Gerência de Redes de Computadores através de Novos Agentes

Marco Antonio da Rocha * Carlos Becker Westphall †

CPGCC, Instituto de Informática, UFRGS
Caixa Postal 15064
91501-970 Porto Alegre - RS

UFSC, CTC, INE
Caixa Postal 476
88040-970 Florianópolis - SC

Sumário

Este artigo apresenta o resultado da implementação de novos agentes para a Gerência da Rede do Computadores do Instituto de Informática da UFRGS, mostrando cinco novos agentes com novas funções de gerência colocando em aplicação prática conceitos teóricos ministrados na disciplina de Gerência de Redes de Computadores do curso de Pós-Graduação em Ciência da Computação da UFRGS. O ambiente para validação prática foi o software de gerência de redes SunNet Manager na rede local do Instituto de Informática da UFRGS.

1 Introdução

As redes foram concebidas, inicialmente, como um meio de compartilhar dispositivos periféricos mais caros como impressoras, modens de alta velocidade, impressoras laser, painéis pc-fax e etc... Entretanto, à medida que as redes crescem e tornam-se integradas às organizações, o compartilhamento dos dispositivos toma aspectos secundários em comparação às outras vantagens oferecidas. Atualmente, as redes valem mais pelos recursos e serviços que oferecem a seus usuários e pela maneira como estes podem interagir entre si.

Considerando este quadro, torna-se cada vez mais necessário a Gerência do ambiente de redes de computadores.

A gerência em redes de computadores torna-se difícil porque as redes crescem em performance e complexidade, suportando um grande conjunto de serviços. Os sistemas de telecomunicações são muito complexos e serão cada vez mais no futuro.

*Mestrando do CPGCC (Curso de Pós-Graduação em Ciência da Computação) da UFRGS.

†Professor Responsável pela Disciplina de Gerência em Redes de Computadores do CPGCC da UFRGS.

Eles poderão ser gerenciados somente se uma estrutura com bons princípios for seguida [WES 92].

Admitindo-se que as ferramentas para gerência de redes não abrangem toda a gama de problemas de uma rede e que estas nem sempre são usadas nas organizações que possuem redes, se faz necessário que outros mecanismos de gerência sejam utilizados para suprir suas carências mais evidenciadas.

Partindo destas premissas citadas acima, sentiu-se a necessidade de cobrir este subconjunto particular das redes de computadores que não são atingidos pelas ferramentas de gerência e que confere a cada organização as particularidades que diferenciam sua rede de outras, bem como tornar mais fácil ao administrador da rede a tarefa de gerência desta. Após um estudo sobre o problema foi adotada a estratégia do uso de agentes na gerência de redes de computadores.

Assim, este artigo visa realizar um compêndio da aplicação prática de alguns conceitos ministrados na disciplina de Gerência de redes do Curso de Pós-Graduação em Ciência da Computação do Instituto de Informática da UFRGS, no primeiro semestre de 1993. O trabalho desta disciplina, que motivou a elaboração deste artigo, foi direcionado para a implementação de novos agentes para a gerência em redes de computadores, sendo utilizado para a validação prática os equipamentos da rede do Instituto de Informática e o ambiente SunNet Manager. Utilizaram-se workstation Suns, sistema operacional Sun OS 4.1 compatível com o sistema UNIX 4.3 BSD, compilador C do sistema Sun OS, o ambiente de janelas Open Windows 2.1 e microcomputadores ligados a rede do Instituto.

O artigo encontra-se organizado da seguinte maneira:

- Na seção 2 são abordados os aspectos relevantes à gerência de redes de computadores em geral, com uma breve especificação da gerência no ambiente do SunNet Manager.
- Na seção 3 são apresentados os novos agentes propostos para otimizar o ambiente de gerência do Instituto com uma breve descrição da aplicação de gerência do agente.
- Na seção 4 são discutidos, detalhadamente, a estratégia de implementação particular de cada agente.
- Na seção 5 são apresentados os aperfeiçoamentos sugeridos para a aplicação em cada agente.
- Na seção 6 temos a conclusão do artigo com um breve comentário dos resultados obtidos e na seção seguinte os agradecimentos aos mestrandos alunos desta disciplina.

2 A Gerência em Redes de Computadores

Em uma rede de computadores as informações devem ser trocadas de modo confiável e rápido e para que isso aconteça é importante que estes dados sejam

monitorados de maneira que os problemas que porventura possam existir sejam resolvidos na medida do possível. Uma rede sem mecanismos de gerência pode apresentar problemas como congestionamento do tráfego, recursos mal utilizados, recursos sobrecarregados, problemas com segurança e outros.

A gerência está associada ao controle de atividades e ao monitoramento do uso de recursos da rede. As tarefas básicas da gerência em redes, simplificadamente, são obter informações da rede, tratar estas informações, possibilitando um diagnóstico, e encaminhar as soluções dos problemas. Para cumprir estes objetivos, *funções de gerência* devem ser embutidas nos diversos componentes de uma rede, possibilitando descobrir, prever e reagir a problemas [WES 88].

Para resolver os problemas associados a gerência em redes a ISO através do OSI/NM propos três modelos [WES 91]:

- O Modelo Organizacional estabelece a hierarquia entre sistemas de gerência em um domínio de gerência, dividindo o ambiente a ser gerenciado em vários domínios.
- O Modelo Informacional define os objetos de gerência, as relações e as operações sobre esses objetos. Uma MIB (Management Information Base) é necessária para armazenar os objetos gerenciados.
- O Modelo Funcional descreve as funcionalidades de gerência: gerência de falhas, gerência de configuração, gerência de performance, gerência de contabilidade e gerência de segurança.

Gerência de rede é uma aplicação distribuída que envolve as trocas de informações de gerência entre processos de gerência com a finalidade de monitorar e controlar os diversos recursos da rede. Os processos envolvidos em uma associação específica assumem dois papéis possíveis: Gerente e/ou Agente. O *gerente* é a parte da aplicação distribuída que gera operações de gerência e recebe notificações. O *agente* é parte da aplicação distribuída que gere os objetos gerenciados a ele associados (respondendo às operações solicitadas pelo gerente e emitindo notificações que refletem o comportamento dos objetos).

2.1 O ambiente de Gerência SunNet Manager

O SunNet Manager é um pacote de software que contém serviços que auxiliam a gerenciar elementos de uma rede de computadores. Este software é composto por uma interface gráfica de apresentação da topologia da rede representada por figuras e que permite a interação dos usuários com os elementos componentes desta através da manipulação dos respectivos icones e uma biblioteca de serviços gerente/agente que realizam a monitoração de vários aspectos da rede.

O ambiente SunNet Manager é baseado no modelo gerente/agente no qual o gerente é um processo disparado pelo usuário, normalmente da console do SunNet Manager, e o agente é um processo que coleta dados dos objetos gerenciados

reportando-os ao gerente. A biblioteca de serviços do SunNet Manager possue vários serviços de monitoração e um conjunto de agentes disponíveis para o usuário. O ambiente SunNet Manager é uma plataforma que suporta o desenvolvimento de novas aplicações de gerência através da possibilidade de confecção de novos agentes que passam a fazer parte do conjunto original de funções de gerência, que é o objeto deste trabalho.

3 Os Novos Agentes Propostos para Gerência de Redes

Os agentes propostos procuraram implementar funções de gerência em que se possa auxiliar o administrador da rede a enxergar, de uma maneira mais particular, o ambiente da rede local e otimizar as ferramentas disponíveis. Neste contexto, os novos agentes proporcionam: análise qualitativa no tráfego de rede, confirmação de recebimento de mails utilizando o protocolo SMTP, monitoração do tráfego dos pacotes TCP/IP, monitoração do uso de microcomputadores ligados na rede, análise do congestionamento da rede.

3.1 Agente 1: Análise Qualitativa no Tráfego da Rede

O agente 1 se baseou no estudo do agente traffic do SunNet Manager que informa o tráfego global do barramento de uma maneira génerica. O objetivo do agente 1 é detalhar mais a nível das aplicações de maior uso na rede para possibilitar ao administrador da rede condições de um gerenciamento mais consistente sobre estas aplicações e o impacto que estas causam na rede.

3.2 Agente 2: Monitoração do uso de microcomputadores ligados na rede

O Agente 2 foi desenvolvido com a finalidade de monitorar e apresentar estatísticas sobre transmissões e recepções de microcomputadores na rede, bem como analisar o tipo de serviço solicitado pelos usuários da rede através dos microcomputadores.

3.3 Agente 3: Confirmação de recebimento de mails utilizando o protocolo SMTP.

O agente 3 foi idealizado com o objetivo de oferecer um serviço de confirmação ao protocolo SMTP no envio de mails de uma máquina para outra, introduzindo maior confiabilidade ao envio de mensagens via correio eletrônico e-mail.

3.4 Agente 4: Monitoração do Tráfego dos pacotes TCP/IP

O agente 4 tem por objetivo coletar os pacotes TCP/IP trafegando na rede local SUN do laboratório do Instituto de Informática e transformar estes pacotes lidos para um lay-out mais amigável à leitura e facilitar a análise pelos administradores da rede.

3.5 Agente 5: Análise do congestionamento da rede

O agente 5 tem por objetivo medir o congestionamento de um barramento ethernet para ter uma medida de qualidade e desempenho dos serviços de comunicação da rede por uma monitoração do volume do tráfego e a verificação da quantidade dos erros.

4 Elaboração dos Novos Agentes para Gerência

No desenvolvimento deste artigo, iremos ao detalhamento individual do desenvolvimento particular de cada agente, mostrando a estratégia adotada para a construção do agente, mas abstraindo a interface com o SunNet Manager e o método de desenvolvimento de um agente para o ambiente de gerência [SUN 89].

4.1 Agente 1: Análise Qualitativa no Tráfego da Rede

O novo agente dispõe detalhar melhor o tráfego de algumas aplicações possibilitando ao administrador da rede condições para um gerenciamento mais efetivo sobre esses tipos de aplicações e sobre o impacto que eles causam na rede como um todo.
Visa analisar o tráfego da rede relacionado com os pacotes das aplicações FTP (File Transfer Protocol), TELNET (Acesso Remoto) e SMTP (Simple Mail Transfer Protocol).
Apresentando os resultados da análise do tráfego, o número de pacotes das aplicações e a quantidade de bytes num tempo determinado. Foi adotado os seguintes passos:

1. Captura dos pacotes e análise dos mesmos

   Foi usado um módulo já desenvolvido (network.c), para a captura de pacotes do barramento utilizando a facilidade do sistema operacional NIT (Network Interface Tap), e fazendo uma cópia em memória utilizando estruturas já definidas, tanto para pacotes IP como TCP ou UDP.
   Da estrutura onde se jogou o pacote IP, se lê o campo que indica o tipo de protocolo de transporte, para saber se é TCP ou UDP, interessando para o

desenvolvimento do agente 1 somente os pacotes TCP.

Já sabendo que o pacote é TCP, se passa a averiguar qual tipo dos serviços de aplicação é o conteúdo desse pacote, para isto se lê o campo que indica o número de porta.

2. Acumulação de ocorrência do tráfego.

Depois de identificados os pacotes dos serviços de aplicação, a ocorrência dos mesmos é contabilizada em variáveis que são passadas ao gerente. Os valores que se contabilizam são: número de pacotes SMTP, número de pacotes TELNET, número de pacotes FTP.

Além de obter o número de ocorrências dos pacotes obteve-se o tamanho em bytes de todos os pacotes de cada aplicação, acumulando o total em variáveis correspondentes.

3. Apresentação dos resultados

O agente pode ser rodado com duas opções, ALL e ALL-TAMANHO:

- Opção ALL, com esta opção os resultados apresentados são:
  - npgeral : quantidade de todos os pacotes analisados na rede.
  - nptotal : somatório dos pacotes de ftp, telnet e smtp.
  - npftp : número de pacotes ftp identificados.
  - nptelnet: número de pacotes telnet identificados.
  - npsmtp : número de pacotes smtp identificados
- Opção ALL-TAMANHO, com esta opção é apresentado o tamanho em bytes dos pacotes nas seguintes variáveis:
  - tpgeral : tamanho de todos os pacotes analisados
  - tptotal : somatório do tamanho dos pacotes ftp, telnet e smtp.

- tpftp : tamanho dos pacotes ftp identificados.

- tptelnet: tamanho dos pacotes telnet identificados.

- tpsmtp : tamanho dos pacotes smtp identificados.

Ambas opções podem ser rodadas em modo comando e/ou modo gráfico:

- Modo comando:

  Se tiver sido escolhida a opção ALL, poderá ser apresentado o total de número de pacotes de cada um dos atributos: FTP, TELNET, SMTP e um total geral;

  Escolhendo a opção ALL-TAMANHO, poderia ser apresentado o total em bytes de cada um dos atributos: FTP, TELNET, SMTP e um total tanto destas aplicações como das aplicações mencionadas.

- Modo gráfico:

  A representação gráfica feita pelo gerente pode ser com qualquer das duas opções (ALL e ALL-TAMANHO), podendo escolher um só atributo da tabela ou todos ao mesmo tempo, e o gerente apresentará o gráfico dos atributos escolhidos.

4.2 Agente 2: Monitoração do uso de microcomputadores ligados na rede

O novo agente se propõe a fazer uma monitoração na utilização dos microcomputadores ligados à rede do Instituto de Informática. Para esta tarefa foi necessário colher os dados necessários à esta gerência em cada microcomputador.

Devido a impossibilidade de alteração do arquivo CONFIG.SYS da servidora de arquivo da rede de PCs do Instituto de Informática e, aproveitando que o software Netwatch estava operacional em um PC na rede do domínio CESUP, optou-se pela execução do software nesta máquina;

Decifrando, posteriormente, o conteúdo do arquivo gerado pelo Netwatch foi descoberta a estrutura, que contém o sumário da observação da rede, foi realizado um Estudo do agente **Etherif**, o qual serviu de molde para o agente 2.
Iniciou-se a interpretação dos dados contidos no arquivo, sendo realizada a triagem dos dados pertinentes e a contabilização dos dados estatísticos que o agente 2 apresenta ao gerente.

O funcionamento do agente 2 exige executar o Netwatch em separado, na rede dos micros, para a aquisição do arquivo com os dados, dentro do agente 2, no arquivo func.c, é feita a leitura e "quebra" dos datagramas IP, para identificar o protocolo e os tipos de serviços, para depois de identificar os tipos de servicos, a ocorrência dos mesmos e os respectivos endereços dos micros. Os valores são acumulados nas estruturas.

- As estatísticas que se contabilizam são:

  Por Serviço:

  - total de pacotes FTP
  - total de pacotes TELNET
  - total de pacotes SMTP
  - total de pacotes GOPHER
  - total de pacotes LOGIN

  Por máquina:

  - Micro que mais emitiu FTP
  - Micro que mais emitiu TELNET
  - Micro que mais emitiu MAIL

O agente deve ser executado com a opção INPUT, e os resultados apresentados são:

tftp - total geral de pacotes FTP
ttelnet - total geral de pacotes TELNET
tmail - total geral de pacotes MAIL
tgopher - total geral de pacotes GOPHER
tlogin - total geral de pacotes LOGIN
tdestn - total geral de pacotes DESTINO NAO ENCONTRADO
tdescart - total geral de pacotes DESCARTADOS
terrcab - total geral de pacotes com ERRO DE CABECALHO
m-ftp-f - micro que mais emitiu FTP
m-telnet-f - micro que mais emitiu TELNET
m-mail-f - micro que mais emitiu MAIL

4.3 Agente 3: Confirmação de recebimento de mails utilizando o protocolo SMTP.

Atualmente, em redes Internet, ambiente TCP/IP, quando queremos enviar um mail de um usuário para outro, o remetente não tem a confirmação que o mail enviado chegou ao seu destino e também não tem como confirmar que realmente enviou a mensagem podendo com isso gerar situações constrangedoras.

O correio eletrônico utiliza a técnica de spooling. Quando o usuário envia uma mensagem , o sistema a cópia para um depósito privado (spool) com a identificação do remetente , destinatário e a hora em que a mensagem foi gravada no spool. O sistema inicia o envio da mensagem após a cópia , permitindo que o usuário remetente prossiga com outras atividades computacionais.

O SMTP utiliza comandos pré-definidos para realizar a conexão entre máquinas e o envio de mensagem de mail's. Abaixo mostramos alguns cenários típicos de conexão do protocolo SMTP.

Cenário: Mensagem Para um usuário

R: 220 USC-ISIE.ARPA Simple Mail Transfer Service Ready
S: HELO MIT-AI.ARPA
R: 250 USC-ISIE.ARPA
S: MAIL FROM: < JQP@MIT-AI.ARPA >
R: 250 OK
S: RCPT TO: < @USC-ISIE.ARPA:Jones@BBN-VAX.ARPA >
R: 250 OK
S: DATA
R: 354 Start mail input; end with <CRLF > . <CRLF >
S: Date: 2 Nov 81 22:33:44
S: From: John Q. Public < JQP@MIT-AI.ARPA >
S: Subject: The Next Meeting of the Board
S: To: Jones@BBN-Vax.ARPA
S: Bill:
S: The next meeting of the board of directors will be
S: on Tuesday.
S: John.
R: 250 OK
S: QUIT
R: 221 USC-ISIE.ARPA Service closing transmission channel

Tecnicamente , o protocolo SMTP se mostra confiável , pois opera em um protocolo orientado á conexão o TCP/IP (Figura 1). O protocolo TCP/IP torna possível a transferência universal de mensagens porque ela provê uma interconexão universal de máquinas. Uma troca padrão de mensagens é então possível.

Em um ambiente heterogêneo , ou em ambientes de grandes redes , faz-se necessário para a transferência de mensagens de mail usar um " mail gateway " ou "passagem de correio". Nestes sistemas a máquina remetente não contacta diretamente a máquina receptora , porém envia a mensagem através de uma ou mais máquinas intermediárias que a repassam.

Uma desvantagem introduzida no uso de "mail gateways" ou "passagem de correios", é que eles introduzem inconfiabilidade ao serviço. Quando uma máquina remetente transfere uma mensagem para a primeira máquina intermediária , ela descarta a cópia local. Portanto , enquanto a mensagem esta sendo transmitida , nem o remetente nem o receptor possuem a cópia. Falhas na intermediação da

mensagem , podem causar a perda de mensagens sem que o remetente e o receptor da mensagem sejam informados.

Para solucionar este problema podemos criar um agente para monitorar as mensagens nos seus destinos e enviar respostas ao seu originador.Este agente deve ser localizado na máquina servidora de mails e pode ser implementado com as seguintes filosofias:

- **Comportamento OSI:** Agente residente no servidor e sendo ativado a cada mensagem que chegar.
- **Comportamento SNMP:** Agente faz polling periódico.

Para esta implementação devemos usar o protocolo SMTP e o agente em qualquer filosofia deve:

- Escutar a rede
- Verificar se os pacotes extraídos são SMTP

Partindo disto identificar os que são pacotes de dados e os de sincronização e extrair os mails originador e os receptores , gerando um mail resposta ao originador confirmando a recepção da mensagem.

Esta implementação se dará em uma extensão, com os citados fins, do agente elaborado pela colega Ana Benso do CPGCC do grupo de Comunicação de Dados.

Após análise da "conversa" entre máquinas da rede do Instituto de Informática , percebemos que a versão do Protocolo SNMP local , possuia um dialeto próprio que diferia um pouco do mostrado nos RFC's. A partir desta análise confeccionamos a máquina de estados do agente3 e depois então o seu código (figura 1).

Foi necessário restringir o domínio dos usuários que receberiam a confirmação do agente para não causar incomodo aos usuários do instituto durante o desenvolvimento do agente. Para torná-lo geral retirar-se a rotina nome_domínio do programa func.c.

O protocolo SMTP possui nas suas conexões entre máquinas , códigos de erros que nos permite diagnosticar algumas situações. Foram selecionados quatro códigos de erros do agente3 para realizar posteriormente diagnósticos :

- Código **55O** : indica que o usuário remetente mandou um mail para um endereço que não existe naquele domínio.
- Código **450** : indica que o servidor de mail ou "gateway" ou "passagem de correio" solicitado para conexão não está ativo.
- Código **251** : indica que mensagens de mail's foram "forwarded" ou "repassados" pois o domínio não correspondia , mas o "gateway" ou "passagem de correio" sabia para onde redirecionar a mensagem.

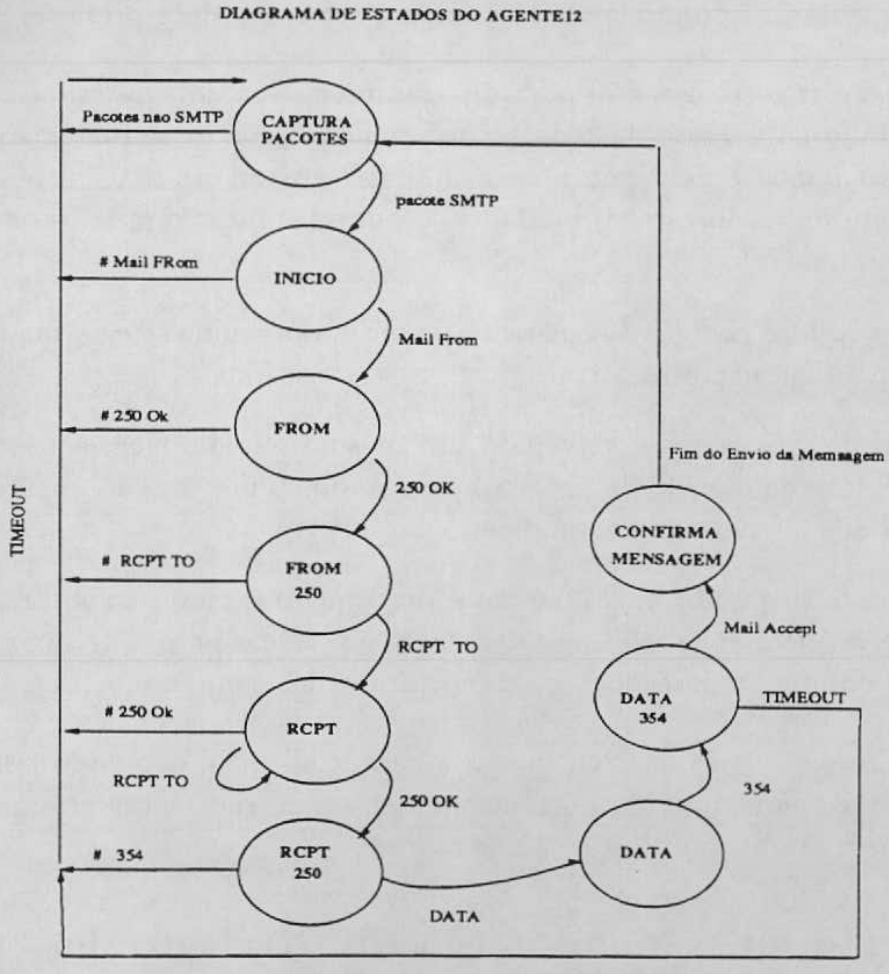

Figura 1: Diagrama de Estados do agente3

- Código **Vrfy** : indica que um "gateway" ou "passagem de correio" pergunta a outro sobre a existência daquele usuário no domínio.

Durante a execução do agente , será gravado um arquivo de log com estes códigos de erros e os respectivos endereços dos remetentes e destinatários da mensagem. Ao terminar a monitoramento dos pacotes SMTP da rede , o agente lerá o arquivo de log gerado e produz um relatório com a seguinte interpretação dos dados:

- Se mais de três códigos 550 para um mesmo par de destinatário e remetente, é solicitado ao gerente da rede a verificação de nomes similares ao endereço de mail enviado e existindo nomes similares enviar um mail resposta para o remetente indicado as possibilidades , com os nomes completos obtidos pelo comando finger.
- Se mais de três códigos 450 para uma mesma máquina , registrar mensagem que a máquina não está ativa.
- Se mais de três códigos Vrfy para um mesmo par de usuários , solicitar ao gerente da rede o envio de um mail para o remetente com o e-mail correto do usuário que ele deseja se comunicar.
- Se mais de três códigos 251 no total do arquivo de log , solicitar ao gerente da rede verificar as tabelas de roteamento e verificar porque tantos mail foram "forwaded" ou "repassados".Possíveis problemas com as tabelas.

O número de três ocorrencias para cada código foi escolhido por questões de teste de funcionamento. Para o funcionamento real será necessário uma análise do que realmente indica uma situação de alarme.

4.4 Agente 4: Monitoração do tráfego dos pacotes TCP/IP

O novo agente se propõe a partir de um programa em linguagem C elaborado para a leitura e interpretação de um arquivo binário gerado pelo utilitário Netwatch (software executável em PC que tem como opção gravar o conteúdo dos cabeçalhos dos pacotes que trafegam na rede em formato binário), partiu-se para a realização de objetivo semelhante, desta vez capturando pacotes TCP/IP "on the fly" e traduzindo-os para uma forma que possibilite ao técnico verificar, com certa agilidade, a sequência dos pacotes num determinado intervalo de tempo.

Graças às facilidades da biblioteca de rotinas do Unix e do próprio SunNet Manager, foi poupado o trabalho de localização e armazenamento dos octetos dos pacotes nas variáveis destinadas a este fim.

A elaboração do agente 4 foi inspirado no utilitário tcpdump do Unix, cuja autoria e' de Van Jacobsen, Craig Leres e Steve McCanne, todos do Laboratório Lawrence Berkeley, da Universidade da California, Berkeley, CA.

A coleta de pacotes TCP/IP que trafega na rede local padrão Ethernet que interliga as estações SUN do Laboratório do Instituto de Informática da UFRGS é realizada no período da captura, os cabeçalhos dos pacotes lidos são decodificados e transformados para um lay-out que possibilita fácil leitura humana, sendo armazenados historicamente em um arquivo LOG.

Este tipo de amostragem histórica de pacotes normalmente é utilizada por sistemas geradores de alarmes, que disparam o registro do tráfego no momento em que constata o(s) evento(s)-problema(s), concomitantemente com outras ações, para subsidiar a análise e diagnóstico pelo corpo técnico responsável pela supervisão da rede.

O agente 4 lê todos os pacotes que trafegam na rede e seleciona os pacotes de protocolo IP. Destes, são selecionados os que possuem protocolo do tipo TCP. A partir desta filtragem, é montada a linha de registro do log, que tem o seguinte lay-out.

- "src ¿ dst: flag data-segno ack window urgent"

  onde:

- "src " e' o endereço IP do host de origem e a porta/tipo de serviço TCP,
- "dst " e' o endereço IP do host de destino e a porta/tipo de serviço TCP,
- "flag " o flag setado, que pode ser (F)IN,(S)YN,(R)ST,(P)USH e (.) ACK,
- "data-segno " no formato: seq-number:proximo seq-number(bytes de dados/pacote),
- "ack " acknowledge number,
- "window" tamanho do buffer de recepção, em número de octetos,
- "urgent " urgent pointer (se houver flag setado).

O formato de "data-segno" é obtido da seguinte forma: seq-number é o próprio "Sequence Number" do header TCP; o próximo seq-number é obtido através da soma entre o "Sequence Number" e o número de bytes de dados transportados pelo pacote; este, por sua vez, é obtido através da diferença entre o "Total Length" do datagrama IP e os campos "IHL" (Internet Header Length) do IP e "Offset" do TCP, cujos campos contém o número de "words" de 32 bits ocupados, no pacote, pelos headers do IP e TCP respectivamente.

Diferente da implementação do tcpdump pela equipe da Universidade de Berkeley, optou-se por testar os flags pela lógica da máquina de estados do protocolo TCP, ou seja, enquanto o tcpdump testa os flags FIN, SYN, RST e PUSH em quatro sequências de testes, o agente13 considera os quatro flags mutuamente exclusivos. A vantagem da implementação da equipe de Berkeley é que o tcpdump pode registrar a ocorrência de erros nos bits de flags dos pacotes circulantes.

4.5 Agente 5: Análise do congestionamento da rede

O agente 5 tem por objetivo medir o congestionamento de um barramento ethernet. Outras medidas de qualidade e desempenho dos serviços de comunicação da rede seriam a monitoração do volume de tráfego e a verificação da quantidade de erros. O congestionamento se difere do volume de tráfego principalmente pela distribuição das transmissões. Se o volume de tráfego é alto, mas está sendo gerado todo a partir de uma mesma máquina, então o congestionamento da rede, do ponto de vista desta máquina, não é considerado alto.

A medida de congestionamento da rede utilizada se baseia em comparar o número de tentativas de transmissão pela interface de um host para um barramento ethernet com o número de colisões ocorridas nessa transmissão. Se a porcentagem de colisões ocorridas é alta, isto indica que a rede está congestionada, pois há pouco tempo livre, isto é, sem que alguém já esteja transmitindo. Esta medida é obviamente dependente da máquina em que é feita a consulta.

Se a máquina em que roda o agente está gerando muito tráfego e as demais máquinas da rede não estão transmitindo quase nada, o número de colisões será pequeno, não refletindo o volume real de transmissões feitas. O volume real de tráfego só pode ser medido através da contagem de todos os pacotes que passam pela rede. No entanto, esta diferença verificada não é prejudicial à medida de congestionamento desejada, pois se a estação em que roda o agente é a que está transmitindo demais, para ela não há congestionamento. E para as demais estações, só haverá congestionamento na medida em que elas tentarem transmitir mais, o que também será refletido na estação do agente, com o aumento do número de colisões.

Para obter a porcentagem de colisões, calcula-se a relação número de colisões e o número de tentativas de transmissão ocorridas no intervalo entre o tempo atual e a última consulta.

O agente 5 opera em dois modos básicos suportados pelo SNM: monitoração de dados e monitoração de eventos.

Pela monitoração de dados, o agente fica em execução contínua, fazendo uma consulta a cada intervalo de tempo. Ao final de cada consulta os dados recuperados são enviados ao gerente (SNM). Este envio periódico de dados permite a geração de gráficos por parte do SNM e também o armazenamento dos dados recuperados em consultas anteriores no próprio agente, que pode então gerar estatísticas sobre o andamento do sistema de comunicações.

A monitoração de eventos funciona basicamente como a monitoração de dados, porém não tem a finalidade de mostrar ao usuário através de números ou gráficos todos os dados recuperados, mas somente determinados eventos sobre estes dados. Estes eventos são gerados basicamente quando um dado monitorado atinge ou ultrapassa determinado valor ("threshold"). Desta forma é possível controlar se um dado recuperado está dentro de uma gama de valores tidos como aceitáveis. Caso este dado saia fora desta faixa o evento informa o administrador de algum modo para que ele possa verificar a situação e tomar a medida necessária.

Uma vez que o SNM suporta a geração automática de eventos como "beep", "flash" ou "send mail" e permite a especificação de vários tipos de "thresholds", a implementação deste modo de funcionamento no agente 5 não trouxe nenhum tipo de ônus ao seu desenvolvimento.

A simples monitoração de dados a cada intervalo pequeno de tempo não nos permite concluir facilmente se a rede está seriamente congestionada ou não, pois rajadas de transmissão acontecem normalmente. Como exemplo, se pudermos obter a medida proposta a cada tentativa de transmissão, os dados recuperados seriam sempre 0 ou 100% de congestionamento, o que seria difícil de ser interpretado por alguém. Esta situação é agravada no modo de monitoração de eventos, pois não interessa de modo algum a um administrador receber um evento informando que a taxa de colisões foi, por exemplo, de 30% no último segundo.

Por outro lado, se obtivermos uma medida de congestionamento durante todo o período de vida do sistema, esta média seria bastante baixa e não iria refletir bem os problemas ocorridos durante alguns períodos.

Para permitir um controle mais inteligente da situação de congestionamento da rede, é necessário que o agente informe então uma média deste dado nos últimos N intervalos de tempo. A escolha deste número de intervalo N deve ser feita com o objetivo de modelar bem a situação do sistema com relação ao tempo real e de acordo com as necessidades de administração.

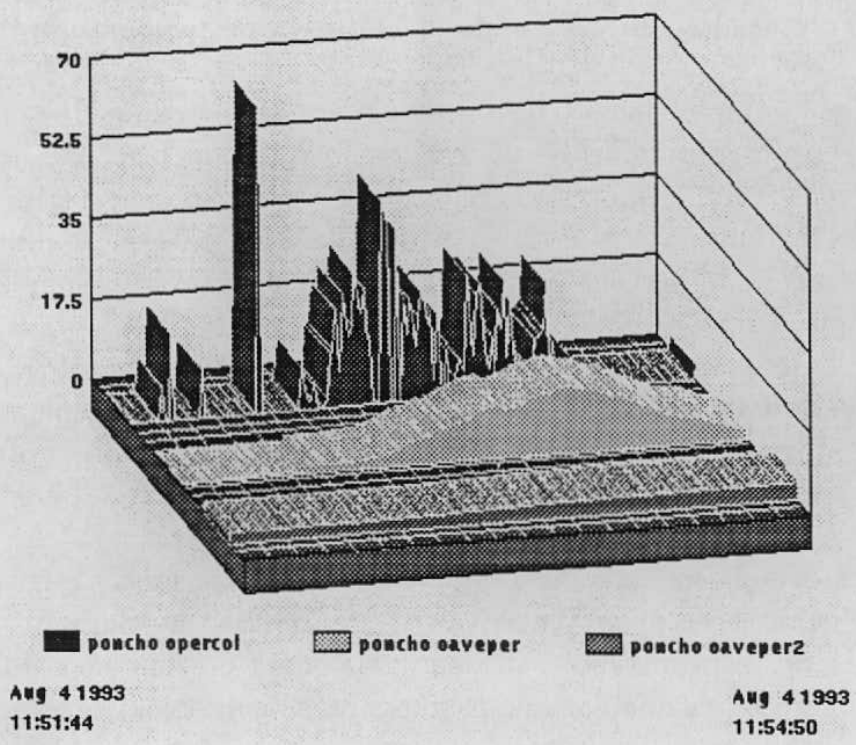

Figura 2: Gráfico com a porcentagem de colisões, média 1 e média 2.

A partir desta média é possível então se ter uma visão mais ampla e realmente gerar eventos úteis informando que o congestionamento da rede nos últimos

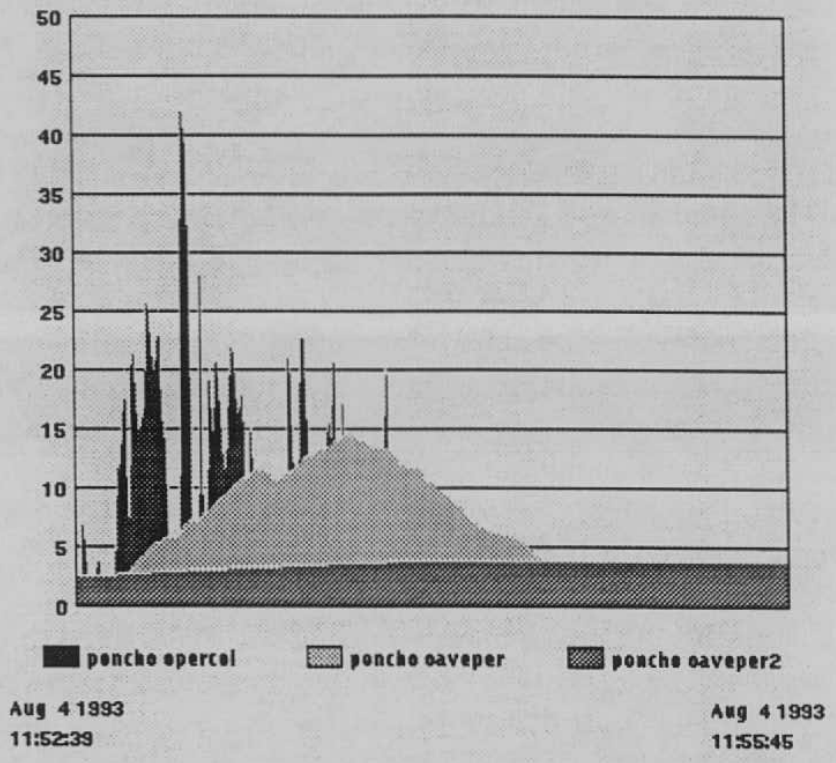

Figura 3: Mesmo gráfico da figura 1 em duas dimensões.

tempos está crescendo e ultrapassando os limites impostos para um funcionamento correto.

O agente implementado possui uma única tabela chamada "output". Nesta tabela são recuperados todos os parâmetros correspondentes à tabela de mesmo nome do agente etherif e mais três atributos específicos do agente 16.

Estes atributos são "opercol" – percentual de colisões a cada intervalo básico; "oaveper" – média do percentual nos últimos 60 intervalos; "oaveper2" – média do percentual nos últimos 900 intervalos;

O cálculo da média é atualizado a cada intervalo. Este cálculo não consome muito tempo de CPU porque o algoritmo utilizado mantém na memória do agente a soma dos últimos 900 e dos últimos 60 intervalos, bastando subtrair-se o mais antigo, somar-se o mais recente e efetuar duas divisões (por 900 e por 60) para se obter as novas médias.

O cálculo da média a cada intervalo (a cada consulta) é feito dividindo-se a diferença de colisões pelas tentativas de transmissão no período. Este número de tentativas de transmissão é calculado pela soma da diferença de tentativas de RE-transmissão com a diferença de pacotes transmitidos com sucesso.

Como esperado, a medida de congestionamento nos intervalos básicos (tempo em segundos colocado na interface do SNM) é muito inconstante, sendo composta de seguidas rajadas refletindo o congestionamento quando alguma aplicação necessita grandes transferências de dados.

Na média calculada com os últimos 60 intervalos básicos, sucessivos picos

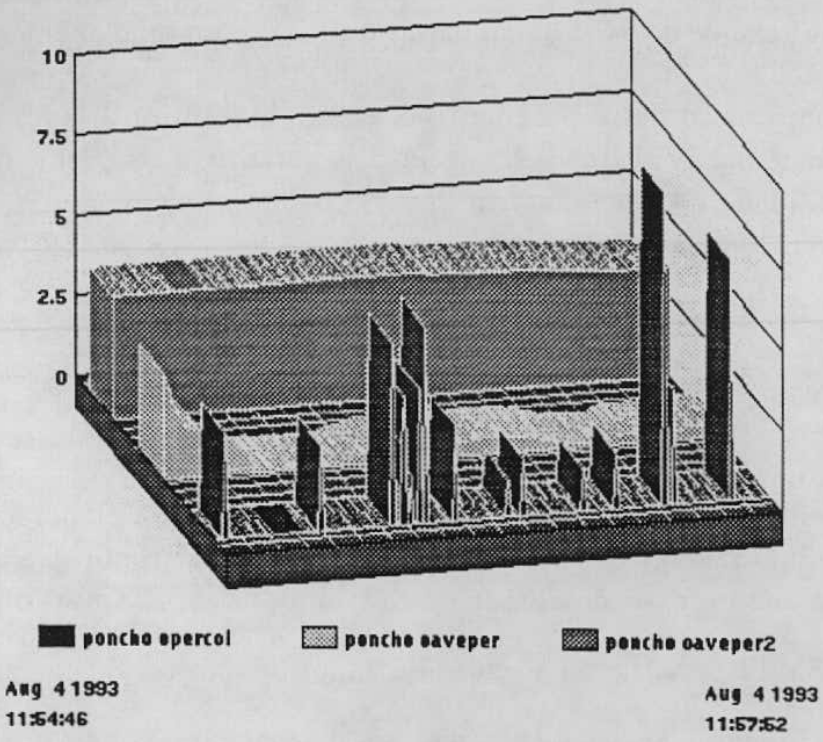

Figura 4: Gráfico com os atributos do agente 5 em uma situação real.

elevados se refletem como um aumento razoavelmente grande no congestionamento das transmissões, indicando que a situação está crítica naquele período.

A média calculada a cada 900 intervalos básicos, no entando, é pouco sensível a alterações causadas por uma ou outra aplicação que necessita grandes transferências. Pelo contrário, sua grande estabilidade reflete mais o estado de utilização da rede em geral, por todos os usuários durante um período mais longo, a partir de 15 minutos.

É bastante interessante ressaltar justamente a diferença na interpretação dos dados a cada intervalo e das médias 1 e 2. Observamos principalmente a elevada "inteligência" da segunda média, apesar de todos os três dados serem na essência a mesma média, apenas que com intervalos de tempo distintos.

Todas estas características podem ser confirmadas observando-se as figuras 2, 3, e 4. Os resultados das figuras 2, e 3 foram produzidos com o auxílio de um programa chamado spray, que envia um certo número de pacotes de determinado comprimento para uma estação. Assim, foi possível aumentar sensivelmente o congestionamento da rede nos momentos em que se desejava observar situações distintas de tráfego. Já à figura 4 foi resultado do funcionamento normal da rede do vocabulário gaudério, onde estava sendo executado o agente. A especificação de valores de "threshold" foi experimentada e produziu os resultados desejados, os quais somente podem ser vistos na prática. Foram utilizados valores baixos para que os eventos fossem disparados, tanto nos picos como nas médias 1 e 2.

Com a observação dos dados retornados pelo agente 5 em situações nor-

mais ou forçadas, pode-se sentir exatamente as características de um funcionamento normal em um barramento ethernet. Percebe-se a partir disto a importância fundamental de uma taxa de colisões baixa para garantir o bom funcionamento do sistema de comunicação.

A monitoração deste parâmetro é, então, bastante útil para fins de gerenciamento do sistema. A utilidade do agente, no entanto, é grandemente enriquecida pela disponibilidade das duas informações de média implementadas, permitindo a geração de eventos de alerta importantíssimos.

5 Aperfeiçoamentos

Para o agente 1 *(análise qualitativa do tráfego da rede)*

O agente1 atingiria uma melhor performance com a elaboração de gráficos estatísticos comparando os valores das aplicações entre si com os valores totais por estações, uma análise mais detalhada de cada uma das aplicações como:

- - Mail(SMTP): distinguir pacotes de dados de pacotes de comandos;
- - Telnet: identificar pacotes de dados e de controle.

A coleta de pacotes poderia ser mais eficiente com o desenvolvimento de um coletor de tráfego que rode em paralelo com o agente e grave os dados coletados do barramento numa área de mémoria compartilhada, que seria controlada por semáforos.

Para o agente 2 *(monitoração do uso de microcomputadores ligados na rede)*

O agente 2 atingiria uma melhor performance com o concurso das seguintes medidas:

- - desenvolvimento de uma interface para poder captar o arquivo da rede de micros, isto em ambientes multitarefa, multiusuário, onde o Netwatch poderia enviar o arquivo de dados gerado via ftp para o agente 2(ouvidor), após uma requisição deste mesmo agente;
- - coletar dados , ou seja acionar o Netwatch em horários de pique para que se possa ter uma melhor visualização das estatísticas.;
- - realizar estatísticas de tráfego de micros também na rede Sun;
- - ampliar a tabela de endereços IP, residente no agente, para que se possa supervisionar mais máquinas na rede;
- - pode-se também gerar estatísticas diferentes visto que o agente mantém uma estrutura de dados pré-selecionados.

Para o agente 3 *(Confirmação de recebimento de mails utilizando o protocolo SMTP.)*

Para aprimorar o código do agente 3 , faz-se necessário aplicar os conceitos de programação paralela. Deve haver um paralelismo entre a captura de pacotes e o tratamento dos mesmo. Na programação sequencial há perda de pacotes durante o seu tratamento , não podendo assim atingir o objetivo do agente que é confirmar 100 % os mail's enviados.

Outra sugestão seria utilizar o utilitário "Mail " com a opção -s , para colocar um subject padrão nas mensagens. Nos nossos testes a chamada de system para este software nao era executada e por razões de tempo ,optamos pela solução apresentada. Os comando do Mail poderiam ser usados também sem a chamada de system , através de um script pré-determinado.

O agente 3 teria suas funções melhores desempenhadas se fosse um agente residente no servidor de mail.

Para o agente 4 *(monitoração do tráfego de pacotes TCP/IP)*
A atual versão do agente 4 é bastante simples, por capturar somente pacotes TCP/IP. Eventuais implementações futuras poderão ampliar, com relativa facilidade, a captura e formatação de outros protocolos (UDP, ICMP), assim como identificar os diferentes tipos de serviços das camadas superiores.
Novas extensões mais sofisticadas poderão agregar inteligência ao agente 4, implementando a estrutura de dados chamada "Bloco de Controle de Transmissao" (ou TCB) para o registro das conexões estabelecidas e verificação da transição de estados das conexões TCP, e a partir de eventuais falhas (ou ultrapassagem de limites pré-estabelecidos) nos "diálogos" do protocolo apresentar mensagens de alerta, assim como oferecer um diagnóstico inferencial sobre o problema e propor uma prescrição corretiva.
Para o agente 5 *(análise do congestionamento da rede)* Como sugestões para aprimoramentos de um agente como este surgiram as seguintes propostas:

- Medida de tráfego total da rede, através da contagem de todos os pacotes que passam no barramento ethernet;
- Medida da taxa de erros nas transmissões;
- Pesquisa e comparação da mesma medida de congestionamento com outros atributos utilizados pelo agente etherif. Estes atributos alternativos, já mencionados, parecem conter as mesmas informações de tentativas de transmissão e de colisões ocorridas, porém apresentam pequenas variações que podem ser úteis em determinados casos;
- Criação de um sistema de alarme mais inteligente tentando encontrar o responsável pelas situações anômalas. Isto poderia fazer parte de uma aplicação (um gerente) baseada no uso deste e de outros agentes;

6 Conclusão

O problema da gerência de redes é por demais complexo e sabemos que à medida que as redes crescem e aumentam seus recursos oferecidos, cresce também a necessidade de coordenar estas facilidades. O advento de agentes, com novas funções de gerência, permite a monitoração de funções mais abrangentes e específicas, possibilitando a adequação do ambiente particular de rede local a uma comunidade maior de usuários.

O principal objetivo, ao realizar este trabalho, foi atingido. A aplicação dos conceitos téoricos obtidos em aula proporcionando um bom trabalho de pesquisa com boa qualidade técnica e que pudesse substanciar a realidade da gerência de redes. A definição dos novos agentes de acordo com as necessidades do ambiente de redes e a integração com o software de gerência de redes culminaram com a implementação destes sendo citadas ,também, sugestões para novos aperfeiçoamento, pois pretende-se que esta base inicial origine outros trabalhos neste mesmo contexto.

7 Agradecimentos

Gostariamos de agradecer a valorosa contribuição dos mestrandos: Ana clara Pinto, Esmilda Saenz Artola, Roseclea Medina, Rita Suzana, Leo Stapler, Rodolfo Gross Vilanova, Joaquim Eulalio, Fernando Soto e Marcelo Johann que implementaram os novos agentes, cedendo material de pesquisa ,possibilitando que este trabalho fosse realizado.

Referências

[COM 91] COMER, D. E. **Internetworking with TCP/IP: Principles, Protocols, and Architeture**. Volume 1. Seg. Edição. Prentice-Hall, Englewood Cliffs, NJ, 1991.

[POS 81] POSTEL, J.B. **Internet Protocol**. Request for Comments 791, DDN Network Information Center, SRI International, Setembro, 1981, 45pp.

[POS 81a] POSTEL, J.B. **"Internet Control Message Protocol - DARPA Internet Program Specification"**. Request for Comments 792, 1981.

[SUN 89] Sun Microsystem Inc. **SunNet Manager Tutorial - How Write an Agent**, 1989.

[SUN 89a] Sun Microsystem Inc. **Network Programming Guide**, 1989.

[STE 90] STEVENS, W.R. **UNIX Network Programming**.Prentice-Hall Inc. Englewood Cliffs, NJ, 1990.

[SUN 90] Sun Microsystems Inc. **SunOS Reference Manual**. Vol I, 1990.

[WES 88] WESTPHALL, C. B. **Proposição de Funções em Gerência de Comunicação de Dados**. *Dissertação de Mestrado*, Porto Alegre, UFRGS-CPGCC, Maio 05, 1988.

[WES 91] WESTPHALL, C. B. **Conception et développement de l'architecture d'administration d'un réseau métropolitain**. *Thèse de Doctorat nouveau régime*. Université Paul Sabatier. Toulouse, 16 Juillet 1991.

[WES 92] WESTPHALL, C. B. & ASSUOL, S. **Management Architecture for Networks of the Future**. IFIP/IEEE International Workshop on Distributed Systems: Operations & Management. October 12-13, 1992. Munich, Germany.