Internet-Draft

Yasuhiro Katsube
Ken-ichi Nagami
Yoshihiro Ohba
Shigeo Matsuzawa
Hiroshi Esaki
(Toshiba Corporation)

December 1997

Cell Switch Router
- Architecture and Protocol Overview -

<draft-katsube-csr-arch-00.txt>

Status of this memo

Abstract

This memorandum describes an internetworking architecture of Cell Switch Router (CSR) and related control protocol overview. Cell Switch Router is an ATM-based label switching router that can provide ATM cut-through paths for packet flows with various levels of granularity while retaining current router-based internetworking architecture. The proposed architecture is able to provide the cut-through path in response to the creation of IP forwarding entry (topology-driven), the arrival of data packets (traffic-driven), and the reception of control packets such as RSVP (request-driven). One important feature that is provided by the proposed architecture is interoperability with the emerging ATM network platform, specified by the ATM Forum and/or ITU-T, which provides PVC (Permanent Virtual Channel), VP (Virtual Path), or SVC (Switched Virtual Channel) services.

Table of Contents

1. Introduction

The Internet is growing in both size and traffic volume. In addition, emerging applications may require specific bandwidth and quality of services (QoSs) in addition to best effort. Such changes require conventional routers with more sophisticated processing capability, which tends to raise the cost of routers, and accelerate investigations of a new internetworking architecture that relies on powerful datalink switching capabilities.

The proposed internetworking architecture is composed of i)CSRs that have ATM label switching capability as well as conventional layer 3 packet forwarding, ii)edge nodes that are located at boundaries between the proposed network and legacy networks (e.g., ATM networks with legacy routers, non-ATM networks), and iii)end hosts that are capable of speaking with the CSRs.

Direct ATM level connectivities from ingress edge nodes (or hosts) to egress edge nodes (or hosts) are provided via intermediate CSRs on the path with the ATM label switching capability inside (we refer to this ATM level connectivity as an "ATM cut-through path"). The cut-through path is controlled by each of the CSRs on the path as

well as by ingress/egress edge routers or hosts, which keeps conventional hop-by-hop control discipline for managing dynamic layer 3 state for unicast and multicast routing, RSVP, and so on. The proposed internetworking architecture is designed so as to be able to operate over standard ATM networks which are compliant with ATM Forum and/or ITU-T that support PVC (Permanent Virtual Channel), VP (Virtual Path), or SVC (Switched Virtual Channel) services, as well as over point-to- point links.

2. Internetworking Architecture Based on Cell Switch Router

2.1 Architectural Overview

Cell Switch Router(CSR) is a key network element of the proposed internetworking architecture[13]. It is interconnected with ATM networks through ATM UNI interface[1] and provides cell switching functionality in addition to conventional IP packet forwarding. It is able to concatenate incoming and outgoing ATM VCs at the ATM layer, bypassing packet header processing. By carrying out such ATM VC concatenations at multiple CSRs consecutively, ATM level cut-through paths composed of multiple VCs, each of which connects neighboring CSRs (or CSR and hosts/edge routers), can be provided.

Two different kinds of VCs for transmitting packets are defined between neighboring CSRs or between CSR and hosts/edge routers.

1) Default-VC : a general-purpose VC used by any communications that select conventional hop-by-hop IP forwarding paths. All incoming cells received from this VC are assembled into IP packets and handled based on their IP headers.

2) Dedicated-VC : used by a specific packet flow, which is specified by, e.g., {dst.IP address, src.IP address} or {dst.IP address, src.IP address, protocol, dst.port, src.port}. It can be concatenated with other Dedicated-VC(s) that accommodate the same packet flow as itself, and can constitute an ATM cut-through path for those packet flows.

The route for a cut-through path follows IP routing information in each CSR. As shown in Figure 1, packets from an ingress edge router (or source host) X.1 to an egress edge router (or destination host) Z.1 are transferred over the route X.1 --> CSR1 --> CSR2 --> Z.1 regardless of whether the communication is on a hop-by-hop IP forwarding basis or cut-through path basis.

An example of the IP packet transmission mechanism is as follows.

- The ingress edge X.1 checks an identifier of each IP packet flow,

which may be the "destination IP address (or prefix)", "source/destination IP address (prefix) pair", "source/destination IP address and port" or "source IP address and group address". Based on such identifiers, it determines over which VC the packet should be transmitted.

- The CSR1 and CSR2 check the VPI/VCI value of each incoming cell. When the mapping from the incoming interface/VPI/VCI to outgoing interface/VPI/VCI (which may be plural in the case of multicast) is found in an ATM forwarding table, it is directly forwarded to the specified interface(s) with the new VPI/VCI value through an ATM switch module. When the mapping is not found in the ATM forwarding table (or the table shows an IP processing module as an output interface), the cell is transmitted to an IP processing module and assembled into an IP packet and then forwarded to an appropriate outgoing interface/VPI/VCI based on the header of the packet.

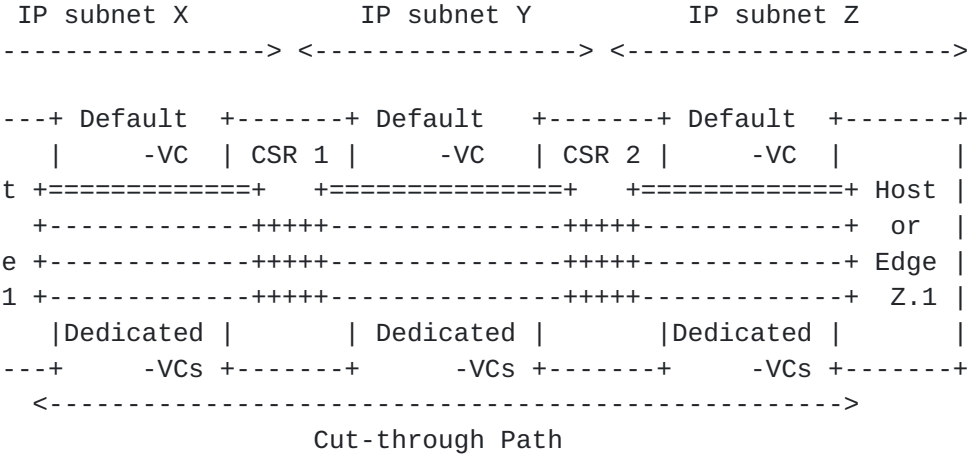

Figure 1 Internetworking Architecture based on CSR

A CSR becomes the termination point (egress edge) of a cut-through path when it is an edge of the ATM cloud regarding the end-to-end path, it is an edge of the CSR-capable router cloud regarding the end-to-end path, or it cannot create a Dedicated-VC toward the downstream neighbor for the end-to-end path for some reason. The CSR-capable router is required to understand a control protocol that exchanges mapping information between each dedicated-VC and a specific packet flow that will be transmitted over the VC.

Note that the egress edge of the cut-through path can also perform the cut-through forwarding which bypasses IP processing. Since the

egress edge router can memorize the association between each of the cut-through paths it terminates and the specific packet flow which is transmitted over the path by using the control protocol described in section 3, it can obtain the same information as by referring to the IP header, i.e., source IP address and destination IP address etc., by referring to the identifier of the incoming dedicated-VC (VPI/VCI). That means that the egress edge router can forward packets received from the dedicated-VC to a proper downstream neighbor without referring to their IP header even though the corresponding outgoing dedicated-VC does not exist.

In the rest of the document, all the CSR-capable devices including CSR, edge router, and end host will be referred to as "CSR" for simplicity unless there is a need to distinguish among them.

2.2 Triggers for Cut-Through Path Establishment

CSR is able to initiate cut-through path establishment in response to the creation of IP forwarding table entries (topology-driven), the arrival of data packets (traffic-driven), and the reception of control traffic such as RSVP resource reservation request (request-driven)[2].

This subsection describes three triggers for cut-through path establishment by CSRs, together with possible granularity of packet flows (conditions that specify the packet flow conveyed over the cut-through path) in each of the cases.

1) Topology-driven path establishment :

In topology-driven, the cut-through path establishment procedure is initiated when a new IP level forwarding table entry is created at a CSR. The cut-through path can naturally accommodate aggregated packet flow which is specified by, e.g., {ingress edge router, dest.prefix}, {ingress edge router, egress edge router}, {*, dest.prefix}, or {*, egress edge router}. The latter two may require ATM switches to provide flow merging capability while avoiding AAL5 frame interleaving.

Note that the topology-driven aggregated paths should not be extended beyond the points where the processing for individual end-end flows (e.g., packet filtering or QoS differentiation) should be carried out but be terminated at those points.

2) Traffic-driven path establishment :

In traffic-driven, the path setup procedure is initiated when the CSR determines that it is worth providing the path for a specific packet flow, e.g.,

* transmission of a packet with specific upper layer protocols defined by the port ID of TCP/UDP
* transmission of TCP SYN packet
* transmission of a packet with specific source/destination IP addresses
* transmission of more than a certain amount of packets in a predetermined period

Granularity of the packet flow for the traffic-driven path could be {src.IP_addr, dest.IP_addr} as a default, although aggregated cut-through paths specified by, e.g., {ingress edge router, dest.prefix}, can also be established with traffic-driven.

3) Request-driven path establishment :

In request-driven, the path setup procedure is initiated when the CSR receives some control messages (requests) which are not specific to CSR network but affect the cut-through operation of the CSR. An example of such a control message is RSVP Reservation (Resv) request

[3] which requests the CSR to provide specific quality of services with regard to the packet forwarding. The CSR which has received a Resv message prepares a dedicated-VC for the requested RSVP flow.

Granularity of the packet flow for the request(RSVP)-driven path could be {src.IP_addr/port, dest.IP_addr/port} as a default although {src.IP_addr, dest.IP_addr} may be allowable in some cases. Reservation styles shared by multiple senders (Wild Card style and Shared Explicit style) should be supported by the cut-through paths dedicated to individual senders like a Fixed Filter style for simplicity.

2.3 Interoperation with Standard ATM Network Platform

Interconnecting multiple CSRs through point-to-point (p-p) links such as SONET link is a straightforward configuration that is easy to implement. In addition, CSRs are designed to be interconnected with each other over the emerging ATM network platform that is compliant with the ATM Forum or ITU-T standard UNI. That enables the ATM network platform to be utilized for Internet/Intranet services as well as other services such as telephony and native ATM services. In addition, Internet/Intranet services based on CSRs can coexist with and operate over classical IP over ATM[4] networks, which provide intra-subnet communications.

CSR operations over three types of ATM networks should be taken into account;

1) VP-based ATM network : provides a VP as a tunnel between neighboring CSRs and picks up an unused VCI in the VP each time a dedicated-VC is needed.

2) PVC-based ATM network : provides a number of PVCs between neighboring CSRs at an initialization phase and picks up one of them each time a dedicated-VC is needed.

3) SVC-based ATM network : provides an SVC between neighboring CSRs through ATM signaling each time a dedicated-VC is needed.

In the case 3), it is possible that a number of SVCs are set up in advance through ATM signaling and are registered as a stock, which we call "VC pool" approach[5]. Then one of them can be picked up each time a dedicated-VC is needed, which is a similar approach to

the PVC case. Although the necessary VC resources with the VC pool approach will be larger than the on-demand SVC setup, the VC pool approach can decrease latency for setting up the cut-through path as there is no delay for ATM signaling. In addition, the VC pool approach can reduce the processing burden for setting up or releasing SVCs when the number of surplus VCs between neighboring CSRs is controlled between a predetermined lower bound and an upper bound. That is, an additional SVC is set up only when the number of surplus SVCs becomes smaller than a predetermined lower bound, whereas one of the surplus SVCs is released only when it becomes larger than a predetermined upper bound. Whether the "on-demand setup approach" or "VC pool approach" should be applied is a matter of local decision in each network, taking cost and the system responsiveness into account.

ATM networks can be utilized either as logical point-to-point links in which IP addresses are assigned to a CSR for each neighbor CSR, or as a multi-access (NBMA) link in which a single IP address is assigned to a CSR for each logical IP subnet (LIS) composed of several neighbor CSRs. When CSRs are operated over multi-access ATM LIS environment, point-to-point (p-p) dedicated-VCs or point-to-multipoint (p-mp) dedicated-VCs toward its next-hop(s) are utilized by each CSR to provide intra-subnet connectivity. ATMARP server[4] or MARS [6] will be used when the CSR does not know an ATM address(es) of its neighbor CSR(s) or edge node(s). Note that this does not exclude the use of other methods for unicast/multicast ATM address resolution.

3. Cell Switch Router Control Mechanism

This section presents an overview of "FANP (Flow Attribute Notification Protocol)", that is a protocol between neighboring nodes (CSRs, edge routers, and end hosts) in order to establish, maintain, and tear down the cut-through paths.

There are several changes in an updated version of FANP (FANP version 2) from FANP v1[7]. They are i)provision of a neighbor discovery protocol[8] that enables CSRs to recognize their neighbors, ii)adoption of two modes of cut-through path control mechanism; Distributed Control mode (DC-mode)[9] and Ingress Control mode (IC-mode)[10], and iii)support of interoperability with variety of ATM network platforms. Each of them will be explained in this

section.

3.1 Neighbor Discovery

The neighbor discovery (ND) is used for recognizing neighbors that understand FANPv2, obtaining FANPv2 protocol attributes of the neighbors, and checking whether consistent states are maintained by the neighboring CSRs. A FANP-capable node recognizes that FANP is running on a neighbor node provided it periodically receives ND messages from the neighbor.

The ND procedure takes different actions depending on whether the underlying network interface is point-to-point or multi-access. Detailed procedure for each type of interface is described in [8].

3.2 Two Modes of Protocol Operation

CSR supports two modes of control operation; Distributed Control mode (DC-mode)[9] and Ingress Control mode (IC-mode)[10]. An overview and examples of application of each operation mode are described below. Which mode of operation each control message belongs to is distinguished by a bit in the common header of the FANP message.

3.2.1 Distributed Control Mode (DC-mode)

3.2.1.1 Operational overview

In the DC-mode, the cut-through path establishment procedure for a packet flow is initiated at individual CSRs on its path in a distributed manner. Each of them transmits control messages to its downstream neighbor in order to notify the mapping relationship between the packet flow and the outgoing dedicated-VC that will

convey the flow. The downstream CSR that has received the control message from its upstream neighbor checks the validity of the message, memorizes the received mapping information at its incoming interface, and transmits an acknowledgment to the upstream neighbor.

This message exchange with an upstream neighbor at the CSR does not initiate the exchange of any control messages with its downstream neighbor in the DC-mode. A control message exchange for a flow between a pair of neighboring CSRs is initiated and carried out

independently from the message exchange for the same flow between any other pair of CSRs. As a result of control message exchanges performed at individual pair of CSRs, a CSR realizes that both the incoming and the outgoing dedicated-VC are associated with the same packet flow, and then begins cut-through forwarding.

The release of the cut-through path is also initiated at individual CSRs on the path. A CSR that has detected the trigger to release the cut-through path transmits control messages to its downstream neighbor to cancel the association between the packet flow and the outgoing dedicated-VC that conveys the flow. The reception of the control message at a CSR from the upstream neighbor does not initiate the transmission of the control message to the downstream neighbor.

As no information regarding the cut-through path with edge-to-edge importance can be obtained in the DC-mode, an ingress edge knows neither the number of hops for the path nor the constitution of the loop in the path. It is easy to change the configuration of cut-through paths according to dynamic changes in the router state, e.g., unicast routing, multicast group membership/routing, and RSVP reservation state.

The common rule with regard to the trigger selection for the cut-through path establishment (the condition to initiate the cut-through establishment) and release, and the granularity level of the packet flow should be configured to individual CSRs in a domain, since no such information is conveyed hop-by-hop by the control messages in the DC-mode.

3.2.1.2 Examples of DC-mode Operation

The DC-mode operation can be adopted for establishing the traffic-driven unicast cut-through paths. Individual CSRs on the path can recognize the flow of the layer 3 level end-to-end granularity by referring to the data packets (e.g., {src.IP_addr., dest.IP_addr}). They can also commonly recognize the aggregated flow of {src.IP_addr., dest.prefix} granularity individually as long as they have the IP forwarding table entry with the same CIDR prefix

given by the routing protocol.

Control of multicast cut-through paths is suitable for the DC-mode operation as the management of group membership, which may change

frequently, is carried out by individual CSRs on the distribution tree. Each CSR is able to add a new leaf to or delete a leaf from the active cut-through path in response to detection of join or leave of a group member at corresponding interfaces. The granularity of {src.IP_addr., multicast group addr.} is straightforward although the shared tree defined by, e.g., {Rendezveus Point, multicast group addr.} is also possible. Concrete triggers for cut-through establishment or release may depend on the routing protocol deployed and implementation. Arrival of the data traffic, creation of the multicast forwarding cache, or reception of PIM Join messages can be the trigger.

Control of cut-through paths in response to the RSVP reservation state (request-driven) at individual CSRs on the path will also be appropriate for the DC-mode operation. Reception of the reservation (Resv) messages at a CSR from its downstream neighbor initiates the control message exchange, which notifies the mapping relationship between the flow corresponding to the RSVP session and the dedicated-VC that will convey the flow, with the downstream neighbor. Then the CSR transmits the Resv message further upstream. Here we assume the use of current standard RSVP message format[3] with no additional object defined for this purpose.

3.2.2 Ingress Control Mode (IC-mode)

3.2.2.1 Operational overview

In the IC-mode, the cut-through path establishment procedure for a packet flow is initiated by a CSR that is hoping to become an ingress edge of the cut-through path. The ingress edge transmits control messages to its downstream neighbor in order to notify the mapping relationship between the packet flow and the Dedicated-VC that will convey the flow. The message is composed of i)information that identifies the flow, ii)information that identifies the dedicated-VC, iii)ingress information that is uniquely created by the ingress node for the cut-through path, and iv)a hop count that is set to one by the ingress edge. The last two information elements are specific to the IC-mode operation, which provides a capability to prevent the creation of a potential loop of the cut-through path.

The CSR that has received the messages for the notification of the mapping relationship from the upstream neighbor checks the validity of the message, and memorizes the received mapping information at its incoming interface. Then the CSR reconstructs and transmits

control messages further downstream along the path of the flow to notify the mapping relationship between the flow notified by the upstream neighbor and a dedicated-VC that will convey the flow.

The same procedure is performed at every CSR along the path of the flow until the notification message reaches the CSR that cannot extend the cut-through path any more (e.g., an egress edge of the CSR cloud). The CSR that becomes the egress endpoint of the cut-through path returns the acknowledgment message to its upstream neighbor, which is forwarded hop-by-hop toward the ingress edge (the ingress point of the cut-through path).

This ingress to egress and egress to ingress message forwarding facilitates association of related information about the cut-through path. As mentioned above, the control message that notifies the mapping relationship contains "a hop count from the ingress edge" and "an ingress information that is determined by the ingress edge for the cut-through path it originates". The hop count value is initially set to one by the ingress edge and is incremented by one at each of the CSRs along the cut-through path. When a CSR recognizes that the hop-count value in the notification message reaches a predetermined threshold, it determines that there is a potential loop in the cut-through path. The CSR also determines that there is a potential loop when it has received a notification message that contains the packet flow identifier and ingress information, both of which are the same as those already registered, but contains the dedicated-VC identifier that is not the same as has been registered. The CSR that detects the potential loop stops creation of the cut-through path toward its downstream, and returns an error message to the upstream neighbor.

The ingress edge is able to know the number of hops from itself to the egress endpoint of the cut-through path by referring to the acknowledgement messages initiated by the egress node. The hop-count in the acknowledgement message transmitted by the egress node is set to one and incremented by one at each of the CSRs along the reverse path of the cut-through. The ingress edge may decrement the TTL value of the received packet by the number of hops it learned, or may decrement that by one.

In the IC-mode, the CSR that has failed to extend the cut-through path toward its downstream for specific reasons retries path establishment after some specified intervals. When the CSR has succeeded in extending the cut-through path by the retry procedure, the number of hops from the CSR to the egress edge may change, which means that the number of hops from the ingress edge to the egress edge may also change. The CSR that has succeeded in extending the cut-through path transmits a message that notifies an updated

hop-count from the egress edge toward the ingress edge.

3.2.2.2 Examples of IC-mode Operation

The IC-mode operation can be adopted for establishing the unicast cut-through paths with aggregated packet flows as well as flows with fine granularity level. Examples of the flow granularity are {ingress edge's IP_addr., dest.prefix} and {ingress edge's IP_addr., egress edge's IP_addr.}. The trigger to establish the cut-through path may be either topology-driven or traffic-driven. Irrespective of the flow granularity and cut-through establishment trigger, the notification message is processed at each CSR along the path and transmitted hop-by-hop until it arrives at an egress edge.

3.3 Operations Dependent on the Type of Underlying ATM Networks

As described in 2.3, CSRs should be interconnected over the following four types of datalink:

(a) Point-to-point link that interconnects neighboring CSRs directly
(b) VP-based ATM network that provides logical point-to-point link
(c) PVC-based ATM network
(d) SVC-based ATM network

The core procedure of the FANPv2 control mechanism performed by the neighboring CSRs is a notification of the association between a packet flow and a dedicated-VC that will convey the packet flow, and an acknowledgment to the notification, which we call "flow notification procedure". The use of the VPI/VCI value as an identifier of a dedicated-VC in the flow notification procedure would suffice in the case (a) and (b). It, however, does not work when CSRs are interconnected over an ATM network that provides PVC or SVC services. Since VPI/VCI values at the origination point (outgoing interface of the upstream CSR) and the termination point (incoming interface of the downstream CSR) of a VC are not the same when there are standard ATM switches in between, the VPI/VCI value cannot be used as an identifier of a dedicated-VC in the flow notification procedure.

A "VCID (Virtual Connection IDentifier)"[11] is introduced instead, which can be uniquely identified by the neighboring CSRs to indicate a dedicated-VC in the flow notification procedure. In the case of (c)PVC-based ATM network and (d)SVC-based ATM network, a procedure to assign the VCID to each dedicated-VC, which we call "VCID notification procedure", should be performed before the flow notification procedure. Note that in the case of (a)the p-p link and (b)the VP-based ATM network, no explicit VCID notification procedure is needed since the VPI/VCI (or just the VCI) value in the cell header can be used as the VCID in those cases.

The concrete procedure for the VCID notification differs depending on the type of the underlying ATM network: PVC-based ATM or SVC-based ATM[12].

3.3.1 PVC-based ATM network

An upstream CSR transmits a message that includes a VCID value over the PVC itself (in-band notification). The VCID value is determined by the upstream CSR and should be unique to the pair of CSRs. When the downstream CSR transmits the acknowledgment of the above in-band message to the upstream CSR, the upstream and downstream CSRs can share the same identifier VCID for the PVC. This in-band VCID notification procedure can be carried out either immediately after the PVC setup or at the time when one of PVCs is picked up for a specific cut-through path in response to cut-through establishment trigger.

3.3.2 SVC-based ATM network

There are two ways for the VCID notification in the case of the SVC-based ATM network. One is the in-band notification described above; an upstream CSR conveys the VCID value over the SVC that is being utilized as a dedicated-VC. This would be adopted when the other way described below is not applicable.

An alternative way for the VCID notification is the use of an Information Element (IE) with end-to-end significance in a SETUP message of ATM signaling. When an upstream CSR transmits an ATM SVC SETUP message toward its downstream neighbor, it determines a unique ID value as the VCID and includes it in the IE that is transparently conveyed by the ATM switches in between. After that, the upstream CSR is able to perform the flow notification procedure by using the above VCID as an identifier of the dedicated-VC. A "user specified layer 3 protocol information field" of the BLLI (Broadband Low Layer Information) IE is the most appropriate field for this purpose. An issue in this method is that the user specified layer 3 protocol information field of the BLLI IE is given just 7 bits, which can identify only 128 VCs simultaneously between neighboring CSRs.

In order to resolve the limitation of the 7-bit BLLI IE, an additional message exchange that notifies the mapping between the 7-bit number conveyed in the BLLI IE (a temporal VCID) and an actual VCID, which is determined uniquely by the upstream CSR and is given enough bit space, is carried out at the VCID notification phase. Namely, after the upstream CSR has set up an SVC with the 7-bit temporal ID value, it transmits a control message that replaces the temporal ID with the VCID. At this stage, the temporal ID value is

released and could be reused by the other SVC. The flow notification

procedure will be performed by exchanging the message that conveys the association between the VCID and a specific packet flow. The procedure is:

1) SVC SETUP with temporal ID in the BLLI IE
2) VCID notification : message exchange that replaces "temporal ID" with "VCID" (temporal ID is released for the other SVCs)
3) Flow notification : message exchange that notifies association between the "VCID" and a specific "packet flow"

In the case that the "VC pool" approach described in 2.3 is applied, the above steps 1) and 2) are carried out when preparing a dedicated-VC for future use, and the step 3) is carried out when establishing a cut-through path. In the case that the "on-demand setup" approach described in 2.3 is applied, it is possible to perform the above two steps 2) and 3) by a single message exchange. By making the flow notification message convey the "temporal ID", "VCID", and "packet flow", the VCID notification step can be merged into the flow notification step. The procedure comes to:

1) SVC SETUP with temporal ID in the BLLI IE
2) Flow notification : message exchange that notifies association between the "temporal ID", "VCID" and a specific "packet flow" (temporal ID is released for the other SVCs)

The detailed procedure for the cut-through establishment and release in individual cases is described in [9].

4. Security Considerations

Security issues are not discussed in this document.

5. Intellectual Property Considerations

Toshiba Corporation may seek patent or other intellectual property protection for some or all of the aspects of the technology discussed in this document. If any standards arising from this document are or become protected by one or more patents assigned to Toshiba Corporation, Toshiba intends to license them on reasonable and non- discriminatory terms.

6. References

[1] The ATM Forum, "ATM User-Network Interface Specification, v3.1",

Sept. 1994.
[2] R. Callon, et al., "A Framework of Multiprotocol Label Switching", IETF Internet-Draft (work in progress), draft-ietf-mpls-framework-01.txt, July 1997.
[3] R. Braden, et al., "Resource ReSerVation Protocol (RSVP), Version 1 Functional Specification", IETF RFC2205, Sept. 1997.
[4] M. Laubach, "Classical IP and ARP over ATM", IETF RFC1577, Oct. 1993.
[5] N. Demizu, et al., "VC Pool", IETF Internet-Draft (work in progress), draft-demizu-mpls-vcpool-00.txt, Oct. 1997.
[6] G. Armitage, "Support for Multicast over UNI 3.0/3.1 based ATM Networks", IETF RFC2022, Nov. 1996
[7] K. Nagami, et al., "Toshiba's Flow Attribute Notification Protocol (FANP) Specification", IETF RFC2129, April 1997.
[8] K. Nagami, et al., "Flow Attribute Notification Protocol Version 2 (FANPv2) Neighbor Discovery", IETF Internet-Draft (work in progress), draft-nagami-fanpv2-nd-00.txt, Dec. 1997
[9] K. Nagami, et al., "Flow Attribute Notification Protocol Version 2 (FANPv2) Distributed Control Mode", IETF Internet-Draft (work in progress), draft-nagami-csr-fanpv2-dcmode-00.txt, Dec. 1997.
[10] Y. Ohba, et al., "Flow Attribute Notification Protocol Version 2 (FANPv2) Ingress Control Mode", IETF Internet-Draft (work in progress), draft-ohba-csr-fanpv2-icmode-00.txt, Dec. 1997.
[11] N. Demizu, et al., "VC-ID: Virtual Connection Identifier", IETF Internet-Draft (work in progress), draft-demizu-mpls-vcid-01.txt, Oct. 1997.
[12] N. Demizu, et al., "ATM SVC Support for ATM-LSRs", IETF Internet-Draft (work in progress), draft-demizu-mpls-atm-svc-00.txt, Oct. 1997.
[13] Y. Katsube, et al., "Toshiba's Router Architecture Extensions for ATM : Overview", IETF RFC2098, Feb. 1997.

7. Authors' Addresses

Yasuhiro Katsube
Research and Development Center, Toshiba Corporation
1, Komukai Toshiba-cho, Saiwai-ku, Kawasaki 210
Japan
Phone : +81-44-549-2238
E-mail : katsube@isl.rdc.toshiba.co.jp

Ken-ichi Nagami
Research and Development Center, Toshiba Corporation
1, Komukai Toshiba-cho, Saiwai-ku, Kawasaki 210
Japan
Phone : +81-44-549-2238

E-mail : nagami@isl.rdc.toshiba.co.jp

Yoshihiro Ohba
Research and Development Center, Toshiba Corporation
1, Komukai Toshiba-cho, Saiwai-ku, Kawasaki 210
Japan
Phone : +81-44-549-2238
E-mail : ohba@csl.rdc.toshiba.co.jp

Shigeo Matsuzawa
Research and Development Center, Toshiba Corporation
1, Komukai Toshiba-cho, Saiwai-ku, Kawasaki 210
Japan
Phone : +81-44-549-2238
E-mail : shigeom@isl.rdc.toshiba.co.jp

Hiroshi Esaki
Computer and Network Division, Toshiba Corporation
1-1-1 Shibaura, Minato-ku, 105-01,
Japan
Phone : +81-3-3457-2563
E-mail: hiroshi@isl.rdc.toshiba.co.jp