High Availability of ISDN Access in IP network

RADO SLATINEK
Faculty of Electrical Engineering and Computer Science
University of Maribor
Smetanova 17, 2000-Maribor
SLOVENIA

Abstract: - This paper describes the solutions needed when high availability of ISDN access established over IP network is required. SIGTRAN protocols standardized by The Internet Engineering Task Force (IETF) enable successful, reliable and timely delivery of information. These protocols are used for carrying sensitive signalling information about telecommunication and supplementary services requested by users. Although the protocols are very important, the overall availability of access is questionable without redundancy of systems involved in protocols and call handling. In this paper we describe our solution where the protocol functions and system duplications are used to offer reliable services evolved from ISDN.

Key-Words: - IP network, signalling gateway, call server, IUA, SCTP, ISDN, DSS1 access

1 Introduction

IP network has become an universal transport medium for different types of services including voice communication. In the past few years IP telephony has been mostly used for IP telephone interconnections, and lately for Signalling System No.7 (SS7) messages transport between VoIP (Voice over IP) gateways and call servers. Integrated services digital network (ISDN) operators nowadays try to reduce communication costs using IP network as a transport medium. IP network can be used as a core and as an access network. IP core network interconnects the existing ISDN exchanges and new call servers via signalling gateways (SG). This part has no effect on end users if Quality of Services (QoS) is fulfilled. Gradually also ISDN local exchanges will have to be replaced due to amortization or failures. This will change the architecture of ISDN access and will have effect on the end user. The main problem will appear when subscribers, specially the older ones, will not be ready to replace their ISDN telephones with new IP telephones. This problem can be solved by:

1. replacing the network termination type 1 (NT1) next to the ISDN terminal with an integrated access device (IAD) enabling access gateway functionality, or by
2. using large access gateways instead of local ISDN exchanges.

The first solution is expensive and requires the extension of IP accesses to the end users. It is more demanding for the operator because IP addresses of all subscribers have to be maintained in the management node.

The second solution is based on the usage of the existing time division multiplexed (TDM) lines. ISDN terminals are connected to access gateways (AG). The AG provides the protocol conversion needed to interconnect TDM lines with IP network. It is a better choice for the operators to replace local exchanges with AG because user administration and maintenance is more simple and call control is concentrated in a few call servers (CS).

The introduction of IP technology to ISDN access requires reliable, secure and timely delivery of information, specially for services control. Therefore, appropriate protocols were developed by the IETF for ISDN telephony over IP. ISDN access established over IP network between AG and CS requires ISDN User Adaptation (IUA) layer protocol [1], Stream Control Transmission Protocol (SCTP) [2] and IP protocol.

In the first part of the paper we will discuss the IP network structure for ISDN telephony and protocol stack architecture of user accesses. The key features of IUA and SCTP protocols associated with the availability of ISDN access will be presented. We will explain our solution to fail-over when the call server or signalling gateway are out of service and calls are switched over to the redundant system.

2 ISDN access in IP Network

The existing functions of IUA and SCTP protocols solve most problems with reliable, secure and timely delivery of signalling information. While some other applications are based upon UDP-IP protocol stack, IUA uses Stream Control Transport Protocol (SCTP) services for messages transport between

gateways and call servers which are also called Media Gateway Controllers (MGC).

Users expect that services provided by network operator will be available at any time. Strict reliability requirements of SS7 signalling issued by International Telecommunications Union - Telecommunication Standardization Sector (ITU-T) must be fulfilled by signalling gateways when connecting two SS7 signalling points. While gateways can carry both SS7 and DSS1 signalling, the same requirements are fulfilled also for the availability of the ISDN access.

2.1 Network structure for ISDN access

2.1.1 ISDN network

ISDN Switched Circuit Network (SCN) for voice communication consists of user equipment like ISDN telephones and Private ISDN Exchanges (PINX), access network elements (AN), ISDN exchanges and interconnecting links.

Local and transit ISDN exchanges have the main role in the network where call handling and circuit switching functions offer telecommunication services to the end users. At ISDN terminal equipment the Primary Rate Accesses (PRA) or Basic Rate Access (BRA) to ISDN exchanges are established. Example of ISDN structure is shown in Fig. 1.

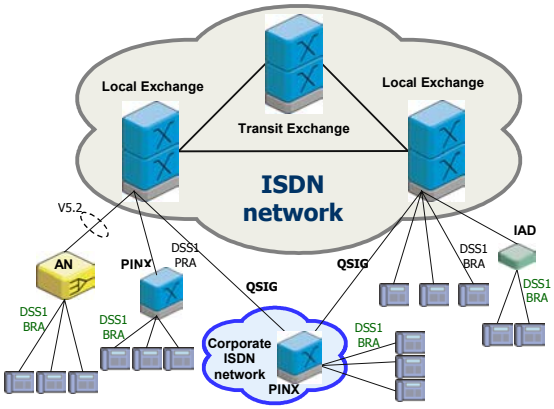

Fig. 1: ISDN network

2.1.2 IP network

If the network operator offers telecommunication services to ISDN users over the IP network, the gateways and call servers should be used. The signalling gateway (SG) works by intercepting the users' Digital Subscriber Signalling No.1 (DSS1) messages and transports them to call servers over the IP network. In order to allow high availability of ISDN accesses, SG is connected to two different segments of the IP network and communicates with two or more call servers. This ensures that there is no single point of failure provisioned in the network architecture between SG and CS [1]. The Private Integrated Network Exchanges (PINX) able to use DSS1 or QSIG signalling can also be connected to SG.

The PCM coded voice stream in the bearer channel, generated by the ISDN telephone, is transformed into packets by media gateway (MG). MG sends voice packets directly to the MG where the other user involved in a call is connected. Both, signalling and media gateway reside in one equipment called access gateway.

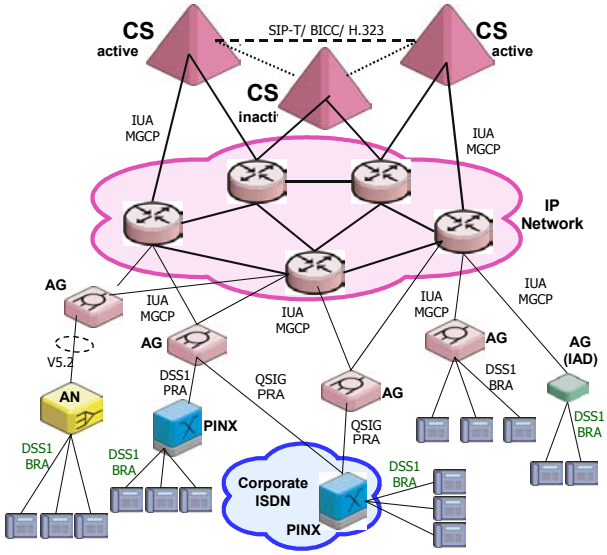

Fig. 2: DSS1oIP network structure

SG routes the users signalling traffic to the active call servers. The call server handles only calls, while switching function is performed by the IP network. Fig. 2 shows exactly the same structure of ISDN users as Fig. 1, only the ISDN network is replaced with access gateways, IP network and call servers.

2.2 ISDN access over IP architecture

Access is represented as a protocol stack on the path between terminal equipment and call server. Originally, ISDN access is defined as a 3 layered stack including physical (ITU-T I.430 for BRA and I.431 for PRA), data link (ITU-T Q.921) [3] and network layer (ITU-T Q.931). ISDN access over IP includes layer 3 protocol used for establishing of ISDN calls as indicated above, including all protocols for backhauling the ISDN user messages

over IP. Fig. 3 shows protocol entities at user port in SG and at IP connection in SG and CS. The physical and the data link layer of ISDN access are terminated in the signalling gateway, while the network layer spans over IP to the call server.

Because the data link layer and the network layer of ISDN access reside in different systems (SG and CS), the IP protocol stack in the network layer is used to overcome the existing gap. Therefore, the IP protocol is not enough to carry DSS1 information over the unreliable data network. To achieve the requested reliability objectives, two protocols in adjacent layers are used. SCTP in the transport layer and IUA in the adaptation layer offer the needed functions and features for ISDN access availability when faults occur in the network or in CS.

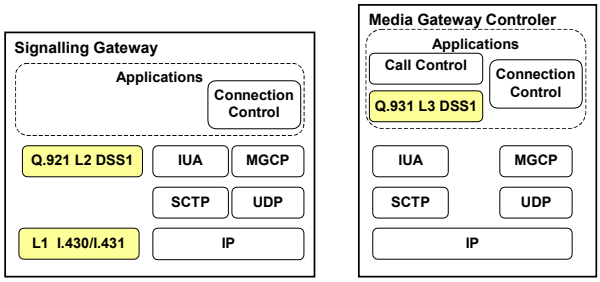

Fig. 3: DSS1oIP architecture

IUA/SCTP alone is not the only indispensable element of ISDN telephony over IP. There are also MGCP/UDP protocols for controlling the bearer channels between end users and RTP/RTCP protocols for voice packets transport over IP network as shown in Fig. 4.

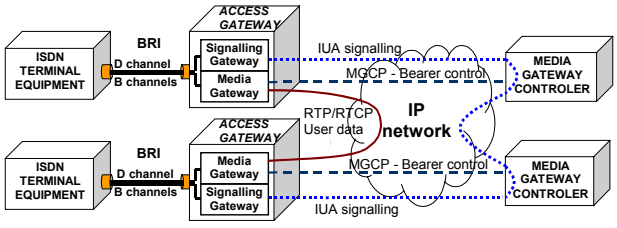

Fig. 4: DSS1 call/connection over IP

The same principle is used for SS7 signalling transfer when ISDN exchanges are connected with the call servers, where instead of IUA, the MTP layer 3 user adaptation (M3UA) or similar adaptation layer protocol is used.

3 ISDN access availability features

ISDN access availability identifies protocol features, systems redundancy and software design solutions as the key points to achieve the requested reliability. The first two key points are interdependent and have an important influence on software design. SCTP and IUA protocols offer different features to avoid unavailability of ISDN access. Features like multihoming or fail-over require path or endpoint redundancy.

3.1 SCTP features for ISDN access

SCTP is a transport layer protocol defined by IETF [2]. The main features of the SCTP to achieve the requested reliability are based on network redundancy (multihoming) and traffic segregation [4].

Traffic control: Different SCTP protocol parameters and timers enable checking the activity of the opposite side of association. If the opposite side is not active, the access is unavailable unless a redundant SG or CS is used.

SCTP association availability is measured by sending Heartbeat signal and waiting for response to verify the delays of SCTP association.

Multistreaming is used like unidirectional independent channels. Each channel is represented as a stream of application messages. Application (e.g. Layer Management or user adaptation layer) has assigned a stream for communication to avoid head-of-line blocking. If one of the packets in an unidirectional packet flow over IP is unconfirmed, then the transmission is stopped until the occurred problem is eliminated. SCTP solved such problems with traffic segregation. Faulty or lost signalling messages have only effect on the D-channel traffic associated with stream, while messages in other streams can still be passed without any delay. The network operator can use concentration to avoid IP connection overloading. Concentration means that the number of signalling channels is greater than the number of streams. When all streams are assigned, the next activated signalling channel cannot be connected to any stream.

In systems with lack of memory one stream could be used by more than one signalling channel (D-channel). We exploit this possibility because the receiving side uses a port identifier (or interface identifier IID) for application messages extraction rather than a stream identifier. Active streams are occupied mainly at the beginning and at the end of a call. During the call, the stream is used sporadically by supplementary services (i.e. billing, conference call). To exploit the stream more efficiently, a group of D-channels (e.g. like up to 30 users on PRA) can use only one stream. We used this solution only for BRAs, but concatenation of D-channel traffic has an

unwanted effect, where the problem on one D-channel affects all signalling channels assigned to the same stream.

Multihoming is a SCTP function used to improve the fault tolerance of the transport network. In this case SCTP association between two endpoints has more than one path. Multihoming is based on network redundancy where CS or SG have multiple network interfaces, each with its own IP address. One path is primary and used for communication. Other paths maintain the status of opposite side accessibility. Only when primary path becomes unreachable, one of the secondary paths is used by SCTP association for further message transfer.

3.2 IUA reliability functions

IUA protocol functions maintain operation of ISDN accesses if IP network congestions/faults or call server faults inhibit the calls operation. Such problems could be overcome by IUA layer functions for management of SCTP streams and paths as described in previous section and signalling traffic routing or rerouting.

IUA protocol has two standardized functions to enable ISDN access availability [1]. The first one is fail-over and the second one is traffic handling.

Fail-over function enables keeping alive ISDN accesses when all SCTP association paths between IUA peers in SG and CS become out of order, overloaded or the operational call server becomes unreachable.

For users, who need high reliability of services, the SG should be connected to more than one call server to achieve access availability by rerouting them. ISDN ports at SG are registered in all call servers where user signalling could be controlled.

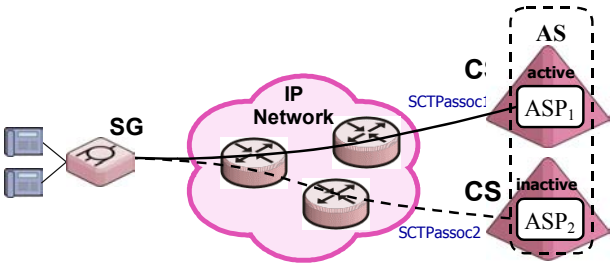

Fig. 5: SCTP associations established between SG and two ASPs

Each call server performs instances of Application Server (AS). Application server is a logical entity serving a specific application instance [1]. AS instance is represented as an Application Server Processes (ASP) handling the ISDN calls including DSS1 layer 3 messages. While the ISDN port is registered in more than one ASP, the access on that port could be established to different call servers or ASPs as shown in Fig. 5.

Access on active ISDN port is always controlled by a single ASP. Only at port reactivation or during active ASP failure, the other ASP can take over the controlling of that access. The first SCTP association (SCTPassoc1) is terminated at active ASP1 and carries signalling messages, while the second association terminates at inactive ASP2 and does not carry any signalling traffic at all.

During the ISDN port activation the D-channel signalling messages are routed to one of the SCTP association streams. As shown in Fig. 5, SG routes messages in IUA packets via SCTP association to the active ASP1. If connectivity to the ASP1 is lost, the ASP2 is activated and all traffic from D-channels at active user ports registered at ASP2 is switched over (rerouted) to ASP2.

Traffic management is the second, but not so important feature to obtain high availability of ISDN access. One of the two traffic management modes is provisioned to AS, and is used by SG to routes the signalling messages to particular ASP. SG will use the load-sharing method to distribute the D-channels traffic among two or more active ASPs where user ports are registered. Load-sharing enables that the loads are evenly distributed among SCTP associations and active ASPs. Every active ASP handles only a portion of the SG traffic. Another traffic management mode is over-ride and is used by ASP, which exclusively controls the users ports in SG.

3.3 Server and gateway redundancy

ASP distribution over at least two call servers is discussed in the previous section (Fig. 5). IUA and SCTP protocols solved only the problems on SG-ASP connection if ASP fails. How to keep alive the active calls if ASP or SG have failed, is not covered by IETF standards. As SG is part of the access gateway and also carrying signalling messages, the same requirements as for the CS are considered if a great number of user accesses are served by a particular SG.

3.3.1 ASP distribution

Our basic model includes one duplicated SG and two stand alone call servers. Each ASP resides in a different call server (e. g. Fig. 5) and has its own IP

address. All user ports at SG (ISDN users) are registered in both ASPs. The active ASP1 operates normally and transfers all necessary information about the established call and the connection to the standby ASP2, which is inactive. Information received by ASP2 enables to retain all active calls/connections after the activation of ASP2, if active ASP1 has failed. This implies that processes in ASP1, which handle call/connection entities, have the specially positioned probes to generate signals, when associated entity states change. The common application process on active CS collects these signals and passes them to the peer application process in ASP2. The peer application process in the standby side supervises the status of the active call server and routes the received signals to appropriate processes.

Entities involved in ISDN call/connection handling and their states for active call are shown in Table 1. Some entitles in the standby ASP2 can operate autonomously, while others are conducted by the active side and are masked as DS (Duplicated State). Our standby ASP2 resides in the stand alone call server and has established its own SCTP association with SG. It reacts according to the state changes of ASP1. If the administrator deactivates ASP1, the event is reported to ASP2, where the call server takes over signalling and call processing after activation of ASP2. The states of entities in standby side controlled by active side are only the duplicated figure of the active side. Entities marked with DS are not active and do not generate any traffic between SG and ASP1. Other entities are operational and communicate with peer entities over the IP network.

Table 1: Entitys in call servers

	Active ASP	**Standby ASP**
Entity	**state**	**state**
SCTP instance	Registered	Registered
SCTP association	Established	Established
AS	Active	Active
ASP	Active	Inactive
DSS1 call	Active	DS
Call Control	Active	DS
Bearer Connection	Channel connected	DS

Probes are implemented only in processes unable to operate independently in a standby ASP. So each process in an active ASP can send signals to its peer in standby ASP including entity states information and parameters when associated entity state changes. As an example of communication between active and standby ASP, the DSS1 call handling process in layer 3 is used. The active ASP handles the received Q.921 signals from the data link connection (DL) process in SG. Whenever a signalling call enters the active state or leaves it, a probe in the process generates a signal with the following information:

- Transaction Identifier,
- Application Server Identifier,
- Application Server Process Identifier,
- Remote user port (or D-channel) Identifier,
- Data Link Connection Identifier,
- Call Identifier (Call Reference),
- Call state,
- Process identifier.

The peer process in ASP2 receives this signal and changes its state according to the state parameter value. Other parameters enable routing of the received signal to the peer process instance. The described probes and signals are intended to preserve the active call operation by passing the call state information from the active to the standby ASP. Any ASP can be active while the other one is in standby state. Other processes involved in a call processing send signals with own parameters.

3.3.2 SG processor duplication

Our solution of SG redundancy is the duplication of the SG processor board, while both processors still use the existing hardware of user ports. This approach enables to reduce the overall costs to the minimum. Only the active processor has access to user ports and communicates with ASPs.

SCTP associations are established between the active processor in SG and all ASPs distributed among call servers, where user ports are registered (Fig. 5). Active processor (SGa) maintains the states of the ASPs. If SGa fails, the active and the inactive ASP recognize that event, while the SCTP Heartbeat signal is not confirmed by the opposite side. The standby processor (SGsb) in SG also finds out that the primary processor is out of order. After activation of the standby processor, the SCTP associations are reestablished on the same IP address. Appropriate sequences of IUA messages (ASP UP/ASP UP Ack, ASP AC/ASP AC Ack) are sent to the activated processor in the SG to update ASPs states.

The reduced message sequence chart for processors switch-over in SG is shown in Fig. 6. The SCTP association setup and reestablishment are done by utilizing the four way handshake sequence represented with a double arrow. ASPs are not

aware that the SG processor has changed, they only know that SCTP associations have been reestablished. SG like ASP uses the same procedure for passing the entity states information from the active to the standby processor. SG does not control any call, therefore only entitles for DSS1 data link and IP connections are presented in Table 2.

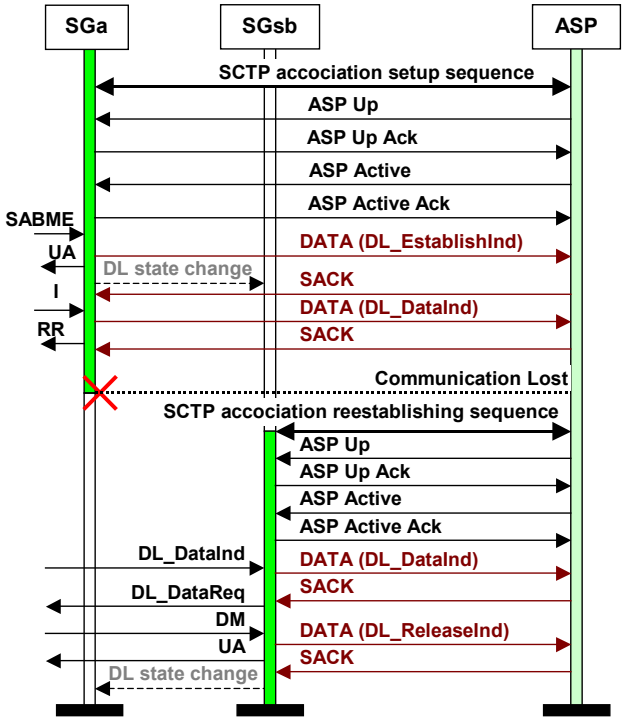

Fig. 6: Duplicated SG switch-over

Table 2: Entities in SG

SG processor	Active SGa	Standby SGsb
Entity	**state**	**state**
SCTP instance	Registered	Not created
SCTP association	Established	Not created
AS	Active	DS
ASP	Active	DS
Data link connection	Established	DS
Bearer Connection	Channel connected	DS

The data link connection (DL) entity [3] handles the Q.921 frames and passes them to the IUA layer for transporting over IP network. Whenever DL is activated or deactivated, an integrated probe in the DL process generates a signal with the following information:

- Transaction Identifier,
- Application Server Identifier,
- Application Server Process Identifier,
- User port (or D-channel) Identifier,
- Data Link Connection Identifier,
- State of Data Link Connection,
- Process identifier.

No entity in the standby SGsb operates autonomously. If the entity state is not backed-up in the standby processor, the associated process instance is not created.

4 Conclusion

The replacement of local ISDN exchanges with access gateways and the installation of call servers are not yet in the first plan of network operator activities because the ISDN network still works perfectly at a standardized quality of service. However, the new subscribers will use IP telephones and will be connected directly to IP network. The strong tendency to minimize the network operation costs leads to IP network as a common transport network, where all subscribers requests and needs should be considered, including those of existing ISDN users.

In this paper we addressed the IP protocol features and redundant system solutions used to achieve the requested ISDN access availability if ISDN access is setup over IP network. System redundancy is a very important element in telecommunication networks and is used for all services where great availability is required.

When we designed the protocols functions, we used open source code for transport (SCTP) and other lower layer IP protocols, while we used SDL tool to develop the IUA protocol and interface to SCTP protocol. ISDN access protocols have been developed previously. Other protocols for enabling user-to-user voice communication over IP like MGCP, have been designed by other teams.

References:

[1] RFC 3057; ISDN Q.921 – User Adaptation Layer; Network Working Group, Feb 2001.

[2] RFC 2960; Stream Control Transmission Protocol; Network Working Group, Oct 2000.

[3] ITU-T Recommendation Q.921, Digital Subscriber Signalling System No. 1 – Data Link Layer.

[4] Shaojian Fu, Mohammed Atiquzzaman, SCTP: State of the Art in research, Product, and Technical Challenges, IEEE Communications magazine, Vol. 42, No. 4, April 2004, pg. 64 – 76.