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

Helio Corrêa Filho

CONTROLE DE ACESSO PARA GERÊNCIA DE SEGURANÇA DE REDES VIRTUAIS EMULADAS

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

Orientador: Carlos Becker Westphall, Dr.

Florianópolis, outubro de 2000

CONTROLE DE ACESSO PARA GERÊNCIA DE SEGURANÇA DE REDES VIRTUAIS EMULADAS

Helio Corrêa Filho

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação na Área de Concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Carlos Becker Westphall, Dr.

Orientador

Fernando A. Ostuni Gauthier, Dr.

Coordenador do Curso

Banca Examinadora

Carlos Becker Westphall, Dr.

Orientador

Solange Terezinha Sari, M.Eng.

Co-orientadora

Roberto Willrich, Dr.

Joni da Silva Fraga, Dr.

"Nada, além do conhecimento, garante nossa liberdade."

(Autor desconhecido)

Dedico este trabalho à minha família
pelo apoio e incentivo por todos esses
anos em que estiveram ao meu lado.

AGRADECIMENTOS

Durante a realização do trabalho muitas pessoas, de alguma forma, foram envolvidas direta ou indiretamente nas contribuições, tornando difícil enumerar todas elas. Dentro destas contribuições, existem distinções significativas, que devem ser registradas. Portanto, relaciono, aqui, pessoas e instituições que ajudaram a tornar possível este trabalho.

A Deus pela vida, saúde e oportunidades oferecidas.

Ao professor e orientador Dr. Carlos Becker Westphall cuja competência, determinação, conhecimento e profissionalismo foram dedicados à minha orientação e permitiram-me que alcançasse a realização deste trabalho. Assim como à M.Eng. Solange Teresinha Sari pela co-orientação e apoio na organização deste trabalho.

Aos professores do Curso de Pós-Graduação em Ciência da Computação, pelos conhecimentos transmitidos no decorrer do curso.

À Universidade Federal de Santa Catarina, pela oportunidade e ao Departamento do Curso de Pós-Graduação em Ciências da Computação, inclusive aos técnicos administrativos, especialmente à Vera Lúcia S. Teixeira e Valdete J. da Rocha, pela atenção dispensada;.

Ao Laboratório de Redes e Gerência pelo acolhimento pelo incentivo à pesquisa que foi de suma importância para minha formação.

Aos integrantes do Laboratório de Interoperabilidade do Núcleo de Processamento de Dados da UFSC, especialmente a Edson Melo, Fernando Cerutti e Kathia Juca, pelo apoio e suporte teórico/prático.

Aos membros da Rede Metropolitana de Alta Velocidade de Florianópolis por permitir utilizar a estrutura física e em especial ao Walter Ferreira Siqueira pelo suporte técnico.

Ao Grupo de Análise e Projeto Mecânico pela bolsa que muito contribuiu no meu aprendizado e pelas amizades construídas ao longo do tempo.

Aos professores integrantes da banca examinadora pela apreciação do trabalho e valiosas contribuições na redação final.

À minha namorada, Arlete Moraes, por seu amor, companheirismo, auxílio, paciência e incentivo na realização deste trabalho, que por tantas vezes foram necessários.

Aos colegas de curso pelas amizades construídas e convívio, que muito auxiliaram na formação acadêmica, em especial à Gentil Veloso Barbosa, José Gonçalo dos Santos e Sedecias Lopes Cavalcante.

SUMÁRIO

LISTA DE ABREVIATURAS

ABR	*Avaliable Bit Rate.*
ALL	*ATM Adaptation Layer.*
AS	*Security Agent.*
ATM	*Assynchronous Transfer Mode.*
BUS	*Broadcast and Unknown Server.*
CCITT	*Comité Consultafit International Télégraphique et Téléphonique*
ELAN	*Emulated Local Area Network.*
ESI	*End System Identifier.*
HEC	*Header Check Error*
ICI	*Inter-exchange Carrier Interface.*
ILMI	*Integrated Local Management Interface*
IP	*Internet Protocol*
LAN	*Local Area Network.*
LANE	*LAN Emulation*
LE-ARP	*LAN Emulation Address Resolution Protocol.*
LEC	*LAN Emulation Client.*
LECS	*LAN Emulation Configurator Server.*
LES	*LAN Emulation Server.*
LNNI	LAN Emulation Network-Network Interface
LNNI	*LAN Emulation Network to Network Interface*
LUMI	LAN Emulation User-Network Interface
MAC	*Medium Access Control.*
MIB	*Management Information Base.*
NNI	*Network to Network Interface.*
OAM	*Operations And Maintenance*
OSI	*Open System Interconnection.*
PCI	*Protocol Control Information.*
PM	*Performance Monitoring*
QoS	*Quality of Service.*
RD	*Route Descriptor*
RFC	*Request For Commnet*
SDU	*Service Data Unit.*
SNMP	*Simple N etwork Management Protocol.*
SVC	*Switched Virtual Circuit*
TCP	*Transmission Control Protocol.*
UNI	*User Network Interface.*
VBR	*Variable Bit Rate.*
VC	*Virtual Circuit.*
VCC	*Virtual Channel Connection.*
VCI	*Virtual Circuit Indentifier.*
VPC	*Virtual Path Connection.*
VPI	*Virtual Path Identifier.*
VPL	*Virtual Permanent Link*

LISTA DE FIGURAS

LISTA DE QUADROS

RESUMO

Visando incrementar a segurança no ambiente de redes virtuais emuladas, este trabalho apresenta procedimentos de controle de acesso para prevenir e reagir a diversos tipos de ameaças. O estudo apresenta três categorias de ameaças ao serviço de LAN *Emulation* (LANE): Confidencialidade, Integridade e Disponibilidade. Também descreve as políticas de segurança estabelecidas pelo ATM *Forum*, as quais foram avaliadas por meio de experimentos. Os experimentos foram realizados em uma rede que possui *backbone* ATM e sub-redes *Ethernet*. Com base nas ameaças, foram definidos procedimentos de controle de acesso usando as políticas de segurança e atributos de controle do próprio equipamento. Esses procedimentos de controle são implementados pelo gerenciamento *Simple Network Managament Protocol* (SNMP), o qual utiliza regras de produção para tomada de decisão.

ABSTRACT

Aiming at to develop the security in the environment of emulated virtual networks, this work presents procedures of access control to prevent and to react the diverse types of threats. The study it presents three categories of the threats to LAN Emulation Service: Confidentiality, Integrity and Availability. Also it describes the policies of security established by ATM Forum, which had been evaluated through experiments. The experiments had been carried through in a network that has an ATM backbone and Ethernet sub-networks. Based in the threats, procedures of access control were defined using the security policies and attributes of control of the proper equipment. These procedures of control are implemented through the management Simple Network Managament Protocol (SNMP), which uses rule set production for decision taking.

1. INTRODUÇÃO

1.1. Visão Geral

A tecnologia ATM ainda possui alto custo e não é tão difundida quanto o *Ethernet*, ficando restrita às grandes empresas e instituições (privadas e públicas). Essa dificuldade de acesso ao ATM pode ser a razão pela qual o registro de ataques neste ambiente não serem freqüentes.

O uso de redes IP (*Internet Protocol*) sobre o ATM (*Assynchronous Transfer Mode*) tem se mostrado preponderante no mercado atual. Uma solução que reúne a intensa disseminação das redes IP com as características de alta velocidade e qualidade de serviços das redes ATM. O IETF (*Internet Engineering Task Force*) especifica dois serviços para redes locais virtuais; primeiramente a especificação do IP Clássico que ocorre de modo nativo, e depois em conjunto com o ATM *Forum* a especificação LANE, que ocorre pela emulação de redes locais.

O surgimento da arquitetura LANE está proporcionando um aumento da disseminação do uso de redes *Ethernet* sobre ATM, tornando mais acessível o uso do ATM, que por outro lado fica mais susceptível a ameaças de segurança devido à flexibilidade no registro de novos elementos de rede independentemente da localização física.

1.2. Justificativa

Com a implantação dos *backbones* ATM das redes RNP (POP-SC), RCT (POP-UFSC), redeUFSC, e RMAV-FLN foi observado a necessidade de conhecer as limitações da tecnologia ATM em termos falhas, configuração, desempenho e principalmente em segurança.

Cada rede mencionada implementa o serviço LANE, onde estão configurados um ou mais servidores (configuração, resolução de endereços e *broadcast*). Essas redes suportam aplicações de missão crítica que exigem qualidade e segurança na transmissão de dados, áudio e vídeo.

Atualmente é possível uma máquina que está fisicamente em uma rede conectar-se a diferentes redes locais virtuais, facilitando o roteamento de pacotes e

consequentemente o desempenho das aplicações de videoconferência, biblioteca digital, processamento paralelo e outras. O benefício das redes virtuais também trouxe preocupação com relação a segurança, devido a ataques intencionais ou não.

Desta forma, faz-se necessário um estudo detalhado das características de segurança dos equipamentos e a implantação de um sistema de gerência de segurança.

1.3. Trabalhos Existentes

O ATM *Forum,* através da especificação de segurança AF-SEC-0100.000 [SEC100/99] define procedimentos de segurança em redes ATM. Este documento especifica mecanismos de autenticação, confidencialidade, integridade de dados, e controle de acesso para o plano de usuário. Também especifica mecanismos para autenticação e integridade para o plano de controle (sinalização UNI e NNI). Não faz parte do escopo desta especificação a segurança no plano de gerenciamento.

Uma análise do fluxo de dados para o serviço LANE é descrita por Laurent em [LAUREN/96]. Onde a autora apresenta os possíveis ataques, sem mencionar como combatê-los.

1.4. Objetivos e Metas

O objetivo geral é implantar procedimentos de controle de acesso para gerência de segurança em redes virtuais locais emuladas, por meio de estudo de caso que utiliza políticas de segurança definidas pelo ATM *Forum* para prevenir e evitar diferentes ataques.

Para atender a este objetivo e delinear o desenvolvimento do trabalho, são estabelecidas as seguintes metas:

- Pesquisar aspectos de segurança em redes ATM;
- Estudar documentos especificados pelo ATM *Forum*;
- Descrever as diferentes formas de ataques à arquitetura LANE;
- Fazer experimentos para testar as políticas de segurança pré-estabelecidas;
- Criar procedimentos de controle para prevenir ou reagir aos ataques no serviço LANE;
- Implementar procedimentos de controle através do sistema de gerência.

1.5. Apresentação do Trabalho

Foram estabelecidos neste item os objetivos do trabalho, a motivação encontrada para realização deste, bem como o estado atual da linha de pesquisa. No item 2 é dado uma visão geral sobre as redes ATM, mencionando as funções de gerenciamento e controle, sinalização e endereçamento. O serviço LAN *Emulation* é apresentado no item 3, descrevendo as funções de suas entidades. Em particular, no item 4, são apresentados os aspectos de segurança do ambiente LANE, em que são descritas três categorias de ameaças e as políticas de segurança existentes para combater os possíveis ataques. No item 5 é descrito o ambiente de estudo utilizado para realização de experimentos feitos para avaliação das políticas de segurança. Os procedimentos de controle de acesso ao serviço LANE, baseados nas análises das ameaças são apresentados no item 6, bem como os detalhes da implementação desses procedimentos pelo gerenciamento SNMP. As conclusões e perspectivas de trabalhos futuros são mostradas no item 7. Por fim são apresentadas as referências bibliográficas e o Anexo 1 que traz a descrição dos objetos gerenciados utilizados no presente trabalho.

2. VISÃO GERAL DE REDES ATM

O ATM é uma tecnologia orientada à conexão que baseia-se no modo de transmissão assíncrono (não é vinculada a um relógio mestre), podendo transportar simultaneamente diversos tipos de tráfego digitalizados, utilizando-se de altas taxas de transmissão, mantendo um nível predeterminado de *Quality of Service* (Qualidade de Serviço - QoS) [TANENB/96], [ALLES/95]. O ITU-T (*International Telecommunications Union*), em sua especificação [ITU-T/95] define modo de transferência, como o termo utilizado para designar a tecnologia empregada na transmissão, multiplexação e comutação de células.

A ATM é uma tecnologia na qual a definição dos padrões está centralizada em dois órgãos de padronização, que são:

- ITU-T, órgão de padronização de telecomunicações da *International Telecommunications Union* (ITU), que está creditando à tecnologia ATM a responsabilidade de transportar os serviços da B-ISDN (*BroadBand Integrated Digital Network* – Rede Digital de Serviços Integrados de Banda Larga), principalmente no que se refere à parte pública das redes das provedoras de serviços;
- ATM *Forum*, é uma organização sem fins lucrativos formada com o objetivo de acelerar o uso de produtos e serviços ATM. É composto por um consorcio de várias empresas e usuários, onde os principais objetivos são desenvolver a tecnologia e padronizar as redes privadas.

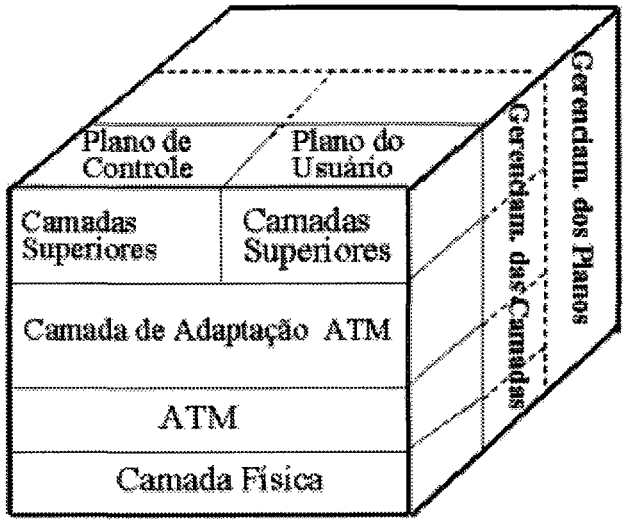
Atualmente, o ATM é uma tecnologia que não está mais confinada somente ao contexto das B-ISDN. É encontrada cada vez mais em aplicações como LANs, MANs, Comutadores LAN, *backbones* e estações de trabalho. Porém percebe-se que o ATM tende a predominar nos *backbones* e as tecnologias baseadas no *Ethernet* nas bordas.

2.1. Funções de Gerenciamento e Controle

A B-ISDN que utiliza o ATM tem um modelo próprio de referência, que é diferente dos modelos OSI e TCP/IP (Internet). O modelo de referência do ATM definido pelo CCIT [CCIT/91] e descrito por Tanenbaum [TANENB/96] é composto pelos seguintes planos, distribuídos por todas as camadas, conforme Figura 2.1-1.

- **Plano de Usuário** – utilizado na transferência de informação dos usuários;
- **Plano de Controle** – responsável pelas funções de controle, tais como: sinalização, roteamento e manutenção das conexões ATM;
- **Plano de Gerenciamento** – é composto de dois tipos de gerenciamento: dos planos e das camadas que estão relacionados ao gerenciamento de recursos e à coordenação entre camadas.

Figura 2.1-1- Modelo de referência B-ISDN



O Quadro Iapresenta a estrutura das camadas: Física, ATM e AAL e suas funções conforme o modelo de referência B-ISDN.

Quadro I - Camadas da Tecnologia ATM.

Camada OSI	Camada ATM	Subcamada ATM	Funcionalidade
¾	AAL	CS	Oferecer interface padrão (convergência)
		SAR	Segmentação e Remontagem
2/3	ATM		Controle de fluxo Geração e remoção de cabeçalho de célula Gerenciamento de caminho/circuito virtual Multiplexação/Demultiplexação de células
2	FÍSICA	TC	Desacoplamento de taxa de células Geração e verificação de soma de verificação Geração de célula Compactação/descompactação de células a partir do envelope delimitador Geração de quadro
1		PMD	Sincronização de bits Acesso à rede física

Camada Adaptação ATM

Como a maioria das aplicações não trabalha diretamente com as células, definiu-se uma Camada de Adaptação ATM (AAL) acima da Camada ATM, com o objetivo de permitir que usuários possam enviar pacotes maiores do que uma célula.

As Camadas de Adaptação ATM e Física são divididas em duas subcamadas, sendo que a subcamada inferior é responsável pela realização do trabalho à ela destinado, a subcamada superior tem a função de realizar a interface com a camada acima dela.

Camada ATM

A camada ATM (ATM *Layer*) faz todo o seu processamento a partir da geração e inspeção dos campos de cabeçalho da célula ATM, do estabelecimento e liberação de circuitos virtuais, bem como o controle de congestionamento.

Estas células possuem tamanho fixo de 53 *octetos*, sendo 48 *octetos* de carga útil (dados de usuário) e 5 *octetos* de cabeçalho, que são transmitidas através de conexões de circuitos virtuais estabelecidos, sendo a entrega e comutação feitas pela rede baseada na informação do cabeçalho.

Camada Física

A camada física (*Physical Layer- PHY*) envolve a especificação de um meio de transmissão e um esquema de codificação de sinal. As taxas especificadas na camada física são de 155 Mbps e 622 Mbps, sendo que pode haver taxas inferiores ou superiores.

Presente em todos os equipamentos da rede a camada física oferece facilidades de transmissão das células através dos meios físicos que conectam os dispositivos ATM.

Na transmissão, a subcamada de Convergência de Transmissão (TC) recebe um fluxo de células, vindo da camada ATM e efetua a seguinte seqüência de operações, segundo Soares [SOARES/95]:

1. Gera o HEC (*Header Error Check*) para cada célula e o insere no campo destinado no cabeçalho;
2. Transforma o fluxo de células em um fluxo de bits (ou *bytes*, dependendo da *Performance Monitoring* - PM) adequado para a transmissão pela subcamada inferior (PM), inserindo informações que permitirão à subcamada TC do receptor recuperar as fronteiras das células transmitidas;
3. Conforme o fluxo de saída é gerado no item anterior, passa para a subcamada de meio físico que se encarregará da transmissão de bits pelo meio físico (PM).

2.2. Sinalização em ATM

O plano de controle do Modelo de Referência de Protocolos (PRM) para as redes B-ISDN, é o responsável pelo processo de sinalização utilizado para o estabelecimento, supervisão, controle e liberação das chamadas e conexões ATM (PVCs e VCCs). Chamadas são conexões ou conjunto de conexões entre dois ou mais participantes [SOARES/95].

Conforme Tanenbaum [TANENB/96], antes de uma chamada ser feita é preciso enviar uma mensagem para configurar a conexão virtual da origem ao destino. Em seguida todas as células subseqüentes seguirão o mesmo caminho em direção a seu destino. A entrega das células não é garantida, mas sua ordem de transmissão é respeitada.

Segundo Soares [SOARES/95] a recomendação I.311 do ITU-T especifica as características de sinalização da redes B-ISDN e menciona suas funções:

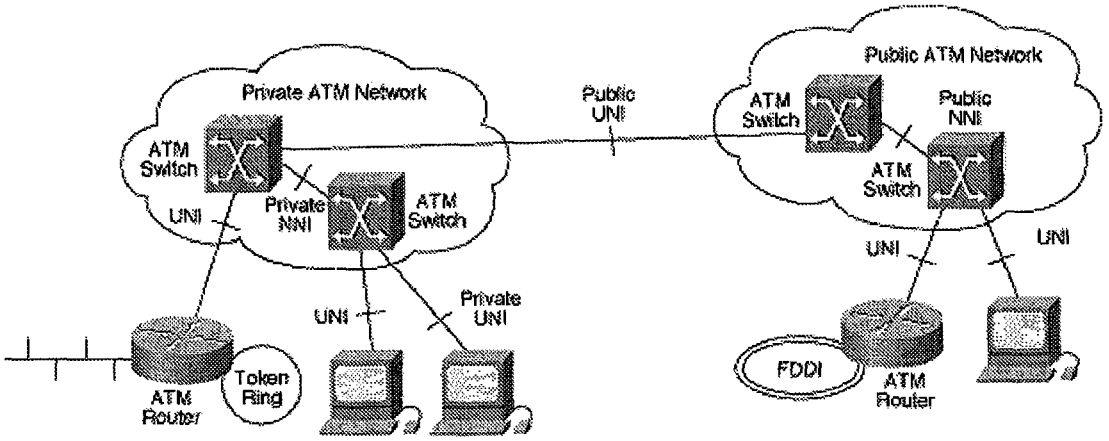
1. Estabelecimento, manutenção e liberação de conexões, que podem ser sob demanda, semi-permanentes ou permanentes, e que devem ser administradas de forma a manter as características solicitadas e descritas pelos parâmetros de qualidade de serviço;
2. Suporte à configuração ponto-a-ponto, multiponto e difusão;
3. Suporte às chamadas com várias conexões e participantes, incluindo a possibilidade de adição e remoção de conexões a uma chamada existente, entrada de novos participantes com adições de conexões e saída de participantes;
4. Renegociação das características de tráfego de uma conexão já estabelecida.

2.2.1. Operação na rede ATM

Segundo Alles [ALLES/95], em uma rede ATM, todos os sistemas finais ATM são conectados através de um ou mais *comutadores* ATM , conforme mostra Figura 2.2-1. Os comutadores são ligados aos sistemas finais ATM e, entre si, através de ligações físicas ponto-a-ponto, em que são associados certos tipos de interfaces. Os comutadores ATM suportam dois tipos de interfaces:

1. **Interface Usuário-Rede** (*User-network interfaces*-UNI) - conecta sistemas finais ATM (como *hosts* e roteadores) a um comutador ATM em uma rede ATM privada;
2. **Interface Rede-Nodo** *(Network-node interfaces-NNI)* - os comutadores se interligam usando uma interface NNI privada. No caso da ligação de uma rede ATM privada a uma rede ATM pública, será utilizada uma interface de usuário (UNI).

Figura 2.2-1 - Interfaces de rede ATM.



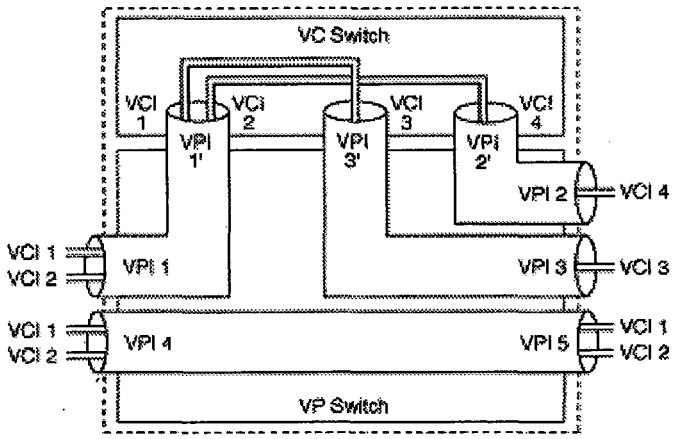
Os comutadores ATM usam os campos VPI e VCI, contidos no cabeçalho da célula, para identificar o próximo segmento de rede que a célula precisa percorrer para

alcançar o seu destino. Este endereço identifica unicamente uma conexão virtual ATM numa interface física.

Observa-se na Figura 2.2-2, que os caminhos virtuais são identificados pelo VPI e os canais virtuais identificados pela combinação de um VPI e um VCI.

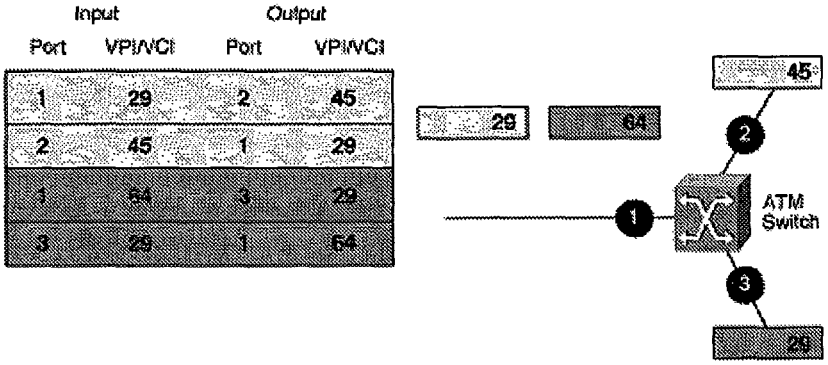
Um canal virtual é equivalente a um circuito virtual e descreve uma conexão lógica entre dois sistemas finais. Caminho virtual é um grupo lógico de circuitos virtuais que permitem que um comutador ATM realize operações em grupos de circuitos virtuais. Todos os VCI e VPI, entretanto, somente têm significado local através de uma ligação particular e são remapeados de forma apropriada em cada comutador. Em operação normal, os comutadores alocam todas as conexões UNI com VPI=0.

Figura 2.2-2 - Circuitos Virtuais e Comutação de Caminhos Virtuais.



A operação básica de um comutador ATM é muito simples: recebe uma célula através de uma ligação física num valor VCI e VPI conhecidos, procura o valor da conexão na tabela de tradução local para determinar a(s) porta(s) de conexão e o novo valor VPI e VCI nesta ligação física, e então, retransmite a célula na ligação de saída com os identificadores de conexão apropriados, conforme Figura 2.2-3.

Figura 2.2-3 - Operações de um Comutador ATM.



A operação de um comutador é simples, porque os mecanismos externos configuram a tabela de tradução local antes de qualquer transmissão de algum dado. A forma como essas tabelas são configuradas determinam os dois tipos fundamentais de conexões ATM:

Conexões Virtuais Permanentes (*Permanent Virtual Connections*-PVC) - é uma conexão configurada por mecanismos externos, tipicamente gerência de rede, na qual um conjunto de comutadores entre um sistema ATM origem e um sistema ATM destino são programados com os valores VPI/VCI apropriados. A sinalização ATM é facilitada pela configuração de PVCs, mas por definição PVCs sempre requerem alguma configuração manual;

Conexões Virtuais Comutadas (*Switched Virtual Connections*-SVC) - é uma conexão que é configurada automaticamente através de um protocolo de sinalização. SVCs não precisam de intervenção manual, diferentemente da configuração de PVCs e, por isso, são mais utilizadas.

2.2.2. Estabelecimento e Encerramento de Conexão

Tecnicamente o estabelecimento de conexão não pertence a camada ATM, mas é manipulada pelo Plano de Controle, usando um protocolo ITU-T bastante minucioso cujo nome é Q.2931 [ITU-T/95].

O estabelecimento de um circuito virtual utiliza os seis tipos de mensagens listados no Quadro II. Cada mensagem ocupa uma ou mais células e contém tipo, tamanho e parâmetros da mensagem.

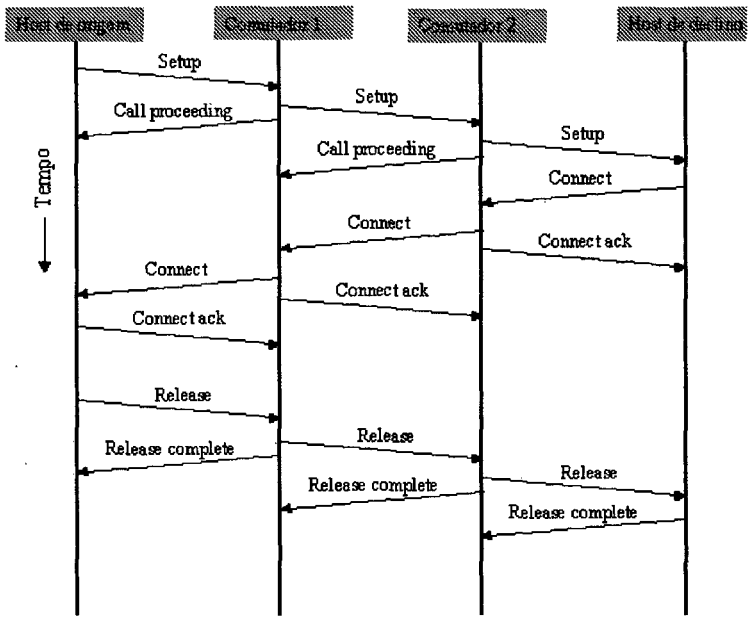
Quadro II - Mensagens usadas para o estabelecimento e encerramento da conexão.

Mensagem	Significado quando enviada pela estação	Significado quando Enviada pela rede
SETUP	Estabelecer um circuito	Chamada recebida
CALL PROCEEDING	Confirmação do recebimento da chamada	A sua solicitação de chamada será processada
CONNECT	Aceito a chamada recebida	Aceitação da chamada
CONNECT ACK	Confirmação da conexão	Confirmação da realização da chamada
RELEASE COMPLETE	Confirmação de liberação	Confirmação de liberação

Quando uma estação deseja se comunicar com outra, é necessário que exista uma conexão virtual estabelecida entre os dois pontos. O procedimento normal para o estabelecimento de uma chamada é fazer com que a estação envie a mensagem *SETUP* em um circuito virtual especial. Em seguida, a rede responde com *CALL PROCEEDING* para confirmar o recebimento da solicitação. Quando se propaga na direção do destino, a mensagem *SETUP* é confirmada em cada *hop* por *CALL PROCEEDING.* Quando a mensagem *SETUP* finalmente chega, a estação destino pode responder com *CONNECT* para aceitar a chamada. Em seguida, a rede envia a mensagem *CONNECT ACK* para indicar que recebeu a mensagem *CONNECT.* Quando a mensagem *CONNECT* é propagada na volta em direção da origem, cada comutador que a receber deverá confirmá-la com uma mensagem *CONNECT ACK* [TANENB/96].

A seqüência que encerra é igualmente simples, a estação que deseja desconectar-se só precisa enviar a mensagem *release*, que se propaga até a outra extremidade e faz com que o circuito seja encerrado. a mensagem é confirmada com *release complet* em cada um dos *hops* ao longo do caminho a Figura 2.2.2-1mostra a seqüência completa de requisições de estabelecimento e encerramento da conexão.

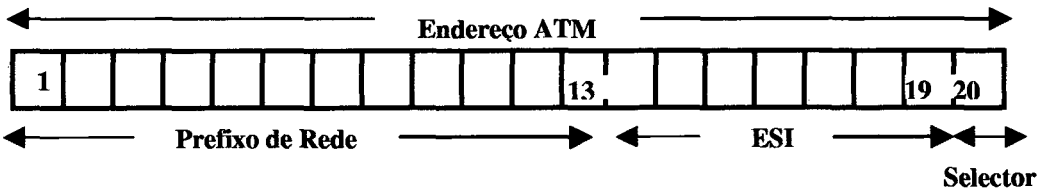
Figura 2.2.2-1 - Configuração e encerramento de uma conexão em uma rede ATM.



2.3. Endereçamento ATM

Seguindo o padrão sugerido pelo fornecedor dos equipamentos usados no presente estudo [IBM/99b], o endereçamento ATM utiliza 20 bytes hierárquicos, sendo os primeiros 13 *octetos* o prefixo de rede, que é fornecido pelo comutador aos sistemas finais aos quais está ligado, conforme Figura 2.3-1. Todos os comutadores pertencentes a uma mesma rede ATM tem o mesmo prefixo de rede.

Figura 2.3-1 - Endereço ATM



Os próximos 6 *bytes* são os identificadores de sistema final (*End System Identifier* - ESI) e o último *byte* é chamado de *selector* (selecionador). Os sistemas finais formam seus endereços pela concatenação de um *ESI* e do *selector* ao prefixo de rede fornecido pelo comutador. O *selector* somente é importante no sistema final, pois não é usado para roteamento no comutador ATM, mas é utilizado nos sistemas finais para identificar unicamente a origem e o destino de uma conexão .

O ESI é composto pelos *octetos* do 14 ao 19. Cada sistema final ligado a um mesmo comutador deve usar um grupo separado de ESIs. O campo ESI é especificado para ser igual ao endereço MAC nível 2, conforme definido pelo IEEE, isso facilita o uso de LANs.

O *selector* é o 20 *octeto* usado para multiplexação local nas estações finais, não possuindo significado algum para a rede. As estações finais obtêm prefixo de rede do comutador e do próprio endereço anexando ESI e *selector*. Estes endereços devem ser registrados no comutador, que rejeita o registro se o endereço ATM não for único.

2.4. Serviço de Segurança

Os procedimentos de segurança para redes ATM estão definidos pela especificação af-sec.0100.000 do ATM *Forum* [SEC100/99]. Este documento especifica mecanismos de autenticação, confidencialidade, integridade de dados, e controle de acesso para o plano de usuário. Também especifica mecanismos para autenticação e integridade para o plano de controle (sinalização UNI e NNI). Não faz parte do escopo desta especificação a segurança no plano de gerenciamento.

2.4.1. Serviços de Segurança no Plano de Usuário

São executados em um par de circuitos virtuais, onde um circuito pode ser qualquer conexão de canal virtual (VCC) ou uma conexão de caminho virtual (VPC). Serviços de segurança para ligações físicas não estão disponíveis na especificação [SEC100/99].

No plano de usuários são definidos os seguintes serviços de segurança que são suportados em conexões ponto-a-ponto e ponto-multiponto, tanto para conexões chaveadas ou permanentes (SVCs ou PVCs):

- **Autenticação** – é realizada no início da conexão, identificando se a origem e/ou destino da chamada é verdadeira. Desde que este serviço ofereça proteção contra disfarce ou *spoofing*, torna-se ideal para o estabelecimento de conexões seguras. Por essa razão, a autenticação é essencial à operação de outros serviços de segurança, incluindo troca de chaves e troca segura de parâmetros de negociação.
- **Confidencialidade** – utiliza recursos de criptografia para proteger dados de usuário em um VC contra acesso não-autorizado. A especificação define confidencialidade no ATM em nível de células, criptografando apenas a área de dados,

tornando desnecessário descriptografá-los nos pontos intermediários, uma vez que os campos do cabeçalho permanecem inalterados.

- **Integridade** – os serviços de integridade de dados provêem mecanismos que permitem detectar a modificação nos valores de dados ou seqüência de valores de dados. Até mesmo a presença de modificações maliciosas. Este serviço é oferecido entre as camadas ATM, AAL ¾ e ALL 5, dos pontos finais a nível de Unidade de Dados de Serviço (*Service Data Unit* – SDU).
- **Controle de Acesso** – é a aplicação de um grupo de regras para requerimento de um serviço. Essas regras podem depender dos atributos da entidade executada, tais como identidade, atributos de parâmetros de referência, um endereço designado, atributos de sistema, tempo, histórico, prioridade de serviço, ou outras entidades clientes.

2.4.2. Serviços de Segurança no Plano de Controle

O plano de controle é o mecanismo que permite dispositivos de configuração de rede alcançar alguns objetivos (por exemplo, estabelecer um circuito virtual comutado), desde que as mensagens do Plano de Controle possam afetar o estado e a disponibilidade da rede, sua proteção é extremamente importante.

Na especificação de segurança, é definido um mecanismo de sinalização que pode oferecer criptografia para integridade de dados com proteção *replay/reordering*. Este mecanismo permite às entidades do plano de controle ATM verificarem a origem e o conteúdo das mensagens de sinalização antes dos recursos serem alocados pelo requerente.

- **Autenticação e Integridade** – é o serviço de segurança ATM que associa uma mensagem de sinalização ATM à sua origem. Criando esta associação, o receptor da mensagem pode verificar confidencialmente se esta mensagem procede da origem confirmada. Este mecanismo minimiza o número de ameaças de confidencialidade, integridade e disponibilidade.

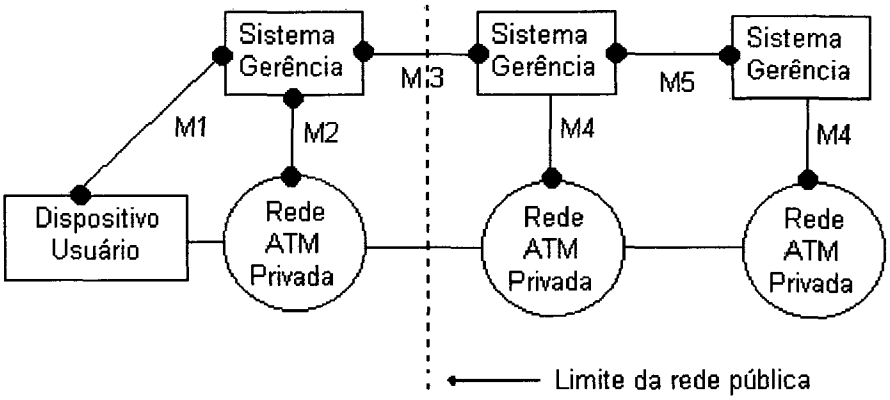
2.5. Gerenciamento de Redes ATM

O gerenciamento de redes ATM está baseado nas seguintes interfaces de gerenciamento, conforme Figura 2.5-1, Cerutti [CERUTTI/99], e Barbosa [BARB/00]:

- M1, necessária para realizar a gerência em um dispositivo ATM;

- M2, interface que atua entre a aplicação de gerenciamento e o dispositivo ATM (rede ATM privada);
- M3, permite que o usuário supervisione sua porção em uma rede pública ATM;
- M4, necessário no gerenciamento de uma rede pública ATM. Pois esta interface inclui as funções de gerenciamento de elementos de rede e serviços;
- M5, utilizada para gerenciar a interação entre dois sistemas de gerência de rede pública ATM.

Figura 2.5-1 - Modelo de gerenciamento de redes ATM



- Interface ILMI (*Interim Local Management Interface*), definido pelo ATM *Forum* (ATM UNI), é o protocolo local usado dentro de dispositivos ATM adjacentes para o gerenciamento do enlace e registro do endereço.

SNMP é o protocolo de gerenciamento usado através dessas interfaces:

- SNMP sobre UDP/IP na interface M2-*type*;
- SNMP sobre AAL5 nas interfaces ILMI e SSI.

Recursos que podem ser gerenciados incluem:

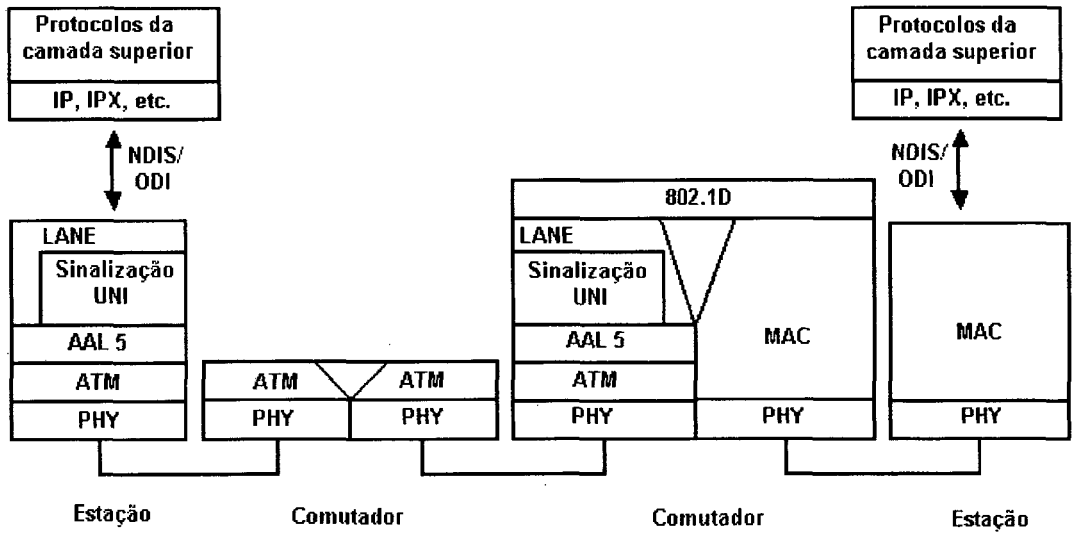
- Recursos Físicos
  - Interfaces ATM – são identificadas pelas variáveis SNMP (o *index* da MIB II);
  - As interfaces podem também serem reconhecidas diretamente pelos seus *slots* e número de portas;
  - Módulos ATM ;
  - Dispositivos ATM .
- Recursos Lógicos

- *Links* Virtuais - estão associados com a interface física e são identificados pelo valor VPI (*Virtual Permanent Link* -VPL) ou um valor VPI e VCI (VCL);
- Conexões Virtuais – devem ser PVCs ou *Switched Virtual Circuit* – SVCs.

3. LAN EMULATION

O ATM *Forum* iniciou o trabalho de especificação do LAN Emulation (LANE) em 1993, concluindo a primeira versão em 1995 [LANE21/95]. Tornando possível manter compatibilidade com os protocolos e redes comuns às redes locais já existentes. Foi determinada a emulação de redes locais no subnível MAC (parte da camada 2 do modelo OSI), por isso não há modificações nas aplicações. A Figura 2.5-2 mostra a arquitetura de protocolos LANE apresentada em camadas dos diferentes equipamentos representados pelas estações LAN e ATM e pelos equipamentos de interconexão (comutador e roteador) [DOWN/2000].

Figura 2.5-2 - Arquitetura de protocolos LANE.



O objetivo principal do serviço LANE é conseguir executar aplicações existentes em LANs no ATM, de forma transparente, bem como utilizar novas aplicações desenvolvidas para o ATM, como se estivesse executando em redes locais tradicionais (*Ethernet* ou *Token-Ring*).

Mesmo não explorando todos os benefícios do ATM, o LANE é útil na migração para a tecnologia ATM, por permitir que os investimentos em *software* e *hardware* sejam preservados.

O LANE é um serviço de conectividade de rede que permite aos sistemas finais conectarem-se a uma rede ATM como se fosse a uma LAN tradicional, conforme

características mostradas no Quadro III, que podem ser emuladas sobre o ATM usando o LANE [REINERT/97].

Quadro III – Características de rede locais tradicionais e emuladas.

LAN Tradicional	**LAN Emulada**
Segmento LAN (*Token-Ring* IEEE 802.3 e *Ethernet* IEEE 802.5)	Interconexão de ELAN e LANs tradicionais através de comutadores (ATM/LAN). Os segmentos ELAN e LAN interconectados formam um domínio *broadcast*.
Domínio *Broadcast* – Corresponde ao grupo de segmentos LAN interconectados através de *bridges* ou comutadores. Domínios *broadcast* são interconectados através de roteadores.	Domínio *broadcast* – (ELANs isoladas ou ELANs conectadas a LANs tradicionais por meio de *bridges* e comutadores). Domínios *broadcast* são interconectados através de servidores de *broadcast*.

O artigo de Alles [ALLES/95] apresenta os principais componentes do serviço LANE, descrevendo suas funções básicas:

Servidores

LES (*LAN Emulation Server)* – fornece um ponto de controle central para os LECs encaminharem informações de registro e de controle;

BUS (*Broadcast and Unknow Server*) – Servidor de *multicast* utilizado para o fluxo de tráfego de endereços de destino desconhecido e para o encaminhamento de tráfego de *broadcast* e de *multicast* aos clientes em uma determinada ELAN. Sendo que cada LEC está associado a somente a um BUS por ELAN;

LECS (LAN *Emulation Configuration Server)* – o LECS mantém um banco de dados de LECs e das ELANs às quais os LECs pertencem. Esse servidor aceita consultas realizadas pelos LECs e responde com o identificador de ELAN apropriado, isto é, o endereço ATM do LES que serve a ELAN apropriada. Um LECS por domínio administrativo serve a todas as ELANs existentes nesse domínio.

Clientes

LEC (LAN *Emulation Client*) – é uma entidade em um sistema final, que executa o encaminhamento de dados, a resolução de endereços e o registro de endereços MAC com o servidor de emulação de LAN (LES). O LEC também fornece uma interface

padrão de LAN para os protocolos de nível superior em LANs tradicionais. Um sistema final ATM conectado a várias ELANs terá um LEC por ELAN.

Proxy LEC (*Proxy* LAN *Emulation Client*) – permite às estações LANs tradicionais participarem de uma determinada ELAN (*bridge* e comutadores ATM/LAN).

Um dispositivo ATM pode implementar qualquer número de instâncias:
Somente um dispositivo implementa o LECS, exceto quando tiver a finalidade de *backup;*

Um ou mais dispositivos implementam o LES e o BUS;

Dispositivos de borda (ATM/LAN *bridges* ou comutadores) implementam uma ou várias instâncias de LEC *proxy;*

Roteadores e estações de trabalho LANE ATM implementam uma ou várias instâncias de LEC.

3.1. Endereço ATM dos Componentes LANE

Os endereços ATM devem ser únicos entre os componentes LANE. Porém, os servidores LES e BUS da mesma ELAN podem compartilhar um endereço ATM. Esses números geralmente serão diferentes do endereço ATM do LECS, devido à atualização do seletor para cada instância.

Componentes LANE são configurados por uma interface ATM particular. Pode optar-se pelo uso do endereço MAC (disponível no equipamento) como valor ESI, veja o formato do endereçamento ATM no item 2.3.

3.2. Função do LECS

O uso do LECS é opcional na configuração do LEC. Embora seja recomendado, se o LECS não for usado, cada componente LANE deve ser configurado com o endereço ATM do LES da ELAN. O uso do LECS reduz o gerenciamento da rede, pois este serve como um repositório centralizado para dados de configuração, minimizando a configuração dos LECs.

A conexão dos LECs ao LECS utiliza procedimentos bem definidos. O LEC segue os seguintes passos, respectivamente até que seja estabelecida uma conexão de canal virtual (VCC):

1. Conectar o LECS usando qualquer informação do endereço LECS configurado;
2. Obter uma lista de endereços LECS usando ILMI e tentar conectar-se em cada lista, até que um VCC seja estabelecido;
3. Estabelecer um VCC bem conhecido para um endereço ATM, definido pelo ATM *Forum.*

O ILMI é o método preferido dos LECs para localização do LECS [IBM/99b]. O endereço LECS bem conhecido é requisitado, mas o método ILMI não é suportado por todos os comutadores ATM. A configuração do endereço LECS nos LECs faz-se necessário somente quando o método ILMI não for suportado pelo comutador ATM e o endereço LECS bem conhecido não for suportado pelo serviço LANE.

O LECS deve disponibilizar os dados iniciais de configuração para o LECs, sendo o endereço ATM do LES mais importante do que o endereço ATM no serviço LANE. Para disponibilizar as informações do LEC, o LECS deve ser capaz de identificar o LEC e determinar o LES adequado ao LEC. O LECS identifica o LEC usando informações do *frame* de requisição de configuração no LEC. A requisição da configuração pode conter as seguintes informações para identificar a ELAN que o LEC está tentando conectar:

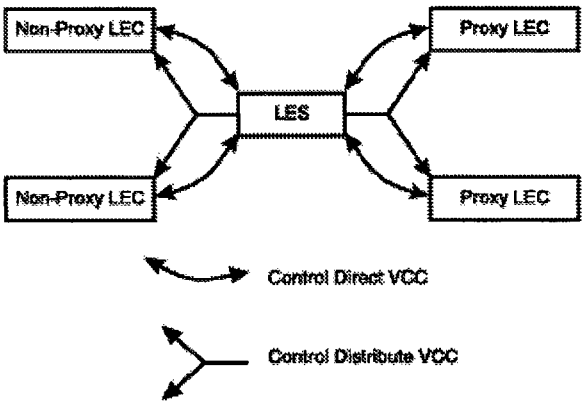
1. Endereço ATM primário do LEC – identifica unicamente o LEC;
2. LAN *destination* associada com o LEC – este campo pode conter o endereço MAC ou um descritor de rota que identifica o LEC, ou pode não ser especificado;
3. Nome da ELAN – nome que indica a ELAN ou requisição LEC;
4. Tipo da ELAN - especifica se o LEC pertence a uma ELAN *Ethernet* ou *Token-Ring* ou pode ser não especificado;
5. Tamanho Máximo do *Frame* – especifica o tamanho máximo do *frame* de dados que pode ser processado pelo LEC, ou pode ser não especificado. O LECS não pode determinar LECs para uma ELAN com o tamanho máximo de *frame* maior que o especificado pelo o LEC. Se a ELAN permitir tamanho de *frames* maiores do que o LEC possa manipular, o LEC não pode funcionar na ELAN.

3.3. Conexão LEC - LES

A Figura 3.3-1mostra as conexões feitas pelo LEC após obter o endereço ATM do LES. O LEC inicializa um *Control Direct* VCC para o LES. Quando este VCC for

estabelecido, o LEC envia uma requisição de conexão para o LES, que responde adicionando o *Control Distribute* VCC (ponto a multiponto) e retorna uma resposta de conexão. Por *default* o LES particiona clientes *proxy* e não *proxy* em *Control Distribute* VCCs separados [IBM/99a].

Figura 3.3-1 - Conexão *default* entre LECs e o LES



No entanto o LES pode ser configurado para usar um único *Control Distribute* VCC para todos os LECs e reduzir o número de VCCs ponto a multiponto requeridos. O particionamento dos VCCs é usado para reduzir a quantidade de tráfego excedente enviado aos clientes não *proxy*, nenhuma requisição ARP é enviada para clientes não *proxy*.

3.3.1. Registro de endereços

Os LECs registram as LANs de destino com o LES para garantir exclusividade e permitir ao LES responder ao pedido do protocolo de resolução de endereço do LANE (LE_ARP_*REQUESTS*), no qual o LECS aprende o endereço ATM associado com o destino de uma LAN particular [IBM/99b].

O registro inclui LAN destino e endereço ATM que o LEC associa. A LAN destino pode ser um endereço MAC ou um descritor de rota. LECs *proxy* não registram o endereço MAC das estações em segmentos LAN que não estejam repassando para a ELAN. LECs não *proxy* devem registrar as LANs destino que representam, e todos os descritores de rota devem ser registrados, sem considerar se estão associados com um LEC *proxy* ou não *proxy*. Descritores de rota são aplicáveis apenas para *LECs* proxy que executam o repasse de rota. Um descritor de rota contém o número de *bridge* do

LEC *proxy* e o número do segmento de um anel do LEC que está sendo repassado, isto é equivalente a uma volta.

3.3.2. Resolução de endereços

Comunicação em LANs é baseado no endereço MAC de origem e destino. Na comunicação LAN/ATM é necessário resolver o endereço MAC para endereço ATM [IBM/99b].

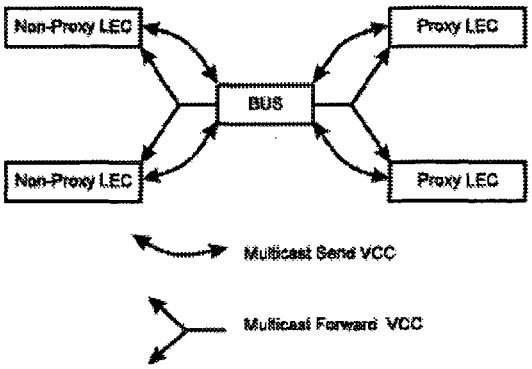
O LEC envia um LE_ARP_*REQUESTS* para o LES aprender o endereço ATM de uma LAN destino particular. Se a LAN destino estiver registrada, o LES responde com o endereço ATM associado com a LAN destino. Caso contrário a requisição é reenviada para todos os LECs *proxy* do *Control Distribute* VCC. Não é necessário enviar a requisição para os LECs não *proxy*, porque suas LANs de destino são registradas. No entanto, se o LES estiver configurado para usar um *Control Distribute* VCC simples, os LECs *proxy* e não *proxy* receberão a requisição. O *Control Distribute* VCC dispõe de uma maneira eficiente para o LES distribuir *frames* de controle para múltiplos LECs.

Os LECs *proxy* respondem ao LE_ARP_*REQUESTS* de endereços MAC não registrados. O LE_ARP_*REQUEST* é enviado pelo LES no *Control Distribute* VCC, e o LES repassa a resposta.

3.4. Conexão LEC - BUS

A Figura 3.4-1 mostra as conexões feitas pelo LEC após obter o endereço ATM do LES [IBM/99b]. O LEC emite um LE_ARP_*REQUEST* para todos os primeiros endereços MAC *broadcast*. O LES responde com o endereço ATM do BUS, então o LEC inicia o estabelecimento do *Multicast Send* VCC do BUS, o qual responde adicionando no LEC o *Multicast Forward* VCC ponto-a-ponto. Por *default* o BUS particiona os LECs *proxy* e não *proxy* em *Multicast Forward* VCCs separados. No entanto, no caso do *Control Distribute* VCC, o BUS pode ser configurado para o uso de um *Multicast Forward* VCC simples.

Figura 3.4-1 - Conexão *default* entre LECs e o BUS



3.4.1. Função do BUS

O BUS tem duas funções básicas que são [IBM/99b]:

1. Distribuir *frames multicast* para todos os LECs na ELAN;
2. Repassar *frames unicast* para o destino apropriado.

Um LEC envia *frames unicast* para o BUS, caso este não tenha conexão direta com o LEC destino correspondente. Para evitar gargalos no BUS, a taxa de *frame unicast* que o LEC pode enviar para o mesmo é limitada.

Se particionar o Domínio *frame unicast*, o BUS usará dois *Multicast Forward* VCCs. Caso contrário, o BUS usará um *Multicast Forward* VCCs simples.

Se um *Multicast Forward* VCCs simples é usado, todos os *frames* recebidos serão reenviados a todos os LECs. Neste caso, *frames unicast* destinados para LECs não *proxy* são transmitidos diretamente para o LEC destino em um *Multicast Forward* VCC, e os outros *frames unicast* são transmitidos apenas para LECs *proxy* usando o *proxy Multicast Forward* VCC. Quando são usados dois *Multicast Forward* VCC, o *Multiprotocol Switch Service* - MSS é considerado um BUS inteligente (IBUS).

O modo IBUS reduz *frames unicast* redundantes, e quando estes não são destinados aos clientes: os clientes *proxy* não recebem *frames unicast* destinados a clientes não *proxy,* e estes não recebem *frames unicast* redundantes. Porém, o processamento aumenta os *frames multicast* que serão transmitidos duas vezes (um em cada *Multicast Forward* VCC). Geralmente, a operação IBUS é recomendada, no entanto essa opção deve ser desabilitada em configurações com origem em roteadores de rotas não *proxy* que ligam a ELAN.

3.5. Funções da ELAN

Conforme Laurent [LAUREN/96], antes de qualquer transmissão de dados através da rede ATM, os LECs (estações de trabalho, repetidores, roteadores) devem-se conectar sucessivamente aos servidores LANE que são: LECS, LES e BUS, respectivamente para obter sucesso na conexão de uma ELAN. Em particular, os LECs têm que registrar todos os seus endereços MAC alcançáveis.

Se o LEC for uma estação ATM, será necessário registrar apenas um par de endereços (endereço ATM e endereço MAC), mas se o LEC for um roteador ou um repetidor, terá tantos endereços MAC para serem registrados quanto o número de estações conectadas à LAN.

Após completar a fase de inicialização, os LECs conseguem comunicar através da rede ATM. No primeiro caso (1) dados são enviados para uma estação final específica, e no segundo caso (2) realiza-se *broadcast* de dados para múltiplas estações finais. As duas alternativas são descritas a seguir:

1. Considerando que o LEC origem (LEC_o) com o endereço MAC (MAC_o) desejam transmitir dados para um LEC destino (LEC_d). Todas as operações implementadas por essa transferência de dados são executadas pelo LEC_o na camada LANE. Se a camada conhece o endereço ATM do LEC_d, configura-se uma conexão direta para o LEC_d ou reusa uma conexão aberta anteriormente. Caso contrário, envia um LE-ARP *request* para o LES, informando o endereço ATM do seu LEC_d, e então configura uma conexão direta para o LEC_d. A alternativa é repassar todos os dados para o BUS, que os redirecionará para LEC_d se conhecer o endereço ATM ou para todos cujo LECs registrados. De qualquer modo, os dados serão recuperados pelo LEC_d. A transferência por meio de roteadores e repetidores (veja) depende se a transferência de dados é originada de uma estação ATM ou uma estação LAN. Desde que a rede ATM considere repetidores e roteadores como LECs pelos quais muitas estações LAN podem ser alcançadas, bem como que as LANs sejam consideradas como elementos de rede normais, os roteadores e repetidores têm que realizar além de suas funções clássicas, funções de adaptações (resolução de endereços ATM/MAC e adaptação de células/*frames*) que são processadas atualmente por suas camadas da instância LANE. É importante observar que a transferência de dados através de um repetidor requer somente uma resolução de

endereço (ATM/MAC), enquanto que transferência de dados através de um roteador requer duas resoluções de endereços (MAC/rede, tipicamente IP), normalmente executado pelo roteador e a resolução do endereço ATM/MAC requerido pela instância LANE.

2. Se um LEC precisar difundir os dados, sua instância LANE transmite estes dados para o BUS, que torna a repassá-los para os LECs.

3.6. Gerenciamento de Servidores LANE

A seguir são listadas as especificações do ATM *Forum* (ATM *Forum Technical Committee*) relacionadas com a descrição e gerenciamento do serviço LANE:

- LAN *Emulation Over* ATM na especificação af-lane-0021.000 [LANE21/95], descreve o serviço de LANE.
- LAN *Emulation Servers Management Specification* 1.0 af-lane-0057.000 [LANE57/96], descreve o gerenciamento dos servidores LANE.
- LAN *Emulation over* ATM *Version* 2 – LAN *Emulation Network to Network Interface* (LNNI), *Specification* af-lane-0112.000, [AFLANE/99] descreve a interface de interconexão de redes.

A especificação do gerenciamento dos servidores LANE [LANE57/96], descreve o modelo de gerenciamento em três módulos MIB:

1. ELAN.MIB - gerencia as mudanças de configuração das ELAN através de um repositório de informações estáticas;
2. LES.MIB - gerencia o serviço de resolução de endereço e fornece informações estatísticas das conexões dos LECs;
3. BUS.MIB - gerencia o tráfego entre as instâncias e fornece informações estatísticas do desempenho de cada instância LANE.

Essa especificação cobre as seguintes áreas de gerenciamento: Configuração, Desempenho e Falhas; e não são contempladas as áreas de Segurança e Contabilização. No Anexo 1 são descritas as tabelas e variáveis de interesse desta especificação.

4. SEGURANÇA LANE

Vários autores mencionados por Jain [JAIN/97] afirmam que o ATM, bem como outras redes, sofre muitas ameaças tais como: escuta, *spoofing*, negação de serviço, roubo de conexão virtual e análise de tráfego. Sendo que conexão virtual e análise de tráfego ocorrem apenas nas redes ATM.

Neste item estão apresentados as ameaças ao serviço LANE mostrando os pontos susceptíveis a ataques nos diferentes componentes do serviço, bem como são descritas as políticas de segurança definidas pelo ATM *Forum* e implementada pelo fornecedor do equipamento.

4.1. Categorias de Ameaças

De acordo com Laurent [LAUREN/96] as especificações do serviço LANE possuem poucas características de segurança para conexões ELANs. Uma delas é a própria topologia da rede ATM, que não permite difundir *frames unicast* nas ELANs; sendo estes enviados para à estação final de destino. Outra característica é a autenticação física da chamada da estação de origem, que é executada na entrada do comutador. Esta autenticação consiste na verificação da consistência entre o endereço ATM solicitado e a porta de entrada do comutador aonde chega a requisição.

Considerando, que a proteção permanece limitada e raramente é implementada, as comunicações nas ELANs são vulneráveis para vários tipos de ameaças. A autora mencionada descreve três categorias clássicas de ameaças à segurança das ELANs: confidencialidade, integridade e disponibilidade.

4.1.1. Confidencialidade

Um ataque sobre confidencialidade ocorre quando o intruso conhece a informação em trânsito. Neste caso há três possibilidades: desvio de conexão, conexão espiã e conexão imprópria.

- **Desvio de Conexão**

Este ataque consiste no desvio de tráfego à estação espiã. Assim, o espião pode capturar os dados de interesse e deduzir o conteúdo. Há duas maneiras de realizar um

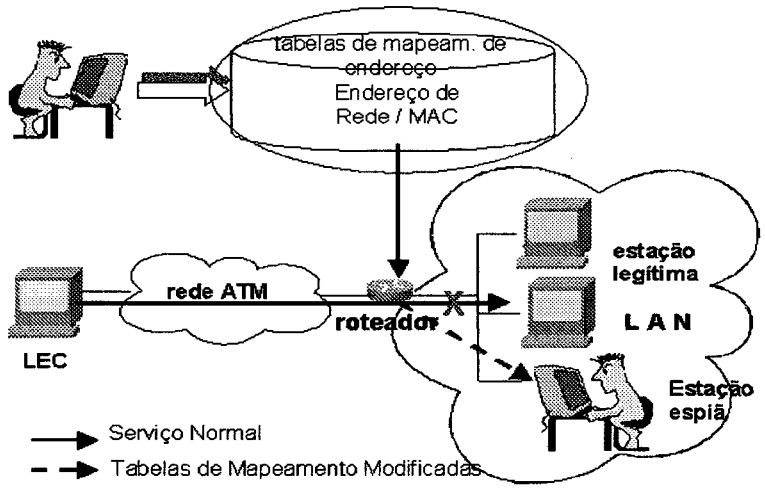
ataque de desvio de conexão, antes da conexão ser configurada ou após a conexão ser configurada, dependendo de onde seja efetuado o ataque.

- **Desvio da conexão depois de ser configurada**

Para realizar este ataque, um método radical é substituir a estação verdadeira por uma estação espiã, para fazer posterior apropriação de todo o tráfego, inicialmente enviado a estação verdadeira. Para obter êxito, o atacante deve cortar o cabo ou desconectá-lo da estação legítima.

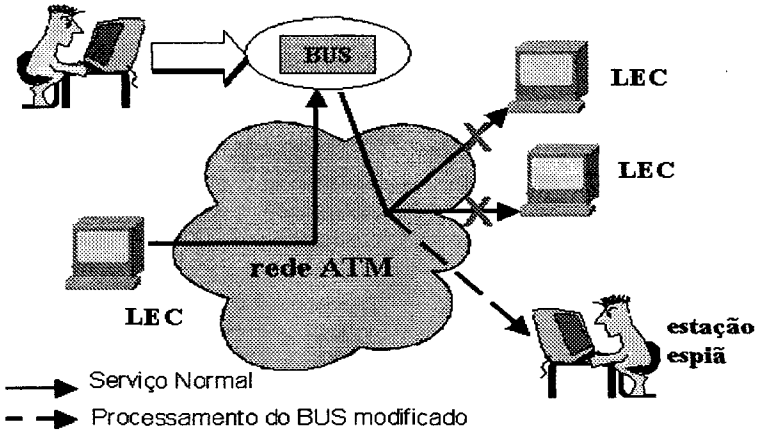
O atacante também pode realizar um desvio de conexão semelhante, modificando nos comutadores ou roteadores ATM a informação usada para rotear o tráfego através da rede. Nos comutadores ATM, isso consiste na modificação das tabelas de mapeamento VPI/VCI. Nos roteadores este ataque consiste na modificação da tabela de resolução de endereços (endereço MAC/endereço de rede). A Figura 4.1-1 mostra o fluxo do tráfego quando ocorre alteração na tabela de roteamento. Neste caso o tráfego inicialmente enviado à estação legítima é redirecionado para uma estação espiã, sem que a estação legítima perceba.

Figura 4.1-1 Ameaça de desvio da conexão depois de ser configurada, através de alteração da tabela de roteamento .



Outra alternativa para desviar a conexão após a configuração requer suporte de administrador para modificar o processamento do servidor do BUS. Deste modo parte ou todo o tráfego enviado através do BUS é redirecionado para qualquer estação espiã pertencente ou não a mesma ELAN, conforme mostra a Figura 4.1-2.

Figura 4.1-2 - Ameaça de desvio da conexão depois de ser configurada, através de alteração do processamento do BUS.

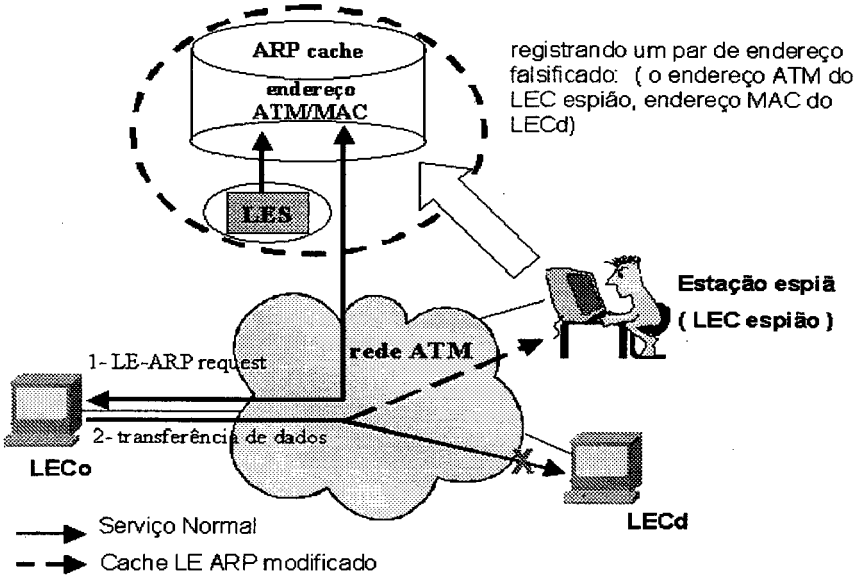


- **Desvio da conexão antes de ser configurada**

Existem dois métodos para realizar o desvio da conexão antes que seja efetivada a configuração. O primeiro método é modificar o processamento do LEC (microprograma) ou carregar um microprograma falsificado de modo que, cada vez que o LEC precisar conectar-se com uma estação destino ($estação_d$), o microprograma troca na mensagem de inicialização o endereço ATM da $estação_d$, com o endereço ATM associado a uma estação espiã. Assim, como resultado deste ataque, quando o LEC precisar comunicar com estação destino, uma conexão será iniciada (entre o LEC e a estação espiã) e desde então o LEC acredita estar conectado a estação destino. Todo o tráfego enviado para a estação destino é desviado para a estação espiã.

No segundo método, o atacante em um LEC espião engana o LES, levando-o a acreditar que esse LEC representa uma subrede, com qualquer endereço ATM que desejar. Então registra no LES, além do próprio par de endereços (ATM-MAC), alguns outros pares de endereços ATM adicionais. Como mostra na Figura 4.1-3 o par de endereços (ATM do LEC espião; o endereço MAC de uma estação existente, denominada LEC_d) são registrados e se necessário apagando no LES o par de endereços da estação legítima (o endereço ATM do LEC_d; o endereço MAC do LEC_d). Quando o LEC_o enviar uma requisição de comunicação com o LEC_d, o LES retornará o endereço ATM alterado. Estabelecida a conexão direta do LEC_o com o LEC espião ao invés do LEC_d os dados serão enviados.

Figura 4.1-3 - Ameaça de conexão espiã através da alteração do processamento do BUS para duplicar conexões.



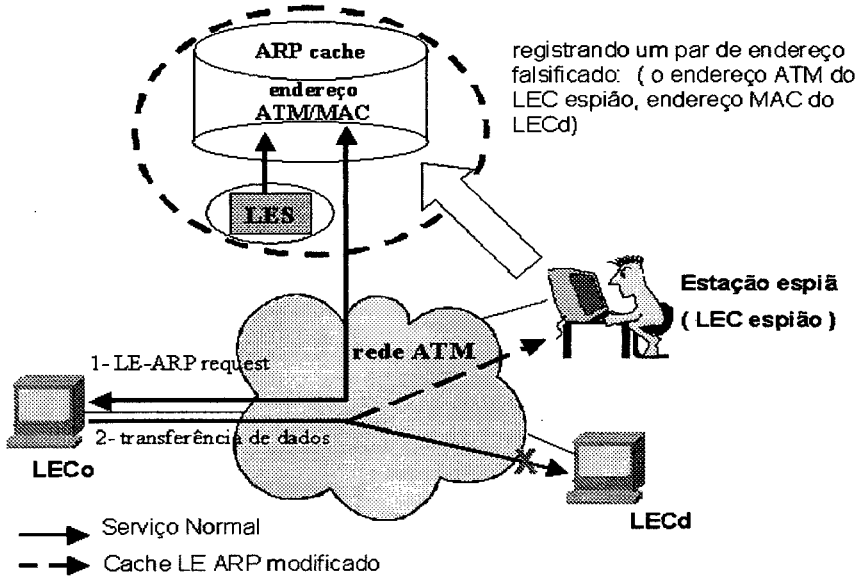
- **Conexão espiã**

Este ataque assume que um intruso se posicione em um ponto da rede para observar o tráfego e capturar células ATM com propósitos específicos (com o mesmo VPI/VCI), de forma que os conteúdos das mensagens possam ser deduzidos.

Outro ataque resulta, diretamente do fato que ELANs emulam aplicações de comunicação LANs e essas aplicações são inseguras. Considerando a difusão de pacotes, um atacante pode escutar todo ou parte do tráfego *broadcast* usando filtros apropriados em uma estação (estação ATM, roteador ou repetidor). No contexto LANs, espionagem se aplica a todo o tráfego que passa através das LANs, no contexto ELANs, isso é limitado pelo tráfego *broadcast/multicast/unicast* transmitido para o BUS.

Outra solução é modificar o processamento do BUS, quando inicializado, se necessário, algumas conexões adicionais à estação espiã e então duplicar todo ou parte do tráfego que passa através do BUS para a estação espiã, conforme mostra aFigura 4.1-4.

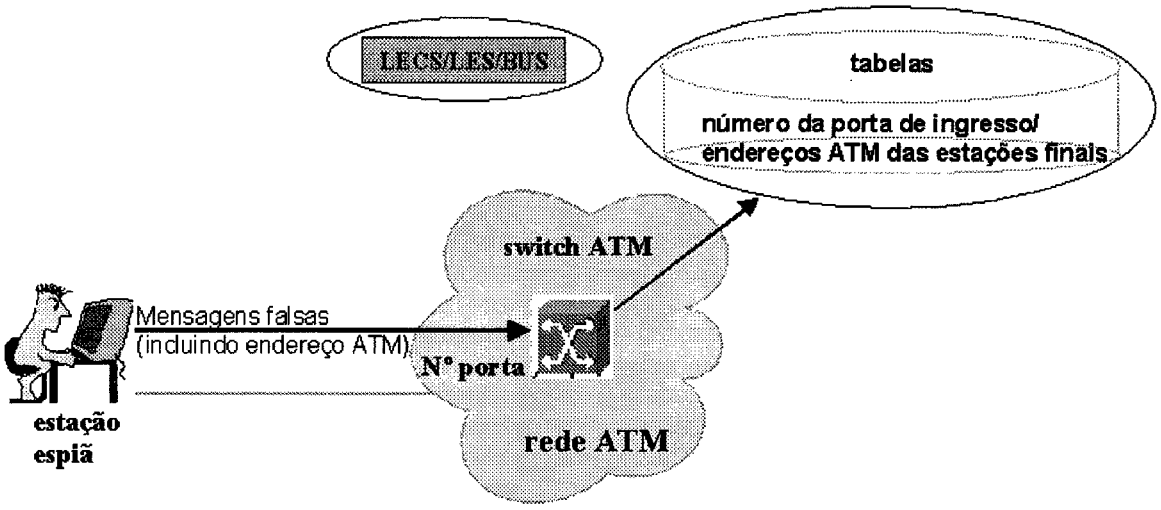
Figura 4.1-4 - Ameaça de conexão espiã através da alteração do processamento do BUS para duplicar conexões.



- **Conexão imprópria**

Uma conexão imprópria ocorre quando o atacante em uma estação (LAN ou LEC), consegue se conectar a uma ELAN na qual este não está autorizado, se passando por uma estação autorizada nos servidores LECS, LES, e BUS. Essa conexão ilegal é bastante atrativa para o atacante, que pode receber tráfego *broadcast* da ELAN e também se conectar a qualquer LEC, restaurando primeiro o endereço ATM do LEC, a partir do LES. Este ataque consiste em emitir diretamente algumas mensagens falsas na rede, sem afetar a integridade dos dados transmitidos, podendo partir de uma ELAN ou LAN. A Figura 4.1-5 mostra uma estação espiã enviando mensagens falsas para uma rede ATM, a qual esta tentando se conectar.

Figura 4.1-5 - Ameaça de conexão imprópria através de mensagens falsas enviadas para uma rede ATM.



4.1.2. Integridade

Um ataque em integridade ocorre quando o atacante consegue injetar, modificar ou apagar informações em trânsito. Deve ser observado mesmo se a maioria dos ataques de integridade resultam em revelação de informação, ataques sobre integridade não devem ser confundidos com ataques em confidencialidade, pois no ataque sobre confidencialidade é passivo não afetando a integridade dos dados em trânsito. Os três tipos de ameaças de integridade são mascaramento: (1) durante a configuração da conexão, (2) com conexão configurada e (3) injeção de dados.

1- Mascaramento durante a configuração da conexão

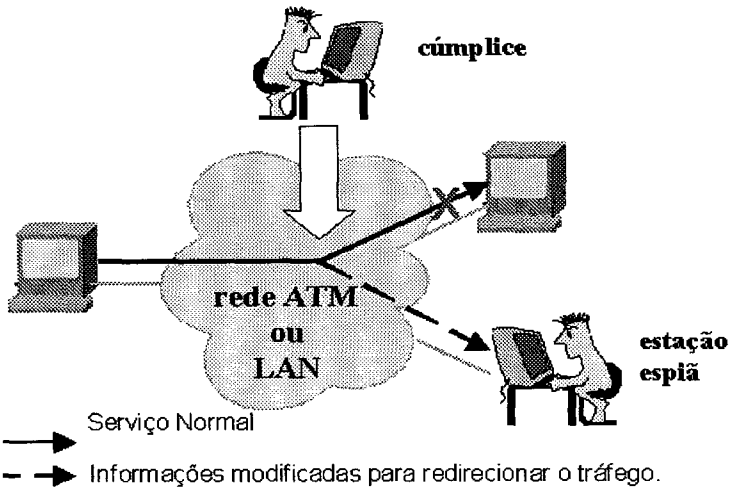
Este ataque assume que duas partes desejam comunicar. O ataque consiste em modificar as mensagens de sinalização em trânsito, quando apropriado, de modo a forçar a conexão a ser configurada entre uma estação maliciosa e uma das duas partes. Este ataque é conhecido como um mascaramento desde que a parte que permaneça conectada a estação maliciosa acredite que esteja conectada a outra parte.

2- Mascaramento com conexão configurada

Este ataque assume que uma conexão já esteja configurada entre duas partes. O atacante então se mascara como uma das partes. Como mostrado na Figura 4.1.2-1, um cúmplice do atacante está em um ponto da rede LAN ou ATM, modifica a informação

em trânsito de modo que todo ou parte dos dados em trânsito seja redirecionado à estação espiã.

Figura 4.1.2-1 - Mascaramento após a conexão ter sido configurada: modificações apropriadas das informações trocadas sobre a rede, faz com que o tráfego seja redirecionado para a estação espiã.

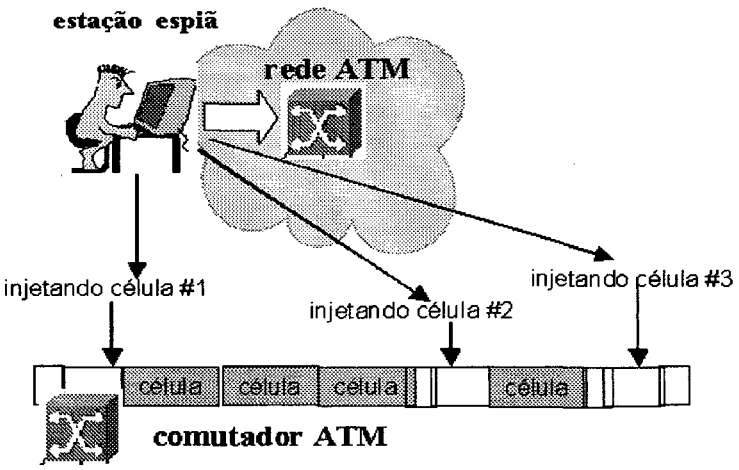


1. Injeção de Dados

Este ataque consiste na inserção de alguns dados de usuários (células ATM) sobre uma conexão em processo. Isso visa atrapalhar a conexão, especialmente enganando a estação de destino, uma vez que a maior parte das células injetadas é detectada pelas camadas superiores das estações finais de destino e o processamento de detecção consome tempo.

Na rede ATM (um atacante se posiciona em um comutador ATM ou no meio de transmissão). Como mostra a Figura 4.1.2-2, o ataque é efetuado através da inserção de algumas células ATM com os mesmos identificadores VPI/VCI e com objetivo de atrapalhar a conexão sem apagar nenhuma célula legítima.

Figura 4.1.2-2 - Ameaça de injeção de dados em um comutador ATM modificando o fluxo de células sem apagar as células legítimas.



4.1.3. Disponibilidade

Um ataque em disponibilidade, usualmente denominado serviço negado, consiste em tornar os recursos da rede indisponíveis aos usuários autorizados.

Acessos não autorizados e repetitivos

Este ataque ocorre quando um intruso tenta repetidamente acessar um servidor LANE para conectar-se na ELAN. Dessa forma, o atacante pode causar uma sobrecarga no recurso do terminal, tornando indisponíveis para outros usuários por muito tempo. Também pode comprometer seriamente a rede ATM desde que todo o tráfego ELAN seja UBR ou ABR, tendo em vista que todas as conexões ELAN compartilham os recursos da rede (por exemplo: largura de banda).

Obstrução de comutadores ATM, roteadores ou repetidores .

Este ataque consiste em sobrecarregar um comutador ATM, roteador ou repetidor devido ao envio de informações falsificadas (endereço de destino) que romperá as atividades ou impedirá de processar o legítimo tráfego de entrada.

Um comutador ATM pode ser atrapalhado por mensagens de entrada de conexão falsas (com um endereço de destino ATM falsificado), que causa no comutador ATM desperdício de tempo consultando as tabelas de roteamento em vão. Este ataque pode ser gerenciado a partir de uma estação LEC, qualquer servidor ELAN (repetidor, roteador, comutador ATM ou o meio de transmissão), o mais provável é a estação LEC.

4.2. Atributos de Segurança

Conforme recomendações do fornecedor IBM [IBM/99b], LANs tradicionais oferecem segurança pois a conexão física garante que duas máquinas estejam fisicamente na mesma rede. Mesmo não estando conectadas fisicamente duas máquinas podem pertencer a uma mesma ELAN, porque várias redes emuladas podem coexistir em uma única rede ATM. Esta situação apresenta risco de segurança, uma vez que estações sem autorização possam conectar-se ao LES e tentar usar os serviços de rede.

Para controlar os membros da ELANs, o LES pode ser configurado para validar solicitações de pedido de registro do LANE (LE_*JOIN_REQUESTs*) com o LECS. Deste modo, o LES forma o pedido de configuração do LANE (LE_*CONFIGURE_REQUEST*) como representante do LEC, usando informações do LE_*JOIN_REQUEST*.

As requisições LE_*CONFIGURE_REQUESTs* incluem o código da LAN destino, código do endereço do ATM, tipo da ELAN, tamanho máximo de *frame* e nome da ELAN do LE_*JOIN_REQUEST*, junto com a segurança proprietária IBM, denominada *type lengthy value* (TLV). O pedido de segurança será transmitido ao LECS por um componente de multiplexação chamado de interface LECS, o qual deve validar o pedido usando a base de dados da sessão ELAN, antes de permitir que LECs sejam anexados a ELAN.

Uma interface LECS está associada a uma interface ATM, e todos os LESs configurados sobre o ATM usam a mesma interface LECS. As interfaces LECS preservam recursos VCC para multiplexação de pedidos de segurança de múltiplos LESs sobre um único VCC para o LECS.

A interface LECS localiza o LECS dinamicamente usando o *Integrated Local Management Interface* (ILMI) e mecanismos de endereçamento LECS conhecido. Após estabelecer o VCC para o LECS, a interface LECS realiza uma consulta local para determinar se o LECS está localizado no mesmo servidor. Se estiver, uma interface local será usada para confirmar a requisição e anexá-lo sem transmitir sobre a rede ATM.

Com a interface LECS, o servidor pode assegurar que um LEC conecta-se a uma ELAN somente se o LECS aprovar a conexão. Isto transfere a responsabilidade da segurança do LES para o LECS. Infelizmente, o LECS também não é seguro, porque

aceita conexões e consultas de qualquer estação sem verificação. Uma estação intrusa pode se conectar ao LECS e realizar consultas, repetidamente de suas várias configurações. O intruso também pode se passar por outra estação e baixar configurações de outras estações.

O controle de acesso do LECS permite ao usuário configurar uma lista de prefixos de endereços ATM os quais não terão permissão para acessar a base de dados de configuração do LECS. Todas as tentativas de conexão LECS e LE_*CONFIGURE_REQUESTs* compatíveis com os endereços ATM são automaticamente rejeitados. E quando usados em conjunto com a interface LECS, um ambiente de LAN segura é disponibilizado.

4.2.1. Maximização da segurança de ELAN

Estes passos asseguram que as estações sejam identificadas corretamente e que apenas estações autorizadas consigam conectar-se a ELAN:

1. O uso de endereços ATM pelo LECS para designar LECs para os LES;
2. Ativar a interface LECS no servidor MSS;
3. Ativar a opção de segurança no LESs;
4. Utilizar filtros de endereços nos comutadores ATM. Esta opção provoca a validação das chamadas das estações a utilizar os atuais endereços ATM das mesmas em sua configuração, não podendo assim, ser clonada para outras estações.

4.3. POLÍTICAS DE SEGURANÇA

Política é um critério que o LECS utiliza para definir LEC para LES. O valor de política é um par (valor, LES) que determina qual o valor será definido para especificar o LEC.

De acordo com a especificação de gerenciamento dos Servidores LANE [LANE57/96], as políticas de determinação do LEC são:

1. Endereço ATM;
2. Endereço MAC;
3. Descritores de Rota;
4. Tipo da ELAN;
5. Tamanho Máximo do *Frame*;
6. Nome da ELAN.

O LECS examina as políticas de acordo com a prioridade. Políticas com baixa prioridade são consideradas primeiro do que as de maior prioridade, e simultaneamente quando as prioridades forem iguais. Assim, o LECS define um LEC para um LES, quando todas as políticas e seus respectivos níveis de prioridade forem satisfeitos e aceitas. Políticas são satisfeitas quando um valor de prioridade da política conferir com o campo correspondente na requisição de configuração de cada política no atual nível de prioridade. E as políticas são aceitas quando os conjuntos de conferências incluem o LES que é comum a todas as políticas. Se essas condições não forem encontradas, o LECS considera as políticas no próximo nível. Se o LECS for incapaz de encontrar o LES em qualquer nível de prioridade, retorna para o LEC uma mensagem de resposta de configuração não completada.

Conforme o Quadro IV, se o LEC fornece um endereço MAC = X400000121225 e ELAN = ELAN_1 as políticas são satisfeitas, mas não aceitas, porque diferem nos LESs.

Quadro IV – Exemplo da configuração da política MAC.

Exemplos de políticas	
MAC, LES_A	X400000121225, LES_A
ELAN, LES_B	ELAN_1, LES_B

Após determinar o LES correto para um LEC, o LECS retorna uma resposta de configuração incluindo as seguintes informações: Endereço ATM do LES, Tipo da ELAN, Tamanho Máximo do *Frame* e Nome da ELAN. A resposta de configuração também pode incluir parâmetros de *Type*, *Length*, e *Value* (TLV). Os parâmetros TLV oferecem um método de *download* opcional ou parâmetros definidos pelo o usuário para o LEC.

4.3.1. Política de endereço ATM

O LECS permite dois tipos de valores de políticas de endereçamento ATM. O primeiro tipo de valor é uma variável com prefixo do endereço ATM extenso. Por exemplo, o valor da política (39999999999999000000102,LES_A) significa que todos os LECs, cujo endereço ATM inicia com 3999999999999900000102 devem ser sinalizado para o LES_A .

O segundo tipo de valor de endereçamento ATM é um identificador de sistemas finais (ESI) e selecionador de endereço ATM. Por exemplo, o valor da política (10002345003281,LES_A) significa que o LEC utilizando um ESI de 100023450032 e um selecionador 81 deve ser designado para o LES_A.

Quando um determinado endereço ATM de um LEC, o LECS procura primeiro por um selecionador e ESI igual. Se não encontrar é retornado, o LECS procura pelo valor do prefixo do endereço ATM longo.

O endereço ATM ESI e o selecionador de valores de políticas podem ser usados para atribuir clientes para os LESs de maneira independente da localização física do LEC (o ESI e o selecionador estão definidos localmente para o cliente). Prefixo de endereços ATM são apenas valores de políticas, que indicam qualquer informação geográfica.

4.3.2. Política de destino de LAN

LECs podem ser atribuídos para o LESs baseado no endereço MAC ou descrição de rota, porque somente a LAN destino identifica o LEC de uma maneira independente da localização geográfica, essa política é útil por assegurar que o LEC seja atribuído a LAN correta independente da localização física. Por exemplo, retendo os membros da ELAN de uma estação de trabalho quando movendo de um comutador para outro.

4.3.3. Política por nome da ELAN

A política nome de ELAN é o critério de atribuição mais flexível. Alguns valores possíveis para esta política são:

Uso do nome atual da ELAN

Se o LES_A servir a ELAN 1, cria-se o valor de política. O LEC especifica a ELAN 1 no pedido de configuração poderá ser atribuído no LES_A.

Uso de cognome para a ELAN

Baseado no exemplo, em que todos os LECs pertencem aos membros do departamento de contas da engenharia, que podem ser configurado para uso da conta do nome da ELAN, dependendo do número de LEC nas ELANs, os nomes podem ser direcionados para a mesma ELAN por configuração dos valores de políticas.

(Conta, LES_A)

(Engenharia, LES_A)

Ou para diferentes ELANs por configuração dos valores de política

(Conta, LES_A)

(Engenharia, LES_B)

A inicialização requer configuração do LEC com o nome correto da ELAN.

Usando nome para LE clientes

Cada LEC pode fornecer o próprio nome. Por exemplo, pode se criar valores de políticas: João, LES_A e Maria, LES_A. O LEC configurado com o nome possibilita direcioná-lo para o mesmo LES. Esse método requer configuração do nome da ELAN em cada LEC e no LECS. Permitindo a João e Maria mover o cliente para uma nova localização, através do cliente para ter um novo endereço ATM ou MAC, retendo membros da ELAN original. Essa técnica também oferece uma quantidade moderada de segurança se os nomes de cada LEC são considerados como senhas.

4.3.4. Política de tipo de ELAN

Valores de políticas de tipo de ELAN são úteis para disponibilizar ELANs *default*. Por exemplo, os seguintes valores de políticas irão assegurar que todos os LEC sejam atribuídos para um dos LESs:

(*Token-ring* ELAN *Type*, LES_A)

(*Ethernet* ELAN *Type*, LES_B)

(*Unspecified* ELAN *Type*, LES_C)

4.3.5. Políticas de tamanho máximo de *frame* e de valores duplicados

Política de tamanho máximo de *frame* pode ser usada para fornecer uma sessão padrão da ELAN.

A duplicação ocorre quando o mesmo valor de política está associado com múltiplos LESs para uma determinada política. Os valores de políticas duplicados são permitidos a um tipo de ELAN e uma política de tamanho do quadro máximo, não sendo permitidos para outras políticas. Os valores duplicados são usados somente quando combinados com uma diferente, de mesma prioridade. Por exemplo, considerando os três tipos de ELAN:

- ELAN *Ethernet* com um tamanho de quadro máximo de 4544 *bytes*;
- ELAN *Token-ring* com um tamanho de quadro máximo de 4544 *bytes*;
- ELAN *Token-ring* com um tamanho de quadro máximo de 18190 *bytes*.

O LEC poderá atribuir a uma ELAN a configuração do tipo de ELAN utilizando políticas de tamanho máximo de *frame* para o mesmo nível de prioridade, definindo os seguintes valores de políticas:

(*Ethernet* ELAN *Type*, LES_1) (Tamanho máximo de *frame*= 4544, LES_1)
(*Token-ring* ELAN *Type*, LES_2) (Tamanho máximo de *frame*= 4544, LES_2)
(*Token-ring* ELAN *Type*, LES_2) (Tamanho máximo de *frame*= 18190, LES_2)

4.3.6. Política de tipo de endereço MAC

Pode ser usada para assegurar que um LEC seja designado para a ELAN apropriada sem levar em consideração sua localização física na rede. O valor da política de endereço MAC deve ser único, assegurando que o mesmo seja válido.

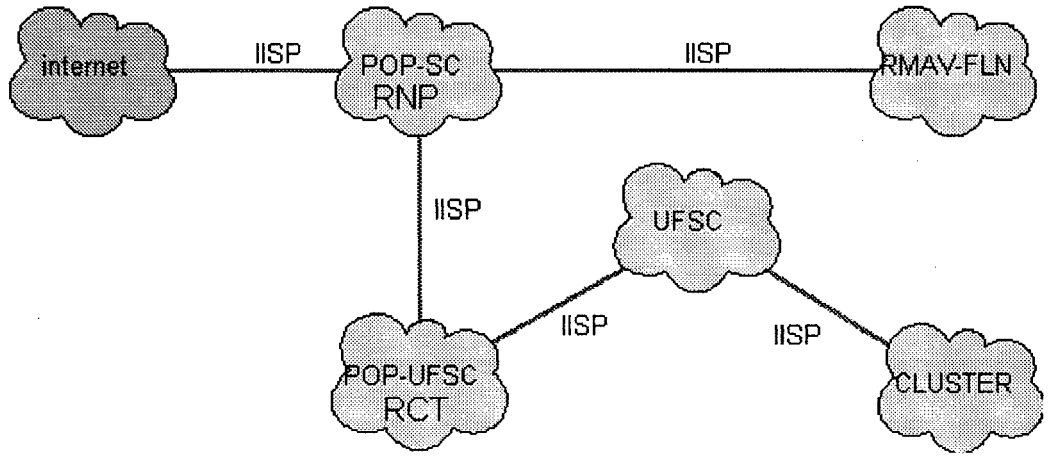
Não confunda os 6 *bytes* do campo ESI do endereço ATM com o endereço MAC. LECs também podem usar o ESI como endereço MAC, embora possa usar um valor diferente.

5. AVALIAÇÃO DAS POLÍTICAS DE SEGURANÇA

5.1. Infra-estrutura da Rede

A estrutura principal do ambiente de teste, utiliza equipamentos ATM que conectam as redes: POP-SC (Ponto de Presença da Rede Nacional de Pesquisa em Santa Catarina - RNP), POP-UFSC (Ponto de Presença da Rede Catarinense na UFSC), redeUFSC e Cluster da UFSC e da RMAV-FLN (Rede Metropolitana de Alta Velocidade de Florianópolis). As conexões são de interfaces (IISP) com 155 Mbps, conforme Figura 5.1-1.

Figura 5.1-1 - *Backbone* Central ATM



A rede do POP-SC tem a função de prover serviço de acesso ao *backbone* da RNP, enquanto que o POP-UFSC provê acesso ao *backbone* da Rede Ciência e Tecnologia de Santa Catarina (RCT-SC). A redeUFSC possui um *backbone* ATM próprio, permitindo acesso aos diversos departamentos técnicos e administrativos da UFSC. Paralelo ao *backbone* da rede UFSC, está a rede Cluster que tem por objetivo avaliar novas tecnologias associadas às aplicações de multimídia e processamento paralelo. Com este objetivo a RMAV-FLN, conecta além da UFSC outras três instituições: Universidade do Estado de Santa Catarina (UDESC), Centro Integrado de Meteorologia e Recursos Hídricos de Santa Catarina / Empresa de Pesquisa Agropecuária e Extensão Rural de Santa Catarina (CLIMERH/EPAGRI) e Empresa de Telecomunicações de Santa Catarina (TELESC).

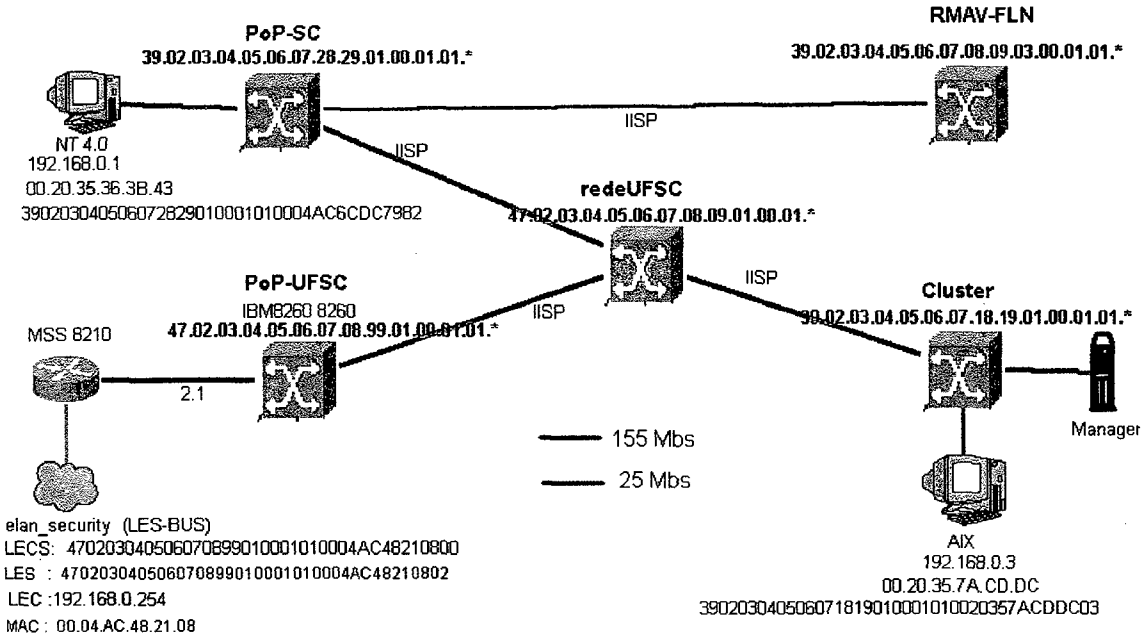
As redes mencionadas utilizam-se do serviço de redes emuladas para constituir as redes virtuais, de modo que o estudo apresentado, quanto à segurança do serviço

LANE é aplicado a todas as redes em questão. Nestas redes não é recomendado efetuar testes que possam comprometer experimentos específicos ou serviços de missão crítica, por essa razão foi configurado um ambiente de estudos específico para os experimentos de segurança, como segue:

5.2. Descrição do Ambiente de Estudos

O ambiente de teste é suportado pelo *backbone* ATM central, utilizando os equipamentos das redes relacionados anteriormente. Para a realização dos experimentos de segurança foi adicionado um roteador (IBM 8210) e duas estações (NT e AIX) com as mesmas características dos demais, conforme mostra a topologia física da Figura 5.2-1.

Figura 5.2-1 - Topologia física do ambiente de estudos.



Nesta configuração os servidores LANE são implementados no roteador. Onde é configurada uma rede virtual, denominada elan_security, para avaliar as políticas de segurança. As entidades do serviço LANE são apresentadas no Quadro V.

Quadro V - Entidades LANE: Servidores (LECS, LES e BUS) e Clientes (LECs).

Servidores: LES, LECS e BUS	IBM 8210 MSS
Clientes:	1. IBM 8210 MSS – V2.2 PTF 7 2. PC *Pentium* 233 Mhz, 60 MB, WinNT 4.0, *Turboways* 25 PCI *Adapter* (15 clientes); 3. Estação RISC6000–E30 AIX 4.3.2, 233Mhz 448MB *Turboways* 155 (15 clientes);
Gerente	Estação RISC6000-F40 AIX 4.3.2 166Mhz 512MB *Turboways* 155 .

5.3. Recursos de Segurança do Equipamento

A solução implementada possui os seguintes recursos de segurança: sistema de registro de eventos, controle de acesso de usuários e controle de acesso ao LECS, descritos reciprocamente:

5.3.1. Sistema de Registro de Eventos

Este sistema registra os eventos de diversos protocolos e serviços, em particular os subsistemas do serviço LANE:

- LEC - ATM LAN *Emulation Client*
- LES - LAN *Emulation Services*
- LECS - LAN *Emulation Configuration Server*
- ILEC - ATM IBM LAN *Emulation Client*

Os eventos, individualmente ou agrupados, podem ser mostrados na *console* ou enviado para uma estação através de um arquivo de *log*, ou ainda podem ser enviado à estação de gerência através de mensagens (*traps*). O nível de registro, é um campo que classifica a mensagem pelo tipo de evento que o gerou.

Quadro VI – Níveis de registro dos eventos no IBM8210 MSS.

Nível de Registro	Tipo
UI-ERROR	Erros internos incomuns
CI-ERROR	Erros internos comuns
UE-ERROR	Erros externos pouco comum
ERROR	Inclui todos os níveis de erros acima
U-INFO	Comentário informacional incomum
C-INFO	Comentário informacional comum
INFO	Inclui todos os níveis de comentários acima
STANDARD	Inclui todos os níveis de erros e todos os níveis de comentários (*default*)
P-TRACE	*Trace* por pacote
U-TRACE	Mensagem de *trace* por pacote em operação incomum
TRACE	Inclui todos os níveis de *trace* acima
ALL	Inclui todos os níveis

5.3.2. Controle de Acesso de Usuários

A configuração desse equipamento (roteador) permite um máximo de 50 nomes, senhas e níveis de permissão. Para cada usuário será determinado uma senha e o nível de permissão. Estes níveis são: Administração, Operação e Monitoração.

5.3.3. Controle de Acesso ao LECS

Este atributo do equipamento permite configurar uma lista de prefixos de endereços ATM (1-20 *octetos*) os quais não terá acesso a base de dados do servidor de configuração. Nesse caso, todas as requisições de conexões com os endereços listados serão rejeitadas.

5.4. Características de Configuração

A opção LES/LECS *Interface to Validate Joins* é habilitada para criar uma interface de comunicação entre os servidores LECS e o LES. E depois deve se habilitar à segurança no LES-BUS (LECS *validation of joins*).

net 0/le-service/ SECURITY (LES/LECS Interface to Validate Joins)/ ADD e ENABLE

net 0/le-service/les-bus/<elan>/ENABLE/ SECURITY (LECS validation of Joins)

5.5. Experimentos

O ATM *Forum* em sua especificação [LANE21/95], definiu seis tipos de políticas para o ambiente LANE e que foram adotadas pela IBM para inibir o acesso de

clientes indesejáveis, das quais cinco delas serão utilizadas nos experimentos de segurança, com exceção da política *byRteDesc* – Descritor de Rota - que é usado apenas por estações *proxy*. Políticas são regras que devem ser obedecidas para que se consiga atingir um objetivo pré-determinado. Os experimentos descritos a seguir têm como objetivo avaliar a segurança das políticas descritas no item 4.3 – Endereço ATM, Endereço MAC, Tipo da ELAN, Tamanho Máximo de *Frame* e Nome da ELAN - baseados nos tipos de ataques descritos no item 4.1 – confidencialidade, integridade e disponibilidade.

5.5.1. Nome da ELAN

Definição: Política baseada no nome da ELAN, faz que com o LECS retorne o endereço LES baseado no nome da ELAN. O nome da ELAN é incluído no LE_CONFIGURE_REQUEST do LEC.

Configuração: Utilizando a política de Nome da ELAN (byElanNm) no LECS com prioridade 10, especificando a política nome da ELAN .

Net 0 /le-service/LECS/Policies/ADD...

```
Enabled   Priority    Type
=======   ========  ==========
  Yes      10        byElanNm
```

Net 0 /le-service/LECS/ELANs/Select <elan>/Policies ADD ...

```
Enabled Value => LES
======= ====================
    Yes elan_name
      => Local LES for: elan_security
```

Mesmo Nome da ELAN

Objetivo: Configurar o nome da ELAN no LEC da estação NT utilizando o mesmo nome registrado no LECS e verificar se o LEC se registra.

Resultado: O LEC se registrou com sucesso, de acordo com a política pré-estabelecida, sendo denominada de elan_security. Desta forma não foi registrado nenhuma mensagem de *log*.

Nome Diferente da ELAN

Objetivo: Alterar o nome da ELAN na configuração do LEC da estação NT e verificar se o mesmo se registra.

Resultado: O LEC não se registrou, pois o nome da ELAN na configuração do LEC é diferente do especificado na política. A estação NT a qual estava com o nome da ELAN alterado não conseguiu se registrar como pode ser observado na mensagem de *log* LES.266. E os LECs (estação AIX e roteador) que estavam com o nome da ELAN correto registraram-se com sucesso.

0004AC482108 47020304050607089901000101000 4AC48210803 R 0001 0 *router* 0020357ACDDC 390203040506071819010001010020357ACDDC03 R 0002 0 AIX
00:15:58 **LES.266**: LES/BUS:'elan_security':JOIN fld:access *denied* LEC ATM addr = x390203040506072829010001010004AC6CDCC281 (NT)

5.5.2. Tipo da ELAN

Definição: Política baseada no Tipo da ELAN (*Ethernet* ou *Token-Ring*) faz que o LECS retorne um endereço LES baseado no identificador do tipo da ELAN que o LEC incluiu em seu LE_CONFIGURE_REQUEST.

Configuração: Utilizando a política de Tipo de ELAN (byLanType) no LECS com prioridade 10, especificando o Tipo da Rede como *Ethernet*. Sendo que a ELAN foi configurada como *Ethernet*.

Net 0 /le-service/LECS/Policies/ADD...

```
Enabled   Priority    Type
=======   ========  ==========
  Yes     10        byLanType
```

Net 0 /le-service/LECS/ELANs/Select <elan>/Policies ADD ...

```
ELAN types for ELAN 'elan_security'
Enabled   Value => LES
=======   ======================
      Yes Ethrnt => Local LES for: elan_security
```

Tipo da ELAN : *Unspecified*

Objetivo: Alterar o Tipo da ELAN na configuração do LEC de *Ethernet* para *unspecified* na estação NT e verificar se o mesmo se registra.

Resultado: Não foi possível testar esta política com o valor não especificado (*unspecified*), devido a interface de configuração dos LECs não possuírem este tipo de rede.

Tipo da ELAN : *Token-Ring*

Objetivo: Testar a política de segurança utilizando o Tipo da ELAN (byLanType), como *Ethernet*, e tentar incluir o LEC na estação NT com o tipo da ELAN *Token-Ring*.

Resultado: O LEC não se registrou, uma vez que a rede definida foi o *Ethernet*, sendo que a estação NT não conseguiu se registrar por estar com o tipo de rede inválido na requisição (*Token Ring*), como mostra a mensagem de *log* LES.160.

```
00:02:56 LES.160: LES/BUS:'elan_security':JOIN fld:invld LAN Type (x2),
LEC ATM addr = x39020304050607282901000101000 4AC6CDCC283
```

5.5.3. Endereço MAC

Definição: Política baseada no endereço MAC faz com que o LECS retorne um endereço LES, baseado no endereço MAC *unicast* do LEC incluído no LE_CONFIGURE_REQUEST.

Configuração: Definida a política MAC no LECS com prioridade 10, especificando o endereço MAC do LEC da estação AIX.

Net 0 /le-service/LECS/Policies/ADD...

```
Enabled      Priority      Type
=======  ========  ==========
   Yes          10    byMacAddr
```

Net 0 /le-service/LECS/ELANs/Select <elan>/Policies ADD ...

```
MAC addresses for ELAN 'elan_security'
 Enabled  Value => LES
=======  ====================
    Yes  00.20.35.7A.CD.DC (AIX)
         => Local LES for: elan_security
```

Mesmo Endereço MAC

Objetivo: Testar a política de segurança utilizando a política de endereço MAC (byMacAddr), e configurar um LEC na estação AIX com o mesmo número MAC definido na política.

Resultado: O LEC foi registrado com sucesso, embora isso lhe assegure que os demais LECs criados, nesta estação, também sejam incluídos, devido à possibilidade de configurar número MAC diferente para cada interface.

```
0020357ACDDC 390203040506071819010001010020357ACDDC03 R 0001 0 AIX
```

Endereço MAC Diferente

Objetivo 1: Testar a política de endereço MAC (byMacAddr), configurando o LEC do roteador sem que seu endereço MAC esteja configurado na tabela de política de Endereço MAC no LECS.

Resultado: O LEC não se registrou, pelo fato que seu endereço MAC não estava configurado na tabela de políticas de endereços MAC no LECS. Embora os servidores LANE estejam no roteador à entidade LEC obedeceu à política estabelecida. No entanto, não houve registro de mensagens de *log*.

Posteriormente foi adicionado o endereço MAC do LEC do roteador na tabela de políticas do LECS, tornando possível o registro do LEC do roteador na ELAN.

```
0004AC482108 47020304050607089901000101 0004AC482108 03  R 0001  0 roteador
0020357ACDDC 39020304050607181901000101 0020357ACDDC 03  R 0002  0 AIX
```

Objetivo 2: Testar a política de endereço MAC (byMacAddr), configurando o LEC da estação NT sem que o seu endereço MAC esteja configurado na tabela de política de Endereço MAC no LECS.

Resultado: O LEC também não se registrou como no experimento anterior, devido ao seu endereço MAC não estar configurado na tabela de políticas MAC no LECS. Assim, o LEC na estação NT só foi incluído na ELAN após inserir o endereço MAC da estação NT na tabela de política de endereço MAC do LECS.

```
00:0X:XX  LES.266: LES/BUS:'elan_security':JOIN fld:access denied
LEC ATM addr = x39020304050607282901000101 0004AC6CDCC281
0004AC482108 47020304050607089901000101 0004AC482108 03  R 0001  0 roteador
002035363B43 39020304050607282901000101 0004AC6CDCC2 82  R 0003  0 NT
0020357ACDDC 39020304050607181901000101 0020357ACDDC 03  R 0002  0 srv03
```

Endereços MAC Repetido

Objetivo 1: Configurar o LEC na estação AIX utilizando o mesmo endereço MAC da estação NT, já registrado.

Resultado: O LEC da estação AIX não conseguiu se registrar, pois esta tentava incluir um endereço MAC já registrado pela estação NT, como mostra a mensagem de *log* LES.154, informando que o endereço MAC não é único.

```
0004AC482108 47020304050607089901000101 0004AC482108 03 R 0002  0  (roteador)
```

```
002035363B43 39020304050607282901000101010004AC6CDCC283 R 0001 0    (NT)
LEC ATM addr = x39020304050607181901000101002035 7ACDDC03
58:39:48 LES.154: LES/BUS:'elan_security':JOIN fld:dplct MAC addr (x002035363B43), (AIX)
```

Objetivo 2: Configurar o LEC na estação AIX com o mesmo endereço MAC da estação NT (já registrado), mas desconectada fisicamente da rede.

Resultado: O LEC se registrou com sucesso, mostrando que quando a estação estiver desconectada fisicamente da rede, perde-se o registro de endereço da tabela LES. No momento da desconexão apresentou a mensagem de *log* do LES.122 seguido do LES.111.

```
002035363B43 39020304050607181901000101002035 7ACDDC03 R 0001    0
LEC ATM addr = x39020304050607181901000101002035 7ACDDC03
58:49:19  LES.122: LES/BUS:'elan_security':Non-Proxy Mcast Fwd leaf rlsd:cause 47,
LEC ATM addr = x39020304050607282901000101000 4AC6CDCC283
58:49:19  LES.111: LES/BUS:'elan_security':Non-Proxy Ctrl Dist rlsd:cause 47
```

5.5.4. Endereço ATM

Definição: Política baseada no endereço ATM faz com que o LECS retorne um endereço LES baseado no endereço ATM completo do LEC ou parte dele.

Configuração: Definido a política de endereço ATM (byAtmAddr) no LECS com prioridade 10, especificando o prefixo de rede da RCT e *Cluster*.

Net 0 /le-service/LECS/Policies/ADD...

```
Enabled      Priority      Type
=======  ========  ========
    Yes          10     bvAtmAddr
```

Net 0 /le-service/LECS/ELANs/Select <elan>/Policies ADD ...

```
MAC addresses for ELAN 'elan_security'
 Enabled  Value => LES
=======  ====================
    Yes  39.02.03.04.05.06.07.08.99.01.00.01.01 (RCT)
    Yes  39.02.03.04.05.06.07.18.19.01.00.01.01 (Cluster)
=> Local LES for: elan_security
```

Endereços MAC Repetido

Objetivo: Testar a política de endereço ATM, após incluir os prefixos de rede RCT e *Cluster* na política byAtmAddr no LECS. Tentar configurar os LECs roteador e estação AIX, os quais pertencem aos prefixos de rede definidos no LECS.

Resultado: Os LECs foram registrados com sucesso, tanto do roteador como da estação AIX, em função de seus endereços estarem de acordo com a política estabelecida.

```
0004AC482108  47020304050607089901000101000 4AC48210803  R 0001   0
0020357ACDDC 390203040506071819010001010020357ACDDC03 R 0002   0
```

Prefixos de Rede Diferentes

Objetivo: Tentar registrar o LEC da estação NT que não pertence aos prefixos de rede definidos na tabela de política byAtmAddr no LECS.

Resultado: Primeiramente o LEC não foi registrado, pois não estava incluído na tabela de política de endereço ATM no LECS, consequentemente, a tentativa de registro do LEC da estação NT gerou um evento de *log* de acesso negado. No entanto, após adicionar o prefixo da rede POP na tabela de política byAtmAddr no LECS, o LEC se registrou com sucesso.

```
00:00:53 LES.266: LES/BUS:'elan_security':JOIN fld:access denied
LEC ATM addr = x39020304050607282901000101000 4AC6CDCC282
002035363B43 39020304050607282901000101000 4AC6CDCC281 R 0001   0
```

5.5.5. Tamanho Máximo de *Frame*

Definição: Política baseada no tamanho máximo de *frame* faz que o LECS retorne um endereço LES baseado no tamanho máximo de *frame* que o LEC incluiu no LE_CONFIGURE_REQUEST.

Configuração: Definida a política byPktSize no LECS com prioridade 10, especificando o tamanho do *frame* igual 1516, o que foi definido na configuração da ELAN.

Net 0 /le-service/LECS/Policies/ADD...

Enabled	Priority	Type
Yes	10	byPktSize

Net 0 /le-service/LECS/ELANs/Select <elan>/Policies ADD ...

```
MAX FRAME SIZES FOR ELAN 'ELAN_SECURITY'
ENABLED VALUE => LES
======= ====================
  YES 1516 => LOCAL LES FOR: ELAN_SECURITY
```

Tamanho de *Frame* Diferente

Objetivo 1: Tentar incluir um LEC na estação NT com tamanho de *frame* 4544, que é diferente do tamanho de *frame* que está especificado na política byPktSize que é de 1516.

Resultado: O LEC da estação NT não se registrou devido à restrição imposta pelo tamanho de *frame* diferente na tabela de configuração do LECS.

Na estação AIX não foi possível definir um tamanho de *frame* maior que 1516 na interface *Ethernet*.

Mesmo Tamanho de *Frame*

Objetivo 2: Tentar registrar um LEC utilizando o mesmo tamanho de *frame* definido na política byPktSize na tabela do LECS, o qual neste caso é de 1516.

Resultado: Definindo o LEC da estação NT com tamanho de *frame* igual ao especificado na política, o LEC se registrou com sucesso.

```
0004AC482108  47020304050607089901000101000 4AC48210803   R 0001  0  router
0020357ACDDC  39020304050607181901000101002 0357ACDDC03   R 0002  0  AIX
002035363B43  39020304050607282901000101000 4AC6CDCC282   R 0003  0  NT
```

5.6. Resultados da Avaliação das Políticas

Após configurar configurar as políticas de segurança, de acordo com a IBM, realizou-se experimentos, anteriormente descritos num ambiente específico, localizado no Cluster/RMAV-FLN, conforme item 5.2 – Descrição do Ambiente de Estudos, foram observados os seguintes resultados.

1. **Política de endereço ATM (byAtmAddr)**: nos experimentos realizados os LECs foram registrados com sucesso, devido os endereços estarem de acordo com a política de endereço ATM. Porém, quando testados com prefixo de rede diferentes, que não estavam incluídos na política, o acesso foi negado.

   A utilização do prefixo de rede ATM apresenta maior segurança, pois seu tamanho e flexibilidade dificultam a dedução do mesmo, consequentemente restringe o acesso

a ELAN, todavia permite o acesso apenas aos LECs que estiverem seus prefixos incluídos na política;

2. **Política de Endereço MAC (byMacAddr)**: os testes efetuados na política de endereço MAC visavam testar as diferentes possibilidades de registro de endereço MAC, dentre as quais: configurar um LEC na estação AIX utilizando o mesmo número do endereço MAC, configurar o LEC do roteador sem que seu endereço MAC esteja configurado na tabela de endereço MAC no LECS, etc.
   Os resultados obtidos nos testes apresentam vulnerabilidade, devido a facilidade com que o atacante pode alterar o endereço MAC, uma vez que esta política permite a troca de endereço sem restrições;

3. **Política Tipo da ELAN (byLanType)**: baseado nos três tipos de ELANs (*Ethernet*, *Token-Ring* ou *Unspecified*), foram realizados experimentos no intuito de alterar o tipo da ELAN na configuração do LEC. Uma vez que a rede definida foi o tipo *Ethernet,* verificou-se que utilizando o tipo da ELAN *Token-Ring* ou *Unspecified,* o LEC não foi registrado.
   Contudo, esta política é usada para especificar o tipo de rede a ser configurada (*Ethernet*, *Token-Ring* ou *Unspecified*), sendo muito fácil de ser deduzida, considerando que há somente três tipos de ELANs a serem testadas;

4. **Política de Tamanho Máximo de *Frame* (byPktSize)**: a política estabelecida possui tamanho de *frame* igual 1516, definido na configuração da ELAN. Nos experimentos efetuados tentou-se incluir um LEC na estação NT com tamanho diferente do especificado. Sendo que não houve registro devido a restrição imposta pelo tamanho de *frame* diferente na tabela de configuração do LECS. Esta política é útil na criação de uma ELAN *default* designando LECs para tal função, baseado no tamanho de *frame*;

5. **Política de Nome da ELAN (byElanNm)**: nos experimentos realizados a política baseada no nome da ELAN, visa configurá-la no LEC da estação NT, utilizando o

mesmo nome registrado no LECS. Enquanto que ao testar com o nome da ELAN diferente na configuração do LEC da estação NT, verificou-se que o registro foi negado, consequentemente torna-se mais difícil o acesso a configuração de um LEC. Porém, a política nome da ELAN proporciona maior flexibilidade na designação de um LEC para ELAN, sendo que o LEC tem a opção de usar um nome atual ou um *alias*.

Baseado nos experimentos realizados percebe-se que para obter maior confiabilidade na segurança, o ideal é a utilização de três políticas: de endereço ATM (byAtmAddr), nome da ELAN (byElanNm) e tipo da ELAN (byLanType), estabelecidas com valores de prioridades diferentes. Sendo que o menor valor de política deve ser do byAtmAddr, por ser a política mais segura devido ao seu tamanho e flexibilidade que dificultam a dedução do prefixo de rede ATM; a Segunda política utilizada deve ser o byElanNm, considerando que suas características oferecem restrições ao acesso na configuração de um LEC, e também por permitir a utilização de um *alias*, personalizando, assim, cada ELAN; e por último deve-se utilizar a política byLanType, que define qual o tipo da ELAN que será aplicada na configuração do LEC, restringindo a três tipos de ELAN - *Ethernet*, *Token-Ring* ou *Unspecified*.

Dessa forma para que um LEC consiga se registrar ele terá de atender os requisitos especificados nas três políticas, lembrando que a menor prioridade será verificada primeiro, resultando em maior segurança no controle de acesso nas ELANs.

6. PROCEDIMENTOS DE CONTROLE

Para inibir as ameaças ao serviço LANE são definidos procedimentos de controle utilizando as políticas de segurança, bem como os recursos de segurança adicionais oferecidos pelo ambiente de estudo.

6.1. Análise das Ameaças ao Serviço LANE

Para cada ameaça categorizada no item 4, são analisadas as possibilidades de ocorrência e as possíveis ações preventivas e reativas, sempre procurando inibir ou restringir o acesso de clientes não-autorizados.

O controle de acesso de usuários (em diversos níveis) e o sigilo de senhas são considerados como regras básicas de segurança. Como procedimento de controle básico considera-se o uso das políticas nome da ELAN, tipo da ELAN e prefixo ATM (conforme avaliação no item 5) e correlaciona os objetos das MIBs. Outro controle básico é a verificação da tabela de registros de erros para cada servidor LANE.

Procedimento 1 – Verificar o número de acessos negados no LES e LECS, bem como o número de requisições inválidas, e depois comunicar ao operador.

Procedimento 2 – Analisar a tabela de registro de erros do servidores LECS, LES e BUS (lecsErrLogTable, lesErrLogTable, busErrLogTable respectivamente).

6.1.1. Confidencialidade – Desvio da conexão após ser configurada

1) Desconectando fisicamente a estação-alvo.

Foi observado durante os experimentos que ao desconectar fisicamente uma estação o LEC deixa de existir na ELAN em poucos segundos. Então, para que a estação espiã mascarada com a configuração da estação desconectada possa aproveitar as configurações do LES e dos demais LECs o atacante deverá ser muito habilidoso.

Procedimento 3: Conferir o endereço MAC do LEC recém conectado e fazer a autenticação na porta do comutador.

2) Modificar o mapeamento nos comutadores ATM ou roteadores:

Quando o atacante conhece o VPI/VCI de uma conexão, pode-se estabelecer um caminho virtual permanente (PVC), na porta do comutador origem até a estação espiã.

Além da segurança básica no comutador deve ser verificado se as estações finais definidas por PVCs satisfazem às políticas de segurança.

No caso de modificar a tabela de resolução ARP (MAC-> IP) na camada rede, a estação espiã deve estar na mesma rede da estação legítima. Caso contrário, o próximo roteador pode identificar a fraude. Deve ser observado também que os comutadores de nível 3 também podem sofrer esse tipo de ataque.

Esta alteração pode ser executada na configuração do protocolo ARP a partir da console do roteador. Neste caso devem ser observadas as regras básicas de segurança.

Procedimento 4: Criar procedimentos de controle para a camada de rede.

Procedimento 5: Identificar os LECs conectados por PVCs nos comutadores e verificar as políticas de segurança.

6.1.2. Confidencialidade - Desvio antes da conexão

1] Modificar o processamento do LEC (microprograma) ou carregar um microprograma falsificado.

Para ocorrer esta ameaça, embora o LEC não contenha informações importantes como os servidores, ele pode atuar em modo promiscuo na escuta ou alterações de informações. A diversidade de informações de rede impossibilita a verificação do código utilizado pelo LEC numa tentativa de evitar ataques.

Procedimento 6: Detectar apropriações indevidas de conexões usando *Sniffer*.

2] Modificar a tabela ARP em qualquer LEC ou LEC *proxy*, ou mesmo no LES. Este ataque somente será possível se a estação espiã e a estação a ser espiada compartilharem a mesma ELAN. Isto é, se estiverem ligados ao mesmo LES a estação espiã pode ser qualquer LEC da ELAN (estações ATM, roteadores ou repetidores), o atacante não usa qualquer propriedade de roteador ou repetidor específico, quando requer o suporte da administração para ser montado.

A configuração desta ameaça é bastante provável de ocorrer haja vista as possibilidades de alteração da tabela ARP, seja no servidor ou seja nos clientes. No servidor LES, esta alteração pode ser feita utilizando requisições SNMP na tabela lesLeArpMacTable. Embora se possa saber quem fez a alteração (gerente ou agente), esta informação não evita o ataque.

Uma alternativa é a configuração da política que restringe o acesso pelo endereço MAC. No entanto, esta política tira a flexibilidade das ELANs que possuem muitos LECs.

Com o uso das políticas nome da ELAN, tipo da ELAN e prefixo ATM um nível básico de segurança é oferecido, mas não impede a ocorrência desta ameaça. O que vai dificultar ou impedir é a autenticação do endereço ATM nas portas do comutador.

Fica em aberto como controlar as modificações indevidas nas tabelas ARP dos LECs e LECs *Proxy*.

Além do procedimento de controle básico deve ser implementado o controle das alterações da tabela lesLeArpMacTable examinando as alterações não feitas pelo agente.

> **Procedimento 7**: Se a modificação na tabela lesLeArpMacTable for feita pelo gerente deve ser feita uma verificação se este LEC não é um espião.

6.1.3. Confidencialidade – Conexão espiã

1] Capturar o tráfego (células ATM) em qualquer ponto da rede filtrando a conexão desejada através do VPI/VCI. Isto, assume que o atacante saiba qual VPI/VCI do canal do usuário nomeado pela rede para aquela conexão, portanto, pode-se aprender com os resultados de escutas anteriores efetuadas na inicialização de conexões.

2] Filtrar o tráfego *broadcast/multicast/unicast* no BUS. O atacante pode se posicionar em qualquer sistema intermediário (comutadores ATM, roteadores ou BUS), através dos quais passam uma grande parte do tráfego, que possibilitam escutar a conexão desejada, filtrando o tráfego nos identificadores VPI/VCI.

3] Modificar o processamento do BUS, clonando as conexões e duplicando o tráfego. O ataque poderá ser montado no meio de transmissão, onde a realização prática varia significativamente com o tipo de meio (cabo coaxial, fibra óptica).

Nos casos mencionados o atacante necessita conhecer o VPI./VCI da conexão a ser espiada. Estes valores podem ser fornecidos pela LES.MIB, lesLecCtlDirectVpi e lesLecCtlDirectVci. Mesmo sendo variáveis de leitura e escrita, não foi possível modificar remotamente seus valores no equipamento usado para teste. Geralmente o VPI é zero e o VCI é alocado dinamicamente. O valor da instância do LEC também é obtido pela MIB, lesLecIndex. Dessa forma o atacante pode descobrir as interfaces da conexão fazendo uma requisição SNMP. De modo semelhante os valores do VPI/VCI

podem ser obtidos remotamente a partir do comutador ATM, monitorando as conexões cruzadas. E da mesma forma não podem ser alteradas, nem mesmo pela console.

Para detectar esse ataque faz-se necessário mecanismos de filtragem com maior granularidade atuando no meio físico. Isso sugere o uso de ferramentas denominadas *sniffers*.

Procedimento 6: Detectar apropriações indevidas de conexões usando *Sniffer*.

6.1.4. Confidencialidade - Conexão Imprópria

Neste caso, o LEC ATM (estação LEC, servidores LANE, roteadores, repetidores ou comutadores ATM) executa o ataque na inicialização da conexão emitindo mensagens falsas, com um endereço ATM de origem falsificado.

Essa tentativa de mascaramento poderá falhar se ao ingressar no comutador ATM for verificada a consistência entre o número da porta de onde o pedido de configuração originou e o endereço ATM requisitado na mensagem de conexão. Isso só poderá acontecer se a estação legítima for desconectada e conectar a estação espiã.

Assim para detectar o mascaramento pela estação espiã, deve ser verificada a consistência entre o número da porta de entrada e o endereço de origem (incluído na mensagem de configuração).

Procedimento 1 – Verificar o número de acessos negados no LES e LECS, bem como o número de requisições inválidas, e depois comunicar ao operador.

6.1.5. Integridade - Mascaramento durante o estabelecimento da conexão

Este ataque consiste em modificar as mensagens de sinalização em trânsito, quando apropriado, de modo forçar a conexão a ser configurada entre uma estação maliciosa e uma das duas partes.

Considerando, o procedimento de configuração da conexão, há duas maneiras de montar tal ataque: pela troca do endereço ATM na mensagem de configuração com o endereço ATM da estação do atacante, ou refazer a troca dos identificadores VPI/VCI da mensagem SET UP ou *CONNECT* com o VPI/VCI de outra conexão previamente configurada pelo atacante.

Um ataque semelhante, teoricamente pode ser montado de qualquer sistema intermediário (comutador ATM, regenerador, meio de transmissão) ao inserir um dispositivo de filtragem ou modificação de células, embora atualmente esse ataque seja

inviável, porque o *hardware* existente não é eficiente o bastante comparado ao desempenho ATM.

6.1.6. Integridade - Mascaramento com conexão estabelecida

Se localizado em uma rede ATM (comutadores ATM ou meio de transmissão) o cúmplice pode redirecionar todas as células de uma conexão (com o mesmo VPI/VCI) para outra conexão previamente configurada pelo atacante. Isso pode ser feito de dois modos:

1- Pela injeção de um dispositivo de modificação ou filtragem de células, o cúmplice pode filtrar o tráfego nos identificadores VPI/VCI e alterar adequadamente os campos VPI/VCI.;

2- Não tendo nenhuma medida de proteção para garantir a integridade dos microprogramas do comutador ATM, o cúmplice pode então modificá-lo, em vez de carregar um microprograma falsificado para transformar os identificadores VPI/VCI quando apropriados.

No primeiro caso, o ataque é inviável, porque tais dispositivos de modificação e filtragem de células requerem alto desempenho que não podem ser definidos com as técnicas correntes. O segundo ataque é tecnicamente possível desde que consiga modificar o processamento do comutador ATM. E diferentemente do primeiro, é possível alterar células simultaneamente com o processo usual de comutação.

6.1.7. Integridade - Injeção de Dados

A inserção de células ATM em uma conexão em processo tende a atrapalhar a conexão, especialmente enganando a estação de destino final, uma vez que a maior parte das células injetadas são detectadas pelas camadas superiores das estações finais de destino e o processamento de detecção consome tempo.

Devido ao desempenho do ATM, este ataque é aparentemente inviável, porque os *hardwares* existentes não são rápidos o suficiente para inserir células em certas posições no fluxo de células ATM.

6.1.8. Disponibilidade – Acesso não-autorizado e repetitivo

Neste caso o atacante pode montar seu ataque de qualquer posição da rede, embora as estações LEC sejam as preferidas. Esta preferência é devida ao fato de que os

servidores LANE (roteadores e repetidores) necessitam obter o suporte do administrador e estações LAN não fornecem acesso direto aos servidores LANE. Outro fato é a dificuldade de inserir dados nos comutadores ATM, como visto anteriormente.

Ataques ao servidor LES diminui o desempenho da resolução de endereços, mas não compromete o desempenho da rede. Entretanto ataques através do BUS poderão sobrecarregar totalmente a rede ATM. A solução para este problema é incluir um mecanismo de proteção no BUS, de modo que os impactos dos ataques fiquem limitados ao tráfego *broadcast.*

Procedimento 8: Verificar o tráfego no BUS por LEC.

6.1.9. Disponibilidade - Obstrução de comutadores ATM, roteadores ou repetidores.

O envio de informações falsificadas sobrecarrega os equipamentos rompendo as atividades e impedindo o processamento do tráfego legítimo. Isso acontece quando uma estação LAN envia mensagens falsas (por exemplo: pacote/*frame* com endereço de destino falso) à rede ATM, obstruindo o roteador ou repetidor, fazendo que este perca tempo na localização do destino correspondente, gerando um tráfego denso com as consultas ao LES (ARP *request*) ou ao BUS (por células *brodcasting* no ATM).

Procedimento 1 – Verificar o número de acessos negados no LES e LECS, bem como o número de requisições inválidas, e depois comunicar ao operador.

Procedimento 9: Verificar o incremento de requisições de resolução de endereços no LES.

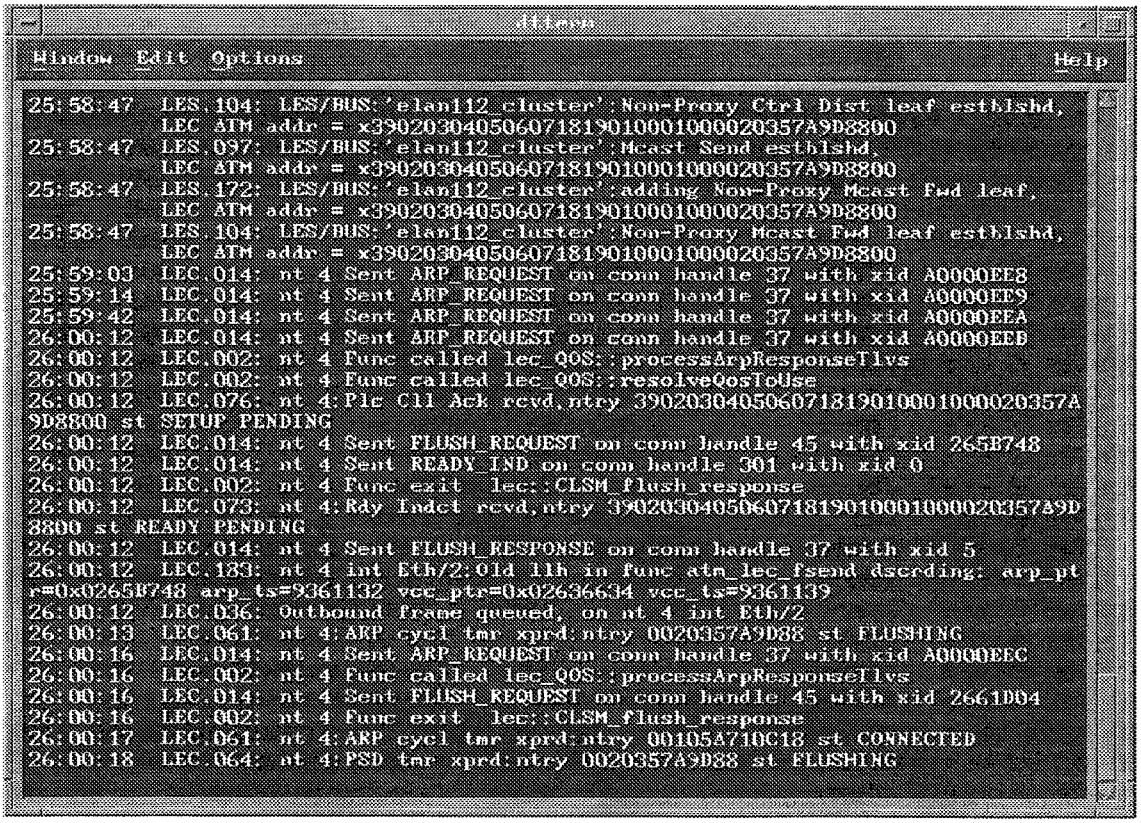
6.2. Implementação dos Procedimentos de Controle

Para implementar os procedimentos de controle de segurança destinados a inibir as ameaças do serviço LANE foi utilizado o sistema de registro de erros dos servidores LANE (item 5.3.1) e o sistema de gerenciamento de redes SNMP.

O sistema de registro de erros implementado no equipamento que fornece o serviço LANE possui uma interface pouco amigável, conforme mostra a Figura 6.2-1. Os erros são registrados seqüencialmente, mostrando o subsistema, a descrição do erro e a causa provável. Embora o sistema seja flexível na apresentação dos eventos, o mesmo não permite a inferência de informações. Analisando dois ou mais subsistemas, em uma

rede com muitos LECs, os eventos são registrados tão rapidamente que fica impraticável a visualização dos dados . Os eventos podem ser armazenados em um arquivo de uma máquina remota que possua o sistema de registro (*syslogd*), no entanto a forma de apresentação e análise continua a mesma. A alternativa é enviar os eventos (*traps*) para uma máquina de gerência que pode analisar os dados e fazer inferências tomando ações quando necessário.

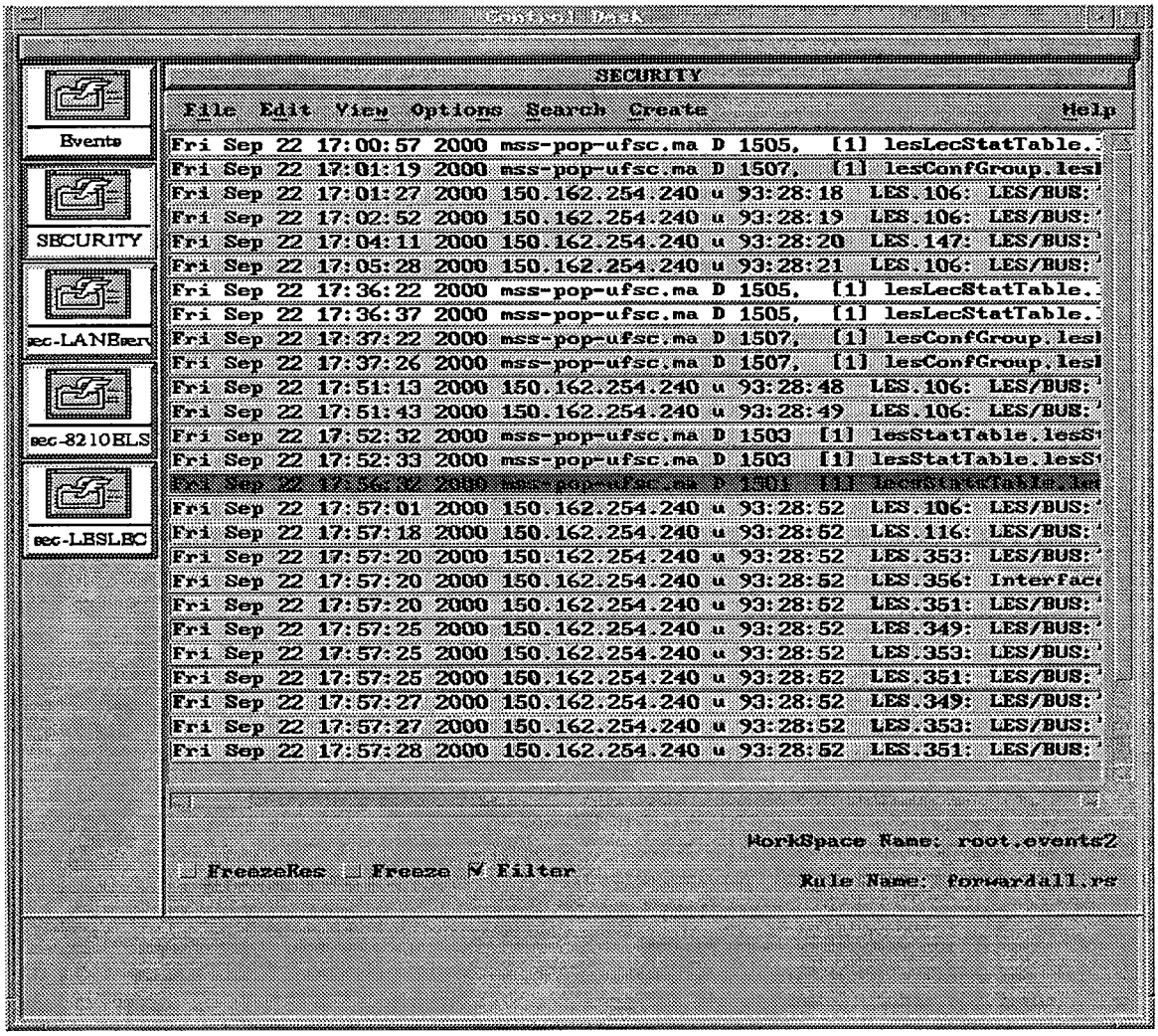
Figura 6.2-1 - Sistema de registro de eventos do IBM8210-MSS, mostrando os eventos associados aos subsistemas LES e LEC em um determinado momento.



A ferramenta de gerenciamento *Tivoli NetView* 5.12 para AIX é utilizada para monitoramento dos objetos gerenciáveis, bem como para a correlação de variáveis através de regras. Lembrando que os objetos gerenciáveis estão definidos na especificação af-lane.0057 [LANE21/95] e descritos sumariamente no Anexo 1. Na console da ferramenta é apresentada a topologia da rede baseada no endereçamento IP, bem como uma área de controle de eventos (*workspace*), conforme mostra a Figura 6.2-2. A área de trabalho denominada '*Events*' apresenta todos os eventos associados aos diversos nodos das diferentes redes. Utilizando-se de filtros, a área '*Security*' mostra

somente os eventos relacionados aos equipamentos utilizados nos experimentos. As demais áreas estão associadas às regras utilizadas para correlação de variáveis, as quais estão baseadas nos procedimentos especificados no item 6.1. A implementação dos procedimentos de controle é restritiva às capacidades dos sistemas de gerência.

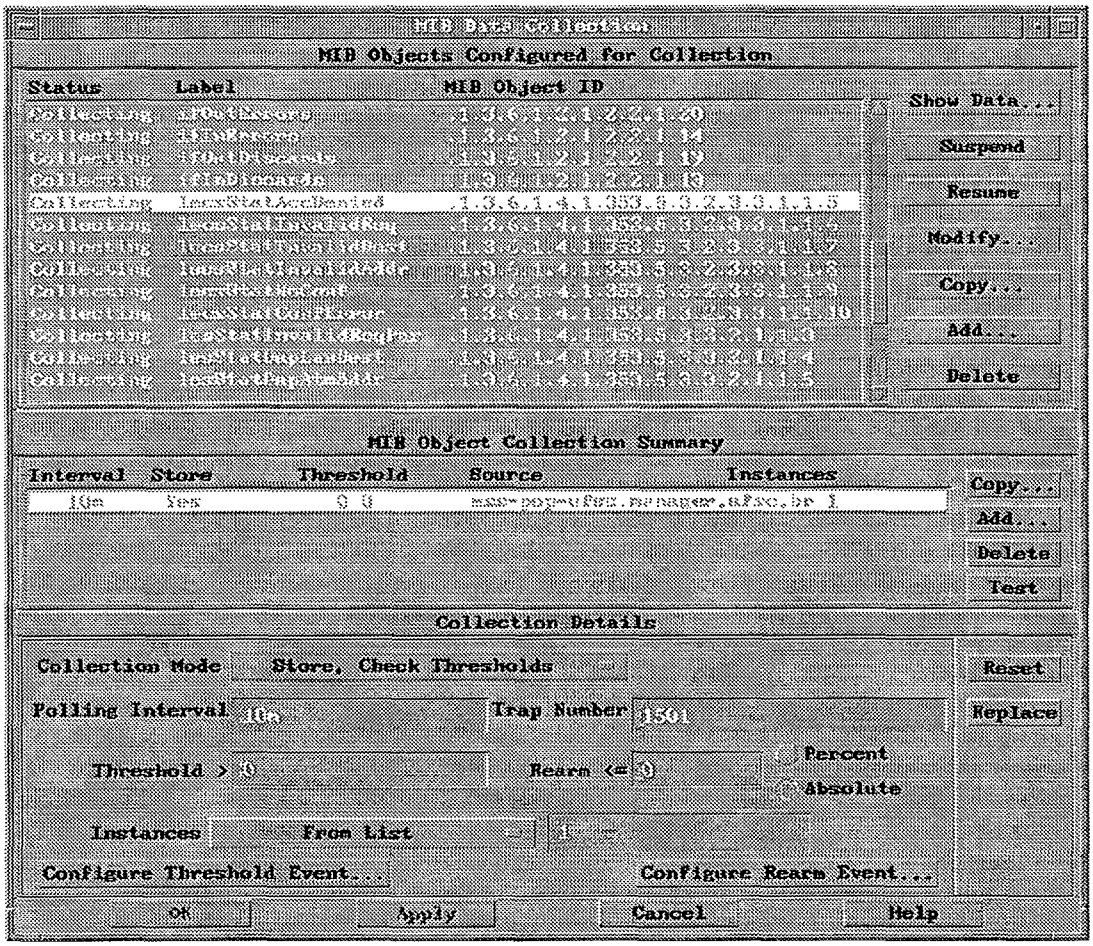
Figura 6.2-2 - Área de controle de eventos com diversas áreas de trabalho em particular a área *security* mostrando o *status* e descrição dos diversos eventos ocorridos em um determinado período.



Para fazer a correlação, são selecionadas variáveis para serem coletadas periodicamente e em seguida são definidos eventos de notificação. Na Figura 6.2-3 o coletor de dados mostra a configuração de diversas variáveis, em particular do grupo LES e LECS, bem como a definição dos valores limites do evento para um objeto gerenciável. Neste exemplo, identificado por *trap* 1501, quando a variável lecsStatAccDenied for diferente de zero para a instância 1 (somente um LECS) do

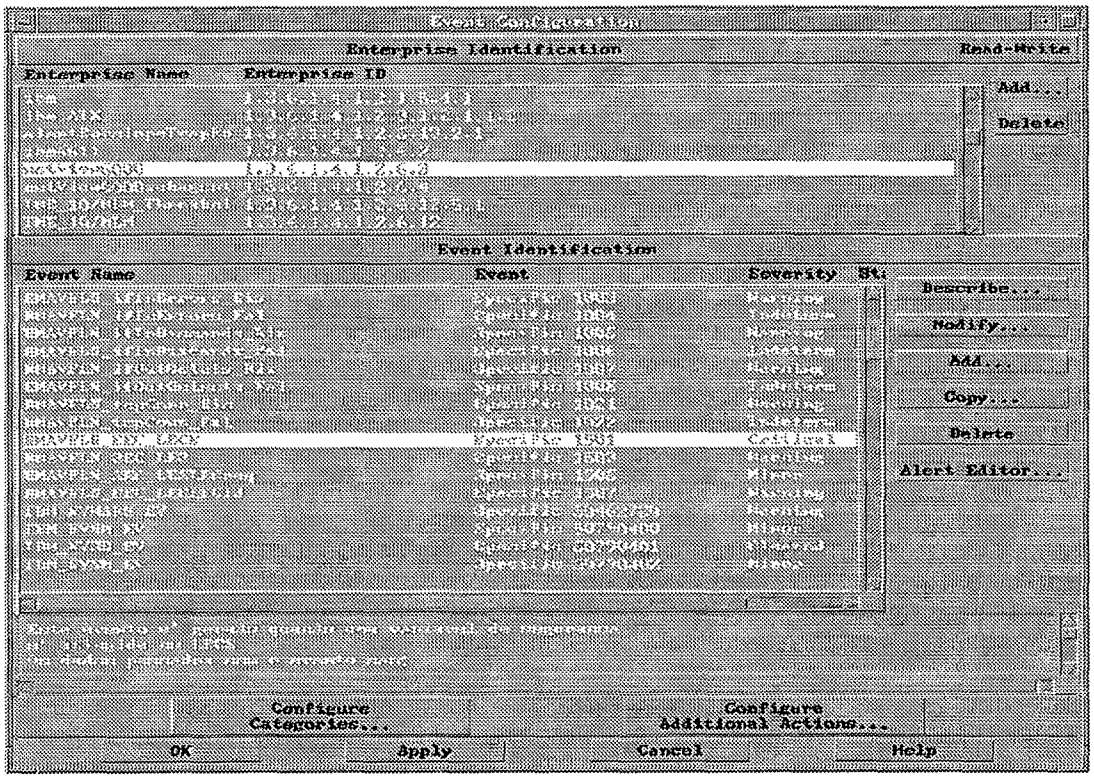
servidor LANE (denominado mss-pop-ufsc.manager.ufsc.br) a mensagem de erro será gerada.

Figura 6.2-3 - Coletor de dados do NetView mostrando as variáveis armazenadas e os valores limites para a inicialização do *trap* de um determinado objeto.



Observando que este evento é uma mensagem configurada no próprio *Netview*, conforme Figura 6.2-4, onde são definidos os atributos do evento. Seguindo o exemplo anterior, o evento 1501 denominado RMAVFLN_SEC_LECS registra os ataques ao LECS com severidade crítica. Outros eventos configurados podem ser emitidos pelo próprio agente, mas nem sempre é clara a definição de seus atributos.

Figura 6.2-4 - Configuração de Eventos no NetView onde são mostrados as classes dos eventos (nome da empresa) bem como o nome, o número e a severidade de cada evento.



Utilizando eventos previamente configurados, a seguir são descritas as regras de correlação baseadas nos procedimentos de controle.

6.2.1. Estatística dos Servidores LANE

Baseada no Procedimento 1, esta regra analisa o número de acessos duvidosos aos servidores LANE. São definidos os seguintes eventos:

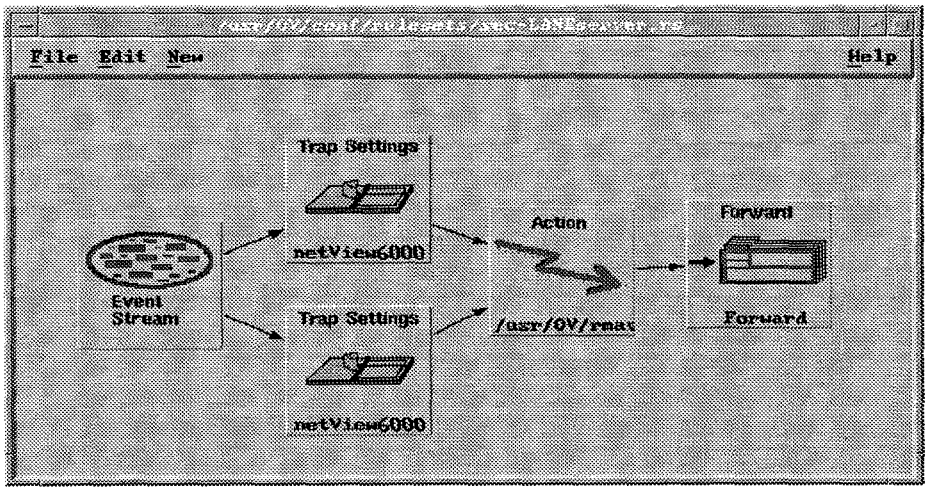
1501: Valor diferente de zero para as variáveis: `lesStatAccDenied`, `lecsStatAccDenied`, `lecsStatInvaldReq`, `lecsStatInvaldDest`, `lecsStatInvaldAddr`, `lecsStatNoConf` e `lecsStatConfError` da tabela `lecsStatTable`.

1503: Valor diferente de zero para as variáveis: `lesStatInvalidReqPar`, `lesStatDupLanDest`, `lesStatDupAtmAddr`, `lesStatAccDenied`, `lesStatInvalidReqId`, `lesStatInvalidLanDest`, `lesStatInvalidAtmAddr` e `lesStatOutRegFails` da tabela `lesStatTable`.

A Figura 6.2.1-1mostra que se ocorrer um desses eventos será executada uma ação. Esta ação é o registro do evento em um arquivo e o envio de uma mensagem de

notificação para o operador, identificando o servidor ameaçado, conforme *script* mostrado no Quadro VII.

Figura 6.2.1-1 - Regra sec_LANEserver para tratamento dos eventos 1501 e 1503 relacionados aos ataques efetuados nos servidores LECS e LES.



Quadro VII - *Script* que define a ação tomada na regra sec_LANEserver.

```
#!/bin/sh
# Coletar variaveis dos eventos netView6000 RMAVFLN_SEC_LANEservers
# Parametros de entrada:
# NVATTR_2 Host Name
# NVATTR_3 Descricao do Evento
# NVATTR_4 Dados Internos
#
TMP=/tmp/.secLANEserver.log
LOGPATH=/usr/OV/rmav/log
LOGFILE=sec_LANEServer.log
SUBJECT="LOGFILE: secLANEserver"
cat > $TMP << __EOF__
Possivel ataque ao servidores LANE:
 Node:       $1
 Evento:     $2
 Descricao: $3
__EOF__
cat $TMP >> $LOGPATH/$LOGFILE
cat $TMP | mail -s "$SUBJECT" operator@rmav-fln.ufsc.br
rm -rf $TMP > /dev/null 2>&1
```

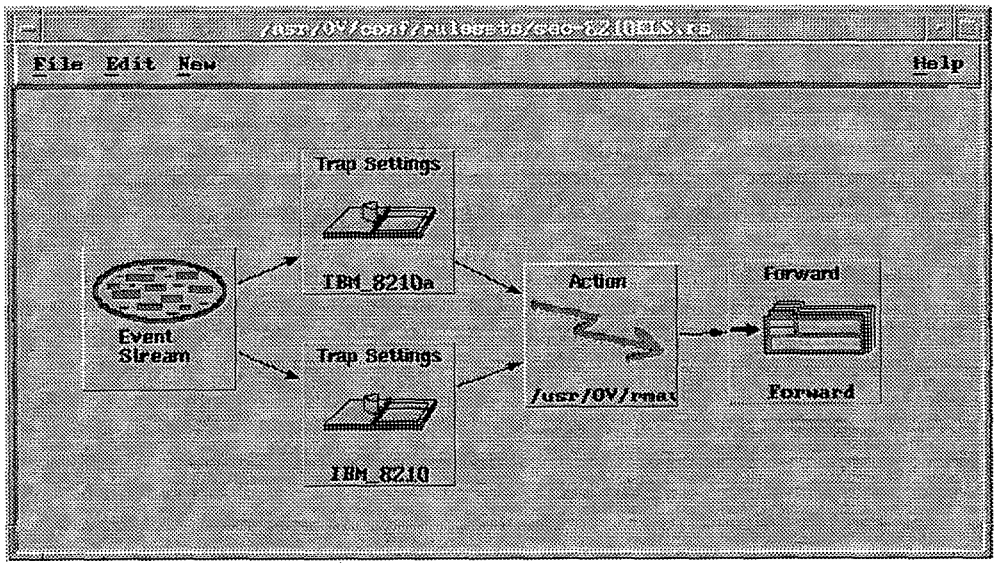
6.2.2. Registro de Eventos do Equipamento

Como mencionado no item 5.3.1 o sistema de eventos registra vários níveis de informação sobre o equipamento. Dentre os eventos com maior incidência nos subsistemas UDP, TCP, IP, LECS, LES, LEC e ATM, foram selecionados aqueles pertencentes a classe ERROR para serem enviados como mensagem de alerta para o

gerente (*traps*). Esta evento quando recebido pelo gerente, é tratado e depois enviado para área de controle, conforme mostra a Figura 6.2.2-1. Observe que são considerados dois tipos de eventos IBM_8210 e IBM_8210a dado que são dois equipamentos semelhantes mas com identificadores diferentes.

Considerando que o evento recebido possui formato diferente dos eventos configurados pela ferramenta de gerência, faz-se necessário um *parse* para selecionar a informação de interesse. O Quadro VIII mostra o *script* que filtra a mensagem enviada pelo equipamento, e para cada evento é tomada uma decisão específica.

Figura 6.2.2-1 - Regra sec_8210ELS para tratamento dos eventos da classe IBM_8210 relacionados aos eventos emitidos pelo sistema de registro de eventos do equipamento.



Quadro VIII - *Script* que define a ação tomada na regra sec_8210ELS.

```
#!/bin/sh
# hr:min:sec
# subsys_name.event_num:
# message_text
#
TMP=/tmp/.sec8210els.tmp
LOGPATH=/usr/OV/rmav/log
LOGFILE=sec8210els.log
SUBJECT="LOGFILE: sec8210els"
cat > $TMP << __EOF__
Registro de Evento do IBM8210 MSS
---------------------------------
 Time Stamp : $1
 ATM addr   : ${17}
__EOF__
case $2 in
 "LES.382:")
  cat $TMP | mail -s "$SUBJECT" operator@rmav-fln.ufsc.br
  ;;
  *)
   cat $TMP >> $LOGPATH/$LOGFILE
  ;;
esac
rm -rf $TMP > /dev/null 2>&1
```

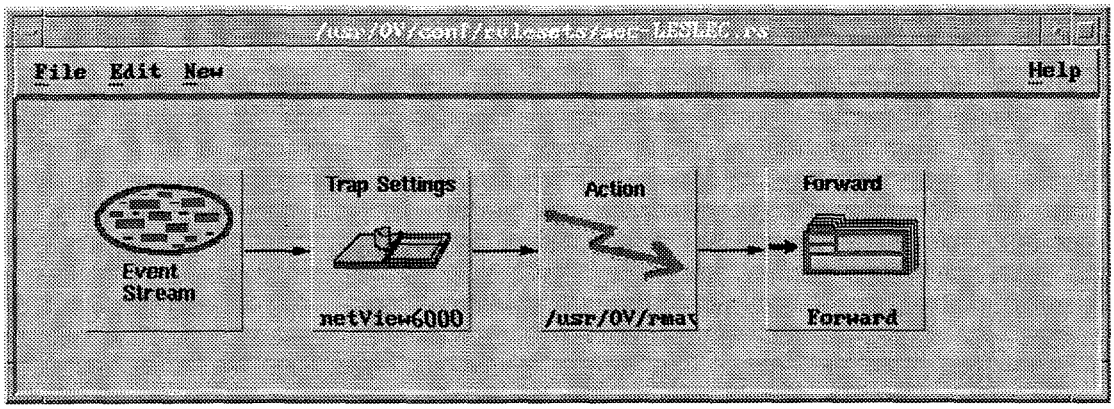
6.2.3. Registro do LEC nos LES

O fato do LES não registrar um determinado LEC pode evidenciar a tentativa de uma máquina espião registrar-se na rede. Baseado no Procedimento 5 faz-se necessário comunicar ao operador o endereço do cliente que enviou as requisições não atendidas. Para isso foi definido o seguinte evento:

1505: Valor diferente de zero para as variáveis: `lesLecInUnReg`.

A regra para tratamento deste evento é mostrada na Figura 6.2.3-1. Quando o evento for recebido uma ação será tomada, conforme *script* do Quadro IX, antes de ser enviada para área de controle de eventos. A ação identifica a instância que disparou o evento e encaminha para o operador uma notificação com o endereço ATM do LEC e o *status* da conexão.

Figura 6.2.3-1 - Regra sec_LESLEC para tratamento do evento 1505 relacionado aos possíveis ataques dos LECs ao LES.



Quadro IX – *Script* que define a ação tomada na regra sec_LESLEC.

```
# Coletar variaveis dos eventos netView6000 RMAVFLN_SEC_LESLEC
# NVATTR_1 : numero de requisicoes (.1.3.6.1.4.1.353.5.3.3.3.1.1.5)
# NVATTR_2 : Hostname
# NVATTR_4 : Instancia
# NVC      : Comunidade
TMP=/tmp/.secLESlec.log
LOGPATH=/usr/OV/rmav/rs
LOGFILE=sec-LESLES.log
SUBJECT="LOGFILE: secLESles"
CMDPATH=/usr/OV/bin
lesLecAtmAddr=`$CMDPATH/snmpget -c $3 $2
.1.3.6.1.4.1.353.5.3.3.1.8.1.2.$3`
lesLecState=`$CMDPATH/snmpget -c $3 $2
.1.3.6.1.4.1.353.5.3.3.1.8.1.9.$3`
cat > $TMP << __EOF__
Requisicoes do LEC nao registradas no LES:
 no. de requisoes  : $1
 Servidor LES      : $2
 Instancia         : $3
 Endereco ATM      : $lesLecAtmAddr
 Status            : $lesLecState
__EOF__
cat $TMP >> $LOGPATH/LOGFILE
cat $TMP | mail -s "$SUBJECT" operador@rmav-fln.ufsc.br
rm -rf $TMP > /dev/null 2>&1
```

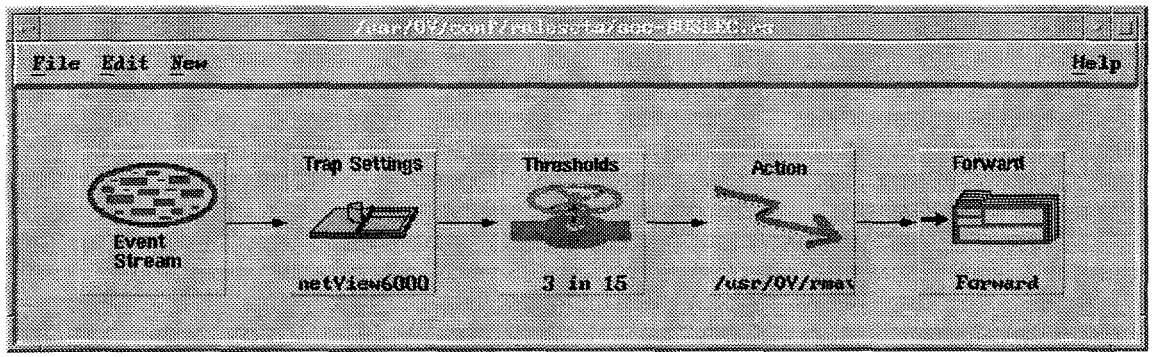
6.2.4. Requisições do LEC ao BUS

Ataques repetitivos ao BUS poderão comprometer o desempenho da rede, então a monitoração do tráfego no BUS por LEC pode detectar possíveis atacantes, conforme Procedimento 8. Neste caso a variável busLecRecvs (número de requisições *broadcast*, *multicast* e desconhecidas recebidas pelo BUS de um determinado LEC) é monitorada com limiares para ativar (*rising*)e desativar (*falling*) o evento. Os parâmetros associados ao evento 1511 referem-se a um equipamento específico:

1511: rising=130000 e falling=100000: `busLecRecvs`.

É necessário calibrar os limiares para cada equipamento. Então para evitar notificações excessivas, a regra mostrada na Figura 6.2.4-1 acrescenta um limiar de eventos. Neste exemplo, num período de 15 minutos em cada 3 eventos só será processado um. Este processamento é a ação descrita no *script* do Quadro X, que identifica a instância do LEC que excedeu aos limiares, registra em arquivo e notifica o operador informando o endereço ATM e o número da interface da conexão (VCI).

Figura 6.2.4-1 - Regra sec_BUSLEC para tratamento do evento 1511 relacionado aos possíveis ataques dos LECs ao BUS.



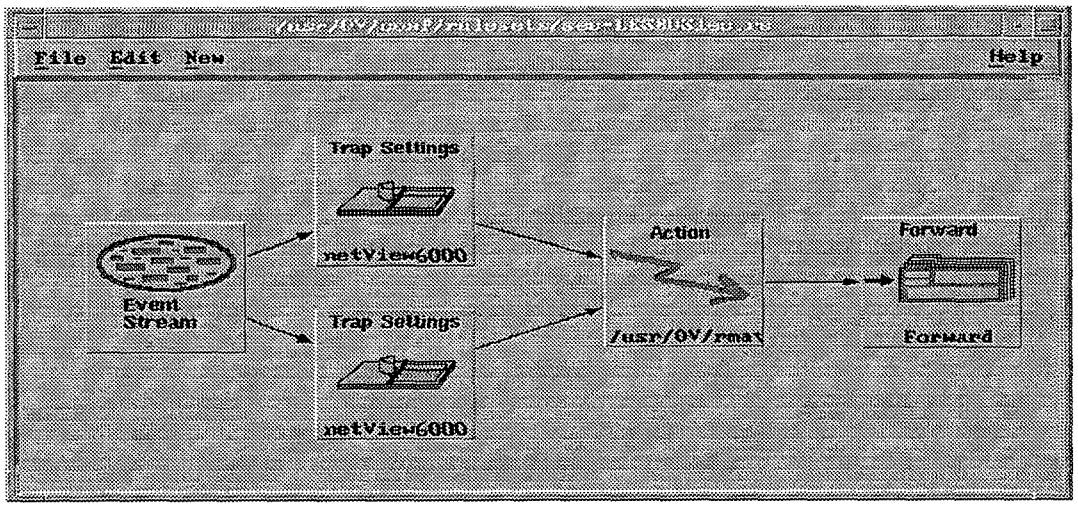
Quadro X - *Script* que define a ação tomada na regra sec_BUSLEC.

```
#!/bin/sh
# Coletar variaveis dos eventos netView6000 RMAVFLN_SEC_ BUSLEC.
# Parametros de entrada:
# NVATTR_2 : Hostname
# NVATTR_4 : Instancia
# NVC      : Comunidade
TMP=/tmp/.secBUSlec.tmp
LOGPATH=/usr/OV/rmav/log
LOGFILE=sec-BUSLEC.rs
SUBJECT="LOGFILE: secBUSlec"
CMDPATH=/usr/OV/bin
busLecAtmAddr=`$CMDPATH/snmpget -c $3 $1
.1.3.6.1.4.1.353.5.3.4.1.5.1.1.$2`
busLecMcastSendVci=`$CMDPATH/snmpget -c $3 $2
.1.3.6.1.4.1.353.5.3.4.1.5.1.5.$2`
cat > $TMP << __EOF__
Requisicoes do LEC nao registradas no LES:
 Servidor BUS      : $1
 Instancia         : $2
 Endereco ATM    : $busLecAtmAddr
 VCI          : $busLecMcastSendVci
__EOF__
cat $TMP >> $LOGPATH/$LOGFILE
cat TMP | mail -s "$SUBJECT" operator@rmav-fln.ufsc.br
rm -rf $TMP > /dev/null 2>&1
```

6.2.5. Requisições do LEC ao LES (BUS)

Para evitar os ataques de disponibilidade ao servidores LANE é interessante integrar as variáveis associadas ao LES e ao BUS. Como visto anteriormente a sobrecarga no BUS poderá reduzir o desempenho do serviço, bem como o tráfego denso com consultas ao LES através do número excessivo de requisições LE_ARP. A Figura 6.2.5-1 mostra o tratamento dos eventos 1511 e 1513 relacionados aos possíveis ataques dos LECs aos servidores LES e BUS. A ação identifica a instância em ambos servidores, registra e notifica o operador o endereço ATM do cliente, conforme *script* do Quadro XI.

Figura 6.2.5-1 - Regra sec_BUSLESLEC para tratamento dos eventos 1511 e 1513 relacionados aos possíveis ataques dos LECs ao BUS e ao LES.



Quadro XI - *Script* que define a ação tomada na regra sec_BUSLESLEC.

```
#!/bin/sh
# Coletar variaveis dos eventos netView6000 RMAVFLN_SEC_ BUSLESLEC.
# Parametros de entrada:
# NVATTR_2 : Hostname
# NVATTR_4 : Instancia
# NVC      : Comunidade
TMP=/tmp/.secBUSLESlec.tmp
LOGPATH=/usr/OV/rmav/log
LOGFILE=sec-BUSLESLEC.rs
SUBJECT="LOGFILE: secBUSLESlec"
CMDPATH=/usr/OV/bin
busLecAtmAddr=`$CMDPATH/snmpget -c $3 $1
.1.3.6.1.4.1.353.5.3.4.1.5.1.1.$2`
lesLecAtmAddr=`$CMDPATH/snmpget -c $3 $1
.1.3.6.1.4.1.353.5.3.3.1.8.1.9.$2`
cat > $TMP << __EOF__
Requisicoes do LEC nao registradas no LES:
 Servidor BUS      : $1
 Instancia         : $2
 Endereco ATM    : $busLecAtmAddr
 Endereco ATM    : $lesLecAtmAddr
__EOF__
cat $TMP >> $LOGPATH/$LOGFILE
cat $TMP | mail -s "$SUBJECT" root@srv01-ufsc.rmav-fln.ufsc.br
rm -rf $TMP > /dev/null 2>&1
```

7. CONCLUSÕES

Neste trabalho foram apresentados os procedimentos de controle de acesso para gerência de segurança em redes virtuais locais emuladas. Sendo que estes procedimentos baseiam-se em experimentos realizados em redes de alta velocidade, com um *backbone* ATM, no qual está implementado o serviço LANE, que possui políticas de segurança definidas pelo ATM *Forum* para prevenir e evitar diferentes ataques.

A pesquisa sobre ATM leva-nos a considerar, que esta tecnologia não está mais confinada somente ao contexto das B-ISDN. Portanto, a tecnologia ATM é também uma alternativa eficiente para integrar redes locais (*Ethernet* e *Token Ring*), de modo que utilizem as vantagens de seus recursos, como as aplicações B-ISDN (imagem gráfica, áudio, vídeo - multimídia) no intuito de obter melhor desempenho. Assim, percebe-se que o ATM tende a prevalecer nos *backbones*, enquanto que as tecnologias baseadas no *Ethernet*, predominam nos equipamentos de bordas. Os procedimentos de segurança para redes ATM estão restritos ao plano de usuário (mecanismos de autenticação, confidencialidade, integridade de dados, e controle de acesso) e ao plano de controle (mecanismos para autenticação e integridade); não incluindo o plano de gerenciamento. A dificuldade de acesso ao ATM pode ser a razão pela qual o registro de ataques neste ambiente não serem freqüentes.

Com a implantação do serviço LANE é possível executar aplicações existentes em redes locais (LANs) no ATM, de forma transparente, bem como utilizar novas aplicações desenvolvidas para o ATM, como se estivesse executando em redes locais tradicionais (*Ethernet* ou *Token-Ring*). Mesmo não explorando todos os benefícios do ATM, o LANE é útil na migração para a tecnologia ATM, por permitir que os investimentos em *software* e *hardware* sejam preservados.

No trabalho foram analisadas as diferentes categorias de ameaças ao serviço LANE – confidencialidade, integridade e disponibilidades, relacionando-as aos diversos ataques às redes locais virtuais: escuta, *spoofing*, negação de serviço, roubo de conexão virtual e análise de tráfego. Sendo que conexão virtual e análise de tráfego ocorrem apenas nas redes ATM. Para combater ou amenizar essas ameaças foram avaliadas as políticas de segurança definidas pelo ATM *Forum* e implementadas pelos fabricantes

(endereço ATM, endereço MAC, nome da ELAN, Tamanho Máximo de *Frame*, Descritor de Rota e Tipo da ELAN).

Os estudos foram realizados num ambiente de testes pré-estabelecido para tal finalidade, suportado pelas redes: RNP (POP-SC), RCT (POP-UFSC), redeUFSC, *Cluster* e RMAV-FLN, que permitiram a avaliação das políticas de segurança do serviço LANE a partir de uma solução proprietária - implementado pela IBM. Constatou-se que para obter maior confiabilidade, no que se refere a segurança, o ideal é a utilização de três políticas: endereço ATM, nome da ELAN e tipo da ELAN, com valores de prioridades diferentes.

Com a análise das ameaças ao serviço LANE foi possível estabelecer alguns procedimentos de controle às diversas camadas da rede ATM. A implementação desses procedimentos ficou restrita às ações preventivas e reativas configuráveis no sistema de gerência local ou remoto. Na gerência local foram configuradas as políticas de segurança para o LECS e para cada instância LES/BUS, isto é, só será permitido acesso aos LECs que possuírem o mesmo prefixo de rede (política byATMaddress), o mesmo nome da ELAN (política byElanName) e também com o mesmo tipo de ELAN (política byElanType), proporcionando assim, maior segurança aos recursos gerenciados. No sistema de registro de eventos, foram analisados os eventos associados a quebra de segurança nos subsistemas dos servidores LANE, e posteriormente configurados para enviar mensagens de alerta para o gerente remoto. À gerência remota ficou incumbida de coletar e analisar as variáveis estatísticas que representam erros e falhas nos servidores LANE. A ferramenta de gerência (*Netview*) permitiu fazer inferências sobre os eventos recebidos, bem como tomar ações corretivas e preventivas dos possíveis ataques analisados.

Para a realização deste trabalho, muitos desafios foram encontrados, dentre eles pode-se citar: 1) a compreensão do ambiente LANE, ATM e das MIBs, bem como da ferramenta de gerência, uma vez que os materiais encontrados, são manuais, artigos e especificações, sendo necessário tratamento diferenciado das informações; 2) configuração de um ambiente específico.

Este trabalho apresenta uma significativa contribuição a respeito de segurança em ambiente LANE, por ter proporcionado um estudo teórico/prático de como ampliar o nível de segurança utilizado nos recursos implementados no equipamento em questão.

Valendo do uso de políticas de segurança estabelecidas pelo ATM *Forum*, na sua especificação de gerenciamento af-lane-0057.000, sendo que estas são definidas no LECS.

O trabalho mostrou-se relevante por diversos motivos, dentre os quais destacam-se:

- A forma inovadora de gerenciamento de segurança em ambiente LANE utilizando variáveis de gerenciamento de Configuração e Falha da MIB af-lane;
- Habilitação de *traps* no roteador, os quais serão capturados pelo *software* de gerência, sendo selecionados os *traps* que contenham informações significativas por meio de filtros, em seguida essas informações são enviadas para o gerente via *e-mail* enviado por um *script*;
- Documentação detalhada de como fazer uso das políticas e benefícios por ela proporcionados.

A finalidade é que a gerência de segurança com o aumento do uso de redes de computadores tenha uma evolução significativa, sendo que este trabalho possa contribuir de alguma forma.

Ao término deste trabalho fica em aberto os seguintes segmentos para ampliar a pesquisa:

- Propor uma MIB que forneça dados relativos à segurança;
- Realizar um estudo de desempenho em uma ELAN que utiliza políticas de segurança e comparar o seu desempenho com uma ELAN que não faça uso das políticas de segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

[ALLES/95] ALLES, Antony. ATM Internetworking. In: Engineering InterOp. Las Vegas: Cisco Systems, Inc. May, 1995. http://www.cisco.com/warp/public/614/12.html.

[AFLANE/99] ALTMAN, Asher, BULLARD, Carter, FINKELSTEIN, Louis et al. AF-LANE-0112.000 - LAN *Emulation over* ATM *Version 2* – LNNI *Specification*, Feb., 1999a. ftp://ftp.ATMforum.com/pub/approved-specs/af-lane-0112.000.pdf

[BARB/00] BARBOSA, Gentil Veloso. Controle de conexões, sinalizações e fluxos de células em uma rede ATM utilizando Java e SNMP. Dissertação de Mestrado. Florianópolis, UFSC, 2000.

[CCIT/91] CCITT Recommendation I.321. B-ISDN *Protocol Reference Model And Its Application*. Geneva, 1991.

[CERUTTI/99] CERUTTI, Fernando Antônio. Implantação de um Ambiente de Gerência em Redes ATM Utilizando a Tecnologia WEB. Dissertação, Universidade Federal de Santa Catarina, Ago, 1999

[DOWN/2000] DOWNES, Kevin. FORD, Merille et al. *Internetworking: manual de tecnologias: uma referência essencial para todos os profissionais de rede*; tradução da 2.ed, Campus, 2000.

[FIPS/94] *Federal Information Processing Standards Publication* 188 (FIPS PUB 188). *Standard Security Label for Information Transfer* Set., 1994.

[IBM/99a] IBM *Corporation.* ATM *User`s Guide. Nways Manager* – ATM. *Version* 2.0.. USA, May., 1999. http://www.networking.ibm.com/support

[IBM/99b] IBM *Corporation. Interface Configuration and Software User`s Guide. Nways Multiprotocol Switched Service Serve. Version* 2.2. USA, *Edition* n. 5, Feb., 1999.

[ITU-T/95] ITU-T Recommendation Q.2931 (1995). *B-ISDN – Digital Subscriber Signalling System No. 2 (DSS 2) – User-Network Interface (UNI) Layer 3 Specification For Basic Call/Connection Control* – Telecommunication Standartization Sector of ITU – Series Q: B-ISDN Application Protocol for Access Signalling.

[JAIN/97] JAIN, Raj, *A Survey on* ATM *Security*, 1997. http://www.cis.ohio-state.edu/~jain/cis7887/ATM_security/index.htm

[KAUFM/95] KAUFMAN, C., PERLMAN, R. & SPECINER, M. *Network Security, Private Communication in a public world*. Englewood Cliffs NJ 07632. Prentice Hall, 1995.

[LANE21/95] ALTMAN, Asher, BULLARD, Carter, FINKELSTEIN, Louis et al.*The* ATM *Forum Technical Committee*: LAN *Emulation Over* ATM, *Version 1.0*, af-LANE-0021.000, Jan., 1995. ftp://ftp.ATMforum.com/pub/approved-specs/af-lane-0021.000.mib.

[LANE57/96] ALTMAN, Asher, BULLARD, Carter, FINKELSTEIN, Louis et al.The ATM *Forum Technical Committee*: LAN *Emulation Servers Management Specification 1.0*, af-LANE-0057.000 – Mar., 1996. ftp://ftp.ATMforum.com/pub/approved-specs/af-lane-0057.000.mib

[LAUREN/96] LAURENT, Maryline. *Security Flows Analysis of the* ATM *Emulated* LAN *Architecture*. IFIP, *Conference on Communications and Multimedia Security*. Essen, Germany, Set.,1996. ftp.rennes.enst-bretagne.fr/pub/security/ml_CFIP96.ps.gz

[REINERT/97] REINERT, R. R. & SOUZA, A. Implantação de uma Rede ATM Integrada com a redeUFSC. Monografia, Universidade Federal de Santa Catarina, Nov, 1997.

[SEC100/99] ALTMAN, Asher, BULLARD, Carter, FINKELSTEIN, Louis et al. The ATM *Forum Technical Committee*: ATM *Security Specification Version* 1.0 AF-SEC-0100.000. Feb., 1999b. Ftp://ftp.ATMforum.com/pub/approved-specs/af-sec-0100.000.pdf

[SOARES/95] SOARES, Luiz Fernando G. Redes de Computadores: das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Ed. Campus, 2ª edição, 1995.

[TANENB/96] TANENBAUM, Andrew S. Redes de Computadores (Tanenbaum, A., trad. da terceira edição). Rio de Janeiro: Ed. Campus, 1997 (trabalho original publicado em 1996).

[VOYDO/83] VOYDOCK, V. L. & KENT, S. T. *Security mechanisms in high-level network protocols*. ACM *Computing Surveys*, Vol 15, n. 2, 1983.

ANEXO 1 - MIBS DOS SERVIDORES LANE

LAN Emulation Servers Management Specification 1.0

Af-lane-0057.000 – ATM *Forum* – March, 1996.

Esta especificação cobre as seguintes áreas de gerenciamento: Configuração, Desempenho e Falhas; e não são contempladas as áreas de Segurança e Contabilização.

DESCRIÇÃO DA ELAN.MIB

Esta MIB gerência as mudanças de configuração das ELAN através de um repositório de informações estáticas.

Grupo de Administração da ELAN

Fornece um registro para os tipos de políticas para conexão do LEC. A definição dessas políticas é representada pela tabela elanAdminPolicyVal.

elanAdminPolicyVal	byAtmAddr byMacAddr byRouteDescriptor byLanType byPktSize byElanName

Grupo de Configuração da ELAN

Fornece informações de configuração sobre as ELANs, bem como informações do LES relacionados a uma ELAN, conforme tabelas a seguir.

Tabela de Configuração

A tabela elanConfTable lista todas as ELANs, as quais o agente mantém informações. Uma ELAN é definida pelo nome, um grupo de TLVs, e outros parâmetros. Uma ELAN é composta de quatro entidades: LECS, LES, BUS e LEC. Sendo que o suporte ao LECS é opcional.

elanConfName	O nome desta entrada LAN Emulation. Quando o tamanho deste objeto é zero o nome da ELAN não é especificado. Os clientes designados para esta ELAN também deverão ter uma string de tamanho zero como o nome da ELAN. O valor deste objeto é usado na resposta de configuração LAN Emulation para o LECS, se este for suportado.
elanConfLanType	O tipo da ELAN desta entrada ELAN

Tabela LES

A tabela elanLesTable lista todos os LES associados com as ELAN gerenciadas pelo agente. Cada ELAN pode ter mais de um LES disponibilizando serviços LANE. Cada LES pode servir apenas uma ELAN. Todas as tabelas de definição do LEC são indexadas pela ELAN (elanConfIndex) e LES (elanLesIndex) para permitir a seleção de um endereço LES específico para qualquer cliente dentro da ELAN.

elanLesIndex	Número arbitrário que identifica unicamente o LES da elan.
elanLesAtmAddress	O endereço ATM do LES. Se o LECS for suportado, o LECS retorna o endereço ATM do LES para o LEC. Se o LECS não for suportado, o valor deste objeto permanece o endereço disponibilizado pelo gerente da rede.

Tabela de Políticas

A tabela elanPolicyTable descreve as políticas em uso, definidas pelo LECS para uma particular ELAN e LES. Um grupo de políticas pode ser selecionado pelo LECS com prioridades (elanPolicyPriority) iguais ou diferentes, onde prioridades baixas são avaliadas primeiro e prioridades iguais são avaliadas ao mesmo tempo com operador E.

elanPolicyPriority	A prioridade desta política. Políticas são avaliadas pela entidade a qual provê serviços de configuração da ELAN (LECS). Políticas com a mesma prioridade deverão ser avaliadas ao mesmo tempo com o operador E. O valor 1 tem a mais alta prioridade.
elanPolicyType	O valor deste objeto deve referenciar uma definição de tipo da política. Algumas das definições estão na sub-árvore elanAdminPolicyVal. Outras formas podem ser definidas na sub-árvores enterprise.

Tabela Definição do LEC por Endereço ATM

Indexada pelo index da ELAN o qual aponta para a ELAN do LEC no LES usando o endereço ATM.

Tabela Definição do LEC por Endereço MAC

Indexada pelo index da ELAN o qual aponta para a ELAN do LEC no LES usando o endereço MAC.

Tabela Definição do LEC por Descrição de Rota

Indexada pelo index da ELAN o qual aponta para a ELAN do LEC no LES usando a descrição de rotas.

Grupo de Configuração do LECS

Abilita os gerentes de rede a configurar e monitorar LECSs.

Tabela de Configuração

A tabela lecsConfTable contém as configurações e informações de status para todos os LECSs gerenciados pelo agente. Usada para criar, excluir ou configurar um LECS.

lecsConfIndex	Um inteiro arbitrário que representa um LECS deste agente gerenciado.
lecsAtmIfIndex	Uma interface ATM na qual o LECS recebe requisições de configuração. Este valor deve ser igual a um valor existente na ifTable. Este objeto é configurado para zero quando a interface ATM não é especificada ou há mais de uma interface ATM sendo usada pelo LECS.
lecsAtmAddrSpec	Um endereço ATM especificado pela rede ou gerente local que, com a máscara do endereço ATM, determina a parte do endereço ATM que o LECS na interface ATM determinada usará para derivar o atual endereço ATM da rede ou LMI.
lecsAtmAddrMask	A máscara do endereço ATM associado com com o objeto lecsAtmAddrSpec.
lecsAtmAddrActual	O endereço ATM resultante do LECS aceita requerimentos de configuração na interface indicada pelo objeto lecsAtmIfIndex. Este endereço é o resultado do endereço ATM especificado, sua máscara e interação através do ILMI com o comutador. Este objeto só será válido quando o lecsOperStatus correspondente estiver ativo.
lecsPolicySelIndex	Grupo de políticas usadas pelo LECS em requerimentos de determinação de membros ELAN. As políticas são definidas na elanPolicyTable. O valor deste objeto deve existir na elanPolicyTable.
LecsLastInitialized	O valor do sysUpTime desde que o LECS foi ativado novamente através do objeto lecsOperStatus.
lecsOperStatus	Este objeto reflete o estado atual do LECS o qual pode diferir do

	objeto lecsAdmnStatus. Podendo ocorrer quando a interface ifOperStatus estiver desativada, mesmo que o lecsAdminStatus esteja ativo.
lecsAdminStatus	O estado desejado do LECS nesta interface como prescrito pelo operador. A ação do agente deverá eventualmente resultar no estado desejado sendo refletido no lecsOperStatus.

Tabela de Mapeamento

A tabela LecsElanTable contém o mapeamento entre ELANs e LECS. Quando o LECS é deletado do lesConfTable, todas as entradas associadas a esta serão deletadas.

LecsElanRowStatus	Este objeto é usado para criar ou deletar uma entrada nesta tabela.

Tabela TLV

Usada para configurar TLVs (Type, Length, e Value) no LECS. Estes grupos podem incluir não apenas o padrão TLV especificado na especificação LANE (Spec. 1.0 [1]) embora também os parâmetros adicionais trocados entre o LECS e o LEC. Esta tabela é indexada por um index selecionador, o qual permite mais de uma TLV ser selecionada por uma ELAN; e a TLV tag. O qual especifica o tipo de TLV; e a TLV index a qual é usada para distinguir entre diferentes entradas com o mesmo TLV tag. Como fazer o LECS tratar as TLVs que não estão especificadas nesta tabela de requisição de configuração não definido nesta MIB.

lecsTlvSelectorIndex	O valor deste objeto indica um grupo de TLVs que podem ser selecionadas.
lecsTlvTag	O valor deste objeto representa o tipo do conteúdo do lecsTlvVal que falharam na entrada.
lecsTlvIndex	O índice de entrada TLV. O valor deste objeto pode ser usado para distinguir entre diferentes entradas com o mesmo valor de lecsTlvTag.
LecsTlvVal	O valor de entrada TLV.
lecsTlvRowStatus	Este objeto é usado para criar ou destruir entradas nesta tabela.

Tabela de VCC

Esta tabela contém todas as conexões de configuração do LECS. As conexões de configuração são usadas pelo LEC para enviar/receber requisições/respostas de

configuração paro/do LECS. Esta tabela pode ser modificada se um PVC for usado ou somente leitura se um SVC for usado.

LecsVccIfIndex	A interface ATM na qual a configuração VCC é estabelecida. Este valor deve existir na tabela ifTable. O valor deste objeto é configurado para zero quando a interface ATM for uma conexão interna.
LecsVccVpi	O valor VPI da configuração VCC. O objeto lecsVccIfIndex, lecsVccVci e este objeto identificam unicamente um VCC em um sistema ATM.
LecsVccVci	O valor VCI da configuração VCC. O objeto lecsVccIfIndex, lecsVccVpi e este objeto identificam unicamente um VCC em um sistema ATM.
LecsVccRowStatus	Este objeto é usado para criar ou destruir entradas nesta tabela.

Grupo de Estatísticas do LECS

Fornece estatísticas dos contadores de erro no LECS.

Tabela de estatísticas

Lista todos os contadores associados com o LECS no agente.

lecsStatSuccessful	O número de requisições de configuração com sucesso desde a última vez que o agente foi inicializado.
lecsStatInBadFrames	O número de requisições de configuração mal formadas e excluídas pelo LECS.
lecsStatInvalidParam	O número de requisições de configuração rejeitadas devido a erros nos parâmetros da requisição.
lecsStatInsufRes	O número de requisições de configuração rejeitadas devido à insuficiência de recursos.
lecsStatAccDenied	O número de requisições de configuração rejeitadas devido a acesso negado.
lecsStatInvalidReq	O número de requisições de configuração rejeitadas por ter o identificador inválido.
lecsStatInvalidDest	O número de requisições de configuração rejeitada por ter destino inválido.
lecsStatInvalidAddr	O número de requisições de configuração rejeitadas por ter endereço ATM inválido.
lecsStatNoConf	O número de requisições de configurações rejeitadas devido ao LEC não reconhecer o erro.
lecsStatConfError	O número de requisições de configuração rejeitadas devido a erro LE_CONFIGURE.
lecsStatInsufInfo	O número de requisições de configuração rejeitadas por falta de informação.

Grupo de Gerenciamento de falhas do LECS

Tabela de Controle de Erros

A tabela lecsErrCtlTable é usada para controlar erros de *log* no LECS. O gerente da rede pode habilitar ou desabilitar erros de *log* (error logging) de um LECS particular gerenciado pelo agente. Também pode reinicializar o erro de *log* de um LECS. O LECS deve limpar todos as entradas de erros de *log* requisitadas.

lecsErrCtlAdminStatus	Este objeto é usado para habilitar/desabilitar registro de erros de (*log* de erros) para o LECS.
lecsErrCtlOperSatatus	Indica o resultado do objeto lecsErrCtlAdminStatus. Valores Possíveis: other(1) – não especificado; active (2) – registrando erros; outOfRes(3) – saída do buffer; failed (4) – falha ao iniciar o *log* de erros; disable (5) – registro desabilidado.
lecsErrCtlClearLog	Este objeto é usado para limpar entradas de erros associadas com este LECS.
lecsErrCtlMaxEntries	Número de máximo de entradas de erros de *log* que um LECS pode suportar.
lecsErrCtlLastEntry	O índice para a última entrada de erro na tabela de *log* associada com este LECS.

Tabela de Erros

A tabela lecsErrLogTable contém erros de *logs* das instâncias do LECS abilitadas na tabela lecsErrCtlTable. Cada entrada descreve quando o erro ocorreu, a natureza do erro e o endereço ATM do cliente cuja requisição resultou em erro.

LecsErrLogIndex	Um inteiro arbitrário que identifica unicamente uma entrada de erro.
lecsErrLogAtmAddr	O endereço ATM do requisitor que enviou uma requisição de registro e causou um erro. O erro correspondente é especificado pelo objeto lecsErrLogErrCode.
lecsErrLogErrCode	O código que indica a causa do erro ocorrido durante a requisição de registro enviado pelo requisitor identificado pelo objeto lecsErrLogAtmAddr.
LecsErrLogTime	O tempo (sysUpTime) desde quando a entrada foi registrada pelo LECS.

DESCRIÇÃO DA LES.MIB

Módulo da MIB para gerenciamento ATM em servidores LANE.

Grupo Configuração do LES

Tabela de Configuração

A tabela lesConfTable contém todos os servidores de LANE deste agente gerenciado.O LES é um dos componentes na ELAN que implementa a função de condenação de controle.

lesConfIndex	O valor que indica unicamente uma linha conceitual no lesConfTable.
lesAtmAddrSpec	Um endereço ATM (especificado pela rede ou gerenciamento local) e a máscara deste endereço determinam a parte do endereço ATM do LES em uma determinada interface ATM, a qual será usada para direcionar o endereço ATM atual pela rede ou ILMI.
lesAtm AddrMask	O endereço ATM da máscara associado com o objeto lesAddrSpec.
lesAtmAddrActual	O endereço ATM resultante em uso pelo LES. Este objeto é um produto do endereço ATM especificado, máscara e interação com a rede. Este objeto é criado pelo agente.
lesElanName	O nome da ELAN deste LES.
lesLanType	Identifica o tipo da ELAN no LES.
lesLastChange	O tempo (sysUpTime) desde quando o LES entrou no estado indicado pelo objeto lesOperStatus.
lesMaxFrame	O tamanho máximo AAL-5 SDU de *frames* de dados que o LES pode garantir.
lesControlTimeOut	Período de tempo entre interações de *frames* de requisição e resposta.
lesOperStatus	Estado operacional desta entrada LES.
lesAdminStatus	O estado desejado do LES designado pelo operador.
lesRowStatus	Objeto usado pra criar ou destruir entradas na elanConfTable.

Tabela de VCC

Lista todas as conexões de controle distribuídas usadas no LES para distribuir tráfego de controle para os LECs participantes.

lesVccAtmIfIndex	A interface ATM na qual a distribuição de controle VCC está executando.
lesVccCtlDistVpi	O valor VPI do eontrole de distribuição VCC.
lesVccCtlDistVci	O valor VCI do controle de distribuição VCC.
lesVccRowStatus	Este objeto é usado para criar ou destruir entradas na elanConfTable.

Tabela ARP para Endereço MAC

A tabela lesLeArpMacTable fornece acesso a tabela de resolução MAC-ATM. Contém entradas para endereços Unicast e endereços broadcast.

lesLeArpMacAddr	Endereço MAC no qual a tabela fornece a resolução.Quando o LES usa o LE-ARP no BUS o valor deste objeto será o endereço MAC broadcast.
lesLeArpLecId	LECID da entrada. Se a entrada for do BUS este valor é zero.
lesLeArpAtmAddr	Endereço ATM do BUS ou do LEC cujo MAC é estocado em lesLeArpMacAddr.
lesLeArpEntryType	Indica como a entrada LE-ARP foi criada. Possíveis valores: viaRegister (1) – agente, staticVolatile (2) – gerente ou staticNonVolatile (3) – gerente.

Tabela ARP para Descritor de Rotas

A tabela lesLeArpRdTable fornece acesso ao cache de resolução RouteDescriptor-ATM. As entradas nesta tabela são configuradas pelo agente ou pelo gerente da rede dependendo do tipo de entrada.

lesLeArpRdSegId	Identificação da LAN como descritor de rota na IEEE 802.5 associado com este LES.
lesLeArpRdBridgeNum	Número da Bridge como descritor de rota na IEEE 802.5 associado com este LES.
lesLeArpRdLecId	LECID da entrada.
lesLeArpRdAtmAddr	Endereço ATM associado com o descritor de rota.
lesLeArpRdEntryType	É usado para indicar como a entrada LE-ARP aprendeu. Possíveis valores: viaRegister(1) – agente, staticVolatile(2) – gerente ou staticNonVolatile(3) – gerente.

Tabela de Topologia : LES-LEC

A tabela lesLecTable lista todos os clientes servidos pelos LESs especificados na tabela lesConfTable. Esta tabela pode ser usada para a topologia de uma ELAN, i.e. o mapeamento dos LECs de cada LES.

lesLecIndex	Um inteiro arbitrário com identificação única.
lesLecAtmAddr	Endereço ATM do cliente LANE. Este é o endereço ATM primário usado na fase de conexão (join).
lesLecProxy	Clientes *Proxy* são permitidos a representar endereços MAC não registrados e receber cópias de pacotes LE_ARP_REQUEST para tais endereços.
lesLecId	Identificação do LEC. O LECID é trocado em requisições de controle e deve ser usado em *frames* multicast.
lesLecAtmIfIndex	O IfIndex da porta ATM onde o LEC estabeleceu uma conexão de controle direto para o LES. O valor deste objeto mapea o ifIndex na tabela ifTable da MIB-II.
lesLecCtlDirectVpi	O VPI da conexão direta biredicional entre o LEC e o LES.
lesLecCtlDirectVci	O VCI da conexão direta biredicional entre o LEC e o LES.
lesLecLastChange	O valor sysUpTime da entrada indicado pelo estado do LEC – lesLecState.
lesLecState.	Valores possíveis: other (1) – estado desconhecido; noLesConnect (2) – LEC não esta conectado no LES; lesConnect (3) – LEC estabeleceu uma conexão VCC para o LES; joining (4) – O LES recebeu uma requisição de join do LEC; addLec (5) – LES configurou o VCC deste LEC; joinnedLes (6) – O LEC foi conectado com sucesso.

Grupo Estatística no LES

Contém todos os contadores dos LESs, de acordo com a tabela lesConfTable. Fornece contadores de falhas e desempenho em um LES base, conforme tabela LesStatTable descrita a seguir.

Tabela Estatística do LES

LesStatJoinOK	Número de respostas enviadas para o LES notificando o sucesso da conexão (join).
LesStatVerNotSup	Número de erros referentes a versões não suportadas.
LesStatInvalidRegParam	Número de erros referentes a parâmetros de requisição inválidos.
LesStatDupLanDest	Número de erros referentes a destino LAN duplicado.
LesStatDupAtmAddr	Número de erros referentes a endereço ATM duplicado.
LesStatInsRes	Número de erros referentes a recursos insuficientes.
LesStatAccDenied	Número de erros referentes a acesso negado por razões de segurança.
LesStatInvalidRegId	Número de erros referentes a LECID inválido.
LesStatInvalidRegLanDest	Número de erros referentes a destino LAN inválido.
LesStatInvalidAtmAddr	Número de erros referentes a endereço ATM inválido.

LesStatInBadPkts	Número de erros referentes a requisições ARP ATM mal formadas .
LesStatOutRegFail	Número de falhas de registros enviadas pelo LES.
LesStatLeArpIn	Número total de *frames* LE_ARP_REQUEST aceitos pelo LES desde sua última inicialização.
LesStatLeArpFwd	Número total de *frame* LE_ARP_REQUEST repassado para os elientes.

Grupo Estatística no LES-LEC

Tabela de Clientes no LES

A tabela lesLecStatTable contém todas as requisições LE-ARP relacionadas com os contadores e erros em um par LEC-LES.

lesLecRecvs	Número de requisições recebidas deste LEC. Inclui todos os *frames* de controle assim como as requisições LE-ARP.
lesLecSends	Número de requisições ou respostas enviadas para a entrada LEC deste LES. Número de requisições registradas e recebidas deste LEC.
lesLecInRegReq	Número de requisições de registro recebidas deste LEC.
lesLecInUnReg	Número de requisições não registradas recebidas deste LEC.
lesLecInLeArpUcast	Número de requisições LE-ARP recebidas com endereços Unicast deste LEC.
lesLecInLeArpBcast	Número de requisições de LE-ARP recebidas com endereços Multicast e Broadcast deste LEC.
lesLecInLeArpResp	Número de respostas LE-ARP recebidas deste LEC.
lesLecInNArp	Número de requisições NARP reeebidas deste LEC.
lesLecLastChange	Tempo que a entrada LEC esta ativa, indicada pelo objeto lesLecState.

Grupo Gerenciamento de Falhas no LES

Tabela de Controle de Erros

A tabela lesErrCtlTable é usada para controlar erros de *log* no LES. O gerente da rede pode habilitar ou desabilitar erros de *log* (error logging) de um LES particular gerenciado pelo agente. Também pode reinicializar o erro de *log* de um LES.

lesErrCtlAdminStatus	Este objeto é usado para habilitar/desabilitar o registro de erros (*logs* de erros) no LES.
lesErrCtlOperSatatus	Indica o resultado do objeto lecsErrCtlAdminStatus. Valores Possíveis: other(1) – não especificado; active (2) – registrando erros; outOfRes(3) – saída do buffer; failed (4) – falha ao iniciar

	o *log* de erros; disable (5) – registro desabilidado.
lesErrCtlClearLog	Este objeto é usado para limpar as entradas de erros associadas com este LES.
lesErrCtlMaxEntries	Número de máximo de entradas de erros que um LES pode suportar.
lesErrCtlLastEntry	O índice para a última entrada de erro na tabela de *log* associada com este LES.

Tabela de Erros : LEC

A tabela lesErrLogTable contém erros de *logs* das instâncias do LES abilitadas na tabela lesErrCtlTable. Cada entrada descreve quando o erro ocorrido, a natureza do erro e o endereço ATM do cliente cuja requisição resultou em erro.

lesErrLogIndex	Um inteiro arbitrário que identifiea unicamente uma entrada de error.
lesErrLogAtmAddr	O endereço ATM do requisitor que enviou uma requisição de registro e causou um erro. O erro correspondente é especificado pelo objeto lesErrLogErrCode.
lesErrLogErrCode	O código que indica a causa do erro ocorrido durante a requisição de registro enviado pelo requisitor identificado pelo objeto lesErrLogAtmAddr.
LesErrLogTime	O tempo (sysUpTime) desde quando a entrada foi registrada pelo LES.

DESCRIÇÃO DA BUS.MIB

Grupo Configuração

Tabela Configuração

Lista todas as entidades gerenciadas do BUS pelo agente.

Tabela VCC

Lista todas as conexões de repasse multicast usadas no BUS para repassar o tráfego multicast para os LECs participantes.

Tabela Topologia BUS-LEC

Lista os LECs que estão servidos pelo BUS. Pode ser usada para determinar o mapa entre BUSs e LECs.

Grupo Estatística

Tabela Estatística

Contém todos os contadores mantidos pelo BUS. Esta tabela esta relacionada com a tabela busConfTable.

Tabela Estatística BUS-LEC

Contém todos os contadores LEC contidos no BUS.

Grupo Gerenciamento de Falhas BUS

Tabela de Controle de Erros

A tabela busErrCtlTable é usada para controlar erros de *log* no BUS. O gerente da rede pode habilitar ou desabilitar erros de *log* (error logging) de um BUS particular gerenciado pelo agente. Também pode reinicializar o erro de *log* de um BUS.

Tabela de Erros : BUS

A tabela busErrLogTable contém erros de *logs* das instâncias do BUS abilitadas na tabela busErrCtlTable. Cada entrada descreve quando o erro ocorrido, a natureza do erro e o endereço ATM do cliente cuja requisição resultou em erro.