Controle de Acesso em Gerência de Segurança para a redeUFSC

Elvis Melo Vieira
E-mail: elvis@npd.ufsc.br

Maria Cristina Boschetta
E-mail: cristina@inf.ufsc.br

Carlos B. Westphal
E-mail: westphal@inf.ufsc.br

Núcleo de Processamento de Dados - NPD
Departamento de Informática e Estatistica - INE
Universidade Federal de Santa Catarina, Florianópolis, SC

Resumo

Neste trabalho, apresenta-se um mecanismo para controle de acesso via linha discada à redeUFSC. Ele permite que os usuários possam conectar-se a rede e tornem-se, eles próprios, um nó e não apenas uma emulação de terminal. Este mecanismo é muito importante para garantir a segurança e o gerenciamento da rede. Seu foco principal está direcionado para o gerenciamento de segurança usando uma função específica para controlar o acesso por linhas discadas à rede.

Abstract

In this paper, a mechanism to control the remote access throught dial line up to UFSC Network is presented. It permits that the users can get connections the network while becoming, themselves, a node and, not, an emulated terminal. This mechanism is very important for graranteeing the security and management of the network. Its main focus is directed to the management of security by using a especific function for control line the access to network

1 Introdução

O crescimento da abrangência e do número de usuários está tornando a gerência operacional de redes um elemento dinâmico e vital para o planejamento de outras áreas da informática.

Com o dinamismo existente numa rede de computadores, a equipe de gerência deve possuir um certo preparo para solucionar os constantes problemas que surgem no dia a dia. Uma gerência operacional eficaz é imprescindível para que as falhas sejam solucionadas o mais

rapidamente possível , de preferência, sem que o usuário sinta a perda do serviço pretendido. Em função destes e de outros fatores que envolvem a gerência de uma rede, é que se diz gerenciar uma rede significa manter sob controle todo o seu funcionamento, abrangendo entre outras atividades, o controle da configuração da rede, do acesso aos recursos compartilhados e a manutenção do tráfego em níveis aceitáveis [1].

Vários aspectos devem ser analisados na gerência de uma rede. Estes aspectos são classificados nas cinco áreas funcionais abaixo:

1. **Gerência de Configuração:** Envolve o controle da configuração da rede e de seus recursos, instantânea ou periodicamente, visando alcançar as configurações de trabalho desejáveis. Deve permitir uma visão geral da estrutura do sistema.

2. **Gerência de Performance**: Envolve a monitoração e o controle de todos os recursos visando acompanhar sua performance individual e da rede como um todo, dentro de certos níveis predefinidos. Deve permitir medições e informações sobre a disponibilidade de recursos, taxas de utilização, tempo de resposta, etc.

3. **Gerência de Falhas:** é o monitoramento e o controle das falhas ocorridas nos diversos recursos, o que significa detectar, isolar e corrigir problemas nos componentes. Inclui a manutenção de arquivos de *log* de erros, manipulação de alertas, execução de diagnósticos e procedimentos de correção de erros.

4. **Gerência de Segurança** : Visa controlar o acesso e a integridade dos recursos e das informações na rede através de mecanismos de autorização e autenticação de acesso, manutenção de arquivos com registros de acesso e tentativas de violação dos procedimentos de segurança, alertas sobre tentativas de invasão, prevenção de vírus e auditoria das operações realizadas.

2 Gerência de Segurança

Na Arquitetura de Segurança do Modelo de Gerência OSI são definidos cinco serviços de segurança [1]:

- **autenticação** tanto de entidades pares quanto da origem dos dados;
- **confidencialidade** dos dados;
- **controle de acesso** aos recursos e dados da rede
- **não-rejeição** de serviços e dados para usuários legítimos.

Os serviços de segurança são providos por mecanismos de segurança, os quais têm a função de garantir que a política de segurança estabelecida para a rede seja cumprida. Para compreender como se define uma política de segurança convém, antes, adquirir-se conhecimento em segurança de redes.

3 Segurança de Redes

Além de se ter mecanismos bem elaborados para proteger a rede de adversários e de ameaças naturais (acidentes), faz-se necessário também a determinação de políticas claras de segurança, e o correto esclarecimento das pessoas para evitar que a definição dos mecanismos a implantar seja feita de forma empírica, e também, evitar que ocorra displicência no tratamento da segurança em relação ao sistema. Antes de se definir uma política de segurança, e desenvolver mecanismos que atendam a esta política, é necessário que seja feita a determinação do que precisa ser protegido, o que é necessário proteger, do que e como proteger [11]. Para isso dois elementos devem ser elaborados:

- Identificação dos recursos;
- Identificação dos problemas;

Quando feita a identificação dos recursos, algumas coisas podem ser óbvias e outras podem ser negligenciadas. Para auxiliar nesta identificação é conveniente listar todos os recursos que poderiam ser afetados por algum problema de segurança.

Após a identificação dos recursos que requerem proteção, é necessário associar a eles os problemas possíveis de ocorrerem. Esta associação ajuda na identificação de quais problemas está requerendo proteger os recursos da rede. A seguir estão descritos alguns dos problemas mais comuns de ocorrer:

Acesso não autorizado: O acesso não autorizado aos recursos da rede e/ou informações armazenadas ou transitando pela mesma pode ocorrer de muitas formas diferentes. entre estas formas estão: o uso de cadastro (conta , senha) de um outro usuário para conseguir ter acesso ao sistema, o uso de qualquer recurso sem permissão, o acesso à rede via linha discada por um usuário que não possui permissão para tal tipo de serviço, etc;

Descoberta de Informações: Determina o valor ou a sensibilidade da informação armazenada. A descoberta de um arquivo de senhas, por exemplo, pode permitir um futuro acesso não autorizado;

Negação de Serviço: Devido a possibilidade de compartilhamento de recursos, as redes provêm vários serviços aos seus usuários, e estes serviços auxiliam na execução dos trabalhos destes usuários. Portanto, quando um usuário legítimo não consegue ter acesso a um recurso ou serviço ao qual ele tem direito, ocorre uma perda na sua produtividade.

Segurança em informática pode ser considerada como a garantia ou confiança que os usuários têm em determinados sistema [3]. Dentre os diversos pontos de interesse da confiabilidade em redes de computadores, se destacam dois pontos importantes: a proteção dos elementos que compõem a rede (servidores, interfaces, meios de comunicação, pontos de acesso, etc), e o gerenciamento dos recursos. Quanto maior e mais heterogêneo for o sistema de redes de computadores, mais o sistema está exposto a possíveis ameaças, sendo o serviço de acesso ao sistema por linha discada, por exemplo, um dos serviços de considerável importância quando da fixação de políticas e mecanismos de segurança que sejam capazes de proteger as instalações da rede de possíveis ataques externos.

4 Modelos de Gerência

Qualquer modelo de gerência de redes é caracterizado por dois aspectos [1]:

i) a Estrutura de Informação de Gerenciamento (ou ***SMI-Struture Management Information***) ; e

ii) as **operações de gerenciamento** do protocolo suporte.

A *SMI* define as regras de como os objetos gerenciáveis são descritos e como ter acesso às operações do protocolo de suporte. As operações de gerenciamento especificam as primitivas, implementadas pelo protocolo de suporte, disponíveis para o usuário manipular a informação de gerenciamento.

Os processos de gerenciamento podem assumir duas formas: de **gerente** que envia pedidos e recebe respostas ou notificações; ou de **agente** que responde a pedidos ou envia notificações ao gerente.

A definição de um **objeto gerenciado** é usado como uma abstração de um recurso real da rede, o qual pode ser lógico ou fisico. O conjunto de definições das informações de gerenciamento sobre recursos é especificado na **Base de Informações de Gerenciamento - MIB** [5].

Dois modelos de gerência são mais relevantes no contexto atual: o **Modelo OSI** da ISO [1] e o **Modelo Internet**, que diferem basicamente na SMI empregada e nas operações do protocolo de gerenciamento.

5 Modelo de Gerência Internet

A estrutura de informações de gerenciamento do modelo Internet é mais simples, onde as próprias variáveis são consideradas como objetos, enquanto no modelo OSI são atributos de objetos, portanto, é dito que o modelo *Internet* é baseado em objetos.

Os objetos no Modelo de Gerência *Internet* são especificados usando-se a *Structure Management Information - SMI* [8], que apresenta os modelos da MIB para a Internet. O protocolo usado para manipular as informações de gerência no modelo *Internet* é o *Simple Network Management Protocol- SNMP* [2]. As operações polimorfas neste modelo são:

a) Inicializadas pelo gerente: ***Get***, para obter o valor de uma variável; ***GetNext***, para obter, seqüencialmente, os valores de uma variável; e ***Set***, para atribuir um novo valor a uma variável.

b) Inicializada pelo agente: ***Trap***, para informar o gerente da ocorrência de algum evento.

O código de um agente geralmente envolve a manipulação de estruturas complexas do núcleo do sistema operacional, tornando a adição de novos agentes por parte de usuários pode ser difícil, mesmo que ele não necessite utilizar tais estruturas. Em vista disso, muitas implementações fornecem um protocolo que permite ao usuário escrever processos, os quais são chamados **processos usuários**, bem menos complexos. Um **processo usuário**, é portanto, um processo que comunica-se com o agente SNMP local e implementa os objetos por ele gerenciados em uma MIB privada, ou seja, que não são definidos no conjunto padronizado dos objetos da MIB (MIB-I e MIB-II) da *Internet*.

Quando um processo usuário é criado ele precisa comunicar-se com um agente SNMP, e, uma das maneiras de estabelecer esta comunicação é através do protocolo SMUX [10], que é um protocolo multiplexador do SNMP. Este protocolo é muito utilizado quando o sistema operacional é um Unix. O processo usuário que comunica-se diretamente com o agente SNMP, via SMUX, pode também ser chamado **par SMUX**.

Quando um processo usuário, condicionado ao SMUX, deseja exportar um módulo de sua MIB, ele inicia uma conexão SMUX com o agente SNMP local. Ele solicita ao agente o registro da subárvore do(s) objeto(s) por ele implementado(s), e atende as operações de gerenciamento sobre estes objetos em um módulo da sua MIB.

A figura 1 ilustra a comunicação entre agente SNMP e o processo usuário através do protocolo SMUX:

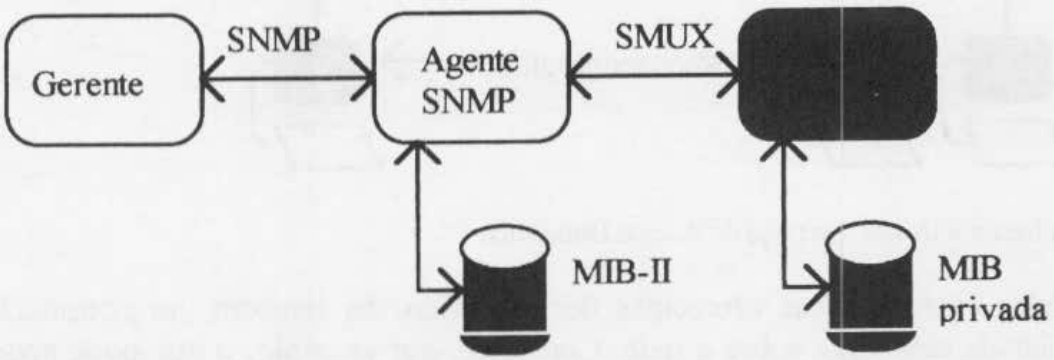


Figura 1 - Protocolo Multiplexador do SNMP - SMUX

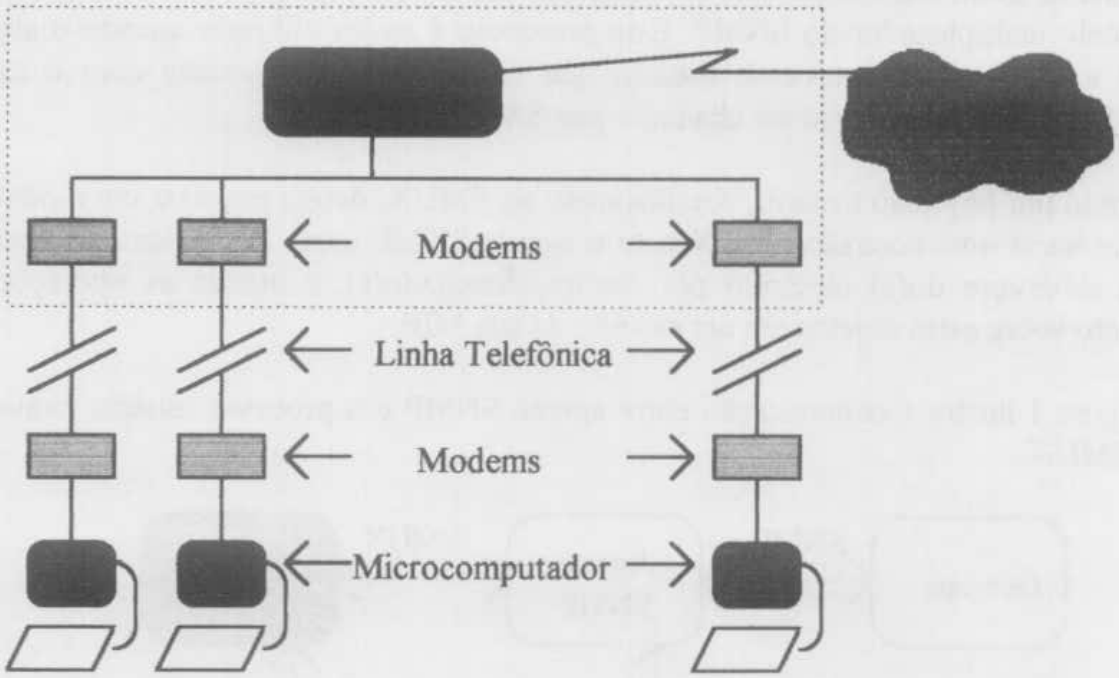
6 Serviço de Acesso Discado

Conhecido também por "Acesso Doméstico", o acesso por linha discada é um serviço oferecido por uma rede particular, com o qual é possível ter acesso aos recursos computacionais da rede através de um microcomputador, um modem, um software de emulador de terminal e uma linha telefônica, podendo assim emular um terminal ou fazer transferências de arquivos, por exemplo.

No caso em particular da redeUFSC, o acesso de usuários externos à rede é feito via linha discada, sendo que as linhas disponíveis para esse fim, estão ligadas cada uma, a um modem. Estes modems estão ligados a um único Servidor da rede do qual o usuarios externos

emulam um terminal remoto e permitindo desta forma, o acesso dos usuários a redeUFSC. A figura 2, ilustra esta configuração.

O serviço de acesso discado é de grande importância para instituições como uma universidade, pois permite que professores, alunos de pós-graduação e outras pessoas da comunidade universitária possam desenvolver seus trabalhos de pesquisa e manter-se em contato com a instituição mesmo em dias e horários que não seja disponível sua presença na mesma.



A figura 2 ilustra o serviço de Acesso Doméstico:

Pelas características oferecidas deste serviço, há também um considerável grau de vulnerabilidade resultante sobre a rede. Considere, por exemplo, o que pode acontecer se um usuário permitir que terceiros obtenham sua conta e senha. Deve-se aqui ressaltar que este é um problema que não ocorre apenas através do acesso doméstico. Uma pessoa não autorizada poderá ter acesso a rede através desta conta, descobrindo informações pertinentes ao dono da conta, havendo assim, a quebra de confidencialidade e talvez até de integridade das informações. Além disso, esta pessoa poderá prejudicar o desenvolvimento dos trabalhos de usuários legítimos, beneficiando-se com o uso de recursos compartilhados, o roubo de ciclo de CPU, etc. O problema no serviço de "acesso doméstico" é que desta forma é impossível localizar a origem, tornando muito difícil a sua identificação.

7 Novo Serviço de Acesso Discado

O que se pretende fazer é disponibilizar para a categoria de usuários com permissão de acesso à redeUFSC por linha discada, um serviço que não se restrinja apenas a emular um terminal VT100, mas sim, que ao se conectar à rede, ele tenha possibilidade de tornar-se um nó da mesma, com a atribuição de um endereço IP durante o período em que a conexão estiver

estabelecida. Isto será possível através da utilização do protocolo Serial Line IP - SLIP, que é um protocolo utilizado para a comunicação ponto-a-ponto via interface RS-232.

Neste sentido, existem muitas implementações, inclusive comerciais, que ja fazem isto. Entretanto, até o momento, nenhuma fornece a possibilidade de gerenciamento através de um gerente SNMP ou OSI. Desta forma, o Serviço de Acesso Discado com estas implementações ficaria fora da plataforma de gerência usada na redeUFSC (o IBM NetView/6000).

7.1 Gerência do Acesso Discado

Para proporcionar maior segurança aos recursos da rede e aos seus usuários, e, vinculado a disposição do novo serviço, é que está sendo desenvolvido um mecanismo de controle de acesso via linha discada, que será anexado a uma plataforma de Gerenciamento de Redes TCP/IP (inicialmente ao IBM NetView/6000 Versão 3), pertencendo a Área Funcional de Gerência de Segurança, seguindo o modelo Internet. Tal mecanismo está sendo desenvolvido na linguagem C++ com o compilador gcc, em uma estação de trabalho sobre o sistema operacional UNIX (AIX 3.2.5) .

7.2 Descrição Funcional

O mecanismo de controle de acesso é composto dos processos *scheduler* e *login* (os diagramas de estados destes processos podem ser vistos nas figuras 4 e 5) os quais implementam duas classes de objetos gerenciáveis: *port* e *user* (figura 3).

O processo *scheduler* tem como funções:

- Prover alocação dinâmica de endereços IP;
- Monitorar e controlar o *status* das portas de comunicação via modem;
- Comunicar-se com os objetos *port* e *user* via agente SNMP local e protocolo SMUX.

O processo *login* é responsável por efetuar as funções primárias do controle de acesso de usuários à rede, que são as seguintes:

- Identificação do usuário: obtenção do nome da conta do usuário;
- Autenticação do usuário: verificação se o usuário é realmente quem diz ser. É feita através da sua senha;
- Autorização da requisição de acesso: se tal usuário estiver cadastrado como um usuário com direito de fazer acesso doméstico, então o seu acesso é permitido.

7.3 Descrição das Entidades

O processo *scheduler*, por comunicar-se com o agente SNMP local via protocolo SMUX, é conhecido no âmbito de gerenciamento Internet, como par SMUX, ou ainda, processo usuário, e o processo *login* é um processo normal do Unix. A classe *port* representa as portas de comunicação via modem, da qual serão instanciados os objetos *port*, e a classe de

objetos *user* representa os usuários que utilizam o serviço de acesso discado. A figura 3 a seguir representa as classes de objetos *port* e *user*:

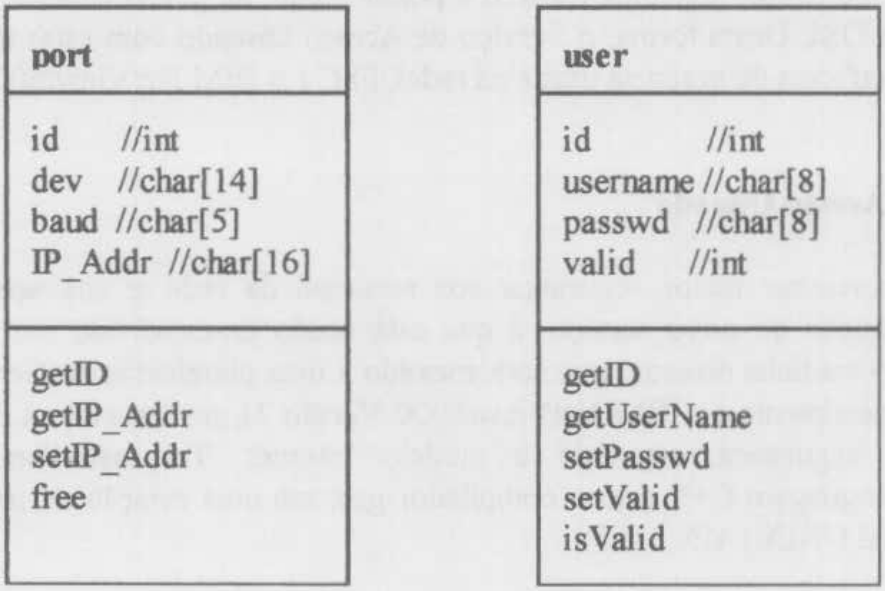


Figura 3 - Resumo das classes *port* e *user*

7.4 Descrição Dinâmica

A comunicação entre processo *scheduler* e o agente SNMP local é realizada através do protocolo SMUX, definido em [9]. Tanto o agente SNMP quanto os processos *scheduler* e *login* e a MIB particular (definição dos objetos port e user) devem estar no Servidor de Serviços Gerais apresentado na figura 6.

O processo *scheduler*, que é um *daemon* do Unix, tem como função efetuar *polling* nas portas de acesso à rede, com o objetivo de verificar seu status. Se for verificado que a porta possui um endereço IP e uma conexão SLIP, significa que esta porta está sendo utilizada por um usuário. Neste caso, o processo *scheduler* efetua um teste de conexão IP usando-se o comando ping (que envia pacotes de dados e espera seu eco). Se este teste falhar (por tempo expirado, ou seja, *timeout*) é efetuado outra tentativa. Se o número de tentativas do teste de conexão atingir um valor máximo estabelecido, efetua-se uma operação para liberar a conexão SLIP e a entrada do arquivo é liberada.

Se o teste de conexão falhar e número de tentativas for menor que o valor máximo, efetua-se uma operação para liberar a conexão SLIP, uma operação para conectar o SLIP novamente, incrementa-se o número de tentativas e se efetua um novo teste de conexão IP. E, se a conexão IP já existir e for válida, inicia-se um novo ciclo de *polling* sobre o arquivo das portas de comunicação. Se for atingido o final de arquivo, o processo *scheduler* volta ao início do mesmo e reinicia o ciclo de *polling*.

Caso a entrada no arquivo de portas esteja livre, verifica-se a existência de um processo *login* associado àquela porta. Não existindo tal processo, o *scheduler* irá iniciar um processo login. Se já existir, deve-se verificar se tal processo está ativo, se não estiver, então um novo processo *login* será iniciado e o ciclo de *polling* será reiniciado. Se estiver ativo, será

efetuada uma operação para liberar a conexão SLIP, e a entrada do arquivo de portas será liberada e também reinicia-se o ciclo de *polling*.

O processo *login*, logo após ser ativado pelo *scheduler*, solicita ao usuário que forneça sua conta, efetua a identificação e, se a conta for válida, ele solicita ao usuário a sua senha.

Figura 4 - Diagrama de estados resumido do processo *scheduler*

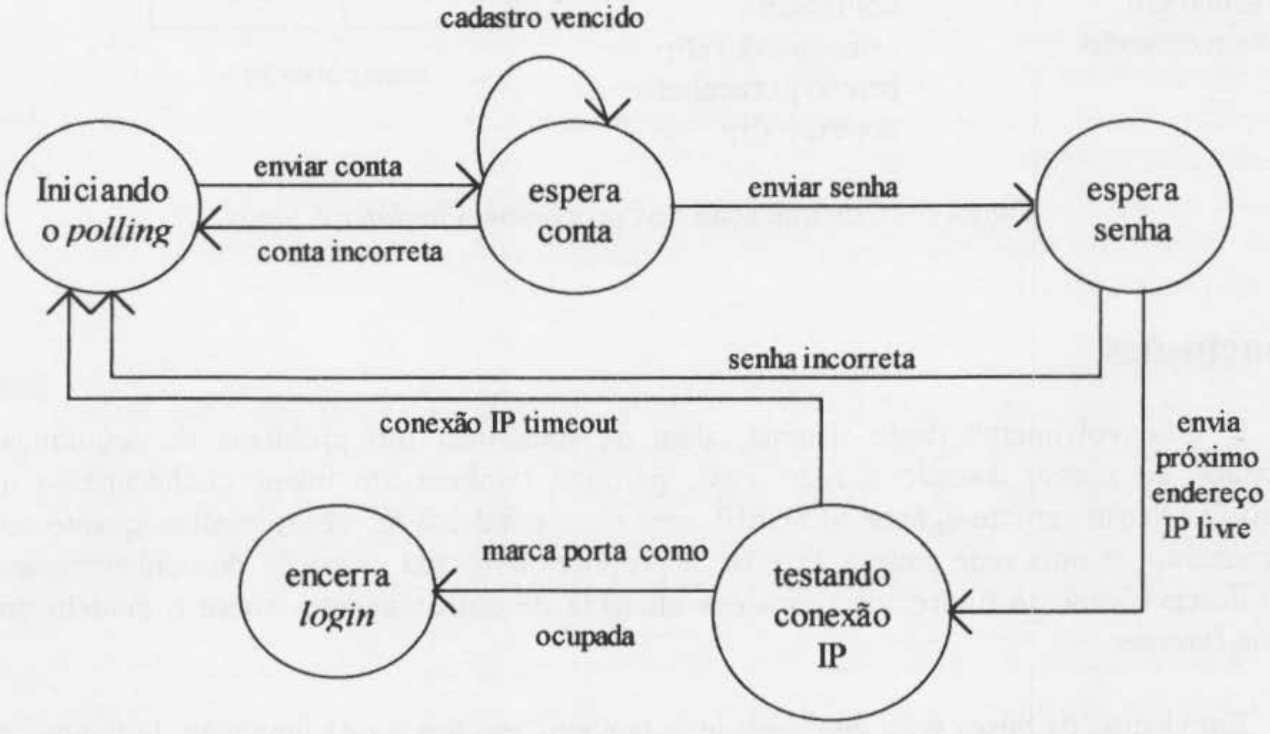


Figura 5 - Diagrama de estados resumido do processo *login*

A figura 6 ilustra a comunicação entre os processos *scheduler*, *login* e o agente SNMP local, no Servidor de Serviços Gerais:

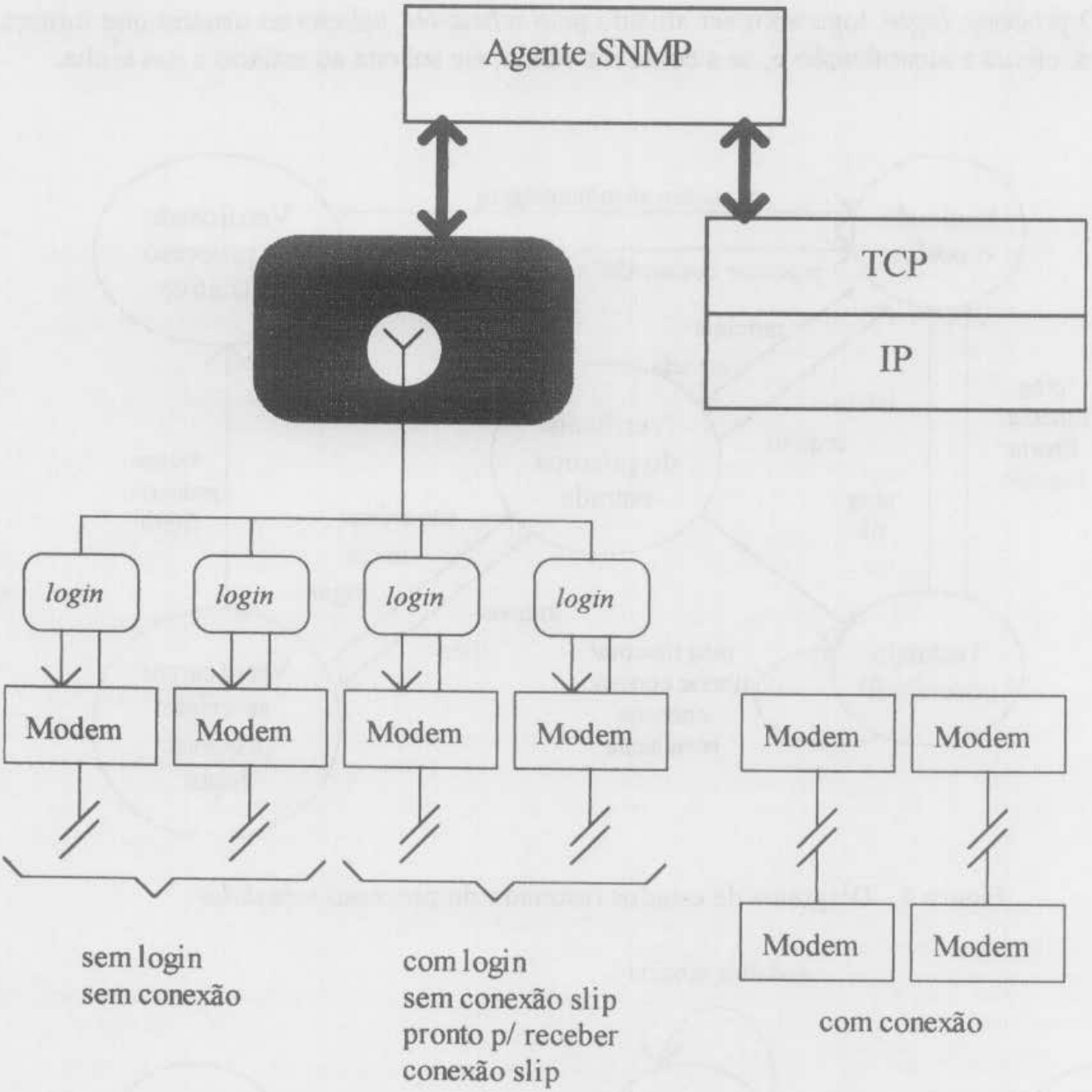


Figura 6 - Comunicação dos processos *scheduler* e *login*

8 Conclusões

O desenvolvimento deste sistema, além de solucionar um problema de segurança relacionado ao acesso discado à redeUFSC, permitiu também um maior conhecimento a respeito da relação gerente-agente do SNMP, uma visão geral dos fatores relevantes quanto ao gerenciamento de uma rede padrão TCP/IP, e proporcionou uma absorção de conhecimento para o desenvolvimento futuro mais rápido e eficiente de outros agentes sobre o modelo de gerência *Internet*.

Em virtude da busca pela simplicidade, e também, em função da limitação de tempo, a que esteve associado este trabalho, optou-se pela utilização do protocolo SLIP (IP para linha serial) para obtenção de uma conexão ponto-a-ponto via linha serial. Porém, com o intuito de

prover maior segurança ao serviço de acesso via linha discada, fica como observação, a possibilidade de futuramente substituir-se o protocolo SLIP pelo protocolo PPP (Point-to-Point Protocol), mais complexo e seguro. E, pela vulnerabilidade causada pela comunicação via linha telefônica, considera-se também que se pode implementar um mecanismo de criptografia de senhas, protegendo os usuários de ataques e escutas no meio físico.

Bibliografia

[1] BRISA, Gerenciamento de Redes: Uma Abordagem de Sistemas Abertos, Makron Books, Telebras, 1993.

[2] CASE, J., FEDOR, M.SCHOFFSTALL, M. DAVIN, J., Network Management Protocol-SNMP, May 1990.

[3] COOPER, J. A., Computer and Communication Security. Strategies forthe 1990's, Mc Graw-Hil, 1989.

[4] LUCCA, J. E. de, WESTPHALL, C. B., SPECIALSKI, E. S., CPGCC, INE/UFSC., Maio 1994.

[5] McCLOGHRIE, ROSE, M., Management Information Base for Network Management of TCP/IP-Based Internet, May 1990.

[6] PETHIA, R., CROCKER, S., FRASER, B., Guidelines for the Secure Operation of the Internet, November, 1991.

[7] QUITÉRIO, João, Gerenciamento I, Connections. A Revista de Redes, Ano III, n.25, pg.42, Junho 1994.

[8] ROSE, M., McCLOGHRIE, Struture and Identification of Management Information for TCP/IP-based Internet, May 1990.

[9] ROSE, M., McCLOGHRIE, K., Concise MIB Definitions, March 1991.

[10] ROSE, M., SNMP MUX Protocol and MIB, May 1991.

[11] SITE SECURITY POLICY HANDBOOK WORKING GROUP, Site SecurityHandbook, July 1991.

[12] TECHNICAL COMMITTE ISO97, Information Processing Systems, Open Systems Interconection, Basic Reference Model, Part 2 : Security Architeture, ISO 7498-2, Switzerland, 1989.

[13] ROMKEY, J., A Nonstandard of Transmission of IP Datagrams Over Serial Lines: SLIP, June 1988.

[14] VALLADÃO, Ronald, Longe de Intrusos, Connections. A Revista de Redes, Ano III, n.23, pg.42, Abril 1994.