

**UNIVERSIDADE DE BRASÍLIA  
FACULDADE DE TECNOLOGIA  
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

**REQUISITOS DE CONFIGURAÇÃO DE REDE IP PARA  
TRANSPORTE DE INTERFACES 3GPP**

**DAVID PFANNEMÜLLER GUIMARÃES**

**ORIENTADOR: PAULO HENRIQUE PORTELA DE CARVALHO**

**DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA**

**PUBLICAÇÃO: PPGENE DM 074/2010**

**BRASÍLIA / DF: OUTUBRO / 2010**



**UNIVERSIDADE DE BRASÍLIA  
FACULDADE DE TECNOLOGIA  
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

**REQUISITOS DE CONFIGURAÇÃO DE REDE IP PARA  
TRANSPORTE DE INTERFACES 3GPP**

**DAVID PFANNEMÜLLER GUIMARÃES**

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE PROFISSIONAL EM ENGENHARIA ELÉTRICA.

APROVADA POR:

---

PAULO HENRIQUE PORTELA DE CARVALHO, Doutor, UnB  
(ORIENTADOR)

---

PRISCILA SOLIS BARRETO, Doutor, UnB  
(EXAMINADOR EXTERNO)

---

FLAVIO ELIAS DE DEUS, Doutor, UnB  
(EXAMINADOR INTERNO)

DATA: BRASÍLIA/DF, DIA 13 DE OUTUBRO DE 2010.



## **FICHA CATALOGRÁFICA**

GUIMARÃES, DAVID PFANNEMÜLLER

Requisitos de configuração de rede IP para transporte de interfaces 3GPP [Distrito Federal] 2010.

xxix, 159p. 297 mm

(ENE/FT/UnB, Mestre, Engenharia Elétrica, 2010)

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica

1. redes de sinalização 2. SCTP  
3. SIGTRAN

I. ENE/FT/UnB. II. Título (Série)

## **REFERÊNCIA BIBLIOGRÁFICA**

GUIMARÃES, DAVID PFANNEMÜLLER. (2010). Requisitos de configuração de rede IP para transporte de interfaces 3GPP. Dissertação de Mestrado, Publicação PPGENE DM074/2010, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, xxix,159p.

## **CESSÃO DE DIREITOS**

NOME DO AUTOR: David Pfnannemüller Guimarães

TÍTULO DA DISSERTAÇÃO: Requisitos de configuração de rede IP para transporte de interfaces 3GPP

GRAU/ANO: Mestre/2010.

É concedida à Universidade de Brasília permissão para reproduzir cópias desta Dissertação de Mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte deste documento pode ser reproduzida sem a autorização por escrito do autor.

---

David Pfnannemüller Guimarães  
Av. Gal. Olyntho Pillar, 355 bloco 2 ap 201  
CEP 22.793-610 – Rio de Janeiro – RJ - Brasil



Dedico esse trabalho a todos os engenheiros de telecomunicações que, cientes de sua vocação como aperfeiçoadores da criação de Deus, desenvolvem soluções para permitir que as pessoas se comuniquem sem que a distância seja um problema.



## **AGRADECIMENTOS**

Agradeço a Deus pela vocação recebida e oportunidade de estar sempre aprendendo.

Agradeço a minha família pelo apoio durante os estudos e paciência nos dias em que foi necessário trocar a proximidade pela distância. Especialmente à minha esposa Sarinha pelo carinho.

Agradeço à BrasilTelecom por acreditar no desenvolvimento contínuo de seus colaboradores.

Agradeço a UnB por ter tornado esse curso possível.

Agradeço aos professores pelo empenho, especialmente ao Prof. Paulo Portela pela orientação.



## **RESUMO**

### **REQUISITOS DE CONFIGURAÇÃO DE REDE IP PARA TRANSPORTE DE INTERFACES 3GPP**

**Autor: David Pfannemüller Guimarães**

**Orientador: Paulo Henrique Portela de Carvalho**

**Programa de Pós-Graduação em Engenharia Elétrica**

**Brasília, Outubro de 2010**

Os serviços de telecomunicações dependem cada vez mais das redes de sinalização. Com o aprimoramento e desenvolvimento crescente dos serviços, uma única chamada ou sessão de dados gera uma quantidade cada vez maior de mensagens de sinalização.

O transporte da sinalização é feito por redes dedicadas. Inicialmente estas redes foram construídas usando-se meios de transmissão dedicados, através de circuitos comutados. Com o desenvolvimento da tecnologia das redes de pacotes, as redes de sinalização têm sido construídas sobre estas redes, inicialmente ATM (*Asynchronous Transfer Mode*), e atualmente em IP (*Internet Protocol*).

As redes de pacotes, porém, não tem, em sua essência, a mesma garantia de desempenho que era obtida nas redes dedicadas, e foi necessário o desenvolvimento de protocolos específicos, visando garantir os requisitos de qualidade exigidos pelas aplicações dos serviços de telecomunicações.

A proposta deste trabalho é apresentar uma forma de garantir a transparência da rede de transporte para as camadas superiores do protocolo, seja pela adoção de topologia de conexão à rede adequada, seja pelo ajuste dos parâmetros do protocolo SCTP (*Stream Control Transmission Protocol*), protocolo esse usado na camada de transporte dos protocolos de sinalização.



## **ABSTRACT**

### **REQUISITOS DE CONFIGURAÇÃO DE REDE IP PARA TRANSPORTE DE INTERFACES 3GPP**

**Author: David Pfannemüller Guimarães**

**Supervisor: Paulo Henrique Portela de Carvalho**

**Programa de Pós-Graduação em Engenharia Elétrica**

**Brasília, September of 2010**

Telecommunications services are increasingly dependent on signaling networks. The improvement and development of new services, a single call or data session generates a very huge amount of signaling traffic.

The signaling transport is made by dedicated networks. Initially, these networks were built using dedicated transmission resources, through circuit switched networks. The development of the technology of packet networks drove the signaling networks to be built over these networks, using initially ATM (*Asynchronous Transfer Mode*), and currently in IP (*Internet Protocol*).

Packet networks, however, doesn't have, the same performance qualities that was obtained on dedicated networks, and it was necessary to develop specific protocols in order to ensure the quality requirements demanded by telecommunications services applications.

The purpose of this work is to present a configuration that ensures the transparency of the transmission to the upper layers of the protocol, through the adoption of network connection topology fit, either by adjusting the parameters of the SCTP protocol, that is the protocol used for the layer transport stack in signalling networks.



## SUMÁRIO

1. INTRODUÇÃO.....	1
1.1. TRANSPORTE DE SINALIZAÇÃO SS7.....	1
1.2. TRANSPORTE DE SINALIZAÇÃO EM REDES IP.....	2
1.3. OBJETIVOS.....	3
2. A REDE DE SINALIZAÇÃO.....	5
2.1. NECESSIDADE DE UMA REDE DE SINALIZAÇÃO.....	9
2.2. EXEMPLO DE SEQUÊNCIA DE MENSAGENS.....	9
2.3. EXEMPLO DE INTERFACES 3GPP.....	13
2.4. PILHA DE SINALIZAÇÃO.....	15
2.5. TECNOLOGIA USADA HOJE NAS REDES DE SINALIZAÇÃO E SUAS LIMITAÇÕES.....	16
2.6. O USO DE REDE DE PACOTES PARA SINALIZAÇÃO.....	18
2.7. REDE DE SINALIZAÇÃO VIA IP.....	19
2.8. GRUPO DE TRABALHO SIGTRAN.....	20
2.9. USOS ATUAIS DA PILHA SIGTRAN.....	22
2.10. REQUISITOS PARA O SIGTRAN.....	24
2.10.1. Atraso máximo.....	24
2.10.2. Redundância.....	26
2.11. CONCLUSÕES.....	26
3. A PILHA SIGTRAN.....	28
3.1. O PROTOCOLO SCTP.....	30
3.2. COMPARAÇÃO TCP, UDP E SCTP.....	30
3.2.1. Diferenças na inicialização.....	31
3.2.2. Bloqueio Head-of-Line.....	32
3.2.3. Limites das mensagens.....	32
3.2.4. Confirmação Seletiva.....	32
3.2.5. Multi-homing.....	33
3.2.6. Procedimento de fechamento.....	33
3.2.7. Extensões do protocolo.....	33
3.3. ASPECTOS DE REDUNDÂNCIA.....	34
3.3.1. Conceito de IP multi-homing.....	34

3.3.2. Multi-homing x single homing.....	35
3.3.3. Topologia para uso do multi-homing.....	35
3.4. TEMPORIZADORES E VARIÁVEIS DO PROTOCOLO.....	36
3.4.1. RTO e variáveis associadas.....	36
3.4.2. Temporizador T3-rtx.....	37
3.4.3. Contador de erros do caminho e da associação.....	39
3.5. PARÂMETROS CONFIGURÁVEIS.....	39
3.5.1. Parâmetros RTOmin e RTOmax.....	39
3.5.2. Parâmetro Path.Max.Retrans – número máximo de retransmissões no caminho .....	40
3.5.3. Parâmetro Association.Max.Retrans – número máximo de retransmissões na associação.....	40
3.5.4. Parâmetro HB.Interval – Intervalo de HeartBeat .....	41
3.5.5. Parâmetro Atraso de SACK.....	41
3.6. VALORES SUGERIDOS.....	42
3.7. CONCLUSÕES.....	42
4. OTIMIZAÇÃO.....	44
4.1. REQUISITOS DAS CAMADAS DE APLICAÇÃO.....	45
4.2. AVALIAÇÃO DO DESEMPENHO DO SCTP.....	45
4.2.1. Requisitos de topologia da rede.....	46
4.2.2. Fatores que afetam o tempo para comutação.....	47
4.2.2.1. Latência .....	49
4.2.2.2. Perfil de tráfego.....	50
4.2.2.3. Parâmetro SACK Delay - Atraso de SACK.....	51
4.2.2.4. Parâmetro Path.Max.Retrans – número máximo de retransmissões no caminho.....	52
4.2.2.5. Parâmetro RTOmin.....	53
4.2.2.6. Parâmetro RTOmax.....	53
4.2.3. Fatores que afetam o atraso máximo das mensagens.....	54
4.2.3.1. Latência.....	54
4.2.3.2. Perfil de tráfego.....	55
4.2.3.3. Parâmetro Atrasos de SACK, Path.Max.Retrans, RTOmin e RTOmax...56	
4.3. SIMULADOR SCTP.....	57
4.3.1. Validação do simulador.....	61

4.4. SIMULAÇÕES.....	63
4.4.1. Simulação 1 - Entre topologias multi-homing.....	64
4.4.2. Simulação 2 – Variação do intervalo entre as mensagens enviadas.....	67
4.4.3. Simulação 3 – Variação do tamanho das mensagens.....	69
4.4.4. Simulação 4 – Efeito da latência de rede.....	71
4.4.5. Simulação 5 – Efeito do parâmetro Path.Max.Retrans.....	73
4.4.6. Simulação 6 – Efeito de alteração do parâmetro de Atraso de SACK.....	74
4.4.7. Simulação 7 – Efeito de alteração do parâmetro RTOmin.....	75
4.4.8. Simulação 8 – Efeito de alteração do parâmetro RTOmax.....	76
4.5. AVALIAÇÃO DOS RESULTADOS.....	82
4.5.1. Ganho na topologia.....	82
4.5.2. Ajuste no parâmetro RTOmin.....	82
4.5.3. Ajuste no parâmetro RTOmax.....	82
4.5.4. Ajuste no parâmetro Path.Max.Retrans.....	83
4.6. CONCLUSÕES.....	83
5. PROPOSTAS DE AJUSTES NOS PARÂMETROS.....	84
5.1. AJUSTE 1 – TOPOLOGIA.....	85
5.2. AJUSTE 2 – PARÂMETRO RTOMIN.....	86
5.3. AJUSTE 3 – PARÂMETRO PATH.MAX.RETRANS.....	86
5.4. AJUSTE 4 - PARÂMETRO RTOMIN.....	87
5.5. AJUSTE 5 – PARÂMETRO RTOMAX.....	87
5.6. AJUSTE 6 – PARÂMETRO PATH.MAX.RETRANS.....	88
5.7. AJUSTES ADICIONAIS.....	89
5.8. SUGESTÕES DE VALORES PARA OS PARÂMETROS.....	89
5.9. CONCLUSÕES.....	95
6. CONCLUSÕES E TRABALHOS FUTUROS.....	96
6.1. TRABALHOS FUTUROS.....	98
BIBLIOGRAFIA.....	99
A.DETALHAMENTO DE CHAMADAS REAIS.....	105
A.1.CONSULTA AO EIR.....	105
A.2.CONSULTA AO AUC.....	112
A.3.CHAMADA ISUP.....	120
A.4.CHAMADA ORIGINADA POR PRÉ-PAGO (CONSULTA CAMEL O-CSI).....	125
A.5.CHAMADA TERMINADA EM PRÉPAGO – CAMEL T-CSI.....	136

B.TABELA COMPARATIVA DE TEMPOS DE COMUTAÇÃO .....	148
C.DIMENSIONAMENTO DE ENLACES DE SINALIZAÇÃO NÚMERO 7.....	152
D.PROGRAMA SIMULADOR SCTP.....	153

## ÍNDICE DE TABELAS

Tabela 3.1 - Comparação entre SCTP, TCP e UDP, conforme (Costa, D., 2005).....	31
Tabela 4.1 - Quantidade de associações paralelas e o tráfego relativo em cada uma.....	51
Tabela 4.2: Comparação de resultados para Atraso Máximo, usando Atraso de SACK de 200ms.....	62
Tabela 4.3: Comparação de resultados para Atraso Máximo, usando Atraso de SACK de 0ms.....	62
Tabela 4.4 - Implementação de divisão de carga em múltiplos caminhos.....	65
Tabela 4.5 - Tempo dos eventos até a comutação para o caminho reserva.....	72
Tabela 5.1 - Tempo e Eventos para os valores propostos na RFC2960.....	85
Tabela 5.2 - Proposta de ajuste para os parâmetros SCTP em função da latência.....	92
Tabela B.1: Tempo de comutação estimado para os diversos perfis.....	148
Tabela B.2: Tempos e Eventos Associados para o perfil 3, latência de 16ms.....	150
Tabela D.1: Descrição das principais rotinas do módulo mod_Endpoint.....	153
Tabela D.2: Descrição das principais rotinas do módulo Rede.....	154
Tabela D.3: Principais rotinas do módulo Aplicação.....	154
Tabela D.4: Principais estruturas de dados usadas no simulador.....	155
Tabela D.5: Exemplo de arquivo exportado pelo simulador.....	158



## ÍNDICE DE FIGURAS

Figura 2.1 - Rede de sinalização sem uso de STPs.....	8
Figura 2.2 - Rede de sinalização com o uso de dois STPs.....	9
Figura 2.3 - Exemplo de troca de mensagens de sinalização em chamada móvel-móvel pré-pago.....	11
Figura 2.4 - Comparação de fluxo de mensagens segundo 3GPP release 99 e 3GPP release 4.....	13
Figura 2.5 - Interfaces 3GPP para uma rede GSM / GPRS básica.....	14
Figura 2.6 - Pilha SS7 e sua comparação com o modelo OSI.....	15
Figura 2.7 - Interfaces de uma rede GSM / GPRS básica que podem ser transportadas pela pilha SIGTRAN.....	23
Figura 2.8 - Interfaces 3GPP especificadas para LTE, conforme 3GPP 23.401 V9.3 (3GPP, 2010C).....	24
Figura 3.1 - Comparação entre pilha de sinalização SS7 convencional e SIGTRAN.....	28
Figura 3.2 - Pilhas SS7 e SIGTRAN conectadas através de um signaling gateway (Immonen, M., 2005).....	29
Figura 4.1 - Conceito de multi-caminhos interligando dois endpoints.....	47
Figura 4.2 - Fatores de influência para o tempo de comutação para o caminho reserva....	48
Figura 4.3 - Oscilação do valor de RTO em função da variação dos valores de atraso na rede.....	49
Figura 4.4 - Fatores de influência para o atraso máximo dos pacotes.....	55
Figura 4.5 - Blocos do Simulador.....	58
Figura 4.6: Diagrama de Blocos do Simulador SCTP.....	59
Figura 4.7 - Exemplo de distribuição de latência implementada no bloco de software de rede, para o valor mínimo de 20 ms e esperança da distribuição de 1 ms.....	60
Figura 4.8 - Implementação de divisão de carga em múltiplos caminhos.....	65
Figura 4.9 - Relação entre o desempenho e o número de associações paralelas.....	66
Figura 4.10 - Efeito do Intervalo de Envio (visão intervalo).....	67
Figura 4.11 - Efeito do Intervalo de Envio (visão frequência).....	68
Figura 4.12 - Razão entre o atraso máximo e o tempo de comutação em função do intervalo entre as mensagens.....	69
Figura 4.13 - Relação entre o desempenho e o tamanho das mensagens.....	70

Figura 4.14 - Desempenho em função da latência de rede.....	72
Figura 4.15 - Relação entre os tempos de comutação e latência, em função da latência.....	73
Figura 4.16 - Tempo de comutação x PMR.....	74
Figura 4.17 - Efeito do Atraso de SACK.....	75
Figura 4.18: Efeito do parâmetro RTOMin.....	76
Figura 4.19 - Tempo de comutação em função do RTOMax (exponencial).....	77
Figura 4.20 - Tempo de comutação em função do RTOMax (linear).....	80
Figura 4.21: Tempo de comutação em função do RTOMax (logarítmico).....	80
Figura 4.22 - Atraso máximo em função do RTOMax.....	81
Figura 4.23 - Efeito do valor de RTOMax no tempo de comutação, para vários valores de Path.Max.Retrans.....	81
Figura 5.1 - Relação entre a razão tempo de comutação por Latência e o parâmetro RTOMax.....	88
Figura 5.2: Desempenho esperado dos diversos perfis em função da latência da rede.....	90
Figura 5.3 - Resultados obtidos com o ajuste dos parâmetros, em relação ao tempo de comutação.....	93
Figura 5.4 - Resultados obtidos com o ajuste dos parâmetros SCTP, em relação ao atraso máximo das mensagens.....	94
Figura D.1: Painel de Controle Principal do Simulador.....	156
Figura D.2: Painel de Controle Principal com algumas opções de execução.....	157
Figura D.3: Tela de acompanhamento de resultados e variáveis.....	157

## LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIACÕES

$\alpha$	parâmetro usado no cálculo da variável RTTVAR
$\beta$	parâmetro usado no cálculo da variável SRTT
3GPP	<i>Third Generation Partnership Project</i>
ACM	<i>Address Complete Message</i>
ANM	<i>Answer Message</i>
ANSI	<i>American National Standards Institute</i>
ASP	<i>Application Service Part</i>
ATM	<i>Asynchronous Transfer Mode</i>
Assoc.Max.Retrans	<i>Association Maximum Retransmission</i>
AuC	<i>Authentication Center</i>
B	fator de <i>back-off</i>
back-off	fator de multiplicação do valor de RTO para as retransmissões
BHCA	<i>Busy Hour Call Attempts</i>
BSS	<i>Base Station Subsystem</i>
CAMEL	<i>Customised Applications for Mobile networks Enhanced Logic</i>
<i>chunk</i>	cada um dos pacotes de dados do protocolo SCTP
control plane	plano de controle
Core Network	rede núcleo de um sistema de telecomunicações

CPG	<i>Call Progress Message</i>
CSV	<i>Comma Separated Values</i>
CTP	<i>Common Transport Protocol</i>
DATA	<i>chunk</i> que carrega informações de dados
datagrama	estrutura unitária de transmissão de dados
dormant mode	modo dormente do SCTP
DTMF	<i>Dual Tone Multi-Frequency</i>
E1	enlace de transmissão digital com taxa de 2,048 kbps
E-NB	<i>Enhanced Node B</i>
EIR	<i>Equipment Identity Register</i>
endpoint	cada um dos elementos que se comunicam pelo protocolo SCTP
Erl	Erlang
fator de <i>back-off</i>	fator de multiplicação do valor de RTO para as retransmissões
G-MSC	<i>Gateway – Mobile Switch Center</i>
GPRS	<i>General Packet Radio Service</i>
GSM	<i>Global System for Mobile Communication</i>
H.323	recomendação do ITU-T que define o protocolo para sessões de áudio e vídeo
HB.Interval	parâmetro de intervalo de envio do <i>chunk</i> HEARTBEAT no SCTP

HEARTBEAT	<i>chunk</i> usado no SCTP para verificação do estado de um caminho
HEARTBEAT-ACK	<i>chunk</i> usado no SCTP para confirmar o recebimento do <i>chunk</i> HEARTBEAT
HLR	<i>Home Location Register</i>
HSPA	<i>High Speed Packet Access</i>
HSS	<i>Home Subscriber Server</i>
IAM	<i>Initial Address Message</i>
IDP	<i>Initial Detection Point</i>
IETF	<i>Internet Engineering Task Force</i>
IMEI	<i>International Mobile Equipment Identifiers</i>
IMS	<i>IP Multimedia Subsystem</i>
INIT	<i>chunk</i> usado no SCTP para inicializar a associação
INIT-ACK	<i>chunk</i> usado no SCTP para confirmar o recebimento do <i>chunk</i> INIT
<i>inter-MS</i> C handover	passagem de uma chamada em curso de uma MSC para outra
Internet	rede mundial de computadores construída sobre redes IP
IP	<i>Internet Protocol</i>
ISDN	<i>Integrated Services Digital Network</i>
ISUP	<i>ISDN User Part</i>
ITU	<i>International Telecommunications Union</i>

LTE	<i>Long Term Evolution</i>
M2PA	<i>MTP2 Peer-toPeer Adaptation Layer</i>
M2UA	<i>MTP2 User Adaptation Layer</i>
M3UA	<i>MTP-L3 User Adaptation Layer</i>
MAP	<i>Mobile Application Part</i>
MDTP	<i>Multinetwork Datagram Transmission Protocol</i>
ME	<i>Mobile Equipamet</i>
MGW	<i>Media Gateway</i>
MME	<i>Mobility Management Entity</i>
MPLS	<i>Multi Protocol Label Switching</i>
MSC	<i>Mobile Switching Center</i>
MSC Server	<i>Mobile Switching Center Server</i>
MSU	<i>Message Signal Unit</i>
MTP	<i>Message Transfer Part</i>
MTP1	<i>Message Transfer Part Level 1</i>
MTP2	<i>Message Transfer Part Level 2</i>
MTP3	<i>Message Transfer Part Level 3</i>
MTU	<i>Maximum Transmission Unit</i>

*multi-homing*, associação *multi-homed* – tipo de comunicação que envolve mais de um

	caminho possível.
n	número de associações SCTP usadas em paralelo
OSI	<i>Open Systems Interconnect</i>
<i>path</i>	caminho
Path.Max.Retrans	<i>Path Maximum Retransmission</i>
PCRF	<i>Policy charging and rules function</i>
PDN-Gateway	<i>Packet Data Network Gateway</i>
PMTU	<i>Path Maximum Transmission Unit</i>
PRN	<i>Provide Roaming Number</i>
PSI	<i>Provide Service Information</i>
PTS	Ponto de Transferência de Sinalização
PURDET	<i>Reliable Transport Extensions To UDP</i>
Q.700	Recomendação do ITU-T que define o protocolo SS7
RAN	<i>Radio Access Network</i>
REL	<i>Release Message</i>
RFC	<i>Request For Comments</i>
RLC	<i>Release Complete Message</i>
<i>Round-trip Time</i>	Tempo total de ida e volta de um sinal em uma rede de telecomunicações

RTO	<i>Retransmission Time-out</i>
RTOmax	<i>Retransmission Time-out Maximum</i>
RTOmin	<i>Retransmission Time-out Minimum</i>
RTP	<i>Real Time Protocol</i>
RTT	<i>Round-trip Time</i>
RTTVAR	<i>Round-trip Time Variation</i>
SACK	<i>Selective Acknowledgment</i>
SACK Delay	<i>Selective Acknowledgment Delay</i>
SCCP	<i>Signaling Connection Control Part</i>
SCF	<i>Service Control Function</i>
SCOP	<i>Service Specific Connection-Oriented Protocol</i>
SCP	<i>Service Control Point</i>
SCTP	<i>Stream Control Transmission Protocol</i>
SGSN	<i>Serving GPRS Support Node</i>
SGW	<i>Serving Gateway</i>
SIGTRAN	<i>Signaling Transport</i>
SIP	<i>Session Initiation Protocol</i>
SMS	<i>Short Message Service</i>
SRI	<i>Send Routing Information</i>

SRTT	<i>Smoothed Round-trip Time</i>
SS7	<i>Signaling System 7</i>
SSP	<i>Service Switching Point</i>
SSTP	<i>Simple SCCP Tunneling Protocol</i>
STP	<i>Signaling Transfer Point</i>
SUA	<i>SCCP User Adaptation</i>
SYN	<i>synchronize</i> – pacote usado para iniciar uma sessão TCP
T3-rtx	temporizador interno ao protocolo SCTP
TCAP	<i>Transaction Capabilities Application Part</i>
TDM	<i>Time Division Multiplexing</i>
UDP	<i>User Datagram Protocol</i>
<i>user plane</i>	plano do usuário
UMTS	<i>Universal Mobile Telecommunications System</i>
UTRAN	<i>UMTS Terrestrial Radio Access Network</i>
VLAN	<i>Virtual Local Area Network</i>
VLR	<i>Visitor Location Register</i>
V-MSC	<i>Visited Mobile Switching Center</i>
WCDMA	<i>Wideband Code Division Multiple Access</i>

# 1. INTRODUÇÃO

O 3GPP (3rd Generation Partnership Project – Projeto de Parceria de Terceira Geração) é o órgão que gera as especificações para os elementos constituintes de uma rede móvel GSM (Global System for Mobile Communications - Sistema Global para Comunicações Móveis) e/ou WCDMA (Wideband Code Division Multiple Access – Acesso por Múltipla Divisão de Código em Banda Larga). As especificações 3GPP estão em constante evolução, acompanhando tanto as necessidades dos usuários relativos a novos serviços, como o desenvolvimento e evolução dos equipamentos que compõem as redes.

O 3GPP especifica que a troca de sinalização entre os elementos deve ser feita através de enlaces conhecidos como enlaces de sinalização número 7, ou simplesmente SS7 (Signaling System #7 – Sistema de Sinalização Número 7). O SS7 é definido pelo ITU-T na recomendação Q.700 (ITU-T, 1993).

## 1.1. TRANSPORTE DE SINALIZAÇÃO SS7

As especificações do 3GPP consideram o transporte da sinalização número 7 por meio de enlaces de baixa velocidade, tipicamente estabelecidos sobre canais TDM (*Time Division Multiplexing* – Multiplexação por divisão de tempo) em canalização E1 (enlaces de 2Mbps). Estes enlaces, conhecidos como *low speed links*, suportam uma taxa de 64 kbps e são agrupados de forma a se obter a taxa de transferência necessária para o serviço. Devido a restrições lógicas da configuração destes enlaces, estes estão limitados a um agrupamento máximo de 16, totalizando uma capacidade máxima de 1024 kbps, sendo essa quantidade muitas vezes insuficiente para o tráfego de sinalização requerida, devido à necessidade de ocupação máxima de segurança de 80% e uso de divisão de carga entre enlaces paralelos. Todos esses requisitos tipicamente geram uma disponibilidade máxima de 409 kbps, conforme indicado no anexo C.. Mesmo com o uso de enlaces de alta velocidade, que disponibilizam 2 Mbps por enlace físico, a capacidade de transporte de sinalização fica aquém da necessidade das redes atuais.

Com a evolução da tecnologia, há um crescimento na capacidade de processamento dos elementos de rede. Esse aumento de capacidade resulta em um crescimento de tráfego de sinalização de forma concentrada, fazendo com que a capacidade dos enlaces de

sinalização se esgote rapidamente, gerando a necessidade de outros meios de transporte para a comunicação entre os elementos de rede.

## **1.2. TRANSPORTE DE SINALIZAÇÃO EM REDES IP**

Em paralelo, a IETF (Internet Engineering Task Force – Força Tarefa de Engenharia da Internet) criou a especificação RFC 2719 (Ong, L., Ritina, I., 1999), que estabelece as bases para o transporte de sinalização SS7 sobre redes IP. O grupo de trabalho formado, chamado SIGTRAN (Signaling Transfer – Transferência de Sinalização), acabou denominando a pilha de protocolos definida, que usa o SCTP (*Stream Control Transfer Protocol*) como protocolo de transporte. Essa especificação passou a ser utilizada pelas operadoras de telecomunicações, já que estas possuem redes IP de médio e grande porte, tanto para prover serviços IP aos seus clientes, como para tráfego de informações e gerência dos elementos de rede.

As redes IP já têm funcionalidades de redundância e roteamento de mensagens nativas em sua construção, o que facilita o uso destes recursos pelos serviços que a utilizam. Os principais fatores para adoção do SIGTRAN para transporte de sinalização SS7 são a utilização de redes IP já existentes na operadora e o baixo custo de construção e operação destas redes. Observe-se, porém, que estas interfaces definidas pelo 3GPP foram originalmente criadas considerando-se o uso de transporte via TDM, e posteriormente foram parcialmente adaptadas para transporte via IP, ou seja, SIGTRAN.

O uso de uma rede IP sem garantia de qualidade de serviço é uma opção viável para operadoras de telecomunicações. Porém isso requer uma avaliação detalhada dos requisitos das aplicações que irão trafegar pela mesma. Essa avaliação torna-se mais complexa à medida que são agregados a essa rede serviços nos quais a operadora tem pouco ou quase nenhum controle, como por exemplo acesso à Internet de usuários residenciais.

Por outro lado, as interfaces do núcleo da rede móvel (chamada *core*) foram estabelecidas para trabalhar com meios de transmissão bastante controlados, com enlaces dedicados. As camadas superiores destes protocolos têm temporizações bastante definidas, não compatíveis com as situações de tráfego encontradas em redes IP que são compartilhadas com diversas aplicações.

### 1.3. OBJETIVOS

Este trabalho se propõe a avaliar requisitos das redes de sinalização em telecomunicações para o transporte de sua sinalização, e a forma mais adequada de se estabelecer o transporte via rede IP usando-se a pilha SIGTRAN.

A avaliação envolve conhecer os requisitos das camadas de aplicação, o funcionamento do protocolo SCTP, principal responsável pelo transporte das mensagens entre os elementos, bem como o impacto da configuração de seus parâmetros internos.

O objetivo do trabalho é definir a forma mais otimizada para o uso do transporte da sinalização via SIGTRAN, especificando:

- A topologia mais adequada de configuração dos elementos de rede, ou seja, aquela que maximiza os ganhos de desempenho oferecidos pelo transporte da sinalização via rede IP.
- A configuração otimizada para os parâmetros do protocolo, de forma a garantir a transparência do transporte da sinalização, para que as camadas de aplicação não sintam o efeito de uma possível falha de rede.

Para atingir esse objetivo, será usado um simulador das condições de tráfego de rede e do funcionamento do protocolo. Essa ferramenta será usada para verificar o impacto da variação do perfil do tráfego de sinalização, comparando as diversas topologias de conexão dos elementos à rede IP, bem como a variação dos parâmetros internos ao protocolo.

Embora haja outros trabalhos envolvendo a otimização do protocolo SCTP para condições de falha, eles consideram situações diferentes das reais encontradas em uma rede de sinalização. Os trabalhos de (Brunstrom, A., Grinnemo, K., 2005) e (Brunstrom, A., Eklund, J., 2006) avaliam o impacto do tráfego no tempo de comutação do protocolo, mas o fazem com tráfego unidirecional. O trabalho de (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010) sugere valores para otimização, mas considera alterações em parâmetros não configuráveis do protocolo. Outros trabalhos, como o de (Rembarz, R., Baucke, S., Mahonen, P., 2005) e (Jungmaier, A., Rathgeb, E. P., 2006), avaliam os impactos dos parâmetros, sem, no entanto, sugerir valores para os mesmos.

Neste trabalho, serão feitas simulações com tráfego com perfil similar ao tráfego de sinalização, ou seja, bidirecional. Também obteremos um conjunto de parâmetros sugeridos para uso, de acordo com a característica observada no enlace a ser utilizado. Será também avaliada a topologia de conexão mais adequada, bem como o efeito do uso de múltiplas conexões lógicas paralelas entre elementos de rede.

## **2. A REDE DE SINALIZAÇÃO**

Uma rede de telecomunicações envolve diversos elementos. Dependendo do serviço a ser prestado, a quantidade de elementos tende a crescer. Isso porque há elementos distintos para cada função desejada.

Uma central de comutação, por exemplo, é responsável pelo tratamento do início da chamada. Porém, se o destino desta chamada não estiver na mesma central, será necessário que esta passe a chamada para outro elemento de rede, que pode ser a central de destino ou ainda uma central trânsito, que fará a função de encaminhar a chamada à central de destino. No caso do serviço pré-pago, antes do encaminhamento da chamada, a central de origem irá solicitar a um elemento externo, onde está implementado o serviço pré-pago, a autorização para que a chamada seja completada. Cite-se ainda a consulta à base de dados de portabilidade, ou a um elemento responsável pelo tratamento do serviço 0800. Para que todas essas interações possam ocorrer de forma rápida e organizada, é necessária uma rede de sinalização.

A rede de sinalização é essencial para que os elementos de rede possam trocar informações sem que o tráfego dos dados em si mesmo (seja ele voz ou dados) tenha que passar pelos elementos de controle.

No início das telecomunicações, cada central telefônica, ou seja, cada nó de rede, tinha todas as informações suficientes em sua programação interna para decidir o tratamento que deveria ser dado a uma chamada. Isso ocorria porque as chamadas eram processadas apenas com a informação do número de destino escolhido pelo cliente.

Desta forma, as informações básicas sobre a chamada, ou seja, o número de origem, o número de destino, a categoria do telefone de origem, eram enviadas pelo próprio canal de voz onde, em seguida, iria ser passada a voz da chamada. Os primeiros protocolos de sinalização, portanto, foram desenvolvidos para serem transportados por canal de voz, sendo que a informação de sinalização era transformada em diversos tons audíveis e em alterações da tensão aplicada sobre a linha que interligava as duas centrais. O processo é similar ao usado hoje na discagem a partir de telefones fixos com discagem por tom, onde cada tecla tem associado a ela dois tons, que são enviados do aparelho até a central para

informar a tecla pressionada. Esse processo é chamado de DTMF (*Dual Tone Multi-Frequency*).

Com a evolução das centrais, essa troca de sinalização passou ser feita em um canal exclusivo. Com o uso de um canal exclusivo, era possível se saber, por exemplo, se o telefone de destino estava livre ou ocupado, evitando-se, portanto, a alocação de um canal que depois seria desligado caso o destino não estivesse disponível. Mas o grande impulso para a criação de uma rede de sinalização completa foi a introdução, na década de 80, de serviços conhecidos como 800, ou 0800. Através deste prefixos, era possível ter-se um número que fosse local em todo o país. Como, devido a questões de encaminhamento, não é possível que um prefixo (no caso o 800) exista em todas as centrais da rede do país, foi adotada a solução de que, para encaminhamento da chamada, é usado um número de telefone comum. A rede então se encarrega de traduzir o telefone do serviço 800 em um número de destino convencional para onde a chamada é completada. Ainda assim, considerando-se que esse serviço foi implantado em todo o território norte-americano, torna-se inviável replicar a tabela de tradução dos números do serviço 800 para o destino final em todas as centrais do país. Desta forma foi criada uma base de dados externa à central para esse fim, onde a consulta era feita via rede de pacotes.

Surgiram, assim, as primeiras redes de sinalização, que passaram a transportar informações sobre chamadas e também informações de consultas a serviços. A sinalização, gradativamente, passou a ser transportada por uma rede totalmente separada da rede usada para o transporte de voz.

Agora que os recursos das redes de sinalização estavam disponíveis, começaram a ser criados outros serviços que tiraram proveito desta topologia. Entre eles estão a portabilidade numérica, o serviço pré-pago e o televoto (Russell, T., 2006).

Assim, estabelecem-se duas redes (ou dois planos): a rede de controle, chamada de plano de controle, e a rede de voz, ou rede de tráfego. O plano de controle, que é transportado pela rede de sinalização, é responsável por carregar todas as informações entre os elementos de rede para permitir o correto processamento da chamada.

A rede de sinalização é composta de elementos chamados de pontos de sinalização, que são elementos capazes de processar mensagens de sinalização. Existem três tipos de pontos de

sinalização:

- *Service Switching Point* – SSP – é o elemento de comutação da rede. Esses elementos efetivamente processam o tráfego (voz ou dados), gerando as mensagens de sinalização necessárias. Um exemplo são as centrais telefônicas em si;
- *Signal Transfer Point* – STP – são os elementos que fazem a transferência da sinalização entre os SSPs e SCPs, evitando a necessidade de conectividade direta entre os elementos;
- *Service Control Point* – SCP – são os elementos que tem a lógica do serviço, porém não processam diretamente o tráfego. São consultados pelos SSPs para definir qual o processamento deve ser dado a uma chamada. São exemplos de SCP uma plataforma de pré-pago, ou HLR (*home location register*) da rede móvel.

O objetivo do STP é fazer com que não seja necessário que os elementos de rede tenham conexão direta entre eles. Conforme a quantidade de elementos em uma rede cresce, a quantidade de conexões diretas entre os elementos de rede (caso não se use STPs) pode tornar inviável a gerência de tantos enlaces de sinalização.

A Figura 2.1 mostra uma rede hipotética, como 4 SSPs e 4 SCPs, onde cada um dos 4 SSPs deve ter acesso aos serviços dos SCPs. Na Figura 2.2 a mesma rede é mostrada já com uso de dois STPs. Observe-se que toda a sinalização será enviada pelos SSPs para os STPs que, baseado na informação de roteamento da mensagem, fará o roteamento desta mensagem para o destino correto. Utilizam-se dois STPs por uma questão de redundância. Neste caso, cada SSP e SCP terá apenas dois enlaces de sinalização, sendo um para cada STP.

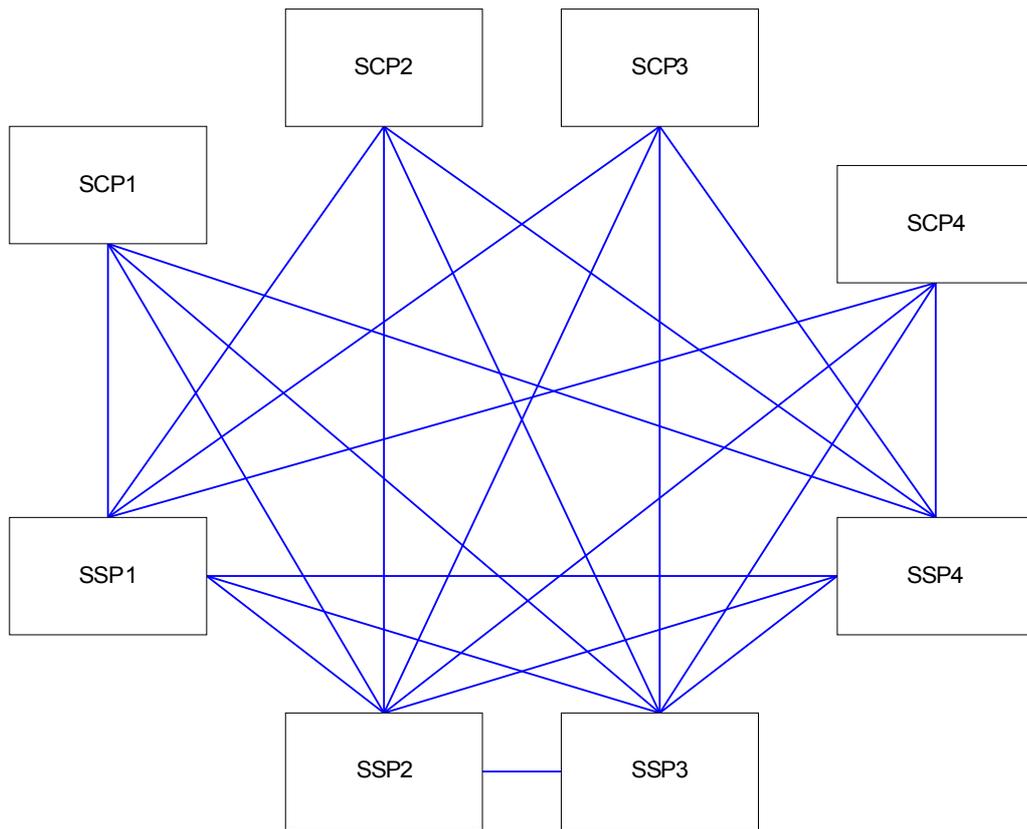


Figura 2.1 - Rede de sinalização sem uso de STPs

Neste trabalho usaremos o termo rede de sinalização para indicar a rede que transporta o plano de controle (*control plane*), e o termo rede de voz para indicar a rede que transporta o plano de usuário (*user plane*), ainda que essa rede seja usada tanto para serviços de voz como para serviços de dados.

A rede SS7 (*Signaling System 7*) é a rede definida pelo ITU-T (*International Telecommunications Union – Telecommunications Standardization Sector*) para o transporte de sinalização, conforme recomendação Q.700 (ITU-T, 1993). Existem versões regionais desta rede, como a rede ANSI (*American National Standards Institute – Instituto Nacional Americano de Padrões*), padronizada pela entidade que leva o mesmo nome. Porém, os protocolos 3GPP utilizam como rede de controle a rede SS7 padronizada pelo ITU-T.

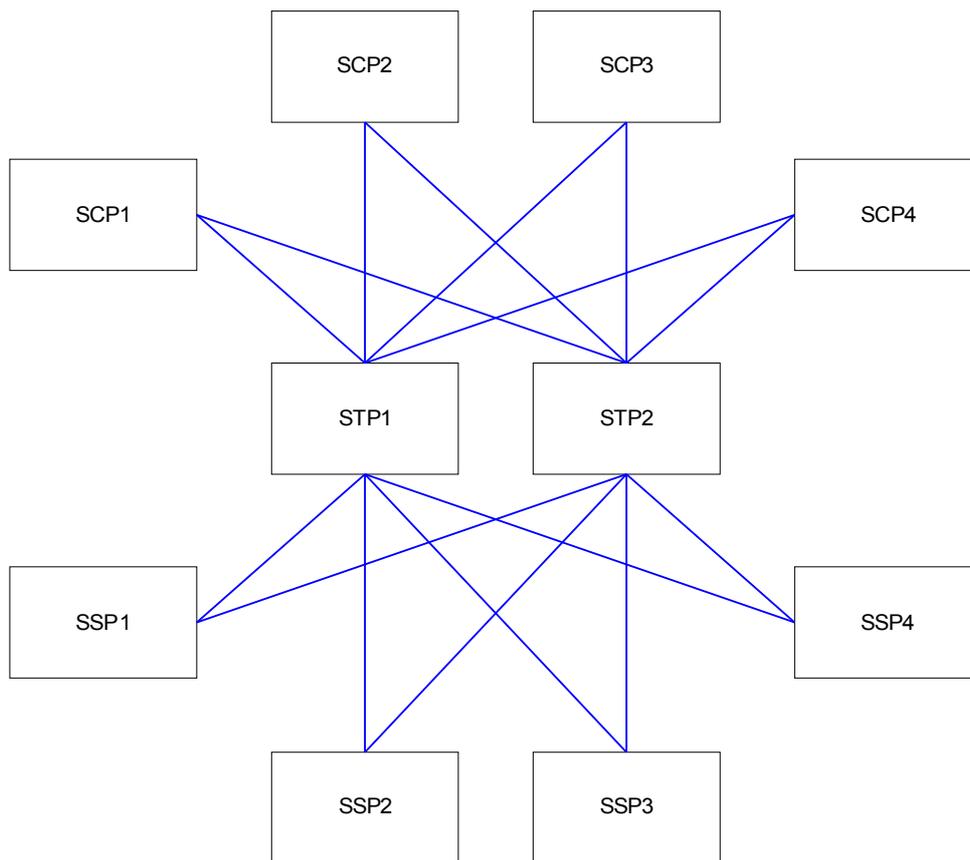


Figura 2.2 - Rede de sinalização com o uso de dois STPs

## 2.1. NECESSIDADE DE UMA REDE DE SINALIZAÇÃO

Enquanto em uma rede preparada para o serviço telefônico convencional (fixo) a necessidade de uma rede de sinalização já é reconhecida, em uma preparada para o serviço móvel essa necessidade é ainda maior. Como o usuário não está fisicamente associado a uma central específica, os seus dados devem ser mantidos em um elemento externo à central. Qualquer operação - seja originação e terminação de chamada, envio de SMS, tráfego de dados – gera uma consulta a uma ou mais bases de dados, para que a informação necessária seja obtida pela central de origem. Após essas consultas a central de origem avalia o destino da chamada, e a envia para o destino. Ou seja, a informação sobre as características e permissões do cliente está distribuída em vários elementos de rede.

## 2.2. EXEMPLO DE SEQUÊNCIA DE MENSAGENS

Tome-se como exemplo de uso de sinalização uma chamada entre dois usuários do serviço

móvel que se utilizam do serviço pré-pago. As mensagens indicadas foram coletadas em uma rede operacional, através de ferramenta de gerência de sinalização. Neste cenário estão envolvidos 4 elementos de rede, sendo estes:

- MSCs (*Mobile Switching Center* – Centrais de Comutação e Controle), onde os usuários estão sendo atendidos;
- SCP (*Service Control Point* – Ponto de controle do Serviço), para o controle da chamada de acordo com as regras do serviço (avaliação do saldo e tarifação em tempo real);
- HLR (*Home Location Register* – Base de Dados Registro) , onde é obtida a informação da localização do usuário que recebe a chamada;
- EIR (*Equipment Identity Register* – Registro de Identidade do Equipamento), que contém a informação sobre o bloqueio do aparelho; e
- AuC (*Authentication Center* – Centro de Autenticação), que tem os dados para autenticação e cifragem da chamada.

Neste exemplo, o EIR e o AuC estão implementados como parte do HLR, embora sejam blocos de *software* específicos, e com base de dados independente. Não foram consideradas nesta avaliação as mensagens de sinalização trocadas entre as MSCs e a rede de acesso, uma vez que essas conexões são feitas normalmente através de enlaces ponto a ponto.

O fluxo de mensagens é indicado na Figura 2.3. Apesar de serem somente 4 elementos de rede neste exemplo, há um total de 11 transações para estabelecimento da chamada, envolvendo 25 mensagens, e 3 transações de desconexão e notificação, num total de 8 mensagens. As mensagens totalizaram 3.822 octetos.

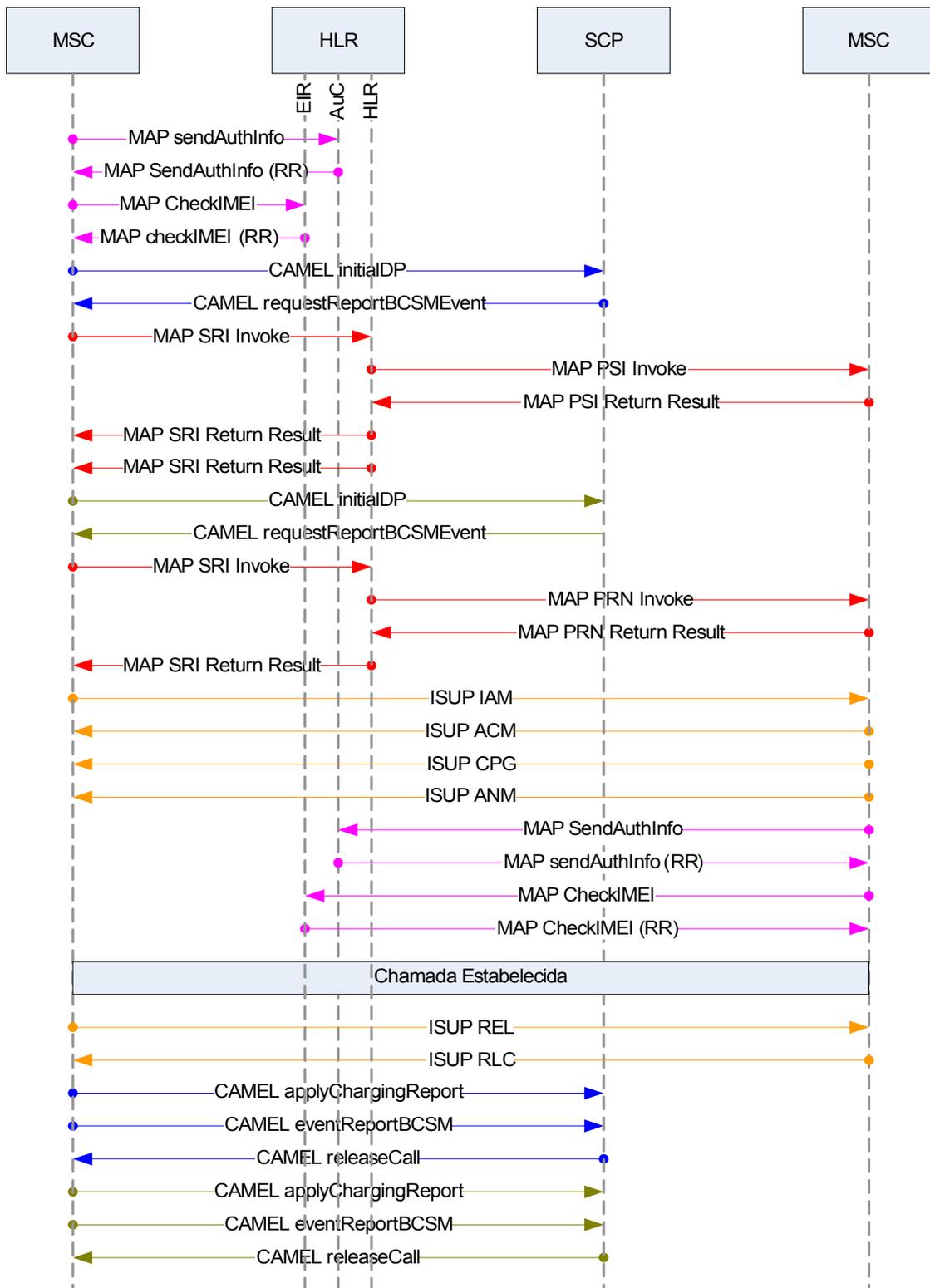


Figura 2.3 - Exemplo de troca de mensagens de sinalização em chamada móvel-móvel pré-pago

O primeiro conjunto de mensagens entre a MSC origem e o HLR envolve a busca de vetores de autenticação junto ao AuC, e a verificação do número de série do aparelho

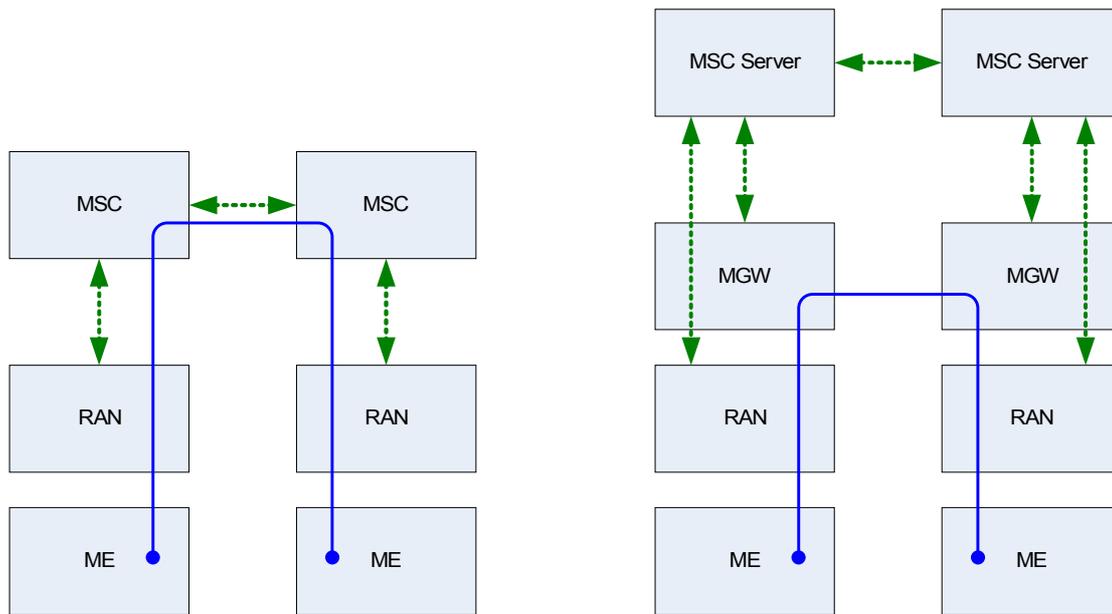
(IMEI) junto à lista negra do EIR. Então uma mensagem em protocolo CAMEL (*Customised Applications for Mobile networks Enhanced Logic*) solicita ao serviço pré-pago, executado no SCP, a autorização para continuidade da chamada. O conjunto de mensagens em protocolo MAP (*Mobile Application Part*) a seguir identifica para a MSC de origem a localização do número de destino, com a ajuda do HLR. Em seguida uma nova troca de mensagens CAMEL é feita, agora para validar a localização do número de destino e autorizar o completamento da chamada para o mesmo. Finalmente a central de origem, usando mensagens MAP via HLR, solicita à MSC de destino informações mais detalhadas para o completamento da chamada. Uma requisição de canal de voz entre as duas centrais é solicitada, via protocolo ISUP (*ISDN User Part*), pela central de origem à central de destino. Após o término da chamada, novas mensagens ISUP são trocadas entre os elementos para que os recursos de voz sejam liberados, neste caso por iniciativa da origem da chamada. Dois novos conjuntos de mensagens CAMEL são usados para informação ao serviço pré-pago que a chamada foi encerrada. Um conjunto para o número que iniciou a chamada e outro para o que a recebeu.

Após o estabelecimento da chamada, dependendo da configuração dos temporizadores, a MSC e o SCP continuam trocando mensagens, validando ou não a continuidade da chamada de acordo com as regras de serviço. Essa situação, porém não está representada.

Outros processos que incluem uma intensa troca de mensagens entre os elementos de rede são: (a) o registro inicial do cliente, ao ligar o telefone, (b) o processo de *handover* inter-MSC, quando o cliente em movimento passa da fronteira de atendimento de uma para outra MSC, (c) chamada terminada não completada com desvio para tratamento secundário (como caixa postal de voz).

Com o avanço das especificações 3GPP, e a entrada em operação de rede baseadas no 3GPP *Release 4*, a separação entre o plano de controle e o plano de usuário ficou ainda maior. Desta forma, procedimentos que anteriormente eram efetuadas dentro de um equipamento passaram a depender da rede de sinalização, e protocolos que anteriormente usavam enlaces dedicados passam a trafegar pela rede de sinalização. Um exemplo é a troca de sinalização indicada na Figura 2.4. Na rede em *release 99*, a MSC é responsável pelo processamento da voz e controle da rede de acesso (RAN – *Radio Access Network*). Já

na versão seguinte das especificações<sup>1</sup> – *release 4* – na nova topologia de rede a *MSC Server* passa a controlar os elementos *MGW* (*Media Gateway*) e *RAN*, sem que o tráfego de voz vindo do *ME* (*Mobile Equipment* – Equipamento Móvel) passe pela mesma. Essa configuração passa a gerar um tráfego maior na rede de sinalização, uma vez que troca de mensagens de controle que anteriormente ficavam dentro do próprio elemento agora passa a depender da rede de sinalização.



Fluxo de chamada em rede com Release 99

Fluxo de chamada em rede com Release 4

Figura 2.4 - Comparação de fluxo de mensagens segundo 3GPP *release 99* e 3GPP *release 4*

### 2.3. EXEMPLO DE INTERFACES 3GPP

Vários estudos de empresas pesquisa sobre o mercado de tecnologia têm previsto que a maior parte da receita dos serviços de telecomunicações virá dos serviços baseados em banda larga móvel. Atualmente o mercado de banda larga móvel utiliza redes baseadas no 3GPP, como UMTS (*Universal Mobile Telecommunications System* – Sistema de Comunicações Movel Universal) e HSPA (*High Speed Packet Access* – Acesso de Pacotes em Alta Velocidade). Prevê-se que, ao final de 2012 haverá 1,3 bilhões de conexões UMTS e HSPA, correspondendo a 78% do mercado de banda larga móvel mundial (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010).

<sup>1</sup> A sequência cronológica das especificações do 3GPP é Phase 1, Phase 2, release 96, release 97, release 98, release 99, release 4, release 5, etc. Após o release 99 decidiu-se que a numeração não deveria mais seguir o número do ano do seu lançamento, e o release 2000 passou a ser denominado release 4 (3GPP, 2010A).

Dentro das especificações do 3GPP, cada uma das interfaces entre os elementos é definida. Cada uma delas tem mensagens e funções específicas. A especificação 3GPP TS 23.002 (3GPP, 2010B) contém a descrição básica das interfaces, e os elementos que ela interliga. O resumo das interfaces, para uma rede GSM (*Global System for Mobile Communication*) / GPRS (*General Packet Radio Service*) básica está mostrada na Figura 2.5.

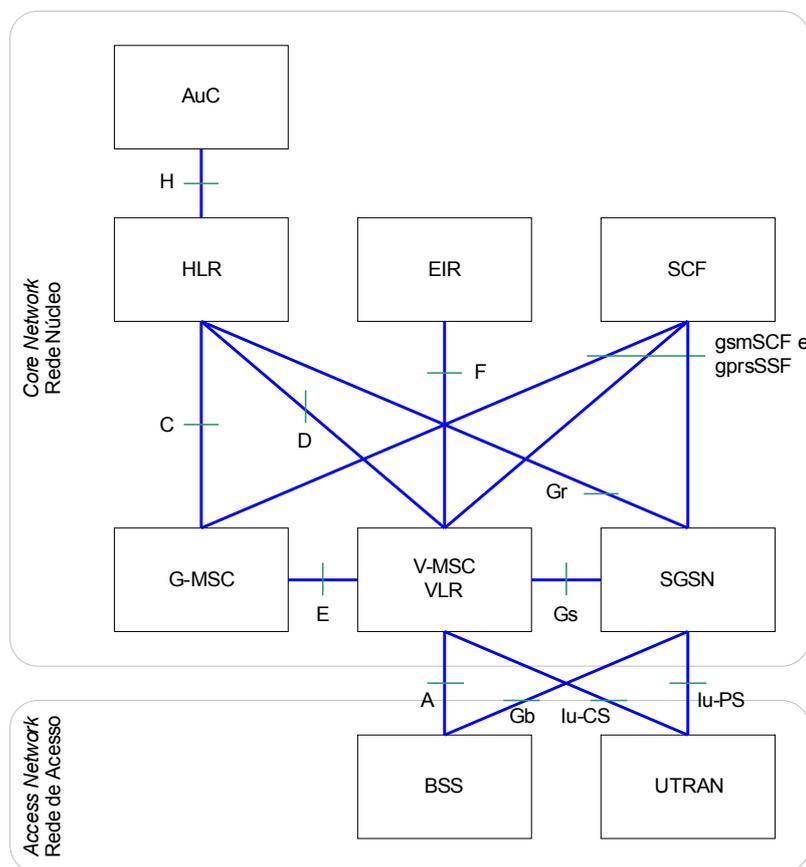


Figura 2.5 - Interfaces 3GPP para uma rede GSM / GPRS básica

Enquanto os elementos da Rede de Acesso (parte inferior da Figura 2.5) se comunicam basicamente com a MSC (*Mobile Switch Center*) e SGSN (*Serving GPRS Support Node*), existe uma interação muito grande entre os elementos da Rede Núcleo. Enquanto os elementos G-MSC (*Gateway – Mobile Switch Center*), V-MSC (*Visited Mobile Switching Center*) e SGSN fazem o controle das chamadas de voz e das sessões de dados, eles dependem de informações recebidas dos elementos HLR, EIR, AuC e SCF para tanto. Embora a MSC e o SGSN tenham as informações sobre roteamento do tráfego a ser processado, as informações relativas às permissões e serviço dos clientes ficam nos elementos HLR, EIR, AuC e SCF. Mesmo após o estabelecimento da chamada existe a troca de informações, tanto para garantir a tarifação correta do cliente, no caso do serviço pré-pago, como para garantir que o serviço do cliente não seja interrompido no caso de

deslocamento entre áreas atendidas por elementos de rede diferentes (*inter-MSCHandover*).

Cada uma destas interfaces é usada para troca de informações entre os elementos da rede. Dependendo do tamanho da rede envolvida, pode haver dezenas ou centenas de elementos de um único tipo. Uma rede de sinalização confiável é essencial para garantir que os serviços sejam prestados com qualidade para o cliente.

## 2.4. PILHA DE SINALIZAÇÃO

A pilha do protocolo SS7 é construído em forma de níveis. Cada um destes níveis tem sua função específica. O seu modelo, no entanto, não segue o modelo OSI (*Open Systems Interconnect*), uma vez que sua definição é anterior a esse modelo. Porém o seu funcionamento é muito similar, e há correspondência de funções, conforme indicado na Figura 2.6 (Russell, T., 2006) (Tanenbaum, Andrew S., 2003).

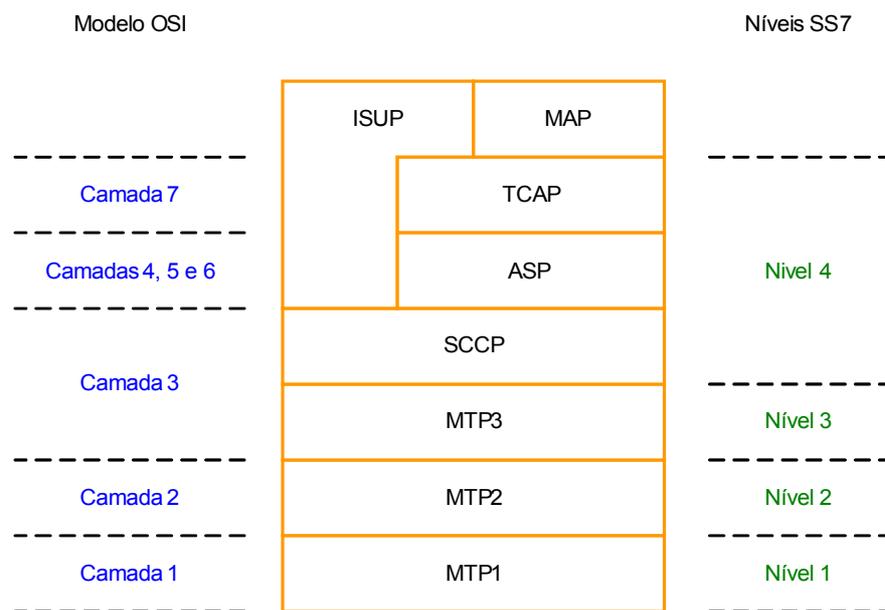


Figura 2.6 - Pilha SS7 e sua comparação com o modelo OSI

Os protocolos O protocolo MAP (*Mobile Application Part*) utiliza as camadas TCAP (*Transaction Capabilities Application Part*) e ASP (*Application Service Part*) sobre o SCCP (*Signaling Connection Control Part*), enquanto o ISUP (*ISDN User Part*) o faz diretamente. O protocolo de transferência de mensagens, MTP (*Message Transfer Part*), é

dividido em 3 níveis. No nível inferior, MTP1 (*Message Transfer Part Level 1*), é definido o enlace físico, tipicamente usando enlaces de 64 kbps ou 2 Mbps, conforme indicado no item 2.5. A camada MTP2 (*Message Transfer Part Level 2*) garante a transmissão entre dois nós adjacentes, implementando o controle de fluxo e checagem de erros. Em caso de falha, a mensagem é retransmitida.

A camada MTP3 (*Message Transfer Part Level 3*) prevê o roteamento entre os elementos de rede na rede SS7. Essa camada é responsável também pela implementação da redundância da rede, controlando possíveis enlaces com defeito ou congestionamento e reencaminhando o tráfego. A camada MTP3 é equivalente à camada de Rede da pilha de referência OSI. Dentro do SS7, a camada MTP-L3 é a mais alta, e é responsável por garantir a confiabilidade da transmissão dos dados, desta forma sendo o ponto onde é implementada a redundância de rede (Brunstrom, A., Grinnemo, K., 2005).

A camada ASP (*Application Service Part*), apesar de especificada, não é implementada na prática. Isso se deve à falta de serviços de sinalização orientados à conexão (Russell, T., 2006).

## **2.5. TECNOLOGIA USADA HOJE NAS REDES DE SINALIZAÇÃO E SUAS LIMITAÇÕES**

Com a evolução do *hardware* dos equipamentos, foi possível construir elementos de rede com capacidade cada vez maior. Isso é válido tanto para os elementos de rede de controle como para os elementos que efetivamente fazem o processamento do tráfego. As operadoras optaram, então, por concentrar o tráfego e o controle em uma quantidade menor de elementos de rede. Segundo (HP, 2010A), entre as vantagens da concentração dos elementos de rede de pequeno porte em poucos nós de grande porte estão:

- Redução do custo de operação pela menor quantidade de elementos a serem gerenciados;
- Redução de espaço físico;
- Redução de consumo de energia;

- Redução de impactos de paralisação durante as atividades de *upgrade* (quantidade menor de equipamentos a serem atualizados);
- Redução da quantidade de interfaces físicas, envolvendo requisitos menores de interfaces em PTS (Ponto de Transferência de Sinalização) e rede de sinalização;
- Redução da necessidade de recursos humanos dedicados e
- Gerenciamento simplificado da rede.

Apesar do risco de segurança que essa tendência gera, pela concentração do tráfego em alguns pontos específicos da rede, as operadoras e fornecedores passaram a trabalhar com poucos equipamentos de grande porte, ao invés de muitos equipamentos de pequeno porte. Atualmente há implementações comerciais de HLRs que suportam entre 8 e 12 milhões de registros em um único equipamento de rede (HP). Similarmente, há implementações comerciais de elementos de core de rede MSCs *Server* e MGWs, capazes de suportar, em um único nó, 7,5 milhões de chamadas em uma hora (BHCA – *busy hour call attempts*), sendo esse valor equivalente ao gerado, em média por 8 milhões de clientes. Um único MGW é capaz de processar até 80 kErl em um único gabinete (Ericsson, 2010).

Essa concentração de processamento se reflete diretamente nas redes de sinalização, uma vez que a troca de sinalização entre os elementos ficará concentrada em poucos nós, ao invés de distribuída entre diversos elementos de rede.

Por outro lado, a capacidade de transporte dos enlaces de sinalização baseados em circuito evoluiu pouco.

As redes de sinalização foram originalmente especificadas para usar os mesmos meios de transmissão que eram usados para o transporte de voz entre os elementos de rede. A transmissão de voz, quando efetuada por circuitos, utiliza-se de enlaces de 2 Mbps, sendo eles canalizados em 31 circuitos individuais de 64 kbps cada um. Para os protocolos que geram um tráfego de sinalização baixo - como o protocolo ISUP, por exemplo – esses enlaces são suficientes, considerando ainda a capacidade de agrupamento dos mesmos em até 16 enlaces paralelos. Com essa configuração, e usando-se os fatores de proteção apropriados (80% de ocupação máxima dos enlaces em modo de falha, com redundância

efetuada por dois caminhos diferentes), temos um tráfego máximo suportado de 409,6 kbps. Este dimensionamento está descrito no Anexo C. Apesar de suficiente para redes pequenas, esses valores não são adequados para redes de grande porte.

Passou-se então, a utilizar-se do enlace de 2 Mbps inteiro para troca de sinalização, de acordo com o definido pelo ITU-T na especificação Q.703 anexo A (ITU-T 1996). Desta forma ganhou-se em capacidade, já que o enlace de 2 Mbps é considerado um único enlace, podendo ainda ser agrupado em 16 enlaces, totalizando 32 Mbps de capacidade máxima. Utilizando-se as mesmas restrições de segurança e redundância podemos chegar a um valor máximo, para o conjunto de enlaces, de 12,8 Mbps.

Apesar de ser um valor bem mais alto do que o suportado pelos enlaces de 64 kbps, os enlaces de 2 Mbps ainda não são adequados para todo o tamanho de equipamento. Junte-se a isso a necessidade de acompanhamento constante do tráfego nos enlaces, a avaliação da distribuição de carga entre os mesmos e a potencial dificuldade na obtenção de transmissão de um circuito entre os elementos envolvidos.

Assim, com as limitações existentes no crescimento dos enlaces de sinalização, surge a necessidade de migrar o transporte de sinalização, de redes baseadas em circuitos, para redes baseadas em pacotes.

## **2.6. O USO DE REDE DE PACOTES PARA SINALIZAÇÃO**

Apesar de, atualmente, boa parte das redes de telecomunicações ser baseada no uso de circuitos comutados, o núcleo das novas redes de telecomunicações será totalmente baseado em redes IP (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010) .

Considere-se também o fato de que as redes das operadoras de telecomunicações têm evoluído para prestar serviços baseados em IP, como acesso à Internet. Com as limitações existentes na topologia convencional de transporte de sinalização via circuitos convencionais e o crescimento das redes de pacotes, especialmente as redes IP, a demanda por uma solução de transporte de sinalização que pudesse ser feito através de redes IP se tornou grande. Existem estudos que indicam a possibilidade de redução do custo de transporte de sinalização entre 40% e 70% pelo uso de redes IP (Chukarin, A., Pershakov, N., Samouylov, K., 2007).

Segundo (Pfützenreuter, E., 2004), entre os motivos fortes da integração das redes SS7 e IP, estão:

- acesso facilitado de serviços entre as duas redes;
- redução de custos de serviços, pelo uso de redes IP;
- integração de dispositivos de telecomunicação à Internet;
- alternativa de conectividade onde somente a rede IP esteja disponível.

## **2.7. REDE DE SINALIZAÇÃO VIA IP**

A maior demanda pelo uso do transporte de sinalização via redes IP veio das redes usadas para o serviço móvel. Um dos motivadores é o fato de estas redes já serem, por definição, distribuídas, o que faz com que um único evento de rede – uma chamada, por exemplo – gere uma troca de sinalização entre vários elementos de rede. A rede fixa, por outro lado, tem uma necessidade menor de novos serviços, o que faz com que a demanda de sinalização seja bem atendida pelas redes de sinalização baseadas em circuito. O último grande serviço implantado na rede fixa que trouxe uma demanda de sinalização adicional foi a portabilidade numérica.

Apesar das vantagens demonstradas pela rede IP no transporte da sinalização, deve-se entender que estas redes têm características bem distintas.

Segundo (Pfützenreuter, E., 2004), entre as principais diferenças entre uma rede SS7 baseada em circuitos e uma rede de pacotes como o TCP/IP estão:

- O SS7 considera que a camada física é confiável, ou que haja um protocolo nas camadas inferiores que garanta essa confiabilidade;
- As mensagens não ultrapassam o tamanho dos datagramas;
- Suporte nativo a enlaces redundantes, com notificação para as aplicações das mudanças desde enlaces;

- Rede com parâmetros estáveis, em relação à desempenho, latência, caminho utilizado entre dois pontos, etc.
- Componentes de rede com inteligência relativamente alta;
- A troca de mensagens feita entre equipamentos e não entre usuários do serviço.

Além disso, deve-se considerar que é necessário construir uma pilha de protocolos que permita que ambas as formas de transporte de sinalização – via circuitos e via rede IP – possam interoperar de forma transparente. Isso é necessário, porque os sistemas atuais não serão substituídos rapidamente. Apesar do avanço em direção ao IP, haverá um longo tempo de transição entre a telefonia baseada em circuitos e a telefonia baseada em IP. Estima-se que haja U\$350 bilhões de equipamentos de redes de telecomunicações baseados em recursos de sinalização de circuitos instalados nas redes ao redor do mundo (Brunstrom, A., Grinnemo, K., 2005). Assim, o grupo de trabalho SIGTRAN do IETF desenvolveu uma arquitetura que é capaz de funcionar de forma conjunta com as redes baseadas em circuitos .

## **2.8. GRUPO DE TRABALHO SIGTRAN**

Devido a esses motivadores, buscou-se utilizar a rede IP para transporte da sinalização das redes de telecomunicações. Em 1998 o ITU formou um comitê, chamado SIGTRAN (*Signalling Transport*) para escolher ou criar um protocolo para atender a essa necessidade (Pfützenreuter, E., 2004).

Inicialmente procurou-se utilizar o próprio TCP ou melhorá-lo, porém essa opção mostrou-se inadequada em função das grandes alterações que deveriam ser feitas no TCP, principalmente devido ao fato de delegar à aplicação a função de separação das mensagens.

Um dos problemas do TCP é que ele é um protocolo orientado a bytes, que força as aplicações a inserirem seu próprios cabeçalhos, caso se deseje enviar mensagens de forma isolada. Esse modo de trabalho do TCP faz com que os pacotes sempre tenham que ser entregues de forma sequencial. Com isso, caso um pacote seja perdido, deve-se aguardar a chegada do pacote retransmitido para que toda a informação seja entregue para a aplicação (Brunstrom, A., Hurtig, P., 2008).

A segunda opção foi a criação de um protocolo operando sobre UDP, o chamado CTP (*Common Transport Protocol*). Seus requisitos eram:

- Servir como transporte para os protocolos de mensagens de telefonia;
- Suportar extensões facilmente;
- Atuar como um serviço confirmado, mesmo sob condições severas de congestionamento;
- Tolerância a falhas pelo uso de caminhos redundantes de rede, notificando as camadas superiores do estado da rede;
- Segurança e autenticação;
- Tempos de time-out e parâmetros de retransmissão configuráveis pela aplicação;
- Compartilhamento de várias instâncias de aplicação em um única instância de transporte, com garantia de ordenamento;
- Transporte de mensagens maiores que o MTU do caminho.

Após essas definições, foram apresentadas algumas propostas:

- UDP for TCAP (T/UDP) (Ma, G., 1998), *Simple SCCP Tunneling Protocol* (SSTP) (Garcia, M., Sanchez, D., 1998);
- *Reliable Transport Extensions To UDP* (PURDET) (Toney, K., 1999)

Também foram considerados protocolos já existentes:

- *Service Specific Connection-Oriented Protocol* (SCOP) (ITU-T, 1994A);
- H.323 Anexo E (ITU-T, 2009); e

- *Real Time Protocol* (RTP) (Schulzrinne, H., et al, 1996).

Paralelamente, e sem relação com o trabalho do comitê SIGTRAN, foi apresentado ao IETF a proposta de um novo protocolo, o MDTP (Multi-Network Datagram Transmission Protocol), por Randall R. Stewart e Qiabing Xie (Stewart R, Xie Q, 1999). O objetivo inicial deste protocolo era resolver algumas das deficiências conhecidas do TCP. O MDTP operava como um protocolo de aplicação, sobre UDP mas atendia a praticamente todos os requisitos do TCP com uma vantagem: já havia uma implementação de testes disponível, com protocolo muito equivalente ao TCP.

Assim, o MDTP foi sendo preparado e elaborado, culminando no desenvolvimento do SCTP (*Stream Control Transmission Protocol*) disponível atualmente. Observe-se, no entanto, que o SCTP não foi criado somente para uso pela pilha SIGTRAN, e tem seu uso indicado para quaisquer protocolos que tenham requisitos equivalentes ao SS7, e procuram rodar sobre IP.

## **2.9. USOS ATUAIS DA PILHA SIGTRAN**

Usando a mesma rede exemplo do item 2.3, observamos na Figura 2.7 quais as interfaces de rede que foram especificadas para rodar sobre redes IP, e que podem fazer uso da pilha SIGTRAN.

Observe-se que todas as interfaces dentro do *Core Network*, e algumas interfaces na rede de acesso podem usar a rede IP para o seu transporte, uma vez que foram especificadas para uso da sinalização SS7.

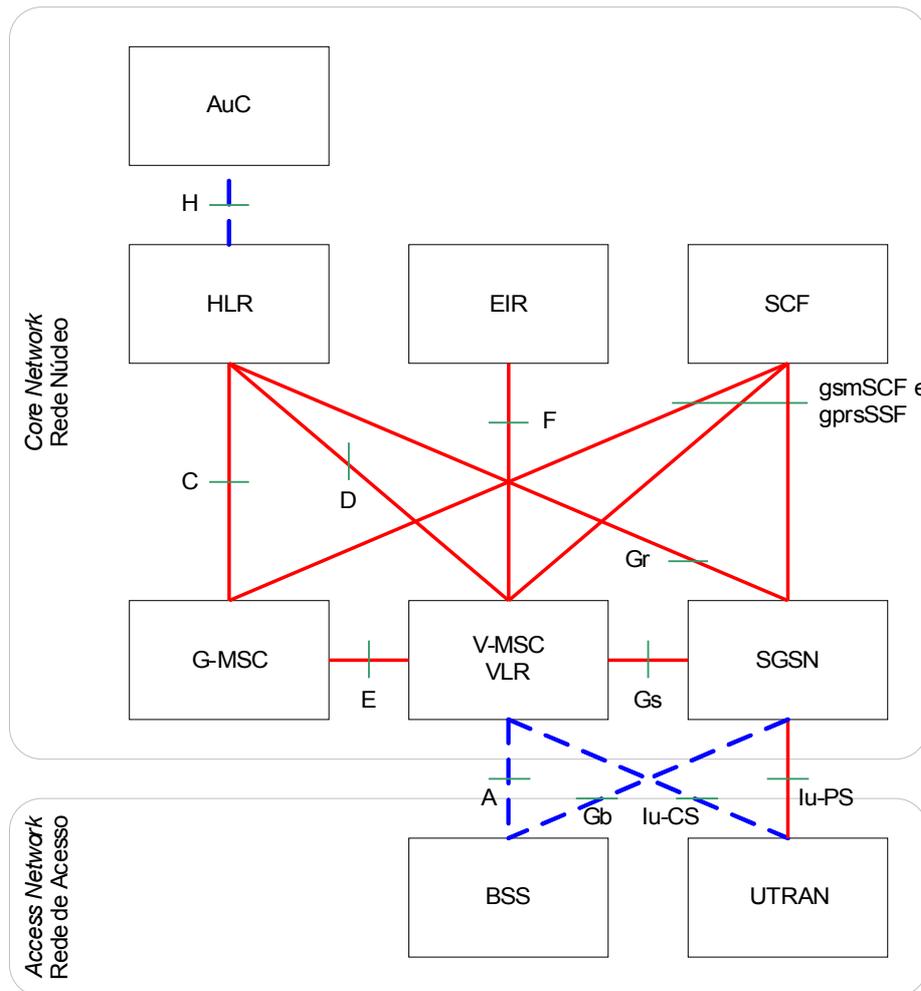


Figura 2.7 - Interfaces de uma rede GSM / GPRS básica que podem ser transportadas pela pilha SIGTRAN

No caso das redes LTE (*Long Term Evolution*), que ainda estão em fase de especificação, todas as suas interfaces já foram especificadas para transporte via rede IP. O LTE está descrito na série 36 das especificações 3GPP, e as suas interfaces estão indicadas na 3GPP TS 23.002 V9.3. (3GPP, 2010B) Um diagrama destas interfaces está indicado na Figura 2.8. O E-NB (*Enhanced Node B*), que é o elemento de acesso, recebe o tráfego da ME (*Mobile Equipment* – Estação Móvel), e se comunicam com o SGW para tráfego e MME (*Mobility Management Entity*) para controle. Os dados dos clientes estão no HSS (*Home Subscriber Server*), enquanto o controle do tráfego é feito pelo PDN-Gateway (*Packet Data Network Gateway*), baseado nas informações recebidas do PCRF (*Policy charging and rules function*). O tráfego, então, é entregue aos serviços IP da operadora, o IMS (*IP Multimedia Subsystem*), por exemplo.

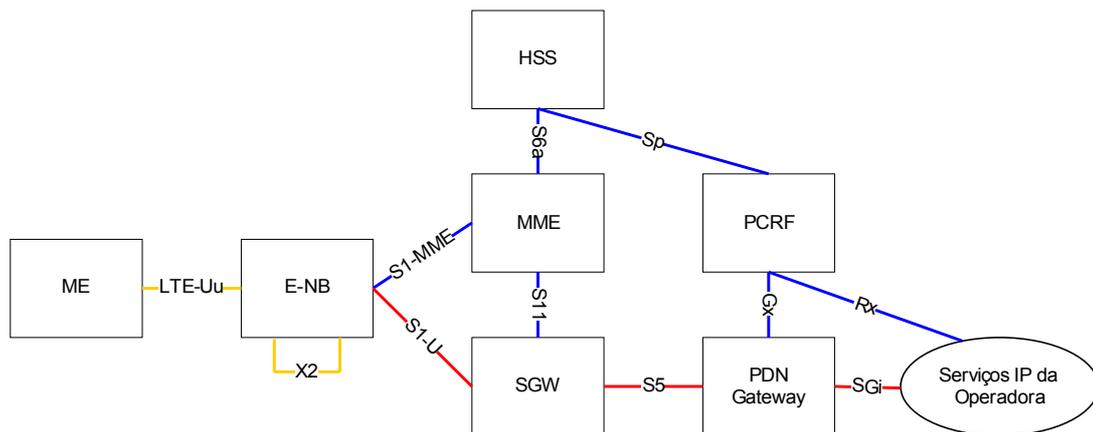


Figura 2.8 - Interfaces 3GPP especificadas para LTE, conforme 3GPP 23.401 V9.3 (3GPP, 2010C)

## 2.10. REQUISITOS PARA O SIGTRAN

Para que a pilha de protocolos pelo SIGTRAN tenha aceitação para uso nas redes de telecomunicações, uma rede usando esses protocolos deve ter um desempenho igual ou superior ao das redes de telecomunicações baseadas em circuitos. Especificamente, ela deve ter o mesmo grau de disponibilidade de uma rede SS7 convencional. Considerando que o ITU-T exige um grau de disponibilidade de 99,9988%, isso significa que uma rede não deve ficar indisponível mais de 10 minutos em um ano, o que é um grande desafio (Brunstrom, A., Grinnemo, K., 2005).

É comum que um enlace SS7 corretamente configurado funcione durante anos seguidos sem que haja desconexão, sendo desligado somente durante processos de atualização de versão de *software* do elemento de rede envolvido.

### 2.10.1. Atraso máximo

A temporização é um fator muito importante em redes de sinalização para sistemas de telecomunicações. Como mostrado no exemplo do item 2.2. , uma única chamada de voz gera uma quantidade grande de mensagens de rede e cada uma delas tem a sua função e relevância dentro do processamento da sessão.

Caso uma das chamadas se perca, haverá problemas, ou completamento da chamada, ou na sua tarifação, ou no seu encerramento. Somente no processo de inicialização da chamada estão envolvidas 25 mensagens em 7 processos e 5 protocolos diferentes. Todo o processo

é necessário para que a chamada se complete. É necessário, portanto, que toda essa troca de mensagens ocorra em um tempo bastante curto, de forma que o cliente não seja afetado. No exemplo acima, o tempo de processamento de cada elemento de rede pode ser medido na faixa dos 40 ms.

Considere-se o exemplo a seguir: uma MSC trabalhando com 1 milhão BHCA (*Busy Hour Call Attempts* – Tentativas de Chamada na Hora de Maior Movimento) irá tratar cerca de 280 tentativas de chamadas por segundo. Com esse dimensionamento, supõe-se que ela tenha, por exemplo, a sua área de memória configurada para suportar até 600 tentativas de chamada. Nessa memória a central irá manter os dados temporários da troca de sinalização entre os elementos de rede, enquanto a chamada não é estabelecida.

Se a rede de sinalização sofrer uma falha, e a central levar 10 segundos para comutar para o caminho de sinalização reserva, haverá 2800 tentativas de chamadas consumindo recursos de memória. Essa sobrecarga de sinalização sem resposta leva muitos equipamentos de rede a uma falha total.

Deve-se, portanto, configurar os elementos envolvidos em sinalização para que tenham sempre uma visão atualizada do estado da rede. Ainda no exemplo acima, se a comutação para o caminho reserva foi feita em um segundo após a falha, a central teria que suportar a sinalização apenas de 560 tentativas de chamada. Outra possibilidade é que a central receba da rede de sinalização a informação de que efetivamente o outro elemento está indisponível. Com essa informação a central passará a recusar novas tentativas de chamada, preservando a integridade de seus recursos até que a sinalização volte a ser restabelecida.

Desta forma, o principal requisito para uma rede de sinalização é o atraso mínimo no transporte das informações entre os elementos de rede, mesmo em caso de falha. Outro requisito considerado importante é a rápida detecção de uma falha de rede pelo elemento de rede.

De acordo com a recomendação Q.706 do ITU-T (ITU-T, 1994B), espera-se que o tempo de comutação de uma rede SS7 seja sempre menor ou igual a 800 ms (Jungmaier, A., Rathgeb, E. P., 2006). Considerando-se que as mesmas aplicações que rodam sobre redes baseadas em circuito são as que atualmente se utilizam do SIGTRAN, os requisitos

continuam sendo os mesmos (Brunstrom, A., Grinnemo, K., 2005).

### **2.10.2. Redundância**

O conceito de redundância está presente em todos os equipamentos das redes de telecomunicações. Usa-se os termos *carrier grade* ou *carrier class* para definir os equipamentos e sistemas que são desenvolvidos para atingir o nível de desempenho solicitado pelas operadoras. Esse nível não é atingido por um único equipamento, o que faz necessário o uso de mais de um equipamento ou recurso em paralelo, através do recurso da redundância (Immonen, M., 2005).

A redundância exige que haja sempre um recurso alternativo para o atendimento ao serviço, em caso de falha no primeiro. Aplicando-se esse conceito para redes de sinalização, deve-se garantir que haja sempre um caminho alternativo para garantir que uma mensagem de sinalização seja entregue ao elemento de destino, em caso de falha no primeiro. Assim, esse conceito é aplicado pelo uso de enlaces de sinalização que usem equipamentos e meios de transmissão independentes. Ao levar o transporte da sinalização para as redes IP, deve-se avaliar as formas disponíveis de se implementar a redundância.

As redes de transmissão e as redes IP têm seus próprios mecanismos de segurança (Rembarz, R., 2004). A rede de transmissão tem também mecanismos de redundância física. Porém os melhores resultados são obtidos quando esses métodos são utilizados em conjunto com a redundância proporcionada pelo SCTP (Rembarz, R., Baucke, S., Mahonen, P., 2005).

## **2.11. CONCLUSÕES**

Observa-se a grande relevância das redes de sinalização para o funcionamento adequado e otimizado das redes de telecomunicações. Ainda que o tráfego de sinalização seja pequeno em comparação com o tráfego do serviço em si (seja ele voz, dados ou vídeo), o desempenho da rede para atender a esse tráfego é uma questão que deve sempre ser levada em conta. Como, para uma única sessão, há uma troca intensa de mensagens de sinalização entre os elementos envolvidos, a rede de sinalização deve ter características de confiabilidade bastante restritas. A rede de transporte, sobre a qual a rede de sinalização é construída, era originalmente feita através de circuitos dedicados, mas uma evolução para o

transporte sobre redes de pacotes é essencial para que garantir o crescimento do tráfego. Deve-se, porém, garantir que a rede de pacotes consiga atender aos requisitos de qualidade exigidos pelo tráfego de sinalização.

Com a necessidade do uso de redes de pacotes para o transporte da sinalização, foi avaliada a viabilidade do uso dos protocolos existentes, de forma a garantir a qualidade necessária para as aplicações envolvidas, nas camadas superiores. Os protocolos existentes, especificamente o TCP e UDP mostraram-se incapazes de atender aos requisitos solicitados, especialmente no tratamento de falhas de rede. Assim, somente com um novo protocolo, no caso, o SCTP junto com as camadas de adaptação previstas, foi capaz de atender aos requisitos impostos.

No próximo capítulo avaliaremos as pilha SIGTRAN, e as camadas que o compõe, dando especial atenção ao protocolo SCTP. Avaliaremos os seus recursos de segurança, olhando com mais detalhes a forma como o mesmo implementa a redundância de caminhos. Avaliaremos também os seus parâmetros configuráveis, e qual a função de cada um.

### 3. A PILHA SIGTRAN

Existe mais de uma forma de se implementar a pilha SIGTRAN. A Figura 3.1 mostra a pilha SS7 em comparação com as implementações possíveis da pilha SIGTRAN.

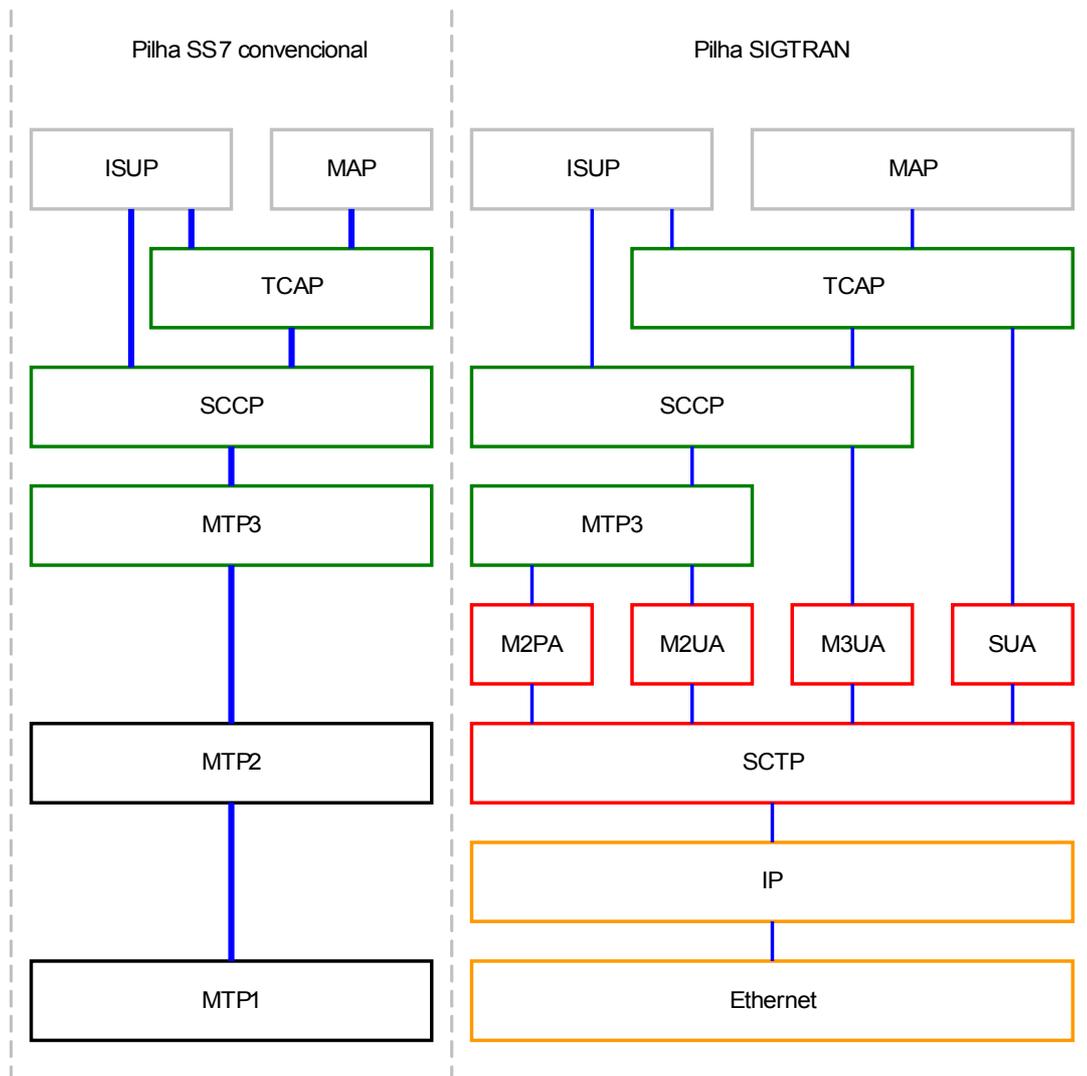


Figura 3.1 - Comparação entre pilha de sinalização SS7 convencional e SIGTRAN

Para garantir o inter-funcionamento entre sistemas de sinalização baseados em circuito e os baseados em IP, foram especificadas várias camadas de adaptação, sendo hoje a mais utilizada a que usa o *MTP-L3 User Adaptation Layer* (M3UA). Essa camada faz o papel da camada MTP3 para as aplicações superiores, interoperando com o Sctp nas camadas inferiores. Assim, é possível que as camadas superiores da pilha de sinalização possam

trabalhar de forma transparente às camadas inferiores, sejam elas baseadas em circuito ou em IP (Brunstrom, A., Grinnemo, K., 2005) e (Pfützenreuter, E., 2004).

Outra camada de sinalização definida é o M2PA (*MTP2 Peer-toPeer Adaptation Layer*), que é usada no caso de enlaces utilizados para interligar duas redes de sinalização.

Existem ainda outras possibilidades, como o M2UA (*MTP2 User Adaptation Layer*), porém eles são utilizados em aplicações específicas, e portanto não são os mais adequados para a substituição das redes de sinalização baseadas em circuitos (GSM Association). No caso específico do SUA (*SCCP User Adaptation*), a falta do suporte ao SCCP não permite que seja usado para a sinalização ISUP (*ISDN User Part*), inviabilizando o seu uso em interconexões que utilizam esse protocolo. Essa característica também o torna inadequado para substituição de sinalização existente. Desta forma, a sua aplicação é mais voltada para novos serviços ou para uso em elementos como bases de dados, onde não é requerido o processamento de voz. É o caso do uso em HLRs e SCPs.

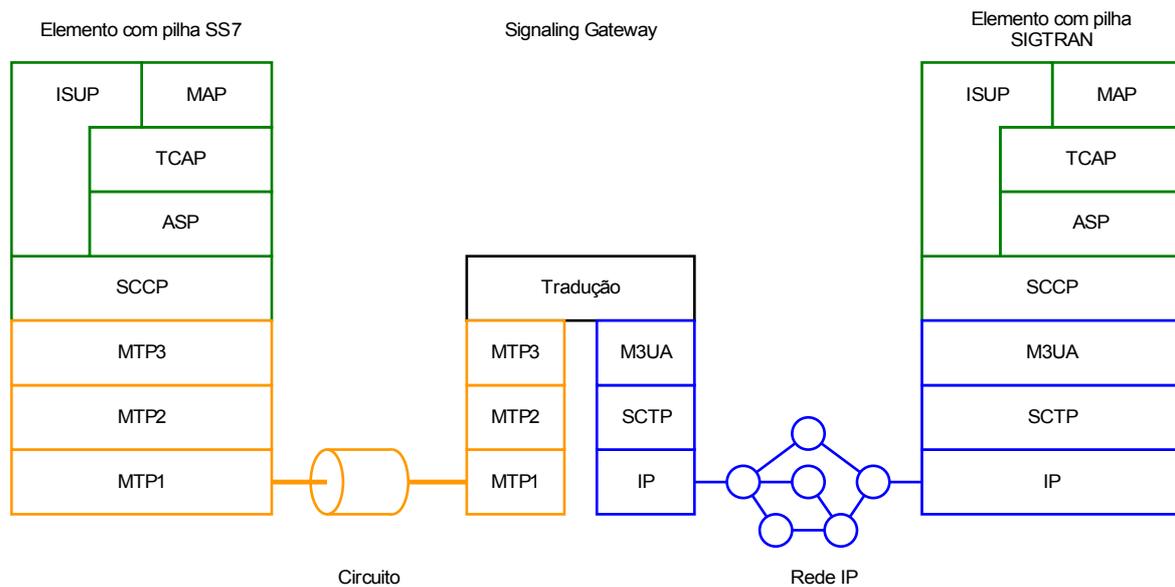


Figura 3.2 - Pilhas SS7 e SIGTRAN conectadas através de um *signaling gateway* (Immonen, M., 2005)

Em seu trabalho, (Pfützenreuter, E., 2004) lembra que a implementação usada pelo SIGTRAN permite o uso de um equipamentos chamado *signaling gateway*, que é capaz de intermediar a troca de sinalização entre equipamentos capazes de operar somente com SS7 puros e SS7/IP. O uso de um *signaling gateway* é transparente para as aplicações,

permitindo que elementos com pilhas de sinalização diferentes possam trocar mensagens sem conhecer ou ser influenciado pela estrutura da pilha do outro elemento de rede (Immonen, M., 2005). A Figura 3.2 mostra as pilhas de protocolos usadas, e o *signaling gateway* efetuando as adaptações necessárias para o transporte transparente da sinalização.

Complementarmente, o SCTP é adequado para qualquer troca de sinalização em redes de telecomunicações, sejam mensagens de sinalização SS7 ou outras, como o DIAMETER, descrito na RFC 3558 (Calhoun, P., Loughney, J., et al, 2003) e interfaces 3GPP.

### **3.1. O PROTOCOLO SCTP**

Na apresentação do protocolo SCTP, na RFC 2960 (Stewart, R., Xie, Q., Morneault, K. et al., 2000), (Pfützenreuter, E., 2004), (Costa, Daniel Gouveia, 2005), o mesmo é apresentado como sendo um protocolo de transporte confiável, como o TCP, mas com funcionalidades adicionais:

- Entrega confirmada de dados de usuário, livre de erros e de duplicação de dados de usuário;
- Fragmentação de dados em conformidade com o MTU (*Maximum Transmission Unit*) descoberto do caminho;
- Entrega sequencial de mensagens de usuário em múltiplos fluxos, com opção para entrega por ordem de chegada de mensagens de usuário individuais;
- Empacotamento opcional de múltiplas mensagens de usuário em um único pacote SCTP; e
- Tolerância a falhas de rede através do suporte a múltiplos caminhos.

### **3.2. COMPARAÇÃO TCP, UDP E SCTP**

Na avaliação de um protocolo adequado para uso no transporte da sinalização, deve-se comparar as facilidades dos três principais protocolos disponíveis para rede IP: TCP, UDP e SCTP. O trabalho de (Costa, D., 2005) propõe a Tabela 3.1, onde são comparadas as

facilidades e recursos dos três protocolos. Destaque-se a vantagem do SCTP em relação aos outros protocolos no que se refere à orientação a transmissão voltada para mensagens, essencial para o transporte de sinalização, a possibilidade de envio de mensagens não ordenadas, e a tolerância a falhas, implementada pelo uso de múltiplos fluxos e múltiplos caminhos.

Tabela 3.1 - Comparação entre SCTP, TCP e UDP, conforme (Costa, D., 2005)

Característica	SCTP	TCP	UDP
Confiabilidade	Sim	Sim	Não
Orientado a conexão	Sim	Sim	Não
Orientação da transmissão	Mensagem	Octeto	Mensagem
Controle de fluxo	Sim	Sim	Não
Controle de congestionamento	Sim	Sim	Não
Tolerância a falhas	Sim	Não	Não
Distribuição de Dados	Parcialmente ordenada	Ordenada	Desordenado
Múltiplos Fluxos	Sim	Não	Não
Múltiplos Caminhos	Sim	Não	Não

Já em (Stewart, R., Xie, Q., 2001) encontramos, na comparação entre o SCTP com o TCP diferenças na inicialização, efeito do bloqueio Head-of-Line, limites das mensagens, confirmação Seletiva, uso do multi-homing, procedimento de fechamento e possibilidade de uso de extensões no protocolo.

### 3.2.1. Diferenças na inicialização

A inicialização um uma sessão usando protocolo TCP utiliza um *handshake* de 3 mensagens, enquanto o SCTP utiliza-se de 4 mensagens. O protocolo UDP não é orientado à conexão, e o conceito de inicialização da sessão não se aplica.

À primeira vista o uso de 3 mensagens de inicialização pode parecer uma vantagem contra 4 mensagens, porém deve-se notar que o envio da terceira mensagem de inicialização já pode conter os primeiros dados da sessão, o que faz com que o SCTP tenha uma inicialização mais rápida. Além disso, o uso de 4 mensagens gera uma proteção contra ataques *SYN flood* (inundação de mensagens SYN), uma vez que o *endpoint* que recebe a

mensagem INIT não reserva recursos ao enviar a mensagem INIT-ACK de retorno (Stewart, R., Xie, Q., 2001). Ou seja, o *endpoint* de destino não cria um TCB (*transmission control block*) para guardar as informações da provável associação em criação. Ao contrário, gera as informações necessárias, mas as envia de volta ao *endpoint* de origem da mensagem INIT, dentro da mensagem INIT-ACK (Stewart, R., Xie, Q., 2001).

### **3.2.2. Bloqueio *Head-of-Line***

Em uma conexão TCP convencional, os pacotes transmitidos da origem em direção ao destino são entregues sempre de forma sequencial. No caso de tráfego alto, a perda de um pacote faz com que todo o fluxo de entrega de informações para a aplicação do destino seja atrasado, para que se aguarde a retransmissão do pacote perdido, mesmo que pacotes subsequentes já tenham sido entregues ao destino. Essa situação é chamada de *head-of-line blocking*.

O SCTP permite, opcionalmente, que os pacotes sejam entregues para a aplicação de destino mesmo fora de ordem, caso haja essa solicitação.

Há também o conceito de múltiplos *streams*, que são fluxos de dados independentes dentro de uma mesma associação SCTP. Caso haja a opção por entrega ordenada, uma perda de pacotes em um dos fluxos não interrompe o tráfego do outro fluxo, sendo que apenas o primeiro fluxo terá que aguardar a retransmissão do pacote perdido.

### **3.2.3. Limites das mensagens**

O SCTP, em comparação ao TCP, permite que as mensagens sejam enviadas com seus limites bem definidos. O TCP simplesmente cria um fluxo de dados, cabendo a camada superior identificar o início e o fim de cada mensagem. Ainda assim será necessário incluir na mensagem informações, no mínimo, sobre o seu comprimento. Com a orientação a mensagens, o SCTP facilita esse processo, especialmente no caso do transporte de mensagens de sinalização para redes de telecomunicações.

### **3.2.4. Confirmação Seletiva**

A confirmação seletiva existe em algumas implementações do TCP, mas é nativa no SCTP.

Esse recurso permite que o elemento de destino reporte à origem a perda de alguns pacotes, indicando especificamente quais devem ser retransmitidos. Comparando a implementação nativa do SCTP com a opcional do TCP, a primeira é ainda melhor, pois permite que uma quantidade indefinida de pacotes sejam solicitados à retransmissão com apenas uma notificação. O TCP limita essa requisição a somente 4 pacotes. No SCTP, a quantidade é limitada pelo tamanho da mensagem de retransmissão que cabe no PMTU (*Path Maximum Transmission Unit*).

### **3.2.5. Multi-homing**

O SCTP permite, nativamente, o uso de múltiplos caminhos para o transporte das mensagens entre os dois elementos de rede, criando uma condição de redundância, onde o tráfego é passado de um caminho primário para um caminho alternativo em caso de falha. Esse recurso será explicado com detalhes no item 3.3.

### **3.2.6. Procedimento de fechamento**

O recurso chamado de *half-closed* usado pelo TCP não foi implementado no SCTP. Como argumento, os autores da RFC indicam o baixo uso desta facilidade em comparação com a complexidade de sua implementação.

Em ambientes de redes de sinalização para telecomunicações não há necessidade de procedimentos específicos para término da conexão, já que elas são estabelecidas e assim permanecem indefinidamente.

### **3.2.7. Extensões do protocolo**

O protocolo SCTP é facilmente extensível. Com isso garante-se que ele possa evoluir de uma forma rápida, sem que para isso haja perda de compatibilidade com versões anteriores. (Pfützenreuter, E., 2004) cita as principais extensões propostas ao protocolo. Entre elas estão:

- Confirmação parcial – nessa implementação define-se se a mensagem enviada por um fluxo deve ou não ser retransmitida em caso de perda de pacotes ou atraso grande;

- Criação de fluxos sob demanda – permite negociação da quantidade de fluxos entre os *endpoints* após o estabelecimento da associação;
- Estado *half-closed* para associações – implementação similar à existente no TCP;
- Balanceamento de carga – permite que haja tráfego entre os vários caminhos definidos entre os *endpoints*, e não apenas no caminho primário.

Apesar destas facilidades, por uma questão de compatibilidade, a pilha SIGTRAN implementa apenas as funcionalidades originais do SCTP, sem extensões.

### **3.3. ASPECTOS DE REDUNDÂNCIA**

Conforme apresentado no item 2.10.2. , o conceito de redundância é essencial para o transporte da sinalização em redes de telecomunicações. Uma das formas principais de implementar esse recurso no SCTP é através do conceito de *multi-homing*, ou múltiplos caminhos.

#### **3.3.1. Conceito de IP *multi-homing***

No caso de rede IP, existe o conceito de IP *multi-homing*, ou multi-caminhos. Por esse conceito, um elemento de rede pode ser acessado por mais de um endereço IP de forma transparente. Segundo (Stewart, R., Xie, Q., 2001) isso pode ser feito de duas formas:

- Pelo uso de múltiplas interfaces de rede, cada uma com seu próprio endereço IP ou;
- Uma única interface de rede que pode receber, simultaneamente, mais de um endereço IP.

Apesar de a segunda forma ser tecnicamente possível, ela não implementa de forma adequada o conceito de redundância, pois com o uso de uma única interface de rede com vários endereços IP perde-se parte do conceito, uma vez que, no caminho entre os elementos de rede envolvidos, há um ponto de falha único.

### **3.3.2. *Multi-homing* x *single homing***

A RFC2960 (Stewart, R., Xie, Q., Morneault, K. et al., 2000) diz que um elemento é considerado *multi-homed* se existe mais de um endereço de transporte que pode ser usado como endereço de destino para se atingir esse *endpoint*. Esse é um grande diferencial do protocolo SCTP em relação ao TCP e UDP.

Com esse recurso, também chamado de multi-caminhos, a troca de mensagens entre os dois elementos de rede pode ser feita por dois ou mais caminhos dentro da rede, garantindo uma maior tolerância a falhas e, por consequência, a continuidade do serviço.

Embora as implementações usadas na prática, e também nesse trabalho, normalmente se limitem a um caminho principal e um alternativo, isso é uma redução do conceito mais completo, que indica apenas a possibilidade do uso de vários caminhos distintos, podendo-se, inclusive, utilizar-se de divisão de carga entre eles. Também não há, no conceito de *multi-homing*, a necessidade de o mesmo número de endereços nos dois elementos de rede. Pode-se em tese, utilizar-se de dois endereços em um lado e três endereços do outro lado. Outra facilidade que pode ser usada é a de que o *endpoint*, através da observação da rede, decida qual caminho deve ser usado como primário de forma dinâmica, sempre garantindo o desempenho otimizado na entrega das mensagens.

Em redes típicas de telecomunicações, utiliza-se dois caminhos distintos, sendo um primário e um alternativo. A especificação do SCTP não define o balanceamento de carga entre múltiplos caminhos. Para esse fim foram propostas extensões (Pfützenreuter, E., 2004), (Jungmaier, A., Rathgeb, E. P., 2006), (Jungmaier, A., Rathgeb, E. P., 2005). Nesta implementação, a transmissão de pacotes é feita por todos os endereços IP definidos no destino, e não apenas para o endereço primário. Assim, todos os enlaces são utilizados o tempo todo, potencialmente aumentando a vazão. Existe, porém, uma forma de se efetuar a divisão de carga entre os múltiplos caminhos sem que seja necessário o uso de extensões no protocolo. Essa forma será descrita nas seções seguintes.

### **3.3.3. Topologia para uso do *multi-homing***

Para que a facilidade *multi-homing* tenha sua eficiência garantida, é necessário que cada endereço do *endpoint* se utilize de um caminho para acesso ao *endpoint* de destino o mais

diverso possível (Brunstrom, A., Eklund, J., 2006). Desta forma, garante-se que em caso de falha em um dos caminhos, o outro esteja disponível para efetuar o tráfego das mensagens.

Em condições normais de operação o tráfego é enviado somente pelo caminho primário. Pelos caminhos secundários são passadas mensagens de continuidade (ou *heartbeat*), que são mensagens enviadas para testar o funcionamento destes caminhos, e também manter uma informação atualizada sobre o RTT (*Round-trip Time*) dos mesmos.

Utilizar-se da facilidade *multi-homing* fazendo com que os dois endereços de rede estejam usando uma mesma estrutura de rede é desperdiçar o recurso de proteção, uma vez que ele estaria sendo usado somente para proteger a interface local do *endpoint*.

### **3.4. TEMPORIZADORES E VARIÁVEIS DO PROTOCOLO**

Para que o protocolo SCTP possa funcionar de forma adequada, é necessário que existam temporizadores e variáveis internas que sejam capazes de avaliar o estado e funcionamento da rede. O conhecimento do funcionamento destas variáveis e temporizadores é essencial para compreender o funcionamento do protocolo e, conseqüentemente, avaliar quais os parâmetros que podem ser alterados visando-se o atendimento dos requisitos para uma rede de sinalização.

#### **3.4.1. RTO e variáveis associadas**

A variável RTO (*Retransmission Timeout*) é responsável por identificar se há ou não a necessidade de retransmissão de uma mensagem novamente, da origem para o destino. Essa variável é essencial para a eficiência e estabilidade de uma associação SCTP.

Essa variável é calculada com base no RTT (*Round-trip Time*) observado na rede. O RTT é medido pela diferença entre o envio de um *chunk* de dados para o *endpoint* de destino e o tempo de recebimento da informação de SACK deste *chunk*, recebido de volta ao *endpoint* de origem. O RTT deve ser calculado para cada um dos caminhos de rede definidos entre os *endpoints*. No caso dos caminhos alternativos, o RTT é calculado com base no envio e recebimento dos *chunks* HEARTBEAT e HEARTBEAT-ACK destes caminhos.

Devido às características da rede, o RTT tem o seu valor em constante variação, já que o

tempo levado pela mensagem da origem ao destino e o envio no sentido contrário da informação da confirmação do recebimento estão sujeitos às condições da rede.

Segundo a RFC 2960, o RTO é calculado, em condições de regime, com a ajuda de duas outras variáveis, SRTT (*Smoothed Round-trip Time*) e RTTVAR (*Round-trip Time Variation*), pelo seguinte procedimento:

$$RTTVAR_{new} = (1 - \beta) \cdot RTTVAR_{old} + \beta \cdot |SRTT_{old} - R_{new}| \quad (3.1)$$

$$SRTT_{new} = (1 - \alpha) \cdot SRTT_{old} + \alpha \cdot R_{new} \quad (3.2)$$

onde  $\alpha$  e  $\beta$  são constantes do protocolo, e tem os valores definidos em 1/8 e 1/4 respectivamente. O valor  $R_{new}$  representa a medição mais recente do RTT. Com os valores acima, o novo valor de RTO é calculado conforme:

$$RTO = SRTT_{new} + 4 \cdot RTTVAR_{new} \quad (3.3)$$

Em seguida avalia-se o valor obtido em relação aos limites estabelecidos em parâmetro, sendo RTOmin o valor mínimo que pode ser usado e RTOmax o valor máximo desta variável.

Desta forma, observa-se que o RTO terá um valor sempre um pouco acima do valor do RTT da rede, pois é composto não só pelas medições de RTT obtidas mas também pelo módulo da sua variação.

### 3.4.2. Temporizador T3-rtx

O valor da variável RTO medida no caminho entre os *endpoints* é usado para definir o valor do temporizador T3-rtx. O objetivo deste temporizador é avaliar se há a necessidade da retransmissão de uma mensagem.

Toda a vez que um *chunk* de dados é enviado para a rede, o temporizador é inicializado. Quando é recebida a confirmação de recebimento deste *chunk*, a partir do *endpoint* de destino, o temporizador é encerrado.

Caso o *endpoint* de origem tenha o temporizador T3-rtx esgotado para um determinado caminho, entende-se que o pacote enviado foi perdido. Isso pode ter sido causado por três

motivos diferentes:

- Um pacote SCTP que leva *chunk* de dados foi perdido devido a um congestionamento de rede;
- O endereço IP de destino está inacessível;
- O *endpoint* de destino está fora de serviço.

O *endpoint* de origem não tem, até esse momento, como distinguir qual das três situações ocorreu, mas deve iniciar imediatamente uma ação para garantir a entrega das mensagens ao destino. Em resumo, são efetuados os seguintes passos:

- Ajustar o valor do RTO do caminho onde houve a expiração do temporizador, dobrando o valor de RTO, ou seja,  $RTO_{\text{new}} = 2 \times RTO_{\text{old}}$ ;
- Incrementar o contador de erros do caminho utilizado e da associação;
- Marcar todas as mensagens que estão na fila de envio para retransmissão;
- Selecionar um caminho alternativo para envio das mensagens marcadas para retransmissão;
- Determinar quantos *chunks* de dados podem ser enviados em um único pacote SCTP. Isso é feito agrupando-se primeiro os pacotes mais antigos (ou seja, os que estão a mais tempo na fila de envio) até que se chegue ao valor máximo de PMTU da rede;
- Criar um pacote SCTP com todos os *chunks* marcados no item anterior, e enviar esse pacote pelo caminho alternativo selecionado;
- Iniciar o temporizador T3-rtx para o caminho alternativo selecionado.

Com o procedimento indicado, especificamente o ajuste do valor do RTO, garante-se que variações na latência de rede sejam absorvidas pelo *endpoint*, e o mesmo não seja

considerado inacessível. Quando for recebida a informação de SACK dos bilhetes retransmitidos, o valor da variável RTO do caminho será, aos poucos, atualizado para refletir o novo perfil da rede. Nesse momento deve ser zerado o contador de erros do caminho.

### **3.4.3. Contador de erros do caminho e da associação**

Os contadores de erros são variáveis importantes na identificação da falha da rede. Como indicado no item 3.4.2. , cada vez que o temporizador T3-rtx se esgota o contadores de erros do caminho e da associação são incrementados. O contador de erros do caminho é individual para cada caminho definido, enquanto o contador de erros da associação é único para a associação SCTP.

## **3.5. PARÂMETROS CONFIGURÁVEIS**

O SCTP foi desenvolvido de forma bastante parametrizável. Vários dos seus parâmetros podem ser configurados pela camada de aplicação, o que garante que ele possa ser adaptado a diversas necessidades de rede. Isso se deve ao fato de o protocolo ter sido desenvolvido para uso genérico em redes IP, mas sem perder a visão das necessidades específicas de desempenho requeridas pelas aplicações de troca de sinalização em redes de telecomunicações. Com o ajuste adequado destes parâmetros pode-se mudar completamente o seu comportamento e, por consequência, o seu desempenho.

### **3.5.1. Parâmetros RTOmin e RTOmax**

Os parâmetros RTOmin e RTOmax definem os limites para variação da variável RTO, que é medida em cada um dos caminhos de rede definidos para a associação. Como a variável RTO é calculada dinamicamente através do comportamento do tráfego observado, estes limites são importantes para que se tenha controle sobre o valor final obtido.

O parâmetro RTOmin objetiva fazer com que a variável não tenha um valor baixo demais, podendo, em alguns casos, fazer com que o *endpoint* efetue uma retransmissão desnecessariamente, já que o temporizador T3-rtx, responsável pela avaliação do tempo máximo que se deve esperar o recebimento da informação de SACK é baseado na variável RTO.

O parâmetro RTOMax serve para limitar o crescimento da variável RTO, especialmente nos momentos em que há uma falha no caminho utilizado entre os *endpoints*. Conforme indicado na seção 3.4.2. , a cada vez que o temporizador T3-rtx se esgota, o valor de RTO é dobrado (fator de *back-off* igual a 2), fazendo com que o valor desta variável cresça exponencialmente. Isso pode ser um problema especialmente quando se usa o parâmetro Path.Max.Retrans com valores altos. Nestes casos, o tempo para detecção da falha pode ser exagerado, e o parâmetro RTOMax pode ser usado para se evitar esse efeito.

### **3.5.2. Parâmetro Path.Max.Retrans – número máximo de retransmissões no caminho**

A comutação do tráfego do caminho primário para um caminho alternativo não é feito logo após uma falha. Isso poderia gerar comutações desnecessárias para o caminho reserva pela perda eventual de poucos pacotes. Para evitar esse efeito indesejável, o parâmetro Path.Max.Retrans, também chamado de PMR, indica quantas falhas são aceitas em um caminho antes que esse seja considerado inacessível. Assim, cada vez que um *chunk* enviado for considerado perdido, pelo esgotamento do temporizador T3-rtx, um contador de erros para esse caminho (ou *path*) é incrementado, até que se exceda o valor Path.Max.Retrans. Somente após esse evento o caminho é considerado inacessível, e o outro caminho deverá ser considerado o caminho primário (Brunstrom, A., Eklund, J., 2006).

Cada vez, porém, que um *chunk* tem a sua entrega confirmada, esse contador é zerado. Assim, são necessárias várias falhas consecutivas para que o caminho seja considerado inacessível.

### **3.5.3. Parâmetro Association.Max.Retrans – número máximo de retransmissões na associação**

Similarmente ao Path.Max.Retrans, existe o parâmetro Association.Max.Retrans, porém este trabalhando no nível de associação. De forma similar, existe um contador de falhas na associação, que é incrementado quando uma falha de envio é detectada (expiração do temporizador T3-rtx). Quando há falhas consecutivas em uma associação, e o valor do Association.Max.Retrans é ultrapassado, ainda que em caminhos diferentes, a associação é considerada fechada.

### 3.5.4. Parâmetro HB.Interval – Intervalo de HeartBeat

O temporizador HB.Interval define o tempo de envio do *chunk* HEARTBEAT. Esse *chunk* é enviado sempre que não houver tráfego de dados em uma associação. O *chunk* HEARTBEAT deve ser respondido imediatamente com um *chunk* HEARTBEAT-ACK, para que o *endpoint* de origem confirme a acessibilidade do *endpoint* de destino através deste caminho específico. Esse procedimento deve ser usado para cada um dos caminhos de rede que interligam os *endpoints*, de forma que o temporizador deve ser controlado para cada par de endereços IP entre a origem e o destino.

### 3.5.5. Parâmetro Atraso de SACK

Quando ocorre a entrega de um *chunk* de dados (*chunk* DATA) em um *endpoint*, esse deve gerar a informação de SACK para ser enviada do *endpoint* de origem. Esse SACK é usado tanto para confirmar o recebimento do *chunk* de dados como para informar, se for o caso, que há *chunks* anteriores que ainda não foram recebidos. Essa informação de SACK deve ser enviada de volta ao *endpoint* de origem do *chunk* de dados, e para isso é utilizado o *chunk* SACK.

O envio de um *chunk* SACK para cada *chunk* DATA recebido por um *endpoint* poderia, no entanto gerar um tráfego grande, consumindo capacidade de rede de forma desnecessária. Assim, o SCTP permite que seja enviado um *chunk* SACK para confirmar a entrega de vários *chunks* de dados que tenham sido recebidos.

O envio do *chunk* SACK de volta ao *endpoint* de origem pode ser feito de duas formas:

- pelo agrupamento do *chunk* SACK junto com um *chunk* de dados que esteja sendo enviado em sentido contrário, ou seja, do *endpoint* que originalmente recebeu o *chunk* de dados para o *endpoint* que o enviou.
- Pelo envio do *chunk* SACK isoladamente, após a expiração do temporizador de atraso de SACK da associação.

Quando a associação leva tráfego bidirecional, o envio do *chunk* SACK agrupado a um *chunk* DATA no sentido inverso é bem efetiva, e não deve haver casos de expiração do

temporizador de atraso de SACK (Stewart, R., Xie, Q., 2001), (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010). Esse é exatamente o caso do tráfego de sinalização, que tem um perfil tipicamente transacional.

### **3.6. VALORES SUGERIDOS**

Com relação aos parâmetros Path.Max.Retrans e Association.Max.Retrans, há um cuidado a ser tomado na definição dos seus valores. Considerando-se associações *multi-homed*, o valor do Association.Max.Retrans deve ser menor do que o valor do Path.Max.Retrans multiplicado pelo o número de caminhos previstos.

Caso esse cuidado não seja tomado, e a implementação do SCTP não tome essa precaução, pode ocorrer de haver falha em todos os caminhos da associação, mas ainda assim essa ser considerada ativa. Neste caso a associação entra em um modo chamado dormente (*dormant mode*) (Stewart, R., Xie, Q., 2001).

Considere-se o exemplo a seguir: em uma configuração *multi-homed* com 4 caminhos, sendo o valor de Path.Max.Retrans = 4, o valor de Association.Max.Retrans deve ser inferior a 16. Garante-se assim que a associação será fechada antes que ocorram todas as tentativas de envio possível.

O estado dormente é considerado indesejável para aplicações em telecomunicações, uma vez que a camada superior não é informada deste estado, e pode continuar enviando dados para transmissão via SCTP sem saber quando serão, e se realmente eles serão entregues.

### **3.7. CONCLUSÕES**

Apesar de o SCTP não ter sido originalmente desenvolvido para o ambiente de redes de sinalização de telecomunicações, observa-se que as adaptações feitas no mesmo atendem aos requisitos requeridos por esse ambiente, especialmente quando esse protocolo é usado em conjunto com as camadas de adaptação previstas. Essas camadas são capazes de tornar a rede de transporte totalmente transparente para as camadas de aplicação, de forma que as aplicações não sabem (e nem precisam saber) qual o tipo de rede de transporte está sendo usado, redes de circuitos ou redes de pacotes.

O protocolo SCTP tem avanços consideráveis em comparação aos protocolos UDP e TCP. Esse avanço reflete novas necessidades dos serviços envolvidos, e também visaram atender requisitos de confiabilidade e segurança até então inexistentes nos protocolos de rede IP. A característica de extensibilidade do protocolo dá a ele a possibilidade de um contínuo desenvolvimento, conforme os requisitos de serviços forem sendo desenvolvidos.

A quantidade de parâmetros existentes para configuração do protocolo SCTP dá a ele a possibilidade de uso em aplicações com requisitos bastante variáveis. Dependendo do tipo de rede a ser usado e necessidades das camadas de aplicação envolvidas, são possíveis vários ajustes, visando a otimização do desempenho do mesmo. Por outro lado, o grande número de parâmetros leva a cuidados especiais na definição de valores para os mesmos. Um conjunto de parâmetros otimizado para uma rede pode não ser adequado para outra, caso as características de latência, velocidade e perda de pacotes seja diferente. O mesmo é válido para as aplicações, que podem gerar configurações com parâmetros diferentes entre si. Assim, é necessária uma avaliação cuidadosa destes requisitos e capacidades do protocolo, de forma a otimizá-lo para as características e necessidades do tráfego de sinalização em redes de telecomunicações.

No próximo capítulo avaliaremos como o funcionamento do protocolo é afetado pelas condições do tráfego de mensagens a ser transmitido. Também será avaliado o efeito que cada um dos parâmetros do protocolo tem sobre o seu desempenho. Finalmente, essas avaliações serão confirmadas por meios de simulações, procurando confirmar os efeitos estudados, abrindo espaço para a sugestão de uma ou mais configurações que sejam consideradas adequadas, visando o atendimento aos requisitos da rede de sinalização.

## 4. OTIMIZAÇÃO

O objetivo deste trabalho é propor uma otimização dos parâmetros do protocolo para conseguir o melhor desempenho possível em situações de falha. Para tanto, devemos primeiro definir o que é uma situação de falha. Se classificarmos as falhas de acordo com seu efeito sobre o tráfego que a rede transporta, podemos identificar três formas como o tráfego é afetado antes de o caminho ser considerado indisponível:

- Aumento gradativo da perda de pacotes até que o funcionamento do protocolo torne-se inviável;
- Aumento gradativo da latência, até que o funcionamento do protocolo torne-se inviável;
- Corte brusco na comunicação, com perda total de todos os pacotes transportados pelo caminho

Uma falha real de rede gerada por sobrecarga em roteadores ou enlaces normalmente contém os três componentes, misturados em proporções diversas. Inicialmente a sobrecarga gera um atraso no processamento dos pacotes, seguido pelo aumento gradativo da perda dos mesmos, culminando com a paralisação total do processamento do elemento de rede em questão.

Essa situação é de difícil definição para estudo e replicação, uma vez que o tamanho dos enlaces, seu tráfego, o tamanho do *buffer* dos roteadores envolvidos e outros fatores vão afetar o momento em que cada um dos eventos acima descritos ocorra. Ou seja, cada vez que esse tipo de falha ocorre, os momentos envolvidos são diferentes.

Por esses fatores, neste trabalho optou-se por considerar uma falha envolvendo somente a terceira situação, a que envolve o corte brusco no tráfego, com perda de todos os pacotes. Esse cenário ocorre, normalmente, em função de uma falha de energia, rompimento do próprio meio de transmissão, ou de falha grave de hardware em algum equipamento de rede.

#### **4.1. REQUISITOS DAS CAMADAS DE APLICAÇÃO**

Uma das grandes vantagens da rede SS7 baseada em TDM é a habilidade de rapidamente tratar situações de falha. Segundo (Rembarz, R., Baucke, S., Mahonen, P., 2005), a comutação para um caminho alternativo de uma rede SS7 é completada usualmente entre 500ms e 2000ms. Assim, é razoável que uma implementação de rede de transporte para sinalização mantenha esses mesmos níveis de desempenho, de forma a ficar totalmente transparente para as camadas de aplicação acima.

#### **4.2. AVALIAÇÃO DO DESEMPENHO DO SCTP**

Considerando os requisitos indicados, observa-se que os principais indicadores de desempenho do SCTP em condição de falha são o tempo para comutação para o caminho reserva e o atraso máximo sofrido pelas mensagens enviadas entre o momento da falha e a comutação do tráfego para o caminho alternativo.

Embora os valores destes dois indicadores de desempenho sejam, normalmente, bastante próximos, e afetados, inicialmente, pelos mesmos fatores de rede, eles têm valores potencialmente diferentes. O atraso médio das mensagens é tipicamente menor do que o tempo de comutação da rede principalmente pelo fato de as retransmissões que ocorrem antes da comutação para o caminho alternativo reduzirem a quantidade de mensagens a serem retransmitidos após a comutação.

O item 6.1 da RFC2960 (SCTP) (Stewart, R., Xie, Q., 2001) define que as mensagens mais antigas sempre são as primeiras a serem retransmitidas. Assim, cada vez que há uma retransmissão o atraso máximo potencial é reduzido, já que ficam, para serem retransmitidas, as mensagens mais novas, ou seja, as que estão na fila de envio a menos tempo.

Esse efeito é mais notado especialmente em condições de tráfego baixo, quando as retransmissões são capazes de enviar mais mensagens em um mesmo pacote de retransmissão. Essa situação será demonstrada no item 4.2.2.2. , e também nos testes efetuados.

Os valores de tempo de comutação e atraso máximo das mensagens são afetados por

diversos fatores, sendo que alguns destes podem ser controlados ou gerenciados no projeto da rede pelo ajuste de parâmetros do protocolo, e outros não, por serem intrínsecos ao tipo de tráfego que está sendo cursado. Entre os fatores que temos controle, estão os relativos à topologia de rede, e ainda a configuração dos parâmetros e temporizadores do protocolo SCTP.

Apesar de termos como objetivo obter um tempo de comutação reduzido em caso de falha, é importante também avaliar o atraso máximo das mensagens transmitidas percebido pela aplicação. Como no caso do transporte de sinalização SS7 as camadas de aplicação estão isoladas da camada SCTP pela camada M3UA, a informação de comutação para o caminho alternativo é transparente para a aplicação, sendo, neste caso, mais importante que o atraso gerado pela rede às mensagens enviadas – esteja ela em fase de comutação para o caminho alternativo ou não – seja mínimo. Considerando-se que em uma rede de sinalização estão sendo cursadas, simultaneamente, mensagens relativas a diversas chamadas totalmente independentes, o efeito desse atraso será percebido por somente poucas chamadas ou sessões que estão sendo processadas pelos elementos de rede naquele momento.

#### **4.2.1. Requisitos de topologia da rede**

Um dos melhoramentos propostos pelo protocolo SCTP em comparação ao TCP e UDP é o uso transparente de múltiplos caminhos entre os elementos de rede envolvidos. A configuração *multi-homed* permite que os elementos de rede estejam conectados através de mais de um caminho de rede, provendo assim uma redundância de meios entre os mesmos.

Para que o efeito positivo das características trazidas pelo uso de multi-caminhos seja máximo, é necessário que a diversidade de caminhos seja maximizada (Stewart, R., Xie, Q., 2001), conforme Figura 4.1.

Idealmente, deve-se garantir que o caminho utilizado pelos pacotes enviados através de uma das interfaces seja totalmente distinto do caminho usado por dados enviados por outra interface. Desta forma, caso haja uma falha em um dos caminhos, a associação continua ativa já que ainda existe conectividade entre os dois elementos de rede. O tráfego passa a ser cursado pelo caminho que ainda está ativo, de forma transparente para as camadas superiores.

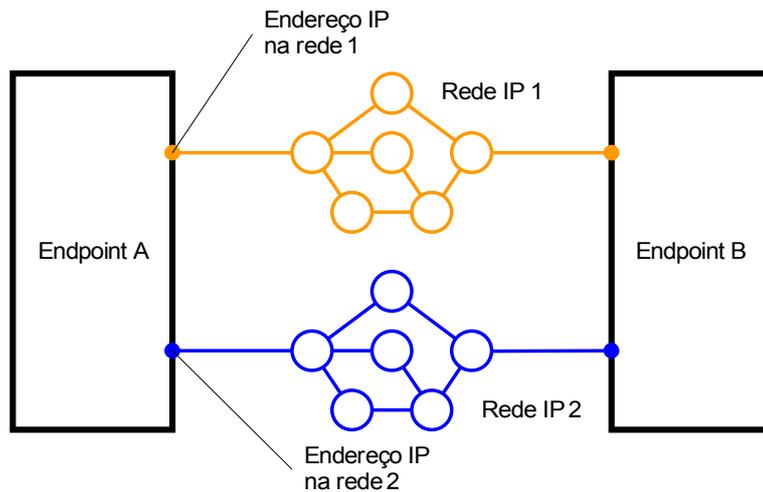


Figura 4.1 - Conceito de multi-caminhos interligando dois *endpoints*

#### 4.2.2. Fatores que afetam o tempo para comutação

A Figura 4.2 indica como esses fatores afetam o desempenho do SCTP no que se refere ao tempo de comutação para o caminho reserva. Como parte da análise serão avaliados os impactos dos parâmetros de latência, perfil de tráfego em mensagens por segundo e tamanho das mensagens. Com relação aos parâmetros do protocolo SCTP, será avaliado o efeito dos parâmetros Atraso de SACK (*Sack Delay*), *RTOmin*, *RTOmax* e *Path.Max.Retrans*. Efetivamente, estes fatores e parâmetros atuam sobre o *Round-trip Time* (RTT), o tempo para que o protocolo detecte a perda de um pacote, o tempo para início das retransmissões (*timer T3-rtx*) e sobre o tempo em que as retransmissões irão ocorrer.

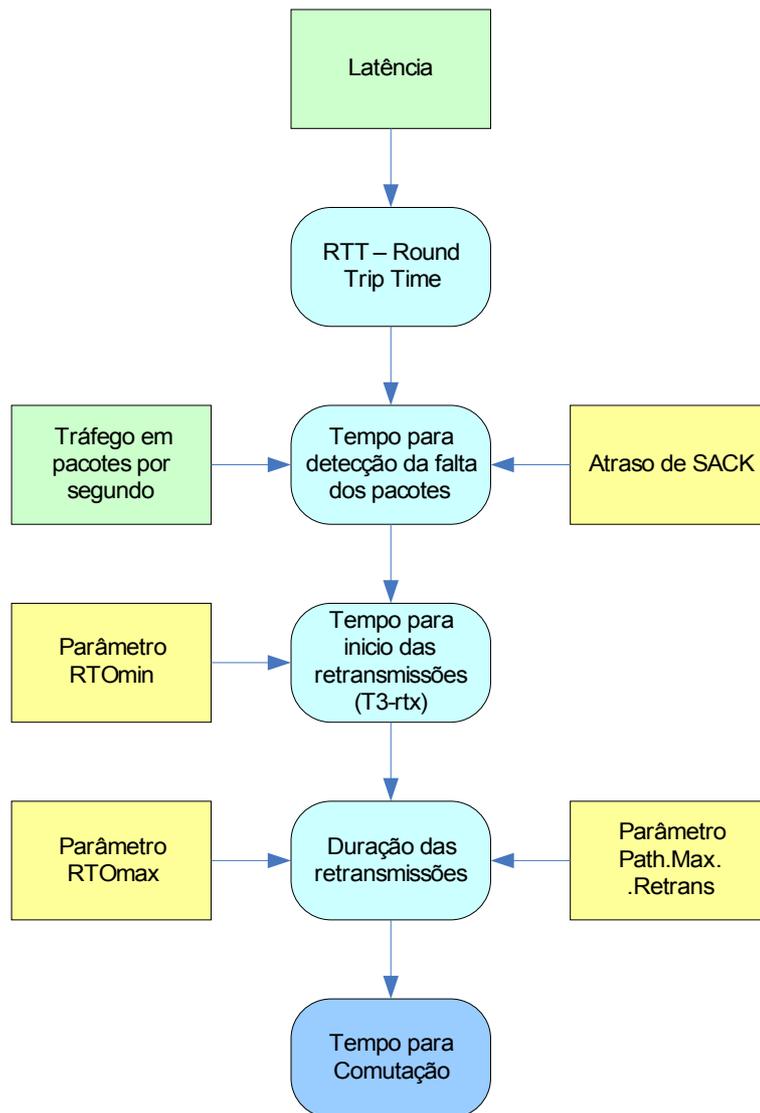


Figura 4.2 - Fatores de influência para o tempo de comutação para o caminho reserva

O *Round-trip Time* é o tempo total observado que um pacote leva para percorrer a rede da origem ao destino e chegue novamente a origem, passando por todos os elementos de rede envolvidos (Stewart, R., Xie, Q., 2001). O tempo para detecção da falta dos pacotes corresponde ao tempo levado pelo protocolo para considerar que um pacote enviado foi efetivamente perdido. Ele é função do *Round-trip Time*, do tráfego em pacotes por segundo e do parâmetro Atraso de SACK (*SACK Delay*). Mesmo após a detecção da perda dos pacotes, o início das retransmissões depende ainda da configuração do parâmetro *RTOmin*. Nesse momento efetivamente ocorrerá a primeira retransmissão, sendo que a sua quantidade e duração são função também do parâmetro *RTOmax* e do parâmetro

Path.Max.Retrans. Somente após a quantidade de retransmissões permitidas ser ultrapassada é que ocorrerá a comutação para o caminho reserva.

#### 4.2.2.1. Latência

O tempo que os pacotes levam para serem entregues a partir da origem até o destino afeta diretamente o RTT, que é o tempo mínimo que um pacote leva para ir de um lado ao outro da rede e voltar. O RTT é constantemente monitorado, e usado para a cálculo do valor de RTO. A forma de cálculo do RTO foi indicada nas equações (6.1), (6.2) e (6.3). O RTO, por sua vez, é usado como padrão para que o *endpoint* que enviou o *chunk* de dados saiba que a informação não foi recebida no destino, pela recepção do *chunk* SACK enviado de volta.

A Figura 4.3 é um exemplo de influência da latência no cálculo do RTT. Em situações normais o RTT terá um valor equivalente a pouco mais de duas vezes a latência da rede. O valor do RTT pode ser alterado devido a variações na latência, já que o módulo variação da latência é um dos componentes aritméticos do cálculo do RTT, como no item 3.4.1.

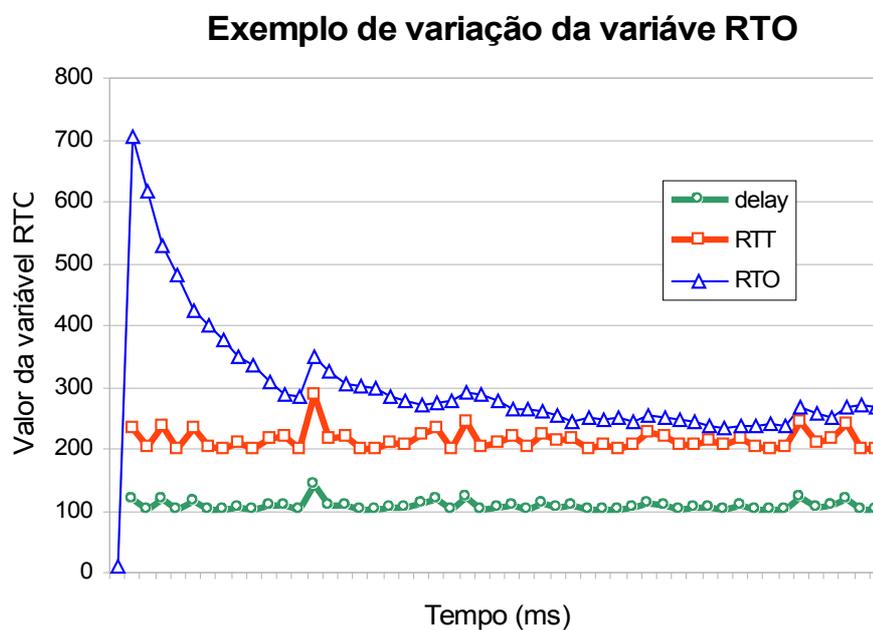


Figura 4.3 - Oscilação do valor de RTO em função da variação dos valores de atraso na rede.

Nesta figura foi feito cálculo do RTT da rede, considerando-se uma latência mínima de

100 ms, acrescida de uma variação com distribuição exponencial com esperança 7 ms. O valor de RTT foi calculado em duas vezes a latência. Observe-se como o valor da variável RTO acompanha o RTT da rede. Porém, quando ocorre uma variação brusca da latência da rede, o valor de RTT cresce para acompanhar a variação, sendo reduzido aos poucos até voltar ao valor próximo de RTT novamente.

Caso a rede imponha, devido às suas características, um atraso grande aos pacotes, o *endpoint* de origem estará aguardando um tempo maior para receber a confirmação de entrega do pacote. Esse tempo é definido pelo valor do temporizador T3-rtx, disparado no envio dos pacotes. O temporizador T3-rtx recebe o valor do RTO medido na rede naquele momento.

Assim, quanto maior a latência da rede, maior o tempo em que a perda de um pacote, e a possível falha na rede, levará para ser detectada pelo transmissor do mesmo.

#### 4.2.2.2. Perfil de tráfego

O tráfego é um fator que tem razoável influência no tempo de comutação para o caminho secundário. Não exatamente o valor da banda ocupada pelo tráfego em si, mas sim a quantidade de mensagens (MSUs) que são enviadas na rede. Essa situação se deve ao fato de a falha na rede ser detectada primariamente pela falta de confirmação de entrega das mensagens ao destino, ou seja, envio do *chunk SACK* a partir do *endpoint* de destino para o *endpoint* de origem. Com a redução do tráfego entre os *endpoints* a detecção da falha fica prejudicada.

Embora essa seja uma situação que aparentemente não pode ser resolvida por topologia de rede ou configuração, deve-se observar que em muitos casos são construídas associações SCTP em paralelo entre os elementos de rede, de forma a dividir a carga entre diversas placas do equipamento. Essa configuração é feita para aumentar a segurança ou por limitações na capacidade de processamento dos elementos envolvidos.

Desta forma, a distribuição do tráfego entre várias associações paralelas, embora traga um aumento na segurança da rede, pode influenciar negativamente o desempenho no que se refere ao tempo de comutação para o caminho reserva, já que o tráfego em cada uma das associações será cada vez mais reduzido conforme aumenta-se a quantidade de associações

paralelas, conforme pode ser visto na Tabela 4.1.

Tabela 4.1 - Quantidade de associações paralelas e o tráfego relativo em cada uma

Quantidade de Associações Paralelas	Tráfego relativo
1	100,00%
2	50,00%
3	33,33%
4	25,00%
5	20,00%
6	16,67%
7	14,28%
8	12,50%
9	11,11%
10	10,00%

Considere-se ainda que a informação de SACK, em caso de redes de sinalização, tipicamente é enviada juntamente com um *chunk* DATA enviado do *endpoint* de destino para o *endpoint* de origem. Com a redução do tráfego, reduz-se também o envio de informações de SACK, ainda que esse atraso seja limitado pela configuração do parâmetro *SACK Delay*, configurado tipicamente para 200 ms.

O temporizador de envio *chunk* HEARTBEAT (Heartbeat timer) poderia ser usado para limitar a dependência do tráfego na detecção da falha, porém são usados valores tipicamente altos para esse temporizador, e reduzi-lo muito iria gerar um tráfego desnecessário na rede.

A troca de *chunks* HEARTBEAT entre os *endpoints* é a forma usada para avaliação da conectividade dos caminhos alternativos entre os *endpoints*. A cada esgotamento do temporizador HB Timer, é enviado um *chunk* HEARTBEAT da origem para o destino, que responde imediatamente com um *chunk* HEARTBEAT ACK.

#### 4.2.2.3. Parâmetro *SACK Delay* - Atraso de SACK

A possibilidade de se atrasar o envio da informação SACK do *endpoint* de destino para o *endpoint* de origem, apesar de ser vantajoso em termos de redução de tráfego na rede, pode

trazer consequências negativas à detecção de uma falha de rede. O valor proposto pela RFC2960 (Stewart, R., Xie, Q., Morneault, K. et al., 2000) para esse atraso é de 200 ms, o que faria com que a perda de um pacote, ainda que em cenários de latência baixa, fosse reportada à origem no mínimo 200 ms após. Essa situação pode ser bastante crítica em casos de redes de sinalização, considerando-se que ainda haverá várias retransmissões, de acordo com a configuração do parâmetro Path.Max.Retrans.

No caso de redes de sinalização, no entanto, esse impacto não deve aparecer, uma vez que o tráfego nas redes de sinalização é tipicamente transacional, ou seja, a quantidade de MSU em ambas as direções é relativamente igual, já que as operações dos protocolos de aplicação requerem confirmação. Nestes casos, o envio da informação de SACK é feita juntamente com o envio de *chunks* de dados do *endpoint* de destino para o *endpoint* de origem. Nestes cenários não há necessidade de *chunk* SACK, e o atraso no envio da informação SACK fica sendo apenas função do tráfego entre os *endpoints*. Quanto maior o tráfego, menor o atraso no envio.

#### 4.2.2.4. Parâmetro Path.Max.Retrans – número máximo de retransmissões no caminho

Quando o *endpoint* de origem identifica que o *chunk* de dados não foi recebido no destino, ele retransmite as mensagens que estejam na fila de envio. O processo de retransmissão é repetido várias vezes, até que o valor do parâmetro Path.Max.Retrans seja atingido. Ao ser superado o valor deste parâmetro, o caminho é considerado inacessível, e ocorre a comutação para o caminho alternativo.

O valor do parâmetro Path.Max.Retrans tem influência direta sobre o tempo de comutação para o caminho alternativo. Valores altos para esse parâmetro farão com que haja retransmissões sucessivas em um caminho que já pode estar inacessível, com uma perda de tempo considerável, considerando-se ainda que a cada retransmissão o valor do RTO do caminho é multiplicado por 2 (fator de *back-off*). Esse fator de *back-off* faz com que o tempo de comutação cresça exponencialmente em função do parâmetro Path.Max.Retrans utilizado.

Por outro lado, o uso do parâmetro Path.Max.Retrans com valor muito baixo poderia fazer com que houvesse uma comutação desnecessária para o caminho reserva, fazendo com que se busque um valor equilibrado para esse parâmetro. O valor sugerido na RFC2960

(Stewart, R., Xie, Q., Morneault, K. et al., 2000) é 5, ou seja, haverá 5 tentativas de retransmissão até que o caminho seja considerado inacessível.

#### 4.2.2.5. Parâmetro RTOmin

O valor da variável RTO é calculado dinamicamente, de acordo com a latência observada na rede. Esse valor é usado para disparo do temporizador T3-rtx, usado para indicar a falta do recebimento da confirmação do recebimento da mensagem. Essa variável pode ter um valor mínimo configurável, definida pelo parâmetro RTOmin. Assim, se como resultado do cálculo da variável RTO for encontrado um valor menor que o parâmetro RTOmin, o RTOmin deve ser usado para o RTO.

O objetivo desta configuração é evitar que o parâmetro RTO tenha valores muito baixos, o que poderia levar a detecções incorretas de falhas na rede. Por exemplo, um atraso na entrega de um pacote SACK poderia ser identificado como falha no envio, gerando uma retransmissão desnecessária.

Por outro lado, a manutenção artificial do RTO em valores inadequadamente altos pode gerar a situação de demora na detecção da perda do pacote, já que o temporizador T3-rtx é gerado a partir do RTO. Observe-se também que o valor de atraso para que as retransmissões sejam feitas é gerado a partir do RTO, que cresce exponencialmente a cada retransmissão.

Assim, o parâmetro RTOmin tem uma influência grande no desempenho do tempo de comutação. O valor sugerido na RFC2960 (Stewart, R., Xie, Q., Morneault, K. et al., 2000) para o RTOmin é de 1 segundo.

#### 4.2.2.6. Parâmetro RTOmax

Quando ocorre uma retransmissão, a especificação do protocolo prevê que o valor do parâmetro RTO seja multiplicado por 2 (fator de *back-off*). Desta forma garante-se que, caso a perda do pacote seja função do aumento repentino do atraso na rede, o pacote retransmitido aguardará a sua confirmação de entrega por um tempo maior do que o tempo do envio anterior. O fator de *back-off* leva a um crescimento exponencial do RTO que, juntamente com valores altos de re-tentativas (parâmetro Path.Max.Retrans) pode fazer

com que o RTO cresça de forma desnecessária.

O parâmetro RTOMax limita o crescimento da variável RTO. Assim pode-se trabalhar com uma quantidade de retransmissões alta sem o efeito, às vezes indesejável, do crescimento exponencial do RTO. Por outro lado não se deve colocar um limite muito baixo para o RTO (uso de RTOMax muito baixo), pois o fator de *back-off* igual a 2, com o resultante crescimento exponencial do RTO faz com que, em uma situação de perda de pacotes gerada por congestionamento na rede, o *endpoint* aumente o tempo entre as retransmissões de forma sucessiva.

### **4.2.3. Fatores que afetam o atraso máximo das mensagens**

A Figura 4.4 indica como os fatores citados afetam o desempenho do protocolo SCTP no que se refere ao atraso máximo sofrido pelas mensagens enviadas pelo SCTP através da rede. Embora a grande parte dos fatores seja similar aos fatores que afetam o tempo de comutação, existem algumas situações diferentes que geram um efeito diferenciado sobre o atraso das mensagens. Além dos fatores já citados, latência, perfil de tráfego em pacotes por segundo, parâmetros Atraso de SACK (*SACK Delay*), RTOMin, RTOMax e Path.Max.Retrans, o atraso máximo também é afetado pelo perfil de tráfego no que se refere ao tamanho das mensagens que se deseja enviar pela rede.

#### **4.2.3.1. Latência**

Da mesma forma que o tempo de comutação para o caminho alternativo, o atraso máximo sofrido pelas mensagens no momento da comutação também é função da latência da rede. A latência afeta diretamente o parâmetro RTT (*Round-trip Time*), sendo que esse tem seu efeito sobre o cálculo do RTO da rede.

Como o *endpoint* de origem continua enviando pacotes sem tomar conhecimento da falha, maior o tempo que se leva para detectar a falha da rede, e maior o atraso que as mensagens sofrerão até serem entregues ao destino.

De acordo com a especificação do SCTP, as primeiras mensagens a serem retransmitidas logo após a falha de rede serão as que sofreram o maior atraso, já que as mensagens passadas ao SCTP para envio pouco antes do momento da comutação terão um atraso bem

menor. Essa situação é parcialmente minimizada pelas retransmissões que, da mesma forma, priorizam as mensagens mais antigas.

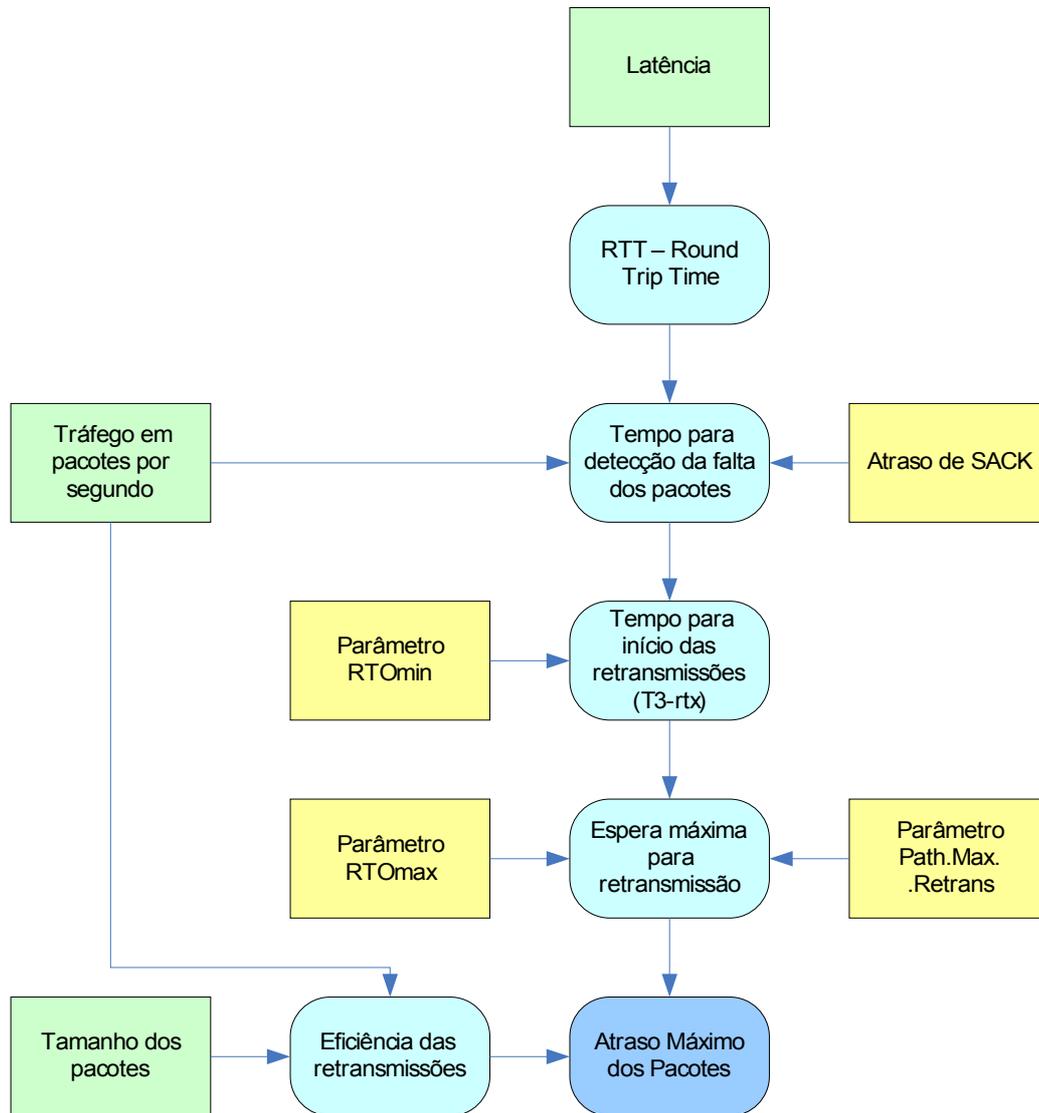


Figura 4.4 - Fatores de influência para o atraso máximo dos pacotes

#### 4.2.3.2. Perfil de tráfego

O perfil de tráfego, no que se refere à quantidade de mensagens (MSUs) que são enviadas pela rede, gera dois efeitos no atraso máximo medido. O primeiro, já avaliado também quanto ao tempo de comutação para o caminho alternativo, tem um efeito positivo sobre o desempenho do protocolo, uma vez que, quanto maior a quantidade de mensagens sendo enviadas pela rede, mais rápida é a detecção da falta da informação de SACK enviada do *endpoint* de destino para o *endpoint* de origem.

Por outro lado, há um efeito negativo do aumento do tráfego no processo de retransmissão das mensagens que estão aguardando para serem transmitidas. Isso porque quanto mais mensagens há para serem enviadas, menor será o efeito benéfico da retransmissão.

Assim, temos um mesmo fator – a quantidade de mensagens enviadas por segundo – gerando efeitos positivos e negativos sobre o desempenho do protocolo.

Outro aspecto a se considerar no que se refere ao perfil de tráfego é o tamanho das mensagens enviadas. Esse fator não afeta a detecção da falha, como ocorre com a quantidade de pacotes enviados, porém afeta o desempenho da retransmissão. Isso porque no processo de retransmissão são enviados os pacotes mais antigos que estiverem na fila de envio do *endpoint* de origem, porém a quantidade de pacotes a serem enviados é limitada pelo PMTU da rede. Ou seja, quanto mais pacotes há para serem enviados no momento em que houver a expiração do temporizador T3-rtx, menor será a eficiência da retransmissão, gerando assim um efeito negativo sobre o atraso máximo dos pacotes.

Aplica-se neste caso, a mesma avaliação feita no item 4.2.2.2. , onde a quantidade de associações paralelas utilizadas pode causar um efeito nas associações individuais, já que quanto mais associações paralelas são usadas, menor é o tráfego de cada uma delas individualmente.

#### 4.2.3.3. Parâmetro Atrasos de SACK, Path.Max.Retrans, RTOmin e RTOmax

O efeito que o parâmetro Atraso de SACK (*SACK Delay*) tem sobre o efeito similar no atraso máximo dos pacotes e no tempo máximo de conexão. Isso se deve ao fato de esse parâmetro influir somente no tempo de detecção da falta de pacotes, conforme indicado na Figura 4.4. O parâmetro define quanto tempo o *endpoint* de destino deve aguardar antes de enviar a informação de SACK em direção ao *endpoint* de origem.

Como o tráfego de sinalização é tipicamente transacional, ou seja, a troca de mensagens envolve transações entre os *endpoints*, tem-se um tráfego equivalente nas duas direções, o que faz com que sempre haja mensagens enviadas nas duas direções. Assim, a não ser que o intervalo entre as mensagens seja superior a 100ms, o temporizador de envio de SACK não expirará, e não serão enviadas mensagens baseadas neste parâmetro.

O parâmetro Path.Max.Retrans tem efeito equivalente ao efeito gerado no tempo máximo de comutação, já que ele indica a quantidade de retransmissões necessárias para que o caminho seja considerado

Os parâmetros RTOmin e RTOmax também exercem efeito similar no atraso máximo dos pacotes e no tempo de comutação, por atuarem nos mesmos pontos. O parâmetro RTOmin influi no tempo necessário para o início das retransmissões. Uma redução do RTOmin tem o potencial de reduzir o tempo para detecção da falha. Já uma redução do RTOmax pode, dependendo do seu valor, reduzir o tempo entre as retransmissões, diminuindo assim o tempo para que o caminho passe a ser considerado inacessível.

### 4.3. SIMULADOR SCTP

A seguir estão as simulações efetuadas, no sentido de avaliar qual o real efeito que cada um dos parâmetros citados acima tem no tempo final de comutação para o caminho reserva e no atraso máximo das mensagens.

Para avaliar o efeito os parâmetros de rede e de configuração citados no desempenho do protocolo, foi desenvolvido um Simulador SCTP. Esse simulador foi escrito em *Visual Basic Express (Microsoft Corporation, 2010)* e implementou todas as rotinas do protocolo que são usadas no processo de verificação de falhas e comutação para o caminho alternativo.

O simulador é constituído por dois ou mais pares de *endpoints* que se comunicam através de uma rede. Nestes *endpoints* são configuráveis todos os parâmetros do protocolo necessários para a avaliação, e que podem influir nos indicadores de desempenho que se deseja medir conforme a Figura 4.5. No que se refere à parametrização dos *endpoints*, é possível configurar:

- o número de associações paralelas, até o máximo de 32 associações;
- os valores dos parâmetros RTOmin, RTOmax, Path.Max.Retrans e SACK Delay.

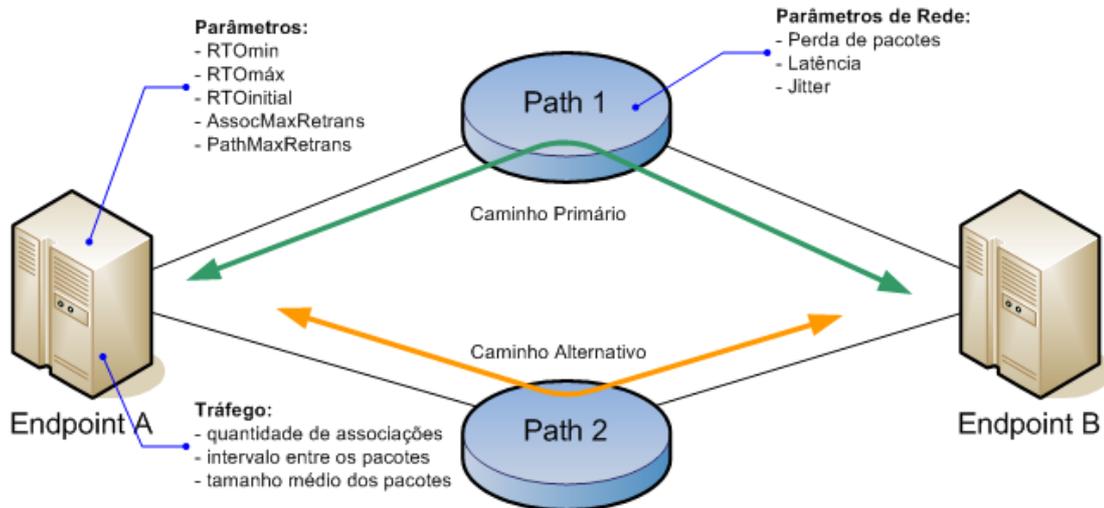


Figura 4.5 - Blocos do Simulador

O perfil do tráfego de mensagens que é trocado entre os *endpoints* também é configurável, e os parâmetros disponíveis são:

- Intervalo de envio entre as mensagens;
- Tamanho dos pacotes enviados;
- Bidirecionalidade do tráfego.

Entre os *endpoints* foi implementado um bloco de *software* que simula as condições que a rede oferece aos pacotes enviados entre os *endpoints*, especificamente a latência e a perda controlada de pacotes.

Na Figura 4.6 está indicado o diagrama de blocos do simulador. O módulo *mod\_endpoint* implementa várias instâncias de *endpoints*. Estes *endpoints* recebem os dados do módulo que simula a aplicação, (módulo aplicação). Estes dados são, então enviados ao módulo que simula os efeitos da rede (módulo Rede) e recebido por outras instâncias de *endpoints*. Todo esse processo é configurado e iniciado pelo *form* *Painel\_De\_Control*e, e reporta suas informações de execução para o *form* *Resultados*. O módulo *Aplicação* é responsável pela geração dos arquivos contendo as estatísticas que são usadas para a geração dos gráficos.

O anexo D contém mais detalhes sobre os módulos de software do simulador, imagens dos *forms* envolvidos e um exemplo de arquivo resultante de uma execução.

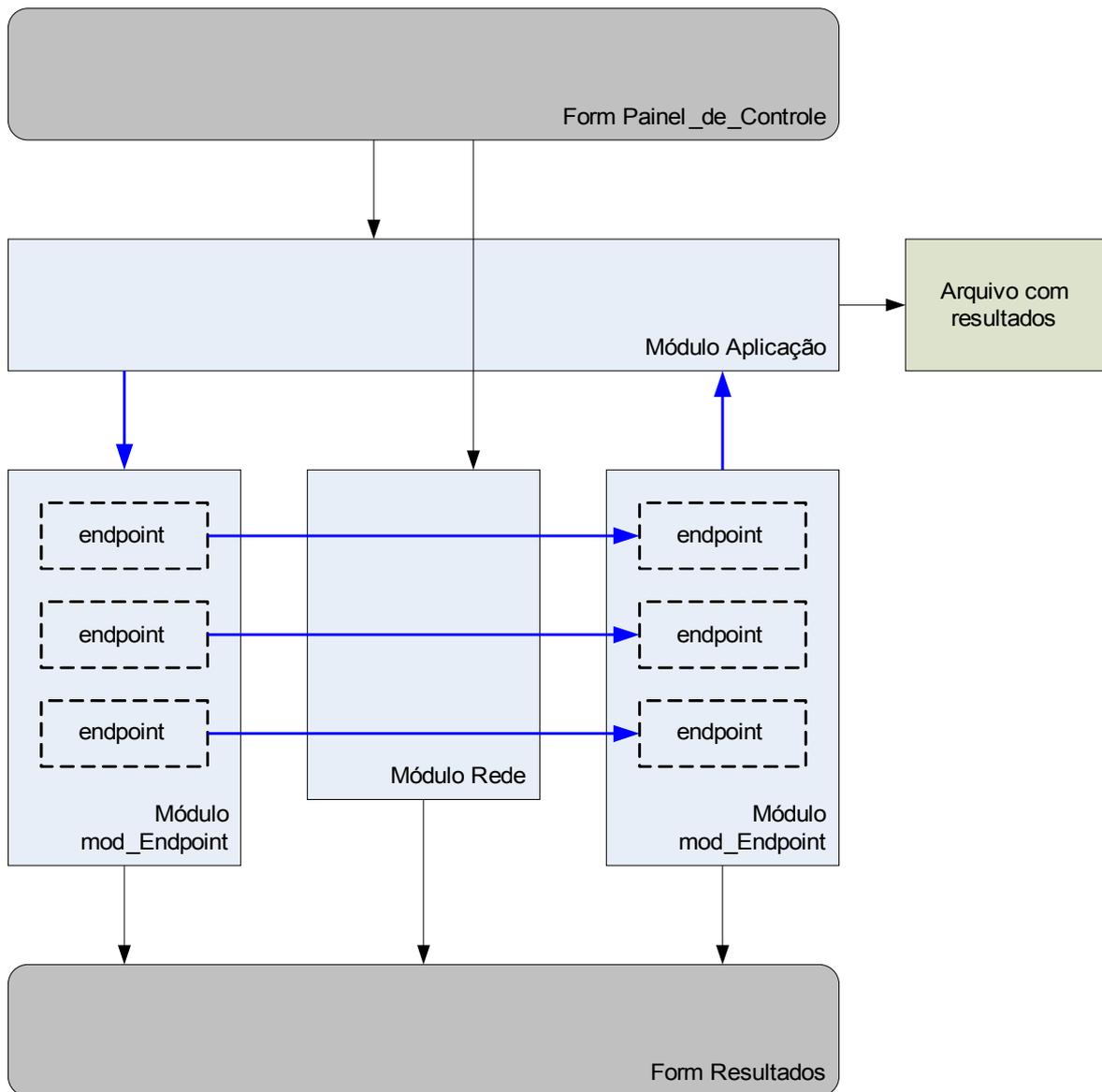


Figura 4.6: Diagrama de Blocos do Simulador SCTP

Para fazer com que o efeito da rede implementada no simulador se tornasse próximo de uma rede real, foi inserida uma variação aleatória no valor da latência. O objetivo é gerar e medir as alterações de comportamento que são da latência, especificamente o tempo de comutação para o caminho alternativo e o atraso máximo dos pacotes. Como a latência é um fator que altera o valor do RTT, e em consequência todo o comportamento do protocolo (conforme itens 4.2.2.1. e 4.2.3.1. ), pequenas variações deste parâmetro geram situações diferentes.

Assim, quanto à rede, é possível alterar, para as simulações:

- A latência mínima absoluta da rede, ou seja, o atraso mínimo imposto a um pacote que atravessa a rede, devido aos equipamentos e distância envolvida;
- A esperança da latência, considerando uma distribuição exponencial negativa, sendo o valor mínimo o valor do parâmetro anterior.

O valor de latência aplicada a cada pacote é gerado aleatoriamente conforme a distribuição exponencial, a arredondado para valores inteiros em milissegundos. A Figura 4.7 mostra um exemplo de distribuição de valor final de latência aplicada aos pacotes, quando se usa a parametrização de latência mínima de 20 segundos, e esperança da distribuição exponencial de 1 segundo.

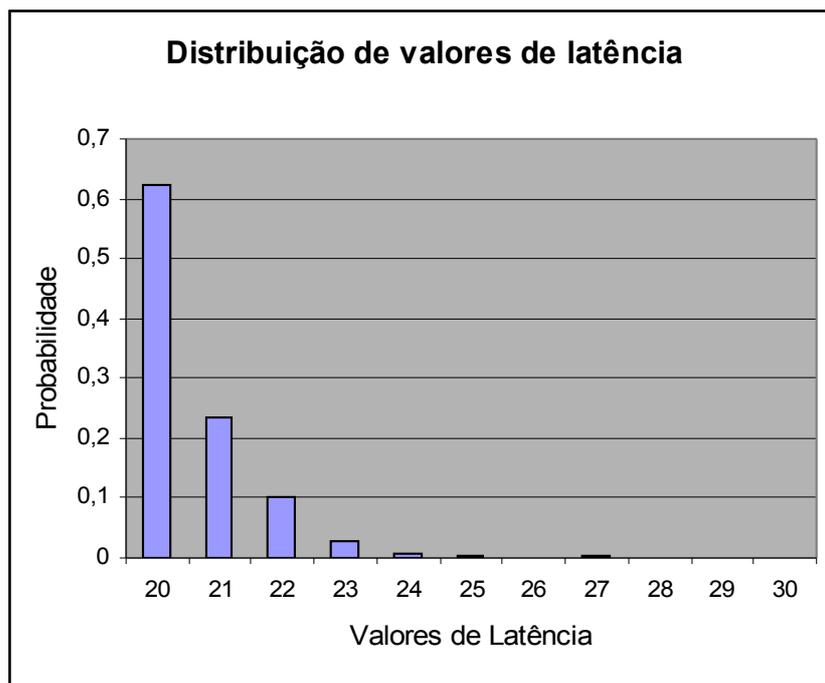


Figura 4.7 - Exemplo de distribuição de latência implementada no bloco de *software* de rede, para o valor mínimo de 20 ms e esperança da distribuição de 1 ms

Na execução, o simulador executa o processo de inicialização das associações (*four-way handshake*) e inicia a transmissão dos dados logo que a inicialização é terminada. Os dados

são trocados entre os *endpoints* sem perda de pacotes durante 10 segundos iniciais, momento onde ocorre a falha do caminho primário. Esse tempo é considerado suficiente para o equilíbrio de todas as variáveis do protocolo (RTO, SRTT, RTTVAR, dos caminhos primários e alternativos). Observe-se se que o temporizador do *heartbeat* dos caminhos alternativos tem o valor definido, pela RFC 2960 (Stewart, R., Xie, Q., Morneault, K. et al., 2000), em 3 segundos, o que faz com que seja necessário um tempo maior para a sua estabilização.

A partir dos 10 segundos de execução são perdidos 100% dos pacotes enviados pelo caminho primário. São, então, observados individualmente todos os pacotes transmitidos, para avaliar o seu tempo de entrega ao *endpoint* de destino. Também é verificado o tempo de comutação deste momento e é medido o atraso dos pacotes até a comutação do tráfego para o caminho alternativo. No caso de múltiplas associações paralelas, essa avaliação é feita em cada uma das associações. O teste continua sendo executado até o tempo final de 15 segundos, de forma a garantir que todos as mensagens que estão na fila, durante a falha, sejam entregues.

Para cada configuração de parâmetros o processo é repetido 40 vezes, e o resultado apresentado é a média destas execuções. Ao final das execuções o resultado é gravado em um arquivo texto. Caso necessário, também é possível o registro individual de todas as mensagens enviadas entre os *endpoints*, com registro de sua hora de envio e hora de entrega.

#### **4.3.1. Validação do simulador**

De forma a avaliar o correto funcionamento do simulador, os valores obtidos em sua execução, para medição de tempo máximo de comutação e atraso máximo dos pacotes foram comparados com resultados vistos em trabalhos similares. Os resultados foram comparados aos obtidos em por (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010) e (Brunstrom, A., Eklund, J., 2006). Nestes trabalhos foi usada uma rede real para os testes, com dois computadores executando Linux 2.6.10 trocando mensagens usando dois emuladores de rede implementados em dois computadores rodando FreeBSD com o aplicativo *dummysnet*<sup>2</sup>. A rede usada para o transporte é Ethernet a 100 Mbps.

---

2 O software *dummysnet* é uma ferramenta que permite testes envolvendo o gerenciamento de banda em uma rede IP (Rizzo, L. 2010)

Apesar da validade e utilidade prática do teste usando a rede real, o próprio autor registra a dificuldade na medição exata do momento da comutação para o caminho alternativo, uma vez que as medidas foram feitas observando-se as mensagens entregues à camada de aplicação. Espera-se, portanto, resultados mais exatos com o simulador proposto, já que todos os tempos de todos processos implementados no protocolo estão sendo registrados nos registros de execução dentro do simulador.

A Tabela 4.2 e a Tabela 4.3 comparam os resultados dos trabalhos, para uma avaliação referente ao atraso máximo sofrido pelos pacotes, com vários valores diferentes de latência. Estes resultados se referem a uma rede enviando pacotes a cada 10ms, com tamanho de 250 bytes. O tráfego é unidirecional. A variável RTOmin foi configurada para 80 ms e a variável RTOmax para 10 s. O valor do parâmetro Path.Max.Retrans é igual a 2. Os valores de latência utilizados foram 20 ms, 40 ms e 60 ms.

Tabela 4.2: Comparação de resultados para Atraso Máximo, usando Atraso de SACK de 200ms

Latência	Trabalho de Brunstrom, A. et. al.	Simulador SCTP	Diferença
20 ms	490 ms	541,9 ms	5,10%
40 ms	700 ms	730,6 ms	4,40%
60 ms	1050 ms	1.014,5 ms	-3,40%

Tabela 4.3: Comparação de resultados para Atraso Máximo, usando Atraso de SACK de 0ms

Latência	Trabalho de Brunstrom, A., et al	Simulador SCTP	Diferença
20 ms	490 ms	460,9 ms	-5,90%
40 ms	550 ms	554,8 ms	-0,90%
60 ms	800 ms	834,3 ms	4,30%

Os resultados obtidos são similares ao encontrados nos testes práticos, com tempos algumas vezes inferiores nas medidas feitas pelo simulador proposto. Essa diferença provavelmente se deve ao fato de as medições, no experimento de (Brunstrom, A., Eklund, J., 2006) ter sido feitas usando o resultado observado pelas camadas de aplicação, e não pela observação direta do funcionamento dos estados do protocolo.

#### 4.4. SIMULAÇÕES

As simulações executadas correspondem ao envio bidirecional de pacotes entre os *endpoints*. Cada ponto dos gráficos obtidos corresponde a 40 execuções. Quando não indicado em contrário, os seguintes valores foram usados para as simulações:

- 1 Associação SCTP, ou seja, sem divisão de carga entre várias associações;
- Latência de rede de 20 ms, com variação exponencial com média 1ms. Esse valor permite que as alterações nos parâmetros do protocolo sejam facilmente identificadas nos resultados.
- Mensagens enviadas pela aplicação a cada 2 ms. Esse valor corresponde a um tráfego de cerca de 100.000 BHCA (Busy Hour Call Attempts).
- Tamanho das mensagens de 100 octetos. Esse valor é próximo da média do tamanho das mensagens, considerando o misto de mensagens MAP (*Mobile Application Part*) e ISUP (*ISDN User Part*);
- Parâmetro RTOMin de 10 ms, permitindo assim que o valor da variável RTO oscile, já que o RTOMin é menor que o RTT (*Round-trip Time*) da rede;
- Parâmetro RTOMax de 10 s, conforme RFC 2960;
- Parâmetro Path.Max.Retrans igual a 4, conforme RFC 2960;
- Parâmetro Atraso de SACK de 200 ms, conforme RFC 2960.

Desta forma, foram efetuadas várias simulações, cada uma procurando identificar o efeito que cada parâmetro de perfil de rede ou do protocolo tem sobre os indicadores de desempenho observados. São elas:

- Simulação 1 – Utilização de múltiplas associações SCTP em paralelo;
- Simulação 2 – Efeito da quantidade de mensagens a ser enviada;

- Simulação 3 – Efeito do tamanho das mensagens;
- Simulação 4 – Efeito da latência de rede;
- Simulação 5 – Efeito da variação da quantidade de retransmissões – parâmetro *path.Max.Retrans*;
- Simulação 6 – Efeito da alteração no parâmetro de atraso de SACK - *SACK Delay*;
- Simulação 7 – Efeito da alteração do parâmetro *RTOmin*;
- Simulação 8 – Efeito da alteração do parâmetro *RTOmax*.

#### **4.4.1. Simulação 1 - Entre topologias *multi-homing***

No estabelecimento da conexão SS7 sobre SIGTRAN, normalmente há a opção de se definir quantas associações podem ser configuradas em paralelo, normalmente envolvendo múltiplos endereços IP em cada elemento de rede. A quantidade de placas e endereços IP disponíveis para tráfego de sinalização é dependente das capacidades físicas do equipamento envolvido e da forma de implementação do protocolo por cada fabricante. A distribuição do tráfego entre várias associações em paralelo muitas vezes é necessária devido à capacidade de processamento de tráfego de cada uma das placas físicas dos equipamentos envolvidos. Assim, é comum a existência de 8 ou mais associações SCTP operando em paralelo, cada uma delas com 2 ou 4 caminhos possíveis.

A utilização de várias associações SCTP em paralelo também aumenta a segurança, uma vez que distribui o tráfego por uma quantidade maior de recursos físicos, ainda que a rede IP envolvida seja provavelmente a mesma.

Deve-se tirar proveito da diversidade de configuração IP de cada uma das associações em paralelo, de forma a fazer com que o caminho primário de uma associação seja o caminho alternativo de outra. Desta forma, em caso de falha em um dos caminhos, apenas metade das associações serão afetadas pelo problema, reduzindo a quantidade de mensagens – e conseqüentemente sessões dos protocolos das camadas de sinalização afetadas – que

sofrerão atraso devido à falha. Uma sugestão de implementação está indicada na Tabela 4.4 e Figura 4.8.

Tabela 4.4 - Implementação de divisão de carga em múltiplos caminhos

Associação	Caminho Primário	Caminho Alternativo
X	Rede 1	Rede 2
Y	Rede 2	Rede 1

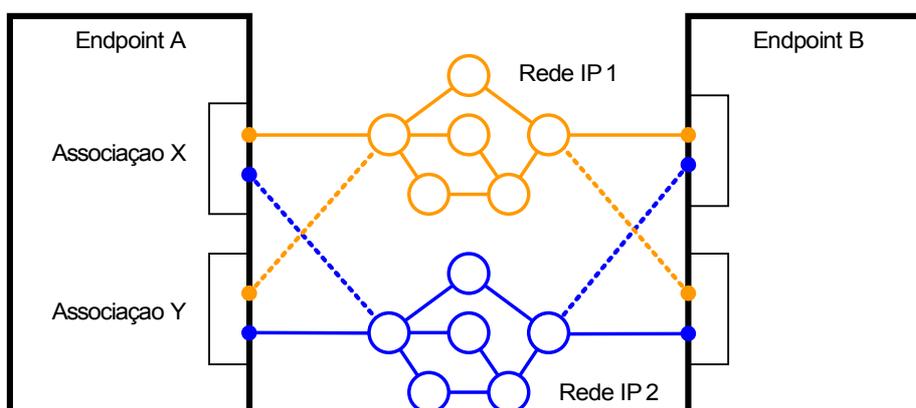


Figura 4.8 - Implementação de divisão de carga em múltiplos caminhos

A diversidade de rede, através do uso de *switches*, roteadores e recursos físicos independentes para cada caminho, já é um argumento suficiente para motivar o uso de pelo menos 2 associações SCTP em paralelo.

Ainda assim, há outros ganhos intrínsecos ao funcionamento do protocolo, quando se usa associações SCTP paralelas. A simulação a seguir visa avaliar se há alguma diferença de desempenho ao se trabalhar com associações paralelas. Apesar das associações trabalharem de forma totalmente independente entre si, o tráfego que cada uma delas irá cursar é menor com o aumento do número de conexões. Assim, na prática, busca-se observar se a variação do tráfego em uma associação tem algum efeito no seu desempenho quando ocorre uma falha na rede IP.

A RFC 2960 (Stewart, R., Xie, Q., Morneault, K. et al., 2000) prevê que, após o esgotamento do temporizador T3-rtx, seja enviado um pacote SCTP com a quantidade máxima de *chunks* que couberem em um único pacote IP (Stewart, R., Xie, Q., Morneault, K. et al., 2000), (Stewart, R., Xie, Q., 2001). Essa quantidade é limitada ao PMTU (*Path*

*Maximum Transmission Unit*) do caminho a ser utilizado para a retransmissão. Considerando-se o cenário A com uma associação SCTP *multi-homed*, e o cenário B onde há  $n$  associações SCTP *multi-homed* em paralelo, pode-se imaginar que, sendo o tráfego por associação  $n$  vezes menor no cenário B em relação ao cenário A, a primeira retransmissão após a falha terá um desempenho potencialmente melhor, já que serão  $n$  associações fazendo a retransmissão dos pacotes no caminho alternativo em paralelo, considerando-se que todas as associações sofreram o efeito da falha.

Na Figura 4.9 pode-se observar o efeito que a distribuição do tráfego entre várias associações tem no desempenho do protocolo, no que se refere ao tempo máximo para comutação ao caminho reserva e no atraso máximo dos pacotes.

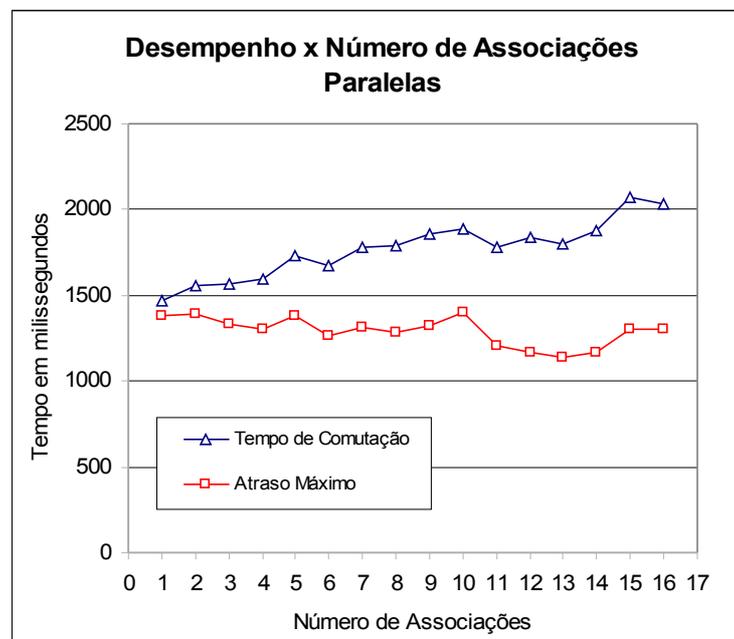


Figura 4.9 - Relação entre o desempenho e o número de associações paralelas

Observe-se que, como esperado, o tempo máximo de comutação aumenta levemente com a quantidade de associações paralelas, devido à redução de tráfego em cada uma delas.

No caso do atraso máximo sofrido pelos pacotes, apesar do aumento do tempo de comutação, pode-se observar o ganho gerado pela quantidade menor de pacotes a ser retransmitida, o que faz com que o processo de retransmissão seja mais eficiente.

#### 4.4.2. Simulação 2 – Variação do intervalo entre as mensagens enviadas

Com o objetivo de se ter uma visão mais completa do resultado da simulação 1, foi executada a simulação 2. Neste teste objetiva-se ver com mais clareza o efeito do intervalo entre as mensagens nos indicadores de desempenho.

Os resultados podem ser vistos na Figura 4.10 e Figura 4.11. Na Figura 4.10 o resultado é apresentado como função do intervalo entre os pacotes em milissegundos, e na Figura 4.11 os mesmos dados são apresentados em função da frequência de envio dos pacotes, em MSU (*Message Signal Unit*) por segundo.

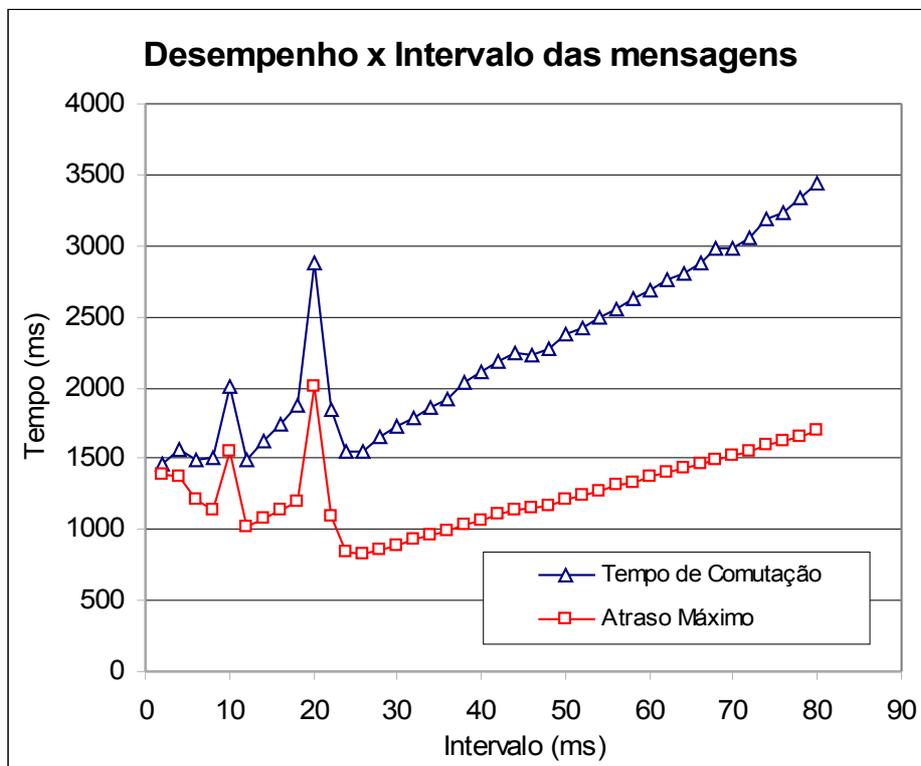


Figura 4.10 - Efeito do Intervalo de Envio (visão intervalo)

Da mesma forma que na simulação anterior, neste resultado pode-se observar o aumento do tempo de comutação conforme o intervalo entre os pacotes aumenta. Esse aumento no tempo deve-se à demora na detecção da falha, uma vez que ela é feita através da falta dos pacotes recebidos nos *endpoint* de destino. Quanto menos pacotes trafegam entre os *endpoints*, mais demorada é a detecção da falha de rede.

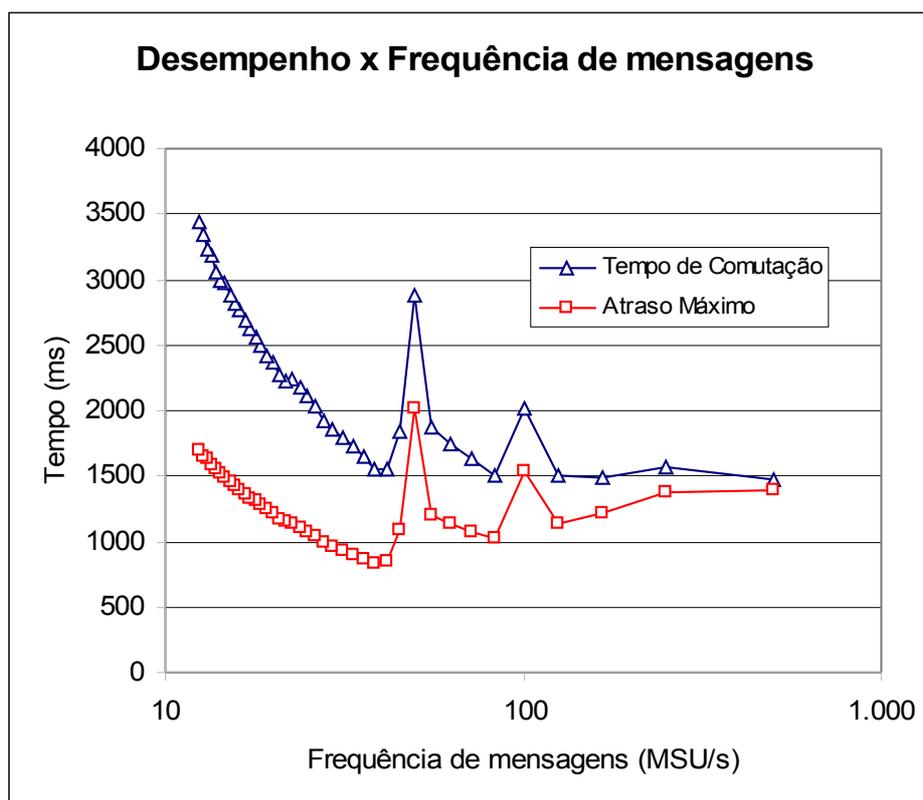


Figura 4.11 - Efeito do Intervalo de Envio (visão frequência)

Nesta segunda simulação trabalha-se com valores para o intervalo de pacotes bem maiores. Observe-se que até o intervalo de 30 milissegundos o desempenho do protocolo, no que se refere ao atraso máximo, aumenta com o crescimento do intervalo. Isso se deve ao fato de a retransmissão ser mais eficiente devido à redução da quantidade de pacotes a serem retransmitidos. A partir deste ponto, porém, esse efeito desaparece, e o atraso máximo passa a acompanhar proporcionalmente o valor do tempo de comutação, conforme a figura Figura 4.12. Esse é o ponto, para os parâmetros adotados, em que o processo de retransmissão atinge a sua eficiência máxima na simulação. Para essa simulação, considerando-se que o tráfego é composto por mensagens de 100 bytes, e que um pacote SCTP é capaz de transmitir até 15 mensagens (15 *chunks*), esse ponto indica que não há mais do que 15 mensagens esperando na fila, e todas foram retransmitidas no pacote gerado no esgotamento do temporizador T3-rtx.

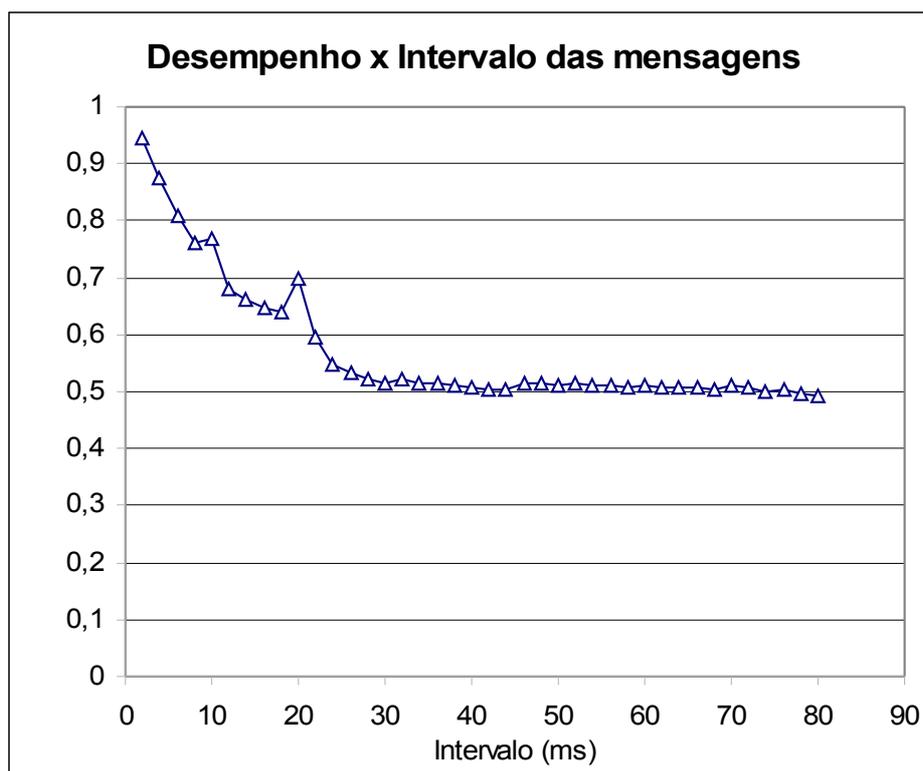


Figura 4.12 - Razão entre o atraso máximo e o tempo de comutação em função do intervalo entre as mensagens

#### 4.4.3. Simulação 3 – Variação do tamanho das mensagens.

Com o objetivo de se avaliar o efeito do tamanho das mensagens sobre os indicadores de desempenho, foi feita a terceira simulação. Foram comparados os resultados obtidos com mensagens de tamanhos variando entre 50 e 250 bytes. As mensagens MAP (*Mobile Application Part*) e CAMEL (*Customised Applications for Mobile networks Enhanced Logic*) têm entre 66 e 216 octetos nos exemplos do anexo A. Ainda que hajam mensagens ISUP (*ISDN User Part*) de tamanho menor (até 16 octetos) estas mensagens estão sempre acompanhadas de mensagens de outros protocolos, conforme mostrado no item 2.2.

Embora o tamanho dos pacotes não tenha efeito sobre o tempo de detecção da falha da rede e conseqüentemente sobre o tempo de comutação, observa-se que pacotes menores geraram um desempenho melhor no que se refere ao atraso máximo (Figura 4.13).

Essa condição ocorre devido à forma com que a retransmissão é efetuada. Quando o temporizador T3-rtx é expirado, o *endpoint* que detectou a falha gera um pacote com todas

as mensagens a serem retransmitidas, porém limitado ao tamanho máximo do pacote IP.

Embora não se tenha controle sobre o tamanho das mensagens que uma aplicação envia para a rede de sinalização, pode-se observar que protocolos com mensagens menores podem ser menos afetados por uma falha de rede do que protocolos com mensagens maiores, ainda que o tempo de comutação para o caminho reserva observado nos dois casos seja igual.

Comparando-se, por exemplo, o protocolo ISUP com o protocolo MAP, o primeiro tem mensagens que tipicamente são menores do que 30 octetos (ou bytes), enquanto o protocolo MAP chega facilmente a mensagens de 200 octetos. A média observada no exemplo do item 2.2. mostra o protocolo ISUP com uma média de 26 octetos por mensagem, enquanto os protocolos MAP e CAMEL tiveram média de 140 e 127 octetos, respectivamente.

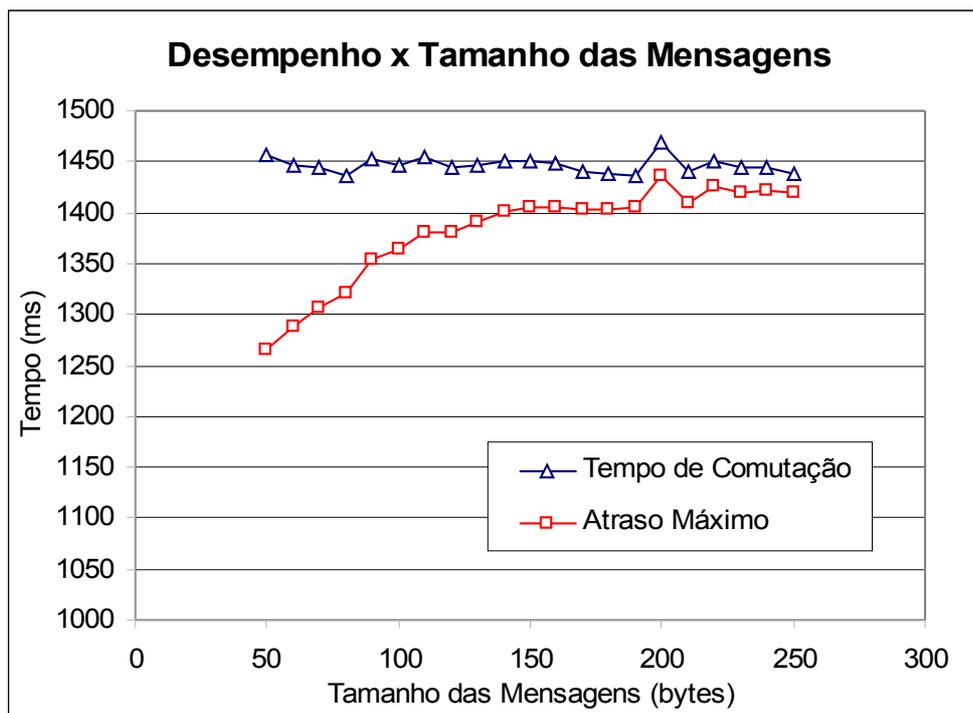


Figura 4.13 - Relação entre o desempenho e o tamanho das mensagens

Como a troca de sinalização entre os elementos de rede normalmente é feita através dos PTSs, mensagens de tamanhos diferentes são enviadas misturadas, sendo que, como pode-se observar no exemplo mostrado no item 2.2. , um cenário de chamada típico envolve muitas mensagens MAP e CAMEL, e poucas mensagens ISUP. Porém, caso haja enlaces

em que se trafegue somente o protocolo ISUP, poderá ser observado um ganho de desempenho no que se refere ao atraso máximo das mensagens em caso de comutação para o caminho alternativo.

#### **4.4.4. Simulação 4 – Efeito da latência de rede**

A latência de rede, ou seja, o atraso imposto pela rede aos pacotes, gera um efeito linear tanto sobre o tempo de comutação como sobre o atraso máximo dos pacotes. Essa situação é explicada pelo fato de todo o processo de detecção de falhas e troca de informações de recebimento (envio da informação SACK do *endpoint* de destino para o *endpoint* de origem) é afetada por esse parâmetro de rede.

Na Figura 4.14 vemos o efeito linear imposto pela latência nos indicadores de tempo de comutação e atraso máximo dos pacotes. Ambos os indicadores crescem proporcionalmente com o crescimento da latência.

Comparando os valores relativos ao tempo máximo de comutação e atraso máximo das mensagens, vemos que, com o aumento da latência, ambos os valores vem a ser cerca de 62 vezes o valor da latência para as condições do teste. Isso se deve à configuração utilizada na rede, especificamente o valor do parâmetro Path.Max.Retrans, que é igual a 4. Nesta situação, com o fator de *back-off* aplicado igual a 2, o valor de RTO dobra a cada retransmissão, gerando um tempo total igual a  $1+2+4+8+16$  vezes o valor de RTT, ou seja 31 vezes o valor de RTO e 62 vezes o valor da latência da rede, considerando que o RTO é igual a duas vezes o valor da latência. Isso é demonstrado na Tabela 4.5.

Tabela 4.5 - Tempo dos eventos até a comutação para o caminho reserva

Evento	Valor das variáveis	Momento
Momento da falha	$RTO = RTT$	0
Deteção da falha, Primeira retransmissão	$RTO = 2 \times RTT$	$RTT$
Segunda retransmissão	$RTO = 2 \times RTT = 4 \times RTT$	$RTT + 2 \times RTT = 3 \times RTT$
Terceira retransmissão	$RTO = 2 \times RTT = 8 \times RTT$	$3 \times RTT + 4 \times RTT = 7 \times RTT$
Quarta retransmissão	$RTO = 2 \times RTT = 16 \times RTT$	$7 \times RTT + 8 \times RTT = 15 \times RTT$
Comutação para o caminho alternativo		$15 \times RTT + 16 \times RTT = 31 \times RTT$ $= 62 \times \text{latência}$

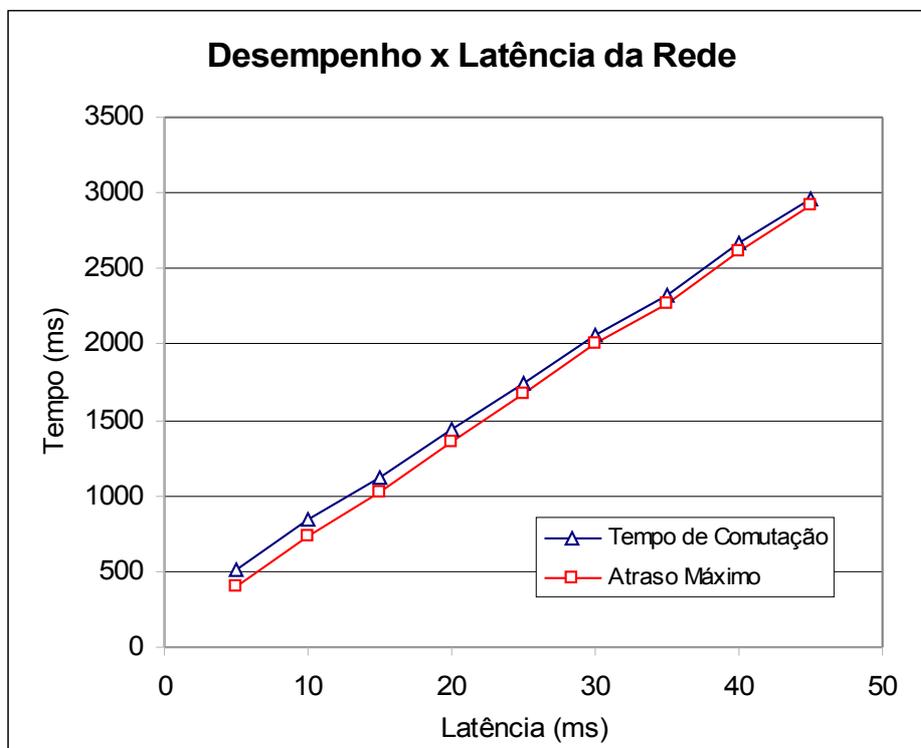


Figura 4.14 - Desempenho em função da latência de rede

Como na simulação efetuada o valor da variação da latência é absoluto, essa variação é mais expressiva para valores menores de latência, o que se reflete nos valores mais altos que aparecem no gráfico da Figura 4.15.

#### 4.4.5. Simulação 5 – Efeito do parâmetro Path.Max.Retrans

Como visto na simulação 4, o responsável pelo crescimento exponencial do valor do RTO é o fato de que, a cada retransmissão, o valor deste ser multiplicado por 2. Assim, o valor do parâmetro Path.Max.Retrans tem um grande efeito nos indicadores de desempenho do protocolo. Na Figura 4.16 pode-se ver o efeito exponencial do crescimento do tempo de comutação e atraso máximo em função do parâmetro Path.Max.Retrans.

Os dois indicadores de desempenho são afetados de forma equivalente pelo aumento do parâmetro Path.Max.Retrans. Podemos observar que o valor do atraso máximo se afasta gradativamente do tempo de comutação, conforme o valor de Path.Max.Retrans cresce. Com o crescimento da quantidade de retransmissões, temos os pacotes mais antigos sendo enviados ainda antes do momento da comutação, melhorando assim, ainda que pouco, o desempenho do indicador de atraso máximo das mensagens.

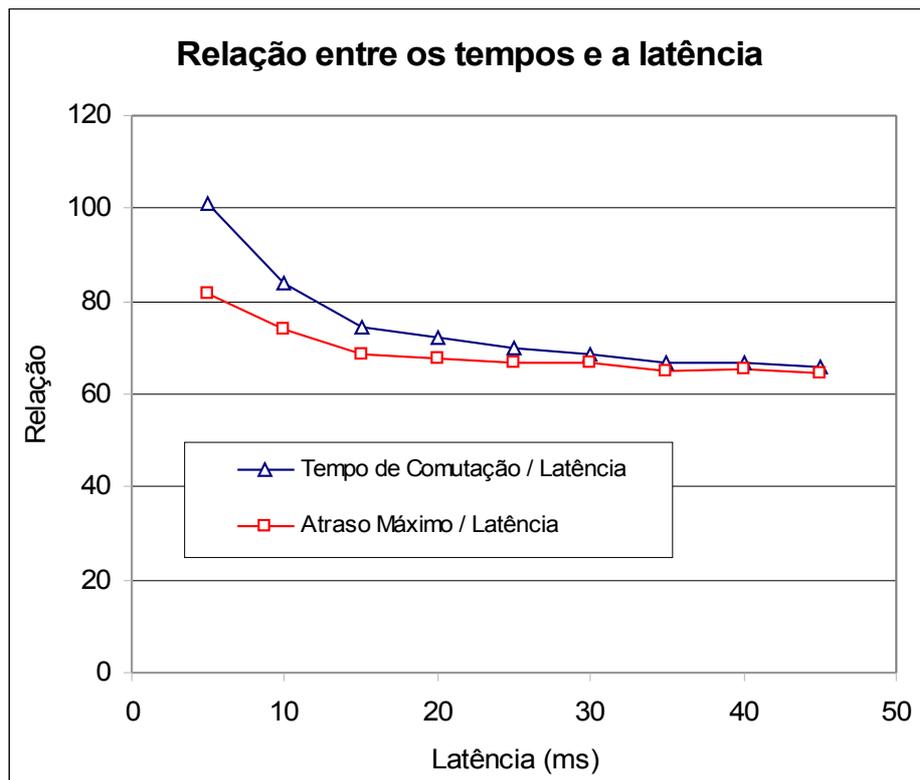


Figura 4.15 - Relação entre os tempos de comutação e latência, em função da latência

#### 4.4.6. Simulação 6 – Efeito de alteração do parâmetro de Atraso de SACK

Na simulação em que se comparam vários valores de atraso de SACK (*SACK Delay*) observa-se que não há diferença significativa no desempenho do protocolo. Esse resultado já era esperado, uma vez que o tráfego de sinalização é bidirecional. Essa característica do tráfego faz com que sempre haja pacotes de dados sendo enviados em ambas as direções. Como a informação de SACK é agrupada a mensagens de dados enviadas do *endpoint* de destino para o *endpoint* de origem, não ocorre a situação em que o temporizador de SACK do *endpoint* de destino se esgote, gerando um pacote específico que contenha o *chunk* SACK de retorno. Mesmo com a redução do valor do atraso de SACK para 20 ms não houve variação do desempenho. Essa situação pode ser observada na Figura 4.17.

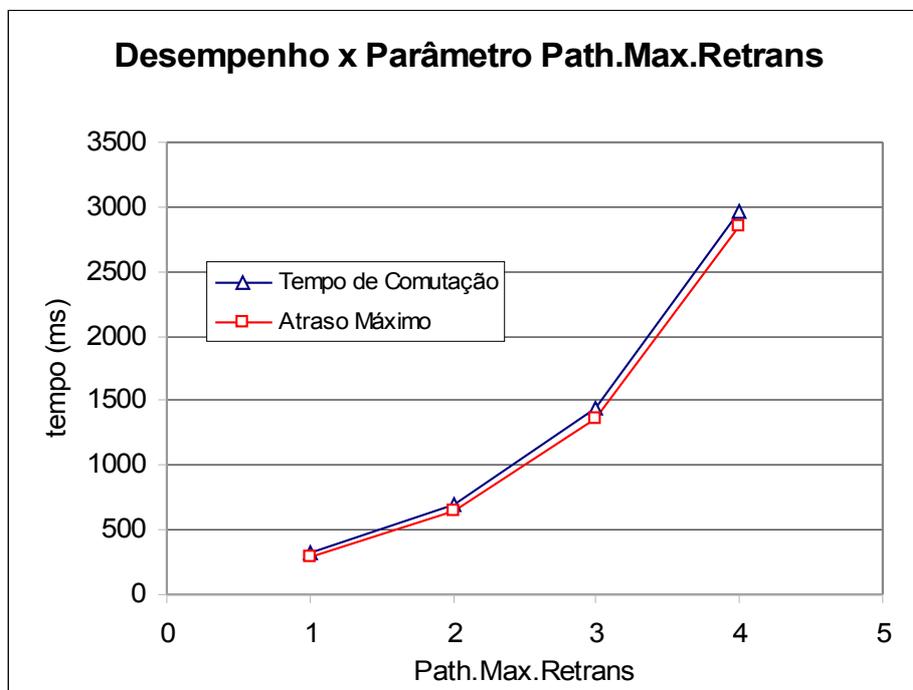


Figura 4.16 - Tempo de comutação x PMR

Observe-se que esse resultado só é válido para tráfego bidirecional - caso do tráfego de sinalização - e que tenha o intervalo de envio entre os pacotes típico abaixo de 100ms. Isso é necessário porque a informação de SACK é enviada após o recebimento do segundo *chunk* de dados recebido pelo destino. Porém, caso o intervalo das mensagens seja superior a 100ms, especificamente o tráfego enviado do *endpoint* de destino para o *endpoint* de origem, esse parâmetro passa a ter um efeito relevante. Essa, porém, não é a característica do tráfego de sinalização no núcleo das redes de telecomunicações atualmente.

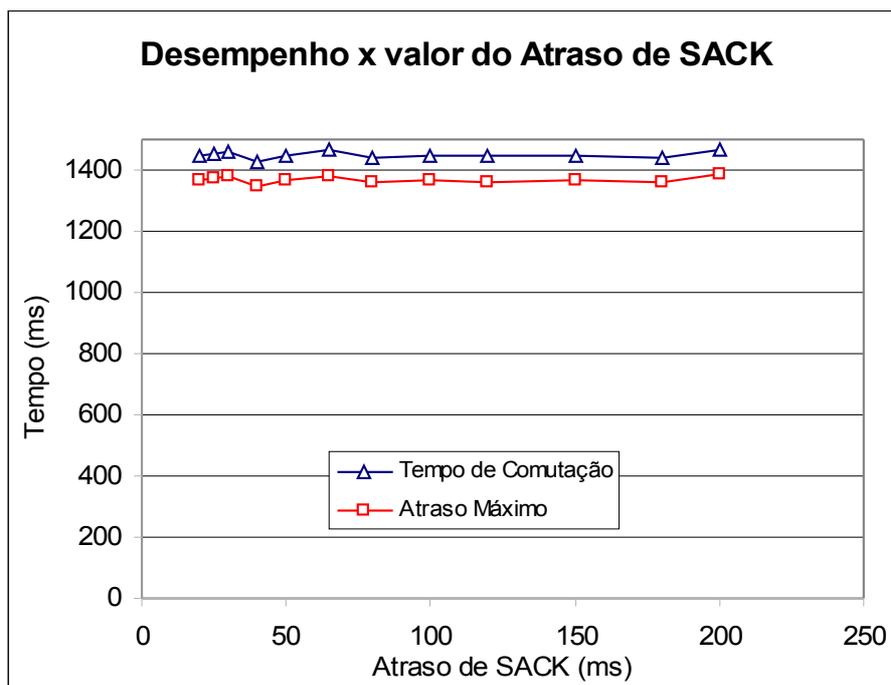


Figura 4.17 - Efeito do Atraso de SACK

#### 4.4.7. Simulação 7 – Efeito de alteração do parâmetro RTOmin

A variação do parâmetro RTOmin é provavelmente uma das que mais traz efeito sobre o desempenho do protocolo. Na Figura 4.18 pode-se observar como a utilização de valores menores gera um ganho tanto no tempo de comutação quanto como no atraso máximo. É importante observar que, na simulação acima, valores de RTOmin menores do que 50ms não melhoram o desempenho do protocolo, enquanto valores maiores do que esse geram um aumento linear constante tanto do tempo de comutação como do atraso máximo. Esse valor corresponde ao ponto onde o RTT (*Round-trip Time*) da rede é igualado ao valor do parâmetro RTOmin.

Quando se usa, para o parâmetro RTOmin, valores menores do que o RTT da rede, o protocolo irá manter o RTO “flutuante”, ou seja, ele irá acompanhar o RTT da rede. Quando se usa valores maiores do que o RTT, estamos dizendo ao protocolo que deve-se considerar o valor de RTOmin ao invés do valor RTT observado na rede.

O estudo de (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010) sugere que o valor de RTOmin não deve ser menor do que o RTT da rede, indicando o uso de RTOmin sempre maior do que duas vezes o valor de RTT. Esse valor iria prevenir que a perda ou

atraso de um ou dois pacotes indicasse ao protocolo que houve uma efetiva perda de conectividade. Isso irá gerar a retransmissão de mensagens, aumentando o tráfego na rede de maneira desnecessária.

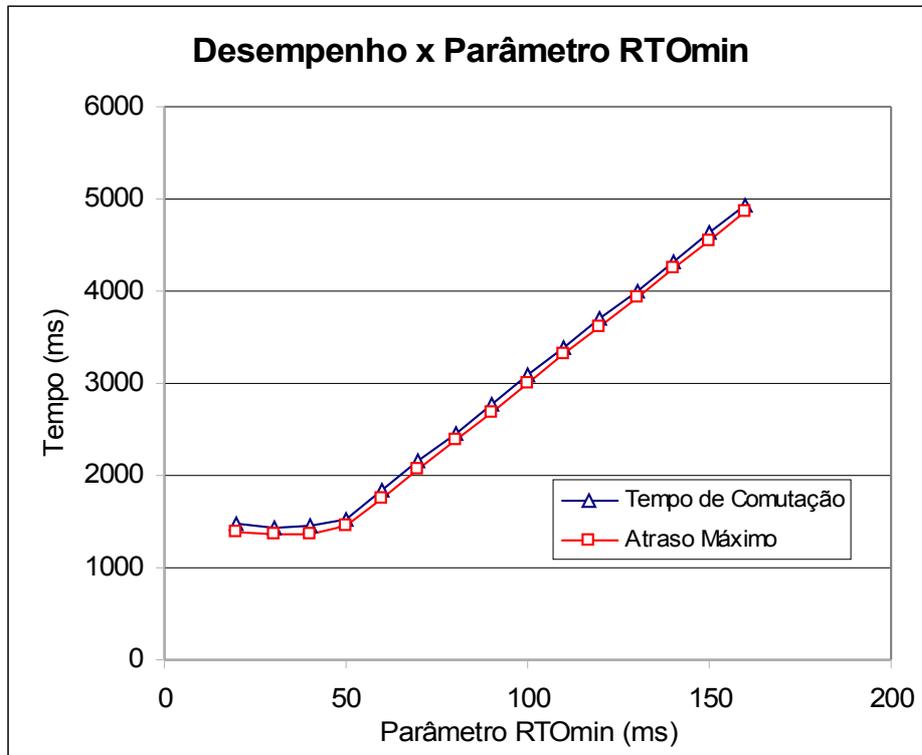


Figura 4.18: Efeito do parâmetro RTOMin

Como indicado no item 3.4.1., o valor da variável RTO não é exatamente o valor do RTT observado na rede, e sim o resultado de um algoritmo que visa garantir a estabilidade do funcionamento do protocolo. A variável RTO é função do RTT e também de sua variação. Assim, se por algum motivo o RTT da rede varia, ocorre também uma variação da variável RTO.

#### 4.4.8. Simulação 8 – Efeito de alteração do parâmetro RTOMax

A variação do parâmetro RTOMax mostrou um ganho considerável no desempenho do protocolo. Conforme observado nas simulações anteriores, o aumento do parâmetro Path.Max.Retrans gera um crescimento exponencial do tempo total de comutação do protocolo, e conseqüentemente do atraso máximo, já que a cada retransmissão o valor da variável RTO é multiplicado por dois.

O parâmetro RTOMax pode ser usado para reduzir o efeito exponencial, definindo um valor máximo para o valor de RTO, conforme descrito no item 4.2.2.6. Assim, pode-se usar esse parâmetro para limitar o crescimento sem que seja necessário alterar o valor de *back-off* do protocolo, o que exigiria alterações na implementação deste, o que, justamente, não é o escopo deste trabalho.

A Figura 4.19 mostra o desempenho do protocolo, no que se refere ao tempo de comutação, para vários valores dos parâmetros Path.Max.Retrans e RTOMax. O resultado desta simulação é muito didático em apresentar o modo de funcionamento do protocolo SCTP.

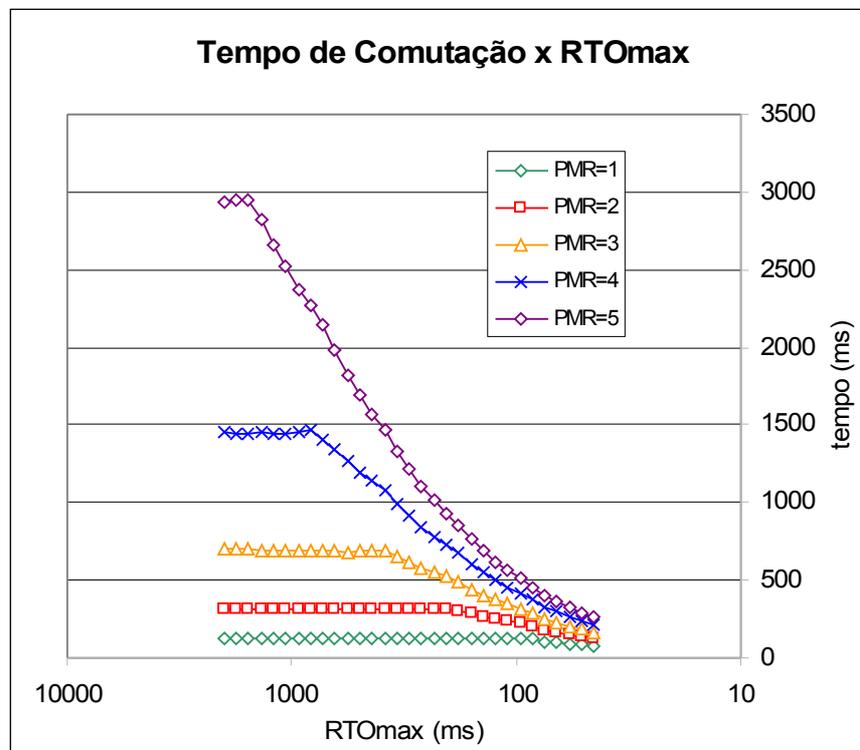


Figura 4.19 - Tempo de comutação em função do RTOMax (exponencial)

As simulações foram executadas com latência de 20ms, e RTOMin abaixo deste valor, ou sejam 10ms. Nestas condições, temos a seguinte situação:

$$\text{Latência} = 20 \text{ ms} \tag{4.1}$$

Considerando-se a variação da latência com uma distribuição exponencial de 1ms de esperança, o algoritmo de cálculo do RTO gera valores em torno de 45ms. Após a primeira retransmissão, o valor de RTO é dobrado, o que gera um novo RTO de 90ms. Chamaremos

de RTO o valor do RTO após cada retransmissão.

Assim:

$$\text{Latência} = 20 \text{ ms} \quad (4.2)$$

$$\text{RTT} = 40 \text{ ms} \quad (4.3)$$

$$\text{RTO} = 45 \text{ ms} \quad (4.4)$$

$$\text{RTO}_1 = 90 \text{ ms} \quad (4.5)$$

$$\text{RTO}_2 = 180 \text{ ms} \quad (4.6)$$

$$\text{RTO}_3 = 360 \text{ ms} \quad (4.7)$$

$$\text{RTO}_4 = 720 \text{ ms} \quad (4.8)$$

$$\text{RTO}_5 = 1440 \text{ ms} \quad (4.9)$$

O tempo de comutação ( $t_c$ ) para cada valor de Path.Max.Retrans (PMR) é a soma do RTO com os RTOs usados após cada retransmissão:

$$t_{c_{\text{PMR}=1}} = \text{RTT} + \text{RTO}_1 = 40 + 90 = 130 \text{ ms} \quad (4.10)$$

$$t_{c_{\text{PMR}=2}} = \text{RTT} + \text{RTO}_1 + \text{RTO}_2 = 40 + 90 + 180 = 310 \text{ ms} \quad (4.11)$$

$$t_{c_{\text{PMR}=3}} = \text{RTT} + \text{RTO}_1 + \text{RTO}_2 + \text{RTO}_3 = 670 \text{ ms} \quad (4.12)$$

$$t_{c_{\text{PMR}=4}} = \text{RTT} + \text{RTO}_1 + \text{RTO}_2 + \text{RTO}_3 + \text{RTO}_4 = 1390 \text{ ms} \quad (4.13)$$

$$t_{c_{\text{PMR}=5}} = \text{RTT} + \text{RTO}_1 + \text{RTO}_2 + \text{RTO}_3 + \text{RTO}_4 + \text{RTO}_5 = 2830 \text{ ms} \quad (4.14)$$

Os tempos observados na simulação correspondem aos valores indicados acima. Observe-se que com tempos de latência altos para o valor  $\text{RTO}_{\text{max}}$  o comportamento do protocolo não sofre alterações, já que o  $\text{RTO}_{\text{max}}$  está configurado para um valor maior do que o maior valor atingido pelo protocolo. Especificamente, o valor inicial usado na simulação, de 2000 ms, é superior ao  $\text{RTO}_5$ , que é o maior valor atingido pela variável nesta situação, após a 5ª retransmissão.

Conforme o valor do  $\text{RTO}_{\text{max}}$  decresce, observa-se que o tempo de comutação começa a

decrecer quando o RTOMax fica abaixo de 1500 ms, que é exatamente o valor gerado para o RTO após a quinta retransmissão ( $RTO_5$ ). Porém o tempo de comutação para o valor  $PMR=4$  só é reduzido quando o RTOMax fica abaixo de 800 ms, que é o valor atingido pela variável RTO após a 4a comutação. Essa situação se repete conforme o valor de RTOMax é reduzido.

Observa-se a distância entre as curvas relativas ao tempo de comutação se aproximando com a redução do RTOMax, justamente pela limitação imposta à variável RTO do protocolo. A diferença entre as curvas, que aparece crescendo exponencialmente conforme o valor do parâmetro Path.Max.Retrans aumenta, passa a diminuir pela limitação do valor do RTO.

Conforme o valor de RTOMax se reduz, ele passa a influenciar progressivamente o desempenho também do protocolo para valores menores do parâmetro Path.Max.Retrans, reduzindo de forma consistente o tempo de comutação para o caminho alternativo. As figuras a seguir demonstram essa situação de diversas perspectivas diferentes. A Figura 4.20 e a Figura 4.21 apresentam os resultados em uma escala de eixo X linear e logarítmica respectivamente, onde é visível o efeito da redução de RTOMax para os valores maiores da variável. Na Figura 4.22 o mesmo aspecto é visível do ponto de vista do atraso máximo sofrido pelas mensagens.

A Figura 4.23 apresenta a relação entre o tempo de comutação e o valor do parâmetro Path.Max.Retrans (PMR), para vários valores do parâmetro RTOMax. Observa-se que a curva, que com valores altos de RTOMax é exponencial devido ao fator de *back-off* do protocolo, vai se tornando linear com a redução do valor deste parâmetro, até se tornar totalmente linear.

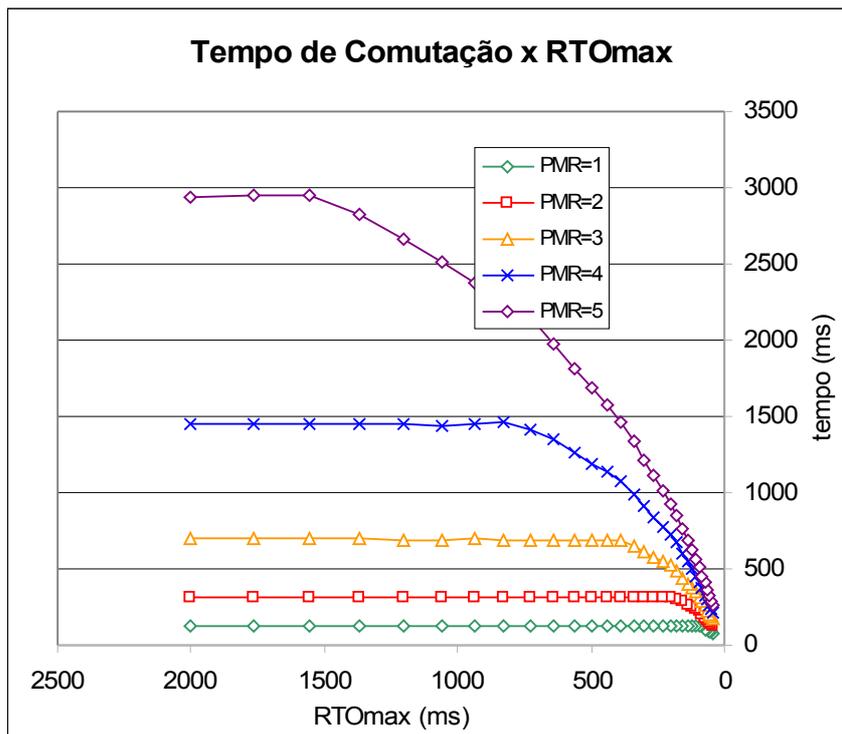


Figura 4.20 - Tempo de comutação em função do RTOmax (linear)

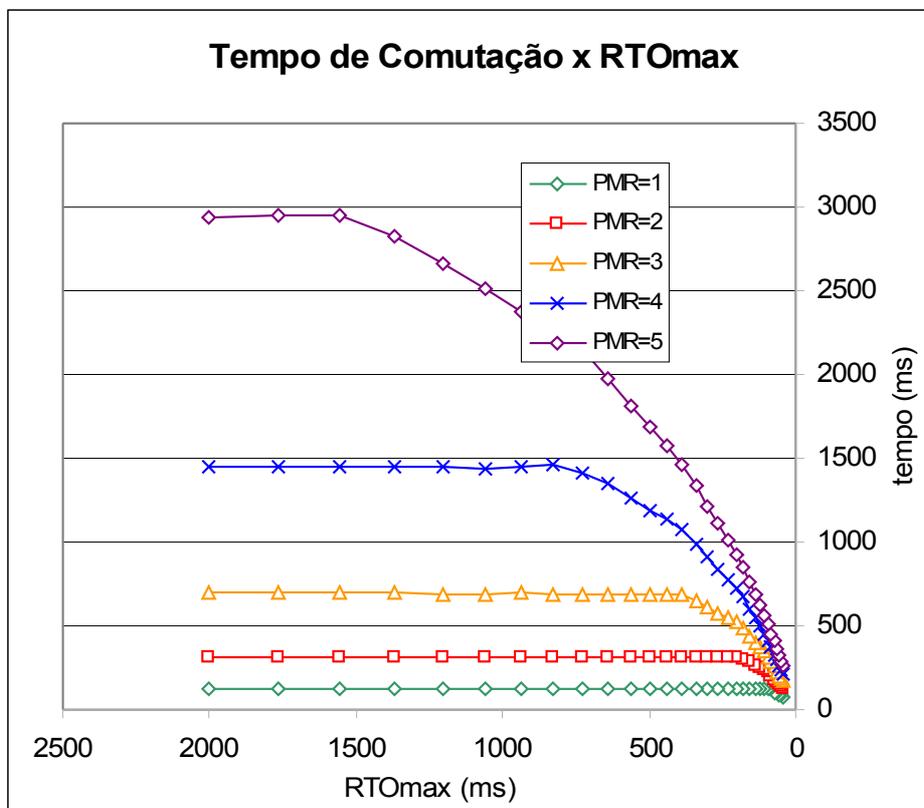


Figura 4.21: Tempo de comutação em função do RTOmax (logarítmico)

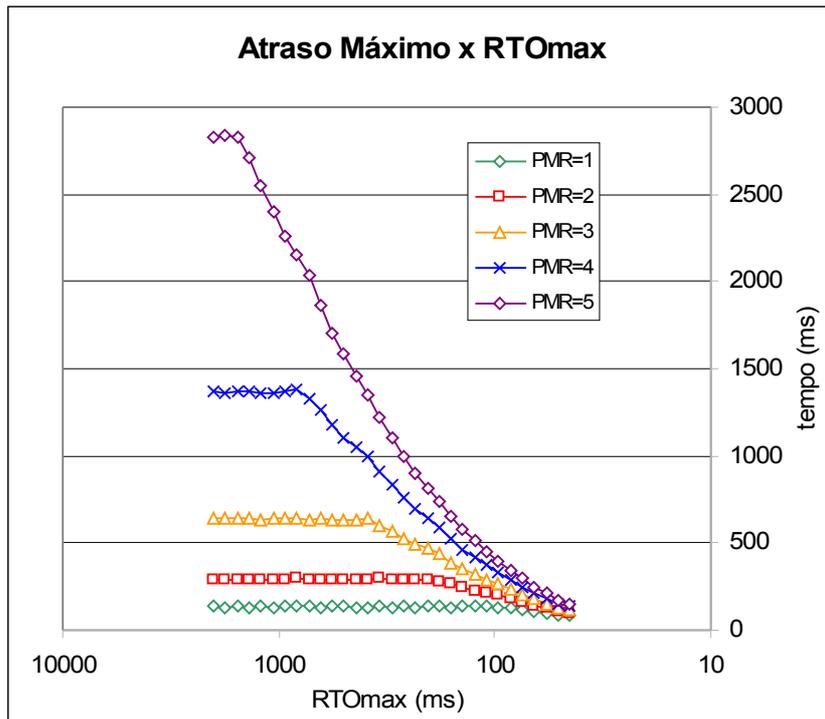


Figura 4.22 - Atraso máximo em função do RTOmax

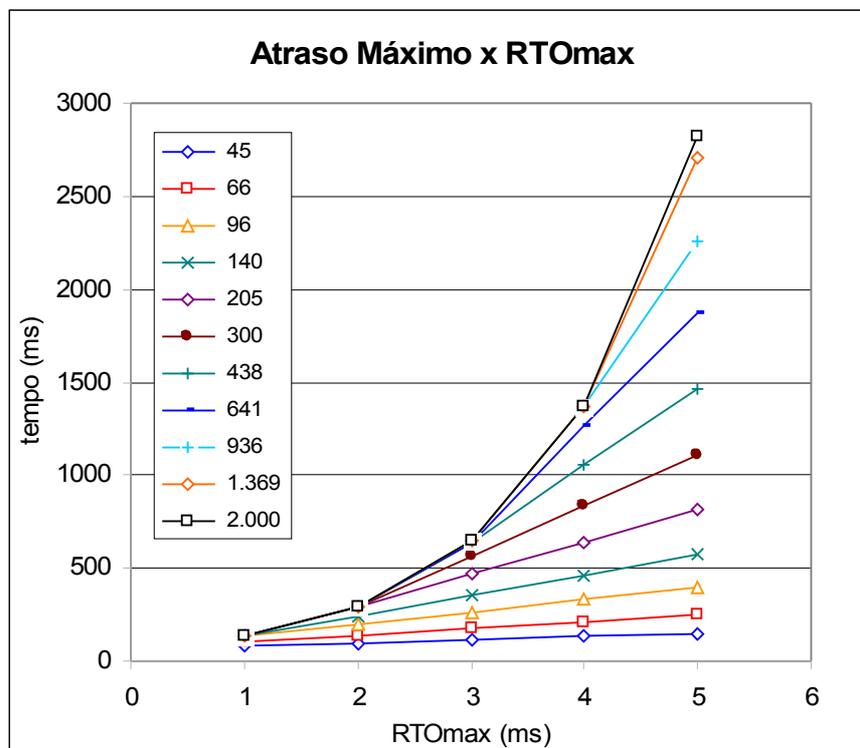


Figura 4.23 - Efeito do valor de RTOmax no tempo de comutação, para vários valores de Path.Max.Retrans

## **4.5. AVALIAÇÃO DOS RESULTADOS**

Observando os resultados das simulações efetuadas, conclui-se que é possível melhorar o desempenho do protocolo em caso de falha de uma forma bastante relevante, sem comprometer o seu funcionamento, pelo uso da topologia correta de rede e pelo ajuste adequado dos parâmetros RTOmin, RTOmax e Path.Max.Retrans. Os principais ganhos encontrados estão resumidos:

### **4.5.1. Ganho na topologia**

Em caso de tráfego baixo, reduzir a quantidade de associações simultâneas, visando maximizar o tráfego em cada uma delas. A utilização de 2 associações paralelas garante o melhor resultado, desde que não haja limitações de tráfego por porta IP nos *endpoints*.

### **4.5.2. Ajuste no parâmetro RTOmin**

Esse parâmetro deve ser reduzido para que fique próximo ao dobro do valor do RTT da rede envolvida. Caso esse ajuste não seja suficiente, pode-se baixar o valor de RTOmin abaixo do valor de RTT, para que a variável RTO tenha o seu valor flutuante conforme as condições de rede.

### **4.5.3. Ajuste no parâmetro RTOmax**

Existe um grande ganho na redução do RTOmax, porém esse ajuste deve ser feito com cuidado, uma vez que ele reduz o efeito exponencial do fator de *back-off* do protocolo. O fator de *back-off* exponencial ajuda a prevenir o congestionamento de rede gerado por retransmissões, de forma que esse recurso deve ser usado somente em caso de redes isoladas. Porém, essa é a situação das redes de sinalização em telecomunicações. O valor inicialmente proposto pela RFC2960 (Stewart, R., Xie, Q., Morneault, K. et al., 2000) para esse parâmetro é de 10 segundos, valor dificilmente atingido pela variável RTO quando se usam valores ajustados para RTOmin.

#### **4.5.4. Ajuste no parâmetro Path.Max.Retrans**

O ajuste neste parâmetro, juntamente com o ajuste no parâmetro RTOmax pode gerar um ganho significativo no desempenho do protocolo. Para que esse ajuste possa ser feito com segurança, é importante avaliar as condições da rede IP envolvidas na sinalização. A redução do valor deste parâmetro fará com que haja uma quantidade menor de re-tentativas antes da comutação para o caminho reserva. O ajuste excessivo deste parâmetro pode resultar em uma comutação para o caminho reserva desnecessária. Considere-se, no entanto, que o valor inicialmente proposto para o protocolo, de 5 re-tentativas, é alto para redes de sinalização de telecomunicações, sendo que há espaço para alterações.

#### **4.6. CONCLUSÕES**

O desempenho do protocolo SCTP é afetado pela configuração de seus parâmetros e também pelo perfil do tráfego a ser transportado. Especificamente no que se refere ao tempo máximo de comutação para o caminho reserva, a topologia da rede, o perfil de tráfego a ser transportado, e os valores utilizados para os parâmetros RTOmin, RTOmax e Path.Max.Retrans afetam o desempenho do protocolo. Já o parâmetro Atraso de SACK não tem efeito sobre o desempenho do protocolo, uma vez que ele tem características transacionais, ou seja, sempre já sinalização sendo transportada nas duas direções.

Através das simulações efetuadas pode-se confirmar que o parâmetro Atraso de SACK não tem efeito real sobre o desempenho do protocolo, quando se considera o transporte de mensagens de sinalização de redes de telecomunicações. Observou-se também que os parâmetros originais propostos para o protocolo SCTP na RFC 2960 não são adequados para uso em redes de sinalização, e que ajustes nos valores dos parâmetros são necessários. Dentro destes, os maiores efeitos podem obtidos com ajustes nos parâmetros RTOmin, RTOmax e Path.Max.Retrans.

No próximo capítulo serão apresentadas propostas para os valores dos parâmetros avaliados. Essas propostas procurarão achar um conjunto de parâmetros adequado para garantir o atendimento dos requisitos das redes de sinalização para diversos valores de latência diferentes. Assim, procura-se garantir o atendimento aos requisitos independentemente das características da rede usada para o transporte.

## 5. PROPOSTAS DE AJUSTES NOS PARÂMETROS

As principais aplicações em redes de sinalização SS7 atualmente são as que usam o protocolo ISUP (ISDN User Part) e TCAP (Transaction Capabilities Application Part). O protocolo ISUP é utilizado para controle do transporte de chamadas de voz entre centrais telefônicas. O protocolo TCAP é o responsável por fazer a troca de sinalização entre elementos de controle da rede móvel. Embora não haja requisitos explícitos para esses protocolos, observa-se que o máximo atraso que um pacote deva sofrer (maximum MSU transfer time) esteja sempre na faixa entre 600 ms e 1 s (Brunstrom, A., Grinnemo, K., 2005).

Para conseguir chegar a atingir o desempenho comparável a uma rede de sinalização baseada em circuitos, o SCTP não poderá usar os valores recomendados na RFC2960 (Stewart, R., Xie, Q., Morneault, K. et al., 2000), usando valores bem mais agressivos no que se refere aos parâmetros envolvidos na comutação para o caminho alternativo. O trabalho de Brunstrom, A., et. al. (2005) sugere que o parâmetro Path.Max.Retrans é o principal responsável pelo tempo máximo de comutação do SCTP, porém os parâmetros RTOmin e RTOmax também tem impacto no tempo total de comutação (Brunstrom, A., Eklund, J., 2006).

Espera-se que a protocolo garanta que, em caso de falha na rede, a comutação do tráfego para um caminho alternativo ocorra o mais rápido possível, de forma a evitar a perda de mensagens, duplicação ou a necessidade de reordenação (Brunstrom, A., Grinnemo, K., 2005).

Utilizando-se os valores padrão para o protocolo SCTP, conforme recomendado na RFC2960, obteremos um tempo de comutação de no mínimo 63 segundos (Rembarz, R., Baucke, S., Mahonen, P., 2005) e (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010). Considerando que temos o parâmetro RTOmin com 1s e o parâmetro Path.Max.Retrans exigindo 5 retransmissões antes da comutação, (Brunstrom, A., Grinnemo, K., 2005) chegamos os eventos indicados na Tabela 5.1.

Tabela 5.1 - Tempo e Eventos para os valores propostos na RFC2960

<b>Tempo</b>	<b>Evento</b>
Antes da falha	$RTO=RTO_{min}$ , ou seja 1 s
0 s	Falha
1 s	Retransmissão, $RTO = 2x RTO = 2$ s
3 s (1 + 2 s RTO)	Retransmissão, $RTO = 2x RTO = 4$ s
7 s (3 + 4 s RTO)	Retransmissão, $RTO = 2x RTO = 8$ s
15 s (7 + 8 s RTO)	Retransmissão, $RTO = 2x RTO = 16$ s
31 s (15 + 16 s RTO)	Retransmissão, $RTO = 2x RTO = 32$ s
63 s (31 + 32 s RTO)	Comutação para caminho alternativo

Independentemente do valor do valor do parâmetro Path.Max.Retrans, alterações nos parâmetros  $RTO_{min}$  e  $RTO_{max}$  permitirão resultados melhores do que os obtidos pelo uso dos valores padrão propostos na RFC 2960 (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010) .

O valor sugerido para o parâmetro  $RTO_{min}$  é de 1 segundo em (Stewart, R., Xie, Q., Morneault, K. et al., 2000) e (Costa, Daniel Gouveia, 2005). Segundo Baucke, S., et. al. (2010), é provável que esse valor tenha origem no fato de que muitas implementações usariam frequência de relógio relativamente altas, forçando a utilização de valores maiores para esse temporizador. Porém essa não é a realidade de equipamentos usados na troca de sinalização das redes de telecomunicações.

Considerando-se as observações acima, pode-se sugerir uma sequência de ajustes visando a melhoria de desempenho do protocolo. Esses ajustes são feitos de forma sequencial, sendo primeiramente efetuados os ajustes que não geram redução da segurança ou da qualidade de funcionamento do protocolo.

### **5.1. AJUSTE 1 – TOPOLOGIA**

Deve-se reduzir a quantidade de associações paralelas até o valor mínimo de duas associações. Estas devem estar construídas de forma a que o caminho primário da primeira associação seja o caminho alternativo da segunda associação, garantindo a divisão de carga entre ambas. Desta forma também temos uma melhora de desempenho no que se refere à quantidade de mensagens afetadas por falha, que é reduzida à metade.

## 5.2. AJUSTE 2 – PARÂMETRO RTOMIN

Existem estudos, entre eles o de Baucke, S., et. al. (2010), que sugerem a utilização do parâmetro RTOmin em um valor sempre acima de duas vezes o valor de RTT (*Round-trip Time*) da rede. Com essa alteração garante-se que as retransmissões serão efetuadas de forma mais rápida, já que elas são efetuadas com base na variável RTO do *endpoint*, que por sua vez é função do RTT, mas com o valor mínimo definido pelo parâmetro RTOmin. Considerando que o valor de RTT é tipicamente igual ao dobro da latência, e com o ajuste proposto em RTOmin, o valor do tempo de comutação deve ser conforme mostrado nas equações, no caso do parâmetro Path.Max.Retrans ser igual a 5:

$$t_c = RTT + 2 \times RTOmin + 4 \times RTOmin + 8 \times RTOmin + 16 \times RTOmin + 32 \times RTOmin \quad (5.1)$$

$$t_c = 125 \times RTT \quad (5.2)$$

$$t_c = 250 \times \text{Latência} \quad (5.3)$$

Para o caso de Path.Max.Retrans igual a 4, os valores obtidos são:

$$t_c = RTT + 2 \times RTOmin + 4 \times RTOmin + 8 \times RTOmin + 16 \times RTOmin \quad (5.4)$$

$$t_c = 61 \times RTT \quad (5.5)$$

$$t_c = 122 \times \text{Latência} \quad (5.6)$$

## 5.3. AJUSTE 3 – PARÂMETRO PATH.MAX.RETRANS

Para atender aos requisitos das redes de sinalização, especificamente em relação ao parâmetro Path.Max.Retrans, no trabalho de (Brunstrom, A., Grinnemo, K., 2005) há a citação de que o seu valor deve ser no máximo 3. Assim o próximo ajuste consiste em reduzir o valor do parâmetro Path.Max.Retrans progressivamente até o valor 3. Com esse valor haverá até três retransmissões das mensagens antes que o caminho seja considerado inacessível. Como esse valor teremos um tempo de comutação

$$t_c = RTT + 2 \times RTOmin + 4 \times RTOmin + 8 \times RTOmin = 29 \times RTT \quad (5.7)$$

$$t_c = 58 \times \text{Latência} \quad (5.8)$$

#### 5.4. AJUSTE 4 - PARÂMETRO RTOMIN

Ajustar o valor de RTOmin para que a variável RTO do protocolo fique flutuante. Valores para o parâmetro RTOmin abaixo do valor do RTT da rede fazem com que o valor de RTO fique flutuante, de acordo com o RTT medido da rede. Essa é a configuração que permite o melhor desempenho (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010) . Com esse ajuste as retransmissões ficam ainda mais rápidas, tendo o seu tempo baseado na latência real da rede, sem folgas. Teremos, então, um tempo de comutação:

$$t_c = RTT + 2 \times RTT + 4 \times RTT + 8 \times RTT = 15 \times RTT \quad (5.9)$$

$$t_c = 30 \times \text{Latência} \quad (5.10)$$

#### 5.5. AJUSTE 5 – PARÂMETRO RTOMAX

Ajustar o valor de RTOmax progressivamente, de forma a limitar o crescimento exponencial da variável RTO do *endpoint*. Considerando-se os ajustes anteriores já efetuados (RTOmin igual ao RTT e Path.Max.Retrans igual a 3), espera-se que o tempo de comutação do protocolo seja função do RTOmax. Na Figura 5.1 está indicado como o parâmetro RTOmax deve afetar o tempo total de comutação, quando o parâmetro RTOmin é equivalente ao RTT da rede, e o parâmetro Path.Max.Retrans está configurado para 3. Neste caso observa-se que o uso do RTOmax acima do valor equivalente a 30 vezes o valor da latência da rede já não gera efeito algum, uma vez que temos um tempo de total de comutação

$$t_c = RTT + 2 \times RTT + 4 \times RTT + 8 \times RTT = 15 \times RTT \quad (5.11)$$

$$t_c = 30 \times \text{Latência} \quad (5.12)$$

Conforme o valor de RTOmax é reduzido a última retransmissão passa a ser efetuada antes, sequencialmente, até que, em uma situação limite, temos um tempo de comutação

$$t_c = RTT + RTT + RTT + RTT = 4 \times RTT \quad (5.13)$$

$$t_c = 8 \times \text{Latência} \quad (5.14)$$

Esse é o limite de atuação da alteração deste parâmetro. Na Figura 5.1 pode-se ver o efeito da redução do parâmetro RTOmax e seu efeito sobre o tempo de comutação. Esta figura

indica a razão entre o tempo de comutação pela latência em função da alteração na razão RTOmax/Latência.

Deve-se ter cuidado na alteração do valor de RTOmax, pois o mesmo pode afetar o efeito exponencial do *back-off*, adiando, de forma indesejável, a comutação para o caminho alternativo. O trabalho de (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010) sugere que esse tipo de alteração seja feito somente em redes IP dedicadas. Esse, porém, é o caso do transporte da sinalização em telecomunicações.

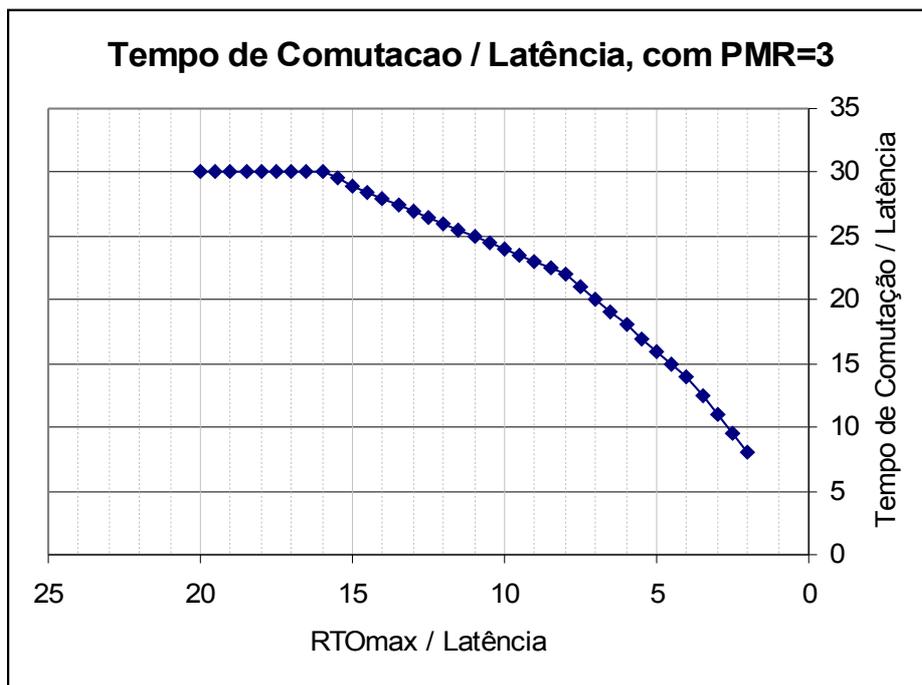


Figura 5.1 - Relação entre a razão tempo de comutação por Latência e o parâmetro RTOmax

### 5.6. AJUSTE 6 – PARÂMETRO PATH.MAX.RETRANS

Caso ainda sejam necessários ajustes, o valor de Path.Max.Retrans pode ser reduzido para o valor 2. Essa alteração, porém, pode comprometer a estabilidade da conexão, levando a comutações desnecessárias. Com essa alteração, o tempo de comutação passa a ser

$$t_c = RTT + RTT + RTT = 3 \times RTT \quad (5.15)$$

$$t_c = 6 \times \text{Latência} \quad (5.16)$$

## 5.7. AJUSTES ADICIONAIS

Existem estudos propondo algumas alterações no protocolo SCTP que poderiam melhorar o desempenho de comutação para um caminho alternativo em caso de falha. Um deles, o de (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010), trata do chamado RTO *back-off factor*, chamado B. O valor de B é multiplicado ao valor do RTO do caminho em caso de falha, fazendo com que o valor de RTO cresça exponencialmente conforme as falhas ocorrem. Isso garante um ajuste adequado do RTO em caso de falha intermitente da rede, que não envolva a sua queda total, mas um aumento brusco do temporizador T3-rtx, usando para detecção da perda da associação.

O uso do valor B=2, conforme previsto na RFC 2960 (Stewart, R., Xie, Q., Morneault, K. et al., 2000), faz com que o valor de RTO cresça de forma rápida, gerando um atraso inconveniente para aplicações de telecomunicações, normalmente sensíveis a atrasos grandes. Isso faz com que se procure trabalhar com valores baixos de Path.Max.Retrans, garantindo-se assim uma comutação rápida. O estudo citado propõe que se trabalhe com um fator de *back-off* para o RTO menor do que 2, tipicamente 1,75. Como resultado, pode-se aumentar o valor de Path.Max.Retrans sem prejudicar o tempo total de comutação. Assim, garante-se um aumento na quantidade de re-tentativas antes da comutação.

Como essa é uma proposta de melhoria do protocolo, que ainda não foi implementada, seu desempenho não foi avaliado neste documento, uma vez que procura-se configurações e ajustes de parâmetros que estejam disponíveis nos equipamentos hoje.

Por outro lado, foi observado que se pode obter um efeito similar pelo ajuste do parâmetro RTOMax, para situações onde a latência de rede é razoavelmente constante. No entanto, caso essa sugestão seja aplicada em novas implementações ou revisões do protocolo SCTP, a possibilidade de ajustes no fator de *back-off* do RTO deve ser avaliada.

## 5.8. SUGESTÕES DE VALORES PARA OS PARÂMETROS

Buscando-se atingir o alvo de um atraso máximo dos pacotes em 500ms, devem-ser feitos ajustes nos parâmetros de rede. Conforme já avaliado, o atraso máximo é função direta da latência de rede, podendo ter esse efeito reduzido de acordo com a configuração dos parâmetros RTOMin, RTOMax e Path.Max.Retrans.

Partindo dos valores iniciais previstos para esses parâmetros, conforme a RFC 2960, obtemos um tempo de comutação de 63 segundos, conforme indicado na Tabela 5.1.

Baseado nas propostas indicadas acima, podemos verificar o desempenho provável de diversas configurações, avaliando qual a faixa de valores de latência que é bem atendida por cada um dos perfis. As diversas configurações sugeridas estão indicadas no Anexo B. Para cada uma delas observa-se uma faixa adequada de utilização, onde essa configuração pode ser usada para se atingir ao objetivo proposto de um atraso máximo de 500ms. Esse desempenho é observado na Figura 5.2.

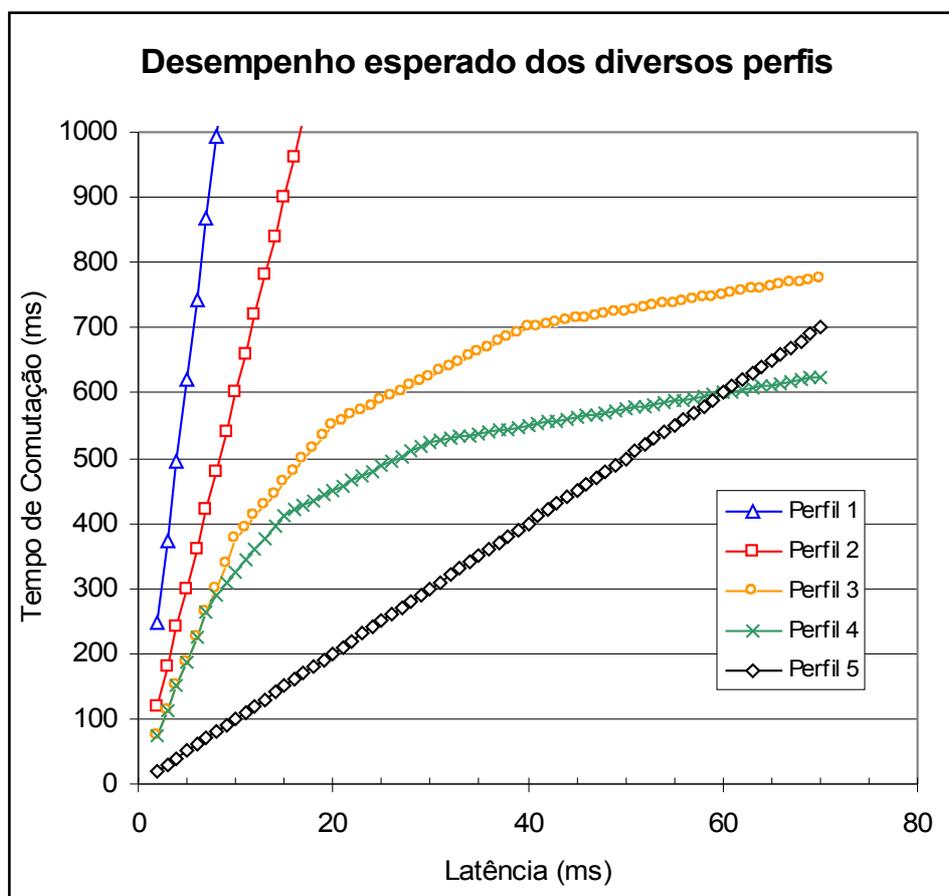


Figura 5.2: Desempenho esperado dos diversos perfis em função da latência da rede

Os perfis foram construídos considerando-se o procedimento sugerido para sequência de ajuste dos parâmetros, conforme indicado anteriormente, sendo o Perfil 0 os valores sugeridos na RFC 2960.

1. Ajuste no parâmetro RTOMin para 2xRTT.

2. Redução do parâmetro Path.Max.Retrans para 3.
3. Ajuste no parâmetro RTOMin para valor igual ou menor ao RTT.
4. Ajuste no parâmetro RTOMax até atingir o valor  $2 \times \text{RTT}$ .
5. Redução do parâmetro Path.Max.Retrans (PMR) para 2.

Os resultados citados são teóricos, uma vez que não são considerados, neste caso, as variações de latência de rede (que pode aumentar o valor do RTT, conseqüentemente o tempo de comutação) e a eficiência das retransmissões (que melhora o desempenho no que se refere ao atraso máximo das mensagens).

Apesar de o perfil 5 ter um resultado melhor que os demais para a maioria dos valores de latência, o seu uso prejudica o funcionamento correto das facilidades de segurança da rede, já que é utilizado um valor reduzido para o parâmetro Path.Max.Retrans, e um valor de RTOMax que retira o crescimento exponencial do valor de RTO. Esse crescimento exponencial é desejável para evitar que pequenas falhas de rede e perdas de pacotes gerem um aumento exagerado do tráfego devido às retransmissões. Assim, cada um dos perfis deve ser utilizado sequencialmente, enquanto o seu desempenho permitir um atraso máximo das mensagens abaixo de 500ms, valor considerado adequado para as camadas superiores.

Como forma de validar os valores sugeridos para os perfis, foram efetuadas simulações com cada um deles, de forma a confirmar o seu desempenho. A latência da rede teve o valor inicial ajustado para 2ms, com variação exponencial com média 1 ms, crescendo linearmente. Para cada ponto deste gráfico a simulação foi executada 10 vezes. Foi colocado como alvo o tempo de comutação sempre menor do que 500 ms. Esse valor é considerado adequado devido aos requisitos padrão das camadas superiores dos protocolos de sinalização. Conforme (Brunstrom, A., Grinnemo, K., 2005), imagina-se que a latência em redes SIGTRAN tenha entre seus valores típicos 5 ms, 10 ms e 20 ms. Os resultados estão indicados abaixo. Para essas simulações, foram usados os perfis abaixo:

- Uma Associação SCTP, de forma a concentrar o tráfego;

- Mensagens enviadas pela aplicação a cada 2 ms. Esse valor representa um tráfego de cerca de 100.000 BHCA em uma rede real. Conforme avaliado, nesta faixa de valores de tráfego de mensagens a quantidade das mesmas já não afeta o desempenho do tempo de comutação;
- Tamanho das mensagens de 100 octetos. Esse valor é próximo da média do tamanho das mensagens, considerando um misto de mensagens MAP e ISUP, em cenários chamadas reais;
- Parâmetro Atraso de SACK de 200 ms, conforme valor padrão previsto na RFC 2960. De qualquer forma, o valor deste parâmetro não afeta o desempenho do protocolo para o tráfego de sinalização.

Pode-se observar na Figura 5.2 que cada um dos perfis propostos tem uma faixa de valores de latência para a qual é atendido o requisito de atraso máximo dos pacotes abaixo de 500ms.

Assim, a simulação foi executada novamente, considerando-se agora a faixa adequada de atuação para cada perfil. Para essa simulação cada ponto no gráfico corresponde a 40 execuções. Utilizando-se esses ajustes, foi obtido o resultado indicado na Figura 2.2. Os ajustes foram feitos conforme a Tabela 5.2.

Tabela 5.2 - Proposta de ajuste para os parâmetros SCTP em função da latência

Perfil	Faixa de valores de Latência	Parâmetros usados
1	Latência < 5 ms	RTOmin = 2x RTT, RTOmax = 10s, PMR=4
2	5 ms ≤ Latência < 10 ms	RTOmin = 2x RTT, RTOmax = 10s, PMR=3
3	10 ms ≤ Latência < 20 ms	RTOmin = RTT, RTOmax = 200ms, PMR=3
4	20 ms ≤ Latência < 40 ms	RTOmin = RTT, RTOmax = 150ms, PMR=3
5	Latência ≥ 40 ms	RTOmin = RTT, RTOmax = 2,5 x Latência, PMR=3

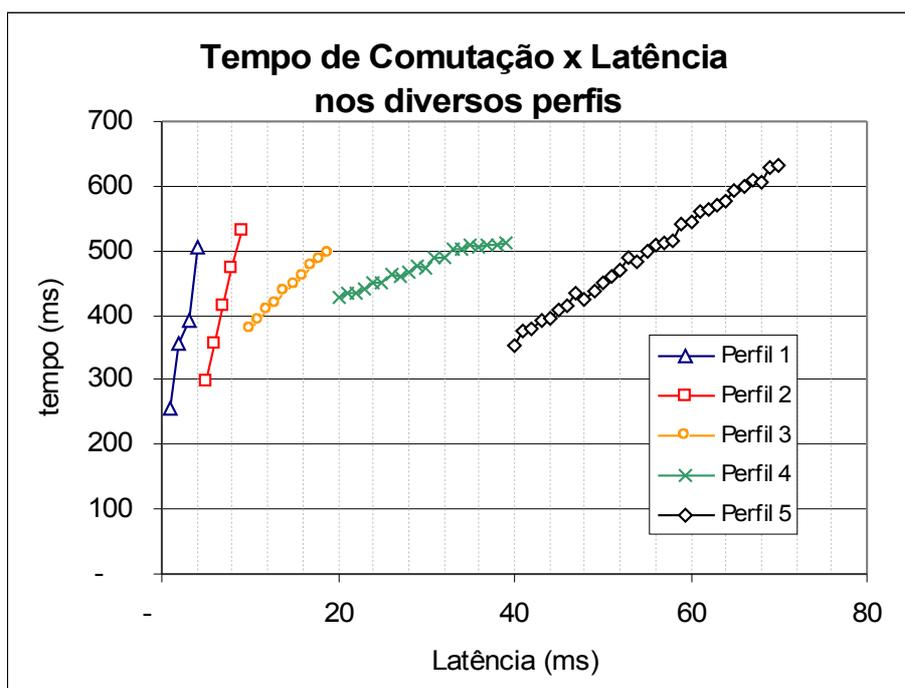


Figura 5.3 - Resultados obtidos com o ajuste dos parâmetros, em relação ao tempo de comutação

Pelos resultados mostrados, observamos o efeito de cada perfil sobre o comportamento do protocolo, sempre mantendo o tempo de comutação abaixo de 500 ms. Na Figura 5.4 está mostrado o desempenho do protocolo no que se refere ao atraso máximo das mensagens para os mesmos perfis.

Observe-se que a partir de uma latência de 5 ms o valor, tanto do tempo de comutação como do atraso máximo das mensagens excede o máximo desejado de 500 ms. Considera-se que, a partir deste valor de latência, é difícil atender o compromisso de manter o tempo de comutação inferior a 500 ms sem que haja redução da quantidade de transmissões (parâmetro Path.Max.Retrans). No perfil 5 esse valor está definido para 3, e a sua redução para valores inferiores pode gerar comutações e retransmissões desnecessárias. Porém, esse tipo de requisito é bastante improvável, pois uma rede com latência de 50 ms irá gerar um *Round-trip Time* de pelo menos 100 ms. Para que a detecção de falhas ocorra e decida-se pela comutação para o caminho alternativo antes que os 400 ms restantes se esgotem, há somente a possibilidade de mais 3 tentativas de troca de mensagens (ou seja, 3 retransmissões). Neste cenário, não há possibilidade de fator de *back-off* que gere um crescimento exponencial do RTO, e as retransmissões ocorrerão em intervalos iguais, no

caso, igual ao RTOMax, definido para 2,5 vezes o valor da latência.

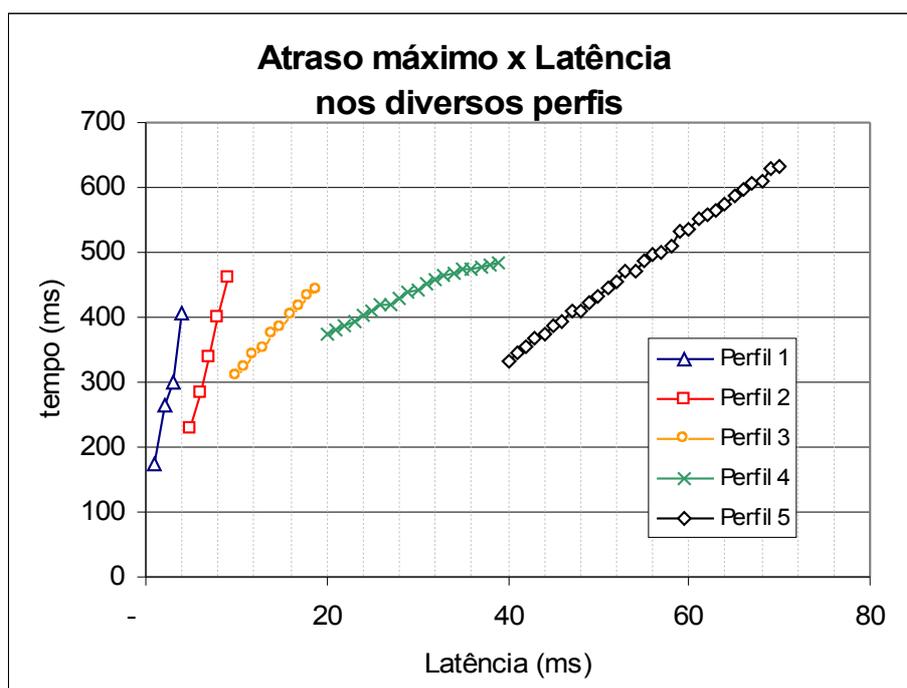


Figura 5.4 - Resultados obtidos com o ajuste dos parâmetros SCTP, em relação ao atraso máximo das mensagens

Observe-se, também, que o uso de RTOMax igual a 2,5 vezes o valor da latência deixa muito pouco espaço para variação da latência de rede, que poderia variar somente 25%. Caso a variação exceda esse valor, a mensagem será considerada perdida, e uma retransmissão efetuada.

Assim, conclui-se que, conforme o valor da latência aumenta, a manutenção do compromisso de comutação em 500 ms fica cada vez mais prejudicada. Dentro de uma rede de pacotes de uma empresa de telecomunicações, porém, os tempos de latência encontrados têm valores máximos na casa dos 25 ms.

Este valor foi obtido em testes efetuados em uma operadora de telecomunicações no Brasil, entre as localidades de Brasília e Rio Branco. Foi efetuada uma bateria de testes de acordo com as recomendações RFC 2544 (Bradner, S., McQuaid, J., 1999) e RFC 1242 (Bradner, S., 1991). Foram utilizados os equipamento Smartbits 600B, da Spirent (Spirent Communications, 2010), em ambas as localidades. Esse equipamento é capaz de gerar, receber e processar o tráfego. Foram executadas medidas em vários dias, com pacotes

variando entre os tamanhos 64 bytes e 512 bytes, num total de 10.000 pacotes enviados para obtenção do valor da média de cada dia. Os valores mínimos de latência observados foram de 23,5 ms, com valores médios de 24 ms. Devido à topologia das redes atuais, é pouco provável que haja situações de enlaces terrestres envolvendo enlaces maiores do que este, de 1900 km.

Para esta faixa de valores de latência há alternativas razoáveis de ajuste, tanto no parâmetro Path.Max.Retrans como nos parâmetros RTOmin e RTOmax, sendo possível garantir o tempo de comutação dentro do desejado.

## **5.9. CONCLUSÕES**

Atender ao requisito de tempo de comutação para o caminho reserva abaixo em até 500ms, gera a necessidade de uma otimização forte nos parâmetros do protocolo SCTP. Essa otimização fica cada vez mais difícil à medida que a latência gerada pela rede aumenta. Isso se deve ao fato de a detecção da falha se dar pela ausência de recebimento da confirmação de entrega pelo *endpoint* de destino. Desta forma, quanto maior a latência, maior o tempo levado para se detectar a falha. Assim, é mais adequado que se usem vários conjuntos de parâmetros, de acordo com a latência observada. Assim pode-se usar a configuração mais adequada para garantir o atendimento aos requisitos sem, no entanto, prejudicar o funcionamento e a segurança do protocolo. Com os perfis de configuração sugeridos, é possível atender com segurança aos requisitos indicados para redes com até 50ms de latência. Esse alcance garante o atendimento com qualidade para grande parte dos enlaces de sinalização de redes de telecomunicações.

## 6. CONCLUSÕES E TRABALHOS FUTUROS

O objetivo deste trabalho foi avaliar o comportamento do protocolo SCTP quando usado em um cenário de transporte de sinalização para rede de telecomunicações, maximizando o seu desempenho em cenários de falhas de rede, tendo em vista as necessidades das camadas de aplicação e o perfil de tráfego da troca de sinalização entre elementos de rede de telecomunicações. Usando por base uma ferramenta de simulação, foi avaliado o comportamento do protocolo sob diversas condições de tráfego, configuração de rede IP e parametrização do protocolo SCTP, sendo buscados valores e topologia mais adequados para garantir o atendimento aos requisitos.

No capítulo 2, foi feita uma apresentação das redes de telecomunicações e a relevância, dentro desta rede, da rede de sinalização. Concluiu-se que as redes de sinalização têm fundamental importância no processamento das chamadas, sendo necessárias várias trocas de mensagens entre os elementos de rede, mesmo para cenários de chamadas aparentemente simples na perspectiva do cliente. Também se verificou a necessidade de evolução das redes de sinalização, que originalmente utilizavam transporte baseado em circuito comutado, para o transporte baseado em redes de pacotes. Discorreu-se sobre os benefícios desta migração, bem como sobre os requisitos demandados por essas redes. Foi avaliado o uso das redes IP para transporte da sinalização, e a incapacidade de atendimento dos requisitos de qualidade pelos protocolos disponíveis, especificamente TCP e UDP.

No capítulo 3 foi apresentado o protocolo SCTP, definido pelo grupo de trabalho SIGTRAN para ser usado em conjunto com o IP, e com as camadas de adaptação M3UA, responsável por manter a transparência da rede para as chamadas superiores, permitindo, assim, a convivência, em uma mesma rede de sinalização, de elementos de rede usando transporte via circuito comutado e outros usando redes de pacotes. Em seguida avaliou-se o funcionamento do protocolo SCTP, especificamente no que se refere às suas facilidades de utilização de múltiplos caminhos (*multi-homing*), parâmetros de configuração e variáveis internas que definem a forma de funcionamento do protocolo. Foi também apresentada a pilha SIGTRAN, que se utiliza do SCTP como camada de transporte, em comparação com a pilha SS7 construída sobre circuito comutado. Também se verificou qual a forma adotada para permitir a coexistência das duas pilhas de sinalização em uma mesma rede. Em

seguida foi discutida uma forma mais adequada de se fazer uso dos aspectos de redundância fornecidos pelo protocolo SCTP, bem como seu funcionamento e sua forma de configuração. Foram apresentados os parâmetros deste protocolo, sua função dentro do funcionamento do protocolo, e os valores sugeridos na RFC 2960 (Stewart, R., Xie, Q., Morneault, K. et al., 2000) para os mesmos.

No capítulo 4 discorreu-se sobre o efeito de cada um dos parâmetros do protocolo, do perfil do tráfego e da topologia de rede no que se refere ao seu efeito no tempo de comutação para o caminho reserva e atraso máximo que é sofrido pelas mensagens quando ocorre a comutação. Especificamente foi avaliada a topologia de rede, perfil do tráfego das mensagens e os parâmetros de atraso de SACK, RTOmin, RTOmax e Path.Max.Retrans. Verificou-se que, com exceção do atraso de SACK, todos os parâmetros têm efeito sobre o tempo de comutação e atraso das mensagens, porém em cenários variados. Concluiu-se que o parâmetro Atraso de SACK não tem efeito no desempenho do protocolo quando este é usado para tráfego de mensagens em redes de sinalização, devido ao fato de essas redes terem um fluxo razoavelmente constante de mensagens, e de o tráfego ser bidirecional, devido à característica transacional das camadas de aplicação das redes de sinalização em sistemas de telecomunicações. Em seguida foram efetuadas simulações para verificar, quantitativamente, qual o efeito que cada um dos parâmetros citados tem sobre o desempenho do protocolo. Foi confirmado que o parâmetro Atraso de SACK não tem efeito sobre o desempenho, e que a latência da rede é o principal fator que prejudica o desempenho do protocolo. Observou-se que os maiores efeitos são gerados pela variação dos parâmetros RTOmin, RTOmax e Path.Max.Retrans. Também se confirmou que os valores padrão sugeridos na especificação do protocolo SCTP não são adequados para uso em redes de sinalização de sistemas de telecomunicações.

No capítulo 5 foi sugerida uma forma de ajuste destes parâmetros, de forma a garantir, para vários valores de latência, o tempo de comutação do protocolo e atraso máximo imposto às mensagens abaixo de 500 ms. Avaliou-se a necessidade de vários perfis de configuração, de acordo com a latência da rede.

Conclusivamente, confirmou-se a viabilidade da garantia do tempo de comutação e atraso máximo de mensagens abaixo de 500 ms, pela utilização de valores adequados para cada faixa de valores de latência. Observou-se também a dificuldade no atendimento destes

requisitos quando a latência tem valores superiores a 50 ms. Para estes casos a tentativa de atendimento do requisito pode gerar retransmissões desnecessárias e, eventualmente, a comutação para o caminho alternativo sem que tenha ocorrido, efetivamente, uma falha no caminho primário. Dentro do escopo deste trabalho não foram encontrados valores adequados para a parametrização do protocolo, sendo sugerido, para estes cenários, o uso de transporte de sinalização SS7 via TDM.

## **6.1. TRABALHOS FUTUROS**

Neste trabalho, foi avaliado o desempenho do protocolo SCTP (*Stream Control Transmission Protocol*) para transporte de mensagens de sinalização em redes onde é utilizada, como camada imediatamente superior, o M3UA (*MTP-L3 User Adaptation Layer*), sendo as camadas de aplicação os protocolos SCCP (*Signaling Connection Control Part*), TCAP (*Transaction Capabilities Application Part*), ISUP (*ISDN User Part*) e MAP (*Mobile Application Part*). Sugere-se que o mesmo estudo seja feito para o uso de outros protocolos, que não são implementados usando-se a camada de adaptação M3UA, como, por exemplo, os protocolos definidos para as redes futuras LTE (*Long Term Evolution*) (Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., 2010), (3GPP, 2010C) e também para o transporte de SIP (*Session Initiation Protocol*) (Brunstrom, A., Hurtig, P., 2008). As interfaces definidas para essa sinalização já são totalmente definidas em IP, tendo, portanto, requisitos de temporização diferentes dos requisitos das redes que foram especificadas para terem sua sinalização transportada por circuito comutado.

Também se sugere a avaliação dos valores adequados para os parâmetros considerando redes que tenham variação de latência grande. Essa não é uma característica das redes de pacotes atualmente usadas para transporte de sinalização, já que a sinalização, em geral, trafega em sub-redes ou VLANs (*Virtual Local Area Network*) dedicadas. Porém, em alguns casos, o uso de redes compartilhadas sem a separação adequada do tráfego de usuário do tráfego de sinalização pode levar a uma condição em que as mensagens de sinalização são fortemente afetadas pelo desempenho da rede.

## BIBLIOGRAFIA

- 3GPP, (2010A) **3GPP Releases** – <http://www.3gpp.org/Releases>, Acessado em 24 de agosto de 2010.
- 3GPP, (2010B) **3GPP TS 23.002 V9.30 - 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network architecture (Release 9)**, Sophia-Antipolis, França
- 3GPP, (2010C) **3GPP TS 23.401 V9.30 - 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 9)**, Sophia-Antipolis, França
- Baucke, S., Brunstrom, A., Eklund, J., Grinnemo, K., (2010). **Tuning SCTP failover for carrier grade telephony signaling**. *Computer Networks*, v54, p. 133-149.
- Bradner, S., (1991). **RFC1242 - Benchmarking Terminology for Network Interconnection Devices**. IETF Network Working Group.
- Bradner, S., McQuaid, J., (1999). **RFC2544 - Benchmarking Methodology for Network Interconnect Devices**. IETF Network Working Group.
- Brunstrom, A., Eklund, J., (2006). **Impact of SACK delay an link delay on failover performance in SCTP**. In *Proceedings of 3rd Conference on Communications and Computer Networks*. Lima, Peru.
- Brunstrom, A., Grinnemo, K., (2005). **Performance of SCTP-controlled Failovers in M3UA-based SIGTRAN Networks**. In *Proceedings of 16th International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE.
- Brunstrom, A., Grinnemo, K., (2005). **Impact of Traffic Load on SCTP Failovers in SIGTRAN**. *Lecture Notes in Computer Science*. v3420, p. 774-783.
- Brunstrom, A., Hurtig, P., (2008). **Enhancing SCTP loss recovery: An experimental evaluation of early retransmit**. In *Computer Communications*. v31, p. 3778-3788.
- Calhoun, P., Loughney, J., et al (2003). **RFC 3558 - Diameter Base Protocol**, IETF

Network Working Group.

Chukarin, A., Pershakov, N., Samouylov, K. (2007). **Performance of Sigtran-based Signaling Links Deployed in Mobile Networks**. In *Proceedings of 9th Internacional Conference on Telecommunications*. IEEE.

Costa, D., (2005). **SCTP – Uma alternativa aos tradicionais protocolos de transporte da Internet**, Editora Ciência Moderna Ltda, Rio de Janeiro, Brasil

Ericsson, **Mobile Softswitching**: <http://www.ericsson.com/ourportfolio/telecom-operators/mobile-softswitching-mss>. Acessado em 23 de agosto de 2010.

Garcia, M., Sanchez, D., (1998) **A Simple SCCP Tunneling Protocol (SSTP) – Internet Draft**, <https://datatracker.ietf.org/doc/draft-sanchez-garcia-SSTP-v1r0/>, acessado em 20 de outubro de 2010

GSM Association, **IR.72 - SIGTRAN Basic Design Principles – 1.0 - 23 June 2005**, Londres, Inglaterra.

HP, **Delivering superior subscriber mobility with HP OpenCall mobility management solutions White paper**, (2010A)  
[http://h20208.www2.hp.com/opencall/library/products/mobility/ochlr/hlr\\_mobility\\_mgmt\\_wp.pdf](http://h20208.www2.hp.com/opencall/library/products/mobility/ochlr/hlr_mobility_mgmt_wp.pdf). Acessado em 23 de agosto de 2010.

HP, **HP OpenCall - NSK Network Elements Product Family**, (2010B)  
[http://h20208.www2.hp.com/opencall/library/general/opencall\\_hlr\\_whitepaper.pdf](http://h20208.www2.hp.com/opencall/library/general/opencall_hlr_whitepaper.pdf), Acessado em 24 de agosto de 2010.

Immonen, M., (2005). **SIGTRAN – Signaling over IP – a step closer to an all-IP network**. Master of Science Thesis. Estocolmo, Suécia.

ITU-T, (2009) **H.323 : Packet-based multimedia communications systems**,  
<http://www.itu.int/rec/T-REC-H.323-200912-I/en>, acessado em 20 de outubro de 2010.

ITU-T, (1994A). **Q.2110 : B-ISDN ATM adaptation layer - Service specific connection oriented protocol (SSCOP)**, <http://www.itu.int/rec/T-REC-Q.2110-199407-I/en>, acessado em 20 de outubro de 2010.

ITU-T, (1993) **Q.700 : Introduction to CCITT Signalling System No. 7 –**  
<http://www.itu.int/rec/T-REC-Q.700-199303-I/e>. Acessado em 20 de outubro de 2010.

- ITU-T, (1996) **Q.703: Signalling link** – <http://www.itu.int/rec/T-REC-Q.703-199607-I/en>.  
Acessado em 20 de outubro de 2010.
- ITU-T, (1994B) **Q.706: Message Transfer Part Signalling Performance** –  
<http://www.itu.int/rec/T-REC-Q.706-199303-I/en>. Acessado em 25 de outubro  
de 2010.
- Jungmaier, A., Rathgeb, E. P., (2005). **A novel method for SCTP load sharing**. *Lectures  
Notes in Computer Science*. V3462, p. 1453-1456.
- Jungmaier, A., Rathgeb, E. P., (2006). **On SCTP multi-homing performance**.  
*Telecommunications Systems*, v31, p. 141-161.
- Ma, G (1998), **UDP for TCAP – Internet Draft**, [http://www.ietf.org/proceedings/43/I-  
D/draft-ma-tudp-00.txt](http://www.ietf.org/proceedings/43/I-D/draft-ma-tudp-00.txt), acessado em 20 de outubro de 2010.
- Microsoft Corporation, **Visual Basic Express**  
<http://www.microsoft.com/express/windows/>, Acessado em 24 de agosto de  
2010.
- Ong, L., Ritina, I. et al., (1999), **RFC 2719 - Framework Architecture for Signaling  
Transport**, IETF Network Working Group
- Pfützenreuter, E., (2004). **Aplicabilidade e desempenho do protocolo de transporte  
SCTP**. Dissertação de Mestrado, Universidade de Brasília, Brasil.
- Rembarz, R., (2004). **Analysis of Redundancy Mechanisms for High Availability IP-  
Based Signaling Transport**. Diploma Thesis. Aachen University, Alemanha.
- Rembarz, R., Baucke, S., Mahonen, P. (2005). **Enhancing Resilience for High  
Availability IP-based Signaling Transport**. In *Proceedings of 16th  
International Symposium on Personal, Indoor and Mobile Radio  
Communications*. IEEE.
- Rizzo, L., (2010). **Dummysnet Home Page**, <http://info.iet.unipi.it/~luigi/dummysnet/>,  
acessado em 25 de outubro de 2010.
- Russell, T., (2006). **Signaling System #7**, Fifth Edition, McGraw-Hill Communications,  
New York, Estados Unidos.
- Schulzrinne, H., Casnet, S., et al (1996). **RFC 1889 – RTP - A Transport Protocol for  
Real-Time Applications**, <http://www.ietf.org/rfc/rfc1889.txt>, acessado em 20

de outubro de 2010.

Spirent Communications (2010), **SmartBits** <http://www.spirent.com/Solutions-Directory/Smartbits.aspx>, Acessado em 24 de agosto de 2010.

Stewart, R., Xie, Q., (1999). **Multi-network Datagram Transmission Protocol – Internet Draft**, <http://tools.ietf.org/id/draft-ietf-sigtran-mdtp-06.txt>, acessado em 20 de outubro de 2010.

Stewart, R., Xie, Q., Morneault, K. et al., (2000). **RFC 2960 – Stream Control Transmission Protocol**. IETF Network Working Group.

Stewart, R., Xie, Q., (2001). **Stream Control Transmission Protocol (SCTP): a reference guide**, Addison-Wesley Professional, Boston, Estados Unidos.

Tanenbaum, Andrew S., (2003). **Redes de Computadores**, Rio de Janeiro, Elsevier, Rio de Janeiro.

Toney, K., (1999). **PURDET Reliable Transport Extensions on UDP – Internet Draft**, <https://datatracker.ietf.org/doc/draft-tony-purdet/>, acessado em 20 de outubro de 2010.

## **ANEXOS**



## A.DETALHAMENTO DE CHAMADAS REAIS

Os detalhes abaixo foram usados para se verificar o tamanho das mensagens de sinalização, para o exemplo usado neste trabalho. Eles foram coletados diretamente na rede de sinalização.

Os campos relativos à identificação dos números envolvidos na chamada foram apagados para preservar a confidencialidade das informações, uma vez que se tratam de chamadas reais obtidas em uma rede comercial.

### A.1. CONSULTA AO EIR

CT (1) - Protocol Level Display (1)

```
02:14:18.901 PM SAT Link: PTS*CTASG1-BrT_IP_0
802.3 / Ethernet
  Source MAC Addr: 00:18:00:aa:00:00 Destination MAC Addr: 00:e0:fc:fb:4f:71
IP Version 4
  Precedence: Routine
  Delay: Normal delay
  Throughput: Normal throughput
  Reliability: Normal reliability
  Total Length: 180 octets
  Protocol: SCTP
  Source Address: 10.187.36.144 Destination Address: 10.185.147.9
SCTP
  Source Port: 4122 Destination Port: 4122
chunk Type: Payload Data
  chunk Flags: U: Ordered B: First fragment E: Last fragment
  Stream Identifier: 16
M3UA Message Class: Transfer Messages
M3UA Message Type: Payload Data
OPC: MSS75FNS DPC: PR-CTAHUA1 SI: SCCP NI/MP: NN SLS: 3
MT: UDT
Called Party Address Length: 11 octets
  Subsystem Number: EIC
  Translation Type: unknown
  Nature of Address Indicator: 4. International number
  Address Information: 550310000009
Calling Party Address Length: 11 octets
  Subsystem Number: MSC
  Translation Type: unknown
  Nature of Address Indicator: 4. International number
  Address Information: 550312001001
TCAP Message Type: Begin
Originating Trans Id Tag: 48
  Originating Transaction Id: 19079414
Component Portion Tag: 6c
Invoke: a1
  Invoke Id: 0
Operation Code Tag: Local Operation Code
Operation Code (Invoke): Check IMEI
IMEI Tag: 4
  IMEI Identity Digits: xxxxxxxxxxxxxxxx
Padding: 0

| | IP.SCTP.MTP ITU
1 | 0000 0000 | I/G = 0, U/L = 0, Destination Address = 00:E0:FC:FB:4F:71
2 | 1110 0000 | Destination Address
3 | 1111 1100 | Destination Address
4 | 1111 1011 | Destination Address
5 | 0100 1111 | Destination Address
6 | 0111 0001 | Destination Address
```

```

7      | 0000 0000 | I/G = 0, U/L = 0, Source Address = 00:18:00:AA:00:00
8      | 0001 1000 | Source Address
9      | 0000 0000 | Source Address
10     | 1010 1010 | Source Address
11     | 0000 0000 | Source Address
12     | 0000 0000 | Source Address
13     | 0000 1000 | Ethernet Type = 0800 - IPv4
14     | 0000 0000 | Ethernet Type
15     | 0100|0101 | IP Version 4, IHL = 5 32-bit words
16     | 000000|00 | Prec. = Routine, Norm delay, Norm thru-put, Norm rel.
17     | 0000 0000 | Total Length = 180 octets
18     | 1011 0100 | Total Length
19     | 1111 1100 | Identification = 64582 dec, FC46 hex
20     | 0100 0110 | Identification
21     | 010|00000 | Flags = Don't fragment, Last fragment
22     | 0000 0000 | Fragment Offset = 0 dec
23     | 0011 1101 | Time To Live = 61 seconds
24     | 1000 0100 | Protocol = SCTP (132 dec)
25     | 0000 0000 | Header Checksum = 0 dec, 0000 hex
26     | 0000 0000 | Header Checksum
27     | 0000 1010 | Source Address = 10.187.36.144
28     | 1011 1011 | Source Address
29     | 0010 0100 | Source Address
30     | 1001 0000 | Source Address
31     | 0000 1010 | Destination Address = 10.185.147.9
32     | 1011 1001 | Destination Address
33     | 1001 0011 | Destination Address
34     | 0000 1001 | Destination Address
35     | 0001 0000 | Source Port Number = 4122 dec, 101A hex
36     | 0001 1010 | Source Port Number
37     | 0001 0000 | Destination Port Number = 4122 dec, 101A hex
38     | 0001 1010 | Destination Port Number
39     | 0000 0000 | Verification Tag = 23333 dec, 00005B25 hex
40     | 0000 0000 | Verification Tag
41     | 0101 1011 | Verification Tag
42     | 0010 0101 | Verification Tag
43     | 0100 1001 | Checksum = 1228088332 dec, 4933240C hex
44     | 0011 0011 | Checksum
45     | 0010 0100 | Checksum
46     | 0000 1100 | Checksum
47     | 0000 0000 | chunk Type = Payload Data
48     | 0000 0011 | chunk Flags: U = ordered, B = first, E = last
49     | 0000 0000 | chunk Length = 148 octets
50     | 1001 0100 | chunk Length
51     | 0100 1100 | TSN = 1277323324 dec, 4C22683C hex
52     | 0010 0010 | TSN
53     | 0110 1000 | TSN
54     | 0011 1100 | TSN
55     | 0000 0000 | Stream Identifier = 16 dec, 0010 hex
56     | 0001 0000 | Stream Identifier
57     | 0111 1010 | Stream Sequence Number = 31399 dec, 7AA7 hex
58     | 1010 0111 | Stream Sequence Number
59     | 0000 0000 | Payload Protocol Identifier = M3UA
60     | 0000 0000 | Payload Protocol Identifier
61     | 0000 0000 | Payload Protocol Identifier
62     | 0000 0011 | Payload Protocol Identifier
63     | 0000 0001 | Version = 01, M3UA Release 1.0
64     | 0000 0000 | Spare octet
65     | 0000 0001 | Message Class = Transfer Messages
66     | 0000 0001 | Message Type = Payload Data
67     | 0000 0000 | Message Length = 132 octets
68     | 0000 0000 | Message Length
69     | 0000 0000 | Message Length
70     | 1000 0100 | Message Length
71     | 0000 0010 | Network Appearance Tag
72     | 0000 0000 | Network Appearance Tag
73     | 0000 0000 | Network Appearance Length = 8 octets
74     | 0000 1000 | Network Appearance Length
75     | 0000 0000 | Network Appearance = 8 (dec), 00000008 (hex)
76     | 0000 0000 | Network Appearance
77     | 0000 0000 | Network Appearance
78     | 0000 1000 | Network Appearance
79     | 0000 0000 | Routing Context Tag
80     | 0000 0110 | Routing Context Tag
81     | 0000 0000 | Routing Context Length = 8 octets
82     | 0000 1000 | Routing Context Length
83     | 0000 0000 | Routing Context 1 = 65535 (dec), 0000FFFF (hex)

```

84		0000 0000	Routing Context 1
85		1111 1111	Routing Context 1
86		1111 1111	Routing Context 1
87		0000 0010	Protocol Data Tag
88		0001 0000	Protocol Data Tag
89		0000 0000	Protocol Data Length = 106 octets
90		0110 1010	Protocol Data Length
91		0000 0000	Originating Point Code, OPC = 9483 (dec), 0000250B (hex)
92		0000 0000	Originating Point Code, OPC
93		0010 0101	Originating Point Code, OPC
94		0000 1011	Originating Point Code, OPC
95		0000 0000	Destination Point Code, DPC = 9276 (dec), 0000243C (hex)
96		0000 0000	Destination Point Code, DPC
97		0010 0100	Destination Point Code, DPC
98		0011 1100	Destination Point Code, DPC
99		0000 0011	Service Ind, SI = SCCP message
100		0000 0010	Network Ind, NI = National Network
101		0000 0000	Message Priority, MP = 0
102		0000 0011	Signalling Link Selection, SLS = 3
			ITU.96.SCCP
103	F	0000 1001	MT = Unitdata (UDT)
104	F	1000 0000	Protocol Class = class 0; Msg handling = return on error
105	F	0000 0011	Pointer to Called Party Address Parameter = 3 octet(s)
106	F	0000 1110	Pointer to Calling Party Address Parameter = 14 octet(s)
107	F	0001 1001	Pointer to Data Parameter = 25 octet(s)
108	V	0000 1011	LI of Called Party Address parameter = 11 octet(s)
109	V	0001 0010	Addr Ind: Int'l; Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
110	V	0000 1001	Subsystem Number = 9 EIC
111	V	0000 0000	Translation Type = 0 unknown
112	V	0001 0010	Numbering Plan = 1. ISDN/telephony, Encoding = 2. BCD even
113	V	0 0000100	Nature of Address Indicator = 4. international number
114	V	0101 0101	Address Signal = 550310000009
115	V	0011 0000	Address Signal
116	V	0000 0001	Address Signal
117	V	0000 0000	Address Signal
118	V	0000 0000	Address Signal
119	V	1001 0000	Address Signal
120	V	0000 1011	LI of Calling Party Address parameter = 11 octet(s)
121	V	0001 0010	Addr Ind: Int'l; Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
122	V	0000 1000	Subsystem Number = 8 MSC
123	V	0000 0000	Translation Type = 0 unknown
124	V	0001 0010	Numbering Plan = 1. ISDN/telephony, Encoding = 2. BCD even
125	V	0 0000100	Nature of Address Indicator = 4. international number
126	V	0101 0101	Address Signal = 550312001001
127	V	0011 0000	Address Signal
128	V	0010 0001	Address Signal
129	V	0000 0000	Address Signal
130	V	0000 0001	Address Signal
131	V	0001 0000	Address Signal
132	V	0011 1100	LI of Data parameter = 60 octet(s)
			3GPP.MAP
133		0110 0010	TCAP Message Type: Begin
134		0011 1010	Length: 58 octets
135		0100 1000	Originating Trans Id Tag: 48
136		0000 0100	Length: 4 octet(s)
137		0001 1001	Originating Transaction Id: 19079414
138		0000 0111	Originating Transaction Id:
139		1001 0100	Originating Transaction Id:
140		0001 0100	Originating Transaction Id:
141		0110 1011	Dialogue Portion Tag: 6b
142		0001 1110	Length: 30 octets
143		0010 1000	External Tag: 28
144		0001 1100	Length: 28 octets
145		0000 0110	Object Identifier Tag: 6
146		0000 0111	Length: 7 octet(s)
147		0000 0000	ccitt recommendation: 0
148		0001 0001	q: 11
149		1000 0110	773: 86
150		0000 0101	Space character: 5
151		0000 0001	as(1): 1
152		0000 0001	dialoguePDU: 1
153		0000 0001	version1(1): 1
154		1010 0000	Single ASN.1 Type Tag: a0
155		0001 0001	Length: 17 octets
156		0110 0000	Dialogue PDU: Dialogue Request
157		0000 1111	Length: 15 octets
158		1000 0000	Protocol Version Tag: 80

```

159 | 0000 0010 | Length: 2 octet(s)
160 | 0000 0111 | Protocol Version: 780
161 | 1000 0000 | Protocol Version:
162 | 1010 0001 | Application Context Name Tag: a1
163 | 0000 1001 | Length: 9 octets
164 | 0000 0110 | Object Identifier Tag: 6
165 | 0000 0111 | Length: 7 octet(s)
166 | 0000 0100 | ccitt recommendation: 4
167 | 0000 0000 | etsi: 0
168 | 0000 0000 | Mobile Domain: 0
169 | 0000 0001 | GSM Network: 1
170 | 0000 0000 | ac_id: 0
171 | 0000 1101 | dialoguePDU: EquipmentMngt
172 | 0000 0010 | version: 2
173 | 0110 1100 | Component Portion Tag: 6c
174 | 0001 0010 | Length: 18 octets
175 | 1010 0001 | Invoke: a1
176 | 0001 0000 | Length: 16 octets
177 | 0000 0010 | Invoke Id Tag: 2
178 | 0000 0001 | Length: 1 octet(s)
179 | 0000 0000 | Invoke Id: 0
180 | 0000 0010 | Operation Code Tag: Local Operation Code
181 | 0000 0001 | Length: 1 octet(s)
182 | 0010 1011 | Operation Code (Invoke): Check IMEI
183 | 0000 0100 | IMEI Tag: 4
184 | 0000 1000 | Length: 8 octet(s)
185 | xxxx xxxx | IMEI Identity Digits: xxxxxxxxxxxxxxxx
186 | xxxx xxxx | IMEI Identity Digits:
187 | xxxx xxxx | IMEI Identity Digits:
188 | xxxx xxxx | IMEI Identity Digits:
189 | xxxx xxxx | IMEI Identity Digits:
190 | xxxx xxxx | IMEI Identity Digits:
191 | xxxx xxxx | IMEI Identity Digits:
192 | ---- xxxx | IMEI Identity Digits:
    |          | NULL.LAYER1
193 | 0000 0000 | Padding
194 | 0000 0000 | Padding

```

```

02:14:19.210 PM SAT Link: PTS*CTASG1-BrT_IP_2
802.3 / Ethernet
Source MAC Addr: 00:34:00:ae:00:00 Destination MAC Addr: 00:00:0c:07:ac:96
IP Version 4
Precedence: Routine
Delay: Normal delay
Throughput: Normal throughput
Reliability: Normal reliability
Total Length: 180 octets
Protocol: SCTP
Source Address: 10.185.147.6 Destination Address: 10.187.36.11
SCTP
Source Port: 4122 Destination Port: 4122
chunk Type: Payload Data
chunk Flags: U: Ordered B: First fragment E: Last fragment
Stream Identifier: 8
M3UA Message Class: Transfer Messages
M3UA Message Type: Payload Data
OPC: PTS64ALD DPC: MSS75FNS SI: SCCP NI/MP: NN SLS: 2
MT: UDT
Called Party Address Length: 11 octets
Subsystem Number: MSC
Translation Type: unknown
Nature of Address Indicator: 4. International number
Address Information: 550312001001
Calling Party Address Length: 11 octets
Subsystem Number: EIC
Translation Type: unknown
Nature of Address Indicator: 4. International number
Address Information: 550310000009
TCAP Message Type: End
Destination Trans Id Tag: 49
Destination Transaction Id: 19079414
Component Portion Tag: 6c
Return Result (Last): a2
Invoke Id: 0
Operation Code Tag: Local Operation Code
Operation Code (Return Result): Check IMEI

```

Padding: 0

```

      |
      | IP.SCTP.MTP_ITU
1     | 0000 0000 | I/G = 0, U/L = 0, Destination Address = 00:00:0C:07:AC:96
2     | 0000 0000 | Destination Address
3     | 0000 1100 | Destination Address
4     | 0000 0111 | Destination Address
5     | 1010 1100 | Destination Address
6     | 1001 0110 | Destination Address
7     | 0000 0000 | I/G = 0, U/L = 0, Source Address = 00:34:00:AE:00:00
8     | 0011 0100 | Source Address
9     | 0000 0000 | Source Address
10    | 1010 1110 | Source Address
11    | 0000 0000 | Source Address
12    | 0000 0000 | Source Address
13    | 0000 1000 | Ethernet Type = 0800 - IPv4
14    | 0000 0000 | Ethernet Type
15    | 0100|0101 | IP Version 4, IHL = 5 32-bit words
16    | 000000|00 | Prec. = Routine, Norm delay, Norm thru-put, Norm rel.
17    | 0000 0000 | Total Length = 180 octets
18    | 1011 0100 | Total Length
19    | 0011 0001 | Identification = 12590 dec, 312E hex
20    | 0010 1110 | Identification
21    | 000|00000 | Flags = May fragment, Last fragment
22    | 0000 0000 | Fragment Offset = 0 dec
23    | 1111 1111 | Time To Live = 255 seconds
24    | 1000 0100 | Protocol = SCTP (132 dec)
25    | 0000 0000 | Header Checksum = 0 dec, 0000 hex
26    | 0000 0000 | Header Checksum
27    | 0000 1010 | Source Address = 10.185.147.6
28    | 1011 1001 | Source Address
29    | 1001 0011 | Source Address
30    | 0000 0110 | Source Address
31    | 0000 1010 | Destination Address = 10.187.36.11
32    | 1011 1011 | Destination Address
33    | 0010 0100 | Destination Address
34    | 0000 1011 | Destination Address
35    | 0001 0000 | Source Port Number = 4122 dec, 101A hex
36    | 0001 1010 | Source Port Number
37    | 0001 0000 | Destination Port Number = 4122 dec, 101A hex
38    | 0001 1010 | Destination Port Number
39    | 1001 1111 | Verification Tag = 9F37674C hex
40    | 0011 0111 | Verification Tag
41    | 0110 0111 | Verification Tag
42    | 0100 1100 | Verification Tag
43    | 1000 1111 | Checksum = 8F6681C5 hex
44    | 0110 0110 | Checksum
45    | 1000 0001 | Checksum
46    | 1100 0101 | Checksum
47    | 0000 0000 | chunk Type = Payload Data
48    | 0000 0011 | chunk Flags: U = ordered, B = first, E = last
49    | 0000 0000 | chunk Length = 148 octets
50    | 1001 0100 | chunk Length
51    | 0000 0000 | TSN = 5658498 dec, 00565782 hex
52    | 0101 0110 | TSN
53    | 0101 0111 | TSN
54    | 1000 0010 | TSN
55    | 0000 0000 | Stream Identifier = 8 dec, 0008 hex
56    | 0000 1000 | Stream Identifier
57    | 1111 0011 | Stream Sequence Number = 62420 dec, F3D4 hex
58    | 1101 0100 | Stream Sequence Number
59    | 0000 0000 | Payload Protocol Identifier = M3UA
60    | 0000 0000 | Payload Protocol Identifier
61    | 0000 0000 | Payload Protocol Identifier
62    | 0000 0011 | Payload Protocol Identifier
63    | 0000 0001 | Version = 01, M3UA Release 1.0
64    | 0000 0000 | Spare octet
65    | 0000 0001 | Message Class = Transfer Messages
66    | 0000 0001 | Message Type = Payload Data
67    | 0000 0000 | Message Length = 132 octets
68    | 0000 0000 | Message Length
69    | 0000 0000 | Message Length
70    | 1000 0100 | Message Length
71    | 0000 0000 | Routing Context Tag
72    | 0000 0110 | Routing Context Tag
73    | 0000 0000 | Routing Context Length = 8 octets

```

74		0000 1000		Routing Context Length	
75		0000 0000		Routing Context 1 = 65535 (dec), 0000FFFF (hex)	
76		0000 0000		Routing Context 1	
77		1111 1111		Routing Context 1	
78		1111 1111		Routing Context 1	
79		0000 0010		Protocol Data Tag	
80		0001 0000		Protocol Data Tag	
81		0000 0000		Protocol Data Length = 113 octets	
82		0111 0001		Protocol Data Length	
83		0000 0000		Originating Point Code, OPC = 12410 (dec), 0000307A (hex)	
84		0000 0000		Originating Point Code, OPC	
85		0011 0000		Originating Point Code, OPC	
86		0111 1010		Originating Point Code, OPC	
87		0000 0000		Destination Point Code, DPC = 9483 (dec), 0000250B (hex)	
88		0000 0000		Destination Point Code, DPC	
89		0010 0101		Destination Point Code, DPC	
90		0000 1011		Destination Point Code, DPC	
91		0000 0011		Service Ind, SI = SCCP message	
92		0000 0010		Network Ind, NI = National Network	
93		0000 0000		Message Priority, MP = 0	
94		0000 0010		Signalling Link Selection, SLS = 2	
				ITU.96.SCCP	
95	F		0000 1001		MT = Unitdata (UDT)
96	F		1000 0000		Protocol Class = class 0; Msg handling = return on error
97	F		0000 0011		Pointer to Called Party Address Parameter = 3 octet(s)
98	F		0000 1110		Pointer to Calling Party Address Parameter = 14 octet(s)
99	F		0001 1001		Pointer to Data Parameter = 25 octet(s)
100	V		0000 1011		LI of Called Party Address parameter = 11 octet(s)
101	V		0001 0010		Addr Ind: Int'l; Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
102	V		0000 1000		Subsystem Number = 8 MSC
103	V		0000 0000		Translation Type = 0 unknown
104	V		0001 0010		Numbering Plan = 1. ISDN/telephony, Encoding = 2. BCD even
105	V		0 0000100		Nature of Address Indicator = 4. international number
106	V		0101 0101		Address Signal = 550312001001
107	V		0011 0000		Address Signal
108	V		0010 0001		Address Signal
109	V		0000 0000		Address Signal
110	V		0000 0001		Address Signal
111	V		0001 0000		Address Signal
112	V		0000 1011		LI of Calling Party Address parameter = 11 octet(s)
113	V		0001 0010		Addr Ind: Int'l; Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
114	V		0000 1001		Subsystem Number = 9 EIC
115	V		0000 0000		Translation Type = 0 unknown
116	V		0001 0010		Numbering Plan = 1. ISDN/telephony, Encoding = 2. BCD even
117	V		0 0000100		Nature of Address Indicator = 4. international number
118	V		0101 0101		Address Signal = 550310000009
119	V		0011 0000		Address Signal
120	V		0000 0001		Address Signal
121	V		0000 0000		Address Signal
122	V		0000 0000		Address Signal
123	V		1001 0000		Address Signal
124	V		0100 0011		LI of Data parameter = 67 octet(s)
				3GPP.MAP	
125		0110 0100		TCAP Message Type: End	
126		0100 0001		Length: 65 octets	
127		0100 1001		Destination Trans Id Tag: 49	
128		0000 0100		Length: 4 octet(s)	
129		0001 1001		Destination Transaction Id: 19079414	
130		0000 0111		Destination Transaction Id:	
131		1001 0100		Destination Transaction Id:	
132		0001 0100		Destination Transaction Id:	
133		0110 1011		Dialogue Portion Tag: 6b	
134		0010 1010		Length: 42 octets	
135		0010 1000		External Tag: 28	
136		0010 1000		Length: 40 octets	
137		0000 0110		Object Identifier Tag: 6	
138		0000 0111		Length: 7 octet(s)	
139		0000 0000		ccitt recommendation: 0	
140		0001 0001		q: 11	
141		1000 0110		773: 86	
142		0000 0101		Space character: 5	
143		0000 0001		as(1): 1	
144		0000 0001		dialoguePDU: 1	
145		0000 0001		version1(1): 1	
146		1010 0000		Single ASN.1 Type Tag: a0	
147		0001 1101		Length: 29 octets	
148		0110 0001		Dialogue PDU: Dialogue Response	

149	0001 1011	Length: 27 octets
150	1000 0000	Protocol Version Tag: 80
151	0000 0010	Length: 2 octet(s)
152	0000 0111	Protocol Version: 780
153	1000 0000	Protocol Version:
154	1010 0001	Application Context Name Tag: a1
155	0000 1001	Length: 9 octets
156	0000 0110	Object Identifier Tag: 6
157	0000 0111	Length: 7 octet(s)
158	0000 0100	ccitt recommendation: 4
159	0000 0000	etsi: 0
160	0000 0000	Mobile Domain: 0
161	0000 0001	GSM Network: 1
162	0000 0000	ac_id: 0
163	0000 1101	dialoguePDU: EquipmentMngt
164	0000 0010	version: 2
165	1010 0010	Result Tag: a2
166	0000 0011	Length: 3 octets
167	0000 0010	Integer Tag: 2
168	0000 0001	Length: 1 octet(s)
169	0000 0000	Result: Accepted
170	1010 0011	Result Source Diagnostic Tag: a3
171	0000 0101	Length: 5 octets
172	1010 0001	Service User Tag: a1
173	0000 0011	Length: 3 octets
174	0000 0010	Integer Tag: 2
175	0000 0001	Length: 1 octet(s)
176	0000 0000	Service User Value: Null
177	0110 1100	Component Portion Tag: 6c
178	0000 1101	Length: 13 octets
179	1010 0010	Return Result (Last): a2
180	0000 1011	Length: 11 octets
181	0000 0010	Invoke Id Tag: 2
182	0000 0001	Length: 1 octet(s)
183	0000 0000	Invoke Id: 0
184	0011 0000	Sequence Tag: 30
185	0000 0110	Length: 6 octets
186	0000 0010	Operation Code Tag: Local Operation Code
187	0000 0001	Length: 1 octet(s)
188	0010 1011	Operation Code (Return Result): Check IMEI
189	0000 1010	Equipment Status Tag: a
190	0000 0001	Length: 1 octet(s)
191	0000 0000	Equipment Status: White Listed
		NULL.LAYER1
192	0000 0000	Padding
193	0000 0000	Padding
194	0000 0000	Padding

## A.2. CONSULTA AO AUC

CT (1) - Protocol Level Display (8)

```

01:21:03.592 PM SAT Link: PTS*BSASG1_BrT_IP_0
802.3 / Ethernet
  Source MAC Addr: 00:28:00:20:00:00 Destination MAC Addr: 00:00:0c:07:ac:96
IP Version 4
  Precedence: Routine
  Delay: Normal delay
  Throughput: Normal throughput
  Reliability: Normal reliability
  Total Length: 184 octets
  Protocol: SCTP
  Source Address: 10.185.3.10 Destination Address: 10.187.0.71
SCTP
  Source Port: 2925 Destination Port: 2925
chunk Type: Payload Data
  chunk Flags: U: Ordered B: First fragment E: Last fragment
  Stream Identifier: 1
M3UA Message Class: Transfer Messages
M3UA Message Type: Payload Data
OPC: DF-BSAHUAL DPC: HLR43BSI SI: SCCP NI/MP: NN SLS: 14
MT: UDT
Called Party Address Length: 13 octets
  Subsystem Number: HLR
  Translation Type: unknown
  Nature of Address Indicator: 4. International number
  Address Information: xxxxxxxxxxxxxxxx
Calling Party Address Length: 11 octets
  Subsystem Number: VLR
  Translation Type: unknown
  Nature of Address Indicator: 4. International number
  Address Information: 550160006220
TCAP Message Type: Begin
Originating Trans Id Tag: 48
  Originating Transaction Id: 7900015a
Component Portion Tag: 6c
Invoke: a1
  Invoke Id: 1
Operation Code Tag: Local Operation Code
Operation Code (Invoke): Send Authentication Info
IMSI Tag: 80
  IMSI Digits: xxxxxxxxxxxxxxxx
  End of contents
Padding: 0

```

```

| | IP.SCTP.MTP_ITU
1 | 0000 0000 | I/G = 0, U/L = 0, Destination Address = 00:00:0C:07:AC:96
2 | 0000 0000 | Destination Address
3 | 0000 1100 | Destination Address
4 | 0000 0111 | Destination Address
5 | 1010 1100 | Destination Address
6 | 1001 0110 | Destination Address
7 | 0000 0000 | I/G = 0, U/L = 0, Source Address = 00:28:00:20:00:00
8 | 0010 1000 | Source Address
9 | 0000 0000 | Source Address
10 | 0010 0000 | Source Address
11 | 0000 0000 | Source Address
12 | 0000 0000 | Source Address
13 | 0000 1000 | Ethernet Type = 0800 - IPv4
14 | 0000 0000 | Ethernet Type
15 | 0100|0101 | IP Version 4, IHL = 5 32-bit words
16 | 000000|00 | Prec. = Routine, Norm delay, Norm thru-put, Norm rel.
17 | 0000 0000 | Total Length = 184 octets
18 | 1011 1000 | Total Length
19 | 1010 1101 | Identification = 44492 dec, ADCC hex
20 | 1100 1100 | Identification
21 | 000|00000 | Flags = May fragment, Last fragment
22 | 0000 0000 | Fragment Offset = 0 dec
23 | 1111 1111 | Time To Live = 255 seconds
24 | 1000 0100 | Protocol = SCTP (132 dec)
25 | 0000 0000 | Header Checksum = 0 dec, 0000 hex
26 | 0000 0000 | Header Checksum

```

```

27 | 0000 1010 | Source Address = 10.185.3.10
28 | 1011 1001 | Source Address
29 | 0000 0011 | Source Address
30 | 0000 1010 | Source Address
31 | 0000 1010 | Destination Address = 10.187.0.71
32 | 1011 1011 | Destination Address
33 | 0000 0000 | Destination Address
34 | 0100 0111 | Destination Address
35 | 0000 1011 | Source Port Number = 2925 dec, 0B6D hex
36 | 0110 1101 | Source Port Number
37 | 0000 1011 | Destination Port Number = 2925 dec, 0B6D hex
38 | 0110 1101 | Destination Port Number
39 | 0010 0101 | Verification Tag = 629551103 dec, 25862FFF hex
40 | 1000 0110 | Verification Tag
41 | 0010 1111 | Verification Tag
42 | 1111 1111 | Verification Tag
43 | 0111 0011 | Checksum = 1929816442 dec, 7306A97A hex
44 | 0000 0110 | Checksum
45 | 1010 1001 | Checksum
46 | 0111 1010 | Checksum
47 | 0000 0000 | chunk Type = Payload Data
48 | 0000 0011 | chunk Flags: U = ordered, B = first, E = last
49 | 0000 0000 | chunk Length = 152 octets
50 | 1001 1000 | chunk Length
51 | 0000 0110 | TSN = 111974021 dec, 06AC9685 hex
52 | 1010 1100 | TSN
53 | 1001 0110 | TSN
54 | 1000 0101 | TSN
55 | 0000 0000 | Stream Identifier = 1 dec, 0001 hex
56 | 0000 0001 | Stream Identifier
57 | 1100 1110 | Stream Sequence Number = 52970 dec, CEEA hex
58 | 1110 1010 | Stream Sequence Number
59 | 0000 0000 | Payload Protocol Identifier = M3UA
60 | 0000 0000 | Payload Protocol Identifier
61 | 0000 0000 | Payload Protocol Identifier
62 | 0000 0011 | Payload Protocol Identifier
63 | 0000 0001 | Version = 01, M3UA Release 1.0
64 | 0000 0000 | Spare octet
65 | 0000 0001 | Message Class = Transfer Messages
66 | 0000 0001 | Message Type = Payload Data
67 | 0000 0000 | Message Length = 136 octets
68 | 0000 0000 | Message Length
69 | 0000 0000 | Message Length
70 | 1000 1000 | Message Length
71 | 0000 0000 | Routing Context Tag
72 | 0000 0110 | Routing Context Tag
73 | 0000 0000 | Routing Context Length = 8 octets
74 | 0000 1000 | Routing Context Length
75 | 0000 0000 | Routing Context 1 = 65535 (dec), 0000FFFF (hex)
76 | 0000 0000 | Routing Context 1
77 | 1111 1111 | Routing Context 1
78 | 1111 1111 | Routing Context 1
79 | 0000 0010 | Protocol Data Tag
80 | 0001 0000 | Protocol Data Tag
81 | 0000 0000 | Protocol Data Length = 118 octets
82 | 0111 0110 | Protocol Data Length
83 | 0000 0000 | Originating Point Code, OPC = 7915 (dec), 00001EEB (hex)
84 | 0000 0000 | Originating Point Code, OPC
85 | 0001 1110 | Originating Point Code, OPC
86 | 1110 1011 | Originating Point Code, OPC
87 | 0000 0000 | Destination Point Code, DPC = 6791 (dec), 00001A87 (hex)
88 | 0000 0000 | Destination Point Code, DPC
89 | 0001 1010 | Destination Point Code, DPC
90 | 1000 0111 | Destination Point Code, DPC
91 | 0000 0011 | Service Ind, SI = SCCP message
92 | 0000 0010 | Network Ind, NI = National Network
93 | 0000 0000 | Message Priority, MP = 0
94 | 0000 1110 | Signalling Link Selection, SLS = 14
| | ITU.96.SCCP
95 | F | 0000 1001 | MT = Unitdata (UDT)
96 | F | 1000 0001 | Protocol Class = class 1; Msg handling = return on error
97 | F | 0000 0011 | Pointer to Called Party Address Parameter = 3 octet(s)
98 | F | 0001 0000 | Pointer to Calling Party Address Parameter = 16 octet(s)
99 | F | 0001 1011 | Pointer to Data Parameter = 27 octet(s)
100 | V | 0000 1101 | LI of Called Party Address parameter = 13 octet(s)
101 | V | 0101 0010 | Addr Ind: Int'l; Route=SSN; GT=TT&NP&ES&NoA; PC=N; SSN=Y
102 | V | 0000 0110 | Subsystem Number = 6 HLR

```

```

103 V | 0000 0000 | Translation Type = 0 unknown
104 V | 0111|0001 | Numbering Plan = 7. ISDN mobile, Encoding = 1. BCD odd
105 V | 0|0000100 | Nature of Address Indicator = 4. international number
106 V | xxxx|xxxx | Address Signal = xxxxxxxxxxxxxxxx
107 V | xxxx|xxxx | Address Signal
108 V | xxxx|xxxx | Address Signal
109 V | xxxx|xxxx | Address Signal
110 V | xxxx|xxxx | Address Signal
111 V | xxxx|xxxx | Address Signal
112 V | xxxx|xxxx | Address Signal
113 V | xxxx|xxxx | Address Signal
114 V | 0000 1011 | LI of Calling Party Address parameter = 11 octet(s)
115 V | 0001 0010 | Addr Ind: Int'l; Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
116 V | 0000 0111 | Subsystem Number = 7 VLR
117 V | 0000 0000 | Translation Type = 0 unknown
118 V | 0001|0010 | Numbering Plan = 1. ISDN/telephony, Encoding = 2. BCD even
119 V | 0|0000100 | Nature of Address Indicator = 4. international number
120 V | 0101|0101 | Address Signal = 550160006220
121 V | 0001|0000 | Address Signal
122 V | 0000|0110 | Address Signal
123 V | 0000|0000 | Address Signal
124 V | 0010|0110 | Address Signal
125 V | 0000|0010 | Address Signal
126 V | 0100 0110 | LI of Data parameter = 70 octet(s)
    | | 3GPP.MAP
127 | 0110 0010 | TCAP Message Type: Begin
128 | 0100 0100 | Length: 68 octets
129 | 0100 1000 | Originating Trans Id Tag: 48
130 | 0000 0100 | Length: 4 octet(s)
131 | 0111 1001 | Originating Transaction Id: 7900015a
132 | 0000 0000 | Originating Transaction Id:
133 | 0000 0001 | Originating Transaction Id:
134 | 0101 1010 | Originating Transaction Id:
135 | 0110 1011 | Dialogue Portion Tag: 6b
136 | 0001 1110 | Length: 30 octets
137 | 0010 1000 | External Tag: 28
138 | 0001 1100 | Length: 28 octets
139 | 0000 0110 | Object Identifier Tag: 6
140 | 0000 0111 | Length: 7 octet(s)
141 | 0000 0000 | ccitt recommendation: 0
142 | 0001 0001 | q: 11
143 | 1000 0110 | 773: 86
144 | 0000 0101 | Space character: 5
145 | 0000 0001 | as(1): 1
146 | 0000 0001 | dialoguePDU: 1
147 | 0000 0001 | version1(1): 1
148 | 1010 0000 | Single ASN.1 Type Tag: a0
149 | 0001 0001 | Length: 17 octets
150 | 0110 0000 | Dialogue PDU: Dialogue Request
151 | 0000 1111 | Length: 15 octets
152 | 1000 0000 | Protocol Version Tag: 80
153 | 0000 0010 | Length: 2 octet(s)
154 | 0000 0111 | Protocol Version: 780
155 | 1000 0000 | Protocol Version:
156 | 1010 0001 | Application Context Name Tag: a1
157 | 0000 1001 | Length: 9 octets
158 | 0000 0110 | Object Identifier Tag: 6
159 | 0000 0111 | Length: 7 octet(s)
160 | 0000 0100 | ccitt recommendation: 4
161 | 0000 0000 | etsi: 0
162 | 0000 0000 | Mobile Domain: 0
163 | 0000 0001 | GSM Network: 1
164 | 0000 0000 | ac_id: 0
165 | 0000 1110 | dialoguePDU: InfoRetrieval
166 | 0000 0011 | version: 3
167 | 0110 1100 | Component Portion Tag: 6c
168 | 1000 0000 | Length: Indefinite
169 | 1010 0001 | Invoke: a1
170 | 0001 1000 | Length: 24 octets
171 | 0000 0010 | Invoke Id Tag: 2
172 | 0000 0001 | Length: 1 octet(s)
173 | 0000 0001 | Invoke Id: 1
174 | 0000 0010 | Operation Code Tag: Local Operation Code
175 | 0000 0001 | Length: 1 octet(s)
176 | 0011 1000 | Operation Code (Invoke): Send Authentication Info
177 | 0011 0000 | Sequence Tag: 30
178 | 0001 0000 | Length: 16 octets

```

```

179      | 1000 0000 | IMSI Tag: 80
180      | 0000 1000 | Length: 8 octet(s)
181      | xxxx xxxx | IMSI Digits: xxxxxxxxxxxxxxxx
182      | xxxx xxxx | IMSI Digits:
183      | xxxx xxxx | IMSI Digits:
184      | xxxx xxxx | IMSI Digits:
185      | xxxx xxxx | IMSI Digits:
186      | xxxx xxxx | IMSI Digits:
187      | xxxx xxxx | IMSI Digits:
188      | ---- xxxx | IMSI Digits:
          | 1111 ---- | Filler: f
189      | 0000 0010 | Number Of Requested Vectors Tag: 2
190      | 0000 0001 | Length: 1 octet(s)
191      | 0000 0001 | Number Of Requested Vectors: 1
192      | 1000 0011 | Requesting Node Type Tag: 83
193      | 0000 0001 | Length: 1 octet(s)
194      | 0000 0000 | Requesting Node Type: VLR
195      | 0000 0000 | End of contents
196      | 0000 0000 |
          |           | NULL.LAYER1
197      | 0000 0000 | Padding
198      | 0000 0000 | Padding

```

01:21:03.633 PM SAT Link: PTS\*BSASG1\_BrT\_IP\_0

802.3 / Ethernet

Source MAC Addr: 00:1a:00:20:00:00 Destination MAC Addr: 00:e0:fc:fb:3f:17

IP Version 4

Precedence: Routine  
Delay: Normal delay  
Throughput: Normal throughput  
Reliability: Normal reliability  
Total Length: 224 octets  
Protocol: SCTP

Source Address: 10.187.0.6 Destination Address: 10.185.3.9

SCTP

Source Port: 4925 Destination Port: 4925

chunk Type: Payload Data

chunk Flags: U: Ordered B: First fragment E: Last fragment

Stream Identifier: 14

M3UA Message Class: Transfer Messages

M3UA Message Type: Payload Data

OPC: HLR43BSI DPC: DF-BSAHUA1 SI: SCCP NI/MP: NN SLS: 6

MT: UDT

Called Party Address Length: 11 octets

Subsystem Number: VLR  
Translation Type: unknown  
Nature of Address Indicator: 4. International number  
Address Information: 550160006220

Calling Party Address Length: 11 octets

Subsystem Number: HLR  
Translation Type: unknown  
Nature of Address Indicator: 4. International number  
Address Information: 550160006100

TCAP Message Type: End

Destination Trans Id Tag: 49

Destination Transaction Id: 7900015a

Component Portion Tag: 6c

Return Result (Last): a2

Invoke Id: 1

Operation Code Tag: Local Operation Code

Operation Code (Return Result): Send Authentication Info

Authentication Triplet Tag: 30

RAND Tag: 4

RAND 1: 4f9d6cd1bc76932a1aa8274ea9f97a7f

SRES Tag: 4

SRES 1: ald40543

KC Tag: 4

KC 1: 185658daabcafc00

Padding: 0

```

          |           | IP.SCTP.MTP_ITU
1      | 0000 0000 | I/G = 0, U/L = 0, Destination Address = 00:E0:FC:FB:3F:17
2      | 1110 0000 | Destination Address
3      | 1111 1100 | Destination Address
4      | 1111 1011 | Destination Address

```

```

5      | 0011 1111 | Destination Address
6      | 0001 0111 | Destination Address
7      | 0000 0000 | I/G = 0, U/L = 0, Source Address = 00:1A:00:20:00:00
8      | 0001 1010 | Source Address
9      | 0000 0000 | Source Address
10     | 0010 0000 | Source Address
11     | 0000 0000 | Source Address
12     | 0000 0000 | Source Address
13     | 0000 1000 | Ethernet Type = 0800 - IPv4
14     | 0000 0000 | Ethernet Type
15     | 0100|0101 | IP Version 4, IHL = 5 32-bit words
16     | 000000|00 | Prec. = Routine, Norm delay, Norm thru-put, Norm rel.
17     | 0000 0000 | Total Length = 224 octets
18     | 1110 0000 | Total Length
19     | 1100 0111 | Identification = 51084 dec, C78C hex
20     | 1000 1100 | Identification
21     | 010|00000 | Flags = Don't fragment, Last fragment
22     | 0000 0000 | Fragment Offset = 0 dec
23     | 0011 1110 | Time To Live = 62 seconds
24     | 1000 0100 | Protocol = SCTP (132 dec)
25     | 0000 0000 | Header Checksum = 0 dec, 0000 hex
26     | 0000 0000 | Header Checksum
27     | 0000 1010 | Source Address = 10.187.0.6
28     | 1011 1011 | Source Address
29     | 0000 0000 | Source Address
30     | 0000 0110 | Source Address
31     | 0000 1010 | Destination Address = 10.185.3.9
32     | 1011 1001 | Destination Address
33     | 0000 0011 | Destination Address
34     | 0000 1001 | Destination Address
35     | 0001 0011 | Source Port Number = 4925 dec, 133D hex
36     | 0011 1101 | Source Port Number
37     | 0001 0011 | Destination Port Number = 4925 dec, 133D hex
38     | 0011 1101 | Destination Port Number
39     | 0000 0000 | Verification Tag = 6536 dec, 00001988 hex
40     | 0000 0000 | Verification Tag
41     | 0001 1001 | Verification Tag
42     | 1000 1000 | Verification Tag
43     | 0110 1010 | Checksum = 1780168820 dec, 6A1B3874 hex
44     | 0001 1011 | Checksum
45     | 0011 1000 | Checksum
46     | 0111 0100 | Checksum
47     | 0000 0000 | chunk Type = Payload Data
48     | 0000 0011 | chunk Flags: U = ordered, B = first, E = last
49     | 0000 0000 | chunk Length = 192 octets
50     | 1100 0000 | chunk Length
51     | 0011 1011 | TSN = 1005259447 dec, 3BEB0AB7 hex
52     | 1110 1011 | TSN
53     | 0000 1010 | TSN
54     | 1011 0111 | TSN
55     | 0000 0000 | Stream Identifier = 14 dec, 000E hex
56     | 0000 1110 | Stream Identifier
57     | 0001 0101 | Stream Sequence Number = 5426 dec, 1532 hex
58     | 0011 0010 | Stream Sequence Number
59     | 0000 0000 | Payload Protocol Identifier = M3UA
60     | 0000 0000 | Payload Protocol Identifier
61     | 0000 0000 | Payload Protocol Identifier
62     | 0000 0011 | Payload Protocol Identifier
63     | 0000 0001 | Version = 01, M3UA Release 1.0
64     | 0000 0000 | Spare octet
65     | 0000 0001 | Message Class = Transfer Messages
66     | 0000 0001 | Message Type = Payload Data
67     | 0000 0000 | Message Length = 176 octets
68     | 0000 0000 | Message Length
69     | 0000 0000 | Message Length
70     | 1011 0000 | Message Length
71     | 0000 0010 | Network Appearance Tag
72     | 0000 0000 | Network Appearance Tag
73     | 0000 0000 | Network Appearance Length = 8 octets
74     | 0000 1000 | Network Appearance Length
75     | 0000 0000 | Network Appearance = 8 (dec), 00000008 (hex)
76     | 0000 0000 | Network Appearance
77     | 0000 0000 | Network Appearance
78     | 0000 1000 | Network Appearance
79     | 0000 0000 | Routing Context Tag
80     | 0000 0110 | Routing Context Tag
81     | 0000 0000 | Routing Context Length = 8 octets

```

82		0000 1000		Routing Context Length
83		0000 0000		Routing Context 1 = 65535 (dec), 0000FFFF (hex)
84		0000 0000		Routing Context 1
85		1111 1111		Routing Context 1
86		1111 1111		Routing Context 1
87		0000 0010		Protocol Data Tag
88		0001 0000		Protocol Data Tag
89		0000 0000		Protocol Data Length = 150 octets
90		1001 0110		Protocol Data Length
91		0000 0000		Originating Point Code, OPC = 6791 (dec), 00001A87 (hex)
92		0000 0000		Originating Point Code, OPC
93		0001 1010		Originating Point Code, OPC
94		1000 0111		Originating Point Code, OPC
95		0000 0000		Destination Point Code, DPC = 7915 (dec), 00001EEB (hex)
96		0000 0000		Destination Point Code, DPC
97		0001 1110		Destination Point Code, DPC
98		1110 1011		Destination Point Code, DPC
99		0000 0011		Service Ind, SI = SCCP message
100		0000 0010		Network Ind, NI = National Network
101		0000 0000		Message Priority, MP = 0
102		0000 0110		Signalling Link Selection, SLS = 6
				ITU.96.SCCP
103	F	0000 1001		MT = Unitdata (UDT)
104	F	1000 0000		Protocol Class = class 0; Msg handling = return on error
105	F	0000 0011		Pointer to Called Party Address Parameter = 3 octet(s)
106	F	0000 1110		Pointer to Calling Party Address Parameter = 14 octet(s)
107	F	0001 1001		Pointer to Data Parameter = 25 octet(s)
108	V	0000 1011		LI of Called Party Address parameter = 11 octet(s)
109	V	0001 0010		Addr Ind: Int'l; Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
110	V	0000 0111		Subsystem Number = 7 VLR
111	V	0000 0000		Translation Type = 0 unknown
112	V	0001 0010		Numbering Plan = 1. ISDN/telephony, Encoding = 2. BCD even
113	V	0 0000100		Nature of Address Indicator = 4. international number
114	V	0101 0101		Address Signal = 550160006220
115	V	0001 0000		Address Signal
116	V	0000 0110		Address Signal
117	V	0000 0000		Address Signal
118	V	0010 0110		Address Signal
119	V	0000 0010		Address Signal
120	V	0000 1011		LI of Calling Party Address parameter = 11 octet(s)
121	V	0001 0010		Addr Ind: Int'l; Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
122	V	0000 0110		Subsystem Number = 6 HLR
123	V	0000 0000		Translation Type = 0 unknown
124	V	0001 0010		Numbering Plan = 1. ISDN/telephony, Encoding = 2. BCD even
125	V	0 0000100		Nature of Address Indicator = 4. international number
126	V	0101 0101		Address Signal = 550160006100
127	V	0001 0000		Address Signal
128	V	0000 0110		Address Signal
129	V	0000 0000		Address Signal
130	V	0001 0110		Address Signal
131	V	0000 0000		Address Signal
132	V	0110 1000		LI of Data parameter = 104 octet(s)
				3GPP.MAP
133		0110 0100		TCAP Message Type: End
134		0110 0110		Length: 102 octets
135		0100 1001		Destination Trans Id Tag: 49
136		0000 0100		Length: 4 octet(s)
137		0111 1001		Destination Transaction Id: 7900015a
138		0000 0000		Destination Transaction Id:
139		0000 0001		Destination Transaction Id:
140		0101 1010		Destination Transaction Id:
141		0110 1011		Dialogue Portion Tag: 6b
142		0010 1010		Length: 42 octets
143		0010 1000		External Tag: 28
144		0010 1000		Length: 40 octets
145		0000 0110		Object Identifier Tag: 6
146		0000 0111		Length: 7 octet(s)
147		0000 0000		ccitt recommendation: 0
148		0001 0001		q: 11
149		1000 0110		773: 86
150		0000 0101		Space character: 5
151		0000 0001		as(1): 1
152		0000 0001		dialoguePDU: 1
153		0000 0001		version1(1): 1
154		1010 0000		Single ASN.1 Type Tag: a0
155		0001 1101		Length: 29 octets
156		0110 0001		Dialogue PDU: Dialogue Response

```

157 | 0001 1011 | Length: 27 octets
158 | 1000 0000 | Protocol Version Tag: 80
159 | 0000 0010 | Length: 2 octet(s)
160 | 0000 0111 | Protocol Version: 780
161 | 1000 0000 | Protocol Version:
162 | 1010 0001 | Application Context Name Tag: a1
163 | 0000 1001 | Length: 9 octets
164 | 0000 0110 | Object Identifier Tag: 6
165 | 0000 0111 | Length: 7 octet(s)
166 | 0000 0100 | ccitt recommendation: 4
167 | 0000 0000 | etsi: 0
168 | 0000 0000 | Mobile Domain: 0
169 | 0000 0001 | GSM Network: 1
170 | 0000 0000 | ac_id: 0
171 | 0000 1110 | dialoguePDU: InfoRetrieval
172 | 0000 0011 | version: 3
173 | 1010 0010 | Result Tag: a2
174 | 0000 0011 | Length: 3 octets
175 | 0000 0010 | Integer Tag: 2
176 | 0000 0001 | Length: 1 octet(s)
177 | 0000 0000 | Result: Accepted
178 | 1010 0011 | Result Source Diagnostic Tag: a3
179 | 0000 0101 | Length: 5 octets
180 | 1010 0001 | Service User Tag: a1
181 | 0000 0011 | Length: 3 octets
182 | 0000 0010 | Integer Tag: 2
183 | 0000 0001 | Length: 1 octet(s)
184 | 0000 0000 | Service User Value: Null
185 | 0110 1100 | Component Portion Tag: 6c
186 | 0011 0010 | Length: 50 octets
187 | 1010 0010 | Return Result (Last): a2
188 | 0011 0000 | Length: 48 octets
189 | 0000 0010 | Invoke Id Tag: 2
190 | 0000 0001 | Length: 1 octet(s)
191 | 0000 0001 | Invoke Id: 1
192 | 0011 0000 | Sequence Tag: 30
193 | 0010 1011 | Length: 43 octets
194 | 0000 0010 | Operation Code Tag: Local Operation Code
195 | 0000 0001 | Length: 1 octet(s)
196 | 0011 1000 | Operation Code (Return Result): Send Authentication Info
197 | 1010 0011 | Sequence Tag: a3
198 | 0010 0110 | Length: 38 octets
199 | 1010 0000 | Triplet List Tag: a0
200 | 0010 0100 | Length: 36 octets
201 | 0011 0000 | Authentication Triplet Tag: 30
202 | 0010 0010 | Length: 34 octets
203 | 0000 0100 | RAND Tag: 4
204 | 0001 0000 | Length: 16 octet(s)
205 | 0100 1111 | RAND 1: 4f9d6cd1bc76932a1aa8274ea9f97a7f
206 | 1001 1101 | RAND 1:
207 | 0110 1100 | RAND 1:
208 | 1101 0001 | RAND 1:
209 | 1011 1100 | RAND 1:
210 | 0111 0110 | RAND 1:
211 | 1001 0011 | RAND 1:
212 | 0010 1010 | RAND 1:
213 | 0001 1010 | RAND 1:
214 | 1010 1000 | RAND 1:
215 | 0010 0111 | RAND 1:
216 | 0100 1110 | RAND 1:
217 | 1010 1001 | RAND 1:
218 | 1111 1001 | RAND 1:
219 | 0111 1010 | RAND 1:
220 | 0111 1111 | RAND 1:
221 | 0000 0100 | SRES Tag: 4
222 | 0000 0100 | Length: 4 octet(s)
223 | 1010 0001 | SRES 1: ald40543
224 | 1101 0100 | SRES 1:
225 | 0000 0101 | SRES 1:
226 | 0100 0011 | SRES 1:
227 | 0000 0100 | KC Tag: 4
228 | 0000 1000 | Length: 8 octet(s)
229 | 0001 1000 | KC 1: 185658daabcafc00
230 | 0101 0110 | KC 1:
231 | 0101 1000 | KC 1:
232 | 1101 1010 | KC 1:
233 | 1010 1011 | KC 1:

```

```
234 | 1100 1010 | KC 1:
235 | 1111 1100 | KC 1:
236 | 0000 0000 | KC 1:
    |           | NULL.LAYER1
237 | 0000 0000 | Padding
238 | 0000 0000 | Padding
```

## A.3. CHAMADA ISUP

CT (1) - Protocol Level Display (1)

12:53:30.056 PM SAT Link: <-BSASG-MSC\*CTA1\*BV\_0

PDU Type: SD: Seqd Connection-mode Data

SI: ISUP SSF: NN DPC: MSS72CTA OPC: PR-CTAMSC1 SLS: 10

CIC: 554

F->MT: IAM

V->Called Party Number Length: 8 octets

Nature of Address Indicator: National Long Distance

Address Signal: xxxxxxxxxxxx

O->Calling Party Number Id

Nature of Address Indicator: National number

Address Signal: xxxxxxxxxxxx

O->Parameter Compatibility Information Id

			ITU.96.HS
1	1000 0101		Service Indicator = ISUP, SSF = National Network
2	0000 0011		DPC : 9475 dec, 2503 hex, 004-160-003 ITU383
3	00 100101		
4	1011 1110		OPC : 11000 dec, 2AF8 hex, 005-095-000 ITU383
5	1010 1010		SLS : 10 dec, A hex
			TELEB.96.ISUP
6	0010 1010		CIC:
7	---- 0010		CIC: 554
8	0000 0001		F->MT: IAM
9	---- --00		F->Nature of Connection Indicators
	---- --00		Satellite Indicator: No satellite circuit in the connection
	---- 00--		Continuity Check Indicator: Not required
	----0 ----		Echo control Device Indicator: Outgoing half echo device not included
10	---- ---0		F->Forward Call Indicators
	---- ---0		National/International Call Indicator: National call
	---- -00-		End to End Method Indicator: No end-to-end method
	---- 0---		Interworking Indicator: No interworking encountered
	---0 ----		End to End Information Indicator: No end-to-end info available
	--1- ----		ISDN User Part Indicator: ISUP used all the way
	01-- ----		ISDN User Part Preference Indicator: ISUP not needed all the way
11	---- ---1		ISDN Access Indicator: Originating access ISDN
	---- -00-		SCCP Method Indicator: No indication
	---0 ----		Collect Call Indicator: Normal call
12	1110 0000		F->Calling Party's Category: Subscriber with special billing
13	0000 0000		F->Transmission Medium Requirement: Speech
14	0000 0010		V->Pointer to Called Party Number: 2 octets
15	0000 1010		V->Pointer to Optional Part: 10 octets
16	0000 1000		V->Called Party Number Length: 8 octets
17	-000 0011		Nature of Address Indicator: National Long Distance
	1--- ----		Odd/Even Indicator: Odd num of address signals
18	-001 ----		Numbering Plan Indicator: ISDN/Telephony
19	xxxx xxxx		Address Signal:
20	xxxx xxxx		Address Signal:
21	xxxx xxxx		Address Signal:
22	xxxx xxxx		Address Signal:
23	xxxx xxxx		Address Signal:
24	xxxx xxxx		Address Signal: xxxxxxxxxxxx
25	0000 1010		O->Calling Party Number Id
26	0000 0111		Length: 7 octets
27	-000 0011		Nature of Address Indicator: National number
	0--- ----		Odd/Even Indicator: Even num of address signals
28	---- --11		Screening Indicator: Network provided
	---- 00--		Presentation Restriction Indicator: Presentation allowed
	-001 ----		Numbering Plan Indicator: ISDN/Telephony
	0--- ----		NI Indicator: Complete
29	xxxx xxxx		Address Signal:
30	xxxx xxxx		Address Signal:
31	xxxx xxxx		Address Signal:
32	xxxx xxxx		Address Signal:
33	xxxx xxxx		Address Signal: xxxxxxxxxxxx
34	0000 1000		O->Optional Forward Call Indicators Id
35	0000 0001		Length: 1 octet
36	---- --00		Closed User Group Call Ind: Non-CUG call
	0--- ----		Connected Line Identity Request Indicator: Not Requested

```

37      | 0001 1101 | O->User Service Information Id
38      | 0000 0011 | Length: 3 octets
39      | ---0 0000 | Information Transfer Capability: Speech
        | -00- ---- | Coding Standard: CCITT standardized
40      | ---1 0000 | Information Transfer Rate: 64 kbit/s
        | -00- ---- | Transfer Mode: Circuit mode
        | 1--- ---- | Extension Indicator: No extension
41      | ---0 0011 | User Info Layer 1 Protocol: Rec. G.711 A-law
42      | 0011 0001 | O->Propagation Delay Counter Id
43      | 0000 0010 | Length: 2 octets
44      | 0000 0000 | Delay: 100ms
        | 0000 0000 | -Undefined Tag: f4h
45      | 0110 0100 | Delay:
46      | 1111 0100 | Octet Value
47      | 0000 0101 | Length: 5 octets
48      | 1100 0101 | Undefined Octet
49      | 1011 0010 | Undefined Octet
50      | 1010 0111 | Undefined Octet
51      | 0000 0000 | Undefined Octet
52      | 0010 1001 | Undefined Octet
53      | 0011 1001 | O->Parameter Compatibility Information Id
54      | 0000 0100 | Length: 4 octets
55      | 0011 0001 | Upgraded Parameter: Propagation delay counter
56      | ---- ---0 | Transit at Intermediate Exchange Indicator:
        |          | Transit interpretation
        | ---- --0- | Release Call Indicator: Do not release call
        | ---- -0-- | Send Notification Indicator: Do not send notification
        | ---- 0--- | Discard Message Indicator: Do not discard message
        | ---1 ---- | Discard Parameter Indicator: Discard parameter
        | -10- ---- | Pass on not possible Indicator: Discard parameter
        | 1--- ---- | Extension Indicator: Last octet
57      | 1111 0100 | Upgraded Parameter: Undefined
58      | ---- ---0 | Transit at Intermediate Exchange Indicator:
        |          | Transit interpretation
        | ---- --0- | Release Call Indicator: Do not release call
        | ---- -0-- | Send Notification Indicator: Do not send notification
        | ---- 0--- | Discard Message Indicator: Do not discard message
        | ---0 ---- | Discard Parameter Indicator: Do not discard parameter
        | -10- ---- | Pass on not possible Indicator: Discard parameter
        | 1--- ---- | Extension Indicator: Last octet
59      | 0000 0000 | O->End of Optional Parameters
        |          | ITU.95.HSATM
60      M | 0001 1011 | Padding octet
61      M | 0100|1000 | PDU Type = SD
62      M | 1000 0011 | N(S)
63      M | 0001 0001 | N(S)
64      M | 0110 1111 | N(S)

```

```

12:53:32.435 PM SAT Link: ->BSASG-MSC*CTA1*BV_0
PDU Type: SD: Seqd Connection-mode Data
SI: ISUP SSF: NN DPC: PR-CTAMSC1 OPC: MSS72CTA SLS: 13
CIC: 554
F->MT: ACM

```

```

        |          | ITU.96.HS
1       | 1000|0101 | Service Indicator = ISUP, SSF = National Network
2       | 1111 1000 | DPC : 11000 dec, 2AF8 hex, 005-095-000 ITU383
3       | 11|101010 |
4       | 0100 0000 | OPC : 9475 dec, 2503 hex, 004-160-003 ITU383
5       | 1101|1001 | SLS : 13 dec, D hex
        |          | TELEB.96.ISUP
6       | 0010 1010 | CIC:
7       | ---- 0010 | CIC: 554
8       | 0000 0110 | F->MT: ACM
9       | ---- --10 | F->Backward Call Indicators
        | ---- --10 | Charge Indicator: Charge
        | ---- 00-- | Called Party's Status Indicator: No indication
        | --01 ---- | Called Party's Category Indicator: Ordinary subscriber
        | 00-- ---- | End to End Method Indicator: No end-end method available
10      | ---- ---0 | Interworking Indicator: No interworking
        | ---- --0- | End to End Information Indicator: No end-end info available
        | ---- -1-- | ISDN User Part Indicator: ISUP used all the way
        | ---- 0--- | Subscriber B Call Holding Indicator: Holding not requested
        | ---1 ---- | ISDN Access Indicator: Terminating access ISDN
        | --1- ---- | Echo Control Device Indicator: Half echo included

```

```

| 00-- ---- | SCCP Method Indicator: No indication
11 | 0000 0001 | V->Pointer to Optional Part: 1 octet
12 | 0010 1001 | O->Optional Backward Call Indicators Id
13 | 0000 0001 | Length: 1 octet
14 | ---- ---1 | Inband Information Indicator:
| | In-band information now available
| ---- --0- | Call Forwarding Indicator: No indication
15 | 0000 0000 | O->End of Optional Parameters
| | ITU.95.HSATM
16 M | 0000 0000 | Padding octet
17 M | 0100|1000 | PDU Type = SD
18 M | 1011 0100 | N(S)
19 M | 0100 0010 | N(S)
20 M | 1101 0011 | N(S)

```

12:53:32.524 PM SAT Link: ->BSASG-MSC\*CTA1\*BV\_0  
PDU Type: SD: Seqd Connection-mode Data  
SI: ISUP SSF: NN DPC: PR-CTAMSC1 OPC: MSS72CTA SLS: 13  
CIC: 554  
F->MT: CPG

```

| | ITU.96.HS
1 | 1000|0101 | Service Indicator = ISUP, SSF = National Network
2 | 1111 1000 | DPC : 11000 dec, 2AF8 hex, 005-095-000 ITU383
3 | 11|101010 |
4 | 0100 0000 | OPC : 9475 dec, 2503 hex, 004-160-003 ITU383
5 | 1101|1001 | SLS : 13 dec, D hex
| | TELEB.96.ISUP
6 | 0010 1010 | CIC:
7 | ---- 0010 | CIC: 554
8 | 0010 1100 | F->MT: CPG
9 | -000 0001 | F->Event Information
| -000 0001 | Event Indicator: ALERTING
| 0--- ---- | Event Presentation Restriction Indicator: No indication
10 | 0000 0001 | V->Pointer to Optional Part: 1 octet
11 | 0001 0001 | O->Backward Call Indicators Id
12 | 0000 0010 | Length: 2 octets
13 | ---- --10 | Charge Indicator: Charge
| ---- 01-- | Called Party's Status Indicator: Subscriber free
| --01 ---- | Called Party's Category Indicator: Ordinary subscriber
| 00-- ---- | End to End Method Indicator: No end-end method available
14 | ---- ---0 | Interworking Indicator: No interworking
| ---- --0- | End to End Information Indicator: No end-end info available
| ---- -1-- | ISDN User Part Indicator: ISUP used all the way
| ---- 0--- | Holding Indicator: Holding not requested
| ---1 ---- | ISDN Access Indicator: Terminating access ISDN
| --1- ---- | Echo Control Device Indicator: Half echo included
| 00-- ---- | SCCP Method Indicator: No indication
15 | 0000 0000 | O->End of Optional Parameters
| | ITU.95.HSATM
16 M | 0000 0000 | Padding octet
17 M | 0100|1000 | PDU Type = SD
18 M | 1011 0100 | N(S)
19 M | 0100 0010 | N(S)
20 M | 1110 0110 | N(S)

```

12:53:39.274 PM SAT Link: ->BSASG-MSC\*CTA1\*BV\_0  
PDU Type: SD: Seqd Connection-mode Data  
SI: ISUP SSF: NN DPC: PR-CTAMSC1 OPC: MSS72CTA SLS: 13  
CIC: 554  
F->MT: ANM

```

| | ITU.96.HS
1 | 1000|0101 | Service Indicator = ISUP, SSF = National Network
2 | 1111 1000 | DPC : 11000 dec, 2AF8 hex, 005-095-000 ITU383
3 | 11|101010 |
4 | 0100 0000 | OPC : 9475 dec, 2503 hex, 004-160-003 ITU383
5 | 1101|1001 | SLS : 13 dec, D hex
| | TELEB.96.ISUP
6 | 0010 1010 | CIC:
7 | ---- 0010 | CIC: 554
8 | 0000 1001 | F->MT: ANM
9 | 0000 0001 | V->Pointer to Optional Part: 1 octet

```

```

10      | 0001 0001 | O->Backward Call Indicators Id
11      | 0000 0010 | Length: 2 octets
12      | ---- --10 | Charge Indicator: Charge
        | ---- 01-- | Called Party's Status Indicator: Subscriber free
        | --01 ---- | Called Party's Category Indicator: Ordinary subscriber
        | 00-- ---- | End to End Method Indicator: No end-end method available
13      | ---- ---0 | Interworking Indicator: No interworking
        | ---- --0- | End to End Information Indicator: No end-end info available
        | ---- -1-- | ISDN User Part Indicator: ISUP used all the way
        | ---- 0--- | Holding Indicator: Holding not requested
        | ---1 ---- | ISDN Access Indicator: Terminating access ISDN
        | --1- ---- | Echo Control Device Indicator: Half echo included
        | 00-- ---- | SCCP Method Indicator: No indication
14      | 0000 0000 | O->End of Optional Parameters
        |          | ITU.95.HSATM
15 M    | 0000 0000 | Padding octet
16 M    | 0000 0000 | Padding octet
17 M    | 1000|1000 | PDU Type = SD
18 M    | 1011 0100 | N(S)
19 M    | 0100 0110 | N(S)
20 M    | 0110 0100 | N(S)

```

```

12:54:17.795 PM SAT Link: ->BSASG-MSC*CTA1*BV_0
PDU Type: SD: Seqd Connection-mode Data
SI: ISUP SSF: NN DPC: PR-CTAMSC1 OPC: MSS72CTA SLS: 13
CIC: 554
F->MT: REL
V->Cause Indicator Length: 2 octets
Cause Value: Normal call clearing

```

```

        |          | ITU.96.HS
1      | 1000|0101 | Service Indicator = ISUP, SSF = National Network
2      | 1111 1000 | DPC :      11000 dec,    2AF8 hex, 005-095-000 ITU383
3      | 11|101010 |
4      | 0100 0000 | OPC :      9475 dec,    2503 hex, 004-160-003 ITU383
5      | 1101|1001 | SLS :      13 dec,      D hex
        |          | TELEB.96.ISUP
6      | 0010 1010 | CIC:
7      | ---- 0010 | CIC: 554
8      | 0000 1100 | F->MT: REL
9      | 0000 0010 | V->Pointer to Cause Indicators: 2 octets
10     | 0000 0000 | V->Pointer to Optional Part: 0 octets
11     | 0000 0010 | V->Cause Indicator Length: 2 octets
12     | ---- 0000 | Location: User
        | -00- ---- | Coding Standard: CCITT standard
        | 1--- ---- | Extension Indicator: No extension
13     | -001 0000 | Cause Value: Normal call clearing
        |          | ITU.95.HSATM
14 M   | 0000 0000 | Padding octet
15 M   | 0000 0000 | Padding octet
16 M   | 0000 0000 | Padding octet
17 M   | 1100|1000 | PDU Type = SD
18 M   | 1011 0100 | N(S)
19 M   | 0101 1010 | N(S)
20 M   | 0010 0101 | N(S)

```

```

12:54:17.844 PM SAT Link: <-BSASG-MSC*CTA1*BV_0
PDU Type: SD: Seqd Connection-mode Data
SI: ISUP SSF: NN DPC: MSS72CTA OPC: PR-CTAMSC1 SLS: 10
CIC: 554
F->MT: RLC

```

```

        |          | ITU.96.HS
1      | 1000|0101 | Service Indicator = ISUP, SSF = National Network
2      | 0000 0011 | DPC :      9475 dec,    2503 hex, 004-160-003 ITU383
3      | 00|100101 |
4      | 1011 1110 | OPC :      11000 dec,    2AF8 hex, 005-095-000 ITU383
5      | 1010|1010 | SLS :      10 dec,      A hex
        |          | TELEB.96.ISUP
6      | 0010 1010 | CIC:
7      | ---- 0010 | CIC: 554
8      | 0001 0000 | F->MT: RLC
9      | 0000 0000 | V->Pointer to Optional Part: 0 octets

```

					ITU.95.HSATM
10	M		0101 1001		Padding octet
11	M		0000 1111		Padding octet
12	M		0110 0100		Padding octet
13	M		1100 1000		PDU Type = SD
14	M		1000 0011		N(S)
15	M		0010 1000		N(S)
16	M		0100 0100		N(S)

## A.4. CHAMADA ORIGINADA POR PRÉ-PAGO (CONSULTA CAMEL O-CSI)

CT (1) - Protocol Level Display (7)

```

12:58:04.687 PM SAT Link: ->CTASG-CTAPPE14_6
SI: SCCP SSF: NN DPC: PR-CTAPPES14 OPC: PR-CTAHUA1 SLS: 14
MT: UDT
Called Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550160000053h
Calling Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550312003001h
MT: Begin
Originating Transaction ID Tag
  Transaction Id: 40019445h
Invoke
Invoke Id Tag
  Invoke Id: 0
Operation Code Tag: Local Operation Code
Operation ID: Initial DP
Service Key Tag
  Length: 2 octets
  Service Key : 8100 dec, 1fa4 hex
Calling Party Number Tag
Calling Partys Category Tag
Location Number Tag
High Layer Compatibility Tag
Bearer Capability Tag
Event Type BCSM Tag
IMSI Tag
  IMSI Digits : xxxxxxxxxxxxxxxx
Location Information Tag
VLR Number Tag
  ISDN Address Digits : 550312003001
Cell Id Fixed Length Tag
Tele Service Code Tag
  ISDN Address Digits : 550312003001
Called Party BCD Number Tag
Time And Timezone Tag

1      |      | ITU.WHITE.LAP
2      | 1|0110001 | BIB = 1, BSN = 49
3      | 1|0111111 | FIB = 1, FSN = 63
4      | 00|1111111 | Length Indicator : MSU, LI = 63 octets
5      |      | ITU.WHITE.MTP
6      | 1000|0011 | Service Indicator = SCCP, SSF = National Network
7      | 1101 1010 | DPC : 16346 dec, 3FDA hex
8      | 00|1111111 |
9      | 0000 1111 | OPC : 9276 dec, 243C hex
10     | 1110|1001 | SLS : 14 dec, E hex
11     |      | ITU.WHITE.SCCP
12     | F | 0000 1001 | MT = Unitdata (UDT)
13     | F | 1000 0001 | Protocol Class = class 1
14     | V | 0000 0011 | Pointer to Called Party Address Parameter = 3
15     | V | 0000 1110 | Pointer to Calling Party Address Parameter = 14
16     | V | 0001 1001 | Pointer to Data Parameter = 25
17     | V | 0000 1011 | LI of Called Party Address parameter = 11 octet(s)
18     | V | 0101 0010 | Addr Ind: Route=PC&SSN; GT=TT&NP&ES&NoA; PC=N; SSN=Y
19     | V | 1001 0010 | Subsystem Number = 146 92h
20     | V | 0000 0000 | Translation Type = 0 Translation Type Not Used
21     | V | 0001|0010 | Numbering Plan & Encoding Scheme
22     | V | 0|0000100 | Nature of Address Indicator
23     | V | 0101|0101 | Address Signal
24     | V | 0001|0000 | Address Signal
25     | V | 0000|0110 | Address Signal
26     | V | 0000|0000 | Address Signal
27     | V | 0000|0000 | Address Signal

```

25	V	0011 0101	Address Signal
26	V	0000 1011	LI of Calling Party Address parameter = 11 octet(s)
27	V	0001 0010	Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
28	V	1001 0010	Subsystem Number = 146 92h
29	V	0000 0000	Translation Type = 0 Translation Type Not Used
30	V	0001 0010	Numbering Plan & Encoding Scheme
31	V	0 0000100	Nature of Address Indicator
32	V	0101 0101	Address Signal
33	V	0011 0000	Address Signal
34	V	0010 0001	Address Signal
35	V	0000 0000	Address Signal
36	V	0000 0011	Address Signal
37	V	0001 0000	Address Signal
38	V	1011 0010	LI of Data parameter = 178 octet(s)
			ETSI.CAMEL.CAP
39	M	0110 0010	TCAP Message Type = Begin
40	M	1 0000001	Total TCAP Message length = 175 octet(s)
41	M	1010 1111	Length Of Contents
42	M	0100 1000	Originating Transaction ID tag
43	M	0 0000100	Originating Transaction ID length = 4 octet(s)
44	M	0100 0000	Transaction ID
45	M	0000 0001	Transaction ID
46	M	1001 0100	Transaction ID
47	M	0100 0101	Transaction ID
48	M	0110 1011	Dialogue tag
49	M	0 0011110	Dialogue length = 30 octet(s)
50	M	0010 1000	External tag
51	M	0 0011100	External length = 28 octet(s)
52	M	0000 0110	Object Identifier tag
53	M	0 0000111	Object Identifier length = 7 octet(s)
54	M	0000 0000	Dialogue-as-ID value ccitt
55	M	0001 0001	Dialogue-as-ID value q
56	M	1000 0110	Dialogue-as-ID value 773
57	M	0000 0101	Dialogue-as-ID value
58	M	0000 0001	Dialogue-as-ID value as
59	M	0000 0001	Dialogue-as-ID value DialoguePDU
60	M	0000 0001	Dialogue-as-ID value version1
61	M	1010 0000	Single-ASN.1-type tag
62	M	0 0010001	Single-ASN.1-type length = 17 octet(s)
63	M	0110 0000	Dialogue Request (AARQ-apdu) tag
64	M	0 0001111	Dialogue Request (AARQ-apdu) length = 15 octet(s)
65	O	1000 0000	Protocol Version tag
66	O	0 0000010	Protocol Version length = 2 octet(s)
67	O	0000 0111	Protocol Version
68	O	1000 0000	Protocol Version
69	M	1010 0001	Application Context Name tag
70	M	0 0001001	Application Context Name length = 9 octet(s)
71	M	0000 0110	Object Identifier tag
72	M	0 0000111	Object Identifier length = 7 octet(s)
73	M	0000 0100	Application Context Name ccitt identified organisation
74	M	0000 0000	Application Context Name etsi
75	M	0000 0000	Application Context Name mobile domain
76	M	0000 0001	Application Context Name GSM/UMTS Network
77	M	0000 0000	Application Context Name AC
78	M	0011 0010	Application Context Name cap-gsmssf-to-gsmscf
79	M	0000 0001	Application Context Name version 2
80	M	0110 1100	Component Portion tag
81	M	1 0000001	Component Portion length = 134 octet(s)
82	M	1000 0110	Length Of Contents
83	M	1010 0001	Component Type Tag = Invoke
84	M	1 0000001	Component length = 131 octet(s)
85	M	1000 0011	Length Of Contents
86	M	0000 0010	Invoke ID tag
87	M	0 0000001	Invoke ID length = 1 octet(s)
88	M	0000 0000	Invoke ID
89	M	0000 0010	Local Operation Code tag
90	M	0 0000001	Local Operation Code length = 1 octet(s)
91	F	0000 0000	Operation Code = Initial DP
92	M	0011 0000	SEQUENCE Tag
93	M	0111 1011	Length = 123 octets
94	M	1000 0000	Service Key Tag
95	M	0000 0010	Length = 2 octets
96	M	0001 1111	Service Key = 8100 dec, 1FA4 hex
97	M	1010 0100	Service Key
98	O	1000 0011	Calling Party Number Tag
99	O	0000 1000	Length = 8 octets
100	O	0 0000100	O/E = Even, NAI = International number

101	O	0001 0101	NI=Complete, NP=ISDN(Teleph), PRI=Restricted, SI=User, passed
102	O	xxxx xxxx	Address Signal = xxxxxxxxxxxxxx
103	O	xxxx xxxx	Address Signal
104	O	xxxx xxxx	Address Signal
105	O	xxxx xxxx	Address Signal
106	O	xxxx xxxx	Address Signal
107	O	xxxx xxxx	Address Signal
108	O	1000 0101	Calling Partys Category Tag
109	O	0000 0001	Length = 1 octet
110	O	0000 1010	Calling Partys Category = Ordinary calling subscriber
111	O	1000 1010	Location Number Tag
112	O	0000 1000	Length = 8 octets
113	O	0 0000100	O/E = Even, NAI = International number
114	O	1001 0111	INN=Not allowed, NP=ISDN(Teleph), PRI=Restricted, SI=Network provid
115	O	0101 0101	Address Signal = 550312003001
116	O	0011 0000	Address Signal
117	O	0010 0001	Address Signal
118	O	0000 0000	Address Signal
119	O	0000 0011	Address Signal
120	O	0001 0000	Address Signal
121	O	1001 0111	High Layer Compatability Tag
122	O	0000 0010	Length = 2 octets
123	O	100 10001	CS = ITU-T,Interpre.= First Id, PM= HLPP
124	O	1 0000001	High Layer Chara.Id=Telephony
125	O	1011 1011	Bearer Capability Tag
126	O	0000 0101	Length = 5 octets
127	O	1000 0000	Bearer Cap Tag
128	O	0000 0011	Length = 3 octets
129	O	100 00000	Bearer Cap
130	O	100 10000	Bearer Cap
131	O	101 00011	Layer ident., User info. layer 1
132	O	1001 1100	Event Type BCSM Tag
133	O	0000 0001	Length = 1 octet
134	O	0000 0010	Event Type BCSM = Collected info
135	O	1001 1111	IMSI Tag
136	O	0011 0010	IMSI Tag
137	O	0000 1000	Length = 8 octets
138	O	0010 0111	MCC2, MCC1 (MCC = 724)
139	O	0001 0100	MNC1, MCC3 (MNC = 16)
140	O	0000 0110	MSIN1, MNC2
141	O	xxxx xxxx	MSIN = xxxxxxxxxxxx
142	O	xxxx xxxx	MSIN
143	O	xxxx xxxx	MSIN
144	O	xxxx xxxx	MSIN
145	O	xxxx xxxx	MSIN
146	O	1011 1111	Location Info Tag
147	O	0011 0100	Location Info Tag
148	O	0001 0111	Length = 23 octets
149	O	0000 0010	Age Of Location Info Tag
150	O	0000 0001	Length = 1 octet
151	O	0000 0000	Age Of Location Info = 0 dec, 00 hex
152	O	1000 0001	Vlr Number Tag
153	O	0000 0111	Length = 7 octets
154	O	1001 0001	NAI = International number, NPI = ISDN/Telephony
155	O	0101 0101	Address Signal = 550312003001
156	O	0011 0000	Address Signal
157	O	0010 0001	Address Signal
158	O	0000 0000	Address Signal
159	O	0000 0011	Address Signal
160	O	0001 0000	Address Signal
161	O	1010 0011	Cell Global Id or SAI or LAI Tag
162	O	0000 1001	Length = 9 octets
163	O	1000 0000	Cell Global Id or SAI Fixed Len Tag
164	O	0000 0111	Length = 7 octets
165	O	0010 0111	MCC2, MCC1 (MCC = 724 hex)
166	O	1111 0100	filler, MCC3
167	O	0110 0001	MNC2, MNC1 (MNC =16 hex)
168	O	0001 0111	LAC = 17EA hex
169	O	1110 1010	LAC
170	O	0000 1101	CI/SAC = 0D90 hex
171	O	1001 0000	CI/SAC
172	O	1011 1111	Ext_basic Service Code Tag
173	O	0011 0101	Ext_basic Service Code Tag
174	O	0000 0011	Length = 3 octets
175	M	1000 0011	Ext Tele Service Tag
176	M	0000 0001	Length = 1 octet

```

177 M | 0001 0001 | Tele Service Code = Telephony
178 O | 1001 1111 | Call Reference Number Tag
179 O | 0011 0110 | Call Reference Number Tag
180 O | 0000 0111 | Length = 7 octets
181 O | 0100 0000 | Call Reference Number = 401D4133089C86 hex
182 O | 0001 1101 | Call Reference Number
183 O | 0100 0001 | Call Reference Number
184 O | 0011 0011 | Call Reference Number
185 O | 0000 1000 | Call Reference Number
186 O | 1001 1100 | Call Reference Number
187 O | 1000 0110 | Call Reference Number
188 O | 1001 1111 | Msc Address Tag
189 O | 0011 0111 | Msc Address Tag
190 O | 0000 0111 | Length = 7 octets
191 O | 1001|0001 | NAI = International number, NPI = ISDN/Telephony
192 O | 0101|0101 | Address Signal = 550312003001
193 O | 0011|0000 | Address Signal
194 O | 0010|0001 | Address Signal
195 O | 0000|0000 | Address Signal
196 O | 0000|0011 | Address Signal
197 O | 0001|0000 | Address Signal
198 O | 1001 1111 | Called Party BCD Number Tag
199 O | 0011 1000 | Called Party BCD Number Tag
200 O | 0000 0101 | Length = 5 octets
201 O | 1000|0001 | NumType=Unknown, NumPlan=ISDN/Telephony
202 O | xxxx|xxxx | Address Signal = xxxxxxxx
203 O | xxxx|xxxx | Address Signal
204 O | xxxx|xxxx | Address Signal
205 O | xxxx|xxxx | Address Signal
206 O | 1001 1111 | Time and Time Zone Tag
207 O | 0011 1001 | Time and Time Zone Tag
208 O | 0000 1000 | Length = 8 octets
209 O | 0000 0010 | Year = 2010
210 O | 0000 0001 | Year
211 O | 0011 0000 | Month= 03
212 O | 1001 0000 | Day = 09
213 O | 0010 0001 | Hour = 12
214 O | 1000 0101 | Min = 58
215 O | 0100 0000 | Sec = 04
216 O | 0010 1001 | Time Zone = -12

```

```

12:58:04.889 PM SAT Link: <-CTASG-CTAPPE14_0
SI: SCCP SSF: NN DPC: PR-CTAHUAL OPC: PR-CTAPPES14 SLS: 8
MT: UDT
Called Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550312003001h
Calling Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550160000053h
MT: Continue
Originating Transaction ID Tag
  Transaction Id: 017b0368h
Destination Transaction ID Tag
  Transaction Id: 40019445h
Invoke
Invoke Id Tag
  Invoke Id: 1
Operation Code Tag: Local Operation Code
Operation ID: Request Report BCSM Event
BCSM Events Tag
Invoke
Invoke Id Tag
  Invoke Id: 2
Operation Code Tag: Local Operation Code
Operation ID: Apply Charging
ACh Bill Charging Chars Tag
Party to Charge Tag
Invoke
Invoke Id Tag
  Invoke Id: 3
Operation Code Tag: Local Operation Code

```

Operation ID: Connect  
Destination Routing Address Tag  
Destination Routing Address Tag  
Calling Partys Category Tag

					ITU.WHITE.LAP
1			1 0100010		BIB = 1, BSN = 34
2			1 0010100		FIB = 1, FSN = 20
3			00 1111111		Length Indicator : MSU, LI = 63 octets
					ITU.WHITE.MTP
4			1000 0011		Service Indicator = SCCP, SSF = National Network
5			0011 1100		DPC : 9276 dec, 243C hex
6			10 100100		
7			1111 0110		OPC : 16346 dec, 3FDA hex
8			1000 1111		SLS : 8 dec, 8 hex
					ITU.WHITE.SCCP
9	F		0000 1001		MT = Unitdata (UDT)
10	F		0000 0001		Protocol Class = class 1
11	V		0000 0011		Pointer to Called Party Address Parameter = 3
12	V		0000 1110		Pointer to Calling Party Address Parameter = 14
13	V		0001 1001		Pointer to Data Parameter = 25
14	V		0000 1011		LI of Called Party Address parameter = 11 octet(s)
15	V		0001 0010		Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
16	V		1001 0010		Subsystem Number = 146 92h
17	V		0000 0000		Translation Type = 0 Translation Type Not Used
18	V		0001 0010		Numbering Plan & Encoding Scheme
19	V		0 0000100		Nature of Address Indicator
20	V		0101 0101		Address Signal
21	V		0011 0000		Address Signal
22	V		0010 0001		Address Signal
23	V		0000 0000		Address Signal
24	V		0000 0011		Address Signal
25	V		0001 0000		Address Signal
26	V		0000 1011		LI of Calling Party Address parameter = 11 octet(s)
27	V		0001 0010		Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
28	V		1001 0010		Subsystem Number = 146 92h
29	V		0000 0000		Translation Type = 0 Translation Type Not Used
30	V		0001 0010		Numbering Plan & Encoding Scheme
31	V		0 0000100		Nature of Address Indicator
32	V		0101 0101		Address Signal
33	V		0001 0000		Address Signal
34	V		0000 0110		Address Signal
35	V		0000 0000		Address Signal
36	V		0000 0000		Address Signal
37	V		0011 0101		Address Signal
38	V		1001 0001		LI of Data parameter = 145 octet(s)
					ETSI.CAMEL.CAP
39	M		0110 0101		TCAP Message Type = Continue
40	M		1 0000001		Total TCAP Message length = 142 octet(s)
41	M		1000 1110		Length Of Contents
42	M		0100 1000		Originating Transaction ID tag
43	M		0 0000100		Originating Transaction ID length = 4 octet(s)
44	M		0000 0001		Transaction ID
45	M		0111 1011		Transaction ID
46	M		0000 0011		Transaction ID
47	M		0110 1000		Transaction ID
48	M		0100 1001		Destination Transaction ID tag
49	M		0 0000100		Destination Transaction ID length = 4 octet(s)
50	M		0100 0000		Transaction ID
51	M		0000 0001		Transaction ID
52	M		1001 0100		Transaction ID
53	M		0100 0101		Transaction ID
54	M		0110 1011		Dialogue tag
55	M		0 0101010		Dialogue length = 42 octet(s)
56	M		0010 1000		External tag
57	M		0 0101000		External length = 40 octet(s)
58	M		0000 0110		Object Identifier tag
59	M		0 0000111		Object Identifier length = 7 octet(s)
60	M		0000 0000		Dialogue-as-ID value ccitt
61	M		0001 0001		Dialogue-as-ID value q
62	M		1000 0110		Dialogue-as-ID value 773
63	M		0000 0101		Dialogue-as-ID value
64	M		0000 0001		Dialogue-as-ID value as
65	M		0000 0001		Dialogue-as-ID value DialoguePDU
66	M		0000 0001		Dialogue-as-ID value version1
67	M		1010 0000		Single-ASN.1-type tag

68	M	0 0011101	Single-ASN.1-type length = 29 octet(s)
69	M	0110 0001	Dialogue Response (AARE-apdu) tag
70	M	0 0011011	Dialogue Response (AARE-apdu) length = 27 octet(s)
71	O	1000 0000	Protocol Version tag
72	O	0 0000010	Protocol Version length = 2 octet(s)
73	O	0000 0111	Protocol Version
74	O	1000 0000	Protocol Version
75	M	1010 0001	Application Context Name tag
76	M	0 0001001	Application Context Name length = 9 octet(s)
77	M	0000 0110	Object Identifier tag
78	M	0 0000111	Object Identifier length = 7 octet(s)
79	M	0000 0100	Application Context Name ccitt identified organisation
80	M	0000 0000	Application Context Name etsi
81	M	0000 0000	Application Context Name mobile domain
82	M	0000 0001	Application Context Name GSM/UMTS Network
83	M	0000 0000	Application Context Name AC
84	M	0011 0010	Application Context Name cap-gsmssf-to-gsmscf
85	M	0000 0001	Application Context Name version 2
86	M	1010 0010	Result tag
87	M	0 0000011	Result length = 3 octet(s)
88	M	0000 0010	Integer tag
89	M	0 0000001	Integer length = 1 octet(s)
90	M	0000 0000	Result = Accepted
91	M	1010 0011	Result Source Diagnostic tag
92	M	0 0000101	Result Source Diagnostic length = 5 octet(s)
93	M	1010 0001	Dialogue Service User tag
94	M	0 0000011	Dialogue Service User length = 3 octet(s)
95	O	0000 0010	Integer tag
96	O	0 0000001	Integer length = 1 octet(s)
97	O	0000 0000	Dialogue Service User = Null
98	M	0110 1100	Component Portion tag
99	M	0 1010100	Component Portion length = 84 octet(s)
100	M	1010 0001	Component Type Tag = Invoke
101	M	0 0100100	Component length = 36 octet(s)
102	M	0000 0010	Invoke ID tag
103	M	0 0000001	Invoke ID length = 1 octet(s)
104	M	0000 0001	Invoke ID
105	M	0000 0010	Local Operation Code tag
106	M	0 0000001	Local Operation Code length = 1 octet(s)
107	F	0001 0111	Operation Code = Request Report BCSM Event
108	M	0011 0000	SEQUENCE Tag
109	M	0001 1100	Length = 28 octets
110	M	1010 0000	BCSM Events Tag
111	M	0001 1010	Length = 26 octets
112	M	0011 0000	BCSM Event Tag
113	M	0000 1011	Length = 11 octets
114	M	1000 0000	Event Type BCSM Tag
115	M	0000 0001	Length = 1 octet
116	M	0000 1001	Event Type BCSM = 0 disconnect
117	M	1000 0001	Monitor Mode Tag
118	M	0000 0001	Length = 1 octet
119	M	0000 0000	Monitor Mode = Interrupted
120	O	1010 0010	Leg ID Tag
121	O	0000 0011	Length = 3 octets
122	O	1000 0000	Sending Side ID Tag
123	O	0000 0001	Length = 1 octet
124	O	0000 0001	ID = Leg 1
125	O	0011 0000	BCSM Event Tag
126	O	0000 1011	Length = 11 octets
127	M	1000 0000	Event Type BCSM Tag
128	M	0000 0001	Length = 1 octet
129	M	0000 1001	Event Type BCSM = 0 disconnect
130	M	1000 0001	Monitor Mode Tag
131	M	0000 0001	Length = 1 octet
132	M	0000 0000	Monitor Mode = Interrupted
133	O	1010 0010	Leg ID Tag
134	O	0000 0011	Length = 3 octets
135	O	1000 0000	Sending Side ID Tag
136	O	0000 0001	Length = 1 octet
137	O	0000 0010	ID = Leg 2
138	M	1010 0001	Component Type Tag = Invoke
139	M	0 0010101	Component length = 21 octet(s)
140	M	0000 0010	Invoke ID tag
141	M	0 0000001	Invoke ID length = 1 octet(s)
142	M	0000 0010	Invoke ID
143	M	0000 0010	Local Operation Code tag
144	M	0 0000001	Local Operation Code length = 1 octet(s)

```

145 F | 0010 0011 | Operation Code = Apply Charging
146 M | 0011 0000 | SEQUENCE Tag
147 M | 0000 1101 | Length = 13 octets
148 M | 1000 0000 | Ach Billing Charging Charac Tag
149 M | 0000 0110 | Length = 6 octets
150 M | 1010 0000 | Time Duration Charging Tag
151 M | 0000 0100 | Length = 4 octets
152 M | 1000 0000 | Max Call Period Duration Tag
153 M | 0000 0010 | Length = 2 octets
154 M | 0000 1011 | Max Call Period Duration = 3000 dec, 0BB8 hex
155 M | 1011 1000 | Max Call Period Duration
156 O | 1010 0010 | Party To Charge Tag
157 O | 0000 0011 | Length = 3 octets
158 O | 1000 0000 | Sending Side ID Tag
159 O | 0000 0001 | Length = 1 octet
160 O | 0000 0001 | Leg Type = Leg1
161 M | 1010 0001 | Component Type Tag = Invoke
162 M | 0|0010101 | Component length = 21 octet(s)
163 M | 0000 0010 | Invoke ID tag
164 M | 0|0000001 | Invoke ID length = 1 octet(s)
165 M | 0000 0011 | Invoke ID
166 M | 0000 0010 | Local Operation Code tag
167 M | 0|0000001 | Local Operation Code length = 1 octet(s)
168 F | 0001 0100 | Operation Code = Connect
169 M | 0011 0000 | SEQUENCE Tag
170 M | 0000 1101 | Length = 13 octets
171 M | 1010 0000 | Destination Routing Address Tag
172 M | 0000 1000 | Length = 8 octets
173 M | 0000 0100 | Destination Routing Address Tag
174 M | 0000 0110 | Length = 6 octets
175 M | 0|0000010 | O/E = Even, NAI = Unknown
176 M | 0|0000000 | INN=Allowed, NP=Spare
177 M | xxxx|xxxx | Address Signal = xxxxxxxx
178 M | xxxx|xxxx | Address Signal
179 M | xxxx|xxxx | Address Signal
180 M | xxxx|xxxx | Address Signal
181 O | 1001 1100 | Calling Partys Category Tag
182 O | 0000 0001 | Length = 1 octet
183 O | 1110 0000 | Calling Partys Category = Reserved for national use

```

```

01:00:05.702 PM SAT Link: ->CTASG-CTAPPE14_6
SI: SCCP SSF: NN DPC: PR-CTAPPES14 OPC: PR-CTAHUAL SLS: 14
MT: UDT
Called Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550160000053h
Calling Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550312003001h
MT: Continue
Originating Transaction ID Tag
  Transaction Id: 40019445h
Destination Transaction ID Tag
  Transaction Id: 017b0368h
Invoke
Invoke Id Tag
  Invoke Id: 1
Operation Code Tag: Local Operation Code
Operation ID: Apply Charging Report
Call Result Tag

```

```

| | ITU.WHITE.LAP
1 | 1|1010011 | BIB = 1, BSN = 83
2 | 1|1100001 | FIB = 1, FSN = 97
3 | 00|111111 | Length Indicator : MSU, LI = 63 octets
| | ITU.WHITE.MTP
4 | 1000|0011 | Service Indicator = SCCP, SSF = National Network
5 | 1101 1010 | DPC : 16346 dec, 3FDA hex
6 | 00|111111 |
7 | 0000 1111 | OPC : 9276 dec, 243C hex
8 | 1110|1001 | SLS : 14 dec, E hex

```

9	F	0000 1001	ITU.WHITE.SCCP
10	F	1000 0001	MT = Unitdata (UDT)
11	V	0000 0011	Protocol Class = class 1
12	V	0000 1110	Pointer to Called Party Address Parameter = 3
13	V	0001 1001	Pointer to Calling Party Address Parameter = 14
14	V	0000 1011	Pointer to Data Parameter = 25
15	V	0101 0010	LI of Called Party Address parameter = 11 octet(s)
16	V	1001 0010	Addr Ind: Route=PC&SSN; GT=TT&NP&ES&NoA; PC=N; SSN=Y
17	V	0000 0000	Subsystem Number = 146 92h
18	V	0001 0010	Translation Type = 0 Translation Type Not Used
19	V	0 0000100	Numbering Plan & Encoding Scheme
20	V	0101 0101	Nature of Address Indicator
21	V	0001 0000	Address Signal
22	V	0000 0110	Address Signal
23	V	0000 0000	Address Signal
24	V	0000 0000	Address Signal
25	V	0011 0101	Address Signal
26	V	0000 1011	LI of Calling Party Address parameter = 11 octet(s)
27	V	0001 0010	Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
28	V	1001 0010	Subsystem Number = 146 92h
29	V	0000 0000	Translation Type = 0 Translation Type Not Used
30	V	0001 0010	Numbering Plan & Encoding Scheme
31	V	0 0000100	Nature of Address Indicator
32	V	0101 0101	Address Signal
33	V	0011 0000	Address Signal
34	V	0010 0001	Address Signal
35	V	0000 0000	Address Signal
36	V	0000 0011	Address Signal
37	V	0001 0000	Address Signal
38	V	0010 1010	LI of Data parameter = 42 octet(s)
39	M	0110 0101	ETSI.CAMEL.CAP
40	M	0 0101000	TCAP Message Type = Continue
41	M	0100 1000	Total TCAP Message length = 40 octet(s)
42	M	0 0000100	Originating Transaction ID tag
43	M	0100 0000	Originating Transaction ID length = 4 octet(s)
44	M	0000 0001	Transaction ID
45	M	1001 0100	Transaction ID
46	M	0100 0101	Transaction ID
47	M	0100 1001	Transaction ID
48	M	0 0000100	Destination Transaction ID tag
49	M	0000 0001	Destination Transaction ID length = 4 octet(s)
50	M	0000 0001	Transaction ID
51	M	0111 1011	Transaction ID
52	M	0000 0011	Transaction ID
53	M	0110 1000	Transaction ID
54	M	0110 1100	Component Portion tag
55	M	0 0011010	Component Portion length = 26 octet(s)
56	M	1010 0001	Component Type Tag = Invoke
57	M	0 0011000	Component length = 24 octet(s)
58	M	0000 0010	Invoke ID tag
59	M	0 0000001	Invoke ID length = 1 octet(s)
60	M	0000 0001	Invoke ID
61	M	0000 0010	Local Operation Code tag
62	M	0 0000001	Local Operation Code length = 1 octet(s)
63	F	0010 0100	Operation Code = Apply Charging Report
64	M	0000 0100	Call Result Tag
65	M	0001 0000	Length = 16 octets
66	M	1010 0000	Time Duration Charging Result Tag
67	M	0000 1110	Length = 14 octets
68	M	1010 0000	Party To Charge Tag
69	M	0000 0011	Length = 3 octets
70	M	1000 0001	Receiving Side ID Tag
71	M	0000 0001	Length = 1 octet
72	M	0000 0001	Leg Type = Leg1
73	M	1010 0001	Time Information Tag
74	M	0000 0100	Length = 4 octets
75	M	1000 0000	Time If No Tariff Switch Tag
76	M	0000 0010	Length = 2 octets
77	M	0000 0100	Time If No Tariff Switch = 1139 dec, 0473 hex
78	M	0111 0011	Time If No Tariff Switch
79	O	1000 0010	Call Active Tag
80	O	0000 0001	Length = 1 octet
81	O	0000 0000	Call Active = FALSE

01:00:05.713 PM SAT Link: ->CTASG-CTAPPE14\_6

SI: SCCP SSF: NN DPC: PR-CTAPPES14 OPC: PR-CTAHUA1 SLS: 14  
MT: UDT  
Called Party Address Length: 11 octets  
Subsystem Number: 146  
Translation Type: Translation Type Not Used  
Nature of Address Indicator: International number  
Address Information: 550160000053h  
Calling Party Address Length: 11 octets  
Subsystem Number: 146  
Translation Type: Translation Type Not Used  
Nature of Address Indicator: International number  
Address Information: 550312003001h  
MT: Continue  
Originating Transaction ID Tag  
Transaction Id: 40019445h  
Destination Transaction ID Tag  
Transaction Id: 017b0368h  
Invoke  
Invoke Id Tag  
Invoke Id: 2  
Operation Code Tag: Local Operation Code  
Operation ID: Event Report BCSM  
Event Type BCSM Tag  
Event Specific BCSM Info Tag  
Leg ID Tag

			ITU.WHITE.LAP
1		1 1010011	BIB = 1, BSN = 83
2		1 1100010	FIB = 1, FSN = 98
3		00 1111111	Length Indicator : MSU, LI = 63 octets
			ITU.WHITE.MTP
4		1000 0011	Service Indicator = SCCP, SSF = National Network
5		1101 1010	DPC : 16346 dec, 3FDA hex
6		00 1111111	
7		0000 1111	OPC : 9276 dec, 243C hex
8		1110 1001	SLS : 14 dec, E hex
			ITU.WHITE.SCCP
9	F	0000 1001	MT = Unitdata (UDT)
10	F	1000 0001	Protocol Class = class 1
11	V	0000 0011	Pointer to Called Party Address Parameter = 3
12	V	0000 1110	Pointer to Calling Party Address Parameter = 14
13	V	0001 1001	Pointer to Data Parameter = 25
14	V	0000 1011	LI of Called Party Address parameter = 11 octet(s)
15	V	0101 0010	Addr Ind: Route=PC&SSN; GT=TT&NP&ES&NoA; PC=N; SSN=Y
16	V	1001 0010	Subsystem Number = 146 92h
17	V	0000 0000	Translation Type = 0 Translation Type Not Used
18	V	0001 0010	Numbering Plan & Encoding Scheme
19	V	0 0000100	Nature of Address Indicator
20	V	0101 0101	Address Signal
21	V	0001 0000	Address Signal
22	V	0000 0110	Address Signal
23	V	0000 0000	Address Signal
24	V	0000 0000	Address Signal
25	V	0011 0101	Address Signal
26	V	0000 1011	LI of Calling Party Address parameter = 11 octet(s)
27	V	0001 0010	Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
28	V	1001 0010	Subsystem Number = 146 92h
29	V	0000 0000	Translation Type = 0 Translation Type Not Used
30	V	0001 0010	Numbering Plan & Encoding Scheme
31	V	0 0000100	Nature of Address Indicator
32	V	0101 0101	Address Signal
33	V	0011 0000	Address Signal
34	V	0010 0001	Address Signal
35	V	0000 0000	Address Signal
36	V	0000 0011	Address Signal
37	V	0001 0000	Address Signal
38	V	0010 1010	LI of Data parameter = 42 octet(s)
			ETSI.CAMEL.CAP
39	M	0110 0101	TCAP Message Type = Continue
40	M	0 0101000	Total TCAP Message length = 40 octet(s)
41	M	0100 1000	Originating Transaction ID tag
42	M	0 0000100	Originating Transaction ID length = 4 octet(s)
43	M	0100 0000	Transaction ID
44	M	0000 0001	Transaction ID
45	M	1001 0100	Transaction ID
46	M	0100 0101	Transaction ID

```

47 M | 0100 1001 | Destination Transaction ID tag
48 M | 0|0000100 | Destination Transaction ID length = 4 octet(s)
49 M | 0000 0001 | Transaction ID
50 M | 0111 1011 | Transaction ID
51 M | 0000 0011 | Transaction ID
52 M | 0110 1000 | Transaction ID
53 M | 0110 1100 | Component Portion tag
54 M | 0|0011010 | Component Portion length = 26 octet(s)
55 M | 1010 0001 | Component Type Tag = Invoke
56 M | 0|0011000 | Component length = 24 octet(s)
57 M | 0000 0010 | Invoke ID tag
58 M | 0|0000001 | Invoke ID length = 1 octet(s)
59 M | 0000 0010 | Invoke ID
60 M | 0000 0010 | Local Operation Code tag
61 M | 0|0000001 | Local Operation Code length = 1 octet(s)
62 F | 0001 1000 | Operation Code = Event Report BCSM
63 M | 0011 0000 | SEQUENCE Tag
64 M | 0001 0000 | Length = 16 octets
65 M | 1000 0000 | Event Type BCSM Tag
66 M | 0000 0001 | Length = 1 octet
67 M | 0000 1001 | Event Type BCSM = 0 disconnect
68 O | 1010 0010 | Event Specific Info BCSM Tag
69 O | 0000 0110 | Length = 6 octets
70 O | 1010 0111 | O Disconnect Specific Info Tag
71 O | 0000 0100 | Length = 4 octets
72 O | 1000 0000 | Release Cause Tag
73 O | 0000 0010 | Length = 2 octets
74 O | 1000|0000 | CS = ITU-T, Location = User(U)
75 O | 1|0010000 | Value = Normal call clearing
76 O | 1010 0011 | Leg ID Tag
77 O | 0000 0011 | Length = 3 octets
78 O | 1000 0001 | Receiving Side ID Tag
79 O | 0000 0001 | Length = 1 octet
80 O | 0000 0001 | Leg Type = Leg1

```

01:00:07.814 PM SAT Link: <-CTASG-CTAPPE14\_0  
SI: SCCP SSF: NN DPC: PR-CTAHUAL OPC: PR-CTAPPES14 SLS: 8  
MT: UDT

Called Party Address Length: 11 octets  
Subsystem Number: 146  
Translation Type: Translation Type Not Used  
Nature of Address Indicator: International number  
Address Information: 550312003001h  
Calling Party Address Length: 11 octets  
Subsystem Number: 146  
Translation Type: Translation Type Not Used  
Nature of Address Indicator: International number  
Address Information: 550160000053h

MT: Continue  
Originating Transaction ID Tag  
Transaction Id: 017b0368h  
Destination Transaction ID Tag  
Transaction Id: 40019445h  
Invoke  
Invoke Id Tag  
Invoke Id: 4  
Operation Code Tag: Local Operation Code  
Operation ID: Release Call  
Cause Tag

```

| | ITU.WHITE.LAP
1 | 1|1110101 | BIB = 1, BSN = 117
2 | 1|1111111 | FIB = 1, FSN = 127
3 | 00|1111111 | Length Indicator : MSU, LI = 63 octets
| | ITU.WHITE.MTP
4 | 1000|0011 | Service Indicator = SCCP, SSF = National Network
5 | 0011 1100 | DPC : 9276 dec, 243C hex
6 | 10|100100 |
7 | 1111 0110 | OPC : 16346 dec, 3FDA hex
8 | 1000|1111 | SLS : 8 dec, 8 hex
| | ITU.WHITE.SCCP
9 F | 0000 1001 | MT = Unitdata (UDT)
10 F | 0000 0001 | Protocol Class = class 1
11 V | 0000 0011 | Pointer to Called Party Address Parameter = 3
12 V | 0000 1110 | Pointer to Calling Party Address Parameter = 14

```

13	V		0001 1001		Pointer to Data Parameter = 25
14	V		0000 1011		LI of Called Party Address parameter = 11 octet(s)
15	V		0001 0010		Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
16	V		1001 0010		Subsystem Number = 146 92h
17	V		0000 0000		Translation Type = 0 Translation Type Not Used
18	V		0001 0010		Numbering Plan & Encoding Scheme
19	V		0 0000100		Nature of Address Indicator
20	V		0101 0101		Address Signal
21	V		0011 0000		Address Signal
22	V		0010 0001		Address Signal
23	V		0000 0000		Address Signal
24	V		0000 0011		Address Signal
25	V		0001 0000		Address Signal
26	V		0000 1011		LI of Calling Party Address parameter = 11 octet(s)
27	V		0001 0010		Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
28	V		1001 0010		Subsystem Number = 146 92h
29	V		0000 0000		Translation Type = 0 Translation Type Not Used
30	V		0001 0010		Numbering Plan & Encoding Scheme
31	V		0 0000100		Nature of Address Indicator
32	V		0101 0101		Address Signal
33	V		0001 0000		Address Signal
34	V		0000 0110		Address Signal
35	V		0000 0000		Address Signal
36	V		0000 0000		Address Signal
37	V		0011 0101		Address Signal
38	V		0001 1100		LI of Data parameter = 28 octet(s)
					ETSI.CAMEL.CAP
39	M		0110 0101		TCAP Message Type = Continue
40	M		0 0011010		Total TCAP Message length = 26 octet(s)
41	M		0100 1000		Originating Transaction ID tag
42	M		0 0000100		Originating Transaction ID length = 4 octet(s)
43	M		0000 0001		Transaction ID
44	M		0111 1011		Transaction ID
45	M		0000 0011		Transaction ID
46	M		0110 1000		Transaction ID
47	M		0100 1001		Destination Transaction ID tag
48	M		0 0000100		Destination Transaction ID length = 4 octet(s)
49	M		0100 0000		Transaction ID
50	M		0000 0001		Transaction ID
51	M		1001 0100		Transaction ID
52	M		0100 0101		Transaction ID
53	M		0110 1100		Component Portion tag
54	M		0 0001100		Component Portion length = 12 octet(s)
55	M		1010 0001		Component Type Tag = Invoke
56	M		0 0001010		Component length = 10 octet(s)
57	M		0000 0010		Invoke ID tag
58	M		0 0000001		Invoke ID length = 1 octet(s)
59	M		0000 0100		Invoke ID
60	M		0000 0010		Local Operation Code tag
61	M		0 0000001		Local Operation Code length = 1 octet(s)
62	F		0001 0110		Operation Code = Release Call
63	M		0000 0100		Cause Tag
64	M		0000 0010		Length = 2 octets
65	M		1000 0001		CS = ITU-T, Location = Prv net serv loc usr (LPN)
66	M		1 0010000		Value = Normal call clearing

## A.5. CHAMADA TERMINADA EM PRÉPAGO – CAMEL T-CSI

CT (1) - Protocol Level Display (6)

```

12:52:42.764 PM SAT Link: ->BSASG-CTAPPE13_0
SI: SCCP SSF: NN DPC: PR-CTAPPE13 OPC: PR-CTAHUA1 SLS: 8
MT: UDT
Called Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550160000052h
Calling Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550312003001h
MT: Begin
Originating Transaction ID Tag
  Transaction Id: 95479231h
Invoke
Invoke Id Tag
  Invoke Id: 0
Operation Code Tag: Local Operation Code
Operation ID: Initial DP
Service Key Tag
  Length: 2 octets
  Service Key : 1000 dec, 3e8 hex
Called Party Number Tag
Calling Party Number Tag
Calling Partys Category Tag
High Layer Compatibility Tag
Bearer Capability Tag
Event Type BCSM Tag
IMSI Tag
  IMSI Digits : xxxxxxxxxxxxxxxx
Subscriber State Tag
Location Information Tag
VLR Number Tag
  ISDN Address Digits : 550312003001
Cell Id Fixed Length Tag
Tele Service Code Tag
  ISDN Address Digits : 550312003001
Time And Timezone Tag

```

```

          |          | ITU.WHITE.LAP
1         | 0|0011011 | BIB = 0, BSN = 27
2         | 1|0010101 | FIB = 1, FSN = 21
3         | 00|1111111 | Length Indicator : MSU, LI = 63 octets
          |          | ITU.WHITE.MTP
4         | 1000|0011 | Service Indicator = SCCP, SSF = National Network
5         | 1101 1001 | DPC : 16345 dec, 3FD9 hex
6         | 00|1111111 |
7         | 0000 1111 | OPC : 9276 dec, 243C hex
8         | 1000|1001 | SLS : 8 dec, 8 hex
          |          | ITU.WHITE.SCCP
9         F | 0000 1001 | MT = Unitdata (UDT)
10        F | 1000 0001 | Protocol Class = class 1
11        V | 0000 0011 | Pointer to Called Party Address Parameter = 3
12        V | 0000 1110 | Pointer to Calling Party Address Parameter = 14
13        V | 0001 1001 | Pointer to Data Parameter = 25
14        V | 0000 1011 | LI of Called Party Address parameter = 11 octet(s)
15        V | 0101 0010 | Addr Ind: Route=PC&SSN; GT=TT&NP&ES&NoA; PC=N; SSN=Y
16        V | 1001 0010 | Subsystem Number = 146 92h
17        V | 0000 0000 | Translation Type = 0 Translation Type Not Used
18        V | 0001|0010 | Numbering Plan & Encoding Scheme
19        V | 0|0000100 | Nature of Address Indicator
20        V | 0101|0101 | Address Signal
21        V | 0001|0000 | Address Signal
22        V | 0000|0110 | Address Signal
23        V | 0000|0000 | Address Signal
24        V | 0000|0000 | Address Signal
25        V | 0010|0101 | Address Signal
26        V | 0000 1011 | LI of Calling Party Address parameter = 11 octet(s)

```

27	V	0001 0010	Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
28	V	1001 0010	Subsystem Number = 146 92h
29	V	0000 0000	Translation Type = 0 Translation Type Not Used
30	V	0001 0010	Numbering Plan & Encoding Scheme
31	V	0 0000100	Nature of Address Indicator
32	V	0101 0101	Address Signal
33	V	0011 0000	Address Signal
34	V	0010 0001	Address Signal
35	V	0000 0000	Address Signal
36	V	0000 0011	Address Signal
37	V	0001 0000	Address Signal
38	V	1011 0000	LI of Data parameter = 176 octet(s)
			ETSI.CAMEL.CAP
39	M	0110 0010	TCAP Message Type = Begin
40	M	1 0000001	Total TCAP Message length = 173 octet(s)
41	M	1010 1101	Length Of Contents
42	M	0100 1000	Originating Transaction ID tag
43	M	0 0000100	Originating Transaction ID length = 4 octet(s)
44	M	1001 0101	Transaction ID
45	M	0100 0111	Transaction ID
46	M	1001 0010	Transaction ID
47	M	0011 0001	Transaction ID
48	M	0110 1011	Dialogue tag
49	M	0 0011110	Dialogue length = 30 octet(s)
50	M	0010 1000	External tag
51	M	0 0011100	External length = 28 octet(s)
52	M	0000 0110	Object Identifier tag
53	M	0 0000111	Object Identifier length = 7 octet(s)
54	M	0000 0000	Dialogue-as-ID value ccitt
55	M	0001 0001	Dialogue-as-ID value q
56	M	1000 0110	Dialogue-as-ID value 773
57	M	0000 0101	Dialogue-as-ID value
58	M	0000 0001	Dialogue-as-ID value as
59	M	0000 0001	Dialogue-as-ID value DialoguePDU
60	M	0000 0001	Dialogue-as-ID value version1
61	M	1010 0000	Single-ASN.1-type tag
62	M	0 0010001	Single-ASN.1-type length = 17 octet(s)
63	M	0110 0000	Dialogue Request (AARQ-apdu) tag
64	M	0 0001111	Dialogue Request (AARQ-apdu) length = 15 octet(s)
65	O	1000 0000	Protocol Version tag
66	O	0 0000010	Protocol Version length = 2 octet(s)
67	O	0000 0111	Protocol Version
68	O	1000 0000	Protocol Version
69	M	1010 0001	Application Context Name tag
70	M	0 0001001	Application Context Name length = 9 octet(s)
71	M	0000 0110	Object Identifier tag
72	M	0 0000111	Object Identifier length = 7 octet(s)
73	M	0000 0100	Application Context Name ccitt identified organisation
74	M	0000 0000	Application Context Name etsi
75	M	0000 0000	Application Context Name mobile domain
76	M	0000 0001	Application Context Name GSM/UMTS Network
77	M	0000 0000	Application Context Name AC
78	M	0011 0010	Application Context Name cap-gsmssf-to-gsmscf
79	M	0000 0001	Application Context Name version 2
80	M	0110 1100	Component Portion tag
81	M	1 0000001	Component Portion length = 132 octet(s)
82	M	1000 0100	Length Of Contents
83	M	1010 0001	Component Type Tag = Invoke
84	M	1 0000001	Component length = 129 octet(s)
85	M	1000 0001	Length Of Contents
86	M	0000 0010	Invoke ID tag
87	M	0 0000001	Invoke ID length = 1 octet(s)
88	M	0000 0000	Invoke ID
89	M	0000 0010	Local Operation Code tag
90	M	0 0000001	Local Operation Code length = 1 octet(s)
91	F	0000 0000	Operation Code = Initial DP
92	M	0011 0000	SEQUENCE Tag
93	M	0111 1001	Length = 121 octets
94	M	1000 0000	Service Key Tag
95	M	0000 0010	Length = 2 octets
96	M	0000 0011	Service Key = 1000 dec, 03E8 hex
97	M	1110 1000	Service Key
98	O	1000 0010	Called Party Number Tag
99	O	0000 1001	Length = 9 octets
100	O	1 0000100	O/E = Odd, NAI = International number
101	O	0 0010000	INN=Allowed, NP=ISDN(Teleph)
102	O	xxxx xxxx	Address Signal = xxxxxxxxxxxx

103	0		xxxx xxxx		Address Signal
104	0		xxxx xxxx		Address Signal
105	0		xxxx xxxx		Address Signal
106	0		xxxx xxxx		Address Signal
107	0		xxxx xxxx		Address Signal
108	0		xxxx xxxx		Address Signal
109	0		1000 0011		Calling Party Number Tag
110	0		0000 1000		Length = 8 octets
111	0		0 0000100		O/E = Even, NAI = International number
112	0		0001 0001		NI=Complete, NP=ISDN(Teleph), PRI=Allowed, SI=User, passed
113	0		xxxx xxxx		Address Signal = xxxxxxxxxxxxxx
114	0		xxxx xxxx		Address Signal
115	0		xxxx xxxx		Address Signal
116	0		xxxx xxxx		Address Signal
117	0		xxxx xxxx		Address Signal
118	0		xxxx xxxx		Address Signal
119	0		1000 0101		Calling Partys Category Tag
120	0		0000 0001		Length = 1 octet
121	0		0000 1010		Calling Partys Category = Ordinary calling subscriber
122	0		1001 0111		High Layer Compatability Tag
123	0		0000 0010		Length = 2 octets
124	0		100 10001		CS = ITU-T,Interpre.= First Id, PM= HLPP
125	0		1 00000001		High Layer Chara.Id=Telephony
126	0		1011 1011		Bearer Capability Tag
127	0		0000 0101		Length = 5 octets
128	0		1000 0000		Bearer Cap Tag
129	0		0000 0011		Length = 3 octets
130	0		100 00000		Bearer Cap
131	0		100 10000		Bearer Cap
132	0		101 00011		Layer ident., User info. layer 1
133	0		1001 1100		Event Type BCSM Tag
134	0		0000 0001		Length = 1 octet
135	0		0000 1100		Event Type BCSM = Term attempt authorized
136	0		1001 1111		IMSI Tag
137	0		0011 0010		IMSI Tag
138	0		0000 1000		Length = 8 octets
139	0		0010 0111		MCC2, MCC1 (MCC = 724)
140	0		0001 0100		MNC1, MCC3 (MNC = 16)
141	0		0000 0110		MSIN1, MNC2
142	0		xxxx xxxx		MSIN = xxxxxxxxxxxx
143	0		xxxx xxxx		MSIN
144	0		xxxx xxxx		MSIN
145	0		xxxx xxxx		MSIN
146	0		xxxx xxxx		MSIN
147	0		1011 1111		Subscriber State Tag
148	0		0011 0011		Subscriber State Tag
149	0		0000 0010		Length = 2 octets
150	0		1000 0000		Assumed Idle Tag
151	0		0000 0000		Length = 0 octet
152	0		1011 1111		Location Info Tag
153	0		0011 0100		Location Info Tag
154	0		0001 0111		Length = 23 octets
155	0		0000 0010		Age Of Location Info Tag
156	0		0000 0001		Length = 1 octet
157	0		0000 0001		Age Of Location Info = 1 dec, 01 hex
158	0		1000 0001		Vlr Number Tag
159	0		0000 0111		Length = 7 octets
160	0		1001 0001		NAI = International number, NPI = ISDN/Telephony
161	0		0101 0101		Address Signal = 550312003001
162	0		0011 0000		Address Signal
163	0		0010 0001		Address Signal
164	0		0000 0000		Address Signal
165	0		0000 0011		Address Signal
166	0		0001 0000		Address Signal
167	0		1010 0011		Cell Global Id or SAI or LAI Tag
168	0		0000 1001		Length = 9 octets
169	0		1000 0000		Cell Global Id or SAI Fixed Len Tag
170	0		0000 0111		Length = 7 octets
171	0		0010 0111		MCC2, MCC1 (MCC = 724 hex)
172	0		1111 0100		filler, MCC3
173	0		0110 0001		MNC2, MNC1 (MNC =16 hex)
174	0		0001 0111		LAC = 17F0 hex
175	0		1111 0000		LAC
176	0		0000 1110		CI/SAC = 0EB1 hex
177	0		1011 0001		CI/SAC
178	0		1011 1111		Ext_basic Service Code Tag
179	0		0011 0101		Ext_basic Service Code Tag

```

180 O | 0000 0011 | Length = 3 octets
181 M | 1000 0011 | Ext Tele Service Tag
182 M | 0000 0001 | Length = 1 octet
183 M | 0001 0001 | Tele Service Code = Telephony
184 O | 1001 1111 | Call Reference Number Tag
185 O | 0011 0110 | Call Reference Number Tag
186 O | 0000 0111 | Length = 7 octets
187 O | 0100 0001 | Call Reference Number = 413901360B8913 hex
188 O | 0011 1001 | Call Reference Number
189 O | 0000 0001 | Call Reference Number
190 O | 0011 0110 | Call Reference Number
191 O | 0000 1011 | Call Reference Number
192 O | 1000 1001 | Call Reference Number
193 O | 0001 0011 | Call Reference Number
194 O | 1001 1111 | Msc Address Tag
195 O | 0011 0111 | Msc Address Tag
196 O | 0000 0111 | Length = 7 octets
197 O | 1001|0001 | NAI = International number, NPI = ISDN/Telephony
198 O | 0101|0101 | Address Signal = 550312003001
199 O | 0011|0000 | Address Signal
200 O | 0010|0001 | Address Signal
201 O | 0000|0000 | Address Signal
202 O | 0000|0011 | Address Signal
203 O | 0001|0000 | Address Signal
204 O | 1001 1111 | Time and Time Zone Tag
205 O | 0011 1001 | Time and Time Zone Tag
206 O | 0000 1000 | Length = 8 octets
207 O | 0000 0010 | Year = 2010
208 O | 0000 0001 | Year
209 O | 0011 0000 | Month= 03
210 O | 1001 0000 | Day = 09
211 O | 0010 0001 | Hour = 12
212 O | 0010 0101 | Min = 52
213 O | 0010 0100 | Sec = 42
214 O | 0010 1001 | Time Zone = -12

```

```

12:52:42.995 PM SAT Link: <-BSASG-CTAPPE13_0
SI: SCCP SSF: NN DPC: PR-CTAHUA1 OPC: PR-CTAPPES13 SLS: 8
MT: UDT
Called Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550312003001h
Calling Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550160000052h
MT: Continue
Originating Transaction ID Tag
  Transaction Id: 017d0208h
Destination Transaction ID Tag
  Transaction Id: 95479231h
Invoke
Invoke Id Tag
  Invoke Id: 1
Operation Code Tag: Local Operation Code
Operation ID: Request Report BCSM Event
BCSM Events Tag
Invoke
Invoke Id Tag
  Invoke Id: 2
Operation Code Tag: Local Operation Code
Operation ID: Apply Charging
ACh Bill Charging Chars Tag
Party to Charge Tag
Invoke
Invoke Id Tag
  Invoke Id: 3
Operation Code Tag: Local Operation Code
Operation ID: Connect
Destination Routing Address Tag
Destination Routing Address Tag
Calling Partys Category Tag

```

			ITU.WHITE.LAP
1		1 0010110	BIB = 1, BSN = 22
2		0 0011110	FIB = 0, FSN = 30
3		00 1111111	Length Indicator : MSU, LI = 63 octets
			ITU.WHITE.MTP
4		1000 0011	Service Indicator = SCCP, SSF = National Network
5		0011 1100	DPC : 9276 dec, 243C hex
6		01 100100	
7		1111 0110	OPC : 16345 dec, 3FD9 hex
8		1000 1111	SLS : 8 dec, 8 hex
			ITU.WHITE.SCCP
9	F	0000 1001	MT = Unitdata (UDT)
10	F	0000 0001	Protocol Class = class 1
11	V	0000 0011	Pointer to Called Party Address Parameter = 3
12	V	0000 1110	Pointer to Calling Party Address Parameter = 14
13	V	0001 1001	Pointer to Data Parameter = 25
14	V	0000 1011	LI of Called Party Address parameter = 11 octet(s)
15	V	0001 0010	Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
16	V	1001 0010	Subsystem Number = 146 92h
17	V	0000 0000	Translation Type = 0 Translation Type Not Used
18	V	0001 0010	Numbering Plan & Encoding Scheme
19	V	0 0000100	Nature of Address Indicator
20	V	0101 0101	Address Signal
21	V	0011 0000	Address Signal
22	V	0010 0001	Address Signal
23	V	0000 0000	Address Signal
24	V	0000 0011	Address Signal
25	V	0001 0000	Address Signal
26	V	0000 1011	LI of Calling Party Address parameter = 11 octet(s)
27	V	0001 0010	Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
28	V	1001 0010	Subsystem Number = 146 92h
29	V	0000 0000	Translation Type = 0 Translation Type Not Used
30	V	0001 0010	Numbering Plan & Encoding Scheme
31	V	0 0000100	Nature of Address Indicator
32	V	0101 0101	Address Signal
33	V	0001 0000	Address Signal
34	V	0000 0110	Address Signal
35	V	0000 0000	Address Signal
36	V	0000 0000	Address Signal
37	V	0010 0101	Address Signal
38	V	1010 1101	LI of Data parameter = 173 octet(s)
			ETSI.CAMEL.CAP
39	M	0110 0101	TCAP Message Type = Continue
40	M	1 0000001	Total TCAP Message length = 170 octet(s)
41	M	1010 1010	Length Of Contents
42	M	0100 1000	Originating Transaction ID tag
43	M	0 0000100	Originating Transaction ID length = 4 octet(s)
44	M	0000 0001	Transaction ID
45	M	0111 1101	Transaction ID
46	M	0000 0010	Transaction ID
47	M	0000 1000	Transaction ID
48	M	0100 1001	Destination Transaction ID tag
49	M	0 0000100	Destination Transaction ID length = 4 octet(s)
50	M	1001 0101	Transaction ID
51	M	0100 0111	Transaction ID
52	M	1001 0010	Transaction ID
53	M	0011 0001	Transaction ID
54	M	0110 1011	Dialogue tag
55	M	0 0101010	Dialogue length = 42 octet(s)
56	M	0010 1000	External tag
57	M	0 0101000	External length = 40 octet(s)
58	M	0000 0110	Object Identifier tag
59	M	0 0000111	Object Identifier length = 7 octet(s)
60	M	0000 0000	Dialogue-as-ID value ccitt
61	M	0001 0001	Dialogue-as-ID value q
62	M	1000 0110	Dialogue-as-ID value 773
63	M	0000 0101	Dialogue-as-ID value
64	M	0000 0001	Dialogue-as-ID value as
65	M	0000 0001	Dialogue-as-ID value DialoguePDU
66	M	0000 0001	Dialogue-as-ID value version1
67	M	1010 0000	Single-ASN.1-type tag
68	M	0 0011101	Single-ASN.1-type length = 29 octet(s)
69	M	0110 0001	Dialogue Response (AARE-apdu) tag
70	M	0 0011011	Dialogue Response (AARE-apdu) length = 27 octet(s)
71	O	1000 0000	Protocol Version tag
72	O	0 0000010	Protocol Version length = 2 octet(s)

73	O	0000 0111	Protocol Version
74	O	1000 0000	Protocol Version
75	M	1010 0001	Application Context Name tag
76	M	0 0001001	Application Context Name length = 9 octet(s)
77	M	0000 0110	Object Identifier tag
78	M	0 0000111	Object Identifier length = 7 octet(s)
79	M	0000 0100	Application Context Name ccitt identified organisation
80	M	0000 0000	Application Context Name etsi
81	M	0000 0000	Application Context Name mobile domain
82	M	0000 0001	Application Context Name GSM/UMTS Network
83	M	0000 0000	Application Context Name AC
84	M	0011 0010	Application Context Name cap-gsmssf-to-gsmscf
85	M	0000 0001	Application Context Name version 2
86	M	1010 0010	Result tag
87	M	0 0000011	Result length = 3 octet(s)
88	M	0000 0010	Integer tag
89	M	0 0000001	Integer length = 1 octet(s)
90	M	0000 0000	Result = Accepted
91	M	1010 0011	Result Source Diagnostic tag
92	M	0 0000101	Result Source Diagnostic length = 5 octet(s)
93	M	1010 0001	Dialogue Service User tag
94	M	0 0000011	Dialogue Service User length = 3 octet(s)
95	O	0000 0010	Integer tag
96	O	0 0000001	Integer length = 1 octet(s)
97	O	0000 0000	Dialogue Service User = Null
98	M	0110 1100	Component Portion tag
99	M	0 1110000	Component Portion length = 112 octet(s)
100	M	1010 0001	Component Type Tag = Invoke
101	M	0 0111110	Component length = 62 octet(s)
102	M	0000 0010	Invoke ID tag
103	M	0 0000001	Invoke ID length = 1 octet(s)
104	M	0000 0001	Invoke ID
105	M	0000 0010	Local Operation Code tag
106	M	0 0000001	Local Operation Code length = 1 octet(s)
107	F	0001 0111	Operation Code = Request Report BCSM Event
108	M	0011 0000	SEQUENCE Tag
109	M	0011 0110	Length = 54 octets
110	M	1010 0000	BCSM Events Tag
111	M	0011 0100	Length = 52 octets
112	M	0011 0000	BCSM Event Tag
113	M	0000 1011	Length = 11 octets
114	M	1000 0000	Event Type BCSM Tag
115	M	0000 0001	Length = 1 octet
116	M	0001 0001	Event Type BCSM = T disconnect
117	M	1000 0001	Monitor Mode Tag
118	M	0000 0001	Length = 1 octet
119	M	0000 0000	Monitor Mode = Interrupted
120	O	1010 0010	Leg ID Tag
121	O	0000 0011	Length = 3 octets
122	O	1000 0000	Sending Side ID Tag
123	O	0000 0001	Length = 1 octet
124	O	0000 0001	ID = Leg 1
125	O	0011 0000	BCSM Event Tag
126	O	0000 1011	Length = 11 octets
127	M	1000 0000	Event Type BCSM Tag
128	M	0000 0001	Length = 1 octet
129	M	0001 0001	Event Type BCSM = T disconnect
130	M	1000 0001	Monitor Mode Tag
131	M	0000 0001	Length = 1 octet
132	M	0000 0000	Monitor Mode = Interrupted
133	O	1010 0010	Leg ID Tag
134	O	0000 0011	Length = 3 octets
135	O	1000 0000	Sending Side ID Tag
136	O	0000 0001	Length = 1 octet
137	O	0000 0010	ID = Leg 2
138	O	0011 0000	BCSM Event Tag
139	O	0000 1011	Length = 11 octets
140	M	1000 0000	Event Type BCSM Tag
141	M	0000 0001	Length = 1 octet
142	M	0000 1110	Event Type BCSM = T no answer
143	M	1000 0001	Monitor Mode Tag
144	M	0000 0001	Length = 1 octet
145	M	0000 0000	Monitor Mode = Interrupted
146	O	1010 0010	Leg ID Tag
147	O	0000 0011	Length = 3 octets
148	O	1000 0000	Sending Side ID Tag
149	O	0000 0001	Length = 1 octet

```

150 O | 0000 0010 | ID = Leg 2
151 O | 0011 0000 | BCSM Event Tag
152 O | 0000 1011 | Length = 11 octets
153 M | 1000 0000 | Event Type BCSM Tag
154 M | 0000 0001 | Length = 1 octet
155 M | 0000 1101 | Event Type BCSM = T busy
156 M | 1000 0001 | Monitor Mode Tag
157 M | 0000 0001 | Length = 1 octet
158 M | 0000 0000 | Monitor Mode = Interrupted
159 O | 1010 0010 | Leg ID Tag
160 O | 0000 0011 | Length = 3 octets
161 O | 1000 0000 | Sending Side ID Tag
162 O | 0000 0001 | Length = 1 octet
163 O | 0000 0010 | ID = Leg 2
164 M | 1010 0001 | Component Type Tag = Invoke
165 M | 0|0010101 | Component length = 21 octet(s)
166 M | 0000 0010 | Invoke ID tag
167 M | 0|0000001 | Invoke ID length = 1 octet(s)
168 M | 0000 0010 | Invoke ID
169 M | 0000 0010 | Local Operation Code tag
170 M | 0|0000001 | Local Operation Code length = 1 octet(s)
171 F | 0010 0011 | Operation Code = Apply Charging
172 M | 0011 0000 | SEQUENCE Tag
173 M | 0000 1101 | Length = 13 octets
174 M | 1000 0000 | Ach Billing Charging Charac Tag
175 M | 0000 0110 | Length = 6 octets
176 M | 1010 0000 | Time Duration Charging Tag
177 M | 0000 0100 | Length = 4 octets
178 M | 1000 0000 | Max Call Period Duration Tag
179 M | 0000 0010 | Length = 2 octets
180 M | 0000 1011 | Max Call Period Duration = 3000 dec, 0BB8 hex
181 M | 1011 1000 | Max Call Period Duration
182 O | 1010 0010 | Party To Charge Tag
183 O | 0000 0011 | Length = 3 octets
184 O | 1000 0000 | Sending Side ID Tag
185 O | 0000 0001 | Length = 1 octet
186 O | 0000 0010 | Leg Type = Leg2
187 M | 1010 0001 | Component Type Tag = Invoke
188 M | 0|0010111 | Component length = 23 octet(s)
189 M | 0000 0010 | Invoke ID tag
190 M | 0|0000001 | Invoke ID length = 1 octet(s)
191 M | 0000 0011 | Invoke ID
192 M | 0000 0010 | Local Operation Code tag
193 M | 0|0000001 | Local Operation Code length = 1 octet(s)
194 F | 0001 0100 | Operation Code = Connect
195 M | 0011 0000 | SEQUENCE Tag
196 M | 0000 1111 | Length = 15 octets
197 M | 1010 0000 | Destination Routing Address Tag
198 M | 0000 1010 | Length = 10 octets
199 M | 0000 0100 | Destination Routing Address Tag
200 M | 0000 1000 | Length = 8 octets
201 M | 0|0000100 | O/E = Even, NAI = International number
202 M | 0|0010000 | INN=Allowed, NP=ISDN(Teleph)
203 M | xxxx|xxxx | Address Signal = xxxxxxxxxxxxxx
204 M | xxxx|xxxx | Address Signal
205 M | xxxx|xxxx | Address Signal
206 M | xxxx|xxxx | Address Signal
207 M | xxxx|xxxx | Address Signal
208 M | xxxx|xxxx | Address Signal
209 O | 1001 1100 | Calling Partys Category Tag
210 O | 0000 0001 | Length = 1 octet
211 O | 1110 0000 | Calling Partys Category = Reserved for national use

```

```

12:53:42.198 PM SAT Link: ->BSASG-CTAPPE13_0
SI: SCCP SSF: NN DPC: PR-CTAPPES13 OPC: PR-CTAHUA1 SLS: 8
MT: UDT
Called Party Address Length: 11 octets
Subsystem Number: 146
Translation Type: Translation Type Not Used
Nature of Address Indicator: International number
Address Information: 550160000052h
Calling Party Address Length: 11 octets
Subsystem Number: 146
Translation Type: Translation Type Not Used
Nature of Address Indicator: International number
Address Information: 550312003001h

```

MT: Continue  
 Originating Transaction ID Tag  
 Transaction Id: 95479231h  
 Destination Transaction ID Tag  
 Transaction Id: 017d0208h  
 Invoke  
 Invoke Id Tag  
 Invoke Id: 1  
 Operation Code Tag: Local Operation Code  
 Operation ID: Apply Charging Report  
 Call Result Tag

			ITU.WHITE.LAP
1		0 1000110	BIB = 0, BSN = 70
2		1 0100001	FIB = 1, FSN = 33
3		00 1111111	Length Indicator : MSU, LI = 63 octets
			ITU.WHITE.MTP
4		1000 0011	Service Indicator = SCCP, SSF = National Network
5		1101 1001	DPC : 16345 dec, 3FD9 hex
6		00 1111111	
7		0000 1111	OPC : 9276 dec, 243C hex
8		1000 1001	SLS : 8 dec, 8 hex
			ITU.WHITE.SCCP
9	F	0000 1001	MT = Unitdata (UDT)
10	F	1000 0001	Protocol Class = class 1
11	V	0000 0011	Pointer to Called Party Address Parameter = 3
12	V	0000 1110	Pointer to Calling Party Address Parameter = 14
13	V	0001 1001	Pointer to Data Parameter = 25
14	V	0000 1011	LI of Called Party Address parameter = 11 octet(s)
15	V	0101 0010	Addr Ind: Route=PC&SSN; GT=TT&NP&ES&NoA; PC=N; SSN=Y
16	V	1001 0010	Subsystem Number = 146 92h
17	V	0000 0000	Translation Type = 0 Translation Type Not Used
18	V	0001 0010	Numbering Plan & Encoding Scheme
19	V	0 0000100	Nature of Address Indicator
20	V	0101 0101	Address Signal
21	V	0001 0000	Address Signal
22	V	0000 0110	Address Signal
23	V	0000 0000	Address Signal
24	V	0000 0000	Address Signal
25	V	0010 0101	Address Signal
26	V	0000 1011	LI of Calling Party Address parameter = 11 octet(s)
27	V	0001 0010	Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
28	V	1001 0010	Subsystem Number = 146 92h
29	V	0000 0000	Translation Type = 0 Translation Type Not Used
30	V	0001 0010	Numbering Plan & Encoding Scheme
31	V	0 0000100	Nature of Address Indicator
32	V	0101 0101	Address Signal
33	V	0011 0000	Address Signal
34	V	0010 0001	Address Signal
35	V	0000 0000	Address Signal
36	V	0000 0011	Address Signal
37	V	0001 0000	Address Signal
38	V	0010 1010	LI of Data parameter = 42 octet(s)
			ETSI.CAMEL.CAP
39	M	0110 0101	TCAP Message Type = Continue
40	M	0 0101000	Total TCAP Message length = 40 octet(s)
41	M	0100 1000	Originating Transaction ID tag
42	M	0 0000100	Originating Transaction ID length = 4 octet(s)
43	M	1001 0101	Transaction ID
44	M	0100 0111	Transaction ID
45	M	1001 0010	Transaction ID
46	M	0011 0001	Transaction ID
47	M	0100 1001	Destination Transaction ID tag
48	M	0 0000100	Destination Transaction ID length = 4 octet(s)
49	M	0000 0001	Transaction ID
50	M	0111 1101	Transaction ID
51	M	0000 0010	Transaction ID
52	M	0000 1000	Transaction ID
53	M	0110 1100	Component Portion tag
54	M	0 0011010	Component Portion length = 26 octet(s)
55	M	1010 0001	Component Type Tag = Invoke
56	M	0 0011000	Component length = 24 octet(s)
57	M	0000 0010	Invoke ID tag
58	M	0 0000001	Invoke ID length = 1 octet(s)
59	M	0000 0001	Invoke ID
60	M	0000 0010	Local Operation Code tag

```

61 M | 0|0000001 | Local Operation Code length = 1 octet(s)
62 F | 0010 0100 | Operation Code = Apply Charging Report
63 M | 0000 0100 | Call Result Tag
64 M | 0001 0000 | Length = 16 octets
65 M | 1010 0000 | Time Duration Charging Result Tag
66 M | 0000 1110 | Length = 14 octets
67 M | 1010 0000 | Party To Charge Tag
68 M | 0000 0011 | Length = 3 octets
69 M | 1000 0001 | Receiving Side ID Tag
70 M | 0000 0001 | Length = 1 octet
71 M | 0000 0010 | Leg Type = Leg2
72 M | 1010 0001 | Time Information Tag
73 M | 0000 0100 | Length = 4 octets
74 M | 1000 0000 | Time If No Tariff Switch Tag
75 M | 0000 0010 | Length = 2 octets
76 M | 0000 0010 | Time If No Tariff Switch = 525 dec, 020D hex
77 M | 0000 1101 | Time If No Tariff Switch
78 O | 1000 0010 | Call Active Tag
79 O | 0000 0001 | Length = 1 octet
80 O | 0000 0000 | Call Active = FALSE

```

```

12:53:42.208 PM SAT Link: ->BSASG-CTAPPE13_0
SI: SCCP SSF: NN DPC: PR-CTAPPES13 OPC: PR-CTAHUA1 SLS: 8
MT: UDT

```

```

Called Party Address Length: 11 octets
Subsystem Number: 146
Translation Type: Translation Type Not Used
Nature of Address Indicator: International number
Address Information: 550160000052h
Calling Party Address Length: 11 octets
Subsystem Number: 146
Translation Type: Translation Type Not Used
Nature of Address Indicator: International number
Address Information: 550312003001h
MT: Continue

```

```

Originating Transaction ID Tag
Transaction Id: 95479231h
Destination Transaction ID Tag
Transaction Id: 017d0208h

```

Invoke

```

Invoke Id Tag
Invoke Id: 2

```

```

Operation Code Tag: Local Operation Code
Operation ID: Event Report BCSM
Event Type BCSM Tag
Event Specific BCSM Info Tag
Leg ID Tag

```

```

1 | | ITU.WHITE.LAP
2 | 0|1000110 | BIB = 0, BSN = 70
3 | 1|0100010 | FIB = 1, FSN = 34
4 | 00|1111111 | Length Indicator : MSU, LI = 63 octets
5 | | ITU.WHITE.MTP
6 | 1000|0011 | Service Indicator = SCCP, SSF = National Network
7 | 1101 1001 | DPC : 16345 dec, 3FD9 hex
8 | 00|1111111 |
9 | 0000 1111 | OPC : 9276 dec, 243C hex
10 | 1000|1001 | SLS : 8 dec, 8 hex
11 | | ITU.WHITE.SCCP
12 F | 0000 1001 | MT = Unitdata (UDT)
13 F | 1000 0001 | Protocol Class = class 1
14 V | 0000 0011 | Pointer to Called Party Address Parameter = 3
15 V | 0000 1110 | Pointer to Calling Party Address Parameter = 14
16 V | 0001 1001 | Pointer to Data Parameter = 25
17 V | 0000 1011 | LI of Called Party Address parameter = 11 octet(s)
18 V | 0101 0010 | Addr Ind: Route=PC&SSN; GT=TT&NP&ES&NoA; PC=N; SSN=Y
19 V | 1001 0010 | Subsystem Number = 146 92h
20 V | 0000 0000 | Translation Type = 0 Translation Type Not Used
21 V | 0001|0010 | Numbering Plan & Encoding Scheme
22 V | 0|0000100 | Nature of Address Indicator
23 V | 0101|0101 | Address Signal
24 V | 0001|0000 | Address Signal
25 V | 0000|0110 | Address Signal
26 V | 0000|0000 | Address Signal
27 V | 0000|0000 | Address Signal

```

```

25 V | 0010|0101 | Address Signal
26 V | 0000 1011 | LI of Calling Party Address parameter = 11 octet(s)
27 V | 0001 0010 | Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
28 V | 1001 0010 | Subsystem Number = 146 92h
29 V | 0000 0000 | Translation Type = 0 Translation Type Not Used
30 V | 0001|0010 | Numbering Plan & Encoding Scheme
31 V | 0|0000100 | Nature of Address Indicator
32 V | 0101|0101 | Address Signal
33 V | 0011|0000 | Address Signal
34 V | 0010|0001 | Address Signal
35 V | 0000|0000 | Address Signal
36 V | 0000|0011 | Address Signal
37 V | 0001|0000 | Address Signal
38 V | 0010 1010 | LI of Data parameter = 42 octet(s)
    | | ETSI.CAMEL.CAP
39 M | 0110 0101 | TCAP Message Type = Continue
40 M | 0|0101000 | Total TCAP Message length = 40 octet(s)
41 M | 0100 1000 | Originating Transaction ID tag
42 M | 0|0000100 | Originating Transaction ID length = 4 octet(s)
43 M | 1001 0101 | Transaction ID
44 M | 0100 0111 | Transaction ID
45 M | 1001 0010 | Transaction ID
46 M | 0011 0001 | Transaction ID
47 M | 0100 1001 | Destination Transaction ID tag
48 M | 0|0000100 | Destination Transaction ID length = 4 octet(s)
49 M | 0000 0001 | Transaction ID
50 M | 0111 1101 | Transaction ID
51 M | 0000 0010 | Transaction ID
52 M | 0000 1000 | Transaction ID
53 M | 0110 1100 | Component Portion tag
54 M | 0|0011010 | Component Portion length = 26 octet(s)
55 M | 1010 0001 | Component Type Tag = Invoke
56 M | 0|0011000 | Component length = 24 octet(s)
57 M | 0000 0010 | Invoke ID tag
58 M | 0|00000001 | Invoke ID length = 1 octet(s)
59 M | 0000 0010 | Invoke ID
60 M | 0000 0010 | Local Operation Code tag
61 M | 0|00000001 | Local Operation Code length = 1 octet(s)
62 F | 0001 1000 | Operation Code = Event Report BCSM
63 M | 0011 0000 | SEQUENCE Tag
64 M | 0001 0000 | Length = 16 octets
65 M | 1000 0000 | Event Type BCSM Tag
66 M | 0000 0001 | Length = 1 octet
67 M | 0001 0001 | Event Type BCSM = T disconnect
68 O | 1010 0010 | Event Specific Info BCSM Tag
69 O | 0000 0110 | Length = 6 octets
70 O | 1010 1100 | T Disconnect Specific Info Tag
71 O | 0000 0100 | Length = 4 octets
72 O | 1000 0000 | Release Cause Tag
73 O | 0000 0010 | Length = 2 octets
74 O | 1000|0000 | CS = ITU-T, Location = User(U)
75 O | 1|0010000 | Value = Normal call clearing
76 O | 1010 0011 | Leg ID Tag
77 O | 0000 0011 | Length = 3 octets
78 O | 1000 0001 | Receiving Side ID Tag
79 O | 0000 0001 | Length = 1 octet
80 O | 0000 0010 | Leg Type = Leg2

```

```

12:53:42.397 PM SAT Link: <-BSASG-CTAPPE13_0
SI: SCCP SSF: NN DPC: PR-CTAHUA1 OPC: PR-CTAPPES13 SLS: 8
MT: UDT
Called Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550312003001h
Calling Party Address Length: 11 octets
  Subsystem Number: 146
  Translation Type: Translation Type Not Used
  Nature of Address Indicator: International number
  Address Information: 550160000052h
MT: Continue
Originating Transaction ID Tag
  Transaction Id: 017d0208h
Destination Transaction ID Tag
  Transaction Id: 95479231h

```

Invoke  
 Invoke Id Tag  
 Invoke Id: 4  
 Operation Code Tag: Local Operation Code  
 Operation ID: Release Call  
 Cause Tag

1		1 0100100	ITU.WHITE.LAP
2		0 1001001	BIB = 1, BSN = 36
3		00 1111111	FIB = 0, FSN = 73
			Length Indicator : MSU, LI = 63 octets
			ITU.WHITE.MTP
4		1000 0011	Service Indicator = SCCP, SSF = National Network
5		0011 1100	DPC : 9276 dec, 243C hex
6		01 100100	
7		1111 0110	OPC : 16345 dec, 3FD9 hex
8		1000 1111	SLS : 8 dec, 8 hex
			ITU.WHITE.SCCP
9	F	0000 1001	MT = Unitdata (UDT)
10	F	0000 0001	Protocol Class = class 1
11	V	0000 0011	Pointer to Called Party Address Parameter = 3
12	V	0000 1110	Pointer to Calling Party Address Parameter = 14
13	V	0001 1001	Pointer to Data Parameter = 25
14	V	0000 1011	LI of Called Party Address parameter = 11 octet(s)
15	V	0001 0010	Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
16	V	1001 0010	Subsystem Number = 146 92h
17	V	0000 0000	Translation Type = 0 Translation Type Not Used
18	V	0001 0010	Numbering Plan & Encoding Scheme
19	V	0 0000100	Nature of Address Indicator
20	V	0101 0101	Address Signal
21	V	0011 0000	Address Signal
22	V	0010 0001	Address Signal
23	V	0000 0000	Address Signal
24	V	0000 0011	Address Signal
25	V	0001 0000	Address Signal
26	V	0000 1011	LI of Calling Party Address parameter = 11 octet(s)
27	V	0001 0010	Addr Ind: Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
28	V	1001 0010	Subsystem Number = 146 92h
29	V	0000 0000	Translation Type = 0 Translation Type Not Used
30	V	0001 0010	Numbering Plan & Encoding Scheme
31	V	0 0000100	Nature of Address Indicator
32	V	0101 0101	Address Signal
33	V	0001 0000	Address Signal
34	V	0000 0110	Address Signal
35	V	0000 0000	Address Signal
36	V	0000 0000	Address Signal
37	V	0010 0101	Address Signal
38	V	0001 1100	LI of Data parameter = 28 octet(s)
			ETSI.CAMEL.CAP
39	M	0110 0101	TCAP Message Type = Continue
40	M	0 0011010	Total TCAP Message length = 26 octet(s)
41	M	0100 1000	Originating Transaction ID tag
42	M	0 0000100	Originating Transaction ID length = 4 octet(s)
43	M	0000 0001	Transaction ID
44	M	0111 1101	Transaction ID
45	M	0000 0010	Transaction ID
46	M	0000 1000	Transaction ID
47	M	0100 1001	Destination Transaction ID tag
48	M	0 0000100	Destination Transaction ID length = 4 octet(s)
49	M	1001 0101	Transaction ID
50	M	0100 0111	Transaction ID
51	M	1001 0010	Transaction ID
52	M	0011 0001	Transaction ID
53	M	0110 1100	Component Portion tag
54	M	0 0001100	Component Portion length = 12 octet(s)
55	M	1010 0001	Component Type Tag = Invoke
56	M	0 0001010	Component length = 10 octet(s)
57	M	0000 0010	Invoke ID tag
58	M	0 0000001	Invoke ID length = 1 octet(s)
59	M	0000 0100	Invoke ID
60	M	0000 0010	Local Operation Code tag
61	M	0 0000001	Local Operation Code length = 1 octet(s)
62	F	0001 0110	Operation Code = Release Call
63	M	0000 0100	Cause Tag
64	M	0000 0010	Length = 2 octets
65	M	1000 0001	CS = ITU-T, Location = Prv net serv loc usr (LPN)

66 M | 1|0010000 | Value = Normal call clearing

## B. TABELA COMPARATIVA DE TEMPOS DE COMUTAÇÃO

A Tabela B.1 tem o tempo de comutação estimado para diversos perfis de configuração sugeridos. Considerando-se o tempo alvo de 500ms, observa-se que cada um dos perfis é efetivo até um valor específico de latência.

A estimativa foi feita pela aplicação direta das regras de funcionamento do protocolo SCTP (*Stream Control Transmission Protocol*), conforme estabelecido pela RFC 2960 (Stewart, R., Xie, Q., Morneault, K. et al., 2000).

Tabela B.1: Tempo de comutação estimado para os diversos perfis

Latência	Perfil 0	Perfil 1	Perfil 2	Perfil 3	Perfil 4	Perfil 5
2	63.000,0	248,0	120,0	75,0	75,0	20,0
3	63.000,0	372,0	180,0	112,5	112,5	30,0
4	63.000,0	496,0	240,0	150,0	150,0	40,0
5	63.000,0	620,0	300,0	187,5	187,5	50,0
6	63.000,0	744,0	360,0	225,0	225,0	60,0
7	63.000,0	868,0	420,0	262,5	262,5	70,0
8	63.000,0	992,0	480,0	300,0	290,0	80,0
9	63.000,0	1.116,0	540,0	337,5	307,5	90,0
10	63.000,0	1.240,0	600,0	375,0	325,0	100,0
11	63.000,0	1.364,0	660,0	392,5	342,5	110,0
12	63.000,0	1.488,0	720,0	410,0	360,0	120,0
13	63.000,0	1.612,0	780,0	427,5	377,5	130,0
14	63.000,0	1.736,0	840,0	445,0	395,0	140,0
15	63.000,0	1.860,0	900,0	462,5	412,5	150,0
16	63.000,0	1.984,0	960,0	480,0	420,0	160,0
17	63.000,0	2.108,0	1.020,0	497,5	427,5	170,0
18	63.000,0	2.232,0	1.080,0	515,0	435,0	180,0
19	63.000,0	2.356,0	1.140,0	532,5	442,5	190,0
20	63.000,0	2.480,0	1.200,0	550,0	450,0	200,0
21	63.000,0	2.604,0	1.260,0	557,5	457,5	210,0
22	63.000,0	2.728,0	1.320,0	565,0	465,0	220,0
23	63.000,0	2.852,0	1.380,0	572,5	472,5	230,0
24	63.000,0	2.976,0	1.440,0	580,0	480,0	240,0

25	63.000,0	3.100,0	1.500,0	587,5	487,5	250,0
26	63.000,0	3.224,0	1.560,0	595,0	495,0	260,0
27	63.000,0	3.348,0	1.620,0	602,5	502,5	270,0
28	63.000,0	3.472,0	1.680,0	610,0	510,0	280,0
29	63.000,0	3.596,0	1.740,0	617,5	517,5	290,0
30	63.000,0	3.720,0	1.800,0	625,0	525,0	300,0
31	63.000,0	3.844,0	1.860,0	632,5	527,5	310,0
32	63.000,0	3.968,0	1.920,0	640,0	530,0	320,0
33	63.000,0	4.092,0	1.980,0	647,5	532,5	330,0
34	63.000,0	4.216,0	2.040,0	655,0	535,0	340,0
35	63.000,0	4.340,0	2.100,0	662,5	537,5	350,0
36	63.000,0	4.464,0	2.160,0	670,0	540,0	360,0
37	63.000,0	4.588,0	2.220,0	677,5	542,5	370,0
38	63.000,0	4.712,0	2.280,0	685,0	545,0	380,0
39	63.000,0	4.836,0	2.340,0	692,5	547,5	390,0
40	63.000,0	4.960,0	2.400,0	700,0	550,0	400,0
41	63.000,0	5.084,0	2.460,0	702,5	552,5	410,0
42	63.000,0	5.208,0	2.520,0	705,0	555,0	420,0
43	63.000,0	5.332,0	2.580,0	707,5	557,5	430,0
44	63.000,0	5.456,0	2.640,0	710,0	560,0	440,0
45	63.000,0	5.580,0	2.700,0	712,5	562,5	450,0
46	63.000,0	5.704,0	2.760,0	715,0	565,0	460,0
47	63.000,0	5.828,0	2.820,0	717,5	567,5	470,0
48	63.000,0	5.952,0	2.880,0	720,0	570,0	480,0
49	63.000,0	6.076,0	2.940,0	722,5	572,5	490,0
50	63.000,0	6.200,0	3.000,0	725,0	575,0	500,0
51	63.000,0	6.324,0	3.060,0	727,5	577,5	510,0
52	63.000,0	6.448,0	3.120,0	730,0	580,0	520,0
53	63.000,0	6.572,0	3.180,0	732,5	582,5	530,0
54	63.000,0	6.696,0	3.240,0	735,0	585,0	540,0
55	63.000,0	6.820,0	3.300,0	737,5	587,5	550,0
56	63.000,0	6.944,0	3.360,0	740,0	590,0	560,0
57	63.000,0	7.068,0	3.420,0	742,5	592,5	570,0
58	63.000,0	7.192,0	3.480,0	745,0	595,0	580,0
59	63.000,0	7.316,0	3.540,0	747,5	597,5	590,0
60	63.000,0	7.440,0	3.600,0	750,0	600,0	600,0

<b>61</b>	63.000,0	7.564,0	3.660,0	752,5	602,5	610,0
<b>62</b>	63.000,0	7.688,0	3.720,0	755,0	605,0	620,0
<b>63</b>	63.000,0	7.812,0	3.780,0	757,5	607,5	630,0
<b>64</b>	63.000,0	7.936,0	3.840,0	760,0	610,0	640,0
<b>65</b>	63.000,0	8.060,0	3.900,0	762,5	612,5	650,0
<b>66</b>	63.000,0	8.184,0	3.960,0	765,0	615,0	660,0
<b>67</b>	63.000,0	8.308,0	4.020,0	767,5	617,5	670,0
<b>68</b>	63.000,0	8.432,0	4.080,0	770,0	620,0	680,0
<b>69</b>	63.000,0	8.556,0	4.140,0	772,5	622,5	690,0
<b>70</b>	63.000,0	8.680,0	4.200,0	775,0	625,0	700,0

O perfil 0 representa os valores propostos pela RFC 2960 e não atende aos requisitos indicados. O perfil 1 ao primeiro ajuste sugerido, ou seja, o valor de RTOMin equivalente a duas vezes o RTT da rede, com Path.Max.Retrans = 4. O perfil 2 faz a redução do valor do parâmetro Path.Max.Retrans de 4 para 3. O perfil 3 reduz o valor de RTOMax para 200ms. Esse ajuste reduz um pouco o efeito exponencial do crescimento do RTO. O perfil 4 ajusta o RTOMax para 150ms, reduzindo ainda mais o efeito exponencial, enquanto o perfil 5 elimina totalmente este efeito, uma vez que faz o RTOMax equivalente a duas vezes o RTT. A quantidade de retransmissões, no entanto, é mantida em 3.

Para o cálculo destes tempos de comutação, foi considerado que o RTT da rede é igual a 2,5 vezes a sua latência. A estimativa foi feita pela aplicação direta de funcionamento do protocolo.

Por exemplo, no caso de latência de 16ms, para o perfil 3 (RTOMin = RTT, RTOMax = 200ms, Path.Max.Retrans = 3), temos os eventos indicados na Tabela B.2, onde aparece o tempo de comutação de 480ms.

Tabela B.2: Tempos e Eventos Associados para o perfil 3, latência de 16ms

Tempo	Evento
0 ms	RTO = 40ms (2,5 x Latência)
40 ms	Retransmissão 1, RTO = 2xRTO = 80ms
120 ms (40ms + 80ms)	Retransmissão 2, RTO = 2xRTO = 160ms
280ms (120ms + 160ms)	Retransmissão 3, RTO = 200ms (limite)
480ms (280ms + 200ms)	Comutação para o caminho alternativo



## C.DIMENSIONAMENTO DE ENLACES DE SINALIZAÇÃO NÚMERO 7

Para o correto dimensionamento de enlaces de sinalização, tipicamente considera-se as seguintes premissas:

- Ocupação máxima dos enlaces em 80%, como forma de prever o atendimento a eventuais picos de sinalização
- Redundância de transmissão entre dois meios distintos, de forma que a garantir a segurança. Assim, cada um dos caminhos de transmissão deve ser capaz de suportar todo o tráfego entre os elementos de rede.

Com as premissas acima, calcula-se a capacidade máxima de ocupação conforme abaixo:

$$CapacidadeMáxima = CapacidadeIndividual \times NúmeroDeEnlaces \times 0,5 \times 0,8 \quad C.1$$

Assim, para enlaces de 64kbps, temos

$$CapacidadeMáxima_{64k} = 64kbps \times 16 \times 0,5 \times 0,8 \quad C.2$$

$$CapacidadeMáxima_{64k} = 409,6 \text{ kbps} \quad C.3$$

Para enlaces de 2Mbps, temos

$$CapacidadeMáxima_{2M} = 2Mbps \times 16 \times 0,5 \times 0,8 \quad C.4$$

$$CapacidadeMáxima_{2M} = 12,8 \text{ Mbps} \quad C.5$$

## D.PROGRAMA SIMULADOR SCTP

O simulador SCTP tem três módulos principais, e dois *forms* (telas) de controle. O módulo `mod_Endpoint` (Tabela D.1) tem as funções de controle de cada *endpoint*, sendo que estes são instanciados com as funções definidas nesse módulo. O módulo de rede (Tabela D.2) tem as funções de transporte de mensagens e entrega das mesmas ao *endpoint* de destino, aplicando a latência indicada e gerando a falha no momento adequado. O módulo Aplicação (Tabela D.3) envia os pacotes nos intervalos definidos e os recebe pelo *endpoint* de destino, fazendo as avaliações de atraso dos pacotes. No simulador foram usadas diversas estruturas de dados (Tabela D.4), tanto para armazenar informações internas do endpoint como para manter em memória os dados que estão sendo trafegado pela rede em cada momento.

O *form* `Painel_de_Control` (Figura D.1 e Figura D.2) é usado para configurar os parâmetros da simulação e disparar os mesmos. O *form* `Resultados` (Figura D.3) apresenta dados em tempo real das variáveis internas do protocolo, e é usado basicamente para acompanhamento do comportamento das mesmas.

O resultado final da simulação é um arquivo em formato CSV (*Comma Separated Values* – valores separados por vírgula), onde os dados são gravados após cada execução (Tabela D.5). Estes arquivos são carregados em uma planilha de cálculo para análise e geração dos gráficos.

Tabela D.1: Descrição das principais rotinas do módulo `mod_Endpoint`

<p><code>Sub EP_Initialize(ByRef EP As st_Endpoint)</code></p> <ul style="list-style-type: none"><li>• Inicializa a associação EP, voltando suas variáveis para os valores iniciais</li></ul> <p><code>Sub EP_Associate(ByRef EP As st_Endpoint)</code></p> <ul style="list-style-type: none"><li>• Cria a associação, pela montagem e envio do chunk INIT em direção ao endpoint de destino. Inicializa os temporizadores da associação</li></ul> <p><code>Sub EP_Send(ByRef EP As st_Endpoint, ByVal dados As String, ByVal Path As Integer, ByVal seq As Long)</code></p> <ul style="list-style-type: none"><li>• Envia dados a partir de uma associação, e faz a atualização de suas variáveis e temporizadores</li></ul> <p><code>Sub EP_EnviaDadosMarcadosParaRetransmissão(ByRef EP As st_Endpoint, ByVal Path As Integer)</code></p> <ul style="list-style-type: none"><li>• Envia chunks que estejam aguardando para retransmissão após uma falha</li></ul>
--

<p><b>Sub</b> EP_Receive(<b>ByRef</b> EP <b>As</b> st_Endpoint, <b>ByVal</b> pacote <b>As</b> st_ElementoFilaRede)</p> <ul style="list-style-type: none"> <li>• Recebe e trata chunks recebidos da rede.</li> </ul> <p><b>Sub</b> MontaOSACK(<b>ByRef</b> EP <b>As</b> st_Endpoint, <b>ByVal</b> pacote <b>As</b> st_ElementoFilaRede, <b>ByRef</b> c <b>As</b> Integer)</p> <ul style="list-style-type: none"> <li>• Faz a montagem da informação SACK para envio ao endpoint de origem, de acordo com a fila existente</li> </ul> <p><b>Public Sub</b> EP_Timer_T3_rtx(<b>ByRef</b> EP <b>As</b> st_Endpoint, <b>ByVal</b> iArray <b>As</b> Integer)</p> <ul style="list-style-type: none"> <li>• Trata o esgotamento do timer T3-rtx</li> </ul> <p><b>Private Sub</b> EP_SACKRecebido(<b>ByRef</b> EP <b>As</b> st_Endpoint, <b>ByVal</b> pacote <b>As</b> st_ElementoFilaRede)</p> <ul style="list-style-type: none"> <li>• Trata uma informação SACK recebida e verifica a necessidade de retransmissões</li> </ul> <p><b>Sub</b> CalculaRTO(<b>ByRef</b> path <b>As</b> st_Path, <b>ByVal</b> RTTmedido <b>As</b> Long)</p> <ul style="list-style-type: none"> <li>• Calcula o valor da variável RTO, conforme RFC 2960</li> </ul>
--

Tabela D.2: Descrição das principais rotinas do módulo Rede

<p><b>Public</b> FilaDaRede <b>As</b> New Collection</p> <ul style="list-style-type: none"> <li>• Coleção que contém os dados que estão sendo trafegados pela rede, ou seja, já foram enviados pelo endpoint de origem mais ainda não foram recebidos pelo destino.</li> </ul> <p><b>Public Sub</b> EnviaPacoteParaARede(<b>ByVal</b> qtdChunks <b>As</b> Integer, <b>ByVal</b> Chunks() <b>As</b> st_Chunk, <b>_</b> <b>ByVal</b> Destino <b>As</b> st_Endereço, <b>ByVal</b> HoraEnvio <b>As</b> Long)</p> <ul style="list-style-type: none"> <li>• Recebe o pacote o endpoint de origem e o trata, de acordo com os parâmetros, de forma a verificar se o mesmo deve ser descartado. Em caso negativo, calcula o atraso que esse pacote sofrerá e o coloca na fila da rede.</li> </ul> <p><b>Function</b> AtrasoDevidoAEsteChunk(<b>ByVal</b> caminho <b>As</b> Integer, <b>_</b> <b>ByVal</b> EspLat <b>As</b> Long, <b>_</b> <b>ByVal</b> LatMín <b>As</b> Long) <b>As</b> Long</p> <ul style="list-style-type: none"> <li>• Calcula o atraso devido a cada pacote</li> </ul> <p><b>Sub</b> EntregaPacoteNoDestino(<b>ByVal</b> pacote <b>As</b> st_ElementoFilaRede)</p> <ul style="list-style-type: none"> <li>• Faz a entrega do pacote no endpoint de destino</li> </ul>
---

Tabela D.3: Principais rotinas do módulo Aplicação

<p><b>Private Function</b> AplicaçãoEnviaDadosM3UA(<b>ByVal</b> dados <b>As</b> String) <b>As</b> Boolean</p> <ul style="list-style-type: none"> <li>• Faz o envio de dados da aplicação para o SCTP, simulando a camada M3UA, escolhendo qual das</li> </ul>
---

associações será usada por divisão de carga, se houver mais de uma.

**Public Sub** Loop\_Principal(**ByRef** AlgoOcorreu **As Boolean**)

- Loop principal de execução do programa que verifica, a cada 1ms da simulação, se há algum evento a ser executado, dentre (1) envio de dados pela aplicação, (2) entrega de dados pela rede, (3) esgotamento de temporizadores

Tabela D.4: Principais estruturas de dados usadas no simulador

```
Structure st_Endpoint
  Public SCTP_id As String           'ID da associação, como STRING
  Public index As Integer            'indice da associação 1 a 8
  Public Side As Integer             'Lado, 1 ou 2
  Public Status As Integer           'indica o status da associação
  Public T1_init As Long             'timer T1-init, de espera de um INIT-ACK
  Public T1_enviado As Long          'hora em que o INIT ou COOKIE foi enviado
  Public INITs_transmitidos As Integer 'número de INITs já transmitidos
  Public PrimaryPath As Integer      'indica qual o caminho que está ativo no momento
  Public OverallErrorCount As Long   'quantidade de erros da associação
  Public NextTSN As Long             'Próximo TSN
  Public AckState As Boolean         'True indica que o próximo pacote deve ter SACK.
  Public AckTimer As Long           'Hora em que o SACK deve ser enviado
  Public Path() As st_Path
  Public CumulativeTSN As Long
  Public LastTSNRcvd As Long
  Public ArrayTx() As st_ArrayEndPointTx
  Public ArrayRx() As st_ArrayEndPointRx
  Public GapAckBlk() As Integer
  Public RetransmissãoPendente As Boolean
End Structure

Structure st_Path
  Public ErrorCount As Integer
  Public ErrorThreshold As Integer
  Public RTO As Long                'valor de Retransmission Timeout observado na rede
  Public SRTT As Double              'valor usado para calculo do RTO
  Public RTTVAR As Double            'valor usado para calculo do RTO
  Public State As Integer            'estado da associação
  Public RTO_Pending As Boolean
  Public HBTimer As Long
  Public HBEnviado As Long          'hora de envio do último HEARBEAT
End Structure

Structure st_ArrayEndPointTx
  Public Dado As String
  Public TSN As Long
  Public HoraEnvioOriginal As Long
  Public T3_rtx As Long
  Public Retransmitido As Boolean
  Public MarcadoParaRetrans As Boolean
  Public SeqEnvio As Long
End Structure

Structure st_ArrayEndPointRx
  Public Dado As String
```

```

Public TSN As Long
Public HoraEnvioOriginal As Long
Public retransmitido As Boolean
Public SeqEnvio As Long
End Structure

Structure st_Chunk
Public Type As Integer
Public GapAckBlk() As Integer
Public TSN As Long 'Somente no caso de Chunk do tipo DATA
Public Dados As String
Public HoraEnvioOriginal As Long
Public SeqEnvio As Long
End Structure

Structure st_ElementoFilaRede
Public Chunks() As st_Chunk
Public Destino As st_Endereço
Public HoraEnvio As Long
Public HoraEntrega As Long
Public id As String
Public Perdido As Boolean
Public qtdChunks As Integer
End Structure

```

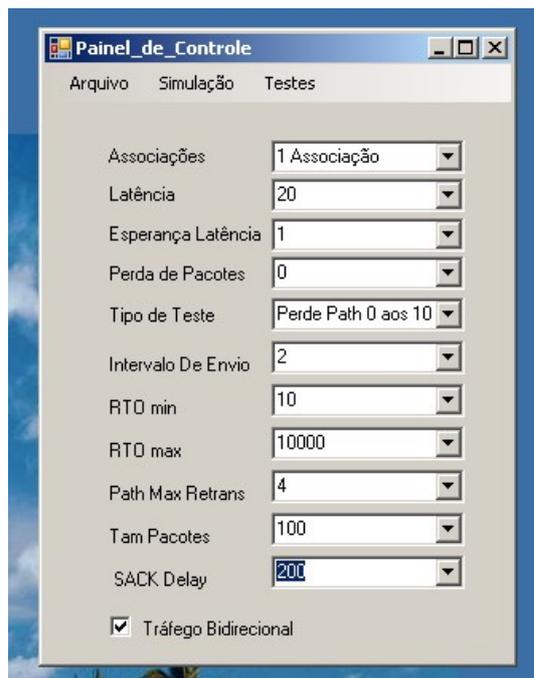


Figura D.1: Painel de Controle Principal do Simulador



- índice da execução (no exemplo, representam diretamente o valor da latência);
- atraso médio dos pacotes recebidos;
- desvio padrão do atraso médio dos pacotes;
- hora da comutação média (considerar que a falha ocorreu no valor 10000, que representa 10 segundos);
- desvio padrão da média da hora da comutação;
- maior valor de atraso de pacotes, ou seja atraso máximo para esse índice.

Tipicamente cada índice representa 40 execuções da simulação.

Tabela D.5: Exemplo de arquivo exportado pelo simulador

```

NumAssoc:1 Associação Latencia:70 EspLat:1 PerdaPac:0 tipoTeste:Perde Path 0 aos 10
segundos intEnvio: 2 RTOmin: 280 PMR: 3
2; 110,285714285714; 3,61403161162085; 10156,8; 11,634431658414; 98,8
3; 117,43; 9,27497169806997; 10185,6; 11,9264412124756; 124,1
4; 137,674922600619; 18,3523196729435; 10237,2; 1,32664990693178; 168,6
5; 166,284072249589; 34,8782036448599; 10295,4; 0,916515140942188; 225,5
6; 188,011224489796; 54,3813525637593; 10355; 1,34164078538921; 283,1
7; 212,922614575507; 70,3984315557925; 10412,8; 1,83303028188438; 339,8
8; 244,528905289053; 85,6487619238995; 10472,6; 0,916515132812938; 399,4
9; 275,642820114049; 101,873962583639; 10531; 1,34164078538921; 459,6
10; 307,317225950783; 118,721956465999; 10590,6; 1,28062484190136; 520,6
11; 334,224884080371; 138,002126741258; 10649,8; 0,600000011920929; 581,6
12; 360,054859464951; 157,563735955232; 10709,2; 0,979795886163199; 642,8
13; 388,009996970615; 176,023444045704; 10767,2; 0,979795886163199; 703,9
14; 419,629609093429; 192,970057447213; 10825,8; 1,40000000298023; 765,2
15; 450,530179028133; 209,899223132995; 10885,4; 1,28062484771929; 826,4
16; 481,416884040787; 227,118719532581; 10944,2; 1,39999999233655; 887,4
17; 512,328543002432; 244,361935754346; 11003,4; 0,916515149071438; 948,7
18; 543,563056533444; 261,638736312215; 11062,6; 1,28062484771929; 1009,6
19; 574,003118300526; 278,777631514442; 11121,6; 0,80000000372529; 1070,1
20; 604,792310522443; 296,120308378745; 11180,8; 0,979795901371633; 1131,3
21; 635,450696864111; 313,38332858562; 11239,4; 0,916515140942188; 1191,5
22; 666,488091300033; 330,815146826632; 11298; 0,894427189333915; 1252,6
23; 697,087846347607; 348,316141745397; 11357,8; 0,600000011920929; 1314,1
24; 727,692758413462; 365,689395769591; 11416,6; 0,916515140942188; 1375
25; 758,261887659819; 383,152628129923; 11475,6; 1,19999999279777; 1435,7
26; 789,109123434705; 400,663340930083; 11534,8; 0,97979590897585; 1496,6
27; 819,095935603062; 418,485597997947; 11593,4; 0,916515140942188; 1558,2
28; 850,018154119589; 435,643251503068; 11652,8; 0,979795916580066; 1619
29; 880,754248685658; 452,985633988063; 11711,8; 0,600000011920929; 1680
30; 910,690420009438; 470,06934961517; 11770,2; 1,07703294593127; 1739,1
31; 940,703201549504; 487,368552240152; 11829,8; 0,600000011920929; 1799,4
32; 971,083608724389; 504,685428074726; 11889; 1; 1859,9
33; 1001,14593326937; 522,093971263501; 11947,8; 0,600000011920929; 1919,4
34; 1031,23316115702; 539,318719376362; 12007; 1,34164079094254; 1980,3
35; 1061,17823865344; 556,640172037091; 12065,4; 0,916515140942188; 2039,8
36; 1090,72821960479; 573,465347122347; 12123,8; 1,07703297360204; 2098,6
37; 1121,50189035917; 591,126842359777; 12183,6; 0,799999991059303; 2160
38; 1151,48198529412; 608,384907162978; 12243; 1; 2220
39; 1181,39119541875; 625,447079444125; 12301,4; 0,916515157200688; 2279,1
40; 1211,15328976035; 642,667847839022; 12360,2; 1,66132476971339; 2338,8
41; 1241,51918505942; 660,232812944782; 12419,8; 0,600000011920929; 2400
42; 1271,83790048845; 677,447831754959; 12478,4; 1,19999999900659; 2459,1

```

43; 1301,38611941504; 694,645140362875; 12537,2; 1,32664991254786; 2519,2  
44; 1331,74254614292; 711,981284997707; 12596,8; 0,979795901371633; 2580  
45; 1361,16039771851; 729,051954927659; 12654,8; 1,83303028188438; 2638,8  
46; 1391,90518864372; 746,619484839595; 12714,6; 1,56204993441817; 2699,8  
47; 1421,42994991161; 763,749702125787; 12773; 1,34164079094254; 2759,2  
48; 1451,47470087934; 780,934103537579; 12832; 1,5491933404067; 2819,3  
49; 1481,81103195316; 798,386738269038; 12891,6; 0,799999991059303; 2879,5  
50; 1511,74162348877; 815,568078891768; 12950,6; 1,79999999437067; 2939,4  
51; 1541,97110569766; 833,028536084685; 13009,8; 0,600000011920929; 2999,4  
52; 1571,58750165848; 850,106971044669; 13068; 0,894427197663918; 3058,9  
53; 1601,72536905768; 867,572014333223; 13127,2; 0,979795886163199; 3119,3  
54; 1632,15567602041; 885,045008763925; 13187; 1; 3180,1  
55; 1661,67768388106; 902,065521682374; 13244,8; 1,32664992378004; 3239,3  
56; 1692,60125299429; 919,710748029741; 13305; 1; 3300,6  
57; 1721,5347771008; 936,772037652651; 13363,2; 1,32664991254786; 3359  
58; 1752,15618889613; 954,083244589574; 13422,8; 1,32664992378004; 3420  
59; 1781,66919000757; 971,153537662837; 13480,8; 0,979795901371633; 3478,8  
60; 1811,78681394151; 988,456298012645; 13540,2; 0,59999998708566; 3538,7  
61; 1841,71728367278; 1005,81813016484; 13599,4; 0,916515140942188; 3598,9  
62; 1872,04026771392; 1023,40462470568; 13659; 1,34164079094254; 3659,6  
63; 1901,54443537415; 1040,49154159673; 13716,8; 1,60000001005828; 3718,7  
64; 1932,06099716168; 1057,68799653259; 13776,2; 1,39999999233655; 3779,2  
65; 1961,98397976391; 1075,16028921689; 13835,2; 0,979795886163199; 3839,2  
66; 1991,59947073474; 1092,23718906421; 13893,8; 0,600000036756197; 3898,4  
67; 2022,22771619758; 1109,83582667988; 13953,6; 0,799999991059303; 3959,9  
68; 2052,53911162533; 1127,25421889422; 14013; 1; 4019,9  
69; 2082,2468034493; 1144,50082568775; 14071,2; 0,979795886163199; 4079,3  
70; 2111,96796092796; 1161,63886959101; 14130,2; 1,07703294593127; 4139