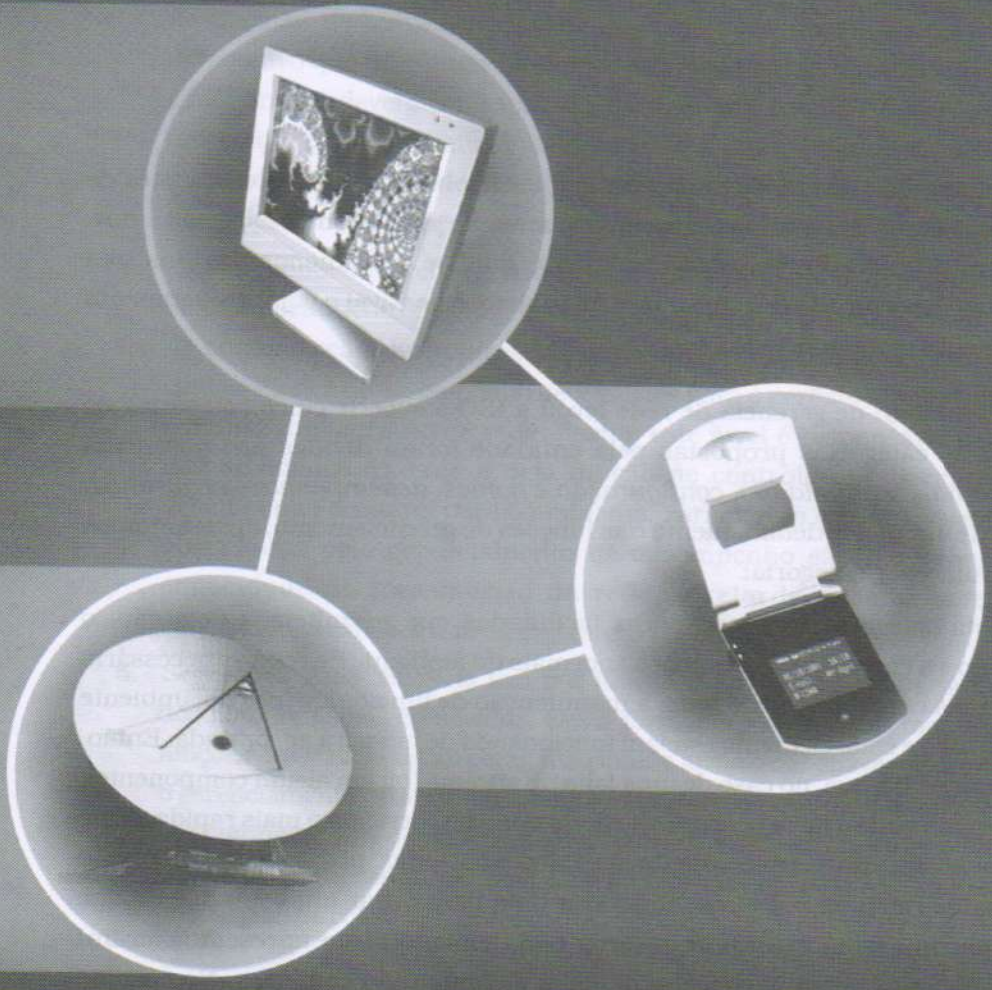
Capítulo 8

Gerência, Segurança e Desempenho de Redes



Introdução

Após o estudo de todo o material apresentado até o momento, fica latente a importância das redes de comunicação e computadores como um instrumento diferencial competitivo para as organizações modernas. Em outras palavras, as redes de maneira geral estão agregando valor às corporações não só pela distribuição de recursos de software e hardware, mas também pela facilidade de prover um poder computacional distribuído nunca antes imaginado. Aplicações das áreas de engenharia, biologia, química, petróleo, meteorologia, telecomunicação, aeronáutica, naval e farmacêutica, entre outras inúmeras áreas, podem se beneficiar dos ambientes de rede com os sistemas computacionais distribuídos.

Por outro lado, é importante observar que o sucesso da transparência do uso dos ambientes de rede se deve muitas vezes a uma gerência eficiente da configuração. Em adição, é necessário que outros aspectos relacionados à gerência, tais como a segurança e o desempenho das redes, também sejam trabalhados. Em outras palavras, podemos dizer que é necessária uma metodologia mais complexa de controle do ambiente de rede para que estas configurações representem um diferencial para as corporações. Neste capítulo, vamos abordar alguns conceitos relacionados com a gerência, a segurança e o desempenho das redes.

Gerência

A gerência de uma rede é um assunto complexo que envolve usualmente os pacotes de software, os dispositivos de hardware e o conhecimento de profissionais especializados. Consonante com outros autores, nossa opinião é que, se pelo menos um dos três elementos for mal especificado durante a fase de projeto, é possível o comprometimento do ambiente de rede como um todo.

A relevância do assunto de gerência de rede levou a ISO a sugerir cinco categorias de gerenciamento. As categorias propostas pela entidade foram divididas nas *gerências funcionais de falha, contabilidade, configuração e nomes, desempenho, e segurança*. Com o objetivo de um maior detalhamento das funções de gerenciamento, apresentamos a seguir um resumo por categoria:

1. Falha: esta categoria compreende as facilidades que permitem a detecção, o isolamento e a correção de operações anormais do ambiente de rede. É necessário que, em uma configuração de rede, a manutenção de funcionamento do ambiente como um todo e cada elemento estejam funcionando de maneira apropriada. Então, esta categoria visa que, no caso de uma falta no sistema (ou em algum componente), seja detectado onde a falha ocorreu, de modo que seja corrigida o mais rapidamente possível. Assim, no gerenciamento de falha são todas providências: isolar o problema do resto da rede, reconfigurar a rede para evitar um componente que apresentou uma falha, e por fim consertar o(s) elemento(s) que apresentou (aram) falha(s). Algumas vezes, o conceito de falha é confundido com erro. No caso de

uma falha, uma situação anormal ocorreu e precisa de uma intervenção para ser reparada. Por outro lado, um erro pode ocorrer de forma esporádica e ser tratado por uma rotina automática.

2. Contabilidade: este nível de gerenciamento deverá prover facilidades que permitam o estabelecimento da contabilização do uso de objetos gerenciáveis e os custos que devem ser identificados na utilização dos objetos. Em uma organização é necessário que os custos relativos ao uso do ambiente sejam computados para os diversos centros de custos da corporação. Em outras palavras, é desejável que todos os usuários do ambiente tenham um custo de uso da configuração de rede. Este parâmetro, por exemplo, auxilia o processo de tomada de decisão para onde o ambiente de rede deve ser expandido e mostra onde os recursos estão sendo mau aproveitados. Um fator diferencial nas redes modernas são os serviços com qualidade de serviço (Quality of Service – QoS) que estes ambientes podem prover. Todavia, os recursos computacionais são finitos, assim como existem custos relativos à disponibilidade de tais serviços.
3. Configuração e nomes: o gerenciamento de configuração e nomes visa prover facilidades como a inicialização/shutdown de sistemas, a distribuição e a atualização de pacotes de software para os elementos de uma rede. Um exemplo é um dispositivo que deve atuar na função de roteamento; desta forma o gerenciador de configuração deverá ser capaz de escolher um pacote de software apropriado e um conjunto de atributos e valores para o equipamento. De uma outra forma, podemos dizer que este nível de gerenciamento é caracterizado pelo controle de identificação dos componentes na rede que visa sua configuração apropriada.
4. Desempenho: no nível de gerenciamento de desempenho, deve existir uma avaliação do comportamento dos objetos gerenciados e sua eficiência quanto às atividades de comunicação. Em outras palavras, a categoria de desempenho se preocupa com os limites de desempenho necessários para o perfeito funcionamento de objetos em uma configuração de rede. Assim, este nível é responsável pela monitoração das atividades da rede e pela função de controle que permite um ajuste de desempenho aceitável para o ambiente. Parâmetros que, por exemplo, devem ser observados pelo gerenciamento de desempenho são o percentual de uso da capacidade de transmissão da rede, o retardo do ambiente, os possíveis congestionamentos e o nível de tráfego da configuração.
5. Segurança: essa categoria tem por função tratar os aspectos relativos à segurança dos componentes gerenciados. Desta forma, é possível imaginar que algumas das funções desse nível sejam gerar, distribuir e armazenar chaves para cifrar. Em adição, o gerenciamento de segurança também engloba o controle e a autorização de acesso aos computadores da rede como um todo e aos aplicativos através da monitoração e controle dos acessos. De forma efetiva, a categoria de segurança emprega uma abordagem de coleta, armazenagem e verificação de arquivos de segurança de eventos.

Ainda com relação ao gerenciamento do modelo OSI, alguns elementos foram estabelecidos segundo suas atribuições funcionais. Apresentamos, a seguir, os elementos do modelo e suas funções:

- Gerente: é uma entidade que pode obter informações atualizadas sobre os objetos gerenciados e controlá-los. Com este objetivo, o gerente transmite operações de gerenciamento aos agentes.
- Agente: é responsável pela execução de gerenciamento sobre objetos gerenciados. O agente também tem a possibilidade de transmitir ao gerente as notificações emitidas pelos objetos gerenciados.
- Objeto gerenciado: é a entidade que representa um recurso que poderá ser gerenciado. Este recurso pode ser, por exemplo, uma conexão ou um dispositivo de comunicação. Os aspectos que são geralmente utilizados para definir os objetos gerenciados são suas propriedades, as operações a que podem ser submetidos, as notificações que podem emitir para informar sobre a ocorrência de eventos de gerenciamento e suas relações com outros objetos gerenciados.

Cada camada do modelo OSI tem seus objetos específicos que podem ser gerenciados. Estes são conhecidos como objetos gerenciados da camada N. Por outro lado, quando um objeto gerenciado é importante para mais de uma camada, este é chamado de objeto gerenciado do sistema. Objetos gerenciados e suas propriedades, quando agrupados em conjunto com relação a um sistema, são chamados de *MIB* (*Management Information Base*).

Devido ao crescimento exponencial das redes, os chamados *sistemas de gerenciamento de rede* têm ganho uma grande importância nas organizações. Um sistema de gerenciamento de rede pode ser compreendido como um conjunto de ferramentas que visam o controle e a monitoração da rede de forma integrada. As características desejáveis de um sistema de gerenciamento são:

- Interface amigável única, mas com um grande potencial para executar um conjunto de comandos de gerenciamento da rede.
- Independência de plataforma. Em outras palavras, é desejável uma certa independência de hardware e software visando que o ambiente computacional da organização seja aproveitado.
- O pacote de software de gerenciamento das tarefas deve residir de maneira distribuída nos computadores e elementos de comunicação (exemplos são os roteadores, pontes e controladores de terminal dentre outros dispositivos).
- O sistema de gerenciamento de rede deve ser projetado para que o ambiente de hardware e software inteiro da corporação seja visto como uma arquitetura unificada.

NOTA

É interessante o leitor observar que o gerenciamento deve agregar valor ao controle do sistema da organização. Certos fabricantes algumas vezes propõem

soluções muito inovadoras à primeira vista, mas desconsideram o parque computacional existente. O sistema de gerenciamento de rede deve se adequar ao ambiente de rede da empresa e não o oposto.

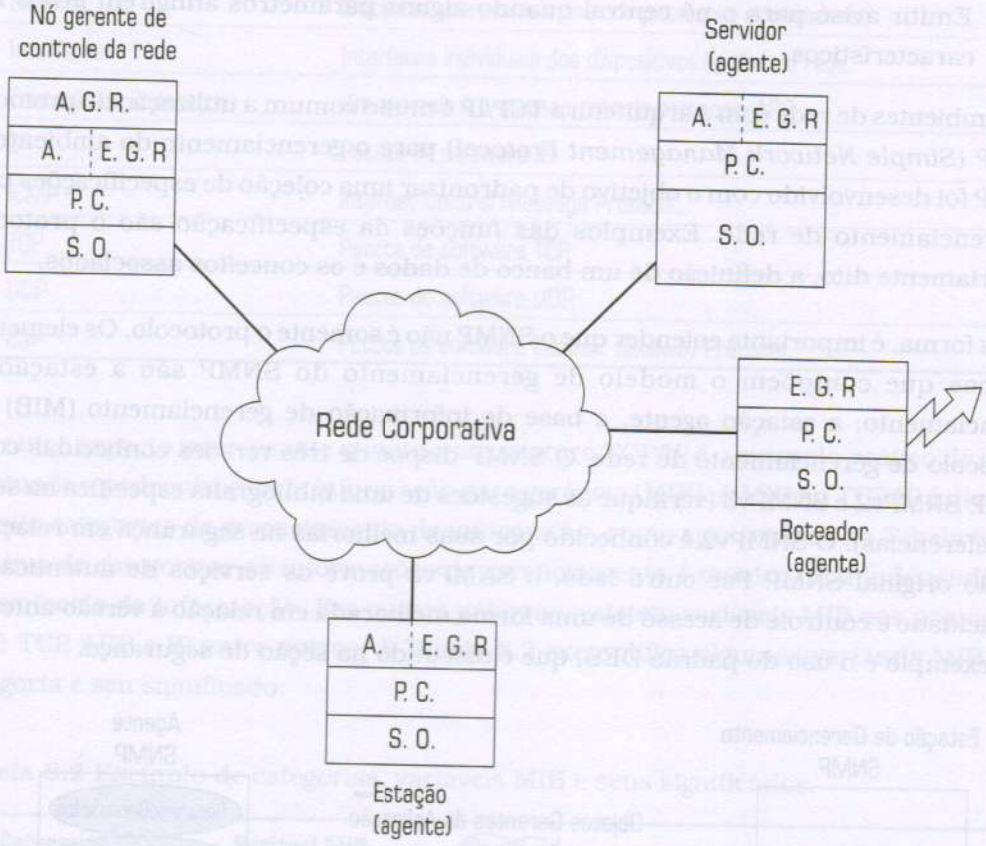


Figura 8.1 Exemplo de um sistema de gerenciamento de rede.

Na Figura 8.1, ilustramos um exemplo de um sistema de gerenciamento de rede caracterizando alguns dispositivos do ambiente. Dispositivos clássicos na arquitetura são: o nó central de gerenciamento, o servidor, o computador e o roteador. Em cada equipamento da configuração, relacionamos os pacotes de software que são comuns nos dispositivos de rede. Exemplos dos pacotes são o sistema operacional (S.O.), o pacote de comunicação (P.C.), a entidade de gerenciamento de rede (E.G.R.) e, quando for o caso, a aplicação (A).

Nosso principal foco nesta seção deve ser a entidade de gerenciamento de rede (NME – Network Management Entity). Desta forma, tarefas que são usualmente implementadas nos pacotes de software de gerenciamento local são:

1. Fazer uma coleta de dados das atividades de comunicação da rede.
2. Armazenar localmente as informações coletadas.

3. Responder aos comandos do nó central. Os comandos podem incluir a transmissão dos dados coletados, troca de parâmetros, fornecimento de informações de controle de estado e geração de tráfego quando um teste for solicitado.
4. Emitir aviso para o nó central quando alguns parâmetros atingirem níveis não característicos.

Nos ambientes de rede com a arquitetura TCP/IP é muito comum a utilização do protocolo SNMP (*Simple Network Management Protocol*) para o gerenciamento do ambiente. O SNMP foi desenvolvido com o objetivo de padronizar uma coleção de especificações para o gerenciamento de rede. Exemplos das funções da especificação são o protocolo propriamente dito, a definição de um banco de dados e os conceitos associados.

Desta forma, é importante entender que o SNMP não é somente o protocolo. Os elementos básicos que compõem o modelo de gerenciamento do SNMP são a estação de gerenciamento, a estação agente, a base de informação de gerenciamento (MIB) e o protocolo de gerenciamento de rede. O SNMP dispõe de três versões conhecidas como SNMP, SNMPv2 e SNMPv3 (verifique as sugestões de uma bibliografia específica na seção de Referências). O SNMPv2 é conhecido por suas melhorias na segurança em relação à versão original SNMP. Por outro lado, o SNMPv3 provê os serviços de autenticação, privacidade e controle de acesso de uma forma melhorada em relação à versão anterior. Um exemplo é o uso do padrão DES, que é discutido na seção de segurança.

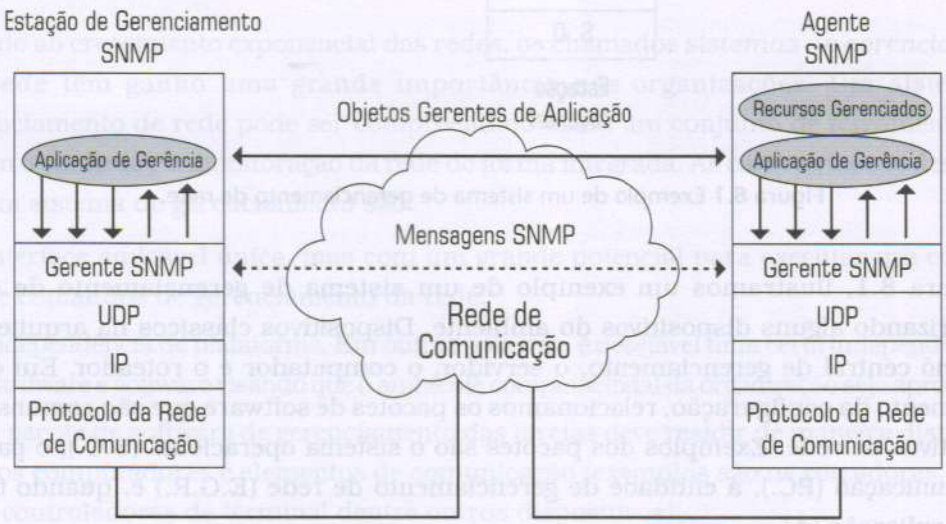


Figura 8.2 Exemplo de uma comunicação SNMP.

A Figura 8.2 exemplifica uma comunicação entre uma estação de gerenciamento e outra estação agente segundo o modelo SNMP.

Tabela 8.1 Categoria de informação na MIB.

Categoria MIB	Informações Pertinentes
Sistema	Sistemas operacionais dos computadores e roteadores.
Interfaces	Interfaces individuais dos dispositivos ligados na rede.
Tradução de Endereços	Um exemplo é o mapeamento do protocolo ARP.
IP	Pacote de software IP.
ICMP	Internet Control Message Protocol.
TCP	Pacote de software TCP.
UDP	Pacote de software UDP.
EGP	Pacote de software Exterior Gateway Protocol.

Um outro aspecto interessante quanto a arquitetura TCP/IP é o exemplo prático de como é efetuada a padronização da informação para gerência (MIB). A MIB no TCP/IP é dividida em oito categorias de gerenciamento de informação, como apresentado na Tabela 8.1. O objetivo de categorizar as informações de gerenciamento é manter uma independência de protocolo da informação. Em outras palavras, existem variáveis MIB aos protocolos UDP, TCP, ARP e IP, entre outros. A Tabela 8.2 exemplifica algumas variáveis MIB, sua categoria e seu significado.

Tabela 8.2 Exemplo de categorias, variáveis MIB e seus significados.

Categoria	Variável MIB	Significado
Sistema	SysUpTime	Tempo decorrido desde a última inicialização.
Interfaces	IfNumber	Número de interfaces de rede.
IP	IpOutNoRoutes	Número de roteamento com falha.
ICMP	IcmpInEchos	Número de ICMP Echo Request recebidos.
TCP	TcpMaxConn	Número máximo de conexões TCP permitidas.
UDP	UdpInDatagrams	Número de datagramas UDP recebidos.
EGP	EgpInMsgs	Número de mensagens EGS recebidas.

Segurança

Como os aspectos de segurança e desempenho são elementos vitais para o perfeito funcionamento de um ambiente de rede, vamos, nesta seção e na próxima, discutir sobre os tópicos segurança e desempenho. Com relação à segurança, vamos abordar os

aspectos da segurança física, criptologia, autenticação, assinaturas digitais e filtragem de pacotes.

Segurança Física

Com certeza o primeiro cuidado que deve ser observado num ambiente de rede de comunicação e computadores é conhecido como a segurança física do ambiente. Este nível de segurança, embora óbvio à primeira vista, e não muito observado em algumas organizações, engloba os aspectos de controle de acesso físico e proteção dos dados contra acidentes (ou ataques) nas configurações de rede.

Quando, por exemplo, uma rede de computadores representar um modelo computacional distribuído diferenciado para uma determinada corporação, é importante lembrar que uma política de cópias de segurança (backups) dos aplicativos e pacotes de software deve existir de maneira formal. Em outras palavras, responsáveis pelas cópias de segurança devem ser indicados, visando não só efetuar o serviço, mas também que estes sejam responsáveis pela política de proteção dos dados.

Como um exemplo prático sobre a segurança física, imaginem uma empresa internacional de consultoria, especializada em assuntos relativos às bolsas de valores. Suponha que, durante vários anos, essa empresa armazenou informações vitais sobre o mercado financeiro e as movimentações de seus clientes num único local da rede. O local escolhido foi aquele onde existia uma sala cofre. Por causa de um ataque de terceiros ao local de armazenagem, todos os dados da empresa se perderam. Você pode imaginar qual o futuro dessa empresa no mercado de consultoria? Um exemplo real foi o ataque terrorista às torres do World Trade Center em Nova Iorque. Imagine que uma empresa semelhante existia e armazenava todos os seu dados num ponto de rede em um daqueles prédios. Podemos inferir que, nesse quadro, a empresa não sobreviveu no mercado.

Podemos pensar em outros exemplos menos catastróficos, porém com resultados tão danosos para a organização quanto um ataque suicida. Imagine que, em uma determinada indústria, o setor de desenvolvimento de produto dispõe de total interligação com as bases de dados da empresa. Caso um intruso tenha acesso a um microcomputador com dispositivo de armazenagem secundário, como por exemplo discos flexíveis, ele poderá efetuar uma cópia e levar consigo informações vitais de um determinado produto da indústria. Um outro exemplo seria o intruso inserir informações maliciosas na base de dados.

Uma forma eficiente (e antiga) de evitar tais problemas é a proibição de acesso de pessoas não-autorizadas nas dependências onde existe o ambiente de rede da empresa. Caso a proibição de acesso não seja exeqüível, um controle de acesso pode ajudar a evitar futuros problemas. Fica claro que o problema de segurança física é cada vez mais crítico nas organizações e que políticas preventivas devem ser elaboradas.

Criptologia

A *criptologia* é um termo oriundo do grego com um significado aproximado de esconder uma palavra. A criptologia é empregada como um guarda-chuva no campo de comunicações secretas. A importância da área de comunicações secretas pode ser mensurada pela formação, em 1983, da International Association for Cryptologic Research, que é uma sociedade de pesquisadores do assunto. A criptologia pode ser subdivida em *criptografia* e *criptoanálise*.

A *criptografia* é uma antiga técnica empregada para *cifrar* mensagens, protegendo as informações que são transmitidas entre um determinado remetente e um destinatário. Essa abordagem, largamente utilizada nos meios militares e diplomáticos, consiste na operação de cifrar um texto de forma que só o destinatário seja capaz de entendê-lo. Em outras palavras, podemos dizer de maneira simplificada que o remetente embaralha uma mensagem original de tal forma que somente o destinatário será capaz de *decifrar* a mensagem original.

Por outro lado, a *criptoanálise* é a arte da quebra do código. Em outras palavras, a criptoanálise visa decifrar na condição de intruso uma mensagem criada pela técnica de criptografia. Desta forma, é importante não confundir '*decifrar de maneira autorizada*' com a '*quebra*' efetuada pela criptoanálise.

A Figura 8.3 ilustra um modelo convencional de criptologia. É interessante observar que, muitas vezes, na literatura, o modelo é chamado de modelo de criptografia. O conceito de criptologia é mais abrangente.

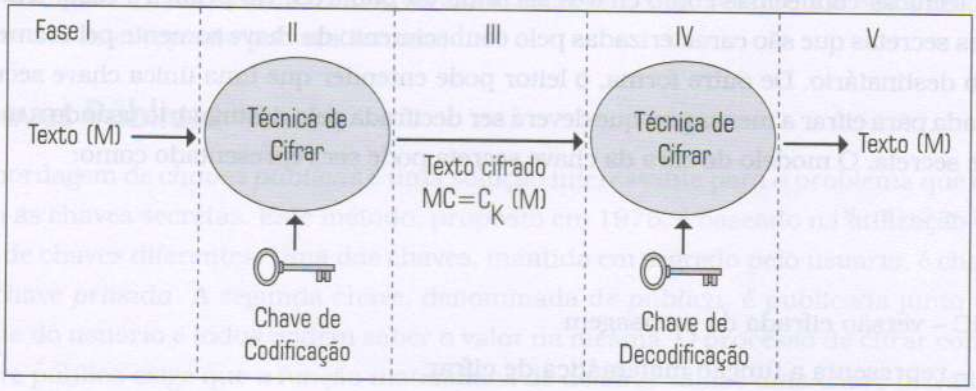


Figura 8.3 Modelo de criptologia com chaves.

Nesta figura, estabelecemos cinco fases distintas que compõem a transmissão de uma mensagem de um remetente a um destinatário. Na Tabela 8.3, fazemos um sumário das fases e a descrição de atividades em cada etapa.

Tabela 8.3 Fases e atividades do modelo de criptografia.

Fase	Descrição de Atividades
I	Uma mensagem M qualquer é enviada pelo remetente para o destinatário.
II	Antes da mensagem M ser enviada, é nessa fase que é aplicada uma técnica para cifrar o texto. Estas técnicas de cifrar são caracterizadas pela transformação do texto original através de uma função parametrizada por uma chave. Vamos denominar a chave de k.
III	Na fase III, a mensagem MC, já cifrada, é enviada pela rede de comunicação. Desta forma, temos a mensagem cifraca representada pela notação $MC=C_k(M)$. C é uma função matemática que utiliza o parâmetro k (chave) para cifrar M. Nesta fase, os intrusos podem interceptar a transmissão para saber o que o remetente está enviando para o destinatário. Os intrusos podem ser classificados em passivos e ativos. Os passivos usualmente só tomam conhecimento da mensagem, enquanto os ativos capturam a mensagem e fazem uma determinada alteração (troca ou adulteração) no conteúdo da mensagem.
IV	Nesta fase é aplicada uma técnica para decifrar o conteúdo da mensagem. Para representar esta operação podemos usar a notação $D_k(MC)$, ou seja, $D_k(C_k(M))=M$. Semelhante a C, D é uma função matemática que utiliza o parâmetro k (chave) para decifrar MC.
V	A mensagem M é recebida pelo destinatário.

Chaves Secretas

As chaves, utilizadas para a codificação e decodificação, podem ser empregadas adotando-se as técnicas conhecidas como chaves *secretas* ou *públicas*. No primeiro caso, temos as chaves secretas que são caracterizadas pelo conhecimento da chave somente pelo remetente e pelo destinatário. De outra forma, o leitor pode entender que uma única chave secreta é utilizada para cifrar a mensagem que deverá ser decifrada pelo destinatário usando a mesma chave secreta. O modelo de cifra da chave secreta pode ser representado como:

```
MC = C (k, M)
```

onde:

- MC – versão cifrada da mensagem
- C – representa a função matemática de cifrar
- k – chave secreta
- M – mensagem original

Do lado do destinatário, a operação de decifrar pode ser representada como:

```
M = D (k, MC)
```

onde:

- M – mensagem original
- D – representa a função matemática de decifrar
- k – chave secreta
- MC – mensagem cifrada

Um exemplo real de chave secreta é o padrão DES (*Data Encryption Standard*). Este padrão foi desenvolvido pela IBM, e adotado pelo governo americano em 1977, para uso no envio de informações não confidenciais. O método codifica blocos de 64 bits de texto gerando 64 bits de texto criptografado, utilizando uma chave de 56 bits com 19 estágios distintos. No primeiro estágio, conhecido como transposição, é efetuada uma modificação do texto independente da chave secreta. Seguem-se 16 estágios que executam a mesma transformação nos dados, nas transposições e substituições de acordo com parâmetros gerados por diferentes funções da chave. No destinatário, essas etapas são efetuadas de maneira inversa. Após a execução dos 16 estágios, é efetuada a troca dos 32 bits mais à esquerda pelos 32 bits mais à direita. Finalizando, o 19º estágio é caracterizado pela transposição inversa. O DES foi largamente usado na área de informática, porém a forma nativa do ambiente não é mais segura. Desta forma, o DES é empregado muitas vezes de maneira modificada ou melhorada. Um exemplo é o IDEA (*International Data Encryption Algorithm*), criado por dois pesquisadores na Suíça. A Figura 8.4 ilustra o método DES e um exemplo de detalhamento de uma iteração dos 16 estágios.

O método DES padece do mau relativo aos algoritmos *simétricos*, pois tem como exigência que o remetente e o destinatário conheçam uma única chave secreta que é usada para cifrar e decifrar a mensagem. O problema se agrava quando, por motivo de distância entre os pares, é necessário o envio da chave secreta. Existe sempre a possibilidade de a chave ser interceptada por um intruso.

Chaves Públicas

A abordagem de *chaves públicas* é uma solução interessante para o problema que ocorre com as chaves secretas. Este método, proposto em 1976, é baseado na utilização de um par de chaves diferentes. Uma das chaves, mantida em segredo pelo usuário, é chamada de chave *privada*. A segunda chave, denominada de *pública*, é publicada junto com o nome do usuário e todos podem saber o valor da mesma. O processo de cifrar com uma chave pública exige que a função matemática de decifrar utilize uma chave privada. Em outras palavras, um usuário remetente utiliza uma chave pública para cifrar uma mensagem. Esta mensagem pode percorrer a rede sem problema, pois só o destinatário que tem uma determinada chave privada pode decifrar a mensagem. Os métodos que utilizam esta abordagem de par de chaves distintas são conhecidos como *assimétricos*.

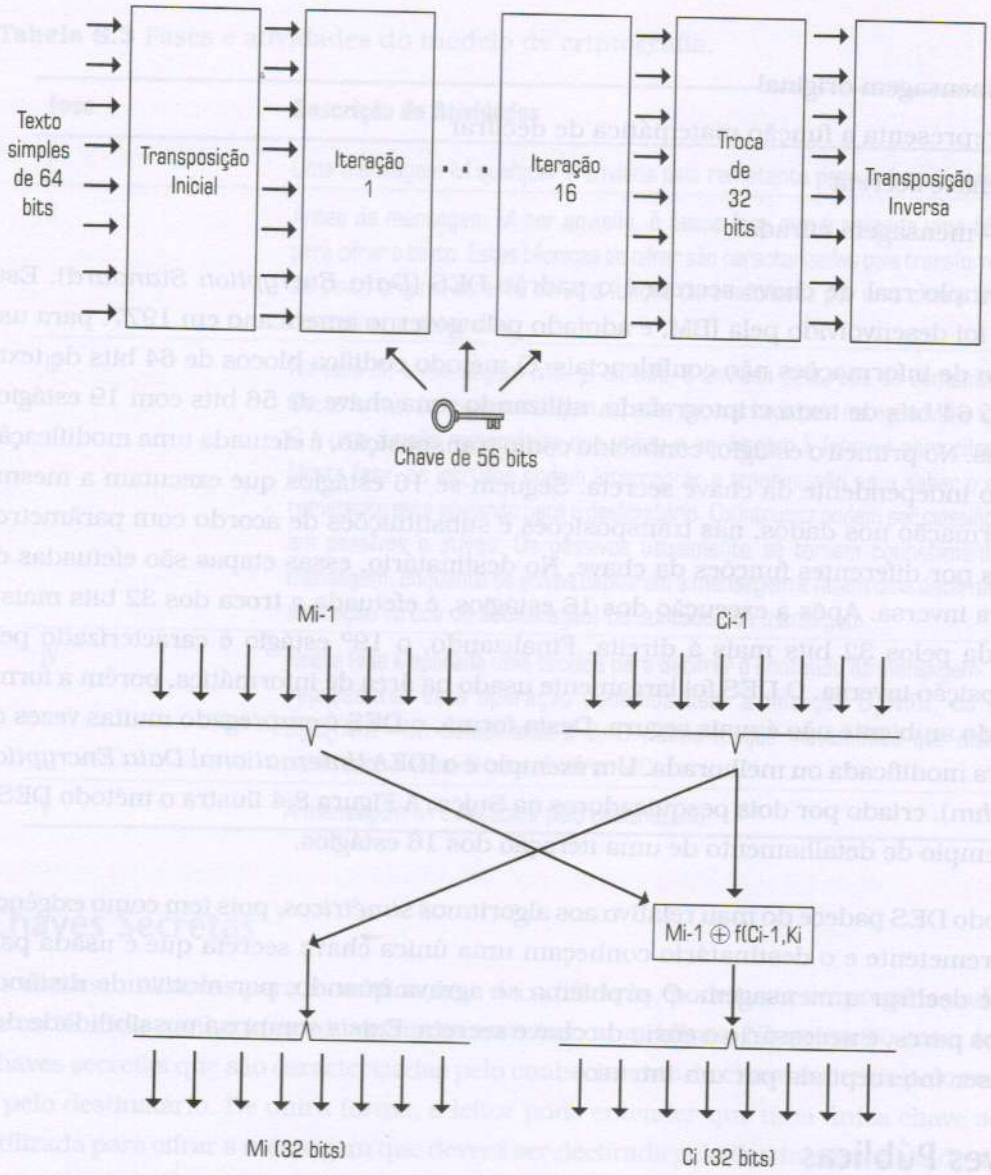


Figura 8.4 Método DES (a) modelo geral e (b) exemplo de uma iteração.

Um exemplo clássico de algoritmo assimétrico é o conhecido *RSA*. Este algoritmo, desenvolvido por pesquisadores da universidade americana MIT, ganhou a denominação de RSA em homenagem a seus desenvolvedores (Rivest, Shamir e Adleman). O método se baseia em alguns princípios da teoria dos números. A idéia do RSA é considerar dois números primos quaisquer, por exemplo p e q, com centenas de bits (superior a casa dos 10^{100}) e calcular n que representa p x q. Em seguida, obtem-se um número z que representa o resultado da multiplicação de (p – 1) x (q – 1). A próxima etapa é a escolha de um número primo em relação a z que vamos denominar de d. Finalmente, é necessário encontrar um número e tal que e x d = 1 mod z.

Os números n, e e d representam os parâmetros necessários para a formação das chaves pública e privada. No caso da chave pública, esta é formada pelo par (e,n). A operação de cifrar uma mensagem (M) é representa por $C = Me \ (mod\ n)$. A chave privada é constituída pelo par (d,n) e a operação de decifrar é representada por $M = Cd(mod\ n)$. Nas referências, apresentamos indicações de uma literatura mais específica sobre o assunto.

Autenticação

O processo de *autenticação* é caracterizado pela confirmação da identificação de um parceiro em uma comunicação. Em outras palavras, o processo de autenticação visa combater um elemento impostor. É interessante lembrar que, em um determinado ambiente de rede, um intruso ativo pode se passar por um parceiro. Assim, podemos inferir que é complexa a tarefa de autenticação.

As abordagens mais utilizadas de autenticação são aquelas baseadas em chaves secretas compartilhadas, por centros de distribuição de chaves, pelo uso do protocolo Kerberos e por intermédio da criptografia com chave pública.

Um conceito, que às vezes é confundido com a autenticação, é o princípio da *autorização*. A autorização, diferente da autenticação, é um processo no qual é solicitado ao usuário uma ou mais senhas que comprovem que o mesmo está autorizado a solicitar determinado serviço (ou acesso).

Assinaturas Digitais

A assinatura digital é um paradigma que visa dar autenticidade de uma maneira digital aos documentos legais dentro de uma corporação. Em outras palavras, essa técnica tem por objetivo prover uma substituição na tramitação dos documentos que são distribuídos segundo procedimentos convencionais para uma forma digital legal.

Com o alto grau de informatização das empresas é desejável que, por exemplo, um pacote de software tenha a força semelhante aos documentos de papel. Desta forma, por exemplo, um determinado chefe em uma empresa pode passar para o serviço de recursos humanos a relação dos empregados que terão aumento de salário, que estarão de férias a partir do próximo mês e a solicitação de compra de passagens para aqueles que devem fazer algum trabalho externo. Poderíamos pensar, também como um outro exemplo, as organizações governamentais, nas quais o tramite de documentação é reconhecidamente moroso. Uma vez que uma determinada decisão fosse tomada, todos os interessados seriam notificados imediatamente. Ainda podemos imaginar situações onde uma determinada ordem pudesse ser cumprida de forma imediata.

Das situações apresentadas no parágrafo anterior, podemos imaginar as seguintes dificuldades na implementação da assinatura digital:

- Como garantir a identidade do remetente?
- Como assegurar que o destinatário não criou uma determinada mensagem?
- Como assegurar que o remetente não possa negar a autoria de uma mensagem?

Estratégias de implementação da assinatura digital são:

- Assinaturas com chaves secretas: nesta abordagem, existe uma entidade central que representa a autoridade que sabe de tudo (isto é, conhece todas as chaves secretas) e na qual todos devem confiar. Cada usuário faz sua escolha pessoal de uma chave secreta e notifica a entidade central. Quando um indivíduo deseja enviar uma mensagem, esta é enviada através da entidade central, que certifica que quem está enviando a mensagem é realmente um determinado usuário, depois redirecionando para quem de direito. O problema dessa abordagem é a concentração de poder na entidade central e também a carga de trabalho, pois a entidade central terá que processar muito rapidamente um volume grande de solicitações. Em adição, a entidade central representa um ponto de falha no sistema e será alvo de todos os intrusos numa tentativa de invadir o ambiente.

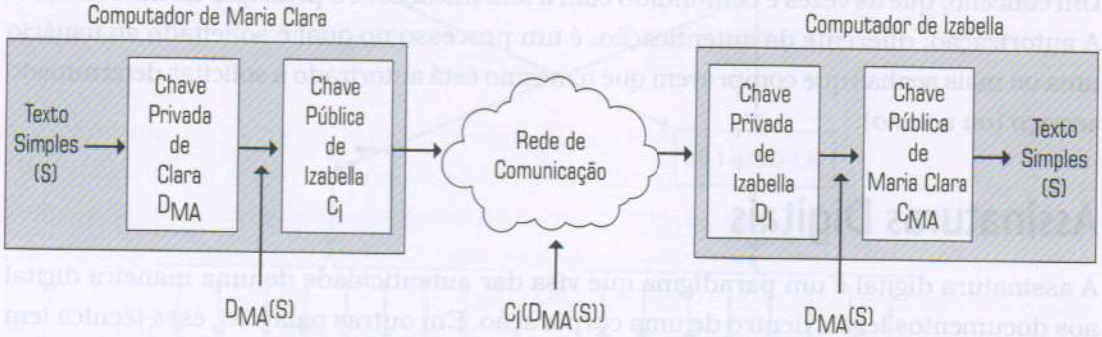


Figura 8.5 Exemplo de assinaturas de chaves públicas.

- Assinaturas com chaves públicas: esta técnica permite que um usuário utilize sua chave privada para cifrar, num primeiro estágio, a mensagem a ser enviada. Em um segundo estágio, o usuário remetente cifra a mensagem cifrada na etapa anterior com uma chave pública do destinatário. Após a dupla operação de cifrar, a mensagem é enviada pela rede de comunicação até o remetente. Quando a mensagem chega ao remetente, é efetuada uma operação dupla de decifrar. O destinatário, num primeiro estágio, emprega sua chave privada para decifrar o primeiro estágio da mensagem enviada pelo remetente. A segunda operação de decifrar é caracterizada pelo uso da chave pública do remetente para decifrar finalmente a mensagem. A Figura 8.5 ilustra um exemplo do uso das assinaturas de chaves públicas.

Filtragem de Pacotes

A filtragem de pacotes é uma abordagem através da qual se faz, por motivo de segurança, uma inspeção em cada datagrama que chega ou sai de determinada configuração de rede. Seguindo um critério preestabelecido pela administração da rede, os datagramas que se enquadrarem nas condições serão enviados normalmente. Por outro lado, datagramas que não se encaixam nas determinações estabelecidas pela gerência da rede serão descartados. A operação de filtragem geralmente é efetuada num roteador que tem funções complementares para tal finalidade. Na Figura 8.6, exemplificamos o uso de um dispositivo com a função de filtragem de pacotes.

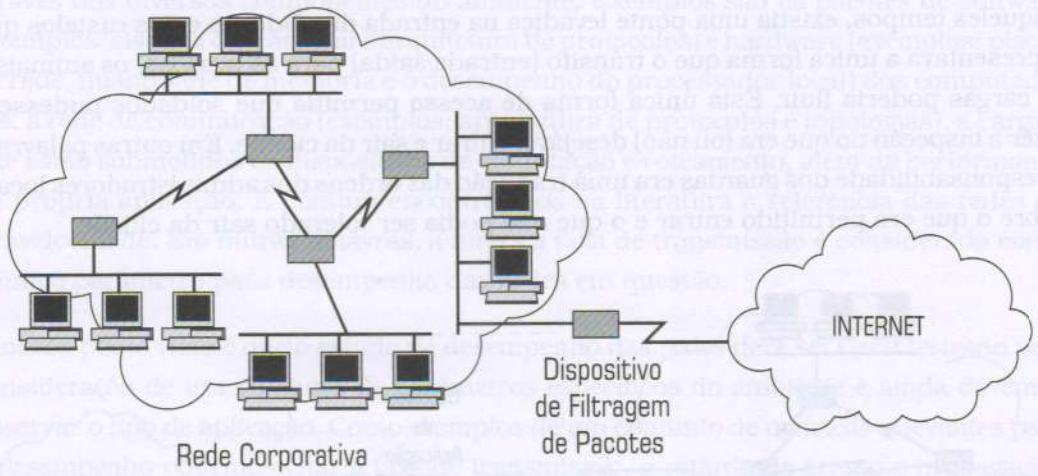


Figura 8.6 Exemplo da filtragem de pacotes.

NOTA

O leitor deve observar que a utilização do roteador, com o dispositivo que tem a função de filtragem, é baseada no fato de que, na maioria da vezes, este é o equipamento de rede que faz a ligação da rede interna da empresa com o mundo exterior. No caso de utilização de outro dispositivo com a função de roteamento, este equipamento é o ponto onde deve ser efetuada a filtragem dos datagramas.

Firewalls

Como estudamos anteriormente neste capítulo, a técnica de criptografia pode prover uma certa segurança com relação ao trânsito de mensagens entre ambientes de rede. Por outro lado, é importante que alguma abordagem exista para a proteção dos dados armazenados na organização, contra a ação de *hackers* ou, por exemplo, para evitar a propagação de vírus digitais no ambiente.

NOTA

Hackers são pessoas, ou grupo organizado de pessoas, não-autorizadas que penetram num sistema computacional com diferentes objetivos escusos (exemplos são a quebra da segurança por brincadeira ou para desmoralizar a instituição, roubo informações confidenciais, captura de senhas de usuários, desvio ilegal de dinheiro entre contas, observação do funcionamento do ambiente para futuros ataques e diversos outros).

Os *firewalls* representam uma técnica de proteção dos sistemas computacionais semelhante ao paradigma adotado na idade média para proteger as cidades e os castelos. Naqueles tempos, existia uma ponte levadiça na entrada das cidades e dos castelos que representava a única forma que o trânsito (entrada/saída) para as pessoas, os animais e as cargas poderia fluir. Esta única forma de acesso permitia que soldados pudessem fazer a inspeção do que era (ou não) desejável entrar e sair da cidade. Em outras palavras, a responsabilidade dos guardas era uma tradução das ordens dos administradores locais sobre o que era permitido entrar e o que não podia ser tolerado sair da cidade.

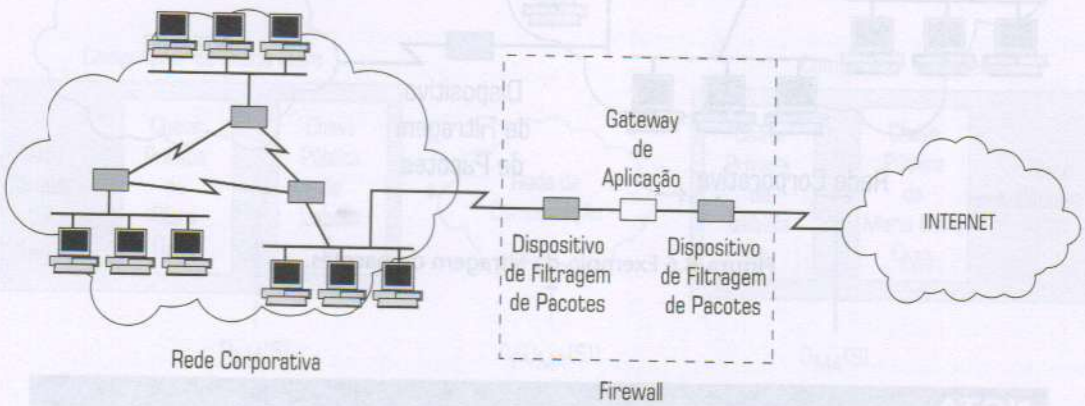


Figura 8.7 Exemplo de uma configuração com firewall.

Em uma configuração de rede, a função da ponte levadiça e dos soldados vigiando o que entra e sai da cidade é representada pela barreira de proteção eletrônica denominada de *firewall*. Na Figura 8.7, apresentamos um exemplo de um ambiente de rede com um *firewall*. É interessante notar que podemos empregar os filtros de pacotes e os chamados *gateways de aplicação* para compor o *firewall*. Diferente dos filtros de pacotes, os gateways de aplicação não trabalham sobre os pacotes de maneira isolada. Em outras palavras, um gateway de aplicação está relacionado à inspeção em nível de aplicação. Então, em uma configuração de rede, podemos ter vários gateways de aplicação cuja função é a permissão (ou bloqueio) de pacotes com relação à aplicação (exemplo: gateway de correio eletrônico).

Desempenho

O desempenho de uma determinada rede é a forma através da qual tentamos tecer comparações de eficiência do ambiente com relação a outra configuração de rede. Uma configuração de rede, onde milhares de computadores existem, torna complexo o estudo de desempenho do ambiente. Tanenbaum (1996) afirma que compreender o desempenho é uma questão mais artística do que científica. Tal afirmação pode ser mensurada pelos inúmeros parâmetros envolvidos numa comparação e seus respectivos pesos com relação a cada configuração de rede.

De uma forma macro, podemos visualizar a complexidade do estudo de desempenho através dos diversos componentes do ambiente. Exemplos são os pacotes de software (exemplos: sistema operacional e arquitetura de protocolos) e hardware (exemplos: placas de rede, quantidade de memória e o desempenho do processador local) dos computadores, a rede de comunicação (exemplos: arquitetura de protocolos e topologias), a carga a que estão submetidos os dispositivos de comutação e roteamento, além da performance da própria aplicação. É comum encontrarmos na literatura a referência das redes de altavelocidade. Em outras palavras, a métrica taxa de transmissão é considerada como o único parâmetro para desempenho das redes em questão.

O nosso ponto vista é que o estudo de desempenho das redes deve ser caracterizado pela consideração de um conjunto de parâmetros específicos do ambiente e ainda devemos observar o tipo de aplicação. Como exemplos de um conjunto de métricas relevantes para o desempenho podemos citar a taxa de transmissão, o retardo de acesso e propagação, número de equipamentos interligados na rede, a arquitetura de protocolo e topologia, entre uma série de outros parâmetros. Quanto à aplicação, é necessário o leitor saber, por exemplo, que uma rede de controle não deve ser projetada com a taxa de transmissão como métrica fundamental. Nestes ambientes, o retardo é um parâmetro essencial e deve ser o mínimo possível, pois as ações inerentes às aplicações de controle são de efetuar uma operação de maneira rápida. A rapidez em uma rede de controle significa uma ação imediata com uma taxa de transmissão geralmente baixa (alguns Mbps).

A seguir, apresentamos diferentes parâmetros de desempenho em exemplos de situações distintas onde estes têm maior relevância do que outras métricas.

1. Topologia: as redes com configuração multiponto, ponto-a-ponto e comutada devem prover desempenho diferenciados quando considerarmos, por exemplo, uma aplicação onde as sincronizações entre processos são necessárias. Imagine que a aplicação de um usuário requer muita comunicação multicast, visando uma sincronização dos vários estágios de inúmeros processos diferentes. Em uma rede multiponto, somente uma host pode ter acesso ao meio por vez. Em uma configuração de rede ponto-a-ponto, todos os processos podem se comunicar instantaneamente com todos os outros processos. Finalmente, em um ambiente

de rede comutada alguma concorrência é possível, uma vez que poderemos ter a comunicação paralela entre várias portas do dispositivo de rede ao mesmo instante.

2. Taxa de transmissão do processador: é conhecido, como Tanenbaum (1996) comenta, que o tempo teórico de uma chamada de RPC (Remote Procedure Call) em um ambiente Ethernet é de 102 μsegundos. Na prática, é verificado que este tempo é maior na ordem de quinze vezes mais (1500 μsegundos, veja Renesse (1988)). Este acréscimo de tempo pode ser todo atribuído aos pacotes de software que estão rodando nos computadores em comunicação. Em adição, imagine que você dispõe de alguns hosts com freqüência igual a 433 MHz e com placas de rede de Gbps. O tempo necessário de envio dos pacotes do host A para um outro host B é consumido em sua maior parte pelo processamento de envio e recebimento nos hosts remetente e destinatário. Em outras palavras, é mais interessante elevar o poder computacional dos processadores em comunicação do que elevar a largura de banda entre os dispositivos. Em adição, no último capítulo, ilustramos um exemplo real no qual são apresentados clusters de computadores homogêneos onde os relógios dos computadores têm um desempenho diferenciado.
3. Protocolos Leves (*Lightweight Protocols*): como vamos estudar no próximo capítulo, protocolos mais leves em comparação aos atuais (exemplo: TCP) podem prover um melhor conjunto de facilidades para aplicações que utilizam redes com grande largura de banda, baixa taxa de erro e redes onde o custo de transmissão é elevado. Um exemplo que ilustra esta situação é uma comunicação via satélite na qual o custo de transmissão é elevado e as retransmissões não são adequadas. Caso uma aplicação esteja utilizando o protocolo de transporte TCP com uma janela deslizante de tamanho igual a 1.000 pacotes, qualquer retransmissão terá um efeito danoso. Em outras palavras, vamos supor que o pacote de número 20 se perca na transmissão. O destinatário irá acusar para o remetente que o pacote 20 não chegou. Uma comunicação, quando suportada pelo protocolo TCP, faz a retransmissão de todos os pacotes a partir do pacote perdido (técnica go-back-n). Assim, todos os pacotes numerados de 20 até 1.000 serão retransmitidos e apenas o de número 20 vai ser aproveitado, os demais serão descartados. É de se esperar que se um protocolo de transporte mais adequado fosse selecionado, o desempenho da aplicação seria melhor.

Exercícios

1) Quais as categorias de gerenciamento sugeridas pela OSI?
2) Descreva as funções de segurança e desempenho sugeridas num modelo de gerenciamento.
3) Faça uma tabela com os elementos funcionais de gerenciamento OSI e suas respectivas atribuições.
4) Descreva a função de uma MIB.

5) Descreva de forma detalhada qual a função de um pacote de gerenciamento de rede.
6) Considerando o modelo SNMP, descreva seus elementos.
7) Comente sobre a importância da segurança física em um ambiente de rede.
8) Descreva com suas palavras a diferença entre criptologia e criptografia.
9) Qual o objetivo da criptoanálise?
10) Explique o funcionamento das chaves secretas.
11) Faça uma diferenciação entre as chaves secretas, privadas e públicas.
12) Como você diferencia uma abordagem de protocolo de segurança simétrico e outro assimétrico?
13) Qual a diferença entre autorização e a autenticação?
14) Qual o objetivo da assinatura digital e quais técnicas podem prover esta facilidade?
15) Quais os problemas que você pode imaginar que ocorreram numa corporação com a implantação de um ambiente de assinatura digital?
16) Descreva a técnica com assinatura de chave secreta.
17) Descreva a técnica com assinatura de chave pública.
18) Explique o porquê da comparação entre um firewall e uma ponte levadiça.
19) Estabeleça a diferença funcional entre um filtro de pacotes e um gateway de aplicação.
20) Explique, com suas palavras, quais métricas você acredita que devem ser consideradas no estudo de desempenho das redes.

Referências

Com relação ao tópico criptografia, o leitor deve com certeza incluir Khan (1967), onde existe um histórico completo sobre assunto. Este interessante livro é difícil de ser encontrado, pois sua edição está esgotada e parece que sua reedição está proibida. As abordagens mais atuais são encontradas em Goldreich (1998), Joyner (2000), Kaufman (1995), Massey (1988), Schneier (1996) e Stinson (1995).

Com relação a uma consulta geral sobre segurança no ambiente TCP/IP, a referência RFC (2001) pode ser interessante. O material é vasto e inclui tópicos como: firewall, VPN, criptografia, segurança de serviços em geral, autenticação, autorização, contabilidade, Kerberos, Remote Authentication Dial In User Service (RADIUS), RADIUS e IPv6, Microsoft Vendor-specific RADIUS Attributes e uma série de outros documentos.

Com relação ao gerenciamento de redes, uma boa leitura pode ser Carvalho (1993); este livro representa um esforço brasileiro na área de gerência de redes através da Brisa (Sociedade Brasileira Para Interconexão de Sistemas Abertos). Quanto às RFCs sobre

gerenciamento, RFC (2001) é um fonte interessante de leitura, na qual por exemplo existe documentação do SNMP (e suas versões SNMPv2 e SNMPv3) sobre IPX, AppleTalk e OSI entre inúmeros outros documentos. Outras leituras convencionais quanto à gerência, e em especial TCP/IP, são Comer (1995), Stalling (2000).

Finalizando, Goyal (2000) e Huston (2000) são referências que podem auxiliar no estudo de desempenho. Jain (1991) é uma boa referência para aqueles com interesse na área de desempenho de uma forma mais completa.

Bibliografia

CARVALHO, T.C.M.B. *Gerenciamento de Redes – Uma Abordagem de Sistemas Abertos*. Makron Books, 1993.

COMER, D.E. *Internetworking with TCP/IP – Volume I Principles, Protocols and Architecture*. 3th ed., Prentice Hall, 1995.

GOLDREICH, O. *Modern Cryptography, Probalistic Proofs and Pseudorandomness*. Springer Verlag, 1998.

GOYAL, M. ET AL. *Performance Analysis of Assured Forwarding*, IETF Draft, Fevereiro, 2000.

JAIN, R. *The Art of Computer Systems Performance Analysis*. John Wiley & Sons, 1991.

JOYNER, D. *Coding Theory and Crytography*. Springer-Verlag, 2000.

HUSTON, G. *Internet Performance Survival Guide*. John Wiley & Sons, 2000.

KHAN, D. *The Codebreakers*. Macmillan, 1967.

KAUFMAN, C., PERLMAN, R., SPECINER, M. *Network Security*, Prentice Hall, 1995.

MASSEY, J. *An Introduction to Contemporary Cryptology*. Proceeding of IEEE, 76: (5) May 1988, IEEE Log Number 8821262.

RFC, http://www.faqs.org/rfcs/np.html, 2001.

SCHNEIER, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. John Wiley, 1996.

STALLING, W. *Local and Metropolitan Area Networks*. 6th ed. Prentice Hall, 2000.

STINSON, D.R. *Criptography Theory and Practice*. CRC Press, 1995.

TANENBAUM, A S. *Computer Networks*. 3th ed. Prentice Hall,1996.

VAN RENESSE, R., VAN STAVEREN, H., TANENBAUM, A.S. *Performance of the Worlds Fastest Distributed Operating Systems*. Operating Systems Rev., 22: 25-34, 1988.