Redes de Computadores

Prof. Ms. Wesley Viana

- Unidade de Ensino: 04
- Competência da Unidade: Redes de Computadores
- Resumo: Introdução a Redes de Computadores
- Palavras-chave: Redes de Computadores; Protocolos; Teleprocessamento; Aplicações; Modelo OSI.
- Título da Teleaula: Gerência de redes e padrões;
- Teleaula nº: 04

Contextualização

- Teoria da gerência de redes e padrões;
- Gerência de falhas e segurança;
- Gerência de desempenho, configuração e contabilização.

Teoria da gerência de redes e padrões

Teoria da gerência de redes e padrões

Segundo Kurose (2006), o gerenciamento em redes pode ser definido como algumas ações de coordenação dos dispositivos físicos (computadores, servidores, nodos, etc.) e lógicos protocolos, endereços e serviços), visando garantir a confiabilidade dos seus serviços, um desempenho aceitável e a segurança das informações.

Teoria da gerência de redes e padrões

A gerência de rede pode ser feita de duas formas básicas:

1. Sistema único de gerência: são um conjunto de ferramentas de monitoramento e/ou controle de dispositivos e/ou serviços, integrados em uma única aplicação.

2. Diversos sistemas de gerência: são ferramentas de monitoramento ou controle de dispositivos ou serviços. Normalmente as ferramentas possuem funções específicas, auxiliando os administradores de redes no monitoramento de diversos serviços

Teoria da gerência de redes e padrões

Para que o gerenciamento possa ter elementos para garantir o seu correto funcionamento, Kurose (2006) aponta três princípios:

Coleta de dados: define-se como a parte do processo responsável por coletar automaticamente dados parametrizados pelo administrador de redes.

Análise e diagnóstico: consiste em organizar os dados coletados a fim de gerar informações que permitam a tomada de decisão.

Controle: após o diagnóstico correto do problema, devese tomar ações a fim de cessar, mitigar ou minimizar os impactos.

Teoria da gerência de redes e padrões

Segundo Kurose (2006), a ISO (Internacional Organization for Standardization) desenvolveu um modelo de gerenciamento de redes, divididos em cinco áreas. São elas:

Gerenciamento de desempenho: o objetivo é quantificar, medir, informar, analisar e controlar o desempenho de dispositivos, serviços e segurança. (SNMP)

Gerenciamento de falhas: visa registrar, detectar e reagir às falhas ocorridas nas redes.

Gerenciamento de configuração: permite que o administrador saiba quais são os dispositivos utilizados na rede e as suas respectivas configurações.

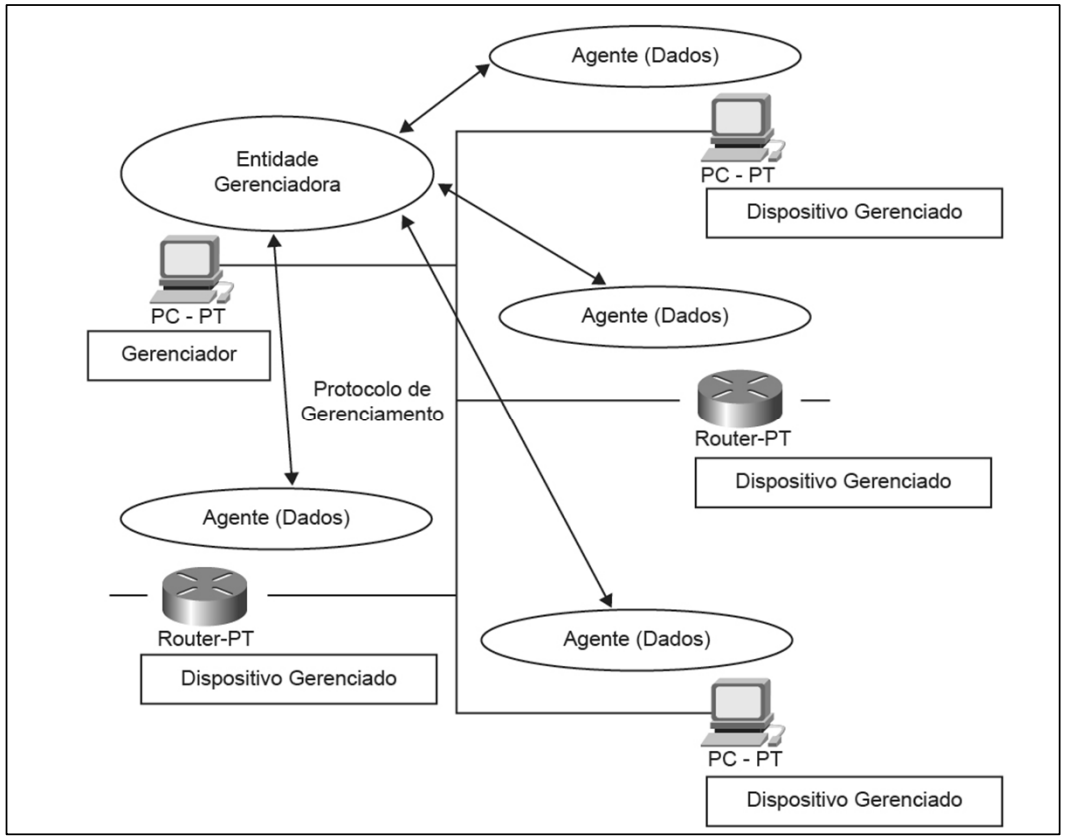
Teoria da gerência de redes e padrões

Gerenciamento de contabilização: permite a especificação, o registro e controle de acesso (para usuários e dispositivos).

Gerenciamento de segurança: é efetuar o controle de acesso aos recursos via mecanismos de segurança (chaves), métodos de mascaramento de mensagens (criptografia) e políticas de prevenção e segurança.

Teoria da gerência de redes e padrões

Para Kurose (2006), a estrutura do gerenciamento de redes deve possuir os elementos.



Teoria da gerência de redes e padrões

Para Kurose (2006), a estrutura do gerenciamento de redes deve possuir os elementos.

Essa estrutura tem os seguintes componentes:

Entidade gerenciadora: é o meio pelo qual o administrador de redes interage com a interface de gerenciamento, podendo realizar as atividades de coleta de dados, processamento, análise para posterior tomada de decisão.

Dispositivo gerenciado: é um dispositivo situado em uma rede gerenciada, o qual pode ser monitorado, ex.: servidores, sensores, switches, etc.

Teoria da gerência de redes e padrões

Protocolo de gerenciamento de rede: é executado entre a entidade gerenciadora e os dispositivos gerenciados, permitindo que os agentes possam informar a entidade gerenciadora sobre a ocorrência de falhas ou violação de

algum parâmetro.

Em cada dispositivo, existe um agente de gerenciamento de rede (software de gerenciamento de rede propriamente dito) que executa testes e envia os resultados para a estação central de gerência de rede.

Teoria da gerência de redes e padrões

Comunicações entre os dispositivos gerenciados e a entidade gerenciadora só ocorre porque o protocolo de gerenciamento de rede permite que aconteçam as investigações.

A arquitetura de gerenciamento de redes fornece genericamente parâmetros para obter um gerenciador aplicável na maioria das redes, porém não oferece elementos que visam garantir a padronização.

Teoria da gerência de redes e padrões

SNMP (Simple Network Information Protocol)

O protocolo SNMP (Simple Network Information Protocol – Protocolo Simples de Gerenciamento de Rede) é definido pela RFC 3410. É um protocolo empregado para efetuar o monitoramento dos dispositivos de redes e os serviços.

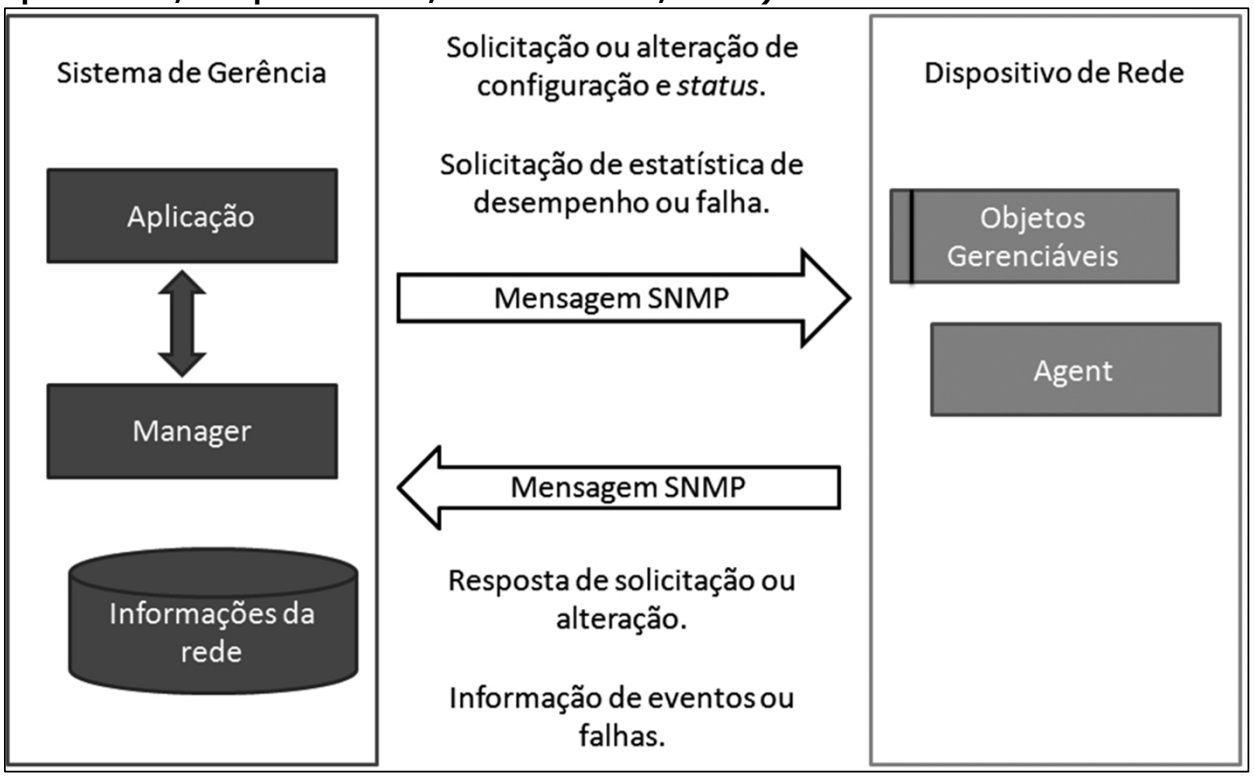
Para que ele possa atuar na rede, necessita de quatro componentes básicos:

- Os nodos gerenciados (agentes).
- As estações de gerenciamento (gerente).
- As informações de gerenciamento (MIB*). (Armazenamento de informações de configuração e status)
- O protocolo de gerenciamento (SNMP).

Teoria da gerência de redes e padrões

Processos envolvidos no SNMP

O SNMP é instalado nos dispositivos gerenciáveis da rede (computador, impressora, câmera IP, etc.)



Teoria da gerência de redes e padrões

CMISE (Commom Management Information Service Element)

O protocolo CMISE é formado por dois outros protocolos: CMIS e CMIP.

CMIS (Common Management Information Service): basicamente define como os serviços serão oferecidos às aplicações de gerenciamento (agente e gerente). Definido em três categorias.

Serviços de associação: (informar os eventos)

Serviços de notificação: (informar eventos)

Serviços de operação: (altere as variáveis do MIB)

- Escopo: parâmetros para alvo do gerenciamento;
- Filtragem: escopo;
- Sincronismo: regras do gerente.

Teoria da gerência de redes e padrões

CMIP (Common Management Information Protocol): é um protocolo de gerenciamento que segue o modelo de referência OSI. Utiliza a mesma estrutura SNMP, também execução de algumas ações utilizando escopo (filtro) para selecionar objetos.

Vantagem: segurança;

Desvantagem: utiliza grande capacidade de sistemas.

Os tipos de mensagens recebidas/enviadas levam em consideração o CMIS.

Teoria da gerência de redes e padrões

TMN (Telecommunications Management Network):

Três arquiteturas, que podem ser implementadas juntas ou separadas.

Arquitetura informacional: assim como o CMIS, as informações são trocadas entre agente e gerente por meio de um protocolo de gerência de rede.

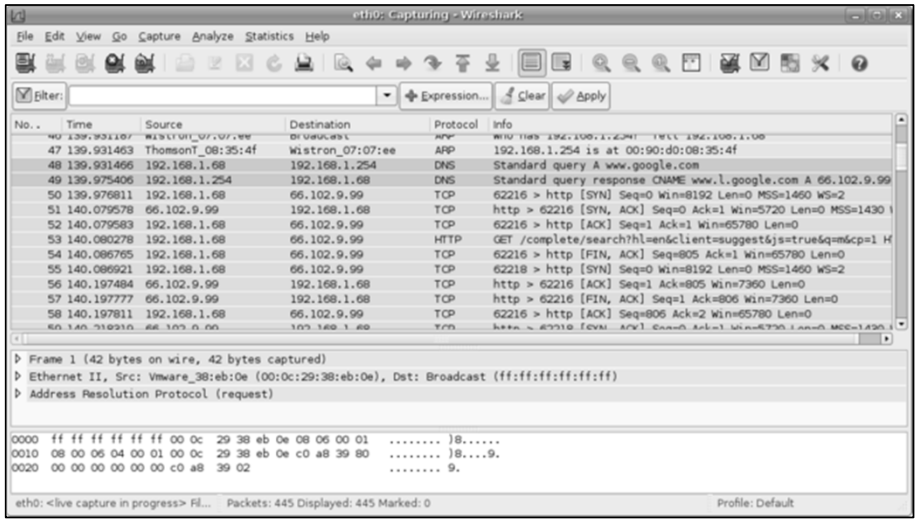
Arquitetura funcional: definir quais serão as funções e os objetivos na gerência de rede.

Arquitetura física: interfaces que garantem a compatibilidade dos dispositivos.

Teoria da gerência de redes e padrões

Sniffig:

Ferramenta que efetua a interceptação e o registro dos dados. Utilizado para checar se uma rede está trabalhando dentro dos parâmetros definidos. Visa capturar os fluxos especificados em sua configuração, podendo ser: e-mail, logins, textos, histórico de internet, entre outros.



Gerência de falhas e segurança

Gerência de falhas e segurança

Segundo Comer (2007), qualquer sistema de comunicação de dados é suscetível a falhas e erros. Pode ocorrer em dispositivos físicos ou em transmissão. Mesmo quando são feitos exaustivos testes de erros ou de stress de rede, tais ocorrências ainda podem aparecer nas estruturas das redes de computadores. Os erros de transmissão são divididos em três categorias:

Interferência:

Distorção:

Atenuação:

Em redes com uma grande infraestrutura e/ou com diversos serviços é prudente fazer teste de stress.

Gerência de falhas e segurança

Segundo Carissimi (2009), em 1984 o cientista americano Claude Shannon publicou as bases matemáticas para determinar a capacidade máxima de transmissão por um canal físico com uma banda passante, em uma determinada relação sinal/ruído

Os erros ocorridos na comunicação de dados não podem ser eliminados por completo, porém aqueles relacionados à transmissão podem ser facilmente detectados, permitindo assim que sejam corrigidos automaticamente.

Gerência de falhas e segurança

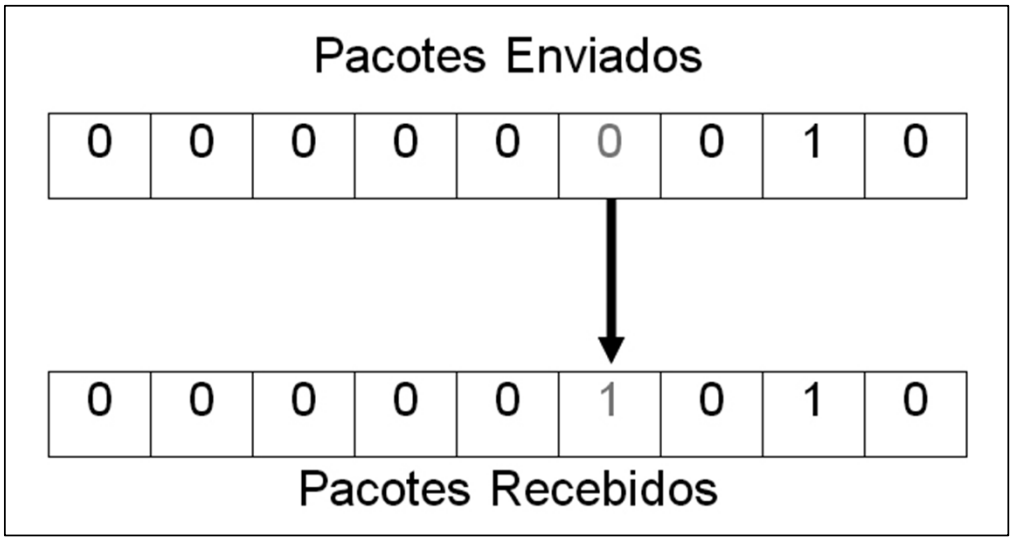
Erros de transmissão podem afetar os dados de três formas:

TIPO DE ERRO	DESCRIÇÃO
Erro em um único bit	Apenas um bit sofre uma alteração e os demais permanecem preservados. A degradação do serviço ocorre por um período bem curto.
Erro em rajada	Vários bits sofrem alterações. A degradação do serviço ocorre por um longo período.
Indefinido	A transmissão que chega ao receptor é ambígua (valores fora do escopo). Podem ocorrer diversos períodos de degradação do serviço.

Gerência de falhas e segurança

Erro em único bit

Erro ocorre em um único dos bits enviados:

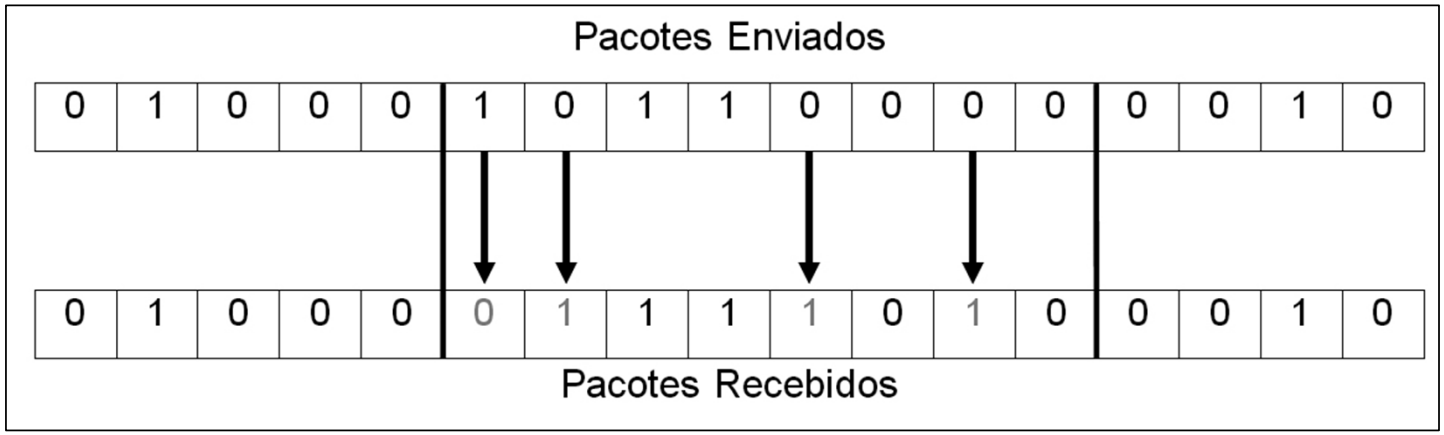


O erro de um único bit (single-bit-error) causa uma degradação com menor duração. (streaming e sties)

Gerência de falhas e segurança

Erros em rajada

Erros ocorrem em rajadas:



Os erros em rajada têm um tempo de duração maior em relação ao erro em único bit. Normalmente a degradação do serviço pode ser sensível nas transmissões. (Jogos)

Gerência de falhas e segurança

Erros são detectados, é necessário efetuar a correção deles. São possíveis dois métodos de correção de erros:

Correção antecipada de erros (FEC – Forward Error Correction): são utilizados bits redundantes (por métodos de codificação), possibilitando que o receptor "adivinhe" os bits.

Correção de erros por retransmissão: quando o receptor encontra um erro, solicita ao emissor para realizar o reenvio da mensagem, processo esse que se repete até que esteja livre de erro.

Gerência de falhas e segurança

Esse tipo de ocorrência está muito presente na vida das pessoas: quando não se consegue efetuar um saque no caixa eletrônico; quando a cancela da praça de pedágio não levanta na cobrança automática (Sem Parar, Conect Car, etc.).

Tanenbaum (1997) define que as falhas em sistemas computacionais são respostas incorretas em relação ao que foi projetado como saída, podendo ser definidas por alguns especialistas como defeito. Essas falhas podem ser geradas por fator humano, meios de transmissão, hardware, lógico (software), entre outros.

Gerência de falhas e segurança

Para prever as falhas são utilizadas as técnicas:

Tempo Médio Entre Falhas (MTBF – Mean Time Between Failures): Tempo médio entre as falhas, prevê as manutenções necessárias. Segue o cálculo:

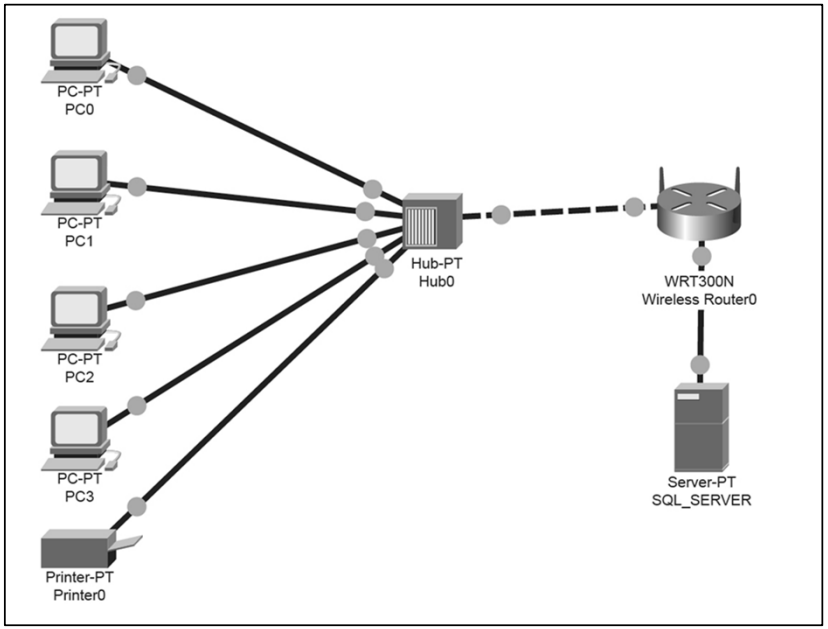
$$MTBF = \frac{\sum(Final - Início)}{Número\ de\ falhas}$$

Tempo Médio para Reparos (MTTR – Mean Time To Repair): Tempo médio para efetuar reparo após a ocorrência de falha.

$$MTTR = \frac{Tempo\ parado\ por\ falha}{Número\ de\ falhas}$$

Gerência de falhas e segurança

Exemplo: O servidor disponível na topologia apresentada disponibiliza acesso das 08h às 17h (9 horas). O servidor ficou indisponível quatro vezes, somando o total de uma hora de parada. Qual é o tempo encontrado entre as falhas? Qual é o tempo necessário para efetuar os reparos?



Gerência de falhas e segurança

Para o cálculo do tempo médio entre as falhas, temos que:

$$MTBF = \frac{(9-1)}{4} \rightarrow MTBF = 2\ horas$$

Com isso, é possível determinar o tempo de manutenção de cada uma das paradas:

$$MTTR = \frac{60}{4} \rightarrow MTTR = 15\,\text{min}$$

Gerência de falhas e segurança

Dessa forma é possível prever, por meio dos cálculos efetuados com os dados históricos/estatísticos, que a cada duas horas o servidor apresentará uma falha e que serão necessários quinze minutos para efetuar a sua manutenção.

Criptografia

Segundo Tanenbaum (1997), quatro grupos contribuíram para o surgimento e o aprimoramento dos métodos de criptografia: os militares, os diplomatas, as pessoas “comuns” que gostam de guardar memórias e os amantes. Basicamente, o processo consiste em transformar uma mensagem de texto com uma chave parametrizada, cuja saída é um texto cifrado, com o uso de um algoritmo criptográfico.

Gerência de falhas e segurança

Criptoanálise: arte de solucionar (“desvendar”) as mensagens cifradas.

Criptografia: arte de criar mensagens cifradas.

Criptologia: estudos acerca de criptoanálise e os métodos de criptografia.

Tanenbaum (1997) sugere um modelo matemático para representar o processo de criptografia, em que:

Gerência de falhas e segurança

$C = E_k (P)$ onde:

P → denota o texto simples.

k → chave para criptografia.

C → texto cifrado.

Para o processo inverso (descriptografia), temos que:

$P = D_k (C)$

Essas notações sugerem que as letras "E" e "D" são funções matemáticas. Dessa forma, tanto na função de criptografia, quanto na de descriptografia há uma chave aplicada a uma função matemática.

Gerência de falhas e segurança

Chave

Segundo Tanenbaum (1997), para a compreensão do conceito de chave no tocante de criptografia é necessário o entendimento do princípio de Kerckhoff. Esse nome é em homenagem ao militar Auguste Kerckhoff que em 1883, publicou que: "Todos os algoritmos devem ser públicos; apenas as chaves são secretas." Dessa forma, podemos compreender que o algoritmo não necessita ser secreto ou sigiloso.

Tamanho da Chave	Aplicação
64 bits	Correio eletrônico, mensagens de chat, entre outros meios de comunicação instantânea que não exijam nível específico de segurança.
128 bits	Uso comercial, empresas, universidades, etc.
256 bits	Comunicação de interesse governamental.

Gerência de falhas e segurança

Em todos os tamanhos das chaves, espera-se que a garantia do sigilo das informações em sistemas computacionais se dê na presença de um algoritmo forte, porém público, e uma chave de longo comprimento.

Logs

Segundo Tanenbaum (1997), são ferramentas importantes para os administradores de redes, pois são recursos de fácil implementação que podem fornecer um histórico para análise. Práticas de monitoramento

- A inspeção dos logs deve ser uma rotina de trabalho;
- Devem-se investigar as causas dos logs;
- Devem-se estabelecer padrões de funcionamento.

Gerência de falhas e segurança

Controle de acesso

Segundo Tanenbaum (1997), também conhecida como NAC (Network Access Control), é um recurso muito importante para auxiliar no gerenciamento das questões relacionadas à segurança.

- Controle de acesso à rede;
- Evitar intrusões fraudulentas;
- Detectar dispositivos vulneráveis.

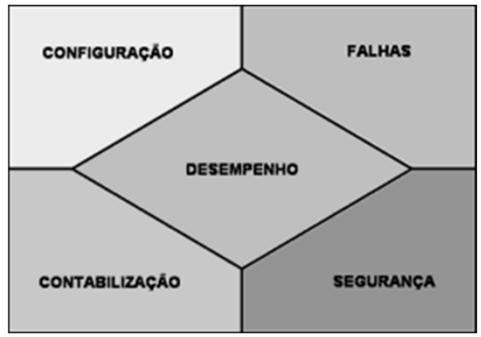
Tais técnicas permitem que os dispositivos e usuários que necessitem conectar-se à rede sejam identificados e, se possuírem credenciais, sejam autorizados a fazê-lo, sendo, portanto, possível verificar o status e a atualização de antivírus, as aplicações, os softwares, etc.

Gerência de desempenho, configuração e contabilização

Gerência de desempenho, configuração e contabilização

Nível de utilização

Segundo Tanenbaum (1997), em diversas situações os engenheiros de redes necessitam avaliar desde a estrutura da rede até os dispositivos individualmente, para então realizar testes probatórios de qualidade. Testes de desempenho são feitos injeção de um determinado tráfego na rede, podem ser observados:



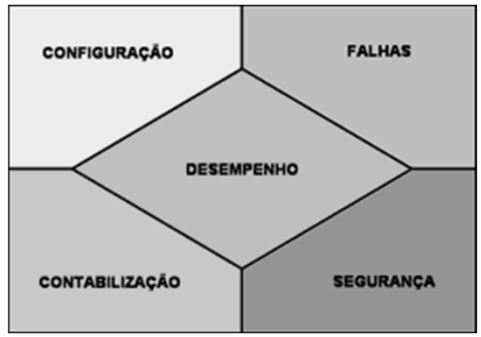
- Taxa máxima suportada;
- Tempo de deslocamento de um pacote;
- Tempo de recuperação a falhas.

Um software muito utilizado por administradores de redes para analisar vazão, latência, jitter e perda de pacotes é o Iperf (Jperf em Linux).

Gerência de desempenho, configuração e contabilização

Perfil de tráfego

Tenambaum (1997) define que as redes devem ser reconfiguráveis graças ao fato de os perfis de tráfego mudarem com muita frequência.

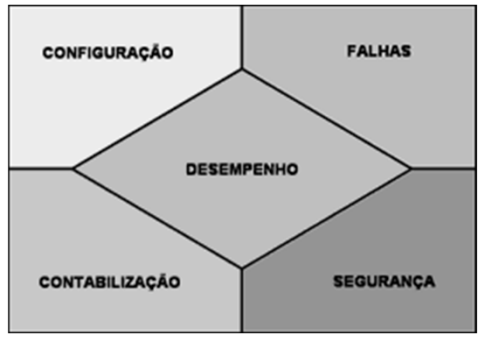


- Novos serviços.
- Crescimento do tráfego.
- Novas tecnologias.
- Padronização e interoperabilidade entre os protocolos e equipamentos.

Gerência de desempenho, configuração e contabilização

Vazão (Throughput)

Segundo Forouzan (2006), a vazão em redes de computadores pode ser definida como a quantidade de dados transferidos entre dispositivos (da mesma rede, ou de redes diferentes), ou mesmo a quantidade de dados processados em determinado tempo.



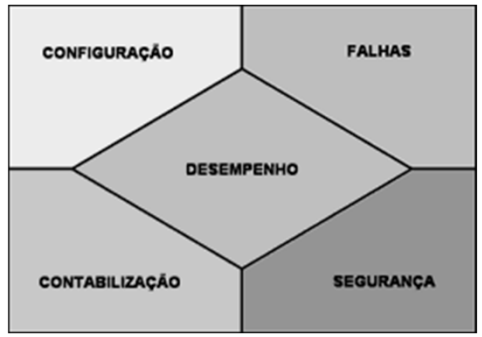
Os fatores que interferem na vazão são:

- Topologia de rede.
- Número de usuários.
- Taxa das interfaces de rede.

Gerência de desempenho, configuração e contabilização

Perda de pacotes

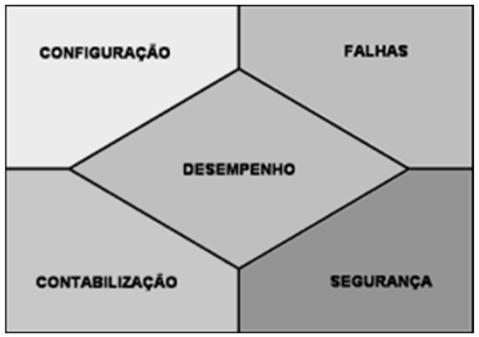
Segundo Tanenbaum (1997), em razão de os roteadores não terem a capacidade de armazenamento de pacotes infinita, após o esgotamento, os pacotes são descartados. Teste com base no qual é possível observar as perdas de pacotes ocorridas em uma rede.




```
C:\Users\Prof. Serginho Nunes>ping 192.168.0.1

Disparando 192.168.0.1 com 32 bytes de dados:
Esgotado o tempo limite do pedido.
Esgotado o tempo limite do pedido.
Resposta de 192.168.0.1: bytes=32 tempo=160ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=1948ms TTL=64

Estatísticas do Ping para 192.168.0.1:
    Pacotes: Enviados = 4, Recebidos = 2, Perdidos = 2 (50% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 160ms, Máximo = 1948ms, Média = 1054ms
```

Gerência de desempenho, configuração e contabilização

```
C:\Users\Prof. Serginho Nunes>ping 192.168.0.1

Disparando 192.168.0.1 com 32 bytes de dados:
Resposta de 192.168.0.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=6ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=4ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=5ms TTL=64

Estatísticas do Ping para 192.168.0.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 1ms, Máximo = 6ms, Média = 4ms
```



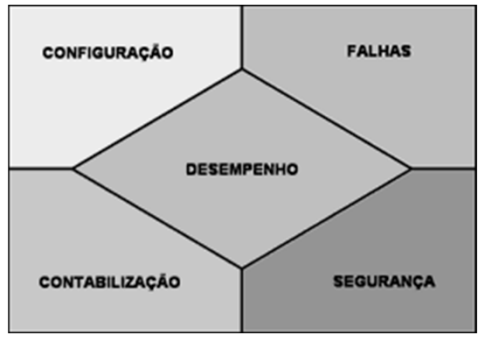
Latência (atraso)

Segundo Carissimi (2009), em redes de computadores, latência é o intervalo de tempo entre o momento que o emissor enviou o pacote e o recebimento da confirmação do pacote por parte do receptor.

Gerência de desempenho, configuração e contabilização

A latência pode ser considerada:

Latência = Tempo de transmissão + Tempo de propagação



Em que:

Tempo de transmissão = Dimensão do pacote (bits) / Velocidade da Transmissão (bps).

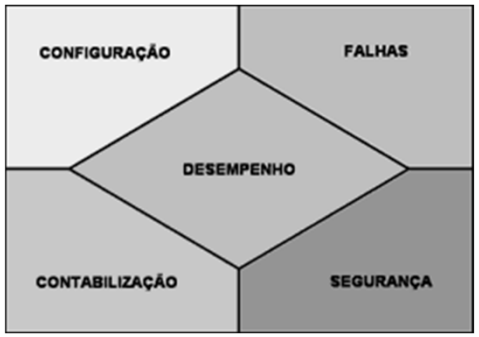
Tempo de propagação = Dimensão do Canal (Km) / Velocidade de Propagação (Km/s).

Segundo Kurose (2006), há dois outros tipos de atrasos que podem provocar latência: o tempo de processamento e o tempo de enfileiramento (gargalos).

Gerência de desempenho, configuração e contabilização

Temos um parâmetro de saída do teste com valores para "mínimo", "máximo" e "média".

Valores	Experimento 1	Experimento 2
Mínimo	160 ms	1 ms
Máximo	1948 ms	6 ms
Média	1054 ms	4 ms



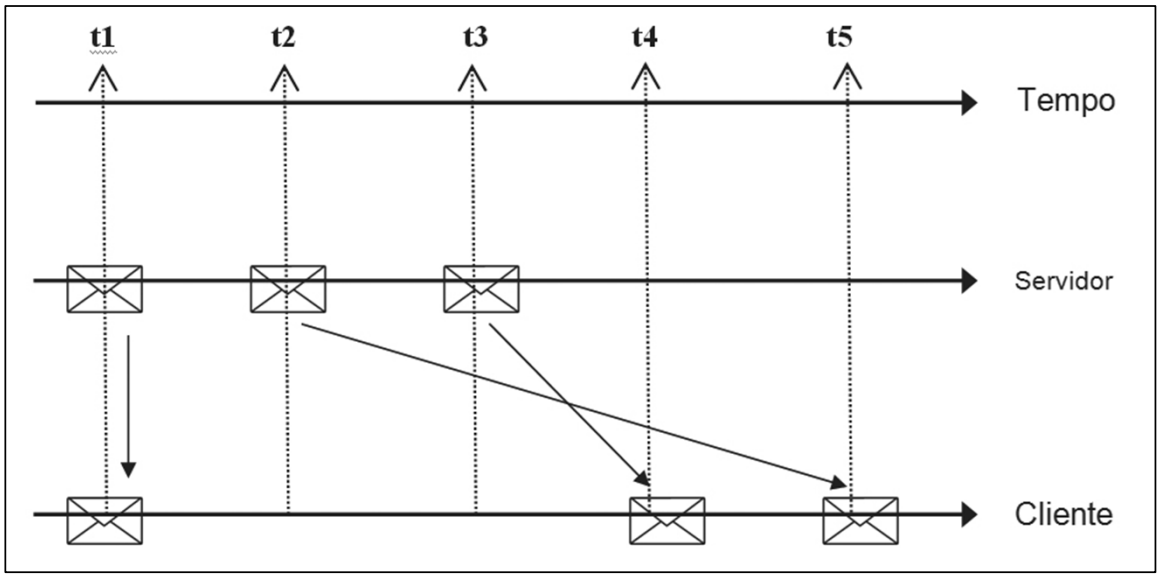
O aumento da latência (atraso) e a perda de pacotes nas transmissões sofrem interferências devido, entre outros fatores, à:

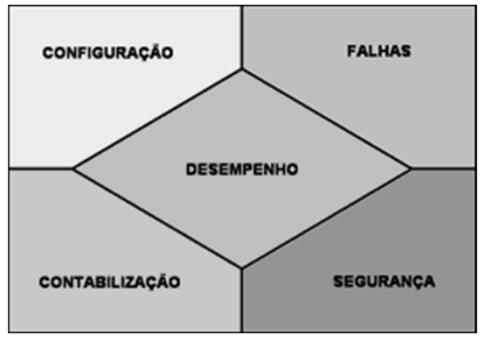
- Distância entre os nodos.
- Distância da antena (em transmissão sem fio).
- Qualidade dos links (cabeado ou sem fio).

Gerência de desempenho, configuração e contabilização

Jitter

Segundo Comer (2007, p. 43), "o jitter pode ser definido como a variação no tempo e na sequência de entrega dos pacotes (PacketDelay Variation) devido à variação da latência (atrasos) na rede". O jitter é analisado na periodicidade na transmissão dos pacotes, como também na variação da entrega dos pacotes.

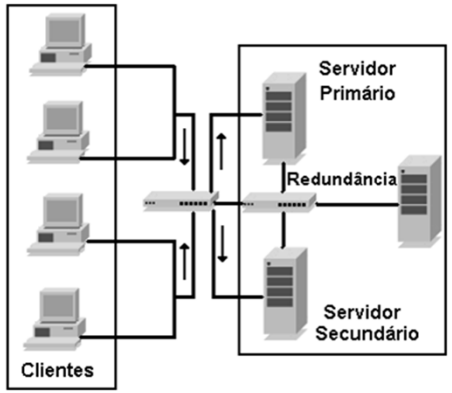




Gerência de desempenho, configuração e contabilização

Disponibilidade

Segundo Comer (2007), as redes de computadores são compostas por diversos equipamentos, como nodos, computadores, servidores, cabeamentos, entre outros, cada um dos quais é um sistema suscetível a falhas.



Para que seja possível calcular a disponibilidade, é necessário compreender o tempo médio para falha (MTTF – mean time to failure): tempo de vida de uma rede que compreende os períodos alternados de operação de falhas. Função de frequência com que as falhas ocorrem:

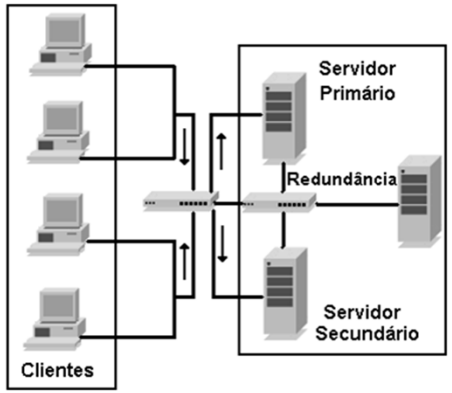
$$D = MTTF / (MTTF + MTTR)$$

Gerência de desempenho, configuração e contabilização

D = MTTF / (MTTF + MTTR)

Para exemplificarmos uma aplicação, imagine que uma rede possua um MTTF de 8.000 horas de operação anual e um MTTR de 36 horas anual.

Nesse caso:



D = 8000 / (8000+36)

D = 99,5

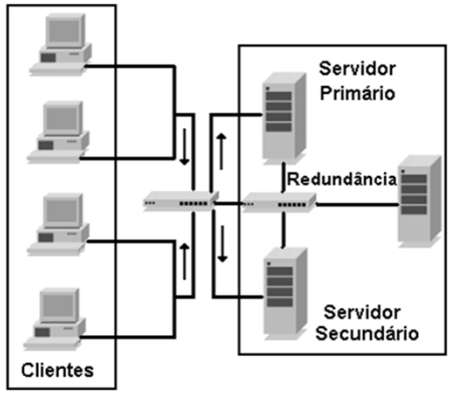
Ou seja, a disponibilidade da rede é de 99,5% ao ano.

Gerência de desempenho, configuração e contabilização

QoS (Quality of Service – Qualidade de Serviço)

Segundo Tanenbaum (1997), qualidade de serviço em redes de computadores pode ser definida como um conjunto de regras, mecanismos e tecnologias que tem o propósito de utilizar os recursos disponíveis de forma eficaz e econômica.

Qualidade de transmissão são: latência, jitter, perda de pacotes e largura de banda disponível. Dois modelos de QoS:

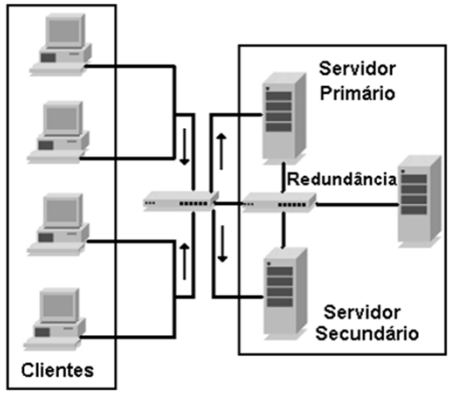


IntServ: utiliza o fluxo dos dados por meio do protocolo no caminho que a mensagem deve percorrer. (Garantia)

DiffServ: conhecido como serviços diferenciados, trata-se de uma marcação no pacote para classificá-los e efetuar os tratamentos necessários de forma independente.

Gerência de desempenho, configuração e contabilização

Qualidade dos serviços, disponibilidade, capacidade de processamento e armazenamento do provedor de serviços são determinados pelo SLA (service level agreement – acordo de nível de serviço).

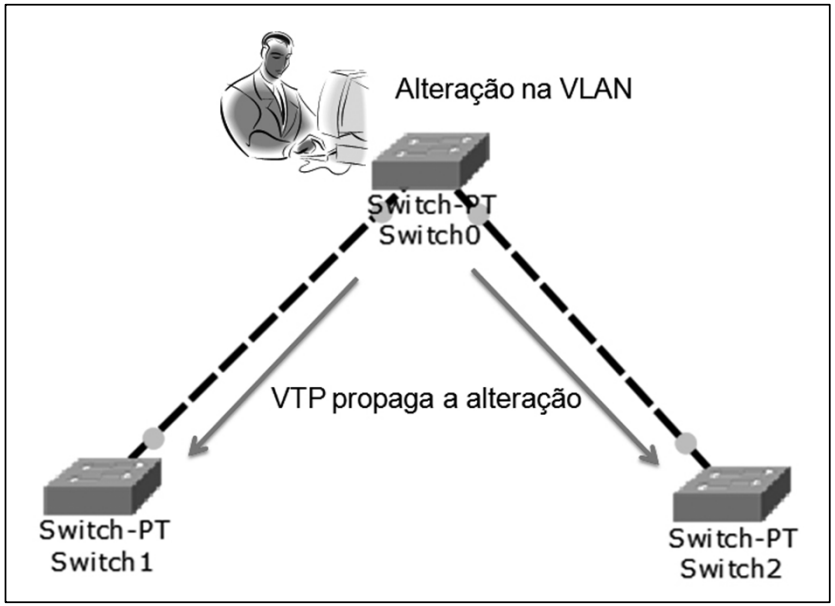


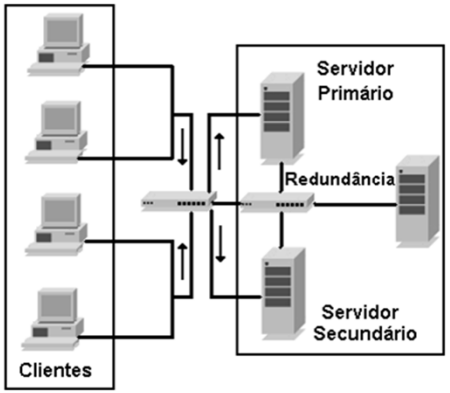
Serviços: as configurações de equipamentos dependem do tipo de serviço que está sendo utilizado na rede.

Dispositivos: existem diversos tipos de fabricantes de equipamentos (roteador, switch, servidor, etc.), cada um com uma forma própria para configuração.

Gerência de desempenho, configuração e contabilização

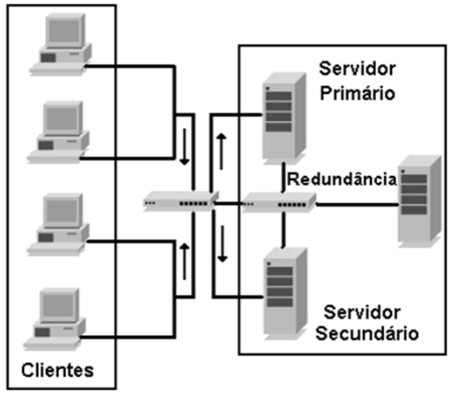
Fillippetti (2008) mostra que VLAN é definida como rede local virtual (virtual lan network). Trata-se de uma maneira de criar sub-redes de forma virtual. Se feita em switchs, cada uma das interfaces pode ser uma VLAN e ter o seu próprio domínio de broadcast.





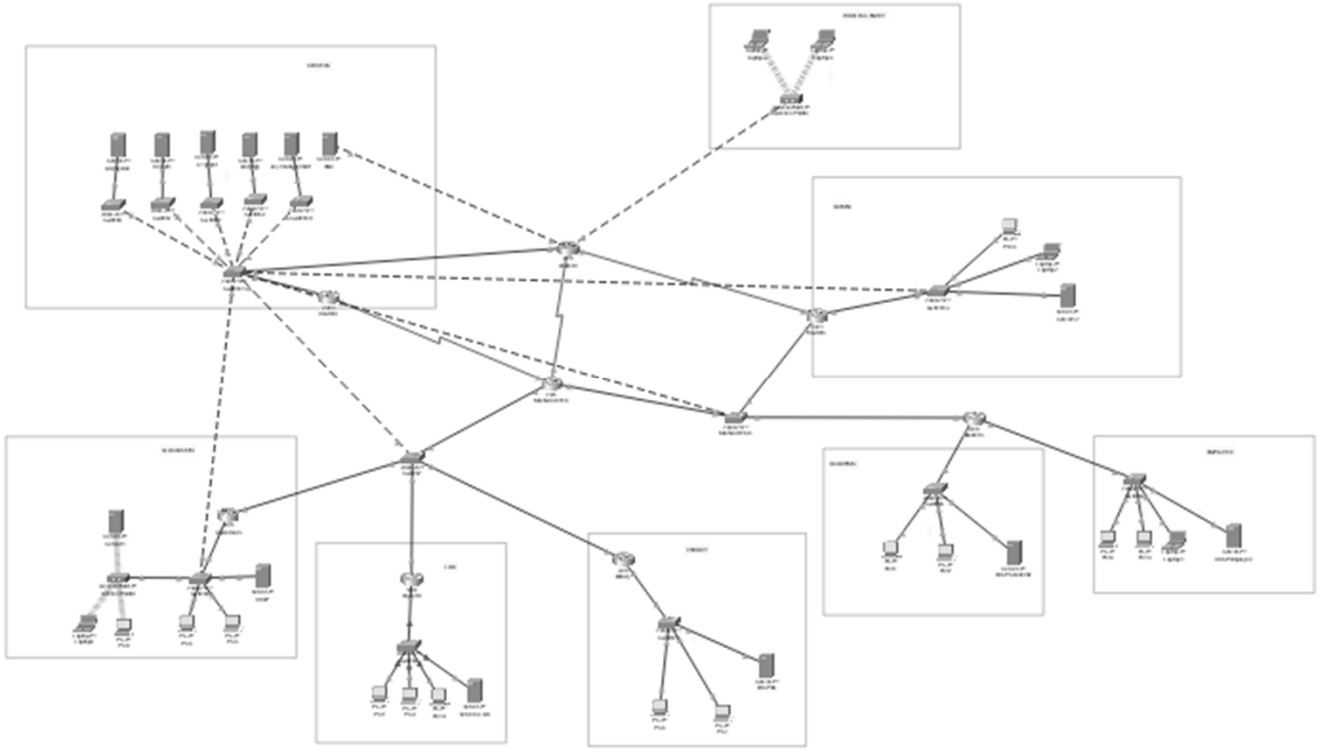
Gerência de desempenho, configuração e contabilização

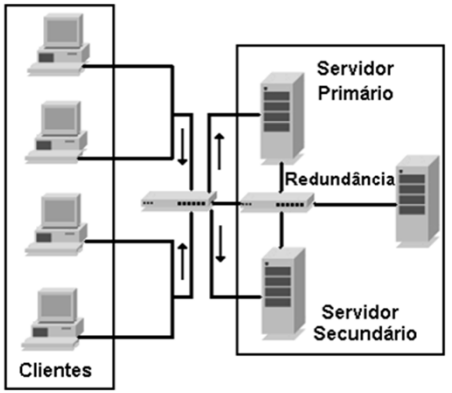
Basicamente, o VTP (VLAN Trunk Protocol) cria uma estrutura do tipo cliente-servidor, em que as alterações obrigatoriamente são feitas no servidor, que, por sua vez, posteriormente as replica aos clientes.



Gerência de desempenho, configuração e contabilização

Exercício:





Recapitulando

Recapitulando

- Teoria da gerência de redes e padrões;
- Gerência de falhas e segurança;
- Gerência de desempenho, configuração e contabilização.