



FACULDADES INTEGRADAS FACVEST
Curso de Ciência da Computação
GERÊNCIA DE SISTEMAS DISTRIBUÍDOS



APOSTILA DE GERÊNCIA DE SISTEMAS DISTRIBUÍDOS

Curso: Ciências da Computação

Professora: Madalena Pereira da Silva

Disciplina: Gerência de Sistemas Distribuídos

Turma: 7ª Fase – Período: Noturno – Ano: 2003

SUMÁRIO

SUMÁRIO.....	2
1. Introdução A GERÊNCIA DE SISTEMAS DISTRIBUÍDOS	3
1.1. Sistemas Distribuídos & Redes de Computadores	3
1.2. Histórico dos Sistemas Distribuídos.....	3
1.3. Necessidades de gerenciamento	8
1.4. Gerência de Redes e Gerência de Sistemas	9
2. Áreas Funcionais de Gerenciamento	15
2.1. Gerenciamento de Falhas	15
2.2. Gerenciamento de Contabilização	15
2.3. Gerenciamento de Configuração	16
2.4. Gerenciamento de Desempenho	16
2.5. Gerenciamento de Segurança	17
3. Funções de gerenciamento de rede	18
3.1. Monitoração.....	18
3.2. Controle de Rede	19
4. Modelos de Gerenciamento de Rede	21
4.1. Software de apresentação	22
4.2. Software de Gerenciamento.....	24
4.3. Software de Suporte ao Gerenciamento	24
REFERÊNCIAS BIBLIOGRÁFICAS	27

1. INTRODUÇÃO A GERÊNCIA DE SISTEMAS DISTRIBUÍDOS

1.1. SISTEMAS DISTRIBUÍDOS & REDES DE COMPUTADORES

Inicialmente iremos realizar uma distinção entre Redes de Computadores e Sistemas Distribuídos.

Em um sistema distribuído, a existência de diversos computadores autônomos é transparente, ou seja, o usuário não possui conhecimento deles. Para executar um programa, o usuário poderá digitar normalmente um comando. Caberá ao sistema operacional selecionar o melhor processador, localizar e transportar todos os arquivos de entrada necessários e colocar os resultados no lugar apropriado. Em outras palavras, o usuário de um sistema distribuído não tem consciência de que há diversos processadores; para ele, é como se existisse um processador virtual. Devem ser automáticas as alocações de tarefas, para os processadores, e de arquivos, para os discos, e a movimentação dos arquivos entre os locais em que foram gerados e aqueles onde são necessários, assim, como as demais funções do sistema.

Em uma rede de computadores, os usuários devem logar-se explicitamente com uma máquina, submeter explicitamente as tarefas remotas e movimentar explicitamente os arquivos. Em um sistema distribuído, nada é explícito; tudo é feito automaticamente pelo sistema, sem o conhecimento do usuário.

Na prática um sistema distribuído é um sistema de software instalado em uma rede. O software dá a ele um alto grau de coesão e transparência. Conseqüentemente, é o software (particularmente o sistema operacional) que determina a diferença entre uma rede e um sistema distribuído, não o hardware.

No entanto os dois assuntos têm uma série de pontos em comum. Por exemplo, os sistemas distribuídos e as redes de computadores precisam movimentar arquivos. A diferença está em quem é o responsável pela movimentação: o sistema ou o usuário.

1.2. HISTÓRICO DOS SISTEMAS DISTRIBUÍDOS

Origem: Sistemas Monolíticos e *Mainframes*

No início eram os *mainframes* a plataforma dominante de tecnologia de informação [figura 1], onde se concentravam as regras ou ambientes de negócios, os bancos de dados e as interfaces do usuário. Todos disponibilizados por vários terminais mudos (burros, sem poder de processamento). Tinha um alto custo e atendiam a um grande número de usuários todos controlados por ele.

Os softwares escritos para esta tecnologia são freqüentemente monolíticos, isto é, a interface do usuário, regras de negócios e acessos aos dados estão todos contidos em uma única aplicação.

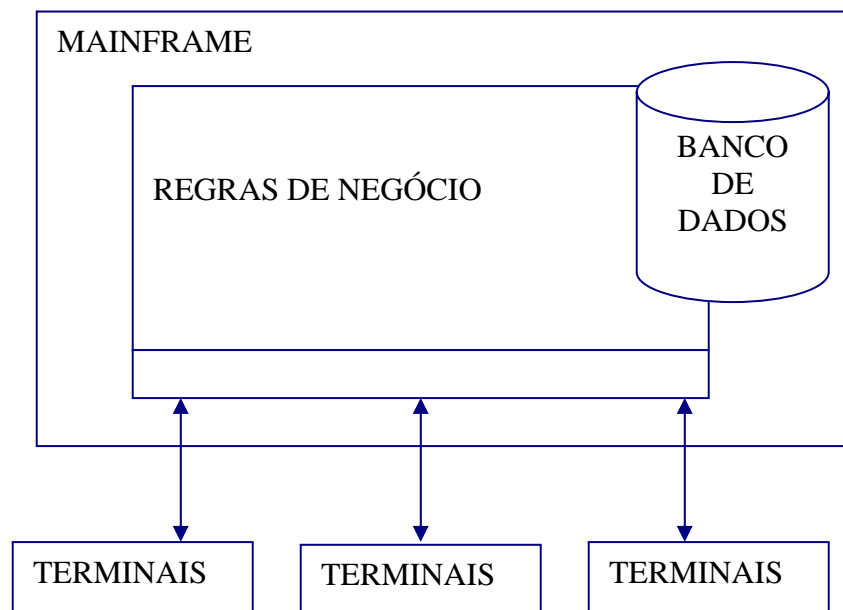


Figura 1 - Arquitetura Típica de Sistemas Monolíticos

Evolução: Modelo Cliente Servidor

Depois surgiu a geração de computadores de médio porte. Esses microcomputadores eram mais leves, mais flexíveis, mais baratos e mais fáceis de utilizar que os computadores de grande porte.

Essas máquinas tiveram uma década de sucesso, mas logo foram vítimas do surgimento de uma nova plataforma: o microcomputador ou computador pessoal (PC). E pela primeira, tarefas básicas de escritórios, tais como o compartilhamento de arquivos e impressoras se tornaram possíveis.

Nessa evolução da tecnologia da informação, surge a computação cliente servidor [figura 2], modelo de gerenciamento de informação que divide o processamento de

informação entre um computador que requer um serviço e outro que devolve um serviço, isto é, desempenha essa função numa plataforma que é mais bem adequada para este desempenho.

Com este modelo, a distribuição dos componentes da aplicação são divididos da seguinte maneira: os componentes da aplicação ficam divididos da seguinte maneira: os componentes da base de dados ficam no servidor; os componentes da interface do usuário ficam no cliente e os das regras de negócios em um ou no outro, ou em ambos.

Porém, este modelo apresentou falhas, pois com a mudança de um componente da parte do cliente, nova cópia do componente cliente (executável ou pacotes executáveis), tem de ser distribuída para cada usuário. Com o avanço de multicamadas no modelo cliente servidor, o modelo original ficou conhecido como arquitetura de duas camadas.

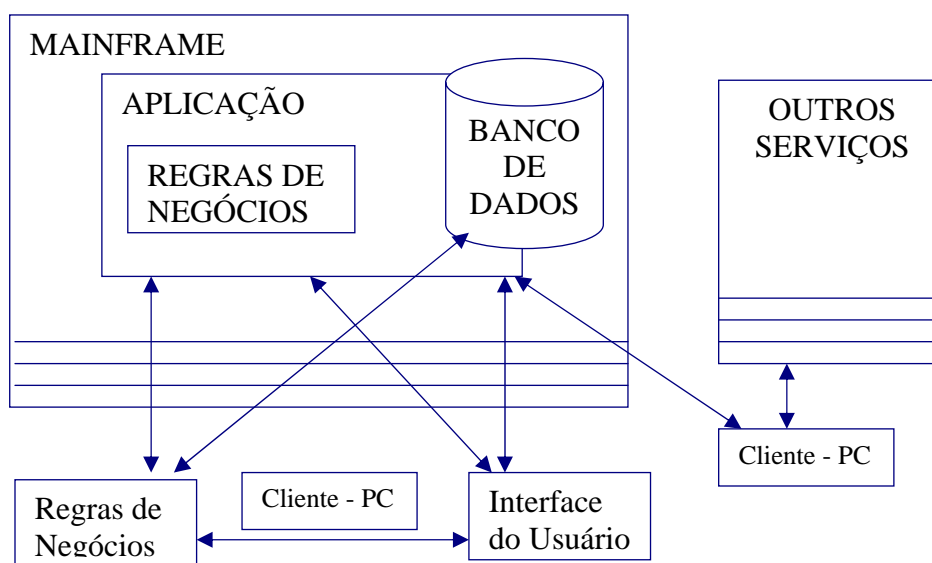


Figura 2 - Arquitetura duas Camadas Cliente Servidor

Evolução das Camadas do Modelo Cliente Servidor

A arquitetura cliente servidor foi sobre vários aspectos, uma revolução na computação. Apesar de resolver problemas das aplicações baseadas em *mainframes*, arquitetura cliente/servidor ainda apresentava falha. Por exemplo, a funcionalidade de acesso ao Banco de Dados (tal como consulta (*Query*)) e regras de negócios, estavam embutidas no componente cliente, e qualquer alteração nas regras de negócios, ou acesso ao Banco de Dados, ou mesmo no próprio banco, freqüentemente obrigavam a

atualização do componente para todos os usuários da aplicação, resultando em uma redistribuição da aplicação.

A tradicional arquitetura cliente/servidor (duas camadas) foi substituída pela de múltiplas camadas [figura 3]. Esta arquitetura divide o sistema em três camadas lógicas: a camada de interface de usuário, a camada de regras de negócio, e a camada de acesso ao Banco de Dados.

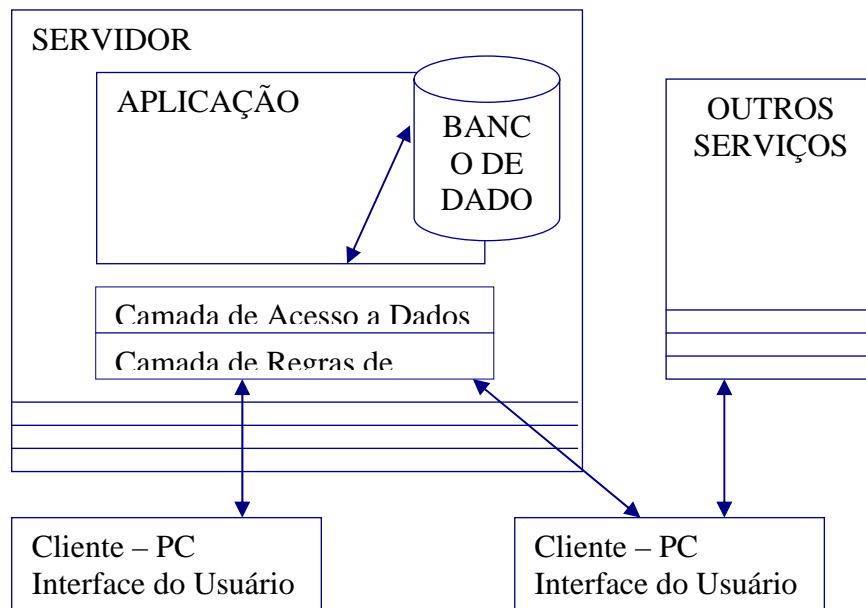


Figura 3 - Arquitetura Três Camadas Cliente Servidor

A arquitetura cliente/servidor multicamadas adiciona à arquitetura de duas camadas importantes pontos:

- Torna a aplicação menos frágil, isolando as alterações do cliente do restante da aplicação;
- Maior refinação nos componentes “escutáveis”, permitindo maior flexibilidade no desenvolvimento de qualquer aplicação;
- Maior isolamento entre as camadas.

A camada de interface do usuário comunica-se somente com a camada das regras de negócio, nunca diretamente com a camada de acesso aos dados. A camada de regras de negócio, por sua vez, comunica-se por um lado com a camada de interface de usuário e por outro lado com a camada de acesso a dados. Deste modo alterações feitas na camada de acesso aos dados não afetarão a camada de interface com usuário, pois são isoladas uma da outra. Esta arquitetura permite que alterações sejam feitas na aplicação

com menor probabilidade de afetar o componente cliente (o qual lembre-se, tem de ser redistribuído sempre que fora alterado).

Nesta arquitetura, os componentes de regra de negócios, acesso a dados, e o próprio banco de dados podem rodar em máquinas diferentes, distribuindo melhor a carga das aplicações, e tornando-as mais robustas e escaláveis, isto é, havendo a distinção entre cliente e servidor, sendo que cliente pode fornecer componente, tal como um servidor.

A Nova Geração: Sistemas Distribuídos

Com a evolução da arquitetura cliente/servidor multicamadas, as aplicações evoluíram sua arquitetura para um modelo de sistemas distribuídos [figura 4]. Unidas ao paradigma de orientação a objetos, as aplicações podem referenciar-se a objetos do sistema em qualquer lugar da rede, proporcionando assim, maior flexibilidade de reutilização de códigos, tornando mais eficiente o desenvolvimento de aplicações.

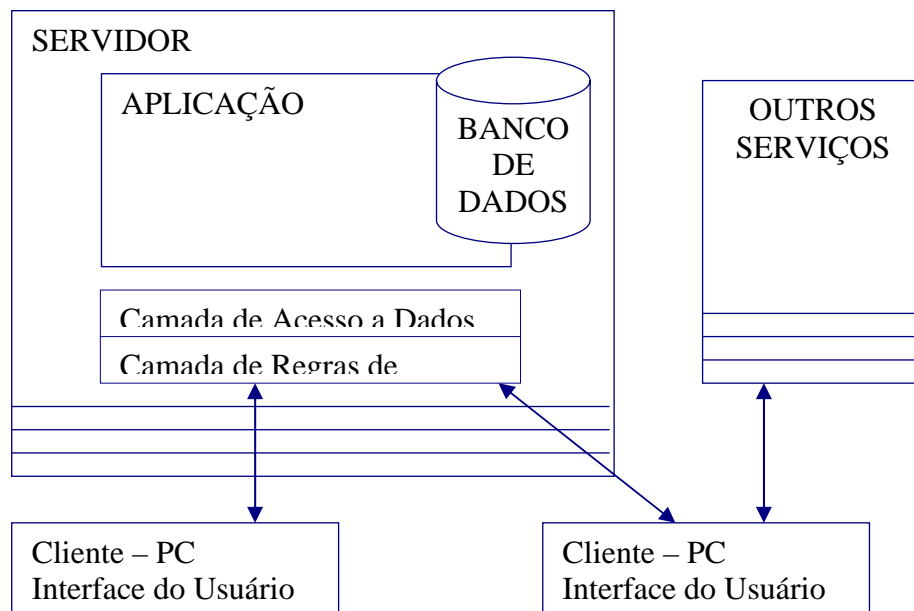


Figura 4 - Arquitetura Multi Camadas

Uma aplicação distribuída é composta por três camadas lógicas:

- Camada de Apresentação: em geral, é centrada nas estações, principalmente em redes cliente/servidor. Em ambientes como a WEB, algumas funções de apresentação também ficam sob a responsabilidade do servidor de dados ou aplicações.

- Camada de Aplicação: responsável pelas regras do negócio e pelo gerenciamento do fluxo de dados. Fica localizada nos servidores de aplicação, mas em alguns aspectos são manipuladas também pelo cliente e pelo servidor.
- Camada de Dados: assume o controle sobre os dados, propriamente dito.

1.3. NECESSIDADES DE GERENCIAMENTO

Independente da dimensão das redes de computadores, a mesma precisa ser gerenciada, a fim de garantir aos usuários, a disponibilidade de serviços a um nível de desempenho aceitável. A expansão das redes aumenta a complexidade de seu gerenciamento, forçando a adoção de ferramentas automatizadas para a sua monitoração e controle. As necessidades de gerenciamento das redes estão atreladas e não limitadas aos seguintes fatores:

- As redes estão ficando cada vez mais importantes para as empresas;
- São infra-estruturas indispensáveis, são de missão crítica, pois não podem parar;
- São cada vez maiores: atingem mais pessoas, mais lugares físicos da empresa, mais parceiros, até mesmo os clientes da empresa;
- São cada vez mais heterogêneas: mesclando tecnologias e fornecedores;
- A complexidade das tecnologias torna-se evidente, pois devem oferecer suporte para as aplicações multimídias, que não sejam de melhor esforço (áudio, vídeo, voz).
- Ainda existe deficiência de pessoal qualificado;
- Resultado: precisamos de boas soluções para gerenciar as redes.

Gerência: é tudo que é necessário para manter as redes funcionando bem. O gerenciamento de redes pode ser entendido como o processo de controlar uma rede de computadores de tal modo que seja possível maximizar sua eficiência e produtividade. Tal processo compreende um conjunto de funções integradas que podem estar em uma máquina ou espalhados por milhares de quilômetros, em diferentes organizações e residindo em máquinas distintas. Aqui, é importante observar que com estas funções pode-se controlar uma rede de computadores e seus serviços, provendo mecanismos de monitoração, análise e controle dos dispositivos e recursos da rede.

1.4. GERÊNCIA DE REDES E GERÊNCIA DE SISTEMAS

Uma rede corporativa não consiste somente da infra-estrutura da rede. Tudo tem que estar funcionando adequadamente, não apenas a infraestrutura da rede [figura 5].

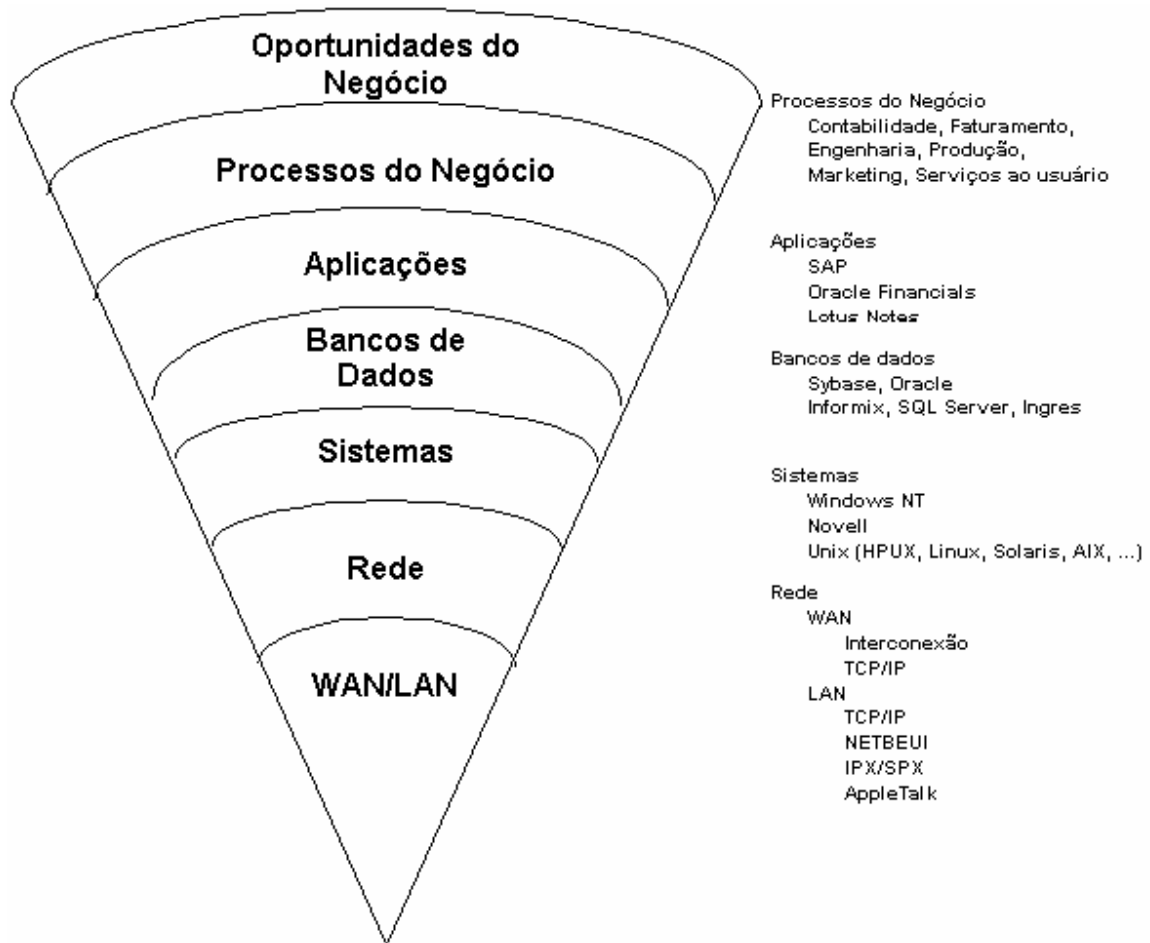


Figura 5 – Estrutura de Uma Rede Corporativa

Gerência de Rede

Na gerência de redes os seguintes elementos que compõem a rede devem ser gerenciados: roteadores; pontes; *switches*, *hubs*, repetidores, cabeamento, *modems*, servidores de terminais, multiplexadores, enlaces, conexões etc. Para cada um dos elementos que formam uma rede, tarefas típicas de gerenciamento devem ser efetuadas.

Tarefas Típicas de Gerenciamento nos Elementos de Rede

- Configuração de dispositivos: está relacionada com a forma que os elementos de rede serão configurados.
- Administração de endereços IP: diz respeito ao modo com que os endereços de rede serão administrados, de forma estática (IPs fixos) ou de forma dinâmica (IPs dinâmicos distribuídos por servidores de DHCP, por exemplo).
- Serviços de Diretórios: que políticas de acessos, atualizações de conteúdos serão aplicadas aos serviços de diretórios. Diretórios são bases de dados otimizados para leitura e podem conter informações sobre pessoas, processos, recursos e grupos. São úteis para uma grande gama de aplicações.
- Monitoração de tráfego: que políticas serão adotadas para realizar a monitoração de todo o fluxo de pacotes que trafegam na rede.
- Diagnóstico de faltas: está intimamente ligada com a prevenção, detecção e solução de problemas que possam causar falhas na rede.
- Tratamento de alarmes: será necessário estabelecer limiares para gerar alarmes. Por exemplo, configurar uma ferramenta de gerência para que um alarme sonoro seja executado antes que uma falha ocorra na rede.
- Restauração de serviço: utilizar mecanismos para recuperar ou restaurar um equipamento de rede.
- Análises de Dados e Relatórios: todos os dados que trafegam na rede devem ser monitorados, analisados e muitas vezes controlados. Para que com base nos dados coletados, seja possível gerar relatórios de forma que os clientes da rede tenham conhecimento da disponibilidade/indisponibilidade de um recurso de rede, por exemplo.
- Registro de Problemas: todos os problemas potenciais ocorridos nos equipamentos da rede devem ser registrados. Neste registro devem conter: hora início e término do problema; operador do equipamento; severidade do problema; descrição do problema; que outros equipamentos estão envolvidos; qual rede os equipamentos pertencem; endereço do equipamento; responsável pelo registro; disposição adotada na solução do problema.
- Segurança de Rede: que soluções de segurança serão implementadas para amenizar a vulnerabilidade da rede. Uma forma segura seria a implantação de uma plataforma *Firewall* (plataformas compostas de hardware e software que

separam e filtram o fluxo de dados local do externo), criando seguranças para o uso interno da companhia e acesso externo.

- Inventário: é necessário ter uma documentação do levantamento preciso e atualizado de todos os componentes da rede.
- Etc.

Gerência de Sistemas

Na gerência de sistemas, os seguintes elementos que estão embutidos nas redes devem ser gerenciados: servidores de arquivos, servidores de impressão, servidores de banco de dados, servidores de aplicação, estações de trabalho, banco de dados, sistemas operacionais, correio eletrônico, aplicações etc. Para cada elemento tarefas típicas de gerenciamento devem ser efetuadas.

Tarefas Típicas de Gerenciamento nos Elementos do Sistema

- Automação de console: geralmente adota-se um servidor se console, onde os gerentes de rede poderão acessar de modo conveniente, seguro e remotas todas as portas console dos equipamentos da rede, a qualquer hora e em qualquer lugar.
- Monitoração de Desempenho: em termos de métricas de Qualidade de Serviço (QoS) ou de serviços de melhor esforço, devem ser analisados se os serviços que estão sendo oferecidos aos usuários estão dentro de níveis pré-aceitáveis. Para isso alguns limiares serão estabelecidos, como por exemplo: qual deve ser o *delay* de uma LAN? Qual deve ser o atraso e a variação de atraso etc.
- Diagnóstico de falhas: saber o porquê os níveis estabelecidos para as métricas não sendo cumpridos, detectar as causas das falhas: se for um problema de colisão na rede, se é um problema no link alocado etc.
- Inventário: é necessário ter uma documentação do levantamento preciso e atualizado de todos os componentes que fazem parte do sistema.
- Distribuição de *software*: conhecer toda a infra-estrutura da rede, serviços, atividades dos usuários, para que os softwares sejam adequadamente distribuídos na rede.
- Controle de licenças de *software*: é imprescindível que se tenha um controle de todas as licenças de softwares de uma organização.

- Administração de usuários (contas): esta tarefa está relacionada com administração e alocação de contas, autorizações, limites e restrições aos usuários.
- Registro de Problemas: todos os problemas potenciais ocorridos nos equipamentos e/ou sistemas da rede devem ser registrados. Neste registro devem conter: hora início e término do problema; operador do equipamento; severidade do problema; descrição do problema; que outros equipamentos e/ou sistema estão envolvidos; qual rede os equipamentos pertencem; endereço do equipamento; responsável pelo registro; disposição adotada na solução do problema.
- Gerência de Armazenamento: realizar um gerenciamento para saber a capacidade que os discos dos servidores podem suportar. Criar rotinas para que o sistema avise o administrador que os discos estão quase no limite de sua capacidade de armazenamento.
- Backup dos Dados: a adoção de uma política de backup bem elaborada evitará problemas futuros. Lembre-se que perdas de informações não são causadas apenas por falhas nos equipamentos, mas também por desastres como fogo, umidade, roubo, explosões. Neste sentido recomenda-se a obtenção de um cofre de segurança para o armazenamento de mídias magnéticas e microfilmes. Não importa a política de backup que será adotada (fita, cd etc) o importante é saber que a mesma deve ser implementada.
- Backup de Equipamento: o ideal seria que as empresas possuíssem equipamentos já prontos, configurados, para que na falha de um outro equipamento, este fosse substituído por um backup.
- Gerência de *Spool*: esta tarefa está relacionada com a área de dispositivos de armazenamento.
- Segurança de sistema: rotina de primordial importância, nela deverá ser realizada as permissões, autorizações, restrições dos usuários que terão acesso nos sistemas da rede. Um bom programa de antivírus deve estar instalado e atualizado em todos os servidores e estações de trabalho.
- Etc.

Através do exposto é possível conhecer que tanto a Gerência de Redes quanto a Gerência de Sistemas são tarefas extremamente complexas e abrangentes, pois são constituídas de inúmeros elementos que necessitam ser gerenciados com eficiência. Para

isto, necessita-se de recursos humanos altamente capacitados e competentes e principalmente de plataformas de Gerência para a monitoração e controle dos elementos que constituem as redes e os sistemas distribuídos.

Plataforma de Gerência

A plataforma de gerência é "sistema operacional" da gerência; oferece funções básicas de gerência (comuns a muitas aplicações), oferece um ambiente para o desenvolvimento e a integração de aplicações; sobre as plataformas estão as diversas aplicações usadas pelos operadores. A plataforma deve prover serviços básicos para as aplicações QUE A USAM. A figura 6 apresenta um exemplo simplificado de plataforma de gerência.

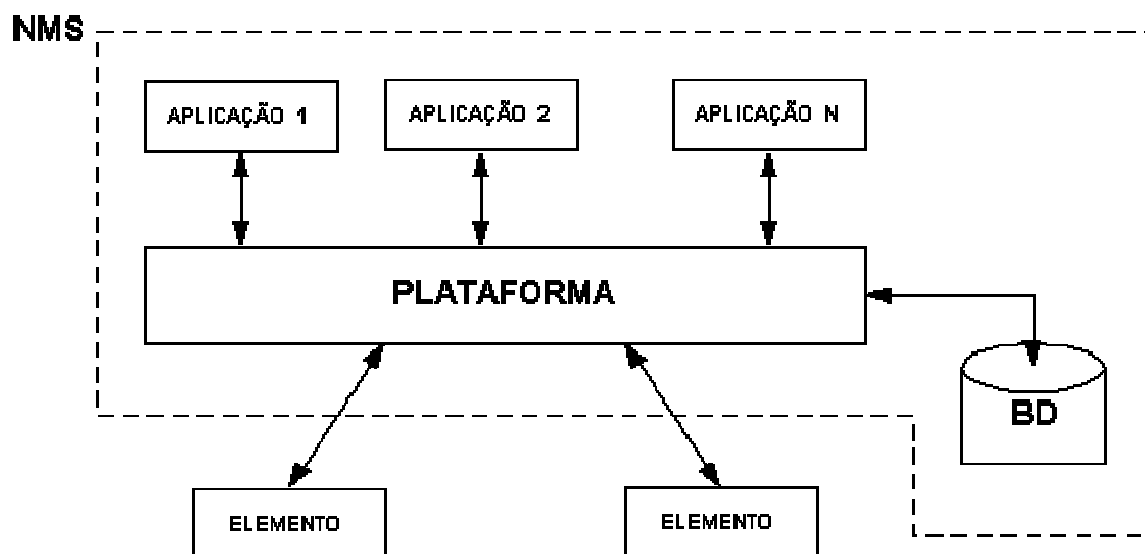


Figura 6 - Exemplo simplificado de uma Plataforma de Gerência

O exemplo acima ilustrou uma plataforma de gerência bem simplificada. Observe que a plataforma de gerência precisa de muitas aplicações com finalidades específicas porque não há como ter uma única aplicação zona de gerência. A dificuldade de construir aplicações está no fato de muitas vezes os fornecedores (desenvolvedores) não se especializam.

São exemplos de plataforma de gerência: *Openview da Hp; Sunnet Manager da Sun Microsystems; Netview da Ibm; Spectrum da Cabletron; Ca-Unicenter da Computer Associates; Whats Up Gold e Advence Net.*

O quadro 1 apresenta exemplos de aplicações de Gerência.

Quadro 1 - Exemplos Aplicações de Gerência

FUNCIÓNLAIDADE	APLICAÇÃO	FABRICANTE
Gerência de Desempenho	NETCLARITY	LANQUEST
Gerência de Faltas	SPECTRUM'S ALARM MANAGERS	CABLETRON
Manipulação de Alarmes	TRAP EXPLORER	EMPIRE TECNHNOLOGIES
Gerência de Segurança	BOKS	SECURIX
Gerência de Bens	ASSETVIEW	HP
Configuração	NETBUILDER	3 COM
Configuração	CISCO WORKS	CISCO

2. ÁREAS FUNCIONAIS DE GERENCIAMENTO

Uma separação funcional de necessidades no processo de gerenciamento foi apresentada pela ISO (*International Organization for Standardization*), como parte de sua especificação de Gerenciamento de Sistemas OSI: falhas, desempenho, configuração, contabilização e segurança.

2.1. GERENCIAMENTO DE FALHAS

Falhas não são o mesmo que erros. Uma falha é uma condição anormal cuja recuperação exige ação de gerenciamento. Uma falha normalmente é causada por operações incorretas ou um número excessivo de erros. Por exemplo, se uma linha de comunicação é cortada fisicamente, nenhum sinal pode passar através dela. Um grampeamento no cabo pode causar distorções que induzem à uma alta taxa de erros. Certos erros como, por exemplo, um bit errado em uma linha de comunicação, podem ocorrer ocasionalmente e normalmente não são consideradas falhas.

Para controlar o sistema como um todo, cada componente essencial deve ser monitorado individualmente para garantir o seu perfeito funcionamento. Quando ocorre uma falha, é importante que seja possível, rapidamente:

- Determinar o componente exato onde a falha ocorreu;
- Isolar o resto da rede da falha, de tal forma que ela continue a funcionar sem interferências;
- Reconfigurar ou modificar a rede para minimizar o impacto da operação sem o componente que falhou;
- Reparar ou trocar o componente com problemas para restaurar a rede ao seu estado anterior.

O impacto e a duração do estado de falha pode ser minimizado pelo uso de componentes redundantes e rotas de comunicação alternativas, para dar à rede um grau de “tolerância à falhas”.

2.2. GERENCIAMENTO DE CONTABILIZAÇÃO

Mesmo que nenhuma cobrança interna seja feita pela utilização dos recursos da rede, o administrador da rede deve estar habilitado para controlar o uso dos recursos por usuário ou grupo de usuários, com o objetivo de:

- Evitar que um usuário ou grupo de usuários abuse de seus privilégios de acesso e monopolize a rede, em detrimento de outros usuários;
- Evitar que usuários façam uso ineficiente da rede, assistindo-os na troca de procedimentos e garantindo o desempenho da rede;
- Conhecer as atividades dos usuários com detalhes suficientes para planejar o crescimento da rede.

O gerente da rede deve ser capaz de especificar os tipos de informações de contabilização que devem ser registrados em cada nodo, o intervalo de entrega de relatórios para nodos de gerenciamento de mais alto nível e os algoritmos usados no cálculo da utilização.

2.3. GERENCIAMENTO DE CONFIGURAÇÃO

O gerenciamento de configuração está relacionado com a inicialização da rede e com uma eventual desabilitação de parte ou de toda a rede. Também está relacionado com as tarefas de manutenção, adição e atualização de relacionamentos entre os componentes e do status dos componentes durante a operação da rede.

Alguns recursos podem ser configurados para executar diferentes serviços como, por exemplo, um equipamento pode atuar como roteador, como estação de trabalho ou ambos. Uma vez decidido como o equipamento deve ser usado, o gerente de configuração pode escolher o software apropriado e um conjunto de valores para os atributos daquele equipamento.

O gerente da rede deve ser capaz de, inicialmente, identificar os componentes da rede e definir a conectividade entre eles. Também deve ser capaz de modificar a configuração em resposta às avaliações de desempenho, recuperação de falhas, problemas de segurança, atualização da rede ou a fim de atender às necessidades dos usuários.

Relatórios de configuração podem ser gerados periodicamente ou em resposta às requisições de usuários.

2.4. GERENCIAMENTO DE DESEMPENHO

O gerenciamento do desempenho de uma rede consiste na monitoração das atividades da rede e no controle dos recursos através de ajustes e trocas. Algumas das questões relativas ao gerenciamento do desempenho são:

- Qual é o nível de capacidade de utilização?
- O tráfego é excessivo?
- O *throughput* foi reduzido para níveis aceitáveis?
- Existem gargalos?
- O tempo de resposta está aumentando?

Para tratar estas questões, o gerente deve focalizar um conjunto inicial de recursos a serem monitorados, a fim de estabelecer níveis de desempenho. Isto inclui associar métricas e valores apropriados aos recursos de rede que possam fornecer indicadores de diferentes níveis de desempenho. Muitos recursos devem ser monitorados para se obter informações sobre o nível de operação da rede. Colecionando e analisando estas informações, o gerente da rede pode ficar mais e mais capacitado no reconhecimento de situações indicativas de degradação de desempenho.

Estatísticas de desempenho podem ajudar no planejamento, administração e manutenção de grandes redes. Estas informações podem ser utilizadas para reconhecer situações de gargalo antes que elas causem problemas para o usuário final. Ações corretivas podem ser executadas, tais como, trocar tabelas de roteamento para balancear ou redistribuir a carga de tráfego durante horários de pico, ou ainda, em longo prazo, indicar a necessidade de expansão de linhas para uma determinada área.

2.5. GERENCIAMENTO DE SEGURANÇA

O gerenciamento da segurança provê facilidades para proteger recursos da rede e informações dos usuários. Estas facilidades devem estar disponíveis apenas para usuários autorizados. É necessário que a política de segurança seja robusta e efetiva e que o sistema de gerenciamento da segurança seja, ele próprio, seguro.

O gerenciamento de segurança trata de questões como:

- Geração, distribuição e armazenamento de chaves de criptografia;
- Manutenção e distribuição de senhas e informações de controle de acesso;
- Monitoração e controle de acesso à rede ou parte da rede e às informações obtidas dos nodos da rede;
- Coleta, armazenamento e exame de registros de auditoria e logs de segurança, bem como ativação e desativação destas atividades.

3. FUNÇÕES DE GERENCIAMENTO DE REDE

As funções de gerenciamento de rede podem ser agrupadas em duas categorias: monitoração de rede e controle de rede. A monitoração da rede está relacionada com a tarefa de observação e análise do estado e configuração de seus componentes; é uma função de “leitura”. O controle da rede é uma função de “escrita” e está relacionada com a tarefa de alteração de valores de parâmetros e execução de determinadas ações.

3.1. MONITORAÇÃO

A monitoração consiste na observação de informações relevantes ao gerenciamento. Estas informações podem ser classificadas em três categorias:

- Estática: caracteriza a configuração atual e os elementos na atual configuração, tais como o número e identificação de portas em um roteador.
- Dinâmica: relacionada com os eventos na rede, tais como a transmissão de um pacote na rede.
- Estatística: pode ser derivada de informações dinâmicas; ex. média de pacotes transmitidos por unidade de tempo em um determinado sistema.

A informação de gerenciamento é coletada e armazenada por agentes e repassada para um ou mais gerentes. Duas técnicas podem ser utilizadas na comunicação entre agentes e gerentes: *polling* e *event-reporting*.

A técnica de *polling* consiste em uma interação do tipo *request/response* entre um gerente e um agente. O gerente pode solicitar a um agente (para o qual ele tenha autorização), o envio de valores de diversos elementos de informação. O agente responde com os valores constantes em sua MIB.

Na técnica de *event-reporting*, a iniciativa é do agente. O gerente fica na escuta, esperando pela chegada de informações. Um agente pode gerar um relatório periodicamente para fornecer ao gerente o seu estado atual. A periodicidade do relatório pode ser configurada previamente pelo gerente. Um agente também pode enviar um relatório quando ocorre um evento significativo ou não usual.

Tanto o *polling* quanto o *event-reporting* são usados nos sistemas de gerenciamento, porém a ênfase dada a cada um dos métodos difere muito entre os sistemas. Em sistemas de gerenciamento de redes de telecomunicações, a ênfase maior é dada para o método de relatório de evento. Em contraste, o modelo SNMP dá pouca importância ao relatório de evento. O modelo OSI fica entre estes dois extremos.

A escolha da ênfase depende de um número de fatores, incluindo os seguintes:

- A quantidade de tráfego gerada por cada método;
- Robustez em situações críticas;
- O tempo entre a ocorrência do evento e a notificação ao gerente;
- A quantidade de processamento nos equipamentos gerenciados;
- A problemática referente à transferência confiável versus transferência não confiável;
- As aplicações de monitoração de rede suportadas;
- As considerações referentes ao caso em que um equipamento falhe antes de enviar um relatório.

3.2. CONTROLE DE REDE

Esta parte do gerenciamento de rede diz respeito à modificação de parâmetros e à execução de ações em um sistema remoto. Todas as cinco áreas funcionais de gerenciamento (falhas, desempenho, contabilização, configuração e segurança), envolvem monitoração e controle. Tradicionalmente, no entanto, a ênfase nas três primeiras destas áreas, tem sido na monitoração, enquanto que nas duas últimas, o controle tem sido mais enfatizado. Alguns aspectos de controle na gerência de configuração e de segurança são apresentados a seguir.

O controle de configuração inclui as seguintes funções:

- Definição da informação de configuração - recursos e atributos dos recursos sujeitos ao gerenciamento;
- Atribuição e modificação de valores de atributos;
- Definição e modificação de relacionamentos entre recursos ou componentes da rede;
- Inicialização e terminação de operações de rede;
- Distribuição de software;
- Exame de valores e relacionamentos;
- Relatórios de status de configuração.

O controle de segurança é relativo à segurança dos recursos sob gerenciamento, incluindo o próprio sistema de gerenciamento. Os principais objetivos em termos de segurança, são relativos a confidencialidade, integridade e disponibilidade. As principais

ameaças à segurança referem-se à interrupção, interceptação, modificação e mascaramento.

As funções de gerenciamento de segurança podem ser agrupadas em três categorias:

- Manutenção da informação de segurança
- Controle de acesso aos recursos
- Controle do processo de criptografia.

4. MODELOS DE GERENCIAMENTO DE REDE

Um sistema de gerenciamento de rede é uma coleção de ferramentas para monitorar e controlar a rede, integradas da seguinte forma:

- Uma única interface de operador, com um poderoso, mas amigável conjunto de comandos, para executar a maioria ou todas as tarefas de gerenciamento da rede;
- Uma quantidade mínima de equipamentos separados, isto é, que a maioria do *hardware* e *software* necessário para o gerenciamento da rede seja incorporado nos equipamentos de usuários existentes.

O *software* usado para realizar as tarefas de gerenciamento reside nos computadores hospedeiros (estações de trabalho) e nos processadores de comunicação (*switches*, *routers*, *hubs*, etc).

Todos os equipamentos da rede, que fazem parte do sistema de gerenciamento, possuem um conjunto de *software* destinado às tarefas de coletar informações sobre as atividades relacionadas com a rede, armazenar estatísticas localmente e responder aos comandos do centro de controle da rede. Estes nodos são referenciados como AGENTES. No mínimo um hospedeiro da rede é designado para as tarefas de controlador da rede (GERENTE) e possui uma coleção de *software* chamada Aplicação de Gerenciamento da Rede. A aplicação de gerenciamento da rede possui uma interface que permite, a um usuário autorizado, gerenciar a rede. A figura 7 apresenta um cenário possível de um sistema de gerenciamento de rede.

Um *software* de gerenciamento genérico é composto por:

- Elementos gerenciados
- Agentes
- Gerentes
- Bancos de Dados de Informações
- Protocolos para troca de informações de gerenciamento
- Interfaces para programas aplicativos
- Interfaces com o usuário

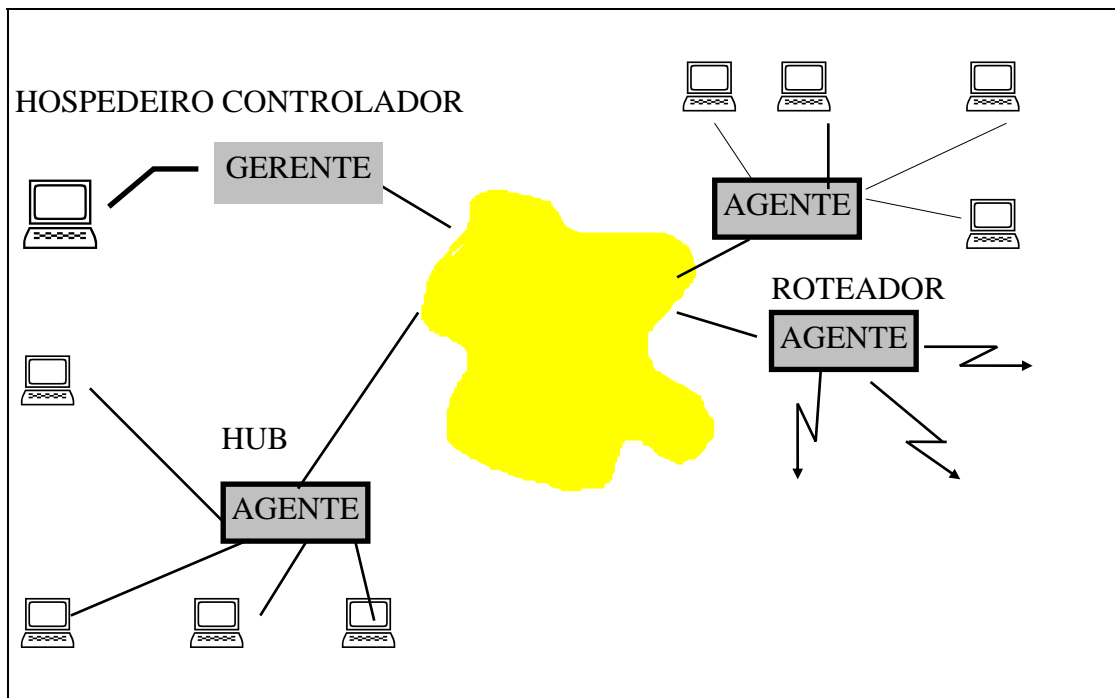


Figura 7 – Configuração de um sistema de gerenciamento de rede.

A arquitetura do software de gerenciamento residente no gerente e nos agentes varia de acordo com a funcionalidade da plataforma adotada. Genericamente, o software pode ser dividido em três grandes categorias:

- *Software* de apresentação (interface)
- *Software* de gerenciamento (aplicação)
- *Software* de suporte (base de dados e comunicação)

4.1. SOFTWARE DE APRESENTAÇÃO

A interface de usuário, em um sistema de gerenciamento, permite que o usuário monitore e controle a rede. Normalmente ela está localizada no sistema hospedeiro gerente. Em alguns casos é comum existir uma interface em alguns agentes a fim de permitir a execução de testes e também a visualização ou alteração de alguns parâmetros localmente. A figura 8 (a) mostra os dois blocos que representam o software de apresentação das informações de gerência.

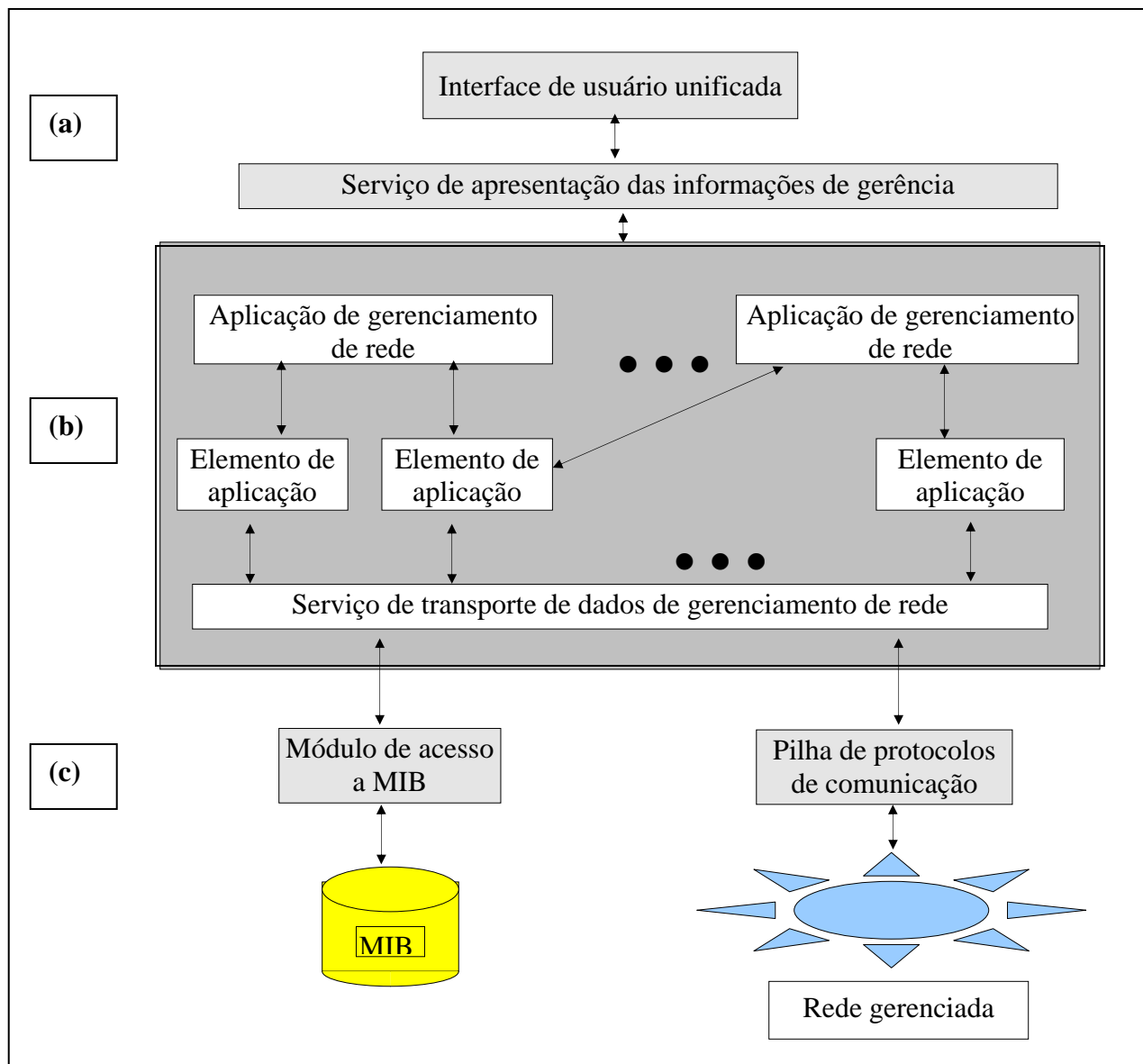


Figura 8 - Arquitetura de um Sistema de Gerenciamento de Rede

O principal, em qualquer sistema de gerenciamento, é que a interface seja unificada, isto é, que ela seja a mesma em qualquer nodo, permitindo que o usuário gerencie uma rede heterogênea com um mínimo de treinamento.

Um dos perigos em qualquer sistema de gerenciamento é a sobrecarga de informações. Dependendo da configuração estabelecida, uma grande quantidade de informações pode ser disponibilizada para o usuário. As ferramentas da interface de apresentação devem organizar, sumarizar e simplificar, tanto quanto possível estas informações. Na maioria dos produtos existentes no mercado, são utilizados gráficos e tabelas para a apresentação das informações.

4.2. SOFTWARE DE GERENCIAMENTO

O software que fornece a aplicação de gerenciamento pode ser muito simples, como é o caso do modelo SNMP, ou muito complexo, como o modelo OSI. A figura 8 (b) mostra uma estrutura genérica de um software de gerenciamento organizada em três níveis: aplicação de gerenciamento de rede, elementos de serviço da aplicação e serviço de transporte de dados de gerenciamento da rede.

A aplicação de gerenciamento de rede provê os serviços de interesse do usuário como, por exemplo, gerenciamento de falhas, de configuração, de segurança, etc. Os elementos de serviço da aplicação implementam as funções com propósito geral, que servem de suporte às diversas aplicações, tais como, alarmes genéricos ou sumarização de dados. O serviço de transporte de dados de gerenciamento consiste de um protocolo usado para a troca de informações entre gerentes e agentes e de uma interface de serviço para os elementos de serviço de aplicação.

4.3. SOFTWARE DE SUPORTE AO GERENCIAMENTO

Para executar suas tarefas, o software de gerenciamento necessita acessar uma base de informações de gerenciamento (MIB) e agentes e gerentes remotos.

A MIB localizada em um nodo agente contém informações de gerenciamento que refletem a configuração e o comportamento do nodo e parâmetros que podem ser usados para controlar a operação do nodo. A MIB localizada no gerente contém informações específicas do nodo onde está localizada e informações resumidas sobre os agentes sob o seu controle.

O módulo de acesso à MIB, mostrado na figura 8 (c), inclui software de gerenciamento de arquivos que habilitam o acesso à MIB. Adicionalmente, o módulo de

acesso a MIB pode converter o formato local das informações para um formato padronizado do sistema de gerenciamento.

O modelo de informação de um sistema de gerenciamento fornece a estrutura para representação, armazenamento e transferência das informações de gerenciamento. Esta estrutura é denominada SMI (*Structure Management Information*) e, dependendo do sistema, poderá apresentar maior ou menor complexidade.

No modelo OSI, a SMI é baseada no paradigma de orientação a objetos, enfatizando as hierarquias de classe, de *containment* e de registro. Já o modelo SNMP, utiliza conceitos de Tipos de Dados, embora a sua nomenclatura refira-se a objetos.

O quadro 2 mostra exemplos de definição de objeto em cada um dos modelos.

Quadro 2 - Especificação de Objetos Gerenciáveis

Modelo SNMP	Modelo OSI
abcObjectType OBJECT-TYPE SYNTAX INTEGER { choicelabel1 (1), choicelabel2 (2) } ACCESS read-only STATUS mandatory DESCRIPTION "Description Text" ::= { pqr 3 }	network MANAGED OBJECT CLASS DERIVED FROM top; BEHAVIOR network-behavior; CHARACTERIZED BY networkPackage PACKAGE ATTRIBUTES networkID GET, networkType GET; REGISTERED AS (exemplo MObjectClass 2);

A comunicação entre gerentes e agentes é suportada por uma pilha de protocolos, tais como a pilha OSI ou a pilha TCP/IP. A arquitetura de comunicação suporta o protocolo de gerenciamento de rede que está localizado na camada de aplicação.

Os serviços básicos de um sistema de gerenciamento de rede são os serviços de monitoração e controle. Estes serviços são obtidos através de primitivas para a leitura e escrita nos valores dos objetos gerenciados. Outros serviços adicionais são: criação e destruição de objetos gerenciados, execução de ações sobre objetos gerenciados e emissão de relatórios de eventos.

A comunicação entre agentes e gerentes, a fim de alcançar estes serviços, deve seguir um conjunto de regras básicas, como em qualquer outra aplicação distribuída. Este conjunto de regras pode apresentar maior ou menor complexidade, dependendo do modelo adotado. O modelo OSI utiliza o protocolo CMIP (*Common Management*

Information Protocol) que apresenta funcionalidades para emitir relatórios diversos sobre a ocorrência de eventos, criar e destruir instâncias de classes de objetos, executar ações sobre objetos, ler e modificar valores de atributos de objetos e para a execução de operações sobre vários objetos a partir da definição de um escopo e de um filtro para a seleção de objetos. O modelo Internet utiliza o protocolo SNMP (*Simple Network Information Protocol*), cuja funcionalidade reside basicamente na leitura e alteração de valores de variáveis e em alguns relatórios de evento para situações específicas.

REFERÊNCIAS BIBLIOGRÁFICAS

- TANENBAUM, Andrew. Redes de Computadores. Rio de Janeiro: Campus, 1997.
- COMER, Douglas E. Redes de Computadores e Internet. Porto Alegre: Bookman, 2001.
- RICCIONI, Paulo Roberto. Introdução a Objetos Distribuídos com Corba. Visual Books, 2000.
- RIGNEY, Steve. Planejamento e Gerenciamento de Redes. Campus, 1996.
- SILVA, Mário Gomes. Gerenciamento de Redes. Érica, 1999.
- SPECIALSKI, Elizabeth Sueli. Apostila de Gerência de Redes de Computadores e de Telecomunicações, 2002.