# IP over ATM

# Spis treści

# 1. Wstęp

## 1.1. Protokół IP

IP (ang. Internet Protocol) jest obecnie dominującym (co nie znaczy najlepszym) wykorzystywanym globalnie, tzn. w Internecie protokołem transmisji danych. Standard IP over ATM zdefiniowany został dla wersji czwartej protokołu IP. Prowadzone są prace mające na celu uruchomienie IPv6 over ATM, ale nie ma na razie ani standardu, ani urządzeń prototypowych.

## 1.2. IP over ATM

Z uwagi na powszechność sieci LAN oraz popularność protokołu IP, zarówno ATM Forum, jak i gremia zarządzające Internetem uznały za celowe podjęcie kroków zamierzających do specyfikacji zasad współpracy sieci pakietowych (w tym sieci LAN) z siecią ATM. Prace prowadzone przez ATM Forum zaowocowały opracowaniem dwóch metod, pozwalających na łączenie i współpracę bezpołączeniowych sieci pakietowych LAN, bądź MAN, z połączeniowo zorientowaną siecią ATM. Tym samym sieć ATM może stać się szybką miejską siecią szkieletową dla rozproszonych sieci LAN. Może też być fragmentem sieci Internet.

Opracowane metody znane są jako:

• metoda emulacji sieci LAN na „wierzchołku" architektury ATM, nazywana metodą LAN Emulation (LANE);

• metoda naturalna (ang. native mode) współpracy z siecią ATM sieci LAN stosujących te same protokoły sieciowe; w przypadku sieci używających protokołu IP metoda „native mode" określana jest mianem „IP over ATM" (IPoATM); w metodzie „native mode" używane są mechanizmy bezpośredniego odwzorowywania adresów warstwy sieciowej na adresy ATM oraz przekształcania pakietów (datagramów) w komórki ATM; pewnym rozwinięciem metody IPoATM jest koncepcja współpracy wieloprotokołowej MPOA (ang. MultiProtocol Over ATM), dopuszczająca współpracę ATM nie tylko z sieciami TCP/IP ale także z innymi rozwiązaniami firmowymi, w tym np. wykorzystującymi sieciowe systemy operacyjne NetWare z protokołem IPX.

Jedną z podstawowych zalet ATM jest możliwość zagwarantowania pewnej określonej wcześniej kontraktem jakości obsługi (QoS ang. Quality of Service), a technologia IP over ATM, która wspiera QoS została zestandaryzowana.

Jak już wspomniano, wysoce wydajne przełączniki ATM są tańsze od wysoce wydajnych routerów. Poza tym mają one jeszcze jedną szczególną cechę – możliwość zarządzania pasmem. Zarządzanie to pozwala na równomierne obciążanie sieci bez jej przeciążania. Dzieje się tak dzięki mechanizmowi sprawdzania, czy dany węzeł i łącze są w stanie „poradzić sobie" z zapotrzebowaniem na określone pasmo, czy nie. Jeśli nie - kontrakt nie zostanie zawarty.

Pewne „szczątkowe" zarządzanie pasmem można zrealizować za pomocą routingu IP opartego na metrykach przypisanych do każdego łącza. Zakładając, że pewne łącze w pewnej sieci jest przeciążone przez większość czasu jego pracy, można zwiększyć wartości metryki, jaką ma to łącze w nadziei, że część ruchu zostanie skierowana inną drogą. Jest to „siłowe" rozwiązanie i na dodatek nie gwarantujące sukcesu. Inną metodą rozwiązania problemu zarządzania pasmem jest manualne stworzenie połączeń permanentnych w przełącznikach. Regulując przepływności każdego z łącz poprzez ich manualną konfigurację można regulować obciążenie poszczególnych fragmentów sieci. W praktyce może to przynieść lepsze wykorzystanie zasobów sieci niż czyste IP[1].

Podsumowując można powiedzieć, że technologia IPoATM nie jest nowością i stanowi mocną, stabilną kombinację stosowaną w obecnym Internecie. Jednakże stosując tę technologię napotykamy kilka istotnych problemów:

• IP jest protokołem warstwy sieciowej i nie może być uruchomiony nad „kablem". Musi zostać uruchomiony nad „czymś", w rozważanym przez nas przypadku, nad ATM, z reguły w jest on uruchamiany nad Ethernetem.

• Protokół IP jest bezpołączeniowy, natomiast ATM jest zorientowany połączeniowo. Używając protokołów sygnalizacyjnych sieć ATM ustanawia połączenia między hostami. IP jako bezpołączeniowy nie posiada żadnych mechanizmów sygnalizacji.

• Sieci IP i ATM mają własne protokoły rutingu. W IP są to: Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Border Gateway Protocol (BGP), natomiast w sieci ATM jest to Private Node-to-Node Interface (PNNI). Niestety, protokoły te nie są ze sobą kompatybilne.

• Sieci IP i ATM mają odmienny system adresacji urządzeń. Nie ma żadnej korelacji między nimi, tzn. adres ATM nie zawiera żadnej informacji o adresie IP danego urządzenia. Znając tylko adres ATM, nie można nic powiedzieć o adresie IP. Adres ATM jest 20 bajtowy: 13 bajtów prefiksu, 6 bajtów identyfikatora stacji (numer MAC interfejsu ATM) i 1 bajt selektora. Natomiast adres IP jest tylko 4 bajtowy, w dodatku jest on nadawany przez administratora; ma więc logiczny charakter dowiązania do interfejsu.

Standaryzacją rozwiązań IP over ATM zajmują się dwie organizacje: ATM Forum oraz Internet Engineering Task Force (IETF).

ATM Forum rozwija technologie znane jako Local Area Network Emulation (LANE) oraz Multiprotocol over ATM (MPOA). Nie są to dokładnie technologie IP, ale warto o nich wspomnieć, ze względu na podobne problemy i podobne sposoby rozwiązania. Rozwiązanie LANE opisuje, w jaki sposób można płynnie i prawie bezboleśnie przejść do sieci szkieletowej, opartej na ATM bez konieczności zmian logicznej struktury istniejącej sieci LAN. MPOA jest rozwinięciem LANE umożliwiającym budowę większych sieci - jak również sieci opartych na innych protokołach.

Organizacja IETF zdefiniowała metody enkapsulacji datagramów IP, zostało to szczegółowo opisane w RFC 1483 zatytułowanym „Multiprotocol Encapsulation over AAL5". RFC 1577 „Classical IP and ARP over ATM" opisuje szczegółowo samą technikę odwzorowywania adresów ATM na IP, i odwrotnie. IETF pracuje także nad standardem Multicast Resolution Server (MARS), który opisuje transmisję jeden do wielu, która to transmisja nie została zawarta w specyfikacji CLIP (ang. CLassical IP), oraz technologię Next Hop Resolution Protocol (NHRP), która umożliwia rozszerzenie możliwości CLIP.

[1] Pojęcie czyste IP oznacza metodę obsługi datagramów metodą największego wysiłku (ang. Best Effort).

# 2. Połączenia w sieci ATM

ATM jest protokołem połączeniowym z komutacją pakietów. Oznacza to, że przed rozpoczęciem transmisji danych musi zostać utworzone wirtualne połączenie pomiędzy nadawcą i odbiorcą, a przesyłane dane dzielone są na fragmenty przekazywane w kolejnych komórkach. Podstawowa operacja wykonywana przez komutator ATM jest bardzo prosta. Składają się na nią następujące kroki:

• odbiór komórki przez jeden z portów wejściowych komutatora;

• odszukanie identyfikatora VPI/VCI odebranej komórki w lokalnej tabeli translacji w celu określenia portu (lub portów) wyjściowego oraz nowej wartości VPI/VCI dla danego połączenia;

• retransmisji odebranej komórki przez odpowiedni port z nowymi wartościami VPI/VCI.

Tak prosty algorytm działania możliwy jest do zrealizowania jedynie dzięki wcześniejszemu stworzeniu lokalnej tablicy translacji, do czego wykorzystywane są mechanizmy uruchamiane przed rozpoczęciem transmisji danych. Przy tworzeniu i modyfikacji tablic wyróżnia się dwa podstawowe, ze względu na przebieg procesu zestawiania, typy połączeń ATM:

**PVC (ang. Permanent Virtual Connection)**; stałe połączenia wirtualne. Są to połączenia zestawiane przez pewien mechanizm zewnętrzny w stosunku do sieci ATM. Polegają one na przydzieleniu stałych wartości identyfikatorów VPI/VCI w zbiorze komutatorów na drodze pomiędzy dwoma wybranymi komutatorami ATM. System sygnalizacji oferowany przez ATM może ułatwiać zestawianie tego typu połączeń, jednak z definicji, zawsze wymagają one pewnej manualnej ingerencji administratora sieci.

**SVC (ang. Switched Virtual Connection)**; przełączane połączenia wirtualne. Są to połączenia zestawiane automatycznie przez protokół sygnalizacji ATM. Nie wymagają one manualnej interakcji, tak jak jest to wymagane w przypadku PVC i jako takie są dużo częściej stosowane. Wszystkie protokoły warstw wyższych operujące na ATM używają głównie tego rodzaju połączeń.

Proces tworzenia połączenia SVC, a w szczególności określenie drogi, którą przebywa żądanie zestawienia połączenia ATM (ang. ATM signaling request) oraz przesyłane w jego obrębie komórki kontrolowany jest przez odpowiednie protokoły routingu.

# 3. Classical IP over ATM na podstawie RFC 1577

## 3.1. Cele specyfikacji

Charakterystyki i możliwości sieci ATM różnią się od tych, które znamy z sieci LAN. Oto kilka podstawowych różnic:

• Sieci ATM są sieciami zorientowanymi połączeniowo. Stosują pojęcie połączenia wirtualnego (VC - Virtual Connection). Wyróżniamy dwa typy połączeń wirtualnych: permanentne (PVC - Pemanent Virtual Connection) oraz dynamiczne (SVC - Switched Virtual Connection). Żądania zestawienia połączeń SVC oraz zarządzanie nimi odbywa się dzięki sygnalizacji użytkownik-sieć (UNI User-Network Interface)

• Dane przesyłane przez połączenia wirtualne są dzielone na komórki 53 bajtowe (5 bajtów nagłówka i 48 bajtów danych).

• Cały proces mapowania jednostek danych użytkownika w pola danych komórek ATM odbywa się w warstwie adaptacji ATM (AAL - ATM Adaptation Layer). W momencie tworzenia połączenia wirtualnego przypisuje mu się odpowiedni typ AAL. Istnieją 4 typy AAL: „AAL1", „AAL2", „AAL3/4", „AAL5". Mapowanie IP oraz ARP realizowane jest tylko z AAL5. Jak już wcześniej wspomniano, typ AAL jest ustalany w momencie zestawiania połączenia, nie ma więc potrzeby aby informacja ta była przenoszona w nagłówku komórki ATM. W przypadku połączeń PVC typ AAL jest odgórnie ustalony przez administratora sieci, natomiast w przypadku SVC informacja ta jest przenoszona wzdłuż kanału wirtualnego (VC) jako część procesu zestawiania połączenia. Format ALL5 specyfikuje rozmiar pakietu, w którym użytkownik może przenieść maksymalnie (64K-1) bajtów danych. Proces enkapsulacji opisuje dokładnie dokument RFC 1483 „Multiprotocol Encapsulation over ATM Adaptation Layer 5". Tu wystarczy powiedzieć, że komórki ATM składające się na jeden PDU są transmitowane od pierwszej do ostatniej, a ostatnia określa koniec PDU. ATM gwarantuje, że kolejność komórek ATM nie zmienia się w trakcie transmisji, jest to oczywiste z uwagi na połączeniowość ATM - wszystkie komórki przekazywane są dokładnie tą samą trasą i nie mogą się „wyprzedzać". Natomiast AAL5 nie gwarantuje poprawności dostarczonych danych, funkcję tą pozostawiono protokołom wyższych warstw, które mogą zażądać retransmisji.

ATM Forum ustandaryzowało procesy zestawianie połączeń typu punkt-punkt oraz punkt-wielopunkt. Połączenia wielopunkt-wielopunkt pozostają nie zdefiniowane.

Celem specyfikacji IPoATM (IP over Asynchronous Transfer Mode) jest umożliwienie transmisji datagramów IP oraz komunikatów protokołu ATM Address Resolution Potocol (ATMARP) w warstwie adaptacji 5 ATM Adaptation Layer 5.

Historia standardu IP over ATM rozpoczęła się w styczniu 1994. Pierwszy oficjalny dokument to RFC 1577 „Classical IP and ARP over ATM".

Należy zaznaczyć wyraźny podział zakresu usług. Protokół IPoATM nie określa żadnych operacji sieci ATM. Usługi, takie jak tworzenie połączeń wirtualnych, czy to permanentnych, czy przełączanych używają AAL 5. Założenia dotyczące umieszczenia sieci ATM w dotychczasowych strukturach sieciowych opisują zastąpienie technologią ATM następujących elementów:

1. Sieci lokalne ( Ethernet, Token Ring, FDDI, ...).
2. Lokalne sieci szkieletowe pomiędzy już istniejącymi LAN'ami.
3. Dedykowane łącza lub permanentne połączenia frame relay pomiędzy routerami.

Dokument RCF 1577 zakłada, że sieć ATM zostanie wykorzystana do zastąpienia sieci, w których używa się protokołu IP. Autorzy dokumentu mają na myśli zarówno sieci lokalne, jak i rozległe linki łączące routery między domenami. Oto charakterystyka „klasycznego" (ang. Classical IP over ATM)modelu:

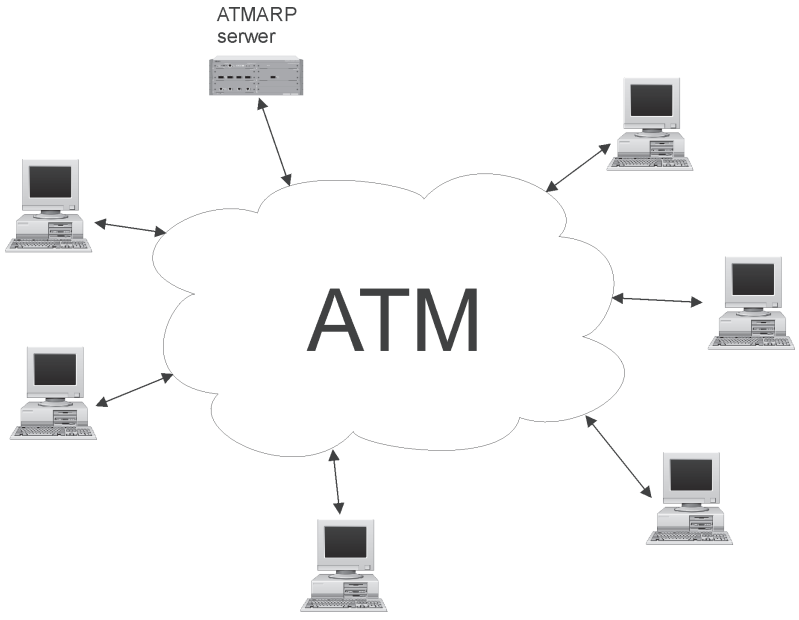
• Wszystkie wirtualne połączenia w obrębie jednej LIS używają tej samej maksymalnej jednostki transmisji MTU(ang. Maximum Transmission Unit). LIS (ang. Logical IP Subnetwork) to pojęcie logicznej podsieci IP, które zdefiniowano poniżej.

• Domyślnie stosowana jest metoda enkapsulacji LLC/SNAP.

• Do translacji adresów z IP na ATM stosowana jest usługa ATMARP. Komunikacja odbywa się wewnątrz LIS. Z punktu widzenia klienta (hosta w LIS, członka LIS) architektura sieci jest dokładnie taka, jak opisana w definicji LIS.

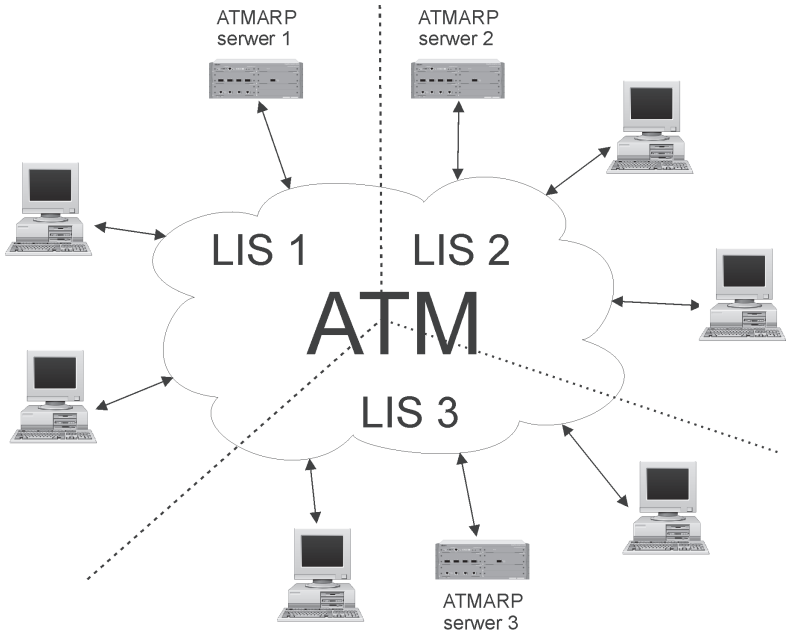
## 3.2. Konfiguracja podsieci IP

Autor dokumentu RFC 1577 opisuje początkowe umieszczenie sieci ATM w sieciach stosujących protokół IP jako bezpośrednie zastępstwo dla sieci lokalnych (Ethernet) oraz jako zastępstwo dla linków łączących routery. Sieci LIS opierają się na założeniu, że każdy administrator konfiguruje swoje hosty i routery (członkowie LIS) jako logiczną, zamkniętą (o skończonej liczbie członków) podsieć IP (rys. 3.1.).



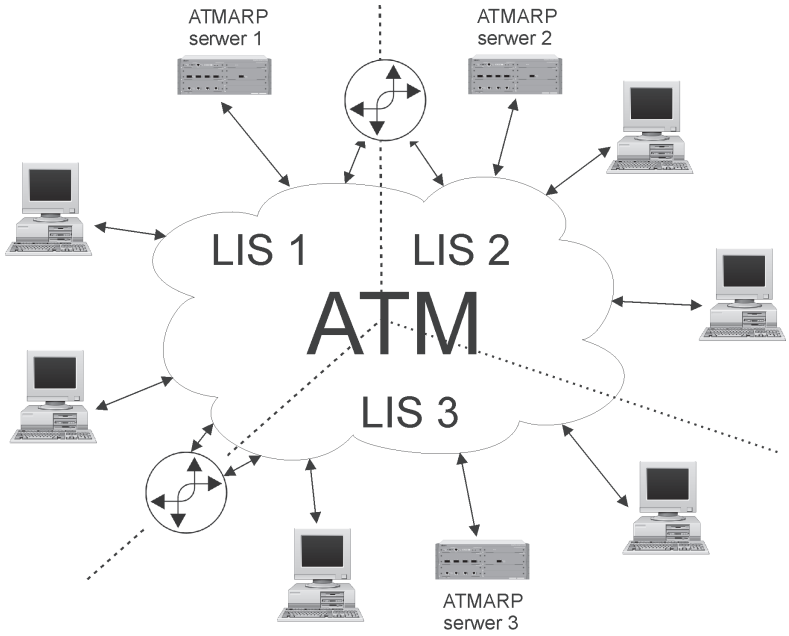

Rys. 3.1. Logiczna, zamknięta podsieć IP

Każda taka podsieć mimo, że istnieje ich wiele w jednej sieci ATM, działa niezależnie od innych LIS (rys. 2.).




Rys. 3.2. Trzy logiczne, zamknięte, niezależne podsieci IP

Komunikacja pomiędzy członkami tej samej LIS odbywa się bezpośrednio, natomiast komunikacja między członkami różnych LIS musi odbywać się za pośrednictwem routera. Sytuacja taka ma miejsce nawet wówczas, gdy istnieje możliwość zestawienia bezpośredniego połączenia między tymi członkami przez sieć ATM. Router musi być tak skonfigurowany, by być członkiem jednej lub więcej LIS (rys. 3.3.).




Rys. 3.3. Trzy logiczne, zamknięte podsieci IP, istnieje możliwość wymiany danych między członkami różnych podsieci.

Wymagania, jakie są stawiane członkom (ang. members) LIS - hostom, routerom:

• wszyscy członkowie posiadają ten sam adres IP sieci oraz maskę,

• wszyscy członkowie w obrębie LIS są bezpośrednio podłączeni do sieci ATM,

• wszyscy członkowie z poza LIS komunikują się za pośrednictwem routera,

• wszyscy członkowie LIS posiadają mechanizm umożliwiający translację adresów IP na adresy ATM dzięki protokołowi ATMARP. Gdy używane są połączenia SVC hosty/klienci muszą również dokonywać translacji odwrotnej z ATM na IP dzięki protokołowi InATMARP,

• wszyscy członkowie LIS używający PVC muszą posiadać mechanizm umożliwiający odwzorowanie istniejących połączeń VC na adresy IP stosując InATMARP,

• wszyscy członkowie LIS muszą mieć możliwość bezpośredniego połączenia z innymi członkami tej LIS.

Istnieją jeszcze dodatkowy wymóg, dotyczący każdego członka LIS. Każdy członek musi mieć możliwość przechowywania co najmniej 2 parametrów zdefiniowanych w RFC 1577:

• pojedynczy adres ATM (atm$ha),

• adres ATM serwera ATMARP zlokalizowanego w danej LIS (atm$arp-req). W przypadku pracy w środowisku połączeń SVC, żądania ARMARP wysyłane są właśnie na ten adres. Serwer ten posiada autorytatywną wiedzę na temat adresów wszystkich członków LIS. W przypadku pracy LIS w środowisku tylko połączeń PVC, parametr ten może nie mieć przypisanej żadnej wartości ponieważ żaden członek LIS nie będzie wysyłał komunikatów do serwera ATMARP.

Zaleca się także, aby routery, których zadaniem będzie rozszerzenie funkcjonalności technologii IPoATM posiadały możliwość łączenia ze sobą odrębnych LIS. W tym celu muszą one zdolne do przechowywania kilku zbiorów parametrów: atm$ha, atm$arp-req, jeden zbiór dla każdej podsieci. Kolejnym zaleceniem jest, by router miał możliwość należenia do wielu podsieci logicznych mimo faktu posiadania tylko jednego fizycznego portu ATM. Port ten powinien więc dopuszczać przyporządkowanie więcej niż jednego końcowego adresu ATM jednocześnie.

## 3.3. Format ramek danych

Implementacje IPoATM muszą być zgodne z enkapsulacją IEEE 802.2 LLC/SNAP opisaną w RFC 1483. LLC/SNAP jest domyślnym formatem ramki. Specyfikacja RFC 1577 nie ogranicza możliwości wykorzystania innych metod enkapsulacji, jednak w roku 1993 nie było, ani głosów sprzeciwu, ani propozycji użycia innych metod. Autorzy dopuszczają nawet możliwość, że w rozwinięciu standard pozwoli na negocjację metody enkapsulacji podczas zestawiania VC.

## 3.4. MTU

Domyślną wartością tego parametru dla urządzeń pracujących w technologii IP over ATM powinno być 9180 bajtów. Jednakże z powodu ośmio bajtowego nagłówka dodawanego do datagramu IP podczas enkapsulacji LLC/SNAP domyślna wartość MTU dla protokołu ATM AAL5 została ustalona na 9188 bajtów. Wartość ta może być inna, jednakże musi być spełniony warunek, wcześniej już opisany, obligujący wszystkie stacje w obrębie jednej LIS do posiadania jednakowej wartości MTU. Tu także autorzy dopuścili możliwość negocjacji tego parametru w trakcie zestawiania połączenia VC.

## 3.5. Translacja adresów ARP (Address Resolution Protocol)

Protokół ATMARP został stworzony na podstawie istniejącego protokołu ARP. RFC 826 opisuje działanie protokołu ARP w sieci Ethernet. InATMARP został oparty na RFC 1293 opisującym protokół InARP w sieci Ethernet. Protokoły ATMARP i InATMARP są tymi samymi protokołami, co ich odpowiedniki z sieci Ethernet, lecz dostosowanymi do pracy w sieci ATM. Użycie tych 2 protokołów jest różne w zależności od zastosowanego środowiska połączeń PVC lub SVC.

### 3.5.1. PVC

Stacje (członkowie LIS) muszą dysponować mechanizmem zapewniającym określenie, które PVC mają do dyspozycji. Może to być np. ręczna konfiguracja określająca identyfikatory połączeń VPI/VCI. W szczególności stacja musi wiedzieć, które połączenia wirtualne stosują enkapsulację LLC/SNAP.

Wszyscy członkowie pracujący w środowisku PVC używają protokołu InATMARP (Inverse ATM Address Resolution Protocol). Odbiorca podejmuje decyzje na podstawie identyfikacji połączenia wirtualnego, z którego otrzymał zapytanie (InATMARP Request), bądź odpowiedź (InATMARP Response). Gdy źródłowy lub docelowy adres ATM są nieznane (nie ma w tablicy wpisu o takim adresie), wtedy w odpowiednim polu określającym długość adresu ATM w pakiecie InATMARP musi zostać wstawiona wartość 0. Natomiast jeśli w tablicy jest wpis o takim adresie w odpowiednim polu pakietu InATMARP, należy wstawić poprawną wartość długości adresu oraz należy podać sam adres ATM w zależności od pytania. Szczegółowy format pakietu InATMARP jest przedstawiony dalej.

### 3.5.2. SVC

Środowisko połączeń SVC wymaga pewnej pomocy. Jest nią serwer ATMARP, który dysponuje autorytatywną wiedzą o wszystkich stacjach w LIS. Serwer musi należeć to tej samej LIS, którą obsługuje. Członków LIS obsługiwanej przez dany serwer ATMARP nazywa się też klientami tegoż serwera.

Serwer nie zestawia żadnych połączeń. Wszystkie czynności wykonują klienci. Członkowie LIS inicjują proces rejestracji w serwerze. Pojedynczy klient łączy się z serwerem używając połączenia VC. Po zakończeniu procedury zestawiania nowego połączenia wirtualnego VC używającego enkapsulacji LLC/SNAP, serwer wygeneruje żądanie InATMARP (InARP_REQEST) w celu ustalenia adresu IP klienta. Odpowiedź InATMARP (InARP_RESPONSE) klienta zawiera informacje, które umożliwiają serwerowi stworzenie tablicy (ATMARP cache). Na podstawie danych zapisanych w tej tablicy serwer odpowiada na zapytania ATMARP, które otrzymuje.

Mechanizm serwera ATMARP wymaga, aby każda stacja znała jego adres ATM. Wcześniej został zdefiniowany parametr atm$arp-req, jako jedna z 2 zmiennych, które klient musi przechowywać, to właśnie w nim przechowywany jest adres ATM serwera. Może istnieć tylko jeden działający serwer ATMARP w pojedynczej LIS. Zalecane jest aby serwer był również stacją IP. Stacja taka musi być tak skonfigurowana, aby działała i rozpoznawała samą siebie jako serwer ATMARP.

### 3.5.3. Wymagania operacyjne serwera ATMARP

Serwer akceptuje wywołania/połączenia od innych stacji ATM. W trakcie zestawiania połączenia, jeśli połączenie będzie obsługiwało enkapsulację LLC/SNAP, serwer wygeneruje do stacji wywołującej żądanie InATMARP (InATMARP_REQUEST) dla każdej LIS, którą obsługuje. Tzn. jeśli obsługuje np. cztery LIS, wyśle cztery żądania. Po odebraniu odpowiedzi InATMARP (InATMARP_REPLY), serwer sprawdza adres IP i adres ATM. Następnie serwer doda lub uaktualni wpis dotyczący tej stacji w tablicy ATMARP. Wpis składa się z adresu ATM, odpowiadającemu mu adresu IP, powiązanemu połączeniu VC oraz znacznika czasu. W przypadku gdy adres IP w komunikacie InATMARP duplikuje się z istniejącym już adresem IP w tablicy ATMARP, a adresy ATM, ten z tablicy i z komunikatu, różnią się oraz istnieje otwarte połączenie VC związane z tym wpisem w tablicy, informacja z komunikatu InATMARP jest ignorowana. Serwer nie wprowadza też żadnych zmian do tablicy. Wpisy w tablicy ATMARP pozostają do czasu, aż minie ich czas życia, bądź zostaną unieważnione. Zerwanie połączenia wirtualnego VC nie powoduje usunięcia wpisu z tablicy.

Serwer po otrzymaniu żądania (ATMARP_REQUEST) od dowolnego klienta, wygeneruje odpowiedni komunikat (ATMARP_REPLY), o ile tylko istnieje w jego tablicy wpis dotyczący stacji o adresie IP odpowiadającym poszukiwanemu adresowi IP. Jeśli nie, serwer wygeneruje odpowiedź negatywną (ATMARP_NAK). Mechanizm negatywnej odpowiedzi został wprowadzony w celu zwiększenia niezawodności protokołu IPoATM. Dzięki niej stacja, która zgłaszała żądanie potrafi rozróżnić sytuację awarii serwera od sytuacji, w której serwer nie posiada informacji, o którą pytała stacja. Format pakietu ATMARP_NAK jest identyczny jak pakiet ATMARP_REQUEST za wyjątkiem pola kodu operacji. Jest to kopia pakietu ATMARP_REQUEST z wartością 10 w polu kodu operacji, która oznacza ATMARP_NAK.

Gdy serwer otrzyma żądanie (ATMARP_REQUEST) poprzez połączenie VC, a adresy IP i ATM zgadzają się odpowiednimi adresami wpisu w tablicy ATMARP powiązanym z tym połączeniem VC serwer może uaktualnić czas życia wpisu w tablicy. Innymi słowy jeśli klient wysyła żądanie ATMARP używając tego samego połączenia VC, którego użył do rejestracji, serwer powinien zauważyć fakt, że klient ciągle „żyje" uaktualniając wpis w tablicy ATMARP.

Dodatkowo, dla zwiększenia niezawodności, kiedy serwer otrzyma ATMARP_REQUEST poprzez VC i dokonując analizy stwierdzi, że nie ma w swojej tablicy ATMARP żadnego wpisu łączącego adres IP i połączenie VC, z którego przyszło zapytanie oraz źródłowy adres IP nie jest powiązany z żadnym innym aktywnym połączeniem VC, wtedy serwer utworzy odpowiedni nowy wpis w tablicy ATMARP.

### 3.5.4. Wymagania operacyjne klienta ATMARP

Klient odpowiada za kontaktowanie się z serwerem ATMARP w celu rejestracji informacji o sobie, do jego obowiązków należy również zbieranie i odświeżanie własnych informacji o innych członkach LIS. Oznacza to, że klient ATMARP również posiada tablicę podobną do tablicy w serwerze, nie zawiera ona jednak informacji o wszystkich członkach LIS, ale tylko o tych, z którymi klient się kontaktował. Klient ATMARP musi:

• zainicjować połączenie wirtualne VC do serwera ATMARP, połączenie to będzie wykorzystane do transmisji pakietów ATMARP i InATMARP,

• odpowiadać na zapytania ATMARP_REQUEST i InATMARP_REQUEST nadchodzące z dowolnego VC,

• posiadać mechanizm umożliwiający generowanie pakietów ATMARP_REQUEST i wysyłanie ich do serwera, oraz interpretowanie odpowiedzi ATMARP_REPLY i ATMARP_NAK. Na podstawie tych komunikatów klient powinien budować/odświeżać własną tablicę,

• posiadać mechanizm umożliwiający generowanie pakietów InATMARP_REQUEST i wysłanie ich oraz interpretowanie odpowiedzi InATMARP_REPLY. Na podstawie tych komunikatów klient powinien budować/odświeżać własną tablicę,

• podobnie jak serwer używać funkcji czasu do określania wieku wpisów w tablicy i usuwać wpisy, które osiągnęły odpowiedni wiek.

Jeśli klient nie utrzymuje połączenia VC z serwerem, to musi odświeżać swój wpis w serwerze co 20 minut, otwierając nowe połączenia VC i wymieniając pakiety inicjujące.

### 3.5.5 Funkcja czasu w tablicy

Serwer i klient posiadają wiedzę o wszystkich otwartych połączeniach VC, ich powiązaniach z wpisami w tablicy i o tym, które z VC stosują enkapsulację LLC/SNAP.

Wpisy w tablicy klienta wygasają po 15, wpisy w tablicy serwera po 20 minutach.

Po upływie 20 minut serwer wysyła przez połączenie VC powiązane z wpisem, który właśnie wygasa, komunikat InATMARP_REQUEST. Jeśli otrzyma odpowiedź InATMARP_REPLY, nie usuwa wpisu, tylko go uaktualnia zerując licznik czasu. Gdy nie istnieje żadne połączenie VC związane wygasającym wpisem, wpis jest usuwany.

U klienta sytuacja różni się tym, że wpisy wygasają po 15 minutach. Jeśli wpis w tablicy klienta wygasa, a klient wie o istnieniu otwartego VC powiązanego z tym wpisem, to przed wysłaniem jakichkolwiek danych musi go uaktualnić. W środowisku PVC klient wysyła zapytanie InATMARP_REQUST bezpośrednio do klienta i aktualizuje wpis po otrzymaniu InATMARP_REPLY, natomiast w środowisku SVC wysyła zapytanie do serwera ATMARP.

### 3.5.6. Format ramek ATMARP i InATMARP

Adresy IP są przydzielane niezależnie od adresów ATM. Każdy host zna swoje adresy ATM i IP.

Pola protokołów są przydzielone następująco:

| | | |
|---|---|---|
| ar$hrd | 16 bitów | typ sprzętu |
| ar$pro | 16 bitów | typ protokołu |
| ar$shtl | 8 bitów | typ i długość źródłowego adresu ATM w bajtach (q) |
| ar$sstl | 8 bitów | typ i długość źródłowego podadresu ATM w bajtach (r) |
| ar$op | 16 bitów | kod operacji (żadanie, odpowiedź, NAK) |
| ar$spln | 8 bitów | długość źródłowego adresu protokołu w bajtach (s) |
| ar$thtl | 8 bitów | typ i długość docelowego adresu ATM w bajtach (x) |

| | | |
|---|---|---|
| ar$tstl | 8 bitów | typ i długość docelowego podadresu ATM w bajtach (y) |
| ar$tpln | 8 bitów | długość docelowego adresu protokołu w bajtach (z) |
| ar$sha | q bajtów | źródłowy adres ATM |
| ar$ssa | r bajtów | źródłowy podadres ATM |
| ar$spa | s bajtów | źródłowy adres protokołu |
| ar$tha | x bajtów | docelowy adres ATM |
| ar$tsa | y bajtów | docelowy podadres ATM |
| ar$tpa | z bajtów | docelowy adres protokołu |

w których:

ar$hrd – jest przypisany do rodziny adresów ATM Forum, przyjmuje wartość 19 dziesiętnie (0x0013)

ar$pro – dla protokołu IP przyjmuje wartość 0x0800

ar$op – możliwe kody typów operacji (dziesiętnie):

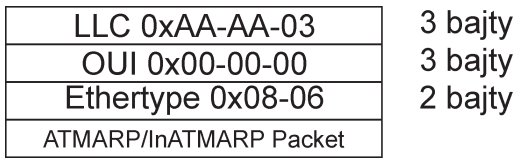
| | |
|---|---|
| ARP_REQUEST | =1 |
| ARP_REPLY | =2 |
| InARP_REQUEST | =8 |
| InARP_REPLY | =9 |
| ARP_NAK | =10 |

ar$spln – Dla protokołu IP wartość 4

ar$tpln – Dla protokołu IP wartość 4

### 3.5.7. Enkapsulacja pakietów ATMARP i InATMARP

Pakiety te muszą być enkapsulowane w PDU warstwy AAL5 za pomocą enkapsulacji LLC/SNAP. Pakiety są umieszczane w polu CPCS-PDU Payload pakietu AAL5 (rys. 3.4.).



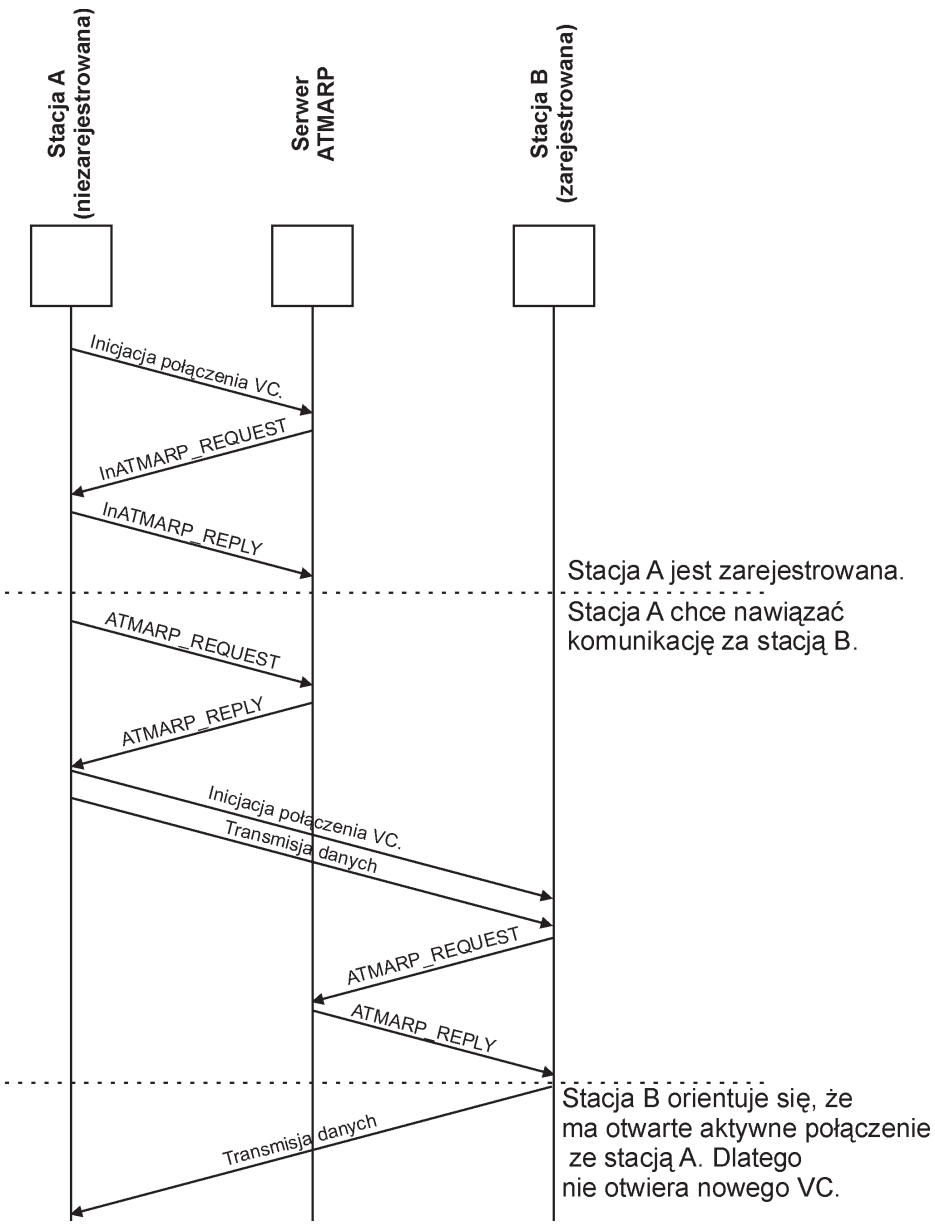

Rys. 3.4. Enkapsulacja pakietów ATMARP/InATMARP - format pola CPCS-PDU Payload pakietu AAL5

Wartość LCC 0xAA-AA-03, 3 bajty, zapowiada obecność nagłówka SNAP.

OUI 0x00-00-00, 3 bajty, informuje, że w następnych 2 bajtach będzie określony Ethertype.

Ethertype 0x08-06, 2 bajty, mówi, że zawartością jest pakiet ARP.

Całkowity rozmiar nagłówka LLC/SNAP jest na stałe ustawiony na 8 bajtów. Zawsze więc po 64 bitach od początku pakietu AAL5 CPCS-SDU rozpoczyna się pakiet ATMARP.




Rys. 3.5. Przykładowa wymiana komunikatów ATMARP w trakcie wymiany danych między stacjami A i B

## 3.6. Podsumowanie

W podsumowaniu należy wspomnieć, że autorzy FRC 1577 dostrzegli potrzebę istnienia zabezpieczeń. RFC 1577 nie definiuje żadnych sposobów szyfrowania danych. Nie ma też żadnych mechanizmów identyfikacji klienta. Stwarza to łatwe możliwości ataku, dzięki podszywaniu się pod innych klientów. Standard nie uwzględnia także takich możliwości jak określenia, których adresów ATM nie obsługuje.

Jest kilka kwestii, które autorzy pozostawili jako otwarte. Między innymi wypracowanie rozwiązania podobnego do działającego w specyfikacji LANE - adres ATM serwera LANE typu „well known”. Dzięki temu, klient nie musiałby znać adresu ATM serwera ATMARP, tylko szukałby go w sieci LIS na podstawie znajomości adresów typu „well known”.

Istnieją otwarte kwestie negocjowanych parametrów połączenia wirtualnego, takie jak: MTU, rodzaj stosowanej enkapsulacji.

Istnieje także problem „migotania". Ma on miejsce wtedy, gdy dwie stacje wywołają się wzajemnie i stworzą 2 połączenia VC. Wtedy jedno z nich musi zostać zwolnione, lecz standard nie mówi które. Może więc dojść do sytuacji, że oba VC zostaną zerwane i kolejne 2 zostaną wywołane. Efekt ten nazywa się właśnie „migotaniem". Najbezpieczniejszą metodą rozwiązania problemu jest pozostawienie zduplikowanych połączeń VC i oczekiwanie aż upłynie ich czas życia.

# 4. Materiały dydaktyczne do laboratorium

## 4.2. Materieały pomocnicze do realizacji ćwiczenia laboratoryjnego

### 4.2.1. Konfiguracja karty Olicom RapidFire OC-615X

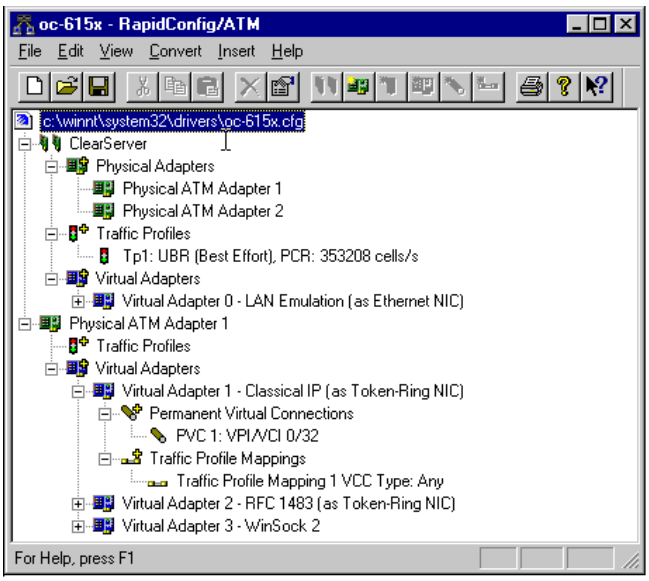
Konfiguracja karty jest odczytywana podczas startu systemu z pliku:

c:\windows\system\oc-615x.cfg

Stąd też wynika obowiązek restartu systemu po każdej zmianie dokonanej w tym pliku.

Istnieją dwie metody edycji tego pliku. Pierwszą z nich z nich jest edycja ręczna w dowolnym edytorze, druga metoda polega na wykorzystaniu specjalnie stworzonego do tego celu narzędzia : RapidConfig.

Widok okna programu RapidConfig przedstawia rysunek 4.7.




Rys. 4.7. Okno programu RapidConfig

Obsługa tego programu jest raczej intuicyjna i nie wymaga szerszego opisu. Wymaga go natomiast struktura pliku oc-615x.cfg, który będziemy edytowali ręcznie w edytorze Notepad. Struktura ramowa pliku wygląda następująco:

```
DefineAdapter
        DefineTrafficProfile 0
                <Traffic Profile Parameters>
        EndTrafficProfile
        DefineTrafficProfile 1
```

```
                <Traffic Profile Parameters>
            EndTrafficProfile
            ; More traffic profiles can be defined here ...
            <Adapter configuration parameters>
            DefineVirtualAdapter (LanEmulation|ClassicalIp|Rfc1483)
                DefineProfileMapping
                    <Traffic profile mapping parameters>
                EndProfileMapping
        ; More traffic profile mappings can be defined here ...
            <Virtual adapter parameters>
            EndVirtualAdapter
            ; More virtual adapters can be defined here ...
            DefinePvc
                <PVC parameters>
            EndPvc
            ; More PVCs can be defined here ...
        EndAdapter
        ; More adapters can be defined here ...
```

Linie rozpoczynające się znakiem „;” stanowią komentarz i nie są interpretowane przez system operacyjny.

Przykładowy plik konfiguracyjny Classical IP ( podobny do jednego z zadań na laboratorium):

```
DefineAdapter
    EnableSvcSupport No
    MasterTiming Yes
    DefineVirtualAdapter ClassicalIP
        IpAddress 192.168.1.1
        LanType Ethernet
    EndVirtualAdapter
    DefinePvc
        IpAddress 192.168.1.2
        Vpi   0
        Vci   133
    EndPvc
EndAdapter
```

Plik opisuje jedną ze stron połączenia back-to-back. Określa typ adaptera wirtualnego, typ sieci, adres IP adaptera oraz definiuje połączenie PVC z maszyną o adresie 192.168.1.2

Należy zwrócić uwagę na fakt, że nie ma znaczenia wielkość znaków użytych w słowach kluczowych, natomiast ważna jest ich kolejność. Nas interesował będzie taki zestaw słów kluczowych:

• DefineAdapter,
• EndAdapter,
• DefineVirtualAdapter,
• EndVirtualAdapter,
• DefinePvc,
• EndPvc,
• EnableSvcSupport,
• MasterTiming,
• IpAddress,
• LanType,
• Vpi,
• Vci,
• ArpServer,
• UniVersion,

Należy dokładnie zapoznać się każdym z tych słów kluczowych i jego opcjami.

Dokładny opis **wszystkich** parametrów, które można określić w pliku oc-615x.cfg na końcu dokumentu. Ma on charakter informacyjny. Nie należy się tego uczyć, ale warto mieć przy sobie na laboratorium.

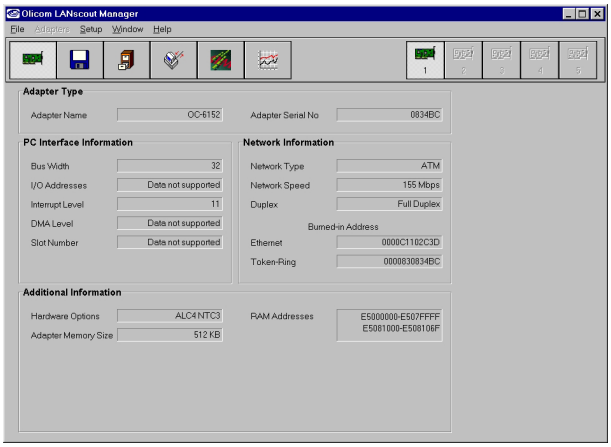
**UWAGA !** Oprogramowanie wymaga, zanim dokonamy zmian adresu IP karty ATM musimy dokonać tego w dwóch miejscach:

• w pliku konfiguracyjnym /windows/system/oc-615x.cfg,

• w systemie Windows - należy zmienić IP we właściwościach „Otoczenia Sieciowego” dla protokołu TCP/IP RapidCellDriver !!!

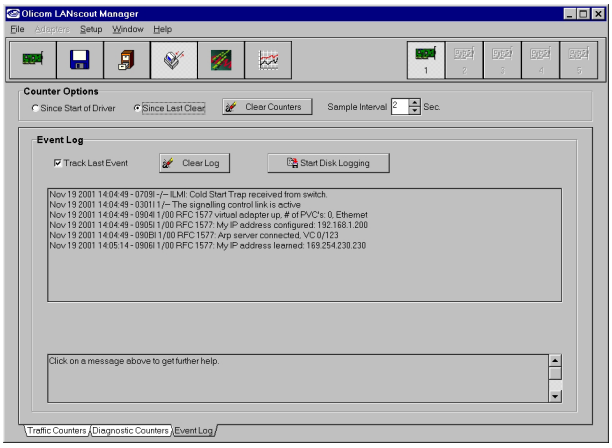
### 4.2.2. Kontrola poprawności działania karty ATM

Warto wspomnieć o narzędziu: Olicom LANScout Manager (rys. 4.8.). Jest to pakiet oprogramowania, który pozwala na obserwację zachowań karty ATM. Wyświetla on wszystkie komunikaty sygnalizacji UNI, potrafi je zapisać, rozpoznaje także pakiety usług IPoATM, LANE i potrafi je liczyć. Pakiet jest uruchamiany na starcie systemu, jest to ikonka w systray`u - koło zegara w Windows.

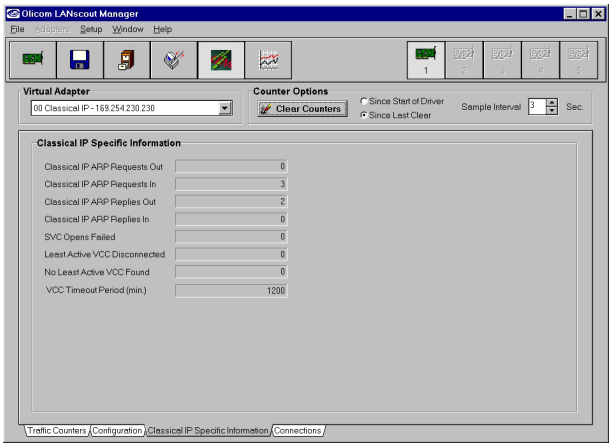



Rys. 4.8. Ilustracja głównego okna programu LANScout

Nas będą interesowały dziennik zdarzeń (rys. 4.9.) i liczniki pakietów (rys. 4.10.)




Rys. 4.9. Ilustracja dziennika zdarzeń (ang. log) programu LANScout




Rys. 4.10. Ilustracja licznika pakietów ATMARP programu LANScout

### 4.2.3. Konfiguracja przełącznika Olicom serii 9x00

Istnieje kilka podstawowych metod zarządzania urządzeniami sieciowymi. Są to:

- konsola – połączenie za pomocą portu RS-232,
- terminal – tak jak konsola, lecz po interfejsie np. Ethernetowym
- SNMP – Simple Network Management Protocol
- WWW – urządzenie ma wbudowany serwer WWW i można się z nim połączyć używając przeglądarki internetowej.

Urządzeniami serii 9x00 można zarządzać na 3 pierwsze sposoby. Pierwsze dwa są najmniej wygodne, ale gwarantują dostęp do wszystkich funkcji. Protokół SNMP pozwala tworzyć wygodne w użyciu narzędzia służące do zarządzania. Firma Olicom przygotowała taką aplikację: ClearSight.

Na pulpicie każdego komputera jest ikona „Network Infrastructure", po dwukrotnym kliknięciu wybieramy urządzenia (ang. devices). Po uruchomieniu pojawi się okno, w którym widoczne będą zarządzane urządzenia. Jeśli będzie ono puste, będzie trzeba dodać przełącznik/router same-

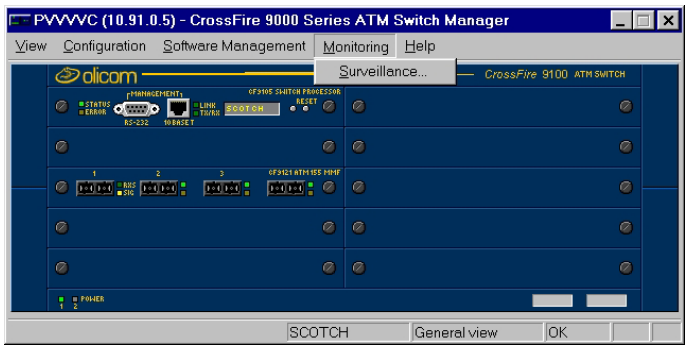
mu. Używamy do tego komendy Add. Przełączniki ATM firmy Olicom występują po symbolami CF-9100 i CF-9200. Chcąc dodać router wybieramy pozycję XL2-XL2Router.

W laboratorium używamy metody zarządzania: „SNMP over MAC" Pozwala to uniknąć niewygody związanej z adresami IP i przynależnością do danej sieci IP. Dodając urządzenie w nowopowstałym oknie podać adres IP bądź numer MAC (w zależności od wykonywanego ćwiczenia) urządzenia i nazwę (ang. label) pod jaką urządzenie będzie łatwo identyfikowane (przez Ciebie). Nazwa nie ma żadnego związku z nazwą na wyświetlaczu przełącznika. Może jednak być taka sama co ułatwia identyfikację. Adres IP podajemy w formacie XXX.XXX.XXX.XXX, natomiast numer MAC XX-XX-XX-XX-XX-XX

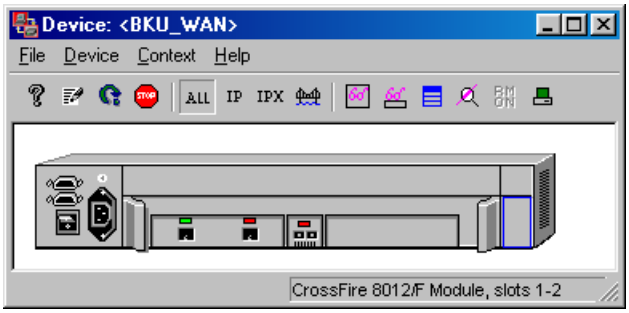
Po dodaniu urządzenia będzie ono widoczne w oknie, jednocześnie menager przeprowadzi test komunikacji z nim i określi jego status. Powinien być <zielony>. Gdyby zostało dodanych więcej urządzeń, menager będzie testował połączenia ze wszystkimi - taka operacja nosi nazwę ankietowania (ang. pooling), odpytywania.

Jeśli status jest <zielony>, ewentualnie <żółty> możemy kliknąć podwójnie na urządzeniu i powinniśmy zobaczyć widok dokładnie naszego urządzenia:

Jak widać na załączonych screenshotach (rys. 4.11. i 4.12.), są to aplikacje Windows, obsługiwane myszką –łatwe w obsłudze.




Rys. 4.11. Ilustracja aplikacji służącej do zarządzania przełącznikiem ATM




Rys. 4.12. Ilustracja aplikacji służącej do zarządzania routerem

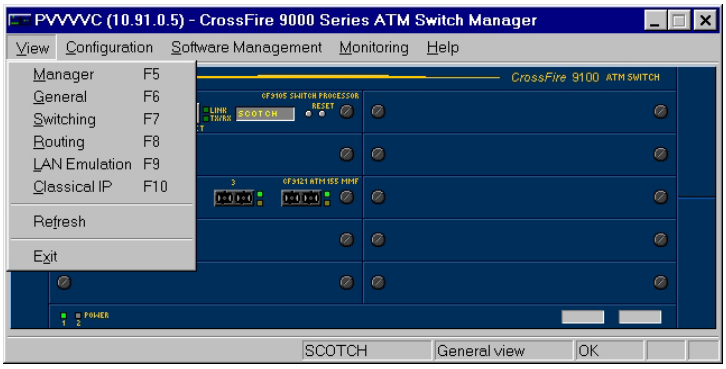
Na laboratorium będzie chwila na zapoznanie się z tą aplikacją i odszukanie takich opcji jak załączone tutaj:

- zestawianie połączeń PVC,
- ustawienia dotyczące CLIP,
- ustawienia serwera ATMARP,

• ustawienia klienta ATMARP,
• tablica ARP.

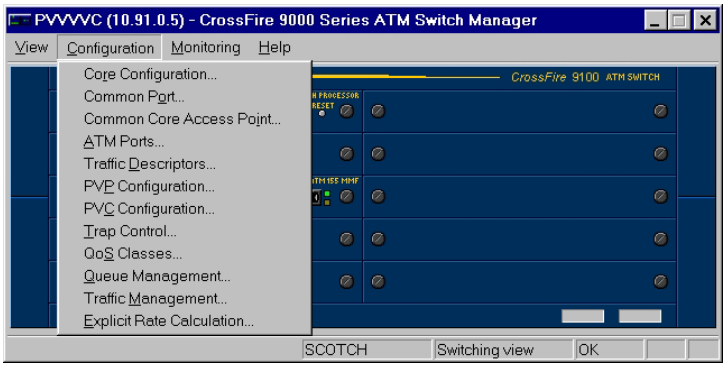
**Połączenia PVC**

Zestawienia połączeń PVC dokonuje się wybierając z menu „View” opcje switching (rys. 4.13.).



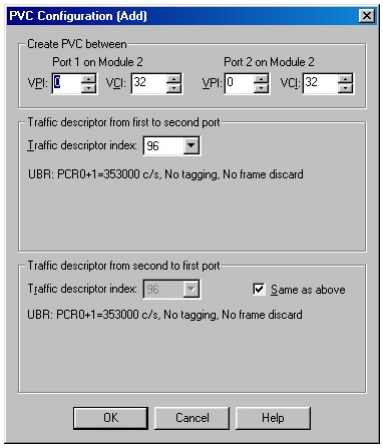

Rys. 4.13. Menu View

Następnie w opcji „Configuration” wybieramy „PVC Configuration” (rys. 4.14.).




Rys. 4.14 Menu Switching/Configuration

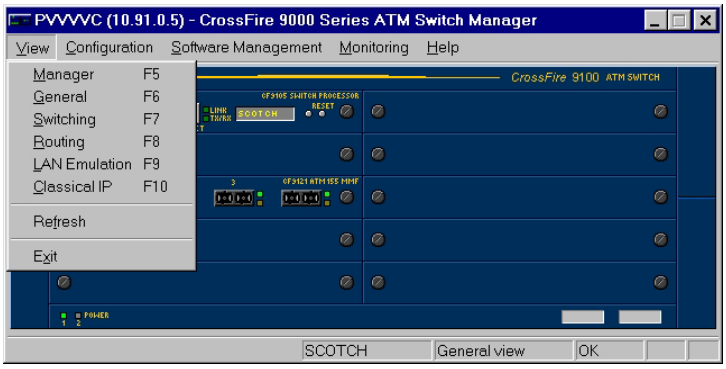
Po wybraniu opcji należy wskazać myszką jeden z portów (wskaźnik myszy zmieni się), nacisnąć lewy klawisz myszy i przeciągnąć wskaźnik na drugi port. W nowo powstałym oknie, jak na rysunku 4.15, zestawić połączenie używając odpowiednich identyfikatorów VPI/VCI.




Rys. 4.15. Menu PVC Configuration

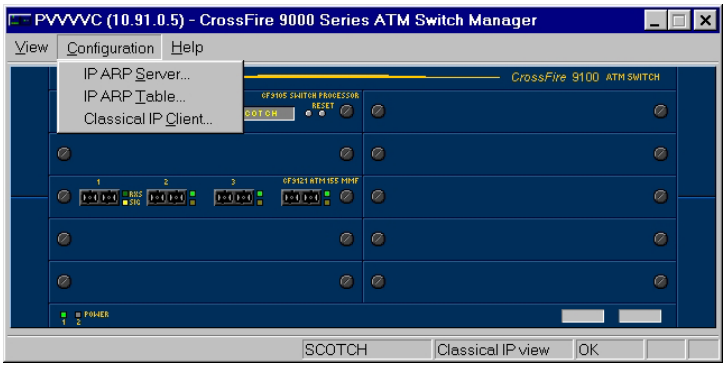
**Połączenia SVC**

Z głównego menu View wybieramy Classical IP (rys. 4.16.).



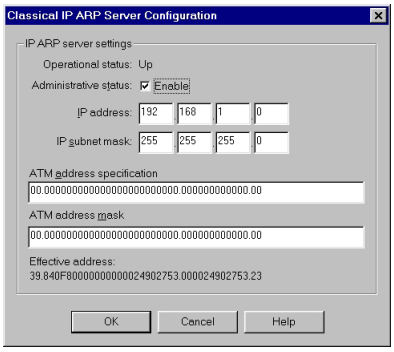

Rys. 4.16. Menu View

Pasek menu zmienił się. W zakładce Configuration dostępne są do wyboru: IP ARP Server, IP ARP Table i Classical IP Client (rys. 4.17.).




Rys. 4.17. Menu CLIP/Configuration

## IP ARP Server (rys. 4.18.)




Rys. 4.18. Menu IPARPSerwer

Operational Status – określa czy usługa serwera ATMARP jest włączona (UP) czy wyłączona (DOWN).

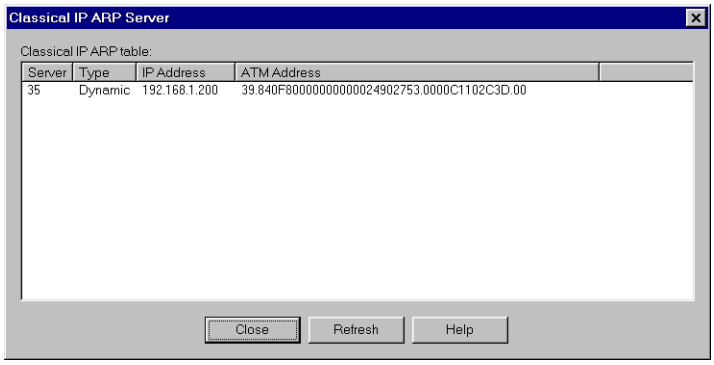
Administrative Status – jeśli zaznaczono serwer jest włączony, jeśli nie wyłączony.

IP address – adres **sieci** (nie pojedynczego hosta), którą serwer ATMARP ma obsługiwać.

IP subnet mask – maska podsieci, która serwer ma obsługiwać,
ATM address specification – adres ATM serwera ATMARP,
ATM address mask – maska serwera ATMARP.

Effective address: wynika z ustawienia dwóch powyższych pól. Jeśli pola te są zerami – przyjmowany jest domyślny adres ATM serwera ATMARP zbudowany w oparciu o numer MAC przełącznika. Na laboratorium będziemy używali ustawień fabrycznych.

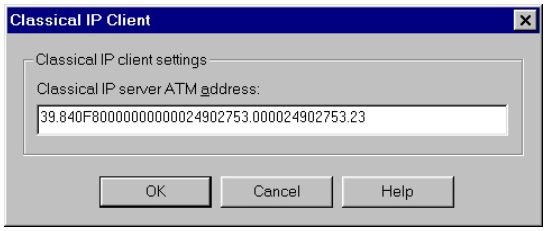
**IP ARP Table (rys. 4.19.)**




Rys. 4.19. Menu IPARPTable

Tablica ARP pozwala zobaczyć, jacy klienci poprawnie zarejestrowali się w serwerze.
Type – typ połączenia: dynamiczne lub statyczne.
IP address – adres IP klienta.
ATM address – adres ATM klienta.

**Classical IP Client (rys. 4.20.)**




Rys. 4.20. Menu IPClient

Przełącznik może być także klientem serwera ATMARP. W szczególnym przypadku może być klientem własnego serwera. Może to posłużyć np. do zarządzania nim, wykorzystując protokół SNMP po sieci ATM bez użycia Ethernetu.

### 4.2.5 Struktura pliku konfiguracyjnego

```
<Global parameters>
DefineAdapter
    DefineTrafficProfile
        <Traffic Profile Parameters>
    EndTrafficProfile
    DefineTrafficProfile
        <Traffic Profile Parameters>
    EndTrafficProfile
    ; More traffic profiles can be defined here ...

    <Adapter configuration parameters>

    DefineVirtualAdapter (LanEmulation|ClassicalIp| \
    Rfc1483|WinSock2)
        DefineProfileMapping
            <Traffic profile mapping parameters>
        EndProfileMapping
        ; More traffic profile mappings can be defined \
        here

        <Virtual adapter parameters>
    EndVirtualAdapter
    ; More virtual adapters can be defined here ...
    DefinePvc
        <PVC parameters>
    EndPvc
    ; More PVCs can be defined here ...
EndAdapter
: More adapters can be defined here ...
```

**Global Parameters**

**LaneDdVccs 32..<Adapter Count> x 992**

Nie dla OS/2 driver.

Maksymalna liczba jednocześnie aktywnych VCC we wszystkich LAN Emulation Virtual Adapters.

Karta docelowa weźmie jeden VCC dla każdego ELAN`u, który jest aktywny.

Default dla Netware and NT: 64 x <Adapter Count> x <ELAN Count>

Default dla others: 32 x <Adapter Count> x <ELAN Count>

**LaneMacAddressCache 32.. 8192**

Nie dla OS/2 driver.

Maksymalna liczba znanych adresów MAC we wszystkich LAN Emulation Virtual Adapters.

Klient weźmie jeden zasób dla każdego znanego ELAN`u, ale normalnie sam klient będzie znany pod różnymi adresami dla każdego ELAN`u.

Default: 4 x LaneDdVccs. Minimum: 512

**LaneAtmAddressCache 32..8192**

Nie dla OS/2 driver.

Maksymalna liczba znanych adresów ATM we wszystkich LAN Emulation Virtual Adapters.

Klient weźmie jeden zasób dla każdego znanego ELAN`u, ale normalnie część adresu ATM zwana selektorem będzie różna dla każdego ELAN`u.

Default: 1.5 x LaneDdVccs.

**DefineAdapter**

**EmptyCells ( Idle | Unassigned )**

Default: Idle.

**EnableSvcSupport ( No | Yes )**

Włącza/wyłącza ILMI, SSCOP (Q.SAAL) i funkcje sygnalizacji.

Default: Yes. Ustawienie "No" wymusza pracę w środowisku połączeń PVC.

**FramingMode ( SONET | SDH )**

Default: SONET

**IlmiRegisterAddresses ( No | Yes )**

Enable/disable ILMI address registration.

Default: Yes

**LecsAtmAddress <20 2-digit hexadecimal numbers>**

Tylko dla pliku konfiguracyjnego dla LANE Client

Ustala ATM address dla LAN Emulation Configuration Server

(LECS). Ten adres jest używany przez wszystkie ELAN`y, dla których żaden LecsAtmAddress albo ServerAtmAddress nie jest skonfigurowany w sekcji DefineVirtualAdapter.

Default: 47 00 79 00 00 00 00 00 00 00 00 00 00 AO 3E 00 00 01 00

**MaxVpiBits (0|1|...|5)**

Maksymalna liczba bitów w części Vpi identyfikatora VCC.

Default: 0 (MaxVpiBits + MaxVciBits = 10).

**MaxVciBits ( 5| 7 | ... | 10 )**

Maksymalna liczba bitów w części Vci identyfikatora VCC.

Default: 10 (MaxVpiBits + MaxVciBits = 10).

**MaxLineRate (<Cells/sec> | <Kbits/sec>Kbps | <Mbits/sec>Mbps | MaxRate)**

Maksymalna przepustowość (w peak`u) pomiędzy kartą a switch`em. To ma wpływ na wszystkie VC bez względu na ich indywidualną charakterystykę ruchu.

przykład:

Bez jednostki: (Cells/sec): 1 - 353208

Kbps (bez nagłóka SONET/SDH): 1 - 149700

Mbps (bez nagłówka SONET/SDH): 1 - 149

"MaxRate" to 353208 cells/sec ~ 149Mbps (bez SONET/SDH overhead).

Default: MaxRate

**MaxPvcs ( 1 | 2 | ... | 128 )**

Maksymalna liczba PVCs.

Default: 16

**MasterTiming ( No | Yes )**

Podczas pracy BTB (back-to-back). Ustawienie decyduje o tym, która z kart będzie generowała podstawę czasu, a która będzie ją odbierała. Ważne jest aby się upewnić, czy oba urządzenia mają przeciwne ustawienia (yes/no). Podczas połączenia ze switch'em, karta powinna pracować w trybie No - można wtedy w ogóle nie podawać tego parametru.

Default: No

**UniVersion ( Uni3.0 | Uni3.1 | Uni4.0 )**

Default: Uni3.1.

**DefineVirtualAdapter**

**AtmAddress <20 2-digit hexadecimal numbers>**

Tylko dla Virtual Adapter typu: LanEmulation , ClassicalIP or WinSock2 type

Konfiguracja adresu ATM klienta. Wszyscy LEC i LES muszą mieć niepowtarzalny adres. Jeśli adres ATM nie zostanie zdefiniowany, zostanie on automatycznie nadany korzystając z: prefiksu pobranego ze switch'a za pomocą ILMI, adresu MAC karty i selektora:

<prefix (13 bytes)><burnt-in MAC address (6 bytes)><selector (1 byte)>

Selektor jest potrzebny w wypadku gdy są zdefiniowane więcej niż 1 Virtual Adapter. W tym przypadku ich numeracja będzie wyglądać:

dla 1: selector=00

dla 2: selector=01

itd...

Gdy ILMI address registration jest wyłączone, adres ATM musi być nadany.

**LanName <text, up to 32 characters>**

Tylko dla Virtual Adapter typu LanEmulation.

Default: none.

**LanType ( Ethernet | Token-Ring )**
Default (LanEmulation): Ethernet.
Default (Classical IP and RFC1483): Token-Ring.

**LecsAtmAddress <20 2-digit hexadecimal numbers>**
Tylko dla Virtual Adapter typu LanEmulation.
Konfiguruje adres ATM dla LAN Emulation Configuration Server (LECS), który będzie użyty dla danego ELAN‘u

**MaxDataFrameSize ( 1516 | 4544 | 9234 | 18190)**
Tylko dla Virtual Adapter typu LanEmulation.
Maksymalna długość ramek do wymiany między klientami. Dla Ethernet‘u jedyną poprawną wartością jest 1516. Wszyscy klienci danego ELAN‘u muszą używać tej samej długości.
Default (Ethernet): 1516.
Default (Token-Ring): 4544.

**ServerAtmAddress <20 2-digit hexadecimal numbers>**
Tylko dla Virtual Adapter typu LanEmulation.
Adres ATM serwera LES dla danego ELAN‘u.
No default.

Poniższe parametry odnoszą się bezpośrednio do specyfikacji „LAN Emulation over ATM, ver. 1.0” i służą do dokładnych ustawień parametrów LANE. Zmienna Cx odpowiada dokładnie tym co w powyższym dokumencie z ATM Forum.

**AgingTime ( 10 | 11 | .. | 300 )**
Tylko dla Virtual Adapter typu LanEmulation.
ATM Forum: C17
Maksymalny czas (w sekundach) aby LEC podtrzymał adres do lokalnego LAN‘u w ARP cache‘u w przypadku braku weryfikacji.
Default: 300.

**ArpResponseTime ( 1 | 2 | .. | 30 )**
Tylko dla Virtual Adapter typu LanEmulation.
ATM Forum: C20
Maksymalny czas (w sekundach) aby LEC czekał na ARP request/response przed ponowną próbą.
Default: 1.

**ArpServer <20 2-digit hexadecimal numbers>**
Tylko dla Virtual Adapter typu ClassicalIP.
Adres ATM serwera ARP. Tylko dla połączeń SVC. 20 dwuznakowych liczb heksadecymalnych oddzielonych spacjami.
Default: none

**ArpTimeout ( 1 | ... | 6000 )**

Tylko dla Virtual Adapter typu ClassicalIP.

Okres odświeżania ATMARP, to jest czas jaki upłynie do wygenerowania zapytania Inverse ATMARP w celu zweryfikowania adresu zdalnego urządzenia, którego dotyczył wpis w tablicy. Zobacz konfiguracja PVC.

Default: 600 seconds

**DefaultTrafficProfile ( 0 | 1 | 2 | ...)**

Tylko dla Virtual Adapter typu LanEmulation, ClassicalIP lub WinSock2.

Profil ruchu, który ma zostać użyty jeśli żaden zdefiniowany profil nie odpowiada otwieranemu nowemu VC. Wartości : Maksymalna wartość zależy od liczby zdefiniowanych profili.

Default: Hardware default profile.

**Encapsulation ( LlcSnap | LlcSnapBridged )**

Tylko dla Virtual Adapter typu Rfc1483.

Rodzaj zastosowanej enkapsulacji, albo prosta LLC snap albo specjalna “bridged” snap z uwzględnieniem typu sieci i 2 bajtowym dopełnieniem.

Default: LlcSnapBridged

**FlushTimeout ( 1 | 2 | 3 | 4 )**

Tylko dla Virtual Adapter typu LanEmulation.

ATM Forum: C21

Maksymalny czas (w sekundach) jaki klient LANE będzie czekał na odpowiedź FLUSH po wysłaniu żądania FLUSH.

Default: 4.

**ForwardDelayTime ( 4 | 5 | ... | 30 )**

Tylko dla Virtual Adapter typu LanEmulation.

ATM Forum: C18

Maksymalny czas (w sekundach) jaki klient LANE będzie przechowywał adres zdalnego LAN'u w swoim cache'u ARP w przypadku braku weryfikacji.

Default: 15.

**IpAddress <ddd.ddd.ddd.ddd>**

Tylko dla Virtual Adapter typu ClassicalIP.

Adres IP tego wirtualnego adaptera. Jeśli pozostanie nieskonfigurowany, adres IP zostanie ustawiony na zgodny z ustawionym w systemie operacyjnym.

Default: Auto-detected

**JoinTimeout ( 5 | 6 | ... | 300 )**

Tylko dla Virtual Adapter typu LanEmulation.

ATM Forum: C7

Okres czasu wykorzystywany jako time-out dla kontroli operacji typu żądanie/odpowiedź

Default 5.

**MaxArpRetryCount ( 0 | 1 | 2 )**

Tylko dla Virtual Adapter typu LanEmulation.

ATM Forum: C13

Maksymalna liczba prób wysłania LE_ARP request dla danego LAN destination po wysłaniu pierwszego LE_ARP request dla tego samego segmentu LAN destination.

Default: 1

**MaximumAcceptedConnections ( 1 | 2 | ... | 2048 )**

Tylko dla Virtual Adapter typu WinSock2.

Maksymalna liczba jednocześnie otwartych połączeń zaakceptowanych przez jeden socket (gniazdo)

Defaults: Windows NT: 10, Windows 95: 5

**MaximumOpenCircuits ( 2 | 3 | ... | 992 )**

Tylko dla Virtual Adapter typu ClassicalIP, RFC1483 i WinSock 2.

Maksymalna liczba aktywnych Vccs (włączając połączenia z LES, BUS or ATM ARP server), które klient może mieć w jednej chwili czasu. Minimalna wartość 2.

Default (NetWare and NT): 64.

Default (Windoews 95): 32

**MaxUnknownFrameCount ( 1 | 2 | ... | 10 )**

Tylko dla Virtual Adapter typu LanEmulation.

ATM Forum: C10

Maksymalna liczba ramek jaką wyśle klient do BUS w czasie MaxUnknownFrameTime (patrz niżej) sekund do nadanego unicast'owego LAN Destination, zanim zacznie rozwiązywać ATM'owy adres docelowy LAN'u (używając ARP).

Default: 1.

**MaxUnknownFrameTime ( 1 | 2 | ... | 60 )**

Tylko dla Virtual Adapter typu LanEmulation.

ATM Forum: C11

Zobacz opis MaxUnknownFrameCount.

Default: 1.

**MaxReceiveRateDifference (<Cells/sec> | <Kbits/sec> Kbps | <Mbits/sec> Mbps )**

Tylko dla Virtual Adapter typu LanEmulation, ClassicalIP lub WinSock2.

Maksymalna różnica między żądaną szybkością transmisji połączenia przychodzącego a szybkością fizycznego połączenia (155Mbps), powyżej której połączenie zostanie odrzucone. Ustawienie wartości maksymalnej 16777215 cells/sec powoduje, że szybkość transmisji nie będzie sprawdzana. Pozwala to zapewnić współpracę z urządzeniami, które nie obsługują odrzucenia połączenia z powodu „User cell rate not available".

Bez jednostki (ie. Cells /sec): 0 - 16777215

Kbps (bez nagłówka SONET/SDH) : 0 - 7113000

Mbps (bez nagłówka SONET/SDH) : 0 - 7113

Default: 16777215 cells/sec

**MaxTransmitRateDifference (<Cells/sec> | <Kbits/sec> Kbps | <Mbits/sec> Mbps )**

Tylko dla Virtual Adapter typu LanEmulation, ClassicalIP lub WinSock2.

Maksymalna różnica między żądaną szybkością transmisji połączenia przychodzącego a najbliższą dostępną w profilach ruchu, powyżej której połączenie zostanie odrzucone. Ustawienie wartości maksymalnej 16777215 cells/sec powoduje, że szybkość transmisji nie będzie sprawdzana. Pozwala to zapewnić współpracę z urządzeniami, które nie obsługują odrzucenia połączenia z powodu „User cell rate not available".

Bez jednostki (ie. Cells /sec): 0 - 16777215

Kbps (bez nagłówka SONET/SDH) : 0 - 7113000

Mbps (bez nagłówka SONET/SDH) : 0 - 7113

Default: 16777215 cells/sec

**MtuSize <number of bytes>**

Tylko dla Virtual Adapter typu ClassicalIP lub WinSock2.

Maksymalna długość ramki bez długości enkapsulacji (narzut). Długość enkapsulacji wynosi 8 bajtów dla Classical IP, 8 bajtów dla RFC 1483 z enkapsulacją LlcSnap i 10 bajtów dla RFC 1483 z enkapsulacją LlcSnapBridged.

Default: 9180.

Notka: W Novell NetWare, ustawienie LanType na Ethernet wpływa na maksymalną dopuszczalną użytą długość ramki. Dla Classical IP i RFC1483 LlcSnap jest to 1514. Dla RFC1483 LlcSnapBridged jest to 1514. Jeśli zostanie skonfigurowany nieprawidłowo sterownik zmieni ustawienia, a zmieniona wartość zostanie wyświetlona przez AIN. Te ograniczenia rozmiaru ramek nie odnoszą się do Windows 95 i Windows NT.

**PromiscuousMode ( No | Yes )**

Tylko dla Windows 95 i Windows NT.

Określa czy sterownik powinien informować system operacyjny o tym, że pracuje w trybie PromiscuousMode. W trakcie używania Microsoft Network Monitor (Netmon), powinien być ustawiony na Yes.

Default: No

**TraceMask <Hexadecimal value>**

Maska bitowa, używana jest do włączenia wyświetlania dodatkowych informacji w dzienniku zdarzeń. Te dodatkowe informacje nie są opisane w instrukcjach obsługi, ale pozwalają firmie Olicom na otrzymanie dodatkowych informacji w przypadku złożonych problemów, takich jak zła współpraca z innymi urządzeniami ATM. Aby włączyć wszystkie ślady należy ustawić wartość FFFFFFFF.

Wartości: 0 ... FFFFFFFF

**VccTimeoutPeriod ( 0 | 1 | ... | 1080 )**

Tylko dla Virtual Adapter typu LanEmulation.

ATM Forum: C12

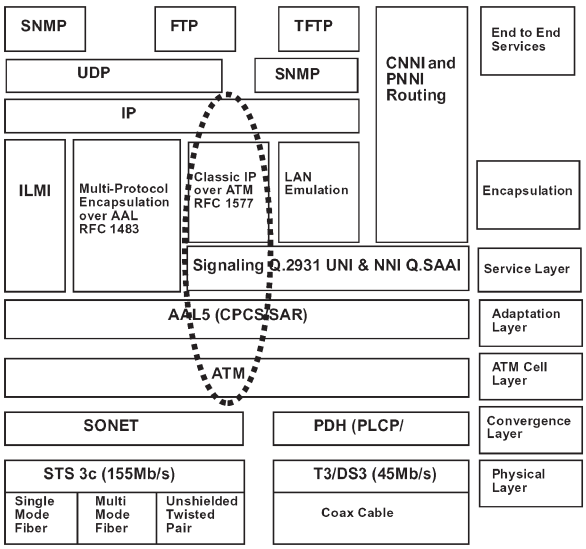
Liczba minut, przez które DD-VCC jest przechowywane zanim zostanie zwolnione przez klienta LANE jeśli nie zostało użyte. "0" Wyłącza zwalnianie nie używanych DD-VCC.

Default: 20.

## 4.3. Enkapsulacja pakietów (LLC/SNAP)

Posiadając podstawową wiedzę o działaniu sieci ATM i o protokole IP rozumiemy, że wymiana datagramów IP w sieci ATM wymaga zastosowania dodatkowych mechanizmów pośredniczących. Cechą sieci ATM jest stała 53 bajtowa długość komórki, podczas gdy datagramy protokołu IP mogą mieć zmienne długości do 65535 bajtów. Użytkową część komórki ATM stanowi 48 bajtów, reszta to nagłówek ATM.

Grupa IETF zdefiniowała metody enkapsulacji pakietów różnych protokołów w komórkach ATM. Dokumentem zawierającym te informacje jest RFC 1483. Nie uszczegóławiając, należy zaznaczyć, że do transportu datagramów IP wykorzystuje się ramki warstwy AAL5.




Rys. 4.23. Struktura warstwowa z zaznaczonymi: IP, CLIP, AAL5, SAR, ATM

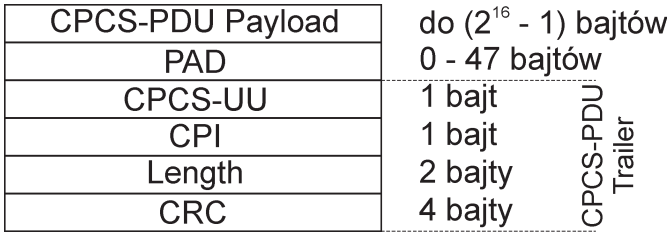
Pakiet IP jest enkapsulowany w polu Payload ramki AAL5 (rys. 4.24.).

Pole PAD stanowi dopełnienie pakietu CPCS-PDU. Dopełnienie musi mieć taką długość, aby koniec pola CPCS-PDU Trailer pokrywał się z końcem ostatniego 48-oktetowego segmentu danych utworzonego przez podwarstwę segmentacji SAR.

Pole CPCS-UU („User-to-User" – wskaźnik użytkownik-użytkownik) jest stosowane w celu przezroczystego przenoszenia danych między użytkownikami. Nie ma ono zastosowania w opisywanym schemacie kapsułkowania, i może być ustawione na dowolną wartość.

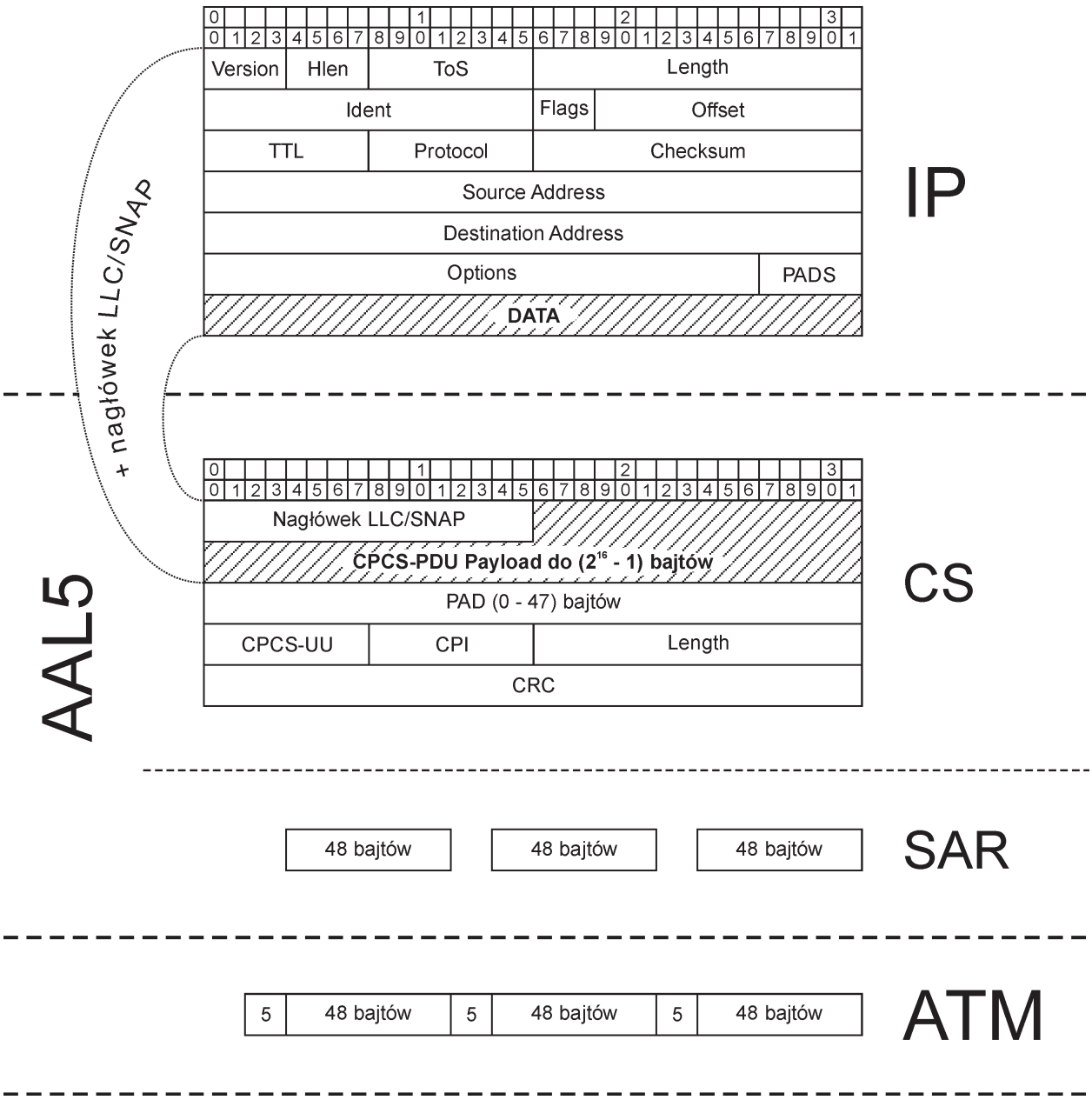
Pole CPI („Common Part Indicator" – wskaźnik części wspólnej) wyrównuje pole CPCS-PDU Trailer do 64 bitów.

Pole CRC zabezpiecza cały pakiet CPCS-PDU oprócz samego pola.




Rys. 4.24. Format ramki AAL5 CPCS-PDU

Tak stworzona ramka AAL5 CPCS-PDU jest segmentowana przez podwarstwę SAR (Segmentation and Reassembly) na 48 bajtowe odcinki (rys. 4.25.). Jej długość jest już tak dobrana, że podzieli się bez reszty. Ostatecznie do każdych 48 bajtów dołączany jest nagłówek ATM, w ten sposób uzyskaliśmy gotowe komórki do wysłania niezależnie od długości pakietu IP. Warto zauważyć, że enkapsulacja LLC/SNAP wprowadza bardzo mały narzut protokolarny. W optymalnym przypadku (pakiety IP o maksymalnej długości ) są to 33 bajty na każde 65535 bajtów.




Rys. 4.25. Poglądowy schemat enkapsulacji datagramu IP