MODELO GLOBAL

Versão 5.02

LIVRO III

CAPÍTULO A
COMUNICAÇÕES - INTERCÂMBIO DE DADOS

A.1 ARQUITECTURA GERAL

A.2 LIGAÇÕES DOS PARCEIROS AO CENTRO ALTERNATIVO

A.3 COMUNICAÇÕES COM MÓDULOS DE SEGURANÇA (HSMs)

A.1 ARQUITECTURA GERAL

A.1.1 INTRODUÇÃO

OBJECTIVOS DO SISTEMA

O sistema de interligação entre computadores que a seguir se aborda é o preconizado pela SIBS para viabilizar as comunicações entre o seu centro de processamento de dados e os centros dos bancos, centrais de *Clearing* ou outros organismos, com os quais necessita de manter comunicações regulares, independentemente dos tipos ou marcas de máquinas envolvidas.

Este sistema privilegiou o uso do standard X.25, como forma tecnicamente mais simples e segura e economicamente mais acessível de estabelecer uma rede de comunicações "*end to end*" que abranja todos os parceiros nacionais, encontrando-se no entanto já aberto à utilização de TCP/IP (ver ponto **A.1.2.4**).

As aplicações a servir são todas aquelas que implicam o intercâmbio de dados, seja por troca de mensagens ou de ficheiros, entre a SIBS e um Participante no Sistema MB.

A rede X.25 assegura a ligação entre os computadores portadores das aplicações clientes, garantido a transferência dos dados em pacotes. Resta (de acordo com o modelo OSI) assegurar as funções de transporte, controlo de sessão e protocolo aplicacional.

Para cobrir as funções referidas, o Sistema MB cria uma aproximação ao modelo referido, com a construção de duas camadas sobre os serviços X.25.

- **PRT** (Protocolo a *Real-Time*) que implementa as necessárias funções de transporte e controlo de sessão.

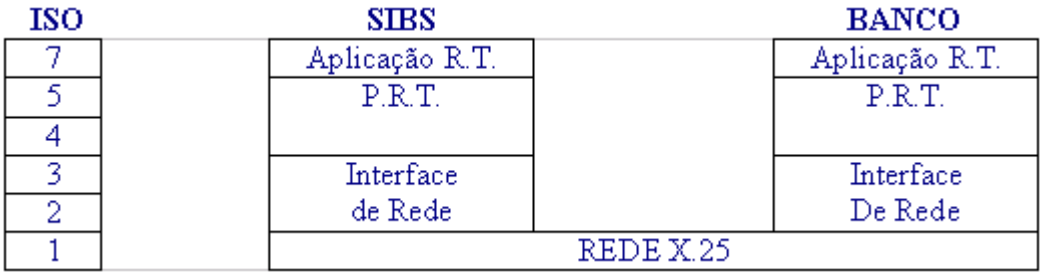
- Camada aplicacional que usa os serviços do PRT e que constrói e interpreta os dados entregues pelo protocolo.

No que diz respeito a teletransmissão de ficheiros, a SIBS define adiante um protocolo próprio (MFT), a utilizar com todas as entidades que necessitem desta funcionalidade.

Nos pontos seguintes é descrita a concepção funcional do sistema.

A.1.2 ARQUITECTURA - REDE, AMBIENTE E MEIOS ENVOLVIDOS

MODELO DE CAMADAS



A nível de rede a comunicação realiza-se em X.25 (puro, isto é, livre dos protocolos dos fabricantes).

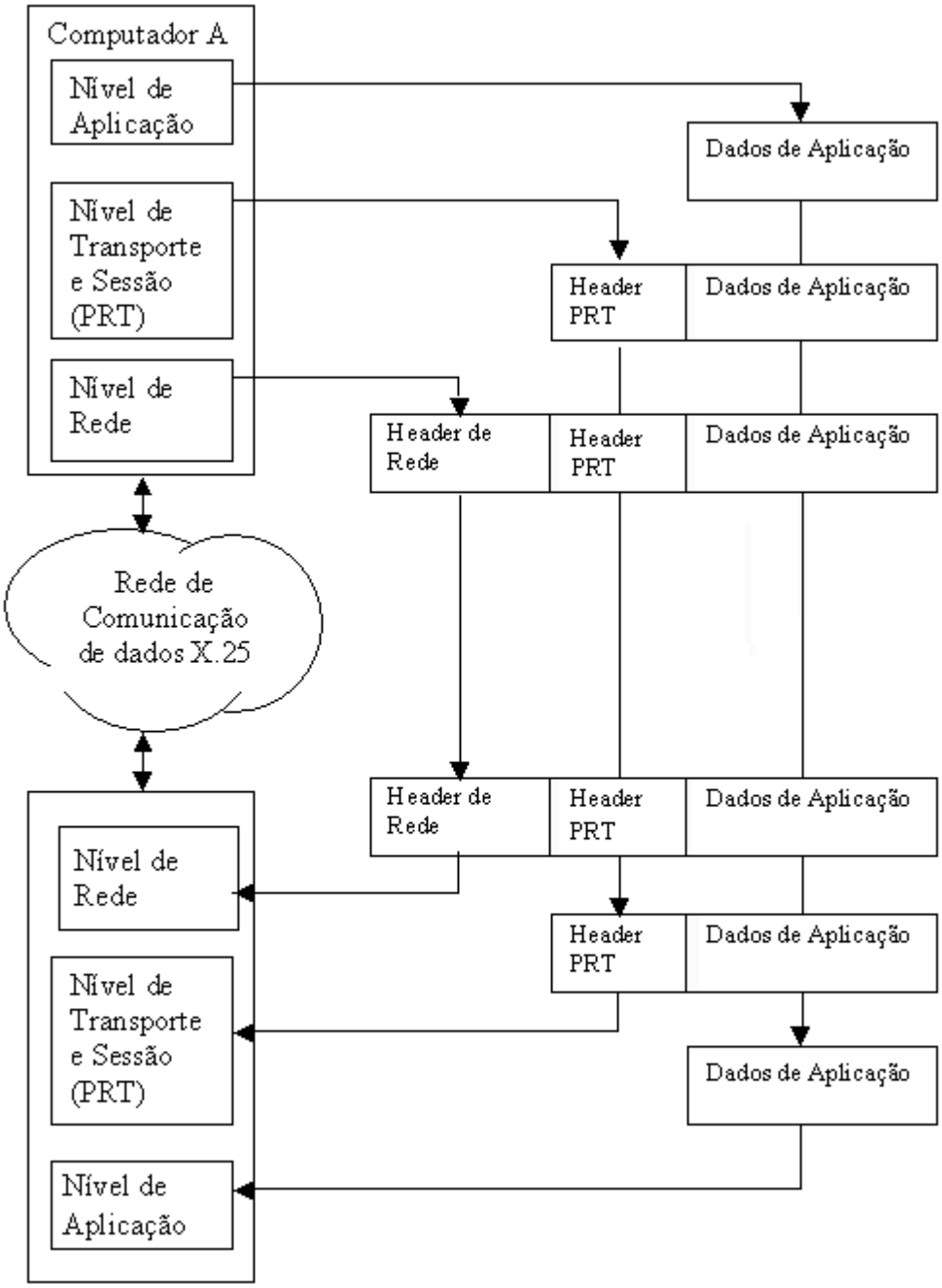
A Rede a usar pode ser uma linha dedicada, a rede privada da SIBS ou a rede pública (combinações destas componentes, ou ainda de redes privadas X.25 dos parceiros, podem também ser consideradas).

O tipo de circuitos X.25 a usar são SVCs que se devem manter permanentemente abertos (a iniciativa de abertura cabe à SIBS, sempre que seja tecnicamente possível; os casos de excepção devem ser discutidos caso a caso).

O protocolo PRT situa-se aos níveis 4 e 5 do modelo OSI, procurando pôr em prática algumas das suas funções e acrescentando outras próprias.

A figura anterior mostra o paralelismo com o modelo OSI, mas só os níveis 1, 2 e 3 são usados integralmente. Está incluído nesta zona o interface X.25 próprio de cada fabricante.

A figura seguinte mostra como se concretiza o diálogo entre os comandos do mesmo nível de ambas as máquinas, através do uso de *Headers* adicionados aos dados recebidos do nível superior.



A.1.2.1 FUNCIONAMENTO GENÉRICO

O nível aplicacional do centro emissor de transacções gera os dados aplicacionais em blocos que constituem mensagens a enviar, e entrega estas ao nível de transporte e sessão (PRT). O PRT gera os procedimentos de diálogo e constrói as mensagens, juntando aos dados o seu *header* e entregando depois cada mensagem ao nível de rede.

Este nível encarrega-se de executar os procedimentos de comunicação, tais como "empacotar" as mensagens, adicionar-lhes o *header* de rede e entregá-las à rede de comunicação de dados.

A rede, encaminha as mensagens para o centro receptor.

O nível de rede do centro receptor processa os pacotes recebidos, subtrai-lhes o *header* de rede e entrega as mensagens recebidas ao nível seguinte.

Este processa e retira o *header* de transporte e sessão e entrega os dados originais à aplicação destino, ficando em sintonia com esta para a devolução da respectiva resposta. A este nível cabe apenas interpretar os dados, de acordo com o protocolo estabelecido com o mesmo nível do centro emissor, e a construção e entrega da respectiva resposta ao nível de diálogo.

O caminho da resposta é inverso ao do pedido.

A.1.2.2 ESPECIFICAÇÕES DO NÍVEL DE REDE

As especificações X.25 são as definidas pela rede pública de comunicação de dados, mas quase todos os fabricantes de equipamentos oferecem o *software* necessário à manipulação deste nível.

Ele corresponde à implementação do primeiro, segundo e terceiro *layer* OSI.

Neste sistema são usadas as seguintes opções deste nível:

- Janela de nível 3 = 2
- Tamanho do pacote = 128 *bytes*
  (pode ser acordado bilateralmente outro tamanho)
- Não usado o campo facilidades do pacote "*call request*"
- Bite D = O
- Bite Q = 0

O "*User data field*" no pacote de chamada, é preenchido com valor a acordar bilateralmente.

A.1.2.3 ESPECIFICAÇÕES DO NÍVEL DE TRANSPORTE E SESSÃO

Este nível usa sempre que possível dois circuitos virtuais para estabelecer a sessão (ou sessões) entre dois sistemas. Um dos circuitos fica reservado a mensagens num sentido e o outro a mensagens no sentido inverso.

O uso de um único circuito para ambos os sentidos pode ser considerado em situações de baixo volume de tráfego, dado que os custos de comunicação são proporcionais ao número de circuitos usados.

A.1.2.4 LIGAÇÕES EM TCP/IP

A crescente disseminação do uso de redes IP, quer nas redes locais que abrangem o acesso aos *mainframes* das entidades, quer nas ligações inter-empresas, bem como a maior capacidade oferecida pelas mesmas e maior versatilidade, levaram a SIBS a abrir a possibilidade de utilização deste protocolo nas comunicações com o seu *mainframe*, possibilitando-a como uma alternativa com vantagens em relação ao *standard* X.25 anteriormente em uso exclusivo.

No entanto, os problemas de segurança que se levantam perante o uso de redes abertas, levaram à adopção de normas de utilização, que garantam o nível de integridade e confidencialidade necessários ao tipo de informação trocada entre a SIBS e os seus parceiros. É neste contexto que se insere o uso de uma rede segura (RSSF), sempre que se pretenda usar os protocolos TCP/IP, entre a SIBS e os seus parceiros.

A SIBS, através de meios próprios ou sub-contratados, efectua a gestão dos mecanismos e filtros de segurança nesta rede.

A.1.2.4.1 ACESSO DOS PARCEIROS À REDE SEGURA

Os Participantes no Sistema MB que pretendem este tipo de ligação, devem solicitá-lo expressamente através dos canais de comunicações usuais entre o Participante e a SIBS, informando as características requeridas (velocidade, linhas de *backup*, localização do acesso, etc.).

Os endereços de rede são fornecidos pela SIBS, através dos seus serviços de comunicações. Cabe aos parceiros efectuar a tradução de endereços para as suas redes internas, se tal for necessário.

A iniciativa de chamada (abertura de *sockets* TCP), cabe:

- *File Transfer* - A qualquer das partes, que pretenda num dado momento enviar ou receber ficheiros;
- *Real-Time* - Sempre à SIBS. É aberto um *socket* para cada sessão RT, o qual é mantido aberto independentemente da frequência de tráfego no mesmo. Em caso de quebra, é também a SIBS a efectuar o restabelecimento.

Seguinte

A.2 LIGAÇÕES DOS PARCEIROS AO CENTRO ALTERNATIVO

A SIBS iniciou em 2002 a preparação de um centro de processamento de *backup*, adiante designado como Centro Alternativo ou CA, com o objectivo de substituir o centro principal em caso de acidente grave neste, assegurando a continuidade imediata dos principais serviços MB.

Dado que o bom funcionamento de muitos desses serviços depende da ligação quer transaccional quer de teletransmissão de ficheiros com os vários parceiros, é necessário garantir também as condições de ligação dos mesmos ao Centro Alternativo, bem como a comutação, sempre que possível sem a sua intervenção.

Para tanto, a SIBS garante a interligação do Centro Alternativo à rede ou redes a que está ligado o Centro Principal, para os protocolos quer X.25 quer TCP/IP.

A.2.1 COMUTAÇÃO DAS COMUNICAÇÕES PARA O CA

A.2.1.1 CIRCUITOS X.25

Os circuitos X.25 a estabelecer do CA para os parceiros (e vice-versa), são os mesmos que são estabelecidos de/para o Centro Principal.

Não é necessária, portanto, qualquer alteração nos recursos ou parametrizações do lado dos parceiros.

A SIBS só activa os recursos de comunicações no CA, após completa paragem do Centro Principal.

- "CALLs" X.25 de iniciativa da **SIBS**:
  Após activação das comunicações no CA, os CALLs são estabelecidos sem intervenção dos parceiros. Para os casos em que a entidade valide o NNA chamador, a SIBS pode fornecer o NNA correspondente ao CA, por forma a que o mesmo possa ser igualmente aceite nessa validação.

- "CALLs" X.25 de iniciativa dos **parceiros**:
  Todas as entidades que efectuam chamadas para a SIBS, devem usar um *HuntGroup* em vez de um NNA simples (a SIBS através do seus serviços de comunicações, informa qual ou quais os *HuntGroups* a usar consoante as Aplicações).
  Em caso de activação do CA, a SIBS desencadeia os necessários procedimentos a nível de rede, por forma a que o referido *HuntGroup* encaminhe para o CA os mesmos CALLs.

A.2.1.2 LIGAÇÕES TCP/IP

Os "*IP address*" das máquinas do CA, são os mesmos que os das máquinas do CP. Dado que não existe funcionamento simultâneo, a rede garante esta facilidade, através da activação de *routers* equivalentes aos principais e de DLCIs de *backup* para o CA.

Esta facilidade permite que seja transparente para os parceiros, o facto de a SIBS usar o CA em lugar do Centro Principal.

- Ligações abertas por iniciativa da **SIBS**:
  Ao activar o CA a SIBS garante o restabelecimento das ligações perdidas no momento do desastre, bem como o início de novas ligações, após intervenção comandada pela SIBS, sem necessidade dos parceiros realizarem alterações das configurações.

- Ligações abertas por iniciativa dos **parceiros**:
  Com a activação dos DLCIs de *backup* e dos *routers* do CA sob controlo da SIBS, as chamadas dos parceiros não têm qualquer alteração. As ligações activas no momento do desastre interrompem-se, restabelecendo-se com o Centro Alternativo após intervenção na rede, comandada pela SIBS, para activação dos interfaces dos *routers* do CA.

A.2.2 SESSÕES PRT

A.2.2.1 SESSÕES RELATIVAS À REDE MB (SIBS -> PARTICIPANTE)

Por motivos relacionados com as aplicações MB, quando executadas no CA (Centro Alternativo), estas apresentam-se, para os parceiros, ao nível do protocolo, com uma identificação diferente daquela que apresentam no Centro Principal.

Assim, os parceiros necessitam de dialogar com o CA (Centro Alternativo) da SIBS, através de sessões *Real-Time* diferentes daquelas usadas para o CP (Centro Principal), o que implica a duplicação de sessões ao nível de PRT.

Porém, dado que não existe utilização simultânea de ambos os conjuntos de sessões, os recursos de comunicações (CICS e VTAM, se existirem) a usar por este segundo conjunto, são os mesmos usados pelo primeiro, uma vez que a "agulhagem" para o CA é de iniciativa da SIBS.

A.2.2.2 SESSÕES RELATIVAS A TRANSACÇÕES PARTICIPANTE -> SIBS

Para as aplicações que a partir dos Participantes no Sistema MB, acedem ao sistema de informação da SIBS, esta deve garantir o funcionamento dos serviços no CA, sem alterações para as primeiras. Por isso, a SIBS replica no CA as mesmas sessões PRT que tem no CP, com as mesmas características.

A comutação para o CA, apenas em caso de desastre e por isso sem o fecho controlado das sessões, pode deixar as mesmas dessincronizadas, bem como algumas mensagens por responder. Neste caso, a ressincronização das sessões, é conseguida com um fecho forçado e nova abertura. As mensagens sem resposta, são entretanto retiradas da sessão, e podem ser de novo enviadas. O processo pode envolver algum controlo manual.

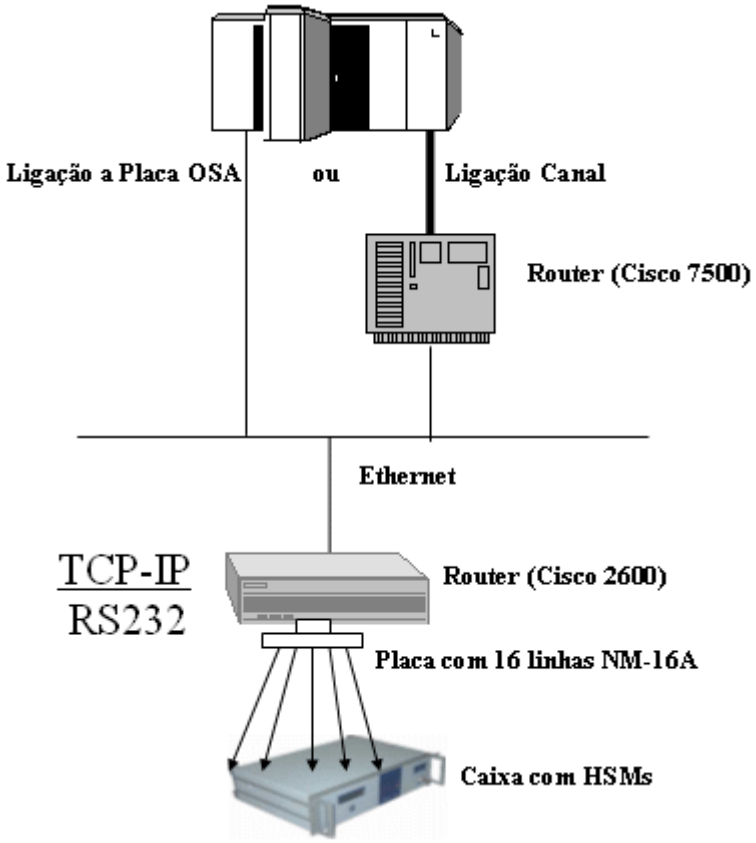
Anterior/Seguinte

A.3 COMUNICAÇÕES COM MÓDULOS DE SEGURANÇA (HSMs)

Pretende-se neste capítulo apresentar, em linhas gerais, os requisitos necessários para estabelecer comunicações em TCP-IP entre Aplicações CICS e HSMs (modelos SSM16K fornecidos pela SIBS), bem como apresentar sugestões de desenho base para a implementação de um interface, que proporcione às Aplicações cliente um acesso fácil e simples.

As sugestões adiante apresentadas, não sendo a única forma de abordar o problema, foram as que serviram de base ao desenvolvimento efectuado para uso na SIBS.

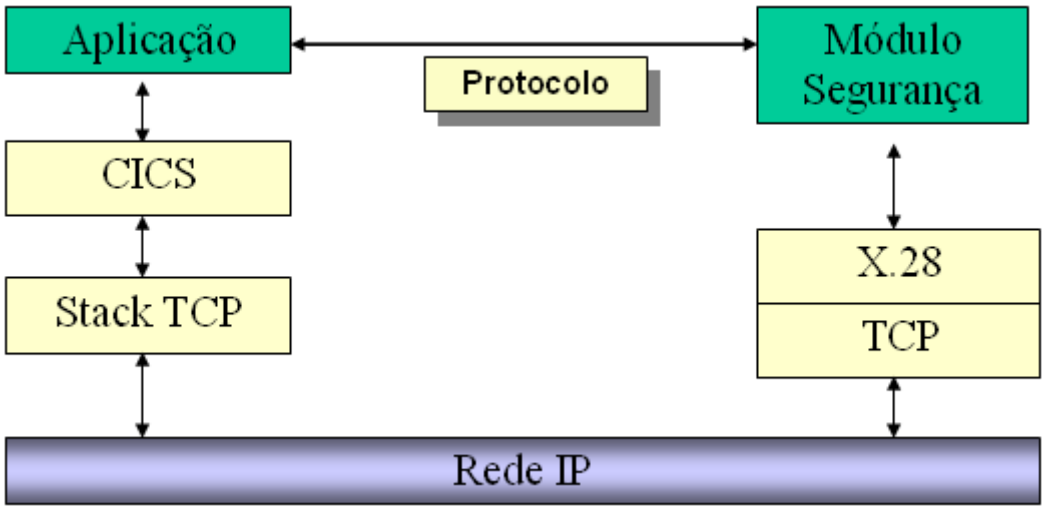
A.3.1 LIGAÇÕES FÍSICAS



O *router* Cisco 2600, deve ter uma porta *Ethernet* e uma placa de 16 linhas assíncronas (NM-16A), cujos cabos terão terminações RJ45.
Os cabos devem ser ligados à portas dos HSMs usando conversores RJ45 para DB9 fêmea.
O *router* deve ser parametrizado, de forma a ter um endereço IP atribuído e uma porta a cada cabo de ligação aos HSMs (assim cada HSM fica identificado em termos de endereçamento por um IP *address/port*).

A.3.2 LIGAÇÕES LÓGICAS

O desenho seguinte mostra as camadas de *software* de base e rede, envolvidas na comunicação entre uma Aplicação CICS e o Módulo de Segurança (SSM 16K).



O rectângulo que representa a Aplicação, pode na prática dividir-se em Aplicação Cliente e uma ou duas camadas que implementam o interface.

Essa(s) camada(s) tem(êm) como funções:

- Tratar o protocolo usado pelos HSMs (envelopagem das mensagens);
- Escolher e controlar o uso dos vários HSMs disponíveis;
- Gerir o manuseamento dos *sockets* TCP a usar;
- Efectuar todos os serviços de interface com o *socket* (*Connect*, *Write*, *Read*, *Close*, etc.).

A.3.3 SUGESTÕES DE IMPLEMENTAÇÃO

A comunicação com um HSM inserido no conjunto de *hardware* atrás apresentado, faz-se por meio de *sockets* TCP, a abrir entre uma transacção CICS e um endereço IP (atribuído ao *Router* que liga ao HSM) e uma porta (atribuída a cada um dos HSMs).

Os serviços de comunicação a implementar, devem usar o "CICS TCP-IP Socket Interface (TCP-IP for MVS)".

Em particular as seguintes funções são necessárias:

INITAPI
SOCKET
CONNECT
WRITE
SELECT
READ
CLOSE

(Consultar Manual "CICS TCP-IP Socket Interface Guide" da IBM)

Com vista a uma implementação modular, sugere-se a criação de uma rotina para efectuar o manuseamento dos *sockets*, capaz de efectuar 4 serviços distintos, sendo-lhe passados como argumentos o serviço requerido e os parâmetros adequados ao mesmo.

A.3.3.1 ROTINA DE COMUNICAÇÃO

O quadro seguinte dá uma ideia dos parâmetros requeridos, e funções envolvidas em cada serviço.

Serviço	Parâmetros	Processo	Funções do *socket*
Abrir *socket*	Id. Destino (HSM)	Fazer mapeamento da id. Destino para um endereço IP e *port* (deve haver uma tabela, para que o cliente não tenha de lidar com endereços). Preparar e efectuar os *calls* necessários ao EZASOCKET. Devolver indicador de sucesso.	INITAPI SOCKET CONNECT
Enviar MSG	Tamanho da MSG MSG	Preparar e efectuar *call*. Devolver indicador de sucesso.	WRITE
Receber MSG	Tamanho do *buffer* *BUFFER*	Preparar e efectuar *call* 'select' (timeout). Verificar se tem dados para receber. Receber dados. Verificar se recebeu tudo (senão volta a receber). Verificar se cabe no *buffer*. Devolver MSG e indicador de sucesso.	SELECT READ
Fechar *socket*	-	Efectuar *call*.	CLOSE

Embora para o caso do HSM, os serviços "enviar MSG" e "receber MSG" pudessem ser reunidos numa só execução (a seguir a um pedido ao HSM tem de haver sempre uma resposta deste), a implementação de dois serviços distintos pode trazer vantagens para outras aplicações.

Esta rotina tem a vantagem de poder ser usada em qualquer das hipóteses adiante sugeridas, bem como em outras aplicações.

A.3.3.2 ROTINA DE INTERFACE COM UM HSM

Esta é a rotina que a Aplicação Cliente deve chamar quando quer enviar um pedido a um HSM e receber a respectiva resposta.

O serviço é só um (sempre que se envia deve-se receber a resposta no retorno) e o argumento deve ser a MSG pedido a enviar/MSG resposta a receber (ou um argumento para o pedido e outro para a resposta).

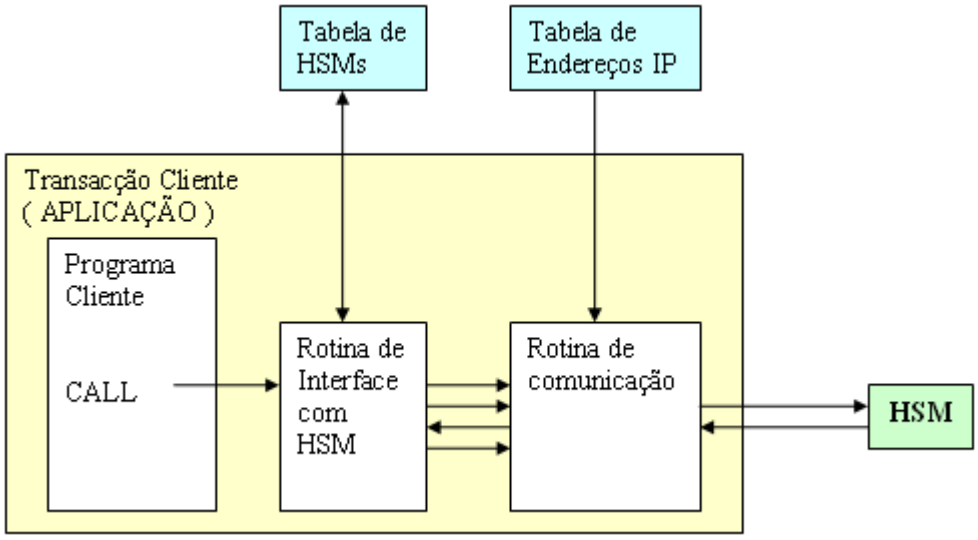
As funções desta rotina podem ser:

- Escolher um HSM a usar (haverá uma pool, mapeada numa tabela); *
- Marcar o HSM escolhido, para não ser usado por outro processo;
- Envelopar a mensagem (colocar DLE STX, *byte sttufing*, DLE ETX, LRC);
- Enviar a mensagem e receber a resposta (apresenta-se mais adiante duas hipóteses de processo de envio, onde se descreve esta parte);
- Desenvelopar a mensagem (o contrário da envelopagem com validação do LRC);
- Libertar HSM usado;
- Devolver a mensagem à aplicação mais indicador de sucesso.

* A tabela de HSMs deve ter, além de uma identificação para cada um, um indicador de uso, possíveis características ou estados diferentes, contadores estatísticos de pedidos, erros, etc. e outra *flag*, que são referidas adiante. A escolha deve ter em conta estes parâmetros, bem como um algoritmo de utilização (rotativo, o primeiro livre, etc.).

Esta rotina também deve ser usada em qualquer das duas hipótese que se seguem.

A.3.3.3 HIPÓTESE 1 - TODO O INTERFACE INCORPORADO NA APLICAÇÃO

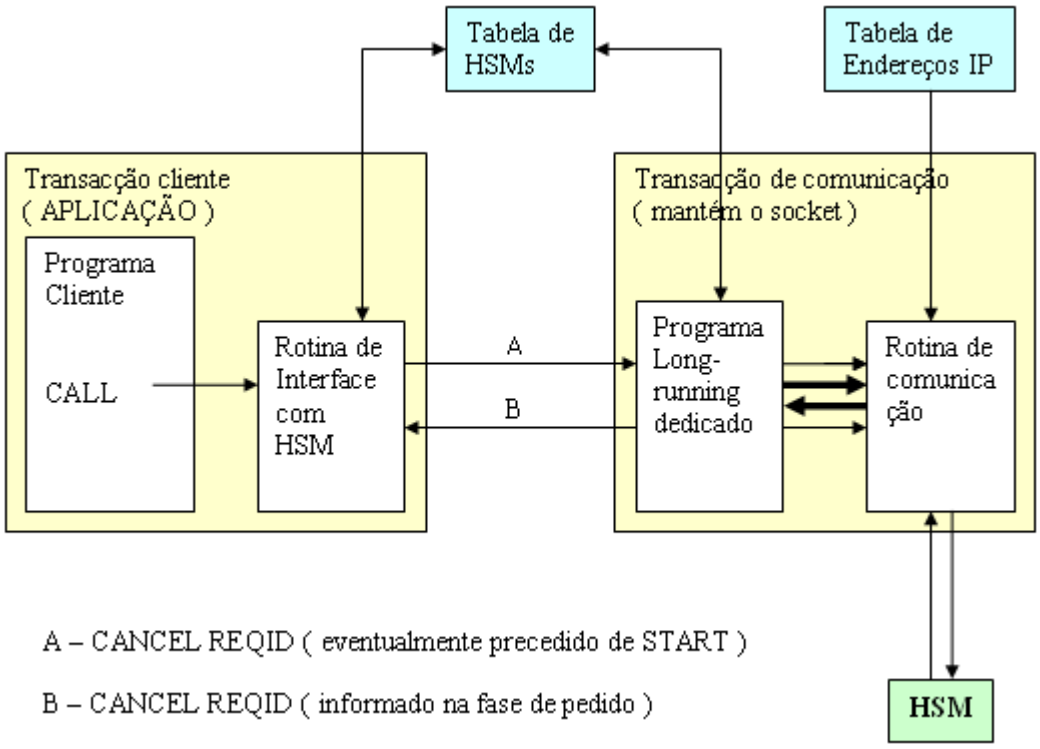


Neste caso, a rotina de interface com o HSM chama directamente 4 vezes a rotina de comunicação (usando os 4 serviços definidos), para abrir comunicação, enviar MSG, receber resposta e fechar comunicação.

O *socket* fica portanto associado à transacção cliente, não havendo outras transacções envolvidas, e sendo usado um *socket* para cada transacção cliente que queira enviar um pedido ao HSM.

Esta hipótese, sendo a mais simples de implementar, não é no entanto a mais "performante", dado que implica uma abertura e um fecho de *socket* por cada pedido ao HSM.

A.3.3.4 HIPÓTESE 2 - TRANSACÇÃO DE COMUNICAÇÃO SEPARADA DA TRANSACÇÃO CLIENTE



Nesta hipótese, temos uma transacção CICS dedicada à comunicação, que, sem fechar o *socket*, pode satisfazer sucessivos pedidos de diferentes transacções cliente.

Existe uma instância desta transacção para cada HSM *, associada portanto a cada ocorrência da tabela de HSMs.

A tabela de HSMs deve ter indicadores de estado (o HSM está disponível, a respectiva Trans. está à espera de trabalho, o HSM está a ser usado, etc.), que permitam a sincronização entre a rotina de interface com HSM e a transacção de comunicação.

* Também é possível fazer um desenho desta transacção, que permita que uma só instância sirva todos os HSMs e todas as Aplicações Cliente. Porém esse desenho torna-se um pouco mais complexo, uma vez que o mesmo programa tem de manusear em simultâneo vários *sockets*.

A rotina de interface com HSM, após preparar a mensagem para enviar, deve usar a seguinte lógica:

- Colocar a MSG na área de passagem para a transacção de comunicação;
- Acordar a transacção de comunicação (CANCEL REQID). Se esta não estiver "viva", arrancá-la por START;
- Esperar pela resposta (DELAY com REQID), por um tempo limitado (*timeout*);
- Obter a resposta na área de passagem da transacção de comunicação.

A transacção de comunicação deve ter a seguinte lógica:

1. Procurar uma ocorrência adequada no tabela de HSMs;
2. Marcar a ocorrência;
3. Abrir a comunicação com o HSM (primeiro serviço da rotina de comunic.);
4. Mudar estado do HSM na tabela para "ocupado";
5. Verificar se tem novo serviço para executar;
6. Se não tiver, passar ao ponto 15;
7. Se o serviço indicar que deve terminar, fechar a comunicação (serviço de fecho da rotina de comunic.) e terminar;
8. Ler a nova MSG a enviar;
9. Enviar a MSG ao HSM (serviço da rotina de comunic.);
10. Receber a MSG resposta " " " " ;
11. Verificar se a resposta é um NACK (se for, voltar a enviar a mensagem);
12. Devolver resposta à rotina de interface com HSM;
13. "Acordar" a rotina (CANCEL REQID indicado na tabela de HSM);
14. Mudar estado do HSM na tabela para "à espera de trabalho";
15. Ficar à espera de novo trabalho (DELAY REQID);
16. Voltar ao ponto 4.

Passagem de dados (MSGs) entre a rotina de interface com HSM e a transacção de comunicação:

- As mensagens podem ser passadas da rotina para a transacção de comunicação e vice-versa de várias maneiras;
- *Buffer* de memória integrado ou associado a cada ocorrência da tabela de HSMs;
- *Queue Temporary Storage*;
- *Queue Transient Data*;
- Etc.

Fim da transacção:

- A transacção de comunicação, tem de ter uma forma de terminar controladamente;
- Uma possibilidade, é receber um pedido especial, que indique que deve terminar;
- Esse pedido pode ser feito por um programa específico, a executar no fecho do CICS, ou a executar por outro processo.

A.3.3.5 PRESSUPOSTOS E POSSÍVEIS DIVERGÊNCIAS

As hipóteses apresentadas acima são no pressuposto de que a comunicação vai ser estabelecida directamente da região CICS onde corre a Aplicação (AOR) para o HSM.

Nada impede que cada AOR, estabeleça no entanto a suas comunicações com um ou vários HSMs, mas cada HSM não pode ser partilhado por diferentes AORs. Significa isto que, cada AOR deve ter uma *pool* de HSMs própria.

Se se pretender ter as comunicações concentradas numa única região CICS, sendo todos os HSMs ligados a essa região e usados pelas diferentes AORs, então a 1ª hipótese não é viável e a 2ª tem de ser adaptada:

- A transacção de comunicação deve correr na região de comunicações, onde também devem residir as tabelas;
- A rotina de interface com HSM também passa a correr na região de comunicações, mas deve ser chamada por LINK e os argumentos têm de ser passados em COMMAREA.

A.3.3.6 GESTÃO DAS TABELAS

As tabelas referidas (tabela de HSMs e tabela de endereços IP) devem ter um suporte com acessos múltiplos, rápidos e no caso da tabela de HSMs, actualizável em cada serviço executado:

- Tabela *assembler*
- GETMAIN *Shared*
- Tabela DB2
- Outro

Para a sua actualização (inserção, modificação, abate ou consulta de ocorrências), deve ser implementada uma transacção ou outro processo equivalente.

No caso de se usarem áreas de memória volátil, devem obviamente ter um suporte em disco para as informações base (a carregar em cada arranque de CICS).

Anterior