Aspectos de implantação para redes locais tolerantes a falhas*

Afonso Jorge Ferreira Cardoso. É graduado em Tecnólogo em Processamento de Dados (1987) e Especialista em Informática (1988) pela Universidade Federal do Pará e Mestre em Ciência da Computação (1997) pela Universidade Federal do Rio Grande do Sul. Atualmente exerce as funções de Professor Adjunto III no Departamento de Informática da UNAMA e Analista de Sistemas III na EMBRAPA Amazônia Oriental. As áreas de interesse envolvem Redes de Computadores, Tolerância a Falhas e Sistemas Distribuídos. Curso de Especialização em Redes de Computadores. Departamento de Informática - Universidade da Amazônia (UNAMA). Av. Alcindo Cacela, 287 CEP 66060-000 Belém - PA Tel: (091) 242-2100 Fax: (051) 225-3909. afonso@cpatu.embrapa.br

Ingrid Jansch-Pôrto. Dr.Ing. em Microeletrônica, INPG, FR, 1985. Profa. do Instituto de Informática, UFRGS. Áreas de interesse: tolerância a falhas, sistemas distribuídos, arquitetura de computadores. Curso de Pós-Graduação em Ciência da Computação. Instituto de Informática - Universidade Federal do Rio Grande do Sul. Caixa Postal 15064 CEP 91501-970 Porto Alegre - RS. Tel.: (051) 316-6168 Fax: (051) 336-5576. ingrid@inf.ufrgs.br

RESUMO: Este trabalho apresenta alguns requisitos de tolerância a falhas na implementação de redes locais de computadores. Os requisitos foram selecionados, considerando as principais exigências dos usuários dos sistemas, com ênfase nas redes de controle industrial e considerando também o suporte disponível no mercado.

Quanto ao hardware, os requisitos abordados são referentes à arquitetura de computadores, cabeamento, concentradores (*hubs*) e comutadores (*switches*). No software são tratados os requisitos referentes aos sistemas operacionais de rede e protocolos.

1. INTRODUÇÃO

A instalação de uma rede local de computadores é justificada, freqüentemente, como uma forma de compartilhar recursos que de outro modo ficariam sub-utilizados, ou deveriam ser desnecessariamente multiplicados. Porém, as redes locais possibilitam, também, comunicação entre as pessoas através de correio eletrônico, permitem que planos de trabalho sejam atualizados por múltiplos envolvidos à medida que mudanças ocorram, ajudam a organizar as atividades de uma empresa, possibilitam a transferência direta de arquivos de um equipamento para outro, propiciam o compartilhamento de dados, facilitam a atividade de gerência e muitas outras ações, que permitem que os serviços sejam agilizados, com o conseqüente aumento da produtividade.

A implantação de uma rede local requer um planejamento bem elaborado. O projetista deve levar em consideração diversos

* Trabalho apresentado nas 3eras Jornadas de Informática e Investigación Operativa, 6° Encuentro del Laboratório de Ciencia de la Computación da Facultad de Ingeniería de Montevideo, Uruguay e I Simpósio Regional de Tolerância a Falhas em Porto Alegre - RS - Brasil.

fatores como: avaliação de custos (projeto e implementação do sistema, recursos computacionais etc), condições impostas pela empresa na relação custo/benefício, localização dos usuários, localização dos equipamentos, definição das necessidades dos usuários, tipos de transações, volume do tráfego, topologia adequada, número de nodos, software e hardware disponíveis no mercado e disponíveis na empresa, necessidades futuras de expansão etc.

Além dos fatores citados acima, um outro fator merece atenção: a qualidade, disponibilidade e confiabilidade esperados quanto ao funcionamento da rede, que podem ser traduzidos para a especificação do sistema nos requisitos de tolerância a falhas que seriam necessários na implementação de uma rede local. Os requisitos necessários serão dependentes do ambiente e objetivos funcionais da rede. A segurança de funcionamento da rede como um todo e de cada um dos seus nodos estará associada à aplicação na qual ela se insere: provavelmente uma rede empregada em um ambiente acadêmico terá requisitos de funcionamento bastante diversos de outra que controle um ambiente industrial. Para que se possa justificadamente depositar confiança no funcionamento desta segunda rede, na correção dos serviços prestados e na manutenção permanentes destes, é preciso agregar a ela técnicas de tolerância a falhas.

Atualmente, características de tolerância a falhas são introduzidas de forma independente nos diversos níveis que formam a rede: arquitetura, sistema operacional, protocolos de comunicação, aplicações, etc. A integração dessas características na implementação de uma rede local torna-se um desafio devido aos custos envolvidos e às técnicas de execução, pois é uma área de pesquisa relativamente nova.

Neste artigo serão apresentados vários aspectos na implementação de uma rede local tolerante a falhas não-intencionais, incluindo aspectos de hardware, software e de manipulação das informações. Não serão tratados aspectos de segurança de acesso que têm merecido atenção dos administradores e encontram boas soluções de software no caso das redes locais.

2. REDES LOCAIS TOLERANTES A FALHAS: Aspectos de Hardware

O hardware envolvido em uma rede merece considerações em dois momentos diferentes: como técnica de prevenção de falhas, é necessário pensar no uso de componentes confiáveis, num projeto bem feito e numa implementação enquadrada em parâmetros de qualidade. Os componentes incluem os utilizados como nodos, como elementos de interligação e interfaces/ adaptadores existentes entre estes. Posteriormente, para o funcionamento do sistema, é necessário empregar técnicas de tolerância a falhas que aumentam a robustez da rede na ocorrência de falhas.

As redes locais de computadores mais comuns, ou seja, redes que são encontradas na maioria das instituições, utilizam microcomputadores pessoais como nodos da rede. Os computadores pessoais disponíveis comercialmente não possuem arquitetura tolerante a falhas em sua origem, exceto por algumas poucas técnicas de suporte. Portanto, o uso de técnicas de tolerância a falhas relacionadas à arquitetura dos nodos, em redes locais, não pode se valer de caracerísticas fundamentadas em comportamento controlável ou conhecido dos nodos. Exemplos deste tipo de nodos são os que se desligam automaticamente quando ocorrem

falhas internas com as quais eles não conseguem lidar ("*fail-stop*"). Em aplicações que exijam disponibilidade permanente, entretanto, podem ser empregados nodos com arquitetura baseada em grande redundância, por exemplo, redundância tripla, garantindo continuidade de funcionamento. Deve-se ressaltar, no entanto, que estas características são obtidas apenas através do uso de técnicas e estruturas especiais, não disponíveis em microcomputadores pessoais.

As redes ponto-a-ponto dependem da topologia empregada para definir a necessidade de nodos tolerantes a falhas. Em alguns casos em que o controle da rede é centralizado (topologia estrela), é necessário que apenas o nodo central e eventuais nodos críticos possuam arquitetura robusta; os nodos não críticos podem ser isolados sem afetar o funcionamento da rede. Em outros casos, quando nodos da rede são interligados através de concentradores ativos (*hubs*) sem nodo centralizador (topologia anel), apenas nodos funcionalmente críticos necessitam de robustez pois neste caso o próprio concentrador, que contém o anel, retira o nodo defeituoso e refaz o anel interno. Uma possibilidade para a implementação destes nodos envolvendo máquinas comerciais seria o uso de estações de trabalho com componentes da arquitetura duplicados, que pudessem ser configurados de modo a apresentar redundância funcional em módulos isolados.

Para manter alta disponibilidade, as redes cliente-servidor não necessitariam obrigatoriamente possuir nodos clientes com arquitetura tolerante a falhas apesar desta característica ser desejável. Devido à sua estrutura, caso o cliente falhe, basta isolá-lo, e o restante da rede continuará funcionando normalmente. O servidor, ao contrário, é essencial para o funcionamento da rede: assim, uma rede local cliente-servidor necessita de um servidor com arquitetura tolerante a falhas ou alguma estratégia de funcionamento como, por exemplo, a utilização de servidores de arquivos duplicados.

Os elementos físicos e a forma de execução do cabeamento também merecem atenção. Segundo [DER94], os sofisticados e complexos componentes da rede podem ter sua atividade inibida se um pequeno fio estiver em contato com outro atrás da parede ou se um motor qualquer gerar um campo elétrico capaz de produzir ruídos no cabo da rede local. Aspectos de tolerância a falhas no cabeamento são resolvidos pelo uso de alternativas pré-estabelecidas de rotas de comunicação, conforme segue.

Em algumas redes locais ponto-a-ponto, os cabos que interligam as estações são duplicados, a exemplo das redes FDDI (*Fiber Distributed Data Interface*), mas apenas um atua de forma ativa; o outro fica como reserva para uso em caso de falha do primeiro.

Para as redes cliente-servidor, a duplicação pode ser efetivada utilizando servidores que trabalham com dois controladores Ethernet conectados na mesma rede local Ethernet, com seus respectivos transceptores (*transceivers*). Se um dos controladores ou transceptores falhar, o sistema manterá em atividade as sessões da rede local. Essa ação é transparente para

protocolos de alto nível incluindo TCP/IP e OSI [TAN95]. Este esquema de comunicações múltiplas que facilita ações de recuperação é ilustrado pela figura 1, extraída de [TAN95].

Um outro aspecto importante é a interligação física dos nodos de uma rede. As topologias mais utilizadas anteriormente, anel e barramento, passaram a ser vistas como uma topologia estrela devido ao emprego de *hubs* e *switches*.

Os *hubs* são elementos do *hardware* que funcionam como concentradores de ligações e repetidores, assumindo posição de elemento crítico no sistema. Entretanto, com o objetivo de corrigir esta dependência crítica, em aplicações de controle industrial, os *hubs* possuem aspectos de tolerância a falhas com o objetivo de maximizar o tempo de funcionamento. Essas características compreendem: fonte de alimentação redundante, arquitetura de repetição distribuída, ligações com capacidade de recuperação, módulos com reserva-quente (*hot-standby*), redundância com módulos cruzados, etc.. [3CO95a].

Os comutadores (*switches*) são elementos de *hardware* que surgiram devido a demanda por maiores taxas de transmissão e melhor utilização dos meios físicos; eles possibilitam a troca de mensagens entre várias estações simultaneamente e uma das principais características que possuem é a configuração de proteção contra falhas de equipamento e cabeamento em ambientes com missões críticas. Possuem outras características como: verificação através de redundância cíclica (CRC), proteção bloqueadora de mensagens *broadcast* / *multicast*, módulos com reserva-quente e fonte de alimentação redundante [3CO95b].

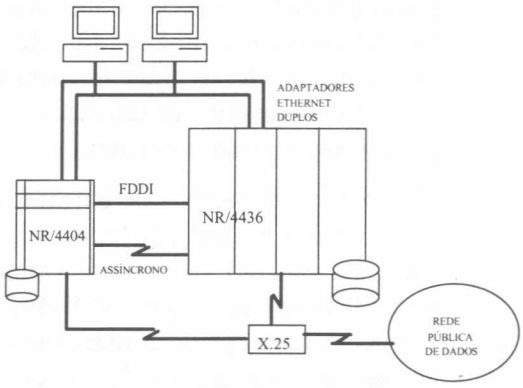

Figura 1: Configuração redundante na modalidade cliente-servidor.

3. REDES LOCAIS TOLERANTES A FALHAS: Aspectos de Software

O software envolvido em uma rede é extremamente variado e técnicas de tolerância a falhas podem ser elaboradas em todos os níveis, desde o sistema operacional até os aplicativos. A seguir exemplos de como essas técnicas podem ser desenvolvidas.

3.1 Sistemas Operacionais de Redes

Os fabricantes, nos últimos anos, estão investindo fortemente em software para redes locais com características de tolerância a falhas; principalmente ao nível dos sistemas operacionais para redes baseadas no uso de nodos não tolerantes. O *Windows NT* é um bom exemplo, com a agregação de novas características a cada nova versão, como o sistema RAID (*Redundant Array of Inexpensive Disks*) e a provisão de setores reservas, conforme explicado a seguir.

O RAID é um método de armazenamento de dados onde estes são distribuídos por vários discos através de uma técnica de entrelaçamento de bits ("*bit-interleaving*"), que proporciona entrada/saída de alto desempenho desde que a leitura de diferentes

partes dos dados possa ser feita em paralelo. Os dados são armazenados de forma redundante em discos diferentes para garantir que, no caso de falha de um disco, os dados possam ser acessados em outro.

Neste sistema, as estratégias de tolerância a falhas são padronizadas e categorizadas em seis níveis, variando do nível 0(zero) ao 5(cinco). Esses níveis oferecem técnicas de armazenamento de dados com variações de desempenho, confiabilidade e custo. Entretanto, tolerância a falhas efetiva é fornecida apenas pelos níveis 1 e 5 [MIC93] [MIC94], que correspondem respectivamente ao Espelhamento de Disco e à Aplicação de Paridade sobre Listras de Dados (*Shipping with Parity*). Nos demais níveis, o sistema é frágil a falhas que envolvam quantidades substanciais de informações no disco.

Entre os serviços de tolerância a falhas que podem ser oferecidos por um sistema operacional de rede está a capacidade de recuperação do conteúdo de setores com defeito no sistema de arquivos, durante a operação normal do sistema. O sistema de arquivos verifica todos os setores quando um volume é formatado: os ruins são tratados pelo serviço de setores reservas. Este serviço funciona da seguinte forma: se setores ruins forem encontrados durante uma operação de E/S, a unidade tolerante a falhas tentará mover os dados para um setor bom e gerará um mapa com os setores ruins. O sistema de arquivos dispara mensagens de alerta caso ocorra insucesso na operação.

Para ambientes que necessitam de alto nível de confiabilidade e tem disponíveis apenas microcomputadores ou estações de trabalho sem arquitetura tolerante a falhas, a solução de servidores duplicados é uma alternativa. O ambiente pode ser composto por dois servidores, um primário e outro secundário. Apenas o servidor primário deve estar ativo do ponto-de-vista dos usuários. O servidor secundário trabalha em *background*, mas mantém a mesma imagem de memória e o mesmo conteúdo do disco do servidor primário. Se o servidor primário falhar ou sofrer uma pausa longa demais, o secundário assume o controle do sistema e atribuições de servidor primário. Todo este processo deve ser feito de forma automática e transparente para os usuários da rede.

3.2 Protocolos

Entre os protocolos de acesso ao meio em rede local, destaca-se o CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), que faz parte do conjunto de padrões conhecido como IEEE 802. Esses padrões diferem nas camadas física e MAC (*Medium Access Control*), mas são compatíveis na camada de enlace de dados [TAN89].

O protocolo CSMA/CD funciona da seguinte forma: quando determinado nodo deseja enviar uma mensagem, ele observa se o canal (barramento) não está sendo utilizado. Se estiver livre, ele inicia a transmissão; caso contrário, ele aguarda um tempo pré-definido e depois volta a observar o canal. Existe a possibilidade de mais de um nodo tentar transmitir simultaneamente, ocorrendo uma colisão. Os nodos envolvidos, ao perceberem a colisão, abortam a operação e aguardam durante períodos aleatórios; ao final desse tempo, voltam a testar o canal para saber se o mesmo está livre e reiniciar a tentativa. Entretanto, este protocolo, não garante que uma mensagem difundida às outras estações seja recebida pelos destinatários. Problemas de *buffer* ou de conexões de rede podem resultar em mensagens perdidas. Apesar de não ser freqüente a perda de mensagens em redes locais, em alguns ambientes é necessário garantir o recebimento adequado,

o que exige um protocolo especial de apoio à difusão confiável.

Um CSMA/CD com difusão confiável foi proposto por [JAL94] e determina que, adicionalmente às características de funcionamento já explicadas do CSMA/CD, cada nodo mantenha um contador e toda mensagem a ser enviada receba um número de seqüência. Se não ocorrer colisão (a difusão funcionar), o contador é incrementado. No recebimento da mensagem, se o número de seqüência da mensagem é maior ou igual ao valor do contador do nodo, o contador é atualizado para um valor igual ao número de seqüência da mensagem que está chegando incrementado de uma unidade (*m.seq* + 1). Se o número de seqüência for menor que o valor do contador, este último permanece inalterado. A camada de transporte é responsável por assegurar a manutenção do ordenamento parcial entre as mensagens.

4. CONSIDERAÇÕES FINAIS

A implantação de redes locais tolerantes a falhas não é comum, devido a dois fatores básicos que ainda criam resistências em parte dos usuários: a baixa taxa de erros e os custos envolvidos. Entretanto, os usuários de redes de suporte a atividades industriais começam a perceber que manter a produção dentro da qualidade e tempo esperados, depende da confiabilidade e da alta disponibilidade dos seus sistemas de computação. Porém, para se alcançar essas características é necessário um projeto completo de rede que inclua desde requisitos básicos como a estabilização da rede elétrica e aterramentos até os requisitos de hardware e software.

Vale ressaltar que esse projeto não deve ter a pretensão de tornar todos os componentes da rede tolerante a falhas; ele deve considerar os requisitos de tolerância a falhas que o usuário realmente necessita, criando com isso condições de custos compatíveis e benefícios reais.

Maiores informações sobre aspectos abordados neste artigo, com análise de software comercialmente disponível, podem ser encontrados em [CAR95].

REFERÊNCIAS BIBLIOGRÁFICAS

[CAR95] CARDOSO, A. J. F. Requisitos de tolerância a falhas na implementação de redes locais de computadores. T.I. n.481. CPGCC-UFRGS, 1995.

[DER94] DERFLER, Jr. F.J.; Freed, Les. Get a Grip on Network Cabling. Ziff-Davis Press, Emeryville, Califórnia, USA. 1993.

[JAL94] JALOTE, P. Fault Tolerance in Distributed Systems. Englewood Cliffs: Prentice-Hall, 1994, 432p.

[MIC93] Microsoft Corporation. Concepts and Planning Guide. Microsoft Windows NT Advanced Server Version 3.1. 1993.

[MIC94] Microsoft Official Curriculum. Student Workbook. Supporting Microsoft Windows NT Server 3.5 Version 1.0. 1994.

[STA94] STANG, D.J.; Moon, S. Segredos de segurança em redes. Berkeley Brasil Editora: Rio de Janeiro. 1994.

[TAN89] TANENBAUM, A.S. Computer Networks. Prentice Hall. Englewood Cliffs: New Jersey. 1989.

[TAN95] TANDEM Computers Incorporated. Integrity FT Systems Family. USA, 1995. (Product description)

[3CO95a] 3COM Corporation. Guide to 3Com Hubs. USA, 1995.

[3CO95b] 3COM Corporation. Guide to 3Com Switches. USA, 1995.