Asynchronous Transfer Mode in TCP/IP environment: Adaptations and Effectiveness

Dipl.-Ing. Kai-Oliver Detken
Bremen Institute of Industrial Technology and
Applied Work Science at the University of Bremen (BIBA)
Hochschulring 20, D-28359 Bremen
Email: det@biba.uni-bremen.de
URL: http://www.biba.uni-bremen.de

1 Abstract

This paper discusses the effectiveness of ATM cells within a TCP/IP environment and the adaptation possibilities. This examination within the project EIES was necessary, because ATM cells are used for the communication lines between the distributed ports (Bremen, Bordeaux, Brest, and Santander) within a heterogeneous network. The reason why IP packets are used for the project EIES is the user desire for platform independence and the different network environments. IP packets are the most suitable solution to realise such a heterogeneous network without adjustment problems. But IP was developed for the Internet with narrowband data access. For advanced multimedia applications ATM has to be used, because ATM supports real-time audio-, video-, and data transmission with a defined quality of service (QoS). Therefore the interworking between ATM and IP plays always a central role for heterogeneous networks.

The results of the examination show that TCP buffer sizes and the Maximum Transmission Unit (MTU) have a dramatic impact on the data throughput. Several other parameters are also important for an efficient data rate. This paper describes the ATM adaptations of IP, describes the bottlenecks, and offers a solution for effective use of ATM in TCP/IP environment.

2 Introduction

The project European Information Exchange System for the communication between harbour areas (EIES) is an European project within ACTS. The project aims at the definition, implementation and experimentation of an advanced communication service which has the tasks to support routine and non-routine communication between different maritime players (harbour authorities, ship owners, customs or fire brigades, etc.) within harbour areas, on a pre-commercial basis. EIES takes considerations of the users point of view and examine the following users application needs into the special EIES service:

- Computer Supported Co-operative Work (CSCW)
- Distribution of multimedia information about different databases (BluePages+ and Port Entry Guide)
- Integration of Electronic Data Interchange (EDI) and Electronic Mail (Email)
- Build-up a global ATM network between the participated harbours for the EIES platform with also network access over lower bandwidth (ISDN direct lines and Internet)
- Mobile Communication (DSRR, DECT and Inmarsat) for the mobile access to the multimedia services

For the realisation of the ATM network platform EIES identified the user requirements, the quality of service and the network requirements for a heterogeneous network. Around in the local network or wide network area TCP/IP protocols are the de-facto-standard for all applications from the user point of view, because the benefits of TCP/IP is the transparency, because it can run over any physical network (Ethernet, FDDI, Token Ring, X.25, Frame Relay, fibre-channel, async, etc. Therefore EIES uses TCP/IP protocols in their heterogeneous network area.

However, TCP/IP protocols are developed for the Internet environment and therefore for very low data rates. Today new applications like Computer Supported Co-operative Work (CSCW) systems with videoconference and application-sharing services fulfil the increasing desire of the user to co-operate over large distances. Higher bandwidth are required to meet these requirements. ATM is the best solution to achieve this objective, but some specifications and customisations on ATM are needed for an efficiently transmission of TCP/IP protocols over ATM.

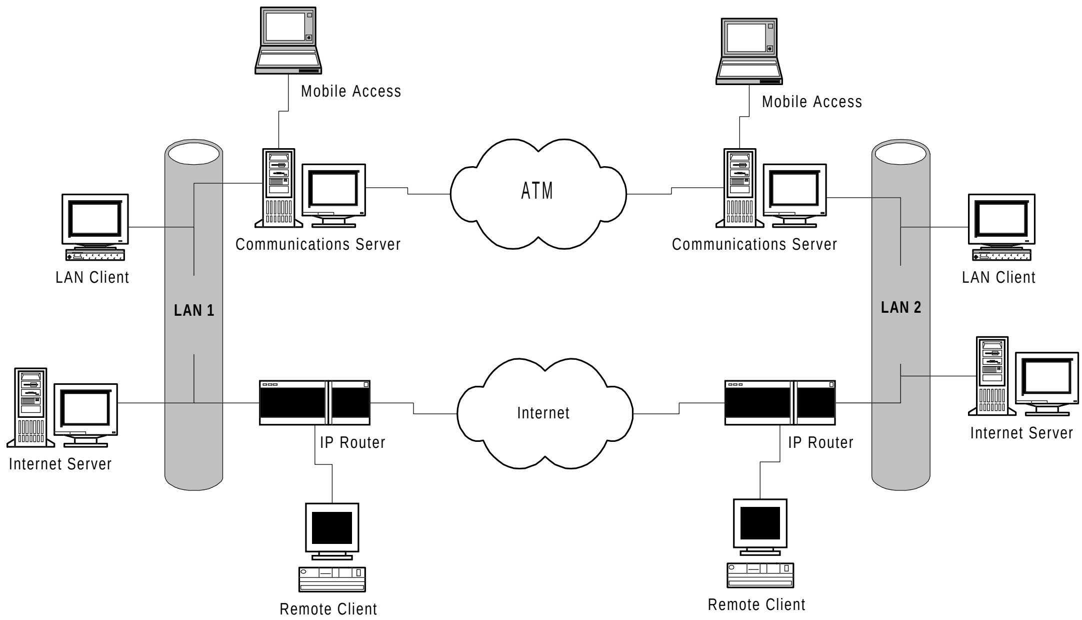

Figure 1: EIES hardware platform [1]

EIES investigated the possibilities and the bottleneck of IP-over-ATM (IPoATM) for CSCW applications over MBONE tools in a real ATM network environment in Bremen. Also, other demonstrations like the Brussels event on 2nd October 1996 and the trade fair „Global Access Exhibition“ in Stockholm on 26-28th May 1997 made measurements over various National Hosts in co-operation with JAMES (Joint ATM Experiments on European Services) possible.

Figure 1 shows the EIES hardware platform which is based on IP/ATM/ISDN routers. IP packets encapsulated into AAL-5 ATM cells are being exchange between the EIES ports. The remote PCs are connected with a TCP/IP stack over ISDN lines via Point-to-Point-Protocol (PPP) to the router. The communication server acts as a bridge between TCP/IP and the mobile access possibilities (DSRR, Inmarsat, and DECT). All applications run over TCP/IP. Therefore, ATM is hidden from the application developers. As IP/ATM routers work in AAL-5 mode, quality-of-service (QoS) features will be concealed from the application developers. This does not affect data applications (e.g. email, file transfer), but for circuit switched nature applications with real-time behaviour (audio and video data streams). Real-time applications like CSCW are LAN/WAN-based type applications, using IP multicast with ATM/IP routers supporting MBONE for instance.

Using AAL-5 is an attractive way to integrate ATM in the EIES project, because all existing real-time applications use TCP/IP protocol stack. Additionally, the IETF and the ATM-Forum are searching for a better implementation or adaptation for IP-over-ATM, like MPOA and „Native ATM Service“ over IP in their own working groups, because they know about the dissemination of the TCP/IP protocol stack. So, in the future it is possible to use a quality-of-service (QoS) if you use the Internet Protocol (IP). Actually, they are defining several additional protocols for variable bandwidth, guaranteed data rates, etc. over IP. [1]

This contribution is an overview over existing IPoATM possibilities still being tested in the EIES project. Furthermore, the effectiveness of IP for real-time applications, existing bottlenecks and solutions will be described.

3 IP-over-ATM difficulty

The completely different structures and characteristics of the two transmission modes of IP and ATM constitute a problem for the successful adaptation.

ATM has its own addressing structure and hierarchical routing functions, uses signalling to set-up and tear down virtual connections (VPC/VCC) with a specified traffic contract and QoS, and is universally scalable technology. Small packets, called cells, are transported over pre-established connections. The QoS of ATM defines parameters like bandwidth, loss rates, delays, jitters, etc. These defined parameters are promised to the participant and must be kept. But there will be only exclusively point-to-point connections established.

On the other hand, TCP/IP is a connectionless network protocol designed to forward data packets on a hop-by-hop basis, network-to-network, independent of the underlying network. It defines a robust and flexible set of host and network behaviour that enables adaptation to dynamic network conditions. TCP/IP is supported on almost every network device and is universally accepted as de-facto networking protocol. Its basic mechanisms have changed over the years and the stability as well as its ability to run on any platform have contributed to its widespread deployment.

For shared media LANs like Ethernet or Token-Ring, IP uses the Address Resolution Protocol (ARP) to resolve an IP address with the associated Medium Access Control (MAC). ARP uses the broadband support of the underlying shared media to accomplish this. MAC protocols also don't work for connection-orientated in the local network area and no acknowledgement mechanisms have therefore been implemented at the receiver site. Lost data packets must be requested high protocol layers such as TCP protocol mechanisms via the IP protocol.

Furthermore at local area network data will be transmitted on a physical medium, so the information is available for any attached station by access mechanisms. Broadcast functions are possible by sending from one station to the others and evaluating the data through all attached stations. Clear communication connections with other net participants are build-up by special detail of the destination address. This characteristics are in strong contrast to the ATM mechanisms.

IP multicast enables one or more senders to send packets to multiple destinations by addressing them to a group address. Broadcast or multicast messages are exclusively practicable about many virtual connection paths which is created by signalling mechanisms with the help of assignment tables. But ATM does not still support multicast mechanisms by the user network interface (UNI) signalling protocol of version 4 yet.

On the other hand, TCP does lack some important capabilities. It is a data network protocol only. That means real-time data like audio and video can not be supported. An exception is the use of a very carefully controlled network configuration with more than sufficient bandwidth. The Multicast Backbone (MBONE) is an example of this.

Additionally, IP and ATM have different addressing structures. Two addressing models exist: peer and separated. The peer model supports an algorithmic translation of the IP address to an ATM address and vice-versa. One address scheme to administer would be desirable, but it requires that a host perform this function, thus requiring a change in host behaviour. There is also the issue of mobility and consistency across address hierarchy boundaries. The separated model keeps the IP and ATM address spaces separately. A dynamic mapping or association of an IP address with an ATM address is required.

Furthermore, IP has no knowledge of the underlying data link it is running on. For instance, IP packets are encapsulated in Ethernet frames when running on an Ethernet network. ATM uses AAL-5 or AAL-3/4 for data transmission. AAL-5 contains less overhead than AAL-3/4 but does not support multiplexing of cells from different AALs on the same VC. [2]

Additional problems appear to the different characteristics in the area of various transmission rates and incompatible packet or cell formats. Nowadays these difficulties can however be overcome by efficient routers how this is realise at the edges of Ethernet and Token Ring to FDDI networks. But the address translation and the routing itself should consider as not non-trivial.

4 IP-over-ATM possibilities

To adapt ATM to other protocols and traditional networks, three different solutions have been developed in the meantime:

- Classical IP
- LAN-Emulation (LANE)
- Multiprotocol over ATM (MPOA)

Classical IP (RFC-1577) and ARP over ATM was the first implementation of IPoATM. The Classical IP model positions ATM as a replacement for the wires or LAN segment connecting two workstations on the same subnet. IP routers are still required to interconnect two or more IP subnets. Indeed the classical model purposely limits ATM to intra-subnet connectivity. The components and operation of Classical IP and ARP over ATM are contained in a series of Request For Comments (RFCs) issued by the IETF Internetworking over NBMA (ION) working group. The RFC’s (RFC-1577, RFC-1483, RFC-1626, RFC-1755) describe an encapsulation technique, ATMARP service, UNI signalling flows, and default MTU size. Without fully exploiting the capabilities of ATM, they have provided developers and vendors with initial and stable set of guidelines for developing IP over ATM.

LAN Emulation (LANE) is the second solution for IPoATM and can be best characterised as a service developed by the ATM Forum that will enable existing LAN applications to run over an ATM network. To do so this service must emulate the characteristics and behaviours of traditional Ethernet, Token Ring and FDDI networks. It must also support a connectionless service, because current LAN stations send data without first establishing a connection. Therefore it must support broadcast and multicast traffic such as the kind allowed over shared media LANs. It must enable the interconnection of traditional LANs with the emulated LAN and maintain the MAC address identity associated with each individual device attached to a LAN. And finally, it must protect the vast install basis of existing LAN applications and enable them to work unchanged over an ATM network. That became realise over the OSI layer 2, why the LANE technology can be understood as a bridging technology.

Similar to Classical IP and LANE, Multiprotocol over ATM (MPOA) is based on a client/server model. MPOA clients established VCCs with the MPOA server components to forward data packets or request information so that the client can establish a more direct path. MPOA supports various kinds of routable protocols (IP, IPX, AppleTalk, etc.) and integrate existing internetworking protocols (RFC-1577, NHRP, MARS, RSVP) from the IETF and ATM Forum solutions (LANE, P-NNI) into a virtual router environment. MPOA is a service with layer 3 internetworking support for hosts attached to ELANs, ATM networks, and legacy LANs. So the real premise behind MPOA is to provide and deliver the function of a router and take advantage of the underlying ATM network as much as possible. MPOA works as a virtual router on the OSI layer 3. [3]

4.1 Classical-IP

RFC-1577 defines the Classical-IP and ARP over ATM. It was developed by the Internet Engineering Task Force (IETF) in 1993. Hosts on a subnet are still assigned an IP address and

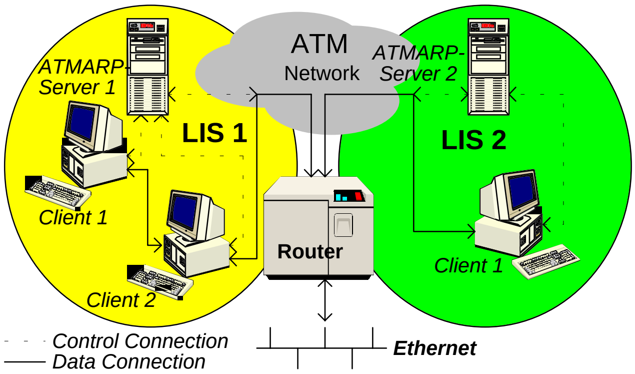

Figure 2: Classical-IP architecture [1]

ATM physical layer address. When communicating with another host on the same subnet using ATM, it is necessary to resolve the destination IP address with the ATM address of the endpoint.

The characteristics can be summarised as the following points:

- Maximum Transmit Unit (MTU) size of 9180 byte is used as a default for all Virtual Channels (VCs) on a subnet.
- LLC/SNAP encapsulation of IP packets in AAL 5 cells as described in RFC-1483 is used.
- IP addresses are resolved to ATM addresses by use of an ATMARP service within the Logical IP Subnet (LIS) via an additional server. The scope of the ATMARP service is limited to the LIS, just as the scope ARP is limited to a single subnet.
- A single LIS can support many hosts and routers with the same IP network and subnet mask. Communications between any two members of the LIS takes place over an ATM PVC or SVC.
- The traditional IP model is unchanged.

But by Classical-IP's simple structure there arise also several disadvantages. Classical-IP over ATM does not support multicast or broadcast, only IP will be adapted to ATM, high delay of the connections, and scalability is limited. Furthermore, Classical-IP does also not provide QoS and direct coupling of different subnets.

But Classical-IP is a stabile standard, can use direct IPoATM, and establish PVC/SCV connections, and a higher packet encapsulation (9180 byte). The limit of the MTU is important for the effectiveness of IPoATM.

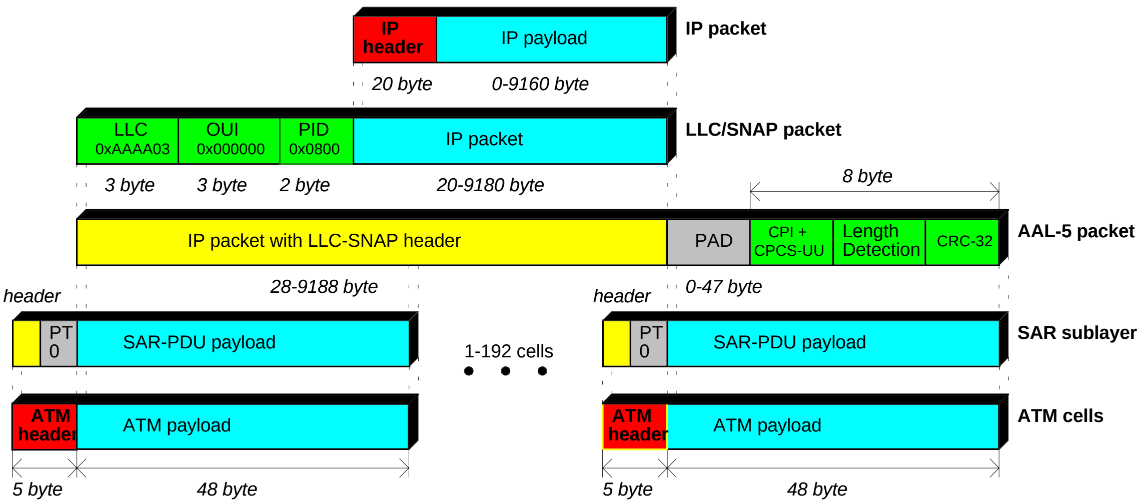

Figure 3: LLC/SNAP encapsulation (RFC-1483) [1]

Very recently, RFC-1483 was defined for the encapsulation routed and/or bridged packets in ATM-AAL-5 cells. The first technique is called LLC/SNAP encapsulation and works with an additional LLC/SNAP header on each packet. This is necessary for the identification of the protocol within the payload field. The LLC/SNAP header consists of a 3 byte Logical Link Control (LLC), a 3 byte Organisational Unique Identifier (OUI), and a 2 byte Protocol Identifier (PID) field. With the PID field every protocol can be distinguished from others. Figure 1 shows the LLC/SNAP encapsulation of an IP packet. The second technique described in RFC-1483 is called VC multiplexing and differs from LLC/SNAP solution in that the VC is terminated directly at a layer-3 endpoint. This means, the VC-multiplexed connection will carry one protocol only. In a multiprotocol environment, this scheme would use additional VCs. But for the use of IPoATM, the LLC/SNAP technique is the default method, because the UNI signalling required to initiate a LLC/SNAP encapsulated Switched Virtual Connection (SVC). This is defined in RFC-1755. The important advantage its that multiple protocols can share a VC thus limiting the numbers of VCs required in an IP and multiprotocol environment. On the other hand, it uses an additional 8 byte per AAL frame (Figure 3).

RFC-1483 Permanent Virtual Channels (PVCs) between two routers is an effective technique for ATM, having some of the advantages of higher bandwidth and supporting IP as well as other protocols. This is the reason, why RFC-1483 is also occurred for LAN-Emulation and Multiprotocol over ATM (MPOA). [2, 3]

4.2 LAN-Emulation (LANE)

LANE is a further development of the IPoATM adaptation. But LANE has a more complex structure as Classical-IP, because the adaptation of different traditional networks like Ethernet, Fast-Ethernet, Token-Ring, FDDI, etc. is possible by LANE. Therefore not only IP is supported, other routable protocols such as IPX, APPN, DECnet, and AppleTalk can be included as well. Even non-routable protocols such as NETBIOS, LAT, and SNA can be supported.

LANE must enable the interconnection of traditional LANs with the emulated LAN (ELAN), which client stations directly attached to an ATM network. It must maintain the MAC address identity associated with each individual device attached to a LAN. Additional, it must protect the vast install base of existing LAN applications and enable them to work unchanged over an ATM network.

LANE is available in the version 1.0 and includes the following key requirements:

- Connectionless service is emulated over ATM.
- Broadcast/multicast traffic is supported over an emulated LAN using standard techniques such as transparent and source-route bridging.
- MAC addresses are still used to identify emulated LAN clients. Similar to the ATMARP server approach, a server exists (LES) which maintains a table of MAC-to-ATM addresses.
- LAN applications can run unchanged over an emulated LAN.

LANE is a standard with a high functionality, because the complete MAC layer will emulate.

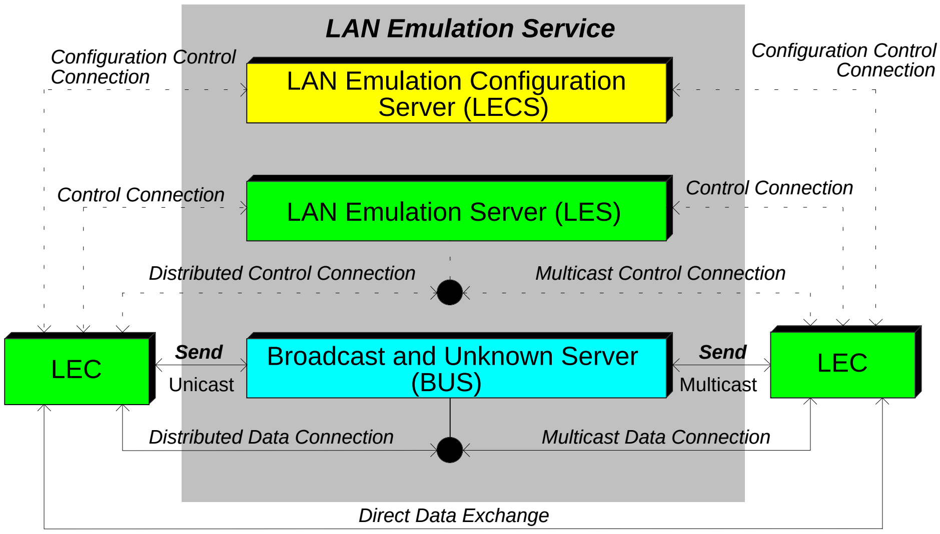

Figure 4: LAN-Emulation architecture [3]

Therefore, LANE defines protocols and operation for a collection of client functions as a single ELAN (Ethernet or Token-Ring). Furthermore, LANE specifies a set of services for each instance of an ELAN. The services provide configuration, address resolution (MAC-to-ATM), multicast/broadcast function. Membership in an ELAN is not based on physical location but rather on the association with a specific set of services. Therefore, LANE enables constructing and managing virtual LANs (VLANs).

The LANE architecture includes the following devices to fulfil the requirements:

- LAN Emulation Clients (LEC)
- LAN Emulation Server (LES)
- LAN Emulation Configuration Server (LECS)
- Broadcast and Unknown-Server (BUS)

The LANE components consist of a client (such as workstation), file-server, bridge, or router (LEC) and the LANE services itself (LES, LECS, and BUS). The LEC performs address resolution, data forwarding, and other control functions. The LEC presents a MAC-level interface to the higher layers and implements LANE User Network Interface (L-UNI) when communicating with other components in the ELAN.

The LES functions as a registry and address resolution server for the LECs attached to the ELAN. The LES provides a facility for LECs to register their MAC and ATM addresses. A LEC may also query a LES for resolution of a MAC to ATM address. The LES will either respond directly to the LEC or forward the query to other LECs that may be able to respond.

The LECS is used to initialise a LEC with information specific to the ELAN that the LEC will be joining. The LECS will provide a LEC with the ATM address of the LES. The LECS can provide this information to the LEC, based on the client's ATM address, MAC address, or some other pre-configured policy. The LECS enables a LEC to autoconfigure itself and provides some level of control as to who can join an ELAN.

The BUS handles data addressed to the MAC broadcast address, all multicast traffic, and unicast frames sent by a LEC before the ATM address of the destination has been resolved. All LECs maintain a connection to the BUS and are leave on a point-to-multipoint VC with the BUS as a root. This enables LECs to send data frames without first setting up a connection, thus maintaining the presence of a connectionless data-transfer service to the higher-layers service present in each LEC.

The server entities (LECS, LES, and BUS) can reside in a single physical device or can run in

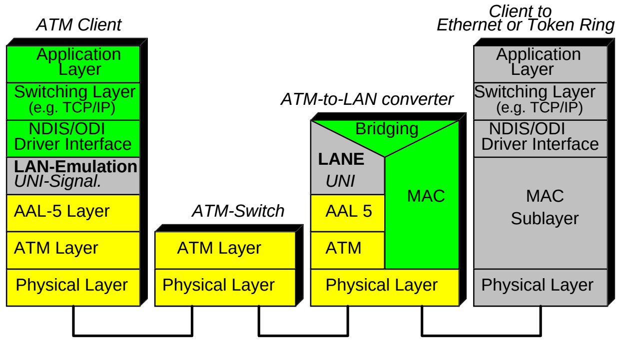

Figure 5: LANE layer architecture [3]

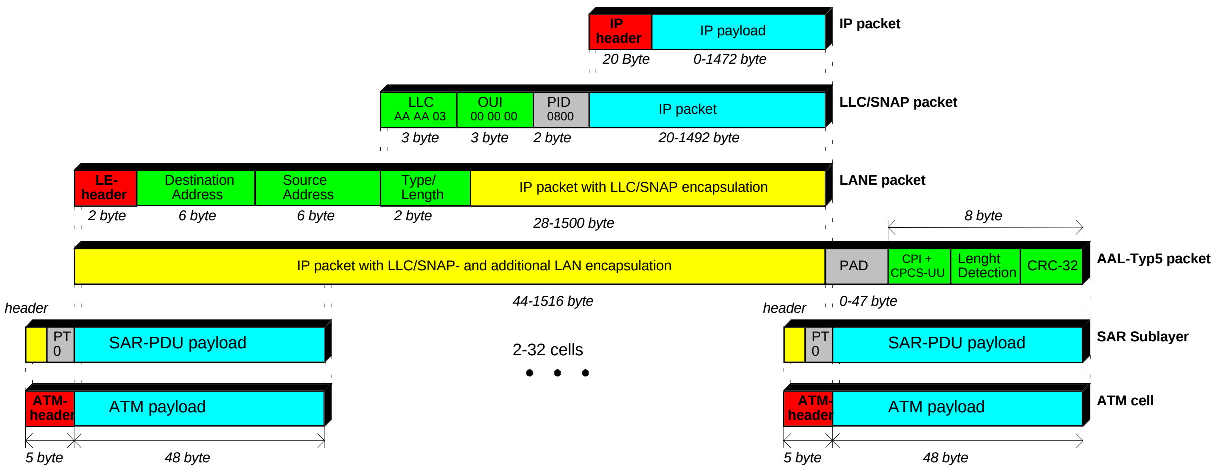

Figure 6: LANE encapsulation over the AAL-5 layer [3]

separate devices over an emulated LAN. An emulated LAN requires a single instance of a LES/BUS pair and supports only one type of emulated LAN: Token-Ring or Ethernet. In other words, a single LES/BUS can not support some clients that are emulating Token-Ring or Ethernet. The layer architecture of LANE defines how and where the LANE entity is positioned and operates within a LAN client.

Figure 5 shows the LANE applications on the top, the functional layers with ATM at the bottom, and the LANE entity between these two layers. The Physical and ATM layer are common to any end user or switch implementing ATM. LANE makes use of standard AAL services to support signalling and data transfer. The functional layers interact through a set of specified interfaces between the different layers. LANE clients and server interact over the LANE User Network Interface (L-UNI). LANE server interacts with other server via the LANE Network-to-Network-Interface (L-NNI). But this interface has not been standardised yet.

Figure 6 shows the Internet Protocol encapsulation, which is due to similar to the Classical-IP mechanism, the LLC/SNAP header has been used. The differences between both adaptations is the additional LANE packet with the receiver, transmitter address, and the LANE header field, which limited the packet size to 1500 byte. After that adaptation, the LANE packet will submit to the AAL-5 ATM layer.

Furthermore, LANE has not only advantages. Actually, the following disadvantages are obvious:

- Maximum Transmission Unit (MTU) has a size of only 1500 byte (normal Ethernet packet size)
- Therefore, the payload size is smaller than at Classical-IP
- MTU size must be the same in all participated networks (1500 byte)
- BUS limited LANE for multimedia applications
- Traditional LAN driver boards limit also the bandwidth
- Scalability is not efficient - only usable for small and medium networks
- QoS is not available

From this limited point of view, new solutions must be found for better adaptations of IP or further protocols to ATM. The following version for LANE is 2.0, which will include a redundant BUS structure, more scalability, and complete standardisation. At the end of 1997, the ATM Forum will complete this new version. [2, 3]

4.3 MPOA

Today many networks run a multitude of different protocols (e.g. IP, IPX, AppleTalk) and will continue to do so in the near future. Therefore these layer-3 internetworking protocols correctly imply the existence of multiple networks.

Solutions exists for internetworking IP (RFC-1577, NHRP, MARS) over an ATM network, but LANE supports only multiple protocols via a single ELAN. A single ELAN is logically a flat network within there is no need to route data streams. However, if a network consists of multiple ELAN that need to be connected, and the ELANs represent different layer-3-subnets, than a router is needed.

Therefore, the ATM-Forum develops the Multiprotocol over ATM (MPOA) specification. MPOA is a service, which support layer-3 internetworking for hosts attached to ELANs (running a LEC), hosts attached to ATM networks, and hosts attached to legacy LANs. MPOA provides and delivers the functions of a router and takes advantage of the underlying ATM network as much as possible. That means, MPOA works as a virtual router with real QoS features of ATM.

Figure 7 illustrates the idea of a virtual router. This router consolidates a number of different internetworking solutions over ATM. Therefore, the IETF specifications for intra- and

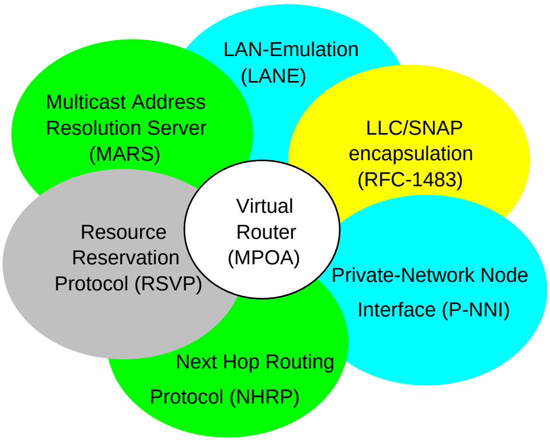

Figure 7: Virtual router of MPOA [3]

inter-subnet address resolution protocols (ATMARP and NHRP), IP multicast support (MARS), resource reservation (RSVP), and encapsulation solution for the multiple protocols (RFC-1483) will integrate into MPOA. Additionally, the ATM-Forum implements LANE and Private-Network-to-Network-Interface (P-NNI) into the virtual router environment. Both organisations work strongly together for the set-up of a comprehensive internetworking solution.

Next Hop Routing Protocol (NHRP) allows the use of shortcuts for the transmission of IP packets over ATM. Therefore, it is possible to send IP packets directly to other devices in other subnets without hop-by-hop routing between all subnets. Multicast Address Resolution Server (MARS) makes the support of IP multicast possible. MARS works as a virtual multicast server and allows also direct connections to the destination address. However, the Resource Reservation Protocol (RSVP) works as an bandwidth reservation mechanism. Thus, the ATM characteristics (QoS) can be adapted to IP packets. The P-NNI protocol of the ATM-Forum is a solution for the efficient routing of ATM cells. A P-NNI extension exists which allows also an IP routing.

The functions of a virtual router are similar like a real router, because the router has to fulfil two key functions: path computation and packet forwarding. But this virtual router is distributed over the ATM network. The advantages of a virtual router can be summarised in the following points:

- Support multiple protocols effective over ATM networks
- Distribute the routing functions between route servers that run the rooting protocol and inexpensive, high-performance data forwarding devices
- Separate routing from switching functions
- Leverages performance and QoS capabilities of ATM network
- Enables direct connections between ELANs rather than passing through traditional routers
- Enables direct Virtual Channel Connections (VCC) between data forwarding devices
- Interworking with unified routers
- Enables subnet members to be distributed across entire ATM network rather than physically collocated to unified router port
- Scalability of the ATM network is efficient enough for all kind of network sizes.

MPOA based on a client/server architecture like Classical-IP and LANE. MPOA clients establish VCCs with the MPOA server components for forward data packets or request information so that the client can establish a more direct path.

The functions of MPOA will be provided by the MPOA architecture. It can be described by the following components:

- Edge Device
- ATM host
- Default Forwarder Functional Group (DFFG)
- IASG Co-ordination Function Group (ICFG)

The edge device is a physical device that forwards packets from legacy LAN to an ATM LAN, at any protocol. An edge device may use a destination's network address or MAC address to forward a packet. Additionally, a query of an MPOA server for information before forwarding a packet is possible. Edge devices can be described as bridges or multi-layer switches, which allow clients which are not MPOA-capable to work within a MPOA architecture. An edge device is also a MPOA

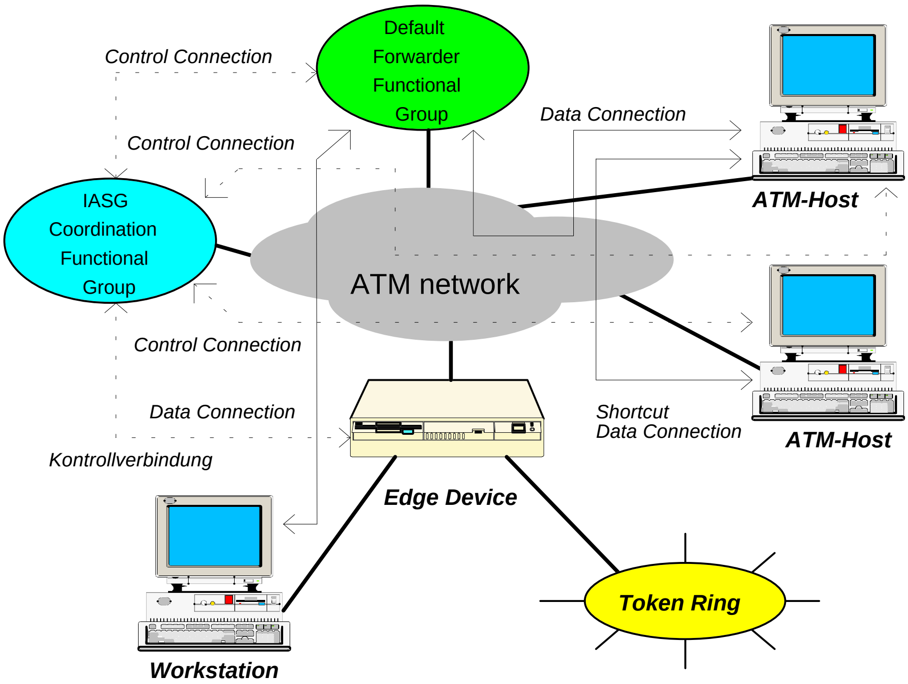

Figure 8: MPOA architecture [4]

client, which is called in a group Edge Device Functional Group (EDFG).

Another ATM client implementation that can query a MPOA server as well as forward packets at the network of MAC level is the ATM host. If there exist more than one ATM host it can be combined to a ATM Host Functional Group (AHFG).

Figure 8 shows the MPOA architecture which includes also the MPOA server Internetwork Address Subgroup Co-ordination Functional Group (ICFG). The Internetwork Address Subgroup (IASG) is a collection of devices that share a common layer-3 address prefix. The ICFG is a MPOA server which supports the distribution of a single subnet range across multiple legacy ports on edge devices or ATM hosts. The ICFG is coresident with the route server and one exists for each ISAG that the route server is attached to. For instance, if the route server was supporting IP and IPX there would be two ICFGs, one for IP and one for IPX.

Another MPOA server is the Default Forwarder Functional Group (DFFG), which allows to reduce the ATM connections to the ICFG. In addition, the call duration can be reduced. This would occur if IP packets of a transmitter can not assigned to a ATM connection to the receiver. In this case, the DFFG takes the packets, why it does not appear a connection set-up delay. If the DFFG recognises the receiver location, then the IP packets are transmitted further.

Besides the ICFG and DFFG servers, MPOA defines several other server types like Route Server Functional Group (RSFG), Remote Forwarder Functional Group (RFFG), and the Configuration Server Functional Group“ (CSFG). This servers are not showed in Figure 8, but complete the MPOA functionality.

CSFG commits the start configuration of the participated components. That means, CSFG assigned ATM addresses to the devices of the MPOA network. Additional, the maximum packet size (MTU) and the supported protocols will be defined.

RFFG and RSFG are responsible for the communication between several virtual networks. RFFG includes the forwarding part of the virtual router with multicast functions between MPOA clients, which do not need an edge device. Thereby, the MARS attempt is be realised and implemented in the ICFG. Before any multicast groups are sending or receiving, the MPOA clients have to ask the MARS.

However, RSFG realises the routing part of the virtual router. Also traditional router will be supported. Both router server offer a multitude of functions to map subnets onto the ATM network layers. The router server can work as standalone device or as additional functions inside a real router or switch. The router server includes address tables for the network layer and MAC addresses for ATM for the connection to ATM hosts and edge devices. Therefore, direct connections between two arbitrary devices are now possible.

MPOA has also some disadvantages like Classical-IP and LANE:

- MPOA is not a full defined specification of the ATM-Forum. First the IETF protocols have to develop further, before the MPOA is a final standard.
- The scalability is an extremely complex issue in a large network environment. Actually, it does not provides stable MPOA network.
- The standardisation of the IETF protocols NHRP, RSVP, and MARS is a difficult task, which needs more development. Therefore, the full MPOA architecture will be probably available in 1999.

LANE and MPOA are two efforts of the ATM-Forum that will enable traditional LANs and internetworks to run on top and coexist with ATM switched-based networks. LANE enables a group of ATM-attached clients to emulate the functions and protocols of a traditional Token-Ring or Ethernet LAN. An ELAN can internetwork with traditional legacy LANs through a bridge function. MPOA will enable multiple protocols to be routed and bridged over an ATM network with real QoS features. MPOA can also internetwork with traditional router-based networks. [4, 5]

The last chapters showed the possibilities of IP adaptations to ATM (Classical-IP, LANE, and MPOA). But the effectiveness of IP protocols, developed for low data rates, and the additional overhead are important as well. This issue will be described in the next chapters.

5 IP effectiveness

The Internet Protocol (IP) is very important to reach interoperability in a heterogeneous network. But the effectiveness of IP in high speed networks is not well-known. Especially, TCP performance is doubtful, because the acknowledgement mechanisms, overhead size, and parameter setting is a big obstacle. UDP is better suitable for real-time data streams, but has not any security mechanisms. This chapter will give a short overview about the effectiveness and parameter dependency of the IP protocol.

5.1 Protocol overhead

At first, the overhead over an IPoATM connection seems to be an obstacle. In the literature, overhead is described as an influencing factor for the effectiveness of IP datagrams over high speed networks, which the author agrees upon. However, applications which will be transmitted over a network do not use the whole bandwidth as it is the case in 155 Mbps OC-3c-SDH connections. Here, the overhead for the correct data transport is 5,76 Mbps for a SDH line using FDDI or DS-3 the overhead is even higher.

Figure 9 shows the different layers from the physical layer to the application layer. Each layer needs an own overhead for the integration of the IP and TCP/UDP protocol. This means, further headers or trailers will be added to the data stream and increase the overhead. Besides check of the protocol reliability, further fields are necessary, including Header Error Control (HEC), AAL-5-Cyclic Redundancy Check (CRC), and IP checkpoints. Additional fields are needed for multiplexing such as virtual paths/channels, IP sources and receiver addresses, and UDP/TCP port-numbers if available. Additionally, all fields process a length information of the Protocol Data Unit (PDU) and the connection status.

For the analysis of overhead effectiveness, different physical layers have to be analysed. This paper will give a impression about the Synchronous Digital Hierarchy (SDH) in a STM-1 (OC-3) frame. SDH is based on the transmission of STM-1 frames. One frame is sent every 125 microseconds, for a total of 8000

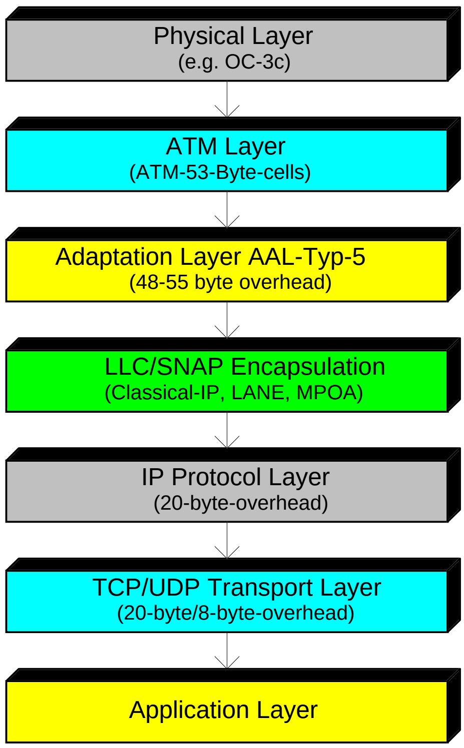

Figure 9: IPoATM layer sequence

Protocol Layers	OC-3c Interface		
Transmission Rate (PHY)	155,520 Mbps		
ATM Layer	149,760 Mbps		
Adaptation Layer 5	135,632 Mbps		
Maximum Transport Unit (MTU)	576 byte	9 180 byte	65 527 byte
LLC/SNAP Encapsulation	126,937 Mbps	135,220 Mbps	135,563 Mbps
Internet Protocol (IP)	125,198 Mbps	135,102 Mbps	135,547 Mbps
Transport Layer	120,851 Mbps	134,808 Mbps	135,506 Mbps
Application Layer via TCP	116,504 Mbps	134,513 Mbps	135,464 Mbps
Application Layer via UDP	119,112 Mbps	134,690 Mbps	135,489 Mbps
Σ Overhead for TCP/UDP (in percent)	39,016 / 36,408 Mbps (25,1 / 23 %)	21,007 / 20,830 Mbps (13,5 / 13,4 %)	20,056 / 20,031 Mbps (12,9 / 12,9 %)

Table 1: OC-3c interface overhead [6]

frames per second. The size of the frame depends on the data rate. An OC-3 or OC-3c frame is 2430 bytes long (9 rows of 270 bytes), for a data rate of 155,52 Mbps. SDH has three types of overhead: section overhead (SOH), line overhead (LOH) and path overhead (POH). SOH, LOH and POH consume 90 bytes of the 2430 byte OC-3c frame, or in other words 5,76 Mbps of an OC-3c stream, leaving 149,76 Mbps available to the layer above.

After the physical layer, the ATM layer contributes quite a bit to protocol overhead. Each ATM cell is 53 byte long, comprising a 5-byte header and a 48-byte payload, so 9,4% of each cell is overhead. Fields in the header provide for multiplexing (virtual paths and channels), traffic type indicators, and a header checksum.

There are two sources of overhead in AAL-5: protocol overhead in the form of a trailer at the end of the data unit, and the fact that an AAL-5 PDU occupies an integral number of ATM cells. AAL-5 has an 8-byte trailer which is appended to each PDU. AAL-5 uses further an integral number of cells for each PDU. The AAL trailer occupies the last 8 bytes of the last cell. Since AAL-5 PDUs are variable length with a maximum of 65,535 byte, there may be up to 47 byte of padding. For instance, a 576-byte PDU exactly fills 12 ATM cells, leaving no room for the AAL-5 trailer: a 13th cell would therefore be required. It would contain 40 byte of padding and the 8-byte AAL-5 trailer.

Then the data stream will be encapsulated for the adaptation of IP datagrams. The SNAP/LLC encapsulation needs an additional header for LLC, OUI, and PID field and amount to 8 byte per datagram.

The overhead at the IP layer consists of the IP header. Although the header is variable in length (1-65535 byte), it is always 20 byte long for an efficient processing (its minimum length). Like IP, TCP's overhead consists of the TCP header. Again, the header is variable in its length, but is usually 20 byte length. In this paper, TCP has always 20 byte of overhead per segment, and each TCP segment corresponds to an IP datagram. However, the UDP's overhead consists only of 8 byte, because the header provides for multiplexing and data integrity.

Table 1 shows the amount of bandwidth that remains after each successive layer has claimed its share of the overhead. Each row in the table shows how much bandwidth is available for the indicated protocol layer as throughput. Therefore, three different MTU sizes are indicated:

- 576 byte (standard size for Internet)
- 9180 byte (standard size for IPoATM)
- 65527 byte (maximum IP size over AAL-5)

For an OC-3 stream, the bandwidth available to the application is in the range of 116,504 to 135,498 Mbps. But it is very important for a low overhead that the MTU size amount is 9180 byte. The overhead does not change between 9180 and 65527 byte. This is the reason, why 9180 byte described as a Default-Maximum Transmission Unit (D-MTU). The limitation of the D-MTU can reduce the transmission errors, because the loss of one ATM cell means the loss of the whole AAL-5 layer packets. Therefore, the maximum size of data packets is only a theoretical value which is not relevant for practical transmissions.

Differences between TCP and UDP transmission does not exist hardly concerning the overhead. That is not unusual, because the difference in the overhead size between these both application layer protocols is only 12 byte.

Altogether, the overhead of an OC-3 frame is relatively smaller (approx. 14%) if you use a MTU size of 9180 byte. Other physical interfaces (e.g. DS-3) can have a higher overhead. But in principle, the overhead is not an obstacle for the IPoATM effectiveness. [6]

5.2 TCP throughput obstacles

Originally, the TCP/IP protocol stack was not designed for high speed performance networks. Several extensions of the TCP protocols have been suggested to achieve higher performance over these networks and for connections with a high bandwidth delay. New bandwidth-intensive applications, such as multimedia conferencing systems (CSCW), and the characteristics of high speed networks have triggered a lot of research on advanced transport protocols. Therefore, the discovery of additional error sources are not surprising. The following identified factors are responsible for inefficiency of TCP protocols over ATM:

- Send and receive socket buffer size
- Network: Maximum Transport Unit (MTU)
- Protocol: Maximum Segment Size (MSS)
- Transmitter: use of Nagle's algorithm
- Round Trip Time (RTT)
- Receiver: delayed acknowledgement mechanisms
- Transmitter: Silly Window Syndrome (SWS)
- Copy strategy at the socket interface
- Network congestion and lost notice

The throughput of a TCP/IP connection can dramatically drop, if the socket buffer sizes, such as send socket buffer of 16 kbyte and a receive socket buffer of 32 kbyte were chosen. The TCP/IP protocols use the size of the network MTU to compute the MSS. The ATM MTU is given by the ATM Adaptation Layer which is the end-to-end-service on an ATM network. The larger the MTU the larger the MSS.

The dramatic drop in the performance is caused by the deadlock situation in the TCP connection which is broken up by 200 milliseconds timer generated TCP acknowledgement. It causes TCP to behave as stop-and-go protocol with one or two data segments sent very 200 milliseconds. The deadlock occurs when the amount of data sent to the receiver is not enough to trigger a TCP window update packet, and the same time there is not enough buffer space in the sender buffer to create a segment of size MSS byte. Nagle's algorithm prohibits the sending of non-MSS segments if there are unacknowledged bytes. Since TCP acknowledgement on window updates, the connection is deadlocked until the receiver sends a timer generated acknowledgement.

The deadlock problem also exists for small MSSs and low speed connections, but it is not so probably. Actually, it will not happen for socket send buffer which are larger than three MSS segments. Furthermore, for small MSSs the discrepancy between the normal and degraded throughput is not that big, which makes it difficult to detect or uninteresting to investigate into. The most straightforward way to prevent many of the deadlock situations is to switch off the Nagle's algorithm. There is hardly any performance penalty having it switched off. A straightforward avoidance solution it to ensure that the send socket buffer is equal or greater that the receive socket buffer. These is one alternative next to others which requires small changes in the TCP implementation.

TCP's end-to-end flow control is through a sliding window mechanism where the receiver announces its free buffer space to the transmitter. Therefore, when data is copied to the application the receiver checks if a window update packet should be returned (Silly Window Syndrome). The algorithm for sending a window update works if the window slide more than either 35% of the receiver buffer size or two MSS segments. Both the socket send and receive buffers limit the amount of data that can be outstanding between two communicating TCP peers. The available space (maximum – current amount of data bytes) of the socket receive buffer is used to set the announced TCP window size to ensure that the sender will not send more data than can be received. The send socket buffer is used as the repository for TCP segments to be used in case of re-transmissions. Since data byte remain in the send socket buffer until they are acknowledged, the available space for copying in new data into the socket send buffer is reduced (Silly Window Avoidance).

Furthermore, acknowledgements are also necessary after a connection establishment via a TCP/IP protocol. That means, every 200 milliseconds the sender sends an acknowledgement to the receiver. If TCP segments are lost, the function Retransmission Time Out (RTO) will be started, which retransmits lost data. The effective throughput is decreasing during the repeated data transmission. After an acknowledgement for the reception by the receiver, which confirms faultless transmission, the acknowledgement messages are being only sent in intervals of 500 millisecond (RFC-1122). In case of losses the connection will interrupted.

The Round Tip Time (RTT) is an additional throughput factor. RTT is the time which needs a TCP segment from the sender to the receiver and vice versa. RTT depends also on the time-out value. If the time-out value is to low, then the transmission can be repeated during less RTT fluctuations. If the time-out value is to high, then segments can be lost. Both cases influence the throughput of a TCP/IP connection. Therefore, to find the appropriate RTT value is a critical issue for the TCP performance.

A further possibility to have less throughput in TCP/IP connections is the network congestion and lost notice. In the past, switch buffers have not been built for high data streams and there was no congestion control of the ATM network. Nowadays, the smaller sized TCP packets without need for fragmentation and the larger buffer sizes of the ATM switches improve the situation and make the data transmission much more effective. Also congestion control is available for ATM networks, why this point is not relevant for networks any more. But if the ATM networks will expand in the next years, real network traffic will be a problem.

The EIES project had not the resources and the experience to carry out measurements for the different TCP obstacles without any external aid. Literature, small own measurements, and relevant project results such as EXPERT (Experimental Platform for Engineering Research and Trials) was collected.

5.3 Sender and receiver buffers

Table 2 shows the average throughput for various sender and receiver buffers. As this table shows in general TCP throughput increases as the sender's and receiver's buffer sizes increase. Some experiments show a decrease in the throughput when send and/or receive buffer sizes are too small.

The throughput measurements have been carried out over a 155 Mbps connection between two separate UNIX workstations with Solaris2.5. In each measurement, the source transmitted 32 Mbytes of data to the sink. Of course, all measurements used AAL-5 to encapsulated IP packets. The sender buffer are ordered into the horizontal lines and vary between 16-52 kbyte, while the receiver buffer are ordered into the vertical lines with the same values.

Table 2 shows clear drops of the throughput if the sender or receiver buffer is to small. Especially, the throughput rate at a sender buffer size of 16 kbyte is low. Here the data rate fluctuates between 0,319 and 15,05 Mbytes. Buffer sizes over 28 kbyte have an essential better throughput.

S/E	*16 kbyte*	*20 kbyte*	*24 kbyte*	*28 kbyte*	*32 kbyte*	*36 kbyte*	*40 kbyte*	*44 kbyte*	*48 kbyte*	*52 kbyte*
16 kbyte	15,05	13,60	0,322	0,319	0,319	0,467	0,469	0,466	0,469	0,469
20 kbyte	15,99	14,60	15,07	14,87	15,40	14,24	1,095	1,095	0,548	0,549
24 kbyte	17,71	16,79	16,74	16,32	17,40	17,31	17,42	17,12	0,760	0,740
28 kbyte	16,57	17,69	17,93	18,13	18,36	19,20	19,74	19,78	18,38	18,20
32 kbyte	14,63	18,96	18,42	19,23	19,14	19,74	19,96	20,31	19,69	19,17
36 kbyte	14,33	19,22	18,12	19,82	19,77	19,92	20,56	20,49	20,13	20,20
40 kbyte	15,16	19,34	18,85	19,73	20,11	20,41	20,81	20,74	20,69	20,57
44 kbyte	14,80	19,40	18,27	20,39	20,16	20,74	20,99	20,87	20,89	20,70
48 kbyte	14,62	19,46	18,34	20,48	20,26	20,41	20,85	20,83	20,93	20,83
52 kbyte	13,92	19,41	18,26	20,50	20,06	20,21	20,88	20,91	21,21	21,06

Table 2: Throughput in Mbps for the transmission of TCP/IP over ATM [7]

The reason for the deadlock phenomenon is the too less dimensioned sender and receiver buffers, as mentioned already. This sizes are not suitable to process efficiently the defined MSS size of 9140 byte (9180 byte minus the 40 byte header of the TCP/IP packet). This value of the MSS causes a circular idle situation which creates a lockstep interaction with an unnecessary long delay. Therefore, a neutral situation arises for the network, because the devices wait of a further data transport. This is one reason why the throughput decreases rapidly.

Deadlock does not appear if the maximum buffer sizes are used for sender and receiver. This is the reason why both buffer sizes shall ever have the maximum size of 54 kbyte for Solaris 2.4.1 and 64 kbyte for Solaris 2.5. Windows95/NT has even a fixed buffer size of 64 kbyte. However, the receiver buffer is not ever eligible. Therefore, it is enough to set the sender buffer size to at least three times higher than the MSS size. Then deadlocks will not appear. [6, 7]

5.4 RTT and MTU deadlocks

TCP segments will only be transported if the sliding window mechanism makes this possible. After one packet is sent, the sender waits of an acknowledgement from the receiver for each segment. This acknowledgement message will be put into the sequence number field of the next TCP segment. In the process TCP needs a time-out value for each transmitted segment. If any packet can not confirm its arrival at the receiver site before time-out the data will be retransmitted.

This is the reason why the time-out value depends on the round trip time (RTT). If the time-out value is to low, then unnecessary retransmission is the consequence, because the RTT value can vary by the different switch routes. However, by to high values it can lead to segment losses. This means, the appropriate choice of the time-out value has a substantial effect of performance.

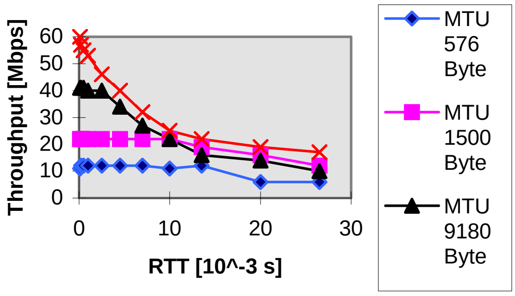

Figure 10: TCP throughput and RTT for different MTUs [8]

Figure 10 shows the importance of the MTU values regarding the throughput. Therefore, the MTU value of 9180 byte approaches very well the maximum window size. This can be compute by the following formal:

$$WindowSize_{\max} = \frac{W}{T_{Processing} + RTT}$$

W contains the receiver buffer size and $T_{Processing}$ is the processing time which arises between sender and receiver if a define data amount will transport to the receiver through the whole protocol stack. The time response here 6,495 milliseconds and will add to the RTT value for get the effective RTT. This RTT value can be defined as a function of the TCP implementation (TCP buffer size, MSS, MTU, etc.). The maximum window size is 65536 byte and will be limited by the receiver buffer.

Furthermore, Figure 10 shows ever less the RTT value is, the throughput is increasing. This means also that the values are limited by the ATM clients, because the window size limit has not been reached. If RTT is higher, the throughput decreases to values between 10-17 Mbps, because the delays are too high. Additional small MTU values like 576 byte (Internet standard) and 1500 byte (LANE) do not reach bandwidth over 60 Mbps. This does not depend on the RTT delay, because an additional fragmentation is necessary and therefore the performance goes down. That means, the MTU is smaller as the used packet size, which the packets at the sender will be fragmented and must be reassembled at the receiver. This indicates additional processing time. [8]

5.5 UDP performance

User Datagram Protocol (UDP) provides a network- independent transport service for the transmission of datagrams for higher protocol layers. By the use of UDP a minimum of protocol mechanisms are be used. UDP does not include end-to-end control, nor acknowledgement mechanisms, duplicate detection, sequence retention at the receiver, and retransmission. Therefore the data will be sent without control of the protocol. Other protocols must control the throughput and the correct data transmission.

Due to the connectionless structure of UDP the adaptation of this protocol to ATM is more difficult than the TCP protocol. The virtual

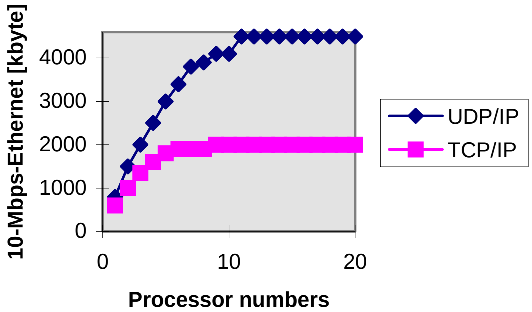

Figure 11: Performance measurement in multi-processor environment [6]

channel/path structure of ATM connections can be better used by the connection-oriented TCP packets.

The locking effects give a good overview about the performance of both protocols. Locks are used to protect shared protocol state and data. Mutual exclusion by locking can be costly if the parallel protocol code frequently accesses shared state and data. This can has an effect on the performance.

TCP uses a big amount of locking mechanisms, which prevents the simultaneous access to a simultaneous state. Therefore, both performance prevents of a network are the contention situations of the locking mechanisms and the clients. Locking limits mainly depend on the protocol implementation, and not on the machine it runs on. On the other hand, machine contention (contention for shared resources such as busses or memory) is machine dependent.

In multiprocessor environments a few measurements have been done for the comparison of both protocols. There, an Ethernet-based LAN (10 Mbps) was used. Figure 11 shows the performance of both protocols at the direct write and read of data from the kernel buffer. A repletion is reached for UDP at 4500 kbyte and for TCP at 2000 kbyte. This means, that the locking mechanisms in a parallel shared memory multi-processor system the throughput limited. Especially the TCP protocol is affected, because of its locking mechanisms. UDP does not need many locking mechanisms and therefore the performance is not limited on the same way. UDP gets only limitation by the CPU performance, data bus access, and the shared memory. [6, 9]

5.6 Client performance

High data throughput needs high speed networks like ATM to support real-time and multimedia applications. But networking software or hardware is often a major bottleneck in this context. Analysis of the components of networking software reveals that the data copy and checksum overhead dominates processing time for high throughput applications. Older generation networking software and hardware often required multiple data copy and separate data checksum operations on each byte of a data packet. Since the last four years it gives a number of successful implementations (such as in the Solaris operation system) introducing single-copy (CPU copy). They are often combined with the TCP checksum calculation in one single loop, resulting in substantial throughput improvement. A further improvement for a better throughput is the zero-copy method, which the data transport between the application domain and the network interface without CPU load. The goal of the zero-copy mechanism is to reduce the per-byte cost from the current single-copy + checksum design.

The overhead in networking software can be broken up into per-packet and per-byte costs. Generally, the per-packet cost is roughly constant for a given network protocol, regardless of the packet size, whereas the per-byte cost is determined by data copying and checksum overhead. To reduce per-byte cost, Solaris 2.4 and 2.5 introduced combined single copy and checksum design.

High throughput applications often send large packets to amortise per-packet costs over many data. However, the communication link imposes an upper bound on the packet size that can be accepted. This limit (MTU) is relatively small for traditional network media (1500 byte for Ethernet). Therefore, the communication overhead on those networks is still dominated by the per-packet cost.

Other communication media employ larger MTUs (e.g. FDDI: 4352 byte). The per-byte cost on these networks adds up to a significant portion of the total networking overhead, as showed by Figure 12.

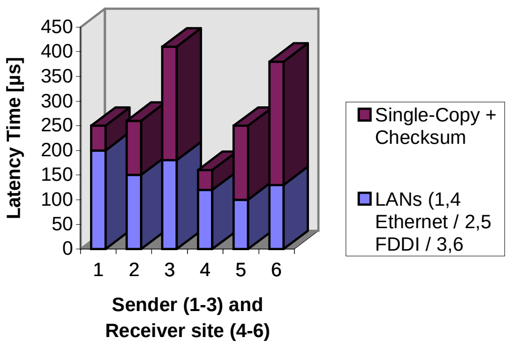

Figure 12: Networking overhead in Solaris 2.5 [10]

Figure 12 shows a memory-to-memory TCP test with the operation system Solaris 2.5. For TCP/IP packets going through ATM networks, the copy + checksum overhead accounts for over 60% of the total networking software overhead on the end hosts. Ethernet needs only 25% copy + checksum overhead for the same work. That means, the process effort and the requirements for the client are higher if the MTU size and the data rate increase. By the additional process effort increases also the latency time. An important criteria for clients is therefore the process time of the machines which is limited by the following points: [6, 10]

- Operation system (inter-process communication)
- Data processing
- CPU performance
- Memory speed
- I/O bus bandwidth
- ATM adapter implementation

5.7 Performance improvements

Actually, the clients are by the traditional LAN networks for high speed networks false configured. For the usage of the high bandwidth the clients must be better configured. The following criteria can be helpful for compensated the mentioned disadvantages:

- *Maximum Transmission Unit (MTU):* The MTU value limited the frame size of a system. That means, the connected clients must use the same MTU value. For Classical-IP 9180 byte is standardised and LAN-Emulation uses only 1500 byte. These values does not change in every cases, because they are defined for the ATM adaptation.
- *Path Maximum Transmission Unit:* This value define the minimum size of a MTU value for all connected networks between two communicated clients. The minimum value define the biggest IP packet, which does not need fragmentation. RFC-1191 specified one method to recognise this value.
- *TCP sender and receiver buffer:* The window size is given by the buffer size. For the best performance the chosen value must be the at least two times bigger than the actual MTU value. The maximum value at the operation system Solaris 2.5 is 64 kbyte and should be taken.
- *Maximum Segment Size (MSS):* The MSS limits the size of TCP segments. For local networks the default is 536 byte. A value of 1436 byte is without problems in high speed networks, but may cause some problems on slower connections. Together with Path-MTU Discovery (RFC-1191) this size should use of the interface MTU.
- *Window Scale Option:* The standard RFC-1323 describes a further improvement for a better performance. RFC-1323 allows to get a larger window size of maximum 2^{30} byte. This option is bi-directional and will establish during the set-up of the connection. A timestamp-option is also available which must be supported by both communication partners. Additional the TCP header gets higher from 20 to 32 byte. By this function the RTT value gets also higher. Therefore less critical time-outs arises.

If the right setting is used, the data rates like the theoretical data rate of a 155 Mbps connection can be reached. Prerequisite is the use of workstations with high performance (e.g. DEC, Alpha, or Ultra-SPARC). The following values are measured on a 155 Mbps connection (OC-3c) for Classical-IP and LANE with simple file transfer between two workstations under optimised conditions:

- Classical-IP: MTU 64 kbyte, time delay 10 milliseconds, bandwidth 134,01 Mbps
- LANE: MTU 64 kbyte, time delay 10 milliseconds, bandwidth 117,63 Mbps

Classical-IP has a better performance for a point-to-point connection between two workstations as LANE. Further test will started to check the performance for complex network structures under real conditions.

6 Conclusions

The project EIES and especially the partner BIBA analysed the various kinds of IPoATM solutions and the IP effectiveness. The IP effectiveness depends on several characterise of TCP / IP protocols like overhead, sender and receive buffers, MTU / MSS sizes, and others. This analysis was necessary for the interoperability and efficient interactions of the EIES network platform, which consist of fixed networks like ISDN and ATM and the mobile network access possibilities like DSRR, DECT or / and Inmarsat.

The user requirements and the interoperability between thus different networks were necessary for the implementation of the Internet Protocol (IP) in the EIES environment. Therefore, Classical-IP and LANE were tested in a real ATM environment (the High Speed Network in Bremen). Further studies are needed to implement MPOA in the next step for a real QoS.

For an efficient IPoATM implementation it is further necessary to investigate enough time to configure the participated devices and software for a high performance. ATM is a new technology which considerable extents the usable bandwidth with regards QoS parameter. Nowadays, workstations are only tuned for the work in traditional networks such as Ethernet or Token Ring. This deadlocks must be compensate for an efficient use of IPoATM.

Summarised, the UDP protocol is a better solution for using real-time application, because of its simple structure. But there must be other protocols implemented which can guarantee the end-to-end control. The TCP protocol is the better solution for a secure end-to-end connection, but the configuration for the clients is non-trivial. Additionally, other protocols will develop for QoS features at IP such as RSVP, MARS, and NHRP. In the near future, ATM and IP can be used without limitations via MPOA.

Author

Kai-Oliver Detken studied at the technological highschool of Bremen electrical engineering and communication before he changed to the University of Bremen to the field information technology. Parallel to his study and after his final examination he works in several European projects like MOEBIUS, SECURENET-II, and EIES.

Actually, he is a research scientist at the Bremen Institute of Industrial Technology and Applied Work Science at the University of Bremen (BIBA) in the department Manufacturing Systems, Communications and Telematics.

References

[1] K.-O. Detken, U. Kaufmann, Dr. C. Böttger, J. Shin, E. Novoa, L. Pachali: *Detailed specification of EIES demonstrator*; Deliverable 6 of the project EIES; Brussels, January 1997

[2] G. C. Sackett, C. Y. Metz: *ATM and Multiprotocol Networking*; McGraw-Hill Series on Computer Communications; New York 1996

[3] K.-O. Detken: *IP-over-ATM*; professional journal Gateway 03 / 97; Heinz Heise publishing house; Hanover 1997

[4] K.-O. Detken: *Virtual Router: Multiprotocols over ATM - part 1;* professional Journal Gateway 04 / 97; Heinz Heise publishing house; Hanover 1997

[5] K.-O. Detken: *Services with Quality: Multiprotocol over ATM - part 2;* professional Journal Gateway 05 / 97; Heinz Heise publishing house; Hanover 1997

[6] K.-O. Detken: *IP-over-ATM effectiveness*; professional Journal Gateway 05 / 97; Heinz Heise publishing house; Hanover 1997

[7] Douglas E. Comer, John C. Lin: *TCP Buffering and Performance over an ATM network*; Purdue Technical Report CSD-TR 94-026 (Revision); Pordue University; Department of Computer Sciences; West Lafayette, Indiana (USA) 1994

[8] Witters, Jaussi, Van den Berg, Foreest, Gijsen, Winstanley, Louis, Ooghe, Blaabjerg, Andrade, Ramón, Pettersen, Aarstad, Müller, Baumann, Blondia, Peeters, Spaey, Casals, Barcelo, Cerda, Lorang, Renger: *Specification of Integrated Traffic Control Architecture;* Deliverable 6 of the project EXPERT; Brussels, September 1996

[9] Mats Björkman, Per Gunningsberg: *Locking Effects in Multiprocessor Implementations of Protocols;* Department of Computer Systems and Swedish Institute of Computer Science; Uppsala University; SIGCOMM'93; Computer Communication Review; Sweden 1993

[10] Hsiao-keng Jerry Chu: *Zero-Copy TCP in Solaris;* Internet Engineering Group at Sun Microsystems and SunSoft Inc.; USA 1994