

Técnico em Informática

Redes de Computadores

Silvio Bandeira
Dailson Fernandes

2013



Presidenta da República
Dilma Vana Rousseff

Governador do Estado de Pernambuco
Eduardo Henrique Accioly Campos

Vice-presidente da República
Michel Temer

Vice-governador do Estado de Pernambuco
João Soares Lyra Neto

Ministro da Educação
Aloizio Mercadante Oliva

Secretário de Educação
José Ricardo Wanderley Dantas de Oliveira

**Secretário de Educação Profissional e
Tecnológica**
Marco Antônio de Oliveira

Secretário Executivo de Educação Profissional
Paulo Fernando de Vasconcelos Dutra

Diretor de Integração das Redes
Marcelo Machado Feres

Gerente Geral de Educação Profissional
Luciane Alves Santos Pulça

Coordenação Geral de Fortalecimento
Carlos Artur de Carvalho Arêas

Gestor de Educação a Distância
George Bento Catunda

Coordenação do Curso
João Ferreira

Coordenação de Design Instrucional
Diogo Galvão

Revisão de Língua Portuguesa
Letícia Garcia

Diagramação
Izabela Cavalcanti



Sumário

INTRODUÇÃO.....	3
1.COMPETÊNCIA 01 A COMUNICAÇÃO E AS REDES DE COMPUTADORES.....	5
1.1 Objetivo.....	5
1.2 Comunicação	5
1.2.1 Componentes da Comunicação	6
1.2.2 Fluxo de Dados	6
1.3 Redes	7
1.3.1 Topologias de Rede	9
1.3.1.1 Mesh (malha)	9
1.3.1.2 Topologia em Estrela	10
1.3.1.3 Topologia em Barramento	12
1.3.1.4 Topologia em Anel	13
1.3.1.5 Topologia Híbrida.....	15
1.3.2 Modelos de Rede	16
1.3.2.1 LAN	16
1.3.2.2 MAN	17
1.3.2.3 WAN	18
1.4 A Internet	19
1.5 Dispositivos de interconexão	21
1.5.1 Repetidores	21
1.5.2 HUBS.....	22
1.5.3 Bridge	23
1.5.4 Switch.....	24
1.5.5 Roteador.....	25
1.5.6 AP – Access Point	26
1.5.7 Placa de Rede	27
1.6 Resumo.....	28
2. COMPETÊNCIA 02 PROTOCOLOS DE COMUNICAÇÃO	30
2.1 Objetivos	30
2.2 Modelo OSI.....	33
2.3 O Modelo TCP/IP	36



2.4 Modelo OSI X TCP/IP	40
2.5 Estudo das Camadas.....	41
2.5.1 Camada de Rede	42
2.5.2 Camada Internet	42
2.5.3 IP: Protocolo Internet.....	43
2.6 Camada de Transporte e Aplicação.....	57
2.6.1 Comunicação Entre Processos	59
2.6.2 Protocolo UDP (User Datagram Protocol).....	61
2.6.3 Protocolo TCP (Transmission Control Protocol).....	62
2.6.4 DNS (Domain Name Service).....	63
2.7 Configurações de Redes no Windows	66
2.7.1 Acessando a Configuração de Rede no Windows	67
2.7.2 Resumo.....	76
3. COMPETÊNCIA 03 A CAMADA FÍSICA E SUAS APLICAÇÕES.....	80
3.1 Objetivos	80
3.2 Transmissão Analógica e Digital.....	80
3.3 Indicadores de Desempenho.....	86
3.4 Meios de Transmissão.....	87
3.4.1 Meios Guiados.....	88
3.4.2 Cabeamento Estruturado.....	102
3.5 Projeto de Redes	115
3.6 Resumo.....	121
REFERÊNCIAS	124
MINICURRÍCULO DO PROFESSOR.....	125



INTRODUÇÃO

Prezado (a) Aluno (a)

Convido você a entrar nesta maravilhosa e desafiante disciplina de Redes de Computadores. Com certeza, o seu olhar para o mundo da Tecnologia da Informação irá mudar radicalmente. Nesta disciplina, você entenderá como funciona todo o fascinante conjunto computacional, envolvendo os equipamentos e dispositivos que são capazes de se comunicar uns com os outros nesta operação.

Além disso, você passará a conhecer toda a estrutura da rede de computadores que fornece serviços desde uma pequena corporação até grandes redes de computadores. Você irá descobrir que a base é a mesma.

Hoje, o mercado está sedento de profissionais que dominem esta tecnologia. Tenho certeza de que você terá sucesso não só neste curso, mas levando o conhecimento para o crescimento de todos!

Não tenha como base apenas este caderno. Use todos os vídeos e sites propostos neste material. As tarefas trazem a realidade do mercado e deixarão você pronto para enfrentar novos desafios.

Estudaremos uma parte de fundamental importância na área de computação. Este ramo é, por si só, uma das principais subdivisões da informática, e há grande carência no mercado de profissionais que o dominem. Além disso, os conhecimentos fundamentais que serão apresentados constituem um grande diferencial, mesmo para quem atua em outras áreas da computação, como, por exemplo, bancos de dados, desenvolvimento de software e multimídia.

A informação é o bem mais valioso da humanidade. Nós, como profissionais da área de T.I. (Tecnologia da Informação), devemos conhecer bem as tecnologias que manipulam as informações. O transporte, a segurança e o



armazenamento de dados são tarefas inerentes à profissão e conhecer os melhores meios e métodos faz parte da nossa jornada nesta disciplina.

Desde que a informação foi, finalmente, reconhecida como a coisa mais importante em qualquer área, vivemos num mundo em que a comunicação se tornou a ferramenta mais importante para lidar com as pessoas. A comunicação faz com que possamos usufruir de todo o potencial das informações.

Nesse sentido, estudaremos os princípios fundamentais da comunicação entre computadores, como a divisão em camadas. Ela é compartilhada por diversas disciplinas do currículo e é importante para as redes de computadores. Também é responsável por nortear a elaboração de grande parte da literatura na área, incluindo este material que você tem em mãos. Em cada semana, estudaremos os tópicos de uma ou mais dessas camadas.

A disciplina está dividida em três volumes. No primeiro, veremos os conceitos básicos de comunicação e equipamentos de redes. No segundo, abordaremos os protocolos de comunicações e suas principais características. Na última semana, estudaremos os componentes do cabeamento estruturado, parte essencial das redes de computadores.

Bons Estudos!

Competência 01

1. COMPETÊNCIA 01 | A COMUNICAÇÃO E AS REDES DE COMPUTADORES

1.1 Objetivo

Compreender o que é a comunicação e seus principais componentes.

1.2 Comunicação

Vamos iniciar esta competência falando sobre o bem mais precioso da humanidade atualmente: A informação. A “era da informação” chegou para ficar. A única maneira de se conseguir sucesso em qualquer profissão é através do conhecimento e manipulação das informações. Assim como qualquer mercadoria, a informação tem um tempo de vida útil e a velocidade com que temos acesso a ela é decisiva.

Tomemos o computador isoladamente, como era comum nos primeiros anos em que a computação foi popularizada. Este computador, mesmo sem se comunicar através de uma rede, é uma ferramenta de manipulação de informações, nada mais. Por que, então, sempre houve uma demanda de capacidade e velocidade nos computadores, muito acima do que os fabricantes conseguem fornecer? Por que, caro (a) aluno (a), sempre ansiamos por computadores mais rápidos e com mais recursos? Acontece que as informações são tão fundamentais para nossas atividades que nunca estamos satisfeitos com a quantidade e velocidade com que podemos captar, manipular e gerar novas informações, subsidiando todas as nossas decisões.

A partir do momento em que conseguimos comunicação entre computadores, principalmente a longas distâncias, conseguimos ampliar essas ações. Resultado? Progresso em todas as áreas da atividade humana como nunca se viu na história.



Mídias Integradas:

Veja o Filme “A Rede”. Ele demonstra o poder da conexão atual de tudo e de todos. Nele você verá que mesmo sem você querer, você está na grande rede: A Internet.
Recomendadíssimo!
www.imdb.com/title/tt0113957/.

Competência 01



1.2.1 Componentes da Comunicação

Vamos conhecer agora o que o renomado autor na área de Tecnologia da Informação, Forouzan, cita no seu livro “Comunicação de Dados e Redes de Computadores”, os cinco componentes do sistema de comunicação:

- **Mensagem** – a informação (dado) a ser transmitida. Formatos comuns à informação abrangem figuras, sons, vídeos e texto;
- **Emissor** – o agente que envia a informação. Pode ser uma pessoa ou um equipamento;
- **Receptor** – o agente que recebe a informação;
- **Meio de transmissão** – todo aparato físico por onde a mensagem trafega durante a comunicação. Pode ser o próprio ar, quando nos comunicamos através da fala; ou meios mais pesados, como os cabos na comunicação entre computadores (os equipamentos em si);
- **Protocolo** – conjunto de regras que regem a comunicação. Deve ser de conhecimento, obrigatoriamente, do emissor e do receptor.

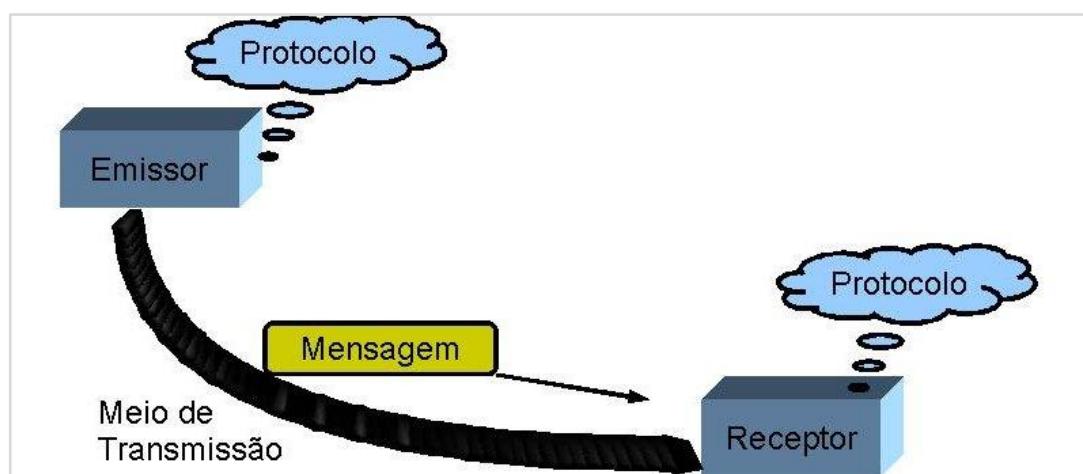


Figura 1- Componentes da comunicação

Fonte: Prof. Sílvio Bandeira - www.dei.unicap.br/~silvio/



Saiba Mais

Formalmente, definimos o protocolo como o conjunto de regras que regem a comunicação. Mas, intuitivamente, já temos este conceito em nossa mente.

Por exemplo, quando falamos ao telefone, usamos um protocolo simples. Ouvimos o toque, acionamos o telefone e falamos um sonoro “Alô!”. Com essa palavra, indicamos ao agente, na outra ponta, que o canal de comunicação foi estabelecido e se pode, então, iniciar uma conversa. Outras informações são implicitamente enviadas com essa simples palavra, como o volume e a clareza com que o som está sendo transmitido pela linha, o que pode levar os agentes a tomar decisões quanto à comunicação (por exemplo, desligar e tentar novamente).

1.2.2 Fluxo de Dados

Você sabia que quando há comunicação ela pode acontecer de algumas

Competência 01



formas interessantes? Nesta parte do nosso caderno iremos conhecer os tipos de fluxos que uma informação pode seguir. Classificamos as comunicações com relação ao fluxo de dados nas seguintes categorias:

- **Simplex** – quando há fluxo de dados apenas em uma direção, como na televisão normal. Você apenas recebe as imagens para assistir, mas não envia nada para a emissora;
- **Half-Duplex** – na qual os dados podem ir e voltar, mas apenas um sentido de cada vez. Rádios de comunicação pessoal daqueles que seguranças geralmente usam. Aperta um botão para falar e solta o botão para ouvir, (*walkie-talkies*), são bons exemplos, quando apenas um dos comunicantes pode falar por vez;
- **Full-Duplex** – na qual os dados podem fluir pelo meio nos dois sentidos ao mesmo tempo. Quando falamos ao telefone, podemos ter as duas pessoas falando ao mesmo tempo e cada uma realmente escuta a outra. Um bom exemplo é o nosso aparelho de celular ou ainda o telefone convencional.

1.3 Redes

Afinal, o que é uma rede? Colocando de forma simples, é um sistema que interliga coisas. Essas coisas podem ser dispositivos, pessoas ou até outros sistemas.

Por que ela é importante? Simplesmente porque uma rede permite que as “coisas” se comuniquem (já vimos a importância da comunicação anteriormente, lembra?).

Podemos ter uma rede de amigos, uma rede de ferrovias, ou mesmo uma rede de lojas. Mas aqui estamos interessados nas **redes de computadores**.

Uma rede de computadores nada mais é que um sistema envolvendo equipamentos e conexões que interliga computadores. Porém, computadores



ATENÇÃO

Imagine uma rodovia de mão-dupla como as nossas BRs. Suponha que a rodovia é o meio de transmissão e os carros são os dados.

Em qual das categorias acima você classificaria esta “comunicação”?

Como, então, você classificaria um trecho onde há obras com um dos sentidos interrompido e os operários utilizando as famosas placas “PARE/SIGA” para controlar a utilização de meia pista?

Competência 01

não são tão inteligentes como pessoas e, portanto, precisamos especificar cada mínimo passo para que um computador se comunique com outro.

Quando conectamos computadores em uma rede podemos fazê-lo de duas maneiras. Ligando apenas duas máquinas com um cabo temos uma **conexão ponto-a-ponto**. Este cabo é o meio de transmissão, e como está ligando as máquinas chamamos de ligação ou *link*. O meio de transmissão é exclusivo para essas duas máquinas, e nenhuma outra pode “ver” os dados que passam por aquele *link*. Se ligarmos mais de uma máquina no mesmo meio de transmissão (Figura 2) temos uma **conexão multiponto**.

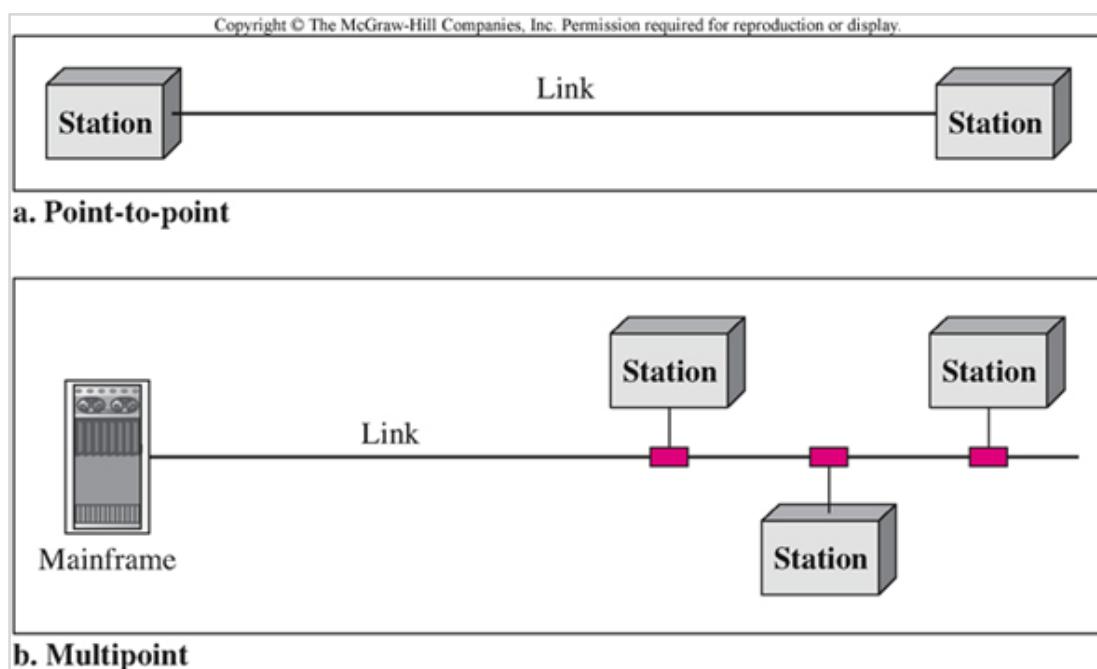


Figura 2- Conexão ponto-a-ponto (a) e multiponto (b)

Fonte: (FOROUZAN, 2007)

Você sabia que uma das características mais importantes das conexões multiponto é que uma máquina pode mandar uma mensagem, de uma única vez, para todas as outras, sem precisar repeti-la. Isso acontece porque todas as outras máquinas estão ligadas, ou conectadas, ao mesmo meio de transmissão, ou seja, todas “veem” os dados que são transmitidos.

Competência 01

Já nas conexões ponto-a-ponto isso não acontece. Cada *link* é “visto” apenas pelas máquinas a que está ligado em cada ponta.

Fazendo uma combinação de conexões ponto-a-ponto e multiponto em um conjunto de máquinas podemos criar redes com geometrias diferentes. Esta característica é chamada de topologia.

1.3.1 Topologias de Rede

A topologia descreve como os equipamentos estão interligados, ou seja, a forma física como eles estão interligados. A topologia tem a ver como os dados fluem na rede. Esses dados são divididos em Barramento (bus), Anel (ring), Estrela (Star) e Redes em malha (Mesh).

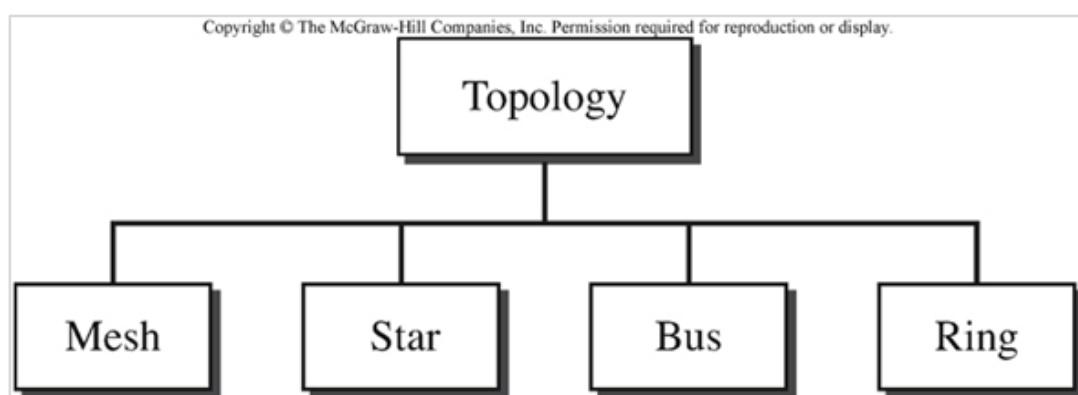


Figura 3 - Topologias de Rede
Fonte: (FOROUZAN, 2007)

1.3.1.1 Mesh (malha)

Utilizando uma rede apenas com conexões ponto-a-ponto, precisaremos ligar cada máquina com todas as outras (lembre que uma conexão ponto-a-ponto só liga duas máquinas). Portanto, precisamos de uma conexão para cada par de máquinas na rede, como mostra a figura 4.

A rede em *mesh* tem características interessantes, uma delas é a velocidade. Já que cada *link* é independente dos outros (o meio físico não é

Competência 01

compartilhado), podemos ter, ao mesmo tempo, comunicações diferentes em *links* diferentes. Além disso, como temos vários *links*, se um deles falhar, podemos redirecionar os dados por outro caminho. As desvantagens dessa topologia são a quantidade de dispositivos de rede (placas) que cada máquina precisa ter (uma para se conectar a cada outra máquina) e a quantidade de cabos necessária para conectar todas essas máquinas entre si.

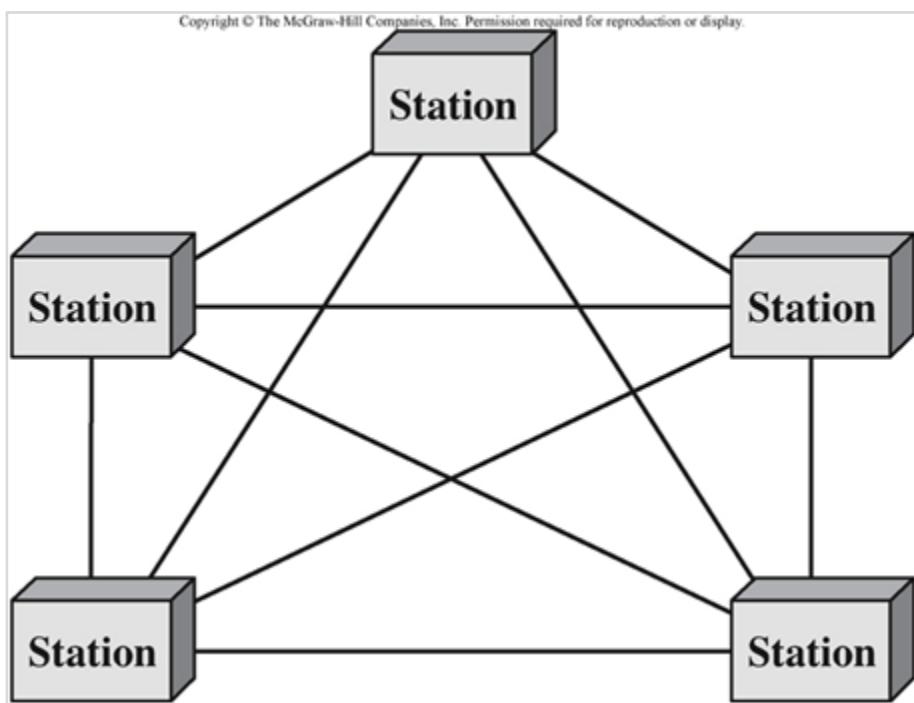


Figura 4 - Rede com topologia Mesh. Note que para ter comunicação cabos devem ser ligados a cada estação (Station) que você quer que se comunique. Cada traço representa um cabo e cada cabo está ligado a uma placa de rede.

Fonte: (FOROUZAN, 2007)

1.3.1.2 Topologia em Estrela

Atente bem! Nesta topologia, as máquinas são todas ligadas a um dispositivo concentrador (Figura 5). Esse dispositivo central é normalmente um *hub*, que está representado na Figura 6. Ele tem a função de receber os dados e repassar para as outras máquinas da rede.

Competência 01

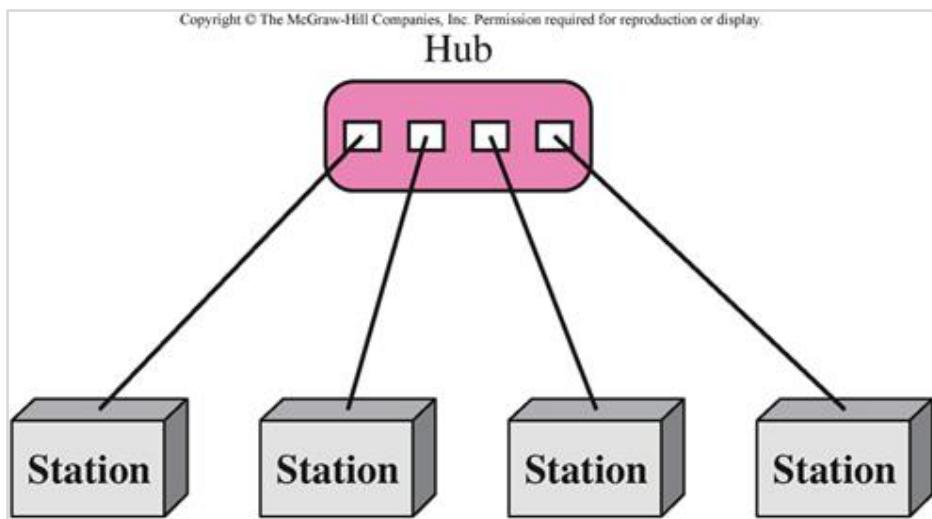


Figura 5 - Note a ligação de cada computador (station) com o dispositivo concentrador, o Hub.
Fonte: (FOROUZAN, 2007)



Figura 6- Imagem de um hub.
Fonte: <http://www.sxc.hu/photo/84393>

Observe que na topologia em estrela (*star*) não há conexão direta entre as máquinas. Todas as comunicações passam obrigatoriamente pelo dispositivo central. Daí, podemos já identificar dois problemas. Um deles no quesito desempenho, pois o meio de transmissão (o *hub*) é compartilhado, portanto, não podemos ter mais de uma comunicação ao mesmo tempo. Então, seu desempenho é menor que na topologia *mesh*. Outra desvantagem é a

Competência 01

dependência de todo o sistema com relação ao dispositivo central. Se houver um problema nesse equipamento, toda a rede fica desativada.

Será que esta topologia só tem desvantagens? Não, absolutamente. Não é à toa que a maioria das redes locais (redes pequenas como em um escritório ou residência) é desse tipo. Vejamos, então, quais as suas vantagens.

Atente que a rede estrela necessita de bem menos cabos e placas de rede para sua instalação comparada com a topologia *mesh*, pois cada máquina só precisa de uma placa e um cabo para se conectar ao *hub*. Isso diminui muito os custos de aquisição e instalação. O *hub*, apesar de ser um ponto de falha importante, tem um hardware bastante simples e, portanto, é relativamente barato além de dificilmente dar problemas. Outra vantagem: como cada máquina é fisicamente isolada das outras; adicionar, mover e remover máquinas na rede não causa qualquer problema nas que já estão funcionando. Até mesmo se uma das máquinas falhar, as demais podem continuar trabalhando normalmente. Portanto, para esses casos, a rede em estrela também tem tolerância a falhas.

1.3.1.3 Topologia em Barramento

Note que esta topologia usa conexões multipontos. Há apenas um cabo longo que se estende pela instalação completa, ao qual todas as máquinas são ligadas. Esse cabo longo é a “espinha dorsal” (do inglês *backbone*) da rede. Cada máquina tem um cabo específico e um conector para ligá-la ao cabo principal conforme a Figura 7.



ATENÇÃO

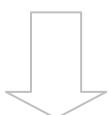
Saiba Mais

Tolerância a falhas é a característica que permite a um sistema continuar funcionando, mesmo que parcialmente, quando ocorre um problema.

Normalmente, isso é feito duplicando-se partes essenciais.

O sistema não precisa ser computacional, pode ser um sistema elétrico ou mecânico, por exemplo. Esta área

é bastante interessante, inclusive, tema de pesquisa em várias universidades. Para saber um pouco mais sobre este assunto, acesse: <http://tinyurl.com/redes11>



Competência 01

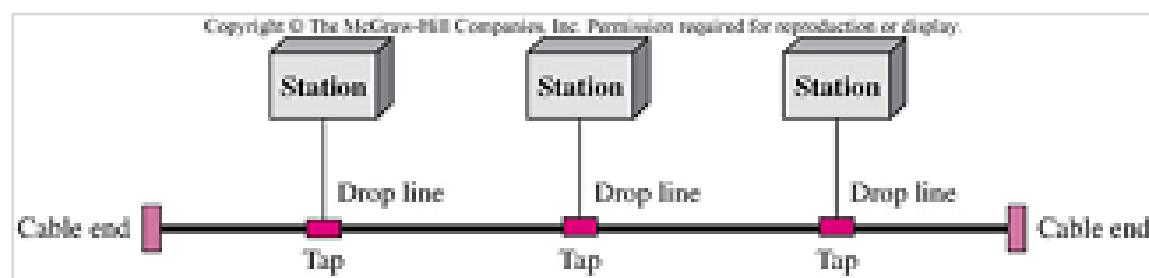


Figura 7- Rede com topologia Barramento2. Note que cada máquina se comunica com o cabo principal através de um conector chamado de T (Tap). Nas extremidades de cada ponta do cabo existem duas peças chamadas terminador (Cable end).

Fonte: (FOROUZAN, 2007)

Como, nesse caso, o cabo principal é mais extenso que nas outras topologias, o sinal elétrico pode perder energia à medida que trafega por toda a sua extensão. Isso é chamado de **atenuação do sinal**, e pode causar perda de informações. Para evitar que isso aconteça, há algumas limitações na instalação quanto ao tamanho máximo desse cabo, uma quantidade de máquinas que podem ser ligadas a um único cabo e o espaço mínimo entre as ligações das máquinas. As vantagens dessa topologia incluem facilidade de instalação e uso de menos cabo, comparando-se com as topologias anteriores.

Quanto às desvantagens, destacamos falha na rede quando há uma quebra no cabo principal, que é difícil de ser localizada, e paralisa toda a rede. Além disso, por causa das limitações no espaço entre as máquinas, uma vez que a instalação feita é difícil modificá-la, como adicionar uma máquina, por exemplo. Por esses motivos, as redes em barramentos não são a escolha certa mesmo para redes locais.



Atenção:

A topologia em barramento não é mais utilizada em redes locais. Ela foi substituída pela topologia estrela.

1.3.1.4 Topologia em Anel

Uma rede em anel (*ring*) consiste em máquinas com duas conexões ponto-a-ponto, uma para a máquina anterior e outra para a máquina posterior, formando realmente um anel. Uma característica importante dessa topologia é a necessidade de os dados trafegarem no anel em apenas um sentido (unidirecional). Dessa forma, se uma estação recebe um dado que não lhe

Competência 01

pertence, ela simplesmente o passa a frente. Esse processo continua até que a estação destino seja alcançada.

Para evitar que mais de uma máquina envie dados ao mesmo tempo (o que poderia gerar uma confusão na comunicação), uma permissão de acesso é passada, continuamente, de uma máquina para a outra. Uma estação, portanto, só pode mandar dados pela rede quando está de posse dessa permissão. Depois de enviar seus dados pela rede, a estação deve repassar a permissão para a máquina a sua frente no anel. A permissão de acesso nada mais é do que uma mensagem, e é chamada também de *token* (pode-se traduzir esta palavra como “ficha”, para o controle de acesso ao meio).

Essa topologia é fácil de instalar, de adicionar novas máquinas e de configurar. Porém, possui desvantagens muito sérias. Sua escalabilidade, ou seja, a capacidade de crescer em quantidade sem perder desempenho é desfavorável, pois, quando aumentamos o número de máquinas, o *token* pode demorar muito para dar uma volta completa no anel. Se um dos dispositivos desconectar, em qualquer ponto, toda a rede fica parada. Alguma máquina pode perder o *token* (se, por exemplo, travar quando estiver com ele), o que é difícil detectar e impede que as outras usem a rede.

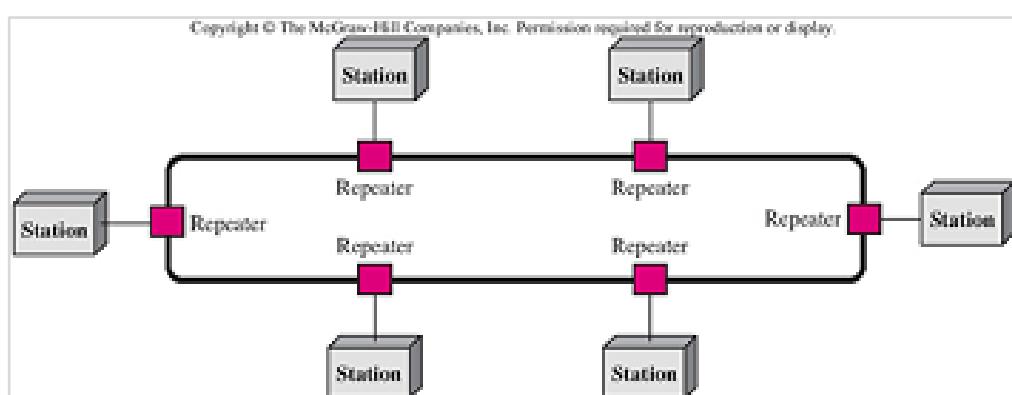


Figura 8- Rede com topologia em Anel
Fonte: (FOROUZAN, 2007)

Quando falamos de rede em anel estamos falando do fluxo dos dados. A informação percorre a rede em forma de anel, ou seja, de uma máquina para

Competência 01

outra. Mas fisicamente ela é igual a uma rede estrela e o nome do aparelho concentrador é o MAU – Multistation. Conforme Figura 9.

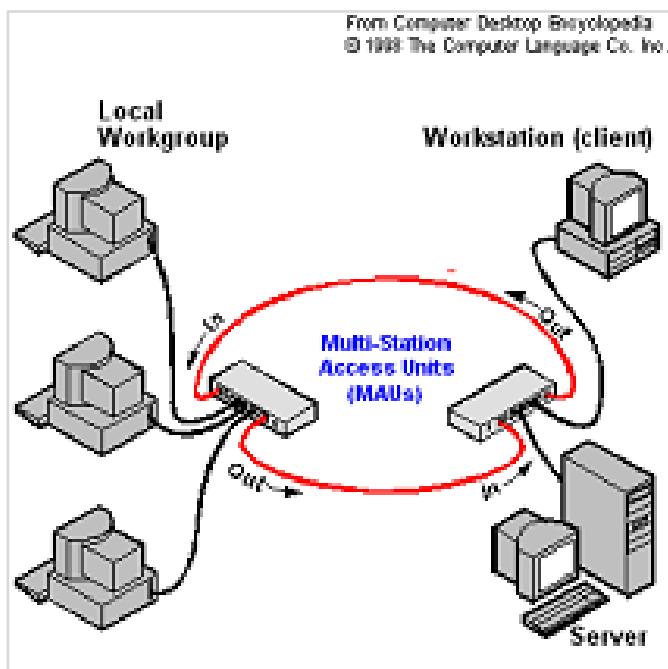
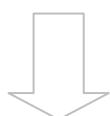


Figura 9- Rede com topologia em Anel. Note a presença dos dois MAUs que controlam o Token

Fonte: The Free Dictionary: <http://img.tfd.com/cde/TOKENRNG.GIF>

1.3.1.5 Topologia Híbrida

Podemos também ter uma rede com topologia mista, para adequar uma determinada instalação no intuito de combinar as vantagens de duas ou mais topologias diferentes. É o caso da rede com topologia híbrida. (figura 10)



Competência 01

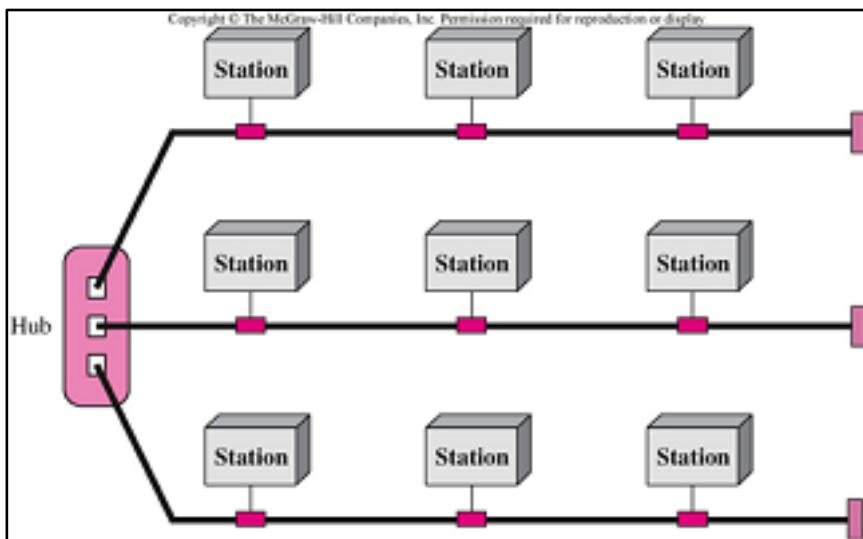


Figura 10-Rede com topologia Híbrida (estrela e barramento)

Fonte: (FOROUZAN, 2007)

1.3.2 Modelos de Rede

Classificamos as redes, também, com relação à área geográfica que cobrem. Neste sentido as redes podem ser:

1.3.2.1 LAN

Do inglês, LAN significa *Local Area Network* (rede local), é uma rede privada (pertence a apenas uma empresa ou pessoa, no caso de ser doméstica) e conecta as máquinas em uma sala, laboratório ou prédio. Esse tipo de rede pode ter duas ou mais máquinas, mas tem seu tamanho sempre limitado, de alguns metros a poucos quilômetros.

Podemos ter mais de uma rede local numa mesma empresa ou instituição. Isso se dá quando os administradores querem separar em redes diferentes máquinas ou usuários com propósitos distintos. Por exemplo, podemos separar o conjunto de máquinas de uma empresa em uma LAN para os programadores e outra para a diretoria e o setor financeiro.

Competência 01

Em geral, uma LAN usa apenas um tipo de meio de transmissão. A topologia mais comum é estrela.

A velocidade de transmissão em uma LAN, atualmente, varia entre 100 (o mais comum) e 1000 Mbps (mega bits por segundo). Quer dizer que um arquivo de 200 megabits pode ser transferido de uma máquina para outra em pouco mais de 2 segundos. Redes locais que utilizam a tecnologia *wireless* (sem fio) atingem velocidades menores que 100 Mbps, mas têm a vantagem de não precisar de cabos para ligar as máquinas.

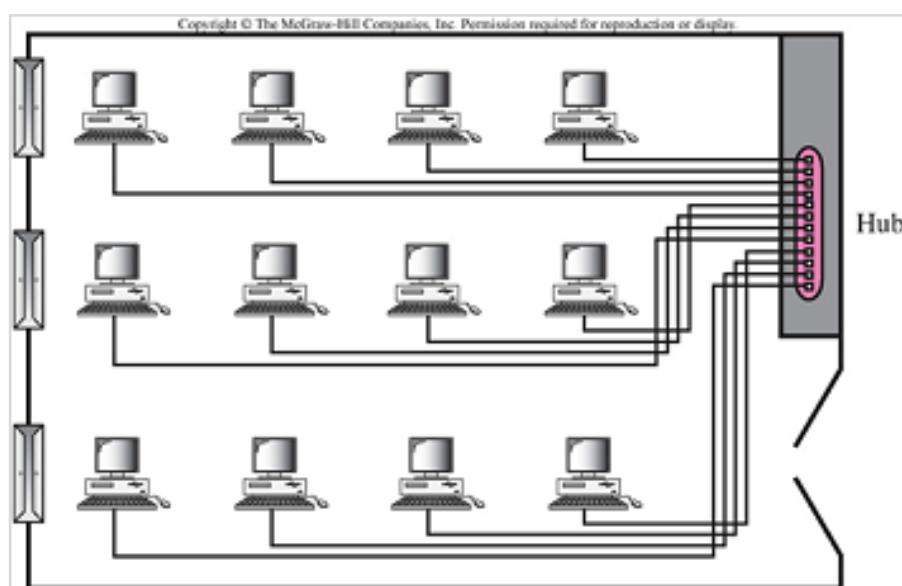


Figura 11- Rede local (LAN)

Fonte: (FOROUZAN, 2007)

1.3.2.2 MAN

Você sabia que a também chamada rede metropolitana (*metropolitan area network*) cobre uma área de uma cidade, como um bairro, ou uma cidade inteira. É uma rede controlada por uma empresa (pública ou privada) e fornece conexão para outras empresas e/ou residências. Um exemplo fácil de entender é a rede de antenas que dão cobertura aos celulares em uma cidade. Note que podemos ter mais de uma em uma mesma cidade, da mesma forma como temos mais de uma operadora de celular.

Competência 01

Em Pernambuco, um excelente exemplo de rede metropolitana é a da ATI – Agência Estadual de Tecnologia da Informação www2.ati.pe.gov.br/web/site-atи que mantém serviços em todo o estado de Pernambuco interligando secretarias, prefeituras e órgãos do governo.

Note na Figura 12 um exemplo de rede metropolitana.

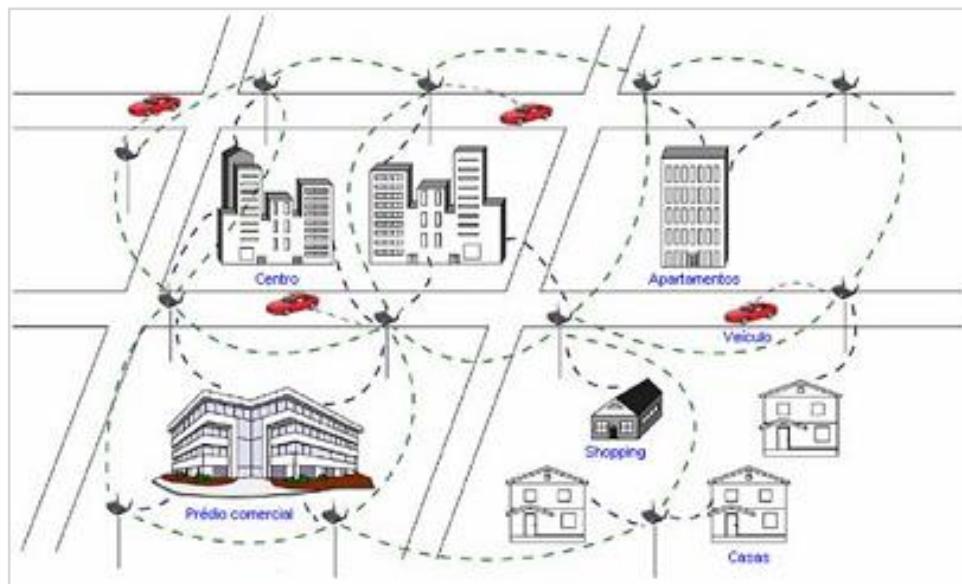


Figura 12- Um exemplo de uma rede metropolitana.

Fonte: www.gta.ufrj.br/grad/06_2/felipe/arquitetura_f.htm

1.3.2.3 WAN

Você sabia que WAN (*wide-area network*) é a chamada rede de longa distância, e pode cobrir cidades, países e até continentes? É uma rede bem mais complexa e pode interligar redes metropolitanas e locais. A *internet* é o melhor exemplo de WAN que conhecemos, porque interliga redes diferentes, de empresas diferentes, e com infraestruturas (meio de transmissão e topologias) diferentes (Figura 13)

Competência 01

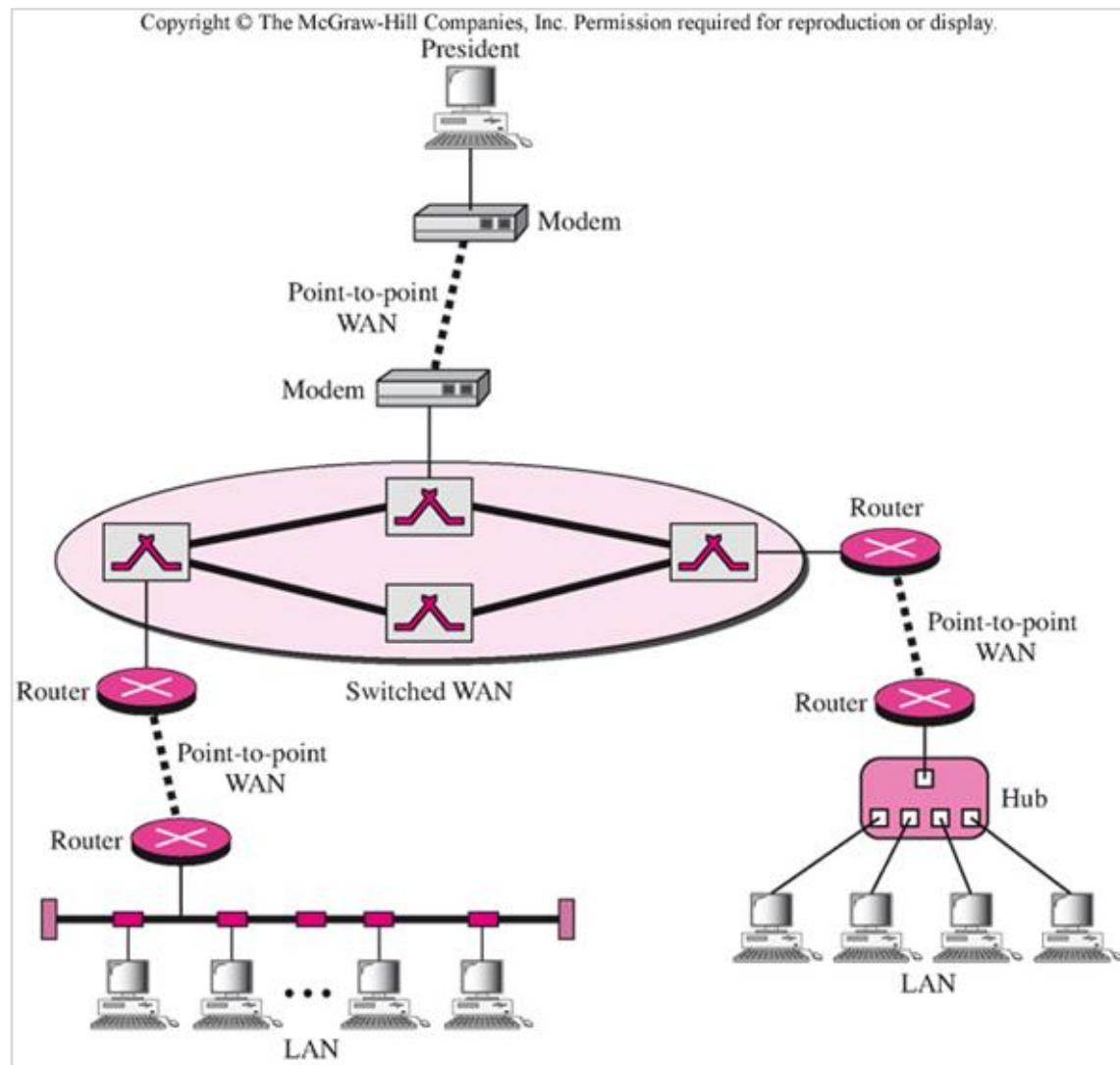


Figura 13- Rede de longa distância (WAN) interligando diferentes redes locais (LANs)

Fonte: (FOROUZAN, 2007)

1.4 A Internet

Você sabia que de uma maneira bem simples, podemos definir a *Internet* como uma rede de redes. A maior de todas. E, na verdade, o próprio termo *internet* quer dizer isso, interconexão (*inter*) de redes (*nets*). É, mais formalmente, um sistema mundial de redes interconectadas para comunicação e compartilhamento de informações, em todas as suas formas. Quando ligamos nosso computador na *Internet*, podemos ter acesso a informações armazenadas em seus milhões de computadores. Nela temos acesso, hoje em dia, a conteúdos sobre todas as áreas da atividade humana. E

Competência 01



isto é só a “ponta do *iceberg*”. Podemos ter telefonia pela *Internet*, salas de bate-papo, correio eletrônico, ou seja, uma infinidade de serviços que facilitam e agilizam nossas vidas.

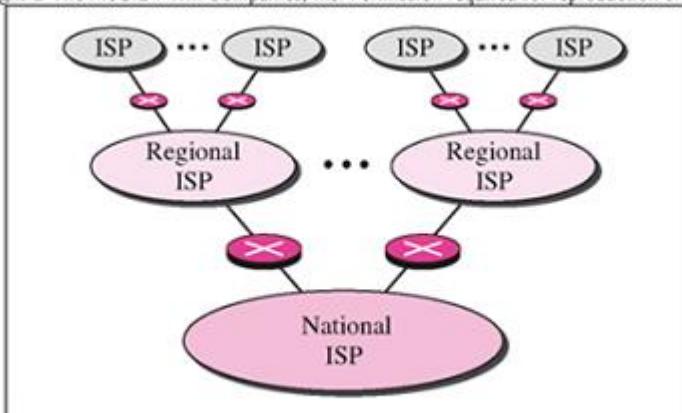
A *Internet* é hoje formada por inúmeras WANs e LANs conectadas. Quase todos os usuários se ligam através de empresas chamadas **provedores de Internet** (do inglês *Internet service provider* ou ISP). Esses provedores existem em vários níveis: locais, regionais, nacionais e internacionais. Nesse sistema, ISPs locais fornecem conexão a seus clientes que, por sua vez, são clientes dos ISPs regionais, que são clientes dos nacionais e assim por diante (figura 14).



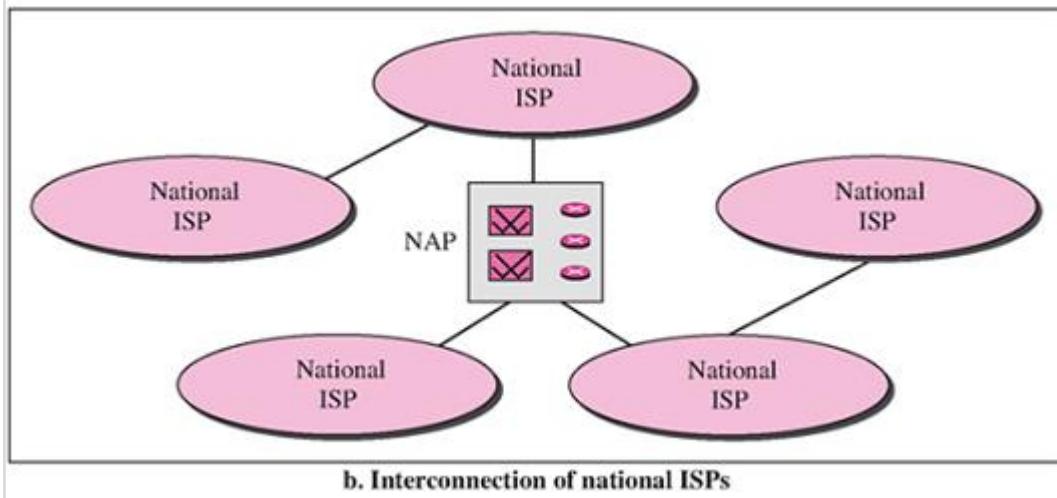
SAIBA MAIS:

O termo *internet* significa redes interligadas. Já com o 'i' maiúsculo, *Internet*, refere-se à rede mundial.

Copyright © The McGraw-Hill Companies, Inc. Permission required for reproduction or display.



a. Structure of a national ISP



b. Interconnection of national ISPs

Figura 14 - Estrutura hierárquica dos ISPs na Internet. Note que os ISPs de cada país (National ISP) se intercomunicam entre si através do NAP – Network Access Point, ou pontos de acesso a rede.

Fonte: FOROUZAN(2007)

Competência 01

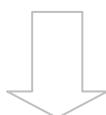
1.5 Dispositivos de interconexão

Note que, independente da tecnologia ou do uso da rede, existem equipamentos que tornam a comunicação real. Vamos conhecer os dispositivos mais comuns que interconectam redes ou segmentos de redes?

1.5.1 Repetidores

Você sabia que este equipamento serve para aumentar o tamanho de uma rede, ligando partes separadas de uma rede a outra. Geralmente, os repetidores são utilizados quando as distâncias são maiores que a tecnologia da rede permite. A função de um repetidor é copiar todos os dados que aparecem em um lado para o outro, em ambas as direções. Como o sinal sofre **atenuação** (perda) ao chegar próximo ao limite de comprimento de uma rede, o repetidor também tem a função de regenerar o sinal para que ele possa atravessar todo o outro segmento da rede, onde vai ser copiado.

Lembre-se: o repetidor não é um simples amplificador, ele regenera o sinal (figura 15). Ele também não conecta redes diferentes, apenas segmentos da **mesma LAN**, e trabalha apenas na camada física (figura 16).



Competência 01

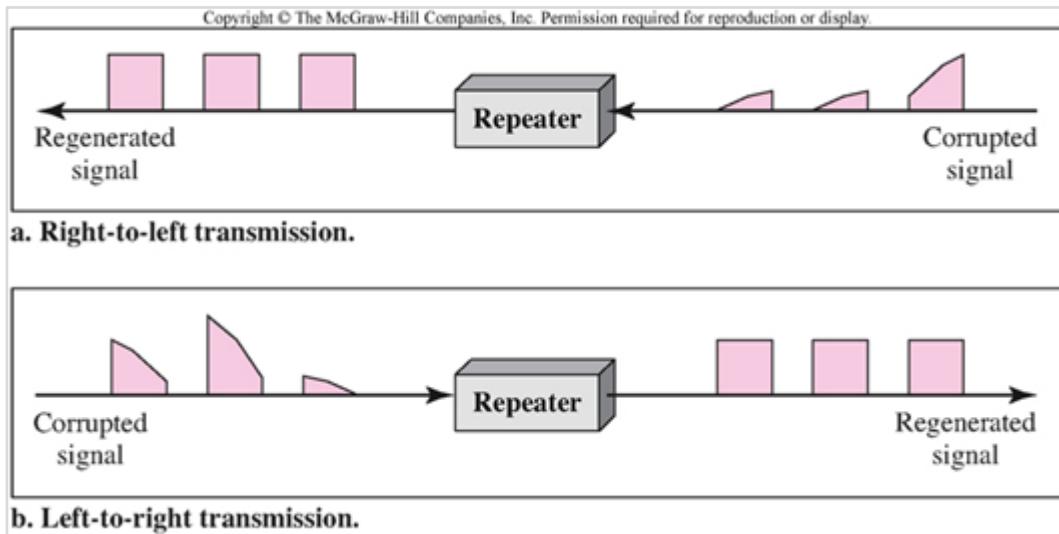


Figura 15- Função do repetidor. Perceba que o sinal corrompido (Corrupted Signal) ao passar pelo tratamento do Repetidor (Repeater) é regenerado (Regenerated Signal). Note também que o repetidor trabalha nos dois sentidos

Fonte: FOROUZAN (2007)

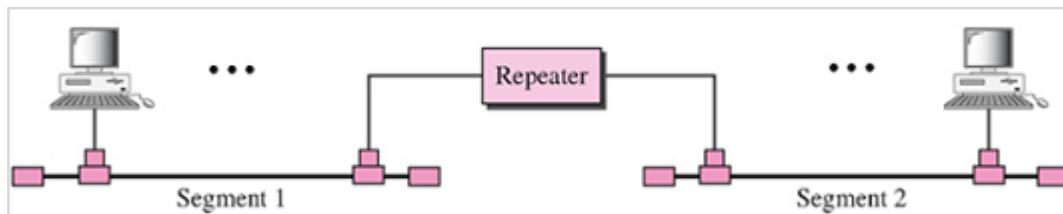


Figura 16- Repetidor conectando dois segmentos de uma LAN. O Comportamento deste equipamento na rede é transparente, ou seja, não há mudanças no método de comunicação.

Fonte: FOROUZAN (2007)

1.5.2 HUBS

Pois bem! Vamos agora conhecer um HUB, que pode ser visto como um repetidor multiporta. É usado para criar uma rede com topologia estrela, porém, como também trabalha apenas na camada física, todos os pacotes são “escutados” por todas as máquinas ligadas. É como se ele fosse um barramento inteiro em um único dispositivo.

Pode-se ligar mais de um HUB para aumentar a sua capacidade, fazendo o que se chama de cascamenteamento, como na figura 17

Competência 01

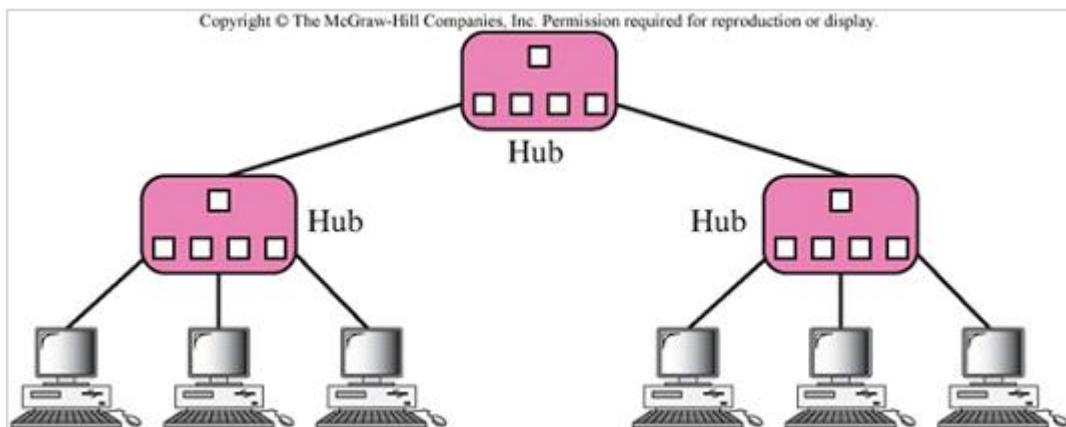


Figura 17- HUBs interligados formando uma hierarquia. O Hub do meio se comporta como um repetidor neste exemplo. Mesmo tendo 3 equipamentos, esta rede é de apenas um seguimento.

Fonte: FOROUZAN (2007)

1.5.3 Bridge

Já a *bridge* faz mais que um repetidor ou um HUB, porque ela sabe quais máquinas estão em qual segmento da rede, pois, à medida que ela recebe as informações, vai formando uma tabela com os endereços de emissor, para saber quais máquinas estão em qual segmento. Observe a figura 1.18, se um quadro chega do segmento 1 endereçada para primeira máquina (com final :61:41), ela não copia este quadro para o segmento 2, porque sabe que a máquina destino está no mesmo segmento de onde a informação veio. O endereço que este tipo de equipamento conhece é o MAC – *Media Access Control*, um número único que todo dispositivo de rede tem. Esse número é único no mundo inteiro.

Observação: a *bridge* analisa os endereços MAC. Ela os usa apenas para formar a tabela, indicando que máquina está de que lado. E isso é feito dinamicamente, ou seja, se você mudar uma máquina de um lado para outro, com o tempo a *bridge* percebe a mudança e atualiza a tabela.

Outra grande vantagem das *bridges* é que, como ela não copia todas as informações de um lado para o outro e como ela conhece os endereços de cada lado, conforme Figura 18, é capaz de isolar informações apenas no lado



Saiba mais:

Tanto o HUB quanto o Repetidor não conhecem o endereçamento dos equipamentos que estão conectados a eles e, por isso, repetem tudo para todas as portas que eles possuem, para ter certeza de que a informação chegue ao destino.



Saiba Mais

O endereço MAC tem 48 bits e tem o seguinte formato: 00-00-0c-12-34-56. Os três primeiros dígitos (00-00-0c) indicam o fabricante do dispositivo. Os três últimos correspondem ao endereço físico do dispositivo.

Competência 01

do segmento de rede que é devido. Isso é chamado isolamento de **domínio de colisão**.



Saiba Mais:
Domínio de colisão é uma área lógica da rede onde os pacotes podem colidir uns com os outros. Quanto mais colisões houver, menor será a eficiência da rede. Um dispositivo como um HUB ou um Repetidor provoca bastantes colisões, por não conhecerem o endereço das máquinas ao longo de uma rede.

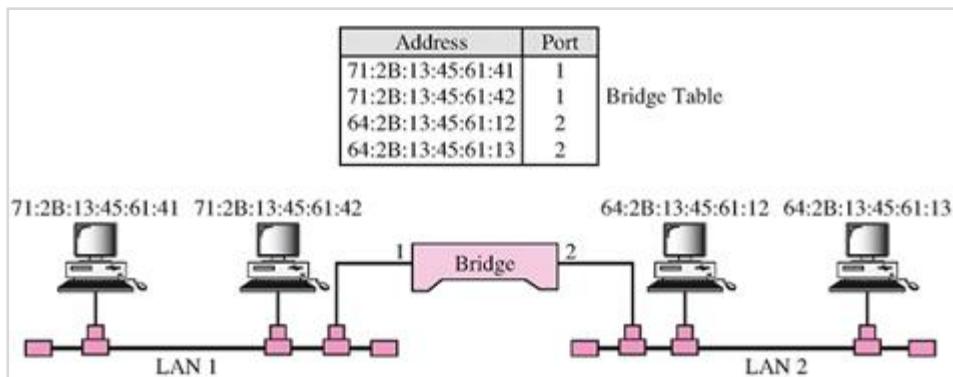
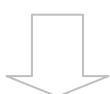


Figura 18- Uma bridge conectando duas LANs. Note que a Bridge constrói a tabela de endereços MACs de cada lado, isolando as informações no seu devido segmento.

Fonte: FOROUZAN (2007)

1.5.4 Switch

Do mesmo modo que um *hub* pode ser visto como um repetidor multiponto, um *switch* pode ser visto como uma *bridge* multiponto, com a diferença que em cada porta é ligada uma única máquina. Isso significa maior desempenho que os *hubs*, pois não há mais competição pelo meio de transmissão. Colisões também não ocorrem, pois cada máquina agora tem seu próprio **domínio de colisão**. Além disto, pares de máquinas diferentes podem se comunicar ao mesmo tempo, pois o *switch* isola o tráfego por máquina. Observe a figura 19.



Competência 01

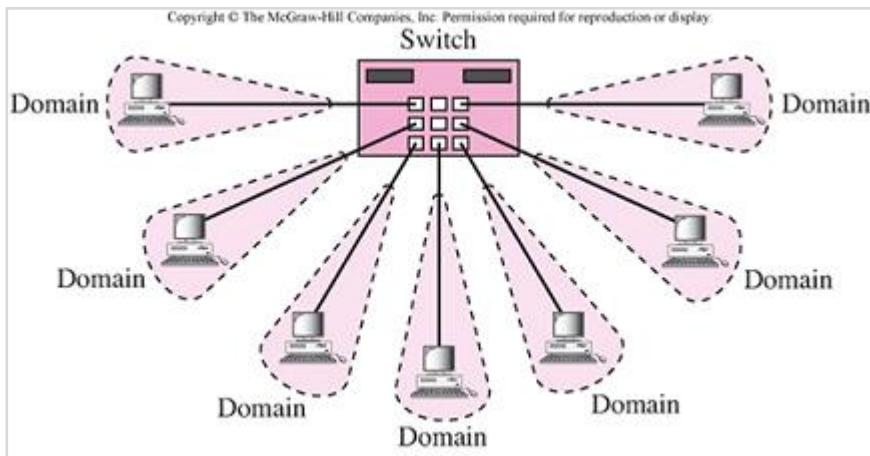


Figura 19- Rede utilizando um Switch. Note que este equipamento isola as máquinas em domínios de colisões diferentes (Domain). Isso provoca um aumento na performance porque as colisões são evitadas e os dados vão apenas para o destino correto.

Fonte: FOROUZAN (2007)

1.5.5 Roteador

Você sabia que o Roteador é um equipamento responsável pela interligação das redes locais entre si e redes remotas em tempo integral. Em outras palavras, permite a comunicação de uma máquina de uma determinada rede LAN a máquinas de outra rede LAN remota, como se as redes LAN fossem uma só. O Roteador possui a função de decidir o melhor caminho que deve ser percorrido pelas informações entre as várias LAN's até que cheguem ao destino.

Os roteadores trabalham com tabelas internas que são capazes de decidir o caminho mais rápido para que a informação trafegue na rede. Esses equipamentos, também, são capazes de fazer compressão e descompressão de dados e, ainda, de priorizar tipos de tráfegos de acordo com a configuração preestabelecida.

Note a função e posicionamento de um roteador na Figura 20

Competência 01

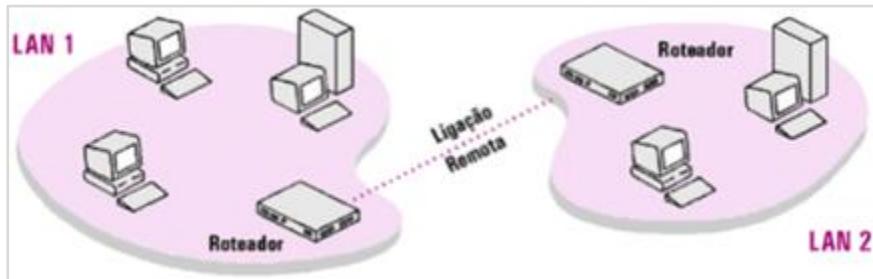


Figura 20-Imagine a LAN1 em Petrolina e a LAN2 em Fernando de Noronha. Os roteadores são capazes de achar a melhor rota entre elas e fazer com que os dados trafeguem entre as duas redes.

Fonte: www.unifesp.br/proex/dac/eaoc/apostilas/word_2003/apostila_rede.pdf



Figura 21- Um roteador de grande porta da Avaya

Fonte: Wikimedia.org - <http://pt.wikipedia.org/wiki/Ficheiro:ERS-8600.JPG>

1.5.6 AP – Access Point

Você sabia que um Access Point ou Ponto de Acesso é um dispositivo, em uma rede sem fio, que realiza a interconexão entre todos os dispositivos que usam tecnologia Wireless. Em geral, se conecta a uma rede cabeada, servindo de ponto de acesso para outra rede, como por exemplo, a Internet. Veja o uso de um AP na Figura 22 em uma residência.

Competência 01



Figura 22- O Access Point, ou simplesmente AP, é o concentrador de uma rede Wireless.

Fonte: <http://upload.wikimedia.org/wikipedia/commons/3/34/Linksys-Wireless-G-Router.jpg>



Saiba Mais:

Wireless é um termo que quer dizer sem fio. Um equipamento wireless transmite seus dados pelo ar em forma de ondas, semelhantes a ondas de rádio ou TV. Quando dizemos que um dispositivo de rede é Wireless estamos afirmado que ele não usa fios para se conectar a uma rede.

1.5.7 Placa de Rede

Uma placa de rede (também chamada adaptador de rede ou NIC, do acrônimo inglês Network Interface Card) é um dispositivo de hardware responsável pela comunicação entre os computadores de uma rede.

A placa de rede é o hardware que permite aos computadores conversarem entre si, através da rede. A sua função é controlar todo o envio e recepção de dados. Cada arquitetura de rede exige um tipo específico de placa de rede, sendo as arquiteturas mais comuns às redes em anel **Token Ring** (Topologia Anel) e a tipo Ethernet (Topologia Barramento e Estrela).



Figura 23- Detalhes de uma placa de rede.

Fonte: -

http://upload.wikimedia.org/wikipedia/commons/9/9e/Network_card.jpg

Competência 01

Existem também as placas destinadas a redes sem fio, são as placas wireless e, em vez de um local para a conexão de um cabo, existe a antena de transmissão, conforme a figura 24.

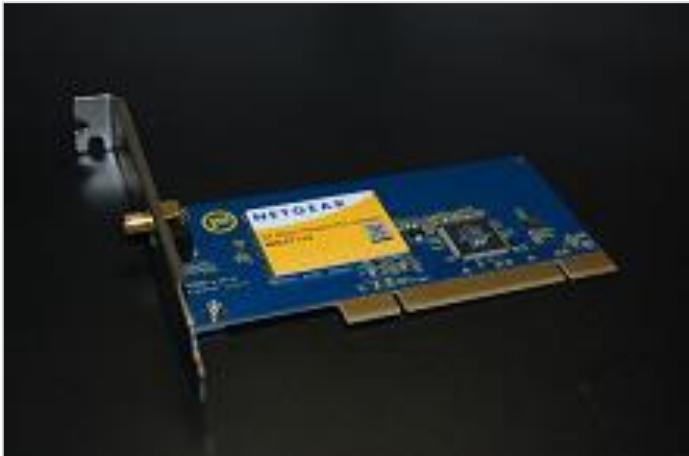
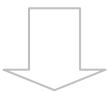


Figura 24- Detalhes de outra placa de rede.

Fonte: -

http://upload.wikimedia.org/wikipedia/commons/2/21/Netgear_Wireless_PCI_WG311v3.jpg



Mídias Integradas:

Para entender como funcionam os equipamentos e a comunicação em uma grande rede de computadores, veja o vídeo “Guerreiros da Internet”. Nele, você compreenderá os principais conceitos, em um vídeo muito bem elaborado.

Guerreiros da Internet Parte 1 -
<http://www.youtube.com/watch?v=tFKVFWfc2nk>

Guerreiros da Internet Parte 2 -
<http://www.youtube.com/watch?v=J7xzZUuinPE>

Para complementar o nosso caderno, veja este excelente vídeo “Como Funciona a Internet” :
<http://www.youtube.com/watch?v=E4gcWJaw8aQ>

Competência 01

1.6 Resumo

Pois bem! Vamos Revisar?!

A comunicação de dados consiste na transferência de informações (dados) de um dispositivo para outro, através de um meio de comunicação. Um sistema de comunicação é composto de cinco elementos básicos: emissor, receptor, mensagem, meio de transmissão e protocolo. Protocolo é um conjunto de regras que regem a comunicação. Quanto ao fluxo dos dados, podemos classificar o canal de comunicação em: *simplex*, *half-duplex* e *full-duplex*.

Rede é num conjunto de dispositivos (normalmente computadores) interligados por um meio de transmissão, podendo ter diversas topologias, de acordo com seu arranjo físico e/ou lógico: *mesh*, estrela, barramento, anel e híbrida (ou mista). Existem determinados tipos de rede:

1. LAN – rede local que interliga dispositivos em uma residência, escritório ou um prédio, mas sempre numa área geográfica pequena (alguns quilômetros);
2. MAN – rede que cobre uma área correspondente a um bairro ou uma cidade e que interliga dispositivos de pessoas ou instituições diferentes;
3. WAN – aquela que comunica sistemas em áreas geográficas muito extensas como países e continentes;
4. *Internet* – rede de redes (comunicação entre redes).

A *Internet* (com 'I' maiúsculo) é a rede mundial de computadores. É composta por inúmeras redes independentes em escala global. Existem servidores de acesso à *Internet* locais, regionais, nacionais e internacionais.

Competência 02

2. COMPETÊNCIA 02 | PROTOCOLOS DE COMUNICAÇÃO

2.1 Objetivos

- Compreender como o protocolo age sobre a comunicação de dados.
- Conhecer o modelo de comunicação em camadas.
- Conhecer o Modelo OSI e suas camadas.
- Conhecer o Modelo TCP/IP, seus protocolos e camadas.
- Entender a relação entre os Modelos OSI e TCP/IP.
- Conhecer os protocolos de Transporte TCP e UDP.
- Conhecer o protocolo IP e suas regras de endereçamento.
- Conhecer o conceito de Portas de Endereçamento TPC e UDP.
- Saber a função dos protocolos DNS, DHCP, ARP e RARP.
- Saber configurar o Protocolo IP no Windows.

Durante a semana passada, estudamos sobre comunicação, redes de computadores e diversas classificações deste ramo da Tecnologia da Informação. Logo após, conhecemos um pouco sobre a Internet e sobre os principais dispositivos que fazem a rede funcionar. Lembrou de tudo??? Nesta semana, vamos conhecer a parte lógica da rede de computador. Entenderemos as principais características e suas principais configurações. E na nossa semana final, conheceremos a parte física, parte esta que faz a interligação dos dispositivos de uma ou mais redes.

Para haver comunicação, seja em que meio for, é necessário que quem envie a mensagem (emissor) e quem a receba (receptor) falem a mesma linguagem. Isso é primordial para que esta mensagem seja entendida. Ao ler este material, você consegue entender, porque está escrito em um idioma que você consegue ler e compreender. Ao conversar com o professor, tutor ou mesmo um colega de classe, você fala em português e seu colega lhe responde no mesmo idioma. Se você encontrar um turista grego na rua e falar com ele em português e ele lhe responder em grego, a comunicação não será

Competência 02

estabelecida, pois nem ele conhece o nosso idioma e nem você fala grego. Neste caso, a comunicação não foi estabelecida e o emissor e o receptor não conseguem se comunicar.

Pois bem, este idioma citado no parágrafo acima na área de Tecnologia da Informação é chamado **de Protocolo de Comunicação**. Os dispositivos que estão em rede precisam “falar” o mesmo idioma, ou seja, precisam trocar informações sobre o mesmo protocolo (regras). Se dois protocolos diferentes forem usados, não há comunicação, semelhante ao exemplo do turista grego.

Porém esta comunicação sob um protocolo de comunicação não é tão simples como uma conversa entre pessoas. A tarefa é bem mais complexa. E para lidarmos com um problema complexo, nada melhor que dividi-lo em problemas menores. Dessa forma, utilizamos o princípio da **Comunicação em Camadas**.

Como funciona? Na verdade, já estamos acostumados com esse princípio e o utilizamos todos os dias. Por exemplo, ao falar com outra pessoa no telefone, não nos preocupamos em saber como nossa voz é transmitida. Podemos então dizer que a rede de telefonia é a “**camada**” que fornece o meio de comunicação. Então, temos você (usuário) como estando na camada superior. O seu telefone, como sendo o meio de comunicação, está na camada logo abaixo. O seu telefone se comunica com o outro telefone na ponta da comunicação, e esse outro telefone reproduz sua voz para a outra pessoa. Então, na verdade, quem está se comunicando fisicamente? Resposta: Apenas os dois telefones. Nesse modelo, apenas a camada inferior realmente transmite a mensagem (os dois telefones). As camadas mais altas apenas repassam ou recebem a mensagem da camada logo abaixo (você e a outra pessoa).

A comunicação entre computadores é mais complexa e, portanto, precisaremos de mais camadas, porque cada uma vai cuidar de um ou mais detalhes do problema como um todo. Veja na Figura 25 o problema de

Competência 02

transmitir uma carta entre duas pessoas, decomposto em problemas menores, onde cada parte do problema é resolvida por uma camada.

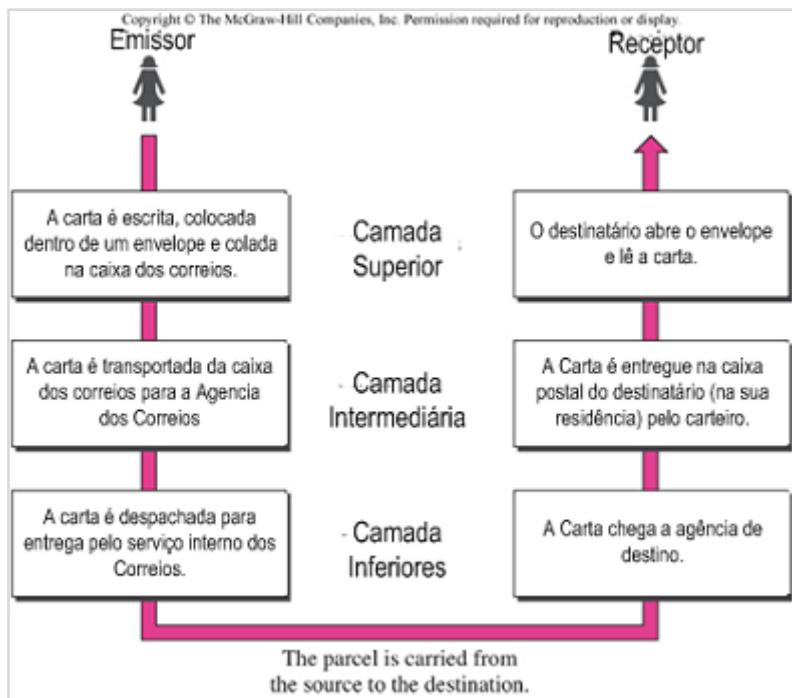


Figura 25- A comunicação em camadas.

Fonte: (Forouzan, 2007)

Na comunicação por computadores, apenas a camada mais baixa resolve o problema de enviar fisicamente a mensagem, e, portanto, precisa de equipamento (*hardware*) para o envio propriamente dito (por exemplo, uma placa de rede). As camadas de cima, resolvem problemas como verificar se a mensagem chegou sem erros ao receptor. Essas camadas mais superiores são implementadas por programas (*software*).

As camadas trabalham de forma independente. Elas têm rotinas próprias. Podem alterar o conteúdo da mensagem, corrigir erros, melhorar algum item e repassar estas alterações para a camada posterior. Essa característica é chamada de dependência, entre partes de um sistema é chamada de **modularidade**.

Competência 02

A quantidade e função de cada camada precisam ser muito bem definidas. O conjunto de camadas e suas definições detalhadas formam o que chamados de **modelo de camadas**.

Estudaremos dois modelos: o modelo OSI, e o modelo TCP/IP. O modelo OSI é predominante na literatura em redes, e o segundo é o modelo utilizado na *Internet*.

2.2 Modelo OSI

Você sabia que o modelo OSI foi desenvolvido pela *International Organization for Standardization (ISO)*. É composto de sete camadas (Figura 26). As camadas de um modelo são sempre dispostas de baixo para cima. Então, a primeira camada é a camada física e a última a de aplicação. Pois bem, vamos lá conhecer estas camadas!



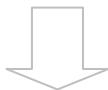
Figura 26- Camadas do Modelo OSI
Fonte: Produzido pelo autor

- **Camada Física:** lida com características mecânicas, elétricas e de acesso ao meio físico de transmissão. Por exemplo, se o meio é compartilhado (conexão

Competência 02

multiponto), essa camada faz com que apenas uma máquina transmita por vez, evitando que as mensagens se misturem.

- **Camada de Enlace de Dados:** trata da transferência das informações de uma máquina para outra *na mesma rede*. Verifica erros na transmissão e controle de fluxo.
- **Camada de Rede:** é responsável pelo envio da mensagem da máquina emissora para a máquina receptora, mesmo que elas estejam *em redes diferentes*. Note que é um problema diferente da camada de enlace. Quando temos redes diferentes interconectadas, a mensagem não pode viajar do emissor para o receptor diretamente. Ela precisa passar por máquinas que ligam uma rede a outra, como uma ponte que liga ruas locais. Um dos tipos de máquinas que interligam duas ou mais redes são chamadas **roteadores**, porque quando recebem uma mensagem, precisam saber por qual **rota** precisam enviá-la para que chegue ao seu destino correto. Na figura 27 temos um *Roteador* ligando três redes distintas, inclusive com topologias e meios de transmissão diferentes. Uma é estrela, a verde, e as outras duas, a vermelha e a azul, são barramento. Note que para a mensagem ir da máquina A para a máquina B, precisa passar pelo **roteador**, e este precisa enviá-la pela rede correta (azul) para que a mensagem não se perca.



Competência 02

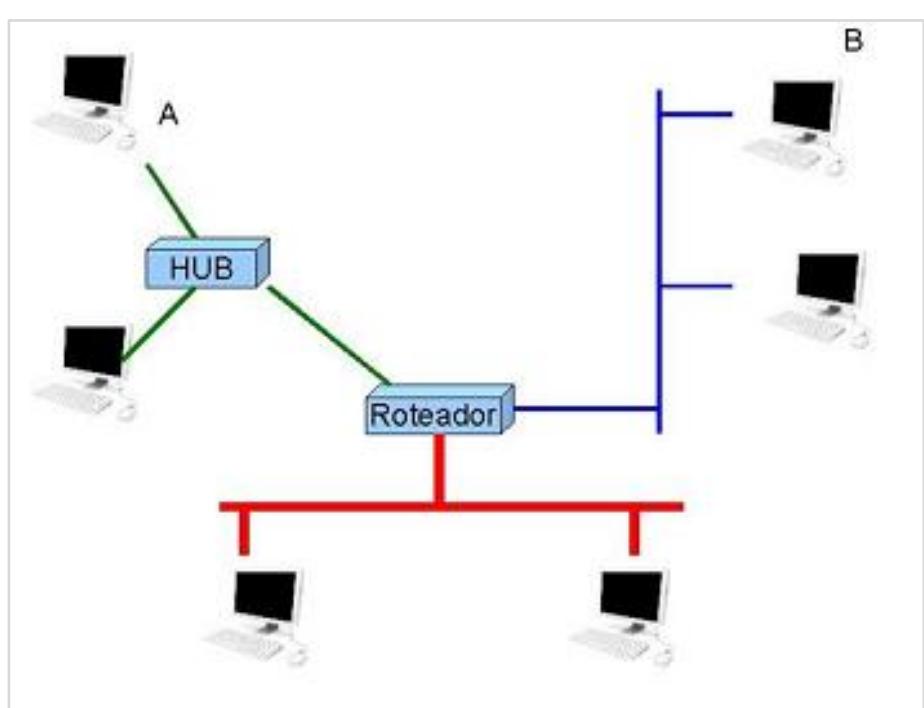


Figura 27- Um roteador ligando três redes distintas.

Fonte: Prof: Sílvio Bandeira - www.dei.unicap.br/~silvio/

- **Camada de Transporte:** preocupa-se com a comunicação de um processo para outro. Nesta camada, são resolvidos problemas como ordenação das mensagens. Esta tarefa garante que as mensagens cheguem ao programa do receptor na mesma ordem em que o emissor enviou. Também são inerentes a esta camada o controle de conexão, o fluxo de dados e os erros.
- **Camada de Sessão:** estabelece, mantém e sincroniza o diálogo entre o emissor e o receptor.
- **Camada de Apresentação:** lida com a tradução no formato dos dados, criptografia e compressão.
- **Camada de Aplicação:** Proporciona acesso à comunicação dos usuários (que pode ser uma pessoa ou um programa). Neste nível, temos a noção de um fim útil para a comunicação, como enviar um *e-mail* (correio-eletrônico), transferir um arquivo ou uma mensagem instantânea (p.ex. *MSN*).

Competência 02

Todo e qualquer equipamento que participe de uma rede de comunicação está sob os padrões do modelo OSI. Veja o modelo da Figura 28 sob o Modelo OSI.

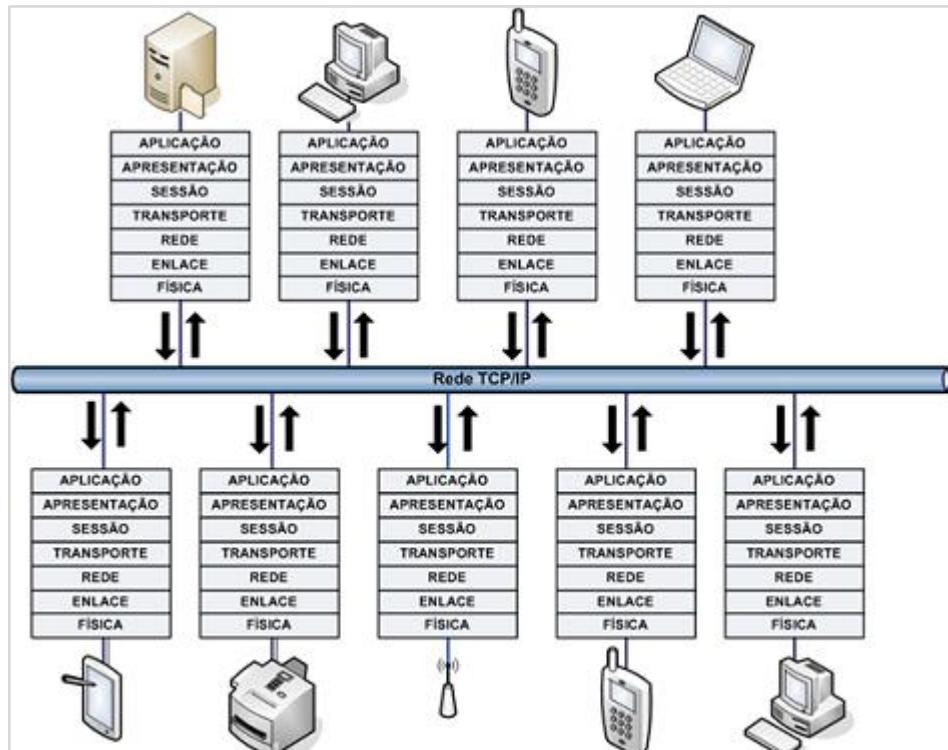


Figura 28- Fluxo de troca de mensagens entre emissor e receptor em uma rede local. Independente do aparelho (hardware) o Modelo OSI é usado como padrão.

Fonte: Produzido pelo autor

Atente bem: O Modelo OSI e TCP/IP são padrões que atuam sobre hardware e software. Eles são independentes, porém se relacionam. Eles estão interligados através da parte física e da parte lógica. Apesar de serem independentes, eles conversam entre si e há intercâmbio de informações entre eles. Você aprenderá sobre este assunto mais adiante no tópico 27.

2.3 O Modelo TCP/IP

Você sabia que em redes de computadores, o protocolo mais utilizado no mundo é o TCP/IP – *Transmission Control Protocol / Internet Protocol*. (Protocolo de Controle de Transmissão / Protocolo Internet). Este protocolo

Competência 02

faz computadores, tablets e celulares do mundo inteiro se comunicarem através da “Rede das Redes”, a Internet.

A sigla TCP/IP traz dois protocolos na sua descrição. O TCP tem a ver com o transporte dos dados pela rede. O IP tem a ver com o endereçamento do dispositivo na rede (computador, tablet ou um celular). Em poucas palavras, o TCP transporta a informação de um endereço para outro. O IP é o responsável pelo endereço do emissor e receptor. Fazendo uma comparação, o carteiro que transporta a informação (carta) é o TCP e o endereço de onde a carta saiu até a sua casa (que tem informações como cidade, rua, número e bairro) é regido pelo IP.

Na verdade, o TCP/IP não significa apenas dois protocolos resumidos em uma sigla. O TCP/IP é um conjunto (arquitetura ou suíte) de protocolos divididos em camadas. Estas camadas têm funções específicas, cada uma com suas especialidades (semelhante ao Modelo OSI). Note na figura 29 as camadas que classificam o TCP/IP. As camadas são numeradas de baixo para cima. A camada física está mais ligada aos meios de transmissão e a camada de aplicação tem a ver com os softwares e protocolos utilizados por você para trocar informações em uma rede local ou mesmo na Internet.



Figura 29- Camadas do Protocolo TCP/IP.
Fonte: Produzido pelo autor.

Competência 02

A Figura 30 traz o mesmo modelo só que, desta vez, com os principais protocolos de cada camada. Perceba que quando utilizamos o nosso navegador de internet (Internet Explorer, Firefox ou Chrome) estamos utilizando um protocolo da camada de aplicação, o HTTP. Quando digitamos um endereço como o <http://ead.educacao.pe.gov.br> as outras camadas são acionadas (de cima para baixo, da 4^a para a 1^a) para estabelecer a comunicação com o servidor que contém esta página. Nesta fase, entram o TCP para transportar, o IP para procurar o endereço e as tecnologias para a transmissão dos dados (Placas de Rede, Fibras Óticas, Roteadores e Switchs). É isto que faz o maravilhoso mundo da Internet funcionar.

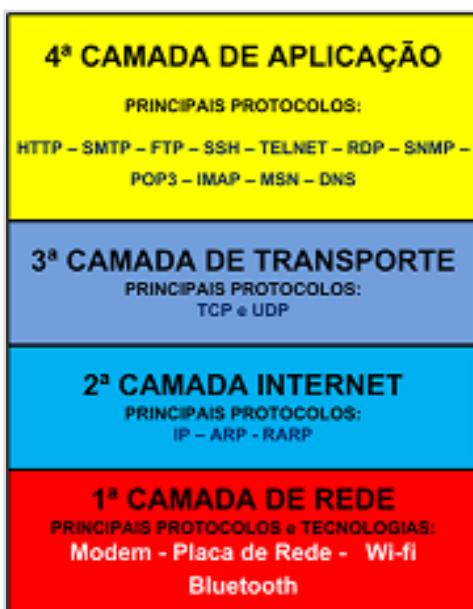


Figura 30- Camadas do Protocolo TCP/IP e seus principais protocolos.
Fonte: Produzido pelo autor.

Lembrando que as duas extremidades (emissor e receptor) que estão “conversando” em TCP/IP utilizam estas camadas, também chamada de Pilha. Veja o fluxo da Figura 31. Todo e qualquer dispositivo que entra em uma rede local ou na Internet precisa falar o protocolo da rede. No nosso caso o TCP/IP. Note que a Pilha TCP/IP está embutida em todo aparelho, seja ele um PC, Tablet, Celular ou Impressora. Perceba que é a mesma figura utilizada na Figura 28. O Modelo TCP/IP e o Modelo OSI estão intimamente interligados,

Competência 02

um mais voltado a padrões de hardware e transmissão e o outro relacionado ao protocolo de comunicação.

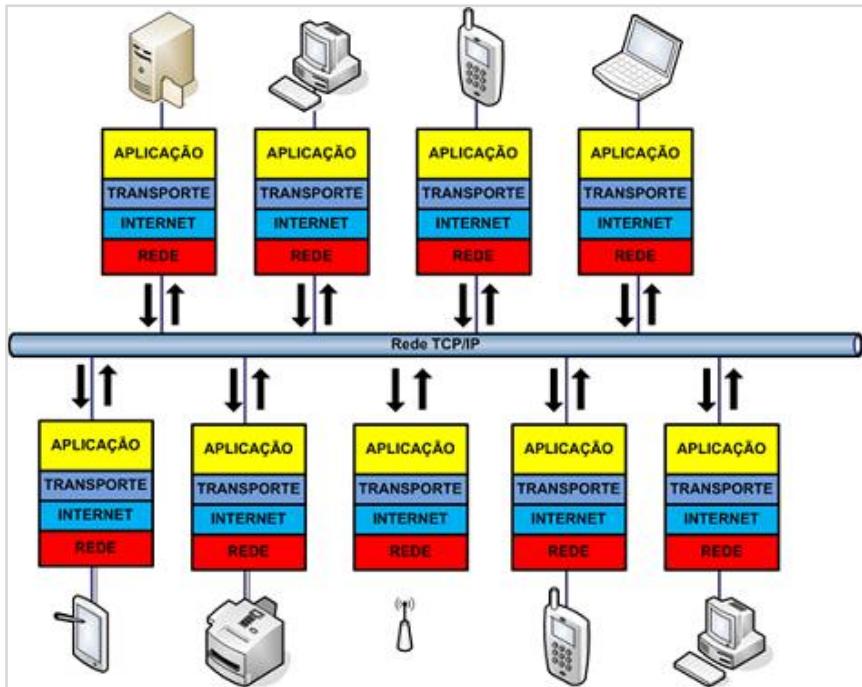


Figura 31- Fluxo de uma rede com o protocolo TCP/IP.

Fonte: Produzido pelo autor

Vamos conhecer um pouco de cada camada e suas funções? Lembrando que vamos estudar de acordo com a hierarquia do Modelo TCP/IP: Camada Rede, Camada de Internet, Transporte e Aplicação.

- **Camada de Rede:** as funções aqui são as mesmas que no modelo OSI, porém, o TCP/IP não define qualquer protocolo de maneira fixa. A ideia é que o modelo possa funcionar sobre qualquer protocolo e com qualquer meio de transmissão disponível.
- **Camada Internet:** nesta camada, o protocolo utilizado é o IP (*Internet Protocol*). Protocolo não orientado a conexão (estudaremos isto mais adiante) e sem controle de erros e confirmações de que a mensagem foi entregue ao destino. Isto significa que estes controles precisam ser feitos nas camadas superiores, se forem necessários.

Competência 02

A unidade básica de mensagem no IP é o **datagrama**. A mensagem que a camada superior passar para o IP. Essa mensagem pode ser subdividida em datagramas, se ela for muito grande. Isto acontece porque o datagrama tem um tamanho máximo.

A camada de Internet ainda suporta outros protocolos: ARP, RARP, ICMP e IGMP. Cada um presta um serviço específico para a comunicação.

- **Camada de Transporte:** três protocolos podem ser utilizados nesta camada: TCP, UDP (*User Datagram Protocol*) e SCTP (*Stream Control Transmission Protocol*). O SCTP é o mais novo e serve para transmissão de conteúdo multimídia, como voz. Os restantes diferem quanto aos controles de erro, sequência e confirmações de entrega de que falamos na camada de rede. O TCP fornece esses controles, ao passo que o UDP não. Portanto, o UDP é normalmente utilizado em redes locais, pois as chances de erro na transmissão são pequenas.
- **Camada de Aplicação:** combina as camadas de sessão, apresentação e aplicação do modelo OSI. Aqui, as aplicações definem seus próprios protocolos que, por sua vez, utilizam os protocolos da camada de transporte. Nesta camada, temos aplicações para as mais diversas tarefas, como transferência de arquivos e transferência de páginas Web (que você usa no navegador).

2.4 Modelo OSI X TCP/IP

Atenção! O Modelo TCP/IP foi desenvolvido antes do modelo OSI. Inicialmente, este modelo tinha apenas quatro camadas: aplicação, transporte, rede e a camada de acesso à rede. Esta última corresponde às camadas Física e Enlace do modelo OSI. Por causa disso, hoje se considera que o modelo TCP/IP possui na verdade **cinco camadas**: *aplicação, transporte, rede, enlace e camada física*. (Forouzan, 2007).



Saiba Mais:

Alguns autores, como Forouzan, citam o modelo TCP/IP em cinco camadas, subdividindo a camada de Rede em duas Camadas: Física e de Enlace, ficando a divisão da seguinte forma:

- Aplicação,
- Transporte, Rede,
- Enlace e Física.

Outros autores citam a camada de Rede como uma única camada. Preferimos seguir o modelo em quatro camadas.

Alguns livros trazem ainda a camada de Rede com o nome de **Acesso a Rede**.

Competência 02

Quando o modelo OSI foi desenvolvido, achava-se que ele iria ser o modelo padrão nas redes de computadores, porém, isso não aconteceu (STALLINGS, 2005). O TCP/IP virou o protocolo dominante. Quando as empresas começaram a reconhecer a necessidade de interoperabilidade entre as redes, somente o TCP/IP estava disponível e maduro o suficiente para ser utilizado. Além disso, o modelo OSI é mais complexo e não tem uma distribuição uniforme de tarefas entre as camadas. Algumas camadas ficaram com muita responsabilidade, enquanto outras, com responsabilidades muito simples.

Na figura 32 temos as camadas do modelo TCP/IP aplicadas sobre as camadas do modelo OSI, para facilitar a comparação.

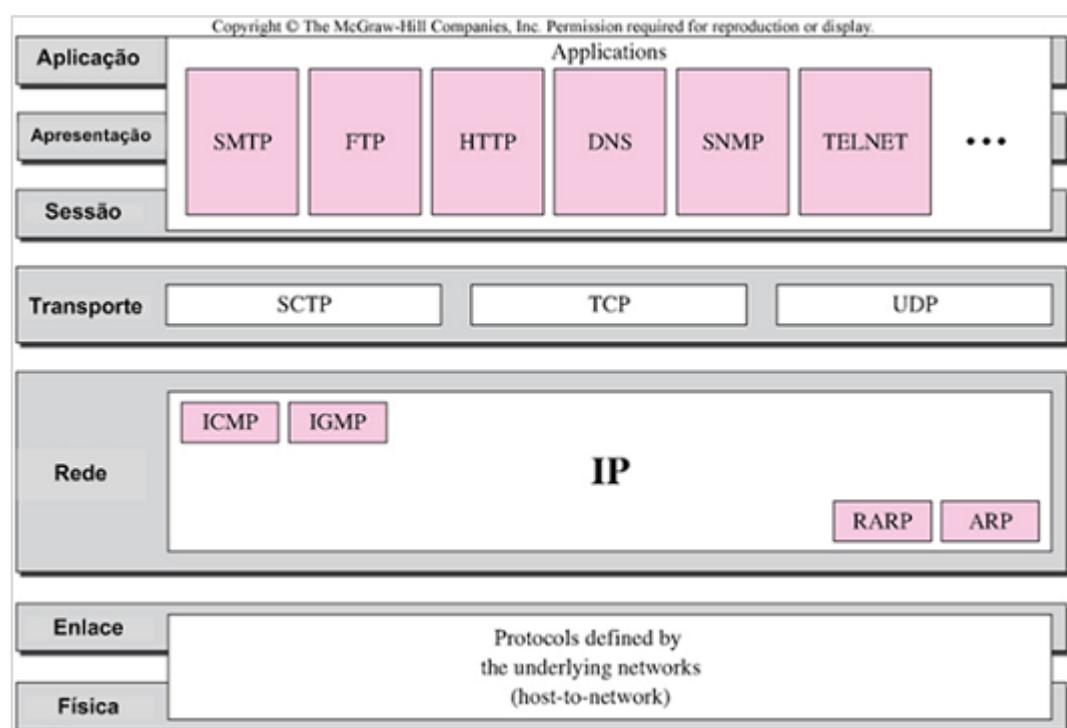


Figura 32- Camadas do modelo TCP/IP sobre o Modelo OSI. Perceba a relação das 7 camadas em cinza por baixo das 5 camadas do TCP/IP. Note, por exemplo, que as camadas de Aplicação, Apresentação e Sessão do OSI relacionam-se diretamente com a camada de Apresentação do Modelo TCP/IP.

Fonte: (FOROUZAN, 2007)

2.5 Estudo das Camadas

A partir de agora, caro (a) aluno (a), apresentaremos o nosso curso na ordem

Competência 02

das camadas. Para entender bem de redes de computadores, é necessário que você perceba onde está localizado o recurso que você está utilizando e de quais camadas ele faz uso. Além disso, as camadas prestam serviços umas às outras. Estudaremos de acordo com os modelos, de baixo para cima. Começando da camada mais baixa (Física e Rede) até a camada mais alta (Aplicação).

2.5.1 Camada de Rede

A camada de rede está intimamente ligada à camada física. Esta camada tem a ver com cabos, conversores, placas e interfaces. Na nossa terceira semana, detalharemos esta camada, seus principais componentes e aplicações.

2.5.2 Camada Internet

Enquanto a camada física (rede) se preocupa em transferir a mensagem de uma máquina para outra na mesma rede, a camada de rede é responsável pela entrega das mensagens desde a origem até seu destino final, independente de quantas redes haja no caminho.

Quando interligamos redes independentes, para ir de um ponto a outro, passando por redes diferentes, é possível ter mais de um caminho. Da mesma forma quando uma pessoa vai viajar entre cidades distantes. Em cada cidade intermediária é necessário consultar um mapa para saber qual caminho ou rota tomar. É este “mapa” da rede que a camada de enlace não conhece (camada abaixo). Mas a camada de rede sim, e sua principal função é traçar estes caminhos ou rotas para cada mensagem. Este processo é chamado de **roteamento**.

Na camada de rede temos também o problema do endereçamento. Vimos que na camada de enlace cada máquina tem um endereço físico, chamado endereço MAC. Porém, este endereço funciona como um número serial que é atribuído à placa de rede (ou a um dispositivo equivalente) pelo fabricante.



Fique de Olho

Poderíamos imaginar que o roteamento é feito apenas uma vez para cada mensagem na sua origem, como uma pessoa que planeja uma viagem. Porém, não é o que acontece. O roteamento é executado todas as vezes que a mensagem passa na fronteira entre uma rede e outra. Desta forma, o roteamento fica mais flexível e se adapta, por exemplo, a uma falha temporária em algum dos caminhos, quando então a mensagem é enviada por uma rota alternativa. Os dispositivos que interligam as redes e, portanto, fazem o roteamento para as **mensagens são chamados de roteadores**.

Competência 02

No caso da camada de rede, como precisamos nos preocupar com um endereçamento global das máquinas, precisamos de um tipo de endereço que, sozinho, seja suficiente para identificar e localizar uma única máquina no meio de tantas redes interligadas. O endereço MAC é apenas um número, e precisamos de um endereço como *rua, bairro, cidade, estado*, ou seja, um endereço de uma estrutura hierárquica. Desta forma, poderemos direcionar cada mensagem para uma rede mais próxima do seu destino observando cada parte do endereço, como fazem os correios.

Para se ter uma ideia do poder da estrutura hierárquica, lembre-se de que podem existir várias casas de número 120, mas estando uma em cada rua, podemos achar cada casa sem confusão. Agora, que tal conhecer como funciona o endereçamento da camada de rede?

2.5.3 IP: Protocolo Internet

a) Endereçamento Lógico

Como vimos, precisamos de um endereço que identifique unicamente um computador em toda a rede mundial, e não apenas na rede local. Os endereços são ditos lógicos, pois os endereços físicos são os da camada de enlace (Endereço MAC).

No IP (*Internet Protocol*), chamamos isto de **endereço IP**. Consistem em 32 bits (4 bytes ou **octetos**). O **IPv4** é o endereçamento IP versão 4, e ainda é o mais utilizado.

Com 32 bits podemos criar até 4,294,967,296 endereços diferentes, e ter, então, até esta quantidade de dispositivos ligados à *Internet*. Porém, para poder atender a especificações especiais e manter uma ideia de hierarquia para possibilitar o roteamento correto, a quantidade de endereços utilizáveis é bem menor.

Competência 02

Como são 4 octetos, a notação utilizada é escrever os valores dos octetos separados por pontos. Ela é conhecida como **notação decimal**.

Por exemplo: **74.125.53.99**

Agora, deve ter surgido uma pergunta, não é, caro (a) aluno (a)? Se o endereço é um número, como usá-lo para achar um endereço na rede global, como um endereço com campos número, cidade, país, etc? Na verdade, o endereço IP é dividido não fisicamente, mas logicamente, em endereço de rede e de máquina (*host*). Da mesma forma, os números de telefone não indicam a região do país, a cidade e até o bairro da residência. Se eu lhe der o número 8134530122, ou na “notação decimal” 81.1234.5678, você automaticamente sabe que se trata de um telefone de Pernambuco por causa do DDD 81, correto? Mas, note que esta divisão não aparece diretamente no endereço. Neste caso nós sabemos pela experiência em usar números de telefone, mas não é o caso com os endereços de rede.

É necessário outro parâmetro para identificar onde termina uma parte do endereço e começa a outra, porque *este limite não é fixo*. Este parâmetro é chamado **máscara de rede (subnet mask)**.

No endereço IP, a parte da rede está sempre da ponta esquerda para o centro, e o do *host* usa o restante dos *bits* até a ponta direita. Então, a máscara de rede é um número também de 32 *bits*, que tem *bits* 1 da ponta esquerda até onde o endereço de rede deve terminar. Os demais *bits* são 0 e correspondem à parte do endereço que cabe ao *host*.

Exemplo:

74.125.53.99 com máscara 255.0.0.0

Esta máscara tem os primeiros 8 *bits* com valor 1 (representado pelo número 255) e todos os outros zero. Portanto, a parte do endereço 74.125.53.99 que corresponde à rede são só os primeiros 8 bits, que contêm o número **74**. Os



Fique de Olho

Cada octeto, por ter 8 *bits*, pode gerar até $2^8 = 256$ endereços, que vão do 0 ao 255. Outro grande lembrete: o endereço IP é um número só de 32 bits, e, portanto, não tem divisão. A divisão aparente na notação acima é apenas para facilitar a visualização.

Competência 02

outros 24 bits, são para o endereço do *host*. Vamos estudar mais detalhes sobre isto mais a frente.

b) Classes de Endereços

Os mais de 4 bilhões de endereços que o endereço IP pode gerar são divididos em 5 classes: A, B, C, D e E. Mas, não foram divididos igualmente em termos de quantidade.

A classe “A” ficou com metade de todos os endereços, a classe B com um quarto, a classe C com um oitavo, e as classes D e E com 1/16 cada. Veja figura 33.

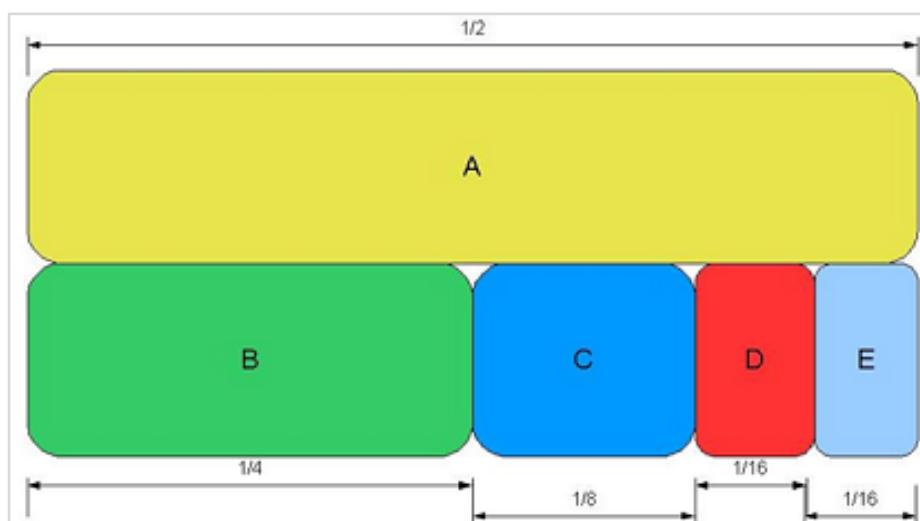
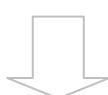


Figura 33- Distribuição quantitativa dos endereços IPv4 em classes

Fonte: Prof. Sílvio Bandeira - www.dei.unicap.br/~silvio/

Pode-se achar a classe de um endereço. Basta observar os primeiros dígitos do endereço, seja na notação binária ou decimal, como mostra a figura 34.



Competência 02

Copyright © The McGraw-Hill Companies, Inc. Permission required for reproduction or display.				
	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

Figura 34- Determinando a classe de um endereço

Fonte: (Forouzan, 2005)

As classes A, B e C têm máscaras padrão (*default masks*). Isto não se aplica às camadas D e E. Observe a tabela 1.

Classe	Binário	Máscara	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Tabela 1- Notações de endereços de IP e Máscaras de Rede.

Fonte: o autor

Observe a última coluna da Tabela 2.1, trata-se de outra maneira de especificar a máscara. Este número $/n$ indica quantos *bits* da máscara são 1, ou seja, o tamanho da parte de rede (*netid*) do endereço. Portanto um endereço 192.168.1.2/24 tem sua máscara definida como um número de 32 bits com os primeiros 24 bits com valor 1, ou seja: **255.255.255.0**

Veja alguns exemplos:

Endereço: 10.0.0.0/8

Corresponde a: **10.0.0.0/255.0.0.0**

Endereço da Rede: **10.**

Endereço dos Hosts: **de 10.0.0.1 a 10.255.255.254**

Total de computadores na mesma rede: **16.777.214**

Competência 02

Endereço: 172.16.0.0/16

Corresponde a: **172.16.0.0/255.255.0.0**

Endereço da Rede: **172.16.**

Endereço dos Hosts: **de 172.16.0.1 a 172.16.255.254**

Total de computadores na mesma rede: **65.534**

Endereço: 192.168.0.0/24

Corresponde a: **192.168.0.0/255.255.255.0**

Endereço da Rede: **192.168.0**

Endereço dos Hosts: **de 192.168.0.1 a 192.168.0.254**

Total de computadores na mesma rede: **254**

c) Endereço de Rede e de Broadcast

Um conceito importante nesta parte é o **endereço de rede**. Este endereço corresponde ao primeiro endereço disponível naquele bloco. Portanto, o endereço de rede é calculado colocando-se zero em todos os *bits* que não sejam da parte da rede, ou seja, na parte do *hostid*. Usando o exemplo anterior, teremos os seguintes endereços de rede para cada bloco:

10.0.0.0/8 endereço de rede **10.0.0.0**

172.16.0.0/16 endereço de rede **172.16.0.0**

192.168.1.0/24 endereço de rede **192.168.1.0**

O endereço de rede representa a organização para o resto da *Internet*, e não uma máquina apenas.

Nas redes de computadores, às vezes é necessário que uma máquina envie uma mensagem a todas as outras que estão na mesma rede. Para evitar que esta máquina tenha de enviar uma cópia para cada uma das máquinas, o que levaria mais tempo, criou-se o conceito de endereço comum, ou **endereço de difusão**, conhecido como **endereço de broadcast**. Ao contrário do endereço de rede, este é calculado colocando-se 1 (um) em todos os *bits* do endereço



Saiba mais:
Os endereços reservados para redes locais (LAN) são:

10.0.0.0/8
172.16.0.0/16 a 172.31.255.255/16
192.168.0.0/24 a 192.168.255.255/24

Quem controla a distribuição dos endereços IPs pelo mundo é o IANA - Internet Assigned Numbers Authority
– www.iana.org



Competência 02

do host (*hostid*). Já que todas as máquinas ligadas a uma rede conhecem a máscara utilizada, todas podem calcular o endereço de *broadcast*. Quando uma mensagem com este endereço aparece na rede, todas as máquinas devem ler.

Vejamos quais os endereços de *broadcast* no exemplo utilizado:

10.0.0.0/8	endereço de broadcast 10.255.255.255
172.16.0.0/16	endereço de broadcast 172.16.255.255
192.168.1.0/24	endereço de broadcast 192.168.1.255

d) ARP/RARP

Vimos que a camada de enlace tem um endereço físico, que é o MAC. Aqui na camada de Rede do Modelo OSI temos outro endereço que chamamos lógico. Naturalmente, surge a pergunta: qual a relação entre um endereço e outro?

As mensagens só podem ser enviadas de uma máquina para outra através do endereço físico (MAC). Portanto, precisamos mapear os endereços IP para os endereços MAC. Existe um programa que faz isso, e as máquinas o utilizam o tempo todo para fazer este mapeamento. Seu nome é **ARP Address Resolution Protocol**, ou Protocolo de Resolução de Endereço. Sempre que uma máquina tem um endereço IP da rede local, e quer saber quem tem este endereço, ela usa este protocolo. Funciona assim: a máquina envia uma mensagem para todos da mesma rede contendo o endereço IP e perguntando de quem é aquele endereço. Apenas a máquina dona do endereço IP enviado responde a quem pergunta enviando seu próprio endereço MAC. Pronto! A máquina emissora já sabe o endereço físico do receptor. Observe na figura 35 que a máquina “A” tenta descobrir qual máquina tem endereço IP 141.23.56.23.



Saiba Mais:
Utilize o site <http://jodies.de/ipcalc> para calcular todos estes parâmetros de endereçamentos IPs. Lá, você coloca o IP e Máscara e ele calcula todo o resto. Procure entender através deste site as numerações padrões como:

10.0.0.0/8
172.16.0.0/16
192.168.1.0/24

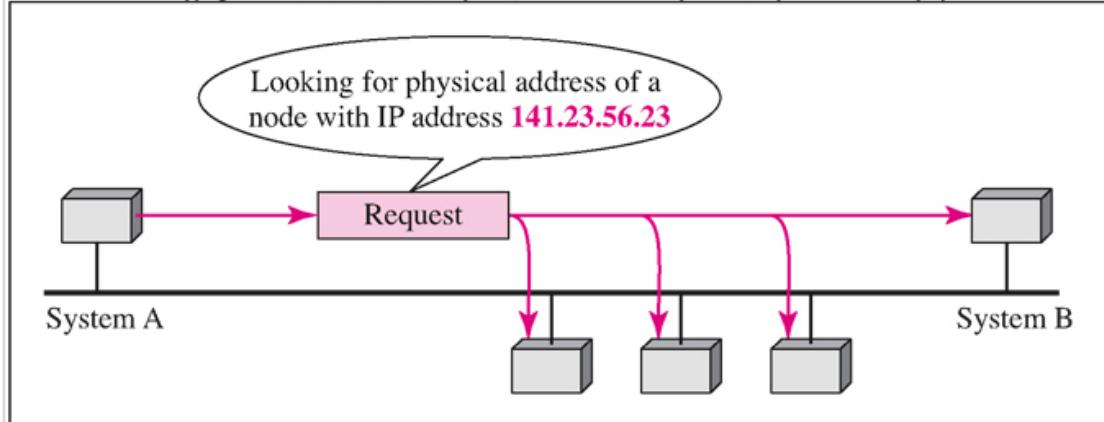
E também máscaras especiais como **192.168.0.1/20**



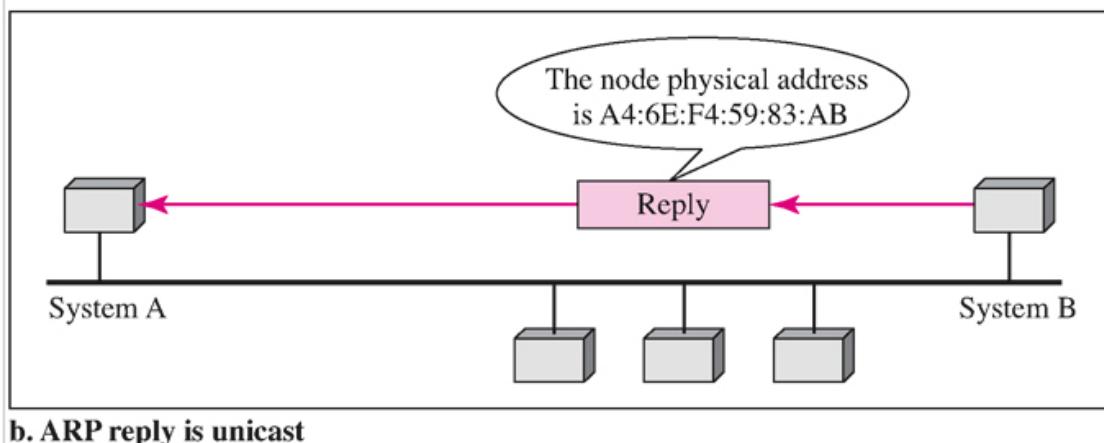
Fique de Olho
Os endereços de rede e de *broadcast* não devem ser atribuídos a nenhuma máquina na rede.

Competência 02

Copyright © The McGraw-Hill Companies, Inc. Permission required for reproduction or display.



a. ARP request is broadcast



b. ARP reply is unicast

Figura 35- Funcionamento do protocolo ARP

Fonte: (Forouzan, 2005)

E quanto ao mapeamento inverso? Quer dizer, se eu souber o MAC de uma máquina e quiser seu endereço IP?. Simples, usamos outro programa: o **RARP** (*Reverse Address Resolution Protocol*, ou ARP Reverso). Aqui, o emissor envia um endereço MAC para receber como resposta o IP correspondente.

Apesar de poder ser usado para saber o IP de uma máquina qualquer, o RARP é usado para uma máquina descobrir seu próprio IP, quando o administrador da rede não colocou um endereço de IP nela manualmente. Serve para configurar os IPs das máquinas automaticamente através de um servidor. Assim, quando uma máquina é iniciada, ela envia o próprio endereço MAC para todos na rede, usando este protocolo, na esperança de haver um servidor local que lhe indique qual IP ela pode usar.

Competência 02

Apesar de o RARP resolver este problema, outros protocolos como o DHCP são a escolha para configurar o IP das máquinas a partir de um servidor.

e) Protocolo DHCP

Para resolver o problema do tópico anterior, usa-se o **DHCP** (*Dynamic Host Configuration Protocol*, ou Protocolo de Configuração Dinâmica de Hosts). O DHCP foi criado para fornecer tanto mapeamento fixo (estático) como dinâmico de IPs. Assim, você indica, no seu servidor DHCP, qual a faixa de IPs da rede que podem ser dado às máquinas que não estão na tabela. Ele, então, escolhe um endereço disponível quando uma máquina assim solicita um IP.

Considere o DHCP como um dos mais importantes serviços dentro de uma infraestrutura de uma rede. Ele é tão importante para facilitar a vida de quem pretende entrar em uma rede de computadores quanto para o administrador da rede que, devido à configuração automática de um número de IP, fica livre para outras tarefas. O DHCP tem facilitado a nossa vida diariamente, mesmo que nós não percebemos. Um exemplo bem prático: toda vez que você conecta na rede 3G da sua operadora; ou entra em um shopping ou faculdade/colégio que tem acesso à Internet de forma gratuita; ou ainda em cidades como Caruaru que tem serviço de Wi-Fi (Redes sem fio) funcionando em alguns bairros; o seu dispositivo (celular, computador ou tablet) recebe todas as configurações necessárias para ingressar na rede, dentre elas, um número de IP, a máscara de subrede, o gateway padrão e os servidores DNS da rede. Após esta etapa, é que seu dispositivo estará apto para navegar na rede local ou mesmo na Internet.

Já imaginou se toda vez que você quisesse dar uma olhada nos seus e-mails ou dar uma espiadinha no facebook fosse necessário uma configuração deste tipo?

Número de IP do Celular: 200.249.243.33

Máscara de Subrede: 255.255.255.0

Competência 02

Gateway: 200.249.243.245

DNS Primário: 200.249.243.1

DNS Secundário: 200.249.243.2

E toda vez que você desligasse o 3G e quisesse conectar novamente teria que digitar todos estes números? Imaginou? Que transtorno...

Para facilitar a vida do Sysadmin (Profissional que administra uma rede de computadores), um Servidor DHCP pode ser montado. Geralmente, em pequenas organizações, este profissional pode optar em colocar IPs fixos nas estações de trabalho. Mas, se em determinado momento, a empresa solicitar que exista uma rede sem fio para que funcionários e visitantes possam acessar, a única maneira de deixar esta operação de forma automática é usando este servidor.

Um servidor DHCP é tão simples de montar, que já vem embutido em Access Points do Mercado (Pontos de Acessos de Rede sem fio) do tipo estudado no tópico 1.5.6 da semana passada. Vejam uma configuração simples de um Servidor DHCP em um Roteador Wi-Fi disponibilizado pelas operadoras do Estado de Pernambuco:

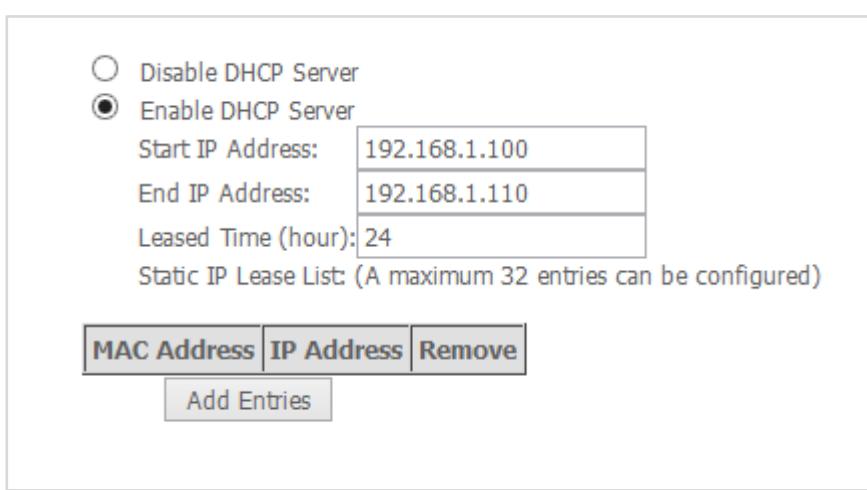


Figura 36 - configuração de um Servidor DHCP em um Roteador Wi-Fi
Fonte: Produzida pelo autor

Competência 02

Note que foi disponibilizado 10 endereços de IPs. De 192.168.1.100 até 192.168.1.110, ou seja, esta rede sem fio suportará até 10 dispositivos conectados ao mesmo tempo. Esta faixa de IPs é chamada de **RANGE** (intervalo em inglês). Se chegar o 11º ele será negado. Outro campo importante é a duração do Lease (aluguel) do endereço IP. Note que um dispositivo ficará no máximo 24 horas com este endereço garantido, após este tempo, haverá uma renovação do aluguel.

É possível atribuir endereços de IPs automaticamente de três maneiras: dinâmica, automática e manual.

- **Dinâmica:** É o método mais comum. O Servidor DHCP tem uma faixa de endereços (conhecida como range) e aluga (lease) estes endereços por um tempo determinado. Quando este dispositivo é desligado, o endereço IP fica livre novamente para outro dispositivo.
- **Automática:** Este método é parecido com o dinâmico, a principal diferença é que o servidor DHCP irá “preferir” fornecer o último endereço alugado para o mesmo dispositivo. Caso isto não seja possível, outro endereço é atribuído.
- **Manual:** Esta forma requer algumas configurações. Garante que um dispositivo sempre irá receber o mesmo IP (diferente da forma automática, que faz isso se for possível). Nesta forma um endereço IP é reservado para o dispositivo e este número não poderá ser utilizado por outro. A reserva é feita atrelando o número de IP ao MAC da placa de rede. Assim, toda vez que a máquina for ligada e solicitar um número de IP na rede, ele será direcionado a ela.

Como funciona o Protocolo DHCP?

O DHCP usa a estrutura de Cliente/Servidor. O Servidor DHCP tem números de IPs para oferecer. Mas, como as estações são capazes de receber um número

Competência 02

de IP se elas não têm conhecimento de quem é o servidor? Nesta hora, entram os controles deste protocolo, que faz que em qualquer rede um dispositivo possa solicitar as configurações necessárias para ingressar nesta rede.

Esse procedimento envolve quatro passos: Discover, Offer, Request e Acknowledge.

- **Discover** – Quando o cliente solicita o endereçamento.

O Cliente (dispositivo) envia um pacote denominado de **DHCPDiscover** para todos os equipamentos da rede utilizando o recurso de Broadcast (vimos no tópico 2.4.3). Esta mensagem é do tipo, “Quem tem um IP para me oferecer?”

- **Offer** – É fornecido o endereço ao cliente.

O Servidor DHCP ao reconhecer o **DHCPDiscover** manda um pacote UDP chamado de **DHCPOffer**, oferecendo um endereço IP para a estação que acabou de solicitar.

- **Request** - O endereçamento é aceito.

Quando o dispositivo recebe o pacote **DHCPOffer**, envia mais um pacote ao servidor solicitando utilizar este número de IP. Esta solicitação é feita através de um pacote UDP chamado **DHCPRequest**.

- **Acknowledge** – O endereço é listado no servidor, o IP é nomeado como pertencente àquele host ou interface.

Ao receber o pacote **DHCPRequest** que veio do dispositivo, o servidor DHCP confirma o empréstimo através do pacote **DCHPAck**.



Competência 02

Notaram que a conversa é bem educada? Na figura 37, há um resumo desta negociação do protocolo DHCP:

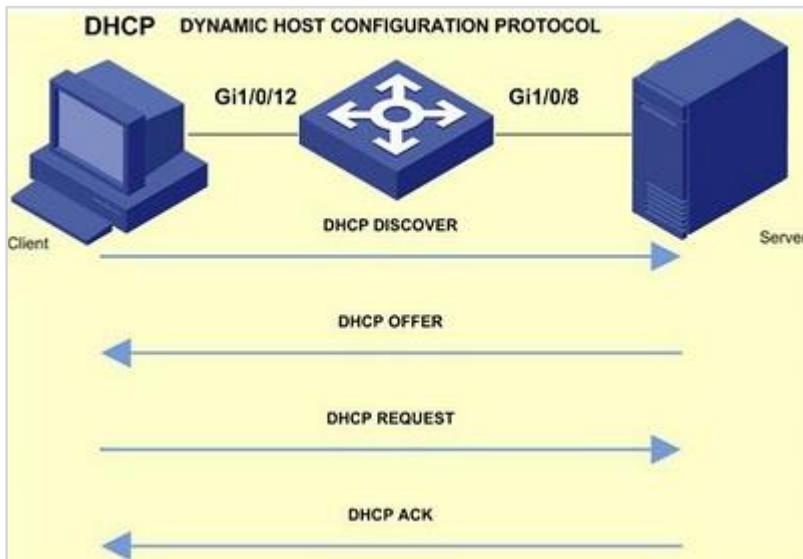
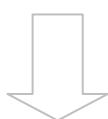


Figura 37- negociação do protocolo DHCP
Fonte: www.esli-hux.com/2012/07/dhcp-guia-completo.html



Competência 02

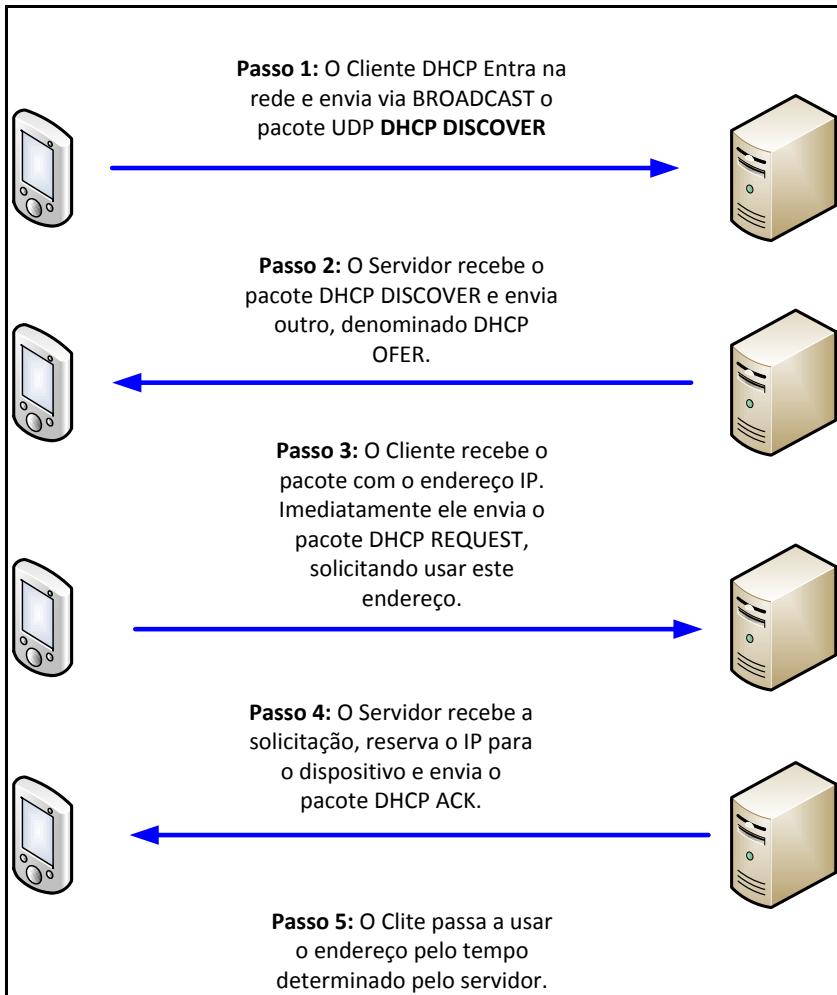


Figura 38 - o fluxo resumido

Fonte: Produzido pelo autor.

Você achou interessante conhecer um protocolo de forma detalhada?

Você mesmo pode visualizar toda esta “conversa do protocolo” utilizando softwares que capturam os pacotes da rede. Estes softwares são chamados de Analisadores de Protocolos ou ainda Sniffers (farejadores em inglês). Vamos ver uma demonstração utilizando o Wireshark, que é um Analisador gratuito e pode ser obtido no seguinte endereço: www.wireshark.org/download

Note que na figura 39 foi colocado no campo FILTER (em verde) que queremos ver apenas pacotes bootp.dhcp. Depois deste passo, é necessário clicar no botão para iniciar a captura (o 3º botão). Em seguida, é preciso forçar uma operação de DHCP. Se você quiser fazer isto no Windows, basta abrir o



Competência 02

prompt de comando e digitar: ipconfig /renew. Se você estiver utilizando linux, acesse o terminal como root e digite: dhclient eth0. Vejam o resultado:

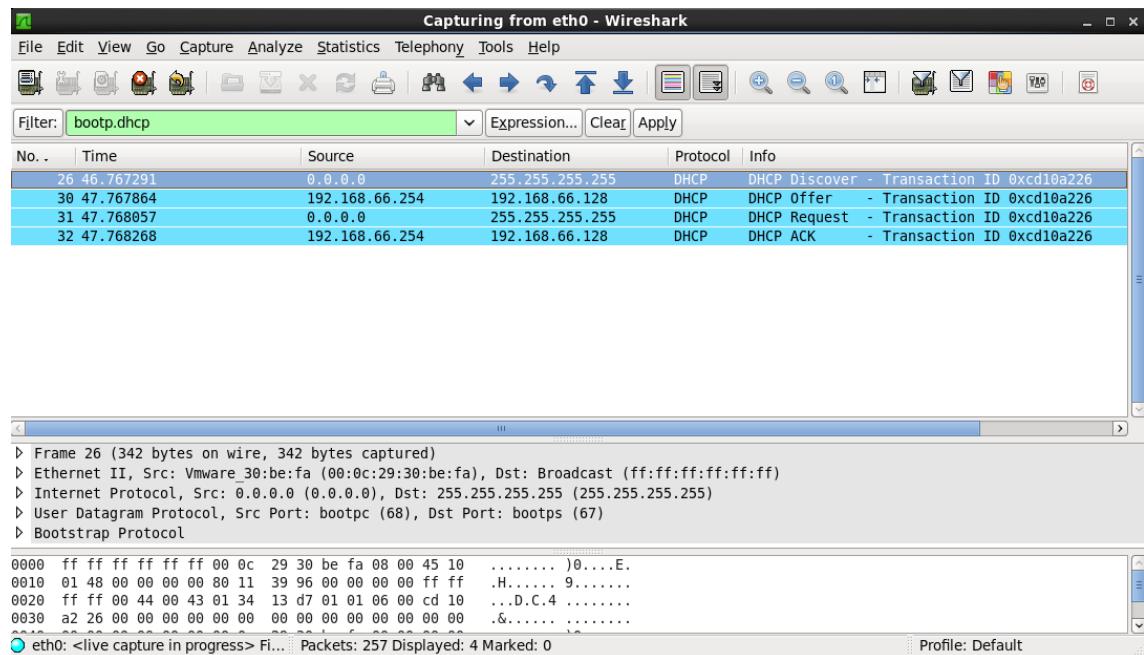


Figura 39 -

Fonte: Produzida pelo autor.

Acompanhe os 4 passos na primeira coluna No, que é o número do pacote na transação do DHCP Server com o DHCP Client.

- **Pacote número 26:** A máquina não tem IP. Está como 0.0.0.0 no campo source (origem) e envia para o endereço de broadcast 255.255.255.255 (destination) o pacote DHCP DISCOVER.
- **Pacote número 31:** O Servidor DHCP tem o IP 192.168.66.254 e oferece o IP 192.168.66.128 através do DHCP OFER.
- **Pacote número 31:** A máquina envia de novo via broadcast o DHCP REQUEST solicitando este endereço
- **Pacote número 32:** O Servidor Confirma através do DHCP ACK.



Saiba Mais

APIPA: Quando o servidor está inacessível, os dispositivos que chegam à rede solicitando endereço IP ficam sem receber as respostas como o DHCPOfer. A maioria dos sistemas operacionais, como Linux e Windows, utilizam um recurso chamado APIPA (Automatic Private IP Address). Este recurso consiste em usar um IP aleatório na faixa de 169.254.X.X com a máscara 255.255.0.0. Isso possibilita que vários dispositivos que não recebem IP válido na rede possam se comunicar mesmo sem a presença do Servidor DHCP. Porém, este endereço não lhe permite acessar redes externas, nem mesmo a Internet.

Competência 02

2.6 Camada de Transporte e Aplicação

Interessante não? Vamos conhecer mais uma camada: A camada de transporte é responsável pela comunicação de uma mensagem inteira, entre processos. E qual seria, caro (a) aluno (a), a diferença para a camada de rede? É que na camada de rede o objetivo é entregar os pacotes desde a máquina emissora até a receptora, sem se preocupar com a mensagem à qual o pacote pertence (lembre-se de que uma mensagem pode ser quebrada em mais de um pacote). Além disso, quando o pacote chega ao receptor a camada de rede não sabe a qual programa ela pertence. Um computador pode rodar mais de um programa (quando o programa está rodando nós o chamamos de **processo**).

Então, a camada de transporte se preocupa em saber a qual mensagem aquele pacote pertence e em que ordem os pacotes devem ser montados para formar a mensagem original e também determinar a qual processo aquela mensagem é destinada.

Você precisa entender a diferença entre as responsabilidades desta camada em comparação com a de rede.

Mas como esta camada sabe para qual processo enviar a mensagem? Simples, mais um endereço. Aqui, definimos o tipo do endereço como **porta de comunicação**. Estas portas são únicas em cada máquina, então um processo pode reservar uma delas e ser identificado pelo endereço desta porta. Como temos mais de um protocolo nesta camada, as portas de comunicação precisam ser identificadas também pelo tipo de protocolo que usam. Então o endereço de uma porta de comunicação contém: ***o protocolo, o endereço da porta e o endereço de rede da máquina***. Lembre-se: são três valores que endereçam uma porta na camada de transporte.

Competência 02

O endereçamento de rede já foi explicado neste capítulo, mas como funciona o endereço da porta? Ele é um número de 16 *bits*, ou 2 *bytes*. Portanto, para cada protocolo da camada de transporte temos 64k endereços de porta.

Em geral, a comunicação de rede funciona como uma caixa postal nos correios. O processo pode receber “cartas” (mensagens) de qualquer outro processo e elas são tratadas como independentes. Cada mensagem tem um conteúdo e os endereços do emissor e receptor (remetente e destinatário). Este tipo de tratamento é chamado de **não orientado à conexão**.

Porém, nesta camada, um protocolo pode utilizar o conceito de **conexão**. Antes de enviar mensagens em qualquer direção (**emissor → receptor ou receptor → emissor**) é necessário que um **caminho virtual** ou conexão seja estabelecido entre os dois. Compare isso com a comunicação através do telefone. É necessário discar o número para onde você está ligando, esperar que alguém atenda (estabelecimento da conexão), para depois começar a “conversa”. A conexão é muito útil, principalmente para a ordenação das mensagens. Como a *Internet* é feita por múltiplas conexões diferentes, pode acontecer de as mensagens tomarem caminhos distintos e chegarem fora de ordem. Numa conexão, cada mensagem recebe um número sequencial de acordo com a ordem em que são enviadas. Quando chegam ao receptor, ele tem condições de verificar se a ordem está correta. Isto, claro, vai depender do protocolo. Em geral, protocolos **orientados à conexão** lidam com **erros de transmissão e fluxo de controle**, ao passo que os **não orientados à conexão** não fornecem esses mecanismos. Estudaremos dois protocolos desta camada: o *User Datagram Protocol (UDP)*, que é **não orientado à conexão**, e o *Transmission Control Protocol (TCP)* que é **orientado à conexão**.

Na camada de transporte, as mensagens individuais são chamadas de **segmentos** e de **datagramas**, dependendo do protocolo usado. Só para diferenciar de **frames** (quadros) da camada de enlace e de **pacotes** da camada de rede. Os nomes servem apenas para diferenciar as mensagens em cada camada.

Competência 02

2.6.1 Comunicação Entre Processos

Você sabia que processos se comunicam usando um conceito chamado **cliente-servidor**. Em um processo local, o cliente utiliza os serviços de outro processo, normalmente remoto, chamado servidor. Por exemplo, usando um navegador como o *Firefox* ou o *Internet Explorer* para acessar uma página na *web* como o www.dominiopublico.gov.br/ você estará usando um cliente (o navegador) para ver o conteúdo armazenado no servidor (o servidor *web* do site citado).

Até agora temos a comunicação na camada de enlace (nó a nó), na camada de rede (**máquina a máquina, ou emissor → receptor**). Para completar a comunicação, a camada de transporte comunica os processos individuais em cada máquina.

Lembre-se de que em uma máquina podem rodar muitos processos ao mesmo tempo (você pode abrir o *office* e um ou mais navegadores). Os vários níveis de comunicação estão exemplificados na figura 40.

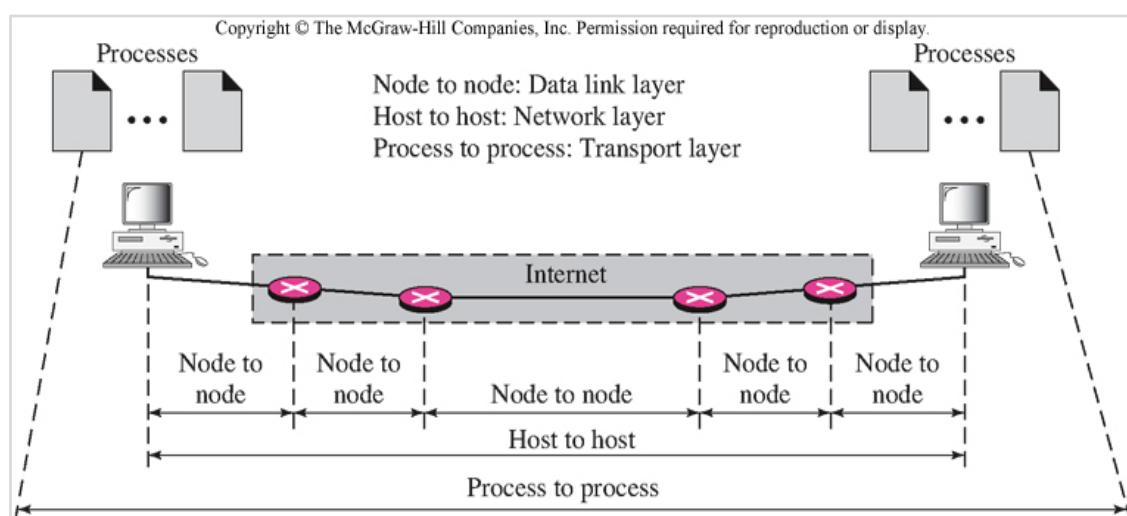


Figura 40- Comunicação vista em vários níveis

Fonte: (FOUROUZAN, 2008)

Competência 02

a) Endereçamento

Nós já vimos que cada nível tem um endereço. Na camada de transporte, este endereço contém o protocolo e o endereço de porta. Vamos nos aprofundar um pouco mais neste assunto?

A porta que o cliente usa pode ser qualquer uma disponível na máquina em que ela é executada. Porém, para se comunicar, o cliente precisa saber qual porta o servidor está usando (além do protocolo e endereço da máquina do servidor). A estratégia utilizada é reservar um número de porta para cada serviço. Então, a porta do servidor não pode ser atribuída aleatoriamente. Por exemplo, para você ligar para sua casa, pode usar qualquer telefone disponível (público ou de um amigo), mas precisa saber o número do telefone de sua casa.

Os serviços que são padrões na *Internet*, como servidores de páginas *Web*, têm portas definidas por uma autoridade reguladora chamada IANA (*Internet Assigned Number Authority*). Assim, os 64k endereços de porta são divididos nas seguintes categorias:

- **Portas bem conhecidas:** de 0 a 1023, são controladas pela IANA.

Exemplo:

Servidor DNS – Porta 53 (UDP)

Servidor HTTP – Porta 80 (TCP)

Servidor FTP – Porta 21 (TCP)

Servidor SMTP – Porta 25 (TCP)

Servidor POP3 – Porta 110 (TCP)

- **Portas registradas:** de 1024 a 49151 não são controladas, mas podem ser registradas para evitar duplicação.

Exemplo:

Competência 02

Servidor Nessus – Porta 1241 (TCP e UDP)

Servidor OPENVPN – Porta 1194 (TCP e UDP)

- **Portas dinâmicas:** de 49152 a 65535 não são controladas nem podem ser registradas. São dinâmicas e podem ser usadas por qualquer processo, seja cliente ou servidor.

2.6.2 Protocolo UDP (User Datagram Protocol)

O protocolo UDP é **não orientado à conexão** e não faz controle de ordenação de mensagem, retransmissão nem controle de fluxo. Por isso, é chamado um **protocolo não confiável**. Este tipo de protocolo não adiciona muita coisa ao serviço fornecido pela camada de rede (IP), a não ser o endereçamento do processo.

Qual a sua utilidade então? A **resposta**: Eficiência. Como é um protocolo simples, exige menos espaço de memória e tempo de processamento para as mensagens. Isto é bom, principalmente se a comunicação usa uma rede com baixa taxa de erros, como uma fibra ótica. Também pode ser usado se a velocidade da comunicação for mais importante e a perda de alguns pacotes não for um problema.

O protocolo UDP utiliza o *checksum* (algoritmo de checagem de erros) para checagem de erro de transmissão, no entanto ele não faz o controle de erros. Isto porque ao detectar um erro em uma mensagem, o UDP simplesmente a descarta e não avisa ao processo nem ao emissor nem ao receptor.

Protocolos como esses são aplicados em videoconferência e em audioconferência. A razão é simples: dados e voz consomem exageradamente a capacidade da rede. Além disso, se protocolos de correção de erros forem utilizados, ninguém conseguirá conversar ou ver um vídeo via Internet. Um bom exemplo é a ligação de celular. Quando a pessoa do outro lado da linha

Competência 02

fala e há uma falha e você não consegue entender, o que você faz? Pede para a pessoa repetir, ou seja, o pacote foi perdido e você pediu a retransmissão.

2.6.3 Protocolo TCP (Transmission Control Protocol)

Ao contrário do UDP, o TCP é um protocolo **orientado à conexão**. Ou seja, para haver comunicação entre os processos uma conexão precisa ser estabelecida. O cliente solicita a conexão ao servidor usando uma mensagem especial. Essa mensagem é utilizada apenas pelo protocolo e não chega ao emissor nem ao receptor. Se o servidor aceitar a conexão, outra mensagem especial é enviada de volta ao cliente para confirmar a conexão. Só depois desse processo, o cliente e o servidor podem trocar dados. A conexão cria um caminho virtual entre os dois processos e as mensagens fluem através deste caminho (figura 41).

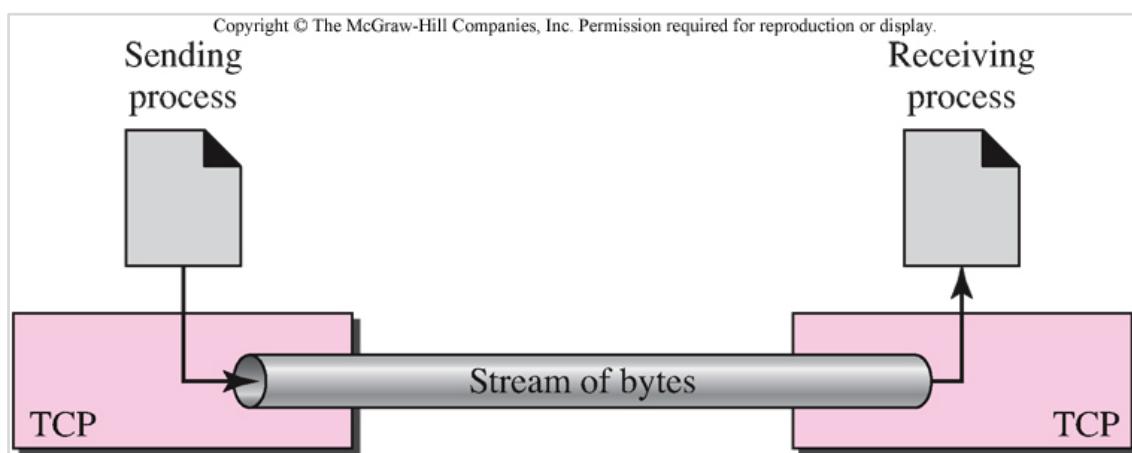


Figura 41- Comunicação utilizando o protocolo TCP
Fonte: (FOUROUZAN, 2008)

Desta forma, os pacotes chegam ordenados, pois o protocolo faz a checagem de ordenação, incluindo um número sequencial em cada um. Além disto, o TCP ainda faz o controle de fluxo. Quer dizer que ele avisa ao emissor quando a velocidade está mais alta do que a que o receptor pode aceitar, para não sobrecarregá-lo nem perder mensagens. Há também o controle de erro com

Competência 02

checksum e retransmissão. Se alguma mensagem chegar com erros ou for perdida no meio do caminho, o emissor receberá um aviso para retransmiti-la. Ao final da comunicação, a conexão deve ser terminada utilizando-se outra mensagem especial. Tanto o cliente como o servidor podem solicitar a quebra da conexão. Notou porque não podemos usar o TCP em uma transmissão de voz e vídeo?

2.6.4 DNS (Domain Name Service)

Nesta seção, iniciamos a **Camada de Aplicação**, que é responsável por fornecer acesso à rede para o usuário. Isto requer um grande número de serviços para envio de correio eletrônico (*e-mail*), compartilhamento e transferência de arquivos, acesso a páginas *web*, gerenciamento de redes, entre outros.

Estudaremos agora um serviço essencial nesta camada, que também é básico para outros serviços: o **DNS**, ou serviço de resolução de nomes. Sabe a sua agenda telefônica, de papel ou no celular? Pois bem, aposte que você sabe praticamente todos os nomes das pessoas que estão cadastradas. Mas de quantos números você se lembra? Ainda que você seja um(a) superdotado(a), não vai recordar da maioria. Isto acontece porque nosso cérebro funciona melhor com nomes que com números. Porém, os computadores usam números para tudo, principalmente para endereços. Lembra do tópico de endereçamento? Muitos números!!!

Para resolver esta diferença entre nós e os computadores, precisamos de um mapeamento, mais ou menos como a agenda telefônica faz: você sabe o nome da pessoa e é feita uma procura na agenda para saber o número do telefone correspondente. A mesma coisa o DNS faz, só que o número que ele retorna é o endereço de rede (aquele tipo 192.168.1.10).

A *Internet* é formada por uma estrutura hierárquica de muitos níveis, ilustrada como uma árvore. Observe a figura 42.

Competência 02

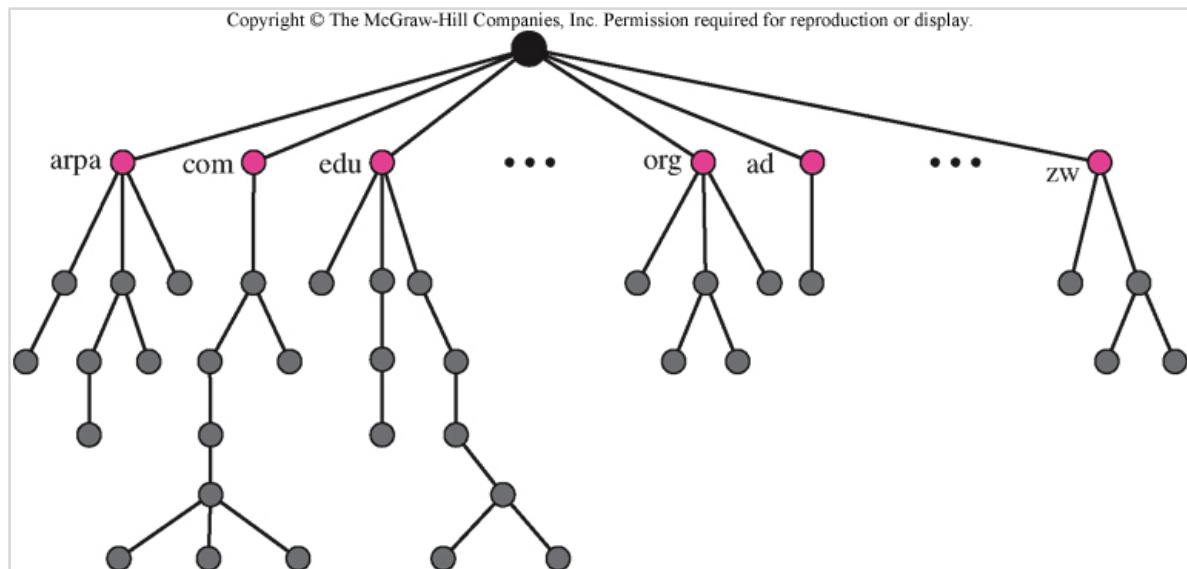


Figura 42- Estrutura hierárquica da Internet. Note os domínios .com, .edu, .org na estrutura. Todos eles partem de um ponto único chamado de Raiz ou root em inglês.

Fonte: (FOUROUZAN, 2008)

Cada “galho” desta árvore, também chamado de subárvore, define um compartimento ou diretório, exatamente como a estrutura de diretórios do seu computador. Só que aqui nós chamamos os diretórios de domínios. E cada domínio pode ter subdomínios, como diretórios podem ter subdiretórios.

Pois bem, quando você quer um arquivo no seu computador você não pode usar o nome completo dele, apenas juntando os nomes dos diretórios desde a raiz até o nome do arquivo. Exemplo: **C:\Meus Documentos\Musica\Luiz_Gonzaga\Asa_Branca.mp3**

Este “caminho” indica que o arquivo Asa_Branca.mp3 está no subdiretório Luiz_Gonzaga, que está no subdiretório Musica, etc. Até chegar na raiz ou '\' (barra).

Analogamente, quando você quer acessar um site na Internet, você também indica onde ele está a partir da raiz.

Exemplo: **www.google.com**

Competência 02

Indica que você quer acessar o servidor de páginas web (www), do google, que é um subdomínio do domínio “com”, que por sua vez é um subdomínio do raiz (root) ou '.' (ponto). A diferença é apenas que no endereço da Internet você começa pelo objeto (a máquina www), ao passo que nos arquivos você começa pela raiz (C:\). E também o símbolo que separa um subdiretório de outro passa da '\' (barra) para o '.' (ponto). Mas a ideia é exatamente a mesma. Observe a figura 43.

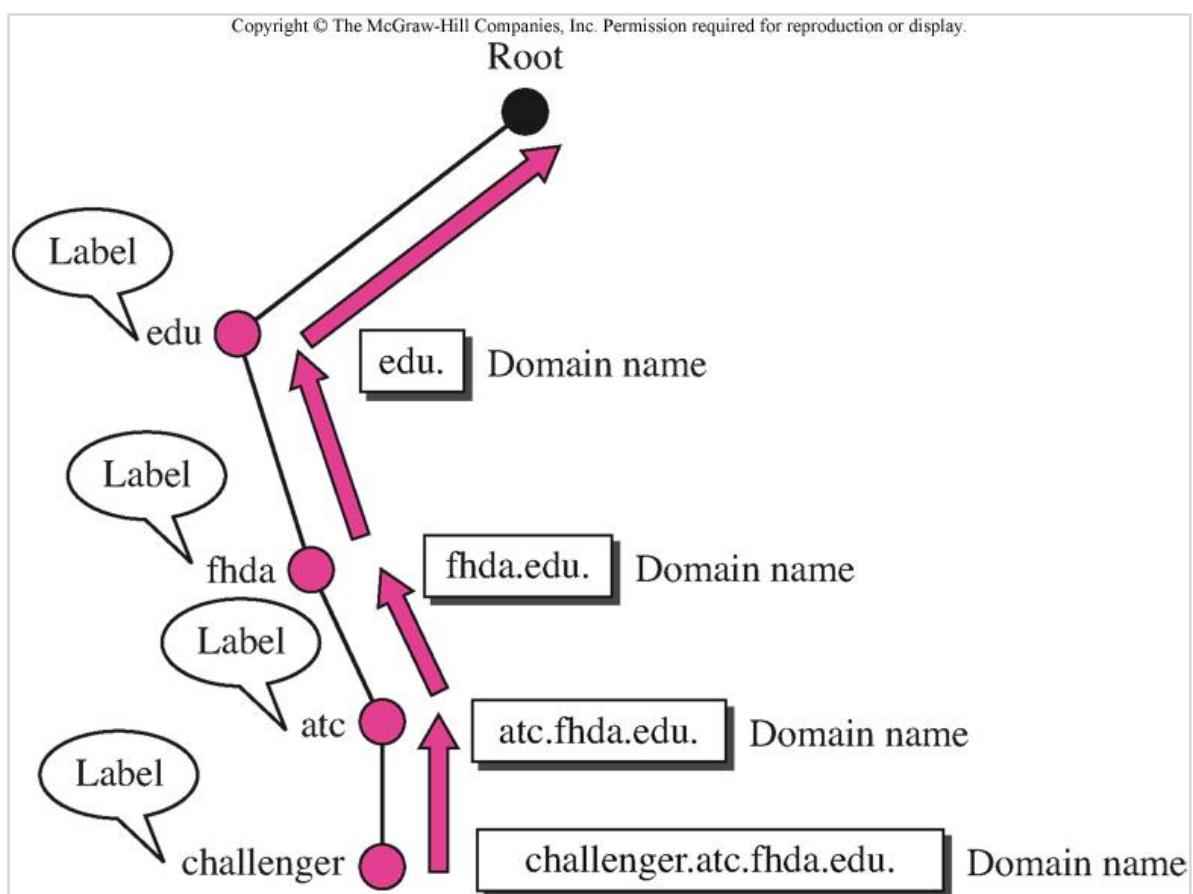


Figura 43- Domínios e subdomínios formando o nome de uma máquina.

Fonte: (FOUROUZAN, 2008)

Pelo fato de haver milhões de computadores ligados à Internet, precisamos de muitos servidores DNS para guardar todos estes endereços e também responder às solicitações de todos os clientes. Desta forma, o DNS não existe em um único servidor, mas há pelo menos um deles em cada rede independente ligada à rede global. Quando você digita um endereço web no seu navegador, ele se encarrega de se comunicar com o servidor DNS do seu

Competência 02

site, ou do seu provedor de Internet, para transformar o nome que você passou em endereço. Um servidor DNS normalmente trabalha em conjunto com os outros servidores espalhados para resolver um nome. Assim, uma requisição sua pode ser repassada por vários domínios na Internet até chegar ao servidor da máquina que você quer acessar, porque ele é que tem o endereço IP (end. de rede) procurado.

2.7 Configurações de Redes no Windows

Depois de vermos toda a teoria necessária para endereçar máquinas sob uma rede TCP/IP o que você acha de praticar um pouco? Então, vamos lá! Vamos ver o exemplo de uma rede simples com endereçamento de rede local 192.168.0.0/24.

Observe na rede da Figura 44, como distribuímos os endereços de IP nesta LAN.

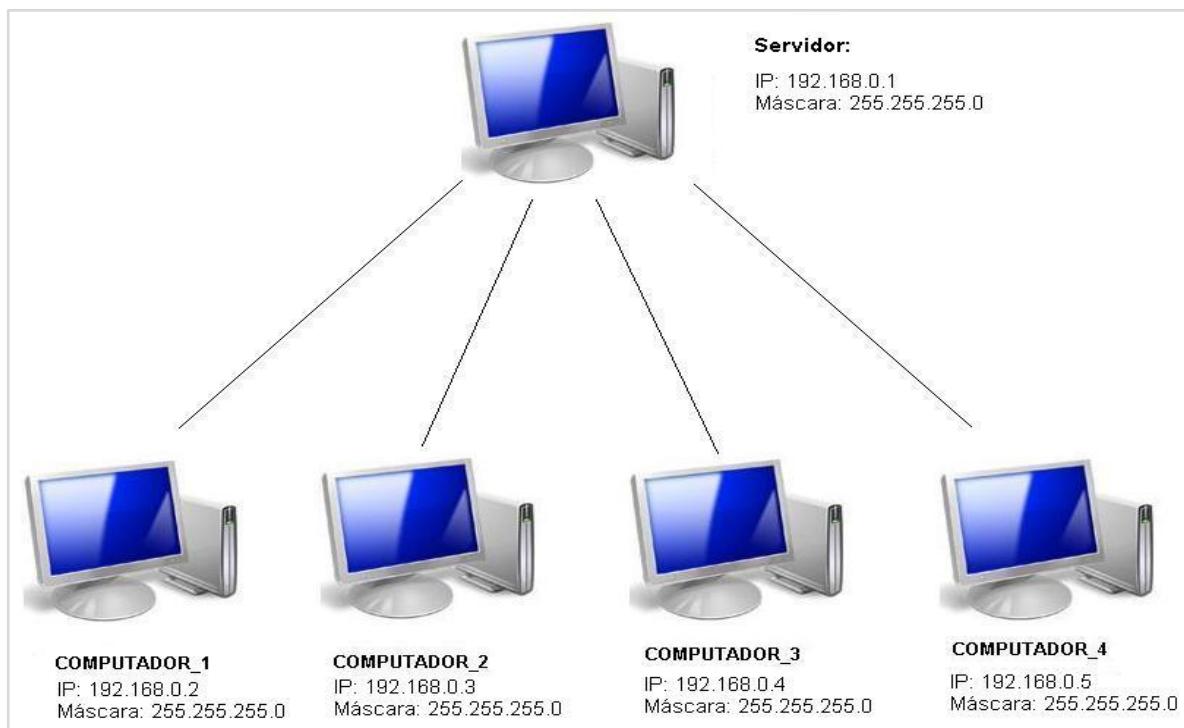


Figura 44- A rede é mantida em todos os hosts (192.168.0) e apenas variamos o último número (octeto). Foi criado em ordem, porém não é obrigatório, podemos atribuir qualquer número aos hosts entre 1 e 254.

Fonte: produzido pelo autor



Saiba Mais

Para estudar um pouco mais sobre o DNS acesse,
<http://tinyurlp.com/redes51>



Atenção:

O primeiro número (octeto) de um endereço de IP e o último número não podem ser 0 quando utilizado em identificação dos hosts.

O último número (octeto) de um endereço de IP tem que estar entre 1 e 254.

Exemplo:
 192.168.0.0 → Endereçamento inválido.
 0.168.0.1 → Endereçamento inválido.
 192.168.0.255 → Endereçamento inválido.

Competência 02

2.7.1 Acessando a Configuração de Rede no Windows

Para acessar as configurações de rede do Windows execute um dos passos abaixo:

- Iniciar / Configurações / Conexões de Rede ou
- Iniciar / Configurações / Painel de Controle / Conexões de Rede ou
- Botão Direito no ícone da Área de Trabalho / Meus Locais de Rede e Propriedades.

A tela resultante deverá ser semelhante a da Figura 45:

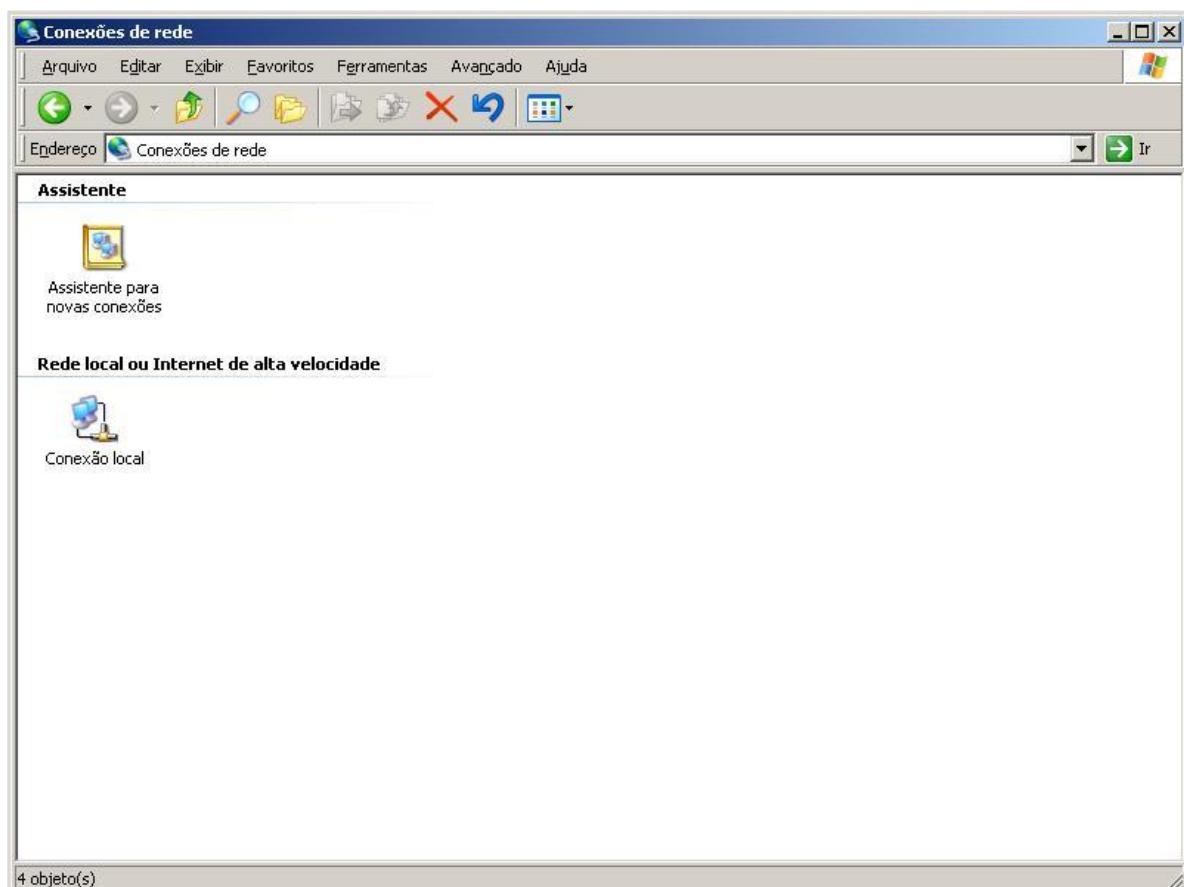


Figura 45- Tela de configuração de Redes do Windows
Fonte: produzido pelo autor

Competência 02

A sua tela poderá ter outras conexões de rede. Mas a que nos interessa é a que está aparecendo na imagem acima, a “Conexão Local”. Para acessar as configurações de rede clique em propriedades. Conforme a Figura 46.

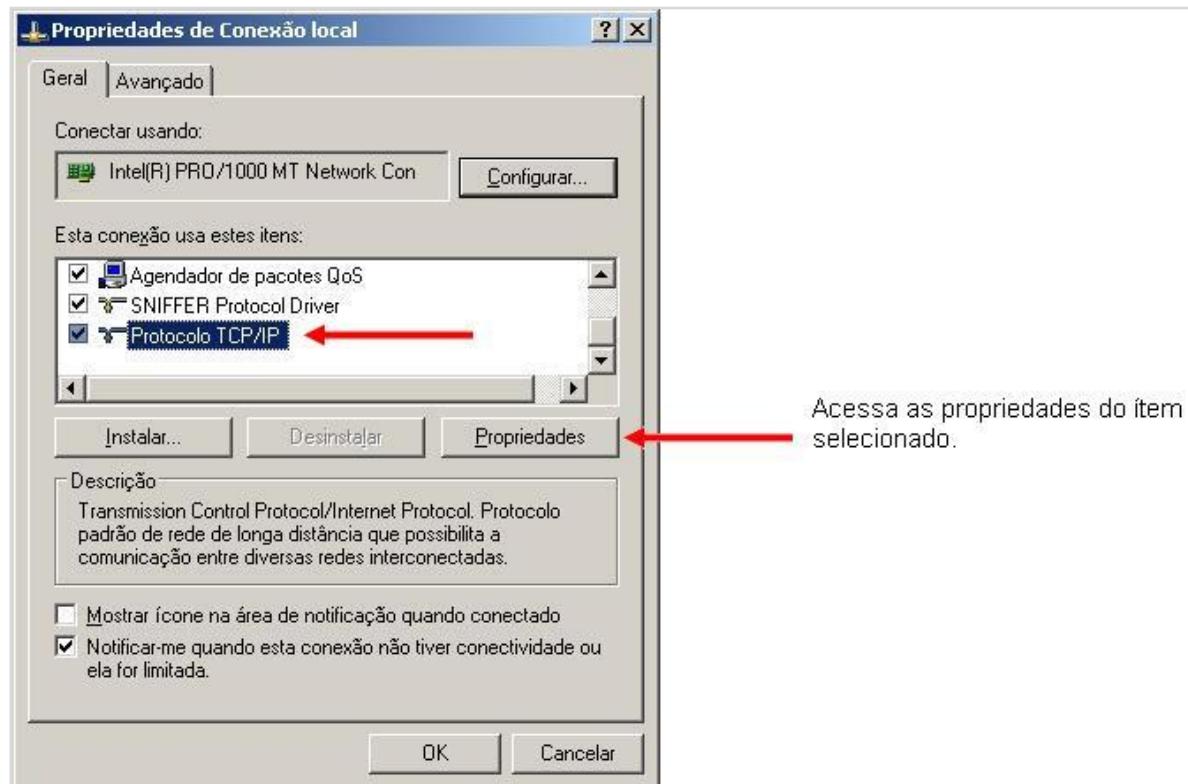
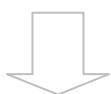


Figura 46- Tela de Propriedades de Conexão Local.

Fonte: produzido pelo autor



Competência 02

Clique em Protocolo TCP/IP e depois em Propriedades. A Tela de configuração do TCP/IP é semelhante a da Figura 47:

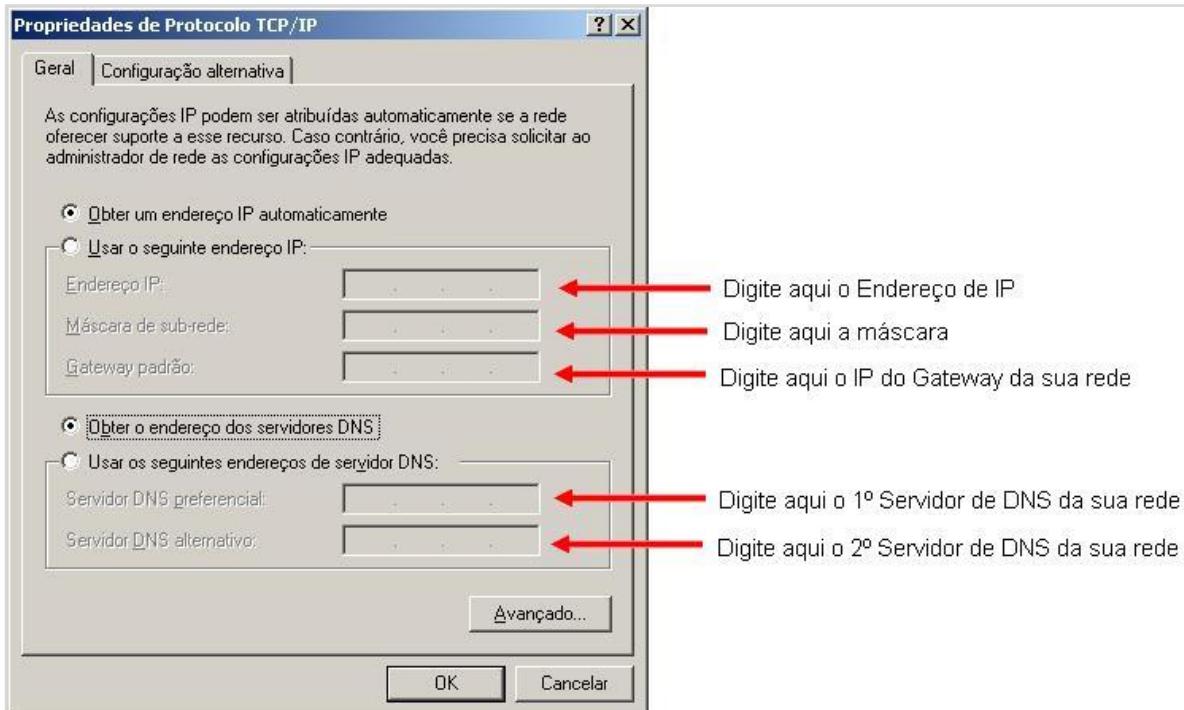


Figura 47- A tela de configuração vem configurada para receber IP automaticamente através de um servidor de números de IP (Servidor DHCP).

Fonte: produzido pelo autor

Note na Figura 2.19 que você precisa preencher os seguintes endereços:

Endereço IP: O endereço de IP desta máquina

Máscara de sub-rede: Máscara de rede desta máquina.

Gateway: É uma máquina intermediária geralmente destinada a interligar redes ou mesmo traduzir protocolos. Exemplos de gateway podem ser os routers (ou roteadores) e firewalls, já que ambos servem de intermediários entre o utilizador e a rede. Um proxy também pode ser interpretado como um gateway (embora em outro nível).

Geralmente o gateway em redes locais é a máquina que dá acesso à Internet (firewall ou proxy).

Servidor DNS Preferencial: Servidor de DNS da rede.

Servidor DNS Alternativo: Servidor de DNS da rede.



Saiba mais: DHCP:
Dynamic Host Configuration Protocol é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede. A função básica do servidor DHCP é distribuir números de IPs de forma automática, facilitando e muito as tarefas de configuração de uma rede local. Em poucas palavras, é um servidor de números de IP.

Competência 02

No nosso caso, vamos por enquanto preencher apenas o endereço de IP e a máscara. Isso já é suficiente para colocarmos as máquinas em rede.

Para colocar um endereço de IP clique em “**Usar o seguinte endereço de IP**” Conforme figura 48:

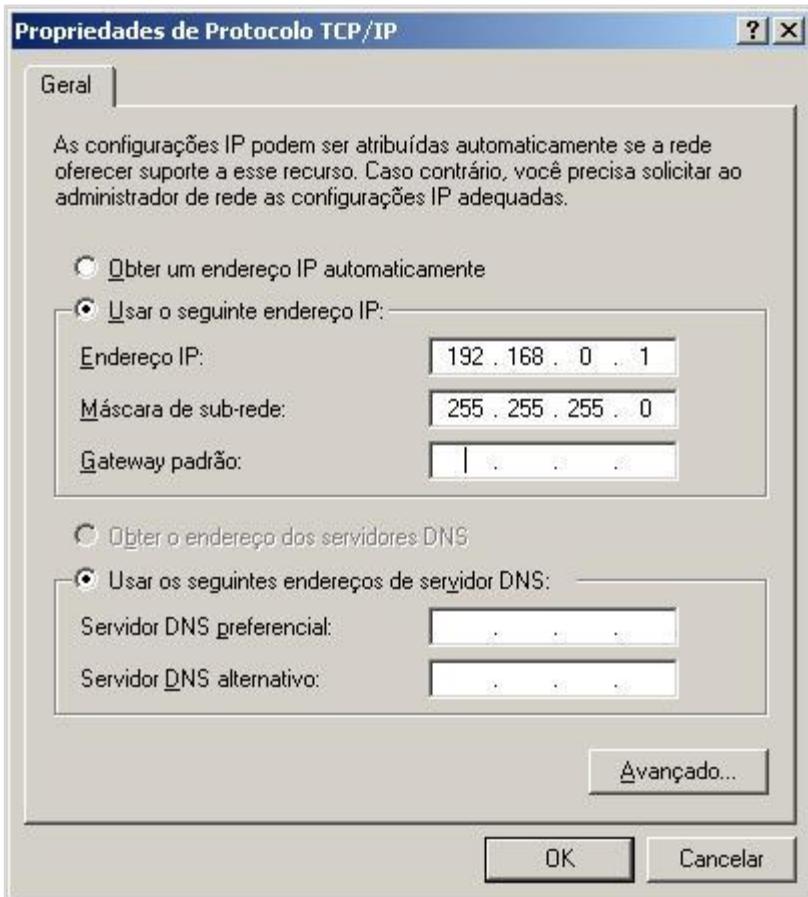


Figura 48- Configuração do Endereçamento de IP

Fonte: produzido pelo autor

Basta repetir este processo nas outras máquinas da sua rede, claro que nas outras mudando o último octeto:

192.168.0.1 → Computador_1

192.168.0.2 → Computador_2

192.168.0.3 → Computador_3

192.168.0.4 → Computador_4

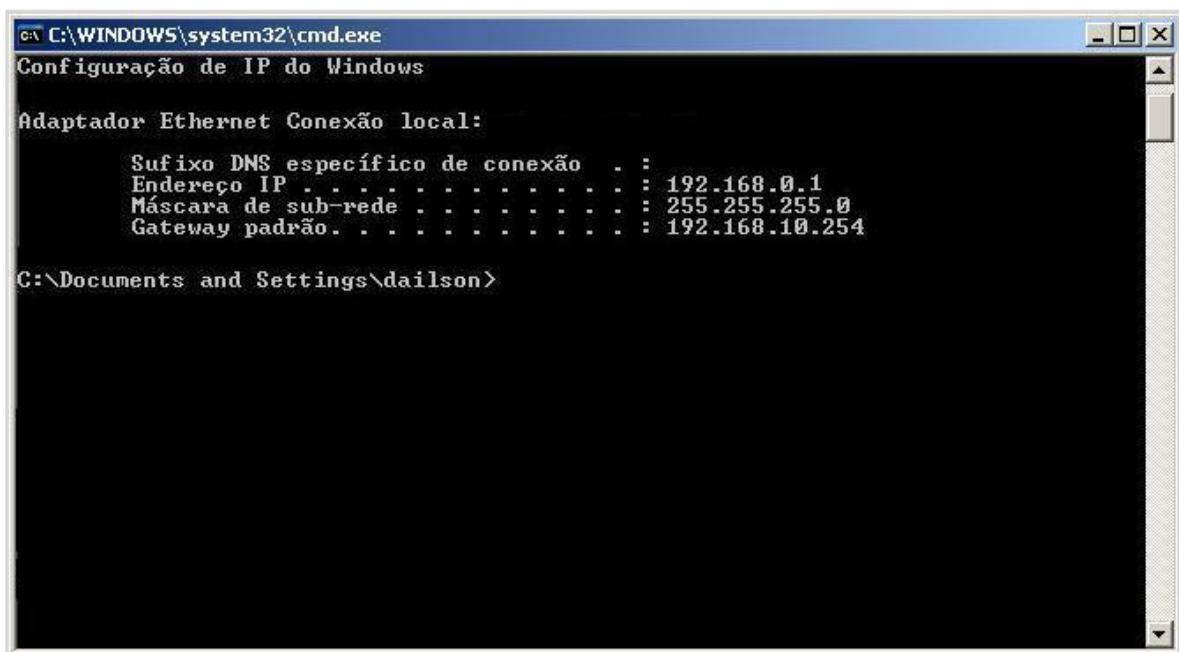
Competência 02

E assim por diante.

Vamos agora mexer um pouco na **Camada de Aplicação**, visualizando e testando as configurações de IP.

Para visualizar de forma rápida o endereçamento de IP, vá em Iniciar / Executar e digite cmd e enter.

Na tela do Shell do Windows (também conhecido como Prompt de Comando) digite o comando ipconfig e tecle enter. O resultado é semelhante a Figura 49:



```
C:\WINDOWS\system32\cmd.exe
Configuração de IP do Windows

Adaptador Ethernet Conexão local:

  Sufixo DNS específico de conexão . . . . . : 
  Endereço IP . . . . . : 192.168.0.1
  Máscara de sub-rede . . . . . : 255.255.255.0
  Gateway padrão. . . . . : 192.168.10.254

C:\Documents and Settings\dailson>
```

Figura 49- Resultado do comando ipconfig

Fonte: produzido pelo autor

Para realizar testes de rede, basta utilizar o comando PING. O comando ping envia um pacote de dados a uma máquina especificada e espera que ele volte à máquina de origem. Caso isso aconteça, há conexão e a rede está funcionando.

Para usar o comando PING, vá em Iniciar / Executar e digite cmd e enter.

Na tela do Shell do Windows digite o comando Ping e o IP destino.

Competência 02

Exemplo:

Você está na máquina 192.168.0.1 e quer saber se existe rede com o computador 192.168.0.2. Faça o seguinte comando na máquina 192.168.0.1

```
ping 192.168.0.2
```

A resposta deve ser:

Disparando contra 192.168.0.2 com 32 bytes de dados:

```
Resposta de 192.168.0.2: bytes=32 tempo<1ms  
TTL=128
```

Estatísticas do Ping para 192.168.10.13:

```
Pacotes: Enviados = 4, Recebidos = 4, Perdidos =  
0 (0% de perda),
```

Aproximar um número redondo de vezes em milissegundos:

```
Mínimo = 0ms, Máximo = 0ms, Média = 0ms
```

Note que foram enviados 4 e recebidos 4 e houve 0% de perda. A rede está estabelecida. Já no exemplo abaixo, temos problemas de conexão:

Disparando contra 192.168.0.2 com 32 bytes de dados:

```
Esgotado o tempo limite do pedido.
```

```
Estatísticas do Ping para 192.168.0.2:
```

Competência 02

Pacotes: Enviados = 4, Recebidos = 0, Perdidos = 4 (100% de perda),

Note que foram enviados 4 e recebidos 0 e houve 100% de perda. A rede está inoperante.

O comando PING é uma ferramenta diária que todo administrador de redes usa. Antes de quebrar a cabeça com alguma coisa que não está funcionando, não se esqueça de usar o PING. Ele lhe diz o básico, se a rede está em ordem. Daí em diante você pode partir para testar outros recursos.

Vamos agora alterar o comportamento de alguns protocolos da Camada de Rede:

Nas máquinas com Windows XP SP2 (Service Pack2) em diante, existe o *Firewall* do Windows instalado e por padrão o comando PING é proibido, dando a impressão de que a rede está com problemas. IkljhkllklkjPorém, não é um problema e sim uma configuração padrão, pois, neste caso, é o protocolo ICMP (utilizado pelo comando ping) que está sendo negado.

Para liberar o protocolo ICMP e liberar o comando ping, é necessário que você faça uma exceção no firewall do Windows. Para isso vá em:

- Iniciar / Configurações / Conexões de Rede ou
- Iniciar / Configurações / Painel de Controle / Conexões de Rede ou
- Botão Direito no ícone da Área de Trabalho/ Meus Locais de Rede e Propriedades.

Após estar na tela de Conexões de Redes, siga os seguintes passos:

Botão direito em “**Conexão Local**” / Propriedades

Clique na aba “**Avançado**”

Clique no botão “**Opções**”

Competência 02

Na tela que apareceu clique em “Avançado”. A tela de configuração é de acordo com a Figura 50:

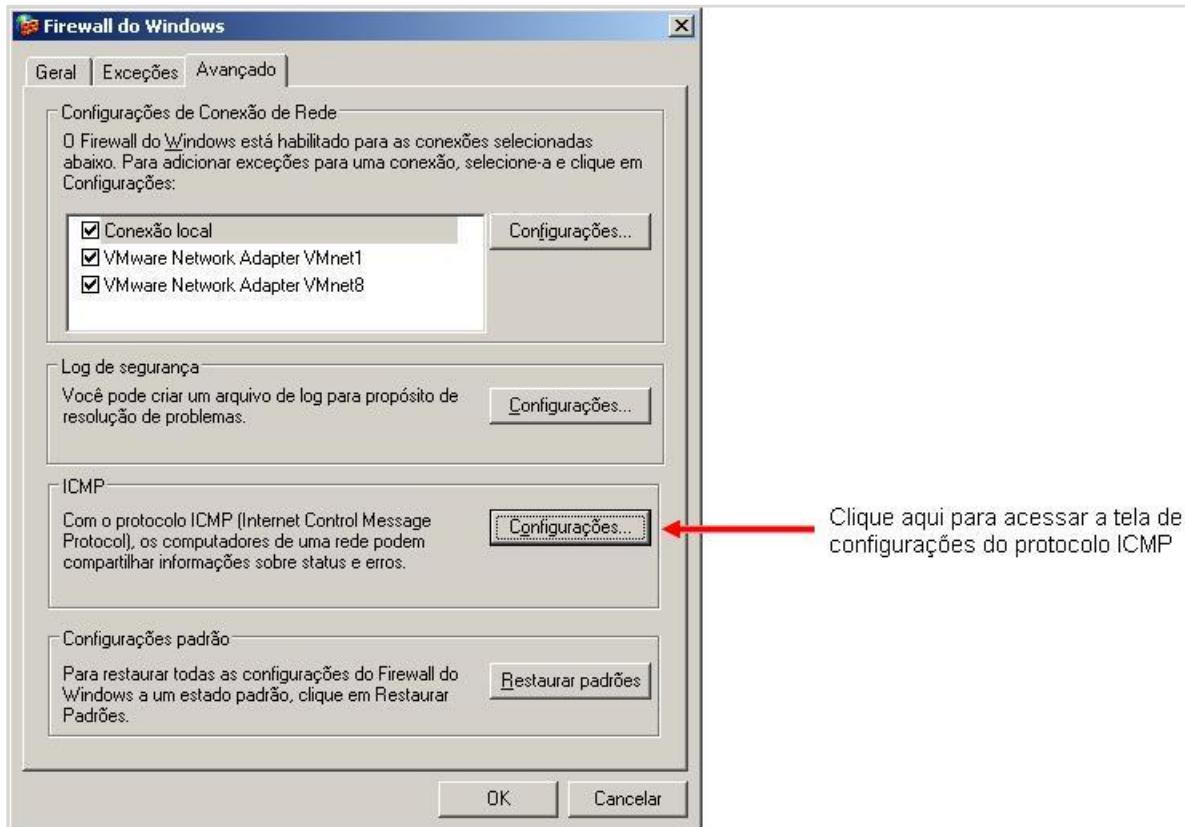


Figura 50- Configurações avançadas do Firewall do Windows
Fonte: produzido pelo autor

Após clicar no botão configurações, basta marcar a primeira opção:

“Permitir solicitação de eco de entrada”. Conforme Figura 51.



Competência 02

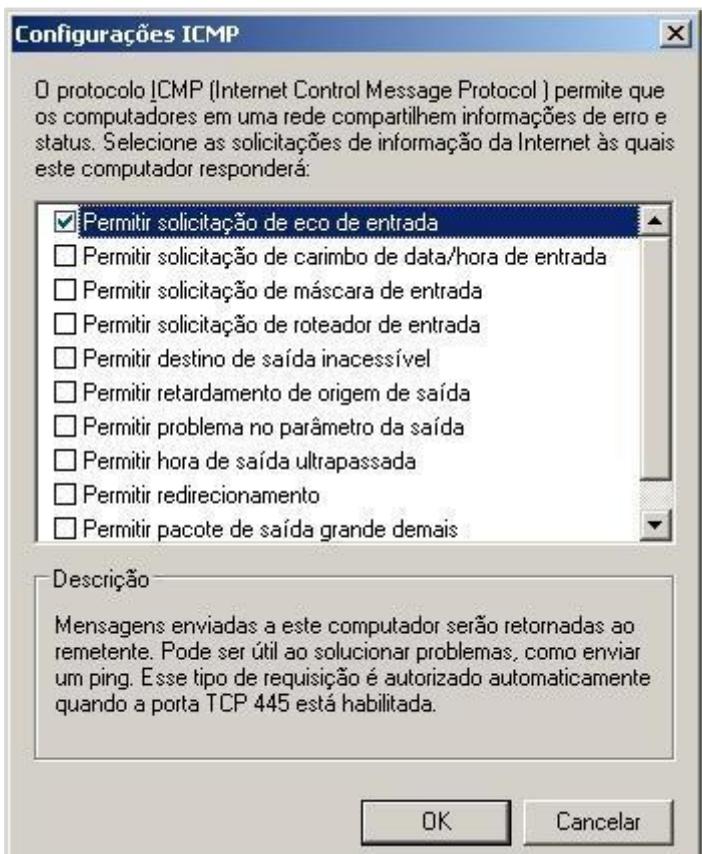


Figura 51- Liberando o protocolo do PING.

Fonte: produzido pelo autor

Não esqueça! Você deve fazer isso em todas as máquinas da sua rede para que você tenha o ping funcionando e com resultados corretos.



Saiba Mais:

ICMP é a sigla para **Internet Control Message Protocol**. É um protocolo que dentre outras funções é utilizado para gerar relatórios de erros de conexão entre máquinas e indicar rotas alternativas de roteamento. Este protocolo é nativo da camada de Rede do Protocolo TCP/IP.

Fim do Boxe

Mídias Integradas:

Para entender como funcionam os equipamentos e a comunicação em uma grande rede de computadores mais uma vez recomendamos o vídeo “Guerreiros da Internet”. Nele, você compreenderá os principais conceitos que vimos nesta semana em um vídeo muito bem elaborado e empolgante. Guerreiros da Internet - http://www.youtube.com/watch?v=h0Zov_rh3U

Competência 02

2.7.2 Resumo

Atenção! Chegou a hora da revisão!

Protocolo é o conjunto de regras que estabelecem como as informações trafegam em uma rede de dados.

O Protocolo de Comunicação que é mais utilizado no mundo é o TCP/IP. É ele que rege a troca de dados na Internet.

A troca de dados em uma rede é feita em Camadas. Estas camadas têm funções distintas e uma camada presta serviço à camada posterior.

O Modelo OSI que padroniza o mercado de redes de computadores e dispositivos está dividido em sete camadas.

O Protocolo TCP/IP também é dividido em camadas. Atualmente, alguns autores classificam em 5 camadas. Outros autores consideram a camada de rede e a camada física como uma só camada.

O Roteamento é a técnica utilizada em uma rede para transportar pacotes de dados de uma rede para outra pelo caminho mais rápido.

O Modelo TCP/IP e OSI fazem inter-relação direta pelas camadas que têm serviços semelhantes.

O Endereço MAC é um endereço único que identifica um hardware.

O Endereço IP é um endereço lógico do protocolo TCP/IP. Todo IP é atrelado ao endereço MAC do hardware.

Competência 02

Um dado em uma rede TCP/IP pode ser chamado de frame, pacote, datagrama e mensagem. O que vai decidir é em que camada do modelo ele se encontra no momento.

Um endereço IP tem 32 bits e pode endereçar 4,294,967,296 de dispositivos únicos.

A Máscara de Rede classifica o endereço IP e divide o endereço da rede e os endereços dos hosts.

Atualmente o endereçamento IP está na versão 4: IPv4.

A próxima geração de endereçamentos de IP é o IPv6.

O Protocolo ARP é utilizado quando se sabe o número IP e é necessário descobrir a qual endereço MAC ele pertence.

O Protocolo RARP é utilizado quando se sabe o MAC e é necessário descobrir qual o IP a que ele pertence.

O Protocolo DHCP é responsável por distribuir IPs.

Conhecemos o protocolo DHCP e toda a negociação de um dispositivo cliente solicitar um IP a um servidor DHCP.

O Servidor DHCP é capaz de alugar IPs a um cliente. Este aluguel é chamado de LEASE.

O Servidor DHCP pode ter faixas de IP para a alugar. Esta faixa é chamada de RANGE.

Um servidor DHCP além de alugar IP, pode informar quem é o IP do Servidor DNS da Rede e também o roteador padrão (Gateway).

Competência 02

Entre a solicitação de um novo endereço IP até a configuração final estão envolvidos 4 pacotes UDPs, sendo eles: DHCP DISCOVER, DHCP OFFER, DHCP REQUEST e DHCP ACK.

APIPA é um recurso que alguns sistemas operacionais proveem para evitar que um dispositivo fique sem endereço IP caso o servidor DHCP esteja indisponível.

É possível usar software denominados de Analisadores de Protocolos ou ainda Sniffers para visualizar todas as fases de negociação de um protocolo como o DHCP.

Os processos de um dispositivo podem oferecer recursos através de portas de comunicação.

Na arquitetura cliente/servidor uma aplicação na máquina local, chamada cliente, precisa dos serviços de outra aplicação em uma máquina remota, chamada servidora.

Cada aplicação tem uma porta que a distingue de outras aplicações que estejam rodando na mesma máquina.

UDP é um protocolo da camada de transporte sem controle de fluxo nem de erro, exceto pela detecção de erro através de *checksum*.

TCP é um protocolo da camada de transporte que fornece serviço confiável e orientado à conexão.

O DNS é uma aplicação cliente/servidor que identifica cada máquina na *Internet* com um nome único e fácil de lembrar. Na hora de acessar uma máquina, o DNS traduz o nome em endereço IP (camada de rede).

Competência 02

O DNS organiza o espaço de nome em uma estrutura hierárquica e descentraliza a responsabilidade de administração dos nomes e endereços. Cada nó na árvore tem um nome de domínio.

Competência 03

3. COMPETÊNCIA 03 | A CAMADA FÍSICA E SUAS APLICAÇÕES

3.1 Objetivos

Conhecer os métodos de transmissão analógico e digital.

Conhecer os principais fenômenos que alteram a transmissão de dados.

Entender os conceitos de portadora, frequência, largura de banda e vazão de dados.

Conhecer os principais meio de transmissão de dados (guiados e não guiados).

Conhecer as características de cabos par trançado, coaxial e fibra ótica.

Conhecer as principais características do meio de transmissão Wireless.

Conhecer e aplicar os princípios básicos de cabeamento estruturado.

Aprender a fazer um mini projeto de cabeamento estruturado.

Durante a semana passada, estudamos como os dados trafegam em uma rede de computadores seguindo algumas regras denominadas de protocolos. Lembrou????? Conhecemos a padronização que regem os equipamentos de rede e também conhecemos o protocolo TCP/IP e suas camadas. Agora, convido você, caro (a) aluno (a), a conhecer a primeira camada do Modelo OSI, a Camada Física. Vamos descobrir os métodos de transmissão, as características e os principais meios utilizados? Depois, aplicaremos os meios físicos a projetos físicos de redes locais.

3.2 Transmissão Analógica e Digital

Você sabia que para ser transmitida por um meio físico, a mensagem tem de se moldar a este meio? Pois é! Na comunicação de computadores, a

Competência 03

transmissão é feita utilizando-se impulsos elétricos, portanto, a mensagem precisa ser transformada nessa forma de energia para a transmissão. Esta transformação pode ser feita de forma analógica ou digital.

Qual a diferença? Mais uma vez, tomemos o exemplo de um telefone. Quando você fala, sua voz é transmitida através de vibrações no ar, que são conduzidas a todas as direções, atingindo assim o ouvido de outra pessoa. O aparelho telefônico, simplesmente reproduz essas vibrações no fio elétrico. O aparelho na outra ponta faz a transformação inversa, de vibrações elétricas para vibrações sonoras. Note, na figura 52 que a variação no sinal elétrico (gráfico) acompanha as mudanças da voz. Quando você fala mais alto, o sinal aumenta, quando fala mais baixo, ele diminui. Isso faz com que o sinal elétrico seja análogo ao sinal sonoro. Daí vem o termo analógico.

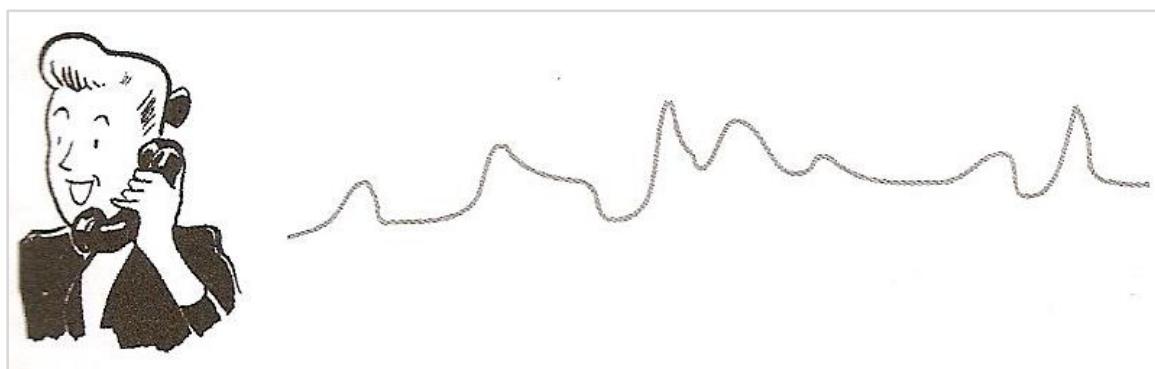


Figura 52- Neste gráfico de um sinal analógico típico, as variações na amplitude e frequência expressam as graduações de volume e timbre na fala ou música. Utilizam-se sinais semelhantes para transmitir imagens de televisão, mas em frequências muito mais altas.

Fonte: (STALLINGS, 2005)

O sinal digital também copia as variações do sinal original (voz, neste exemplo). Porém, o sinal digital é formado por números ou dígitos. Esta palavra vem de “dedos”, daí o termo digital.

Na prática, o sinal digital não muda de valor de forma contínua como o analógico faz. Ele dá “saltos”. Por exemplo, se você olhar um termômetro comum, desses de vidro com uma coluna de mercúrio vermelha, verá que, apesar de termos marcações ao longo do seu corpo, a coluna vermelha não

Competência 03

“salta” dos 36 graus para os 37 graus. Há infinitos pontos entre os dois. Se você observar, então, um termômetro digital, verá que ele pode passar dos 36 para os 37, utilizando saltos de 0,1. Por exemplo, 36,1 36,2 ... até 37 graus. Assim, os sinais analógicos têm infinitos níveis de intensidade, já o digital tem um número finito destes níveis, e passa de um para o outro de uma vez, como se fossem “degraus”. Você pode ver isso claramente na figura 53.

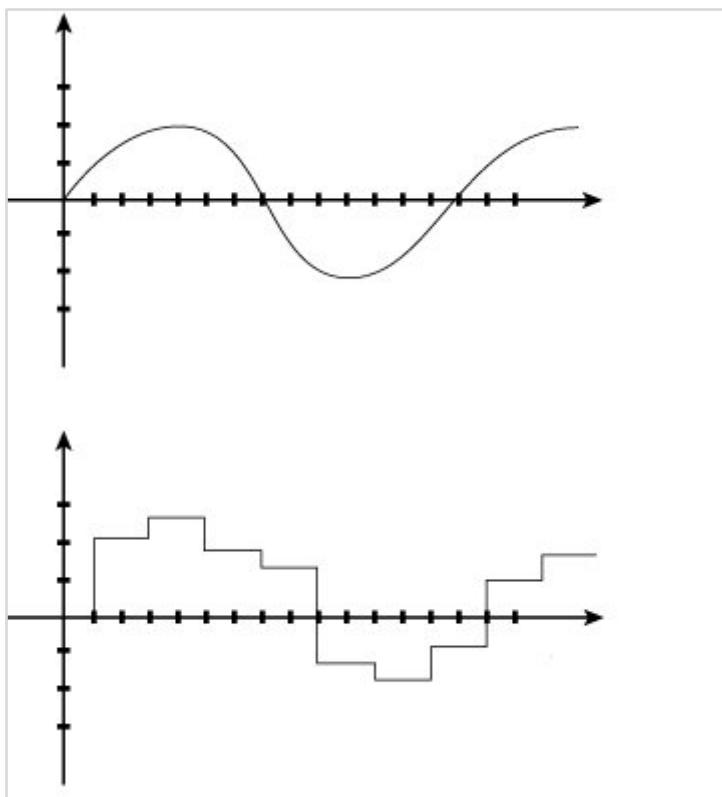


Figura 53- Um sinal analógico “imitado” por uma aproximação digital
Fonte:<http://tinyurl.com/pokxla>

Nos computadores, todos os dados transmitidos estão no formato digital. Ou seja, as mensagens estão no formato de *bits* (binário). Mas, então, surge um novo problema: como transmitir uma informação binária usando um canal elétrico? Há diversas maneiras. Vamos estudar algumas?

Veja que interessante: Uma mensagem digital é um número binário como 1001, o que significa que esta mensagem vai depender da interpretação da aplicação que está na camada superior (pode ser apenas o número 9, ou a

Competência 03

representação de um ponto colorido em uma imagem). Tendo um canal de comunicação entre dois computadores podemos representar os bits 0 e 1 como sendo o nível da voltagem. Por exemplo, uma carga de 5v (volts) pode ser interpretada como 1, e uma carga de 0v como 0. Supondo o meio de transmissão como um fio elétrico, quanto maior for este fio, mais difícil de o sinal que foi gerado numa ponta chegar à outra sem modificações. Digamos que o sinal chega ao outro lado “enfraquecido”. O receptor (por exemplo: um repetidor ou um hub) precisa regenerar ou recuperar o sinal a partir dos níveis elétricos que ele lê do canal (sinal recebido). Utiliza-se então a seguinte regra: se o sinal for maior que a metade dos 5v (2,5v), ele é considerado 1. Se estiver abaixo, é considerado 0. Observe atentamente a figura 54. Note especialmente a linha pontilhada verde que indica o limite de 2,5v e veja a correspondência entre o nível do sinal e o dígito que foi interpretado pelo receptor (sinal regenerado pelo receptor). E lembre-se: se essa regra de comparar com o valor 2,5v for usada, ela já vai fazer parte do protocolo de comunicação nessa camada.

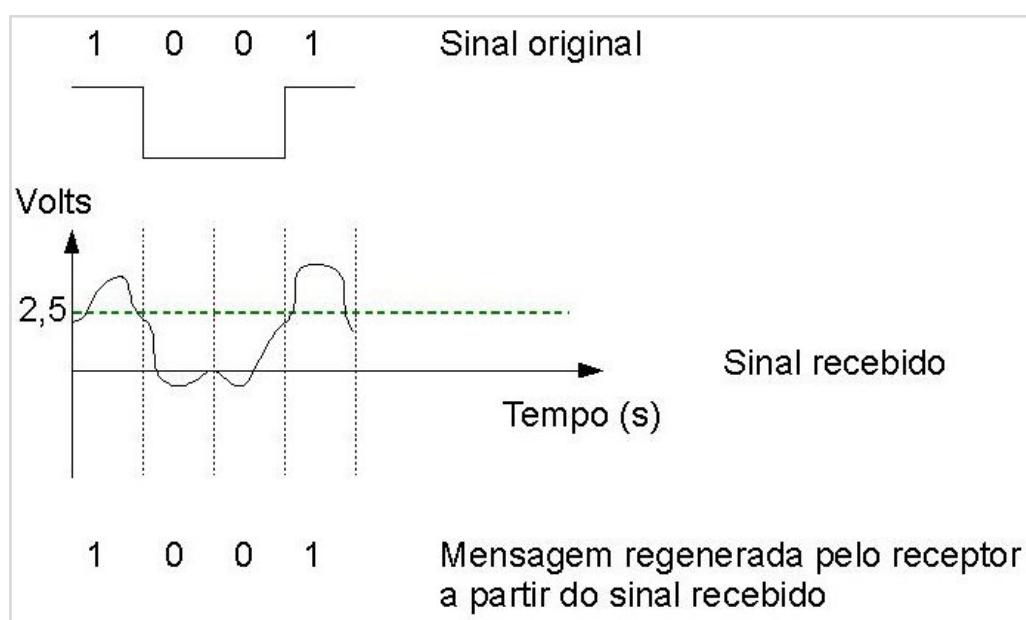


Figura 54- Transmissão de uma mensagem digital usando níveis de tensão
Fonte: Prof: Sílvio Bandeira - <http://www.dei.unicap.br/~silvio/>

Ao passar pelo fio, o enfraquecimento que o sinal sofre é um fenômeno chamado de **atenuação**. Isto acontece porque uma parte da energia é

Competência 03

transformada em energia térmica, ou seja, o fio aquece um pouco por causa da resistência elétrica. Por isso, cada tipo de cabo tem um limite no comprimento. Se um comprimento maior for necessário, amplificadores precisam ser usados para compensar esta perda e restaurar o nível de energia do sinal. Veja figura 55.

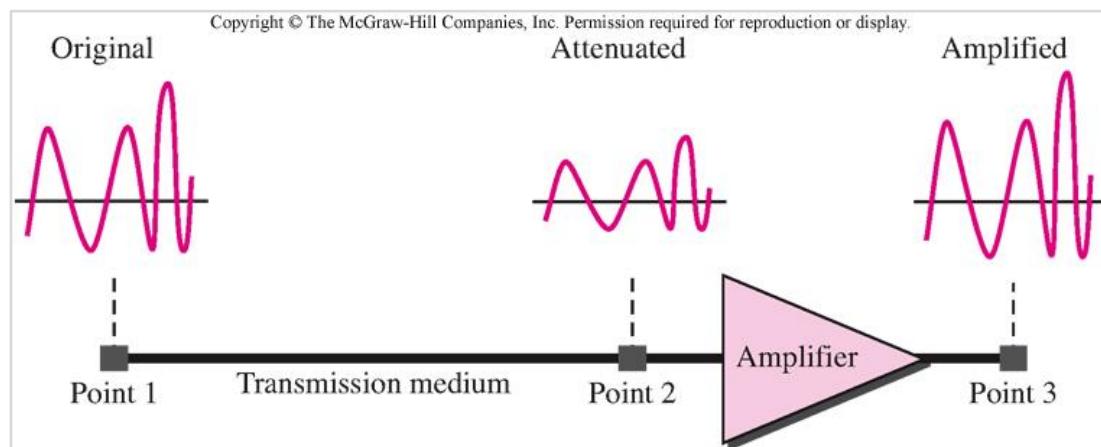


Figura 55-Note o sinal Original do Ponto 1 passando pelo meio de transmissão. Ao chegar ao Ponto 2, o sinal está enfraquecido. Aí entra a figura do Amplificador, que regenera o sinal que é apresentado no Ponto 3.

Fonte: (STALLINGS, 2005)

Ainda observando a figura 54, note que o receptor precisa saber onde começa e onde termina cada *bit*. Quer dizer que o emissor e o receptor precisam estar sincronizados, pois o receptor precisa testar o nível do sinal bem no meio do *bit* (entre as linhas pontilhadas verticais) para decidir entre 0 e 1.

Isto é possível, mas é difícil de conseguir utilizando este método. Outra maneira de transmitir torna esta tarefa mais fácil. Podemos inserir no meio de transmissão um sinal que varia de maneira constante (mais ou menos como se o emissor transmitisse 0, 1, 0, 1... o tempo todo). Utiliza-se um sinal periódico para este fim com o formato senoidal, porque se assemelha ao gráfico da função “seno” que é uma onda constante. Matemática? Sim, um pouco, mas não se preocupe ☺. Esta onda é enviada o tempo todo, o que mantém emissor e receptor sincronizado. Porém, como é um sinal constante, esta onda sozinha não carrega nenhuma mensagem.

Competência 03

Aonde vai a mensagem então? A mensagem vai ser enviada por meio de mudanças nesta onda, e, por isso, é chamada de portadora.

Tá certo. Mas, como mandamos uma mensagem nesta “onda”? Simples, mudamos uma das características da onda quando queremos mandar 1, e mudamos a mesma característica para outro valor quando queremos mandar 0.

Podemos mudar a “altura” da onda para indicar os valores binários. Na figura 56(a) temos a mesma mensagem digital: 1001. Na figura 56(b) temos o sinal enviado modificando a portadora de modo que as ondas ficam “altas” para indicar o *bit* 1, e ficam “achatadas” para indicar o 0. A altura da onda é chamada de amplitude do sinal.

Podemos também mudar a quantidade de ondas em um mesmo intervalo. Com muitas ondas “espremidas”, indicamos o valor 1. Com as ondas mais “espaçadas” indicamos o valor 0. Observe atentamente, então, a figura 3.5(c). A quantidade de ondas em um dado intervalo chama-se **frequência** do sinal.



Competência 03

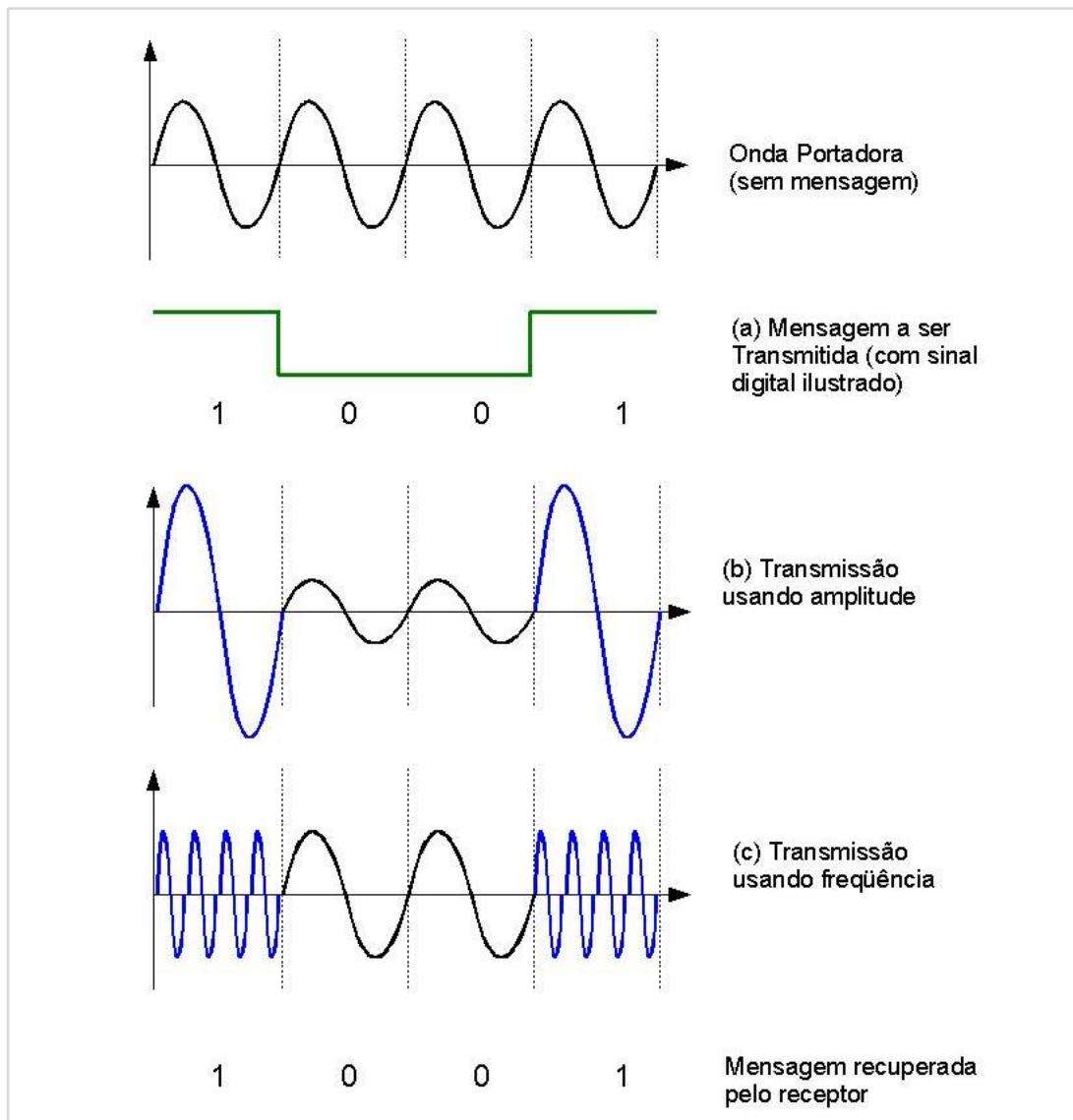


Figura 56- Transmissão usando modulação de amplitude (b) e de freqüência (c)

Fonte: Prof: Sílvio Bandeira - www.dei.unicap.br/~silvio/

3.3 Indicadores de Desempenho

Existem várias medidas para avaliar o desempenho de uma transmissão ou de um canal de comunicação. Uma das mais importantes é a **largura de banda**, ou *bandwidth* em inglês. É o máximo da quantidade de *bits* por segundo (**bps**) que o canal pode transmitir. Por exemplo, um *link* de uma rede *Fast Ethernet* tem largura de banda de 100Mbps, ou seja, pode transmitir até (aproximadamente) 100 milhões de *bits* por segundo (**bps**).

Competência 03

Em engenharia elétrica, *bandwidth* também quer dizer a largura da faixa de frequências que um canal pode transmitir sem erros. A quantidade de *bits* por segundo depende diretamente da largura desta faixa de frequência. Daí vem o termo largura de banda. **Lembre-se: quanto maior a largura desta faixa de frequência, mais bps no canal.**

Outra medida é a **vazão** ou *throughput*. Também é medida em bps, como a largura de banda. Qual a diferença? A largura de banda é o máximo que o canal aguenta e a vazão é a quantidade de dados transmitidos em um determinado momento. Então, a vazão pode variar e a largura de banda é o seu valor máximo.

A **latência** ou *latency* é o tempo que a mensagem leva pra chegar ao emissor. Isso desde o momento em que o primeiro *bit* é transmitido até o instante em que a mensagem está completamente disponível para o receptor. Entram nesta conta o tempo de propagação, mais o tratamento da mensagem por todas as camadas de protocolo até chegar ao processo receptor.

3.4 Meios de Transmissão

Agora, vamos estudar a parte realmente física desta camada. Os meios de transmissão usados em redes são cabos metálicos, fibras óticas e simplesmente o espaço (no caso de redes sem fio).

Assim, temos os meios guiados e os meios não guiados:

- **Meios Guiados:**

- Cabo Coaxial;
- Cabo Par Trançado;
- Fibra Ótica.

Competência 03

- **Meios Não Guiados:**

Transmissão sem fios, o ar. (Wireless)

3.4.1 Meios Guiados

Estes meios fornecem um conduíte para os dados. Temos, então, o **par trançado, cabo coaxial** e a **fibra ótica**. Os dois primeiros utilizam um condutor metálico. A fibra ótica transporta sinais na forma de luz.

a) Par Trançado

O cabo tipo par trançado é formado por dois fios de cobre com isolamento plástico e são torcidos um sobre o outro (figura 57). Veja na figura 58b a imagem real de um cabo UTP.

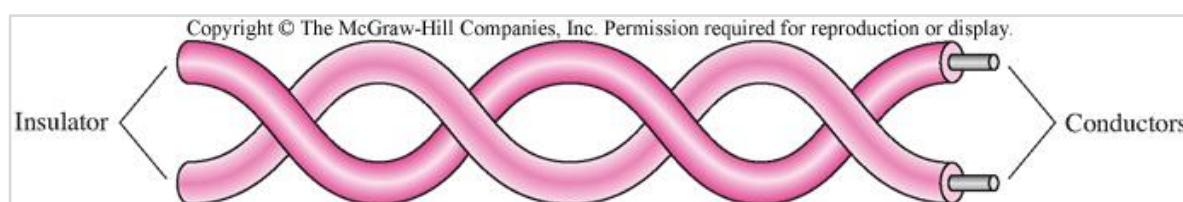


Figura 57- Par trançado

Fonte: (STALLINGS, 2005)

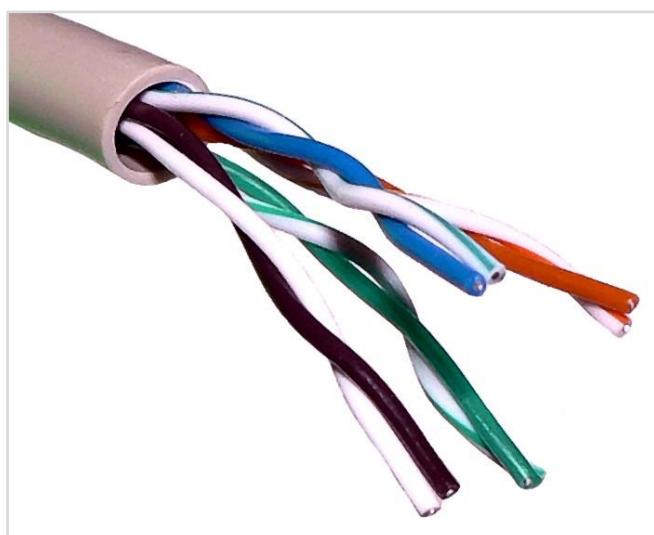


Figura 58 - Em detalhe o cabo UTP decapado.

Fonte:http://upload.wikimedia.org/wikipedia/commons/c/cb/UTP_cable.jpg

Competência 03

Cada par de fios conta com apenas um canal de transmissão. Isto porque um deles é o famoso “fio terra”. O receptor mede a energia do sinal (lembra do gráfico da Figura 54 com 2.5v?) comparando a diferença de voltagem entre os dois. E por que os dois fios são torcidos? Para minimizar os efeitos de **interferência** elétrica, também conhecido como **transientes**. Suponha que o cabo esteja passando junto de um transformador ou qualquer outro equipamento que gere um campo magnético forte. Se os cabos fossem paralelos, o que estivesse mais próximo do equipamento sofreria mais interferência (sim, mesmo sendo a distância de um para o outro muito pequena). Torcendo os cabos, aumentam-se as chances de uma interferência alterar os sinais dos dois fios na mesma intensidade, com isso as diferenças entre os dois permanecem iguais.

Esse tipo de cabo pode ter uma blindagem, uma proteção metálica contra interferências. O que não tem é chamado de par trançado sem blindagem ou *Unshielded Twisted-Pair (UTP)*, e o que tem de par trançado com blindagem ou *Shielded Twisted-Pair (STP)*. Observe a diferença entre os dois na figura 59. O tipo UTP é o mais usado em redes de computadores. Na figura 60 é apresentado um cabo STP blindado. Veja que há uma proteção em cada par. Essa proteção reduz os transientes e torna o cabo mais indicado para ambientes com grandes problemas de campos magnéticos ou interferências.

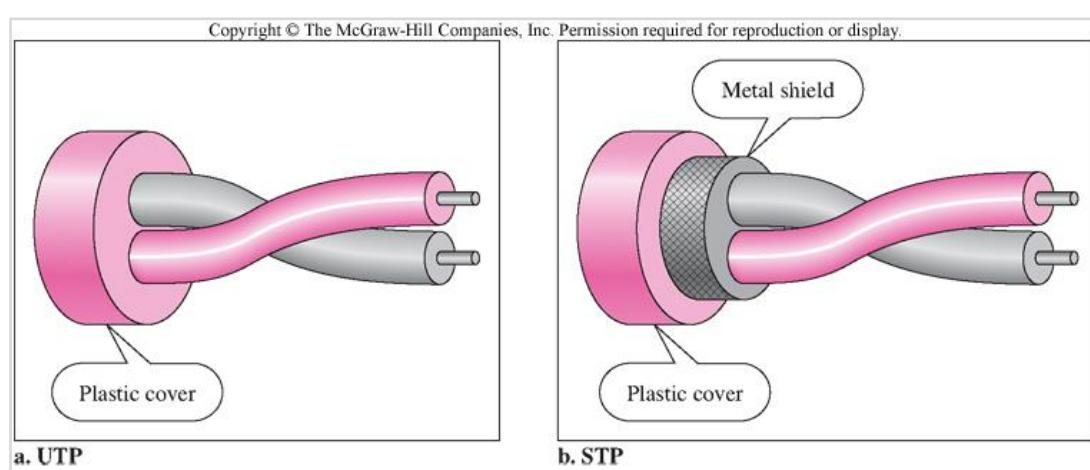


Figura 59- Par trançado. Note a diferença na proteção metálica (Metal Shield) que diminui os transientes.
Fonte: (STALLINGS, 2005)

Competência 03

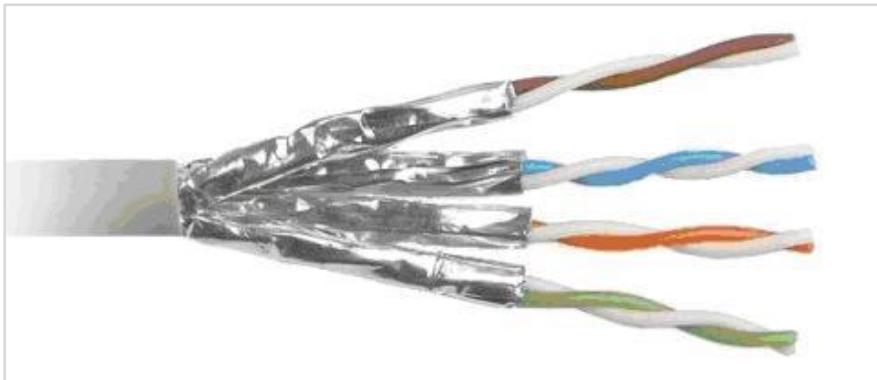


Figura 60- A imagem de um cabo STP. Em detalhe, a blindagem individual de cada par.
Fonte: www.regitel.com.br/userfiles/imagem10.JPG



Saiba Mais
Um excelente material com explicações e curiosidades sobre cabos UTP encontra-se disponível no endereço <http://tinyurl.com/edes12>. A leitura deste texto será parte importante para a resolução das nossas atividades da semana.

Atente bem! Os cabos utilizados em redes padrão *Ethernet*, que é o tipo de rede física mais comum para LANs, utilizam um cabo com 4 pares de fios. Nas placas de rede de até 100Mbps, apenas dois pares são utilizados, um para transmitir sinais e outro para receber. Estes cabos utilizam conectores chamados RJ-45 (do inglês *Registered Jack*). Observe a figura 61. Ela traz o RJ-45 Fêmea (que é encontrado na placa de rede do computador ou notebook e também nas tomadas) e o RJ-45 Macho, que fica nas extremidades do cabo. Uma foto do conector RJ-45 Macho é apresentada na figura 62. Já na figura 63, o conector fêmea é apresentado.

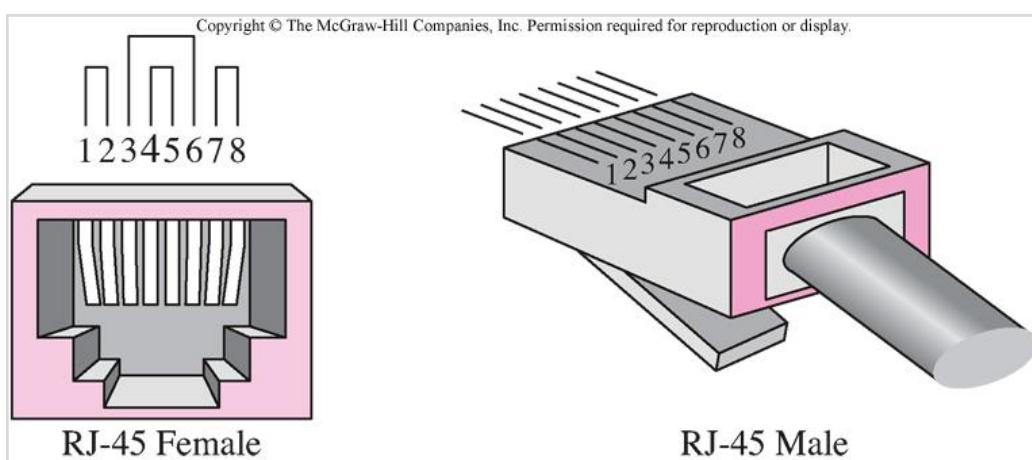


Figura 61- A representação de um conector RJ-45 macho e fêmea. Estes conectores são utilizados no cabo par trançado, tanto UTP quanto STP.

Fonte: (STALLINGS, 2005)

Competência 03



Figura 62- A representação de um conector RJ-45 macho.
http://upload.wikimedia.org/wikipedia/commons/6/6b/Re-45_crimped1.jpg

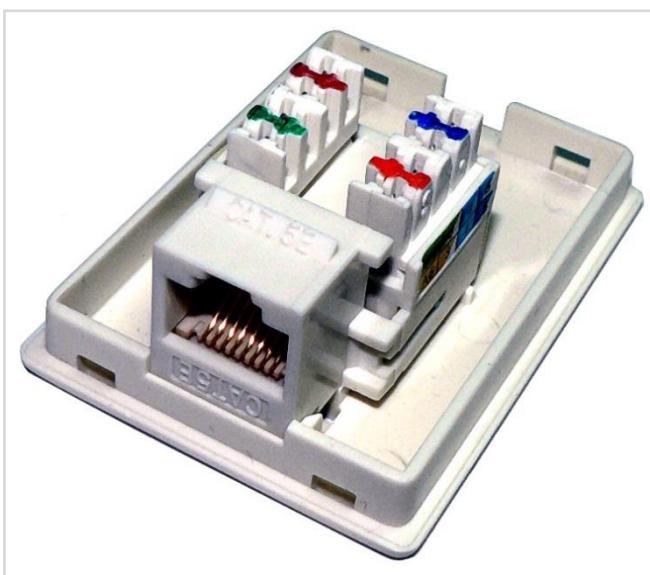


Figura 63- A representação de um conector RJ-45 Fêmea, utilizado em tomadas.
http://upload.wikimedia.org/wikipedia/commons/f/f3/RJ-45_female_unshielded.jpg

b) Cabo Coaxial

Você sabia que cabos coaxiais têm este nome porque seus dois fios compartilham o mesmo eixo (axial = eixo). Interessante não é?. A construção destes cabos é bem diferente. Observando a figura 64, você pode perceber que temos, na verdade, um fio “dentro” de outro. O cabo interno é único, ao passo que o externo é uma malha metálica que serve de condutor e barreira contra interferências. Entre um e outro há um isolante e por fora mais duas

Competência 03

camadas protegem todo o cabo. A figura 65 traz uma imagem com detalhes deste cabo.

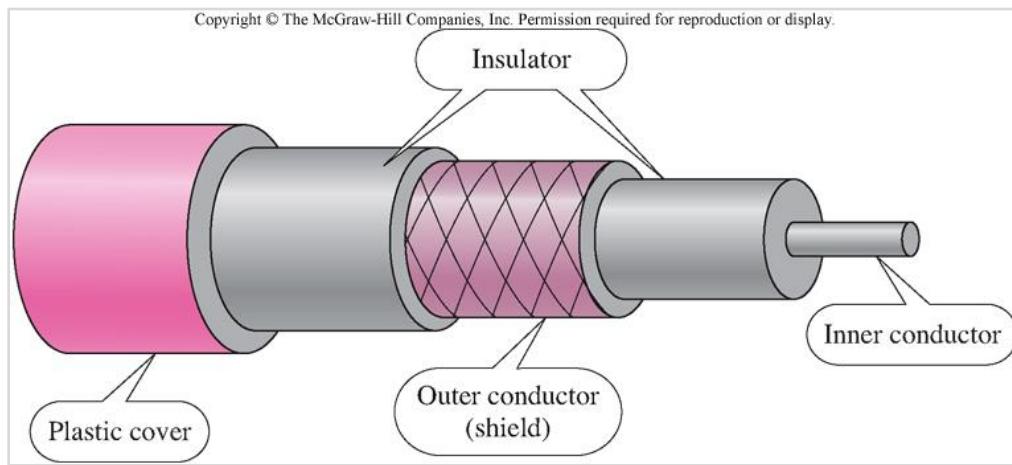


Figura 64- Cabo coaxial.
Fonte: (STALLINGS, 2005) CORRESPONDE À FIGURA 7.7 NO LIVRO



Figura 65-Detalhes de um cabo coaxial.
Fonte: http://upload.wikimedia.org/wikipedia/commons/0/08/Coaxial_cable_cut.jpg

Este tipo de cabo é muito usado em redes de tv por assinatura e também nas redes com topologia em barramento. Para ligar uma máquina nele, precisamos de um conector especial, e, se a máquina estiver distante de onde passa o cabo principal, precisamos também de um cabo secundário só para cobrir esta distância. Na figura 66 temos os conectores BNC. O conector no formato de um "T" (BNC T) é o mais comum para ligar uma máquina no cabo

Competência 03

principal, no caso de não ser a última máquina. A figura mais à direita, mostra um terminador. Este dispositivo é colocado no final do cabo, para que esta ponta não fique “aberta”, e serve para evitar que o sinal seja refletido de volta no cabo quando atingir uma das pontas. A Figura 67 detalha o terminador e o conector BNC T.

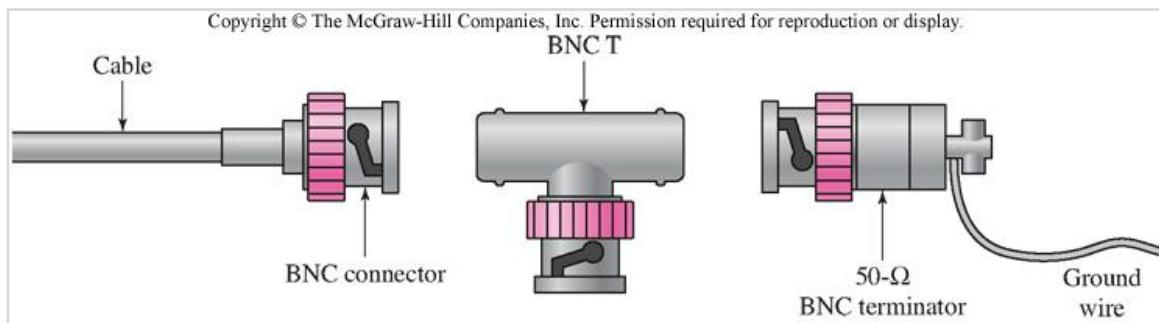


Figura 66- Conectores Bayone-Neill-Concelman (BNC) para cabo coaxial
Fonte: (STALLINGS, 2005)



Figura 67- Conectores Bayone-Neill-Concelman (BNC) para cabo coaxial. Note a presença do terminador na foto, tanto do lado esquerdo (com a cor verde) já encaixado no conector BNC T quanto sozinho do lado direito. No meio, o BNC T em outro detalhe.

Fonte:<http://upload.wikimedia.org/wikipedia/commons/5/5f/BNC-Technik.jpg>

O cabo coaxial, pela maior resistência a interferências, admite distâncias maiores e mais estações que o par trançado. Oferece também uma maior capacidade, porém é mais caro e sua instalação tem menos flexibilidade que uma instalação com par trançado. Por isso, não tem sido utilizado ultimamente para LANs, onde o par trançado e a fibra ótica são mais comuns.

Competência 03

c) Fibra Ótica

Veja que interessante: O cabo de fibra ótica é feito de material transparente, pois conduz o sinal na forma de luz, sendo capaz de transmitir a luz em curvas por meio do fenômeno da reflexão. Sabe quando você vê um peixe dentro da água e ele parece estar mais perto da superfície do que realmente está? Isto acontece porque quando a luz passa de um meio para outro com densidade diferente (como da água para o ar), a luz muda de direção. Se ela passa de um meio para outro o fenômeno é a refração. Porém, se uma fonte de luz (lâmpada, ou mesmo a luz do sol) estiver acima da água, em um ângulo bem aberto, você poderá vê-la na superfície da mesma. Este fenômeno é a reflexão. Este último é o utilizado nas fibras óticas, porque queremos que o raio de luz permaneça no canal e não escape. Portanto, construindo a fibra com camadas de materiais com densidades diferentes e cuidadosamente estudados, podemos fazer com que a luz permaneça no mesmo caminho do cabo através de inúmeras reflexões, como você pode ver na figura 68. O núcleo transparente da fibra é revestido por um material menos denso, de modo que quando a luz chega ao limite entre os dois, com um ângulo aberto, ela seja refletida de volta ao núcleo.

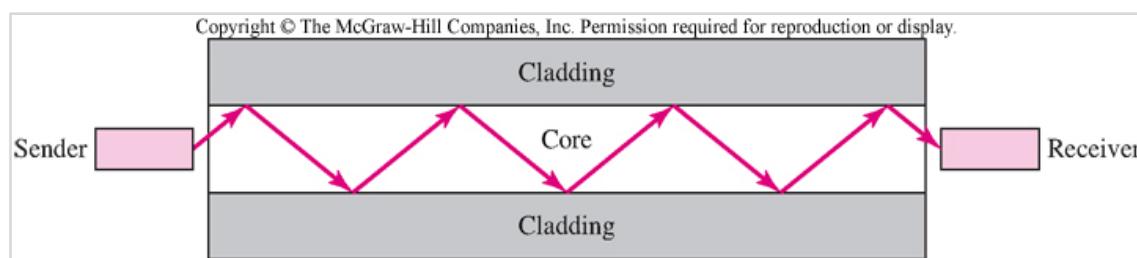


Figura 68- Propagação da luz numa fibra ótica. Perceba que a camada mais densa (Cladding) reflete o sinal de volta para a fibra.

Fonte: (STALLINGS, 2005)

Há dois tipos básicos de fibras óticas: **monomodo** e **multimodo**.

No tipo multimodo, os raios de luz podem atravessar a fibra em ângulos diferentes. Os que entram com ângulos mais abertos (mais paralelos ao eixo do cabo) fazem menos reflexões durante a travessia. Observe a figura 69 (a).

Competência 03

Estes raios chegam ao final do cabo primeiro que os outros, mesmo que os dois tenham saído juntos no início. Se o núcleo da fibra for de material homogêneo, ou seja, com densidade constante, a luz só se refletirá quando atingir o revestimento (figura 37). Este tipo é **o monomodo com índice (de densidade do material) de passo**, porque há um “passo” ou uma diferença abrupta da densidade do núcleo comparado ao revestimento. Se o núcleo tiver sua densidade diminuída *gradualmente* à medida que vai chegando perto do revestimento, o raio de luz vai sendo desviado também gradualmente. Isto melhora a transmissão porque como o centro do núcleo é mais denso, os raios que passam no meio viajam a uma velocidade menor. Os raios que não estão bem centralizados, apesar de fazer um caminho mais longo, percorrem a parte do núcleo menos densa, o que aumenta a velocidade e compensa o caminho maior (figura 69 b). Este tipo é chamado de **monomodo de índice gradual**. Nas LANs que utilizam fibras óticas este é o mais escolhido.

No tipo **monomodo**, a ideia é reduzir ao máximo o ângulo de entrada da luz no cabo, fazendo o núcleo bem mais fino (figura 69 c). Desta forma, apenas os raios que estão perfeitamente alinhados com o eixo do cabo serão transmitidos e, então, a distorção encontrada no cabo multimodo é evitada. Este tipo de cabo é muito utilizado em aplicações de longas distâncias (como telefonia).



Competência 03



Copyright © The McGraw-Hill Companies, Inc. Permission required for reproduction or display.

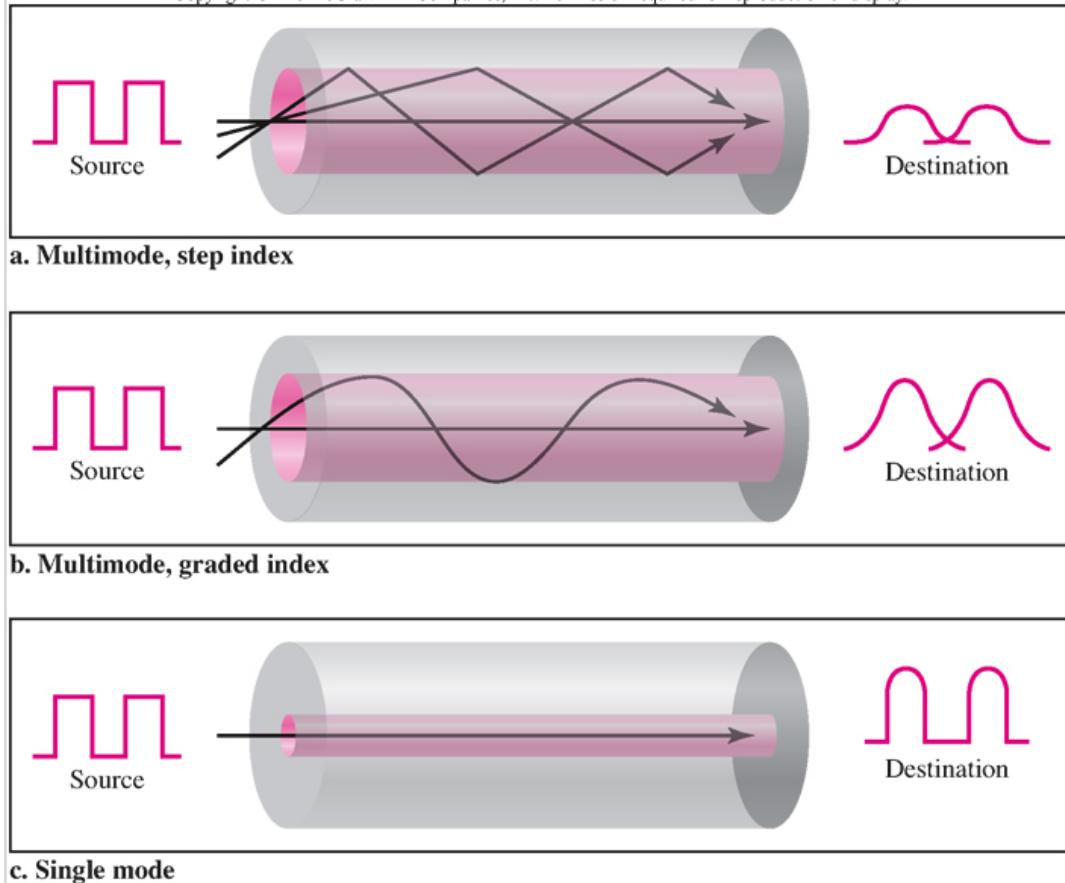


Figura 69- Propagação da luz numa fibra ótica

Fonte: (STALLINGS, 2005)

A figura 70 mostra a constituição de uma fibra ótica. Note que a fibra é revestida de *Kevlar* para dar resistência ao cabo. Este é o mesmo material usado em coletes à prova de balas.

A figura 71 mostra os conectores mais comuns. A figura 72 demonstra a foto destes dois conectores.



Competência 03

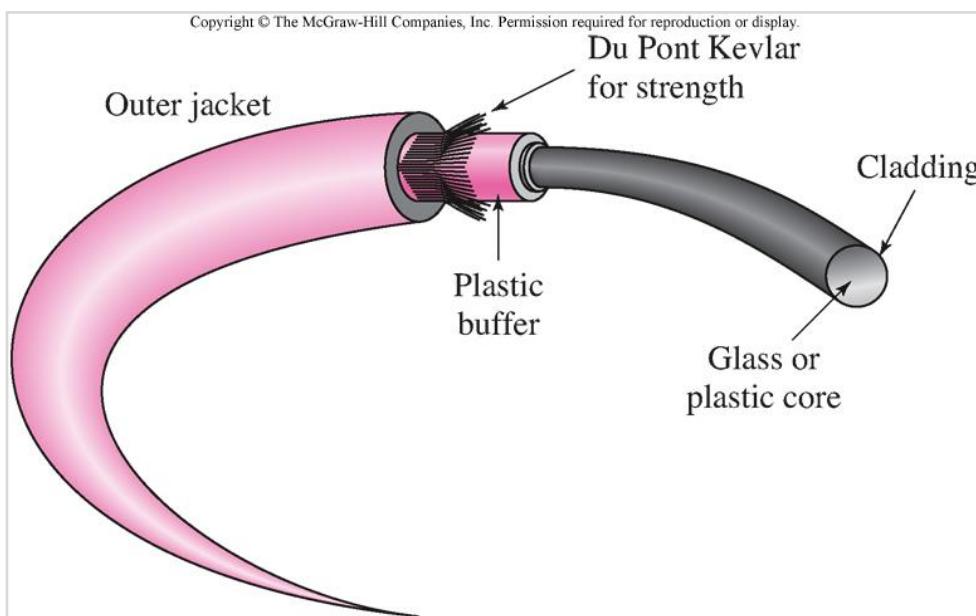


Figura 70- Estrutura física de um cabo de fibra ótica

Fonte: (STALLINGS, 2005)

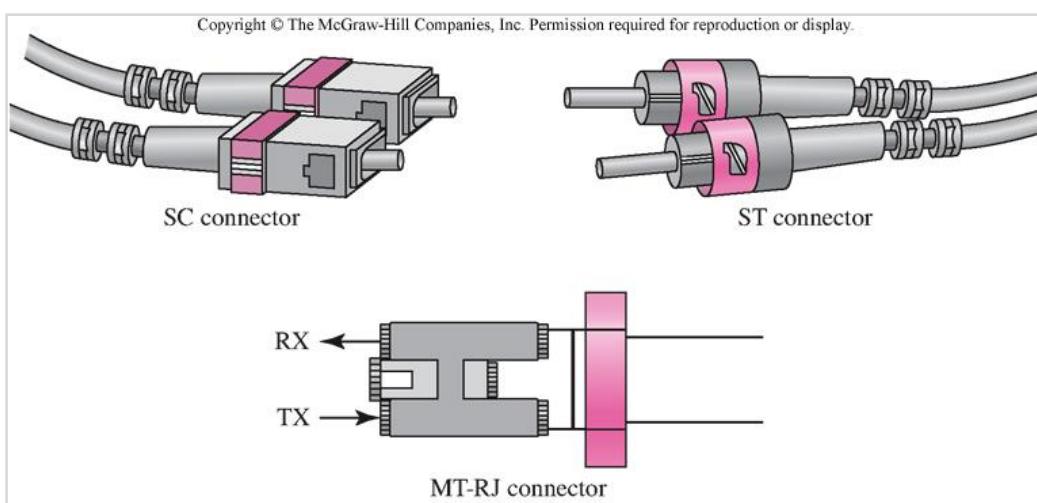


Figura 71- Conectores para cabos de fibra ótica

Fonte: (STALLINGS, 2005)

Competência 03

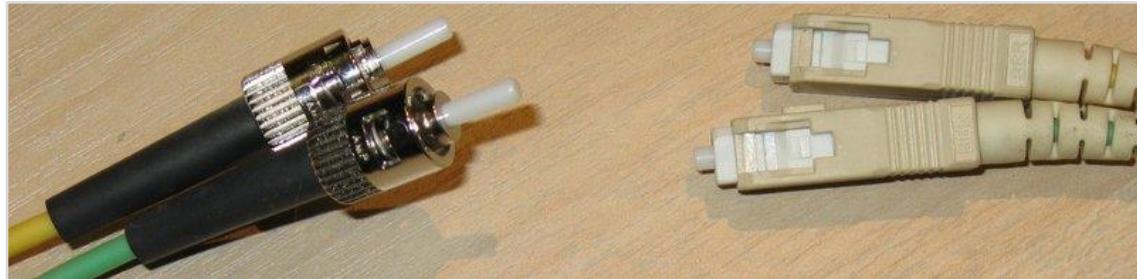


Figura 72- Conectores ST e SC respectivamente.

<http://upload.wikimedia.org/wikipedia/commons/c/c8/St-sc-fiber-connectors.jpg>

Vamos comparar os cabos de fibra ótica com os cabos metálicos que vimos anteriormente?

- **Capacidade:** a largura de banda da fibra ótica é muito maior que a dos cabos metálicos. Já foram demonstradas taxas de transferência acima de 100 Gbps (G = giga = bilhão) com cabos de mais de 10km de extensão.
- **Tamanho e peso:** a fibra ótica é mais leve e fina.
- **Atenuação do sinal:** muito menor.
- **Interferência eletromagnética:** as fibras óticas são simplesmente imunes a este tipo de interferência.
- **Segurança:** por não sofrerem nem gerarem interferência eletromagnética e serem muito difíceis de “grampear”, as fibras ganham também neste quesito.

E não há desvantagens? Há sim. Fibras óticas são bem mais caras, é necessário profissionais mais especializados (com o valor da hora de trabalho bem mais cara) para instalar. Além disso, não permitem transmissão bidirecional, portanto, para emitir e receber é preciso ao menos um par de fibras.

d) Meios de Transmissão Sem Fio (Wireless)

Competência 03

Estes são os meios de transmissão que não utilizam condutores (fios). Eles utilizam ondas eletromagnéticas que se propagam no espaço e não necessitam de um meio físico para serem transmitidos. Podem se propagar inclusive no vácuo. É o caso dos sinais de televisão e de rádio.

Essas ondas são geradas e também captadas através de antenas especiais. As antenas, por sua vez, podem emitir as ondas em todas as direções (**antenas omnidirecionais**) ou restringir a transmissão a uma só direção (**antenas unidireccionais**). Conforme figuras 73 e 74.

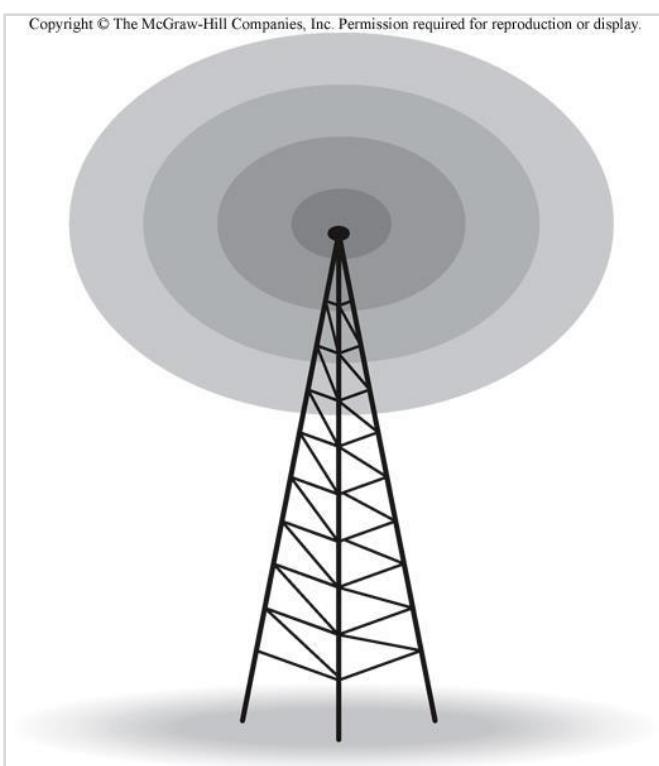


Figura 73- Antena Omnidirecional
Fonte: (STALLINGS, 2005)



Competência 03



Copyright © The McGraw-Hill Companies, Inc. Permission required for reproduction or display.

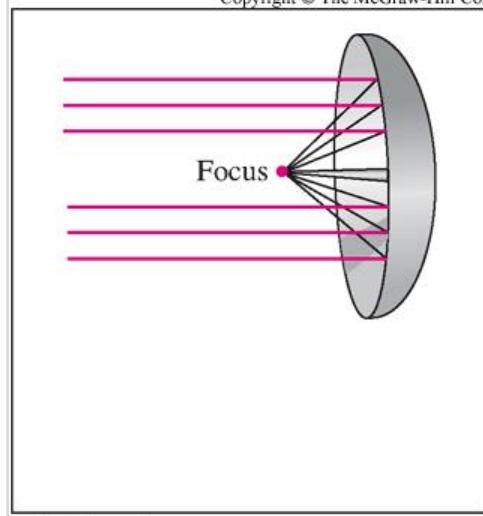
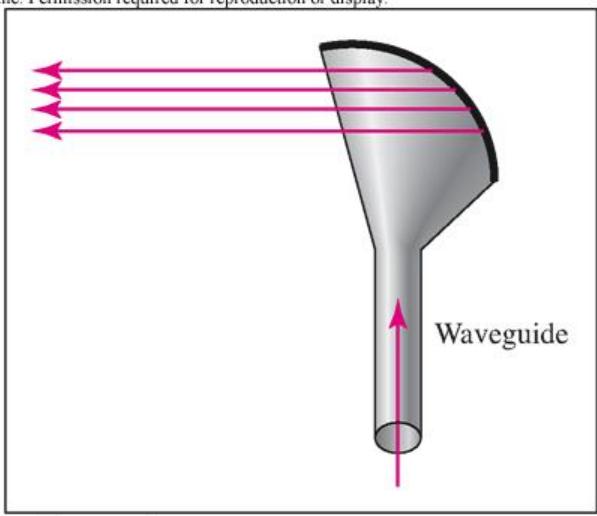
**a. Dish antenna****b. Horn antenna**

Figura 74- Antenas Unidireccionais

Fonte: (STALLINGS, 2005)

Quanto à propagação, a onda eletromagnética pode ser transmitida por terra entre antenas omnidirecionais, utilizando frequências baixas. Com o mesmo sistema, apenas aumentando a frequência do sinal, podemos transmitir através de grandes distâncias utilizando a ionosfera do planeta para refletir as ondas de volta ao solo. Fenômeno igual ao que vimos na fibra ótica. A ionosfera é uma camada de ar menos densa e quando a onda a atinge com um ângulo bem aberto é refletida. Este fenômeno pode ser percebido durante uma viagem, quando já longe da cidade conseguimos captar o sinal de uma emissora de rádio AM.

Você pode estar pensando... isso é Física? Geografia? Computação? É caro (a) aluno (a), realmente é necessária a integração de várias ciências para aquilo que você acha tão simples, como o envio de uma atividade para que o EAD funcione bem, por exemplo. Agora, você está começando a ter uma noção de como tarefas muito complexas se escondem atrás de uma operação tão simples para os usuários.

A figura 75 resume estes métodos de propagação. Nela, você também pode ver outro tipo de propagação: a chamada visada direta (figura mais à direita), que utiliza sinais de frequência muito alta e antenas direcionais uma de frente

Competência 03

para a outra, sem obstáculos. Quanto à distância alcançada na transmissão, em qualquer caso vai depender da potência do sinal. Quanto maior, mais longe os dispositivos podem ficar.

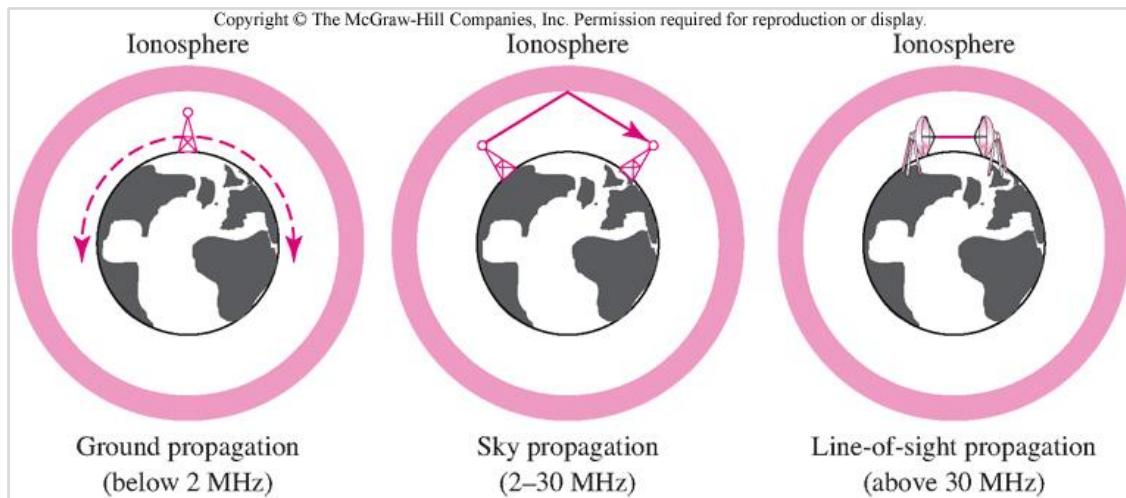


Figura 75- Propagação de ondas eletromagnéticas

Fonte: (STALLINGS, 2005)

As ondas eletromagnéticas utilizadas para comunicação são classificadas em **ondas de rádio, micro-ondas e infravermelho**, de acordo com as faixas de frequência. Ondas de rádio variam de 3 kHz a 1 GHz. De 1GHz até 300 Ghz são as micro-ondas, ficando as infravermelhas na faixa de 300 GHz a 400 THz ($T = \text{Tera}$). Acima disto, temos o espectro de luz visível.

As ondas de rádio, como possuem frequência mais baixa que as demais, conseguem penetrar obstáculos, como as paredes de um prédio, mais facilmente. Podem ser transmitidas a longas distâncias (usando a ionosfera). Porém, sua faixa de frequência (lembra da largura de banda?) é de apenas 1GHz. Esta faixa é adequada para transmissão de voz, que não requer uma taxa alta de transmissão (bps), mas é muito estreita para comunicação de dados, porque é necessário dividir a faixa de frequência para que vários dispositivos possam se comunicar ao mesmo tempo sem misturar as mensagens e, nesta divisão, cada subfaixa ficaria muito estreita.

Já as micro-ondas têm uma faixa de frequência bem larga, são quase 300GHz, permitindo boa taxa de transmissão nas subfaixas. Possui menos penetração

Competência 03

em construção, em especial se utilizarmos a parte mais alta desta faixa. Com antenas direcionais, consegue-se transmissão com baixa taxa de erros. Esta faixa é a utilizada para comunicações em celulares, satélites e redes sem fio (wireless).

As ondas infravermelhas, pela altíssima frequência, não conseguem atravessar paredes e outros objetos. Por isso, só se prestam à comunicação de curta distância. Um exemplo de uso são os controles remotos e comunicação de computadores com periféricos, como impressoras, utilizando uma porta chamada IrDA (*Infrared Data Association*).

3.4.2 Cabeamento Estruturado

Até agora, estudamos sobre cabos de rede, fibra ótica, equipamentos de conexão, repetidores, hubs, switches, roteadores e toda a infraestrutura de uma rede, seja de pequeno ou de grande porte. Porém, precisamos montar esta rede, torná-la funcional. Quando falamos em montar uma rede, uma série de equipamentos são requeridos. São esses equipamentos que tornam possível a troca de dados entre dispositivos com o mínimo de perda de dados, atenuação e interferências.

Cabeamento Estruturado é um conjunto de normas internacionais que regula (cria normas, regras) a disposição organizada e padronizada de cabos, fios, conectores, tomadas, conduítes e dispositivos de transmissão para redes de computadores, voz, imagem, controles prediais, residenciais, industriais e telefonia através de um meio físico padronizado. O Cabeamento Estruturado permite que desktops, servidores, impressoras, telefones, switches, hubs, Access Points, sistemas de alarmes, sistemas antifurto, sistemas de incêndios e roteadores sejam interligados em qualquer infraestrutura independente do layout do prédio ou construção. Esse conjunto de normas possibilita organização, economia e uma maior gerência sobre uma rede seja ela de 10 pontos ou uma imensa rede de uma fábrica ou de um Shopping Center.

Competência 03

A função principal do cabeamento estruturado é disponibilizar cabos em todos os pontos dentro de uma empresa ou residência (pontos de telefone e de dados) e concentrá-los em um ponto central. Este ponto central é o local onde ficarão os equipamentos como hub, switches, roteadores e Access Points. O local que concentra todos os cabos é chamado de **Sala de Equipamentos**, que deve abrigar os equipamentos ativos e passivos de toda a infraestrutura da rede.

Em algumas empresas, esta sala é chamada de CPD – Central de Processamento de Dados (termo em desuso) ou Datacenter, algo como o centralizador de Dados. Grandes empresas gastam fortunas nos seus Datacenters, com segurança, sistema contra incêndio, geradores de energia, acesso biométrico e sistemas de câmeras. Tudo isso porque lá estão todos os dados da empresa, toda a inteligência, toda a infraestrutura que faz a empresa funcionar.

O Padrão internacional de normas de Cabeamento Estruturado é o ANSI/TIA/EIA-568B. No Brasil corresponde a norma NBR 14565, publicada pela ABNT (Associação Brasileira de Normas Técnicas) em 2001. Quando o padrão é seguido, anomalias como a figura 76 jamais serão vistas em uma empresa.

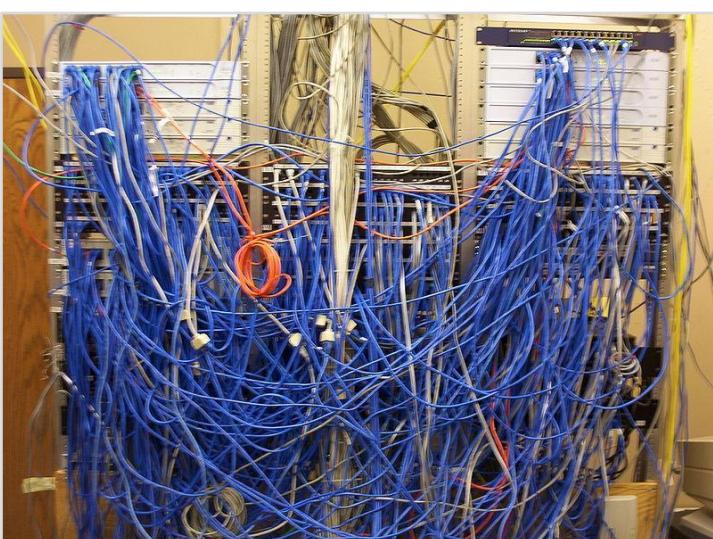


Figura 76- Um cabeamento totalmente desestruturado

Fonte: http://upload.wikimedia.org/wikipedia/commons/8/82/Cable_closet_bh.jpg



Saiba mais:
Equipamentos Passivos: São aqueles que não necessitam de energia elétrica para funcionar.
Exemplo: cabos, conectores, racks, painéis e tomadas.

Equipamentos Ativos: São aqueles que necessitam de energia elétrica para funcionar.
Exemplo: Hub, Switches, roteadores e Access Points.



Mídias Integradas
Conheça um dos maiores Datacenters do Brasil:
http://www.youtube.com/watch?v=8yW0cyvO_Cw
Conheça o Datacenter do Facebook:
<http://www.youtube.com/watch?v=-DRxqHrPrFw>

Competência 03

Quando as normas são seguidas, o cabeamento se torna limpo e com um visual agradável, além de qualquer cabo ser identificado e rapidamente encontrado. (Figura 77)

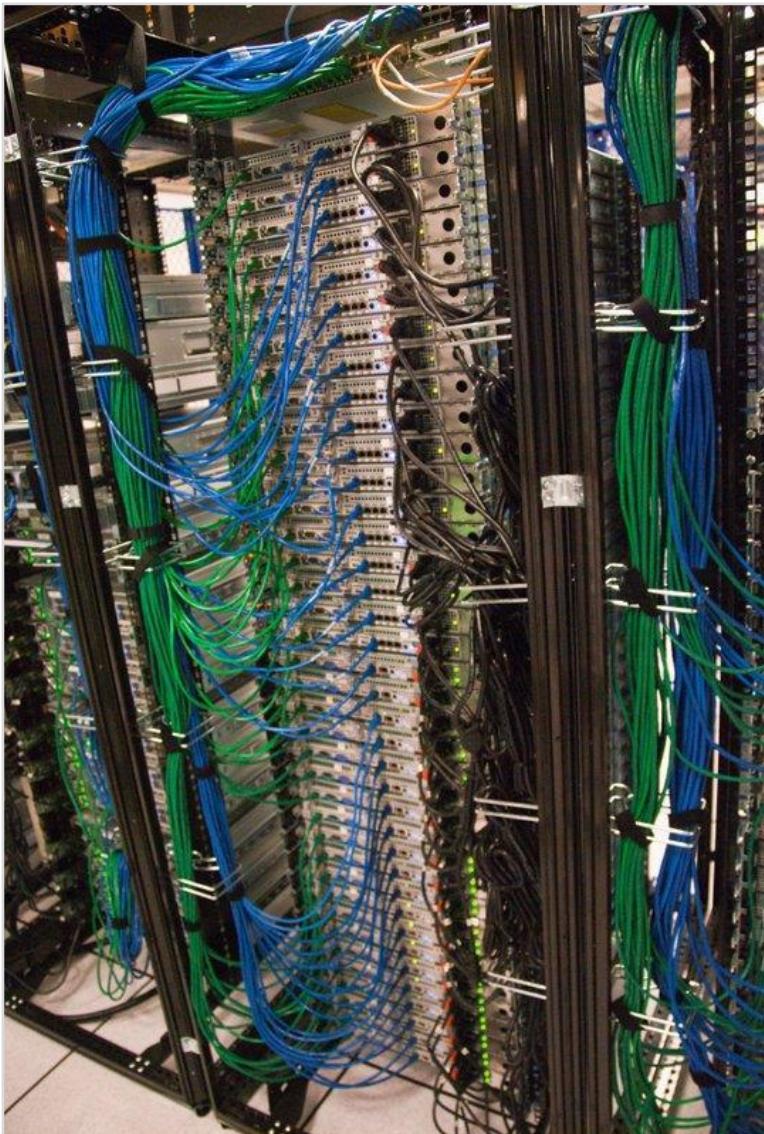


Figura 77- Detalhe de um Datacenter com o uso do Cabeamento Estruturado.
Fonte: http://upload.wikimedia.org/wikipedia/commons/a/aa/Sdtpa_wmf-6.jpg

Na Sala de Equipamentos já citada ficam os Armários de Telecomunicações. Normalmente o armário de telecomunicações é um Rack metálico. Conforme Figura 78. Os Racks também podem ser abertos, conforme Figura 79. Em estruturas menores, você provavelmente vai encontrar racks nas paredes, chamados também de Racks de Distribuição (Figura 80).

Competência 03



Figura 78- Detalhe de um Datacenter. Racks que abrigam servidores e equipamentos de redes.

Fonte: http://upload.wikimedia.org/wikipedia/commons/a/aa/Sdtpa_wmf-6.jpg



Competência 03

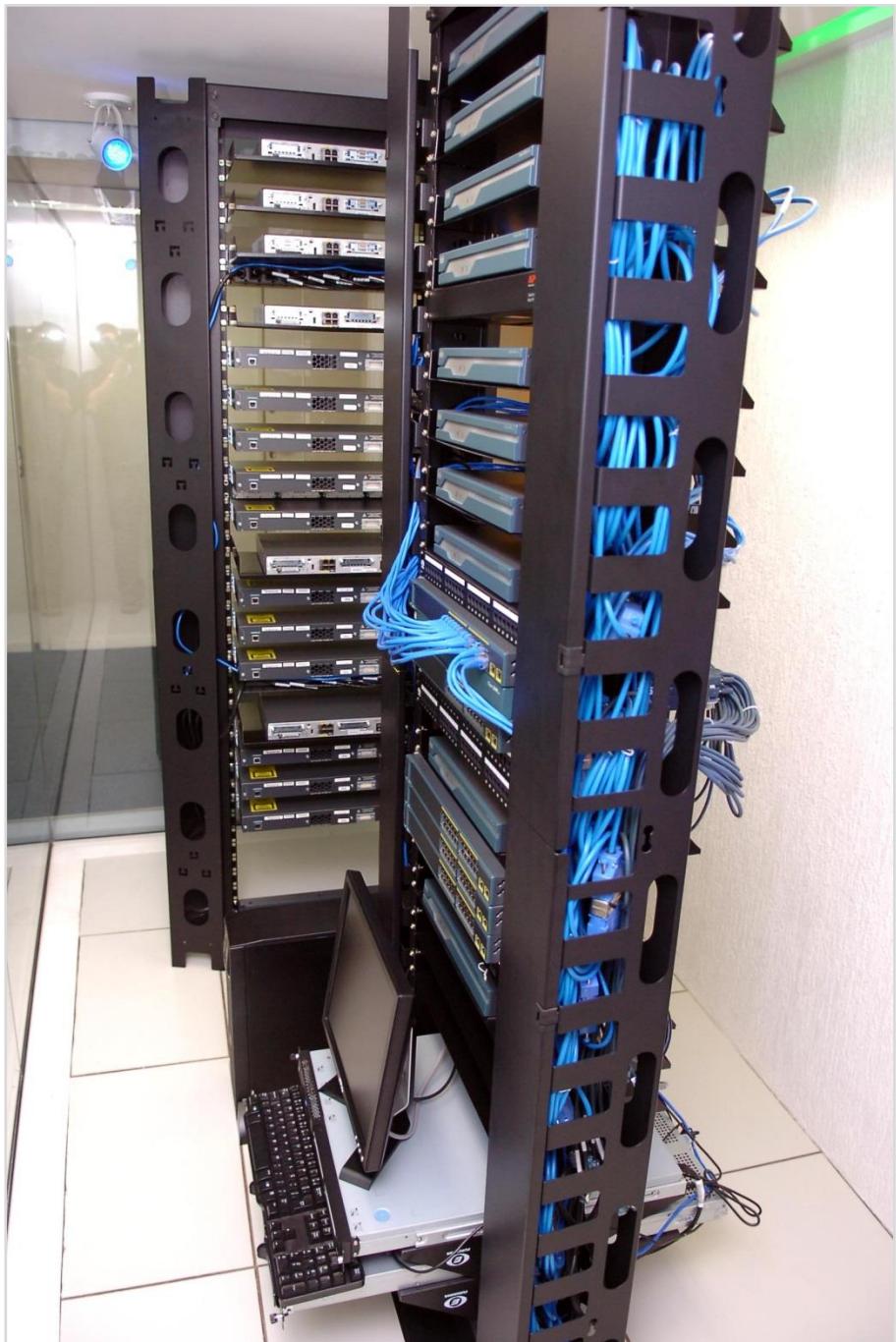


Figura 79- Detalhe de um Datacenter. Um Rack Aberto.

Fonte: http://upload.wikimedia.org/wikipedia/commons/e/ee/Cisco_Hall_Infnet.jpg

Competência 03



Figura 80-Um Rack de distribuição. Fica preso na parede e normalmente recebe apenas switchs e patch panel.

Fonte: http://upload.wikimedia.org/wikipedia/commons/e/ea/Rack_distribution_box.jpg

Dois itens básicos ficam abrigados dentro de um Rack, seja ele aberto ou fechado: o dispositivo ativo, que irá fazer a rede funcionar, como um switch (Figura 81), e um equipamento passivo que tem a função de receber os cabos e distribui-los pelas portas do Switch. Este equipamento é o Patch Panel, ou Painel de Conexão (Figura 82). Do mesmo jeito que se compra um Switch pela quantidade de portas (8, 16, 24 e 48 portas), o Patch Panel também segue esta lógica. Então se compramos um Switch de 24 portas, também deveremos comprar um Patch Panel de 24 portas.

Competência 03



Figura 81- Switch de 24 Portas. Nesta imagem temos dois. Note as abas laterais. São utilizadas para fixar no Rack.

Fonte:

http://upload.wikimedia.org/wikipedia/commons/7/76/Switch_fastethernet_dlink.jpg

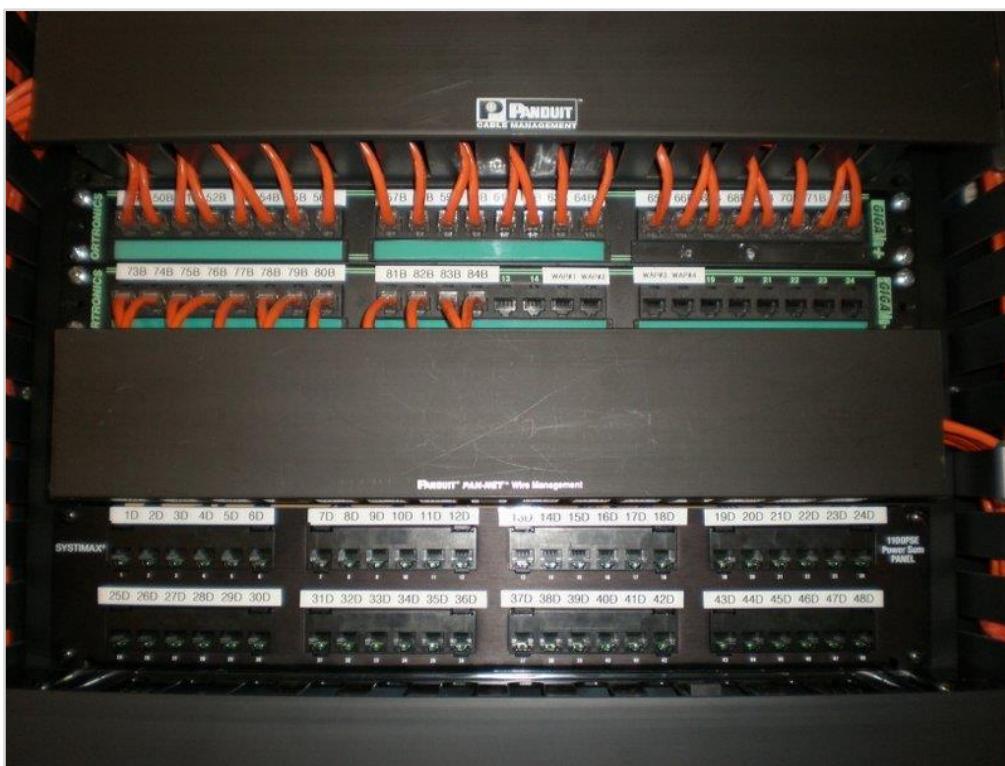


Figura 82- Note a presença de 4 Patch Panels. Eles já estão fixados no Rack.

Fonte: http://upload.wikimedia.org/wikipedia/commons/5/55/Panduit_Pan-Net_Cable_Management_System_detail_2.JPG

Competência 03

Note que da frente do Patch Panel saem cabos que devem ser ligados ao equipamento ativo da rede. Estes cabos são denominados de Patch Cord.

O cabo que normalmente é utilizado na confecção de uma rede é UTP Categoria 5e ou o UTP Categoria 6a. O cabo sai de cada ponto (onde fica o computador ou o telefone) e deve ser identificado através de etiquetas e fixado na traseira do Patch Panel. É necessário utilizar uma ferramenta chamada de Punch Down (Figura 83)

Do outro lado, onde fica o computador, fica uma tomada RJ-45 Fêmea (figura 63) fixada na parede. Esta tomada irá receber o cabo que sai da placa de rede do computador até a parede. Este cabo também é conhecido como Patch Cord (Figura 84).



Figura 83- PunchDown. Esta ferramenta é utilizada tanto para prender o Cabo UTP na traseira do Patch Panel, quanto para fazer o conector fêmea da tomada RJ-45 Fêmea.

Fonte: http://upload.wikimedia.org/wikipedia/commons/7/70/Punchdown_tool.jpg

Competência 03



Figura 84- Detalhes de um Patch Cord.

http://upload.wikimedia.org/wikipedia/commons/d/d5/Pkuczynski_RJ-45_patchcord.jpg

A situação que a figura 85 demonstra não deve ser seguida. Os cabos estão indo diretamente para o Switch. Como vimos, o correto é primeiro ir ao Patch Panel. Uma das razões é a de que o peso dos cabos pode danificar a porta do equipamento.



Competência 03



Figura 85- Um exemplo de um erro comum. Cabos indo direto para o Switch.
http://upload.wikimedia.org/wikipedia/commons/4/4d/Rack_system3.jpg

No Rack existe um equipamento passivo chamado de Guia de Cabos, mas é conhecido popularmente de Organizador de Cabos (Figura 86) que tem a função de deixar os cabos organizados. Ele geralmente é posicionado entre o Switch e o Patch Panel.

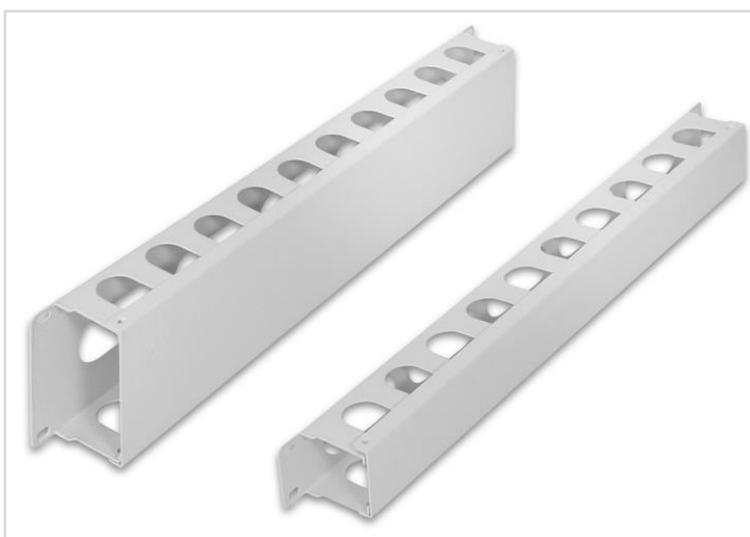


Figura 86- Organizador de Cabos
Fonte: <http://loja.awtec.com.br/images/awtec.com.br/produtos/718546.jpg>

Competência 03

O Cabeamento pode seguir dois padrões segundo a norma ANSI/TIA/EIA-568B. Ele pode ser confeccionado sob o padrão EIA/TIA 568A ou EIA/TIA 568B. Esses padrões explicam como os 8 fios do cabo UTP devem ser organizados para serem encaixados no conector RJ-45 Macho (Figura 87 e Figura 88).

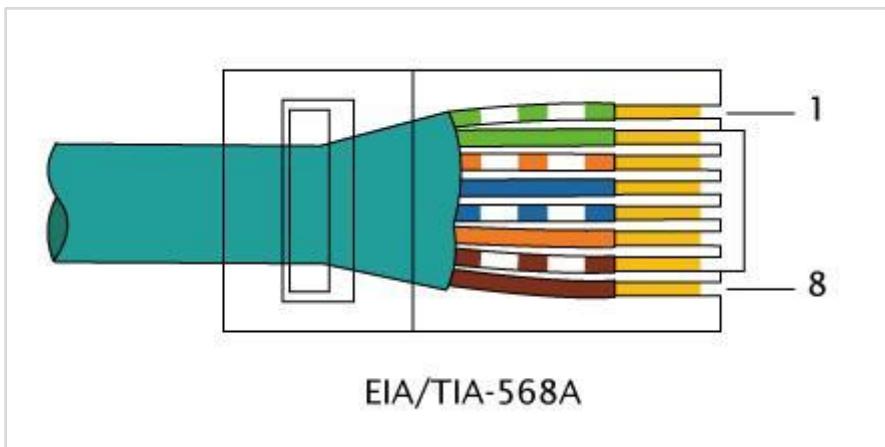


Figura 87- Padrão 568-A. Um dos padrões da norma. Ao fazer um cabo sob esta norma, as duas pontas do cabo devem estar no mesmo padrão.

http://upload.wikimedia.org/wikipedia/commons/7/75/RJ-45_TIA-568A_Right.png

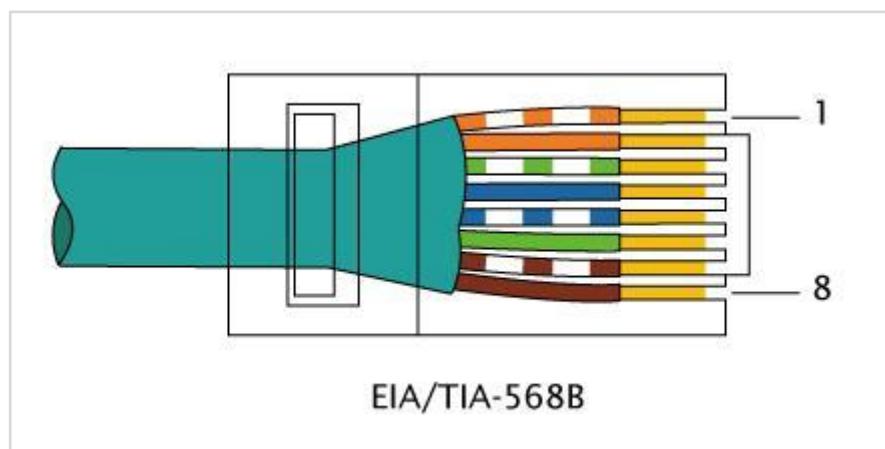


Figura 88- Padrão 568-B. Um dos padrões da norma. Ao fazer um cabo sob esta norma, as duas pontas do cabo devem estar no mesmo padrão.

http://upload.wikimedia.org/wikipedia/commons/e/ef/RJ-45_TIA-568B_Right.png

A figura 89 traz uma tabela que detalha a organização destes cabos dentro do cabo UTP. Não existe regra que indique o que usar, se padrão A ou B, porém o padrão mais popular é o padrão 568-A.

Competência 03

Pino	Par 568A	Par 568B	Fio	Cor 568A Color	Cor 568B
1	3	2	tip	 branco/verde	 branco/laranja
2	3	2	ring	 verde	 laranja
3	2	3	tip	 branco/laranja	 branco/verde
4	1	1	ring	 azul	 azul
5	1	1	tip	 branco/azul	 branco/azul
6	2	3	ring	 laranja	 verde
7	4	4	tip	 branco/marrom	 branco/marrom
8	4	4	ring	 marrom	 marrom

Figura 89- Disposição dos fios em cada um dos padrões da norma.

http://pt.wikipedia.org/wiki/Crossover_%28cab%C3%A3o%29

O ato de fazer um cabo de rede é chamado de “Crimpar”, uma palavra que não existe na nossa língua. Ela foi “aportuguesada” da ação de cravar (*Crimping*) o cabo no conector. A Figura 90 demonstra a “crimpagem” com um alicate de “crimpar”.



Figura 90- O Ato de crimpar um cabo de rede.

http://upload.wikimedia.org/wikipedia/commons/b/bc/Alicate_crimpar.jpg

Fazer um cabo de rede não é uma tarefa muito fácil, pois as oito conexões têm que ter sido crimpadas corretamente dentro do conector RJ-45. Para auxiliar nessa tarefa, existem testadores de cabos, como o da figura 91.

Competência 03



Figura 91- Testadores de cabo. Estes modelos são bem simples e só informam se o cabo está corretamente crimpado nos conectores.

http://upload.wikimedia.org/wikipedia/commons/0/04/Network_cable_tester.jpg

Existem outros tipos de testadores (figura 92) que certificam o cabo. Estes são bem mais caros, porém eles são capazes de informar se o cabo tem o comprimento correto, se está com problemas de conectividade e informam dados como problemas com atenuação.

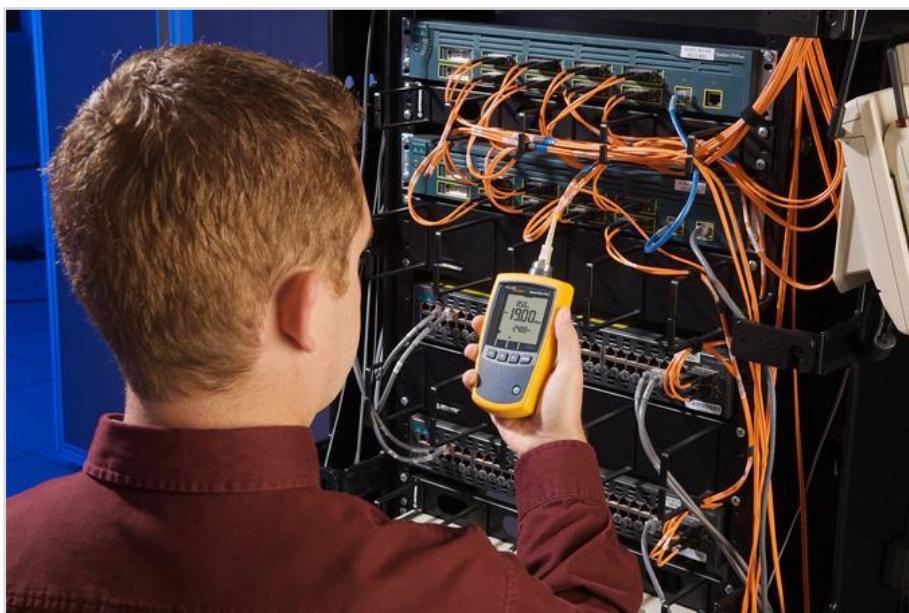


Figura 92 Certificadores de Cabo

http://upload.wikimedia.org/wikipedia/commons/2/26/Fn-SimpliFiberPro_11a_s.jpg

Competência 03

3.5 Projeto de Redes

Agora que já conhecemos alguns componentes do Cabeamento estruturado, vamos aplicar a uma pequena estrutura? Observe a figura 93

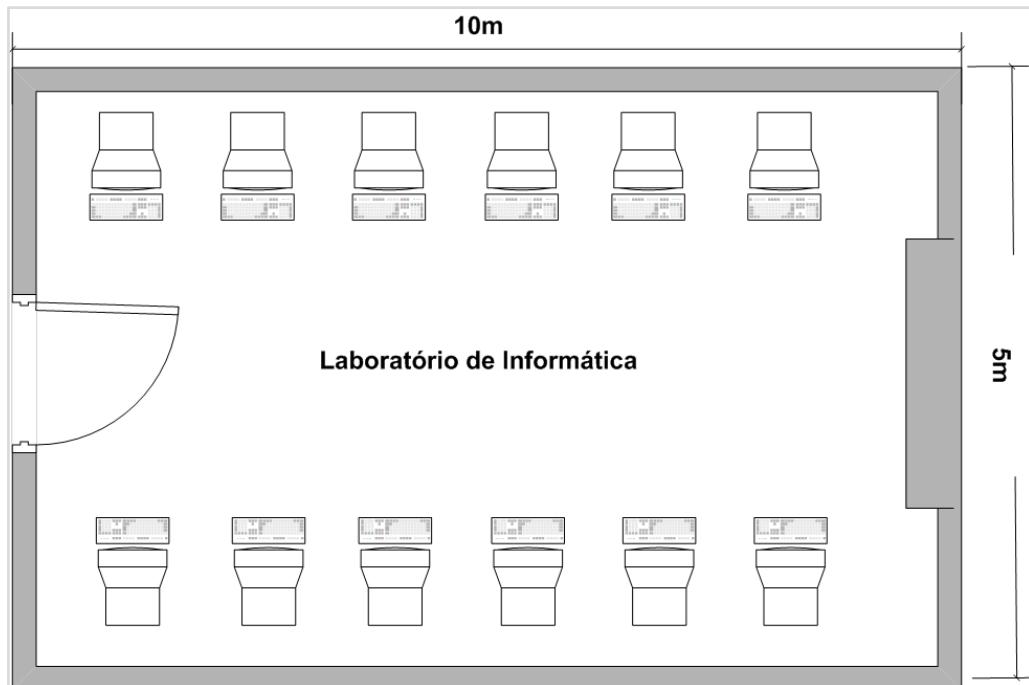
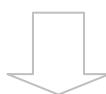


Figura 93- Uma planta de um laboratório de informática.

Fonte: Produzido pelo autor

Vamos fazer o projeto do cabeamento estruturado para este laboratório de informática ?

Primeiro passo: Onde ficará o rack? Vamos colocá-lo ao lado do quadro da sala. Vamos supor que a sala tenha 3m de altura. Então o rack ficará do lado esquerdo da sala, no teto, conforme a figura 94.



Competência 03

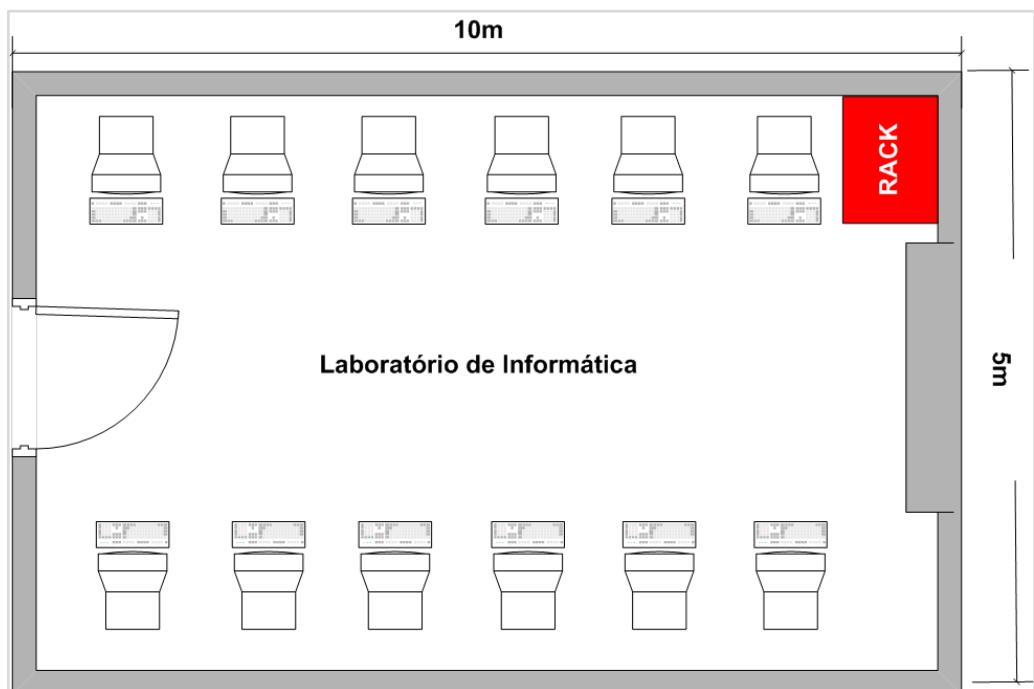


Figura 94- Posicionamento do rack.

Fonte: Produzido pelo autor

Segundo passo: Medir os cabos. Aqui vai uma dica: sempre calcule com folga, para não ter surpresa e faltar cabos, conectores e tomadas.

Temos 10 máquinas e o comprimento da sala tem 10m.

5 Máquinas estão do mesmo lado do rack. Então, uma conta rápida seria:

5 Máquinas X 5m = 50m, mesmo sabendo que algumas máquinas estão mais próximas e outras no fim da sala. Lembre-se ainda que o rack está a 3m de altura. Então, cada cabo vai subir mais 3m:

$$5 \text{ Máquinas} \times 3\text{m} = 15$$

$$\text{Somando tudo: } 50\text{m (5 Máquinas)} + 15\text{m (Altura do Rack)} = 65\text{m}$$

Mas, ainda falta o outro lado da sala. A conta seria a mesma, só que há 5 metros de distância a mais que a largura da sala. Então:

Competência 03

O Cálculo para uma máquina seria:

$$5\text{m} \text{ (Largura da sala)} + 10\text{m} \text{ (distância)} + 3 \text{ (Altura do rack)} = 18\text{m}$$

$$5 \text{ Máquinas} \times 18\text{m} = 90\text{m}$$

Nossa primeira medição: **90 metros** de Cabeamento Horizontal. **Cabeamento Horizontal ou Cabeamento Secundário** é o cabeamento que sai da máquina direto para o rack.

Agora, vamos calcular os Patchs cords.

No rack, a norma fala que um Patch Cord tem que ter no mínimo 1,5m. Então temos 10 máquinas \times 1,5m = 15m.

Ainda falta calcular o Patch Cord que liga o computador direto na tomada na parede. Este cabo também pode ter entre 1,5m e 3m. Essa folga é para que o usuário tenha a possibilidade de mudar o computador de local sem ter que alterar o lugar da tomada. Vamos fazê-lo com 3m. Então são 10 máquinas \times 3m = 30m.

Não se perca ☺:

$$90\text{m} \text{ (Cabeamento Horizontal)} + 15\text{m} \text{ (Patch Cord do rack)} + 30\text{m} \text{ (Patch Cord do computador)} = 135\text{m} \text{ de Cabo UTP Categoria 5e}$$

Nosso primeiro número: **135m de Cabo UTP Categoria 5e**

Obs: Uma caixa de Cabos UTP tem 180m. Então vamos optar por comprar uma caixa de cabos.

Terceiro passo: Cálculo dos conectores.

Competência 03

Patch Cord do Rack = 2 Conectores RJ-45 Macho (um de cada lado).

10 Cabos X 2 Conectores = 20 conectores.

Patch Cord da máquina = 2 Conectores RJ-45 Macho (um de cada lado).

10 Cabos X 2 Conectores = 20 conectores

20 + 20 conectores = 40 Conectores RJ-45 Machos.

Como é comum na hora de crimpar os cabos haver erros, sempre colocamos uma folga de 10 a 20%.

Nosso segundo número: 50 conectores Rj-45 machos

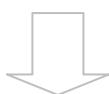
Quarto Passo: Cálculo das tomadas RJ-45 Fêmea.

Esse é fácil: Cada computador vai consumir uma tomada. Então,

10 Computadores X 1 Tomada = 10 Tomadas RJ-45 Fêmea.

Nosso terceiro número: 10 Tomadas RJ-45 Fêmea de Sistema X.

Como não queremos quebrar as paredes para embutir o cabeamento (isto torna o custo do projeto muito caro), usaremos tomadas padrão Sistema X, conforme a figura 95.



Competência 03



Figura 95- Tomadas Sistema X

Fonte: www.dicomp.com.br/foto/6838_1_g_canaleta-sistema-x-20-x10-x2000-mm-branco-palha-tramontina.jpg

Como o nosso cabeamento será externo, deveremos proteger nossos cabos com canaletas de Sistema X, o mesmo utilizado para as tomadas externas. Basta uma canaleta de cada lado da sala e uma passando por baixo do quadro e subindo até o rack.

As canaletas são compradas em milímetros (em relação a largura). Para caber os 5 cabos de cada lado da sala, uma canaleta de 100mm é suficiente. Então:

10m (um lado da sala) + 10m (outro lado da sala) + 5m (largura da sala) + 3m (altura do rack) = 28m de canaleta.

Nosso quarto número: 30m de Canaleta Sistema X 100mm (foi arredondado, ok?)

Vamos agora montar nosso rack. Como redes de computadores estão em constante crescimento, não vale a pena comprar um switch pequeno. Pouco tempo depois, aparecerão novos pontos na sala como, por exemplo, o micro do professor que não foi contemplado, ou pontos novos fora da sala ou ainda os notebooks dos alunos que podem acessar diretamente de uma bancada com pontos de redes ou ainda um acesso Wireless (via rede sem fio). Então, vamos sugerir um Switch de 24 portas. Seguindo nossos estudos, vamos também adquirir o Patch Panel de 24 portas. Não se esqueça do organizador

Competência 03

de cabos e vamos adicionar um novo componente, uma régua elétrica, conforme a figura 96.



Figura 96- Régua Elétrica

Fonte: www.dicomp.com.br/foto/1962_1_g_regua-19-4-tomadas-para-rack-cabo-2-80m-preto.jpg

Quase íamos esquecendo... E o rack?

Bom, como é uma pequena rede, vamos optar pelo rack de distribuição. Como cada equipamento que irá ocupar o nosso rack irá ocupar um U, compraremos um rack de 6Us de altura.

Nossos últimos dados:

1 Rack de 6Us

1 Switch 24 Portas 100Mbps

1 Patch Panel 24 Portas

1 Guia de Cabos (Organizador de Cabos)

1 Régua Elétrica de 5 tomadas.

Vamos resumir esse projeto na tabela 2, simulando um orçamento para o curso de informática do dono desta sala. Os preços praticados nesta tabela são fictícios.

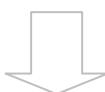
Competência 03



DESCRÍÇÃO	QUANTIDADE	PREÇO
Caixa de Cabo UTP Cat. 5e	1 Caixa	R\$ 100,00
Conectores RJ-45 M	50 Unidades	R\$ 25,00
Tomadas RJ-45 F Sistema X	10 Unidades	R\$ 70,00
Canaletas 100mm Sistema X	30 Metros	R\$ 150,00
Rack 6Us	1 Unidade	R\$ 100,00
Switch 24 Portas 100Mbps	1 Unidade	R\$ 900,00
Patch Panel 24 Portas Cat 5e	1 Unidade	R\$ 120,00
Guia de Cabos	1 Unidade	R\$ 80,00
Régua de 5 Tomadas	1 Unidade	R\$ 60,00
Mão de Obra	-	R\$ 1.000,00
Total		R\$ 2.605,00

Tabela 2-Orçamento simulado para curso de informática

Fonte: o autor



Competência 03

3.6 Resumo

Você é um guerreiro(a) ! Esta é a nossa última revisão!!! Vamos lá?

Dados precisam ser transformados em sinais eletromagnéticos para a transmissão.

A largura de banda, que define a taxa de transmissão, depende da faixa de frequência suportada pelo canal.

Atenuação, distorção e ruído podem atrapalhar a comunicação.

Os meios de transmissão guiados utilizam um conduíte físico para o sinal.

Par trançado consiste em dois fios isolados e enrolados. São usados para comunicação de voz e dados.

Cabos coaxiais consistem em um condutor central e outro ao seu redor, que funciona como uma blindagem. São usados em redes de TV e LANs padrão Ethernet.

Cabos de fibra ótica são meios transparentes e transmitem sinais em forma de luz. Têm alta taxa de transferência e são imunes a interferências.

Transmissão sem fio usam ondas eletromagnéticas e não usam meios físicos.

Ondas eletromagnéticas são classificadas como ondas de rádio, micro-ondas e infravermelho.

Cabeamento estruturado é um conjunto de normas internacionais que regula a disposição de cabos, conectores, tomadas, conduítes e dispositivos de transmissão.

Competência 03

A norma internacional que regula o cabeamento estruturado é a ANSI/TIA/EIA-568B.

A Sala de equipamentos é o local onde fica o Armário de Telecomunicações, que abriga os componentes ativos e passivos da rede.

O Rack é o componente que abriga os equipamentos de rede.

Switch, Patch Panel, Guia de Cabos e Régua Elétrica são equipamentos que ficam dentro do Rack.

Os racks podem ser abertos, fechados e de distribuição.

Os cabos sob a norma podem ter dois padrões de construção: 568A ou 568B.

Os cabos podem ser testados através de um aparelho chamado Testador de Cabos.

Certificadores de cabos são aparelhos mais sofisticados que medem a eficiência de um cabo.

Patch Cord é o nome do cabo que liga o Patch Panel ao Switch.

Enfim, aprendemos a fazer um pequeno projeto de cabeamento estruturado sob as normas internacionais.



REFERÊNCIAS

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 4 ed. São Paulo. McGrawHill Brasil, 2008.

WEBER, Taisy S. **Tolerância a falhas**: conceitos e exemplos. Universidade Federal do Rio Grande do Sul, 2001. Disponível em: < www.inf.ufrgs.br/~taisy/disciplinas/textos/ConceitosDependabilidade.PDF>. Acesso em: jul. 2009.

STALLINGS, William. **Redes e Sistemas de Comunicação de Dados**: teoria e aplicações corporativas. 5 ed. Rio de Janeiro. Elsevier, 2005.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 4 ed. São Paulo. McGrawHill Brasil, 2008.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 5 ed. São Paulo. McGrawHill Brasil, 2008.

PETERSON, Larry L. e Davie, Bruce S. **Redes de Computadores**. Tradução da 3 ed. Rio de Janeiro. Elsevier, 2004.

STALLINGS, William. **Redes e Sistemas de Comunicação de Dados**: teoria e aplicações corporativas. 5 ed. Rio de Janeiro. Elsevier, 2005.

FERNANDES, Dailson. **Sistemas Operacionais**. 1 ed. Recife. ETEC.

DHCP, Guia Completo - www.esli-nux.com/2012/07/dhcp-guia-completo.html, Acessado em Outubro de 2013.

Como funciona o DHCP - <http://softwarelivre.org/andre-ferraro/blog/redes-o-que-e-e-como-funciona-um-servidor-dhcp> , acessado em Outubro de 2013.

MINICURRÍCULO DO PROFESSOR



Graduado em Análise de Sistemas, Pós-Graduado em Redes de Computadores pela Universidade Católica de Pernambuco, Administrador de Sistemas e Analista de Segurança, Certificado RHCSA, RHCE, LPI-1, LPI-2, Linux Administrator for SUSE Linux Enterprise, IBM TSM Deployment, IBM System X e ITIL v3. Professor Universitário na Unibratec - União Brasileira dos Institutos de Tecnologia em Recife - PE e Professor de Ensino a Distância pela Secretaria de Educação do Estado de Pernambuco.

