Redes de Computadores

Sinais Analógicos e Digitais

Os tipos de sinais utilizados na comunicação podem ser divididos em dois: Analógicos e digitais.

Em redes de computadores esses dois sinais também estão presentes nos tipos de transmissão e determinam a qualidade do serviço.

Sinal Analógico

Segundo Tanenbaum (2003), os sinais analógicos são ondas eletromagnéticas que assumem infinitos valores ao longo do tempo. Esse sinal é representado por uma onda senoidal com as seguintes características:

- **Amplitude:** Representa intensidade mais alta dos sinais elétricos (volts).
- **Frequência:** É medida em hertz, define a quantidade de ciclos em um intervalo de tempo.
- **Fase:** Define o formato da onda senoidal, pode ser medida em graus ou radianos.

Sinal Digital

Em contrapartida, o sinal digital é representado por 0 e 1, ou seja, é um sinal binário. A representação dos seus valores é dada como discreta ao longo do tempo e amplitude. Então, é possível diminuir a taxa de oscilação, fenômeno este responsável pelo aumento na qualidade de serviço. Quando ocorre uma transmissão de dados, ocorre um processo de codificação (digitalização) desse sinal. Com isso, os sinais digitais:

- Não sofrem degradação dos serviços por interferência ou ruídos.
- Pode ser transmitida maior quantidade de informações.

Esses sinais em uma transmissão feita por uma internet cabeada (oferecida pelas operadoras), em que se pretende acessar um site a partir de um dispositivo, ocorrem da seguinte forma:

1. Os modems fornecidos pelas operadoras fazem a adequação do sinal digital com o meio disponibilizado pela operadora.
2. O modem recebe os sinais emitidos pelo computador (entende-se notebook, tablet e smartphone) e os coloca no meio de transmissão fornecida pela operadora (processo conhecido como modulação).
3. Ao chegar ao destino, é efetuado o processo inverso.

Os modos de transmissão dos sinais nas redes de comunicação de dados podem variar conforme o sentido em que ocorrem as trocas de mensagens, o número de bits enviados simultaneamente e a sincronização entre computador e servidor.

Componentes de Uma Rede

Para estruturar as redes, existem alguns componentes de hardware que são básicos, porém essenciais para prover a comunicação entre os dispositivos. Entre eles podemos citar:

- Placas de rede.

- Modem.
- Hub.

Placas de Rede

O controlador de interface da rede (NIC – Network Interface Controller) pode estar ou não integrado à placa-mãe.

A arquitetura de seu barramento pode ser na forma PCI, PCI Express, ISA, e USB, ou seja, o formato de encaixe na placa-mãe. A sua função lógica é efetuar o tratamento de endereçamento no envio e recebimento das mensagens.

Modem

O modem tem a função de fazer a modulação e demodulação das mensagens, e também é conhecido como transceptor.

Em sua forma analógica, os dados são transmitidos pelo canal de voz, já na sua forma digital, é feita a codificação da banda base. Esse equipamento está entre os mais populares dos hardwares encontrados nas redes.

Hub

O hub pode conter várias linhas de entrada que são responsáveis por distribuir conexão. Esse equipamento assume o papel de um repetidor, pois a mensagem ao chegar é replicada para todas as portas.

Pode ter o comportamento de repetidor dentro de uma rede e pelo motivo de replicar uma mensagem para todos os dispositivos conectados a ele, deve-se evitar o cascateamento.

Tipos de Rede Intranet e Extranet

Em uma rede privada os recursos e sistemas compartilhados ficam restritos à organização e podem estar estruturados de duas formas:

- **Intranet:** Compreende uma rede privada que utiliza em uma estrutura física e lógica o módulo de internet. No entanto, os serviços de rede, como servidores de arquivos e impressão, servidor web e as aplicações são de uso interno.
- **Extranet:** Conhecida popularmente como internet. A diferença é que os recursos só podem ser acessados com autorização de um administrador da rede de uma companhia.

Topologias de Rede

As redes utilizadas diariamente possuem em suas infraestruturas alguns equipamentos essenciais para prover a comunicação entre os dispositivos, independentemente da sua localização geográfica. Tais equipamentos e as suas respectivas configurações são imperceptíveis para o usuário final, porém o desempenho dos seus serviços pode ser sentido (positivamente ou negativamente). Nessa aula você verá:

- Roteador.
- Switch.

- Bridges (Pontes).
- Gateway.

Roteador

O roteador forma tabelas lógicas dos equipamentos disponíveis nas redes, como roteador, switch, computadores, dispositivos móveis, impressoras IP e câmeras IP. Para auxiliar nesse processo é utilizado um mecanismo de descoberta de dispositivos “vizinhos”, que é efetuado por roteadores e switches por meio de protocolos de comunicação:

- **ICMP:** Esse protocolo faz o diagnóstico da rede, bem como relata os erros de recebimento de pacotes e no informe de características da rede.
- **ARP:** Efetua o mapeamento dos endereços físicos (MAC) por meio do endereço lógico.
- **RARP:** Faz o inverso do ARP, associando um endereço lógico ao físico.

Dessa forma, um roteador envia periodicamente um protocolo de atualização de vizinhança aos roteadores conhecidos, e um vai enviando a atualização aos outros sucessivamente, fazendo com que a tabela lógica de endereçamento dos equipamentos continue sempre atualizada.

Segundo Kurose (2006), o roteador (sem fio) recebe a mensagem pela porta de entrada, repassa o pacote para o processador que efetua o roteamento, no qual ocorre a análise do endereçamento destino, e encaminha para a porta de saída, apontando a interface de rede (placa Ethernet).

Switch

Esse tipo de equipamento é comumente encontrado em empresas, faculdades, ou seja, redes que necessitam maior número de dispositivos. Quando a mensagem chega a uma das interfaces de rede, o sistema do equipamento lê o endereço destino do cabeçalho e envia para a interface apropriada. Switches normalmente possuem diversas portas.

Bridges (Pontes)

Quando o administrador de redes necessita conectar duas redes distintas, uma solução viável pode ser utilizada – as bridges (pontes). Esse tipo de equipamento possui características muito parecidas com o switch. Porém, as suas aplicações em uma infraestrutura são bem distintas.

Enquanto o switch é utilizado para conectar dispositivos da rede, a bridge é utilizada para inteligar duas redes (LAN). Mas nada impede que o administrador utilize o switch para interligar duas redes, desde que devidamente configurado e planejado.

A vantagem em se utilizar as bridges é que a sua configuração é mais simples, necessitando apenas apontar o endereço das interfaces dos equipamentos das redes que estão sendo conectadas. Já ao se utilizar o switch, o ganho no processamento das informações pode proporcionar um ganho de desempenho na comunicação entre os dispositivos de redes distintas.

Gateway

Este conceito está diretamente ligado a um termo muito utilizado por profissionais de redes de computadores, que é “borda de rede”.

O gateway pode ter funções específicas nas redes, dependendo do planejamento do administrador de redes. Entre elas, podemos destacar:

- **Direcionamento:** No qual todas as mensagens são enviadas para o nó da rede, podendo ser roteador ou switch.
- **Proxy:** Uma lista de sites cujo acesso é ou não permitido por meio dos dispositivos da rede interna.
- **Firewall:** Um dispositivo de segurança que verifica o conteúdo dos pacotes e efetua seu bloqueio, quando nocivo aos serviços disponíveis na rede.

Protocolos e Serviços de Rede

Padronizar a forma das pessoas de se comunicarem pode garantir que as informações sejam passadas e compreendidas de forma correta. Os processos necessários para a padronização podem variar conforme o tipo de aplicação ou entidade que fará os estudos e análises.

As entidades que efetuam esse tipo de trabalho estão espalhadas pelos continentes. Explore a galeira e conheça-as em destaque:

- **ISO (Internacional Organizantion for Standardization):** Organização não governamental responsável pela padronização, sendo dividida em:

- **ANSI (American National Starndards Institute).**
- **ABNT (Associação Brasileira de Normas Técnicas).**
- **ANFOR (Associação Francesa).**
- **DIN (Associação Alemã).**
- **EIA (Eletronic Industries Association):** Grupo que visa a padronização das transmissões elétricas.
- **IEEE (Institute of Eletrical and Eletronics Engineers):** A maior organização internacional de desenvolvimento e padronização nas áreas de engenharia elétrica e computação.
- **ITU-T (Telecommunication Standardization Sector):** Entidade responsável pela padronização dos assuntos relacionados a telecomunicações.

Segundo Tanenbaum (1997), o desejo da ISO era desenvolver um modelo para interconexão de sistemas abertos. Para isso, foi desenhado um modelo em sete camadas que deveriam atender os seguintes requisitos:

- A função das camadas deve ser escolhida em razão dos protocolos que foram padronizados.
- Cada camada deve executar a função a qual foi destinada.
- Os limites entre as camadas devem ser escolhidos de forma que minimize os esforços ao fluxo das mensagens pelas interfaces.
- O número de camadas deve ser do tamanho suficiente para alocar todas as funcionalidades possíveis nas redes.

Segundo Tanembaum (1997), o modelo de referência OSI efetua todos os processos necessários para que ocorra a transmissão de dados, fazendo com que as camadas (ou layers) nele existentes efetuem a divisão dos processos lógicos.

Dessa forma, a ISO desenvolveu o modelo de referência OSI (Open Systems Interconnection – Sistemas Abertos de Conexão), que foi um marco para o desenvolvimento dos protocolos de

comunicação que são utilizados nos serviços consumidos diariamente pela internet. A arquitetura do modelo é a seguinte:

7	Aplicação
6	Apresentação
5	Sessão
4	Transporte
3	Rede
2	Enlace
1	Física

A partir de 1984, os fabricantes de hardware e desenvolvedores de softwares entenderam que o modelo proposto em camadas tinha como intuito permitir a interoperabilidade entre equipamentos de diferentes origens, o que poderia dar uma vantagem competitiva no mercado, abrindo espaço para parcerias e novos desenvolvimentos.

O Modelo de Referência ISO/OSI

Hierarquia e Interfaces dos Protocolos nos Serviços de Redes

Segundo Tanenbaum (1997), assim como determina o modelo de referência OSI, os protocolos são organizados em pilhas ou camadas. Porém, em todas as redes, a função primordial é fornecer serviços às camadas superiores.

Para isso, o mecanismo utilizado faz com que a camada “n” de um dispositivo se comunique com a camada “n” de outro dispositivo. Basicamente, o protocolo efetua a “negociação” entre as partes para que seja provida a comunicação.

Quando os dados são transferidos, cada camada processa o seu serviço respectivo. Para que isso ocorra, a cada par de camadas existe uma interface responsável por definir as operações e os serviços que a camada inferior tem que encaminhas à layer superior.

Conheça os protocolos definidos por Tanenbaum:

- **HTTP:** Trata-se de um protocolo utilizado para acessar conteúdo web na rede mundial de computadores. Permite que ocorra a transferência ponto a ponto entre clientes e servidores de serviços do tipo elástico e streaming multimídia.
- **SMTP:** É o protocolo utilizado para efetuar o envio e recebimento de e-mail de um servidor a outro.
- **SSH:** Esse protocolo é utilizado para se efetuar acesso remoto em outro dispositivo, por meio de um terminal, assim como o prompt de comando do DOS. A grande diferença das outras técnicas (Telnet e RSH) de acesso remoto está na segurança. Ao fazer um acesso remoto em um dispositivo, a transmissão de dados recebe uma criptografia que pode variar conforme o algoritmo de encriptação das mensagens, garantindo assim a integridade do que é compartilhado.
- **RTP:** É o protocolo de transporte utilizado na camada de aplicação para prover streaming de áudio e vídeo.

- **SIP:** Apesar deste protocolo não pertencer à camada de aplicação e sim à de sessão, vale ressaltar seu grau de importância para os serviços multimídia. Este protocolo é responsável pela criação, modificação e finalização de sessões de transferência de arquivos de serviços multimídia.
- **POP3:** Essa expressão pode ser traduzida como protocolo de correio, já disponível em sua terceira versão. Ele permite que o usuário descarregue as mensagens que estejam localizadas em um servidor de e-mail em seu dispositivo. Essa ferramenta permite o recebimento das mensagens, mas não o envio.
- **IMAP:** Este protocolo, assim como ocorre com o POP3, sincroniza as mensagens que estão alocadas em um servidor de e-mail. Entretanto, o IMAP se mantém conectado, a fim de sincronizar, em tempo real, as mensagens recebidas.
- **NTP:** Ele tem como função sincronizar os relógios dos servidores, roteadores e computadores das redes.

A hierarquia dos domínios é dividia em três categorias:

- **Domínio Genérico:** São definidos com os registros conforme o segmento do site, podendo ser: .com, .net, .org, .edu, .gov, entre outros.
- **Domínio de Países:** É utilizada a abreviatura com dois caracteres para identificar em qual país o domínio foi registrado, podendo ser: .br, .us, .ar, entre outros.
- **Domínio Reverso:** Faz o processo reverso a consulta ao servidor DNS. Quando um servidor recebe uma solicitação, é feita uma consulta em sua “tabela”, que por sua vez encaminha o pedido do cliente ao servidor relacionado à URL digitada pelo usuário, sendo utilizado o endereço IP.

O Protocolo TCP/IP

Filippetti (2008) afirma que o padrão TCP/IP foi desenvolvido pelo DOD (Departamento de Defesa dos EUA) para garantir a integridade das mensagens enviadas em caso de guerra. Isso é compreensível, pois, em razão do envolvimento em diversos conflitos ao longo dos tempos, o exército necessitou de técnicas relacionadas à comunicação.

A arquitetura do protocolo TCP/IP foi desenvolvida em quatro camadas, e um conjunto de processos – ou aplicações – e utilizado para prover diversos serviços. Para compreender suas camadas, observe a tabela abaixo, que compara o modelo de referência OSI e o protocolo TCP/IP:

OSI	TCP/IP
Aplicação	Aplicação
Apresentação	
Sessão	
Transporte	Host-to-Host
Rede	Internet
Enlace	Acesso à Rede
Física	

Para isso, podemos definir a função de cada uma das camadas do protocolo TCP/IP como:

- **Aplicação:** Nesta camada define-se como os programas vão se comunicar com as diversas aplicações disponíveis nas redes. Ainda é de responsabilidade desta camada efetuar o gerenciamento da interface pela qual o usuário vai interagir com a aplicação.
- **Transporte (Host-to-Host):** É idêntica à camada de transporte do modelo de referência OSI, ou seja, responsável por prover, gerenciar e encerrar uma conexão ponto a ponto. Ao efetuar o gerenciamento da conexão, visa-se garantir a integridade dos dados pelo sequenciamento dos pacotes segmentados para efetuar o envio/recebimento das mensagens.
- **Rede (Internet):** Tem o mesmo objetivo da camada de rede do modelo de referência OSI, sendo responsável por definir o endereçamento dos dispositivos por meio do IP e garantir o roteamento dos pacotes nas redes.
- **Física (Acesso à Rede):** Desempenha a mesma função das camadas de enlace e física do modelo de referência OSI. Efetua o monitoramento do tráfego e analisa o endereçamento de hardware antes da transmissão pelo meio físico.

Podemos destacar algumas semelhanças entre o modelo OSI e o protocolo TCP/IP:

- Divisão em camadas.
- As camadas de transporte e rede são equivalentes.
- A comutação de pacotes é definida no modelo e efetuada no protocolo.
- Os profissionais de redes necessitam conhecer ambos.

Redes e Sub-Redes

O endereçamento IP e as suas técnicas de sub-redes são um dos mais importantes tópicos relacionados à rede de computadores.

Nesta aula, você conhecerá os principais conceitos da versão 4 do protocolo, o IPv4, além de obter informações sobre notação e classes de endereço.

Segundo Kurose (2006), o Internet Protocol, ou simplesmente IP, é o endereço lógico feito para que um dispositivo possa se comunicar com qualquer outro dispositivo, independentemente de sua localização geográfica. O protocolo está definido na camada de rede, sendo o seu pacote denominado datagrama.

A notação de um endereço IP é separada por ponto, fazendo com que uma parte identifique a rede (net), e a outra, o dispositivo (host).

Tendo como exemplo o endereço: 172.16.30.110, temos:

- **172.16:** Identificam a qual rede o dispositivo pertence.
- **30.110:** Identificam o endereço do dispositivo.

Segundo Kurose (2006), os endereçamentos utilizados nas redes foram divididos em classes, para utilização conforme o número de dispositivos da rede. Veja a correspondência de cada uma delas:

- **Classe A:** Rede-Host-Host-Host, intervalo de 0 a 127.
- **Classe B:** Rede-Rede-Host-Host, intervalo de 128 a 191.
- **Classe C:** Rede-Rede-Rede-Host, intervalo de 192 a 223.
- **Classe D:** Reservada para endereços de multicast.
- **Classe E:** Reservada para pesquisa.

Além da divisão por classes, a utilização deve obedecer:

- **IP para Rede Privada:** Números de IP reservados para utilização dentro das LANs, sendo utilizados os seguintes endereçamentos nos seguintes intervalos: Classe A de 10.0.0.0 a 10.255.255.255, Classe B de 172.16.0.0 a 172.31.255.255 e Classe C de 192.168.0.0 a 192.168.255.255.
- **IP para Rede Pública:** São faixas de números de IP utilizados para dispositivos acessíveis pela internet. Por exemplo, os servidores como o 201.55.233.117 (endereço do site google.com.br).

Ethernet

Nesta aula, você conhecerá os conceitos básicos sobre redes Ethernet e como são definidas suas velocidades de transmissão de dados.

Segundo Filippetti (2008), o tipo de tecnologia aplicada ao cabeamento dita a velocidade que cada um deles pode atingir. Clique nas abas e conheça as mais utilizadas nas aplicações IEEE 802.3:

- **Fast Ethernet:** Definida como IEEE 802.3u, que permitiu que a velocidade de transmissão atingisse 100 megabits. É encontrada como: 100Base-TX, 100Base T e 100Base-FX.
- **Gigabit Ethernet:** Dez vezes superior à Fast Ethernet, essa versão permite velocidades de transmissão de até 1000 megabits. O padrão foi definido como 802.3z, possibilitando quatro tipos possíveis: 1000Base-LXX, 1000Base-SX, 1000Base-CX e 1000Base-T.
- **10 Gigabit Ethernet:** Da mesma forma como ocorreu na versão anterior, esse padrão multiplicou a sua capacidade em 10 vezes, permitindo atingir uma velocidade de 10 Gigabit Ethernet, também conhecido como 10G. Entre as opções estão as tecnologias: 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-SR, 10GBase-LRM e 10GBase-CX4.

Métodos de Transmissão Ethernet

Tanembaum (1997) define que as comunicações desse tipo de rede são efetuadas pelo protocolo Carrier Sense Multiple Access with Collision Detection (CSMA/CD), permitindo que qualquer dispositivo da rede possa efetuar uma transmissão sem hierarquizar quem tem prioridade.

Basicamente, para o funcionamento do protocolo, os dispositivos verificam se não há nenhuma comunicação ocorrendo para assim fazer uma transmissão. Caso acorra de dois dispositivos emitirem, simultaneamente, uma mensagem um para o outro, uma colisão acontece e a transmissão é interrompida, sendo retomada em um tempo aleatório.

IPv6

O IPv6 surgiu da necessidade de se obter mais endereços IP, em virtude do esgotamento do protocolo IPv4, gerado pelo aumento do acesso à internet nos novos serviços multimídia multiplataformas (smart TV, celular e videogames) e pela popularização da internet móvel.

Nesta aula, vamos conhecer as principais características desse novo protocolo e suas diferenças em relação à versão anterior.

Inicialmente, o IPv6 surge no cenário de redes de computadores para suprir as necessidades do IPv4.

Segundo Tanembaum (1997), o novo protocolo deve:

1. Resolver a escassez de endereços.
2. Simplificar o cabeçalho, facilitando o processamento dos pacotes e o aumento da velocidade do envio/recebimento.
3. Tornas os campos obrigatórios do cabeçalho como opcionais, facilitando, assim, o roteamento dos pacotes.
4. Garantir a segurança das transmissões, tornando o IPSec obrigatório.

O endereçamento do protocolo IPv6 possui 128 bits, enquanto o IPv4 possui apenas 32 bits. Isso possibilita 2^{128} endereços disponíveis, ou ainda, 340 undecilhões.

Segundo Hagen (2002), IPv6 e IPv4 coexistirão por muitos anos. Veja alguns dos impactos previstos por Tanembaum (1997) nesse longo período de transição:

- **Falhas:** Os administradores devem efetuar um plano de contingência para que as redes continuem operando com IPv4 e IPv6.
- **Contabilização:** Deve-se recalcular os limites de utilização dos recursos, pois, com os dois protocolos em operação, o consumo muda em relação às redes somente com IPv4.
- **Configuração:** Para permitir que os dois protocolos possam conviver nas redes, é necessário diversas configurações.
- **Desempenho:** Com a mudança de cenário (redes com os dois protocolos operando), o desempenho da rede necessita de adaptações para garantia do acordo de nível de serviço (Service Level Agreement – SLA).
- **Segurança:** O administrador deve optar por alguma técnica que garanta a interoperabilidade, sem que gere riscos à segurança da rede e/ou usuários.

Teoria da Gerência de Redes e Padrões

Você já viu como as redes são planejadas no nível físico e lógico, agora vamos nos aprofundar no estudo das técnicas de gerenciamento utilizadas para garantir o funcionamento correto dos serviços.

Esse gerenciamento é essencial para garantir o perfeito funcionamento das redes, que estão ficando cada vez maiores e mais complexas, e com um alto nível de integração entre dispositivos.

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.

Ainda segundo Kurose Apud Saydam (1996), “as atividades de gerenciamento de redes visam oferecer, integrar e coordenar os elementos de hardware, software e usuários. A fim de se monitorar, testar, consultar, configurar, analisar, avaliar e obter o controle dos recursos da rede, para que sejam atendidas as necessidades peculiares de cada rede, com um custo razoável”.

Kurose (2006) acredita que existem três princípios para que o gerenciamento tenha elementos que garantam o seu funcionamento:

- **Coleta de Dados:** Definida como a parte do processo responsável por coletar automaticamente dados parametrizados pelo administrador de redes. Nessa seção será vista a técnica definida como sniffing.

- **Controle:** Após o diagnóstico correto do problema, deve-se tomar ações a fim de se cessar, mitigar ou minimizar os impactos. Posteriormente, o administrador de redes deve ter o controle para que o mesmo evento não comprometa a qualidade ou funcionamento da rede e/ou serviços.
- **Análise e Diagnóstico:** Consiste em organizar os dados coletados, a fim de se gerar informações que permitam a tomada de decisão. A análise pode ser feita manualmente, ou por softwares de tratamento de dados. O diagnóstico correto do problema permite que seja feita a correção no menor tempo possível.

Realizar essa atividade de forma eficiente requer seguir padrões de qualidade. Pensando nisso, a ISO (Internacional Organization for Standardization), desenvolveu um modelo de gerenciamento de redes divididos em cinco áreas:

- **Desempenho:** Seu objetivo é quantificar, medir, informar, analisar e controlar o desempenho de dispositivos, serviços e segurança.
- **Falhas:** Visa registrar, detectar e reagir às falhas ocorridas nas redes, tendo como maior compromisso tratar de imediato as falhas transitórias da rede. Isso ocorre diariamente, quando ocorrem interrupções de serviços, hospedagem, falha de hardware e software de nodos.
- **Configuração:** Permite que o administrador saiba quais os dispositivos utilizados na rede, e as suas respectivas configurações. Nessa área de gerenciamento estão contidos o planejamento dos IPs e suas sub-redes.
- **Contabilização:** Permite a especificação, o registro e controle de acesso (para usuários e dispositivos). Também estão definidas as quotas de utilização (balanceamento de carga conforme prioridade).
- **Segurança:** Efetua o controle de acesso aos recursos via mecanismos de segurança (chaves), métodos de mascaramento de mensagens (criptografia) e com políticas de prevenção e segurança.

Os equipamentos e softwares evoluem constantemente, mas, mesmo utilizando tecnologia de última geração, não estão imunes a erros.

Por isso, todo sistema crítico para um negócio deve ser frequentemente monitorado para evitar interrupções que prejudiquem as atividades da empresa.

Gerência de Falhas e Segurança

Você certamente já se deparou com alguma dessas situações:

- Eco da sua voz ao utilizar serviço de telefonia celular.
- Áudio e vídeo de programas de TV fora de sincronismo durante a transmissão.

Mesmo quando são feitos exaustivos testes de erros ou de stress da rede, tais ocorrências ainda podem aparecer nas estruturas das redes de computadores.

Segundo Comer (2007), qualquer sistema de comunicação de dados é suscetível a falhas e erros, podendo ocorrer em dispositivos físicos, ou em falha de transmissão. Os erros de transmissão são divididos em três categorias:

- **Interferência:** São radiações eletromagnéticas que, quando geradas, podem causar ruído e, consequentemente, degradar os sinais de rádio ou os sinais que trafegam pelo meio cabeado.
- **Distorção:** Normalmente os dispositivos físicos de transmissão como os cabos fazem a distorção dos sinais. O excesso de distorção de sinais pode causar desde a degradação do serviço, até a perda de sinal.
- **Atenuação:** Em meios não guiados, a atenuação se dá quando o sinal necessita atravessar barreiras físicas (parede, vidro, fibra, etc.), e pela distância do receptor da antena. Já no meio guiado, a distância é o fator de degradação dos serviços.

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. Para efetuar o tratamento desses erros, existe uma relação de custo-benefício, pois é adicionada uma sobrecarga no processo de transmissão.

Os erros de transmissão podem afetar os dados de três formas:

- **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.

Erro em Único Bit

Observe que o quinto bit foi transmitido com o valor “0”, e recebido como “1”. O erro de um único bit (single-bit-error) causa uma degradação com menor duração. Porém, dependendo do que está sendo transmitido, pode ser mais ou menos degradante:

- 00000010
- 00001010

Erros em Rajada

Os erros em rajada podem ocorrer sem que sejam em bits consecutivos. Para contabilizá-los, após a ocorrência de um erro, agrupa-se um bloco de oito bits. Pode-se observar que ocorreram quatro erros.

- 00101000 10110000 00100110
- 00101000 01111010 00100110

Os erros em rajada possuem um tempo de duração maior em relação ao erro em único bit. Normalmente, a degradação do serviço pode ser sensível tanto nas transmissões streaming, quanto elástico.

Detectados os erros, é necessário efetuar sua correção, mas para isso o número de bits corrompidos deve ser determinado:

- **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 que o emissor realize o reenvio da mensagem. Esse processo se repete até que esteja livre de erro.

Saber identificar os diferentes tipos de erro é essencial para realizar o gerenciamento de redes, para que você possa tomar as ações corretivas necessárias para corrigi-los de forma rápida e eficiente.

Gerência de Desempenho, Configuração e Contabilização

Você já viu como as falhas e erros que ocorrem nas redes de computadores podem degradar os serviços disponíveis nas infraestruturas.

Gerenciar o tráfego de informações exige que se garanta a qualidade mínima do processo.

Para suprir essa necessidade, é necessário implementar uma política de qualidade de serviço (QoS ou Quality of Service, em inglês), que conheceremos em mais detalhes a seguir.

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.

Os fatores que interferem diretamente na qualidade de transmissão são: A latência, o jitter, perda de pacotes e a largura de banda disponível.

Para que sejam atendidas as necessidades das redes, são utilizados dois modelos de qualidade de serviço, o IntServ e DiffServ:

- **IntServ:** Utiliza o fluxo dos dados por meio do protocolo no caminho que a mensagem deve percorrer. Possui serviço garantido no envio/recebimento de mensagens fim a fim, e o controle (balanceamento) de carga.
- **DiffServ:** Conhecido como serviços diferenciados, se baseia em uma marcação no pacote para classificá-los e efetuar os tratamentos necessários de forma independente. Esse modelo é altamente adotado por fabricante de equipamentos IPv6.

As configurações de computadores, roteadores, switches, impressoras, entre outros equipamentos, dependem de algumas características para atender os requisitos de qualidade:

- **Serviços:** As configurações de equipamento dependem do tipo de serviço que está sendo utilizado na rede, por exemplo, VoIP, videoconferência, aplicações web, etc.
- **Dispositivos:** Cada fabricante de equipamentos possui uma forma própria de configuração, capacidade de processamento, suporte, e demais características técnicas.

A configuração e padronização de procedimentos pode auxiliar os profissionais de tecnologia da informação no gerenciamento das redes de computadores à medida que define padrões de controle e parâmetros que facilitam seu monitoramento.

Dessa forma, é possível garantir a qualidade dos serviços e a disponibilidade da rede.