InterWorking Between IFMP Switching And B-ISDN Access Protocols

L. Cipriani*, D. Di Giorgio*, M. Pugliese*, S. Salsano*
* Ericsson Telecomunicazioni S.p.A., *CoRiTel, Università “La Sapienza” di Roma

Abstract

IP traffic is growing every day and it is reasonable that IP routers will become bottlenecks in the near future. A solution seems to be the IP switching approach. This approach consists in the coupling of IP routing to fast hardware switching, typically ATM. In this work we are focused on a particular IP switching paradigm, the Ipsilon Flow Management Protocol (IFMP). Nowadays IFMP switching is supported within LAN environments. Our effort is focused to export IFMP switching to WAN environments, in particular to public ATM backbones. In this work we introduce an interworking mechanism to couple IFMP switching to B-ISDN access signaling capabilities (ITU Q.2931). This mechanism is fully compliant to both IFMP protocol and B-ISDN signaling. Detailed simulations, using SDT tools, of this interworking mechanism has been carried on and it will be described.

1 Introduction

Due to the growing demand of multimedia application and the progress in high speed communication technologies (Fast Ethernet, Giga Ethernet, FDDI, ATM, etc.), the current IP routers are becoming a critical bottleneck. The IP switching concept, combining the best of IP with the hardware switching of ATM, seems to be the “fashion” solution to overcome the bottleneck. Nowadays the IP switching proposals (CISCO, Ipsilon, Toshiba, etc.) find applications mainly for campus and corporate environments (LANs).

Moving from the private LAN scenarios to the Wide Area Networks (WAN), usually managed by the Public authorities, new interesting market perspectives can arise for the Public Network Operators (PNOs). IP switching functionality in WAN scenarios can be added at the access section. In WAN scenarios switched connections are desirable, as they allow scalability and internal network resource optimization and they can cope with the foreseeable increasing in IP-based services demand capillarity.

In the paper an approach for the extension of IP switching paradigms into a Public Network is proposed. In particular we considered one of the most promising proposal for IP switching, the IFMP (Ipsilon Flow Management Protocol) [1] approach supported by Ipsilon Inc., and its interworking with the Public B-ISDN access signaling protocol (e.g. ITU-T Rec. Q.2931), provided by the Public LEXs. Although we will not focus on it, an alternative approach has been proposed by Toshiba in their FANP protocol and published by the IETF in RFC 2129, April 1997.

2 IFMP Switching Paradigm

The goal of a device implementing the IFMP solution is to provide the functionality, scalability and robustness of IP, as well as the performance of fast switching technologies (mainly ATM). Two functionality, intelligent IP routing and fast ATM forwarding, both recognized as important for future high-speed networks are thus combined on a single platform.

An IFMP switch is basically an enhanced IP router, and as such it is fully interoperable with the existing base of IP routers. From the point of view of the network administrator, it is not different from a router, so it does not create new management problems. In the traditional IFMP approach, two adjacent IP switches are connected by a dedicated ATM link. In both directions there is a default ATM channel where IP packets are conveyed by default and a set of available VPI/VCI over which one IFMP switch can request the other one to redirect the IP flows by means of IFMP redirection protocol. The core of this mechanism is the flow recognition algorithm, which selects the IP flows which are worth to be redirected on a dedicated ATM VC connection. From now on we will use the term “IFMP switch” to refer to an IP switch implementing the IFMP paradigm.

In our paper we will distinguish between IFMP switch and IFMP gateway switch. The IFMP switch is the fundamental component of traditional IP switching and its behavior will be briefly recalled in this section. The gateway switch is intended as an “edge device” to provide fast interconnection of legacy and high-speed LANs to remote IP-switched backbones via public network or to interconnect high-speed island each other via the public network. The behaviour of the gateway switch will be defined in the next sections.

When an IFMP switch boots, it is configured to use a “default” virtual channel with VPI = 0 and VCI = 15 over all its ATM physical interfaces. When cells first arrive on an ATM port, the IFMP switch reassembles AAL5 frames and IP datagrams. As in “conventional” IP paradigm the IP router module processes these packets and forwards the data on the proper outgoing ATM interface according to the destination address, using the default VC (0, 15). In the same time the data stream is classified in traffic flows. The classification mechanism may be based on traffic observation and protocol header information. A basic form of classification identifies flows as sequences of packets with the same transport protocol type and the same IP source and destination addresses and transport port numbers. Flow classification is an internal operation that is made independently of switches, without network-wide co-ordination. This improves the robustness and scalability of
the architecture. Once a particular flow is recognized in consecutive IFMP switches on the path it follows, its packets can avoid IP-level processing, because cut-through happens at the ATM level. The following procedure describes this operation.

- The intermediate IFMP switch recognizes the flow and asks the upstream switch (see Figure 1), using the IFMP protocol, to create a new virtual channel connection for the newly-identified flow. A VCC here is characterized by the VPI/VCI identifier that is specified in the request. Note that there is no ATM signaling procedure to invoke.
- The upstream switch “redirects” the flow data from the default channel to the new channel. Now, the intermediate switch receives the flow data on the new virtual channel.
- The same procedure, in turn, may happen between the downstream and the intermediate switch.
- If both the procedures have been completed, the input and output virtual channel identifiers for the flow in the intermediate switch are fully defined. The IFMP switch controller (see Figure 2) can request the switch fabric (using GSMP [2]) to cut-through the flow, so that the flow data can be switched by the ATM hardware without being processed at the IP level.

As outlined above, in the context of a private IFMP network, each port of an IFMP switch is directly connected to another IFMP switch. This mechanism cannot easily be extended to the Public Network. If an IFMP switch in a private network wished to establish a link, across the Public Network, with any other remote IFMP switch, we should foresee as much ports at the UNI, as the possible destinations. In this paper we envisage some solutions to interconnect IFMP switches across the Public Networks.

2.1 Aspects of IFMP protocols

The aim of this section is to provide a brief and general description of the IFMP protocol [2]. We will focus the attention only on those aspects we need for our work. The IFMP protocols consist of:

- the Adjacency protocol: it allows a host or router to discover the identity of a peer at the other end of a link. It is also used to synchronize state across the link, to detect when the peer at the other end of the link changes, and to exchange a list of IP addresses assigned to the link;
- the Redirection protocol: it allows two adjacent switches, synchronized by adjacency protocol, to exchange messages in order to re-direct IP flows on dedicated virtual channel.

The following table (see Figure 3) shows the set of messages in the IFMP protocols.

<table>
<thead>
<tr>
<th>Adjacency Protocol</th>
<th>Redirection Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN</td>
<td>REDIRECT</td>
</tr>
<tr>
<td>SYNACK</td>
<td>RECLAIM</td>
</tr>
<tr>
<td>RSTACK</td>
<td>RECLAIM ACK</td>
</tr>
<tr>
<td>ACK</td>
<td>LABEL RANGE</td>
</tr>
<tr>
<td>ERROR</td>
<td></td>
</tr>
</tbody>
</table>

For a detailed description of the IFMP protocols messages and procedures, you can refer to [3]. As far as the redirection protocol is concerned, each message is composed by a common set of header fields and by a message body specific to the message. We will briefly describe the REDIRECT message, which will be used in the next section. The message body of the Redirect message is shown in Figure 4.

The Redirect message element is used to instruct an adjacent node to associate a given label (i.e. a VPI/VCI identifier) to packets belonging to an identified IP flow for a specified period of time. The redirect message is not acknowledged, and can be repeated to “refresh” the association before it expires. In order to show the main features of the Redirect Message, together with its use, in Figure 5 we have shown a typical scenario with a data transfer between an FTP server and an FTP client along a path on an IP switched backbone. IP addresses of some interfaces are shown. The flow data is carried on the default channel with all other data.

As shown in Figure 5, the architecture of IFMP networks allows for efficient and flexible data transfer across the Public Network. The use of virtual channels and cut-through switching enables high-performance data transmission, avoiding the overhead of IP-level processing. This is made possible through the use of the IFMP protocol, which allows for the establishment of virtual channel connections and the redirection of data traffic.

In summary, the IFMP protocol provides a robust and scalable solution for network connectivity, particularly in scenarios where high-speed data transfer is required without the overhead of IP-level processing. The ability to dynamically create and manage virtual channel connections ensures that network resources are utilized efficiently, while the cut-through switching mechanism further enhances performance by reducing latency and improving overall network throughput.
encapsulated in an IP packet. This is shown in Figure 6. The message contains the IP destination address (i.e. the node 1 address), the flow type (type 2, in this example), the lifetime (i.e. the validity duration of the redirection), the label (a VPI/VCI identifier) to be assigned to the flow on the link between the two nodes, and the flow identifier for type 2 flows (which is composed of source IP address and destination IP address). For an explanation of the flow types please refer to [3].

REDIRECT

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 6: Example of a REDIRECT message

As a result of the Redirection message, the IP flow will be redirected on the specified VCC, which is shown as a dashed line in the picture.

3. Scenarios for interworking

In this section we provide two scenarios for the interworking of IFMP switches and the Public Network.

In the first scenario we assume that a single remote IFMP switch can be reached through the Public Network from a “gateway” IFMP switch. This scenario is shown in Figure 7. The remote IFMP switch could be owned by a Service Provider which gives global Internet connectivity to a private network of IFMP switches. The natural evolution is to allow the gateway IFMP switch to be connected to a set of remote IFMP switches through the public UNI interface. This is depicted in Figure 8. We could think of a set of IFMP based local area networks interconnected through the Public Network.

The main technical challenge is to allow the IFMP flow redirection on a Public Network, where each flow should be mapped on a Switched Virtual Channel corresponding to a Call controlled by Q.2931 signaling. The first scenario above described is preliminary to the second one. Many aspects are simplified, as it is easier to correlate the IFMP flows with the Q.2931 calls when only one possible destination exists on the public UNI. Then the envisaged technical solutions for the first scenario will be extended to fulfill the requirements of the second one, where each “gateway” IFMP is connected to a set of remote IFMP switches.

As shown in Figure 7, in the basic scenario, a set of IFMP switches are interconnected by dedicated ATM links in a private network context. One of the IFMP switch, the “Gateway IFMP switch” is also connected to the Public Network across an UNI interface. A single “Remote” IFMP switch can be reached from the private network. On the interface between the Gateway IFMP switch and the Remote IFMP switch, the traditional default channel (VP = 0, VCI = 15), has to be replaced by a semi-permanent ATM connection, therefore some enhancements to the Gateway IFMP switch logic will be needed. The Gateway IFMP switch will maintain its typical behaviour on the other IFMP interfaces in the context of the private network. The redirection of the IP flows on the (logical) interface between the gateway and the remote IFMP switch will be performed over additional ATM VC connections which will be set-up by means of public UNI signaling. It is reasonable that the IP flow recognition algorithms will be modified in order to take into account the cost of the new connections crossing the Public Network, as well as the longer connection set-up time.

Figure 7: IFMP switching scenario with a single reachable IFMP remote switch

As shown in Figure 8, in the second scenario a gateway IFMP switch must be connected to several remote IFMP switches. A set of ATM VC connections is needed to transport the IFMP default channels linking the Gateway IFMP switch to the remote IFMP switch. Further requirements for the interworking with public network can be envisaged in this scenario, however in the rest of the paper we will be concerned mainly with the basic scenario, while the target scenario is left for further study.

Figure 8: IFMP switching scenario with a set of a IFMP remote switches
4. Proposed architecture for interworking

In order to support the above scenarios, solutions for the interworking of IFMP like protocols and the access signaling protocol, i.e., the ITU-T Rec. Q.2931, are needed. The requirements we have taken into account to define our solution are to limit as much as possible the changes in IFMP protocols and to propose a solution fully compliant to public UNI standards.

The IFMP logic should work as if the connections going through the public UNI were local connections. This does not prevent to introduce some modification to the flow recognition algorithms if we want to take into account that the flow will be redirected to a public network. From the point of view of IFMP protocol message exchange, the same mechanism will be used to redirect a flow on the public network or on a private local connection. An interworking unit within the gateway IFMP switch will allow the IFMP logic to interact with the public signaling domain. The standard public UNI signaling must be used without any change, therefore the mechanisms to convey additional information for IFMP connections must be chosen carefully. In other words, there is no need of a specific support of IFMP in the public network.

In Figure 9 the control plane architecture for the interworking of IFMP and public UNI is shown. The IFMP entity in the gateway switch will have an IFMP relationship with the IFMP entity in the remote switch. As we will show later, the traditional IFMP protocol will run over this relationship with a simple single extension in the semantic. The two IFMP entities will exchange REDIRECT and RECLAIM messages to negotiate the redirection of IP flows. The IWU (InterWorking Unit) extends the IFMP logic on one side to ask for the setup of the connections through the UNI when needed and on the other side to handle the incoming connections. When one IFMP entity receives the REDIRECT request for a flow which will transit through the public network, it will ask the set-up of the connection to the IWU. The IWU in turn will ask to the Q.2931 user side the set-up of the connection. The IWU on the remote side will receive from the Q.2931 the indication of an incoming call and will report it to the IFMP.

It is worth noting that no enhancements are needed within the context of a private IFMP network. Figure 10 shows the control plane architecture for the interface between the gateway IFMP switch and a traditional IFMP switch. Only the traditional IFMP protocols are needed in the IFMP switch.

Let us consider some requirements coming from the proposed interworking architecture. In section 3, we analyzed the architecture of a classical IFMP network, where two adjacent IFMP switch are directly connected, typically in a private network context. In both direction an ATM virtual channel is available for the default IP traffic (and the IFMP protocol messages), while a set of VCs is available to redirect the IP flows. Therefore the VPI/VCI identifier space is common to the two IFMP switches at the edges of the direct ATM link. In the proposed architecture the IP flows will be redirected over dynamically setup connections on the Public Network. If there is no direct link between the two IFMP switches, the VPI/VCI identifier will not anymore identify at both sides an ATM VC Connection. The IFMP redirect messages cannot anymore refer to a real VPI/VCI identifier, but the notion of “IFMP Network Connection Identifier” must be introduced. How to define and transport this identifier using the IFMP protocol will be shown in the next sections.

Another issue to be solved is the correlation of Q.2931 calls and IP flows. The additional connections used to redirect the IP flows will make use of switched ATM VCs. The IFMP logic (by means of the IWU) should ask for a new connection that will be setup by signaling, this new connection must be correlated with the IP flow to be transferred by the two IFMP switches at the ends of the connection. Unfortunately, there is no way to easily identify a call/connection globally in the network. To allow this correlation, mechanisms will be investigated to convey some information along with the setup of the ATM call/connection.
InterWorking solutions: the IFMP Network Connection Identifier (INCI)

InterWorking control information between IFMP and the ITU-T Q.2931 protocol module is exchanged by means of local primitives through the IWU module.

In this section we are focused on the particular technique we used to extend IFMP logic to Q.2931 signaling protocol and to allow the control of the related redirected ATM VCCs, with reference to the basic scenario presented in section 3.

As soon as an IP datagram stream is viewed as an IP flow, an ATM VCC through B-ISDN should be set-up and the related IP flow should run onto it. As underlined before, a traditional IFMP switch can easily bind an IP flow identifier to an ATM VC where to redirect this flow by means of the VPI/VCI value contained in the label field of the REDIRECT message. When the downstream IFMP Gateway Switch recognizes an IP flow, it sends a REDIRECT message towards the upstream IFMP Gateway Switch. The upstream switch sends a SETUP message to request the establishment of an ATM VCC toward the downstream IFMP Gateway Switch. The downstream switch must be able to correlate the incoming SETUP message with the previous REDIRECT message. Unfortunately a standard information element able to uniquely identify an ATM VCC at both interfaces does not exist; we can only identify a VCC at each UNI interface by means of its VPI/VCI value. This means that it is impossible to use the label field as the case of traditional IFMP switching paradigm.

In other words, we have to bind an identified IP flow to its own ATM VCC or, at least, to the VPI/VCI values both at the originating and at the destination UNI interfaces. The proposed solution is to extend the meaning of the label field to that of a generic connection identifier, called IFMP Network Connection Identifier (INCI). Considering the Basic Scenario, the INCI consists of a local coding of the recognized IP flow identifier which is assigned by the downstream switch when sending the REDIRECT message. The key point is that the downstream node must receive back the INCI in the incoming SETUP message. We propose to use the Broadband High-Layer Information Element (B-HLI I.E.), to carry back the INCI identifier. The B-HLI can be optionally included in Q.2931 SETUP message and it must be transparently carried by network. In this information element the field High Layer Information type (1 octet long) specifies the type of information carried, while the High Layer Information field (up to 8 octets) can be filled by the calling user. Therefore the upstream gateway will set the High Layer Information Type field to user-specified and copy the received INCI value in the High Layer Information field. Figure 11 shows the steps for the establishment of ATM VCC to be used for flow redirection.

1. The downstream IFMP Switch Gateway identifies an IP flow, it choose an INCI for the flow and issues a REDIRECT message with INCI included in the label field.
2. The upstream IFMP Switch Gateway validates the redirection request and the IWU module issues a SETUP message, at the local UNI, with the INCI parameter encapsulated in the B-HLI information element.
3. The downstream IFMP Switch Gateway receives the SETUP message and extract the INCI parameter from the B-HLI. If the resources are available, it binds the INCI value to the local VPI/VCI_A values assigned by the network, and
4. it stores this information.
5. The downstream IFMP Switch Gateway issues a CONNECT message towards the upstream IFMP Switch Gateway.
6. The upstream IFMP Switch Gateway receives the CONNECT message, binds the INCI value to the local VPI/VCI_B values assigned by the network, and
7. it stores this information.

![Diagram](image-url)
6 Results from test implementation

In this section we will show the simulation of an IFMP Switch Gateway when sets up an ATM VCC at its local UNI after a redirection request for an IP flow was received. The simulation (see Figure 12) has been performed using the SDT 3.0 by Telelogic. The parameters of the messages are not shown. The whole set of procedures for the interworking (e.g. the release of the connections) has been simulated, but this is not shown in this paper for lack of space.

As it can be easily seen, the IWU acts as the functional core of the gateway. The IWU issues a local Setup-req primitive to the signaling application (Q.2931 User) including the INCI parameter after an Encapsul-req primitive has been received from the IFMP logic. Only when a Setup-conf will be received from the Q.2931, the IWU will issue an Encapsul-req primitive to the Encapsulation module (external to our system) and the recognized IP flow will run onto the established ATM VCC. In this way we are sure IP flow traffic will find an already established connection through the B-ISDN to the downstream IFMP Switch Gateway.

Figure 12 - Message Sequence Chart for the establishment of a redirection ATM VCC

7 References


