UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

IBRAIM DE SOUSA REZENDE

Disponibilidade, Desempenho e Segurança do Ambiente de Tecnologia da Informação com Acordo de Nível de Serviços utilizando ATM

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para obtenção do grau de Mestre em Ciência da Computação

Professor Orientador: João Bosco Mangueira Sobral, Dr.

Florianópolis, Abril de 2002

Disponibilidade, Desempenho e Segurança do Ambiente de Tecnologia da Informação com Acordo de Nível de Serviços utilizando ATM

IBRAIM DE SOUSA REZENDE

Esta Dissertação foi julgada adequada para obtenção do Título de Mestre em Ciência da Computação, Especialidade Sistemas de Computação, e aprovada na sua forma final pelo programa de pós-graduação em ciência da computação

Fernando Álvaro Ostuni Gauthier, Dr
Coordenador do Programa de pós-graduação em Ciência da Computação

Banca Examinadora

João Bosco Mangueira Sobral, Dr
Orientador

Aloysio de Castro Pinto Pedroza, Dr
COPPE UFRJ

Roberto Willrich, Dr

Mirella Sechi Moretti Annoni Notare, Dra

Dedico este trabalho ao meu pai, Antônio;
Minha mãe, Zélia;
Minha esposa, Elza;
Minha filha, Maíra;
Meu filho, Ícaro.

Agradeço à equipe de professores que se dedicaram ao curso de Mestrado em Ciência da Computação fora da sede em convênio com a UNIRONDON:

Prof. Fernando Álvaro O. Gauthier, Dr - Coordenador do CPGCC.

Prof. João Bosco M. Sobral, Dr. – Coordenador Executivo.

Prof. Jorge Muniz Barreto, Dr – UFSC.

Prof. Ricardo Felipe Custódio, Dr. – UFSC.

Prof. Ricardo Pereira e Silva, Dr. – UFSC.

Prof. Luiz Carlos Zancanella, Dr. – UFSC.

Prof. Carlos Becker Westphall, Dr. – UFSC.

Prof. Paulo Sérgio da Silva Borges, Dr. – UFSC.

Prof. Fábio F. Campos, MSc. – UFSC.

Profa. Daniela Barreiro Claro, MSc. – UFSC.

Prof. Cristiano Maciel, MSc. – UNIRONDON.

Agradeço especialmente ao meu professor orientador pela confiança e incentivo, à diretoria do Cepromat pela oportunidade e a todos que de alguma forma contribuíram para conclusão deste trabalho.

RESUMO.

Este trabalho apresenta uma proposta para implementação de recursos visando assegurar uma alta disponibilidade e segurança do ambiente de Tecnologia da Informação. São considerados os aspectos do Acordo de Nível de Serviço (SLA - *Service Level Agreement*) e a implementação da tecnologia ATM(*Asynchronous Transfer Mode*) integrada às redes convencionais. O trabalho apresenta algumas propostas para as diretrizes de segurança da informação de uma organização, visando preservar a confidencialidade, integridade e disponibilidade das informações da instituição. As propostas são aplicáveis aos sistemas informatizados e aos meios convencionais de processamento, comunicação e armazenamento de informações. O trabalho pretende fomentar a busca de orientação para a conduta considerada adequada aos negócios e aos objetivos da organização. São recomendadas tecnologias adequadas ao backbone da rede e ao *Server Farm*, apontando os pontos indispensáveis para manter uma disponibilidade de acordo com as exigências de um SLA. São sugeridas políticas de proteção das informações contra destruição, modificação e divulgação indevida, quer sejam acidentais ou intencionais. São destacadas as alternativas do LANE como serviço de integração das LANs convencionais ao ATM e o VRRP - *Virtual Route Redundance Protocol* como serviço de aumento da disponibilidade no *backbone* ATM e no *Server Farm*. São discutidas as questões da qualidade de serviços(QoS) fim-a-fim.

ABSTRACT.

This work presents a proposal for specification of resources seeking to assure a high readiness and safety of the atmosphere of Technology of the Information. The aspects of the Agreement of Level of Service are considered (SLA - Service Level Agreement) and the implementação of the technology ATM(Asynchronous Transfer Mode) integrated into the conventional nets. The work presents some proposals for the guidelines of safety of the information of an organization, seeking to preserve the privacy, integrity and readiness of the information of the institution. The proposals are applicable to the computerized systems and the conventional means of processing, communication and storage of information. The work intends to foment the orientation search for the considered conduct adapted to the business and the objectives of the organization. Technologies adapted to the backbone of the net and Server Farm are recommended, aiming the indispensable points to maintain a readiness in agreement with the demands of a SLA. They are suggested politics of protection of the information against destruction, modification and improper popularization, wants they are accidental or intentional. They are outstanding the alternatives of LANE as integration service of the conventional LANs to ATM and VRRP - Virtual Route Redundance Protocol as service of increase of the readiness in the backbone ATM and in Server Farm. The subjects of the quality of services(QoS) end-to-end will be discussed.

SUMÁRIO

ANEXOS

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

SIGLA	Descrição
AAL	ATM ADAPTION LAYER
ABR	AVAILABE BIT RATE
ABT	ATM BLOCK TRANSFER
ACL	ACCESS CONTROL LIST
ACK	ACKNOWLEDGEMENT
ACR	ALLOWED CELL RATE
ACSE	ASSOCIATION CONTROL SERVICE ELEMENT
A&G	ADMINISTRAÇÃO E GERÊNCIA
ADAESI	ADABAS EXTERNAL SECURITY INTERFACE
ANOVA	ANALISIS OF VARIANCE
ASN.1	ABSTRACT SYNTAX NOTATION 1
ANSI	AMERICAN NATIONAL STANDARDS INSTITUTE
APDU	APPLICATION PROTOCOL DATA UNIT
API	APPLICATION PROCESS INTERFACE
ARP	ADRESS RESOLUTION PROTOCOL
ASCII	AMERICAN STANDARD CODE FOR INFORMATION INTERCHANGE
ATC	ATM TRANSFER CAPABILITY
ATM	ASYNCHRONOUS TRANSFER MODE
ATMARP	ASYNCHRONOUS TRANSFER MODE ADDRESS RESOLUTION PROTOCOL
BER	BIT ERROR RATE
BD	BANCO DE DADOS
BDLC	BURROUGS DATA LINK CONTROL
BGP	BORDER GATEWAY PROTOCOL
B-ISDN	BROADBAND ISDN
BT	BURST TOLERANCE
BUS	BROADCAST AND UNKNOWN SERVER
BOA	BASIC OBEJECT ADAPTER
CAC	CONNECTION ADIMISION CONTROL

CBR	CONSTANTE BIT RATE
CBQ	CLASS BASED QUEUING
CCITT	COMITÉ CONSULTATIF INTERNATIONAL DE TÉLÉGRAPHIQUE ET TÉLÉPHONIQUE
CDV	CELL DELAY VARIATION
CDVT	CELL DELAY VARIANCE TOLERANCE
CER	CELL ERROR RATIO
CET	CELL EMISSION TIME
CFQ	CLASS-BASED FAIR QUEUING
CIDR	CLASSLESS INTER – DOMAIN ROUTING
CGI	COMMON GATEWAY INTERFACE
CLI	CERTIFICATE LIBRARY INTERFACE
CLP	CELL LOSS PRIORITY
CLR	CELL LOSS RATIO
CLS	CONNECTION - LESS SERVERS
CMISE	COMMON MANAGEMENT INFORMATION ELEMENT
CMR	CELL MISINSERTION RATIO
CMIP	COMMON MANAGEMENT INFORMATION PROTOCOL
CMTC	Cadeias de Markov de Tempo Contínuo
CPCS	COMMON PART CONVERGENCE SUBLAYER
CPU	CENTRAL PROCESSOR UNIT
CRC	CYCLIC REDUNDANCY CHECK
CRF	CELL RELAY FAQ
CRM	CUSTOMER RELATIONSHIP MANAGEMENT
CTD	CELL TRANSFER DELAY
CTP	CONTROLLED TRAFFIC PARAMETERS
COM	COMPONENT OBJECT MODEL
CORBA	COMMON OBJECT REQUEST BROKER ARCHITECTURE
CODEC	DODIFICADOR-DECODIFICADOR
COTEC	CONSELHO ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO
DBR	DETERMINISTIC BIT RATE
DBA	DATABASE ADMINISTRATOR

DES	DATA ENCRYPTION STANDARD
DII	DYNAMIC INVOCATION INTERFACE
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL
DNS	DOMAIN NAME SYSTEM
DLI	DATA – STORAGE LIBRARY MODULE
DLL	DYNAMIC LINK LIBRARY
DLM	DATA – STORAGE LIBRARY MODULE
DIS	DRAFT INTERNATIONAL STANDARD
DAS	DIGITAL SIGNATURA ALGORITHM
DoD	DEPARTAMENTO DE DEFESA AMERICANA
DMI	Design & Manufacturing Institute's
DMZ	DEMILITARIZED ZONE
DQDB	DISTRIBUTED QUEUE DUAL BUS
DP	DRAFT PROPOSAL
DSCP	DIFFERENTIATED SERVICE CODE POINT
ECB	EXTENSION CONTROL BLOCK
EFCI	EXPLICIT FORWARD CONGESTION INDICATION
ELAN	LAN EMULADA
EPD	EARLY PACKET DISCARD
FEC	FOWARD ERROR – DETECTION
FER	BIT ERROR FRAME
FCAPS	FAULT, CONFIGURATION, ACCOUNTING, PERFORMANCE, SECURITY
FDDI	FIBER DISTRIBUTED DATA INTERFACE
FIFO	FIRST - IN FIRST – OUT
FTAM	FILE TRANSFER, ACCESS AND MANAGEMENT
FTP	FILE TRANSFER PROTOCOL
GIOP	GENERAL INTER – ORB PROTOCOL
GFC	GENERIC FLOW CONTROL
GCRA	GENERIC CELL RATE ALGORITHM
GPS	GENERALIZED PROCESSOR SHARING
HEC	HEADER CHECK ERROR
HDLC	HIGHLEVEL DATA LINK CONTROL

HMMP	HYPERMEDIA MANAGEMENT PROTOCOL
HDTV	HIGH DEFINITION TELEVISION
HTML	HYPER TEXT MARKUP LANGUAGE
HTTP	HYPER TEXT TRANSMISSION PROTOCOL
IAB	INTERNETACTIVIES BOARD
IC	ÍNDICE DE CONTROLE
IASG	INTERNET ADDRESS SUMMARIZATION GROUPS
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
IEEE	INSTUTE OF ELETRICAL AND ELETRONIC ENGINEERS
IDS	DETECTOR DE INTRUSÕES
IESG	INTERNET ENGNEERING STEERING GROUP
IETF	INTERNET ENGNEERING TASK FORCE
IDAPI	INTEGRATED DATABASE APLICATION PROGRAM INTERFACE
ILMI	INTEGRATED LOCAL MANAGEMENTE INTERFACE
IMP	INTERNATIONAL MEASURAMENTE POINT
IGMP	INTERNET GROUP MANAGMENT PROTOCOL
ISDN	INTEGRATED SERVICES DIGITAL NETWORK
IP	NTERNET PROTOCOL
IPC	INTER PROCESS COMMUNICATION
IPOA	NTERNET PROTOCOL OVER ATM
IPV4	NTERNET PROTOCOL VERSION 4
IPV6	NTERNET PROTOCOL VERSION 6
IPX	INTERNETWORK PACKED EXCHANGE
ISSLL	INTEGRATEG SERVICES OVER SPECIFIC LINK LAYERS
ISSO	INTERNATIONAL STANDARD ORGANIZATION
ITU-T	INTERNATIONAL TELECOMMUNICATION UNION
JRE	JAVA RUNTIME ENVIRONMENT
LAN	LOCAL AREA NETWORK
LANE	LAN EMULATION
LDAP	LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL
LDP	LABEL DISTRIBUTION PROTOCOL
LE ARP	LAN EMULATION ADDRESS RESOLUTION PROTOCOL

LEC	LAN EMULATION CLIENT
LECS	LAN EMULATION CONFIGURATION SERVER
LES	LAN EMULATION SERVER
LIS	LOGICAL IP SUBNET
LLC/SNAP	LOGICAL LINK CONTROL / SUBNETWORK ACCESS PROTOCOL
LNNI	LANE NETWORK TO NETWORK INTERFACE
LSP	LABEL SWITCHED PATH
LSR	LABEL SWITCH ROUTER
LUNI	LAN EMULATION USER NETWORK INTERFACE
MAC	MEDIA ACCESS CONTROL
MAN	METROPOLITAN AREA NETWORK
MBS	MAXIMUM BURST SIZE
MBR	MAXIMUM BURST RATE
MCR	MINIMUM CELL RATE
MCSN	MONITORING CELL SEQUENCE NUMBER
MFS	MAXIMUM FRAME SIZE
MHS	MESSAGE DIGEST – 5
MIB	MANAGEMENT INFORMATION BASE
MP	MEASURAMENT POINT
MPLS	MULTIPROTOCOL LABEL SWITCHING
MPT	MEASURAMENT POINT AT Tb
MPOA	MULTIPROTOCOL OVER ATM
MPEG	MOTION PICTURE EXPERTS GROUP
MMF	MULTI – MODE FIBER
NCTP	NON CONTROLABLE TRAFFIC PARAMETERS
NHS	NEXT HOP SERVER
NHRP	NEXT HOP ROUTING PROTOCOL
NIC	NETWORK INTERFACE CARD
NIST	NATIONAL INSTITUTE OS STANDARDS AND TECHNOLOGY
NFS	NETWORK FILE SYSTEM
NNI	NETWORK – NETWORK INTERFACE
NNTP	NETWORK NEWS TRANSFER PROTOCOL

N-ISDN	NARROWBAND – INTEGRATED SERVICES DIGITAL NETWORK
NRT-VBR	NON – REAL – TIME VARIABLE BIT RATE
NP	NETWORK PERFORMANCE
NPC	NETWORK PARAMETERS CONTROL
OAM	OPERATION AND MAINTENANCE
OAM&P	OPERATIONS, ADIMINISTRATION, MAINTENANCE, PROVISIONING
OC	OPTICAL CARRIER
OSI	OPEN SYSTEM INTERCONNECTION
OSPF	OPEN SHORTEST PATH FIRST
P2P-CDV	PEAK - TO – PEAK CELL DELAY VARIATION
PAD	PACKET ASSEMBLY AND DESASSEMBLY
PABX	PRIVATE AUTOMATIC BRANCH EXCHANGE
PCM	PULSE CODE MODULATION
PCR	PEAK CELL RATE
PICS	PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENTS
PIXIT	PROTOCOL IMPLEMENTATION EXTRA INFORMATION FOR TESTING
PDU	PROTOCOL DATA UNITS
PDH	PLESIOCHRONOUS DIGITAL HIERARCHY
PDCA	PLAN, DO, CHECK, ACTION
PER	BIT ERROR PACKAGE
PPP	POINT - TO – POINT PROTOCOL
PL	PHYSICAL LAYER
PM	PERFORMANCE MONITORING
PNNI	PRIVATE NETWORK – NETWORK INTERFACE
PT	PAYLOAD TYPE
PTI	PAYLOAD TYPE INDENTIFIER
PVC	PERMANENTE VIRTUAL CIRCUIT
QoS	QUALITY OF SERVICE
RACF	RESOURCE ACCESS CONTROL FACILITY
RAS	REMOTE ACCESS SERVICES
RDSI	REDE DIGITAL DE SERVIÇOS INTEGRADOS
RDSI-FE	REDE DIGITAL DE SERVIÇOS INTEGRADOS – FAIXA ESTREITA

RDSI-FL	REDE DIGITAL DE SERVIÇOS INTEGRADOS – FAIXA LARGA
RED	RANDON EARLY DETECTION
RIP	ROUTING INFORMATION PROTOCOL
RFC	REQUEST FOR COMMENTS
RM – OSI	REFERENCE MODEL – OPEN SYSTEM INTERCONNECTION
RPC	REMOTE PROCEDURE CALL
RTP	REAL TIME TRANSFER PROTOCOL
RTT	ROUND TRIP TIME
RSVP	RESOURCE RESERVATION PROTOCOL
RSA	RIVEST, SHAMIR & AADLEMAN ALGORITHM
RT-VBR	REAL – TIME VARIABLE BIT RATE
ROSE	REMOTE OPERATIONS SERVICE ELEMENT
SAP	SERVICE ACCESS POINT
SAR	SEGMENTATION AND REASSEMBLY
SBR	STATISTICAL BIT RATE
SBM	SUBNET BANDWIDTH MANAGEMENT
SCR	SUSTAINED CELL RATE
SDLC	SYNCHRONOUS DATA LINK CONTROL
SDH	SYNCHRONOUS DIGITAL HIERARCHY
SECBR	SEVERELY ERRORED CELL BLOCK RATIO
SFQ	STOCHASTIC FAIR QUEUING
SGBD	SISTEMA GERENCIADOR DE BANCO DE DADOS
S-HTTP	SECURE HYPERTEXT TRANSFER PROTOCOL
SIPP	SIMPLE INTERNET PROTOCOL PLUS
SMI	STRUCTURE OF MANAGEMENT INFORMATION
SMDS	SWITCHED MULTIMEGABIT DATA SERVICE
SMF	SINGLE MODE FIBER
SMTP	SIMPLE MAIL TRANSFER PROTOCOL
SMP	Semi-Markov Process
SNMP	SIMPLE NETWORK MANAGEMENT PROTOCOL
SONET	SYNCHRONOUS OPTICAL NETWORK
ST-II	STREAM PROTOCOL VERSION II

STM	SYNCHRONOUS TRANSFER MODULE
SSN	SWITCHING / SIGNALING NODE
STP	SHIELDED TWISTED PAIR
STS	SYNCHRONOUS TRANSPORT SIGNAL
SLA	SERVICE LEVEL AGREEMENT
SMDS	SWITCHED MULTIMEGABIT DATA SERVICE
SNA	SYSTEM NETWORK ARCHITECTURE
SNM	SUNNET MANAGER
SSCS	SERVICE SPECIFIC CONVERGENCE SUBLAYER
SVC	SWITCHED VIRTUAL CHANEL
SSL	SECURE SOCKET LAYER
SYN	SYNCRONIZING SEGMENT
Tmax	TIMER FOR DECLARING A CEL LOST
TCB	TRUSTED COMPUTING BASE
TCP	TRANSMISSION CONTROL PROTOCOL
TCP/IP	TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL
TMN	TELECOMUNICATIONS MANAGEMENT NETWORK
TOS	TYPE OF SERVICE
TI	TECNOLOGIA DA INFORMAÇÃO
TQC	CONTROLE DA QUALIDADE TOTAL
TD	TRAFFIC DESCRIPITOR
TUC	TOTAL USER CELL
UAS	UNIFORM ANIVAL AND SERVICE
UDP	USER DATAGRAM PROTOCOL
UBR	UNSPECIFIED BIT RATE
UNI	USER NETWORK INTERFACE
URL	UNIFORM RESOURCE LOCATOR
UPC	USER PARAMETER CONTROL
UTP	UNSHIELD TWISTED PAIR
VBR	VARIABLE BIT RATE
VC	VIRTUAL CHANNEL
VCC	VIRTUAL CHANNEL CONNECTION

VCI	VIRTUAL CHANEL IDENTIFIER
VoIP	Voice over IP
VLAN	VIRTUAL LAN
VP	VIRTUAL PATH
VPI	VIRTUAL PATH IDENTIFIER
VPC	VIRTUAL PATH CONNECTION
VPN	VIRTUAL PRIVATE NETWORK
VRRP	VIRTUAL ROUTER REDUNDANCY PROTOCOL
WEB	WORLD WIDE WEB – WWW
WEBM	WORLD WIDE WEB MANAGEMENT
WAN	WIDE AREA NETWORK
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin
WWW	WORLD WIDE WEB

1 - Introdução

A diferença de poder entre organizações e países pode ser medida em termos de produção de toneladas de aço, toneladas de grãos, barris de petróleo, quantidades de ogivas nucleares e capacidade de processamento. Hoje, o poder de países e organizações é mais dependente da sua capacidade de transferência da informação rápida e segura, que varia no âmbito de imagens de satélite de estratégia militar, condições climáticas, geológicas, fluxo de informação financeira entre organizações e o uso de bancos 24 horas por consumidores. Se este fluxo de informação é rompido ou é alterado, os efeitos para países, organizações e indivíduos podem ser severos ou até mesmo desastrosos.

A ampliação da demanda de comercialização de bens e serviços aumentou a complexidade dos ambientes de Tecnologia da Informação(TI) das empresas, suas aplicações passaram a utilizar transmissão de dados voz e imagens, trazendo a fusão natural da informática com as telecomunicações, aumentando em muito a quantidade de variáveis envolvidas, tornando cada vez mais difícil e complexa a gestão de um ambiente de TI.

As empresas precisam adotar estratégias de captar e reter seus clientes utilizando a infra-estrutura de TI como base do CRM (*Customer Relationship Management*).

A estrutura globalizada exige do ambiente de TI uma parceria com mão de obra especializada, flexibilidade e agilidade em mudanças, rapidez na atualização de equipamentos e sistemas, disponibilidade de 24 horas por dia, 7 dias por semana durante todo o ano. Segurança com nível de confiabilidade máxima, interoperabilidade com os sistemas dos parceiros, custos operacionais reduzidos e contrato de nível de serviços.

No ambiente de TI, a infra-estrutura de gerência de redes envolve três elementos fundamentais: segurança física e lógica, redundância e nível de serviços.

A segurança física abrange itens como restrições de acesso, sistemas de vigilância, gabinetes lacrados, instalações elétricas adequadas, sistemas de cabeamento estruturado, sistemas de *nobreak*, grupo motor-gerador, mecanismos de proteção contra descargas atmosféricas, mecanismos de proteção contra surtos de tensão, sistema de prevenção e combate a incêndios, sala cofre, guarda física da mídia em ambiente que garanta sua vida útil e apólice de seguro contra sinistros.

A segurança lógica tem como objetivo garantir a consistência à integridade e a atomicidade das transações realizadas sobre as bases de dados. O ambiente deve estar sempre configurado de forma a garantir proteção contra vírus, *hacker*, roubo de informações, sabotagem, adulteração de dados, fraude, queda de performance e erros.

Um ambiente seguro deve proteger as informações da organização dentro e fora do seu ambiente de TI. Para se proteger de dentro, as organizações confiam em auditorias internas, para se proteger do exterior, tem que usar tecnologia especial específica para uma organização. Esta tecnologia especial é um conjunto de *firewalls*, que protege o ambiente interno do mundo externo e só permite os protocolos e serviços adotados em uma política de segurança incorporada. Os *firewalls* tem muitas características úteis, tais como autenticação, detecção de vírus, detecção de intrusão, sendo sua meta principal a de proteção.

A redundância deve abranger fontes de energia elétrica, sistemas de *nobreack*, grupos-geradores, sistemas de ar condicionado, *links* de conexão da rede, largura de banda, servidores em rede e o espelhamento de dados. A estrutura redundante deve estar sempre pronta para garantir a disponibilidade do ambiente em caso de queda ou manutenção do sistema principal. O ideal é que uma estrutura redundante seja montada em local diferente do ambiente principal.

O Acordo de Nível de Serviços (*SLA -Service Level Agreement*) constitui-se em uma valiosa ferramenta para provimento de serviços, assim como para acompanhamento de serviços de Clientes. A construção de um SLA requer compromisso sério das partes envolvidas, definição de responsabilidades, definição do processo contínuo, definição das ações corretivas e documentação do acordo.

O SLA deve definir claramente quais requisitos devem ser garantidos para que a(s) aplicação(ões) possam executar com qualidade. Um exemplo típico de SLA para uma aplicação de voz sobre IP (VoIP) com algumas centenas de canais de voz simultâneos numa rede IP WAN poderia ser: **Vazão** maior que 2 Mbps; **Atraso** máximo de 250 mseg; **Disponibilidade** acima de 99,4%.

Outro aspecto a ser considerado é a análise periódica de vulnerabilidades do ambiente de TI utilizando o ciclo PDCA(*Plan-Do-Check-Action*) das metodologias de Qualidade Total, a elaboração e implementação de uma política de segurança dinâmica, baseada em diretrizes visando preservar a confidencialidade, integridade e

disponibilidade das informações, gerando subsídios para continuidade do Acordo de Nível de Serviços (SLA).

A tendência dos modelos de Administração e Gerência de Redes(A&G) é de se tornarem cada vez mais pró-ativos com o crescimento da exigência do nível de serviços prestados, integrando aos sistemas de automação predial e metropolitano.

Uma vez definida e medida a qualidade do serviço (QoS), os administradores mostram o que estão oferecendo em seu domínio de rede e os usuários podem exigir uma qualidade de serviço dentro dos parâmetros previstos no contrato do SLA.

A plataforma de gerência de redes tem seu papel fundamental como elemento de suporte às avaliações de performance e nível de serviço, oferecendo as descobertas automatizadas, controlando os elementos ligados à rede apresentando mapas com níveis de detalhes, verificando status das variáveis das MIBs, atualizando base de dados para ação dos agentes e respondendo a alarmes dos Traps SNMP(Anexo-08).

Os sistemas convencionais de gerência corporativa procuram aderir aos padrões abertos tais como TMN(OSI), SNMP(redes), DMI(sistemas) e ambiente WEB. A maioria dos sistemas de gerência de redes fornece APIs que mapeiam suas camadas permitindo integração das soluções dos usuários. Através de ferramentas disponibilizadas para o ambiente WEB podem ser realizadas consultas SNMP para acessar em tempo real as informações contidas nas MIBs dos elementos ativos de rede permitindo sua visualização através do ambiente Internet.

A área de Inteligência Artificial no âmbito da Inteligência Computacional com suas Redes Neurais, a sua Lógica Nebulosa ou Lógica Difusa(*Fuzzy Logic*) contribuem para automação do ambiente de TI. O sistema composto por agentes que utilizam a tecnologia de redes neurais pode prever falhas antes que elas ocorram ou antecipar tomadas de decisões para, por exemplo, monitorar os índices do SLA, evitar problemas de performance de um segmento de rede, de um elemento ativo de rede ou de um link para acesso à Internet. Esses agentes são capazes de se adaptarem aprendendo e observando a carga dos sistemas ao longo do tempo, podendo lidar com a performance do ambiente de rede, a sua disponibilidade e acompanhar os índices do SLA. Os agentes de gerenciamento em múltiplos níveis podem estar localizados em qualquer lugar da rede, coletando e filtrando dados para os gerentes que se interagem em uma rede corporativa distribuída. A tecnologia de agentes permite a implementação da gerência

dos diversos ambientes nas áreas de segurança e administração das redes corporativas. A tecnologia *Data Warehouse* pode ser empregada para manter informações de toda a organização relacionadas ao tempo. Os *Data Marts* podem ser criados de acordo com cada contrato de serviços(SLA). A técnica de *Data Mine* pode ser utilizada para coletar e armazenar informações estratégicas de apoio a decisões. A tecnologia JAVA e CORBA contribui para facilitar o desenvolvimento de soluções em ambientes distribuídos. A tecnologia ATM contribui para aumento da largura de banda dos backbones, possibilitando a transmissão de dados voz e imagens com o investimento em uma única tecnologia.

1.1 - Objetivos

Este trabalho apresenta uma proposta para implementação de recursos visando assegurar uma alta disponibilidade e segurança do ambiente de Tecnologia da Informação, considerando-se os aspectos do Acordo de Nível de Serviço (SLA - *Server Level Agreement*), implementação da tecnologia ATM integrada às redes convencionais, apresentando alguns exemplos das Diretrizes de Segurança da Informação de uma organização, visando preservar a confidencialidade, integridade e disponibilidade das informações da instituição. A proposta é aplicável aos sistemas informatizados e aos meios convencionais de processamento, comunicação e armazenamento de informações.

O trabalho pretende fomentar a busca de orientação para a conduta considerada adequada aos negócios e aos objetivos da organização, recomendando uma tecnologia adequada ao backbone da rede, apontando os pontos indispensáveis para manter uma disponibilidade de acordo com as exigências de um SLA entre o provedor do ambiente de TI e seus usuários, sugerindo políticas de proteção das informações contra destruição, modificação e divulgação indevida, quer sejam acidentais ou intencionais. As diretrizes sugeridas atingiriam seu objetivo após serem divulgadas, conhecidas e seguidas por todos os colaboradores e parceiros de forma a preservar a imagem da organização e manter seu ambiente de TI dentro de um nível de disponibilidade e integridade conforme o acordo de nível de serviços SLA.

1.2 – Área de abrangência

Segurança e disponibilidade do ambiente TI com acordo de Nível de Serviços (SLA) utilizando a tecnologia ATM em sua topologia de rede.

1.3 – Ambiente contemplado

Qualquer organização com missão de prover Tecnologia da Informação como instrumento de seu negócio.

1.4 – Ambiente de desenvolvimento

A instituição escolhida para realização do trabalho é o CEPROMAT – Centro de Processamento do Estado de Mato Grosso, órgão responsável pela administração da INFOVIA-MT, que tem como missão prover Tecnologia de Informação como instrumento de Gestão Pública, contribuindo para a racionalização de seus recursos aproximando Estado e Cidadão.

A INFOVIA-MT tem como objetivo integrar através de uma rede de comunicação de alta performance e confiabilidade, todos os órgãos do Governo do Estado de Mato Grosso, tanto os localizados no complexo do Centro Político Administrativo, como os localizados na área Metropolitana (Cuiabá/Várzea Grande) e os do interior do Estado, constituindo assim a INFOVIA-MT, a qual permitirá o tráfego simultâneo de voz, dados e imagens, disponibilizando a infra-estrutura necessária para a modernização dos serviços prestados ao cidadão com agilidade, qualidade e segurança.

As implementações serão realizadas utilizando os elementos ativos da Rede INFOVIA-MT(Anexo-03), sendo escolhido um ambiente piloto como laboratório para as avaliações[PIC99].

1.5 – Motivação

O CEPROMAT – Centro de Processamento de Dados do Estado de Mato Grosso tem a missão de prover Tecnologia de Informação como instrumento de Gestão Pública, contribuir para a racionalização de seus recursos aproximando Estado e o Cidadão. O projeto INFOVIA-MT foi elaborado com objetivos de ser um instrumento para garantir ao cidadão disponibilidade, agilidade e integridade no atendimento por

parte da administração pública da Estado de Mato Grosso. Reconhece-se que é um direito e uma necessidade cada vez maior dos usuários, o acesso às facilidades de comunicação tais como: transferência de arquivos, login remoto, acesso à base de dados remotos, correio eletrônico, serviços de voz serviços de videoconferência via redes. Faz-se necessário manter tecnologias e procedimentos que garantam a segurança e a disponibilidade dos ambientes de Tecnologia da Informação interligados, permitindo ao usuário autorizado o acesso aos recursos desejados de modo seguro e confiável, garantindo a integridade dos dados que fluem na rede, garantindo a atomicidade das aplicações, garantindo a identificação dos interlocutores, impedindo acessos não autorizados, impedindo alterações ou destruições indevidas das informações, garantindo a disponibilidade dos recursos para os usuários legítimos.

Os orçamentos para Informática são atualmente um dos que mais recursos movimentam em compras de equipamentos e software nos órgãos do governo Estadual em seus diversos programas de modernização originados de várias fontes. Visando atingir os objetivos do COTEC de minimizar os investimentos compartilhando os recursos adquiridos de hardware e software, minimizando a pirataria através da implantação do controle de gerenciamento de licenças em todo o Estado, minimizando a contratação de circuitos de dados através do compartilhamento de uma única rede para todos os órgãos do Estado, minimizando gastos com ligações telefônicas através da implementação dos serviços de voz.. Inicialmente a INFOVIA-MT implantada apenas para órgãos do executivo atraiu para si os outros poderes, como Tribunal de Contas, Tribunal de Justiça, Ministério da Justiça, Prefeituras e Assembléia Legislativa.

1.6 – Trabalhos correlatos

1.6.1 – Projeto da rede corporativa do Estado de Mato Grosso - INFOVIA – MT.

A INFOVIA-MT foi concebida pelo Governo do Estado de Mato Grosso para integrar, através de recursos da Tecnologia da Informação, todos os órgãos do Governo do Estado de Mato Grosso, tanto os localizados no complexo do Centro Político Administrativo, como os da área metropolitana (Capital e Várzea Grande) e os situados no Interior do Estado, constituindo assim a Rede Infovia-MT, a qual permitirá o tráfego simultâneo de voz, dados e imagens. A INFOVIA-MT disponibilizará a infra-estrutura

necessária para a modernização do Estado, provendo meios de comunicação com a eficiência e segurança exigidas para oferecer um atendimento de qualidade ao cidadão.

A Rede da Infovia-MT será composta de três malhas de redes de computadores, área do complexo do CPA, área Metropolitana(Cuiabá e Várzea Grande), o interior do Estado e uma administração central (CEPROMAT), que se encarregará das funções de gerenciamento destas malhas(Anexo-01).

1.6.1.1 Região do Centro Politico Administrativo – CPA

Nessa região será adotada rede de Fibra Óptica Multimodo, esta rede de fibra óptica dispõe de pontos estratégicos de distribuição (Caixas de Emenda e Distribuição Ópticas), os quais permitirão a interligação dos órgãos entre Secretarias de Estado, Empresas públicas, Autarquias e demais órgãos, todos localizados no Complexo do CPA, e afastados até no máximo 2 Km do DGO do Cepromat, que será o ponto de concentração do Backbone.

1.6.1.2 Região Metropolitana da Grande Cuiabá e Várzea Grande

Os órgãos do Governo localizados nestas localidades, e fora do Backbone óptico do CPA, poderão ser interligados diretamente ao CEPROMAT, através de links dedicados de Fibra óptica monomodo ou qualquer outro meio fisico que venha atender os requisitos desejados de qualidade e preço.

1.6.1.3 Interior do Estado de Mato Grosso

As localidades do interior do Estado de Mato Grosso, deverão ser contempladas com links de satélite, e/ou links terrestres(cabos de fibra óptica, sistemas de rádio-enlace). A partir dos Pontos de Acesso (ou Pontos de Concentração), os órgãos do interior do Estado aqui contemplado serão interligados ao CORE ATM do CEPROMAT, podendo passar por pontos intermediários de repetição de sinal. Os órgãos do Governo em cada localidade poderão ser interligados ao respectivo Ponto de Concentração da localidade.

1.6.2- Benefícios esperados com a implantação da rede proposta

Redução do tráfego de documentos impressos entre os órgãos do Estado, cujas aplicações utilizam o meio eletrônico. Isto contribuirá em muito para a redução dos custos com papel e sua tramitação, agilizando o andamento de processos e permitindo um atendimento rápido e de qualidade ao cidadão.

Ao permitir o gerenciamento centralizado de todas as redes locais dos órgãos atendidos pela rede corporativa, permitindo a descentralização através de domínios de gerência via software de gerenciamento de redes. Isto se traduzirá em um melhor aproveitamento dos recursos existentes, facilitando inclusive a ampliação do número de estações de atendimento em uso nos órgãos. As redes locais passarão a contar, então, com um padrão de qualidade e segurança controlado conforme estabelecido em um SLA, com os custos de administração reduzidos proporcionados pela administração dos IC's de forma centralizada;

Oferecer o transporte de voz; através da disponibilização uma rede de telefonia interna entre os órgãos do Governo do Estado de Mato Grosso, aqui contemplados, independente da rede pública, conectada ao Sistema de PABX Digital do Governo do Estado de Mato Grosso cujos sites centrais encontram-se no prédio da Central Telefônica 313 localizado no CPA. Permitir que os custos de comunicação fossem reduzidos através de investimentos em sua própria infra-estrutura, estabelecendo a qualidade dos serviços de comunicação desejados através de seus próprios critérios de priorização.

Oferecer a possibilidade de videoconferência aos usuários que estão em locais distantes participando de conferências em tempo real, permitindo reuniões entre órgãos e escritórios regionais sem a necessidade de deslocamento físico; na área executiva do governo, possibilitar debates entre equipes de trabalho, oferecer seminários, permitir o treinamento a distancia (formação profissional); contribuindo para a qualificação da mão-de-obra, permitindo um melhor aproveitamento dos recursos gastos com treinamento através da Escola do Servidor Publico, minimizando as dificuldades decorrentes das grandes dimensões do Estado de Mato Grosso.

Flexibilidade na escolha dos equipamentos e grande possibilidade de expansão. A rede corporativa do Estado tem, por princípio, o uso de padrões abertos e a interoperabilidade entre eles; esta, aliás, é uma tendência mundial, e no caso do Estado, uma necessidade. Aderindo aos padrões abertos, mantém-se a liberdade de escolha de fornecedores, oferecendo uma saída moderna e eficiente na substituição das antigas tecnologias proprietárias. Novamente, obtém-se redução de custos e melhoria na qualidade do atendimento aos usuários, possibilitando disponibilizar os dados corporativos a quem necessita deles para a tomada de decisões.

O Estado estará preparado para o futuro; todas as possibilidades de uso citadas acima estão se popularizando rapidamente. Em pouco tempo, elas deixarão de ser vantagens para se tornarem exigências; com o foco do Estado cada vez mais centrado na qualidade da prestação de serviços ao cidadão, torna-se imprescindível à existência de uma infra-estrutura que suporte ambos o crescimento na demanda por serviços e a melhora na qualidade dos mesmos. A rede corporativa do Estado oferecerá esta infra-estrutura, de forma ordenada e racionalizada, evitando o desperdício de recursos públicos, maximizando o retorno dos investimentos em informatização realizados no estado, favorecendo de forma decisiva a modernização da administração pública.

1.6.3-Disponibilidade e interoperabilidade da infra-estrutura central do Cepromat.

A infra-estrutura da administração Central que está localizada no Cepromat, conta com um sistema de aterramento interligado, projetado para eliminar os prejuízos decorrentes das descargas atmosféricas e surtos da rede elétrica, contendo pára-raios e protetores de surto, dois sistemas de grupo-motor-gerador prontos para entrar em funcionamento mediante uma falha de fornecimento da rede da concessionária de Energia Elétrica, dois sistemas de Nobreak com capacidade para atender todos equipamentos centrais, dois sistemas independentes de ar condicionado para manter o ambiente climatizado sem parada para manutenção, Core ATM e roteadores redundantes, servidores críticos redundantes, sistema de backup automático via robô, backup externo, sistema de gerência para garantir uma disponibilidade de 24 x 7.

O ambiente de segurança utiliza soluções de Firewall em servidores com placas ATM diretamente interligados as ELANS da cada órgão da administração estadual,

utilizando os produtos adquiridos tais como Firewall-1 da CheckPoint, IDS , firewall LINUX, Firewall OS/390 e ADAESI. As políticas de Segurança estão sendo implementadas a partir de um trabalho que foi elaborado por consultoria especializada, estruturando o CEPROMAT que é o órgão administrador da Infovia-MT e propagando as políticas através de propostas encaminhadas ao COTEC.

As aplicações do legado de todos os órgãos estão sendo disponibilizadas na INFOVIA, via emuladores de terminais IBM3270, servidores de impressão RPM, APPLINX via Gateway HTML com SSL, autenticado via RACF, integração com LOTUS-NOTES(Correio eletrônico, agenda e work-flow), acesso à Internet, todos os serviços disponibilizados em portais via ferramentas Browser.

1.7 – Metodologia

Será utilizada a metodologia de gerenciamento pelo Controle da Qualidade Total [CVF92], aplicando-se o **PDCA** [WMC99] em todas as etapas de acompanhamento dos itens de controle do SLA, sendo que no planejamento definem-se as metas, freqüências de apuração e os métodos para atingir os ICs(Índices de Controle). Na fase de execução faz-se a implementação do processo. Na fase de verificação faz-se o acompanhamento dos ICs (atuais e previstos) fazendo análise de tendências. De posse das informações de não conformidade serão tomadas ações corretivas se necessário e serão padronizados os processos com resultados esperados. Será dada ênfase aos itens de controle da segurança, desempenho e disponibilidade do ambiente de TI envolvido na administração da INFOVIA-MT.

1.8 – Resultados esperados

- Que o SLA seja assinado, mantido e que os serviços sejam disponibilizados cumprindo os indicadores previstos.
- Que seja promovida uma cultura sobre disponibilidade e segurança da informação na organização provedora de ambiente de TI e seus parceiros.
- Que os acessos às informações sejam feitos através de senhas, registrados e contabilizados.

- Que todos sejam responsáveis pelos seus atos e pelos recursos de informática sob sua guarda conforme os termos do SLA.
- Que a política de segurança e disponibilidade seja monitorada de forma a garantir a sua administração e recuperação de possíveis desastres.
- Que a tecnologia ATM seja integrada às redes tradicionais com os protocolos da Internet (TCP/IP) através do LANE, PNNI e VRRP permitindo o aproveitamento da largura de banda, garantindo performance, disponibilidade e segurança.
- Que a gerência de rede seja implementada de forma a visualizar e controlar o SLA.
- Que a Qualidade de Serviços QoS seja implementada nos serviços fim-a-fim.
- Que as metas estabelecidas para a INFOVIA-MT sejam alcançadas.

2 – A tecnologia ATM no backbone da organização

2.1. Introdução

O ATM(Asynchronous Transfer Mode) tem sido a solução de rede escolhida para uma parcela considerável das organizações que desejam aumentar o desempenho, garantir qualidade de serviços(QoS), propiciar tráfego de (voz, dados e vídeo), utilizar as funções de redes virtuais e otimizar as funções de roteamento.

Há a necessidade de protocolos que permitam a integração das LANs (Local Area Networks) atuais com a tecnologia ATM, onde esta última deve dar suporte às aplicações já existentes nas redes locais e às pilhas de protocolos de nível superior em uso. Partindo deste princípio, alguns protocolos ou serviços de integração LAN à tecnologia ATM foram desenvolvidos.

O primeiro deles, o IP over ATM (IPOA) da IETF (Internet Engineering Task Force)[IIE94], é o mais simples dos protocolos de integração porque restringe seu campo de atuação encapsulamento e transmissão de pacotes IP através da camada de Adaptação ao ATM (AAL) usando o protocolo AAL-5.

O segundo serviço de integração LAN/ATM, o LANE (LAN Emulation) [SWG97] é um padrão do Fórum ATM que opera na camada MAC (Media Access Control) da arquitetura IEEE 802 e possibilita o tráfego Ethernet ou Token Ring sobre ATM, sem nenhum prejuízo ou modificação da aplicação. No LANE, um driver encapsula os pacotes Ethernet e Token Ring em pacotes LANE que, por sua vez, são convertidos em células ATM.

O terceiro protocolo de integração LAN/ATM, o MPOA (Multiprotocol over ATM) [IET93] é também um padrão do Forum ATM desenvolvido para suportar vários protocolos não ATM como IP, IPX, etc. O MPOA opera ao nível da camada 3 do modelo OSI (Open System Interconection)[AWP] enquanto que o LANE trabalha na camada 2.

O padrão I-PNNI (IP-Private Network-Network Interface) [ATF97,ATFC97], também do Fórum ATM, proporciona uma alternativa eficiente para o roteamento simultâneo entre pacotes IP e canais virtuais comutados em um ambiente IP (ou multiprotocolo) sobre ATM. O I-PNNI estende a capacidade de roteamento PNNI

(Private Network-Network Interface) para o protocolo IP, incluindo qualidade de serviço (QoS) e compatibilidade entre switches ATM e roteadores convencionais.

2.2. IPOA

O protocolo IPOA (IP over ATM) [MAG95] trata do encapsulamento e transmissão de pacotes IP através da camada de Adaptação ATM (AAL), usando o protocolo AAL5. No IPOA há basicamente um mecanismo de resolução de endereços IP para que seja identificado o endereço ATM correspondente. O IPOA é conhecido também como o protocolo "IP clássico sobre ATM".

2.2.1 Encapsulamento IP over ATM

O documento RFC 1577 da IETF[IIE94] define o encapsulamento de pacotes IP usado, o mecanismo para mapear endereços IP em endereços ATM e os parâmetros para se avaliar a necessidade de iniciar ou terminar uma conexão virtual entre sistemas. O documento IETF RFC1577 define somente o que ocorre em uma subrede IP lógica (Logical IP Subnet- LIS).

Conexões entre estações em subredes IP diferentes passam pelo roteador, mesmo no caso em que exista conectividade física ATM entre as mesmas.

Os pacotes IP são transportados por PDUs (Protocol Data Units) do protocolo AAL5 da camada de Adaptação ATM. A PDU - AAL5 contem na primeira célula um cabeçalho LLC/SNAP (Logical Link Control/Subnetwork Access Protocol) para identificar o protocolo, um campo para os dados e, por último, um trailer com informações sobre comprimento e CRC (Cyclic Redundancy Check). O tamanho típico do pacote IP over ATM é 9180 octetos, o que é suficiente para os pacotes padrão Ethernet, Token Ring, FDDI e SMDS (Switched Multimegabit Data Service) sem fragmentação.

2.2.2 Arquitetura IPOA

Para usar o serviço ATM de canais virtuais comutados SVC (Switched Virtual Channel), as estações finais deverão fazer o mapeamento de endereço IP para endereço ATM e estabelecer conexões virtuais automaticamente. Isto é feito usando um elemento adicional, o protocolo de resolução de endereços ATM (ATM Address Resolution Protocol - ATMARP).

Um servidor ATMARP possibilita que cada estação de uma subrede IP (LIS) possa fazer pesquisas para encontrar o endereço ATM a ser usado a fim de que o pacote seja entregue a um destino IP. O protocolo ATMARP desempenha o mesmo papel que o protocolo ARP (Address Resolution Protocol) realiza em redes LANs já existentes. O servidor ATMARP mantém automaticamente em cada LIS um banco de dados com o objetivo de mapear endereços IP para ATM. O servidor ATMARP é um módulo de software que pode ser implantado em um servidor de arquivos ou em uma estação de trabalho, além de também poder ser implementado em roteadores ou switches ATM presentes na rede.

Em uma rede ATM com serviço SVC, cada estação em uma subrede IP (LIS) inicialmente conecta-se ao servidor ATMARP para registrar-se. A especificação do IP clássico sobre ATM não aborda como uma estação de trabalho encontra o endereço de um servidor ATMARP. O servidor ATMARP, por sua vez, ao aceitar o registro, envia uma mensagem Inverse ATMARP Request para obter o endereço IP da estação de trabalho. O servidor ATMARP mantém os endereços recebidos em uma tabela local para que possa responder a outras possíveis estações da rede. Com o objetivo de manter informações atualizadas de endereço e para minimizar o tamanho da tabela, o servidor ATMARP descarta os endereços que não forem solicitados em um intervalo de tempo determinado. Uma estação pode manter permanentemente a conexão com o servidor ATMARP ou, periodicamente, refazer a conexão com o objetivo de atualizar a tabela de endereços.

O protocolo IP over ATM não requer nenhuma alteração na infra-estrutura tradicional de roteamento IP já existente. O roteamento pode ser feito da mesma forma que o tradicional: os pacotes são enviados do remetente para um roteador e deste para outros possíveis roteadores até que o destino seja alcançado. Ao longo do caminho, o cabeçalho IP e de outros protocolos de camadas superiores, além dos dados, permanecem inalterados (exceto nos casos em que são acrescentados campos de

controle ou que ocorram possíveis fragmentações de pacotes IP em datagramas IP ainda menores). Por outro lado, no encapsulamento efetuado pela camada MAC inferior pode haver alterações completas de cabeçalho a cada novo roteador alcançado. Pelo fato do protocolo IP comportar-se com a rede ATM da mesma forma que com outros tipos de subredes de comunicação (Ethernet, Token Ring, FDDI, Frame Relay e circuitos WAN), as redes corporativas que já possuem estes tipos de subredes podem facilmente incorporar a tecnologia ATM ao seu backbone.

Em cada subrede IP LIS, o sistema integrado LAN/ATM comunica-se via conexão virtual ATM ponto-a-ponto. Os pacotes IP são encapsulados em PDUs AAL 5. As células ATM nas PDUs são enviadas de switch para switch através da rede ATM, para que sejam remontadas em pacotes IP no destino. Ao nível da camada de Rede (IP), a rede ATM surge apenas como um novo salto, não importando o número de switches ATM envolvidos, da mesma forma que um circuito de telecomunicações é considerado apenas um novo salto para roteadores, não importando o número de switches e multiplexadores que o circuito atravessa.

2.2.3 Divisão em subredes ATM

Na maioria dos ambientes de rede atuais, as subredes IP são associadas à estrutura física da rede. A subrede, no nível mais baixo, é geralmente um segmento LAN, provavelmente atingida por intermédio de uma ponte ou switch. As subredes LAN caracterizam-se pelo broadcast para despachar tanto pacotes broadcast como unicast ao longo da rede. As subredes LANs são implantadas geograficamente de acordo com os limites impostos pelo meio de transmissão e pelo protocolo MAC.

Por outro lado, uma rede ATM consiste de circuitos virtuais ponto-a-ponto e ponto-multiponto. Como os circuitos virtuais não têm nenhuma limitação de distância inerente (a localidade física de dois dispositivos não impede que os mesmos venham a se comunicar diretamente), tem-se que as subredes IP em ATM são baseadas em parâmetros lógicos e não físicos. A estrutura de rede ponto-a-ponto também possibilita que uma estação ATM possa se comunicar com duas ou mais estações sem a necessidade de preocupação com o tráfego de outras estações, até no caso de pacotes multicast.

Com este grau de isolamento entre as subredes IP em um mesmo meio físico, mais de uma subrede lógica IP pode terminar em um único adaptador físico, permitindo que um adaptador ATM substitua, por exemplo, várias placas Ethernet sem que seja necessária qualquer modificação ou combinação de subredes. Esta é uma característica que os adaptadores ,de rede local das tecnologias até então existentes, não podiam ter. As subredes IP lógicas em ATM podem incluir qualquer conjunto arbitrário de estações de trabalho e roteadores localizados em qualquer parte do backbone. Com as subredes IP em ATM pode–se obter vantagem no controle de banda, alocando-se diferentes taxas de velocidades e garantias de qualidade de serviço para cada subrede, proporcionando ferramentas poderosas para aplicações de gerenciamento da banda disponível(Anexo-03).

2.2.4 Estabelecimento de conexão

Considerando o estabelecimento de uma conexão ATM com IPOA. Quando um cliente 1 na subrede LIS deseja enviar dados para um cliente 2 na mesma LIS, o primeiro pacote IP enviado pelo cliente 1 dispara um pedido ao servidor ATMARP. Um módulo IP/ATM (software) presente no cliente 1 envia um pedido ATMARP ao servidor ATMARP, que terá o objetivo de verificar qual o endereço ATM correspondente ao endereço IP inicialmente fornecido referente ao cliente 2. O servidor ATMARP envia ao cliente 1 o endereço ATM desejado. O cliente 1 usa o endereço ATM obtido para estabelecer um SVC diretamente para o cliente 2. Quando o cliente 2 for retornar um pacote IP para o cliente 1, o mesmo também disparará uma requisição para o servidor ATMARP com o objetivo de obter o endereço ATM do cliente 1. Ao receber este endereço, o cliente 2 verificará que já possui uma conexão com o endereço ATM obtido, sendo desnecessário uma nova conexão. O fato de ambos os clientes da subrede LIS A estarem cientes da conexão e dos endereços recíprocos, possibilita uma comunicação direta através do serviço SVC, sem a necessidade de mais envolvimento do servidor ATMARP.

Uma estação pode ter mais de um circuito virtual ativo simultaneamente. Um servidor de arquivos ou de e-mail tem centenas de conexões em um pequeno intervalo de tempo, dependendo do número de clientes que o sistema possui. As conexões que

permanecem inativas por determinado período de tempo são automaticamente desfeitas com o objetivo de liberar o adaptador de rede e tornar disponível os recursos da rede ATM para outras possíveis necessidades naquele momento.

2.2.5 IPOA Com múltiplas subredes LIS

O protocolo IP clássico over ATM foi especificado para trabalhar originalmente apenas em uma subrede LIS ATM. Entretanto, novos trabalhos têm sido desenvolvidos no sentido de abolir esta limitação. No momento, existem duas maneiras para se estabelecer comunicação entre subredes LIS: por intermédio de roteadores ou desviar-se dos roteadores por múltiplas subredes LIS.

Para que duas estações em diferentes subredes LIS estejam habilitadas para se comunicar, deve existir um roteador em cada subrede LIS. Múltiplos servidores ATMARP não são necessários, uma vez que um servidor ATMARP pode ser configurado para lidar com mais de uma subrede LIS independentemente.

Quando um cliente em uma LIS tenta enviar um pacote IP para um cliente em outra subrede LIS, o software IP residente no cliente remetente percebe que o endereço destino é de outra subrede LIS e envia o pacote para o roteador default gateway na sua subrede LIS. Isto dispara um pedido para o servidor ATMARP para que seja descoberto o endereço ATM do roteador de destino, e, em seguida, é estabelecida uma conexão do cliente para o roteador de destino. Uma vez o roteador de destino tendo recebido o pacote IP do cliente remetente, o mesmo emite um pedido de ATMARP para encontrar o endereço ATM do cliente destinatário, em seguida, estabelece a conexão com o cliente destinatário. Isto significa que para ocorrer comunicação entre duas estações por intermédio de um roteador, devem ser estabelecidos dois circuitos virtuais através da rede ATM: um do remetente para a interface ATM do roteador e a outra do roteador para a estação destinatária. A estação remetente segmenta os pacotes IP em células para a transmissão pela rede ATM, para serem remontados no roteador. O roteador tomará então a decisão do caminho pelo qual será enviado o pacote, baseado na informação contida no cabeçalho do pacote IP, segmentando os pacotes para que sejam enviados novamente por um circuito virtual ATM para a estação destinatária.

Alguns roteadores, chamados de one-armed routers, podem ser configurados para rotear pacotes nos dois sentidos (in e out), usando a mesma interface ATM. Roteadores deste tipo proporcionam um filtro de segurança entre diferentes partes de uma rede, como o que acontece entre um campus ATM e uma WAN. Entretanto, se a segurança não for um aspecto relevante para as informações que estão trafegando, os administradores de redes terão preferência em aproveitar aspectos como velocidade e baixa latência das redes ATM, com o intuito de proporcionar maior desempenho para os seus usuários. Uma maneira de se fazer isto usando IP clássico sobre ATM é configurando recursos compartilhados, tipo servidores de arquivos, para serem membros de mais de uma subrede LIS, de forma que as estações estejam numa mesma subrede LIS com os recursos que necessitam mais freqüentemente. Esta estratégia de rede desvia-se dos roteadores, eliminando a montagem e remontagem desnecessária de pacotes e promovendo maior desempenho. Este mesmo procedimento também possibilita aos administradores de rede associar aplicações em subredes LIS separadas, cada uma com sua própria qualidade de serviço, prioridade e vazão.

Apesar de trabalhar adequadamente, o uso do IP over ATM em uma única subrede limita o potencial ATM em uma rede IP porque não há um meio de se comutar tráfego entre subredes IP e uma rede ATM. Isto é considerado um problema pelo fato de não se aproveitar às facilidades de gerenciamento da qualidade de serviço, a latência reduzida e a maior vazão proporcionada pela rede ATM.

2.3 Serviço de emulação de LAN (Lan Emulation)

2.3.1 O padrão LAN Emulation

O serviço LAN Emulation ou LANE[YIM96], é um padrão do Forum ATM que suporta pacotes de LAN convencionais (Ethernet e Token Ring) dentro de um ambiente ATM, permitindo que protocolos e aplicações LAN trabalhem transparentemente sobre ATM e que os equipamentos ligados a LAN possam se comunicar, inclusive com os dispositivos ATM.

Para manter compatibilidade com os protocolos de redes tradicionais (por exemplo, Ethernet/IEEE 802.3 e Token Ring/IEEE 802.5), optou-se por emular LANs na sub camada MAC, a fim de minimizar mudanças necessárias para a migração para ATM.

O subconjunto do serviço LANE, a LAN emulada (ELAN), é definida como um grupo lógico de dispositivos capaz de trocar tipos de quadros similares dentro de um mesmo domínio de broadcast. Muitas ELANs podem existir concorrentemente na mesma rede ATM, mas não podem se comunicar diretamente. Um roteador ou ponte é requerido para a intercomunicação de ELANs [AWP].

2.3.2 Componentes LANE

Para oferecer os serviços que os protocolos tradicionais tem recebido, o serviço LAN Emulation deve oferecer broadcast sem conexão e serviço de multicast baseado no padrão de endereços IEEE 802 MAC. Como estes serviços não são nativos de redes ATM, eles são implementados através de um módulo cliente LAN Emulation Client (LEC) em cada host, de um servidor LAN Emulation Server (LES) que pode estar localizado em qualquer lugar na rede, de um servidor Broadcast and Unknown Server (BUS) e de um servidor LAN Emulation Configuration Server (LECS).

O servidor LES é o servidor de resolução de endereços para a ELAN. Há um servidor lógico LES por ELAN. Quando um cliente LEC recebe um pacote para enviar, ele procura o endereço MAC de destino na sua tabela local. Tem-se uma conexão ATM já associada com o endereço, ele envia o pacote por aquela conexão. Se ele sabe o endereço ATM para aquele endereço MAC, ele pode solicitar que uma conexão seja configurada para o destino. Se, contudo, o cliente LEC não tem a conexão ATM ou o endereço ATM, ele usa o protocolo ARP para obter esse endereço, enviando uma mensagem LE_ARP (LAN Emulation Address Resolution Protocol) para o servidor LES perguntando qual o endereço ATM associado com aquele endereço MAC.

O servidor LES pode manter uma "cache" do endereço MAC para o ATM correspondente. Essa correspondência é mantida diretamente do endereço MAC registrado do cliente LEC com o servidor LES. Se a correspondência é conhecida, o servidor LES pode replicar diretamente para o cliente LEC com o endereço ATM que ele precisa para estabelecer uma conexão com o destino. Por outro lado, se o servidor

LES não sabe o endereço MAC, ele emite um broadcast com a solicitação LE_ARP para todos os clientes LECs usando a conexão Control Distribute VCC(Virtual Channel Conection). Quando um cliente LEC recebe a solicitação LE_ARP, ele checa sua própria tabela de endereços locais para ver se o endereço MAC solicitado é o seu próprio ou se ele está atuando como um proxy para o endereço MAC. Em caso afirmativo, ele envia uma resposta LE_ARP de volta para o servidor LES e este a direciona para o cliente LEC que enviou o pedido original LE_ARP.

2.3.2.1 LAN Emulation Configuration Server (LECS)

O servidor LECS mantém um banco de dados de informações de cada Lan emulada (ELAN).

Quando um cliente LEC é inicializado, uma das suas primeiras ações é estabelecer uma conexão com o servidor LECS e depois enviar uma solicitação para sua configuração, que deverá retornar o endereço ATM do servidor LES que o cliente LEC deve contatar para se associar a uma ELAN. O banco de dados do servidor LECS é geralmente inicializado pelo administrador de rede e gerenciado via aplicações de gerenciamento SNMP. Há um servidor LECS lógico para cada LAN Emulation Service, embora ele possa ser implementado como um banco de dados distribuído.

2.3.2.2 Broadcast and Unknown Server (BUS)

O servidor BUS [ZEI96], é o servidor de multicast para uma LANE. O servidor BUS aceita quadros broadcast/multicast de vários VCCs e os direciona sobre uma conexão ponto-multiponto (Multicast Forward VCC) ou uma conexão ponto-a-ponto específica Multicast Send VCC.

Uma conexão ponto-a-ponto (MulticastSend) de cada cliente LEC na LAN emulada (ELAN) é configurada para o servidor BUS quando o cliente LEC se une a ELAN. Pacotes para serem difundidos do LEC são enviados para o servidor BUS, que os recebe da camada AAL como pacotes completos. O servidor BUS envia os pacotes de volta para todos os clientes LECs usando a conexão ponto-para-multiponto

(MulticastForward). Isto é feito numa FIFO (Fist in first out), um pacote a cada vez, sem que nenhuma célula de diferentes pacotes intercale a conexão.

Os clientes LECs também enviam pacotes, cujo destino é desconhecido, para o servidor BUS. O servidor BUS direciona tais pacotes para todos os clientes LECs que são capazes de recebê-los. Estes clientes LECs de destino podem estar em pontes, switches e roteadores. O servidor BUS envia uma cópia destes pacotes para cada cliente LEC na ELAN, incluindo o cliente LEC de onde o pacote foi originado.

Os clientes LECs devem filtrar o tráfego que chega usando um campo no cabeçalho de cada pacote que identifica unicamente cada cliente LEC.

2.3.3 Formato do pacote LAN Emulation

Os pacotes do cliente LEC ATM são encapsulados, ou no formato IEEE 802.3, ou IEEE 802.5. Isto assegura que a pilha de protocolos não seja trocada e que a LANE seja compatível com os atuais protocolos de LAN. Um cabeçalho LANE de 2 octetos diferencia os pacotes de controle, tais como LE_ARP, dos pacotes de dados. Usando o protocolo AAL5, o adaptador ATM divide o pacote LANE em células ATM e as envia através da rede. No ponto destino, as células ATM são remontadas no seu formato de pacote LANE.

2.3.4 Características do serviço LANE

Embora o serviço LANE tenha sido concebido para ser compatível com as atuais LANs de meio compartilhado, os administradores de rede ainda têm que tomar decisões que afetam a configuração e desempenho das LANs. Isto inclui o tipo de LAN emulada, tamanho máximo do pacote e a localização do servidor LES e do servidor de BUS [YIM96].

Um servidor LES pode ser implementado em qualquer dispositivo ATM, incluindo servidores de arquivos, switches ATM e roteadores, mas somente um servidor LES é permitido para cada configuração LANE.

É tarefa do administrador de rede decidir qual servidor LES usar e onde colocá-lo para conseguir melhor desempenho, já que a principal função do servidor LES é fazer o

mapeamento entre endereços MAC e ATM. Implementar o servidor LES em dispositivos que processem muitos endereços MAC pode reduzir o tráfego de mensagens LE_ARP. Equipamentos como switches e roteadores são as melhores opções para o servidor LES.

Similarmente, o servidor de broadcast (BUS) pode ser implementado em qualquer dispositivo. Como o servidor LES, apenas um servidor BUS é permitido por LANE e o administrador deve decidir onde colocá-lo. Um dispositivo ATM com link de alta velocidade para um switch ATM é sempre uma boa escolha.

Uma vez que o servidor LES e o servidor BUS tenham sido selecionados, o tamanho máximo do pacote e seu tipo devem ser determinados. As LANs de meio compartilhado tem limitações físicas que restringem o tamanho do pacote. Para uma rede Ethernet, o limite é 1.516 octetos e para uma rede Token Ring é 18.190 octetos.

O LAN Emulation Working Group do Forum ATM restringiu o tamanho do pacote para um máximo de 1.516, 4.544, 9.234 e 18.190 octetos para corresponder ao tamanho dos pacotes das LAN de meio compartilhado.

Todos os dispositivos da LAN emulada devem ser homogêneos. Aqueles que devem comunicar-se freqüentemente com dispositivos Ethernet devem ser configurados para o IEEE 802.3, enquanto que os que se comunicam com Token Ring devem ser configurados para IEEE 802.5. Se há necessidade de comunicação entre ambos, como é o caso de alguns servidores ATM ou switches multi-LAN, então um dispositivo ATM pode ser configurado para ter compatibilidade simultânea com as LAN emuladas Ethernet e Token Ring.

O serviço LANE tem também a característica de liberar os dispositivos ATM da limitação Ethernet, Token Ring e FDDI de um único endereço MAC. Com LAN de meio compartilhado, somente um endereço MAC por adaptador e por rede é permitido. Por exemplo, para adicionar uma nova rede para um servidor Novell ou Windows NT, o usuário tem que adicionar um outro adaptador LAN para o servidor e mudar as suas configurações. Ao contrário, dispositivos ATM com uma única interface ATM podem ter um endereço MAC para cada LAN emulada, sendo o único obstáculo o software de drive do dispositivo. Uma LAN emulada não é uma rede física, mas uma rede lógica que permite diferente tamanho e tipos de quadros sobre um único adaptador ATM com conexão ao switch ATM.

Dispositivos tais como roteadores, pontes e servidores que estão diretamente conectados com o backbone podem ser atualizados com interfaces ATM executando LANE. Isto auxilia a progressão da largura de banda enquanto eles continuam a servir aos clientes já instalados Ethernet e Token Ring. Atualizar um backbone ATM com roteadores e switches ATM e LAN Emulation, otimiza e aumenta a capacidade do backbone sem mudar o equilíbrio da infra-estrutura de rede [YIM96].

2.3.5 LANE 2.0

Desenvolvida para melhorar o desempenho das LANs emuladas. O LANE 2.0 inclui duas partes: O Serviço LANE User to Network Interface (LUNI) 2.0 e o LANE Network to Network Interface (LNNI) 2.0 [DOG96].

Os novos recursos do serviço LUNI 2.0 permitem que clientes LANE façam multiplexação de diversas LANs emuladas (ELANs) através do mesmo canal virtual, reduzindo assim o número de canais virtuais necessários. Para isso está sendo incluída a utilização do esquema de encapsulamento LLC/SNAP(Logical Link Control/Subnetwork Access Protocol) já utilizado com o IPOA.

O serviço LUNI 2.0 melhora o suporte a qualidade de serviço (QoS), porque os administradores de rede podem especificar o tipo de serviço de tráfego. O serviço LUNI 2.0 acrescenta também suporte para a separação de tráfego em multicast e permite que o servidor LES repasse suas informações de dispositivo para roteadores não ATM.

O serviço LNNI é uma nova parte do LANE que proporciona uma forma padrão para a distribuição de componentes servidores LANE. O serviço LANE 1.0 não excluía essa distribuição, mas, sem um mecanismo padrão, cada fabricante precisava implementar um enfoque proprietário para suportá-la. O serviço LNNI 2.0 descreve como os componentes podem ser distribuídos e define as interfaces e protocolos pelos quais eles intercambiam controles e dados.

O objetivo do ATM Fórum com a versão LANE 2.0 é que esta arquitetura distribuída habilite uma única ELAN a incluir dois mil clientes (LECs) e 20 servidores LES e BUS.

2.4. MPOA - Multi Protocol Over ATM

2.4.1 Modelo MPOA

O modelo MPOA (Multiprotocol Over ATM) [DOG96]é um conjunto de recursos que fornece a estrutura básica para a implementação de roteamento e bridging ATM através de ambientes diversos no que diz respeito a protocolos, tecnologias de rede e redes virtuais (IEEE 802.1 Virtual LANs). Esta estrutura básica foi projetada no sentido de fornecer um paradigma unificado para o empilhamento dos protocolos da camada 3 OSI (Open System Interconection) com ATM, além de reduzir a latência intrínseca ao processamento destes, através da conectividade direta entre os dispositivos ATM existentes na rede.

Além disso, o MPOA é também capaz de utilizar as informações de roteamento e de bridging para localizar o equipamento conversor LAN/ATM (edge device) mais próximo ao endereço da estação destinatária, aumentando assim, de forma significativa, os índices de desempenho global da rede. O principal objetivo do MPOA, portanto, é fornecer conectividade fim-a-fim entre camadas de Rede pares, através da rede ATM. As estações (hosts) podem estar ligadas diretamente à estrutura ATM, a uma LAN tradicional, ou ainda, a uma rede emulada LANE.

O modelo MPOA pode ser entendido como sendo um roteador virtual, no sentido de que o conjunto de dispositivos MPOA operando na estrutura ATM fornece a dupla funcionalidade de roteamento e bridging.

Os conversores LAN/ATM examinam os endereços de destino dos pacotes recebidos nos segmentos das LANs tradicionais e então tomam a decisão apropriada de envio. Se o pacote deve ser roteado, ele irá conter o endereço MAC da interface do "roteador virtual". Nesse caso, o conversor LAN/ATM toma o endereço nível Rede do destino e o resolve para o endereço ATM correspondente através do servidor de rotas. Em seguida, o conversor LAN/ATM estabelece um circuito virtual direto até o destino. Para o caso de uma operação de bridging, o conversor LAN/ATM utiliza a própria LANE para resolver o endereço ATM e estabelecer o circuito virtual ao destino.

Se o servidor de rotas não conhece o endereço ATM apropriado, ele propaga a solicitação a outros servidores de rotas. Os endereços retornados pelo servidor de rotas serão sempre os endereços de um dispositivo da rede ATM.

2.4.1.1 Modelos de roteamento e endereçamento

No MPOA, a escolha do modelo de roteamento é feita de forma independente da escolha do modelo de endereçamento.

Para a resolução de endereços, pode-se utilizar tanto o modelo Peer Addressing Model, no qual o endereço ATM do destinatário pode ser calculado por meio de algoritmo através do seu endereço nível Rede, quanto o modelo Separated Addressing Model (também conhecido como Overlay Addressing), no qual uma pesquisa dinâmica numa tabela deve ser feita para que se possa conhecer o endereço ATM do destino. Para o roteamento, pode-se utilizar tanto o modelo Integrated Routing Model, no qual as informações das topologias nível Rede e da infra-estrutura ATM são integradas numa única base de dados, quanto o modelo Layered Routing Model (também conhecido como Overlay Routing Model), no qual as informações sobre as camadas de Rede e ATM são dispostas separadamente.

2.4.1.2 Internet Address Sub-Group

No ambiente LAN, é normal que as redes encontrem-se subdivididas em subredes. Como o termo subrede já é usado em redes não ATM, o MPOA utiliza a designação IASG (Internet Address Summarization Groups). Um grupo IASG é protocolo específico; isto é, se uma estação opera com dois protocolos nível Rede, será um membro de pelo menos dois grupos IASGs. Num sistema MPOA, cada grupo IASG é definido de forma única através do protocolo empregado, do prefixo do endereço nível Rede e do comprimento do prefixo do endereço nível Rede. Pode-se pensar no grupo IASG, em termos do protocolo IP, como sendo uma subrede virtual.

2.4.2 Serviços utilizados para transferência de dados

Para a transferência de dados, o MPOA utiliza-se do protocolo ATM AAL5. Utiliza, também, as capacidades de sinalização definidas pelo padrão ATM Forum UNI 3.1, com a opção de utilizar a versão UNI 4.0. Para tratar o roteamento, o MPOA utiliza os serviços de roteamento dos protocolos níveis Rede subjacentes. Para a resolução de alvo, o MPOA utiliza e amplia o protocolo NHRP (Next Hop Resolution Protocol) [WPN 97].

2.4.3 Componentes MPOA

O MPOA define apenas os elementos lógicos de sua implementação, deixando os detalhes físicos da implementação às empresas interessadas no desenvolvimento de produtos MPOA. Os componentes do MPOA são os seguintes:

a) Cliente MPOA-MPC: conjunto de funções, realizadas por um conversor LAN/ATM ou uma estação LANE MPOA e responsáveis pela interconexão da camada de Rede com um outro componente MPOA;

b) Servidor MPOA-MPS: conjunto de funções que fornece as funções de interconexão da camada de Rede no sistema MPOA; inclui um NHS (Next Hop Server)estendido;

c) Grupo RFFG (Remote Forwarder Functional Group): grupo de funções realizadas em associação à distribuição de tráfego entre IASGs.

2.4.4 Fluxos de informação na solução MPOA

Os fluxos de informação no MPOA podem ser classificados da seguinte forma: fluxos de configuração, fluxos de transferência de dados, fluxos de controle cliente-servidor e fluxos servidor a servidor.

As principais características dos fluxos de informação no MPOA são as seguintes:

a) Todos os servidores e clientes MPOA utilizam-se dos fluxos de configuração para recuperar informações de configuração; cada grupo funcional seja cliente ou servidor, cria um circuito virtual no início da operação, e o utiliza para buscar a informação de configuração necessária;

b) Os fluxos de dados são o próprio objetivo da implementação MPOA;

c) Os fluxos de controle cliente-servidor são utilizados pelo cliente para informar e solicitar informações ao servidor MPOA;

d) Finalmente, os fluxos servidor a servidor são utilizados para simular um serviço único enquanto vários serviços estão distribuídos ao longo de múltiplos dispositivos; este último tipo de fluxo é justificado pela necessidade de se disponibilizar a rede com o máximo de sua capacidade o tempo todo.

2.4.5 Serviços ofertados

O MPOA fornece quatro tipos de serviço: configuração (Configuration), descoberta (Discovery), resolução de alvo MPOA (MPOA Target Resolution) e transferência de dados (Data Transfer). As características principais de cada um desses serviços são as seguintes:

a) O serviço de configuração garante que todos os grupos funcionais possuem o mesmo conjunto de informações administrativas. Todos os grupos funcionais contatam um servidor de configuração apropriado para obter suas configurações iniciais. Clientes e servidores realizam processos distintos de configuração;

b) O serviço de descoberta é o processo através do qual os componentes MPOA ligados as LANEs reconhecem a existência e o tipo funcional uns dos outros. O MPOA implementa um dispositivo de descoberta a fim de reduzir a complexidade operacional do seu funcionamento. Os dispositivos MPOA ligados as LANEs utilizam extensões do protocolo LANE LE_ARP para descobrir a existência, o endereço ATM e o tipo (cliente ou servidor) uns dos outros. A informação é obtida dinamicamente.

c) O serviço de resolução de alvo MPOA é a determinação de uma descrição de rota a partir de um endereço nível Rede destino; é esta à parte do sistema MPOA que permite a criação e utilização de atalhos. A resolução de alvo MPOA utiliza uma extensão do protocolo NHRP (Next Hop Resolution Protocol) [WPN97,SWG97] para permitir que clientes determinem o endereço ATM de um edge device ou de um circuito virtual;

d) O serviço de transferência de dados é o processo através do qual dois clientes MPOA transferem dados ao nível da camada de Rede, um para o outro. A transferência de dados unicast através do MPOA opera no modo default ou no modo atalho. No modo

default, o tráfego é enviado através da LANE. No modo atalho, os fluxos são estabelecidos através dos mecanismos de gerenciamento de cache. Quando um cliente MPOA tem um pacote para o qual já existe um atalho, o pacote é enviado pelo circuito virtual associado àquele atalho.

2.4.6 Características do MPOA

O MPOA é uma das tecnologias em desenvolvimento que irá permitir às companhias a implementação de redes corporativas escaláveis baseadas com ATM.

O MPOA visa aumentar o potencial dos benefícios das redes ATM através da utilização direta de canais virtuais comutados (SVCs) para o envio de dados de forma escalonável e da utilização de parâmetros de qualidade de serviço (QoS) para o melhor gerenciamento dos serviços oferecidos. Além disso, mantendo a interoperabilidade com os protocolos da camada de Rede, o MPOA garante que aplicações operando através de LANs existentes continuarão a operar normalmente sobre ATM.

O modelo MPOA também fornece inúmeros benefícios àqueles usuários que necessitam de redes escaláveis baseadas em switching. Isto se deve à implementação do protocolo de roteamento/bridging baseado no protocolo NHRP e ao estabelecimento de circuitos virtuais diretos para a transferência de dados. Através desta implementação, podem ser alcançados baixíssimos índices de latência na comunicação entre quaisquer dois pontos da rede - independentemente da subrede na qual se encontrem esses dois pontos.

2.5 I-PNNI

O I-PNNI [BAN97] proporciona uma alternativa eficiente para o roteamento simultâneo entre pacotes IP e canais virtuais comutados ATM em um ambiente IP (ou multiprotocolo) sobre ATM. É compatível com switches ATM que executam o PNNI, mas que não possuem nenhum conhecimento dos protocolos da camada de Rede como o IP [BAN96]. Não é necessária nenhuma modificação nos hosts, estando estes em redes ATM ou outra rede física qualquer. O I-PNNI foi concebido assumindo o fato de que qualquer ambiente ATM terá um grande número de hosts de diferentes fabricantes

suportando um conjunto variado de protocolos. O I-PNNI é compatível com redes virtuais, LAN Emulation e MPOA. No lugar de calcular uma rota na camada 3 (camada de Rede) e outra na camada 2 (camada de Enlace), possibilita que roteadores, edge devices (dispositivos capazes de enviar pacotes entre interfaces ATM e redes não-ATM) e switches ATM compartilhem informações e calculem um único caminho fim-a-fim.

2.5.1 PNNI

O PNNI (Private Network-Network Interface) [ATF0396,ATF0996] é um protocolo switch-to-switch usado em redes ATM no roteamento e sinalização de canais virtuais comutados. O PNNI possibilita o estabelecimento de rotas segundo critérios de qualidade de serviço. O PNNI é fácil de configurar e possui uma topologia flexível e escalável.

2.5.1.1 A visão hierárquica de rede do PNNI

Para o PNNI, a rede é uma coleção de peer groups (grupo de pares). Um peer group é formado por um switch administrador que traça um círculo lógico em torno de si e dos demais switches do grupo. A partir de um conjunto de peer groups que estejam conectados entre si por switches limítrofes (border switches), pode-se construir uma estrutura hierárquica ao se desenhar um círculo em torno deste ajuntamento de peer groups e se admitir que ele também é um peer group, pai de cada um dos outros que o constituem. Dentro desse peer group pai, um representante de cada peer group filho participa do esquema de roteamento do PNNI, representando este peer group de mais baixo nível, do mesmo modo que os switches participam nos níveis mais inferiores. Alguns elementos (nós) podem ser peer groups rodando PNNI, enquanto outros podem ser realmente switches. Também é possível que alguns estejam executando outro protocolo internamente, mas usando PNNI externamente de forma transparente para os demais.

2.5.1.2 O Funcionamento do protocolo de roteamento

O protocolo de roteamento PNNI é membro da classe de protocolos de roteamento baseados em mapas. Estes protocolos funcionam através da distribuição de informações descritivas sobre a rede ou porções dela. Para dar suporte à hierarquia com PNNI, em cada nível de hierarquia, um switch (ou peer group) disponibiliza um mapa que o descreve, e estes mapas são distribuídos no âmbito do peer group pai. Para uso externo, o líder do peer group (o representante do peer group como um todo), cria um mapa baseado nas informações internas.

2.5.1.3 O tratamento das informações de roteamento

Como os peer groups são formados pela associação de outros peer groups, é necessária uma redução da quantidade de informações descritivas a fim de que a hierarquia seja escalável. A informação sobre a topologia da rede é resumida quando se sobe na hierarquia. Entretanto, há o caso da informação se tornar tão imprecisa a ponto de ser prejudicial, estando o protocolo encarregado de obter dos nós, informações complementares. Ocorre também a propagação de informações do nível mais alto até o nível mais baixo, uma vez que os switches de origem precisam selecionar a saída do peer group que se dirige ao destino, sendo necessária à informação sobre a topologia externa.

2.5.1.4 Escalabilidade

A natureza hierárquica do PNNI permite a construção de redes de tamanho muito grande. Sua natureza recursiva permite uma estrutura escalável e abrangente.

2.5.2 Backbone integrado - roteamento/switching I-PNNI

O roteamento I-PNNI possibilita uma mistura de tecnologias de interconexão de redes: conversores LAN/ATM, roteadores tradicionais em áreas de baixo tráfego e switches ATM em um mesmo backbone. Todos os dispositivos cooperam para usar os recursos da rede eficientemente e assegurar a qualidade de serviço apropriada para cada aplicação. Considerando a topologia da INFOVIA-MT(Anexo-03) o grupo de dois

switches (ASX-1000) do CORE ATM e os roteadores estão executando I-PNNI. Todos os roteadores (inclusive aqueles que não possuem interface ATM) e os dois switches executam o protocolo de roteamento PNNI e são considerados como nós. Para as aplicações que necessitarem de maior largura de banda ou menor latência, os troncos ATM devem ser usados. Já nos casos onde o custo for mais importante que a velocidade, um caminho que utilize roteadores tradicionais será mais apropriado. Caso algum link ou nó apresente falha, os roteadores e os switches estabelecem automaticamente um caminho alternativo.

2.5.3 Modelo de roteamento I-PNNI

O núcleo do backbone integrando roteamento/switching consiste de switches ATM que administram as conexões via PNNI.

Os edge devices e os roteadores ao redor do backbone usam I-PNNI para propagar informações dos vários protocolos.

O I-PNNI acrescenta informações às mensagens de atualização de estados dos links PNNI de forma a permitir que os dispositivos ao redor do backbone não estejam vinculados com os protocolos das LANs e as características das camadas 3 das subredes existentes. O conjunto de informações destes protocolos é transparente para os switches ATM existentes no backbone.

2.6 Descritores de tráfego

O descritor de tráfego é uma lista genérica de parâmetros de tráfego que podem ser usados para capturar as características de tráfego intrínsecas de uma conexão. Um parâmetro de tráfego é especificado mediante uns aspectos particulares do tráfego, qualitativo ou quantitativo. Estes parâmetros podem descrever, por exemplo, a taxa de pico de células ou até mesmo o tipo da fonte (telefone, videofone, etc). Os descritores de tráfego são necessários para assegurar uma alocação de recursos apropriada e garantir a QoS requerida.

A descrição das características de tráfego que uma dada conexão possa oferecer deve ser fornecida pelo usuário na fase de estabelecimento de conexão.

O descritor de tráfego da fonte é o conjunto de parâmetros de tráfego, usado na fase de estabelecimento de conexão, que captura as características de tráfego intrínsecas da conexão pedida pela fonte. Alguns dos parâmetros atualmente definidos para redes ATM são :

Taxa de Pico de Células (PCR) : representa a taxa máxima do tráfego que pode ser submetido pela fonte na conexão ATM. O inverso do PCR representa o tempo mínimo teórico entre chegadas de células em uma fila;

Taxa Média de Célula (SCR - Sustainable Cell Rate) : representa a taxa média de envio de células em um intervalo definido de tempo. O inverso da SCR representa o tempo médio entre chegadas de células com respeito à velocidade do canal;

Taxa Mínima de Células (MCR) e Taxa Disponível de Células (ACR) : são usados pelo serviço ABR. A MCR representa a taxa mínima de transmissão de células garantida pela rede para a fonte. A ACR representa a taxa atual de transmissão de células fornecida pela rede. Seu valor é variável, mas nunca é inferior ao valor de MCR, ou superior ao valor de PCR; e

Tamanho Máximo de Rajada (MBR - Maximum Burst Rate) : representa o número máximo de células que pode ser transmitido à taxa de pico de células pela fonte enquanto de acordo com a taxa média de células.

O gerenciamento de tráfego deve suportar um conjunto de classes de QoS suficientes para todos os serviços previsíveis. Cada classe de serviço tem associado a ela uma característica de tráfego e um determinado nível de QoS. A classe de QoS define os objetivos de desempenho a serem garantidos para cada conexão dentro deste serviço.

Na camada ATM, o nível de QoS é uma função de vários parâmetros, entre os quais se destacam a taxa de perda de células, o atraso de transferência de célula e a variação do atraso de célula.

2.6.1 Taxa de perda de células

A taxa de perda de células (CLR - Cell Loss Ratio) para uma conexão ATM é definida como a razão entre o número de células perdidas ou descartadas e o número total de células transmitidas.

A perda de células em uma conexão ATM pode afetar o serviço de diversas maneiras. Em uma conexão de áudio ou voz, ela será notada como uma quebra na continuidade da apresentação. Numa conexão de vídeo, ela pode representar a perda de uma parte de um quadro ou mesmo de todo ele. Em aplicações de dados, a perda de uma célula pode causar a retransmissão pelos protocolos das camadas superiores dos pacotes danificados. Além disso, se a causa da perda de células é devido a um estado de congestionamento, estas retransmissões podem levar a um quadro ainda mais caótico.

2.6.2 Atraso de transferência de células

O atraso de transferência de célula (CTD -Cell Transfer Delay) representa o tempo gasto na retransmissão de uma célula entre os endereços fonte e destino. O CTD em uma rede ATM pode ser causado por vários fatores. Dentre estes, estão os atrasos de codificação, empacotamento, propagação, transmissão, comutação, fila e remontagem. Um baixo valor de CTD indica uma QoS mais alta.

2.6.3 Variação do atraso de células

A variação do atraso de célula (CDV - Cell Delay Variation) descreve a variação no atraso de transferência de células.

Existem dois modos possíveis para sua medição : em um único ponto ou em dois pontos de referência. A medição de um ponto do CDV dá a medida de variação no padrão de células em um único ponto, sendo igual à diferença entre o tempo real de chegada de uma célula e o seu tempo previsto. A medição em dois pontos usa como ponto de referência à fonte e o destino e é igual à diferença entre o valor real do CDV observado entre estes dois pontos e o seu valor calculado.

Esta variação pode ser causada por diversos fatores, oriundos tanto do terminal do usuário quanto da rede. Dentre as causas desta variação no terminal do usuário, encontram-se a multiplexação de células de duas ou mais conexões, a multiplexação na

camada de adaptação (AAL) e a multiplexação com as células de manutenção. Já a variação do atraso na rede é causada principalmente pelo armazenamento de células em um nó de comutação ATM que altera a forma do fluxo de células que chega no nó seguinte.

2.7 O VRRP (Virtual Router Redundancy Protocol)

As soluções de roteamento implementados para a INFOVIA-MT são soluções integradas de roteamento de alta disponibilidade(Anexo-03). Uma das tecnologias utiliza o protocolo VRRP(Virtual Router Redundancy Protocol) que dinamicamente nomeia responsabilidade para um roteador virtual em uma rede. Conforme a [RFC2338] este protocolo só é utilizado com roteadores IPv4. Uma especificação diferenciada deverá ser produzida se semelhante funcionalidade for desejável em um ambiente IPv6[RFC2026 sessão 10].

Um roteador rodando o protocolo VRRP pode se tornar até 255 roteadores virtuais em um único roteador físico. O roteador virtual é um objeto abstrato gerenciado pelo protocolo VRRP que funciona como o roteador default para os hosts de uma rede local. Esse roteador abstrato possui uma identificação (VRID) associado a um endereço IP comum à rede local como se fosse uma interface real. O roteador virtual pode responder como backup de até 254 roteadores virtuais distribuídos em dois ou mais roteadores físicos.

Um roteador Virtual Máster é eleito para assumir a responsabilidade de encaminhar os pacotes enviados para o endereço IP associado com o roteamento e resolver as questões de ARP. Este endereço IP é o default Gateway das estações da rede. Quando o roteador Master falha, o conjunto de roteadores virtuais estão disponíveis para assumir a responsabilidade de encaminhamento dos pacotes de forma dinâmica. Assim pode-se montar uma estrutura tolerante a falhas como mostra a implementação realizada para a Infovia-MT (Anexo-03).

2.8 Integração SNA com ATM para a INFOVIA-MT.

A IFOVIA-MT inicialmente constituída de um ambiente paramente SNA estruturada em MAJORNODES do VTAM, concentrando vários pontos do interior de Matos Grosso através de circuitos TRANSDATA, vários pontos da região do CPA via cabos coaxiais, interligando todos os estados da Federação através da rede SERPRO, utilizando o APLINC456 para diversas aplicações SNA dentre elas o RENAVAM e RENASH.

A integração dessas redes foi viabilizada através de uma solução compreendendo um roteador IBM-2216 configurado com uma interface ESCON e outra interface ATM OC-3. Como contingência funciona em paralelo uma controladora IBM-3172 configurada com dois canais Ethernet. Ambos equipamentos foram interligados a uma ELAN exclusiva para o ambiente Mainframe. O acesso ao legado SNA pode ser feito por todas as estações das sub-redes IP da INFOVIA-MT, através de autenticação no RACF, controlado pelo sistema de Firewall Central. Qualquer usuário cadastrado no RACF pode ter acesso às aplicações do legado via Internet através de um GATEWAY do APPLINX. O APPLINX transforma automaticamente as aplicações caractere do IBM-3270 em HTML e JAVA para as ferramentas browser do ambiente WEB(Anexo-02).

3 - Elementos importantes para o Acordo de Nível de Serviços.

Os elementos indispensáveis para um acordo de nível de serviços são os parâmetros de desempenho, disponibilidade e segurança da rede (largura de banda, congestionamento, latência, tempo de resposta e vazão)[RJC00]. A ênfase principal está em definir e medir a qualidade do Serviço (QoS), o atendimento e o tratamento aos serviços solicitados pelos usuários, a disponibilidade do ambiente e a sua vulnerabilidade. Empregam-se técnicas de organização e métodos e ferramentas auxiliares para aquisição e medição dos dados dos indicadores do Acordo de Nível de Serviços.

Os requisitos para construção de um Acordo de Nível de Serviços são baseados na coleta de dados para um ponto de partida, o estabelecimento da abrangência do acordo, a definição clara das responsabilidades entre as partes, o ambiente suportado e o horário de atendimento. O PDCA pode ser aplicado em todo o ciclo de acompanhamento dos itens de controle do SLA, sendo que no planejamento definem-se as metas e freqüências de apuração, os métodos para atingir os ICs e os treinamentos. Na fase de execução faz-se a implementação do processo. Na fase de verificação faz-se o acompanhamento dos ICs (Índices de Controle) fazendo análise de tendências, tomando ações corretivas se necessário e padronizando.

Os indicadores podem ser acompanhados pelas medidas, realinhados conforme o estabelecimento de metas entre as partes:

Quesito / Acordo	**I**	**II**	**III**
Tempo de conclusão	48 horas	24 horas	12 horas
Tempo de Resposta	< 10s 50%	< 10s 70%	< 10s 90%
Disponibilidade	90%	98%	100%
Nível de Segurança	N/A	Recomendada	Máxima
Desempenho	Médio	Recomendado	Máximo
Número de usuários	N+10%	N+20%	N+30%
Largura de Banda	Compartilhada fixa	Compartilhada QoS	Dedicada
Freqüência de Auditoria	Mensal	Horária	Proativa
Nível de Contingência	Ass. Técnica	Redundante	Automática

Backup	N/A	Parcial	Completa
Auditoria	N/A	Parcial	Completa
Combate a Vírus	N/A	Servidores	Servidores+estações
Inventário de HW/SW	N/A	Servidores	Servidores+estações

Tabela 3-1 Exemplo de Itens de Controle do SLA

3.1 A Qualidade dos serviços(QoS) Fim a Fim

A Qualidade de Serviço (QoS) em redes é um aspecto importante para as redes de pacote como um todo e para as redes IP em particular. Este item do capítulo que trata o SLA abre uma discussão dos parâmetros, os protocolos e os mecanismos envolvidos com a garantia de qualidade de serviço com ênfase nas redes de pacotes tipo IP. Considerando que o cenário tende para cada vez mais termos computadores utilizando o TCP/IP.

Neste contexto o IP é certamente uma alternativa bastante atrativa como plataforma padrão de suporte para as aplicações fim-a-fim, pois está naturalmente presente em milhões de máquinas. É importante utilizar a metodologia PDCA para estar periodicamente verificando a tendência para as redes como um todo (Redes privadas, redes metropolitanas, redes de telecomunicações, redes industriais) ou se existem outras tendências a considerar, pois o IP não é a única opção tecnológica para o suporte de aplicações em redes.

Existe um certo consenso de que as tecnologias de comutação (Níveis 2 e 3), algumas vezes denominadas genericamente de "comutação de pacotes" (Packet Switching), devem prevalecer como opção tecnológica para as redes de computadores e como suporte às aplicações como um todo. As opções mais comuns de tecnologias de comutação disponíveis para utilização em redes sem maiores restrições de porte, desempenho ou cobertura geográfica (LAN - Local Area Networks, MAN - Metropolitan Area Networks ou WAN - Wide Area Networks) são as seguintes [Tan96]:

ATM - Asynchronous Transfer Mode (Nível 2)

Frame Relay (Nível 2)

IP (Nível 3)

A primeira situação corresponde à utilização da tecnologia ATM como um backbone de rede. Neste backbone, as aplicações utilizam as conexões lógicas de alto desempenho do ATM e, eventualmente, podem prescindir ou depender pouco do IP. Exemplos específicos neste contexto são as aplicações de voz sobre ATM (VTOA - Voice Transport over ATM) [Dan98] e o MPOA (MultiProtocol over ATM) [Dav96]. Este cenário é mais apropriado em redes de alto desempenho.

Uma Segunda situação pode ser citada para o Frame Relay quando o mesmo é utilizado em redes corporativas MAN e WAN. Na segunda situação, o IP predomina e é o maior responsável pela comunicação fim-a-fim (usuário-a-usuário).

Nada impede entretanto que na implementação da comunicação utilize-se em trechos da rede o protocolo IP (Nível 3) sobre algumas das tecnologias de rede de nível 2 citadas. Como exemplos de alternativas possíveis temos o IP over ATM, IP over Frame Relay, IP over Ethernet e IP over Ethernet Switched.

O importante a considerar nesta discussão é que estas tecnologias são, neste caso, meramente mecanismos de transporte de pacotes entre roteadores e, assim sendo, prevalece na rede as características do IP. Este é um cenário típico das redes de grande público (Internet, intranets) e, também, das redes de acesso(Anexo-02).

Assim sendo, as aplicações tendem a executar sobre redes de pacotes e, dependendo do tipo da rede, as opções são de execução sobre IP (com dependência do mesmo) ou sobre alguma tecnologia de nível 2 de alto desempenho.

A rede TCP/IP foi desenvolvida tendo como uma de suas premissas básicas o requisito de poder ser utilizada com os diversos tipos de meios físicos e tecnologias existentes na época de sua criação, de forma a viabilizar a comunicação entre as aplicações fim-a-fim em rede.

Em termos práticos, a rede IP foi desenvolvida de forma a ser capaz de comutar sobre meios físicos e tecnologias de nível 2 confiáveis, não-confiáveis, de alto desempenho e de baixo desempenho. Neste contexto histórico, as decisões arquiteturais tomadas na concepção do protocolo IP foram, na sua maioria, no sentido da simplicidade visando atender o cenário imaginado na época para sua implantação em termos de rede. Este paradigma de concepção impõe algumas restrições técnicas ao IP e,

por conseqüência, restringe as aplicações suportadas às aplicações com poucos requisitos de qualidade.

O cenário atual das aplicações mudou. Hoje, o cenário de utilização das redes IP exige que qualquer aplicação deva rodar com qualidade sobre o IP. De certa forma o paradigma mudou e a questão que segue vem a ser a identificação das eventuais limitações do IP e procedimentos necessários para adequá-lo à nova realidade das aplicações.

A qualidade de serviço em redes IP é adquirida utilizando-se um conjunto de novos recursos dependendo das necessidades das aplicações.

3.1.1 Características das fontes de tráfego utilizando QoS.

3.1.1.1 Fontes de vídeo

Com o desenvolvimento das redes de comunicação, os serviços de vídeo têm assumido uma importância crescente, pois se tornam necessários para atender o grande número de aplicações que envolvem transmissão de vídeo. Faz-se necessário, portanto, uma correta caracterização de suas propriedades para que se possam calcular parâmetros tais como o atraso devido a multiplexação, o tamanho do buffer requerido e a banda passante necessária para a transmissão do vídeo.

Sinais de vídeo geralmente consomem grande banda passante. Por exemplo, para uma fonte transmitindo quadros de 512 x 512 a cada 1/30 s, obter-se-á uma taxa aproximada de 63 Mbps, em codificação PCM. O que ocorre, entretanto, é que, a uma taxa de transmissão de quadros tão alta, a maioria destes, contêm apenas pequenas variações sobre os quadros anteriores, possibilitando assim uma codificação que observe a correlação entre os quadros. As fontes de variação, de um modo geral, podem ser classificadas em mudanças de cenas, que é uma variação descontinua, movimentos dentro de uma cena, que são variações suaves com correlação temporal ou grandes variações ocasionais devido à movimentação de pessoas e da câmera, e mudanças na sutileza dos detalhes das imagens bidimensionais do vídeo.

As variações de longo-intervalo surgem principalmente das mudanças de contexto no vídeo devido a mudanças de cena. A mudança na taxa binária ocorre como um degrau e as características da variação das taxas binárias seguintes à mudança de cena

são completamente diferentes daquelas antes da mudança. A escala de tempo destas mudanças é da ordem de vários segundos.

As variações de curto-intervalo são causadas basicamente pela mudança de contexto da imagem dentro de uma única cena.

Estas variações de taxas binárias mudam suavemente e são correlacionadas temporalmente. Estas correlações decaem exponencialmente com o tempo.

As variações internas surgem principalmente devido ao processamento de blocos dentro de um quadro. Porém, como a maioria dos esquemas de codificação utiliza buffers com tamanho suficiente para absorver estas variações, estas se tornam imperceptíveis externamente. A necessidade de se tratar estas variações somente surgirá no caso em que os dados forem entregues diretamente à rede, sem a passagem pelo buffer.

Um modelo selecionado para o sistema utiliza N fontes independentes de vídeo de taxas binárias variáveis que são suavizados em buffers de entradas individuais e acumulados num buffer principal do montador e desmontador de pacotes (PAD -Packet Assembly and Desassembly). A saída destes buffers é multiplexada em unidades de células ou pacotes de tamanho fixo. Os pacotes se acumulam num buffer comum e são entregues a um canal de alta velocidade segundo uma ordenação FIFO (First In, First Out).

Entre os modelos mais importantes propostos para a resolução do sistema de filas estão os seguintes : os processos auto-regressivos, as cadeias de Markov de tempo contínuo, as cadeias de Markov e os processos de Poisson modulados por Markov. Os dois primeiros são modelos para variações de curto-intervalo, onde apenas são consideradas as variações das taxas binárias dentro de uma cena. Conclui-se, portanto, que esses modelos são úteis para fontes de vídeo que apresentam uma distribuição das taxas binárias sem súbitas variações e alta correlação internas ao quadro. Os dois últimos são modelos para variações de longo intervalo.

Em todos os modelos citados, as fontes são consideradas independentes e apresentam uma grande correlação entre chegadas sucessivas. A análise do processo de chegada de um modelo AR para fins analíticos é muito complexa e, como conseqüência, o seu uso é apenas viável para fins de simulação. Entretanto, esta aproximação produz resultados bastante acurados.

O modelo CMTC permite uma análise bem simples para o processo de chegada de uma fonte de vídeo e de seu agregado.

Sua principal vantagem está no pequeno esforço computacional envolvido, já que seus resultados podem ser obtidos de modo similar ao modelo UAS, usado para fontes de voz.

Os modelos de cadeia de Markov e o MMPP atentam para fontes de vídeo com mudanças de cenas, mas necessitam de uma análise bem mais complexa do que os modelos AR e CMTC. Enquanto nas cadeias de Markov é difícil a determinação de seus parâmetros de modo a combinar com os de uma fonte de vídeo genérica, mais resultados são necessários para a validação do modelo MMPP.

3.1.1.2 Fontes de dados

Uma aproximação simples para o caso de fontes de dados seria tratá-la como um processo de Poisson, para o caso contínuo, ou um processo geométrico do tempo entre chegadas, para o caso discreto.

Em um caso interativo, as taxas de transmissão de pacotes costumam ser baixas, ao contrário do que ocorre na transmissão de um arquivo, quando as taxas costumam ser bem mais altas.

Nas redes tradicionais de pacotes, o tamanho dos mesmos pode ou não variar, o que já não ocorre em redes ATM, onde as unidades transmitidas são células de tamanho fixo e pequeno em relação aos pacotes.

3.1.1.3 Fontes de voz

Podem-se observar dois períodos característicos em uma fonte de voz : os períodos ativos, que é o período de fala, e o inativo, que é o período de silêncio. No período ativo, a fonte gera pacotes de tamanho fixo em intervalos regulares enquanto que no inativo, nenhum pacote é gerado.

Uma boa aproximação para uma conversa normal é aquela que considera o tempo de duração de um período dado por uma distribuição exponencial, embora apresente imprecisões quanto ao período inativo, visto que este pode representar um silêncio

prolongado durante a fala de outra pessoa ou um silêncio curto devido a pausas durante a fala.

Aproximar o processo de chegada por uma exponencial, que é um processo sem memória, significa considerar o processo como sendo um processo de renovação, ou seja, sem correlação entre chegadas sucessivas. Entretanto, ao se considerar o tráfego produzido pelo conjunto de fontes de voz, tem-se que o processo resultante não é mais um processo de renovação visto que a taxa instantânea de chegada varia de acordo com a quantidade de fontes ativas no momento.

Um modelo para superposição de fontes considerando N fontes independentes de voz superpostas, cada uma delas gerando pacotes a uma taxa constante. Todos os pacotes gerados alimentam um buffer comum de tamanho finito que é servido por um servidor, que representa o canal de transmissão, com uma vazão constante.

Entre os protocolos sugeridos para a resolução do sistema de filas destacam-se o modelo de chegada e serviços uniformes (UAS - Uniform Arrival and Service), um modelo de um processo Semi-Markoviano, o SMP (Semi-Markov Process), as Cadeias de Markov de Tempo Contínuo (CMTC); e um modelo de matrizes geométricas, o MMPP de 2 estados.

Nos modelos UAS, CMTC e SMP, todas as fontes são consideradas independentes e possuem processos de chegada representados por um processo de renovação, que alterna entre os períodos ativos e inativos. A diferença entre eles está na modelagem do processo de chegadas durante o período ativo e como o serviço é realizado para fins de tratamento analítico.

Já o modelo MMPP não considera o processo de chegada de uma única fonte de forma isolada, mas sim o do tráfego agregado como um todo.

À exceção do modelo UAS com filas finitas, nenhum dos modelos apresentados possuem fórmulas fechadas para o cálculo dos parâmetros desejados, tal como a taxa de perda de células, que só podem ser obtidos através de resolução numérica.

Além disto, em alguns destes modelos, como o MMPP, o esforço computacional envolvido é muito grande.

3.1.2 Desafios da QoS em redes IP

A base instalada de plataforma IP é muito grande, as aplicações emergentes exigem garantia de qualidade, o IP como protocolo não tem praticamente nenhuma garantia de qualidade, nenhuma garantia de vazão constante, pacotes podem ser descartados ou perdidos, não há compromisso com o tempo de entrega de pacotes.

Tem-se como desafio uma situação de como se adequar às necessidades das aplicações sem efetivamente mudar o protocolo. A mudança para o IP (Versão 6) [Tho96] manteve o paradigma da simplicidade inicial do IPv4. O IPv6 ou Ipng (New Generation) aborda outras questões de implementação do protocolo (Endereçamento, segurança) e não apresenta nenhuma solução completa para os desafios de QoS.

A forma de contornar a inexistência de mecanismos adequados para implantar aplicações dependentes de QoS em IP consiste então em propor novos protocolos, algoritmos e mecanismos que tratem das deficiências tecnológicas intrínsecas ao protocolo e permitam o suporte efetivo de qualquer tipo de aplicação sobre redes IP.

3.1.3 A tendência das novas aplicações sobre IP

A base instalada de IP cresceu consideravelmente e as novas aplicações surgiram com exigências de abrangências a várias tecnologias tais como: Telefonia e Fax sobre IP (VoIP), Comércio Eletrônico, Vídeo sobre IP, Educação à Distância (EAD) , Vídeo-Conferência, Aplicações WorkGroup-WorkFlow, Aplicações Multimídia e Aplicações Tempo Real.

A maioria das aplicações citadas envolvem a transferência de múltiplos tipos de mídia (dados, voz, vídeo, gráficos) com requisitos de tempo e sincronização para a sua operação com qualidade.

3.1.4 A Qualidade de Serviços (QoS) nas redes IP

A qualidade de serviço (QoS) nas redes IP é um aspecto operacional fundamental para o desempenho fim-a-fim das novas aplicações. Assim sendo, é importantes o entendimento dos seus princípios, parâmetros, mecanismos, algoritmos e protocolos desenvolvidos e utilizados para a obtenção de uma QoS.

A obtenção de uma QoS adequada é um requisito de operação da rede e seus componentes para viabilizar a execução de uma aplicação com qualidade.

Qualidade de Serviço (QoS) é um requisito da(s) aplicação(ões) para a qual exige-se que determinados parâmetros (atrasos, vazão, perdas, disponibilidade) estejam dentro de limites bem definidos no SLA (valor mínimo, valor máximo). A QoS é garantida pela rede, suas componentes e equipamentos utilizados. Do ponto de vista dos programas de aplicação, a QoS é tipicamente expressa e solicitada em termos de uma "Solicitação de Serviço" ou "Acordo de Nível de Serviços". A solicitação de QoS da aplicação é denominada tipicamente de SLA (Service Level Agreement) [Job99] [Jam98].

Uma vez que a rede garanta este SLA, tem-se como resultado que a aplicação VoIP em questão poderá executar garantindo a qualidade de voz prevista para os seus usuários se comunicando simultaneamente através da rede IP.

Do ponto de vista dos usuários, tem-se normalmente que a qualidade obtida de uma aplicação pode ser variável e, a qualquer momento, pode ser alterada ou ajustada (para melhor qualidade ou pior qualidade). Por exemplo, pode-se assistir um vídeo com uma qualidade de 32 fps (Frames per Second) ou 4 fps e, fundamentalmente, isto depende da qualidade de vídeo esperada pelo usuário final. Embora este comportamento possa ser dinâmico do ponto de vista dos usuários finais, do ponto de vista das redes os SLAs são estáticos ou com limites bem definidos, eventualmente, podem ser alterados. A alteração num SLA implica numa nova solicitação de qualidade de serviço à rede em questão.

Do ponto de vista de um gerente ou administrador de redes, a percepção da qualidade de serviço é mais orientada no sentido da utilização de mecanismos, algoritmos e protocolos de QoS em benefício de seus clientes e suporte às aplicações. Ou seja, como efetivamente a rede e seus componentes podem garantir os inúmeros SLAs definidos para diversos usuários e aplicações. Outros aspectos importantes do ponto de vista gerencial são a escalabilidade e flexibilidade da solução implantada. A escalabilidade dos protocolos, algoritmos e mecanismos de QoS é um assunto relevante quando consideramos a possibilidade de estender a garantia de QoS através de múltiplos domínios administrativos de IP.

A flexibilidade dos mecanismos de controle de QoS é um fator determinante na aceitabilidade dos mesmos pela comunidade.

3.1.5 Parâmetros de qualidade de serviços

A QoS necessária às aplicações é definida em termos de um SLA. Na especificação do SLA são definidos os parâmetros de qualidade de serviço. Alguns dos mais comumente utilizados são: Vazão (Banda), Atraso (Latência), Jitter, Taxa de Perdas, Taxa de Erros e Disponibilidade.

É necessário considerar que não são todas as aplicações que realmente necessitam de garantias fortes e rígidas de qualidade de serviço (QoS) para que seu desempenho seja satisfatório. Dentre as novas aplicações mencionadas anteriormente, as aplicações multimídia são, normalmente, aquelas que têm uma maior exigência de QoS.

No mínimo, as aplicações sempre precisam de vazão (banda), portanto podemos considerar que este é o parâmetro mais básico e certamente mais presente nas especificações de QoS. Este parâmetro da qualidade de serviço é normalmente considerado durante a fase de projeto e implantação da rede.

Pode-se tentar identificar as exigências em termos de QoS das aplicações multimídia ilustrando algumas situações práticas. Uma aplicação multimídia off-line envolvendo, por exemplo, dados, gráficos e arquivos com animação (vídeo), não necessita de sincronização e, assim sendo, não necessita de QoS da rede. Observe que se tem dado correspondente a uma animação que, em termos práticos, necessita de uma determinada vazão, eventualmente carrega a rede, mas não exige atrasos, sincronização ou tempo de resposta. Este é um caso típico onde a necessidade de QoS reduz-se a uma necessidade de vazão, normalmente atendida pelo próprio projeto da rede.

Para aplicações multimídia de conferência de áudio, garantir apenas a vazão não é suficiente. Neste caso específico, os atrasos de comunicação e as perdas de pacotes influenciam na interatividade dos usuários e na qualidade da aplicação. Considerando números, se esta aplicação gera uma vazão de 64 Kbps, mesmo a utilização de uma LP (Linha Privada) em rede WAN de 256 Kbps pode não ser suficiente, pois os atrasos e perdas decorrentes da operação podem prejudicar a qualidade da aplicação. Diz-se então que a aplicação exige uma qualidade de serviço da rede.

3.1.5.1 A vazão

A vazão (banda) é o parâmetro mais básico de QoS e é necessário para a operação adequada de quase todas as aplicações. Em termos práticos as aplicações geram vazões que devem ser supridas pela rede. Em um projeto de rede deve-se levar em conta o requisito da vazão típica para a qualidade de serviço das aplicações envolvidas:

Aplicação	**Vazão Típica**
Transacionais	1 Kbps a 50 Kbps
Quadro Branco(Whiteboard)	10 Kbps a 100 Kbps
Voz	10 Kbps a 120 Kbps
Aplicações Web (WWW)	10 Kbps a 500 Kbps
Transferências de arquivos(grandes)	10 Kbps a 1 Mbps
Vídeo (Streaming)	100 Kbps a 1 Mbps
Aplicação Conferência	500 Kbps a 1 Mbps
Video MPEG	1 Mbps a 10 Mbps
Aplicação Imagens Médicas	10 Mbps a 100 Mbps
Aplicação Realidade Virtual	80 Mbps a 150 Mbps

Tabela 3.2 - Vazão Típica de Aplicações em Rede

3.1.5.2 Latência (Atraso)

A latência e o atraso são parâmetros importantes para a qualidade de serviço das aplicações. Ambos os termos podem ser utilizados na especificação de QoS, embora o termo "latência" seja convencionalmente mais utilizado para equipamentos e o termo "atraso" seja mais utilizado com as transmissões e propagação de dados.

A latência da rede pode ser adquirida através do somatório dos atrasos impostos pela condição da rede e equipamentos utilizados na comunicação. Do ponto do usuário da aplicação, a latência resulta em um tempo de resposta de entrega da informação pela aplicação.

Os principais fatores que influenciam na latência de uma rede são os atrasos de propagação (Propagation Delay), a velocidade de transmissão e o processamento nos equipamentos incluindo o enfileiramento de pacotes.

O atraso de propagação corresponde ao tempo necessário para a propagação do sinal elétrico ou propagação do sinal óptico no meio físico utilizado, fibras ópticas, satélites, par metálico. E um parâmetro imutável onde o gerente de rede não tem nenhuma influência. No mapeamento da rede podem-se catalogar os valores de atrasos entre os pontos do backbone de uma rede WAN mantendo sob observação os valores para o atraso de propagação entre cidades e seus meios físicos de comunicação:

Trecho	Atraso de Propagação (Round Trip Delay) em mseg	Meio Físico
Cuiabá - Rondonópolis	10	Fibra óptica monomodo
Cuiabá - Cáceres	5	Fibra óptica monomodo
Cáceres – Rondonópolis	17	Fibra óptica monomodo

Tabela 3.3 - Atrasos de Propagação - Fibras Ópticas – Exemplos

A velocidade de transmissão é um parâmetro possível de ser controlado pelo gerente de redes visando normalmente à adequação da rede à qualidade de serviço acordada no SLA. (Em se tratando de redes locais (LANs) [Tan96], as velocidades de transmissão são normalmente bastante elevadas, tendendo a ser tipicamente superior a 10 Mbps dedicada por usuário quando utilizando LAN Switches [Mat97]).

Num cenário de redes locais (LANs) tem-se normalmente o custo de investimento inicial da implementação das LANs cujos materiais de infra-estrutura e serviços são ofertados com garantias de no mínimo 15(quinze) anos.. Em se tratando de redes de longa distância (WANs) as velocidades de transmissão são dependentes da escolha da tecnologia de rede WAN (Linhas privadas, frame relay , satélite, ATM). Embora exista obviamente a possibilidade de escolha da velocidade adequada para garantia da qualidade de serviço, observam-se neste caso restrições e/ ou limitações nas velocidades utilizadas, tipicamente devido aos custos mensais envolvidos na operação da rede. Além desse fator, a disposição geográfica traz algumas restrições quanto à disponibilidade tanto da tecnologia quanto da velocidade de transmissão desejada. Em termos práticos,

trabalha-se em WAN tipicamente com vazões da ordem de alguns megabits por segundo (Mbps) para grupos de usuários.

O resultado das considerações discutidas é que a garantia de QoS é certamente mais crítica em redes WAN onde se trabalha com velocidades (Vazão) mais baixas e a latência (Atrasos) é muito maior quando se compara com o cenário das redes locais(LANs). Outro fator que contribui para a latência da rede é o somatório de atrasos referente ao processamento realizado nos equipamentos. Numa rede IP fim-a-fim os pacotes são processados ao longo do percurso entre origem e destino por roteadores (comutação de pacotes), Switches (comutação de quadros), Servidores de Acesso Remoto (RAS) (comutação de pacotes) e Firewalls(processamento no nível de pacotes ou no nível de aplicação).

Considerando que a latência é um parâmetro fim-a-fim, os equipamentos finais (hosts) também têm sua parcela de contribuição para o atraso. No caso dos hosts, o atraso depende de uma série de fatores, tais como capacidade de processamento do processador, disponibilidade de memória, mecanismos de cache, processamento nas camadas de nível superior da rede, programa de aplicação e banco de dados.

Observa-se que os hosts são também um fator importante para a qualidade de serviço e em determinados casos podem ser um ponto crítico na garantia da QoS. Esta consideração é particularmente muito importante no momento de formulação do SLA para equipamentos servidores (Servers) que têm a tarefa de atender solicitações simultâneas de clientes em rede.

Nos comutadores ATM a latência refere-se ao tempo que o comutador precisou para levar a célula ou quadro quebrado em células da interface de entrada até a interface de saída. Portanto, quanto menor o tempo, melhor. O que se pode assegurar é que, de fato este tempo é pequeno em comutadores ATM, desde que a intensidade do tráfego não seja maior que a capacidade de comutação do equipamento. Nos casos onde começa a haver descartes de células, as células que ficam no sistema tendem a encher os buffers, fazendo com que a demora no atendimento a uma determinada célula tenda a crescer consideravelmente. Portanto é importante o planejamento da capacidade dos buffers. Buffers muito pequenos antecipam os descartes, buffers muito grandes causam menos descarte mas aumentam a latência fazendo com que a célula não alcance o destino por timeout. Nos casos das LANE o protocolo TCP/IP pode entrar em slow-start causando implicações no desempenho do ambiente [KAL96].

3.1.5.3 Jitter

O jitter é um outro parâmetro importante para a qualidade de serviços para as aplicações que dependem de alguma forma da garantia de que as informações (pacotes) devem ser processadas em períodos de tempo bem definidos. Este é o caso, por exemplo, de aplicações de voz/ fax sobre IP (VoIP) e aplicações de tempo real.

Do ponto de vista de uma rede de computador, o jitter pode ser entendido como a variação no tempo e na seqüência de entrega das informações (Packet-Delay Variation) devido à variação na latência da rede. Os atrasos impostos à informação são variáveis devidos aos tempos de processamento diferentes nos equipamentos intermediários da malha da rede pública.

O problema dos pacotes fora de ordem poderia ser resolvido com o auxílio de um protocolo de transporte como o TCP (Transmission Control Protocol) [Ste94] que verifica a seqüência das mensagens e fazem as devidas correções. Entretanto, na prática tem-se que a grande maioria das aplicações multimídia opta por utilizar o UDP (User Datagram Protocol) [Ste94] ao invés do TCP pela maior simplicidade e menor overhead deste protocolo. Nestes casos, o problema de seqüência deve ser resolvido por protocolos de mais alto nível normalmente incorporados à aplicação como, por exemplo, o RTP (Real Time Transfer Protocol) [Mau98].

O jitter introduz distorção no processamento da informação na recepção e deve ter mecanismos específicos de compensação e controle que dependem da aplicação em questão. Genericamente, uma das soluções mais comuns para o problema consiste na utilização da técnica de "buffering".

3.1.5.4 Perdas

As perdas de pacotes em redes IP ocorrem principalmente em função de fatores tais como descarte de pacotes nos roteadores e switch routers e as perdas de pacotes devido a erros ocorridos na camada 2 (PPP - Point-to-Point Protocol, Ethernet, Frame Relay) durante o transporte dos mesmos.

De maneira geral, as perdas de pacotes em redes IP são um problema sério para determinadas aplicações como, por exemplo, a voz sobre IP. Neste caso específico, a perda de pacotes com trechos da voz digitalizada implica numa recusa por parte do usuário em não aceitar o serviço proposto pela aplicação. O que fazer em caso de perdas de pacotes é uma questão específica de cada aplicação em particular.

Do ponto de vista da qualidade de serviço da rede (QoS) a preocupação é normalmente no sentido de especificar e garantir limites razoáveis (Taxas de Perdas) que permitam uma operação adequada da aplicação.

3.1.5.5 Disponibilidade

A disponibilidade é um aspecto da qualidade de serviço que deve ser abordada em todas as fases ao longo do tempo obedecendo a um ciclo PDCA, desde a fase de planejamento, implementação e manutenção da infra-estrutura da rede. A Infra-estrutura que envolve aspectos desde energia elétrica, ar-condicionado, e todos elementos críticos. Em termos práticos, a disponibilidade é uma medida da garantia de execução da aplicação ao longo do tempo e depende de fatores tais como garantia e manutenção da disponibilidade dos equipamentos utilizados na rede proprietária do cliente (LAN, MAN ou WAN) e disponibilidade da rede pública, quando a mesma é utilizada (Operadoras de telecomunicações e provedores).

As empresas dependem cada vez mais das redes de computadores para a viabilização de seus negócios (Comércio eletrônico, home-banking, atendimento on-line) colocando a disponibilidade como requisito bastante rígido. A título de exemplo, requisitos de disponibilidade acima de 99% do tempo são termos de SLA comuns para a QoS de aplicações WEB, aplicações cliente-servidor e aplicações de forte interação com o público.

3.2 As alternativas técnicas de QoS

Uma vez identificado os parâmetros relacionados com a qualidade de serviço das aplicações, discutem-se os protocolos, mecanismos e algoritmos utilizados na implementação efetiva da qualidade de serviço.

Numa rede IP a qualidade de serviço consiste num mecanismo fim-a-fim (host de origem a host de destino) de garantia de entrega informações (Pacotes). Assim sendo, a implementação da garantia de QoS pela rede implica em atuar nos equipamentos envolvidos na comunicação fim-a-fim visando o controle dos parâmetros de QoS. Os parâmetros (atrasos, jitter) que devem ser controlados visando à obtenção da qualidade de serviço não são, infelizmente, localizados num único equipamento ou componente da rede. A figura do Anexo-02 ilustra um exemplo de situação onde na trajetória fim-a-fim dos pacotes com equipamentos tipo LAN Switch, roteadores, Firewalls, utilizando-se uma rede pública de comutação de pacotes e as estações de trabalho dos usuários finais.

Os mecanismos de QoS devem portanto atuar nestes equipamentos, camadas de protocolo e entidades de forma cooperada. Uma das atribuições dos gerentes de Tecnologia da Informação (TI) é justamente a escolha e implementação adequada dos agentes de mecanismos de QoS num cenário com Equipamentos e Componentes de Rede Envolvidos na Qualidade de Serviço (QoS). Uma outra questão importante a perceber-se na implementação dos mecanismos de controle da qualidade de serviço é a percepção do momento onde estes mecanismos são necessários. Efetivamente, a necessidade de garantir a qualidade de serviço se coloca mais fortemente nos períodos de pico de tráfego quando a rede enfrenta uma situação de congestionamento ou de carga muito elevada. Neste tipo de situação os mecanismos de QoS buscam soluções

para decisões de como alocar os escassos recursos de banda, selecionar o tráfego de pacotes, priorizar os pacotes, descartar pacotes (quais e quando).
No Anexo-07 retrata-se a coleta de dados representando o comportamento da vazão para o link de 1 Mbps de acesso à Internet da rede apresentada no Anexo-02.

Algumas alternativas técnicas básicas para implementar a qualidade de serviços em redes IP poderão ser utilizadas conforme exigência da aplicação: IntServ - Integrated Services Architecture com o RSVP (Resource Reservation Protocol); DiffServ - Differentiated Services Framework; MPLS (MultiProtocol Label Switching); SBM (Subnet Bandwidth Management); Dimensionamento e Soluções Proprietárias.

Todas as alternativas citadas acima, excetuando-se as soluções proprietárias, são iniciativas do IETF (Internet Engineering Task Force) [IETF]. O IETF está fortemente empenhado em propor um conjunto de soluções para os mecanismos de controle de QoS que garanta a interoperabilidade dos mesmos entre diferentes fornecedores. Isto se dá em função da importância das redes IP para o suporte de novas aplicações multimídia e tempo real. A estratégia e os mecanismos específicos destas alternativas técnicas são:

3.2.1 Int Serv - Integrated Services Architecture e RSVP - Resource Reservation Protocol

A alternativa técnica IntServ [IntServCharter] está atualmente sendo definida pelo IETF e corresponde a um conjunto de recomendações (RFCs - Request for Comments) visando a implantação de uma infra-estrutura robusta para a Internet que possa suportar o transporte de áudio, vídeo e dados em tempo real além do tráfego de dados transportado na infra-estrutura atual.

O conjunto de recomendações proposto é denominado de arquitetura de serviços integrados (Integrated Services Architecture) [Brad94] e visa uma garantia de qualidade de serviço (QoS) para as aplicações.

A qualidade de serviço (QoS) na arquitetura IntServ é garantida através de mecanismos de reserva de recursos na rede, onde a aplicação faz reserva dos recursos que vai utilizar, antes de iniciar o envio de dados pela rede, através do protocolo de sinalização RSVP (Resource Reservation Protocol) [RFC_2205] cujos equipamentos roteadores e switches possuem recursos para aceitar a solicitação e garantir a demanda

solicitada. Uma vez aceita a reserva, os fluxos de dados (streams) correspondentes à aplicação são identificados e roteados segundo a reserva feita para os mesmos.

O RSVP é um protocolo de sinalização que atua sobre o tráfego de pacotes IP numa rede Internet. O RSVP é um protocolo eficiente do ponto de vista da qualidade de serviço (QoS) na medida em que provê granularidade e controle fino das solicitações feitas pelas aplicações. Sua maior desvantagem é a complexidade inerente à sua operação nos roteadores que, eventualmente, pode causar dificuldades nos backbones de redes com vários domínios.

O RSVP é um protocolo bem aceito pelo mercado e é disponibilizado na grande maioria dos sistemas operacionais e equipamentos de rede de diversos fornecedores.

A maneira de como os elementos da arquitetura IntServ procedem para garantir a qualidade de serviços solicitada está detalhada em várias recomendações (RFCs) [JSMNet] relacionadas a seguir:

RFC 2211 - Specification of the Controlled-Load Network Element Service: Define como um elemento de rede roteador ou switch garante uma solicitação de reserva para um serviço de carga controlada solicitado por uma aplicação.

RFC 2212 - Specification of Guaranteed Quality of Service: Define como um elemento de rede roteador ou switch garante uma solicitação de reserva para um serviço garantido solicitado por uma aplicação.

RFC 2215 - General Characterization Parameters for Integrated Services Network Elements: Definem o conjunto de parâmetros gerais de caracterização e controle dos fluxos com QoS para os elementos da rede roteadores e switches.

RFC 2213 - Integrated Services Management Information Base using SMIv2: Define aspectos técnicos relativos à base de dados de gerenciamento dos serviços na arquitetura IntServ.

3.2.2 DiffServ - Differentiated Services Framework

A alternativa técnica DiffServ é uma outra iniciativa do IETF com o objetivo de permitir também o transporte de áudio, vídeo, dados em tempo real e dados convencionais na Internet.

A qualidade de serviço na solução DiffServ é garantida através de mecanismos de priorização de pacotes na rede sem reserva de recursos, onde os pacotes são classificados e marcados, sendo processados segundo o seu rótulo (DSCP - Differentiated Service Code Point) [RFC_2474].

A idéia básica da solução DiffServ é reduzir o nível de processamento necessário nos roteadores para fluxos de dados definindo poucas Classes de Serviços numa estrutura comum de rede.

Os inúmeros fluxos de tráfego (Pacotes IP) gerados pelas aplicações são agregados a poucas classes de serviço em função da qualidade de serviço (QoS) especificada para o fluxo. Esta tarefa é tipicamente realizada nos roteadores de entrada do backbone (Edge routers) e, desta forma, o processamento nos roteadores intermediários (Core) fica mais simplificado e independente dos fluxos individuais das aplicações.

Os roteadores de backbone(Core) processam os pacotes (Forwarding) segundo basicamente as classes de serviços e roteando um fluxo de pacotes agregados.

Cada pacote recebe um processamento baseado na sua marcação(DSCP) conforme duas classes de serviços relacionadas ao comportamento do roteador ou switche (PHB - Per-Hop Behavior):

Expedited Forwarding (EF) - Esta classe de serviço provê o maior nível de qualidade de serviço, emulando uma linha dedicada convencional minimizando os atrasos a probabilidade de perdas e o jitter para os pacotes. A EF utiliza mecanismos de buferização(buffering) e priorização de filas.

Assured Forwarding (AF) - Esta classe de serviço emula um comportamento semelhante a uma rede com pouca carga mesmo durante a ocorrência de congestionamento. A latência negociada é garantida com um alto grau de probabilidade. O serviço AF define 4 níveis de prioridade de tráfego. Para cada nível de prioridade são definidos 3 preferências de descarte de pacotes (semelhante ao Frame Relay). Este serviço usa mecanismos de Traffic Shaping (Token Bucket) e usa o algoritmo RED (Randon Early Detection).

As alternativas IntServ e DiffServ não são concorrentes ou mutuamente exclusivas, são soluções complementares que podem ser utilizadas conjuntamente. Uma alternativa de uso conjunto das duas soluções seria a utilização do DiffServ no backbone de

roteadores (Core) e o IntServ/RSVP nas redes de acesso(Edge), na medida em que provê um bom controle com granularidade dos requisitos de QoS das aplicações.

3.2.3 Dimensionamento

A alternativa denominada dimensionamento é o que pode se chamar de uma alternativa de projeto básico. No caso, a rede e seus recursos são dimensionados na fase de projeto com implementação de mecanismos proativos de forma a não termos congestionamento. Por exemplo, faz-se um contrato de banda para atender toda a demanda necessária , mas configura-se e se paga somente à banda utilizada o que resulta na ausência de congestionamento e um faturamento justo.

Esta solução apresenta duas dificuldades principais. A primeira corresponde à escassez de recursos do dimensionamento para atender a demanda de pico. Em particular para as redes WAN esta normalmente é uma alternativa proibitiva. A segunda dificuldade é a identificação e gerência dos pontos de ocorrência de congestionamento dada à multiplicidade e diversidade de equipamentos utilizados e a própria complexidade das redes(Anexo-08). De maneira geral, esta é uma solução factível apenas para ambientes de um único domínio de gerência de redes onde se podem adotar mecanismos de alocação dinâmica de recursos(Banda).

3.3 Os Mecanismos do QoS

As alternativas técnicas de QoS são implementadas em roteadores, switches e hosts através da utilização de diversos tipos de mecanismos tais como protocolos de sinalização, algoritmos de prioridade, algoritmos de escalonamento, algoritmos de controle de filas, algoritmos de congestionamento, tendo cada um a sua funcionalidade e aplicabilidade.

3.1.1 Protocolos de Sinalização

A finalidade de um protocolo de sinalização (Signalling Protocol) no contexto da qualidade de serviço em redes IP pode ser entendida como um mecanismo utilizado

pelas aplicações (hosts) para informar ou solicitar à rede sua necessidade de qualidade de serviço (QoS);

Além disso, os protocolos de sinalização permitem também que os equipamentos de rede (Roteadores e switches) possam trocar informações de cooperação mútua visando a garantia da qualidade de serviço aceita pela rede.

Como exemplos de protocolos de sinalização no contexto da qualidade de serviço podemos citar o RSVP - Resource Reservation Protocol: utilizado na iniciativa IntServ do IETF e o LDP - Label Distribution Protocol: utilizado na alternativa MPLS para a distribuição de rótulos entre os equipamentos roteadores.

3.3.2. Prioridades

Os algoritmos de prioridade (Priority Algorithms) são um outro mecanismo utilizado pelos equipamentos de rede para a garantia da qualidade de serviço. Neste contexto, a prioridade pode ser entendida como um mecanismo que provê diferentes tempos de espera para o processamento dos pacotes ou quadros.

Estes algoritmos são tipicamente implementados em roteadores mas algumas tecnologias de rede de nível 2 também suportam a utilização destes mecanismos.

O IP Precedence é definido na RFC 1122 e é uma solução de priorização de pacotes prevista no IPv4 no campo TOS (Type of Service) do cabeçalho dos pacotes IP.

O Priority Queuing é um algoritmo utilizado por alguns fornecedores para priorização de pacotes IP nas filas de saída de roteadores.

A maioria das tecnologias de redes nível 2 suporta mecanismos de priorização para implantação de garantias de QoS, entre elas podemos citar:

ATM (Asynchronous Transfer Mode);

Ethernet em LAN Switches (Padrões IEEE 802.1p e IEEE 802.1Q);

FDDI (Fiber Distributed Data Interface);

Token Ring e 100VG-AnyLAN

3.3.3 Escalonamento

O objetivo do mecanismo de escalonamento normalmente presente em roteadores procura garantir que fluxos (streams) diferentes de pacotes obtenham os recursos que lhes foram alocados (banda e processamento). O recurso banda e processamento adquirido deve ser distribuídos de forma equivalente (Fairness) aos fluxos ativos no equipamento em questão.

Os mecanismos de escalonamento mais utilizados são o WRR - Weighted Round Robin, GPS - Generalized Processor Sharing, CBQ - Class Based Queuing e WFQ - Weighted Fair Queuing.

3.3.4 Controle de filas

Um outro aspecto que deve ser controlado numa fila diz respeito aos mecanismos de descarte de pacotes. A política de descarte de pacotes é necessária na ocorrência de um congestionamento e visa garantir a eqüidade (Fairness) quanto à distribuição da banda e do processamento. Estes mecanismos não evitam proativamente a ocorrência do congestionamento e portanto devem ser parte integrante dos algoritmos de escalonamento de filas.

Os mecanismos mais utilizados nos roteadores para lidar com controle de filas são os algoritmos SFQ - Stochastic Fair Queuing, CFQ - Class-Based Fair Queuing e WFQ - Weighted Fair Queuing.

3.3.5 Congestionamento

Os mecanismos de controle de congestionamento são também importantes para a implantação da qualidade de serviço numa rede IP. A idéia básica destes mecanismos é a inibição dos fluxos de pacotes durante o período de congestionamento de forma que os geradores de fluxos de pacotes IP reduzam a sua carga sobre a rede. Com menor quantidade de pacotes sendo entregue à rede tem-se uma tendência de redução no nível de congestionamento. Neste sentido, estes mecanismos podem ser entendidos como mecanismos de controle de fluxo de pacotes. Os algoritmos mais utilizados para lidar

com o congestionamento de filas de pacotes IP são o RED - Random Early Detection, WRED - Weighted Random Early Detection e ECN - Explicit Congestion Notification.

3.3.6 Serviços providos pela rede ATM para controle do tráfego

Com o advento das aplicações multimídia, iniciou-se uma demanda por serviços que garantissem uma banda passante mínima e níveis baixos de atraso e variação de atraso (jitter).

Dessa forma, serviços heterogêneos devem ser providos pela rede de forma a se adequar ao tipo de tráfego que ela recebe. A partir de um modelo conhecido de tráfego associado a determinados requisitos de qualidade de serviço (QoS), a rede irá alocar recursos ao longo do caminho percorrido pelo fluxo em questão. A alocação dos recursos na rede é controlada pelos mecanismos de controle de admissão de conexão, o qual levam em consideração os parâmetros de serviço contratados e os recursos ainda disponíveis na rede.

Os serviços fornecidos podem ser determinísticos, ou seja, com garantias absolutas de atraso máximo, vazão e taxa máxima de perdas, o que é possível devido à existência de um modelo que forneça limites superiores para as taxas de transmissão. Os serviços podem também ser não determinísticos devido a uma modelagem da fonte geradora de tráfego.

São definidas quatro classes de serviço que buscam caracterizar cada tipo de tráfego, as quais são : o serviço de taxa binária constante (CBR - Constant Bit Rate), o serviço de taxa binária variável (VBR - Variable Bit Rate), o serviço de taxa binária indefinida (UBR - Undefined Bit Rate) e o serviço de taxa binária disponível (ABR - Available Bit Rate).

O serviço CBR acomoda tráfegos com taxas constantes de transmissão tal como vídeo e voz não comprimidos. O serviço VBR acomoda tráfegos com taxas variáveis onde métodos de compressão fazem variar as taxas, determinando períodos de rajada no tráfego, como ocorre, por exemplo, em vídeos MPEG. O serviço ABR se destina a aplicações com requisitos mínimos de vazão e atraso. Finalmente, o serviço UBR se aplica aos casos onde não há qualquer requisito de QoS, e, portanto, são toleradas

quaisquer taxas de transmissão e níveis de atraso, tal como ocorre em transferência de arquivo em background.

Um determinado conjunto de parâmetros deverá ser fornecido pela fonte de forma a permitir o controle do tráfego e uma alocação correta de recursos. Dentro os parâmetros mais utilizados estão à taxa binária de pico, a taxa binária média, o índice de rajada e o tamanho médio de uma rajada. A rajada consiste na quantidade de informação gerada nos momentos de pico e o índice de rajada consiste na razão entre as taxas de pico e média.

3.3.6.1 Serviço VBR

O serviço VBR é aplicado aos casos onde as taxas de transmissão da fonte variam muito. Nesses casos, o tráfego é caracterizado por períodos de atividade e silêncio e/ou tem uma taxa binária que varia continuamente, não sendo possível uma suavização para um tráfego CBR, devido aos altos índices de rajada.

A principal dificuldade está em se caracterizar o tráfego e de se prever como o mesmo se modifica ao longo da rede, o que causa problemas na obtenção do ganho com a multiplexação estatística e na garantia da QoS requerida.

Faz-se então necessário um conhecimento acurado de como se comporta o tráfego para os diversos tipos de fontes existentes conforme descrito em 3.1.1.

3.3.6.2 Serviço CBR

Os serviços CBR geram tráfego constante com índice de rajada igual a 1 e é o que ocorre, por exemplo, com a emulação de circuito, a voz e o áudio e com o vídeo não comprimido.

A voz CBR é transmitida através de modulação PCM, onde cada amostra é quantizada e codificada em um número constante de bits. O áudio, por sua vez, requer taxas de amostragem maiores com maior quantização, o que a difere da voz pela maior quantidade de bits por segundo.

O vídeo CBR mantém uma taxa constante de quadros, porém com uma quantidade de bits por quadro variável, o que leva à necessidade da existência de um buffer de suavização para gerar o tráfego CBR.

O gerenciamento do tráfego CBR é simples, bastando à rede alocar uma banda passante constante para a conexão.

3.3.6.3 Serviço ABR

As aplicações de comunicação de dados, de forma geral, podem suportar atraso e variações de atraso nos pacotes, porém são muito sensíveis às perdas. O serviço ABR informa o usuário sobre um provável congestionamento que pode gerar perdas, através de realimentação, e a aplicação, por sua vez, transmite de acordo com as taxas disponíveis na rede.

Através da realimentação, torna-se possível o suporte a aplicações que não podem caracterizar seus tráfegos no estabelecimento da conexão, mas que podem se adaptar a um protocolo de controle de fluxo. O serviço ABR considera que se a fonte se adequar de certo modo ao controle de fluxo, então nenhum pacote será perdido.

O serviço ABR realiza um suporte econômico ao tráfego de dados, uma vez que ao evitar retransmissões de pacotes por um protocolo da camada superior, ele evita que haja um aumento indiscriminado da vazão, o que poderia também levar a rede a um colapso.

Um conjunto de parâmetros pode ser usado para descrever o serviço ABR. Em redes ATM, por exemplo, existem 3 parâmetros importantes : Taxa mínima de células (MCR), Taxa de pico de células (PCR) e Taxa disponível de células (ACR).

Os parâmetros MCR e PCR são fornecidos pelo usuário, enquanto que o parâmetro ACR é ajustado pela fonte de acordo com as informações recebidas da rede. O parâmetro ABR varia entre MCR e PCR e indica a taxa atual de transmissão de células para a conexão fornecida pela rede.

3.3.6.4 Serviço UBR

O serviço UBR não requer qualquer conhecimento das características do tráfego, não oferecendo qualquer garantia de QoS.

O usuário, nesse caso, deve estar disposto a tolerar qualquer nível de taxa de transmissão, atraso ou perdas de unidades transmitidas. A QoS efetiva pode ser gerenciada através de regras de engenharia. O único mecanismo de realimentação usado é a notificação de congestionamento que poderá ser usado pelos sistemas finais para se adaptarem ao estado de congestionamento.

3.4 A Gerência dos índices de controle do SLA

A cada serviço contratado entre as partes envolvidas no SLA, destacado item para acompanhamento do seu comportamento em relação à meta estabelecida, faz-se necessário utilização dos mecanismo da A&G(Administração e Gerência de Redes) voltada para o negócio envolvido.

No contexto de gerenciamento de elementos ativos de redes a *MIB(Management Information Base)*, tem a função de guardar as informações transferidas ou modificadas pelo uso dos protocolos de gerenciamento. As informações contidas na MIB correspondem a objetos que representam recursos reais que estão sendo gerenciados, seus atributos, as operações que executam e as notificações que fornecem. Com o objetivo de gerenciar a operação das redes de computadores de forma que os serviços oferecidos pelas mesmas sejam eficientes integrados e interoperáveis, a ISO dividiu as atividades de gerenciamento em cinco áreas funcionais específicas:

a) Gerenciamento de Falhas: Investiga a ocorrência de falhas, incluindo funções de diagnóstico e correção.
b) Gerenciamento de Configuração: Identifica mudanças significativas, modelando a configuração dos recursos lógicos e físicos.
c) Gerenciamento de desempenho: Monitora o desempenho da rede permitindo o controle da qualidade do serviço.
d) Gerenciamento de Contabilização: Verifica quais e quanto dos recursos estão sendo usados, determinando o custo associado ao seu uso.
e) Gerenciamento de segurança: Garante a segurança definida para a rede.

Dentro de cada área funcional foram desenvolvidas funções de suporte para o gerenciamento. O gerenciamento de configuração consiste na manutenção e monitoração da estrutura física e lógica da rede, exercendo o controle sobre a configuração da rede, de tal forma que esta possa ser mudada para , por exemplo, aliviar congestionamentos, isolar falhas e atender as necessidades dos usuários. O gerenciamento de falhas permite detectar problemas na comunicação das redes utilizando mecanismos de detecção e isolamento. O gerenciamento de desempenho permite monitorar e avaliar o desempenho dos sistemas em parâmetros como atrasos, vazão, numero de retransmissões, mudar configurações da rede para manter um bom nível de desempenho. O gerenciamento de segurança permite gerenciar serviços de proteção de acesso, autenticação e manutenção de senhas. O gerenciamento de contabilização permite determinar e alocar custos e despesas para uso dos recursos de comunicação.

A função de Supervisão de Alarmes fornece a capacidade para monitorar as falhas dos elementos ativos de rede em tempo quase real, determinando-se a natureza da falha e sua localização, armazenando a ocorrência em um endereço de destino(Servidor de Logs) para um acesso futuro.

Um sistema de LOG alternativo permite garantir a integridade dos sistemas de coleta de dados de fontes diversas na rede, suportando paginação instantânea (informações atualizados até o último minuto), permitindo a execução condicional de comandos com base em informações encontradas nos arquivos do sistema de LOG.

Uma interligação em redes precisa de um software que permita aos administradores detectar problemas, controlar roteamentos, localizar computadores e elementos ativos de redes. Em uma interligação em redes TCP/IP, os roteadores IP conectam-se a redes heterogêneas, os protocolos para gerenciamento da interligação operam em nível de aplicativo e comunicam-se utilizando os protocolos de nível de transporte TCP/IP.

Cada Host ou roteador executa um programa agente de gerenciamento. O administrador seleciona um software cliente que se comunica com o programa agente. Um mecanismo de autenticação é utilizado para assegurar que apenas administradores autorizados possam acessar ou controlar um roteador específico.

O protocolo de gerenciamento de redes TCP/IP mais utilizado atualmente é o SNMP (Simple Network Management Protocol) em suas versões SNMPv1(RFC 1155 e

RFC 1157), SNMPv2(RFC 1441 e RFC 1452) e SNMPv3 criadas para acrescentar maiores níveis de segurança.

O padrão para informações gerenciadas é conhecido como *MIB (Management Information Base)*, que especifica os dados que um roteador ou host deve manter e as operações permitidas em cada um deles.

A MIB para TCP/IP classifica as informações de gerenciamento em categorias codificadas no identificador usado para especificar um objeto. A variável MIB apresenta uma definição lógica de cada dado e o software agente do roteador é responsável pelo mapeamento em sua estrutura interna de armazenamento de dados.

Uma outra estrutura SMI (Structure of Management Information) especifica um conjunto de regras usadas para definir e identificar as variáveis MIB. A SMI faz restrições quanto ao tipo das variáveis permitidas na MIB, especificando regras para nomenclatura, tipos e validações.

O padrão ASN.1 (Abstract Syntax Notation) da ISO especifica uma linguagem formal com duas características: O código usado pelo protocolo e a descrição. Ambos os casos elimina a ambigüidade e assegura a interoperabilidade. O espaço do nome do identificador de objeto é absoluto e hierárquico. A raiz da hierarquia do identificador do objeto não tem nome, dispondo de três descendentes: ISO, ITU e Joint. Os descendentes são strings curtas com números inteiros para identificá-las. O nome de um objeto na hierarquia é a seqüência de rótulos numéricos dos nós ao longo de um caminho da raiz até o objeto. Por exemplo 1.3.6.1.1 denota o nó "diretório".

A MIB agrupa todas as variáveis em oito categorias sub-árvores do nó mib. Assim os nomes de todas as variáveis MIB correspondentes ao IP tem um identificador que começa com o prefixo 1.3.6.1.2.1.4 que é representado textualmente por: *iso.org.dod.internet.mgmt.mib.ip. A uma variável da MIB denominada ipInReceives foi atribuído o identificador numérico 3(três) sob o nó de espaço de nome IP então sua representação textual será "iso.org.dod.internet.mgmt.mib.ip.ipInReceives" e a sua representação numérica correspondente será 1.3.6.1.2.1.4.3*.

O protocolo SNMP lança todas as suas operações em um paradigma de busca de armazenamento (RFCs 1021, 1022, 1023 e 1024).

Uma mensagem SNMP consiste em três partes principais: Uma versão do protocolo, um identificador de comando do SNMP e uma área de dados. A área de

dados é dividida em (Unidades de Dados do Protocolo - PDUs). Cada PDU consiste em uma solicitação enviada pelo cliente ou uma resposta enviada pelo servidor.

A sintaxe da definição específica da PDU para definição de uma mensagem SNMP get-request :

```
GetRequest-PDU::= [0]
    IMPLICIT SEQUENCE {
        Request-id
            RequestID,
        error-status
            ErrorStatus,
        error-index
            ErrorIndex,
        Variable-binding
            VarBinList
    }
```

A forma codificada do ASN.1 utiliza campos de comprimentos variáveis para representar itens. Em geral, cada campo começa com um cabeçalho que especifica o tipo do objeto e o comprimento em bytes. A mensagem começa com um código para sequence que tem um comprimento de 41 octectos. O primeiro item da seqüência é um numero inteiro de octecto que especifica a versão do protocolo. O campo community é armazenado em um string de seis octectos que contém a identificação da comunidade.

3.5 - A continuidade do SLA através do PDCA.

A manutenção do SLA depende das políticas e dos objetivos da qualidade. Para cumprir e atingir os níveis dos IC's estabelecidos no SLA, as metodologias pela qualidade definem a autoridade pelos meios de execução e a responsabilidade pelos resultados obtidos de cada um.

Um Sistema da Qualidade é a estrutura organizacional, responsabilidades, procedimentos, processos e recursos por meio da qual a Política e os Objetivos da Qualidade podem ser cumpridos e atingidos. Uma das principais ferramentas utilizadas para manutenção e melhoria da qualidade é a aplicação do ciclo PDCA[WMC99].

P (Plan-Planejamento): definição dos objetivos a alcançar na melhoria ou manutenção dos processos, e dos métodos que permitirão atingir os objetivos propostos.

D (Do-Execução): realização dos treinamentos necessários, execução das atividades que compõem os processos e realização das medições da qualidade.

C (Check-Verificação): verificação dos resultados das atividades executadas, comparando as medições realizadas com os objetivos estabelecidos.

A (Action-Ação Corretiva): correção de desvios e eliminação de obstáculos seguindo os padrões (manutenção), ou estabelecimento de novos padrões (melhoria).

Somente será possível manter um SLA mediante a institucionalização de princípios básicos de disponibilidade, segurança, desempenho e interoperabilidade nas organizações envolvidas no acordo.

4 – As políticas de segurança recomendadas para a Organização

4.1 – Diretrizes fundamentais para a Organização[PIC99]

Toda e qualquer informação interna gerada, adquirida e processada pela organização deve ser considerada de sua propriedade, devendo ser utilizada exclusivamente para os interesses da instituição. Toda e qualquer informação do cliente gerada, adquirida e processada pela organização deve ser considerada de sua responsabilidade, devendo ser utilizada exclusivamente para os interesses do cliente.

Para garantir o armazenamento adequado e proteção quanto ao seu acesso e uso, as informações devem ser identificadas e classificadas quanto a confidencialidade, integridade e disponibilidade.

Os *ativos* disponibilizados para os colaboradores devem ser os obrigatoriamente necessários e indispensáveis ao exercício de suas atividades. Todo colaborador deve possuir identificação pessoal e intransferível, com prazo de validade definido e liberação de acesso compatível com as atividades a ele atribuídas.

A divulgação de informações de propriedade da organização deve seguir a classificação para elas estabelecidas, devendo ser evitada sua exposição e utilização na presença de pessoas não autorizadas ou em locais públicos. Todo recurso deve ser testado e homologado de forma controlada, preferencialmente em ambiente distinto ao de produção, antes de autorizado o seu uso. Todo recurso de informação deve ser usado de forma a preservar sua integridade física e seu bom funcionamento. Somente deve ser permitido o uso de recurso de informação que esteja homologado e autorizado pela organização, compatível com o ambiente interno, protegido de acordo com a classificação de segurança, inventariado, com documentação atualizada, de acordo com as cláusulas contratuais do SLA e a legislação em vigor.

A utilização de ativos da organização por terceiros deve ocorrer conforme os padrões de segurança adotados pela Empresa, de forma a preservar a confidencialidade, a integridade, a disponibilidade das informações da organização e de seus clientes. A entrada ou saída de ativos nas instalações da organização deve ser autorizada e registrada, sendo proibido o seu transporte sem as medidas de proteção correspondentes. Para liberação de acesso o colaborador deve possuir capacitação mínima nos processos, nos sistemas de informação e na utilização dos recursos necessários à sua rotina de trabalho.

A manutenção preventiva nos recursos de informação deve ser documentada e realizada periodicamente, de acordo com a necessidade e com as recomendações do fabricante, mesmo quando se tratarem de produtos elaborados internamente. O controle da execução de um *processo crítico* em sua totalidade, não deverá estar sob a responsabilidade de um único colaborador. Todos os processos críticos deverão estar documentados pelos seus gestores. Ativos compartilhados devem ser usados de forma que outros colaboradores não sejam prejudicados. A utilização de equipamentos não pertencentes à organização deve ser autorizada e seguir os padrões de segurança internos, sendo necessário identificá-los de forma diferenciada. Os equipamentos devem sofrer avaliação periódica quanto a sua obsolescência. Caso esta seja comprovada, este ativo deve ser substituído. Os *ativos críticos* devem ser suportados por plano de contingência que garanta a continuidade dos serviços e previna ou solucione situações de anormalidade. Este plano deve ser documentado e, periodicamente testado e revisado. Para garantir o cumprimento e a disseminação das questões relativas à segurança da informação, a organização contará com uma Unidade de Segurança da Informação.

A Unidade de Segurança da Informação tem as seguintes responsabilidades: realizar estudos, definir e validar as orientações técnicas relativas à segurança da informação na organização; disseminar a cultura de segurança da informação na instituição; promover a atualização da Política de Segurança da Informação, à medida que novos conteúdos forem sendo agregados aos processos da organização. definir a periodicidade, os critérios e a responsabilidade pela execução de auditoria quanto ao cumprimento da Política de Segurança da Informação da organização.

Os colaboradores devem notificar a Unidade de Segurança da Informação sobre qualquer fraude, sabotagem, desvio ou falha na segurança da informação que chegue ao seu conhecimento. É direito do colaborador o conhecimento total e irrestrito da Política de Segurança da Informação da organização.

Casos omissos a este documento devem ser tratados pela Unidade de Segurança da Informação. O não cumprimento da Política de Segurança da Informação acarretará ao colaborador as penalidades previstas no Regulamento interno da organização, ou outras penalidades cabíveis a serem definidas no âmbito judicial.

4.2 – Requisitos de um SLA com políticas de segurança[PIC99]

4.2.1 - Administração

Os administradores de ambiente informatizado devem possuir substitutos capacitados.

Os administradores de ambiente informatizado são responsáveis por avaliar e atualizar seus respectivos ambientes, devendo informar a Unidade de Segurança da Informação possíveis ameaças à segurança.

Os administradores de ambiente informatizado são responsáveis por manter a documentação física e lógica, dos seus ambientes, atualizada.

Os administradores de ambiente informatizado são responsáveis por manter a infra-estrutura da rede corporativa em perfeitas condições de funcionamento, garantindo a qualidade e disponibilidade dos serviços. Para tal, podem utilizar-se de ferramentas apropriadas.

Antes de adotar novas tecnologias, o gerente da área técnica e a Unidade de Segurança da Informação devem avaliar o impacto da nova tecnologia na segurança das informações.

O responsável pelo suporte deve definir os padrões de sistemas de informática a serem seguidos pela organização.

O administrador do ambiente deverá atualizar as correções de sistemas (*patch*, *service pack*, etc.) periodicamente, conforme procedimento operacional específico do ambiente.

A Unidade de Segurança da Informação deve informar às gerências de informática sempre que disponibilizar novas versões de ferramentas de segurança.

Os servidores, estações de trabalho e equipamentos de interconexão de rede devem possuir data e horário sincronizados, obedecendo ao fuso horário de sua localização geográfica.

Os servidores, estações de trabalho e equipamentos de interconexão de rede devem ter apenas instalados softwares homologados pela organização.

Os administradores do ambiente devem conhecer todos os índices do SLA – Acordo de nível de serviços e providenciar monitoramento de seus índices disparando alarmes quando atingir faixas de alerta.

4.2.2 – Backup

A realização de *backup* dos servidores deve ser preferencialmente feita em horário estabelecido no contrato do SLA, fora do horário de expediente, de forma a não prejudicar o desempenho da rede corporativa.

O *backup* dos servidores deve ser gerado em duas mídias distintas, com conteúdo idêntico, sendo estas armazenadas da seguinte forma:

Uma cópia guardada em lugar seguro contra danos e roubos, próximo à sala do servidor.

Uma cópia a ser guardada em ambiente distinto ao da primeira cópia e que garanta sua recuperação em caso de destruição do ambiente de produção.

A periodicidade para retenção das mídias de backup deve estar de acordo com a necessidade de cada serviço e com as leis que os regulamentem.

Os administradores do ambiente informatizado devem determinar procedimentos para realização de testes de integridade e restauração nos *backups* realizados.

A mídia de *backup* deverá conter senha contra acessos indevidos.

Os administradores do ambiente informatizado devem manter as mídias com os *backups* em uso identificadas de forma a permitir rapidamente sua recuperação.

A troca das mídias utilizadas para realização dos *backups* deve obedecer ao período de vida útil recomendado pelo fabricante

4.2.3 - Auditoria

Os responsáveis pelas aplicações devem identificar a necessidade de geração de *log* e o nível de detalhamento nos sistemas e ambientes sob sua responsabilidade.

A auditoria dos *logs* gerados pelos diversos ambientes tecnológicos existentes na organização é função da unidade específica responsável pela auditoria corporativa segregada das demais unidades tecnológicas.

A auditoria dos *logs* gerados pelos diversos ambientes tecnológicos, deve ser realizada periodicamente conforme procedimento e instrução definido pela unidade responsável.

Deverá haver periodicamente auditoria no ambiente físico conforme registros e procedimentos definidos pelo setor responsável.

O administrador de sistemas deve obedecer ao período de armazenamento dos *logs* de cada ambiente específico, conforme procedimento operacional.

4.2.4 - Combate a vírus

Todos os servidores e estações de trabalho devem estar protegidos pelo software antivírus padrão definido pela organização, estando este sempre ativo e atualizado.

O processo de atualização do software antivírus deve ser preferencialmente realizado automaticamente.

A gerência de redes deve definir procedimentos para contingência no caso de contaminação por vírus eletrônico nos servidores e estações de trabalho.

Todos os arquivos manipulados pelos técnicos devem ser verificados quanto à contaminação por vírus eletrônico antes de sua utilização.

Todos os fluxos de vírus devem ser monitorados contabilizados e comparados com o índice de contaminação estabelecido no SLA.

4.2.5 – Cuidados com os recursos computacionais da Organização

Os servidores e equipamentos de interconexão de rede devem ser preferencialmente instalados em salas específicas para este fim, sendo seu acesso controlado e restringido pelos administradores do ambiente informatizado.

Os servidores e equipamentos de interconexão de rede devem utilizar rede elétrica própria e distinta dos demais equipamentos elétricos.

Os servidores, estações de trabalho e equipamentos de interconexão de rede devem ser lacrados com etiqueta contra violação contendo um número de controle.

O detentor do bem deve informar à área de suporte técnico de informática caso a etiqueta seja violada.

A manutenção preventiva nos servidores e equipamentos de interconexão de rede deve ser realizada pelo menos uma vez a cada seis meses, de acordo com tipo, porte e normas de segurança.

Qualquer manutenção corretiva ou preventiva nos servidores e equipamentos de interconexão de rede deve ser acompanhada e registrada pelo administrador do ambiente informatizado.

Os administradores de ambiente informatizado devem periodicamente atualizar a lista dos softwares básicos homologados, registrando as seguintes informações:

a) tipo.
b) número da licença.
c) número de cópias.

d) locais onde estão instalados

Todo equipamento de informática adquirido pela organização deve ser inventariado registrando, no mínimo:

a) número do patrimônio.
b) número de série.
c) modelo.
d) especificação.
e) dados da etiqueta de lacre.
f) local onde será instalado.

O técnico ao realizar atendimento de suporte deve verificar a integridade do lacre de segurança e a configuração da máquina. Em caso de alteração na configuração o inventário deve ser atualizado.

A solicitação de substituição de estação de trabalho ou periférico deve ser feita formalmente pelo detentor do bem.

O administrador do ambiente informatizado deve avaliar a solicitação e providenciar a substituição do equipamento se confirmada a necessidade.

5 - Sugestão de implementação de políticas de segurança

Com base na arquitetura de disponibilidade e segurança definida para uma organização, devem ser feitas as implementações das políticas de segurança nos principais componentes da topologia planejada, por exemplo nos roteadores de borda, Firewalls e aplicações que utilizam VPN*(Virtual Private Network)*.

A topologia projetada pode contemplar a inclusão de um ou mais firewalls internos separando funções organizacionais[FRA01].

Uma política de segurança pode ser aplicada em todos os componentes da arquitetura projetada , incorporando as ACLs(*Access Control List*) dos roteadores, as regras de firewall, as política de IPSec, levando em consideração as operações empresariais internas , clientes, provedores e parceiros.

Mecanismos de auditoria para a arquitetura de segurança devem ser implementados para avaliar o domínio da topologia. A freqüência dessa auditoria, as implicações em performance, custos e riscos da defesa do domínio devem ser avaliados.

As ameaças ao ambiente de TI devem ser previstas e monitoradas, garantindo a certificação aos níveis de segurança propostos para um SLA.

Ataques à sua arquitetura devem ser simulados de forma a validar periodicamente as políticas implementadas.

Um ataque para cada tipo de firewall deve ser projetado para cumprir seu objetivo.

Deve ser estipulada uma simulação designada para um ataque teórico ao sistema de RAS que use TCP SYN, UDP, ou inundações de ICMP.

5.1 - Topologia proposta para laboratório de implementação da INFOVIA-MT

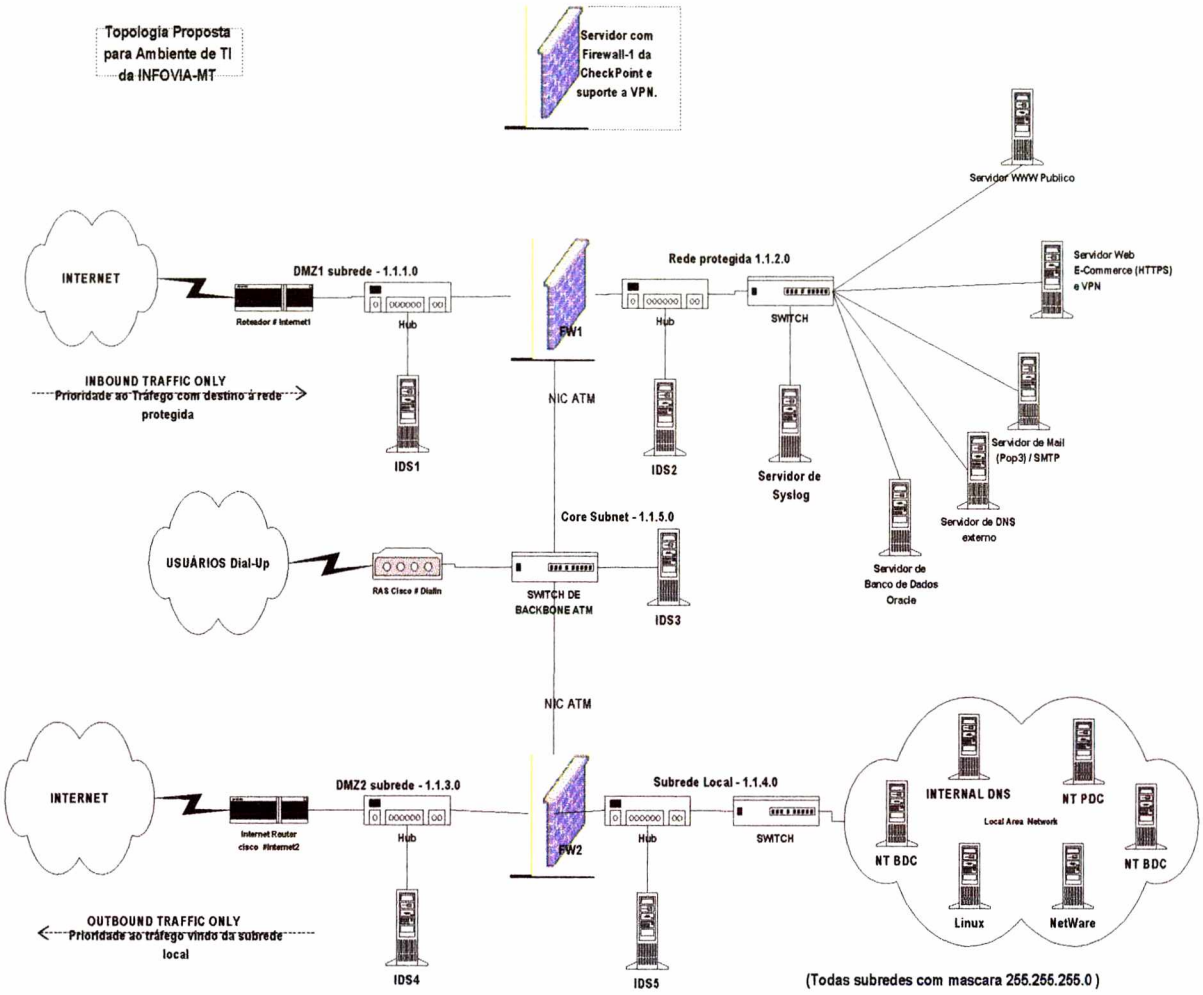


Figura 5-1 – Topologia proposta para implementação de uma política de segurança

5.2 - Roteadores de borda

A topologia do laboratório proposto para implementação de recursos da INFOVIA-MT, define três roteadores para prover acesso externo e servir de importante mecanismo de defesa da linha de borda. Os roteadores propostos suportam três tipos diferentes de lista de acesso: padrão, estendida e reflexiva. O primeiro roteador com conexões vindo para dentro da rede protegida. O segundo só utilizado para tráfico de longo curso (conexões da rede protegida para a Internet). O terceiro roteador para RAS de N usuários simultâneos.

5.3 - Firewalls (Postos de fiscalização)

Dois firewalls de posto de fiscalização (FW1 e FW2) estão com a finalidade de prover segurança da cadeia de servidores. Os firewall são configurados de acordo com o sistema operacional e o produto que se deseja avaliar. Ambos os firewalls estão instalados em um servidor com processador intel Pentium III Dual 1Gz, 1 Gb memória. Estes servidores podem ser atualizados com a versão do Service Pack que se deseja avaliar. Cada Posto de fiscalização estará rodando o software Firewall-1 versão 4.1 com o mais recente Pacote de Serviço (Service Pack 3). Eles estão rodando sobre Windows NT versão 4.0 Service Pack 6, configurados com nível de segurança C2 de acordo com as recomendações do fabricante do sistema operacional. A máquina do FW1 será configurada com um cartão de interface ATM (NIC OC-3 155Mbps OLICOM), sendo definidas 03(três) ELANS (DMZ1, Protegida e RAS). A Elan DMZ1 será associada a subrede 1.1.1.0 e seu endereço de IP é 1.1.1.2. A Elan protegida será associada a subrede 1.1.2.0 e seu endereço IP é 1.1.2.1. A Elan RAS será associada a subrede 1.1.5.0 e seu endereço IP é 1.1.5.1. Também será configurada a máquina do FW2 com as mesmas especificações da máquina do FW1 sendo o NIC ATM OC-3 155 Mbps configurado com 02 (duas) ELANs (DMZ2 e Local), A DMZ2 associada a subrede 1.1.3.0 e seu endereço de IP é 1.1.3.2. A ELAN Local será associada a subrede 1.1.4.0 e seu endereço de IP é 1.1.4.1. O RAS será conectado a Subnet do backbone e seu endereço de IP é 1.1.5.2. Os NICs ATM serão interligados ao switch de backbone via cordão óptico. Os Switches de borda serão interligados ao Switche de Backbone através de seu UP-link ATM OC-3 155 Mbps contendo seus segmentos de vlans fast ethernet associadas às respectivas ELANS. As regras de Firewall para o laboratório utilizando Checkpoint, estão representadas no Anexo-06, devendo ser submetidas a exaustivos testes antes de implementadas em ambiente de produção.

5.4 - VPN para acesso remoto

Os acessos remotos para sócios e usuários da organização serão disponibilizados mediante a sua autenticação. A arquitetura proposta adota o produto Firewall-1 SecuRemote (VPN-1 SecureRemote Version 4.1 – Service Pack 2 3DES) para estabelecer serviços de VPN que estão disponíveis em FW-1. Para o acesso é utilizada a

senha definida no Firewall-1 que identifica o usuário, e autentica com base em suas políticas de segurança.

5.5 - Subrede de servidores protegidos

A sub-rede protegida contém 9 servidoras, O servidor de rede e anti-virus (IP 1.1.2.2), o Servidor de Clientes da rede (IP 1.1.2.3), o Servidor Provedor de Serviços (IP 1.1.2.4), o Servidor dos Parceiros (IP 1.1.2.5), o Servidor de Correio (IP 1.1.2.6), o Servidor de DNS Primário (IP 1.1.2.7), o Servidor de Syslog (IP 1.1.2.9) e o Servidor de IDS (Detetor de Intrusões) (IP 1.1.2.10). Qualquer acesso externo aos dados dessa cadeia de servidores será feito por https que utiliza SSL através de certificado digital comprado da VeriSign. Todas as transações de comércio eletrônico serão executadas por este método.

5.6 - Sistema de detecção de ataques

Cada subnet tem seu próprio Sistema de Detecção de Intrusão que roda em modo promíscuo analisando os pacotes do contexto. O Sistema de Descoberta de Intrusão escolhido envia suas mensagens críticas a um servidor de Syslog em uma rede protegida.

5.7 - Recomendações para implementação das regras de firewall

O modo mais efetivo para interligar uma cadeia de servidores à Internet é instalar um sistema de firewall entre a cadeia de servidores local e a Internet. O firewall assegura que toda a comunicação entre a cadeia de uma aplicação e a Internet seja confrontada com as políticas de segurança estabelecidas. Para prover um nível de segurança ideal, tem que haver um firewall que controla o fluxo de comunicação que atravessa essa barreira de proteção. Um firewall tem que ter a capacidade de obter, armazenar, manipular e devolver a informação derivada de todas as camadas de comunicação e de aplicações.

Uma vez definido que recursos são viáveis de proteção, estipuladas as ações ou procedimentos de administração de risco para proteger recursos incorporados, é necessário que seja projetado mantido e atualizado um jogo básico de regras de segurança a serem implementadas nos firewalls e roteadores de borda. Essas regras devem ser específicas para cada posto de fiscalização não sendo recomendado refletir as mesmas regras em todos os roteadores e firewalls da topologia.

A função principal de um roteador é encaminhar pacotes. Um roteador que propõe fazer as funções firewall não reproduzirá a função de assegurar as políticas de forma completa. Em geral um roteador permite tudo, então só nega serviços específicos ou IPs. Ao contrário o firewall nega tudo, e então permite somente serviços ou IPs específicos. Uma política de segurança básica lista pontos que são sondados e atacados freqüentemente. Bloqueando estes portos cumpre-se uma exigência mínima para segurança desse perímetro. Uma política de segurança rígida bloqueia muitos pontos e fica monitorando constantemente para registrar tentativas de intrusão. Ao bloquear muitos pontos as regras podem incapacitar serviços fundamentais. Então os efeitos potenciais de qualquer recomendação de implementação devem ser avaliados e simulados antes de aplicar em produção.

Nos anexos 04,05 e 06 são apresentadas regras para implementação dos laboratórios de Firewall utilizando-se LINUX (IPchains e Iptables) e Firewall-1 da CheckPoint. O Checpoint para a topologia do laboratório. Uma versão LINUX com ipchains para a topologia do laboratório. Uma versão com LINUX Iptables para qualquer um dos postos de fiscalização da rede WAN.

5.8 – Pontos mais vulneráveis a ataques

Os pontos frequentemente mais sondados e atacados são determinados por portas. Bloquear tais portas é uma exigência mínima para a segurança do perímetro da rede, não sendo a única recomendação para a configuração de um firewall. A regra mais adequada seria bloquear todas as portas que não estão sendo usadas e monitorá-las ativamente para detectar tentativas de invasão.

O bloqueio de certas portas pode desabilitar serviços necessários, portanto deve ser feito um estudo das aplicações envolvidas no ambiente antes da implementação

Somente bloquear estas portas não substitui uma solução detalhada de segurança, pois um atacante poderá obter acesso à rede através de outro meio:

a) Block "spoofed" Addresses:

Pacotes que vêm de fora originados dos endereços da rede privada interna (RFC1918 e 127).

b) Serviços de Login:

Telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin (512/tcp por 514/tcp).

c) RPC e NFS:

Portmap/rpcbind (111/tcp e 111/udp), NFS (2049/tcp e 2049/udp), lockd (4045/tcp e 4045/udp).

d) NetBIOS em Windows NT:

135 (tcp e udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - portas 445(tcp e udp).

e) O X Windows:

6000/tcp por 6255/tcp.

f) Serviços de Nomes:

DNS (53/udp) para todas as máquinas que não são servidores de DNS, DNS de zona de transferência externa (53/tcp) excluindo os secundários externos, LDAP (389/tcp e 389/udp).

g) Correio:

SMTP (25/tcp) para todas as máquinas que não são revezamento de correio externos, POP (109/tcp e 110/tcp), IMAP (143/tcp).

h) Rede WEB:

HTTP (80/tcp) e SSL (443/tcp) excluindo os servidores WEB externos, também pode querer bloquear as portas de alta ordem (8000/tcp, 8080/tcp, 8888/tcp, etc.).

i) Serviços pequenos:

Portas abaixo de 20/tcp e 20/udp, tempo (37/tcp e 37/udp).

j) Miscellaneous:

TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp e 161/udp, 162/tcp e 162/udp), BGP (179/tcp), SOCKS (1080/tcp).

k) ICMP:

Bloco de pedido de eco (ping e traceroute do Windows), bloco partida de respostas de eco, tempo excedido, e mensagens inalcançáveis.

5.9 - Auditoria da Arquitetura de Segurança

O plano de auditoria executará testes na política de segurança instalada em Firewall-1_FW1 e no roteador de borda Internet#1. Para desenvolver este trabalho são necessárias configurações em laboratório com ferramentas apropriadas.

Verificar as regras das políticas do firewall requer medição dos tempos de resposta para determinar se a política está se comportando como planejado, e verificar os índices do SLA. Uma ferramenta utilizada pode ser o nmap com fila de parâmetros para cada caso de teste desejado. As respostas são armazenadas para verificação se o teste passou ou falhou ao notificar qualquer anormalidade. O nmap pode ser usado para registrar serviços desnecessários ou gerar padrões de tráfico para submeter simulações e medir tempos de respostas.

Deveriam ser revisadas contas de usuário e identificados os casos de senhas consideradas fracas. Os troncos de acesso aos servidores e firewalls devem ser analisados para assegurar que só aconteceu tentativa de acesso autorizada.

Os arquivos de log enviados ao Servidor de Syslog pelos roteadores e firewalls deveriam ser auditados e armazenados em backups para referência futura.

A análise de tronco deveria acontecer diariamente, para assegurar que as tentativas de intrusão estão sendo identificados. Porém é importante a observação de que tarefas de auditoria podem consumir 50% dos recursos disponibilizados para usuário.

Toda e qualquer atualização ao firewall externo e aos roteadores devem ser revisadas por pelo menos um outro auditor do grupo de segurança.

Um ataque contra o próprio firewall deve ser projetado e designado para avaliar as vulnerabilidades rotineiramente.

5.10 - Considerações sobre ataques à arquitetura da rede protegida

Quando um sistema chamado pelo cliente tenta estabelecer uma conexão de TCP para um sistema de provedor de serviços (o servidor), o cliente troca com o servidor uma sucessão de mensagens fixas. Esta técnica de conexão aplica-se a todas as conexões de TCP.

O sistema de cliente começa enviando uma mensagem de SYN ao servidor. O servidor reconhece a mensagem de SYN enviando a mensagem de SYN-ACK ao cliente. O cliente termina estabelecendo a conexão respondendo com uma mensagem de ACK. A conexão entre o cliente e o servidor está então aberta, e os dados específicos do serviço podem ser trocados entre o cliente e o servidor.

O potencial para o ataque surge no ponto onde o sistema servidor enviou para o cliente uma mensagem para um reconhecimento (SYN-ACK), porém não recebeu a mensagem de ACK. Isto é chamado de conexão parcialmente aberta(half-open). O servidor enfileirou na memória do seu sistema uma estrutura de dados que descreve todas as conexões pendentes. Esta estrutura de dados é de tamanho finito, e pode se multiplicar criando muitas conexões parcialmente abertas intencionalmente.

Conexões parcialmente abertas são facilmente criadas se realizado spoofing de IP. O sistema atacando envia mensagens de SYN ao sistema de servidor de vítima; estes parecem ser legítimos mas de fato fazem referência a um sistema de cliente que está impossibilitado de responder às mensagens de SYN-ACK. Isto significa que a mensagem de ACK final nunca será enviada ao sistema servidor vítima.

Os dados de conexões parcialmente abertas encherão a estrutura do servidor vítima que ficará impossibilitado de aceitar qualquer conexão entrante nova até o esvaziado da estrutura.

Normalmente há um intervalo de timeout com uma conexão pendente, assim as conexões parcialmente abertas expirarão e o sistema servidor vítima recuperará. Porém, o sistema atacante pode continuar enviando de forma mais rápida pacotes de IP-spoofed que pedem conexões novas simplesmente impedindo que o sistema vítima possa expirar as conexões pendentes.

A localização do sistema atacante é obscura porque a fonte dos pacotes SYN é freqüentemente improvável. Quando o pacote chega ao sistema servidor vítima, não há nenhum modo para determinar sua verdadeira fonte.

Considerando que o protocolo remete pacotes baseados em endereços de destino, o único modo para validar a fonte de um pacote é a introdução de um filtro.

Ë necessário providenciar a configuração de um roteador para que possa reduzir a probabilidade destes ataques. Ë necessário instalar os filtros para proteger a rede interna contra ataques de DDOS. Com a atual tecnologia do protocolo IP, é impossível eliminar pacotes de IP-spoofed. Porém, podem ser criados procedimentos para reduzir o número de pacotes de IP-spoofed. Atualmente, o melhor método é instalar um filtro que proteja a interface externa não permitindo que um pacote obtenha um endereço da rede interna. Além disso deve ser previsto a proteção de ataques de IP-spoofing de origem da rede interna.

Muitos ataques têm êxito porque não são filtrados os conteúdos de pacotes nulos, as assinaturas de IDS não são atualizadas, os sistemas operacionais não tem correções atualizados.

O servidor de rede é um ponto de partida muito utilizado pelos atacantes por várias razões: As aplicações de servidor de rede são de codificação pobre e não são protegidas pelo firewall ou filtradas no roteador, ficando expostas a um grande número de ataques gerando problemas de segurança. Assumir a identidade de um servidor de rede interno é a primeira tentativa buscando prováveis vulnerabilidades. Estas vulnerabilidades podem ser problemas com o sistema operacional, o software de servidor de rede, as aplicações que rodam no local, configurações inseguras do servidor de rede, e práticas de codificações pobres.

Uma vez o atacante escolheu uma vulnerabilidade particular é quase impossível localizar a origem do ataque. Em muitos casos um atacante assumirá identidade de outro hoste na Internet e instalará ferramentas para abrir o caminho pelo servidor de rede de forma que mais tarde o atacante pode voltar e possa executar outro ataque. Também o servidor de FTP e o servidor de DNS pode ser um ponto de entrada usado para uma segunda tentativa.

5.11 - Plano de contingência[PIC99]

A organização deve possuir um plano de continuidade que envolva servidores, equipamentos, aplicações e sistemas críticos de forma a garantir as políticas de

segurança e a disponibilidade dos serviços dentro do Acordo de Nível de Serviços - SLA.

O gestor do recurso deve definir procedimentos para recuperação deste em caso de desastres.

O Plano de continuidade deve ser reavaliado e testado modularmente, semanalmente, mensalmente ou anualmente.

Devem-se prever mecanismos de tolerância à falhas para os equipamentos críticos da rede.

Deve ser instalado grupo motor-gerador para prover energia elétrica em casos de falhas da concessionária.

Devem ser instalados dois grupos de nobreaks sendo um interligado no by-pass do outro para que assuma a carga em casos de manutenção preventiva ou falha.

Devem ser instalados dois sistemas de ar condicionado, sendo um a contingência do outro.

Os sistemas de aterramento, quadros de energia elétrica, circuitos elétricos, cabeamento estruturado e backbone óptico devem ser revisados periodicamente com medições de todas as suas grandezas, registro em sistema especialista de acompanhamento e previsão de anormalidades. Os administradores do ambiente de TI devem tomar todas as medidas preventivas recomendados pelo sistema especialista.

6 – Critérios para avaliação da segurança dos sistemas de computação da Organização

A proposta do Departamento de Defesa Americana enquadra os sistemas de computação em quatro divisões de proteção: D,C,B e A .

Para o DoD o sistema seguro deve controlar, através de uso de características de segurança específicas, o acesso à informação de modo que só os indivíduos devidamente autorizados, ou os processos operando sob seu comando, possam ler, escrever, criar ou apagar informações. Dessa definição[COM95] são extraídos os seis requisitos de segurança básicos para avaliar a segurança de sistemas de computação:

Requisito 1 – Política de Segurança: o sistema deve implementar uma política de segurança explícita e bem definida. Deve existir um conjunto de regras que são seguidas pelo sistema para determinar quando um dado indivíduo, devidamente identificado, tem permissão para acessar um objeto específico devidamente identificado. Os sistemas de computação devem executar uma política de segurança obrigatória que define regras de acesso para manipulação de informação sensível. Essas regras incluem requisitos do tipo: "Nenhuma pessoa que não possua o nível de autorização apropriado pode obter acesso à informação classificada". Adicionalmente , controles de segurança arbitrários são necessários para garantir que apenas usuários, ou grupos de usuários selecionados irão obter acesso aos dados, pois nem todas as pessoas que possuem grau de autorização suficiente para Ter acesso à determinada informação necessitam realmente Fazê-lo.

Requisito 2 – Marcação: rótulos de controle de acesso devem ser associados aos objetos. Deve ser possível marcar todos os objetos com um rótulo que identifique de forma confiável seu nível de sensibilidade.

Requisito 3 – Identificação e autorização: os indivíduos devem ser apropriadamente identificados. Junto com a identificação são guardadas informações sobre o nível de autorização do usuário. As informações de identificação e autorização devem ser mantidas de forma segura pelo sistema de computação, e devem ser associadas a todos os elementos ativos que executem alguma ação relevante para a segurança do sistema.

Requisito 4 – Registro de eventos: informações para auditoria devem ser seletivamente mantidas e protegidas para que as ações que afetem a segurança possam ser rastreadas para identificação do responsável.

Requisito 5 – Garantia: o sistema de computação deve conter mecanismos de hardware/software que possam ser avaliados independentemente, e que forneçam garantias suficientes de que o sistema cumpre os requisitos de 1 a 4. Os mecanismos usados para cumprir esses requisitos são tipicamente embutidos nos sistemas operacionais e são projetados para desempenhar suas tarefas de modo seguro. A base para a confiança nesses mecanismos é a disponibilidade de documentação sobre sua configuração e operação que torna possível a avaliação de sua eficácia.

Requisito 6 – Proteção contínua: os mecanismos que garantem os requisitos básicos devem ser protegidos continuamente contra adulteração ou modificação não autorizada. Nenhum sistema de computação pode ser considerado seguro se os mecanismos que garantem a segurança puderem ser violados. Deve-se prestar uma atenção especial nesse requisito quando forem realizadas atualizações ou reconfigurações do hardware/software do sistema.

Os requisitos acima formam a base para definição dos critérios de avaliação que definem as divisões e classes de segurança

Divisão D: A divisão D engloba os sistemas que oferecem proteção mínima. Essa divisão só contém uma classe , a classe D. São classificados na classe de proteção D os sistemas que foram avaliados mas não cumpriram os requisitos exigidos nas classes de proteção mais altas.

Divisão C: Os sistemas enquadrados nas classes da divisão C são os que fornecem proteção arbitrária, isto é, fornecem mecanismos que permitem definir que indivíduos, ou grupos de indivíduos devem ter acesso a quais recursos , e com que permissões de acesso. Os sistemas nessa divisão devem possuir mecanismos para registrar eventos relevantes à segurança do sistema, os quais serão usados no suporte de auditorias que

permitam contabilizar as ações realizadas por um indivíduo. Nessa divisão os sistemas são enquadrados em duas classes C1 e C2.

Classe C1: A base computacional de segurança enquadrada na classe C1 satisfaz os requisitos de uma política de segurança arbitrária, disponibilizando mecanismos que impeçam o livre acesso dos usuários aos recursos do sistema de computação. Os sistemas nessa classe devem possuir mecanismos de controle capaz de impor limites ao acesso, com base na identificação dos indivíduos. Essa classe de sistemas garante a proteção de informações individuais, ou compartilhadas por um grupo de usuários, contra operações de leitura, modificação ou destruição não autorizadas. Espera-se que o ambiente fornecido pelos sistemas da classe C1 permita que os usuários trabalhem de modo cooperativo, processando dados com o mesmo nível de sensibilidade.

Classe C2: Os sistemas enquadrados na classe C2 devem impor um controle de acesso arbitrário mais refinado que os sistemas da classe C1. Essa classe de sistemas deve garantir a contabilização das ações realizadas por usuários individuais, através de procedimentos de login, de mecanismos para auditoria nos registros de eventos relevantes para a segurança do sistema e do isolamento de recursos alocados a um usuário. Nos sistemas C2, os usuários são impedidos de ler o conteúdo da memória alocada aos outros e de recuperar arquivos apagados ou objetos abandonados por outros usuários.

Divisão B: O principal requisito de uma TCB(Trusted Computing Base) divisão B é a presença da integridade dos rótulos de sensibilidade e sua utilização para colocar em vigor o conjunto de regras de controle de acesso que define uma política de segurança obrigatória. Os sistemas classificados nessa divisão associam rótulos de sensibilidade às estruturas de dados manipuladas no sistema. O fornecedor de sistemas enquadrados na divisão de proteção B deve disponibilizar o modelo da política de segurança no qual o TCB é baseado e fornecer uma especificação da TCB. Devem ser fornecidas evidências que demonstrem que o conceito de monitor de referências foi implementado.

Classe B1: Os sistemas da classe B1 possuem todos os requisitos dos da classe C2, acrescidos de uma descrição informal do modelo da política de segurança, de mecanismos que permitam a associação de rótulos de segurança aos dados, e da presença de mecanismos de controle de acesso obrigatórios, relacionando usuários identificados e enquadrados em níveis de autorização e objetos associados a rótulos de segurança. Os sistemas classificados na classe B1 devem marcar, com os devidos rótulos de segurança, toda informação exportada do sistema; por exemplo, listada em uma impressora. Além disso, o fornecedor do sistema deve comprometer-se a corrigir qualquer falha identificada em testes do sistema.

Classe B2: Nos sistemas de classe B2, a TCB é baseada em uma definição clara e formal do modelo da política de segurança implementada no sistema. Os mecanismos que impõem controle de acesso arbitrário e obrigatório encontrados em sistemas B1 devem ser estendidos a todos os usuários e objetos do sistema de computação. Adicionalmente, são abordados os problemas de segurança causados por canais secretos. A TCB deve ser cuidadosamente estruturada em elementos críticos, ou não, em relação ao aspecto proteção. A interface TCB deve ser bem definida e seu projeto e implementação deve habilitá-lo a se sujeitar a testes mais minuciosos e revisões mais completas. Os mecanismos de autenticação são reforçados e deve ser fornecida uma função confiável de gerenciamento que suporte as funções de administrador e operador. Mecanismos rigorosos de gerenciamento de configuração devem ser impostos para garantir que o sistema não seja adulterado durante a sua fase de operação.

Classe B3: A classe de proteção B3 deve satisfazer os requisitos definidos para um monitor de referências que intermedia todos os acessos dos usuários a objetos do sistema, deve ser aprova de adulterações e deve ser pequeno o suficiente para que possa se sujeitar a análises e testes. Com esse fim, o TCB é estruturado para excluir todo o código que não seja essencial à implementação da política de segurança, sendo os processos de desenvolvimento e implementação da TCB direcionados à minimização de sua complexidade. Deve ser permitida a figura do administrador do sistema. O mecanismo de auditoria deve ser expandido para sinalizar a ocorrência de eventos relevantes à segurança do sistema. Procedimentos de recuperação do sistema, caso

ocorram violações de segurança que comprometam seu funcionamento, devem estar disponíveis.

Divisão A: A divisão A é caracterizada pelo uso de métodos de verificação de seguranças formais que garantam que os controles obrigatórios e arbitrários, empregados no sistema, efetivamente protejam as informações classificadas nele armazenadas e processadas. É exigida extensa documentação do sistema que demonstre que a TCB satisfaz os requisitos de segurança em todos os aspectos do projeto, desenvolvimento e implementação.

Classe A1: Os sistemas da classe A1 são funcionalmente equivalentes aos sistemas da classe B3, no sentido que neles não são adicionados requisitos de políticas ou características de arquitetura. A característica de distinguem os sistemas da classe A é a análise baseada em técnicas de verificação e especificações formais do projeto dos sistemas e o resultante alto grau de garantia que a TCB foi corretamente implementada. Essa garantia baseia-se essencialmente no desenvolvimento, começando com um modelo formal da política de segurança e de uma especificação formal de alto nível do projeto. Em conjunto com a análise extensiva do projeto e de desenvolvimento da TCB necessária aos sistemas de classe A1, um gerenciamento de configuração mais rigoroso é exigido e procedimentos são estabelecidos para que a distribuição física do sistema seja segura.

Tabela 6.1 de relacionamento dos requisitos com as classes de proteção

	Classes de proteção						
Requisitos	**D**	**C1**	**C2**	**B1**	**B2**	**B3**	**A1**
Auditoria			N	C e A	A	A	=
Gerenciamento de Configuração					N	=	C e A
Análise de Canais secretos					N	C	A
Documentação do Projeto		N	=	A	C e A	A	C e A
Verificação e especificação do Projeto				N	C e A	A	C e A
Rótulos nos dispositivos					N	=	=

Controle de acesso arbitrário		N	C e A	=	=	C e A	=
Exportação de informação rotulada				N	=	=	=
Exportação para dispositivos multinível				N	=	=	=
Exportação para dispositivos com nível único				N	=	=	=
Identificação e autenticação		N	A	C	=	=	=
Integridade dos rótulos				N	=	=	=
Rotulação de saída legível				N	=	=	=
Rótulos				N	C	=	=
Controle de acesso obrigatório				N	C	=	=
Reutilização de objetos			N	=	=	=	=
Guia do usuário dos recursos de Segurança		N	=	=	=	=	=
Teste de segurança		N	A	N	C e A	C e A	C e A
Rótulo de Segurança nos usuários					N	=	=
Arquitetura do sistema		N	A	A	N	A	=
Integridade do sistema		N	=	=	=	=	=
Documentação para testes		N	=	=	A	=	A
Distribuição Segura							N
Recurso de Gerenciamento Confiável					N	A	=
Manual dos recursos de segurança		N	A	A	A	A	=
Rota segura					N	C	=
Recuperação segura						N	=

A - requisito adicionado na referida classe e não necessário nas classes inferiores

= - o requisito na classe em questão é igual ao exigido na classe inferior

N – Uma nova definição de requisito substitui a definição feita em uma classe inferior

C – o requisito vem de classe inferior e é modificado na classe em questão

7 - CONCLUSÃO

A implementação da INFOVIA-MT trata-se de um processo contínuo, cuja velocidade de mudanças é ditada pela demanda de número de pontos, pelo incremento de novas tecnologias e pela capacidade de investimento dos interessados. As dificuldades de gestão aparecem quando diferentes interesses às vezes conflitantes necessitem convergir ao único foro do COTEC.

As Organizações da Administração Pública devem fazer suas licitações de forma aberta a qualquer fabricante e fornecedor de soluções de TI, gerando consequentemente um parque heterogêneo de equipamentos, sistemas, aplicações e tecnologias.

O grande desafio está em administrar esses sistemas heterogêneos, assegurar sua disponibilidade e desempenho, automatizar o gerenciamento das aplicações críticas, conhecer as vulnerabilidades, eliminar brechas de segurança, documentar níveis de serviços, oferecer valores em tempo real, fazer planejamento de capacidade, racionalizar os investimentos.

A recomendação do ITU-T para gerenciamento integrado de redes e serviços oferece um modelo abrangente para prover, manter, administrar e operar os serviços do ambiente de TI.

A centralização do backbone tem como vantagem uma maior velocidade de incorporar novas tecnologias. A especificação do CORE central ATM foi a atividade mais importante na fase de projeto da rede. Considerando que o tempo que o comutador ATM precisa para levar a célula (ou quadro quebrado em células) da interface de entrada até a interface de saída está relacionado com sua capacidade de comutação e capacidade dos buffers. Buffers muito pequenos antecipam o descarte de células. Buffers muito grandes podem aumentar a latência. As taxas de descarte das células das classes ABR e UBR são em quantidade superior às células das classes CBR e VBR. O CORE ATM deve ser especificado em função das garantias básicas de desempenho, que é a utilização de buffers por VCC, deve possuir o backplane mais rápido do que a sua capacidade máxima das entradas, deve permitir implementar política de descarte que garanta a prioridade das células mais sensíveis ao retardo.

Os dois principais elementos do Acordo de Nível de Serviços de maior interesse para o usuário são a disponibilidade e o desempenho.

Todos os recursos de infra-estrutura que de alguma forma forneçam elementos para garantir a disponibilidade e desempenho, deverão ser administrados de forma a atingir o valor máximo do indicador de seu Acordo de Nível de Serviço – SLA.

As redes IP já são e deverão continuar sendo uma plataforma cada vez mais importante para as aplicações. Neste contexto, a garantia da qualidade de serviço em redes IP é um aspecto fundamental de sua operação. A garantia de QoS em redes IP envolve vários níveis de atuação em diversos tipos de equipamentos e tecnologias. A gerência da qualidade de serviço exige principalmente um entendimento claro dos componentes e parâmetros envolvidos e uma metodologia clara de implantação de protocolos, algoritmos e mecanismos que garanta a QoS.

Os componentes principais de QoS das redes IP sinalizam a importância da padronização dos protocolos, algoritmos e mecanismos de QoS visando à garantia da interoperabilidade das soluções de mercado entre fornecedores.

Considerando, por exemplo, uma rede IP usando tecnologia Ethernet, que está sendo parcialmente atualizada para ATM, afim de que sejam resolvidos alguns problemas de desempenho, recomenda-se que os servidores de arquivos e de aplicações devem ser mudados para ATM, junto com o backbone da rede. A maioria dos usuários finais deverá permanecer em segmentos Ethernet. Para que isto seja possível, conversores ATM-para-Ethernet são necessários em vários pontos da rede. Roteadores com uma interface ATM certamente poderão prover a conversão, mas switches de LAN Ethernet também podem fazer o trabalho. (Anexo-02).

A diferença é que os switches de LAN hoje são, em geral, uma fração do custo dos roteadores. Baseado em um cálculo simples, há a probabilidade de se ter poucos roteadores e um grande número de switches na rede. Os switches LAN geralmente não roteiam ou executam IP over ATM. Por outro lado, executam o serviço LAN Emulation. A rede ATM deve então ser mista, com o adaptador ATM no servidor de arquivos executando ambos IP/ATM para backups servidor-para-servidor e LAN Emulation para comunicação cliente-servidor através dos switches LAN. No projeto INFOVIA-MT verificou-se uma grande vantagem em implementar os sistemas de Firewall com adaptadores ATM em seus servidores.

No que diz respeito às versões do serviço LANE, pode-se afirmar que não faz sentido atualizar os clientes LANE 1.0 para LANE 2.0. O debate em questão é sobre a

mudança no esquema de encapsulamento usado pelas versões. Enquanto a versão LANE 1.0 usa encapsulamento LANE, a versão LANE 2.0 utilizará o protocolo LLC-SNAP (Logical Link Control-Subnetwork Address Protocol). Este último formato permite aos dispositivos efetuar tráfego de canais virtuais (VC) separados sobre um único canal virtual. Contudo, este tipo de escalabilidade chamado de multiplexação VC também requer capacidades da camada 3, o que o serviço LANE, como protocolo da camada MAC, não suporta.

O Fórum ATM mesmo reconhecendo as limitações do padrão LANE no que se refere a escalabilidade e controle de broadcast, decidiu padronizá-lo como um primeiro passo para trazer os benefícios do ATM as LANs tradicionais. Uma segunda iniciativa tem sido a de criar protocolos de roteamento que transmitam os protocolos tradicionais sobre ATM na camada 3 e tragam o controle e a segurança necessária. Os dois protocolos de roteamento propostos pelo Fórum ATM são o MPOA e o I-PNNI. Ambos visam definir como os equipamentos conversores LAN/ATM (edge devices) da rede ATM se comunicam com outras topologias de rede.

Enquanto o serviço LANE requer a existência de roteadores entre as subredes ou LANs emuladas, o MPOA permite às estações em diferentes subredes se conectarem diretamente sobre ATM, possibilitando que roteadores tradicionais continuem se comunicando com os dispositivos conectados através dos protocolos já existentes tais como o RIP (Routing Information Device) e OSPF (Open Shortest Path First).

Por outro lado, com o I-PNNI, edge devices executam protocolos de roteamento e fazem seus próprios cálculos de rota. Eles usam PNNI para que uma topologia se comunique com outra. Com PNNI, os edge devices têm uma visão unificada da rede que inclui as informações tradicionais e as da rede ATM. (Anexo-03).

Uma desvantagem do MPOA é que ele requer o desenvolvimento de protocolos novos para comunicar informações, enquanto que o PNNI já os contém. Por exemplo, muitos edge devices terão múltiplos enlaces físicos ATM, o que significa que mais de um endereço ATM pode prover uma rota aceitável. Entretanto, uma rota para um dispositivo ATM pode ter melhores opções de QoS em seu caminho, mas o protocolo NHRP - usado para resolver o endereço ATM - não terá como avaliar isto porque não suporta QoS.

Um argumento desfavorável é que ao rodar PNNI no edge device, transforma-se as funções de um switch nas funções de um roteador. Além disso, com a funcionalidade de um roteador será difícil para o edge device com I-PNNI suportar redes locais Virtuais (VLANs), porque os roteadores lidam com cada porta como se fosse sua própria subrede, enquanto que os switches permitem a múltiplas portas estarem na mesma VLAN.

As diferenças técnicas entre MPOA e I-PNNI são pequenas. A única escolha significativa de protocolo que difere é o protocolo utilizado para comunicação entre os edge devices. Se a intenção é integrar ATM a redes já existentes, o I-PNNI oferecerá melhor determinação de rota porque vê ambas as informações ATM e as já existentes. Mas se a utilização do ATM é principalmente em workgroup e deseja-se manter o backbone existente, MPOA é mais fácil de se implementar.

Uma das tecnologias tolerante a falhas utiliza o protocolo VRRP(Virtual Router Redundancy Protocol) que dinamicamente nomeia responsabilidade para um roteador virtual em uma rede conforme a RFC2338. Quando o roteador Máster falha, o conjunto de roteadores virtuais estão disponíveis para assumir a responsabilidade de encaminhamento dos pacotes de forma dinâmica. Na implementação da INFOVIA-MT os quatro roteadores apresentados no Anexo-03 (NSX9500 e ESR5000) estão configurados para suportar qualquer falha de roteamento do backbone central através da tecnologia VRRP.

Dentre os padrões e modelos expostos acima, a escolha de qual utilizar e como, dependerão do projeto, objetivos da rede, suporte que o fabricante ofereça e as vantagens do ATM.

Para suportar aplicações multimídia, as redes devem oferecer capacidades de QoS, ou seja, devem garantir o atendimento a critérios de performance previamente estabelecidos. As implementações com base em diferenciamento dos serviços onde seus pacotes IP correspondentes ao fluxo de melhor esforço tiverem seu campo TOS setado para o valor 0 ou 1 dependendo da prioridade que se deseja atribuir ao fluxo de sua respectiva conexão ATM.

Para o tráfego multimídia, são importantes os controles dos parâmetros da Largura de banda e do atraso. Vídeos coloridos com configuração de tela cheia e *full motion* demandam no mínimo 384 Kbps. Com 128 Kbps é possível realizar uma sessão de

videoconferência com taxa de 15 quadros por segundo, e qualidade de áudio semelhante à de uma conversação telefônica. Em teoria, é possível realizar sessões de videoconferência a partir de 64 Kbps, mas na prática a qualidade de áudio e vídeo fica bastante comprometida. Para a obtenção de taxas menores é necessário diminuir o tamanho da janela (técnica de compressão por manipulação de captura). O atraso: é a soma da latência (o atraso de transmissão inserido pela rede) e do atraso do CODEC (codificação e compactação). O atraso prejudica a interatividade, e será sentido em maior ou menor grau dependendo da utilização do usuário. Idealmente, deve ser o menor possível. Quanto menor o esforço de compactação, menor o atraso de CODEC. Pequenos atrasos até podem ser tolerados, mas o tráfego multimídia não tolera a variação do atraso – também conhecido como *jitter*. As conseqüências do *jitter* são a perda de sincronia e falhas ("buracos") na transmissão. A eliminação do *jitter* é obtida com a priorização do tráfego, uso de buffers e técnica de *time-stamping*. *P*equenas perdas de informação são toleradas por aplicações multimídia, pois não comprometem o entendimento do usuário. Entretanto, após ultrapassar um limite máximo aceitável, pode introduzir os mesmos efeitos do *jitter* (falhas na comunicação). Em ambiente WAN, pode-se adotar como referência as taxas máximas de perdas de pacotes obtidas com o uso de enlaces Frame Relay.

Considerando que a informação é o principal patrimônio de uma organização com a missão de prover TI como instrumento de seu negócio, recomenda-se que todos os produtos sejam fornecidos mediante um Acordo de Nível de Serviços – SLA com base em termos de responsabilidade de cada um no que se refere a segurança da informação, a disponibilidade e performance do Ambiente de TI. Os resultados positivos serão obtidos em conseqüência da exigência de itens de controle que devem ser acompanhados sistematicamente.

A tecnologia ATM implementada na INFOVIA-MT permitiu resultados significativos de redução dos riscos de falta de disponibilidade em roteamento para o CORE central da INFOVIA-MT através da implementação do VRRP e aumento significativo da escalabilidade da rede através do PNNI.

As medições feitas em redes de topologias com roteadores convencionais de borda, que foram migradas para topologia contendo um CORE ATM central e Up-Links ATM nos edge-devices, indicaram uma redução significativa de sua latência.

A escolha da topologia centralizada para a INFOVIA-MT permitiu a possibilidade de implementação de uma política de segurança comum para todos os sites interligados através de um sistema de Firewall centralizado interligado aos sistemas modulres de firewall dos sites, onde cada site descentralizado pode implementar sua própria política de segurança associada a seu próprio proxy.

SUGESTÕES PARA TRABALHOS FUTUROS

- A rede das Organizações contendo seu CORE ATM devem se conectar as redes de outras organizações através do LAN EMULATION ou NNI-NNI. Sugerem-se estudos de desempenho entre LECs, LEC e BUS, LEC e LES para esses casos.

- A gerência de redes é um dos pontos de vulnerabilidades no que concerne à segurança. Sugere-se análise dos aspectos da segurança em ambientes heterogêneos com administração descentralizada.

- Sugere-se o desenvolvimento de aplicativos de análise dos Bancos de Dados utilizando-se a tecnologia de Data Warehouse e Data Mining onde estão armazenados os Logs de Alarmes, posteriormente utilizar as técnicas de Inteligência Computacional e Redes Neurais para extrair um histórico do comportamento dos índices de controle dos SLAs gerenciados, aplicando-se os critérios do PDCA.

REFERÊNCIAS BIBLIOGRÁFICAS

[ABD96] Michel F. Abdalla, "Análise de Mecanismos de Controle de Admissão de Conexão para Redes ATM", Tese de Mestrado,
Universidade Federal do Rio de Janeiro, PEE/COPPE/UFRJ, Rio de Janeiro, setembro de 1996.

[AMR98] Marcelo D. Amorim, "XGOP-B : Um modelo extendido com previsão de ponto de quebra para tráfegos de vídeo MPEG",
XVI SBRC'98, junho de 1998.

[ATF0396] - ATM Forum Techinical Comittee. "af-pnni-0055.000: Private Network-Network Interface Specification version 1.0. Março de 1996.

[ATF0996] - ATM Forum Techinical Comittee. "af-pnni-0066.000: Private Network-Network Interface Specification version 1.0.Addendum. Setembro de 1996.

[ATF97] - ATM Forum Techinical Comittee. "Integrated PNNI (I-PNNI) v1.0 Specification, 1997.

[ATFC97] - ATM Forum Techinical Comittee. "Integrated PNNI (I-PNNI) Requirements, 1997.

[AWP] - Anixter White Paper. "LANE Update", Anixter

[AWP] - Anixter White Paper. "Enterprise Networks - MPOA Model ", Anixter

[BAN96] - Baynetwork News. "I-PNNI Accepted as Work Effort By The Forum ATM", Bay Networks 1996.

[BAN97] - Baynetwork News. "Switched Internetwork Architectures" (atualizado em 1997).

[BGR97] - B. Guttman and R. Bagwill. Internet Security Policy: A Technical Guide.

[CAJ97] - Canover, Joel. "Confused about I-PNNI ?", Network Computing. November 1996.

[CAS97] - Cabletron. "Travelling in the SmartLane". Cabletron Systems. Abril de 1997.

[CHL97] - CHENG, L. Quality of service based on both call admission and cell scheduling. Computer Networks and ISDN Systems 29(5), 555-567, abr.1997.

[CHY93] - CHANG, Y.; SU D.e WAKID, S. The Generic Flow Control (GFC) Protocol: A Performance Assessment. Proceedings of International Conference on Network Protocols (ICNP93), October, 19-22, 1993, também disponível em; www:/isdn.ucsl.nist.gov/misc/hsnt/journals/gfcpaper.html.

[CJA89] - COOPER, J.A., Computer and Communications Security, McGraw-Hill, 1989.

[COM95] - Douglas E. Comer, "Internetworking with TCP/IP - Principles, Protocols and Architecture ", Vol. 1, Prentice-Hall, 1995.

[CRF] - Cell Relay FAQ - ATM Technology Questions.

[CVF92] - Campos, Vicente Falconi, TQC - Controle da Qualidade Total (no estilo japonês), Rio de Janeiro, Bloch, 1992.

[DAN98] - Daniel Minoli and Emma Minoli, "*Delivering Voice over Frame Relay and ATM*", Wiley Computer Publishing, 1998.

[DAV96] - David Ginsburg, "*ATM Solutions for Enterprise Internetworking*", Addison-Wesley, 1996.

[DJE95] - De Lucca, J.E., Arquitetura de Segurança pra Redes Aplicada a Sistemas de Gerência, Dissertação de Mestrado, CPGCC – UFSC, 1995.

[DOC01] - DOUGLAS E. COMER – Interligação em rede com TCP/IP - CAMPUS.

[DOG96] - Dobrowski, George. "Standards Progress Steadies Advances", Lan Times. Setembro de 1996.

[FRA01] - Freire, A, Track II – Firewall and Perimeter Protection Pratical Assignment, SAN S GIAC - February 2001.

[FVS94] - FROST, V. S. e MELAMED, B. Traffic Modeling for Telecommunications Networks. IEEE Communication Magazine, Mar. 1994, p.70-81.

[GJM91] - GALVIN, J.M. & McCLOGHRIE, K.& DAVIN, J.R., Secure Management of SNMP Networks, Proccedings of Integrated Network Management II, 1991.

[IIE94] - IETF Internet Engineering Task Force,RFC 1577. "Classical IP and ARP over ATM", Network Working Group. Janeiro de 1994.

[IET93] - IETF Internet Engineering Task Force,RFC 1483. "Multiprotocol Encapsulation over ATM Adaptation Layer 5", Network Working Group. Julho de 1993.

[JAM98] - James D. McCabe, *Practical Computer Network Analysis and Design*, Morgan Kaufmann Series in Networking, 1998.

[JOB99] - Joberto Martins, "Redes Corporativas MultiServiço - Caracterização das Aplicações e Parâmetros Básicos de Operação", Em http://www.jsmnet.com/slides/AnaliseRequisitos/index.htm

[JSMNet] - "JSMNet - Estado da Arte e P&D em Redes de Computadores". Em http://www.jsmnet.com

[KLE75] L.Kleinrock, "Queueing Systems, Vol.1 : Theory", Wiley Interscience, pp.10-52, 1975.

[MAG95] - Marshall, George. "Classical IP over ATM: A Status Report", Data Communications. Dezembro de 1995.

[MAT97] - Mathias Hein and David Griffiths, "*Switching Technology in the Local Network - From LAN to Switched LAN to Virtual LAN*", Thomson Computer Press, 1997.

[MAU97] - Thomas A. Maufer, "*Deploying IP Multicast in the Enterprise*", Prentice-Hall, 1997.

[MEL94] V.S.Frost e B.Melamed, "Traffic Modeling for Telecommunications Networks", IEEE Communications, pp.70-81, março de 1994.

[MEL96] B.Melamed, "Stochastic Modeling of Traffic Processes", Capítulo incluído no livro "Frontiers in Queueing : Models, Methods and Problems (J.H.Dshabalow, Ed.) CRC Press, 1996", 1996.

[MMRM96] - McLean, Michelle Rae. "Protocol Hype Continues", Lan Times. Março de 1996'.

[MMRA96] - McLean, Michelle Rae. "ATM Progress: Slow but Steady", Lan Times. Abril de 1996.

[MMRN96] - McLean, Michelle Rae. "ATM LANE 2.0 Skips Promised Scaleability", Lan Times. Novembro de 1996.

[Mpls_Charter] - IETF "*Multiprotocol Label Switching*" Working Group. Em http://www.ietf.org/html.charters/mpls-charter.html e http://www.ietf.org/ids.by.wg/mpls.html

[PIC99] – Projeto INFOVIA-MT – Cepromat – 1999.

[REB99] - Russ Eberchart, Pat Simpson, Roy Dobbins, Computational Intelligence PC Tools, Ap Professional, 1999.

[REB01] - Russ Eberhart, Computational Inteligence PC Tools, AP Professional.

[RFC_2205] - R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin, "*Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*", RFC 2205, September 1997

[RFC_2474] - K. Nichols, S. Blake, F. Baker, D. Black, "*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*", RFC 2474, 1998.

[RFC_2475] - S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, "*An Architecture for Differentiated Services* ", RFC 2475, December 1998

[RFC_2597] - J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, "*Assured Forwarding PHB Group*",RFC 2597, June 1999

[RFC_2598] - V. Jacobson, K. Nichols, K. Poduri, "*An Expedited Forwarding PHB*", RFC 2598, June 1999

[RFC_2211] - J. Wroclawski, "*Specification of the Controlled-Load Network Element Service*", RFC 2211, September 1997

[RFC_2212] - S. Shenker, C. Partridge, R. Guerin, "*Specification of Guaranteed Quality of Service* ", RFC 2212, Sept 1997

[RFC_2215] - S. Shenker, J. Wroclawski, "*General Characterization Parameters for Integrated Service Network Elements* ", RFC 2215, September 1997

[RFC_2216] - S. Shenker, J. Wroclawski, "*Network Element Service Specification Template*", RFC 2216, Sept 1997.

[RJC00] - Ribas, J.C., Acordo de Nível de Serviços, Trabalho Final, CPGCC – UFSC, 2000.

[SBM_Draft] - R. Yavatkar, D. Hoffman, Y. Bernet, F. Baker, "*SBM (Subnet Bandwidth Manager): A Protocol for RSVP-based Admission Control over IEEE 802-style networks*", May 1999,
<draft-ietf-issll-is802-sbm-08.txt>, Work in Progress.

[STE94] - W. Richard Stevens, "*TCP/IP Illustrated - The Protocols*", Vol. 1, Addison-Wesley, 1994.

[STW00] - Stallings, William. Ipv6: The New Internet Protocol (http://www.ieee.org/comsoc/stallings.html).

[SWG97] - Swallon, George. "MPOA, VLAN's and Distributed Routers", Cisco Systems. Março de 1997.

[TAN81] - TANENBAUM, A. [1981] – Computers Networks.

[TAN96] - Andrew Tanembaum, "*Computer Networks*", 3rd edition, Prentice-Hall, 1996.

[THO96] - Stephen A. Thomas, "*IPng and the TCP/IP Protocols - Implementing the Next Generation Internet* ", Wiley Computer Publishing, 1996.

[VER90] D.Ferrari e D.Verma, "A scheme for real-time channel establishment in wide-area networks", IEEE Journal on Selected
Areas of Communications, pp.369-379, abril de 1990.

[WMC99] - Werkma, M. C. – A ferramenta da Qualidade no Gerenciamento de Processos – Editora FDG - 1999.

[WPN97] - Newbridge."MPOA - Multiprotocol over ATM", White Paper Newbridge - Vivid. 1997.

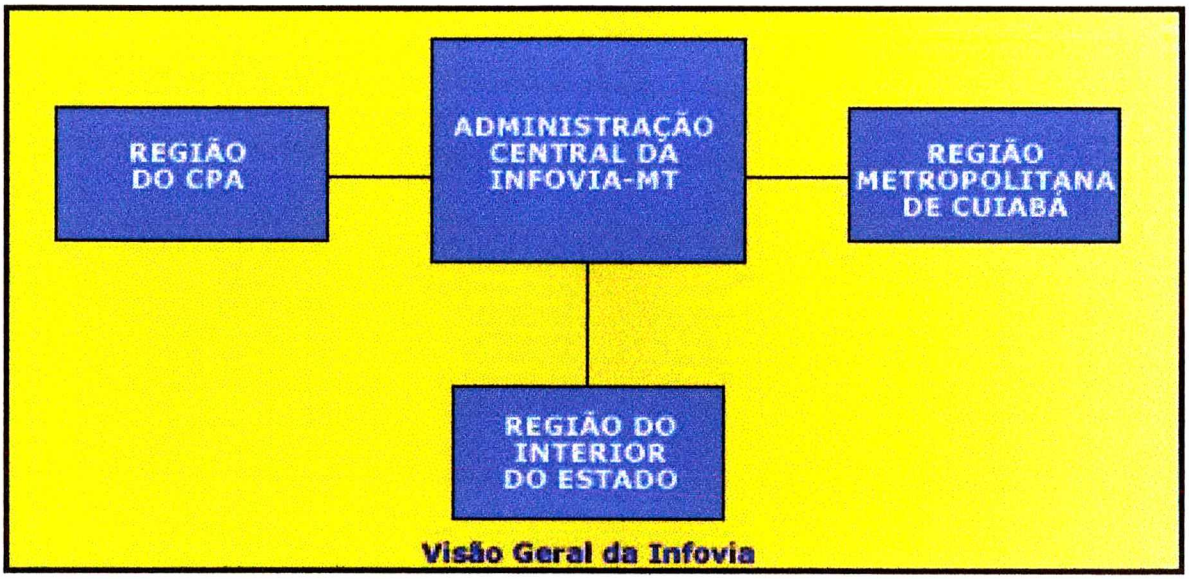
[WU98] - Chwan-Hwa Wu and J. David Irwin, "*Emerging Multimedia Computer Communication Technologies* ", Prentice-Hall, 1998.

[YIM96] - Yip Michael, "ATM in the MIX", LAN Magazine. 1996.

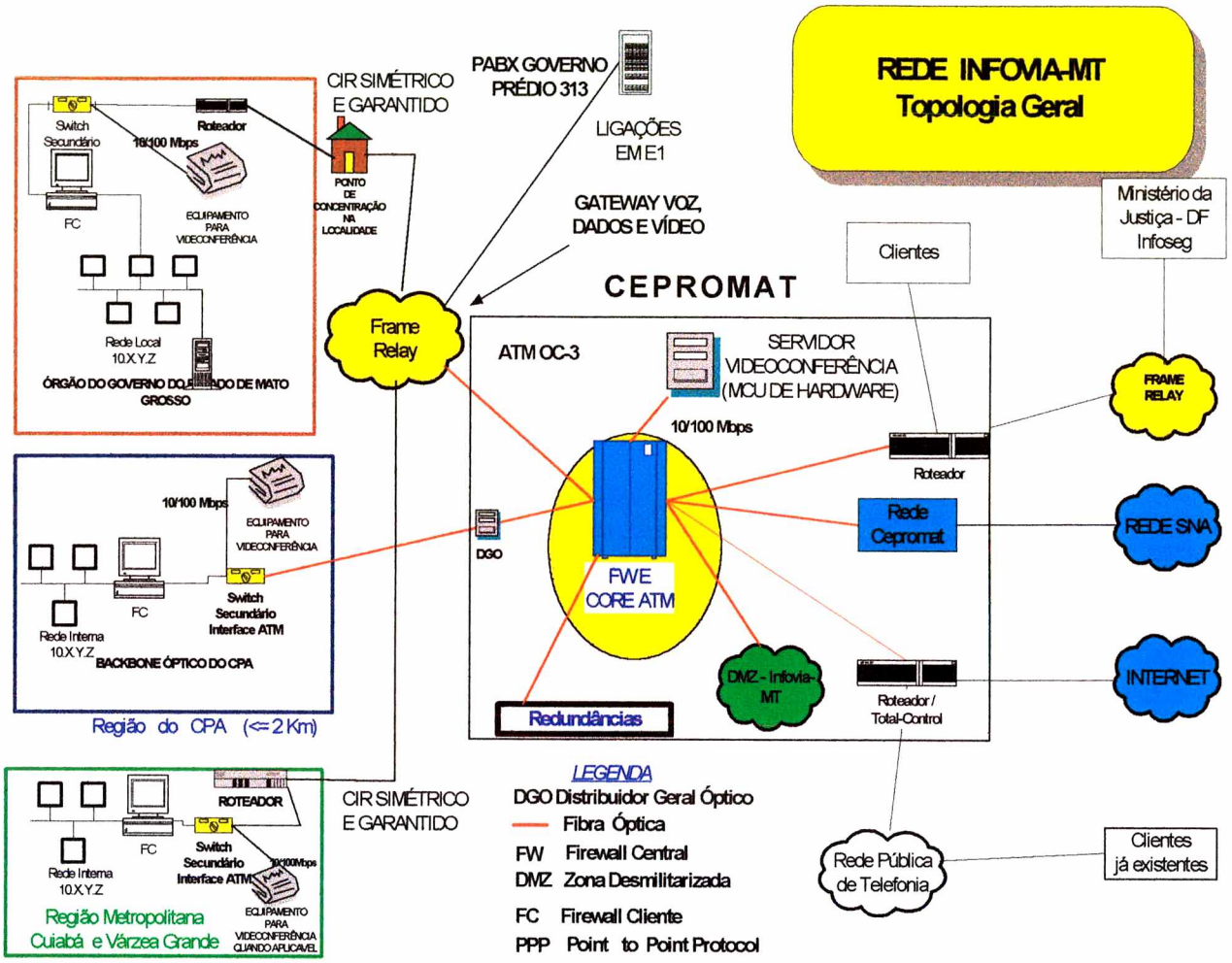
[ZEI96] - Zeitnet. "ATM LAN Emulation in Workgroups Networks", White Paper Zeitnet/Cabetron Outubro de 1996.

ANEXOS

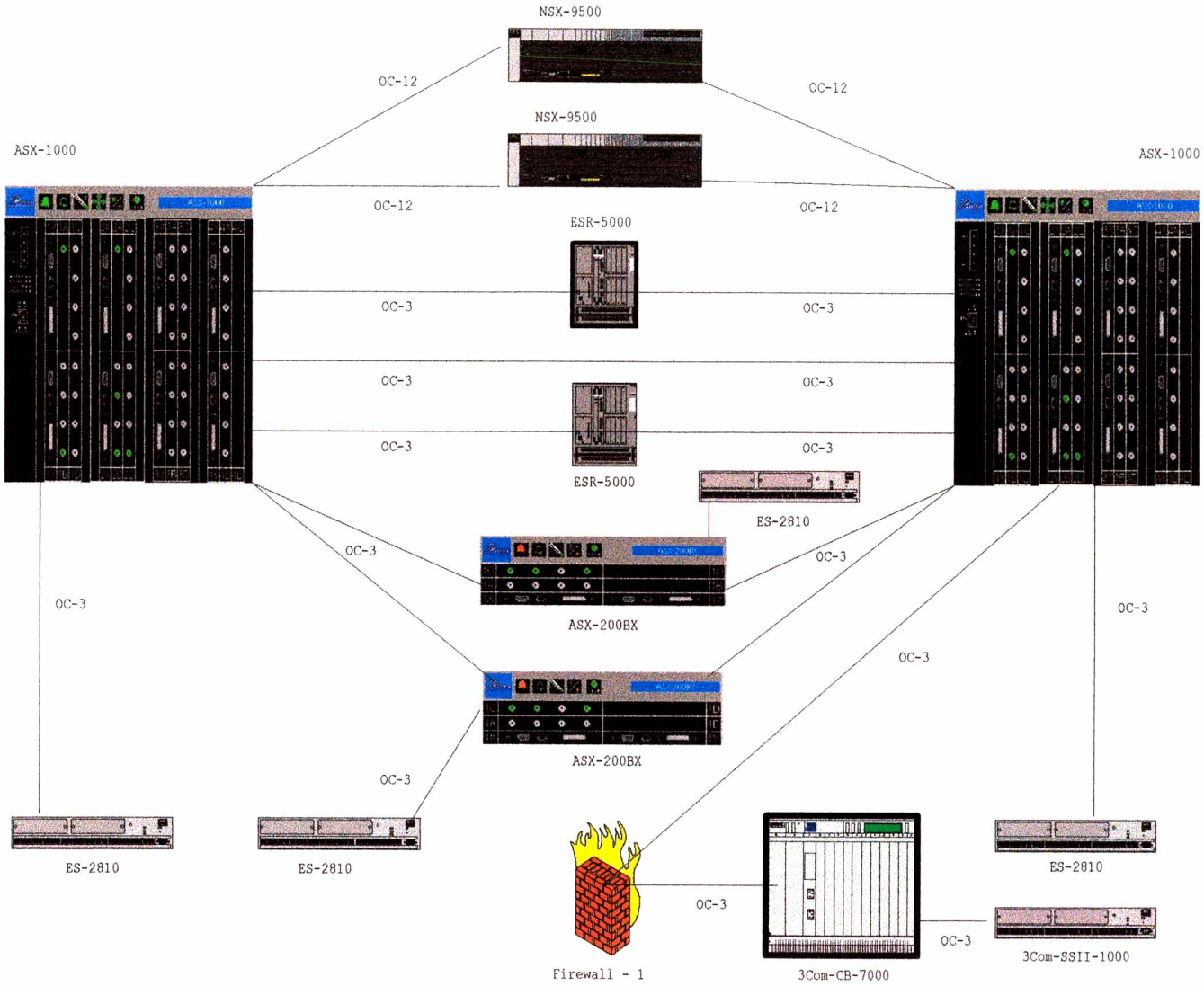
Anexo-01 - Divisão das malhas da rede corporativa.



Anexo-02 - Topologia geral da rede INFOVIA-MT



Anexo-03 - CORE ATM da INFOVIA-MT



INFOVIA-MT - Equipamentos CORE ATM
Marconi & 3Com

Anexo-04 - Regras de um Firewall em LINUX utilizando IPchains

```
##############
# Firewall FW1 #
##############

echo "iniciando FW1"
echo "iniciando regras..."

# Deleta todos os filtros criados por usuarios
ipchains -X

# Zera todas as regras dos filtros input,output,forward
ipchains -F input
ipchains -F output
ipchains -F forward

# Politica de negacao; se o pacote nao se enquadra com as regras abaixo: nega
ipchains -P input DENY
ipchains -P output DENY
ipchains -P forward DENY

# filtro de entrada: input
# filtro de saida: output
# filtro de avanco entre redes: forward

# Ativando proteção contra spoof

if [ -e /proc/sys/net/ipv4/conf/all/rp_filter ]; then
        echo –n "seting up IP spoofing protection..."
        for f in /proc/sys/net/ipv4/conf/*/rp_filter; do
                echo 1 > $f
        done
        echo "done."
else
        echo "Problemas Setting up IP SPOOFING PROTECTION BE WORRIED."
        echo "CONTROL –D will exit from this shell and continue system startup. "
        echo
        /sbin/sulogin $CONSOLE
fi

# Impede Ping
ipchains –A input -p icmp -j DENY –s 0 .0 .0 .0 / 0

# Impede Trinoo
ipchains –A input -p tcp -j DENY –s 0 .0 .0 .0 / 0 27665
ipchains –A input -p udp -j DENY –s 0 .0 .0 .0 / 0 27444
ipchains –A input -p udp -j DENY –s 0 .0 .0 .0 / 0 31335
```

```
# Impede Backdoors
ipchains –A input -p tcp -j DENY –s 0 .0 .0 .0 / 0 666
ipchains –A input -p udp -j DENY –s 0 .0 .0 .0 / 0 666

# Inpede BackOriffice e Netbus
ipchains –A input -p udp -j DENY –s 0 .0 .0 .0 / 0 31337
ipchains –A input -p tcp -j DENY –s 0 .0 .0 .0 / 0 1234
ipchains –A input -p tcp -j DENY –s 0 .0 .0 .0 / 0 12345
ipchains –A input -p tcp -j DENY –s 0 .0 .0 .0 / 0 12346
ipchains –A input -p udp -j DENY –s 0 .0 .0 .0 / 0 2049
ipchains –A input -p tcp -j DENY –s 0 .0 .0 .0 / 0 20034
ipchains –A input -p tcp -j DENY –s 0 .0 .0 .0 / 0 54321

# Bloqueia IRC ( 6667 9000 6666 666 )
ipchains –A input -p tcp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6667
ipchains –A input -p udp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6667
ipchains –A input -p tcp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 9000
ipchains –A input -p udp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 9000
ipchains –A input -p tcp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 666
ipchains –A input -p udp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 666
ipchains –A input -p tcp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6666
ipchains –A input -p udp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6666

# Bloqueia ICQ (padrao)
ipchains –A input -p tcp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 4000
ipchains –A input -p udp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 4000

# Bloqueia Napster
ipchains –A input -p tcp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6702
ipchains –A input -p udp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6702
ipchains –A input -p tcp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6703
ipchains –A input -p udp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6703
ipchains –A input -p tcp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6704
ipchains –A input -p udp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6704
ipchains –A input -p tcp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6705
ipchains –A input -p udp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 6705
ipchains –A input -p tcp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 7777
ipchains –A input -p udp -j DENY –s 1.1.1.0 –d 0. 0. 0. 0 / 0 7777

# Aceita os pacotes de 1.1.2.0/24 (subrede local) com destino a internet
ipchains -A input -i eth1 -s 1.1.2.0/24 -d 0/0 -j ACCEPT

# Aceita os pacotes da internet com destino a 1.1.2.0/24 (subrede local)
ipchains -A output -i eth1 -s 0/0 -d 1.1.2.0/24 -j ACCEPT

# Aceita os pacotes entrando de (subrede local) com destino a internet
ipchains -A input -i eth1 -s 1.1.2.0/24 -d 1.1.1.0/24 -j ACCEPT
```

```
# Aceita os pacotes saindo da internet com destino a  (élan protegida)
ipchains -A output -i eth1 -s 1.1.1.0/24 -d 1.1.2.0/24 -j ACCEPT

# Aceita os pacotes entrando de 1.1.5.0/24 com destino a internet
ipchains -A input -i eth2 -s 1.1.5.0/24 -d 0/0 -j ACCEPT

# Aceita os pacotes entrando de 1.1.5.0/24 com destino a (élan protegida)
ipchains -A input -i eth2 -s 1.1.5.0/24 -d 1.1.2.0/24 -j ACCEPT

# Aceita os pacotes  de 1.1.2.0/24 com destino a 1.1.5.0/24
ipchains -A output -i eth2 -s 1.1.2.0/24 -d 1.1.5.0/24 -j ACCEPT

# Aceita os pacotes de 200.241.69.11/32 com destino a internet
ipchains -A output -i eth0 -s 200.241.69.11/32 -d 0/0 -j ACCEPT

# Aceita os pacotes da internet com destino a 200.241.69.11/32
ipchains -A input -i eth0 -s 0/0 -d 200.241.69.11/32 -j ACCEPT

# Mascara os pacotes da rede 1.1.2.x/24 para a 200.241.69.0/24 - endereco da eth1
ipchains -A forward -s 1.1.2.0/24 -d 200.241.69.0/24 -j MASQ -i eth1

# Mascara os pacotes da rede 1.1.2.x/24 para a 200.241.69.0/24 - endereco da eth2
ipchains -A forward -s 200.241.69.0/24 -d 1.1.5.0/24 -j MASQ -i eth2

# Mascara os pacotes da rede 1.1.4.0/24 (élan protegida) para a internet
# ipchains -A forward -s 1.1.4.0/24 -d 0/0 -j MASQ -i eth0

# Mascara os pacotes da rede 1.1.5.0/24 (Core Subnet) para a internet
ipchains -A forward -s  1.1.5.0/24 -d 0/0 -j MASQ -i eth0

# FIM
echo  "Regras inicializadas ! "
echo  " Firewall  FW1 inicializado ! "
```

```
##############
# Firewall FW2 #
##############

echo "iniciando FW2"
echo "iniciando regras..."

# Deleta todos os filtros criados por usuarios
ipchains -X

# Zera todas as regras dos filtros input,output,forward
ipchains -F input
ipchains -F output
ipchains -F forward

# Politica de negacao; se o pacote nao se enquadra com as regras abaixo: nega
ipchains -P input DENY
ipchains -P output DENY
ipchains -P forward DENY

# filtro de entrada: input
# filtro de saida: output
# filtro de avanco entre redes: forward

# Ativando proteção contra spoof

if [ -e /proc/sys/net/ipv4/conf/all/rp_filter ]; then
        echo –n "seting up IP spoofing protection..."
        for f in /proc/sys/net/ipv4/conf/*/rp_filter; do
                echo 1 > $f
        done
        echo "done."
else
        echo "Problemas Setting up IP SPOOFING PROTECTION BE WORRIED."
        echo "CONTROL –D will exit from this shell and continue system startup. "
        echo
        /sbin/sulogin $CONSOLE
fi

# Impede Ping
ipchains –A input -p icmp -j DENY –s 0 .0 .0 .0 / 0

# Impede Trinoo
ipchains –A input -p tcp -j DENY –s 0 .0 .0 .0 / 0 27665
ipchains –A input -p udp -j DENY –s 0 .0 .0 .0 / 0 27444
ipchains –A input -p udp -j DENY –s 0 .0 .0 .0 / 0 31335

# Impede Backdoors
```

```
ipchains –A  input  -p tcp  -j DENY –s 0 .0 .0 .0 / 0  666
ipchains –A  input  -p udp -j DENY –s 0 .0 .0 .0 / 0  666

# Inpede BackOriffice e Netbus
ipchains  –A  input  -p udp -j DENY –s 0 .0 .0 .0 / 0  31337
ipchains  –A  input  -p tcp  -j DENY –s 0 .0 .0 .0 / 0  1234
ipchains  –A  input  -p tcp  -j DENY –s 0 .0 .0 .0 / 0  12345
ipchains  –A  input  -p tcp  -j DENY –s 0 .0 .0 .0 / 0  12346
ipchains  –A  input  -p udp -j DENY –s 0 .0 .0 .0 / 0  2049
ipchains  –A  input  -p tcp  -j DENY –s 0 .0 .0 .0 / 0  20034
ipchains  –A  input  -p tcp  -j DENY –s 0 .0 .0 .0 / 0  54321

# Bloqueia IRC  ( 6667  9000  6666  666 )
ipchains  –A  input  -p tcp  -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6667
ipchains  –A  input  -p udp -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6667
ipchains  –A  input  -p tcp  -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  9000
ipchains  –A  input  -p udp -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  9000
ipchains  –A  input  -p tcp  -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  666
ipchains  –A  input  -p udp -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  666
ipchains  –A  input  -p tcp  -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6666
ipchains  –A  input  -p udp  -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6666

# Bloqueia ICQ  (padrao)
ipchains  –A  input  -p tcp  -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  4000
ipchains  –A  input  -p udp -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  4000

# Bloqueia Napster
ipchains  –A  input  -p tcp  -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6702
ipchains  –A  input  -p udp -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6702
ipchains  –A  input  -p tcp  -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6703
ipchains  –A  input  -p udp -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6703
ipchains  –A  input  -p tcp  -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6704
ipchains  –A  input  -p udp -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6704
ipchains  –A  input  -p tcp  -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6705
ipchains  –A  input  -p udp -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  6705
ipchains  –A  input  -p tcp  -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  7777
ipchains  –A  input  -p udp -j DENY –s 1.1.3.0 –d  0. 0. 0. 0 / 0  7777

# Aceita os pacotes  de 1.1.4.0/24 (subrede local) com destino a internet
ipchains -A input -i eth1 -s 1.1.4.0/24 -d 0/0 -j ACCEPT

# Aceita os pacotes da internet com destino a 1.1.4.0/24 (subrede local)
ipchains -A output -i eth1 -s 0/0 -d 1.1.4.0/24 -j ACCEPT

# Aceita os pacotes entrando de (subrede local) com destino a internet
ipchains -A input -i eth1 -s 1.1.4.0/24 -d 1.1.5.0/24 -j ACCEPT

# Aceita os pacotes saindo da internet com destino a  (subrede local)
```

```
ipchains -A output -i eth1 -s 1.1.3.0/24 -d 1.1.4.0/24 -j ACCEPT

# Aceita os pacotes entrando de 1.1.5.0/24 com destino a internet
ipchains -A input -i eth2 -s 1.1.5.0/24 -d 0/0 -j ACCEPT

# Aceita os pacotes entrando de 1.1.5.0/24 com destino a (subrede local)
ipchains -A input -i eth2 -s 1.1.5.0/24 -d 1.1.2.0/24 -j ACCEPT

# Aceita os pacotes  de 1.1.2.0/24 com destino a 1.1.5.0/24
ipchains -A output -i eth2 -s 1.1.2.0/24 -d 1.1.5.0/24 -j ACCEPT

# Aceita os pacotes de 200.241.69.12/32 com destino a internet
ipchains -A output -i eth0 -s 200.241.69.11/32 -d 0/0 -j ACCEPT

# Aceita os pacotes da internet com destino a 200.241.69.11/32
ipchains -A input -i eth0 -s 0/0 -d 200.241.69.12/32 -j ACCEPT

# Mascara os pacotes da rede 1.1.2.x/24 para a 200.241.69.0/24 - endereco da eth1
ipchains -A forward -s 1.1.2.0/24 -d 200.241.69.0/24 -j MASQ -i eth1

# Mascara os pacotes da rede 1.1.2.x/24 para a 200.241.69.0/24 - endereco da eth2
ipchains -A forward -s 200.241.69.0/24 -d 1.1.5.0/24 -j MASQ -i eth2

# Mascara os pacotes da rede 1.1.4.0/24 (élan local) para a internet
ipchains -A forward -s 1.1.4.0/24 -d 0/0 -j MASQ -i eth0

# Mascara os pacotes da rede 1.1.5.0/24 (élan core) para a internet
ipchains -A forward -s  1.1.5.0/24 -d 0/0 -j MASQ -i eth0

# FIM
echo "Regras inicializadas ! "
echo " Firewall  FW2 inicializado ! "
```

ANEXO-05 – Regras de Implementação de um Firewall Linux utilizando o Iptables.

```
#---------- Definindo um firewall Default Deny ---------#

logger "Instalando o Firewall"

#---------- Inicialização das variáveis ----------#

EXT_IF="eth1"
LOOPBACK_IF="lo"
ANYWHERE="0/0"
IPADDR=`ifconfig $EXT_IF | grep inet | cut -d : f2 | cut –d\ -f1`
NAMESERVERS=`grep nameserver /etc/resolv.conf | cut -d\ -f2`
LOOPBACK="127.0.0.0/8"
CLASS_A="10.0.0.0/8"
CLASS_B="172.16.0.0/12"
CLASS_C="192.168.0.0/16"
CLASS_D_MULTICAST="224.0.0.0/4"
CLASS_E_RESERVED_NET="240.0.0.0/5"
BROADCAST_SRC="0.0.0.0"
BROADCAST_DEST="255.255.255.255"
PRIVPORTS="0:1023"
UNPRIVPORTS="1024:65535"
SSH_PORTS="1020:1023"
TRACEROUTE_SRC_PORTS="32769:65535"
TRACEROUTE_DEST_PORTS="33434:33523"
XWINDOW_PORTS="6000:6063"
SOCKS_PORT="1080" # (TCP) socks
OPENWINDOWS_PORT="2000" # (TCP) openwindows
NSF_PORT="2049" # (TCP/UDP) NSF

#---------- Definição dos Módulos----------#

modprobe ip_conntrack
modprobe ip_conntrack_ftp
modprobe ip_tables
modprobe ipt_state
modprobe ipt_unclean
modprobe ipt_limit
modprobe ipt_LOG
modprobe ipt_REJECT

#---------- lógica das políticas ----------#

echo 1 > /proc/sys/net/ipv4/tcp_syncoockies
echo 1 > /proc/sys/net/ipv4/ip_always_defrag
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
```

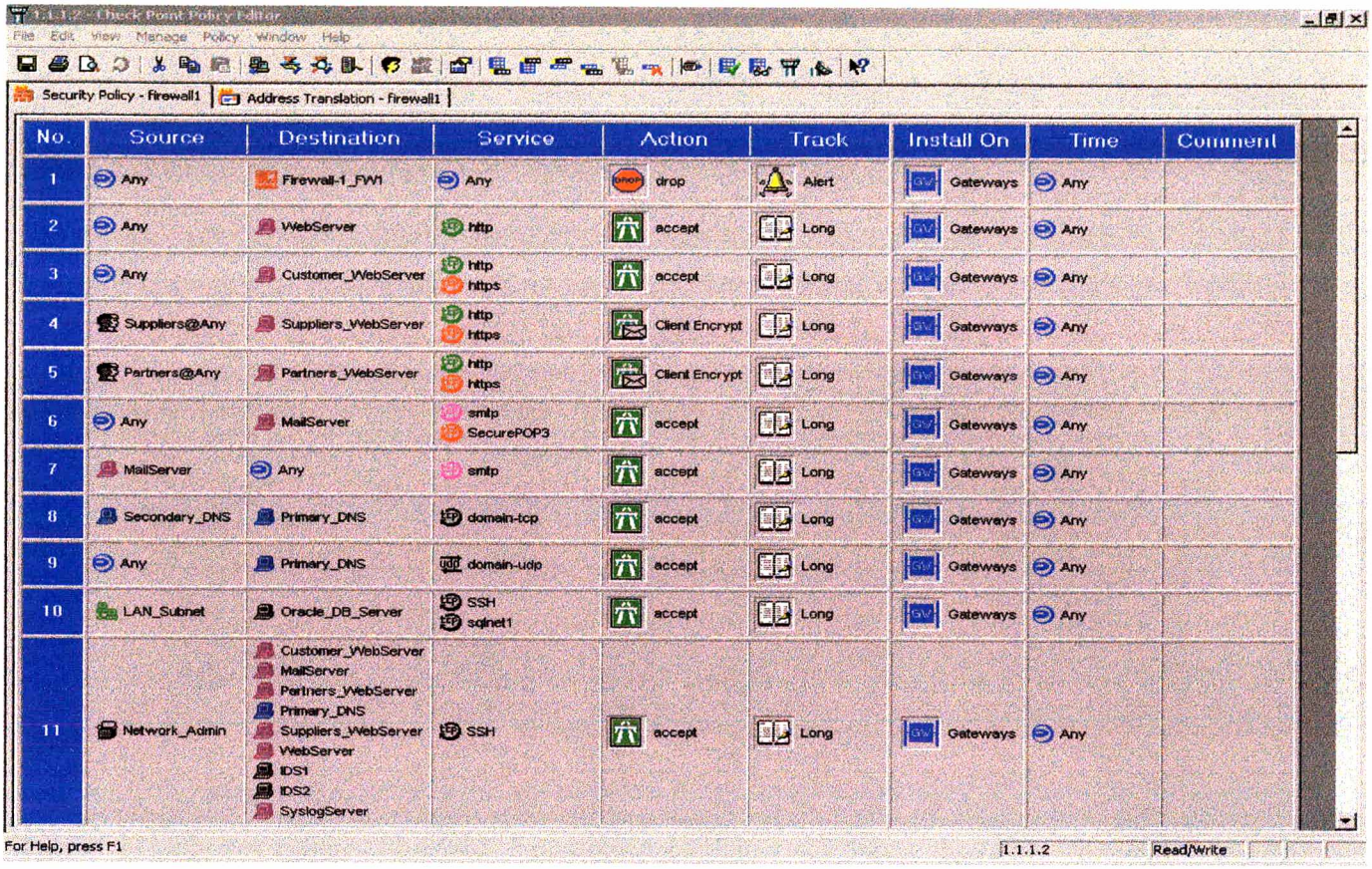
```
echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
for f in /proc/sys/net/ipv4/conf/*/rp_filter;do
echo 1 > $f
done
for f  in /proc/sys/net/ipv4/conf/*/accept_redirects; do
echo 0 > $f
done
for f in /proc/sys/net/ipv4/conf/*/send_redirects; do
echo 0 > $f
done
for f in /proc/sys/net/ipv4/conf/*/accept_source_route; do
echo 0 > $f
done
for f in /proc/sys/net/ipv4/conf/*/log_martians; do
echo 0 > $f
done

#---------- Limpa e Apaga Chains--------#

Iptables –F
Iptables –X
Iptables –P INPUT DROP
Iptables –P OUTPUT DROP
Iptables –P FORWARD DROP

#---------- Chains do Usuário ----------#

Iptables –N log_drop
Iptables –A log_drop -j LOG  --log-level 1 -- log-prefix
DROPPED::
Iptables –A log_drop -j DROP
Iptables –N log_accept
Iptables –A log_accept  -m limit  -j LOG --log-level 1 --log-prefix
ACCEPTED::
Iptables –A log_accept -j ACCEPT
Iptables –N log_reject
Iptables –A log_reject -j LOG --log-level 1 --log-prefix
REJECTED::
Iptables –A log_reject -j REJECT
Iptables –N log_unclean
Iptables –A log_unclean -j LOG --log-level 1 --log-prefix
Unclean::
Iptables –A log_unclean –j DROP
Iptables –N log_fragment
Iptables –A log_fragment –j LOG –log-level 1 –log-prefix
Fragment::
Iptables –A log_fragment –j DROP
Iptables –N log_spoofed
```

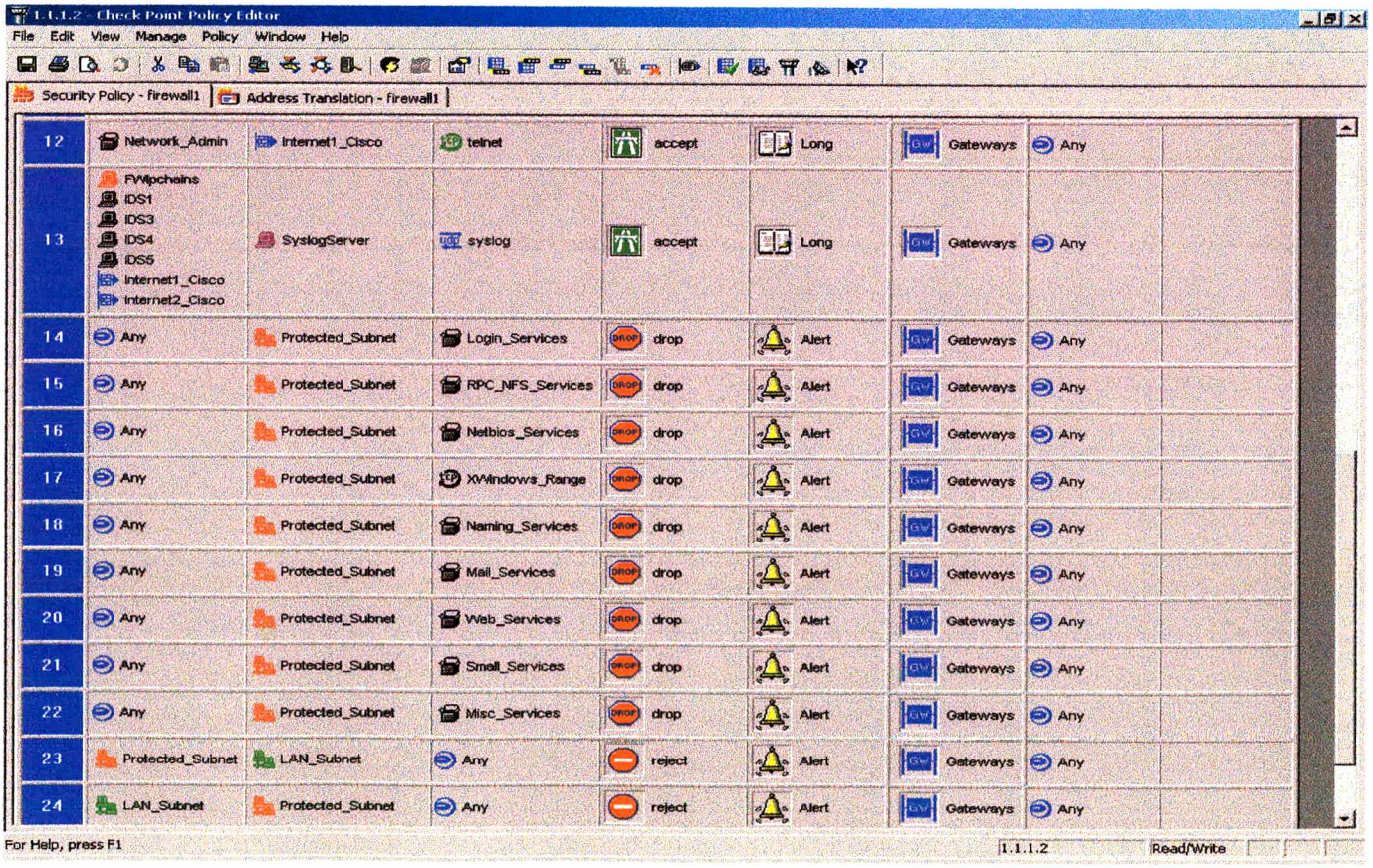
```
Iptables –A log_spoofed –j LOG –log-level 1 –log-prefix
Spoofed::
Iptables –A log_spoofed –j DROP
Iptables –N log_priv
Iptables –A log_priv –j LOG –log-level 1 –log-prefix
Privport::
Iptables –A log_priv –j DROP
Iptables –N log_ass_unpriv
Iptables –A log_ass_unpriv –j LOG –log level 1 –log prefix
Ass_unprivport::
Iptables –A log_ass_unpriv –j DROP
Iptables –N log_traceroute
Iptables –A log_traceroute –j LOG –log-level 1 –log-prefix
Traceroute::
Iptables –A log_traceroute –j DROP
Iptables –N log_in_new
Iptables –A log_in_new –j LOG –log-level 1 –log-prefix
Incoming_new::
Iptables –A log_in_new –j DROP
Iptables –N log_in_invalid
Iptables –A log_in_invalid –j LOG –log-level 1 –log-prefix
Incoming_invalid::
Iptables –A log_in_invalid –j DROP

#----------Loopback----------#

iptables –A INPUT –j SLOOPBACK_IF –j ACCEPT
iptables –A OUTPUT –o SLOOPBACK_IF –j ACCEPT

#----------Pacotes Suspeitos e fragmentos ---------#

iptbles –A INPUT –j $EXT_IF –m uncleam –j log_unclean
iptables –A INPUT –f -j $EXT_IF –j log_fragment

#----------LOG de spoofing ----------#

iptables –A INPUT –i $EXT_IF –s SIPADDR –j log_spoofed
iptables –A INPUT –i $EXT_IF –s SCLASS_A –j log_spoofed
iptables –A INPUT –i $EXT_IF –s SCLASS_B –j log_spoofed
iptables –A INPUT –i $EXT_IF –s SCLASS_C –j log_spoofed
iptables –A INPUT –i $EXT_IF –s SLOOPBACK –j log_spoofed
iptables –A INPUT –i $EXT_IF –s SBROADCAST_DEST –j log_spoofed
iptables –A INPUT –i $EXT_IF –s SCLASS_D_MULTCAST –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 0.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 1.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 2.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 5.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 7.0.0.0/8 –j log_spoofed
```

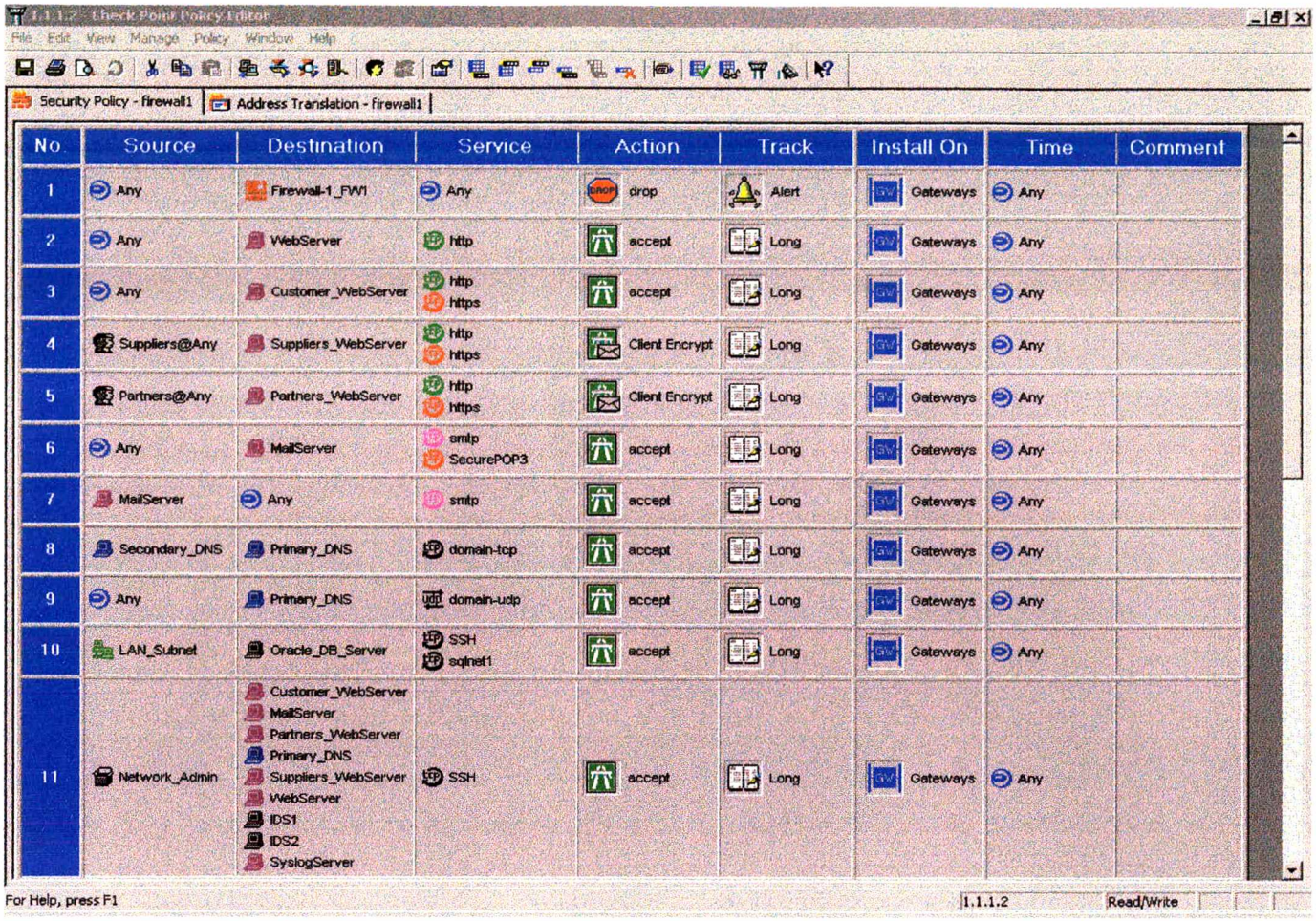
```
iptables –A INPUT –i $EXT_IF –s 23.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 27.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 31.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 36.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 37.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 39.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 41.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 42.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 49.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 50.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 58.0.0.0/7 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 60.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 67.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 68.0.0.0/6 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 72.0.0.0/5 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 80.0.0.0/4 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 96.0.0.0/3 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 169.254.0.0/16 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 192.0.20.0/24 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 197.0.0.0/8 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 218.0.0.0/7 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 220.0.0.0/6 –j log_spoofed
iptables –A INPUT –i $EXT_IF –s 224.0.0.0/3 –j log_spoofed
iptables –A INPUT –o $EXT_IF –d SCLASS_A –j log_reject
iptables –A INPUT –o $EXT_IF –d SCLASS_B –j log_reject
iptables –A INPUT –o $EXT_IF –d SCLASS_C –j log_reject
iptables –A INPUT –o $EXT_IF –d SBROADCAST_SRC –j log_reject
iptables –A INPUT –o $EXT_IF –d $CLASS_D_MULTCAST –j log_reject
iptables –A OUTPUT –o $EXT_IF –d $CLASS_E_RESERVED_NET –j log_reject

#----------Permite os serviços abaixo ----------#

for NSADDR in $NAMESERVERS
do
iptables –A OUTPUT –o $EXT _IF –p udp –s $IPADDR --sport $UNPRIVPORTS \ -d
$NSADDR –dport 53 –j ACCEPT
iptables –A INPUT –i $EXT _IF –p udp –s $NSADDR –sport  53 \ -d $IPADDR –dport
$UNPRIVPORTS –j  ACCEPT
done

#----------Bloqueia todas as portas privilegiadas --------#

iptables –A INPUT –i $EXT_IF –p tcp –dport $PRIVPORTS –j log_priv
iptables –A OUTPUT –o $EXT-IF –p tcp --sport $PRIVPORTS –j log_reject
iptables –A INPUT –i $EXT_IF –p udp --dport $PRIVPORTS –j log_priv
iptables -A OUTPUT –o $EXT_IF –p udp --sport $PRIVPORTS –j log_reject

#---------- bloqueia portas não privilegiadas----------#
```

```
iptables –A INPUT –i $EXT_IF –p tcp \ --dport $XWINDOW_PORTS --syn –j
log_ass_unpriv
iptables –A OUTPUT –o $EXT_IF –p tcp \ --dport $XWINDOW_PORTS --syn –j
log_reject
iptables –A INPUT –m multiport –i $EXT_IF –p tcp \ --dport
$SOCKS_PORT,$OPENWINDOWS_PORT,$NFS_PORT –syn –j log_ass_unpriv
iptables –A OUTPUT –m multiport –o $EXT_IF –p tcp \ --dport
$SOCKS_PORT,$OPENWINDOWS_PORT,$NFS_PORT –syn –j log_reject
iptables –A INPUT –i $EXT_IF –p udp --dport $NFS_PORT –j log_ass_unpriv
iptables –A OUTPUT –o $EXT_IF –p udp --dport $NFS_PORT –j log_reject

#---------- bloqueio de traceroute UDP ----------#

iptables –A INPUT –i $EXT_IF –p udp --sport $TRACEROUTE_SRC_PORTS \ --
dport $TACEROUTE_DEST_PORTS –j log_traceroute

#---------- regras DSUST ----------#

iptables –A OUTPUT –m state --state NEW,ESTABLISHED,RELATE –j ACCEPT
iptables –A INPUT –m state --state NEW –j log_in_new
iptables –A INPUT –m state --state INVALID –j log_in_invalid
iptables –A INPUT –m state --state ESTABLISHED,RELATED –j ACCEPT
iptables – A OUTPUT –m limit –j LOG –log-level 1 \ --log-prefix "OUTPUT POLICY
REJECT"
iptables –A INPUT –m limit –j LOG –log-level 1 \ --log-prefix "INPUT POLICY
DROP"
iptables –A FORWARD –m limit –j LOG --log-level 1 \ --log-prefix "FORWAD
POLICY DROP"

#----------#
logger "Firewall instalado"
exit 0
```

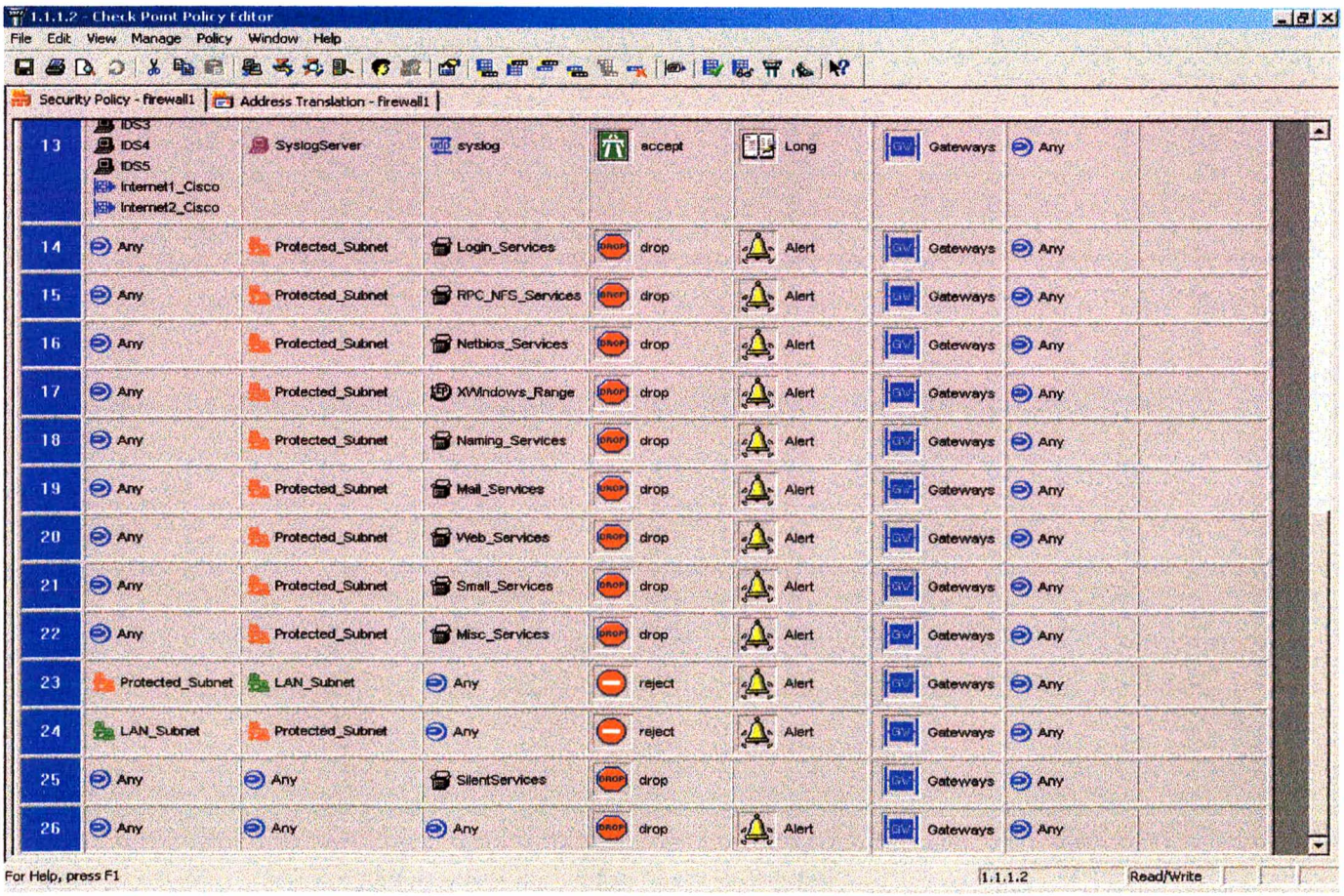
Anexo-06 – Implementação das regras no Firewall-1 Checkpont.



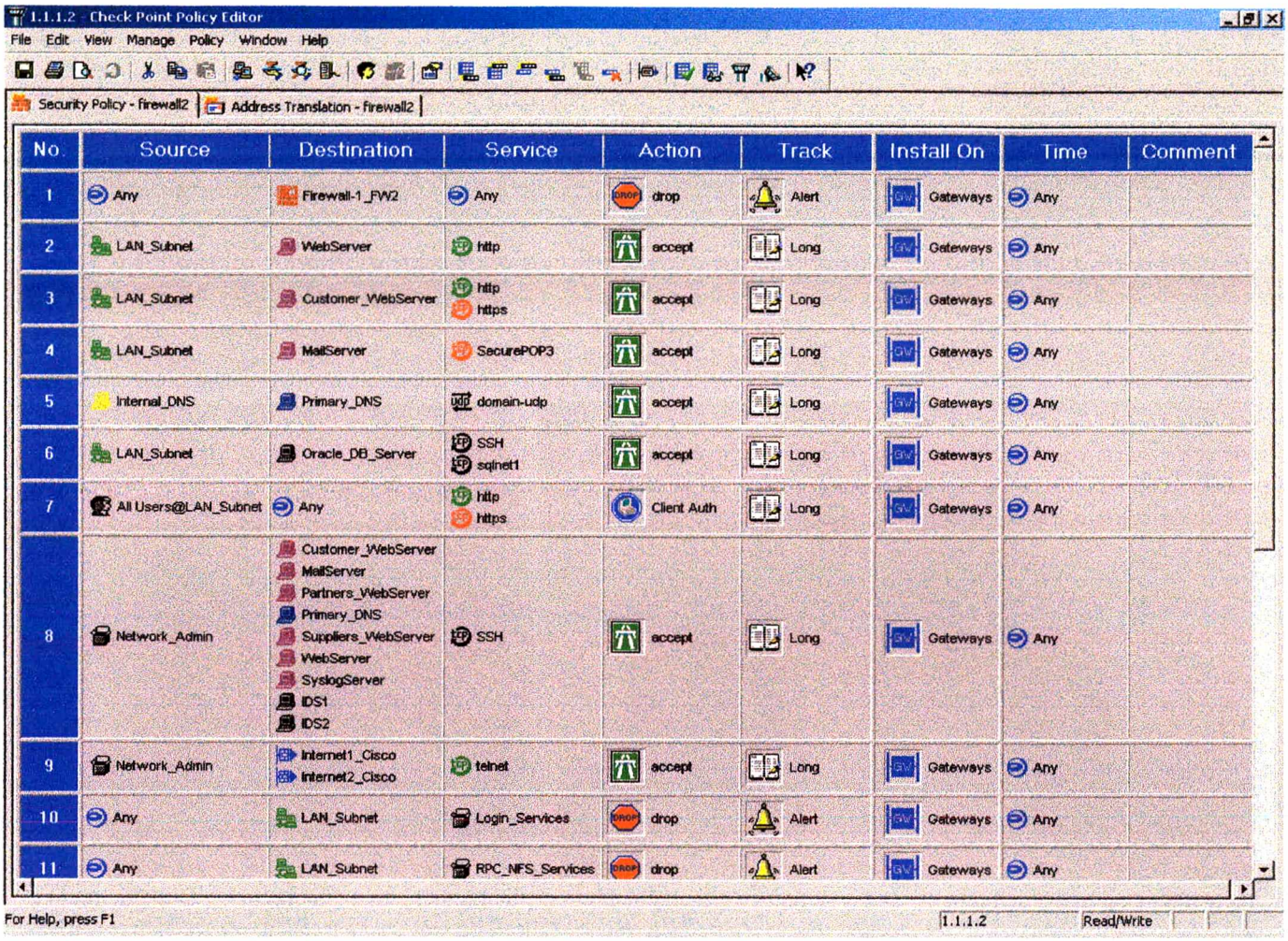


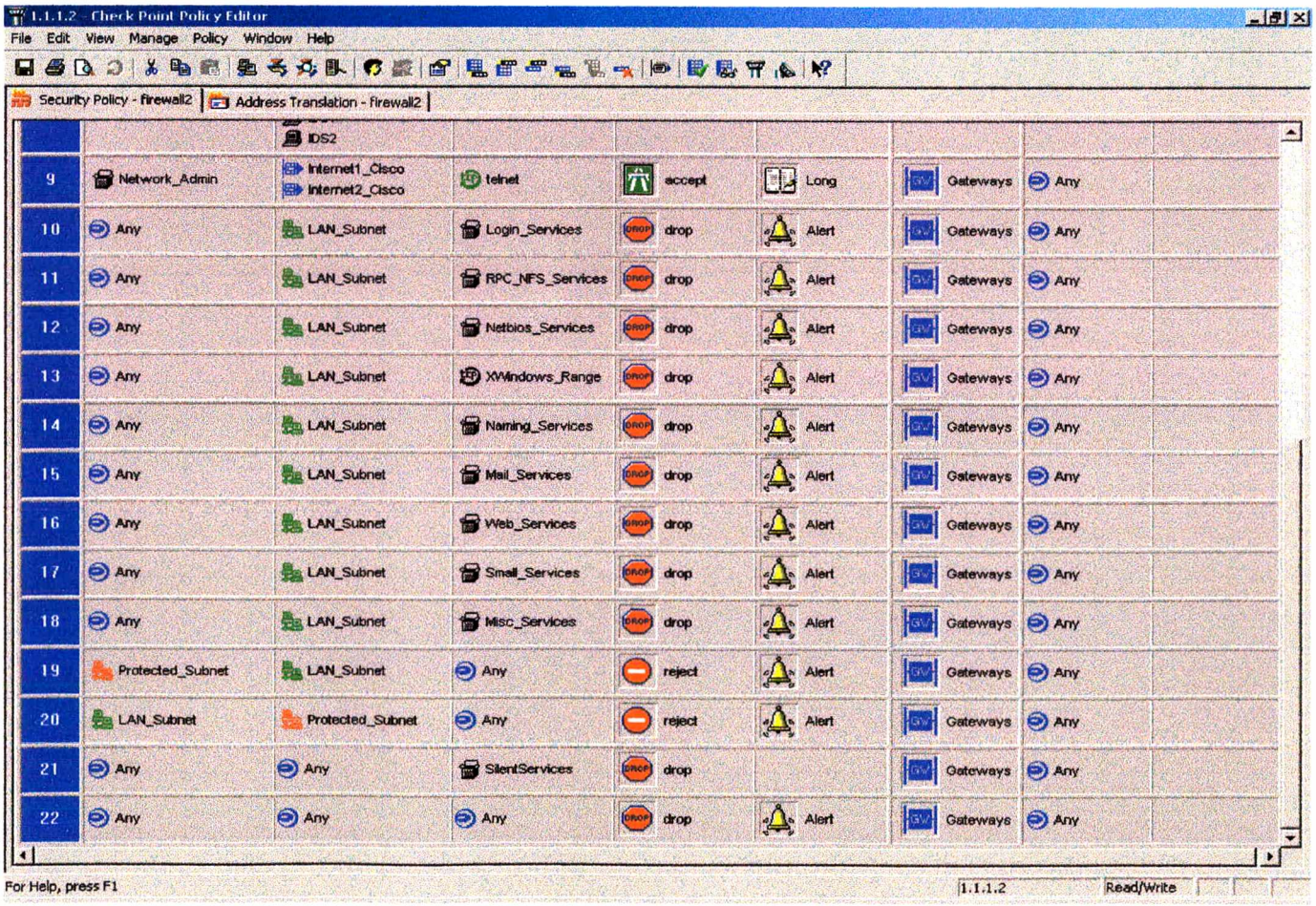


No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Any	Firewall-1_FW1	Any	drop	Alert	Gateways	Any	
2	Any	WebServer	http	accept	Long	Gateways	Any	
3	Any	Customer_WebServer	http https	accept	Long	Gateways	Any	
4	Suppliers@Any	Suppliers_WebServer	http https	Client Encrypt	Long	Gateways	Any	
5	Partners@Any	Partners_WebServer	http https	Client Encrypt	Long	Gateways	Any	
6	Any	MailServer	smtp SecurePOP3	accept	Long	Gateways	Any	
7	MailServer	Any	smtp	accept	Long	Gateways	Any	
8	Secondary_DNS	Primary_DNS	domain-tcp	accept	Long	Gateways	Any	
9	Any	Primary_DNS	domain-udp	accept	Long	Gateways	Any	
10	LAN_Subnet	Oracle_DB_Server	SSH sqlnet1	accept	Long	Gateways	Any	
11	Network_Admin	Customer_WebServer MailServer Partners_WebServer Primary_DNS Suppliers_WebServer WebServer IDS1 IDS2 SyslogServer	SSH	accept	Long	Gateways	Any	

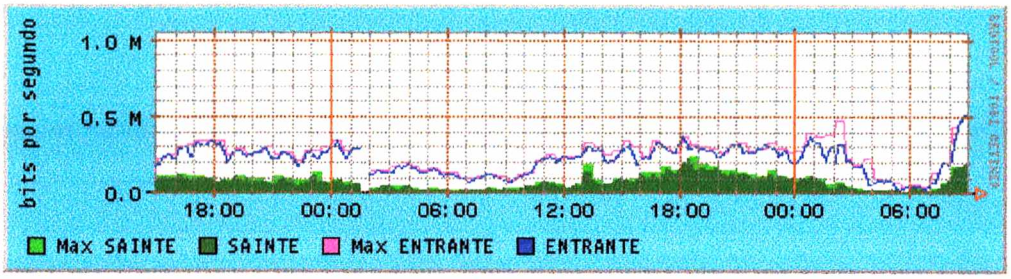


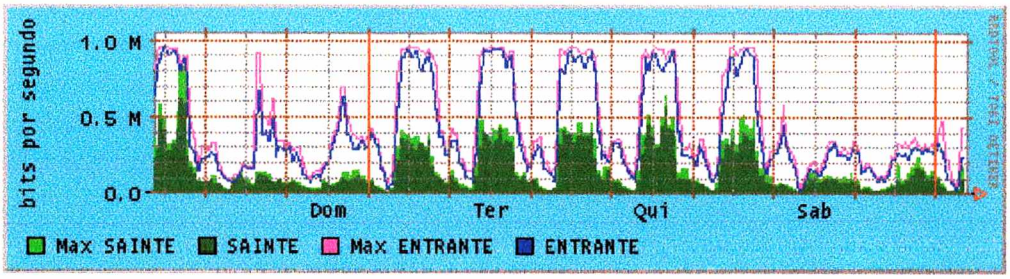
13	IDS3 IDS4 IDS5 Internet1_Cisco Internet2_Cisco	SyslogServer	syslog	accept	Long	Gateways	Any	
14	Any	Protected_Subnet	Login_Services	drop	Alert	Gateways	Any	
15	Any	Protected_Subnet	RPC_NFS_Services	drop	Alert	Gateways	Any	
16	Any	Protected_Subnet	Netbios_Services	drop	Alert	Gateways	Any	
17	Any	Protected_Subnet	XWindows_Range	drop	Alert	Gateways	Any	
18	Any	Protected_Subnet	Naming_Services	drop	Alert	Gateways	Any	
19	Any	Protected_Subnet	Mail_Services	drop	Alert	Gateways	Any	
20	Any	Protected_Subnet	Web_Services	drop	Alert	Gateways	Any	
21	Any	Protected_Subnet	Small_Services	drop	Alert	Gateways	Any	
22	Any	Protected_Subnet	Misc_Services	drop	Alert	Gateways	Any	
23	Protected_Subnet	LAN_Subnet	Any	reject	Alert	Gateways	Any	
24	LAN_Subnet	Protected_Subnet	Any	reject	Alert	Gateways	Any	
25	Any	Any	SilentServices	drop		Gateways	Any	
26	Any	Any	Any	drop	Alert	Gateways	Any	

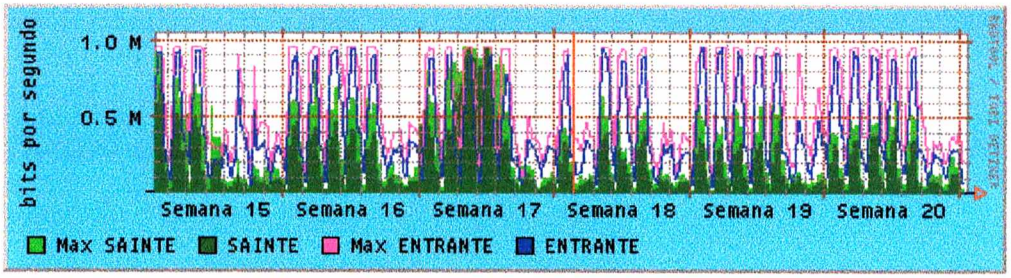

1.1.1.2 - Check Point Policy Editor
File Edit View Manage Policy Window Help
Security Policy - firewall2
Address Translation - firewall2
No. Source Destination Service Action Track Install On Time Comment
1 Any Firewall-1_FW2 Any drop Alert Gateways Any
2 LAN_Subnet WebServer http accept Long Gateways Any
3 LAN_Subnet Customer_WebServer http https accept Long Gateways Any
4 LAN_Subnet MailServer SecurePOP3 accept Long Gateways Any
5 Internal_DNS Primary_DNS domain-udp accept Long Gateways Any
6 LAN_Subnet Oracle_DB_Server SSH sqlnet1 accept Long Gateways Any
7 All Users@LAN_Subnet Any http https Client Auth Long Gateways Any
8 Network_Admin Customer_WebServer MailServer Partners_WebServer Primary_DNS Suppliers_WebServer WebServer SyslogServer IDS1 IDS2 SSH accept Long Gateways Any
9 Network_Admin Internet1_Cisco Internet2_Cisco telnet accept Long Gateways Any
10 Any LAN_Subnet Login_Services drop Alert Gateways Any
11 Any LAN_Subnet RPC_NFS_Services drop Alert Gateways Any
For Help, press F1
1.1.1.2
Read/Write

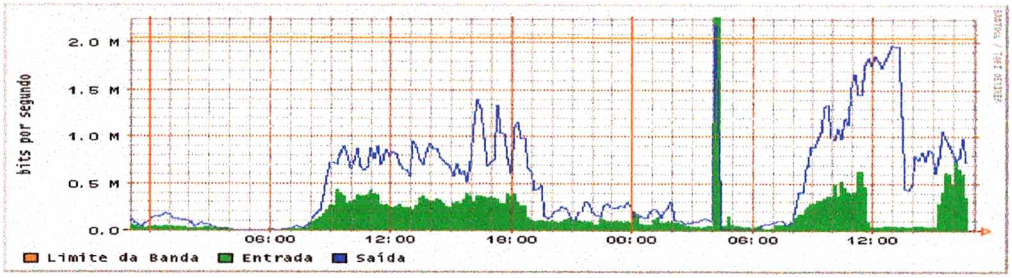

1.1.1.2 - Check Point Policy Editor
File Edit View Manage Policy Window Help
Security Policy - firewall2
Address Translation - firewall2
IDS2
9 Network_Admin Internet1_Cisco Internet2_Cisco telnet accept Long Gateways Any
10 Any LAN_Subnet Login_Services drop Alert Gateways Any
11 Any LAN_Subnet RPC_NFS_Services drop Alert Gateways Any
12 Any LAN_Subnet Netbios_Services drop Alert Gateways Any
13 Any LAN_Subnet XWindows_Range drop Alert Gateways Any
14 Any LAN_Subnet Naming_Services drop Alert Gateways Any
15 Any LAN_Subnet Mail_Services drop Alert Gateways Any
16 Any LAN_Subnet Web_Services drop Alert Gateways Any
17 Any LAN_Subnet Small_Services drop Alert Gateways Any
18 Any LAN_Subnet Misc_Services drop Alert Gateways Any
19 Protected_Subnet LAN_Subnet Any reject Alert Gateways Any
20 LAN_Subnet Protected_Subnet Any reject Alert Gateways Any
21 Any Any SilentServices drop Gateways Any
22 Any Any Any drop Alert Gateways Any
For Help, press F1
1.1.1.2
Read/Write

ANEXO-07 – Coleta de dados do link de acesso à Internet pela INFOVIA-MT.



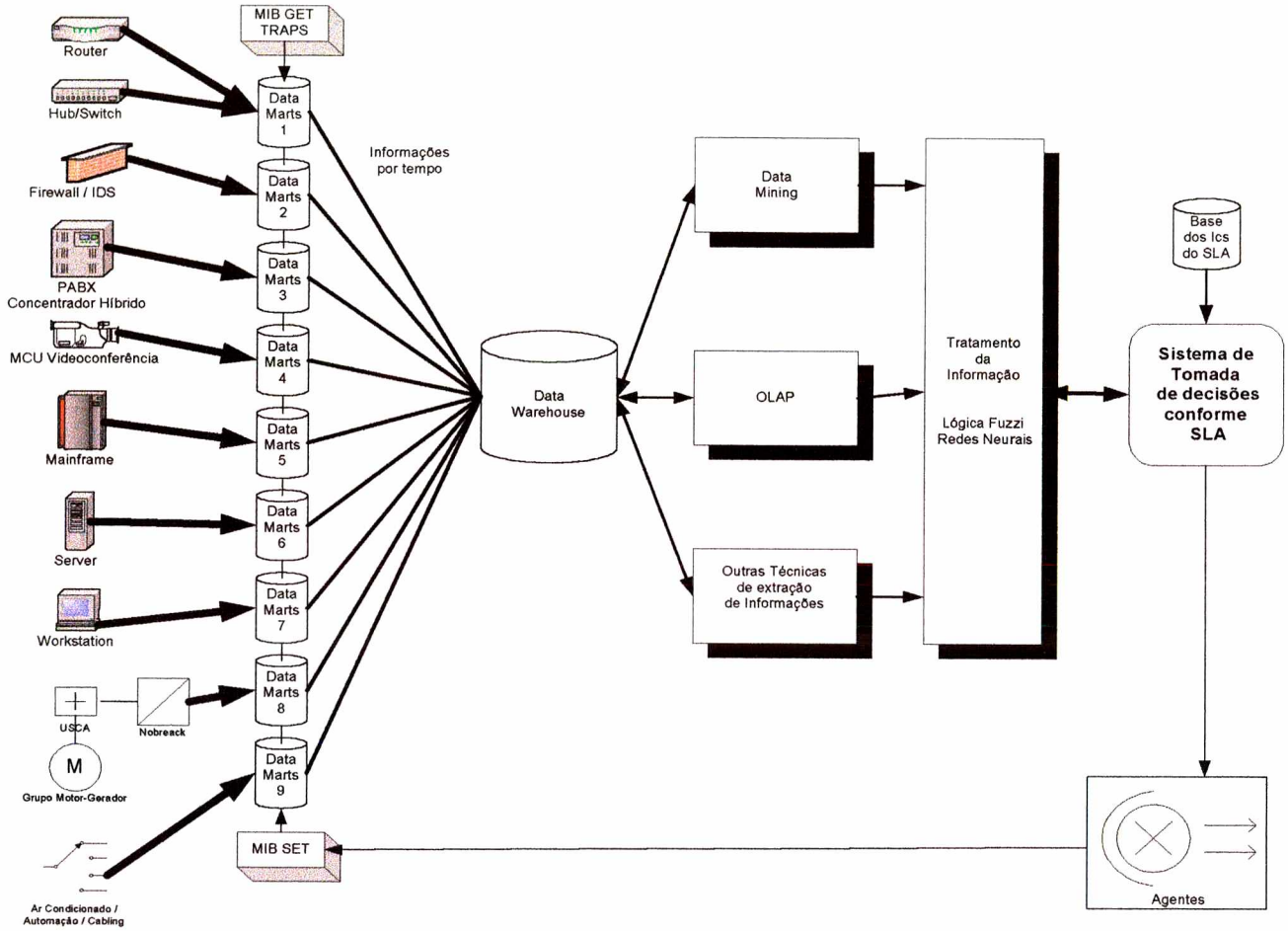




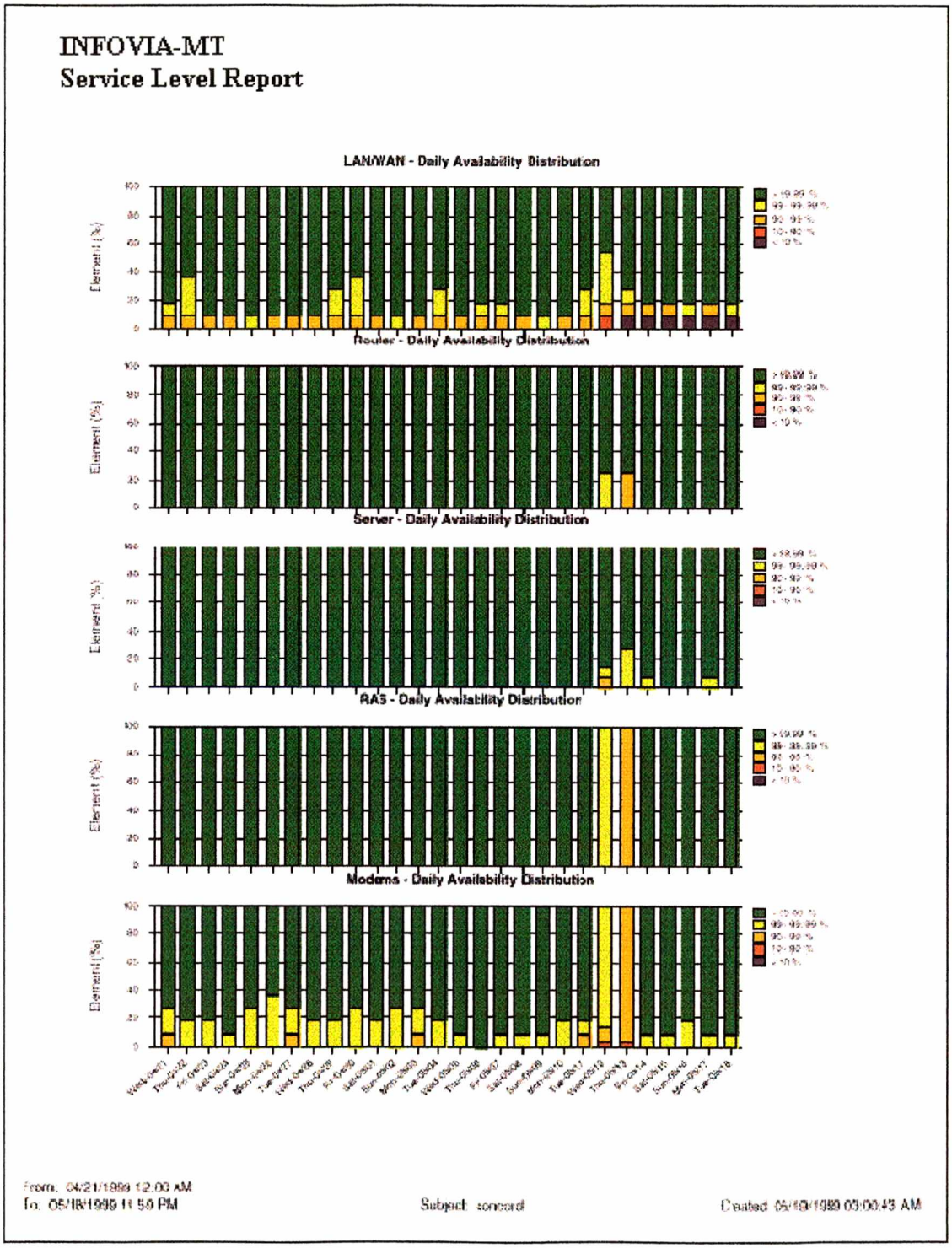


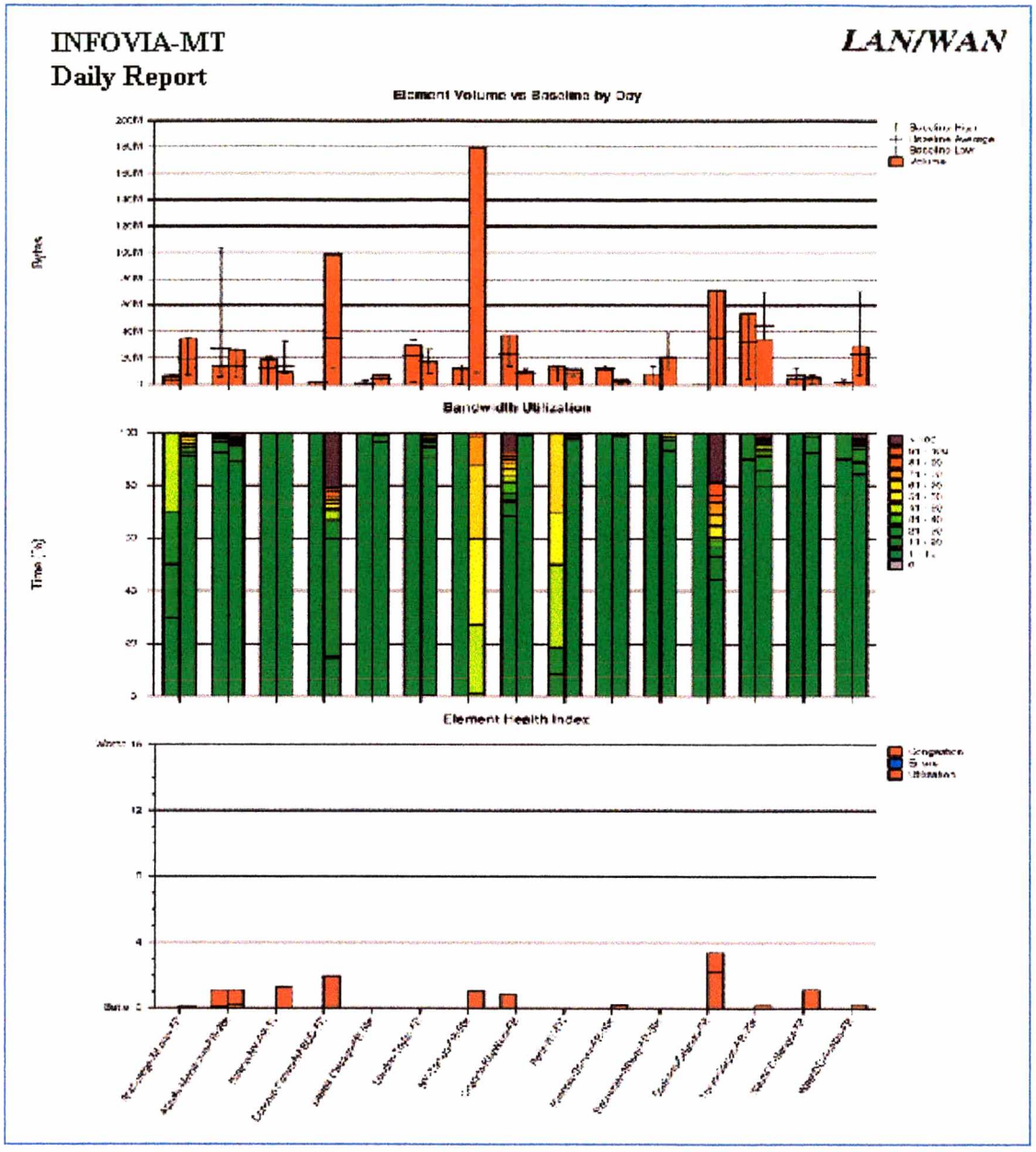
Extraidos ctravés do RRDTOOL / MRTG

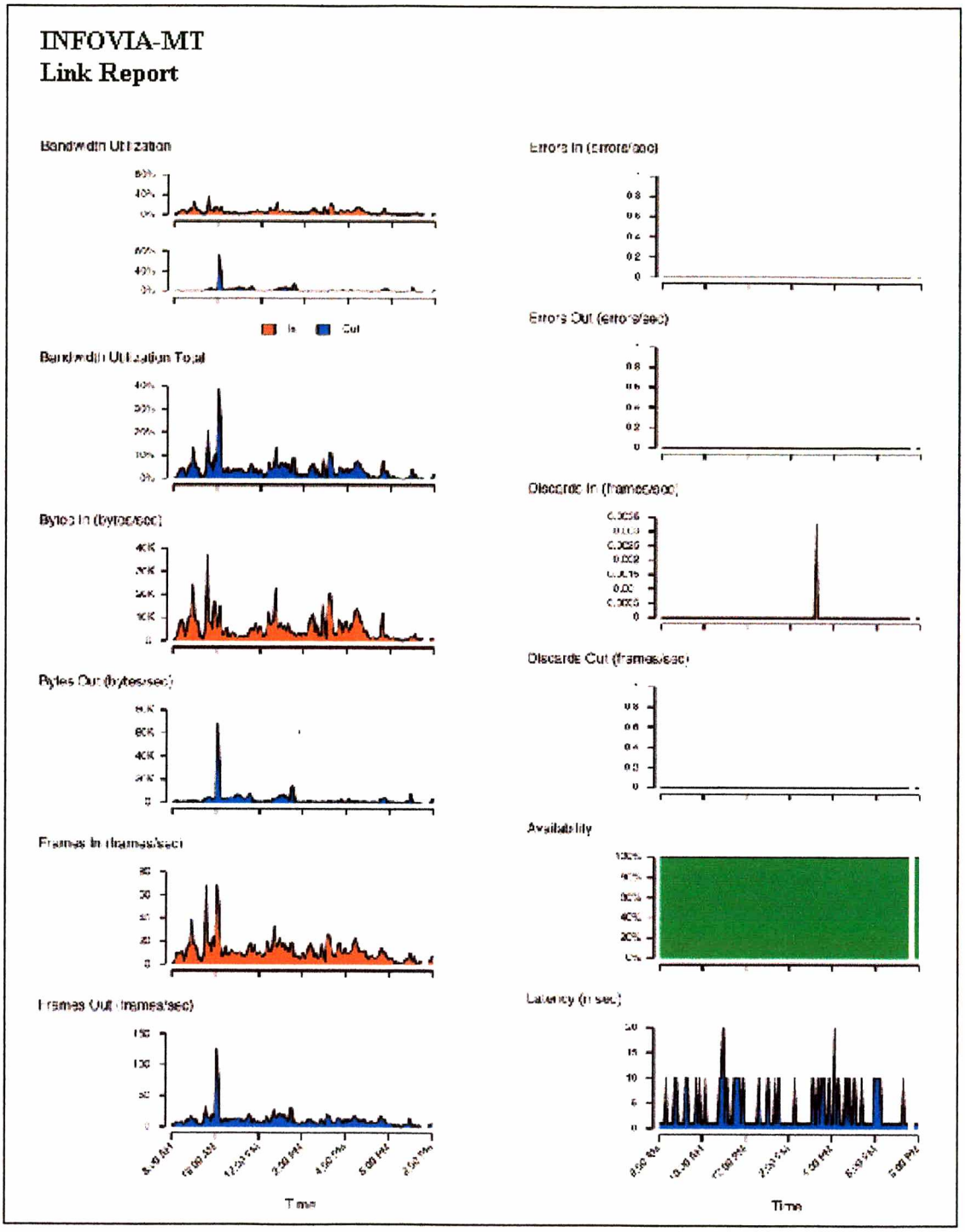
ANEXO-08 – Diagrama de funcionamento de um sistema Data Mining / Data Warehouse de A&G com SLA, proposto para a INFOVIA-MT.

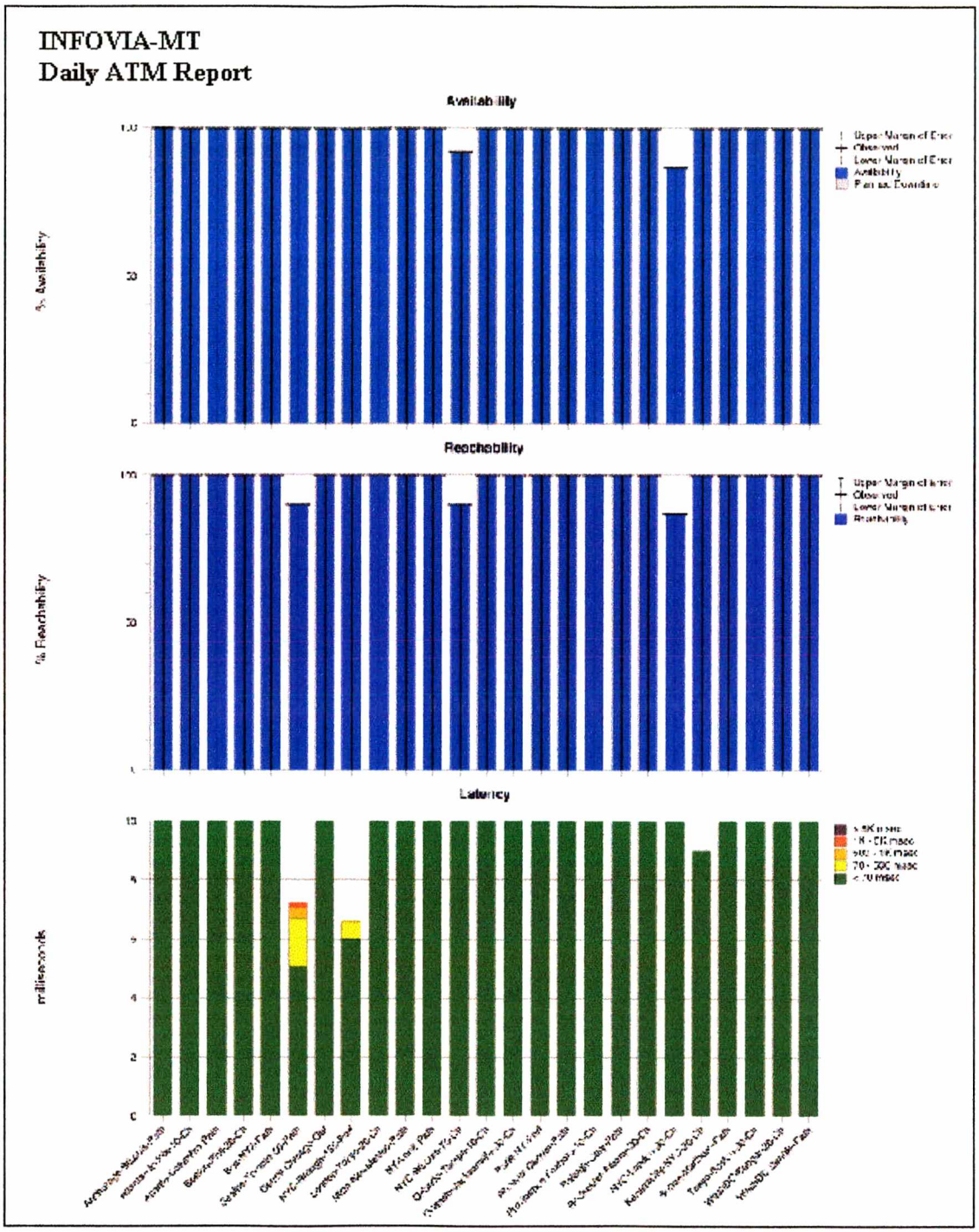


ANEXO-09 – Exemplos de proposta para controle dos Índices do SLA com foco na disponibilidade , Vazão e Desempenho dos vários elementos da rede.

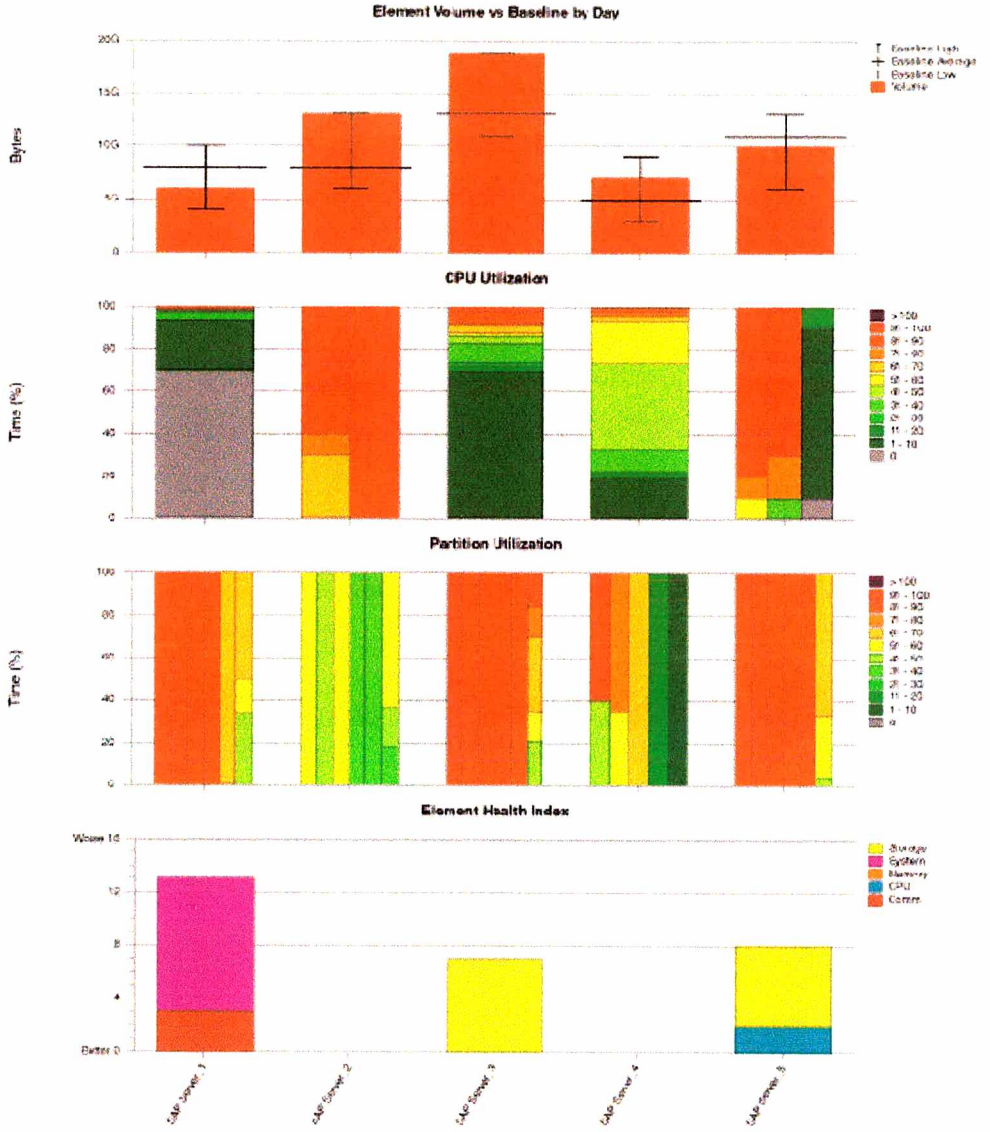



INFOVIA-MT
Daily Report
LAN/WAN
Element Volume vs Baseline by Day
Bytes
Bandwidth Utilization
Time (%)
Element Health Index


INFOVIA-MT
Link Report
Bandwidth Utilization
In
Out
Bandwidth Utilization Total
Bytes In (bytes/sec)
Bytes Out (bytes/sec)
Frames In (frames/sec)
Frames Out (frames/sec)
Time
Errors In (errors/sec)
Errors Out (errors/sec)
Discards In (frames/sec)
Discards Out (frames/sec)
Availability
Latency (msec)
Time

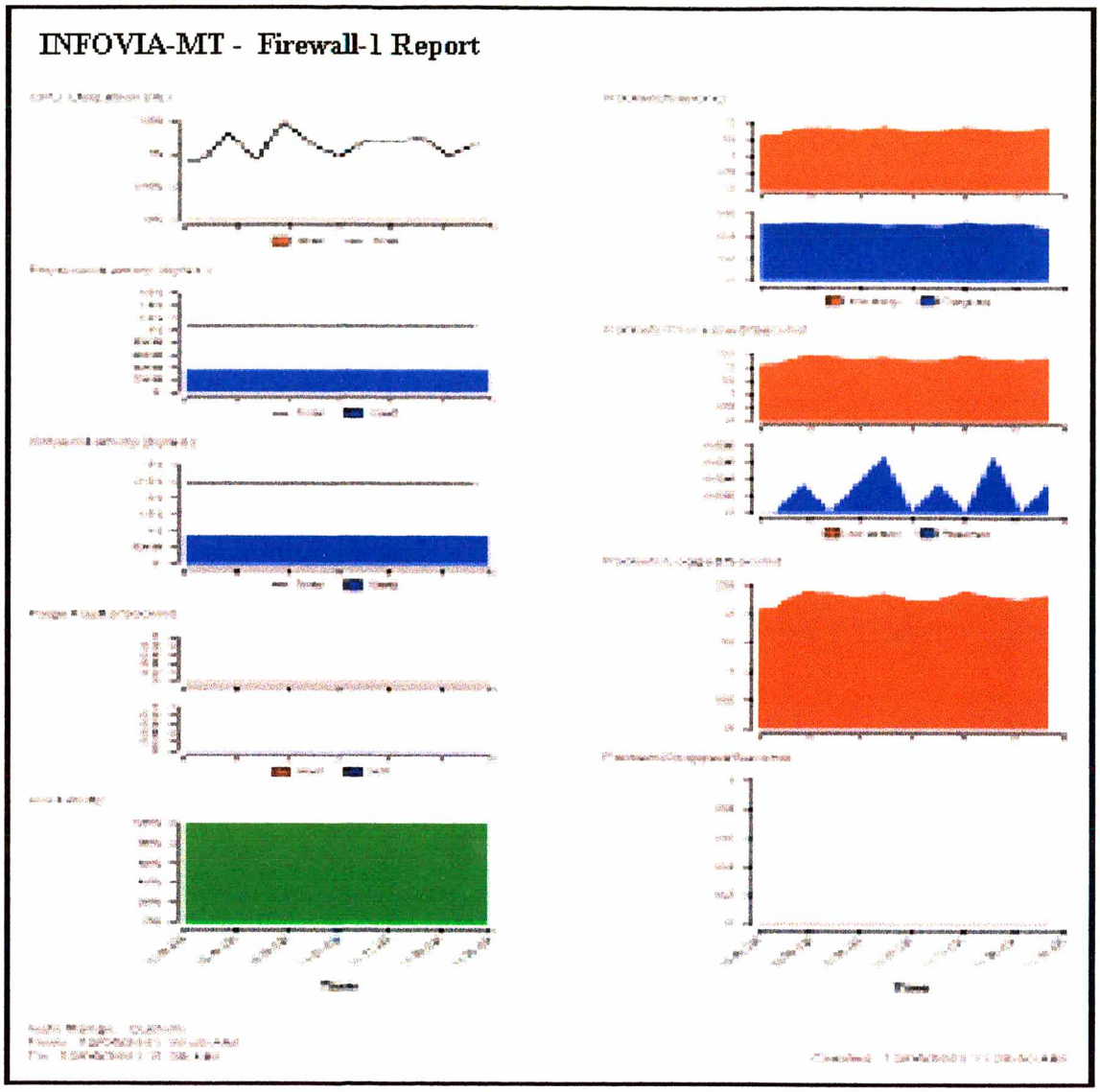

INFOVIA-MT
Daily ATM Report
Availability
% Availability
Reachability
% Reachability
Latency
milliseconds

INFOVIA-MT
Daily Server Report



Baseline: 6 weeks (07/20/1999 to 08/31/1999)

Created: 09/01/1999 01:02:11 AM


INFOVIA-MT - Firewall-1 Report