Faculdade De Tecnologia De Americana

Curso de Análise De Sistemas e Tecnologia da Informação

SEGURANÇA EM SISTEMAS MAINFRAME

MATHEUS HENRIQUE FIRMINO

Americana, SP

2012

Faculdade De Tecnologia De Americana

Curso de Análise De Sistemas e Tecnologia da Informação

SEGURANÇA EM SISTEMAS MAINFRAME

MATHEUS HENRIQUE FIRMINO

matheus_hf@hotmail.com

Trabalho de conclusão de curso
para obtenção de grau de
Tecnólogo em segurança da Informação

Professor Orientador:

Alexandre Vilodres Oliveira

Americana, SP

2012

FICHA CATALOGRÁFICA elaborada pela

BIBLIOTECA – FATEC Americana – CEETPS

F557s	Firmino, Matheus Henrique Segurança em sistemas mainframe. / Matheus Henrique Firmino. – Americana: 2012. 63f. Monografia (Graduação em Análise de Sistemas e Tecnologia da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza. Orientador: Prof. Alexandre Vilodres Oliveira 1.Segurança em sistemas de informação I. Oliveira, Alexandre Vilodres II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana. CDU: 681.518.6

Bibliotecária responsável Ana Valquiria Niaradi – CRB-8 região 6203

MATHEUS HENRIQUE FIRMINO

SEGURANÇA EM SISTEMAS MAINFRAME

Trabalho de Conclusão de Curso aprovada como requisito para obtenção do título de Tecnólogo em Segurança da Informação no curso de Tecnologia em Segurança da Informação da Faculdade de Tecnologia de Americana.

Banca Examinadora

Orientador: _____
Prof. Alexandre Vilodres Oliveira - FATEC

Convidado: _____
Prof. Marcus Vinicius Lahr Giraldi - FATEC

Presidente: _____
Prof. Carlos Henrique Rodrigues Sarro - FATEC

Americana, 26/06/2012

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter me abençoado em mais essa etapa de minha vida.

Aos meus pais, Carlos e Inês, que sempre me apoiaram em todos os passos de minha vida, pela sua compreensão, atenção, ajuda e carinho ao longo de todos esses anos.

À minha irmã, Giovanna, que sempre esteve disposta a me ajudar, pela sua paciência e carinho.

Aos meus amigos de turma que desde o inicio batalharam junto comigo para chegarmos ao final dessa etapa.

Ao professor Alexandre Vilodres Oliveira, pela orientação e ajuda em meu trabalho.

À empresa IBM pela disponibilização do material para realização deste projeto.

DEDICATÓRIA

A toda minha família e meus amigos,
que sempre estiveram ao meu lado
desde o inicio do curso e desse projeto.

RESUMO

Este trabalho tem por objetivo apresentar como funciona um ambiente Mainframe, tanto a sua estrutura física quanto a lógica, suas principais funcionalidades e recursos, a topologia de rede, os principais protocolos e serviços de segurança. O Mainframe é um computador da classe alta plataforma com grande poder de processamento, e é utilizada por grandes empresas e organizações que possuem um grande fluxo de processamento de informações, assim como bancos que realizam diariamente uma grande quantidade de transações. Neste documento será apresentado como funciona a comunicação no ambiente Mainframe, sua arquitetura de rede, os principais protocolos, apresentando a rede SNA, o funcionamento do TCP/IP, FTP, Telnet, entre outros recursos e principalmente sobre as ferramentas utilizadas para manter a segurança lógica nesses sistemas, seus sistemas de criptografia, e o controlador de acesso RACF.

Palavras chave: Mainframe, Resource Access Control Facility (RACF), System Network Architecture (SNA), Virtual Telecommunication Access Method (VTAM).

ABSTRACT

This research has the objective to present how a Mainframe environment works, physical and logical structures, the main features and resources, the network topology, the main protocols and security services. The Mainframe is a powerful computer with high processing power, it is used by big companies and organizations that work with a high flow of data processing, like banks which perform a high flow of transactions. This document will present how the communication on the Mainframe environment works, the network architecture, the main protocols, the SNA network, the TCP/IP, FTP, Telnet, and especially about the tools used to maintain the logical security in these systems, the cryptography and the access controller RACF.

Keywords: Mainframe, Resource Access Control Facility (RACF), System Network Architecture (SNA), Virtual Telecommunication Access Method (VTAM).

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

API	=	Application Programming Interface
ADSP	=	Automatic Data Set Protection
CCA	=	Common Cryptographic Architecture
CCL	=	Communication Controler for Linux
CDLC	=	Chanel Data Link Control Protocol
CDSA	=	Common Data Security Architecture
CIS	=	Customer Information Control System
CKDS	=	Cryptographic Key Data Store
CLAUTH	=	Class Authority
CPU	=	Unidade Central de Processamento
CS	=	Communications Server
CSM	=	Communications Storage Manager
DASD	=	Direct Access Store Device
DES	=	Data Encryption Standard
DNS	=	Domain Name System
DSMON	=	Data Security Monitor
ESM	=	External Security Facility
ESCON	=	Enterprise Systems Connection
FC	=	Fibre Chanel
FID	=	From Indicator
FISCON	=	Fibre Connection
FTP	=	File Transfer Protocol
Gbps	=	Gigabit por segundo
GRPACC	=	Group Access
HMC	=	Hardware Management Console
HSM	=	Hierarchical Storage Management
HSM	=	Hardware Security Module
HTTP	=	Hypertext Transfer Protocol
IBM	=	International Business Machine
ICSF	=	Integrated Cryptographic Services Facility
IMS	=	Information Management System
ISPF	=	Interactive System Productivity Facitity
I/O	=	Input/Output
IOCDS	=	I/O Control Data Set
JCL	=	Job Control Language

JES	=	Job Entry System
KB	=	Quilobyte
LAN	=	Local area Network
LPAR	=	Logical Partition
LU	=	Logical Units
MB	=	Megabytes
MIPS	=	Milhões de Instruções por Segundos
MVS	=	Multiple Visual Storage
NCP	=	Network Control Program
NASA	=	Administração Nacional da Aeronáutica e do Espaço
NAU	=	Network Accessible Unit
OCSF	=	Open Cryptographic Services Facility
OSA	=	Open Systems Adapter
OSI	=	Open Systems Interconnection
OSN	=	Open System Adapter for NC
PIN	=	Personal Identification Number
PIU	=	Patch Information Unit
PKDS	=	Private Key Data Store
PR/SM	=	Processor Resource/Systems Manager
PU	=	Physical Unit
QDIO	=	Queued Direct I/O
RACF	=	Resource Access Control Facility
RACF	=	RW RACF Report Writer
RH	=	Resquest Heard
RH	=	Response Heard
RRI	=	Request/Response Indicator
RSA	=	Ron Rivest, Adi Shamir and Leonard Adleman
RU	=	Request Unit
RU	=	Response Unit
SAF	=	Security Authentication Facility
SDLC	=	Synchronous Data Link Control
SDSF	=	Spool Display and Search Facility
SE	=	Service Element
SGDBR	=	Sistema de Gerenciador de Banco de Dados Relacionais
SHA	=	Secure Hash Algorithm
SNA	=	System Network Architecture
SNMP	=	Simple Network Management Protocol

SSCP	=	System Services Control Point
SSH	=	Secure Shell
T2.0	=	Tipo2.0
T2.1	=	Tipo 2.1
T4	=	Tipo 4
T5	=	Tipo 5
TCP/IP	=	Transmission Control Protocol/Internet Protocol
TG	=	Transmission Group
TH	=	Transmission Hearder
TSO	=	Time Sharing Option
VTAM	=	Virtual Telecommunications Access Method

SUMÁRIO

1. INTRODUÇÂO

O Mainframe é um computador de grande porte com o intuito de realizar um alto processamento de informações, sua utilização possibilita aos usuários centralizarem todo sua demanda de trabalho em um único equipamento. Atualmente o Mainframe é utilizado por empresas que necessitam de um equipamento que possa realizar um alto processamento de informações, assim como sistemas de bancos, finanças, saúde, seguros, serviços públicos ou governo, como, por exemplo, prover o monitoramento do sistema de segurança de uma cidade.

Com o surgimento de grandes servidores, como Linux, Unix ou Windows Server, que são utilizados para banco de dados, interface web ou fornecer acesso á vários tipos de aplicações, para muitos o Mainframe estava extinto. Devido ao sistema ser eficiente e dificilmente apresentar falhas, ele ainda é o maior poder de processamento de todo o mercado, e ainda é utilizado na maioria dos sistemas de grandes empresas e órgãos públicos pelo mundo.

Uma pesquisa realizada pela Consultoria de Tecnologia PN em 2011,relata que, o Mainframe é o responsável pelo processamento de mais de 80% de todos os dados globais, 95% dos dados financeiros ou de seguros mundial estão em Mainframe e 60% dos dados acessados pela web estão em Mainframe.

Segundo uma pesquisa realizada pela empresa BMC Software em 2011, cada vez mais as empresas tentam integrar o Mainframe à seus diferentes tipos de negócios, ao invés de abandonarem o produto. De acordo com Rich Ptak, principal analista da Ptak, Noel & Associates "Esta plataforma continua a ser a primeira e melhor escolha para uma segura e confiável computação de alto volume" (2011), demonstrando que o Mainframe fica cada dia mais forte no mercado.

Um Mainframe pode ser acessado em qualquer local do mundo se estiver na mesma rede, assim, por exemplo, um usuário do Brasil pode processar suas aplicações que estão rodando em um Data Center que fica nos Estados Unidos. Os usuários finais podem acessar diversas aplicações a partir de suas estações de trabalho. Essas aplicações utilizam o Mainframe como ponto central de processamento das informações, sendo assim, um sistema Mainframe deve estar conectado à um sistema distribuído para que seja possível acessar informações ou aplicações.

Para o gerenciamento desse alto processamento, o sistema de Mainframe utiliza-se de vários recursos, como armazenamento de dados, transações online, monitoramento de logs e recursos do sistema, comunicação do mainframe com diferentes tipos de ambientes e a segurança de acesso às informações e recursos.

No decorrer deste trabalho serão apresentados como funcionam a comunicação em rede, os principais recursos de segurança e como eles trabalham, de acordo com as informações de artigos científicos e manuais retirados da empresa International Business Machines (IBM).

1.1. Organização do trabalho

Este trabalho está organizado em sete capítulos, no capitulo dois é apresentado um histórico do Mainframe e sua evolução durante os anos, no capitulo três é explanado como funciona um Mainframe, tanto sua estrutura física quanto lógica.

No capitulo quatro são apresentados a arquitetura, topologia, os principais protocolos e o funcionamento de uma rede neste ambiente, no capitulo cinco falamos sobre a segurança da rede, os principais recursos e a criptografia no Mainframe. Nos capítulos seguintes, seis e sete, a conclusão e as referências bibliográficas, respectivamente.

2. HISTÒRICO

A tecnologia Mainframe já vendo sendo utilizada há várias décadas, pelas maiores empresas do mundo, como já foi dito anteriormente. Sua história tem início na IBM na década de 1950, quando foi criado seu primeiro sistema.

De acordo com a IBM, ela investiu cerca de US$ 750 milhões na engenharia do projeto, foram criadas 5 novas sedes e foram gastos mais de US$ 4,5 bilhões em fábricas e equipamentos para o desenvolvimento do produto, e na época foi o maior investimento em um projeto comercial privado.

O Mainframe veio para suprir a necessidade das grandes empresas na época de gerenciar e processar todo tipo de informação que os clientes possuíam, por ser uma tecnologia nova e um dos primeiros tipos de computadores, apenas poucas empresas utilizavam tal produto. Em seu início, o Mainframe foi criado especificamente para uma empresa, e com o surgimento de novos usuários e empresas, nem sempre esse equipamento se ajustava às suas necessidades, assim em 1964 foi criado um sistema que se adaptava às necessidades e objetivos de cada empresa, com hardware e software genéricos, o sistema System/360.

O System/360 podia possuir, dependendo do cliente, os seguintes recursos: Um armazenamento principal com tamanho máximo de 16 megabytes (MB); Uma ou duas unidades centrais de processamento (CPUs); Entre um e sete canais de comunicação; Unidades de controle para ligar os canais.

Figura 1: System/360 (IBM, 1964)

Em Agosto de 1972 foi criado o System/370, que entre as maiores diferenças para o seu antecessor, estavam o maior poder de processamento, maior número de canais de transmissão e armazenamento virtual, que podiam chegar à 2 quilobytes (KB) ou 4KB páginas de memória. Esse modelo foi utilizado até 1990, quando deu lugar ao novo sistema System/390, que possibilitava uma capacidade de processamento de 1000 Milhões de Instruções Por Segundo (MIPS), sendo esta a medida de processamento em Mainframes.

O System z9 foi desenvolvido em 2005, apresentando a IBM Fibre Connection (IBM FICON), que é capaz de multiplicar a troca simultânea de dados, assim aumentado a velocidade de transmissão de dados.

Foi criado em 2008 o System z10, que atualmente é o Mainframe mais novo do mercado. Entre as principais características desse equipamento estão, sua maior capacidade de virtualização, melhor conectividade à rede que possibilita rápido acesso aos dados, economia de energia devido ao poder de virtualização e possibilitar o incremento de Linux ao Mainframe.

Figura 2: System z10 (IBM, 2008)

3. FUNCIONAMENTO DO MAINFRAME

3.1. Componentes de Hardware

Diferentemente do Mainframe os computadores de baixa plataforma possuem apenas um processador, conhecido como Unidade de Processamento Central (CPU), por possuir vários processadores, existem várias terminologias diferentes para o mesmo em Mainframe.

Em Mainframe o termo Box faz referencia ao equipamento como um todo, ou seja, todo o hardware. Uma Box é composta por processadores, memória (Central Storage), canais de comunicação, Service Element (SE), sistema de refrigeração e sistema de energia, como mostra a figura número 3:

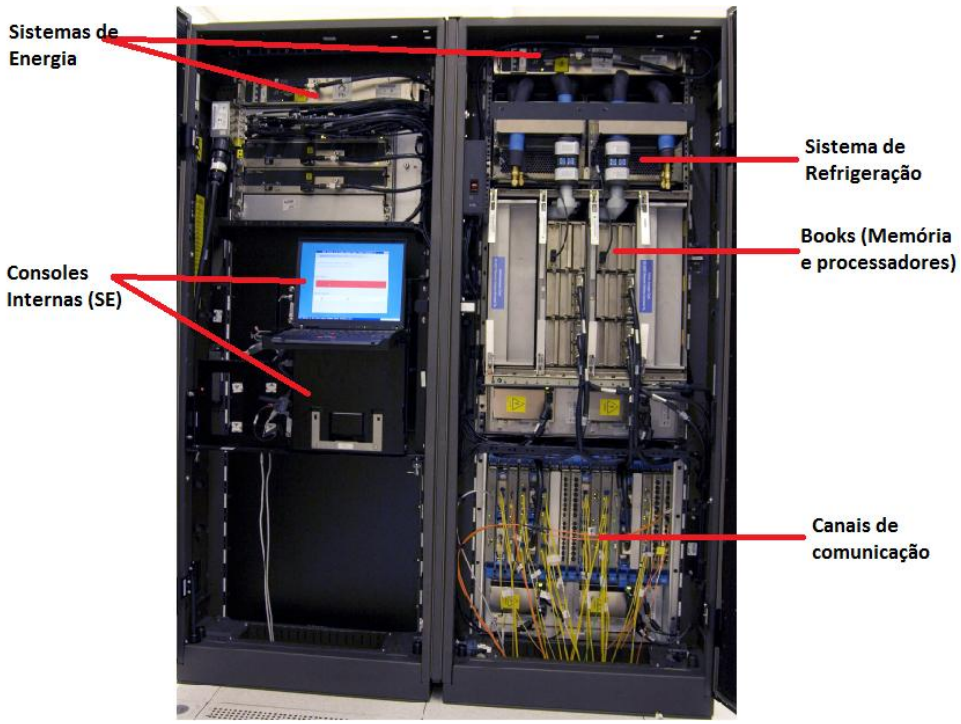

Figura 3: Componentes de uma Box (IBM, 2007)

Processador ou CPU podem fazer referencia a uma Box inteira, ou apenas a um único processador na linguagem técnica em mainframe. Nesta pesquisa utilizaremos CPU para se referir como um único processador e Box para o equipamento como um todo.

Logical Partition (LPAR) significa um espaço lógico utilizado para emular um único sistema, assim LPAR ou sistema tem o mesmo significado em mainframe. Como já foi dito anteriormente, por possuir um grande poder de virtualização, uma CPU pode emular várias LPARes ao mesmo tempo, sendo possível uma única Box possuir vários CPUs e por sua vez vários sistemas.

É possível fazer o compartilhamento de vários tipos de recursos entre diferentes sistemas, como por exemplo, processamento, armazenamento ou utilização de arquivos. O termo Sysplex é uma abreviação para System Complex, que é o responsável por possibilitar esse compartilhamento.

Uma Box contêm os processadores, memória, circuitos de controle e os canais (channels). Atualmente, um Mainframe disponibiliza 1024 canais para entrada e saída (I/O - Input e Output), o que possibilita o alto poder de transmissão de dados. Esses canais são conectados com as Control Units, que possuem uma lógica especifica de trabalho para cada equipamento conectado a ela, por exemplo, a lógica para conexão de uma impressora é diferente de um disco. As Control Units possuem múltiplos canais de conexão em um único equipamento, elas podem se conectar à diferentes devices (dispositivos), como drives de disco, drives de fitas, interfaces de comunicação, impressoras ou até mesmo outros Mainframes.

Podemos ver como funcionam os canais na figura número 4:

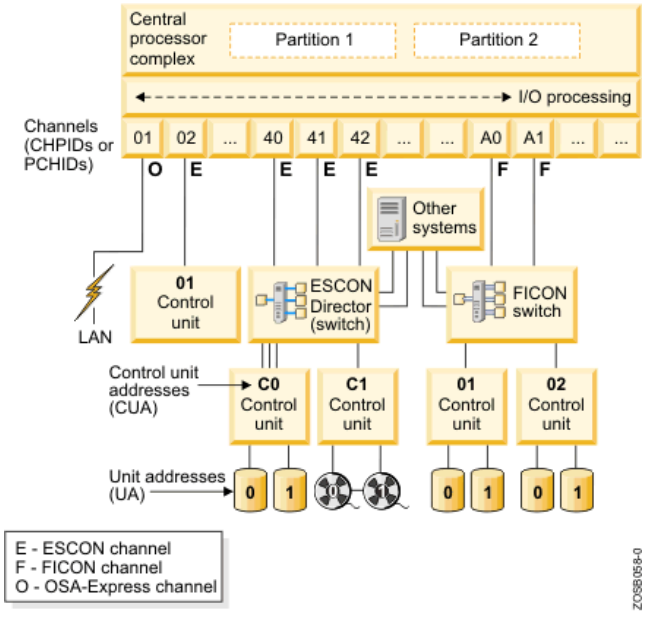

Figura 4: Canais de comunicação de um Mainframe (IBM Redbook, 2011)

O armazenamento de informações no mainframe é feito de duas maneiras, em discos chamados de Direct Access Storage Device (DASD) ou fitas (Tapes). Por serem mais rápidos, volumes de DASD são utilizados para armazenamento de dados ou executar programas, como por exemplo, o sistema operacional ou armazenamento temporário. Uma DASD pode ser compartilhada para diferentes sistemas ou arquivos.

Fitas magnéticas são utilizadas para armazenar informações que não necessitam ser de rápido acesso, como certas informações do sistema, qualquer outro tipo de informação pode ser salvo em tapes. As tapes são gerenciadas por um equipamento chamado de biblioteca, ou em inglês, library. A library possui um robô, que quando é solicitado algum tipo de informação que está gravada em uma tape vai colocar a tape no drive, e assim o sistema poderá ler esses dados.

Na figura número 5 podemos ver uma library vista do lado de fora e seu robô trabalhando do ladro de dentro:

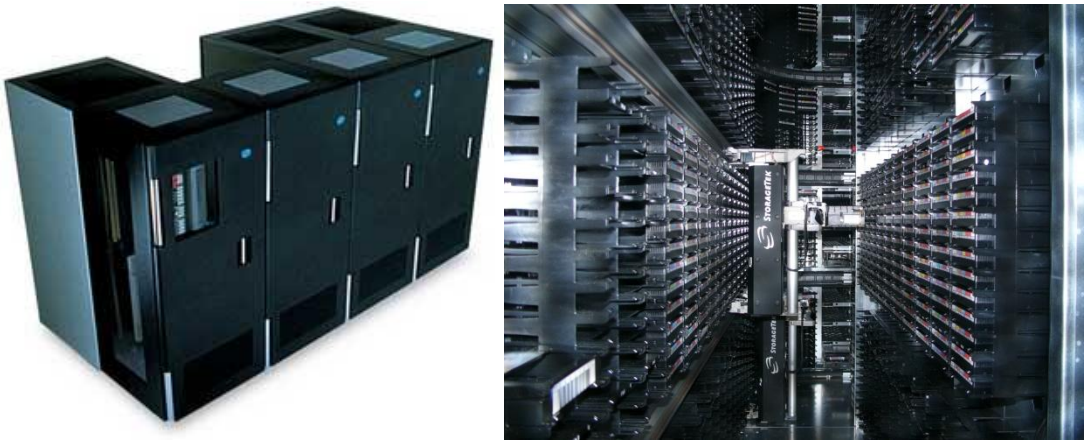

Figura 5: Tape library e seu robo trabalhando (IBM, 2010)

Todo Mainframe possui um monitor acoplado a ele, que é o seu terminal de comandos. Esse terminal é essencial para que o engenheiro possa realizar reparos e manutenções no equipamento, tais como desligar e ligar o Mainframe, ou atualizações. Além de possuir esse monitor, o mainframe pode ser acessado remotamente, para que seja possível a realização de tarefas, tanto na Box, como em uma determinada LPAR.

Para o gerenciamento de processamento e hardware de uma, ou várias Box, o Mainframe oferece um recurso chamado Hardware Management Console (HMC) que se comunica remotamente com a máquina. Este recurso possibilita uma interface entre usuário e Mainframe, utilizando aplicativos em Java. As principais funções do HMC são: gerenciar as partições lógicas, divisão de processamento da box, ativar ou desativar uma partição e controlar os canais de comunicação. A figura número 6 demonstra um exemplo de uma interface HMC:

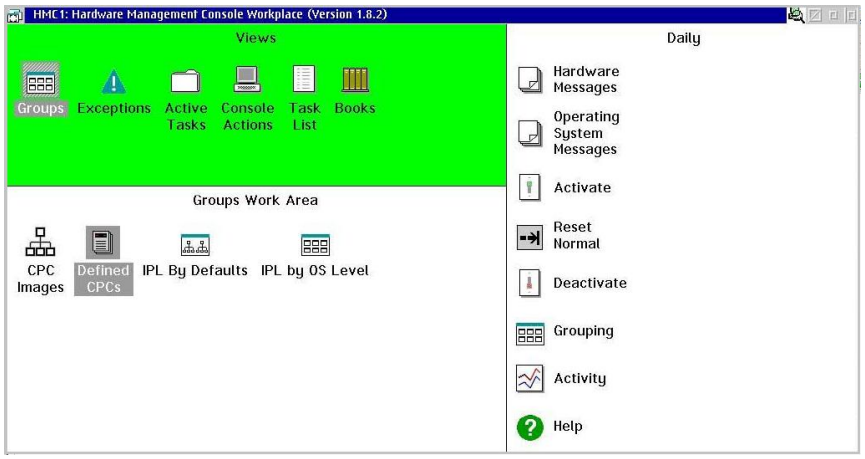

Figura 6: Interface HMC (The Z-Age, 2011)

3.2. Estrutura lógica

O sistema operacional atualmente utilizado é o z/OS, que possibilita a utilização centenas de diferentes programas e interação com os usuários. Para ser possível entender melhor o z/OS são necessários alguns conceitos básicos que serão dispostos nessa seção.

No passado um sistema z/OS era também conhecido como MVS, sigla para Multiple Vistual Storage. Atualmente o z/OS ainda proporciona todos os serviços do MVS, porém como muitas novas funções, incluindo suporte para interfaces UNIX. O z/OS basicamente adicionou um ambiente UNIX através de um componente chamado z/OS UNIX System Services, permitindo que um sistema seja executado em diferentes plataformas. Assim, o MVS e o z/OS UNIX compõem um ambiente de z/OS.

Como dito anteriormente, o Mainframe disponibiliza várias partições lógicas, que podem ser utilizadas para executar diferentes sistemas, sendo assim o z/OS pode ser instalado em qualquer uma dessas partições.

Cada tarefa que o sistema precisar processar é chamado de job, como por exemplo, um usuário utilizando o sistema, programas sendo executados, ou serviços de jobs agendados (Batch). Atualmente o z/OS possibilita que vários jobs sejam executados ao mesmo tempo, assim o sistema distribui espaços de memória para cada trabalho, conhecidos como Address Space. O adress space é único para cada tarefa no sistema, e a alocação de memória é diferente para cada tipo de trabalho.

O z/OS possibilita vários tipos de programas e aplicações (subsystems), que também podem ser chamados de Started Tasks ou apenas Tasks, sejam utilizados no Mainframe, como por exemplo: DB2, IMS, CICS, HSM, JES, automação, programas para gerenciamento de rede e segurança, que serão apresentados nos próximos capítulos. Diferente do job, que executa, realiza sua atividade e depois completa, uma started task está sempre rodando pelo tempo que for desejado. Serão apresentados os principais subsystems nesta sessão.

O DB2 é um Sistema Gerenciador de Banco de Dados Relacionais (SGDBR), baseado em SQL, que foi produzido pela IBM em 1983. O DB2 foi utilizado por muito tempo somente em mainframes, mas com o tempo, com a possibilidade de interação com outros sistemas, atualmente esse banco de dados é utilizado no mainframe, porém funcionam em servidores Unix, Windows, ou Linux.

Customer Information Control System (CICS) funciona como um servidor de transações online, que possibilita rápido e alto processamento de volume de informações online. Atualmente, CICS é responsável pelo processamento de mais de 30 bilhões de transações por dia e representa valores de negócios de 1 trilhão de dólares por semana, segundo Cezar Taurion em seu livro "Bar do Z: um bate papo informal sobre mainframes". O CICS pode ser utilizado para lançamento de folhas de pagamento, gerenciamento de impressoras, transações bancárias, entre várias outras atividades.

Information Management System (IMS) foi desenvolvido pela IBM em 1966 com o intuito de gerenciar o inventário de informações da Administração Nacional da

Aeronáutica e do Espaço (NASA), para o programa Apollo. IMS é um banco de dados hierárquico. Além de ser um gerenciar banco de dados, o IMS funciona como um gerenciador de transações que interage com o usuário final por TCP/IP.

Hierarchical Storage Management (HSM) é um gerenciador de armazenamento de dados, como já explicado anteriormente, o mainframe utiliza-se de discos e fitas para armazenamento, toda informação que necessita ser de rápido acesso são armazenadas em discos, com o tempo, se essa informação não é utilizada frequentemente, é salva em fitas. O HSM é responsável por gerenciar essa transmissão entre discos e tapes, assim quando uma informação que esta em fita é necessária, ela é transmitida para o disco para poder ser utilizada. Além disso, o HSM é responsável por backup, remoção e recuperação de informações.

Job Entry System (JES) é responsável pela entrada e saída de trabalhos (jobs) no sistema. O JES recebe os trabalhos, processa as informações e controla o seu processamento de saída. Existem duas versões utilizadas atualmente, sendo o JES2 e JES3, que trabalham similarmente. JES é uma das principais ferramentas do z/OS, e precisa estar funcionando corretamente para que qualquer tarefa seja executada no Mainframe, desde um usuário se conectando ao sistema, até um job de alta complexidade.

Job Control Language (JCL) é uma linguagem de programação utilizada para a escrita de jobs normais ou de batch. Processamento em batch são jobs que executam trabalhos no Mainframe, com mínima interação humana e que são agendados para serem executados em determinados horários, conforme a necessidade do usuário. Quando um job necessita entrar no sistema, o JES é responsável por ler o JCL e executar o job.

O z/OS oferece alguns recursos para interatividade entre usuário e maquina, o Time Sharing Option (TSO) permite que os usuários entrem no sistema, acessem os programas instalados e utilizem vários comandos no mainframe. Visando uma maior interatividade para o usuário, é utilizado o painel Interactive System Productivity Facility (ISPF), a partir dele é possível acessar vários painéis, arquivos e aplicações de forma mais instrutiva. Dentro do TSO/ISPF é possível acessar o Spool Display and Search Facility (SDSF), que ajuda a gerenciar várias funções do JES,

sendo assim possível acessar a log do sistema, controlar impressoras, monitorar, cancelar ou pausar os jobs, entre várias outras funcionalidades.

4. TOPOLOGIA E ARQUITETURA DA REDE

Com o passar do tempo o Mainframe foi se adaptando as mudanças do mercado e se ajustou para trabalhar com todo tipo de ambiente. Hoje em dia o Mainframe tem a possibilidade de se comunicar com diferentes tipos de plataformas, e devido ao grande numero de informações e usuários utilizando o sistema, ele deve possuir um modo de comunicação muito eficaz e seguro.

Os Mainframes trabalham em grandes Data Centers, e são acessados remotamente pelos usuários. Devido ao grande numero de transações realizadas e a importância dos dados, a rede deve ser muito bem estruturada e segura. Para se ter uma ideia da importância dessa rede, o mainframe é responsável pelo processamento das transações bancárias da maioria dos bancos do mundo, assim quando um cliente está retirando ou depositando dinheiro em um caixa eletrônico, por traz disso, o mainframe esta processando e enviando essas transações.

4.1. Topologia

O Mainframe trabalha a partir da topologia de rede estrela, sendo que o ponto central é o próprio Mainframe, onde todo processamento da rede é realizado, como demonstra a figura número 7, vários terminais conectados ao ponto central:

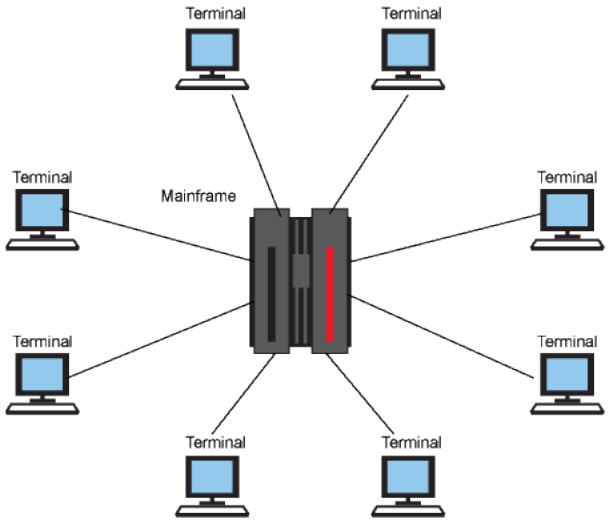

Figura 7: Topologia de rede Mainframe (Dan Orlando, IBM, 2011)

Devido ao seu grande poder de processamento, essa topologia é perfeita para a rede Mainframe, garantindo que todo o processamento seja realizado com o nível máximo de controle.

Uma rede Mainframe é composta por linhas de comunicação, terminais, impressoras, modems, controladoras, switches, e o próprio Mainframe. A rede Mainframe pode se conectar a switches para cabos de fibra ótica ou se conectar a rede utilizando switches convencionais, onde é possível a comunicação com diferentes tipos de dispositivos.

4.1.1. Canais ESCON e FICON

As principais formas de comunicação são: Enterprise Systems Connection (ESCON), que é uma tecnologia criada pela IBM para conexão entre mainframes, é um cabo de fibra óptica, duplex, pois pode se comunicar em ambas as direções, e serial, enviando um bit de cada vez. Além desse cabo, é utilizado o Fibre Connection (FICON), que possui um poder de transmissão de dados muito mais alto.

Os canais ESCON e FICON se conectam a uma única device (dispositivo) ou em uma porta de um switch. Os switches dos Mainframes mais modernos conectam os canais e as Control Units, podendo ser compartilhado por diferentes sistemas. Para fazer a tradução dos endereços físicos de I/O para os endereços lógicos é utilizado um arquivo de controle chamado de I/O Control Data Set (IOCDS), que possui todas as informações para a comunicação lógica em um sistema.

A figura número 8 demonstra dois modelos de switches, IBM System Storage SAN768B-2 e SAN384B-2, que suportam conexões FICON e ESCON, com capacidade para canais de fibra (Fibre Channel - FC) de 8 e 16 Gigabits Por Segundo (Gbps):

Figura 8: Switches de fibra ótica SAN768B-2 e SAN384B-2. (IBM, 2011)

Esses switches conectam-se as Control Units que irão se conectar a diferentes dispositivos, tais como controladoras de disco e fitas, impressoras e outros tipos de dispositivos, como mostra a figura número 9, onde ESCON Director é um switch de fibra ótica:

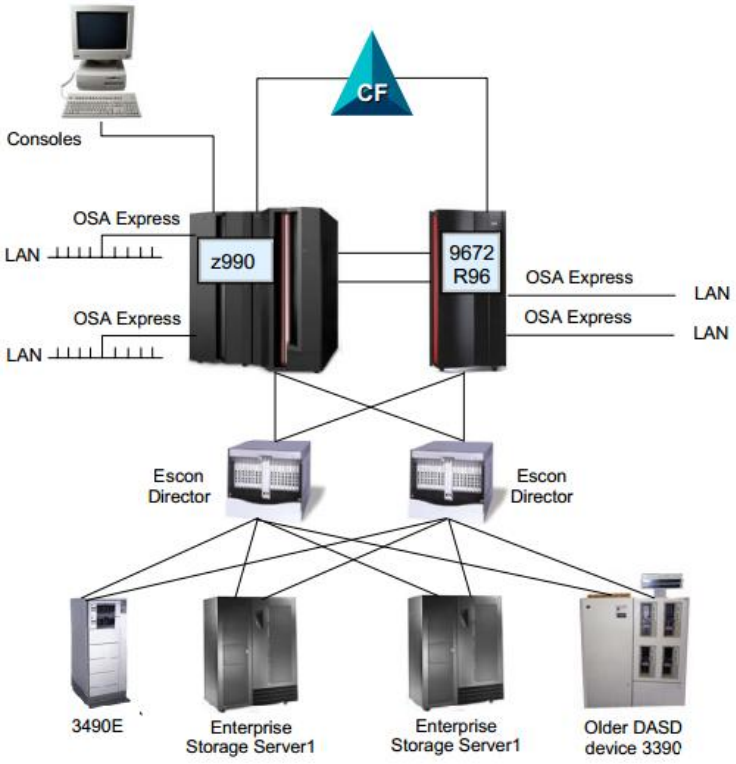

Figura 9: Conexões do Mainframe via switches ESCON ou FICON (IBM, 2006)

4.1.2. Adaptador OSA

Open Systems Adapter (OSA) é um controlador de rede que pode ser instalado em um mainframe, especificamente, nas portas de I/O. Esse adaptador possui vários recursos de hardware e suporta diferentes tipos de protocolos de transporte de rede. O cartão OSA integra a Control Unit e o dispositivo no mesmo hardware. Atualmente existem as seguintes versões: OSA-2, OSA-Express e OSA-Express2. As versões de cartão Express utilizam um método muito mais rápido de acesso, chamado de Queued Direct I/O (QDIO). Além disso, as principais melhorias do Express são a conectividade, largura de banda, transferência de dados, a disponibilidade da rede, confidenciabilidade e recuperação.

Network Control Program (NCP) foi criado pela IBM com o intuito de suportar acesso a dispositivos antigos por programas que utilizam o Virtual

Telecommunications Access Method (VTAM). O NCP roda em um programa chamado de Communications Controler for Linux (CCL). O CCL é a maneira mais fácil de migrar controladoras de redes System Network Architecture (SNA) antigas para dispositivos mais modernos. Open System Adapter for NCP (OSN) é um adaptador para o OSA-Express2 que permite que o OSA se comunique com o NCP, utilizando um canal chamado Channel Data Link Control Protocol (CDLC). É demonstrado na figura número 10 um exemplo dessa conexão:

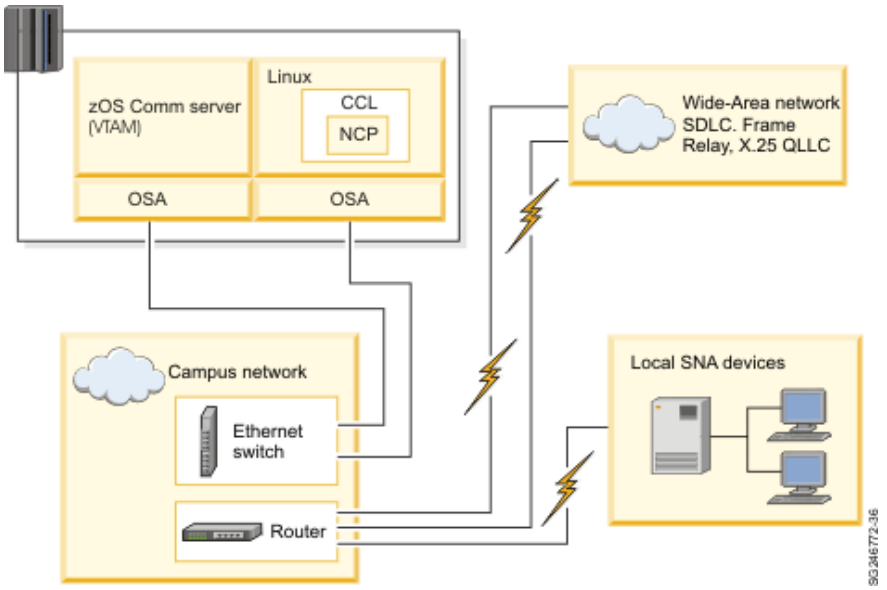

Figura 10: Exemplo conexão CCL,NCP (IBM Redbook, 2006)

4.2. Arquitetura da rede

4.2.1. Protocolo SNA

No passado, os Mainframes utilizavam um protocolo de comunicação chamado de System Network Architecture (SNA), criado pela IBM em 1974. Com o crescimento da utilização do protocolo TCP/IP por todas as grandes corporações e computadores de pequeno porte, hoje em dia é possível a integração ente o TCP/IP e o SNA em Mainframes. O SNA define os procedimentos e estruturas de comunicação entre aplicações ou entre estas aplicações e um terminal.

Os componentes de hardware do SNA consistem em hosts, processadores, controladores de comunicação, controle de dispositivos finais da rede, terminais e impressoras. O software é composto pelo VTAM, que controla o fluxo de dados e

será mais aprofundado na sequência deste capítulo, programas de aplicação que controlam transações e programas de gerenciamento de redes.

Todo componente em uma rede SNA possui seu próprio endereço que o distingue dos outros da mesma rede, cada um desses componentes que possuem um endereço são chamados de Network Accessible Unit (NAU), que são divididos em: Unidades Lógicas (Logical Units, ou LU), Unidade Física (Physical Unit, ou PU) e o Ponto de Controle de Serviços do Sistema (System Services Control Point, ou SSCP).

A LU fornece o ponto de acesso em que o usuário irá se conectar a rede, que são divididas em LU0 (utilizado para acessar a aplicação com poder de livre formatação), LU1 (acesso Remote Job Entry, RJE, são os termos de envio de jobs para o mainframe), LU2 (acesso à terminais), LU3 (acesso à impressoras) e LU6.2 (permite acesso à aplicações com diferentes normas de utilização).

A PU define os dispositivos físicos da rede SNA, como terminais, impressoras, sistemas de comunicação, entre outros. É dividida nas seguintes PUs: PU tipo 2 (responsável por controladoras Control Unit), PU tipo 2.1 (utilizada pela LU6.2), PU tipo 4 (responsável por controladoras de comunicação) e PU tipo 5 (utilizada apenas no mainframe).

O SSCP tem a finalidade de gerenciar a rede SNA, para que seja possível estabelecer e controlar interconexões entre usuários. É responsável por ativar, controlar e desativar recursos subárea da rede. Para poder controlar e prover os serviços, o SSCP estabelece sessões entre os componentes e a rede, por exemplo, o SSCP usa uma sessão para uma aplicação poder localizar e estabelecer uma sessão de comunicação com um determinado destino.

Assim como o protocolo OSI ou TCP/IP, o SNA também é dividido em camadas. Ele é composto por 7 camadas, sendo elas Transaction Services (Serviço de Transações), NAU Services (Serviços NAU), Data Flow Control (Controle de fluxo de dados), Transmission Control (Controle de transmissão), Path Control (Controle de Rotas), Data Link Control (Controle de enlace) e Physical Control (Controle Fisico).

A camada de Transaction Services é responsável pela interação entre LUs de usuários e LUs de programas, fazendo com que seja possível o acesso a diferentes aplicações. NAU Services faz o gerenciamento dos serviços SSCP, LU e PU da rede. O Data Flow Control permite a sincronização do fluxo entre as partes que se comunicam. Transmission Control é responsável por controlar sessões, nesta camada os dados são criptografados quando exigidos. A camada de Path Control faz o roteamento dos dados entre origem e destino, controlando assim o tráfego e congestionamento da rede. Data Link Control gerencia e executa a transmissão de dados de forma segura pelas rotas da rede. A camada Physical Control é responsável por controlar as interfaces físicas por onde estão conectados os meios de transmissão.

É possível comparar protocolos TCP/IP, OSI, SNA e suas respectivas camadas, a partir da figura número 11:

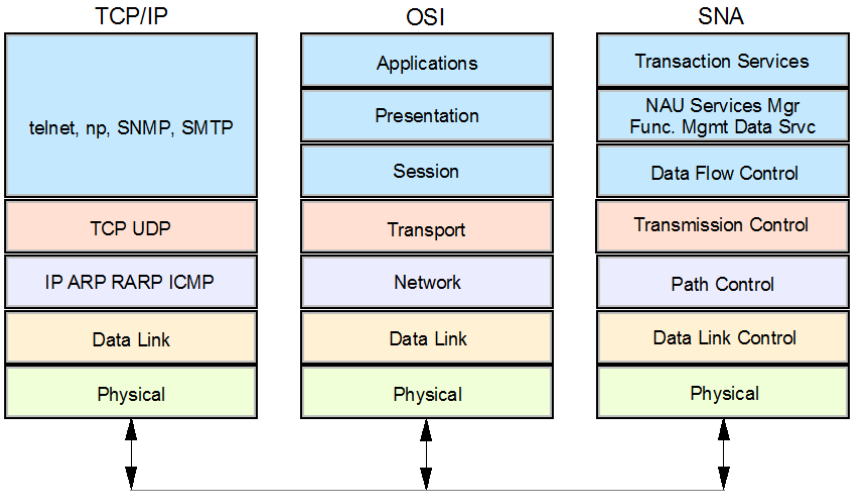

Figura 11: Protocolos TCP/IP, OSI e SNA (IBM, 2006)

Assim como uma rede convencional, a rede Mainframe também possui nós (nodes), os nodes são responsáveis por enviar e receber dados na rede. Links (conexões) são componentes que conectam nodes adjacentes, e juntos são responsáveis pela transmissão de dados da rede. SNA nodes são diferenciados a partir do tipo de componente e as funções que ele realiza. Em SNA existem 4 tipos de nodes, que são equivalentes às PUs mencionadas nesta sessão:

- Tipo 5 (T5): Esse node está localizado apenas no Mainframe. O responsável por executar as funções do node T5 é o Communications Server (CS).

- Tipo 4 (T4): É o node controlador de comunicação ligado aos nodes periféricos, através de linhas de comunicação para outro controlador ou Mainframe.

- Tipo 2.0 (T2.0): Esse node está ligado ao Mainframe ou ao controlador de comunicação (control Unit), pode se conectar à terminais, impressoras ou outros tipos de dispositivos.

- Tipo 2.1 (T2.1): É um node ligado ao Mainframe, Control Unit ou à outro node periférico.

4.2.2. Protocolo SDLC

Synchronous Data Link Control (SDLC) é um protocolo da camada de Data Link Control do SNA. Como já dito anteriormente, essa camada possibilita o trafego seguro de dados na rede, e isso é possível devido ao protocolo SDLC. O SDLC suporta um grande número de tipos de conexões e topologias, podendo ser utilizado com conexões multipoints ou point-to-point, transmissões half-duplex ou full-duplex e em redes packet-switched ou circuit-switched.

Esse protocolo identifica dois tipos de nodes na rede: os primários e secundários. Nodes primários controlam as operações das outras estações, chamadas de secundárias. Os primários organizam os secundários em uma ordem, assim os secundários podem transmitir seus dados quando houver dados de saída. Os nodes primários são responsáveis por configurar e restabelecer conexões que caírem, enquanto que os nodes secundários são responsáveis por transmitir os dados. Esses nodes podem ser conectados pelas seguintes configurações:

Point-to-Point: Envolve apenas dois nodes, um primário e outro secundário.

Multipoint: Envolve apenas um node primário e múltiplos secundários.

Loop: Liga o node primário a múltiplos nodes secundários, conectando-se apenas ao primeiro e ao ultimo node do conjunto de nodes secundários.

Hub go-head: Envolve canais inbound e outbound. O node primário utiliza canais outbound para poder se comunicar com o node secundário, enquanto que os nodes secundários utilizam canais inbound para receber solicitações dos primários.

4.2.3. Pacotes na rede SNA (PIU)

Em uma rede TCP/IP, a unidade enviada pela rede é chamada de pacote (packet), que incluem os dados (payload), o IP e o cabeçalho TCP. Os cabeçalhos são utilizados para rotear o pacote e gerenciar a sessão TCP.

No protocolo SNA, a unidade que é transferida na rede é chamada de Path Information Unit (PIU). As mensagens são enviadas para uma unidade NAU, e os endereços são atribuídos à essas unidades físicas ou lógicas quando são ativadas.

O PIU possui três campos que são utilizados pela NAU para traçar as rotas dos dados na rede, como demonstra a figura número 12:

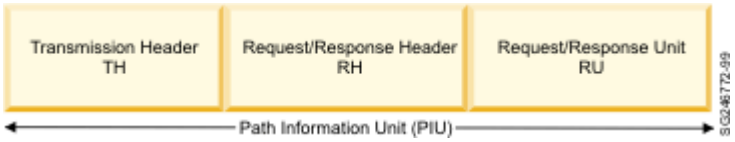

Figura 12: Path Information Unit (IBM Redbook, 2006)

Transmission Header (TH), ou cabeçalho de transmissão: É utilizado para rotear as mensagens através da rede. O TH possui as informações das rotas para transporte na rede. O SNA define diferentes tipos de formatos de TH e identifica os formatos a partir dos tipos de Form Indicator (FID).

Os Transmissions Headers variam de acordo com tipo de FID. Os dois tipos de FID são:

-FID2: Esse formato é utilizado para traçar a rota das informações entre nodes de sub-redes e node periféricos adjacentes.

-FID4: Formato utilizado para traçar a rota das informações entre os nodes das sub-redes.

Request Header (RH), ou cabeçalho de requisição: Cada requisição enviada pelo NAU começa com um Request Header. O RH é um campo de 3 bytes que identifica o tipo do dado, associado à um Request Unit (RU) e também especifica os protocolos da sessão.

Request Unit (RU), ou unidade de requisição: O RU é um campo de tamanho variável, que contém informações do receptor ou comandos de SNA, que é responsável por controlar as operações da rede.

Response Header (RH), ou cabeçalho de resposta: Cada requisição enviada pelo NAU possui um Response Header. Assim como o Request Header, é um campo de 3 bytes que identifica o tipo do dado, associado à um Request Unit (RU). Um bit chamado de Request/Response Indicator (RRI) diferencia o tipo de cabeçalho. O NAU receptor indica qual resposta deve ser retornada ao remetente, positiva ou negativa, definindo em um único bit.

Response Unit (RU), ou cabeçalho de resposta: A Response Unit possui informações da requisição. Respostas positivas aos pedidos geralmente possuem de 1 a 3 bytes, para identificação do pedido. Response Units negativas possuem de 4 a 7 bytes de comprimento e sempre retornam uma resposta negativa.

4.2.4. Virtual Telecommunication Access Method

Virtual Telecommunication Access Method (VTAM) é uma das principais ferramentas de rede do Mainframe. Baseado no protocolo SNA, ele fornece a comunicação para o transporte de dados entre aplicações e usuários do Mainframe, controlando a transferência de informações entre os canais e os adaptadores OSA. O VTAM também possui o recurso Application Programming Interface (API), que permite o desenvolvimento de aplicações que se comunicam usando o SNA.

O VTAM é responsável por várias tarefas em uma rede, por exemplo: monitorar e controlar a ativação e conexão de recursos, estabelecer conexões e gerenciar o fluxo das sessões, fornecer suporte ao terminal interativo (TSO) e oferecer suporte para recursos locais ou remotos. Como já mencionado neste capitulo, cada sessão SNA é chamada de Logical Unit (LU). Uma sessão estabelecida do VTAM é chamada de sessão LU-to-LU.

Uma rede VTAM possui como principais elementos os programas de aplicação VTAM, que estão associados às LUs; o próprio VTAM, na PU tipo 5 ou SSCP; Uma ou mais controladoras de comunicação, nas PUs de tipo 4; os terminais, associados com as LUs; e os links de dados (Data Links), que conectam as PUs ao VTAM e às controladoras de comunicação.

Todo sistema z/OS com VTAM que utiliza o SNA é denominado de domínio. Para estabelecer uma sessão entre domínios é necessário possuir conexões físicas (canais de comunicação, OSA e linhas de comunicação) para ser possível definir uma conexão lógica entre nodes de sub-redes (equivalentes aos nodes T5 e T4). Uma Transmission Group (TG) é uma conexão ou um grupo de conexões físicas com características similares, conectando nodes adjacentes, e é visto como uma única unidade composta pelo roteamento de mensagens no SNA. Essas múltiplas conexões paralelas permitem uma maior proteção contra erros em conexões individuais. Cada TG é identificado pelo mesmo numero em cada conexão do grupo, essa identificação é conhecida como Transmission Group Number. Esses números de identificação de conexões podem ser entre 1 e 255.

O VTAM também é um subsystem, que deve estar instalado no z/OS, com ele sendo executado é possível gerenciar todos os recursos mencionados nesta sessão.

As definições do VTAM estão armazenadas em dois diferentes arquivos, que são utilizados pelo subsystem. Um dos arquivos, chamado de VTAMLST, possui definições da rede SNA, incluindo as conexões, roteadores e componentes de hardware. O outro arquivo é o VTAMLIB, responsável armazenar os módulos de carregamento (arquivos binários) do VTAM.

O VTAM é possível ser inicializado de diferentes maneiras no z/OS, para isso são criadas Start Options (Opções de Inicialização) especificas para atender as necessidades de cada usuário. Para isso deve-se ser criado um membro no arquivo VTAMLST chamado de ATCSTR**yy**, sendo **yy** um valor alfanumérico. O comando de inicialização do VTAM é:

START NET,,,(LIST=**yy**)

O **yy** no comando, define o Start Option do VTAM, por exemplo, se for utilizado LIST=01, o subsystem utilizará a opção ATCSTR01.

Algumas Start Options são necessárias para o total funcionamento do VTAM:

SSCPID: Essa opção fornece um numero único de identificação para o VTAM, que é utilizado por algumas unidades físicas para identificar o VTAM. Esse valor é único para cada host.

SSCPNAME: Essa opção fornece um nome único de identificação para o VTAM.

NETID: Esse Start Option fornece um numero de identificação na rede.

HOSTSA: Usada para especificar o numero da sub-rede do VTAM.

HOSTPU: Opção para especificar um nome de usuário para a unidade física.

Quando o VTAM é inicializado, alguns recursos devem ser ativados, que devem estar definidos em uma Configuration List (Lista de Configuração). Essas configurações ficam armazenadas em um membro do arquivo VTAMLST, chamado de ATCCONxx, sendo xx um valor alfanumérico. Esse arquivo pode ser especificado no comando de inicialização ou dentro da Start Option.

A figura número 13 demonstra uma rede com dois Mainframes HOSTA e HOSTB, conectados usando uma Ethernet LAN, utilizand uma adaptador OSA nos dois hosts:

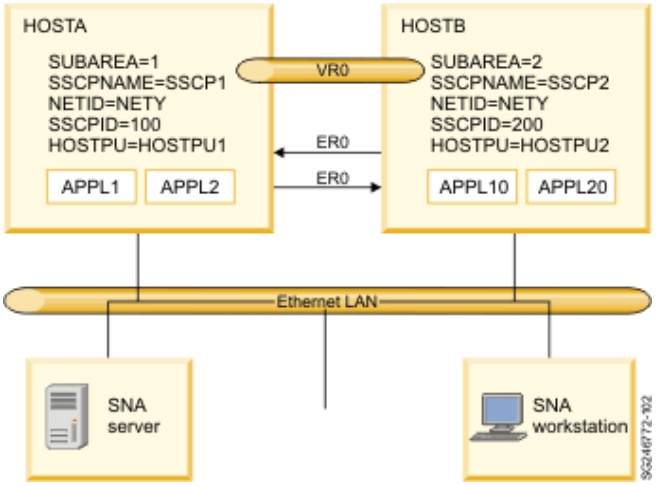

Figura 13: Definições VTAM de uma rede SNA (IBM Redbook, 2006)

A partir do exemplo da figura anterior, podemos observar as definições de configurações de HOSTA e HOSTB na tabela a seguir:

Tabela 1 – Definições de configuração dos HOSTA e HOSTB

HOSTA	**HOSTB**
ATCSTR01 Definition HOSTSA=01, SSCPNAME=SSCP1, NETID=NETY, SSCIP=100, HOSTPU=HOSTPU1, CONFIG=01	**ATCSTR02 Definition** HOSTSA=02, SSCPNAME=SSCP2, NETID=NETY, SSCIP=200, HOSTPU=HOSTPU2, CONFIG=02
PATH Definition PATH01 PATH DESTSA=2, ER0=(2,1), VR0=0	**PATH Definition** PATH01 PATH DESTSA=2, ER0=(2,1), VR0=0
XCA (OSA) major node for attaching peripheral and subarea nodes OSA1 VBUILD TYPE=XCA PORT1 PORT ADAPNO=1, CUADDR=29A, MEDIUM=CSMACD GRP1A GROUP DIAL=YES, AUTOGEN=(5,L,P), CALL=INOUT, ANSWER=ON GRP1B GROUP DIAL=NO LN1B LINE PU1B PU SUBAREA=2, PUTYPE=5, TGN=1, MACADDR=note 1	**XCA (OSA) major node for attaching peripheral and subarea nodes** OSA2 VBUILD TYPE=XCA PORT2 PORT ADAPNO=1, CUADDR=83C, MEDIUM=CSMACD GRP2A GROUP DIAL=YES, AUTOGEN=(5,L,P), CALL=INOUT, ANSWER=ON GRP2B GROUP DIAL=NO LN2B LINE PU2B PU SUBAREA=1, PUTYPE=5, TGN=1, MACADDR=note 1
CDRM major node CDRM1 VBUILD TYPE=CDRM NET1 NETWORK NETID=NETY SSCP1 CDRM SUBAREA=1 CDRM2 CDRM SUBAREA=2	**CDRM major node** CDRM2 VBUILD TYPE=CDRM NET2 NETWORK NETID=NETY SSCP2 CDRM SUBAREA=2 CDRM1 CDRM SUBAREA=1
Application major node APPL1X VBUILD TYPE=APPL APPL1 APPL ACBNAME=APPL1 APPL2 APPL ACBNAME=APPL2	**Application major node** APPL2X VBUILD TYPE=APPL APPL10 APPL ACBNAME=APPL10 APPL20 APPL ACBNAME=APPL20

Fonte: IBM

Tabela 2 – Continuação de definições de configuração dos HOSTA e HOSTB

HOSTA	**HOSTB**
Switched PU major node (SNA server) SWPU1 VBUILD TYPE=SWNET PU1 PU MAXDATA=1033, ADDR=01, CPNAME=SNASRVR, PUTYPE=2	**Switched PU major node (SNA workstation) with dependent LUs** SWPU2 VBUILD TYPE=SWNET PU2 PU MAXDATA=1033, ADDR=01, IDBLK=01A, IDNUM=,30D54, PUTYPE=2 LU1 LU LOCADDR=1 LU2 LU LOCADDR=2
CDRSC major node (Independent LU 6.2) CDRSC1 VBUILD TYPE=SWNET ILU1 CDRSC ALSLIST=PU1	
ATCCON01 PATH01, OSA1, CDRM1 APPL1X, SWPU1, CDRSC1	**ATCCON02** PATH02, OSA2, CDRM2 APPL2X, SWPU2, CDRSC2

Fonte: IBM

4.2.5. Communications Server

O z/OS possui um servidor chamado de Communications Server (CS), que integra um conjunto de softwares que possibilitam a comunicação na rede entre diferentes aplicações do z/OS. Esse servidor permite a comunicação entre a rede externa e as aplicações rodando no z/OS.

O Communication Server prove um conjunto de protocolos de comunicação que suportam conexão peer-to-peer para rede local e de longa distancia (wide-area), incluindo a Internet. Ele também melhora a performance de várias aplicações TCP/IP. Os principais recursos que estão incluídos nesse servidor são o TCP/IP, SNA e VTAM. Essa integração entre diferentes protocolos possibilita a implementação em diferentes ambientes, como AIX, Windows e Linux. Um recurso

muito importante do CS é o Communications Storage Manager (CSM), que disponibiliza uma área de buffer de I/O compartilhada para o fluxo de dados do TCP/IP e do VTAM.

4.2.6. Configuração do TCP/IP

Assim como qualquer outro tipo de serviço, o TCP/IP possui um subsystem instalado no z/OS. Essa task é utilizada para implementar o protocolo IP, e possibilita a execução de inúmeras aplicações IP no sistema. Por exemplo, é possível utilizar o FTP, SNMP, sendmail, Servidores HTTP, SSH, DNS, telnet, entre vários outros. O z/OS suporta totalmente o IPv6, apesar de ainda não ter sido amplamente implementada, por questões de negócios.

A task de TCP/IP utiliza um programa em JCL para ser iniciada, que permite especificar vários parâmetros e perfis (profile) diferentes para a utilização do TCP/IP. O TCP/IP lê o profile de TCP/IP assim que é iniciado, quando alguma mudança nas configurações precisa ser feita após ter sido iniciado, o TCP/IP pode reler o profile dinamicamente e realizar as determinadas mudanças. Um profile de TCP/IP é composto por: configurações de conexão, configurações de IP e TCP (IPCONFIG e TCPCONFIG, respectivamente), roteamento estático (BEGINROUTES) e monitoramento automático de aplicações IP (AUTOLOG).

Configurações de conexão: O TCP/IP permite que diferentes tipos de dispositivos sejam conectados à rede, o mais utilizado é o adaptador OSA-Express. Na configuração do TCP/IP duas coisas devem ser declaradas, o dispositivo e a conexão.

```
DEVICE OSAEDEV1 MPCIPA PRIROUTER
LINK OSAELNK1 IPAQENET OSAEDEV1

DEVICE OSAEDEV2 MPCIPA PRIROUTER
LINK OSAELNK2 IPAQENET OSAEDEV2

DEVICE VIPADEV1 VIRTUAL 1
LINK VIPALNK1 VIRTUAL 1 VIPADEV1

HOME
 201.2.11.9 VIPALNK1
 201.2.11.1 OSAELNK1
 201.2.11.2 OSAELNK2
```

Figura 14: Profile de configurações de conexão do TCP/IP (IBM Redbook, 2006)

Na figura número 14, podemos ver que foi declarado o nome do dispositivo (DEVICE) como OSAEDEV1, que se conecta com um dispositivo chamado MPCIPA, e é especificado o parâmetro PRIROUTER, que é necessário se a conexão irá transportar pacotes para diferentes redes. Por consequência, é declarado a conexão (LINK) com o nome de OSAELNK1, com a definição de OSA para IPAQENET, indicando que a conexão é real, e por fim define o dispositivo desta conexão. É declarado em HOME o endereço IP, relacionando com o nome da conexão.

Configurações de IP: A declaração de grupo IPCONFIG pode ser utilizado para controlar características relacionadas às funções IP do TCP/IP, algumas dessas relacionadas ao funcionamento do Sysplex. IPCONFIG controla o Forwarding de datagramas. Forwarding significa mover um datagrama entre diferentes redes. Com a opção DATAGRAMFWD é possível configurar para que não seja possível o Forwarding de datagramas.

Configurações de TCP: O TCPCONFIG controla as configurações dos parâmetros da camada de TCP. Os principais parâmetros são os controladores de tamanho de buffers enviados e recebidos, cujo impacto pode ser grande para performance da rede. TCPMAXRCVBUFRSIZE é o parâmetro que permite aumentar o tamanho padrão de buffer recebido. O parâmetro padrão do tamanho de buffer recebido é o TCPRCVBUFRSIZE, enquanto que o TCPSENDBFRSIZE é o padrão para buffer enviado.

Roteamento estático: Uma rota estática identifica o destino e o caminho correto para chegar ao destino final. Quando o destino não é especificado, o pacote

é enviado para o roteador padrão, que irá identificar o destino do pacote. A principal vantagem desse recurso é sua simplicidade. As rotas estáticas são declaradas em BEGINROUTES.

```
BEGINROUTES
ROUTE 201.2.11.0 255.255.255.0 =            OSAELNK1 MTU 1500
ROUTE 201.2.11.0 255.255.255.0 =            OSAELNK2 MTU 1500
ROUTE DEFAULT                  201.2.11.100 OSAELNK1 MTU DEFAULTSIZE
ROUTE DEFAULT                  201.2.11.100 OSAELNK2 MTU DEFAULTSIZE
ENDROUTES
```

Figura 15: Profile de roteamento estático do TCP/IP (IBM Redbook, 2006)

Na figura número 15 podemos notar que existem duas rotas equivalentes para acessar a sub-rede 201.2.11.100, e duas rotas padrões ligando à um roteador de IP 201.2.11.100, Existe uma redundância no exemplo, o adaptador pode ser utilizado para acessar a rede e roteador padrão. Outro ponto importante é que, se OSAELNK1 por alguma razão não estiver funcionando, o TCP/IP irá imediatamente trocar para o OSAELNK2.

Monitoramento automático de aplicações IP: Qualquer aplicação IP no z/OS necessita que o TCP/IP esteja funcionando para que as comunicações possam ocorrer, toda vez que o TCP/IP é iniciado os servidores IP também iniciam ao mesmo tempo. O TCP/IP permite que seja possível um monitoramento para se certificar de que as aplicações estão rodando corretamente. A monitoração é possível através do AUTOLOG, que declara uma lista de nomes e tarefas que devem ser iniciadas e permanecer rodando enquanto o TCP/IP estiver em execução. O monitoramento é feito periodicamente para confirmar se a aplicação esta ativa na determinada porta, se for detectado que não está ativa, o TCP/IP para a task e a inicia de novo. O exemplo da figura número 16 demonstra como o AUTOLOG funciona para monitorar e reativar o servidor FTP automaticamente, o processo ocorre a cada 5 minutos:

```
AUTOLOG 5
 FTPD JOBNAME FTPD1
ENDAUTOLOG
PORT
 20 TCP OMVS NOAUTOLOG
 21 FTPD1
```

Figura 16: Exemplo do AUTOLOG para FTP (IBM Redbook, 2006)

O TCP/IP permite que sejam definidos os endereços de internet virtuais da rede (Virtual Internet Protocol Addresses, ou VIPAs). Um endereço pode ser mapeado automaticamente por mais de um sistema z/OS ao mesmo tempo, ele também pode ser transmitido dinamicamente de uma aplicação IP para outra, mesmo se em um sistema diferente. Tudo isso transparente para a rede e suas aplicações. O endereço VIPA pode estar associado à vários dispositivos físicos de um host de z/OS, e não existe um limite para esse número de dispositivos.

4.2.7. Configuração do FTP

O FTP é uma aplicação de sistemas z/OS UNIX, mas ele pode ser inicializado em um ambiente de MVS. Um subsystem de FTP pode ser iniciado executando o /usr/sbin/ftpd, porém ele pode ser automaticamente inicializado a partir do TCP/IP se linguagem JCL for utilizada, como demonstra a figura número 17:

```
//FTPD   PROC MODULE='FTPD',PARMS=''
//FTPD   EXEC PGM=&MODULE,REGION=4096K,TIME=NOLIMIT,
//       PARM='/&PARMS'
//SYSFTPD DD DISP=SHR,DSN=SYS1.TCPPARMS(FTPSDATA)
```

Figura 17: Exemplo de inicialização do FTP por JCL (IBM Redbook, 2006)

Pode-se notar que no JCL anterior foi declarado em SYSFTPD, um arquivo de configuração. Assim como no TCP/IP, o FTP também pode ser inicializado utilizando diferentes parâmetros e perfis (profile), essas informações são armazenadas em um arquivo chamado de FTP.DATA. Esse arquivo pode conter os seguintes itens:

Banner page: Recursos padrões de um servidor FTP.

Anonymous configuration: Diferentes níveis de controle de acesso anônimo podem ser configurados.

Data set defaults: Podem ser especificados os atributos de arquivos, tais como tamanho de bloco, formato de arquivos, entre outras especificações.

Tracing and logging: Registro de usuários e informação de depuração detalhada podem ser ativadas.

File system: O usuário quando acessa o servidor FTP pode ser automaticamente colocado em um sistema de arquivos z/OS UNIX ou apenas no z/OS.

SSL/TLS: Uma sessão segura pode ser requisitada quando conectado ao servidor FTP.

JES and DB2 environments: Um usuário FTP pode interagir com ambientes JES ou DB2.

Qualquer parâmetro que não for especificado no arquivo FTP.DATA, seguira as configurações padrões do FTP. Pode-se observar as configurações do arquivo FTP.DATA na figura número 18:

```
BANNER /etc/ftp.banner
ANONYMOUSLEVEL 3
ANONYMOUSFILEACCESS HFS
FTPLOGGING TRUE
STARTDIRECTORY HFS
```

Figura 18: Configurações do arquivo FTP.DATA (IBM Redbook, 2006)

4.2.8. Terminal 3270

Como dito anteriormente, o protocolo utilizado para comunicação entre usuários e mainframe é o SNA. Para facilitar o monitoramento e trabalhar com mensagens provenientes do mainframe era utilizado uma tecnologia chamada de 3270 DataStream. Para os usuários finais este era um dispositivo conhecido como terminal 3270. Este terminal nada mais era do que uma estação de trabalho, conectado a uma Control Unit utilizando um cabo coaxial.

Com o crescimento da internet, as grandes corporações começaram à implementar o protocolo IP em suas redes. Devido ao grande número de aplicações em SNA 3270, foi encontrada uma maneira de integrar o SNA com o protocolo IP, a tecnologia utilizada para mover aplicações SNA 3270 ao TCP/IP é chamada de TN3270, uma abreviação para Telnet 3270.

Hoje em dia, uma única instância do servidor TN3270E (aprimoramento do TN3270) pode emular cerca de 128.000 terminais 3270. Para emular os terminais é utilizado um software chamado de TN3270 Clients, que pode ser executado em uma

estação de trabalho ou em qualquer computador pessoal. O TN3270E é o método padrão baseado em protocolo IP para comunicação com o Mainframe.

Os Usuários TN3270E utilizam o protocolo TN3270E para acessar recursos do servidor TN3270E, porém, um usuário TN3270E não pode acessar um aplicativo que utiliza protocolo SNA diretamente, sendo assim, o servidor TN3270E funciona como um conversor de protocolos. A figura número 19 demonstra como é feita essa comunicação:

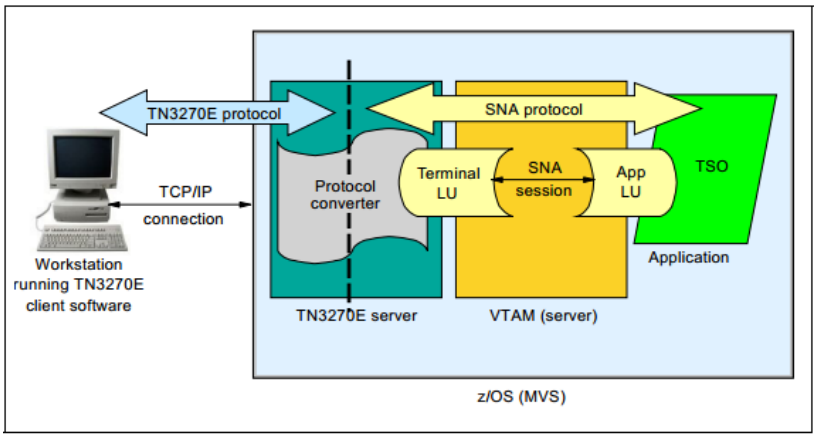

Figura 19: Conexão do protocolo TN3270E (IBM, 2006)

5. SEGURANÇA DA REDE

Devido à grande importância do mainframe no mercado, e seu grande volume de informações e transações processadas diariamente em todo lugar do mundo, tal como transações bancarias, esses sistemas devem ter a máxima segurança possível. O z/OS possui vários recursos para a segurança dos dados do Mainframe.

5.1. Security Access Facility

Security Authentication Facility (SAF) é um componente de segurança do z/OS que tem como objetivo direcionar solicitações dos gerenciadores de recursos, como o TSO, CICS, IMS, DB2, JES, entre outros, para o gerenciador de segurança externo (External Security Manager - ESM) instalado no sistema operacional. Assim, os gerenciadores de recursos são responsáveis por enviar solicitações para o SAF, que irá determinar se um usuário tem permissão ou não de acessar algum recurso, e dependendo do tipo de recurso o SAF envia a solicitação para o ESM.

Um ESM não vem instalado no z/OS, porém existem várias opções disponíveis para instalação. Quando um ESM não é instalado, o SAF é o responsável por manter a estrutura de segurança do sistema.

O SAF possui uma ferramenta chamada de SAF Router, que disponibiliza um ponto focal para interface de todos os produtos, funcionando como um controlador de recursos.

O SAF é acessado a partir de uma macro chamada RACROUTE. Esse macro é responsável por autenticar um usuário, verificar permissões, gerenciamento de logs e obter um adress space seguro no sistema. Independente de um ESM instalado, as aplicações e recursos do sistema utilizam o RACROUTE.

A presença do RACROUTE no z/OS faz com que não seja necessário que uma aplicação requisitando um serviço entenda a infraestrutura de segurança implementada no sistema, a aplicação não precisa saber se existe um ESM instalado no sistema ou não.

O SAF Router utiliza uma tabela de roteamento para associar o ESM com as solicitações do RACROUTE, como se pode observar na figura número 20:

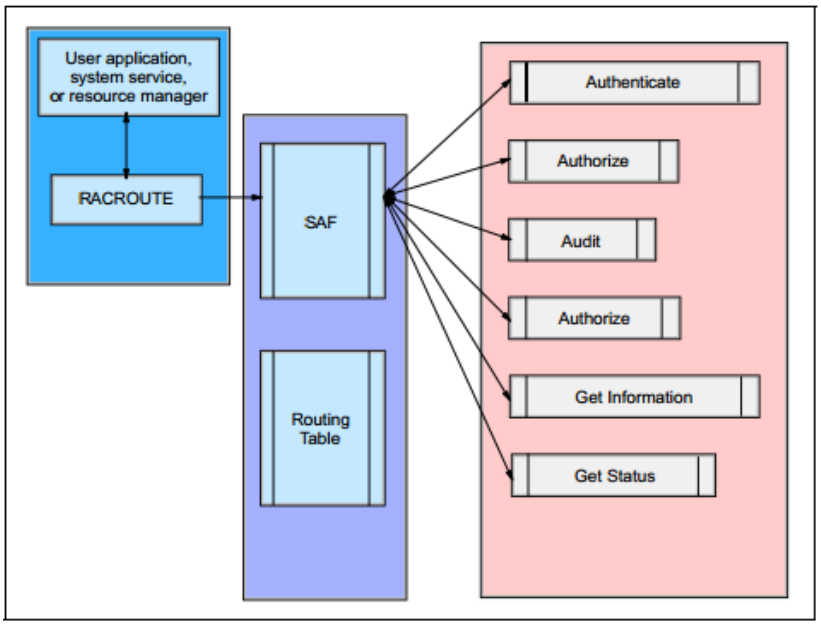

Figura 20: Comunicação entre RACROUTE e o SAF Router (IBM Redbook, 2007)

O RACROUTE possui vários tipos diferentes de requisições (Request Types), sendo os principais:

Audit: Armazena os eventos do sistema em um recurso chamado de System Management Facilities (SMF) e envia mensagens para o administrador da rede.

Auth: Confirma a autoridade do usuário para acessar um determinado recurso.

Define: Define, modifica ou renomeia um profile de um recurso.

DirAuth: Compara duas camadas de segurança.

Extract: Recupera ou substitui determinado campo de profile de segurança.

Stat: Determina se o ESM está ativo.

5.2. Resource Access Control Facility

A principal ESM que é utilizada atualmente no z/OS é o Resource Access Control Facility (RACF). Com a utilização do RACF é possível gerenciar vários recursos, visando manter o sistema seguro. O RACF controla o acesso de usuários

ao sistema, confirma autoridade para acesso de determinados recursos e permite a auditoria do sistema. As principais funções do RACF são:

Autenticação: É necessária a identificação do usuário que está tentando acessar o sistema, após a identificação, é possível a autenticação do usuário.

Autorização: Para acessar determinados recursos ou arquivos, o RACF verifica se o usuário tem a autoridade necessária.

Auditoria: Todo registro de acesso à recursos ou arquivos são armazenados em logs.

5.2.1. Perfil e Banco de Dados RACF

O RACF possui um banco de dados em que são armazenadas as informações referentes aos usuários, grupos, conjunto de dados e entre outros recursos. Os registros que descrevem esses objetos no banco de dados são chamados de perfis (profiles).

Os tipos de perfis de RACF são de usuário, grupo, arquivo e recursos gerais.

Perfil de usuário: Um perfil de usuário possui as definições RACF do usuário. Contém o ID do usuário, nome de usuário, a senha, dono do perfil, atributos do usuário e informações relacionadas aos subsystems.

Perfil de grupo: Os usuários podem ser agrupados em grupos para facilitar o gerenciamento da autoridade dos usuários, dependendo de sua função no sistema. O perfil de grupos contém o nome do grupo, dono do perfil e a lista de usuários no grupo.

Perfil de arquivos (Dataset): Pode proteger um ou mais arquivos. Contém o nome o nome do perfil de arquivos, dono do perfil, autoridade de acesso, lista de acesso e algumas outras informações. O perfil que é responsável por proteger um único recurso é chamado de perfil discreto, enquanto que um perfil que deve proteger vários recursos é chamado de perfil genérico.

Perfil de recursos gerais: Esse perfil fornece proteção aos recursos em geral, não referente à arquivos. Possui o nome do perfil, dono do perfil, autoridade de acesso, lista de acesso e algumas outras informações.

5.2.2. Classes RACF

Classe de RACF é um conjunto de perfis de um mesmo tipo. O RACF já possui várias classes padrões, como por exemplo, USER, DATASET e GROUP, porém é possível ativar mais classes, dependendo da necessidade no ambiente. As classes podem ser gerenciadas a partir do comando SETROPTS, e listar as classes ativas no sistema pelo comando SETROPTS LIST. As principais classes utilizadas no sistema são:

TAPEVOL: Utilizada para a segurança de tapes.

SDSF: Controla o uso de comandos no painel SDSF.

OPERCMDS: Controla a utilização de comandos com autoridade de operador.

DASDVOL: Utilizada para a segurança de discos.

5.2.3. Atributos de usuário

Para determinados acessos no sistema são necessários alguns atributos especiais. Os atributos de usuário têm por objetivo diferenciar diferentes tipos de usuários e sua autoridade no sistema. Esses atributos podem ser especificados na criação dos grupos de usuários. Os diferentes tipos de atributos são:

SPECIAL: É utilizado apenas por administradores, com esse atributo é possível executar qualquer comando de RACF e ter acesso à todos os perfis de usuário.

AUDITOR: Esse atributo é designado para usuários responsáveis pela auditoria do RACF.

OPERATIONS: Atributo fornece acesso a todos os recursos protegidos pelo RACF em DATASET, DASDVOL, GDASDVOL, PSFMPL, TAPEVOL, VMBATCH, VMCMD, VMMDISK, VMNODE e VMRDR.

CLAUTH (Class Authority): O usuário com esse atributo consegue criar perfis dentro de uma classe.

REVOKE: É possível negar o acesso de um usuário ao sistema, utilizando o atributo REVOKE.

GRPACC (Group Access): Quando um usuário possui este atributo, qualquer perfil de grupo de arquivos que o usuário definir para o RACF será automaticamente acessível para qualquer outro usuário que seja membro do grupo.

ADSP (Automatic Data Set Protection): Toda vez que um arquivo é criado pelo usuário com esse atributo, será automaticamente protegido pelo RACF.

RESTRICTED: É possível prevenir que um usuário ganhe acesso temporário com os comandos ADDUSER ou ALTUSER.

5.2.4. Segmentos RACF

Segmentos RACF são opções para o perfil do usuário, eles possuem informações sobre determinados aplicativos e gerenciadores de recursos, como por exemplo, um usuário de DB2 deve possuir em seu perfil, um segmento de DB2 para poder ter acesso aos recursos de DB2. Um único perfil de usuário pode possuir diferentes segmentos, dependendo das atividades que o usuário realiza no sistema. As informações básicas do segmento RACF ficam no perfil de cada usuário, as principais são:

USERID: ID do usuário.

NAME: Nome do usuário.

OWNER: Dono do perfil do usuário.

DFLTGRP: O grupo padrão em que o usuário está inserido.

AUTHORITY: A autoridade que o usuário possui no grupo padrão.

PASSWORD: Senha do usuário.

5.2.5. Definição de Usuários e Grupos

O administrador RACF, por possuir o atributo SPECIAL, pode administrar os atributos ou qualquer outra informação dos usuários a partir do painel de RACF no ISPF, ou por comandos. Os comandos utilizados pelo administrador são:

ADDUSER: Adiciona um perfil de usuário para o RACF.

ALTUSER: Modifica um perfil de usuário do RACF.

CONNECT: Conecta um usuário a determinado grupo.

DELUSER: Remove o perfil do usuário do RACF e qualquer conexão que existir com grupos.

REMOVE: Remove um usuário de um grupo.

LISTUSER: Mostra as informações do perfil do usuário

PERMIT: Permite que um usuário acesse determinado recurso.

PASSWORD: Modifica a senha do usuário.

O administrador também é responsável por gerenciar os grupos, e utilizam os seguintes comandos:

ADDGROUP: Cria um novo grupo.

ALTGROUP: Atribui um subgrupo à um grupo em um nível superior.

DELGROUP: Remove grupos.

LISTGRP: Mostra informações do perfil do grupo

CONNECT: Conecta um usuário à determinado grupo.

REMOVE: Remove um usuário de um grupo.

PERMIT: Permite que um usuário acesse determinado recurso.

5.2.6. Comunicação entre SAF e RACF

Como dito anteriormente, o SAF trabalha juntamente como RACF para possibilitar a autorização ou autenticação dos usuários. O SAF direciona as solicitações dos usuários a partir dos gerenciadores de recursos (Resource Manager), o RACF acessa seu banco de dados e retorna a resposta da solicitação de acordo com a autorização encontrada no banco de dados até chegar ao usuário novamente, assim como demonstra a figura número 21:

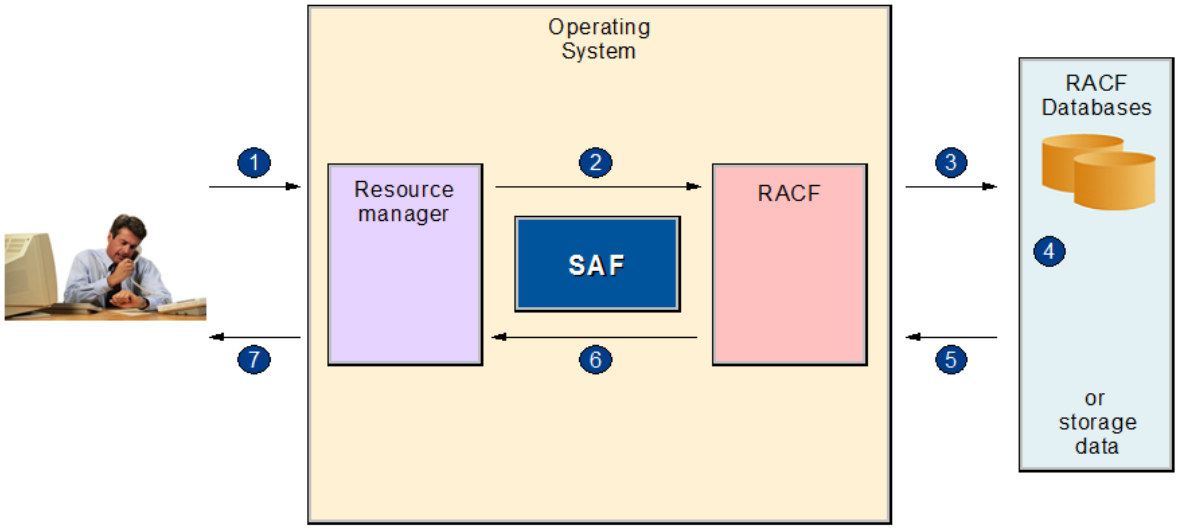

Figura 21: Comunicação entre SAF e RACF (IBM, 2006)

5.2.7. Auditoria RACF

O auditor deve possuir o atributo de AUDITOR no RACF, e é responsável por verificar se o RACF está seguindo todas as diretrizes de segurança instaladas. O controle de acesso significa que é necessário verificar se os acessos permitidos são apropriados para o recurso. Para o auxilio na auditoria de controle de acesso, o RACF disponibiliza alguns recursos:

Logs (Registros): É o registro de determinados eventos no sistema. O RACF utiliza o SMF para o registro dos eventos do RACF. SMF é um recurso do z/OS que coleta informações de todas as atividades no sistema, criando registros dessas informações. Os eventos que o RACF registra são:

-Todos os comandos de MVS utilizados no sistema.

-Toda requisição do RACROUTE que receber uma resposta negativa, por ser uma requisição desconhecida ou não confiável.

-Toda vez que um operador permite acesso a um recurso no processo de failsoft quando o RACF está inativo.

-Toda vez que um usuário tenta alocar ou desalocar um arquivo do sistema.

-Existem vários outros eventos que podem ser registrados pelo RACF, dependendo da necessidade do sistema.

A figura número 22 demonstra o processo de requisições no z/OS até serem arquivadas em logs, a requisição é feita pelo usuário, a partir de uma aplicação, passa pelo Gerenciador de Recursos dessa aplicação, o SAF leva essas requisições até o ESM (por exemplo, o RACF), que procura pelas informações de autoridade e acesso em seu banco de dados. Por fim, o SMF captura todas essas informações e armazena em seu registro (Event Logs):

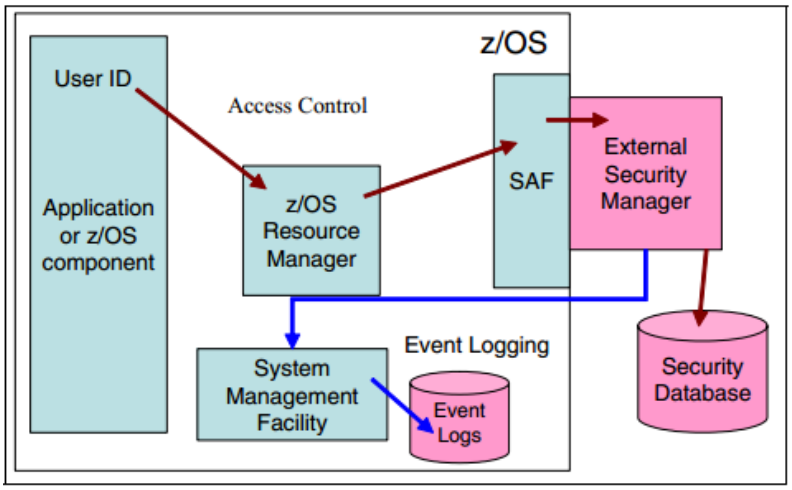

Figura 22: Processo de requisições até armazenamento em logs (IBM Redbook, 2007)

Data Security Monitor (DSMON): É um programa que gera relatórios do status do ambiente de segurança, e em particular, os recursos que o RACF controla. O DSMON pode ser utilizado para auditar o status atual do ambiente de segurança com o status das características pretendidas pelo ambiente. A execução do DSMON pode ser feita a partir de job de batch, e é necessário o atributo de AUDITOR e autoridade de EXECUTE ou RED no programa.

RACF Report Writer (RACFRW): Utilizado para listar o conteúdo dos registros SMF, em um formato de fácil leitura. Com o é possível obter relatórios de:

-Tentativas de acesso à um recurso protegido pelo RACF, informando o nome do usuário, identidade do usuário, numero de acessos bem sucedidos e numero de tentativas de violação de segurança.

-Informações que descrevem o usuário e atividades do grupo.

-Utilização do sistema e seus recursos

RACF SMF Data Unload Utility (IRRADU00): RACF Audit Data são os registros dos eventos relevantes de uma instalação de segurança. Os registros são utilizados para verificar a eficacia da segurança, verificar se os objetivos da segurança estao sendo cumpridos, e identificar eventos inesperados. O IRRADU00 permite instalações para a criação de um arquivo sequencial dos dados importantes de auditoria e de segurança. Esse arquivo sequencial pode ser acessado para exibição direta das informações, utilizado como entrada para instalação de programas ou carregado em um banco de dados relacional.

5.2.8. Acesso aos recursos do RACF

O RACF pode ser acessado a partir do ISFP no TSO. Um painel interativo facilita a visualização e administração dos recursos e ferramentas do RACF. A figura número 23 demonstra o painel e suas várias opções:

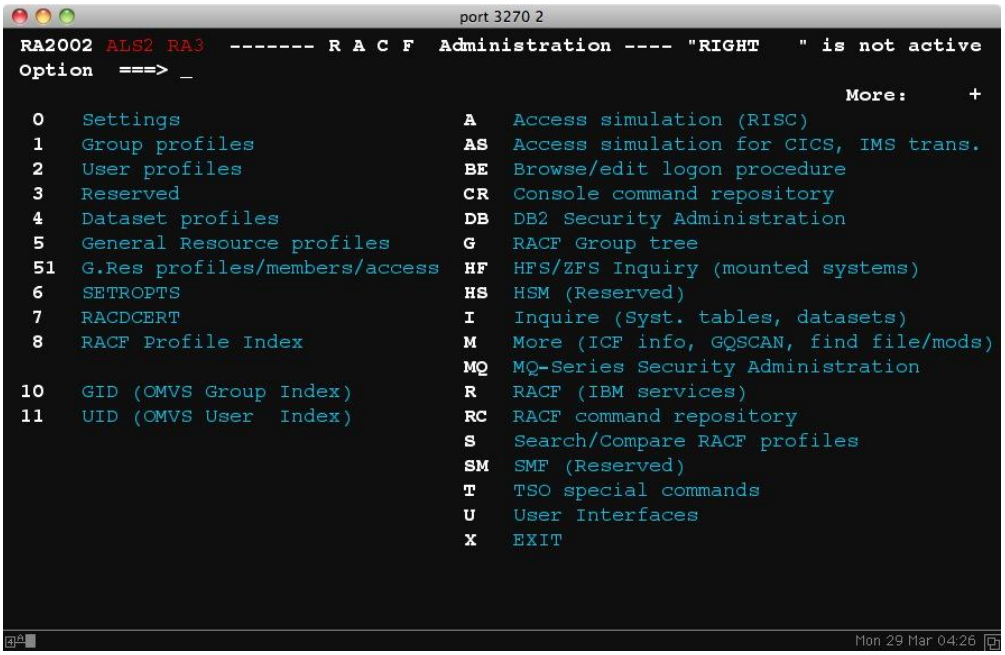

Figura 23: Painel de administração do RACF (racfra2.com Corporation, 2012)

5.3. Criptografia de Hardware no Mainframe

Um dos recursos básicos para segurança de uma rede é a criptografia, possibilitando que os dados trafeguem na rede com total segurança. O Mainframe possui hardwares e softwares capazes de realizar uma criptografia eficaz neste ambiente.

O Mainframe possui hardwares para criptografia que consistem em processadores especiais que realizam a criptografia de diferentes algoritmos. Os equipamentos mais utilizados para o ambiente Mainframe são divididos em duas classes, o Hardware Security Module (HSM) e o Cryptographic accelerator (Acelerador de criptografia).

O HSM, não confundir com Hierarchical Storage Management, é um equipamento projetado para ser a base da segurança criptográfica. Esse equipamento é responsável por armazenar chaves simétricas e assimétricas com segurança máxima. O HSM suporta tanto ataques físicos, como por exemplo, a remoção do hardware, quanto a ataques mais sutis, assim como, pulsos eletromagnéticos ou a radiação emitida pelo equipamento. Quando alguma alteração é detectada, o HSM apaga qualquer tipo de informação secreta de sua memória.

Cryptographic accelerators são equipamentos projetados para dar suporte a um determinado algoritmo de criptografia. Um acelerador para algoritmos Data Encryption Standard (DES) ou Secure Hash Algorithm (SHA) são projetados especificamente para filtrarem grandes quantidades de dados, um acelerador para RSA (Algoritmo de segurança, abreviatura para Ron Rivest, Adi Shamir and Leonard Adleman) é eficaz para a matemática exponencial e modular. Pode-se então notar que o acelerador irá atender especificamente o algoritmo utilizado no sistema. Os aceleradores, diferentemente do HSM, não possuem os mais rigorosos requisitos de segurança, se tornando muito mais rápidos. Assim esse equipamento não impacta o rendimento ou desempenho da criptografia.

O Mainframe suporta uma ampla variedade de hardwares de criptografia de ambas as classes. A figura número 24 é um exemplo deste tipo de hardware de criptografia:

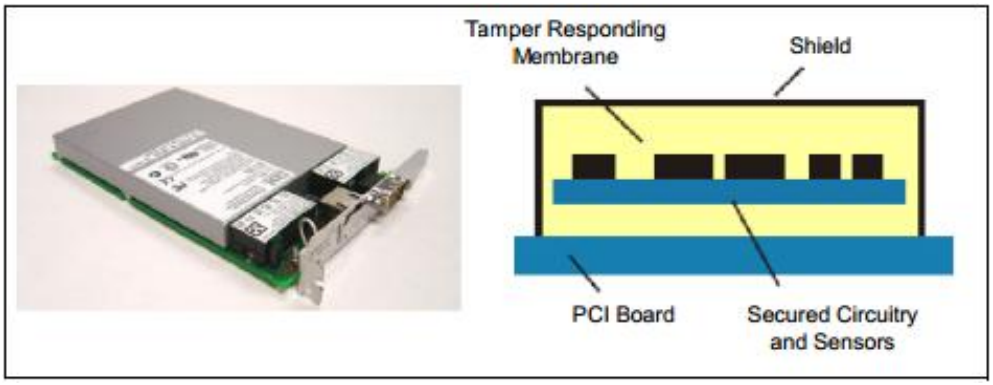

Figura 24: Cartão de criptografia e seus componentes (IBM Redbook, 2007)

5.4. Criptografia do Software no Mainframe

5.4.1. Common Cryptographic Architecture

O sistema Mainframe oferece um pacote de softwares para ser possível o uso dos hardwares de criptografia. As plataformas que suportam equipamentos de criptografia utilizam uma arquitetura chamada de Common Cryptographic Architecture (CCA).

O CCA é uma arquitetura, não apenas de software, ele possui uma variedade de processos de criptografia e de técnicas de segurança de dados. Essa ferramenta define a forma que os serviços são invocados e as chaves são referenciadas, recuperadas, armazenadas e utilizadas dentro do ambiente criptográfico.

Separação de chaves é a capacidade de impor um único propósito para a chave. Por exemplo, uma chave responsável por gerar o PIN (Personal Identification Number) de um cliente, deve ser utilizada apenas para essa tarefa, pois um invasor pode utilizar essa chave para atacar os dados que estava protegendo, ou mesmo para lançar um ataque à chave mestre no HSM. A forma em que o CCA impõe a separação de chaves é chamada de Control Vector (Controle de Vetor). Esses vetores são strings de bits que possuem o mesmo tamanho de uma chave do DES. Quando a criptografia protege uma chave em sua chave mestre, ele primeiro determina o tipo da chave, em seguida modifica a chave mestre simétrica com o correspondente Control Vector (utilizando o XOR), e então utiliza o resultado para criptografar a chave, assim como demonstra a figura número 25:

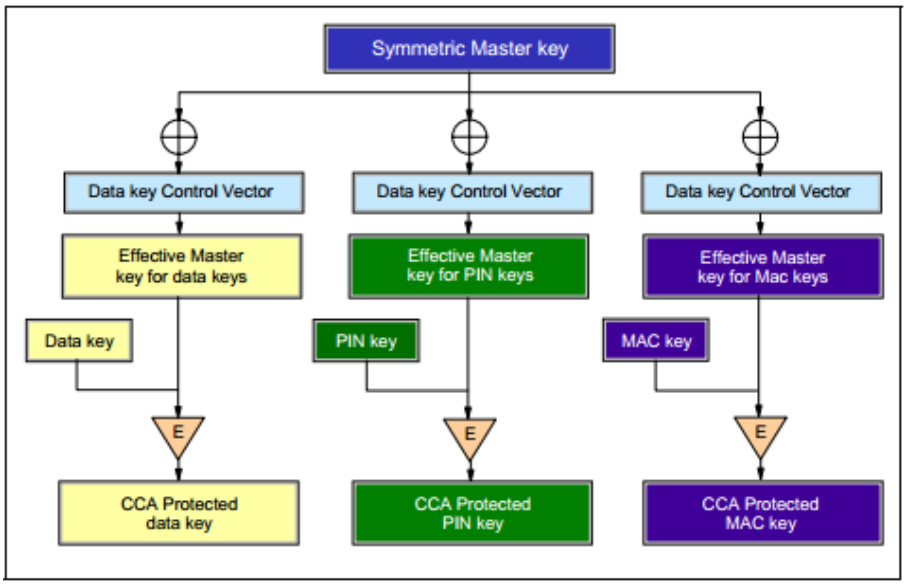

Figura 25: Control Vector (IBM Redbook, 2006)

5.4.2. Application Programming Interface (API)

O CCA influencia o modo de interação com o ambiente de criptografia, definindo a maneira em que os aplicativos podem chamar seus serviços. Independente da plataforma ou sistema operacional, uma chamada para o ambiente criptografado suportado pelo CCA, sempre segue o mesmo formato. Uma chamada para CSNBENC para a criptografia dos dados vai ser o mesmo para linguagens COBOL, Assembler, REXX ou C++.

5.4.3. Cryptographic Software Support para z/OS

Integrated Cryptographic Services Facility (ICSF) é a principal solução para criptografia, ela fornece as APIs do CCA e a interface com o hardware. Além disso, o ICSF executa as seguintes funções:

-Interação com o ESM para garantir que as requisições estão autorizadas a acessar os serviços de criptografia e os recursos requisitados.

-Gerencia de dois arquivos de armazenamento de chaves, o Cryptographic Key Data Store (CKDS) e o Private Key Data Store (PKDS). Quando as chaves são armazenadas nestes arquivos, eles são automaticamente convertidos como parte do

processo de mudança da chave mestre. Este serviço pode ser realizado sem para o processamento criptográfico.

O ICSF interage com o ESM para verificar se as requisições tem autoridade para acessar determinados serviços e recursos, além da interação com o hardware de criptografia instalado, como pode ser observado na figura número 26:

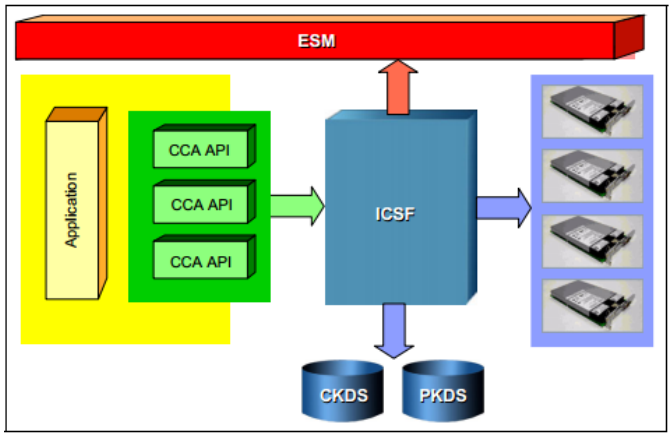

Figura 26: Integrated Cryptographic Services Facility (IBM Redbook, 2006)

5.4.4. Open Cryptographic Services Facility (OCSF)

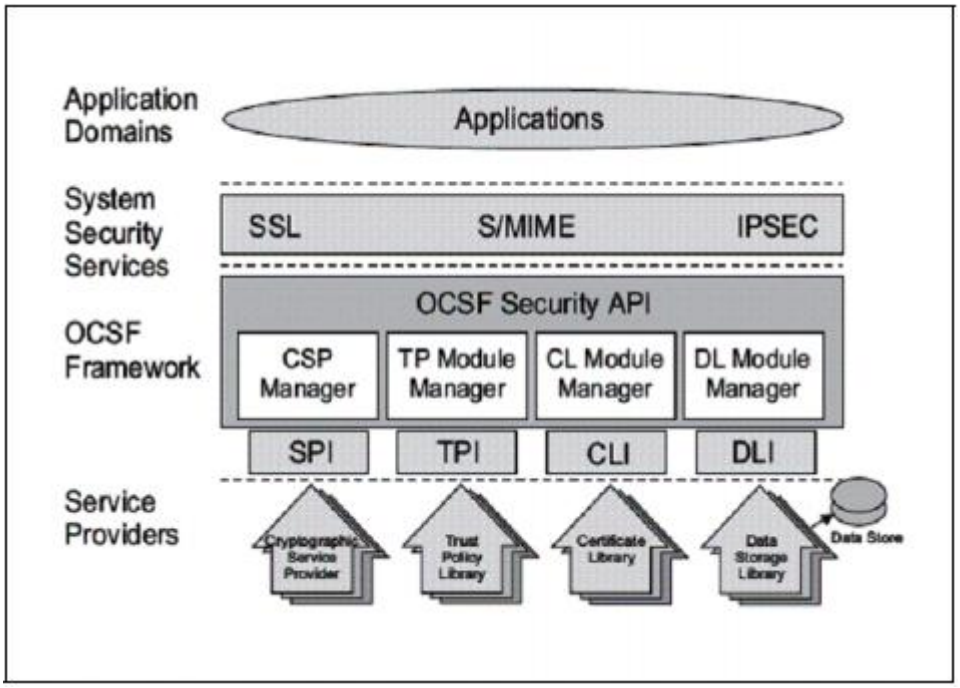

Figura 27: Camadas do CDSA (IBM Redbook, 2006)

O OCSF é implementado no Common Data Security Architecture (CDSA), que foi desenvolvido pelo Open Group. Como é possível ver na figura número 27, o CDSA é composto por quatro camadas principais, cada uma baseia-se no serviço da camada abaixo delas.

-Application Domain (Domínio de Aplicação), que é o nível mais alto, invoca um conjunto de serviços de segurança, como SSL, S/MIME, IPSec, entre outros.

-System Services Layer (Camada de serviços do sistema) invoca o Framework do OCSF para invocar serviços específicos de segurança.

-OCSF Framework proporciona um conjunto padrão de APIs e os relaciona com os módulos de serviço de provedor (Service Providers) instalados.

-Service Providers proporcionam os serviços de segurança ou a interação com outros elementos do sistema para proporcionar os serviços requisitados.

5.5. HiperSockets

O HiperSocket é um recurso da rede que pode ser utilizada em um ambiente Mainframe, ele permite a inter comunicação entre as partições lógicas, simulando uma rede LAN Ethernet. A simulação é realizada pelo microcode (microcódigo) Processor Resource/Systems Manager (PR/SM). O PR/SM é recurso do Mainframe que possibilita ao administrador definir as partições lógicas no sistema.

A transferência de dados a partir da rede LAN simulada, que trabalha movendo os dados a partir da memória física, sendo assim, o HiperSocket não pode abranger vários sistemas físicos, e é restringido a apenas uma única maquina física, controlada pelo PR/SM. Os HiperSockets são ativados a partir de definições no arquivo IOCDS, que contem as configurações de entrada e saída no sistema.

A figura número 28 demonstra um exemplo dessa configuração, onde existem três partições lógicas, conectadas em uma rede segura. As requisições vindas da Internet são filtradas pela primeira partição (no exemplo, uma partição Linux), e então são executadas pela segunda partição (z/OS WebSphere Application Server), e finalmente chegam à terceira partição (z/OS Enterprise Information System). A

rede entre as partições é proporcionada pelo HiperSocket, possibilitando uma rede muita mais rápida, melhorando a performance e a segurança física.

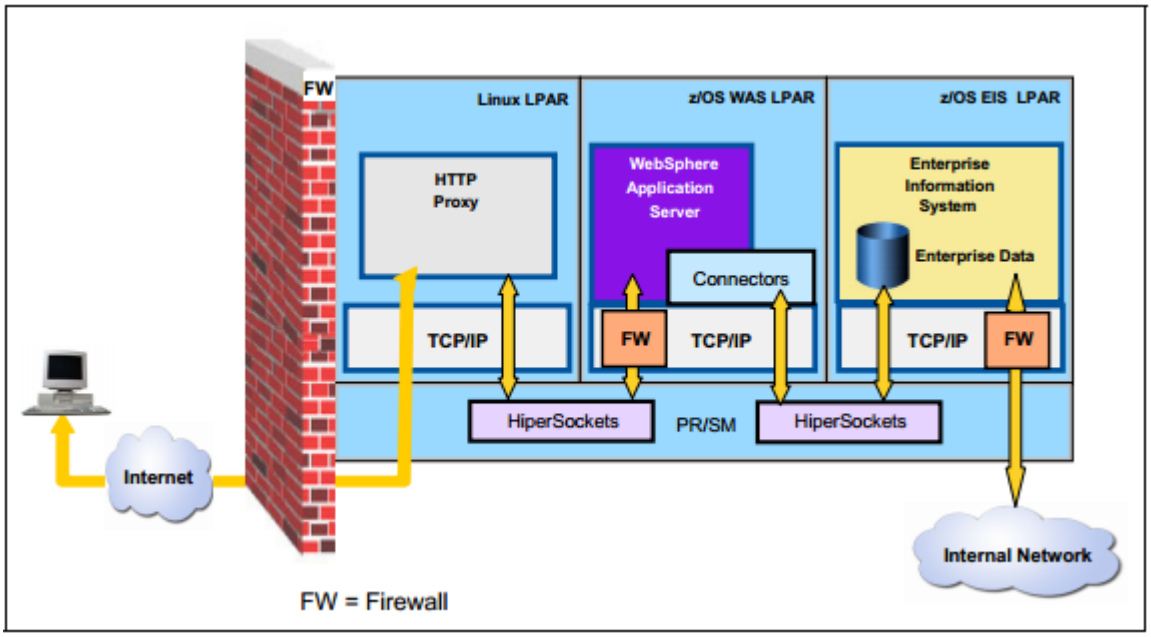

Figura 28: Conexão entre partições lógicas utilizando HiperSocket (IBM Redbook, 2007)

Para a partição lógica, a rede HiperSocket é gerenciada pelo TCP/IP instalado no sistema operacional da partição. Como o HiperSocket proporciona uma rede LAN Ethernet normal, uma tecnologia Firewall convencional pode ser implementada no TCP/IP conectado ao HiperSocket. Porém, um Firewall externo não pode ser instalado em uma rede HiperSocket, já que a rede não existe, ela é apenas simulada.

6. CONCLUSÃO

Este trabalho procurou explanar sobre a tecnologia Mainframe, apresentando seu funcionamento na parte física e lógica, e principalmente a forma como a rede e a segurança de rede funcionam nesse ambiente. Com a pesquisa realizada e as informações obtidas, podem-se levantar algumas conclusões sobre o Mainframe.

O Mainframe foi um dos primeiros computados para grandes empresas, e continua sendo o maior provedor de processamento de dados para essas grandes empresas e organizações, apesar de muitos acharem que o mesmo está extinto. Por ser uma tecnologia que não demonstra muitos riscos ou falhas, continua sendo a mais utilizada para grandes demandas.

Pelo alto processamento de informações confidencias, como por exemplo, dados bancários, a segurança da rede neste ambiente se mostra muito segura, robusta e eficaz, proporcionando diferentes recursos para proteção física e lógica do sistema.

Com o desenvolvimento da tecnologia TCP/IP, a rede utilizada pelo mainframe, o SNA, se adaptou para trabalhar em paralelo a essa tecnologia e a todos os recursos disponibilizados pela mesma. O sistema operacional do Mainframe possibilita a instalação de diferentes ferramentas para facilitar o funcionamento do ambiente, assim como o RACF que demonstra ser uma eficaz ferramenta de controle de acesso aos recursos z/OS.

Como dito anteriormente, com o passar do tempo e a criação de diferentes arquiteturas de rede, assim como o TCP/IP, serviços de criptografia ou transferência de dados, o Mainframe foi se adequando a todas essas novas tecnologias, continuando a trabalhar da mesma maneira, apenas se atualizando as necessidades do mercado.

7. REFERÊNCIAS BIBLIOGRAFICAS

CENTRIC SOLUTIONS. **Ribbon array harness**. *Disponível em:* <http://www.centricsolutions.com/fibcable_ribarray_harness.html>. *Acesso em:* 18 maio 2012

CIVA, G. **BMC: mainframe ainda é forte.** *Disponível em:* < http://www.baguete.com.br/noticias/hardware/11/10/2011/bmc-mainframe-ainda-e-forte>. *Acesso em:* 30 mar. 2012.

CONSUTORA DE TECNOLOGIA. **Mainframe tendência do mercado de trabalho**. *Disponível em:* <http://www.upngo.com.br/2011/SWF/Mercado%20de%20Trabalho%20MAINFRAME%20JAN%202011.swf >. *Acesso em:* 30 mar. 2012.

DANTAS, A. **Introdução a MVS – sistema mainframe**. *Disponível em:* <http://alandantas.blogspot.com.br/2012/02/introducao-mvs-sistema-mainframe.html >. *Acesso em:* 18 maio 2012.

DECISION REPORT. **Uso do mainframe ainda é forte nas empresas**. *Disponível em:* <http://www.decisionreport.com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid=10008&sid=20 >. *Acesso em:* 01 abr. 2012.

EBBERS, M.; KETTNER, J.; BRIEN, W. O.; OGDEN, B. **Introduction to the new Mainframe z/OS basics**. IBM Corp, 2001. 764p. *Disponível em:* <http://www.redbooks.ibm.com/redbooks/pdfs/sg246366.pdf>. *Acesso em:*

EBBERS, M.; HASTINGS, C.; NUTTALL, M.; REICHENBERG, M. **Introduction to the new Mainframe: networking**. IBM Corp, 2006. 390p. *Disponível em:* <http://www.redbooks.ibm.com/redbooks/pdfs/sg246772.pdf>. *Acesso em:*

ELLIOTT, J. **IBM Mainframes – 45+ years of evolution**. IBM, 201046p. *Disponível em:* <http://www.vm.ibm.com/devpages/jelliott/pdfs/zhistory.pdf>. *Acesso em:* 04 abr. 2012.

Fórum de mainframes. *Disponível em:* <http://www.mainframes.com.br/viewtopic.php?f=68&t=921>. *Acesso em:* 18 maio 2012.

FREITAS, L. F.; GIROTTO, D.; KUROIWA, T. H.; BETINI, B.; BARCELLOS, M. **Mainframe.** *Disponível em:* <http://tegrupo7.wordpress.com/>. *Acesso em:* 04 abr. 2012.

GUIA DE GERENCIAMENTO. **Resource Access control facility do OS/390**. *Disponível em:* <http://publib.boulder.ibm.com/tividd/td/user_admin/GC32-0660-02/pt_BR/HTML/admusrgd21.htm#Header_44>. *Acesso em:* 18 maio 2012.

IAM SUCCESS TIPS. **Mainframe security and identity access management**. *Disponível em:* < http://www.iamsuccesstips.com/mainframe-security-identity-access-management-iam>. *Acesso em:* 23 maio 2012

IBM. **Aniversário do mainframe**. *Disponível em:* <http://www-03.ibm.com/press/br/pt/presskit/27169.wss>. *Acesso em:* 04 abr. 2012.

IBM. **Introduction to the new Mainframe**.IBM Corp, 2006. 36p. *Disponível em:* <http://wwwlgis.informatik.unil.de/cms/fileadmin/users/kschmidt/mainframe/lutzkuehner/Chapter02_Hardware_systems_and_LPARs_slides.pdf>. *Acesso em:* 18 maio 2012

IBM. **Mainframes photos album.** *Disponível em:* <http://www-03.ibm.com/ibm/history/exhibits/mainframe/mainframe_album.html >. *Acesso em:* 04 abr. 2012.

IBM. **Planning for CA – ACF2 migration to OS/390 security sever(RACF).** IBM Corp, 1995. 116p. *Disponível em:* <http://pt.scribd.com/doc/92411947/58/System-Authorization-Facility-SAF-and-RACF>. *Acesso em:* 18 maio 2012.

IBM. **RACF security guide**. IBM Corp, 2011. 400p. *Disponível em:* <http://publib.boulder.ibm.com/infocenter/cicsts/v3r2/topic/com.ibm.cics.ts.doc/pdf/dfht5c00.pdf>. *Acesso em:* 23 maio 2012

IBM. **SAN fabric**. *Disponível em:* <http://www03.ibm.com/systems/networking/switches/san/enterprise/index.html>. *Acesso em:* 18 maio 2012.

IBM. **Secure key solution with the common cryptographic architecture application programmer's guide**. IBM Corp, 2007. 362p. *Disponível em:* <http://www-03.ibm.com/security/cryptocards/pdfs/SC33-8294-00.pdf>. *Acesso em:* 24 maio 2012

IBM. **z/OS basic skills information center**. *Disponível em:* <http://publib.boulder.ibm.com/infocenter/zos/basics/index.jsp?topic=/com.ibm.zos.zmainframe/zconc_mfhwterms.html>. *Acesso em:*

IBM. **z/OS security sever RACF auditor's guide**. *Disponível em:* < http://publib.boulder.ibm.com/infocenter/zos/v1r11/index.jsp?topic=/com.ibm.zos.r11.icha800/abstract.htm>. *Acesso em:* 24 maio 2012

ORLANDO, D. **Modelos de serviços de computação em nuvem, parte 3: software como serviço**. *Disponível em:* < http://www.ibm.com/developerworks/br/cloud/library/cl-cloudservices3saas/>. *Acesso em:* 18 maio 2012.

OVERBY, L. **z/OS communications server network security overview**. IBM Corp, 2011. 53p. *Disponível em:* <http://proceedings.share.org/client_files/Share_in_Orlando_2/Session_9250_handout_1315_0.pdf >. *Acesso em:* 18 maio 2012.

PONTES, H. B. **Topologia do SNA (System Network Architecture).** *Disponível em:* <http://apconcursos.blogspot.com.br/2008/04/topologia-sna-system-network.html>. *Acesso em:* 20 abr. 2012.

Protocol suites. *Disponível em:* <http://techprep.mv.cc.il.us:8082/netware/Nettech/html_10/NETECH10.html >. *Acesso em:* 01 abr. 2012.

RACF security - audit and administration. *Disponível em:* < http://www.racfra2.com/introduction/page85/page85.html>. *Acesso em:* 24 maio 2012

REDAÇÃO DA COMPUTERWORLD**. Mobilidade e nuvens são chave no futuro do mainframe, diz estudo**. *Disponível em:* <http://computerworld.uol.com.br/tecnologia/2011/10/11/mobilidade-e-nuvem-sao-chave-no-futuro-do-mainframe-diz-estudo/ >. *Acesso em:* 30 mar. 2012.

REGIS MAINFRAME. **Segurança**. *Disponível em:* <http://regismain.wikidot.com/seguranca>. *Acesso em:* 18 maio 2012.

SALES, D.F. **SNA & Frame relay**. *Disponível em:* <http://www.logicengenharia.com.br/mcamara/ALUNOS/SNA%26Frame.PDF>. *Acesso em:* 20 abr. 2012.

SDLC: Link control synchronous data por IBM. *Disponível em:* <http://www.javvin.com/protocolSDLC.html>. *Acesso em:* 10 maio 2012.

TAURION, C. **Bar do Z um bate papo informal sobre mainframes**. 2009. 26p. *Disponível em:* <http://www.smashwords.com/extreader/read/3245/1/bar-do-z-um-bate-papo-informal-sobre-mainframes>. *Acesso em:* 04 abr. 2012.

THE Z-AGE. **Started task ID – classified**. *Disponível em:* <http://arjungutha.blogspot.com.br/>. *Acesso em:* 20 abr. 2012.

WELLER, R.; CLEMENTS, R.; DUGDALE, K.; FREMSTAD, P.; HERNANDEZ, O.; JOHNSTON, W. C.; KAPPELER, P.; KOCHERSBERGER, L.; TEDLA, A.; THOMPSON, J.; VENKATRAMAN, A. **Introduction to the new Mainframe: security.** IMB Corp, 2007. 524p. *Disponível em:* <http://www.redbooks.ibm.com/redbooks/pdfs/sg246776.pdf>. *Acesso em:*