1. **W jakich technologiach QoS w sieciach komputerowych wykorzystywany jest miękki stan?**

W technologii IntServ.

2. **W jakich technologiach QoS w sieciach komputerowych wykorzystywany jest zarządzanie ruchem wyłącznie na brzegu sieci?**

W technologii DiffServ.

3. **Podaj definicję jakości usług w sieciach komputerowych (QoS).**

Jakość usług w sieciach komputerowych (Quality of Service, QoS) jest to poziom wydajności komunikacji w sieci niezbędny do poprawnego działania określonej aplikacji. Wydajność komunikacji może być mierzona w różny sposób, zależnie od zapotrzebowania aplikacji – może być to średnia lub minimalna ilość dostępnej przepustowości, średnie lub maksymalne opóźnienie, zmienność opóźnień, średnia lub maksymalna ilość traconych pakietów. QoS jest zapewniane przez mechanizmy sieci dające się sklasyfikować w cztery grupy funkcji: klasyfikacji, izolacji, kontroli dostępu i wydajności wykorzystania sieci.

4. **Scharakteryzuj wymagania QoS komunikacji głosu i obrazu.**

Komunikacja głosu i obrazu jest podatna na maksymalne opóźnienie oraz zmienność opóźnień, ale odporna na straty pakietów. Komunikacja głosu wymaga zwykle stałej, niewielkiej przepustowości ze względu na rodzaj stosowanego kodowania (zwykle Constant Bit Rate, CBR). Komunikacja obrazu wymaga zwykle zmiennej, dużej przepustowości (kodowanie Variable Bit Rate).

5. **Jakie są cechy charakterystyczne komunikacji określanej jako „przesyłanie strumieniowe”?**

Odbiorca komunikowanej informacji zaczyna jej przetwarzanie w momencie odebrania dostatecznej ilości danych, ale zanim zostaną odebrane wszystkie dane. Podczas gdy otrzymane dane są przetwarzane (na przykład odtwarzane jest wideo), kontynuowana jest komunikacja pozostałych danych.

6. **Jakie protokoły komunikacyjne mogą być wykorzystywane przez przesyłanie strumieniowe?**
   - RTP (Real-Time Transfer Protocol) – przesyłanie strumienia, kontrola, korekcja, zabezpieczenia
   - RTCP (Real-Time Control Protocol) – siostra RTP, współdziała z RTP, dostarcza pozapasmowo informacji kontrolnych dla RTP
   - RTSP (Real-Time Streaming Protocol) – funkcje związane z odtwarzaniem (pauza, przewijanie, itp.)
   - UDP (User Datagram Protocol)
   - RDT (Real Data Transport) – protokół transportowy dla danych audio/video rozwinięty przez RealNetworks w 1990 roku
   - MMS (Microsoft Media Services poprzednio NetShow Services) – transfer unicast, przez UDP lub TCP
   - RTMP (Real-Time Messaging Protocol) – głównie używany z Macromedia Flash Media Server do strumieniowania audio i video przez internet do klientów Adobe Flash Player

7. W jaki sposób można realizować komunikację dźwięku i obrazu w sieciach best-effort IP?

Poprzez stosowanie metod maskujących zmienną jakość komunikacji w sieciach best-effort oraz zmniejszających wymaganą przepustowość komunikacji. Metody te to między innymi: kompresja, buforowanie, radzenie sobie ze stratami pakietów – kody nadmiarowe, dodatkowy strumień niskiej jakości, przeplatanie danych w pakietach, odtworzenie informacji ze znajomości stanu początkowego i końcowego (interpolacja).

8. Jakich metod używa komunikacja VoIP do zapewnienia jakości w sieciach IP?

W celu niwelowania zmiennych opóźnień oraz ukrywania strat stosowany jest bufor adaptacyjny, w którym musi się znajdować pewna ilość otrzymanych pakietów pozwalających na odtwarzanie dźwięku przez pewien czas zwany opóźnieniem bufora. W celu utrzymania jak najniższej ilości strat pakietów wykorzystywana jest adaptacyjna korekta opóźnienia odtwarzania, która w przypadku dużej ilości strat pakietów (na ogół pakiety spóźnione) umożliwia na podstawie szacowanego opóźnienia sieci skorygować opóźnienie odtwarzania (np. przez wydłużanie okresów ciszy).
W przypadku utraty danych jest możliwość odzyskania utraconych danych poprzez kodowanie nadmiarowe, np. przy strumieniu wysokiej jakości znajduje się drugi niższej jakości, prawdopodobieństwo utraty obu informacji jest mniejsze.
Podział części na jeszcze mniejsze części które dodatkowo są poprzeplatane (wymieszane), umożliwia odtwarzanie pomimo straty kilku następujących po sobie pakietów. W celu ukrycia zgubionej porcji danych stosuje się maskowanie (wydłużenie ciszy, interpolacja itd..)

9. Opisz protokół RTSP.

RTSP (Real Time Streaming Protocol) to protokół warstwy aplikacji mający za zadanie sterowanie komunikacją strumieniową (dane są transportowane przez inny protokół, na przykład RTP), w wielu aspektach podobny do HTTP. Serwer RTSP utrzymuje sesje oznaczoną identyfikatorem, która łączy grupy strumieni i ich stanów, czyli podczas trwania sesji można otwierać wiele połączeń z serwerem w celu wysłania żądania RTSP dla sesji. RTSP może używać TCP lub UDP, jest protokołem stanowym (informacje wysłane od nadawcy mogą służyć do modyfikacji kolejnych żądań).
RTSP umożliwia realizację funkcjonalności „odtwarzacza audio/wideo”, czyli sterowanie rozpoczęciem, zawieszeniem, wznowieniem, zakończeniem odtwarzania.
Główne polecenia (metody) używane przez RTSP:
SETUP - umieszczenie zasobów serwera w strumieniu i utworzenie sesji, PLAY - uruchamia transmisje danych, PAUSE, REDIRECT - wykrywa, że sesja powinna zostać przeniesiona, PING, TEARDOWN - zwalnia zasoby serwera, czyli przerywa sesje.

10. Opisz protokół RTP.

RTP (skrót ang. Real Time Protocol) - protokół czasu rzeczywistego. Jest to standardowy format pakietu do transportu danych czasu rzeczywistego takich jak audio i wideo przez internet. Protokół ten został zdefiniowany w dokumencie RFC 1889. RTP służy do dostarczania danych o wymaganiach czasu rzeczywistego, jak na przykład interaktywne strumienie AV za pomocą połączeń multicast bądź unicast.

Aplikacje zazwyczaj używają protokołu UDP do transmisji danych, jednak RTP może być używane z innymi protokołami transportowymi.
RTP nie zawiera żadnych mechanizmów zapewnienia dostarczenia lub jakości usługi, opierając się w tej kwestii na niższych warstwach. Numer sekwencyjny zawarty w pakietach RTP pozwala zrekonstruować właściwą pozycję pakietu w sekwencji.
RTP składa się z dwu ściśle związanych elementów:

- RTP służącego do przesyłania danych o wymaganiach czasu rzeczywistego
- RTCP do monitorowania jakości usług i informacji o uczestnikach sesji

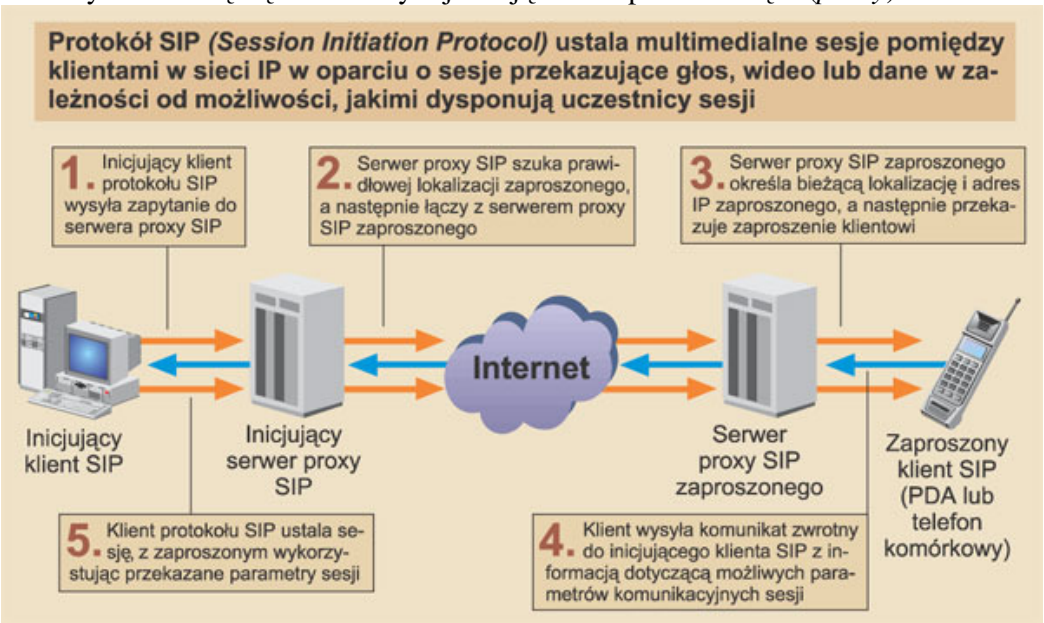
RTP określa strukturę pakietów przenoszących dane czasu rzeczywistego. RTP działa w systemach końcowych. Pakiet RTP zawiera znaczniki czasowe, informacje o kodowaniu, identyfikator sesji.
Pakiety o różnych typach mediów powinny być transportowane w osobnych sesjach RTP; inaczej powstają utrudnienia w dekodowaniu, miksowaniu i transporcie. Pakiety o tych samych typach powinny być transportowane w tej samej sesji RTP z zachowaniem oddzielnych identyfikatorów SSRC. Przykład sesji multimedialnej: Sesja RTP Audio port 5004, Sesja RTP Video port 5006, źródła synchronizacyjne unikalne dla każdego nadawanego strumienia (np. 1, 2, 3, ...)
RTP i RTCP są ściśle związane – RTP dostarcza dane czasu rzeczywistego a RTCP jest używany do dostarczania zwrotnej informacji odnośnie jakości usługi.
RTCP: Real Time Transport Control Protocol (or RTP Control Protocol)
Protokół kontrolny dla RTP działa w oparciu o okresowe transmisje pakietów kontrolnych do wszystkich uczestników sesji przy użyciu tych samych mechanizmów dystrybucji, co pakiety z danymi. Protokół transmisji musi zapewniać multipleksację danych i pakietów kontrolnych, np. za pomocą UDP.
RTCP pełni cztery podstawowe funkcje:

1. RTCP dostarcza informację o warunkach i jakości dystrybucji danych wszystkim uczestnikom sesji (raporty nadawcy).
2. RTCP przenosi stały identyfikator źródła RTP na poziomie warstwy transportowej, tzw. nazwę kanoniczną (CNAME). Ponieważ identyfikatory SSRC mogą się zmienić po wykryciu konfliktu lub restarcie aplikacji odbiorcy mogą użyć CNAME do określenia każdego uczestnika sesji.
3. Pierwsze dwie funkcje wymagają od uczestników wysyłania pakietów RTCP. Na ich podstawie można obliczyć ilość uczestników sesji i szybkość transmisji pakietów.
4. Funkcją opcjonalną jest przesyłanie minimalnego zestawu informacji kontrolnych dla sesji.

11. Opisz protokół SIP.

Protokół SIP (Session Initiation Protocol) jest protokołem warstwy aplikacji odpowiedzialnym za tworzenie, zmianę i kończenie sesji. SIP jest protokołem specyfikowanym przez IETF.
Z przyczyn wydajnościowych protokół SIP używa protokołu UDP, zaś użycie protokołu TCP jest opcjonalne. Ze względu na zawodną naturę protokołu UDP SIP zawiera własne mechanizmy retransmisji, w tym, podczas ustalania sesji, trójstronną wymianę komunikatów pomiędzy węzłami.
Protokołu SIP używa się do zaproszenia uczestników do sesji, natomiast protokół SDP (Session Descriptions Protocol) dekoduje główną część komunikatu SIP, zawierającą informacje o rodzaju mediów, których uczestnicy sesji mogą i chcą użyć. Natychmiast po wymianie i potwierdzeniu informacji wszyscy uczestnicy są zorientowani co do adresów IP uczestników, dostępnego pasma i rodzaju medium.

Następnie rozpoczyna się przekazywanie danych z użyciem odpowiedniego protokołu transportowego. Podczas całej sesji uczestnicy mogą, wysyłając dodatkowe komunikaty protokołu SIP, aktualizować sesję, np. dodać nowy zbiór mediów, dodać nowych uczestników sesji lub dokonać innych zmian.
Adresaci w protokole SIP są reprezentowane przez adresy URI (Uniform Resource Indicator), które mają formaty takie same jak adresy poczty elektronicznej. Oznacza to konieczność użycia systemu DNS do przekształcenia nazw hostów i domen na adresy IP.
W nawiązywaniu sesji uczestniczą oprócz agentów SIP serwery SIP, które służą do odnalezienia użytkownika o podanym adresie oraz umożliwiają przejście przez NAT. Serwery SIP dzielą się na serwery rejestrujące oraz pośredniczące (*proxy*).



12. Do czego służy klasyfikacja komunikowanej informacji (ruchu) w sieciach komputerowych?

Klasyfikacja komunikowanej informacji pozwala na zróżnicowanie jej obsługi przez sieć (rutingu, szeregowania w buforach) oraz na oddzielenie różnych klas ruchu (izolację) poprzez dodatkowe mechanizmy. Klasyfikacja może także służyć do odróżnienia ruchu zgodnego z kontraktem od ruchu niezgodnego (przekraczającego parametry ruchowe kontraktu).

13. Zdefiniuj kontrolę ruchu.

Kontrola ruchu (zwana także monitorowaniem ruchu, *policing*) służy do egzekwowania kontraktu ruchowego, który obowiązuje źródło komunikowanej informacji. Polega ona na dbaniu, by kontrolowany ruch nie przekraczał zadeklarowanych w kontrakcie parametrów (średnia prędkość, maksymalna prędkość, maksymalna wielkość serii). Kontrola ruchu może odrzucać ruch niezgodny z kontraktem lub zmieniać jego klasyfikację.

14. W jaki sposób można uzyskać wysokie wykorzystanie sieci?

Poprzez stosowanie komutacji pakietów oraz utrzymywanie sieci w stanie bliskim maksymalnego wykorzystania przez protokoły kontroli przeciążenia, takie jak TCP lub mechanizmy warstwy adaptacyjnej ABR w sieciach ATM. Dodatkowe

możliwości zwiększenia wykorzystania sieci dają mechanizmy inżynierii ruchu, które można stosować w sieciach MPLS lub ATM.

15. Zdefiniuj kontrolę dopuszczalności połączeń.
Kontrola dopuszczalności połączeń polega na sprawdzeniu, czy sieć posiada zasoby wystarczające do realizacji połączenia z żądaną jakością usług. Kontrola dopuszczalności połączeń może działać poprzez sprawdzenie na każdym przełączniku, czy są dostępne zasoby potrzebne do realizacji połączenia. Kontrola dopuszczalności połączeń może także działać na brzegu sieci we współpracy z centralną jednostką sterującą dostępnymi zasobami w sieci.

16. Opisz działanie kolejki priorytetowej.
Pakiety w kolejce są szeregowane według priorytetów (kolejkę opuszczają pierwsze pakiety o najwyższym priorytecie). Jest to mechanizm gwarantujący wywłaszczanie komunikacji o niższym priorytecie, ale mogący powodować zagłodzenie takiej komunikacji.

17. Opisz działanie kolejki WFQ.
WFQ (Weighted Fair Queuing) jest mechanizmem kolejkowania polegającym na podziale pamięci w buforze na wiele mniejszych niezależnych kolejek, z których każda jest przeznaczona dla pakietów należących do jednego przepływu.
WFQ przyznaje każdemu przepływowi (każdej kolejce) pewną wagę. Podział pasma pomiędzy przepływami zależy od przyznanych im wag.
Zaletami WFQ są proste zarządzanie i konfiguracja, eliminacja zawłaszczania łącza przez jeden przepływ, możliwość współpracy z RSVP.
Wadą jest brak możliwości implementacji wywłaszczania dla ruchu o większymi priorytecie.

18. Opisz mechanizm kontroli ruchu w sieci ATM.
Kontrola ruchu, zwana także monitorowania połączeń (*Usage Parameter Control*, *UPC*), ma na celu zabezpieczenie sieci przed naruszeniem kontraktu ruchowego przez źródło komunikowanej informacji. Mechanizmy kontroli ruchu są wykonywane na brzegu sieci ATM.
Kontrola ruchu wymaga zawarcia przez użytkownika i sieci ATM kontraktu ruchowego. Użytkownik określa w nim parametry ruchowe źródła oraz pożądane parametry jakościowe połączeń. Na ich podstawie funkcja kontroli dopuszczalności połączeń (*Call Admission Control*, *CAC*) podejmuje decyzję o akceptacji lub odrzuceniu wirtualnego połączenia. Przyjęcie połączenia narzuca na obie strony konieczność przestrzegania poprawności jego realizacji za pomocą funkcji kontroli ruchu.
Kontrola ruchu to procedura sprawdzania zgodności deklaracji użytkownika z rzeczywistym generowanym przez niego ruchem. UPC może używać algorytmu GCRA (generic cell rate algorithm), który pozwala na odrzucenie ruchu nadmiarowego. Algorytm GCRA działa na zasadzie „*leaky bucket*”.

19. Na czym polega klasyfikacja ruchu w sieci ATM?
Na podziale ruchu według klasy usług: CBR, VBR, ABR lub UBR. O klasie ruchu decyduje wybrana przez aplikację warstwa adaptacyjna.

20. Opisz kontrolę dopuszczalności połączeń w sieci ATM.
W sieci ATM kontrola dopuszczalności połączeń jest szczegółowa – każdy przełącznik na ścieżce sprawdza, czy może obsłużyć połączenie. Wymaga protokołu sygnalizacyjnego. Do wyboru najlepszej ścieżki o żądanej jakości usług służy ruting QoS.

21. Opisz kontrakt ruchowy w sieci ATM.
Kontrakt ruchowy w sieciach ATM określa parametry ruchu takie jak: Peak Cell Rate (PCR), czyli maksymalną szybkość wysyłania komórek (i maksymalną przepustowość); Sustainable Cell Rate (MCR), czyli średnią szybkość wysyłania komórek, i Maximum Burst Size, czyli maksymalną ilość komórek, które można wysłać z szybkością PCR.

22. Scharakteryzuj kategorie usług: CBR, VBR, ABR, UBR.
ABR – maksymalna i średnia przepustowość opisywana przez PCR i SCR; minimalizacja strat. Nadawca otrzymuje powiadomienia o przeciążeniu od sieci i powinien dostosowywać swoją przepustowość komunikacji.
UBR – odpowiednik best effort w IP
CBR - użytkownik deklaruje, ile potrzebuje przepustowości. Przepustowość, opóźnienie i zmienność opóźnień są gwarantowane na poziomie żądanym przez aplikację. Ta kategoria usług potrzebuje stałej przepustowości przez cały czas trwania połączenia.
VBR - użytkownik deklaruje średnią i maksymalną przepustowość (z gwarancją opóźnień lub nie).

23. Jakie warstwy adaptacyjne ATM są wykorzystywane przez usługi typu CBR, VBR, ABR, UBR?
CBR – AAL1
VBR – ALL2 i AAL5
ABR – AAL5
UBR – AAL3/4

24. Do czego służą adresy w sieciach ATM?
Adresy ATM są wykorzystywane jedynie do zestawiania połączeń, po zestawieniu połączenia nadawany jest 24-bitowy identyfikator określający wirtualny kanał (VCI) i ścieżkę (VPI). Komórki posiadające te same VPI i VCI tworzą wirtualne połączenie.

25. Jaka metoda komutacji jest stosowana w sieci ATM?
Komutacja wirtualnych kanałów – szczególny rodzaj komutacji pakietów.

26. Co to są połączenia wirtualne w sieci ATM?
Połączenie wirtualne w sieci ATM jest to stan sieci ATM pozwalający na komunikację pomiędzy punktami końcowymi tej sieci z wymaganą przez nie jakością usług. Połączenie wirtualne jest identyfikowane przez identyfikatory komórek składające się z dwóch części, identyfikujących wirtualne kanały (VCI) i wirtualne ścieżki (VPI). Połączenie wirtualne może być punkt-punkt (1-1) lub punkt-wielopunkt (1-m, *multicast*). Połączenie wirtualne może używać wielu kanałów i/lub ścieżek wirtualnych. Połączenie wirtualne jest nawiązywane przy wykorzystaniu mechanizmu kontroli dopuszczalności połączeń, który w razie przyjęcia połączenia tworzy stan w przełącznikach ATM stanowiący o rezerwacji odpowiednich zasobów, zależnie od

klasy połączenia. Klasa połączenia jest określana przez warstwę adaptacyjną ATM, która uczestniczyła w nawiązywaniu połączenia.

27. Scharakteryzuj technologię Integrated Services.
Integrated Services (IntServ) jest nieskalowalną technologią QoS w sieciach IP. Technologia IntServ wymaga utrzymywania przez rutery informacji o stanie dla poszczególnych połączeń. Kontrola dopuszczalności połączeń wymaga stosowania protokołu sygnalizacyjnego (Resource Reservation Protocol, RSVP). Parametrami kontraktu ruchowego są T-Spec (specyfikująca parametry ruchu) oraz R-Spec (specyfikująca wymaganą jakość usług). IntServ specyfikuje dwa rodzaje usług: usługe Controlled Load, gwarantującą minimalną przepustowość, oraz Guaranteed Load, gwarantującą żądaną przepustowość i opóźnienie.

28. Do czego służy protokół RSVP?
Protokół Resource Reservation Protocol służy do sygnalizacji kontraktu ruchowego i nawiązywania połączenia w procedurze kontroli dopuszczalności połączeń technologii IntServ. Każdy komunikat IntServ ma identyfikator sesji. Źródło wysyła komunikat Path, służący do inicjalizacji procedury rezerwacji zasobów. Rezerwacja jest dokonywana przez komunikat Resv, stanowiący odpowiedź na komunikat Path. Rezerwacje tworzone przez RSVP są jednokierunkowe. RSVP może także być wykorzystany do innych celów, na przykład do tworzenia wirtualnych kanałów w technologii MPLS.

29. Scharakteryzuj technologię Differentiated Services.
DiffServ to skalowalna technologia QoS w sieciach IP, oferująca statystyczne gwarancje QoS w obrębie jednej domeny DiffServ. W technologii DiffServ pakiety klasyfikowane są na brzegu sieci (domeny DiffServ) przez rutery brzegowe. Klasyfikacja wykorzystuje 6 bitowe pole DS (Differentiated Service), które składa się z części (6 bitów) nagłówka IP Type Of Service (TOS). Po sklasyfikowaniu, pakiety są przekazywane przez rutery szkieletowe zgodnie ze zdefiniowanymi regułami PHB (Per Hop Behavior). Reguły PHB są definiowane oddzielnie dla różnych klas ruchu, ale nie dla oddzielnych połączeń. Klasy ruchu to tzw. FEC (Forwarding Equivalence Classes).

30. Czym różni się technologia ATM od technologii MPLS?
Technologie ATM i MPLS to technologie komutacji pakietów, a dokładniej – wirtualnych kanałów. Obie posługują się przełączaniem etykiet (*label switching*). Jednak ATM jest technologią warstwy trzeciej i posiada zaawansowane funkcje QoS, podczas gdy MPLS jest technologią warstwy 2,5 i nie posiada funkcji QoS. Technologia MPLS może współpracować z wieloma warstwami sieci oraz łącza.

31. Opisz położenie technologii MPLS w modelu warstwowym.
MPLS znajduje się między warstwą łącza oraz sieci (warstwa „2,5").

32. Jaki jest związek technologii MPLS z rutingiem IP?
MPLS rozszerza i uzupełnia ruting IP. IP/MPLS może współistnieć z siecią IP (bez MPLS). Informacja przekazywana przez protokoły rutingu IP nie wystarczy dla MPLS, który potrzebuje jeszcze odwzorowania przekazywanego ruchu na etykiety. Jednakże MPLS wykorzystuje także informację pochodzącą z rutingu IP dla ustalenia, gdzie ma zostać przekazany pakiety (na który port przełącznika MPLS), jednakże

dodatkowo potrzebuje informacji o tym, jaką nadać etykietę przekazywanemu pakietowi.

33. Do czego służy technologia MPLS?

MPLS (Multiprotocol label Switching) - umożliwia inżynierię ruchu, ruting z ograniczeniami (w tym ruting QoS), zarządzanie sieciami VPN (ang. Virtual Private Network) w oparciu o IP. MPLS umożliwia zwiększenie wydajności szkieletu sieci poprzez uproszczenie komutacji (przekazywanie zamiast rutingu).
MPLS można stosować w powiązaniu z ATM, wtedy mamy pełne wykorzystanie parametrów jakości usług QoS, gdyż MPLS buduje sieć LSP w oparciu o połączenia wirtualne sieci ATM, w zwiazku z tym uzyskujemy zaawansowaną platformę do komunikacji multimedialnej.