Gerência de Redes

Motivação

- as redes estão ficando cada vez mais importantes para as empresas
  - não são mais infra-estrutura dispensável: são de missão crítica (não podem parar!)
- as redes são cada vez maiores
  - atingem mais gente na empresa
  - atingem mais lugares físicos da empresa
  - atingem mais parceiros da empresa
  - atingem até os clientes da empresa

Motivação

- as redes são cada vez mais heterogêneas
  - mesclagem de tecnologias
  - mesclagem de fornecedores
- as tecnologias são cada vez mais complexas
  - exemplo: para suportar serviços que não sejam best-effort (vídeo conferência, ...)
- a falta de pessoal qualificado continua
  - resultado: precisamos de boas soluções para gerenciar as redes
- **gerência é tudo que é necessário para manter as redes funcionando bem**

Conceito

- Gerência de Rede
  - processo de controle de uma rede de dados visando maximizar sua eficiência e produtividade
  - atividade que monitora e controla os elementos da rede (físicos ou lógicos), assegurando um certo nível de qualidade de serviço
  - o gerenciamento de rede pode ser definido como a coordenação (controle de atividades e monitoração de uso) de recursos materiais (modems, roteadores, etc.) e ou lógicos (protocolos), fisicamente distribuídos na rede, assegurando, na medida do possível, confiabilidade, tempos de resposta aceitáveis e segurança das informações.

Objetivos

- controlar o funcionamento de uma rede de computadores
- controlar a complexidade da rede
- otimizar o serviço de comunicação
- otimização do uso de recursos disponíveis
- diminuir o tempo de indisponibilidade de uma rede
- auxílio no controle de gastos

Funções de Gerência de Redes

- planejamento inicial da rede
- gerência de configuração
- gerência de falhas
- gerência de segurança
- gerência de desempenho
- gerência de contabilização

Problemas de uma rede sem gerência

- congestionamento do tráfego
- recursos mal utilizados
- recursos sobrecarregados
- problemas com segurança
- ...

Ferramentas de gerência de redes

- ferramentas simples: detectam problemas comuns de conectividade
  - Exemplos: traceroute, ping, route, netstat, ifconfig
  - traceroute: permite descobrir onde o problema está localizado (técnica da porta aberta)
    - Gerência Reativa!
      - baixa escalabilidade: não suporta um grande conjunto de elementos
      - alternativa -> utilização de um sistema de gerência de rede: mapa da rede é apresentado e alarmes são gerados automaticamente quando limiares ou mudanças de estado operacional são detectados

Gerência reativa vs pró-ativa

- gerência reativa
  - todo o processo é acionado após a ocorrência da falha e a perda de conectividade ou queda de desempenho
  - processo consiste então em detectar a falha, isolar, corrigir e documentar
- gerência pró-ativa
  - o administrador busca, continuamente, informações que possam ajudá-lo a antecipar problemas
  - recursos estatísticos e monitoramento diário são usados para acompanhar as mudanças de comportamento e para antecipar-se às falhas e à perda de desempenho

Ferramentas de gerência de redes

- monitores de rede
  - se conectam às redes (um por segmento), monitorando o tráfego
  - através do exame das informações a nível de pacotes, o monitor consegue compilar estatísticas referentes a utilização das redes, tipos de pacotes, número de pacotes enviados e recebidos por cada nó da rede, pacotes com erros e outras variáveis importantes
- analisadores de rede
  - auxiliam no rastreamento e correção de problemas encontrados nas redes
  - apresentam características sofisticadas para análise do tráfego da rede, captura de decodificação de pacotes e transmissão de pacotes em tempo real

Sistema de Gerência de Redes

- coleção de ferramentas integradas para monitoração e controle
- oferece uma interface única, com informações sobre a rede
- pode oferecer também um conjunto poderoso e amigável de comandos que são usados para executar quase todas as tarefas da gerência da rede
- permitem o monitoramento e controle de uma rede inteira a partir de um ponto central (Estação de gerência)
- composto por uma plataforma de gerência de redes (PGR) e aplicações de gerência de redes

Plataforma de Gerência de Redes (PGR)

- sistema operacional da gerência
- sistema único para a gerência integrada de todos os dispositivos da rede
- sobre as plataformas estão as diversas aplicações usadas pelos operadores
- contém funcionalidades comuns a várias aplicações de gerência

PGR - Funcionalidades

- Interface gráfica com o usuário
- Mapa da rede
  - algoritmos de auto-descobrimento de topologia (“automapping”)
  - editores gráficos de topologias
- Sistema de gerência de banco de dados (SGBD);
  - volume de dados muito grande
  - correlação entre as informações
  - geração de relatórios personalizados

PGR - Funcionalidades

- Método padrão de consulta aos dispositivos;
  - coleta de informações de diferentes dispositivos
  - rotinas de acesso a MIB dos agentes utilizando o protocolo de gerência
- Sistema de menus adaptável
  - permite a visibilidade da inclusão de novas funcionalidades
- Histórico (log) de eventos
  - armazena eventos cronologicamente em um formato legível
  - útil em várias tarefas de gerência.

PGR - Características

- contém uma API que permite que várias aplicações especiais sejam construídas e inseridas na plataforma lançando mão de todos os recursos oferecidos pela plataforma
- contém uma aplicação simples de gerência que permite, pelo menos, visualizar graficamente a evolução com o tempo dos valores das variáveis dos agentes. (MIB Browser)
- apresenta uma interface amigável com o usuário, permitindo que qualquer usuário interaja sem necessidade de treinamento, preferencialmente baseada na WEB
- livre de plataforma, podendo assim gerenciar qualquer dispositivo independente da plataforma

PGR - Exemplos

- OpenView da Hewlett Packard
- NetView e Tivoli da IBM
- Spectrum da Aprisma
- CA-Unicenter da Computer Associates
- SunNet Manager da Sun Microsystems
- StarSentry da AT&T

Aplicação de gerência

- funcionalidade específica para um determinado conjunto de dispositivos
- gerenciar efetivamente um conjunto específico de dispositivos
- evitar sobreposição de funcionalidades
- integrar-se com a plataforma através das APIs
- deve ser portátil para várias plataformas

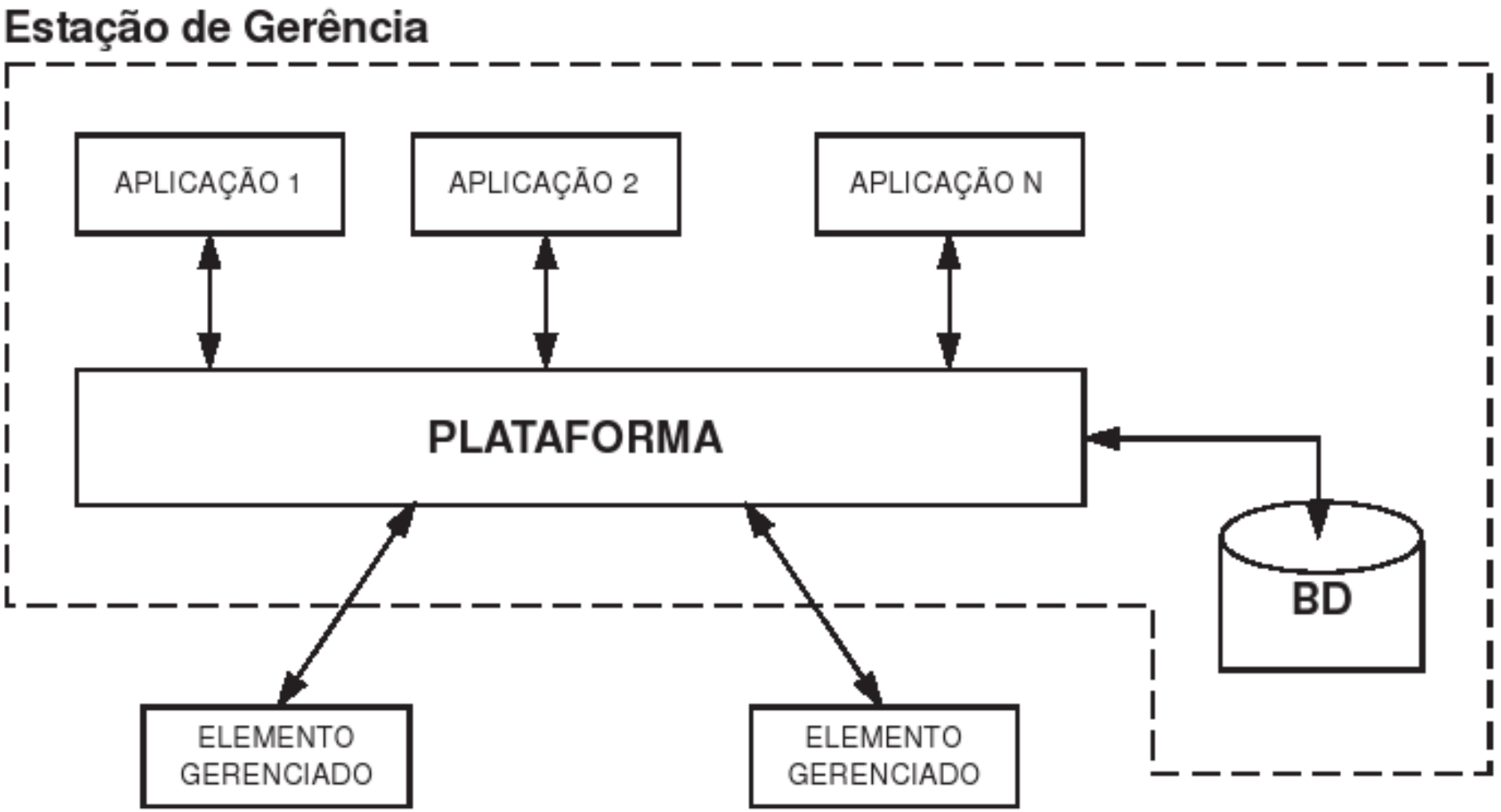
Aplicação de gerência - exemplos

- Netclarity da Lanquest (gerência de desempenho)
- Alarm Manager da Aprisma (gerência de falhas)
- AssetView da Hewlett Packard (gerência de bens)
- CiscoWorks da Cisco (gerência de configuração)
- Spectrum's Alarm Managers da Cabletron (gerência de falhas)
- trap exploder da Empire Technologies (manipulação de alarmes)
- Boks da Securix (gerência de segurança)
- NetBuilder da 3COM (gerência de configuração)

Como escolher um sistema de gerência de redes (SGR)

1. Fazer um levantamento dos dispositivos gerenciáveis
2. Definir as áreas funcionais prioritárias
3. Comparar as aplicações de gerência
4. Escolher a plataforma de gerência

Arquitetura



Sistemas de gerência baseados na Web

- permitem aos administradores da rede monitorá-la e controlá-la a partir de um navegador
- vantagens [3Com-WBM]
  - possibilidade de monitorar e controlar os elementos da rede usando qualquer navegador em qualquer nó da rede
  - interface gráfica da Web já é bem conhecida e as operações realizadas em um navegador também
  - usar a Web para distribuir as informações sobre a operação da rede tem se mostrado uma tarefa eficaz. Por exemplo, informações para os usuários sobre o estado da rede e atualizações que eles precisam realizar (evitaria ligações em demasia ao help desk)

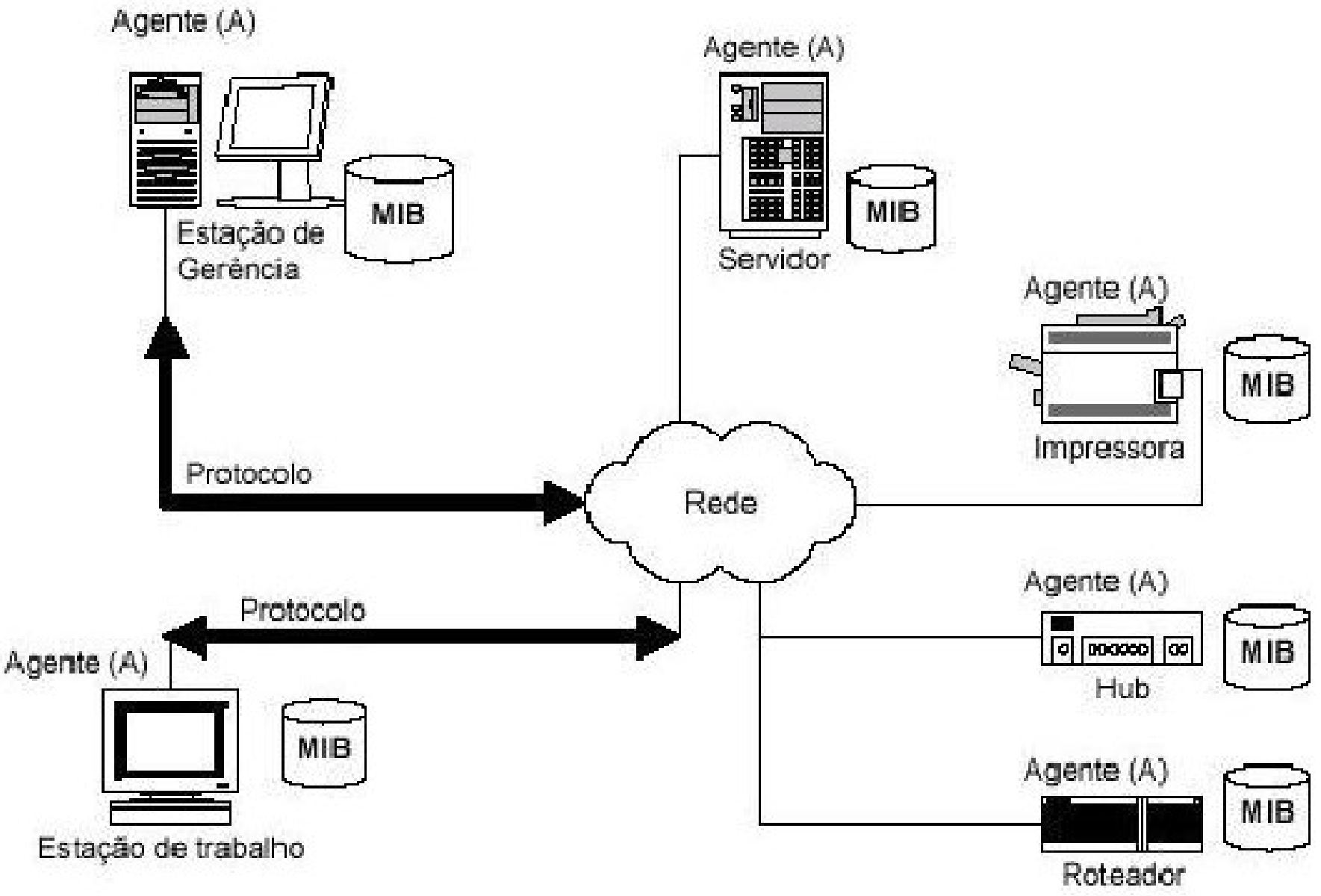
Sistemas de gerência baseados na Web

- padrão
  - WBEM (Web-Based Enterprise Management): objetivo principal é alcançar a gerência unificada de todos os sistemas e redes de uma organização
  - www.dmtf.org/standards/standard_wbem.php e http://wbemservices.sourceforge.net/

Sistema de Gerência de Redes - Arquitetura Geral

- modelo gerente/agente
- quatro componentes básicos: elementos gerenciados, estações de gerência, protocolos de gerência e informações de gerência

Sistema de Gerência de Redes - Arquitetura Geral



Elementos gerenciados

- constituem os componentes da rede que precisam operar adequadamente para que a rede ofereça os serviços para os quais foi projetada
- devem possuir um software especial (Agente) para permitir que sejam gerenciados remotamente
  - Agente: permitem a monitoração e o controle de um componente por uma ou mais estações de gerência, respondendo às solicitações dos indicadores solicitados
- exemplos
  - Hardware: equipamentos de interconexão, enlaces de comunicação, hospedeiros, nobreaks, modems, impressoras etc.
  - Software: sistemas operacionais, servidores de bancos de dados, servidores Web, servidores de mail etc.

Estação de Gerência

- contém o software (Gerente) que conversa diretamente com os agentes nos componentes gerenciados, com o objetivo de monitorá-los ou controlá-los
- gerente: comunicação com agentes através pollings ou trapings
  - Polling (varredura): processo de obtenção das informações junto ao agente em que o gerente toma a iniciativa comunicação
  - Trapings (notificações): processo onde o agente toma a iniciativa de enviar ao gerente (pré-configurado) uma notificação de ocorrência de eventos anormais, previamente configurados

Polling vs Trapping

- Qual utilizar?
- Depende:
  - tráfego gerado
  - robustez
  - retardo
  - volume de processamento no agente
  - volume de processamento no gerente
  - aplicações de monitoramento
  - conseqüência de uma falha no dispositivo monitorado
  - ...

Estação de Gerência

- normalmente centralizadas (freqüente que haja uma única estação de gerência)
- possuem funções automáticas de gerência (ex. poll regular dos agentes)
- pode obter e alterar informação de gerência presente nos agentes
- possuem interface com o usuário para facilitar a gerência

Protocolo de gerência

- define as mensagens usadas entre gerente e agentes para trocar informação de gerência
- permite operações de monitoramento (READ) e operações de controle (WRITE)
- tipos de mensagens
  - operação de leitura e escrita
  - resposta
  - notificação (traps)

Protocolo de gerência

- Exemplo de operação de monitoramento (gerente-roteador): Qual é a quantidade de erros ocorrendo no fluxo de entrada na interface número 17?
- Exemplo de uma operação de controle (gerente-roteador): Desligue sua interface número 17.
- Exemplos de protocolos
  - SNMP (Simple Network Management Protocol), SNMPv2 e SNMPv3
    - usado em redes TCP/IP
  - CMIP (Commom Management Information Protocol)
    - protocolo do modelo OSI
  - outros: WBEM (Web-Based Enterprise Management), TMN (Telecommunications Management Network), Transaction Language 1, JMX (Java Management Extensions) e netconf

Informações de gerência

- define os dados que podem ser referenciados em operações do protocolo na comunicação entre gerentes e agentes
- MIB (Management Information Base) - corresponde ao conjunto das informações de gerência disponíveis em um agente e define os dados que podem ser referenciados em operações do protocolo de gerência.
- exemplos: informação de erro de transmissão e recepção em enlaces de comunicação, status de um enlace de comunicação, temperatura de um roteador, tensão de entrada de um equipamento nobreak etc.

Classificação das Informações

- **Estática**: informações de configuração, que sofrem pouca ou nenhuma alteração
  - Exemplos: nome dos elementos, localização, endereçamento IP, rotas estáticas, etc...
- **Dinâmica**: relacionadas a eventos na rede, sofrendo alterações a cada instante
  - Exemplos: total bytes enviados/recebidos, total de erros, tabelas de rotas dinâmicas, etc...
- **Estatística**: derivada das informações dinâmicas envolvendo conceitos como média, utilização, variância, desvio, etc...
  - Exemplos: taxa de utilização de largura de banda, taxa de utilização de recursos (CPU, disco, memória), utilização média da rede, vazão (bps), etc.

Arquiteturas de gerência de redes

- Centralizada
- Hierárquica
- Distribuída

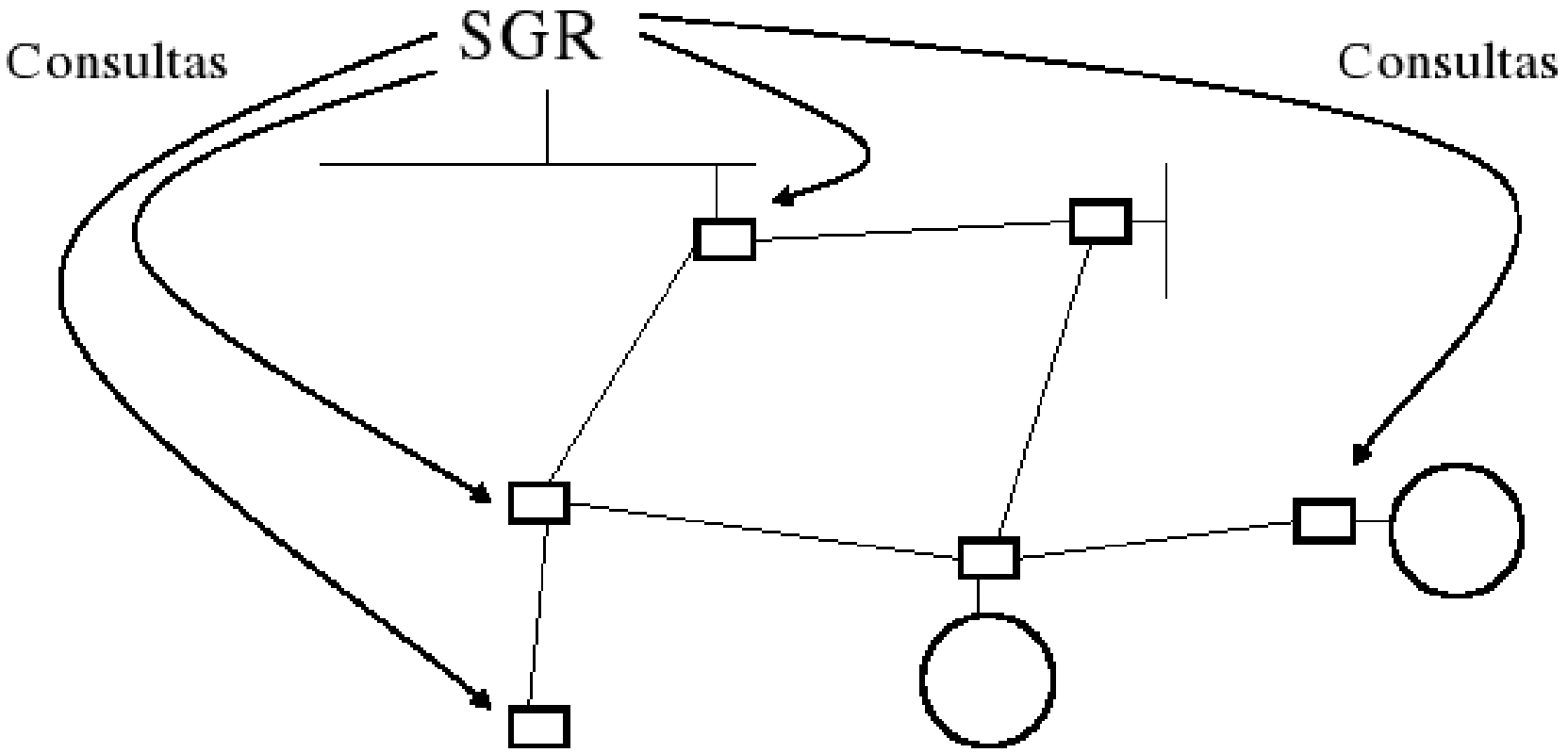
Arquitetura Centralizada

- existe apenas um único Gerente capaz de gerenciar todos os elementos do ambiente
- banco de dados único e centralizado
- único responsável por toda a geração de alertas, coleta e administração das informações de todos os elementos
- Vantagens:
  - simplificação do processo de gerência, uma vez que a informação necessária está concentrada em um único ponto, facilitando a localização de erros e a correlação dos mesmos
  - segurança no que diz respeito ao acesso às informações, pois há necessidade de se controlar apenas um único ponto de acesso
  - permite facilmente identificar problemas correlacionados

Arquitetura Centralizada

- Desvantagens:
  - maior concentração da probabilidade de falhas em um único elemento (o Gerente);
  - necessidade de duplicação total da base de dados para redundância do sistema
  - difícil expansão (baixa escalabilidade)
  - tráfego intenso de dados no gerente
- Exemplo: Netview

Arquitetura Centralizada



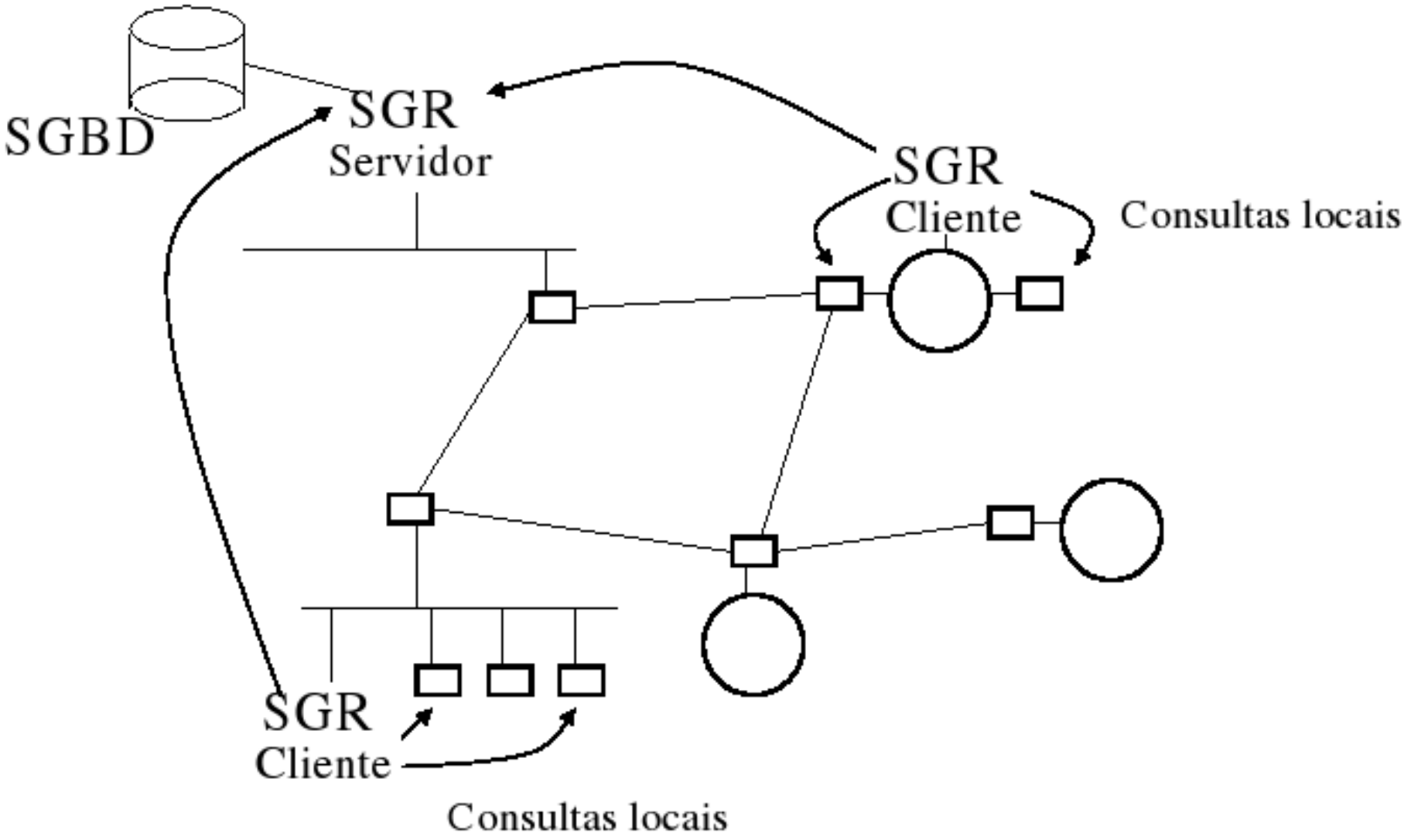
Arquitetura Hierárquica

- um servidor (SGR Servidor) que centraliza as informações dos dispositivos gerenciados no ambiente, porém existe um conjunto de outros servidores (SGR Clientes) que podem atuar como clientes deste servidor central
- divisão das tarefas de gerência entre servidor central e servidores clientes
- com menor capacidade indiviual dos servidores consegue-se realizar gerência de ambientes com grande quantidade de dispositivos
- dados armazenados de forma centralizada
- Vantagens
  - gerência não depende exclusivamente de um único sistema Gerente e há uma distribuição das tarefas de gerência
  - tráfego é balanceamento entre os Gerentes

Arquitetura Hierárquica

- Desvantagens
  - base de dados de gerência continua centralizada, mantendo-se o mesmo problema de concentração da alta probabilidade de falhas em um único ponto
  - definição da hierarquia deve ser cuidadosa para evitar duplicação.
  - recuperação das informações é mais lenta
- Exemplos: SunNet Manager, OpenView, Netview/AIX e At&T StarSentry

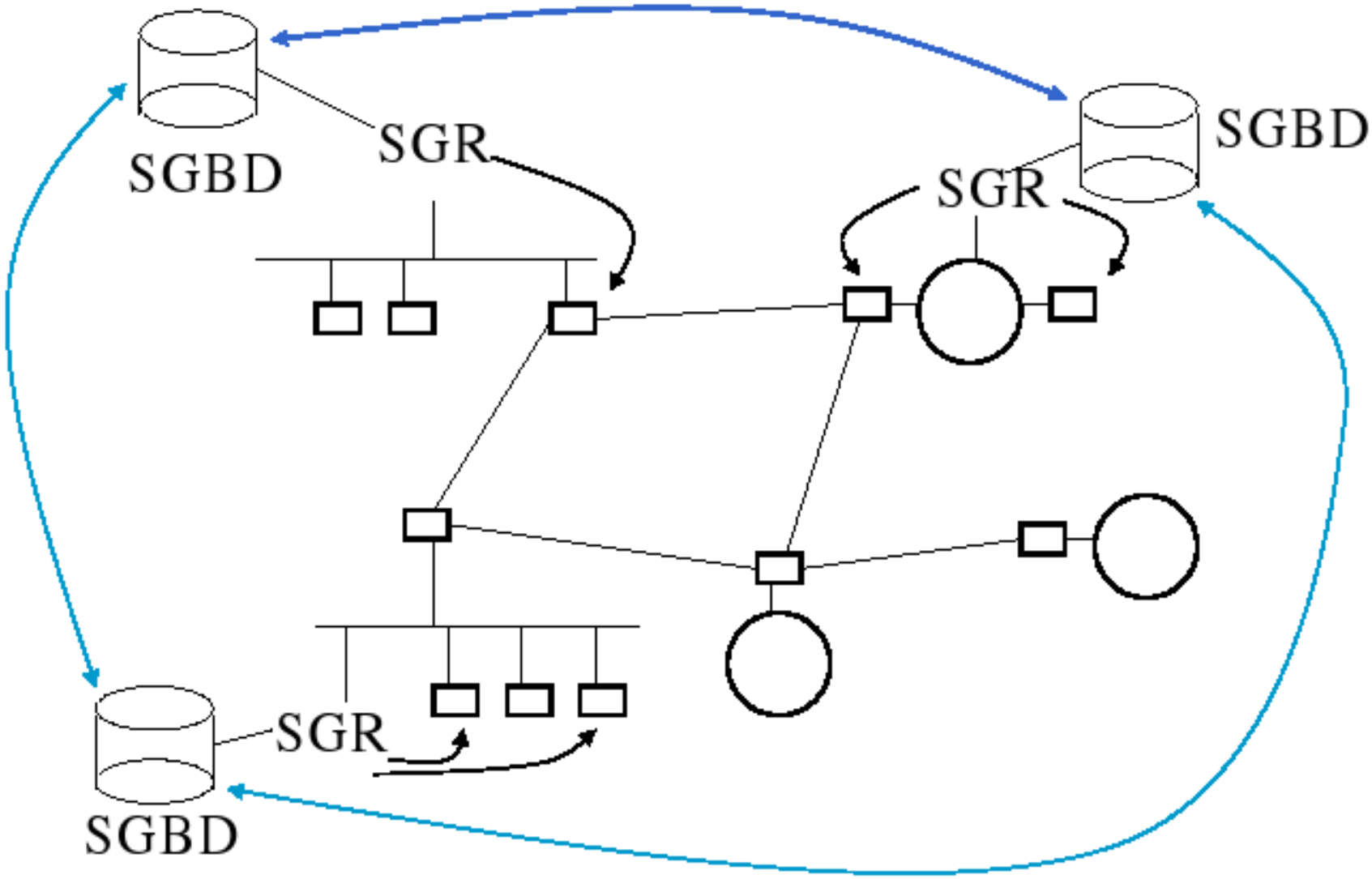
Arquitetura Hierárquica



Arquitetura Distribuída

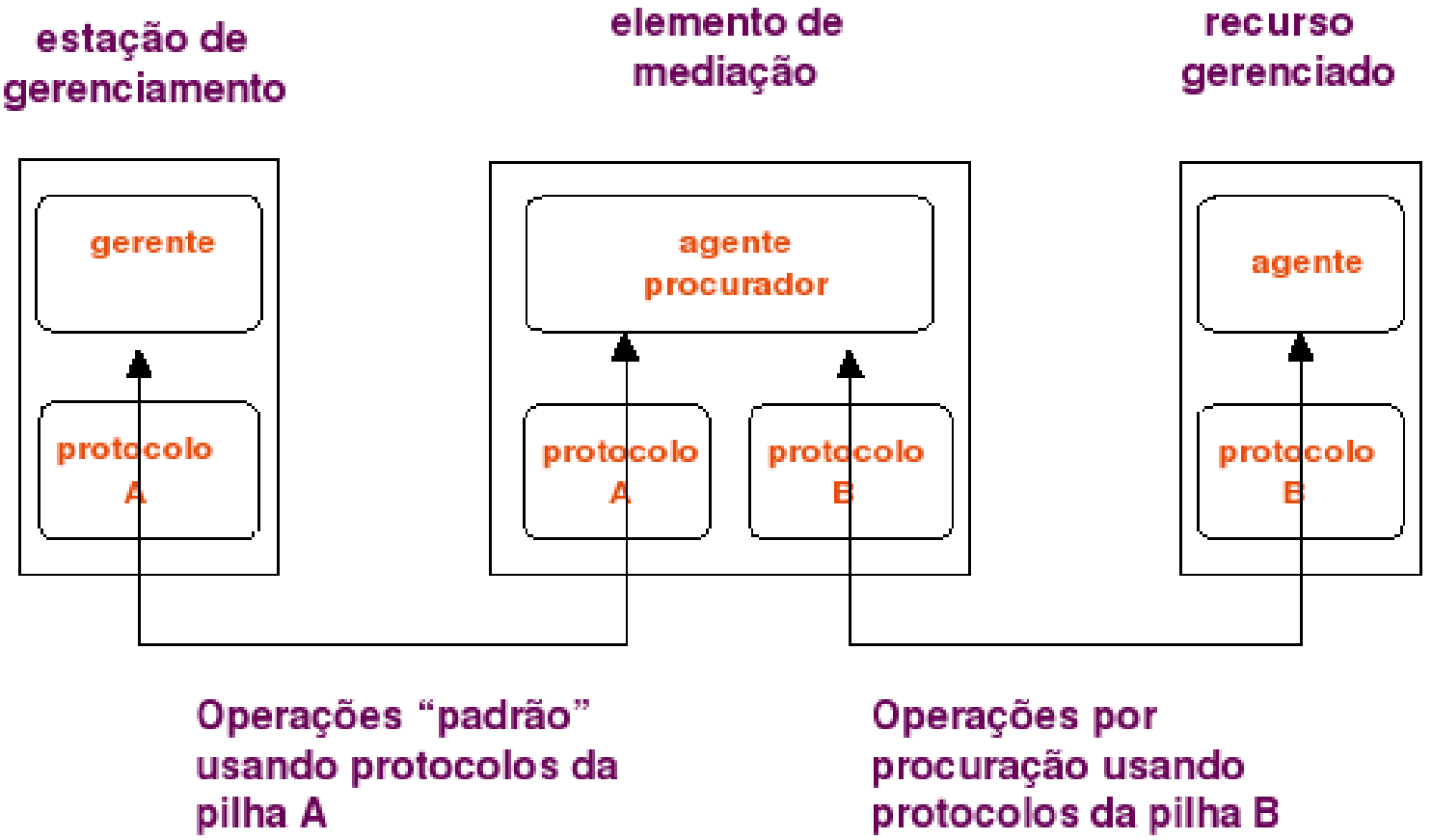
- combina características das arquiteturas centralizada e hierárquica, porém, ao invés de possuir um único servidor ou um conjunto formado por clientes/servidor de gerência, o modelo distribuído utiliza-se de vários servidores num modelo ponto-a-ponto, em que não há hierarquia entre eles e nem centralização da base de dados
- cada servidor é responsável individualmente por uma parte (ou segmento) da rede gerenciada, possuindo, em sua própria base de dados, informações de todo o ambiente, o que lhe permite analisá-lo de forma completa
- distribuição das tarefas de gerência e da base de dados para cada servidor na arquitetura, distribuindo assim também a probabilidade de falhas entre os diversos servidores e evitando a dependência de um único sistema.
- combina as vantagens das duas outras arquiteturas
- esquema de replicação das base de dados (coerência).

Arquitetura Distribuída



Uso de proxies

- intermedia a comunicação entre gerente e agente quando os equipamentos não falam os mesmos protocolos que o gerente;
- o proxy (agente procurador) executa num elemento de mediação, que fala com o gerente usando um protocolo e com o agente usando outro

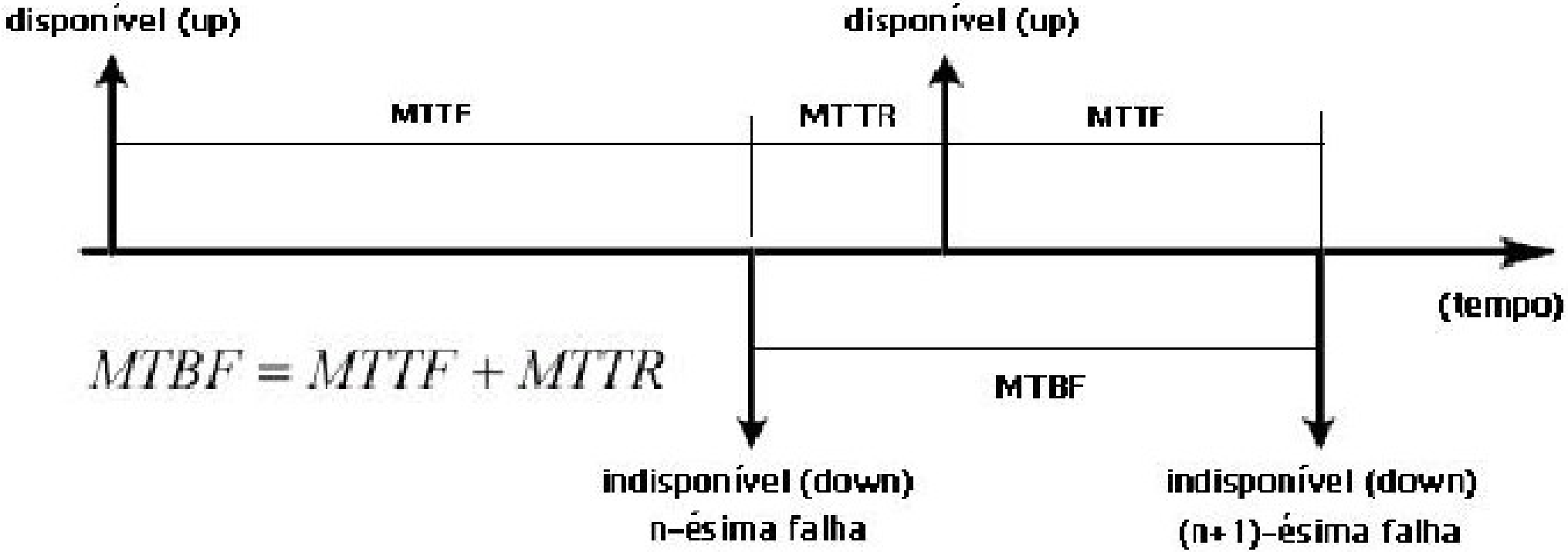


Métricas

Disponibilidade

- indica o tempo que um serviço de rede, componente ou aplicação esteve disponível para seus usuários em relação ao tempo monitorado
  - A média de tempo entre a ocorrência sucessiva de falhas é conhecida como MTTF (Mean Time To Failure).
  - A média do tempo que esse sistema leva para recuperar-se de uma falha é conhecida como MTTR (Mean Time To Repair).
  - A média do tempo entre a ocorrência de 2 (duas) falhas consecutivas é denominada MTBF (Mean Time Between Failure).

Disponibilidade



$$MTBF = MTTF + MTTR$$

$$P_{up} = Disponibilidade = \frac{MTTF}{MTTF + MTTR}$$

$$P_{down} = Indisponibilidade = \frac{MTTR}{MTTF + MTTR} = \frac{MTTR}{MTBF}$$

Disponibilidade

$$Disponibilidade(\%) = \frac{(PeríodoTotalMonitoramento - TempoIndisponível)}{PeríodoTotalMonitoramento} * 100\%$$

Classe de Disponibilidade	Disponibilidade	Indisponibilidade (min/ano)	Tipo de Sistema
1	90,0%	52.560	Não-gerenciado
2	99,0%	5.256	Gerenciado
3	99,9%	526	Bem-gerenciado
4	99,99%	52,6	Tolerante-à-Falhas
5	99,999%	5,3	Alta Disponibilidade
6	99,9999%	0,53	Muito Alta Disponibilidade
7	99,99999%	0,053	Ultra Disponibilidade

Disponibilidade

- sistemas em série (--S1--S2--)
  - disponibilidade de S1 = 0,98
  - disponibilidade de S2 = 0,98
  - disponibilidade do sistema = 0,98 * 0,98 = 0,96
- sistemas em paralelo

```
     /---C1---\
(---|         |---)
     \---C2---/
```

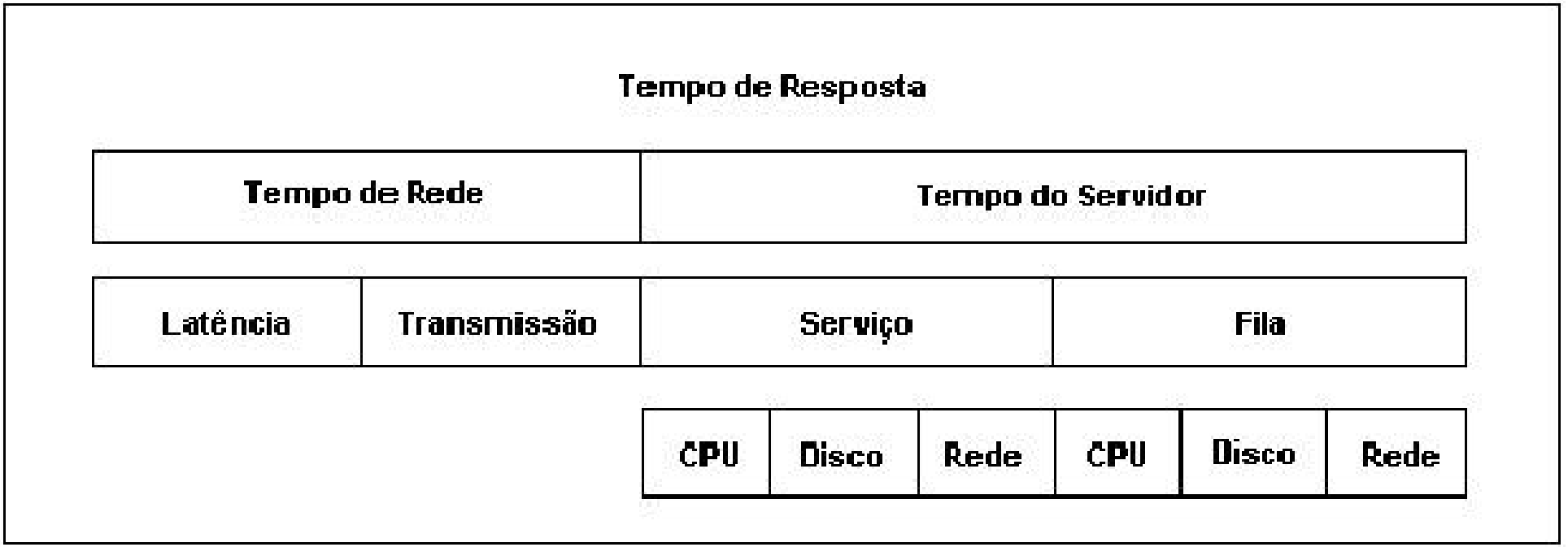
  - disponibilidade de S1 = 0,98
  - disponibilidade de S2 = 0,98
  - disponibilidade do sistema = 1 – (dois sistemas fora) = 1 – ((1-0,98)*(1-0,98)) = 1 – (0,02*0,02) = 1-0,0004= 0,9996

Tempo de Resposta

- representa o tempo decorrido entre a requisição de uma ação ao sistema e a resposta completa à sua requisição
- medição é complexa
- além de apresentar uma enorme possibilidade de situações com definições e formas de monitoramento distintas, o mesmo é composto pela interação de diversos componentes: a quantidade de usuários acessando o serviço, a complexidade das operações solicitadas, a quantidade e a capacidade dos recursos compartilhados utilizados para a realização destas operações.

Tempo de Resposta

- Tempo de Resposta em Aplicações Cliente-Servidor:



Taxa de Erros

- relaciona a quantidade de pacotes, recebidos ou enviados por uma interface de rede, cujo conteúdo (em bits) apresenta erro em relação ao total de pacotes nessa mesma interface.
- normalmente, essa taxa é medida em valores percentuais dentro do período de monitoramento.
- é de difícil detecção e pode ser a causadora de muitos problemas que serão detectados posteriormente.

Latência

- representa o tempo que um pacote leva para ir de um ponto a outro da rede
- normalmente medido em milisegundos
- quanto menor a latência, melhor o tempo de resposta da rede

Vazão (Throughput)

- medida vinculada a uma aplicação
- exemplos: número de transações em um período, número de sessões de clientes para uma dada aplicação em um determinado período

Utilização

- representa a quantidade em uso de um determinado recurso (porcentagem), em relação à sua capacidade total de atendimento
- auxilia na avaliação e detecção de gargalos, uma vez que influenciam diretamente no tempo de resposta da rede e das aplicações envolvidas
- monitorando-se a utilização, ao longo de um determinado período de tempo, é possível observar os intervalos de pico na utilização de um serviço ou recurso
- Exemplos: memória disponível, leitura/escrita em disco, processador (CPU), largura de banda da rede.

Gerência de níveis de serviço

- SLA (Service Level Agreement) - contrato entre um Provedor de Serviços e seus usuários, que obriga o Provedor a manter um certo nível de qualidade do serviço fornecido em que pode ocorrer, inclusive, o oferecimento de compensações, caso os níveis acordados não sejam atingidos

Gerência de níveis de serviço

- SLM (Service Level Management) - tipo de gerenciamento em que as atividades das áreas funcionais de gerenciamento de Desempenho e Falhas visam executar e acompanhar o nível de serviço garantido através dos SLAs.
- funcionamento
  - obtenção de dados dos dispositivos gerenciáveis;
  - manipulação destes dados para transformá-los em indicadores de falha e desempenho;
  - armazenamento destes indicadores para formar uma baseline;
  - geração de relatórios periódicos sobre o comportamento destes indicadores.