Resumão de Redes de Computadores

Autor: Adonai Estrela Medrado (adonaimedrado@hotmail.com)

Revisado em 26 de junho de 2010

Construído tendo como referência MIRANDA, Anibal. D. A. **Módulo de introdução às redes de computadores**. Vitória: ESAB, 2008. Disponível apenas para alunos.
Este material é apenas um resumo disponibilizado para uso acadêmico e didático. Ele não pretende esgotar o assunto ou abordá-lo em sua integralidade. A sua utilidade é relembrar alguns conceitos e estimular o aprofundamento e a pesquisa.

Modelo OSI

O modelo OSI (Open System Interconnection) fornece uma base para desenvolvimento de padrões de rede. São sete as camadas deste modelo: física, enlace, rede, transporte, sessão, apresentação e aplicação. Cada camada inferior dá suporte à camada superior. O OSI delimita e isola em cada camada as funções de comunicação. As unidades básicas são quadro ou *frame* para a camada física e de enlace; pacote ou *datagrama* para a camada de rede; segmento para a camada de transporte.

Dispositivos de Rede

Os repetidores ou amplificadores, trabalham na camada física do modelo OSI e são responsáveis por diminuir os efeitos da atenuação do sinal. Enquanto os repetidores simples trabalham com uma única porta de entrada e uma única porta de saída, os *hubs* trabalham com múltiplas conexões. Os *hubs* ativos têm sua própria fonte de energia e geram novamente os bits, os passivos não têm fonte própria, não geram novamente os bits e por isto não aumentam a distância do cabo. O *bridge* faz a filtragem de pacotes da camada de enlace utilizando-se dos endereços MAC. Os roteadores são dispositivos de camada de rede que têm como finalidade escolher o melhor caminho para o tráfego de informações e interconectar LANs para formar WANs. Estes dispositivos também podem fazer a interconexão entre diferentes tecnologias da camada de enlace. Os principais protocolos de roteamento são: RIP (*Routing Information Protocol*), OSPF (*Open Shortest Path First*), IGRP (*Interior Gateway Routing Protocol*), BGP (*Border Gateway Protocol*) e EGP (*Exterior Gateway Protocol*). Os *gateways* traduzem pacotes de uma rede local para que possam atingir a rede de destino.

A função da placa de rede é adaptar o computador ao meio de transmissão. Os

modens fazem a modulação do sinal analógico em digital e vice-versa. A ADSL (*Assymmetric Digital Subscriber Line*) permite a transferência digital de dados em alta velocidade por meio de linhas telefônicas comuns. A transparência e a possibilidade de fazer chamadas de voz e utilizar a Internet ao mesmo tempo são garantidas pela transmissão da voz em baixas frequências e dos dados em altas frequências. O splitter é o aparelho utilizado para separar a voz dos dados. O DSLAM (*Digital Subscriber Line Access Multiplexer*) limita, agrupa e envia as conexões dos usuários para a rede ATM conectada à Internet.

Redes ATM

A tecnologia ATM utiliza o processo de comutação de pacotes e transmite as células ATM (pequenos blocos de tamanho fixo e estrutura definida). Cada célula carrega um endereço que determina seu destino. A conexão entre os pontos da rede ATM é feita através dos canais virtuais (VP/VC - *Virtual Path*/*Virtual Channel*). O modelo ATM possui 4 camadas: física (meios para transmissão das células ATM), ATM (construção, processamento e transmissão das células e processamento das conexões virtuais; trata o tráfego de entrada e saída), AAL e aplicação. A camada física é dividida em TC (*Transmission Convergence*) que mapeia as células e PM (*Physical Mediu*m) que temporiza os bits. A camada AAL (*ATM Adaptation Layer*) fornece serviços para a camada de aplicação e é dividida em CS (*Convergence Sublayer*) – que prepara a informação do usuário de acordo com o serviço para o ATM – e SAR (*Segmentation and Reassembly*) – que fragmenta a informação para ser encapsulada na célula ATM. As três primeiras camadas correspondem às camadas física e de enlace do modelo OSI. A rede ATM propriamente dita envolve as duas primeiras camadas. Os equipamentos ATM trabalham nas 4 camadas. Os 48 bytes úteis da célula ATM não possuem verificação ou correção de erros, estes papeis devem ser desempenhados pela aplicação. LAN Emulation é a implementação via camada de software de características de redes LAN (*Ethernet*/*Token Ring*) no nível de enlace de dados para garantir uma boa interface entre as LANs e a rede ATM. O protocolo ATM não impõe limitações físicas quanto à distância ou largura de banda.

Administração de Redes

As ferramentas que ajudam na administração da rede podem ser divididas em quatro categorias: físicas, monitores, analisadores e sistemas de gerenciamento. O

computador que será o gerente da rede precisa de um banco de dados com as informações para identificar, rastrear e resolver os problemas no menor tempo possível. O SNMP (*Simple Network Management Protocol*) é utilizado para troca de informações de gerenciamento e funciona com um esquema de gerente/agente onde o agente responde às solicitações do gerente. Ele pode ser utilizado em redes heterogêneas (com diferentes tecnologias, protocolos e sistemas operacionais). O único meio de o agente se comunicar com o gerente sem solicitação é através de uma mensagem *trap*.

Arquitetura Cliente/Servidor

A arquitetura cliente/servidor possui três componentes básicos: computador-cliente, computador-servidor e rede. As vantagens desta arquitetura está na diminuição do tráfego na rede e flexibilidade do usuário para escolher sua plataforma e sistema operacional. Suas desvantagens envolvem a dificuldade de administração, o alto custo administrativo, de pessoal, de hardware e de software.

Internet

A Internet funciona com a arquitetura cliente/servidor. Ela é uma rede de responsabilidade coletiva (não há instituição que a banque, autoridade central ou governo). Entretanto, foi o poder público americano que financiou e subsidiou a sua manutenção durante os primeiros anos. A Internet 2.0 tem por objetivo uma maior interação, facilitando a colaboração e troca de informações entre os usuários, os sites e os serviços virtuais. Dois protocolos utilizados para dar suporte às aplicação da Internet são o TCP e o UDP.

O TCP é um protocolo que no modelo OSI se localiza na camada de transporte. Garante ordem e entrega. Ele possui os seguintes estados: LISTEN, SYN-SENT, SYN-RCVD, ESTABLISHED, FIN-WAIT-1, CLOSE-WAIT, FIN-WAIT-2, LAST-ACK, TIME-WAIT, CLOSED. As mudanças de estado são acompanhadas por meio de *Flags*.

O UDP é um protocolo com menos recursos e cabeçalho menor do que o TCP. Ele é utilizado quando não são necessárias as garantias deste último. Na efetivação da comunicação logo após o **socket** e o **bind** são utilizados o **send to** e o **receive from**, não havendo **listen**, **accept** ou **connect**.

VoIP

A tecnologia de VoIP é caracterizada pela convergência de serviços de dados e

voz e utilização de tecnologias abertas. Ela provê a habilidade de fazer chamadas telefônicas e enviar FAX em redes IP. O SIP (*Session Initialization Protocol*) é um protocolo utilizado para estabelecer, modificar e terminar ligações; ele vem substituindo o H.323 (mais complexo). O IAX (Inter-Asterisk eXchange Protocol) é um protocolo (porta UDP 4569) de controle transmissão de voz e de vídeo através de redes IP; foi desenvolvido pelo criador software PBX Asterisk. Este protocolo é mais simples que o SIP e utiliza a mesma porta para administração e transferência dos dados.

Intranet e extranet

A intranet aplica as tecnologias da Internet dentro das LANs e WANs organizacionais. O conceito de onipresença (comunicação de qualquer lugar para qualquer lugar) facilita a representação de uma mesma realidade para muitas pessoas. O conceito da Internet e da intranet é de busca sob demanda e não envio da informação indiscriminadamente.

Uma extranet é uma intranet que é disponibilizada ao meio externo por acesso controlado. O acesso controlado geralmente é feito utilizando-se esquema de autenticação via usuário e senha. Geralmente há registro das visitas. Conexões seguras e criptografia permitem o comércio eletrônico B2B.

Servidores e serviços

Os tipos de servidores mais utilizados são: servidor de arquivos, servidor de impressão, servidor de rede (monitora a rede), servidor de comunicação (controle de acesso, interface e comunicação dos usuários com o servidor), servidor de *gateway*, servidor *web*, servidor de e-mail, servidor de banco de dados, servidor DNS, servidor *proxy*, servidor de imagens, servidor FTP, servidor *Webmail*. Servidores dedicados são aqueles que agem como um único tipo de servidor. Alguns servidores utilizam fonte de alimentação ininterrupta (UPS - *Uninterruptible Power Supply*).

Um *Web Proxy* provê cache de páginas da Internet. O cache pode ser limpo de acordo com dois algoritmos: *Least Recently Used* (LRU), que remove os menos utilizados considerando o tempo, e o *Least Frequently Used* (LFU), que remove os menos utilizados considerando o número de acessos. O *proxy* transparente é implementado através da técnica de *port forwarding* e obriga os usuários de uma rede a utilizarem-o podendo impor políticas de utilização e recolher dados estatísticos.

Segurança

Existe a segurança lógica e a segurança física. As ferramentas de segurança física (ou segurança computacional) envolvem *nobreaks*, alarmes, fechaduras, circuito interno de televisão e sistemas de escuta. A segurança lógica envolve softwares de segurança. A preocupação com segurança depende do conteúdo da informação. Deve-se criar um plano de segurança (preventivo) e um plano de contingências (reativo).

O *firewall* existe na forma de software e/ou de hardware e sua função é regular o tráfego de dados entre redes distintas. Ele funciona examinando se a comunicação é de entrada ou de saída e permitindo ou negando acesso a determinados tipos de serviços. O *firewall* de pacote (para redes de pequeno e médio porte) trabalham com filtragem de pacotes e, dependendo da complexidade das regras aplicadas, pode causar perda de desempenho na rede ou não ser eficaz. O *firewall* de aplicação (para redes de médio e grande porte) atua como intermediadores e são conhecidos como proxy. Este tipo de *firewall* é mais seguro e complexo do que o *firewall* de filtragem, pois permite o acompanhamento preciso do tráfego.

Como boas práticas de segurança em redes *wireless* pode-se citar: habilitar e configurar a encriptação, desligar o *broadcast* do SSID e/ou alterar seu valor padrão ocultando a marca e modelo do aparelho, mudar a senha de administrador, filtrar por MAC, reduzir a intensidade do sinal ao mínimo necessário e bloquear portas e protocolos não utilizados.