMP?
— Get-request–daj 1 lub wiele zmiennych,
— Get-next-request–daj następną zmienną,
— Get-bulk-request–daj grupę,
— Set-request–modyfikuj 1 lub wiele zmiennych,
— Inform-request–daj MIB,
— SnmpV2-trap–pułapka, informacja do stacji zarządzającej,
— Responce–zmienne lub informacje o błędzie do stacji zarządzającej.

Czym różni się typ Counter32 od Gauge32? Gauge32 sie nie przekręca.

Jakie jest przeznaczenie standardu RMON? Analiza ruchu w sieci (RMON1–warstwa 2, RMON2–warstwy 3-6).

Czy i dlaczego zalecane jest zdalne sterowanie zasilaniem przełączników, routerów i serwerów? Tak, aby móc je w każdej chwili zdalnie zrestartować nawet jeżeli się zawieszą itp.

Dlaczego w przełącznikach istnieje jednocześnie możliwość zarządzania poprzez interfejsy sieciowe, konsoli i AUX? Zasadniczo żeby mieć dostęp do urządzenia na wiele sposobów, np. zdalnie przez interfejs sieciowy, ale jak coś padnie to można przelecieć się na drugą stronę oceanu i podłączyć z konsolą bezpośrednio.

Jakie są zalety stosowania CVS do zarządzania konfiguracjami? Umożliwia trzymanie historii oraz dokumentację zmian–gdy przyjdzie nowy administrator będzie widział co się dzieje.