GOVERNO DO ESTADO DO CEARÁ

Secretaria da Educação

ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL - EEEP

ENSINO MÉDIO INTEGRADO À EDUCAÇÃO PROFISSIONAL

CURSO TÉCNICO DE INFORMÁTICA

REDES DE COMPUTADORES

GOVERNO DO
ESTADO DO CEARÁ
Secretaria da Educação

Governador
Cid Ferreira Gomes

Vice Governador
Domingos Gomes de Aguiar Filho

Secretária da Educação
Maria Izolda Cela de Arruda Coelho

Secretário Adjunto
Maurício Holanda Maia

Secretário Executivo
Antônio Idilvan de Lima Alencar

Assessora Institucional do Gabinete da Seduc
Cristiane Carvalho Holanda

Coordenadora da Educação Profissional – SEDUC
Andréa Araújo Rocha

GOVERNO DO ESTADO DO CEARÁ

Secretaria da Educação

Coordenação Técnica Pedagógica
Renanh Gonçalves de Araújo

Equipe de Elaboração
Adriano Gomes da Silva
Cíntia Reis de Oliveira
Fernanda Vieira Ribeiro
Francisco Aislan da Silva Freitas
João Paulo de Oliveira Lima
Liane Coe Girão Cartaxo
Mirna Geyla Lopes Brandão
Moribe Gomes de Alcântara
Niltemberg Oliveira Carvalho
Paulo Ricardo do Nascimento Lima
Renanh Gonçalves de Araújo
Renato William Rodrigues de Souza

Colaboradores
Maria Analice de Araújo Albuquerque
Maria Danielle Araújo Mota
Sara Maria Rodrigues Ferreira Feitosa

Você, aluno do curso de Redes de Computadores deve estar bastante curioso em relação à sua formação e talvez já tenha se perguntado: "Afinal, o que são Redes de Computadores?". Então chegou a hora. Neste livro vamos falar sobre os tipos de redes, os meios de comunicação e as formas de transmissão de dados. Vamos ainda estudar como funciona uma rede dividindo-a em camadas para que haja uma melhor compreensão. Bons Estudos!

A Autora.

1. INTRODUÇÃO ÀS REDES DE COMPUTADORES

1.1. O QUE SÃO E PARA QUE SERVEM AS REDES DE COMPUTADORES.

Provavelmente você já foi a uma loja ou supermercado e notou que todos os atendentes utilizam computadores com um sistema, ou programa, para efetuar a venda dos produtos. Para que todos os computadores do estabelecimento utilizem o mesmo programa é necessário que os computadores estejam interligados e se comuniquem. Esta ligação pode ser chamada de **Rede**.

Uma rede de computadores é a forma de conectarmos equipamentos a fim de que possamos estabelecer uma comunicação entre os mesmos fazendo com que eles troquem dados, informações e serviços.

Sem uma rede, os estabelecimentos do exemplo acima não conseguiriam usar seu sistema de vendas de forma eficiente. Quando um vendedor finaliza a venda de um produto, este produto passa a não constar mais no estoque. Sem uma rede, este mesmo produto ainda iria constar no sistema de outro vendedor, que correria um grande risco de vender um produto que não existe mais na loja.

As redes estão muito mais presentes em nossa vida do que podemos imaginar. Seja em no celular, na internet, no computador de um hospital ou posto de saúde, no banco, no caixa eletrônico ouno sensor de velocidade. As

redes de computadores, apesar do nome, envolvem muito mais que apenas computadores, mas abrangem uma gama de dispositivos e equipamentos como celulares, tablets, impressoras, TVs, carros, videogames e até eletrodomésticos.

Uma **rede corporativa**, ou seja, uma rede de uma corporação como uma empresa, órgão ou instituição é demasiadamente importante para o bom funcionamento do ambiente de trabalho. Com ela é possível compartilhar arquivos, trocar mensagens, enviar diversos tipos de dados, compartilhar equipamentos como impressoras e aparelhos de fax, distribuir internet, publicar um site interno, gerenciar e-mails, ter acesso ao banco de dados e até mesmo controlar o acesso de usuários na rede. Controle este essencial quando se zela pela **segurança**, evitando o acesso de intrusos que podem capturar informações sigilosas ou desconfigurar algum serviço.

A segurança em redes é um ponto crucial. Apesar de todos os esforços dos profissionais de Segurança das Informações e de todas as ferramentas já criadas para evitar ataques e intrusões, as nossas redes não são 100% seguras. Você verá este assunto de forma mais aprofundada em disciplinas posteriores, mas fica a dica: os trabalhos que envolvem segurança de redes estão em constante crescimento e é uma ótima área para se especializar.

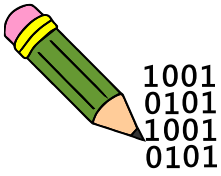
Então tudo bem, já entendi o que é uma Rede de Computadores, mas que tipos de dados ou arquivos eu posso enviar e receber ao usar uma rede?

1.1.1. Dados que podem ser transmitidos

Provavelmente você já viu uma foto ou uma música serem enviadas de um celular para outro através do Bluetooth. Este é um exemplo detransmissão é baseado nas redes de computadores de curta distância.

Sabemos que os computadores processam informações calculando bits que podem ser convertidos em impulsos elétricos, portanto **toda informação que pode ser processada em bits, pode ser transmitida em uma rede**.

Arquivos de **áudio** como músicas, arquivos de **vídeo**, **textos** e **imagens** podem ser convertidos em bits, portanto podem ser enviados através de uma rede. Informações como o aroma de uma flor ainda não podem ser convertidas em bits, portanto não podem ser transmitidas, mas já existem pesquisadores desenvolvendo telas que permitem que o usuário sinta a textura das imagens como a aspereza do caule de uma árvore ou a profundidade de um buraco. Ficou curioso para saber como funciona? Quando tiver um tempo livre, pesquise sobre o assunto na internet!



Exercícios

1. Indique e explique o que está errado na seguinte frase: *"Uma rede de computadores é a forma de conectarmos equipamentos a fim de que possamos bloquear uma comunicação entre os mesmos."*

_____
_____
_____
_____

2. Cite outros locais onde podemos encontrar uma rede de computadores.

_____
_____

3. Diferencie rede corporativa de rede doméstica.

_____
_____
_____

4. Por que devemos zelar pela segurança em uma rede de computadores?

_____

_____

_____

5. Quais tipos de dados podem ser transmitidos em uma rede?

_____

_____

1.2. REDES PONTO-A-PONTO E CLIENTE-SERVIDOR

Existem 2 tipos fundamentais de redes. O primeiro tipo é a rede **ponto-a-ponto**, onde os computadores são ligados entre si para a troca de informações, porém a maioria dos recursos não pode ser compartilhada fazendo com que cada **host** deva possuir os próprios recursos e aplicações como um programa, por exemplo.

Figura 1a. Rede ponto-a-ponto.

HOST: Palavra inglesa que significa hospedeiro.

Em informática, um **host** é um computador ou outro equipamento conectado na rede e que pode compartilhar informações, serviços e recursos.

O segundo tipo é a arquitetura **cliente-servidor**, onde todos os hosts, chamados de clientes, se comunicam com uma máquina principal, chamada de servidor. O servidor provê todas as aplicações e serviços e consegue gerenciar

o acesso aos recursos da rede como impressoras, por exemplo. Neste tipo de arquitetura os hosts não trocam informações entre si de uma forma direta. Cada cliente se comunica com o servidor e este devolve respostas atendendo as requisições de cada um. Por exemplo, em um servidor de banco de dados, o cliente pode acessar a aplicação (programa) e alterar um dado. Esta alteração será feita no servidor. Caso outro cliente acesse a aplicação, ele já verá o dado alterado, pois está buscando a informação diretamente no servidor.

Normalmente um servidor é uma máquina mais robusta que as máquinas clientes, pois ela armazena e processa um grande número de informações, além de precisar estar sempre ligada para que haja tráfego de informações na rede.

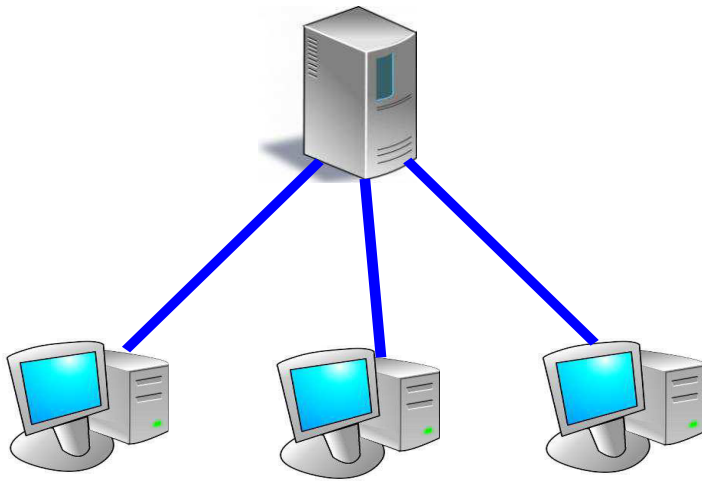


Figura 1b. Rede cliente-servidor.

1.3. COMO FUNCIONA A TRANSMISSÃO

Nós, seres humanos, usamos diversos meios para nos comunicar. Você, por exemplo, se tiver uma dúvida deverá fazer uma pergunta ao seu professor e este, por sua vez, deverá responder à pergunta de forma a tirar sua dúvida. Neste caso, vocês conseguiram se comunicar e tudo ficou resolvido. Porém, se você não perguntar da maneira correta, ou se houver algum ruído durante a pergunta, talvez o professor não compreenda bem e acabe respondendo de forma equivocada. Neste caso, houve um problema na transmissão da informação, consequentemente a comunicação ficou comprometida. Simples, não é mesmo?

Em redes de computadores, os princípios são os mesmos. Sempre existe um transmissor, um receptor e uma informação a ser enviada. A transmissão de dados na computação requer alguns componentes essenciais [Ribeiro, 2010]:

- **Transmissor:** é o dispositivo (computador, telefone, câmera) que envia a informação.
- **Receptor:** é o dispositivo a quem foi endereçada a informação. O receptor vai receber a mensagem enviada pelo transmissor.
- **Mensagem:** são os dados e as informações que precisam ser enviados.
- **Meio:** é o meio físico, ou seja, o caminho pelo qual a mensagem trafegará do transmissor até chegar ao receptor.
- **Protocolo:** controla o envio e recepção da mensagem e define alguns aspectos como formato da mensagem e ordem de chegada. Tanto o transmissor quanto o receptor devem estar seguindo o mesmo protocolo.

No exemplo anterior, o transmissor é você (o aluno); o receptor é o professor; a mensagem é a pergunta; o meio é o ar, por onde a ondas sonoras da sua voz se propagam e o protocolo é a palavra falada em língua portuguesa.

Para que a comunicação de dados obtenha sucesso ela necessita de três atributos:

- **Entrega:** os dados devem estar endereçados corretamente. Deve-se ter a certeza de que a informação será entregue ao destinatário correto.
- **Confiabilidade:** os dados devem chegar ao destino, e mais do que simplesmente chegar, os dados devem estar intactos, sem nenhum tipo de alteração e sem faltar nenhuma parte da informação.
- **Controle do Atraso:** o tempo que a informação possui para chegar ao destino não pode ser indeterminado. Deve haver um tempo limite para

que o destinatário a receba, principalmente no caso de aplicações multimídia em tempo real como áudio e vídeo. Não seria interessante, por exemplo, ao receber um vídeo, ver primeiro as imagens e só depois ouvir o áudio.

Taxa de transmissão

Ao se transmitir um arquivo, seja ele de que tipo for, pela rede, na realidade estão sendo transmitidos vários bits que, em conjunto, comporão o arquivo depois de processados. A taxa de transmissão de uma rede é a velocidade com a qual esses bits trafegam pelos meios de comunicação e é medida em **bps** (bits por segundo), ou seja, a quantidade de bits que são enviados em um segundo, portanto quanto maior a taxa de transmissão de uma rede, mais rápido o arquivo consegue ser transmitido do emissor para o receptor.

Ah, então é por isso que uma internet de 600kbps é mais rápida que uma de 100kbps! Porque são enviados mais bits, ou seja, mais informação, em um mesmo segundo.

Pela lógica, internet de 100kbps precisará de 6 segundos para enviar a mesma quantidade de informação que a internet de 600kbps envia em apenas um segundo.

1.4. MODOS DE OPERAÇÃO

Existem três tipos de operação na transmissão de dados: simplex, half-duplex e full-duplex. Vejamos como funciona cada uma delas:

- **Simplex:** a transmissão é unidirecional. Só existe um transmissor e um canal de transmissão. Quaisquer outros componentes que apareçam na comunicação serão receptores. Exemplos: televisão e radiodifusão.
- **Half-duplex:** a transmissão é bidirecional, ou seja, as duas partes transmitem e também são receptoras, mas, assim como no modo simplex, existe somente um canal de transmissão, portanto só é possível transmitir um por vez. Exemplo: walkie-talkie.
- **Full-duplex:** é o modo de transmissão mais completo, já que ambas as partes podem transmitir e receber dados simultaneamente, pois existem dois canais de transmissão. Exemplo: telefone.

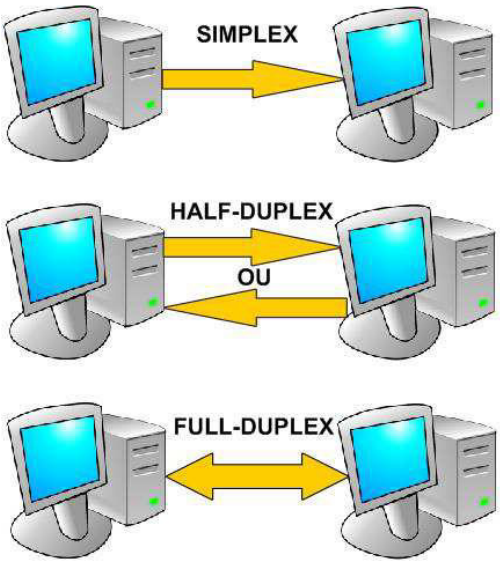
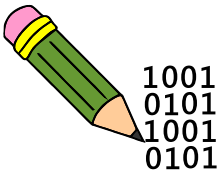


Figura 1c. Modos de Transmissão



Exercícios

1. Marque V para verdadeiro e F para falso:
   ( ) Em uma rede ponto-a-ponto cada host deve possuir os próprios recursos e aplicações.

( ) Em uma arquitetura cliente-servidor, todos os hosts chamados servidores se comunicam com uma máquina principal chamada de servidor.

2. Quais as diferenças no hardware de uma máquina cliente em relação a uma máquina típica para servidores?

_____
_____
_____
_____

3. Qual a importância da taxa de transmissão em uma comunicação?

_____
_____
_____

4. Analise os meios de comunicação abaixo e indique se a transmissão em cada um deles é do tipo (S) simplex, (H) half-duplex ouu (F) full-duplex.
   ( ) radioamador
   ( ) televisão
   ( ) celular
   ( ) radiodifusão

ANOTAÇÕES

2. MEIOS DE COMUNICAÇÃO

2.1. Cabos elétricos, fibras ópticas e ondas de radiofrequência.

Já vimos como funciona uma transmissão de dados entre dois equipamentos em uma rede, mas para que a transmissão aconteça é necessário que exista um meio de os dados saírem de um host e chegarem a outro, ou seja, uma forma de propagação.

Uma das formas de se enviar dados é através da eletricidade. As placas de rede com fio são responsáveis por converter dados em bits e bits em impulsos elétricos que podem trafegar por um cabo de energia. Os cabos mais comumente usados são os **cabos de par trançado** e os **cabos coaxiais**.

Outra forma é transmitindo através da luz em vez da eletricidade. A transmissão feita por raios luminosos é bem mais eficaz que a feita pela eletricidade, pois o sinal se propaga mais rápido e não sofre com interferências eletromagnéticas. Para transmitir desta maneira utilizamos os cabos de **fibra óptica.**

Apesar de toda tecnologia no tocante a cabos, existem alguns casos em que eles não são interessantes. Redes com centenas de hosts requerem muito investimento em cabos. Prédios antigos nem sempre possuem tubulação elétrica própria para efetuar a passagem dos cabos. Uma rede cabeada não possui versatilidade suficiente para que o proprietário mude a posição dos computadores sem um pouco de transtorno. Por esses e outros motivos, torna-se desejável o uso de um meio de comunicação versátil, barato, e abundante: **o ar**. Pelo ar podemos transmitir **ondas de radiofreqüência** através de antenas e efetuar a comunicação entre elementos previamente configurados para este fim. As redes sem fio estão a cada dia mais presentes no nosso cotidiano, nos computadores, celulares, televisores, rádio, entre outros.

Vejamos mais detalhes de cada meio de comunicação de dados:

2.1.1. Cabos de Par Trançado

É o meio de transmissão mais comumente encontrado no nosso dia-a-dia. Com certeza você já deve ter visto uma série de cabos azuis saindo de computadores em um laboratório de informática, cyber café, agência bancária

ou repartições. Esses cabos são compostos por fios de cobre que transmitem através de impulsos elétricos.

Mas porque "par trançado"???

Em todo fio, por onde passa corrente elétrica, cria-se um campo magnético ao redor do mesmo. Esse campo magnético causa interferências eletromagnéticas em fios que estejam próximos e em paralelo. Interferência eletromagnética é uma das grandes causas de problemas em uma rede, podendo fazer com que dados não cheguem ao seu destino e causando instabilidade na rede.

Para tentar diminuir os problemas com a interferência eletromagnética, os fios são enrolados dois a dois, ou seja, em pares. Os pares também são entrelaçados entre si. Este procedimento faz com que diminua a ação da interferência. Além disso, nas redes de até 1000Mb de velocidade, um fio que transmite informação deve ser trançado a um fio que não transmite, ou fio neutro, pela norma EIA/TIA 568 (a qual estudaremos mais adiante).

Existem várias categorias de cabo par trançado, onde podem variar a quantidade interna de fios de cobre e a forma de proteção desses fios.

Os cabos de par trançado são classificados em três tipos básicos:

- UTP (Unshielded Twisted Pair) – São cabos que não possuem blindagem, ou seja, não existe proteção a interferências externas. Os fios de cobre são protegidos somente por uma capa de plástico (a cor azul não é padrão, mas é a mais comum no mercado). Os cabos UTP possuem taxas de transmissão que vão de 10Mbps a 10Gbps em redes locais.
- FTP (Foiled Twisted Pair) – São cabos que possuem uma blindagem feita com uma folha de alumínio que envolve todos os pares e que protege os fios evitando interferências com cabos da rede elétrica ou motores próximos ao cabo. Essa blindagem é de um tipo mais simples em relação ao STP.

- STP (Shielded Twisted Pair) – São também blindados, mas tornam-se mais eficientes que os FTP, pois sua blindagem é feita a cada par de cabos, ajudando assim a reduzir tanto a interferência externa quanto a interna, ou crosstalk, que é a interferência entre os pares de cabos.

Figura 2a. Cabos UTP, FTP e STP, respectivamente.

2.1.2. Cabos Coaxiais

Os cabos coaxiais antecederam os cabos de par trançado na conexão de redes, mas hoje são mais utilizados para transmissão de sinal de TV a cabo. O cabo coaxial possui dois condutores e possui uma blindagem entre os condutores permitindo uma boa taxa de transmissão e poucas perdas.

Os cabos coaxiais podem ser classificados por sua impedância, ou seja, sua resistência à passagem de corrente elétrica. Quanto menor a resist~encia, melhor a transmissão pelo cabo, já que o corrente irá fluir mais rapidamente. Os mais comuns são os de 75ohms, usados normalmente para antenas de TV e os de 50ohms, que possuem resistência menor e portanto são mais utilizados para telefonia celular.

Figura 2b. Cabo coaxial.

2.1.3. Fibras Ópticas

A fibra ótica é um fino e flexível fio de vidro feito de sílica, componente derivado do silício, que, diferente dos cabos elétricos, transmite dados a partir de feixes de luz. Como a velocidade da luz é bem elevada, a transmissão dos dados é muito melhor na fibra ótica, podendo chegar a 16Tbps. A fibra ótica é preferencialmente utilizada em redes de longa distância e de alta velocidade, pois não sofrem com interferências eletromagnéticas e possui perca mínima, sendo muito utilizada em empresas de telefonia e televisão, onde em ambas existe a necessidade de que o som e/ou a imagem cheguem em tempo real e em perfeita sincronia.

Existem dois tipos de fibras ópticas: as multimodo e as monomodo.

Nos cabos de fibra **monomodo**, o núcleo da fibra é tão fino que permite que a luz se propague em um único feixe e evitando também muitas reflexões nas paredes internas do cabo. Devido a isso o sinal em uma fibra monomodo pode propagar-se a até 80km de distância, mas fabricar um cabo de fibra tão fino (cerca de 0,008mm) é muito dispendioso, tornando o cabo muito caro.

Nos cabos **multimodo**, o núcleo da fibra é mais espesso (cerca de 0,125mm), tornando sua fabricação mais barata, porém a espessura do cabo permite mais reflexões de sinal, e consequentemente mais perdas. A fibra multimodo alcança, no máximo, 550m.

Figura 2c. Cabo de fibra óptica pronto para uso.

Figura 2d. Cabo de fibra óptica decapado.

2.1.4. Transmissão via rádio terrestre ou microondas

Os sinais de rádio estão num espectro eletromagnético sem utilização de fios e podem atingir grandes distâncias. Porém estas distâncias variam conforme as condições do local, que pode possuir muitas barreiras físicas ou sinais eletromagnéticos gerando perda e atenuação do sinal, o que pode impedir sua propagação.

Para a propagação são instaladas torres que funcionam como estações repetidoras de microondas. Essas torres devem sempre estar “enxergando” a próxima, pois a transmissão se dá em linha reta de uma torre à outra. Um exemplo de tecnologia que utiliza freqüências de rádio é a telefonia celular.

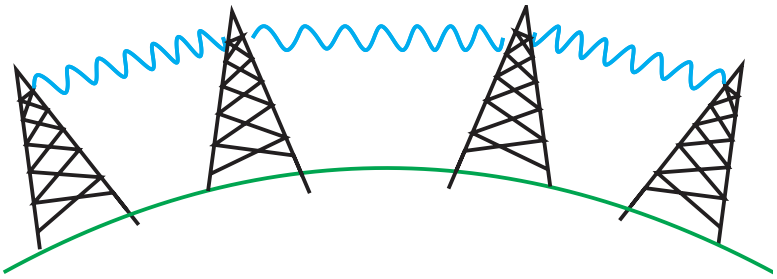


Figura 2e. Estações Repetidoras.

PESQUISA

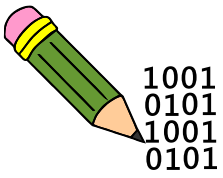
Pesquise os tipos de equipamentos (não obrigatoriamente meios de comunicação) que utilizam ondas de rádio em seu funcionamento.

2.1.5. Transmissão via Satélite

Um satélite liga várias estações repetidoras de microondas as quais citamos anteriormente. Com isso, o satélite é capaz de ligar uma estação terrestre X a outra estação terrestre Y que esteja distante, sem que o sinal tenha que trafegar por todas as estações terrestres vizinhas a X até chegar à estação destino Y. Como isso acontece? Imagine a seguinte situação: *Carlos quer fazer uma ligação de Fortaleza, onde reside, para sua prima Joana em Porto Alegre. Ao efetuar a chamada, o sinal do telefone de Carlos procura a estação repetidora terrestre mais próxima em Fortaleza e ao chegar lá, o sinal é enviado ao satélite que por sua vez localiza e reenvia a chamada para a estação repetidora terrestre mais próxima de Joana em Porto Alegre.*

PESQUISA

Existem alguns tipos de satélites: os GEOS, os LEOS e os MEOS. Pesquise a diferença entre eles e que empresas brasileiras usam satélites.



Exercícios

1. Marque V para verdadeiro e F para falso:
   ( ) Em uma rede sem fio o meio pelo qual os dados trafegam é o ar.
   ( ) Nas fibras ópticas a propagação dos dados é feita através da luz.
   ( ) A fibra óptica do tipo monomodo possui o núcleo tão fino que atrapalha a propagação da luz.

2. Cite os meios de transmissão que utilizam a energia elétrica para a propagação dos dados.

_____

_____

3. Que tipo(s) de cabo(s) de par trançado devemos utilizar em ambientes próximos a grandes antenas de transmissão?

_____

4. Por que os cabos UTP, FTP e STP possuem os pares trançados entre si?

_____
_____
_____
_____
_____

5. Onde encontramos mais facilmente uma instalação feita com cabo coaxial?

_____
_____

6. Diferencie fibra óptica monomodo e fibra óptica multimodo.

_____
_____
_____
_____
_____
_____

7. Por que a transmissão na fibra óptica é mais rápida que nos outros meios de transmissão?

_____
_____
_____
_____

8. Suponha que você foi contratado para instalar uma rede de computadores em um prédio tombado como Patrimônio Histórico, onde as paredes não podem ser quebradas. Que meio de transmissão você utilizaria para melhor atender à solicitação? Como você explicaria para seu cliente a vantagem da escolha feita?

_____
_____
_____
_____
_____

3. TOPOLOGIAS

3.1. Topologias de Redes

A topologia de uma rede nada mais é do que a forma como se define o layout da rede, ou como se organiza estruturalmente os computadores, dispositivos de rede e suas conexões. Uma topologia pode física ou lógica. A topologia física é como os computadores e dispositivos se encontram fisicamente, configurando uma espécie de desenho que é caracterizado pela disposição dos equipamentos. A topologia lógica é a forma como os dados trafegam na rede, logo, uma rede pode obedecer a uma determinada topologia apenas de forma lógica, não sendo necessário que os equipamentos estejam organizados de acordo com a topologia física. Há varias formas de se estruturar uma rede, veja as principais:

3.1.1. Barramento

Na topologia em barramento cada computador é ligado em série, ou seja, um computador atrás do outro em fila, no mesmo meio físico de transmissão de dados. Devido ao fato de todos os computadores compartilharem o mesmo meio de transmissão, só é possível transmitir os dados de um computador por vez. Quando há algum computador transmitindo dados, o meio fica “ocupado” naquele momento. Durante a transmissão todas as máquinas da rede recebem os dados, mesmo que a mensagem seja destinada a apenas uma. Neste momento, se algum outro computador da rede tentar transmitir, acontecerá uma colisão e todo o tráfego deverá ser refeito.

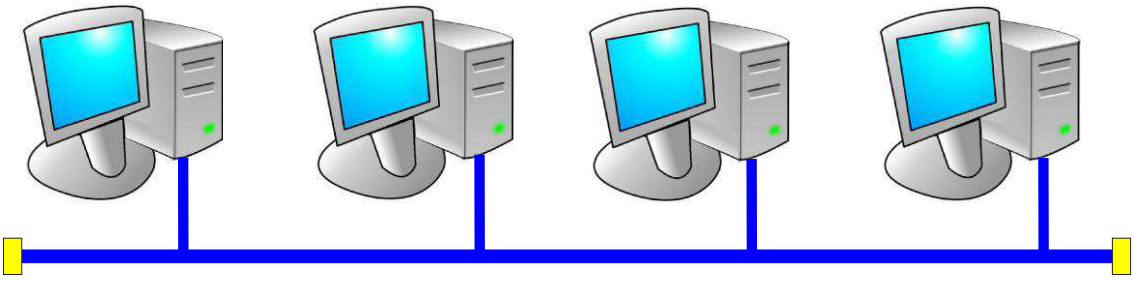


Figura 3a. Topologia em barramento.

3.1.2. Anel

Na topologia em anel, assim como em barramento, os computadores também são ligados em série, porém formam um anel, como na figura abaixo:

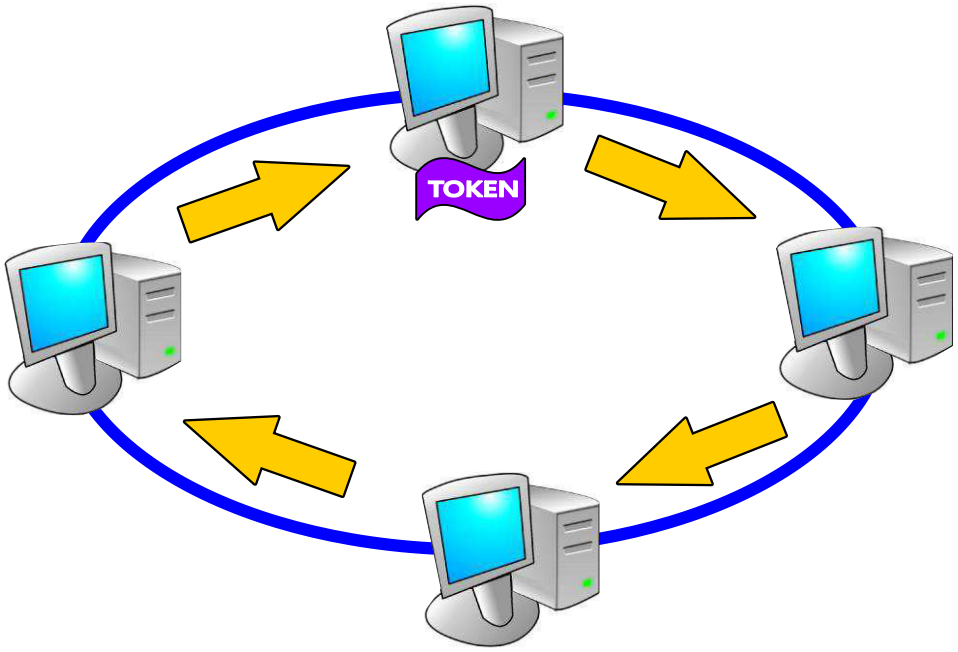


Figura 3b. Topologia em anel com o uso do Token.

Na topologia em anel (também chamada de Token-Ring), os dados são transmitidos de computador em computador através de um único meio de transmissão e de forma unidirecional. Ocasionalmente, podem acontecer colisões quando mais de um computador envia dados em um mesmo momento. Para resolver este problema, são usados os **Tokens**. O Token é como se fosse um passaporte para a transmissão: apenas quem o possuipode enviar dados. Desta forma cada computador tem sua vez de transmitir e precisa aguardar o Token chegar novamente para continuar transmitindo. Quando alguma mensagem é transmitida, ela passa por todos os computadores do anel até encontrar o computador de destino.Quando isso acontece o computador que enviou a mensagem passa a vez, ou o Token, para o seu computador vizinho para que ele possa transmitir. Mesmo que o computador não tenha nada a transmitir, ele vai receber o Token e passar

determinado período de tempo com ele para em seguida passá-lo ao próximo computador e assim por diante.

A topologia em anel é uma das mais seguras, mas em contrapartida, possui algumas desvantagens:

- caso um dos computadores apresente problemas com a transmissão, toda a transmissão da rede será comprometida.
- Devido o uso do Token, se a rede possuir muitos hosts, estase tornará lenta, já que quanto mais computadores houver na rede, mais o Token vai demorar a chegar a cada host.

3.1.3. Estrela

Na topologia em estrela é utilizado um ponto central ou ponto concentrador que normalmente é um hub, switch ou roteador. Neste caso o ponto central é responsável por retransmitir os dados vindos do computador de origem para o computador de destino.

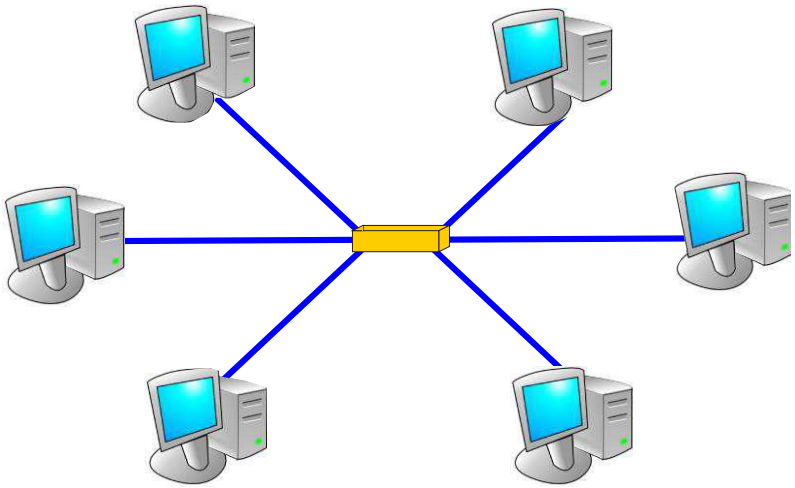


Figura 3c. Topologia em estrela.

Em analogia com a topologia em anel, se algum computador da rede apresentar problemas com a transmissão, somente ele é desativado da rede e o restante dos computadores continua enviando e recebendo dados normalmente. Da mesma forma, quando é necessário adicionar um host, basta

fazer a conexão, caso haja espaço no concentrador. Este processo não interferirá no andamento da rede e nenhum equipamento precisará ser desligado. A topologia em estrela, usando um switch, ou equipamento superior, permite mais de uma transmissão ao mesmo tempo caso as transmissões envolvam **enlaces** diferentes.

ENLACE

É um link de comunicação, ou uma ligação entre dois sistemas de rede. Por exemplo, a ligação entre um computador e um roteador ou a ligação entre dois roteadores em redes locais diferentes.

3.1.4. Árvore

A topologia em árvore caracteriza-se por possuir um ponto central onde são conectadas várias ramificações. Nesta topologia existem mais de um concentrador, criando sub-redes, normalmente em forma de estrela.

Existem níveis hierárquicos em relação aos concentradores, dado que, em uma transmissão de sinal de internet, por exemplo, acontecendo um problema com um concentrador em um nível mais acima na rede, os concentradores abaixo serão afetados, a não ser que existam estruturas de redundância. Em contrapartida, um problema em um concentrador de nível mais baixo, não afetará a rede por completo, podendo parte dela continuar funcionando normalmente.

Provavelmente em sua escola esta topologia seja usada para interligar um ponto central a setores como secretaria, coordenação, laboratórios e etc.

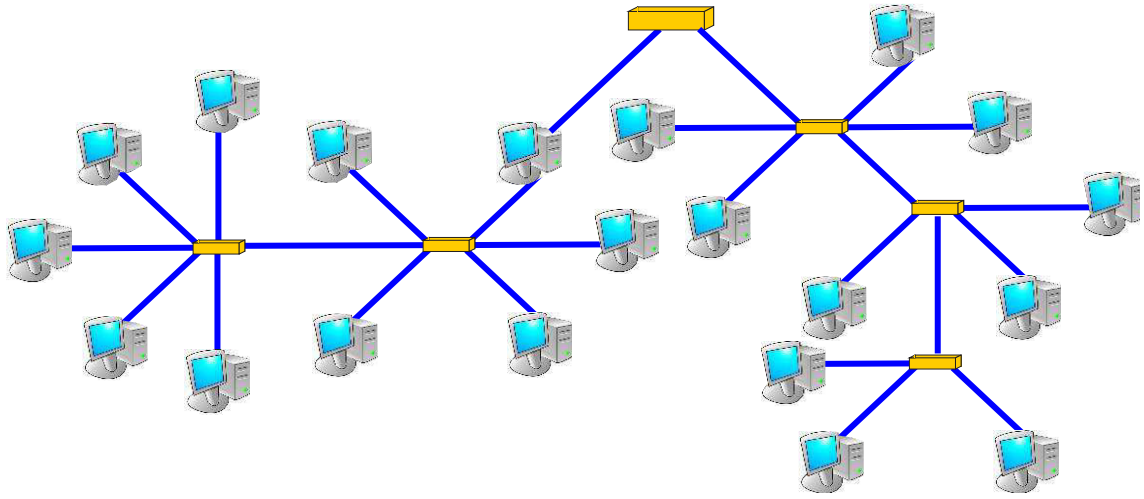


Figura 3d. Topologia em árvore.

3.1.5. Híbrida

A topologia híbrida é a junção de duas ou mais topologias diferentes. Ela é muito utilizada em empresas em constante crescimento onde a rede pode variar em função do local de trabalho, da quantidade de computadores, dos custos que certa topologia poderia gerar ou do número flutuante de computadores que podem aumentar ou diminuir com a necessidade. Nestes casos vale a pena avaliar as vantagens das outras topologias e utilizar os equipamentos disponíveis naquele momento da empresa.

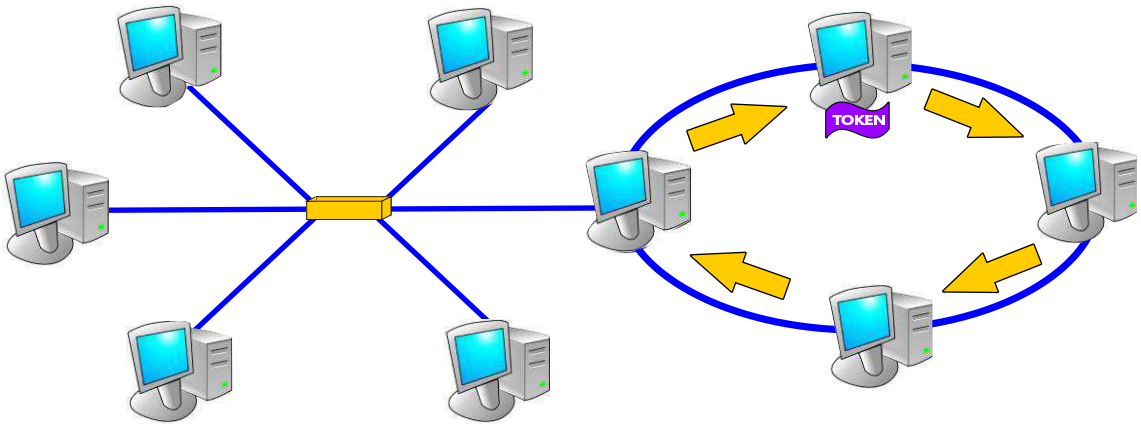


Figura 3e. Topologia híbrida.

3.1.6. Ligação Total – Malha

A topologia em Malha, também conhecida como Mesh, tem como característica a formação de uma malha de ligações entre os hosts da rede. Em uma topologia em Malha é possível sair de cada nó da rede, uma ou mais ligações para os outros nós. A quantidade de ligações que saem de um host pode variar de acordo com a rede. É uma topologia mais incomum em relação às outras, porém é a mais segura.

Existem dois tipos de topologias em malha: a Parcial e Total. Na Parcial um ponto da rede possui ligações com vários nós, mas não necessariamente com todos. Na Total, ou Full-Mesh, cada nó da rede possui, obrigatoriamente, uma ligação para cada outro nó da rede, fazendo assim com que, se um rede possui **n** nós, de cada nó sairá **n-1** ligações. Este último tipo oferece velocidade e disponibilidade maiores, porém é muito cara.

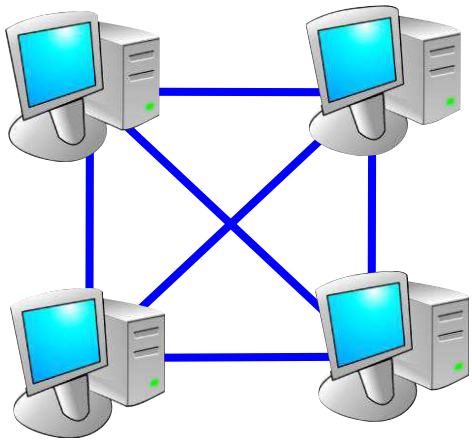


Figura 3f. Topologia em malha.

3.8. Sem fio

A topologia sem fio baseia-se em comunicações através de ondas de radiofrequência. Nela, não é necessário o uso de fios para fazer uma ligação entre dois ou mais nós da rede, fato este que tornou este tipo de rede conhecida como rede wireless, ou seja, sem fios.

Na topologia sem fio, podemos ter a presença de um ponto de acesso, ou access point, que fará a recepção dos sinais enviados pelos hosts e o envio ao receptor de destino. O ponto de acesso faz na rede sem fio, basicamente, a função que um switch faz na rede cabeada.

Podemos ter uma topologia de rede sem fio que não utiliza ponto de acesso: a rede **ad-hoc**. Nas redes ad-hoc, os hosts transmitem dados entre si, utilizando-se de suas próprias placas de rede sem fio. Obviamente, os equipamentos devem estar próximos um do outro, pois a propagação do sinal entre suas antenas é curta. Não é um tipo de rede muito utilizada, pois a transmissão é feita em half-duplex e torna-se muito lenta a medida em que adicionamos equipamentos na rede.

Um exemplo muito comum de rede ad-hoc é a transmissão de arquivos entre aparelhos celulares via Bluetooth.

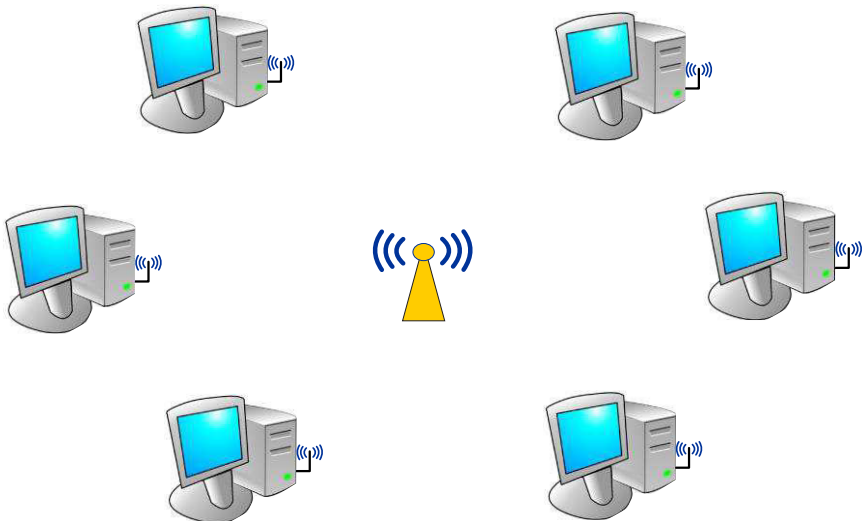
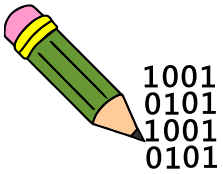


Figura 3g. Topologia de rede sem fio, com o uso de um ponto de acesso.

PESQUISA

- **Que topologia de rede é utilizada no laboratório de informática de sua escola?**
- **Você considera esta topologia adequada ao local pesquisado?**
- **Caso não considere, informe qual topologia você utilizaria e por quê.**



Exercícios

1. Em sua opinião, qual a importância de se organizar o layout físico de uma rede?

_____
_____
_____
_____

2. Defina e explique os termos abaixo:
   a) Topologia física

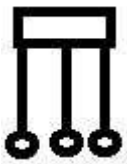
_____
_____
_____

   b) Topologia lógica

_____
_____
_____

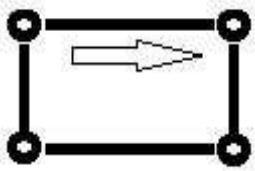
3. Indique a topologia usada nos esquemas abaixo:

a)



_____

b)

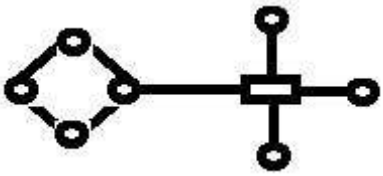


_____

c)

_____

d)



_____

ANOTAÇÕES

4. ESCOPOS DE UMA REDE

4.1. LAN

LAN significa *Local Area Network* ou Rede Local, ou seja, uma LAN é uma estrutura de rede utilizada em um mesmo complexo predial ou em uma área limitada a, no máximo, 10 km de cobertura. São normalmente montadas em casas, escritórios, empresas, escolas e condomínios.

Uma rede local pode ser do tipo ponto-a-ponto ou cliente-servidor, onde no segundo caso, temos um ou mais servidores que conectam computadores, também chamados estações ou hosts, e outros dispositivos periféricos que possam ser conectados como impressoras, por exemplo. Os servidores, como o próprio nome diz, servem. Eles são prestadores de serviço para os hosts, disponibilizando e-mail, banco de dados, arquivos, internet, impressão entre outros serviços. São computadores com alta capacidade de processamento e armazenamento.

Os servidores funcionam com um sistema operacional próprio para gerenciar essas aplicações. Existem vários sistemas para servidores no mercado como o Samba, baseado em Unix e o Windows 2008 Server da Microsoft.

As redes locais podem utilizar tanto meios de comunicação físicos, utilizando o padrão Ethernet (que veremos com mais detalhes posteriormente), quanto sem fio, utilizando ondas de rádio. Podem utilizar, inclusive, os dois simultaneamente.

4.2. MAN

MAN significa *Metropolitan Area Network* ou Rede Metropolitana e são redes que abrangem uma área muito maior que uma LAN podendo interligar bairros e até cidades. As TVs a cabo utilizam MANs para enviar seus sinais.

Grandes empresas lançam mão deste recurso para interligar suas filiais, por exemplo. É uma forma segura de compartilhar arquivos e dados de interesse comum, mas requer um custo elevado, pois necessitam de transmissores e canais de satélite exclusivos.

4.3. WAN

WAN significa Wide Area Network, ou seja, é uma rede que abrange uma grande área geográfica. A internet é o maior exemplo de WAN, pois computadores do mundo todo estão conectados por meio da internet e podem comunicar-se, trocar arquivos, efetuar chamadas telefônicas, entre outras aplicações, caso disponham de softwares específicos.

Um exemplo atual de conexão para WANs é o Wi-Max, uma tecnologia de banda larga sem o uso de fios com grande alcance e velocidade.

1. Quais são os três escopos de rede?

_____

_____

_____

2. Que escopo de rede seria ideal para identificar uma ligação do tipo:
   a) Dois computadores em uma residência.

_____

b) Sedes de bancos em vários países.

_____

c) Vários prédios de uma fábrica em um mesmo complexo industrial.

_____

d) Uma loja e seu depósito localizados em bairros diferentes.

_____

ANOTAÇÕES

5. MODELOS OSI E TCP

Bem, já vimos que com as redes de computadores eu posso comunicar uma empresa, uma pessoa, ou um equipamento a inúmeros lugares do mundo. Todas as pessoas que acessam a internet, por exemplo, fazem parte de uma mesma rede (muito grande por sinal). A internet é uma rede de redes, onde o mapa dessa rede é tão complexo, que nós começamos a chamá-la de **nuvem**.

Entretanto, se você parar para pensar, a diversidade de marcas e de fabricantes de equipamentos de rede espalhados pelo mundo é descomunal.

Como fazer para que todos esses equipamentos consigam se comunicar sem problemas de incompatibilidade?

No início da internet não havia solução para este problema. As redes funcionavam isoladas e cada uma trabalhava com seus tipos de equipamentos do fabricante de sua preferência.

Para solucionar este problema, a ISO (International Organization for Standartization) criou um modelo de referência mundialmente conhecido como **Modelo OSI** (Open Systems Interconnect). Esse modelo trouxe uma **padronização** para o fluxo de informações nas redes, fazendo com que os fabricantes lançassem placas de rede, comutadores, roteadores, cabos e conectores de acordo com as normas, assim, todos poderiam se comunicar, pois estariam usando os mesmos protocolos. Trocando em miúdos, é como se todos passassem a falar o mesmo idioma.

Veja, a seguir, como é o modelo de Referência OSI:

Figura 5a. Modelo de Camadas OSI

Como se pode notar, o modelo OSI é dividido em sete partes, as quais chamamos de **camadas**, onde:

- Cada camada tem a sua função.
- Cada camada necessita dos serviços prestados pelas suas camadas vizinhas.
- Uma camada não sabe como a camada vizinha faz seu trabalho, ela apenas recebe o produto já pronto para ser usado e faz seu trabalho em cima dele, passando-o para a próxima camada. A esta característica damos o nome de **encapsulamento.**

Vamos entender melhor.

Tomaremos dois exemplos: um você indo para outra cidade de ônibus e o outro, você entrando em um site da Web.

No primeiro exemplo você se dirige ao guichê da empresa e compra sua passagem. Nela há a cidade de destino. Depois você pega sua bagagem e se dirige a plataforma. Lá irão verificar sua passagem e indicarão o ônibus correto. Você guarda sua bagagem no porta-malas do ônibus e recebe um ticket com um código. Depois disso você embarca e o ônibus faz a viagem. Ao chegar à cidade de destino, você desce do ônibus, entrega o ticket ao motorista, pega sua bagagem de volta, sai da plataforma, volta à área dos guichês da rodoviária e vai embora.

Se desenharmos seu percurso ele será assim:

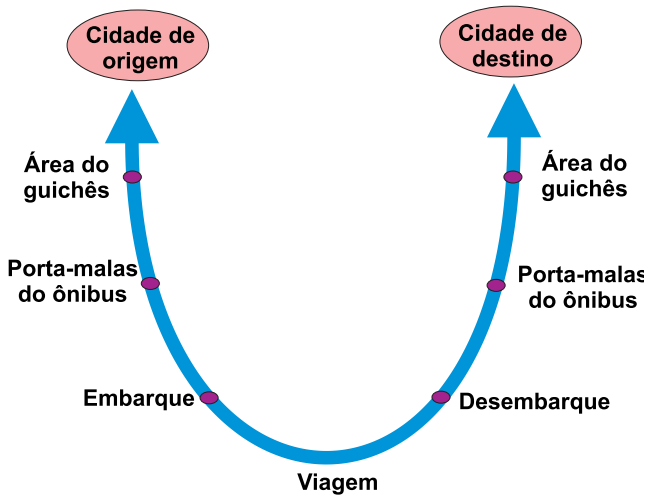


Figura 5b. Analogia com viagem de ônibus

Note que você começa na área dos guichês de uma rodoviária e termina também na área dos guichês de outra rodoviária. Você também se dirige ao porta-malas tanto na saída quanto na chegada. Portanto, o fluxo que é feito no embarque também é feito no desembarque, porém de forma inversa.

Ao voltar à sua cidade de origem, esse fluxo será refeito, invertendo apenas a cidade de origem e a cidade de destino.

Já no segundo exemplo, quando quer acessar um site da Web, você abre o browser do seu navegador de internet e digita um endereço, o qual chamamos de URL. Neste momento você está dando um comando à camada de aplicação. Esta solicitação irá ser "empacotada" e enviada para a próxima camada do seu lado da rede, de cima para baixo, que irá fazer seu trabalho em cima do pacote, colocar outro pacote por cima e passar para a próxima, até chegar à camada física, onde viajará até a camada física do servidor Web em que o site em que você quer navegar está hospedado. Ao chegar à camada física do servidor, o pacote subirá pelas camadas, onde cada uma delas tira uma das embalagens até chegar à camada de aplicação do servidor Web, que abrirá o último pacote e descobrirá a URL que você solicitou. O servidor irá pegar os arquivos do site que você pediu, colocar em um novo pacote e enviar pelo caminho de volta até chegar ao seu browser, conforme você havia solicitado. Tudo isso em questão de segundos ou milissegundos.

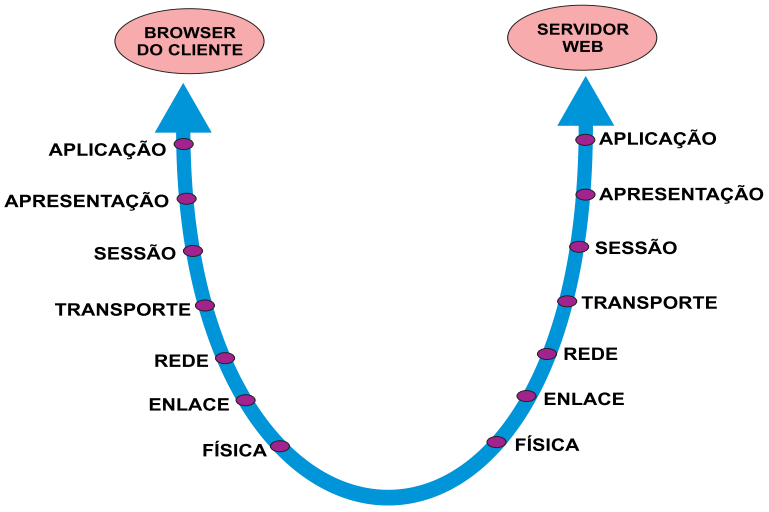


Figura 5c. Fluxo de dados no Modelo OSI

O modelo OSI não é o único modelo de referência. Existe outro modelo chamado de Modelo **TCP/IP** (Transmission Control Protocol/Internet Protocol).

O modelo TCP/IP surgiu junto com a ARPANET, que era a uma rede patrocinada pelo Departamento de Defesa dos EUA, que tinha a intenção de manter comunicantes os órgãos do governo e universidades para enviar avisos sobre catástrofes que pudessem afetar o país. Não por menos, o governo precisava de uma rede robusta, segura e que fosse tolerante a falhas, fazendo surgir então o modelo TCP/IP.

O modelo TCP/IP possui menos camadas que o modelo OSI, pois algumas camadas foram geminadas em uma só, veja:

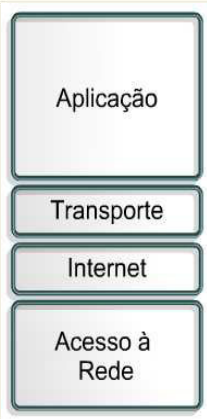


Figura 5d. Modelo de Camadas TCP/IP

A camada de Aplicação do TCP/IP inclui as de Aplicação, Apresentação e Sessão do modelo OSI. A de Transporte é a mesma, a de Internet equivale à de Rede e a de Acesso á Rede juntou as de Enlace e Física.

Veremos no decorrer deste manual, especificidades de cada camada dos Modelos OSI e TCP/IP.

Mas não confunda! Modelos de camadas não alteram o funcionamento de uma rede. Eles são apenas referências e padrões a serem seguidos pelos fabricantes ao lançar um novo equipamento no mercado.

5.1. CAMADA DE APLICAÇÃO (Modelos OSI e TCP/IP)

5.1.1. Serviços e Funções

A camada de aplicação é a camada mais acima dos modelos OSI e TCP/IP. Ela é a camada que está mais próxima ao usuário. É nela que acontecem as solicitações dos aplicativos que o usuário manipula, como por exemplo, um browser para acesso a um site da Web, um gerenciador de e-

mails e um gerente de compartilhamento de arquivos. A camada de aplicação engloba também aplicações que não são apresentadas claramente ao usuário, como os serviços de DNS, que veremos mais adiante.

A camada de aplicação é muito importante porque não existiria lógica na criação de uma rede, sem aplicações que possam servir ao usuário de alguma forma.

As aplicações podem ter dois tipos de arquiteturas: a ponto-a-ponto (ou P2P - *peer-to-peer*) ou a cliente-servidor. Quando um desenvolvedor deseja criar um aplicativo para ser usado em uma rede, ele antes tem que definir qual dessas arquiteturas ele vai usar. Em arquiteturas P2P não é necessário que os sistemas finais estejam sempre ligados, já na arquitetura cliente-servidor, existirá um host servidor sempre disponível na rede para prover os serviços aos quais ele foi destinado.

Em uma aplicação P2P os hosts comunicam-se entre si, trocando informações. Exemplos de aplicações P2P são os compartilhadores de arquivos. Neles, um host pode fazer download de arquivos de outros hosts, mas também pode fazer upload, ou seja, disponibilizar seus arquivos para que outro host da rede faça download deles.

Em aplicações cliente-servidor, os clientes não comunicam-se entre si, em vez disso, cada cliente manda sua requisição ao servidor e este se comunica com o cliente destinatário. Ao passo em que o servidor não está disponível, por motivos quaisquer, a aplicação não pode ser finalizada.

5.1.2. Protocolo HTTP

Uma das aplicações mais comuns na rede é o acesso a páginas da Web. Através de um aplicativo chamado browser, podemos solicitar um endereço da Web e receber uma página cheia de conteúdo dos mais diversos tipos e assuntos. Essa uma típica aplicação cliente-servidor, onde o host que solicita a página é o cliente e o host que armazena a página em seu disco é o servidor.

O protocolo que é usado para este fim é o **HTTP – HyperText Transfer Protocol** ou Protocolo de Transferência de Hipertexto. Este protocolo está presente tanto na máquina do cliente quanto na do servidor, mas atua de forma diferente em cada uma delas.

Uma página da Web é um arquivo, normalmente do tipo HTML, que é constituído por um conjunto de outros arquivos que podem ser texto, imagem, música ou vídeo. Ao hospedar uma página na internet é criado para este arquivo HTML um endereço URL, como por exemplo: *http://www.cursoderedes.com.br/home.index,* note que o protocolo http usado para o tráfego desta página na rede precede o endereço. Caso essa página possua um texto e duas imagens, a referência a estes 3 objetos estará no arquivo com caminho *home.index*.

Quando o usuário insere este endereço no browser, o processo cliente HTTP faz uma comunicação com o host responsável pelo endereço *cursoderedes.com.br* através da porta de conexão 80. Concluída a comunicação, ele envia uma solicitação pedindo o arquivo que está no caminho *home.index* (que normalmente é a homepage do site). O servidor recebe a solicitação e extrai o arquivo home.index do disco, encapsulando-o e enviando de volta ao cliente. Após o cliente receber o arquivo, o processo HTTP cliente envia uma resposta indicando o recebimento. A comunicação é encerrada e o cliente extrai o arquivo do pacote.

Como vimos, esta página possui três objetos: um texto e duas imagens. Ao receber o arquivo *home.index*, ele apenas fará referência aos três objetos e o cliente automaticamente reiniciará o processo para receber do servidor cada um dos objetos separadamente.

É claro que cada solicitação e resposta dessa requer um tempo e é por isso que uma página que possui muitos objetos (fotos, vídeos, texto, etc) demora mais a carregar totalmente.

5.1.3. Protocolo FTP

Uma das funções mais primitivas de uma rede de computadores é a transferência de arquivos entre os hosts. O protocolo responsável por este serviço é o **FTP – File Transfer Protocolo** ou Protocolo de Transferência de Arquivos.

Baseado na arquitetura cliente-servidor, o cliente acessa o FTP para fazer login no servidor FTP com usuário e senha e assim autenticar o seu acesso. Quando um cliente deseja compartilhar seus arquivos ele se conecta ao servidor FTP e um cópia desses arquivos é feita no servidor. Se outro

cliente necessita ter acesso a esses arquivos, ele efetua login e visualiza remotamente os arquivos compartilhados. Caso queira, ele pode efetuar uma cópia para seu disco local.

Ao enviar ou receber arquivos do servidor FTP, são usadas duas portas de conexão: a porta 21 para **conexão de controle** e a porta 20 para **conexão de dados**. Na conexão de controle é feita a identificação dos usuários com senha e são enviados comandos para adicionar ou capturar um arquivo. Na conexão de dados é que acontece a transferência dos dados realmente, ou seja, é o caminho por onde os dados transitam.

5.1.4. Protocolos SMTP e POP3

Outra aplicação bastante popular na internet é o correio eletrônico, o famoso e-mail. Com o e-mail é possível enviar mensagens a um endereço eletrônico de uma pessoa, onde esta, autenticada com usuário e senha, abre a caixa de mensagens onde lhe for mais apropriado e as lê, quando lhe for conveniente. O protocolo usado para envio de e-mails é o **SMTP – Simple Mail Transfer Protocol** ou Protocolo de Transferência de Correio Simples.

O e-mail é um tipo de aplicação que parece ser P2P, já que enviamos mensagens diretamente para o destinatário, mas na verdade é uma aplicação cliente-servidor. Quando queremos enviar uma mensagem, ou visualizar nossa caixa de e-mails precisamos nos conectar a um servidor de e-mails e fazemos isso nos autenticando com usuário e senha. Todas as nossas mensagens ficam armazenadas neste servidor. Quando vamos enviar uma mensagem, nem sempre o servidor de e-mail da outra pessoa é o mesmo que nós usamos, portanto o caminho da mensagem é feito da seguinte forma:

- Nos conectamos ao nosso servidor com usuário e senha.
- Uma aplicação chamada de **leitor de correio** (por exemplo o Outlook Express da Microsoft) permite que tenhamos acesso a nossas mensagens.
- Esta mesma aplicação nos fornece um simples editor de texto para que possamos escrever a mensagem que queremos enviar.
- No cabeçalho da mensagem inserimos o endereço de e-mail do destinatário, em que consta o servidor de e-mail daquela pessoa.

- Ao dar o comando para enviar, o leitor de correio envia a mensagem para o seu servidor de e-mail.
- Ao receber a mensagem, nosso servidor de e-mail inicia um processo cliente SMTP que efetua uma conexão com o servidor SMTP do destinatário e envia a mensagem.
- O processo servidor SMTP entrega a mensagem ao servidor de e-mail do destinatário.
- O servidor de e-mail do destinatário coloca a mensagem na caixa de mensagens.
- Quando o destinatário julgar necessário, ele abrirá seu leitor de correio e visualizará a mensagem que foi enviada.

O SMTP tem como característica ser um protocolo de **envio de informações**. Ele atua no envio da mensagem do host cliente ao servidor de e-mail e de um servidor de e-mail a outro servidor de e-mail. Entretanto, o momento em que o destinatário abre a caixa de mensagens para visualizá-las é caracterizado como uma **recuperação de informações**, ação que o SMTP não abrange.

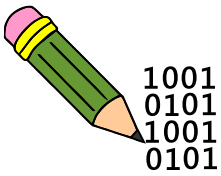
Para recuperar informações é necessário outro protocolo. Um dos mais usados é o **POP3 – Post Office Protocol versão 3**. É um protocolo muito simples e divide seu funcionamento em três etapas: autorização, transação e atualização.

- **Autorização:** é o momento em que o leitor de correio autentica o usuário com senha.
- **Transação:** é o momento em que o protocolo recupera as mensagens do servidor de e-mail e as torna visível no leitor de correio. Nesta fase, o usuário pode marcar mensagens e das o comando para apagá-las.
- **Atualização:** é o momento em que o usuário encerra a sessão. Nesta fase, o protocolo realmente apaga do servidor de e-mail as mensagens que foram excluídas.

Bem, se a conta do seu e-mail é Hotmail, por exemplo, você não utiliza os protocolos SMTP e POP3. O correio eletrônico de empresas como o Hotmail é via Web, portanto o protocolo utilizado para enviar mensagens do host do

destinatário ao servidor de e-mail é o HTTP. Porém, o envio de mensagens entre servidores de e-mail é feito pelo SMTP.

A grande vantagem de se usar um correio eletrônico na Web é a possibilidade de acessar sua caixa de mensagens de qualquer local e em qualquer dispositivo que tenha acesso à internet. Com a popularização dos correios eletrônicos da Web há alguns anos, cada vez menos as pessoas têm utilizado os leitores de correio, que por sua vez só podem ser acessados em computadores previamente configurados com a conta de e-mail.



Exercícios

1. Que solução surgiu para resolver os problemas de incompatibilidade entre os equipamentos de rede de diferentes fabricantes?

_____

_____

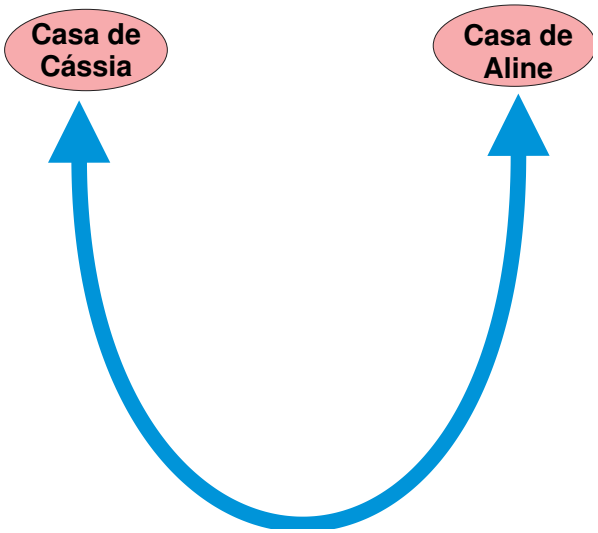
_____

2. Complete o modelo OSI com as camadas que faltam:

APLICAÇÃO
TRANSPORTE
ENLACE

3. Com a ajuda da explicação de seu professor, explique com suas palavras do que se trata um encapsulamento.

4. Faça uma analogia parecida com a feita na Figura 5b, colocando o percurso de uma correspondência enviada por Cássia que mora no Ceará para Aline que mora em Bruxelas, na Bélgica.



5. Diferencie aplicação P2P e cliente-servidor.

_____

_____

_____

_____

6. Relacione o protocolo ou serviço com a sua função principal:

(1) HTTP

(2) FTP

(3) SMTP

(4) POP3

(5) DNS

( ) Protocolo que atua na transferência de arquivos entre hosts.

( ) Serviço que resolve nomes em IPs e IPs em nomes.

( ) Protocolo que atua no envio de mensagens de e-mail.

( ) Protocolo que atua na recuperação de mensagens de servidores de e-mail.

( ) Protocolo que atua no acesso a páginas da Web.

7. Baseado no funcionamento do protocolo HTTP, tente explicar por que a página do Google carrega mais rápido que a página do Facebook.

_____

_____

_____

_____

_____

8. Qual número de porta de conexão é usado pelo HTTP?

_____

9. Por que o FTP utiliza duas portas de conexão?

_____

_____

_____

10. Para que servem os protocolos SMTP e POP3 respectivamente?

_____

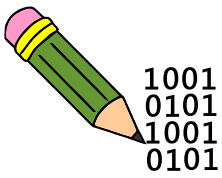
_____

_____

_____

_____

_____



SUGESTÃO DE ATIVIDADE PRÁTICA:
O programa Wireshark é um aplicativo livre e permite que você veja as linhas de cabeçalho de uma requisição HTTP, entre outros pacotes.

5.1.5. Serviços de DNS

Em uma rede, todos os hosts possuem uma identificação. Assim como nós, seres humanos, possuímos um nome e um CPF, os hosts também possuem um nome e um Endereço IP. O endereço IP é um código, que será visto com mais detalhes posteriormente, que identifica cada host em uma rede.

Os equipamentos e protocolos reconhecem um host pelo IP. Entretanto, para as pessoas, torna-se mais complicado decorar números, nem sempre com muito sentido. Imagine que se para cada página da Web que fosse acessar você precisasse digitar na barra de endereços do navegador um código com 12 números! Seria complicado, não?!

Para solucionar este problemas, a camada de aplicação está ligada a mais um serviço: o **DNS – Domain Name System** ou Sistema de Nomes de Domínio. O DNS não é uma aplicação claramente visível para o usuário, mas ele entra em ação sempre que você envia um e-mail, copia um arquivo de um computador da rede, imprime em uma impressora de rede ou acessa uma página da Web.

O DNS é um serviço de tradução (ou resolução) de **nomes** em **IPs** e **IPs** em **nomes**. Ele possui um software para fazer essa tradução chamado de *name resolver*.

Vamos ao exemplo:

- Quando o usuário digita uma URL no browser é iniciado na própria máquina o serviço de DNS.
- O cliente DNS faz uma consulta ao servidor DNS mais próximo.
- O servidor DNS responde à solicitação do cliente com o endereço IP correspondente àquela URL.
- O cliente DNS entrega o endereço IP ao browser que, enfim, permitirá ao protocolo HTTP fazer seu trabalho e disponibilizar a página.

Mas como o servidor DNS consegue encontrar o endereço IP correspondente à URL digitada?

Primeiro você tem que saber que existem alguns servidores DNS específicos:

Servidores DNS raiz: é um conjunto de 13 servidores espalhados em alguns países (não existe nenhum no Brasil) que gerenciam todos os ooutros

servidores DNS. Hierarquicamente estes 13 servidores DNS estão no topo. Eles possuem o mapa dos servidores DNS de Alto Nível (TLD).

Servidores DNS de Alto Nível: são servidores que são responsáveis por domínios de alto nível como: com, edu, org, gov, entre outros. São responsáveis também por domínios de países como: fr, br, PT, entre outros.

Servidores DNS de autoridade: são responsáveis por armazenar os domínios presentes na Web, sejam eles de empresas, escolas, instituições, órgãos e até mesmo pessoais. Todo aquele que quer disponibilizar uma página da Web, deve ter esta ligada a um domínio registrado em um servidor de autoridade, que pode ser próprio ou não.

O DNS recebe a URL e a esmiúça em pequenas partes. O endereço *www.cursoderedes.com.br* é dividido em:

www
cursoderedes
com
br

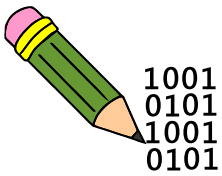
- O código *www*, que significa World Wide Web, indica que o endereço refere-se a uma página da Web.
- O cliente DNS faz uma consulta com o endereço completo ao **servidor DNS local** mais próximo a ele.
- O servidor DNS local faz uma consulta ao **servidor DNS raiz** para descobrir qual servidor TDL é responsável pelo domínio **br**.
- O servidor DNS local faz uma consulta ao **Servidor DNS de Alto Nível (TLD)** responsável pelo domínio **.br** para descobrir o servidor TDL responsável pelo domínio **.com.br**.
- O servidor DNS local faz uma consulta ao **Servidor DNS de Alto Nível (TLD)** responsável pelo domínio **.com.br** para descobrir o servidor de autoridade responsável pelo domínio **cursoderedes.com.br**.
- O servidor DNS local faz uma consulta ao **Servidor de Autoridade** responsável pelo domínio **cursoderedes.com.br** para descobrir qual endereço IP corresponde a esse domínio.

- O servidor DNS local responde ao **cliente DNS** fornecendo o endereço IP solicitado.

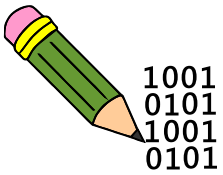
Ufa!!! O servidor DNS trabalha muito! Mas se minutos depois, o usuário solicitar a mesma página novamente, o DNS vai fazer todo esse percurso de novo?!

Não! Para evitar este retrabalho, é implementado um **cache** nos servidores locais, ou seja, uma pasta onde ele armazena as consultas já feitas. Assim, quando o usuário anterior, ou até mesmo outro usuário da rede, solicitar a mesma página, o servidor DNS consultará, antes de mais nada, o seu próprio cachê. Se o registro já existir, o servidor devolve a resposta rapidamente ao cliente. Isso ajuda a deixar o acesso mais rápido.

Como o endereço IP de um host pode mudar a qualquer momento, esse registro é descartado cerca de dois dias depois.



SUGESTÃO DE ATIVIDADE PRÁTICA:
Professor, oriente seus alunos no laboratório para usarem os comandos ping e nslookup.



Exercícios

1. Defina:

a) Servidor DNS raiz.

_____

_____

_____

b) Servidor DNS de alto nível.

_____

_____

_____

c) Servidor DNS de autoridade.

_____

_____

_____

2. Qual a importância do cachê para a velocidade da consulta DNS?

_____

_____

_____

PESQUISA

Pesquise em livros ou na internet o nome de outros protocolos da camada de aplicação e explique a função deles.

ANOTAÇÕES

5.2. CAMADAS DE APRESENTAÇÃO E SESSÃO (Apenas Modelo OSI)

Como você pôde observar, existem algumas diferenças entre os modelos OSI e TCP/IP. Uma delas é que no modelo OSI existem duas camadas entre a camada de aplicação e a de transporte: a camada de Apresentação e a camada de Sessão. No modelo TCP/IP estas camadas são embutidas na camada de Aplicação. Mas afinal, de que se tratam essas duas camadas?

5.2.1. Camada de Apresentação – Serviços e Funções

Como o nome já sugere. A camada de Apresentação é responsável por apresentar os dados que vem das outras camadas à camada de Aplicação e vice-versa. Podemos dizer também que ela prepara os dados para que sejam lidos pelas outras camadas de forma que sejam entendidos, pois cada camada trata os dados de uma forma bastante específica. Esta camada faz três funções básicas: **tradução, compressão e criptografia.**

Ao receber os dados de aplicações de um remetente, como palavras escritas em códigos ASCII em uma mensagem de correio eletrônico, por exemplo, a camada de apresentação **traduz**, ou converte para o padrão usado pelo dispositivo transmissor. Da mesma forma, ao chegar à camada de Apresentação do destinatário, esta vai converter os dados para o padrão a ser usado pela camada de aplicação.

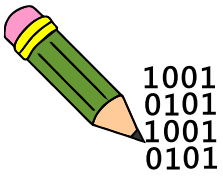
Continuando com o exemplo, ao enviar estes dados, a camada de aplicação entrega-os à de apresentação sem preocupar-se com a forma que estes dados irão trafegar na rede. Para otimizar a transmissão, a camada de apresentação **comprime** os dados, deixando-os menores. Do outro lado da transmissão, a camada de apresentação do destinatário recebe estes dados comprimidos, faz sua **descompressão** e entrega-os perfeitamente à camada de aplicação, que nem toma conhecimento de todo este trabalho.

Algumas aplicações exigem uma transmissão mais segura no sentido de evitar que, uma vez que os dados enviados sejam interceptados por alguém não autorizado, estes não possam ser lidos ou entendidos. Para isso podem ser usadas técnicas de criptografia. A aplicação envia os dados totalmente abertos à camada de apresentação e esta, por sua vez, tem a função de

criptografá-los com alguma técnica escolhida pelo aplicativo. A partir desta camada, os dados trafegam encriptados até chegar à camada de apresentação do destinatário, onde serão **descriptografados** e entregues à camada de aplicação da mesma forma que saíram da aplicação do remetente.

5.2.2. Camada de Sessão – Serviços e Funções

A camada de sessão é responsável **abrir** o canal de comunicação entre dois hosts comunicantes e **encerrá-lo**. Além disso, ela **mantém** aberta a conexão entre os hosts até que estes concluam a transmissão. Mesmo que haja algum problema na rede que impeça a comunicação, a camada de sessão consegue reestabelecer a transmissão de forma rápida e do ponto onde foi interrompida, graças à sua técnica de marcação, pois ela vai incluindo marcações nos dados que estão sendo enviados. Sabe aqueles jogos de videogame, onde você faz marcações e caso haja algum problema, é possível voltar o jogo para o último ponto em que foi marcado? A camada de sessão faz mais ou menos isso com a rede!



Exercícios

1. Qual a função da camada de Apresentação e quais serviços ela oferece?

_____

_____

_____

_____

2. Como se dá a técnica usada pela camada de Sessão para conseguir reestabelecer uma transmissão interrompida?

_____

_____

_____

_____

5.3. CAMADA DE TRANSPORTE (Modelos OSI e TCP/IP)

Pelo que estudamos até agora, vimos que em uma transmissão em uma rede, a camada de aplicação “produz” os dados, a de apresentação “prepara” esses dados para serem enviados e a de sessão abre a conexão e mantém seu estado para que os dados possam trafegar. Durante todo este processo as camadas trabalharam com **dados** Os dados são o **PDU** das três primeiras camadas.

PDU - *Protocol Data Unit*, ou seja, Protocolo de Unidade de Dados

O que é o PDU de uma camada?
Cada camada trata a informação transmitida de uma forma. O PDU de uma camada é a unidade em que são tratadas as informações naquele momento.

Na camada de Transporte, o PDU utilizado é o **segmento**. Ou seja, esta camada receberá os dados da camada de sessão e irá dividi-los em segmentos para serem enviados à camada de rede (ou acesso à rede, no modelo TCP/IP).

5.3.1. Serviços e Funções

Quando usamos uma aplicação de rede, a impressão que temos é que existe uma comunicação direta entre nosso host e o host destinatário. Entretanto existem muitos roteadores de rede fazendo a comunicação física entre os dois hosts, onde muitas vezes centenas de quilômetros os separam.

A camada de transporte faz essa função: comunicar logicamente o processo que roda no host remetente ao processo que roda no host destinatário independente de como esses dados irão chegar até lá, ou seja, independente de por quantos roteadores, enlaces e arquiteturas de rede diferentes eles terão que passar.

Em várias literaturas e até mesmo na internet você encontrará comparações entre uma rede e um serviço de correios. As três primeiras camadas do modelo OSI ou a camada de Aplicações do modelo TCP/IP equivalem ao remetente escrevendo uma carta, colocando-a e em um envelope e entregando-a ao carteiro. Quem irá efetuar o transporte da correspondência realmente é o correio, mas se o carteiro não separar as cartas corretamente e

entregá-las na agência em tempo hábil, o correio nada poderá fazer para garantir que sua carta chegue ao destino. Da mesma forma, ao chegar na agência de destino, se o carteiro não separar as cartas corretamente de acordo com o endereço ou demorar a entregar sua carta, de nada adiantou o trabalho dos correios.

Perceba com esta história duas coisas: primeiro, o bom trabalho do carteiro é extremamente importante para o sucesso do serviço dos correios. Segundo, o carteiro é o elo principal tanto entre o remetente e o correio quanto entre o correio e o destinatário.

Comparando com o nosso modelo de camadas, o carteiro é a nossa Camada de Transporte. Ela faz a ligação entre as camadas a nível de aplicação (Aplicação, Apresentação e Sessão) e as camadas de nível físico (Rede, Enlace e Física no modelo OSI ou Internet e Acesso à Rede no modelo TCP/IP).

Existem dois protocolos usados pela camada de transporte: O **TCP – *Transmission Control Protocol***, ou Protocolo de Controle de Transmissão e o **UDP – *User Datagram Protocol***, ou Protocolo de Datagrama de Usuário. Estes dois protocolos tem a função de entregar os dados dos processos do host remetente ao host destinatário. Vamos analisar estes dois protocolos com mais detalhes.

5.3.2. Protocolo TCP

O protocolo TCP – Transmission Control Protocol é um protocolo de transporte **orientado para conexão**, ou seja, antes de começarem a trocar infoormações, os hosts comunicantes estabelecem uma conexão, que podemos comparar com uma apresentação. É como se o host remetente e o host destinatário efetuassem o seguinte diálogo:

- Oi, você está me ouvindo?
- Sim, estou!
- Ok! Então vou começar a transmitir.

Somente depois de ter certeza que o host destinatário está pronto para receber as informações é que o host remetente começa a enviar os dados, sem

correr o risco de ficar “falando sozinho”. Esta característica do TCP, entre outras coisas, **garante a entrega dos dados** ao destinatário de forma íntegra e ordenada. Isso acontece porque, como os hosts estão conectados um ao outro, ao enviar um pacote ao destinatário, o remetente fica aguardando uma resposta de confirmação. Se o destinatário respondeu confirmando o recebimento do pacote, o remetente envia o próximo pacote, na ordem correta. Se o destinatário não respondeu, o remetente, após esperar um determinado tempo, reenvia o pacote, presumindo que o que ele enviou antes foi perdido por algum motivo. A essa resposta de confirmação de recebimento damos o nome de **acknowledge** ou **ACK.**

Outra implementação é o **controle de congestionamento**, onde a taxa de transmissão dos pacotes é diminuída quando existem muitos pacotes trafegando na rede. Assim o TCP evita que aconteça um travamento ou acúmulo de pacotes em caso de congestionamento.

O TCP também implementa o **controle de fluxo**, ou seja, ele não permite que um remetente envie, ao mesmo tempo, mais dados do que o destinatário pode receber. Isso acontece porque são estabelecidos tanto no host remetente quanto no destinatário um valor de **MTU – *Maximum transmission unit***, ou unidade máxima de transmissão. É o MTU quem diz a quantidade máxima de dados que podem ser enviados/recebidos em um **segmento** TCP.

E como é um segmento TCP?

Vamos analisar com detalhes o segmento TCP abaixo:

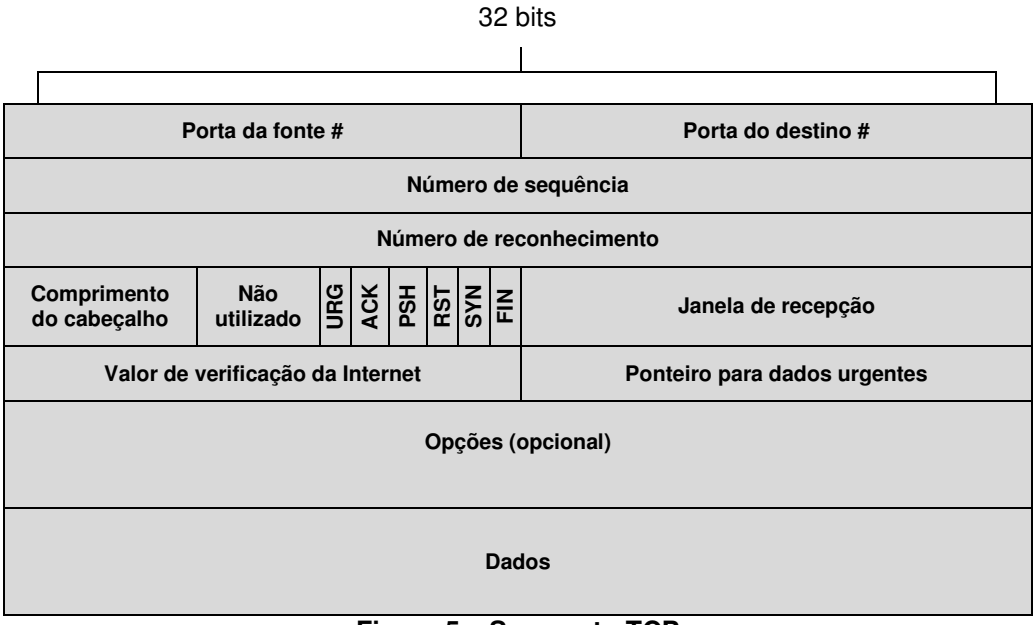


Figura 5e. Segmento TCP

- **Porta da fonte e porta do destino:** Um processo envia dados para a camada de transporte ou recebe dados da camada de transporte através de portas, por exemplo as portas 20 e 21 do protocolo FTP, ou a porta 80 do HTTP, entre outras. Ao enviar dados em um segmento TCP, devem ser informadas a porta da fonte dos dados e a porta do destino destes dados.
- **Número de sequência:** é a cadeia de 32 bits que indica a ordem de envio dos segmentos oriundos de um conjunto de dados.
- **Número de reconhecimento:** devido o TCP ser full-duplex, pode ocorrer de um host ser remetente e destinatário ao mesmo tempo, em uma mesma conexão TCP com outro host. Para que não haja confusão entre os segmentos que estão sendo enviados, são implementados números de reconhecimento que especificam o número do próximo byte que o receptor espera receber. Isso faz com que, em uma transmissão full-duplex, o host A saiba se o segmento que ele está recebendo é um segmento dos dados que o host B está transmitindo, ou se é um segmento de acknowledge (confirmação de recebimento) de um segmento enviado pelo host A.
- **Comprimento do cabeçalho:** são 4 bits que informam o comprimento do cabeçalho. Quase todos os campos do segmento TCP possuem tamanho predefinido, exceto o campo Opções, que é opcional, portanto

o comprimento do cabeçalho pode variar caso o campo Opções esteja preenchido.

- **Não utilizado:** é realmente um campo que ainda não é utilizado pelo TCP, mas fica reservado para uso no futuro.
- **Flags:** são marcações do tamanho de um bit. Onde houver bit 1 nesses campos, estes devem ser levados em consideração:

  URG - Campo de ponteiro Urgente é válido

  ACK - Campo de Reconhecimento é válido

  PSH - Este segmento solicita um PUSH

  RST - Reset da conexão

  SYN - Sincroniza números de sequências

  FIN - O transmissor chega ao fim do fluxo de bytes.

- **Dados:** é no campo Dados que pedaços do conjunto de dados que devem ser enviados são colocados. O tamanho do campo Dados varia de acordo com o MTU preestabelecido.

O protocolo TCP é muito mais complexo, mas estudos mais aprofundados não vêm ao caso neste momento. O importante é você saber que o TCP é confiável e ideal para aplicações orientadas à conexão, que precisam enviar e receber todos os dados, sem percas e em perfeita ordem. Consequentemente, devido aos procedimentos que devem ser feitos para garantir a entrega dos segmentos, a transmissão demora um pouco para acontecer, mas é o preço que se paga pela **qualidade do serviço**.

5.3.3. Protocolo UDP

Diferente do TCP, o UDP – User datagram Protocol, ou Protocolo de Datagrama de Usuário, **não é orientado para conexão**, ou seja, quando o processo do remetente precisa enviar dados, ele simplesmente envia, sem se preocupar se o processo do destinatário está ativo. Sendo assim, o protocolo UDP **não garante a entrega** dos dados enviados.

Então, qual a vantagem do UDP em relação ao TCP?!

Existem várias vantagens em se usar o protocolo UDP. A primeira delas é que como não existe nenhuma apresentação entre os hosts, ou estabelecimento de conexão, a transmissão no UDP é mais **rápida**. A segunda é que, como não existe controle de congestionamento, em **nenhum momento a taxa de transmissão é reduzida**. E por último, o cabeçalho do segmento UDP é bem menor que o cabeçalho do segmento TCP, evitando assim a sobrecarga de cabeçalho. Veja abaixo um segmento UDP:

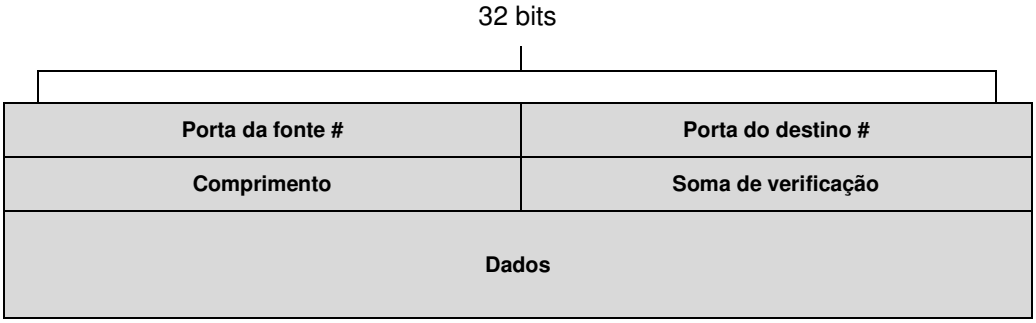
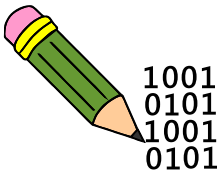


Figura 5f. Segmento UDP

A **soma de verificação** é uma forma de detectar erros dentro do segmento, que podem acontecer devido a alguma interferência no meio da transmissão. Nela é implementado um algoritmo que efetua sequências de adições sobre os bits que compõem o segmento. O resultado deste cálculo é colocado no campo Soma de verificação. Ao receber o segmento, o protocolo UDP do destinatário usa o mesmo algoritmo nos bits do segmento recebido e compara o resultado com o que está no campo Soma de verificação. Se o resultado for igual significa que o segmento chegou intacto, caso contrário o UDP destinatário descobre que há um erro nos dados do segmento.

Como podemos ver, o UDP é um protocolo muito mais leve e rápido que o TCP, por isso é amplamente usado em aplicações multimídia e em tempo real, que toleram algumas falhas e percas de pacotes, mas necessitam

primordialmente de rapidez na entrega dos mesmos, sem atrasos, que prejudicariam a essência da aplicação.



Exercícios

1. Explique o que é uma transmissão orientada para conexão.

_____

_____

_____

2. Qual a função de um acknowledge?

_____

_____

_____

3. Qual a relação entre o MTU e o serviço de controle de fluxo TCP?

_____

_____

_____

_____

_____

4. Cite uma vantagem e uma desvantagem dos protocolos TCP e UDP.

_____

_____

_____

_____

_____

PESQUISA

Pesquise qual protocolo de transporte é comumente usado nas aplicações a seguir*: Resolução de nomes – DNS, carregamento de páginas da Web – HTTP, Telefonia IP – VoIP, Transferência de arquivos – FTP e Envio de e-mails – SMTP*.

5.4. CAMADA DE REDE (Modelo OSI) ou INTERFACE COM A REDE (Modelo TCP/IP)

5.4.1. Serviços e Funções

Na camada anterior, vimos os principais protocolos de transporte de informações na rede. Esses protocolos recebem dados das camadas mais acima e os dividem em segmentos para que possam ser transportados. Cada segmento possui um cabeçalho com todas as especificidades daquele protocolo de transporte, seja TCP ou UDP, e contém também os dados que serão enviados.

Um segmento da camada de transporte é como se fosse um envelope, onde externamente temos as informações daquela camada e internamente temos as informações. Ao enviar para a próxima camada, a camada de Rede, ou Interface com a Rede, este envelope será colocado dentro de outro envelope (até porque uma camada não se importa como a outra manipulou os dados), onde externamente constarão as informações relevantes dos protocolos daquela camada.

O envelope da camada de rede é chamado de **datagrama** e será a PDU desta camada.

Mas afinal, qual é a função da Camada de Rede?

A camada de rede possui duas funções principais: a função de **repasse** e a função de **roteamento**.

Antes de esmiuçarmos cada uma das funções, vamos entender primeiro que, a partir desta camada, estaremos mais diretamente ligados a meios físicos na rede, ou seja, equipamentos. O equipamento fundamental, sem o qual a camada de rede não teria sentido é o **roteador**.

O roteador de rede é a porta de entrada ou saída de uma rede qualquer. Ele tem a função de encaminhar os datagramas da camada de rede até um host diretamente ligado a ele ou até outro roteador vizinho. Sabemos que ao

solicitarmos no browser um site da internet, esta solicitação percorrerá inúmeros roteadores até chegar ao servidor Web que hospeda aquela página. Portanto, mais do que apenas repassar os datagramas ao próximo nó da rede, um roteador tem a função de roteamento, ou seja, ele faz um mapeamento de todos os roteadores existentes do ponto onde ele está até um host de destino (como o servidor Web que hospeda o site, por exemplo) e, além disso, ele decide qual a **melhor rota** a ser percorrida até o destino, com o caminho que demore menos tempo para ser percorrido, seja ele o menor ou o menos congestionado.

5.4.1.1. Função de Repasse

Um roteador pode possuir várias portas as quais chamamos de **interfaces**. Para cumprir sua função de repasse, o roteador deve ter ciência de qual interface deverá ser usada para repassar um determinado datagrama. Essa escolha irá depender do destino daquele datagrama. Essa informação que constará no cabeçalho do datagrama será comparada com uma **tabela de repasse** que estará presente no próprio roteador. Veja e analise a imagem abaixo:

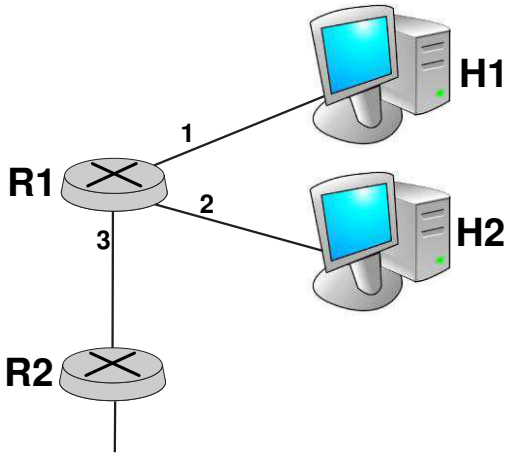


Figura 5g. Enlaces de um roteador R1

Como você pode notar, temos um roteador R1 ligado a dois hosts H1 e H2 e a um segundo roteador R2, portanto o roteador R1 possui três interfaces ativas, cada uma comunicando-se com uma interface de outro equipamento através de um enlace. O roteador R1 do exemplo acima possui a seguinte tabela de roteamento:

TABELA DE REPASSE	
VALOR DO CABEÇALHO	**INTERFACE DE SAÍDA**
1111	**1**
1010	**2**
0011	**3**

Figura 5h. Tabela de repasse do roteador R1.

Podemos concluir que, se o host H1 enviar um datagrama ao roteador R1, com o valor 0011 no cabeçalho, o roteador R1 deverá encaminhar este datagrama à interface 3, que possui um enlace de comunicação com o roteador R2. Da mesma forma, quando o roteador R2 quiser responder à solicitação do host H1, ele deverá enviar um datagrama para o roteador R1 com o valor 1111 no cabeçalho. Assim R1 verificará na tabela de repasse e encaminhará o datagrama corretamente até H1.

Perceba também que, apesar de a tabela de repasse indicar interface de saída, as interfaces de um roteador também são de entrada. Lembre-se que a transmissão neste nível é *full-duplex*.

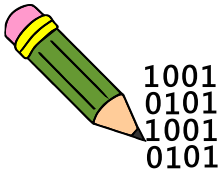
5.4.1.2. Função de roteamento

Cumprir a função de roteamento envolve todos os roteadores desde o de origem até o de destino. Como já falamos, nesta função o roteador irá traças o melhor caminho até chegar ao host destinatário. Qualquer host, em qualquer rede, que esteja ligada à internet, ao enviar uma solicitação para fora da rede local, precisa encaminhar seus datagramas ao **roteador de borda de rede** (também chamado de **roteador default**, ou **roteador de primeiro salto**) que é o roteador mais próximo; aquele que faz a comunicação da rede local com as demais redes. O host destinatário também possui um **roteador default** mais próximo a ele. É entre estes dois roteadores de borda que acontece o roteamento.

Como o roteador consegue determinar qual a melhor rota a ser percorrida pelos pacotes de informações?

O roteador utiliza-se de **algoritmos de roteamento**, que mapeiam todos os roteadores no caminho até o roteador destino e faz algumas mensurações como: a quantidade de enlaces existentes no caminho; a distância física dos enlaces entre os roteadores e a velocidade dos enlaces. Baseados nesses dados os algoritmos de roteamento verificam o **caminho de menor custo** ou **caminho mais curto**. Além disso os algoritmos de roteamento podem mensurar a **carga** de um enlace, ou seja, o nível de congestionamento daquele enlace.

Em resumo, os algoritmos de roteamento verificam o caminho mais curto, porém se o mais curto for, ao mesmo tempo, muito congestionado (o que será bem provável), o algoritmo irá verificar uma segunda opção de caminho que não seja tão longo, mas que não possua congestionamento. **O importante é achar o caminho mais rápido em um determinado momento!**



SUGESTÃO DE ATIVIDADE PRÁTICA:
Usar o Tracerout (Linux) ou Tracert (Windows) para visualizar a rota do host local a qualquer site no mundo e o tempo de viagem de ida e volta.

5.4.2. Protocolo IP

O protocolo mais importante da camada de Rede é o **IP – Internet Protocol**, ou Protocolo de Internet. O IP é responsável pelo endereçamento dos hosts e equipamentos em uma rede. Todo host em uma rede deve ter um endereço lógico que chamamos de endereço IP. Falamos um pouco de endereços IP na seção 5.1.5 quando estudamos sobre Serviços de DNS, lembra?

Bem, como já sabemos, a camada de rede recebe os segmentos da camada de transporte e os transforma em datagramas., que é o tipo de pacote da camada de rede. Esses datagramas possuem um cabeçalho com uma forma predefinida pelo protocolo que os utiliza: o protocolo IP. Estudaremos duas versões de IP, o IP versão 4 (IPv4) e o IP versão 6 (IPv6). A primeira

versão, IPv4, é ainda a mais utilizada atualmente. Veja como é a estrutura de um datagrama IPv4:

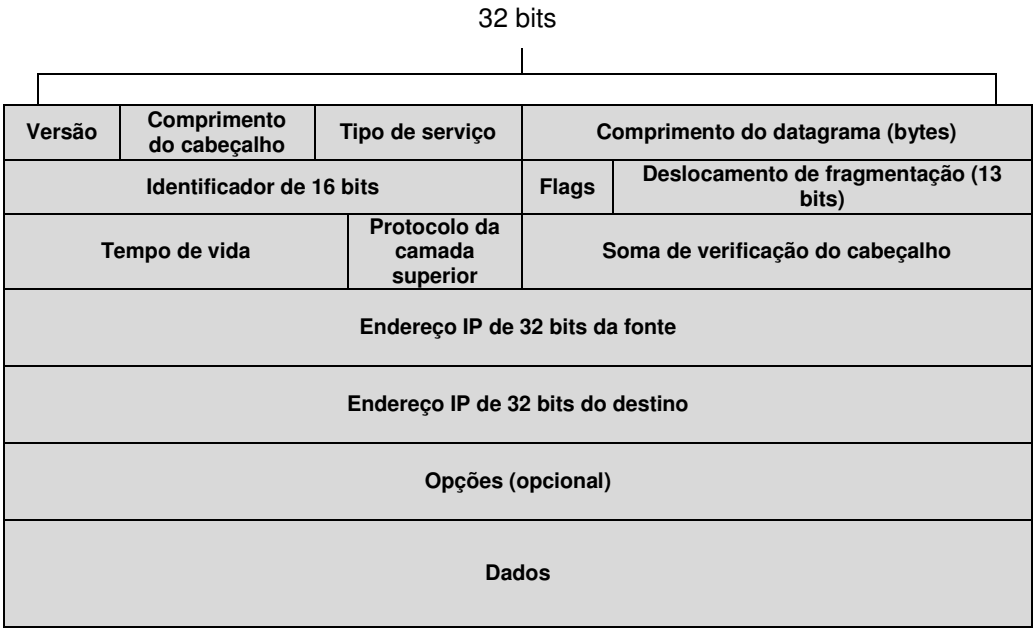


Figura 5i. Datagrama IPv4

- **Versão:** indica de o protocolo usado é o IPv4 ou o IPv6.
- **Comprimento do cabeçalho:** este campo é necessário devido a existência do campo Opções, que pode fazer com que o tamanho do cabeçalho varie.
- **Tipo de serviço:** indica se o datagrama possui alguma particularidade, como se é de uma aplicação em tempo real, se requer baixo atraso, etc.
- **Tempo de vida:** para que o datagrama não corra o risco de ficar viajando de roteador a roteador "eternamente" é inserido neste campo um valor onde, a cada roteador pelo qual o datagrama passa, é decrementado o valor 1 do tempo de vida, assim quando este valor for 0 o datagrama deverá ser descartado.
- **Protocolo de camada superior:** qual a camada superior em relação à camada de rede? A de transporte, não é mesmo? Neste campo é informado qual protocolo da camada de transporte deverá ser usado neste pacote, TCP ou UDP.

- **Soma de verificação do cabeçalho:** como já vimos em cabeçalhos de outras camadas, a soma de verificação é uma forma de detecção de erros no cabeçalho.
- **Endereços IP de fonte e de destino:** trazem, respectivamente, o endereço IP do host remetente e o endereço IP do host destinatário.
- **Identificador de 16 bits, Flags, Deslocamento de fragmentação:** estes 3 campos servem para auxiliar em uma propriedade do protocolo IP: a **fragmentação**. Ao enviar um datagrama abaixo na pilha de camadas, ou seja para a camada de enlace, corre-se o risco de os **quadros** da camada de enlace possuírem uma MTU (unidade máxima de transmissão) menor que o tamanho do datagrama e não suportarem a carga de bits, obrigando a camada de rede a fragmentar seu datagrama em datagramas menores e, só assim, enviá-los pela rede. Os campos Identificador, Flags e Deslocamento servem para identificar cada fragmento e ajudar na reconstrução destes datagramas menores no datagrama original ao chegarem no host destinatário.

Bem, falamos de datagramas IP, mas fica a questão: como surgem os endereços IP nos hosts da rede?

O endereço IPv4 é formado por 32 bits, separados por pontos em 4 conjuntos de 8 bits, que chamamos de octetos. Apesar de serem essencialmente números binários, o endereço IP é tratado por nós em notação decimal. Portanto o endereço IP 192.168.10.56 em notação decimal é formado na verdade por 4 conjuntos de 8 bits: 11000000.10101000.00001010.00111000.

Os endereços IPv4 são divididos em duas partes. A parte mais à esquerda serve para identificar a qual rede o host pertence e a parte mais à direita serve para identificar os hosts daquela rede. É como usar o nome e o sobrenome: o sobrenome identifica a qual família uma pessoa pertence e o nome identifica os membros daquela família.

Se eu usar os 3 primeiros octetos do endereço IP acima para identificar a rede e o último octeto para identificar o host, dessa forma:

11000000. 10101000. 00001010.	00111000
REDE	HOST

O endereço ficará assim:

192.168.100.56/24

Onde o /24 indicará a **máscara de sub-rede**, ou seja, a quantidade de bits que foram usados no endereço para identificar a rede a qual pertence este host. Podemos concluir que, este host especificamente, está na sub-rede 192.168.10 e o código dele é o 56.

É claro que podemos usar diferentes máscaras de sub-rede para identificar uma sub-rede e um host, mas para facilitar as coisas foram criadas as **classes de endereços IP**:

- **Classe A**

Na classe A usamos 1 octeto para identificar a sub-rede e 3 octetos para identificar o host:

Prefixo	Sufixo		

Esta classe é mais usada em sub-redes com grande número de hosts, onde é necessária uma variedade maior de endereços. Neste caso a máscara de sub-rede será /8, pois apenas os 8 primeiros bits do endereço serão usados para identificar a rede. Você também verá a máscara de sub-rede representada assim: 255.0.0.0.

Classe B

Na classe B usamos 2 octetos para identificar a sub-rede e 2 octetos para identificar os hosts:

prefixo		Sufixo	

Nesta classe, a quantidade de endereços reservados para as sub-redes é igual a de endereços reservados para os hosts. A máscara de sub-rede será /16 ou 255.255.0.0.

Classe C

Na classe C usamos 3 octetos para identificar a sub-rede e 1 octeto para identificar os hosts:

<table>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">prefixo</td><td>Sufixo</td></tr>
</table>

Esta classe é a mais usada em redes de pequeno porte, onde o número de hosts na rede não ultrapassem os 253 hosts. A máscara de sub-rede é /24 ou 255.255.255.0.

5.4.3. IPv6

No início da sessão anterior comentamos que existem duas versões do protocolo IP, o IPv4 e o IPv6. Vimos a estrutura tanto do endereçamento IPv4 quanto do datagrama IPv4. Vamos conhecer então, um pouco do IPv6.

Antes de mais nada vamos entender um pouco o motivo da existência do IPv6.

Se você calcular bem, o endereço IPv4 possui 32 bits, o que equivale a 2^{32} possibilidades de endereços, que corresponde a 4.294.967.296 de endereços possíveis. Cada roteador e cada host da rede mundial, ou internet, deve possuir um endereço IP único, o que consequentemente faz com que os mais de 4 milhões de endereços IPv4 possíveis estejam esgotando.

Antes que isto realmente aconteça, grupos de trabalhos de instituições ligadas à internet se dedicaram na criação de uma nova versão do protocolo IP que permitisse a continuação do crescimento da internet possuindo um tipo de endereçamento com um número imensamente maior de possibilidades. A essa versão foi dado o nome de IPv6 (Internet Protocol versão 6).

Agora fiquei curioso! Como seria então um endereço IPv6?

Enquanto o endereço IPv4 possui apenas 32 bits, o endereço IPv6 possui 128 bits, ou seja 2^{128} endereços possíveis. Este cálculo resulta em um número tão grande que dizem que se cada grão de areia no mundo quisesse, poderia ter um endereço IP [Kurose, 2007].

O endereço IPv6 é dividido em 8 conjuntos de 16 bits representados por 4 dígitos em hexadecimal, veja o exemplo:

2051:0fb6:45d2:48d0:9312:5ad9:a340:5217

Muito interessante! Mas se é uma maravilha tão grande, por que ainda não usamos o IPv6?

Toda a rede mundial funciona hoje usando o protocolo IPv4. Migrar para outra versão, que altera o modo como os dados trafegam na rede é um processo bem complicado, principalmente porque são bilhões de equipamentos ligados em rede no mundo todo. Não se pode simplesmente ir dormir usando o IPv4 e acordar usando o IPv6.

Foi cogitado, inclusive, implementar um “dia da conversão”, onde em um determinado dia e em uma determinada hora todas os computadores, impressoras de rede, roteadores, celulares, tablets, enfim, todos os equipamentos ligados à internet teriam que ser desligados e atualizados, migrando do IPv4 para o IPv6. Um técnico em Redes ganharia muito dinheiro fazendo atendimentos para atualizar as máquinas dos clientes, mas provavelmente ele enlouqueceria antes do fim do dia! =)

De fato que não é viável proceder desta forma (até porque ainda existem equipamentos e sistemas operacionais funcionando por aí que não possuem

suporte ao IPv6, portanto eles não poderiam mais ter acesso à internet) essa migração será feita aos poucos.

Os novos sistemas operacionais, drivers de placas de rede, roteadores e demais equipamentos de rede possuem suporte tanto ao IPv4 quanto ao IPv6. Hoje em dia é possível que um host habilitado para IPv6 envie datagramas IPv4 para não interferir no restante da rede, portanto gradativamente o IPv6 será introduzido, de forma bem menos traumática.

5.4.5. Protocolo DHCP

Já está devidamente entendido que cada host, roteador, impressora de rede, ou qualquer outro equipamento que envie e receba pacotes da rede deve ter um endereço IP para ser localizado, mas quem é o responsável por configurar estes números de IP nos hosts? A princípio seria o técnico administrador da rede que faria isso manualmente em cada host, executando uma tarefa repetitiva.

Uma tarefa repetitiva, normalmente pode ser executada por um software. A tarefa de inserir números de IP, máscara de sub-rede, gateway e DNS nos hosts de uma rede pode ser executada por um software em um servidor baseado no protocolo **DHCP – Dynamic Host Configuration Protocol,** ou Protocolo de Configuração Dinâmica de Hospedeiro.

E qual é a vantagem em se usar o DHCP?

Quando temos uma pequena rede, com poucos hosts, normalmente desktops, é realmente interessante que se configure os IPs manualmente para um maior controle. Agora imagine uma rede em que haja muitos computadores e dentre eles muitos notebooks que entram e saem da rede com frequência. Tome como exemplo um hotel, onde cada hóspede pode usar a internet acessando a rede sem fio do estabelecimento em seu notebook, tablet, celular ou afim. Seria muito complicado para o administrador da rede, configurar os equipamentos de todos os hóspedes tendo em vista a rotatividade de pessoas no local.

Neste caso, a melhor solução seria usar o protocolo DHCP para, a partir de um **servidor DHCP,** que pode ser um computador ou um ponto de acesso sem fio, atribuir IPs, máscaras, números de gateway e DNS nos hosts, de forma dinâmica, ou seja, variável.

Voltando ao exemplo, imagine o hóspede que estava usando a rede sem fio do hotel se dirigindo ao aeroporto para voltar à sua cidade de origem. Ao chegar ao aeroporto, este também precisa acessar a rede sem fio para se conectar à internet. Também neste momento, o **servidor DHCP** do aeroporto irá configurar o computador com os códigos da rede local. Note que para que o viajante consiga se conectar em ambas as redes sem precisar atribuir endereços de rede manualmente, em seu computador deverá rodar um software **cliente DHCP**.

Veja como funciona o processo:

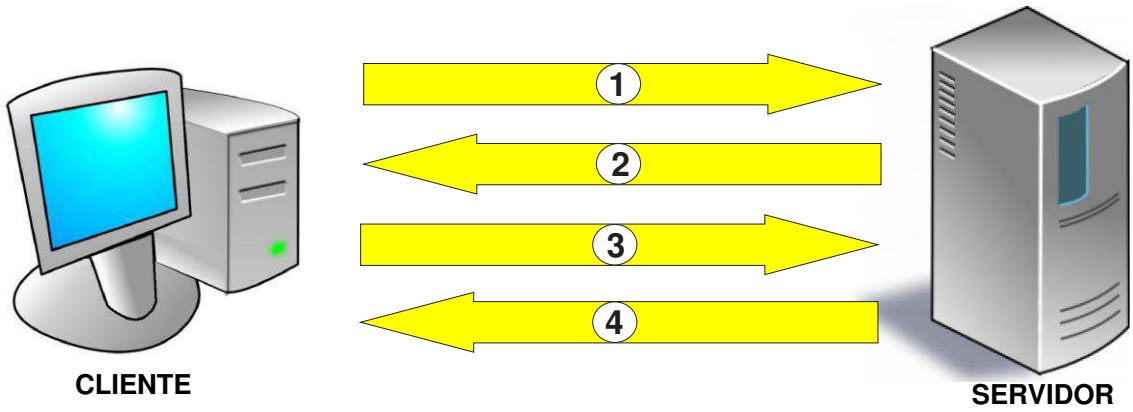
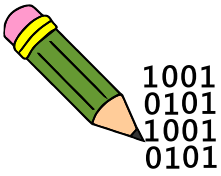


Figura 5j. Etapas do protocolo DHCP

1. **Descoberta DHCP:** o cliente, que acaba de entrar na rede, não sabe qual host poderá fornecê-lo um IP, portanto envia uma mensagem através do protocolo UDP a todos os hosts da rede para o IP 255.255.55.255, que é o endereço de **broadcast**.
2. **Ofertas DHCP:** ao receber a mensagem de descoberta do cliente, o servidor DHCP responde enviando ao solicitante ofertando um IP disponível. Se houverem mais de um servidor DHCP na rede, todos eles enviam uma mensagem de oferta ao cliente.
3. **Requisição DHCP:** ao receber a(s) oferta(s), o cliente seleciona o IP que do servidor ao qual deseja se conectar e envia uma mensagem de requisição.

4. **Confirmação DHCP:** o servidor envia um acknowledge – ACK, confirmando a requisição.



Exercícios

1. Explique brevemente as duas funções básicas da camada de Rede.

_____
_____
_____
_____
_____

2. Retorne à Figura 5g e responda: *"Se o host H2 quiser se comunicar com o host H1, qual valor de cabeçalho deverá conter no datagrama enviado ao roteador R1?"*.

_____

3. Se a versão 4 do IP está funcionando tão bem, por que as redes deverão migrar para a versão 6?

_____
_____
_____

PESQUISA

Pesquise em sua escola como é feita a configuração do IP nas máquinas da rede. Dá-se manualmente ou via DHCP? Por que este método foi escolhido?

5.5. CAMADAS DE ENLACE E FÍSICA (Modelo OSI) OU INTERFACE COM A REDE (Modelo TCP/IP)

Chegamos aos níveis mais baixos dos modelos de camadas. Níveis mais baixos também, pois são os que mais se distanciam da interação com o homem.

Antes de qualquer coisa, vamos lembrar o que é um enlace:

ENLACE

É um link de comunicação, ou uma ligação entre dois sistemas de rede. Por exemplo, a ligação entre um computador e um roteador ou a ligação entre dois roteadores em redes locais diferentes.

Por muito tempo, o enlace foi visto apenas como o **fio** que liga um host ou roteador a outro host ou roteador, mas com o advento das redes wireless, o fio deixou de ser o principal integrante de um enlace. Sendo assim, podemos ver, ou imaginar, um enlace como um canal de comunicação entre um host ou roteador a outro host ou roteador.

O PDU da camada de enlace é o **quadro**. Após receber o datagrama IP, a camada de enlace o coloca dentro de uma estrutura chamada quadro. Estes quadros viajam do host remetente ao host destinatário por uma sequência de enlaces. Ao chegar à camada de rede no destinatário, esta irá retirar o datagrama IP de dentro do quadro da camada de enlace.

Agora pense bem, quando vamos nos conectar a um site da Web, este pode estar em qualquer local do mundo, concorda? Imagine então quantos enlaces existirão no caminho entre o computador local e o servidor Web. Imagine também os mais diferentes tipos de enlaces neste caminho.

Você pode estar usando um notebook e se comunicando com um roteador wireless em uma rede sem fio, isto já é um enlace. Na sequência, o roteador da sua casa pode estar se comunicando com seu provedor de internet via cabo de par trançado, num protocolo Ethernet ou usando uma linha telefônica, outro enlace. Ao chegar ao seu provedor, este poderá se comunicar com outro servidor usando protocolos WAN através de fibras ópticas, depois antenas Wi-Max, passar por outro cabo de par trançado num protocolo PPP (Protocolo Ponto-a-Ponto) e etc.

Em resumo, existem vários tipos de enlaces e a função fundamental da camada de enlace é fazer o datagrama IP passear pelos variados enlaces sem sentir a diferença entre eles e chegar ao destino, assim como prover alguns serviços, como: **garantia de entrega, controle de fluxo, detecção e correção de erros**.

5.5.1. Endereços MAC

Desde a camada de aplicação até a camada de rede, quem implementa os serviços e os protocolos é o host. Na camada de enlace, a implementação é feita por **adaptadores**. Adaptadores são as conhecidas placas de rede, tanto para redes com fio, quanto sem fio. O adaptador deve existir tanto no host remetente, pois é por onde o quadro da camada de enlace sai, quanto no hpst destinatário, que é por onde o quadro chega.

Neste adaptador é inserido um endereço de camada de enlace, ou endereço físico, mas é mais conhecido como **endereço MAC – Media Access Control**, ou Controle de Acesso ao Meio. Cada adaptador de rede do mundo tem seu próprio endereço MAC. É chamado de endereço físico porque fica gravado na ROM do adaptador e não deve ser alterado.

Mas se já existe um endereço IP, qual a necessidade de existir também um endereço MAC?

Veja bem, o endereço IP é um endereço lógico e deve ser inserido de acordo com a distribuição dos hosts pelas redes, e pode ser alterado, dependendo da necessidade. O endereço físico MAC acompanhará o adaptador do host aonde quer que ele vá. É como se o MAC identificasse **o host** e o IP identificasse **onde mora o host**.

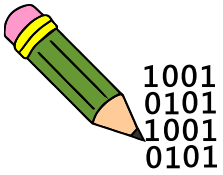
E se a placa de rede (adaptador) de um host ficar defeituosa e for trocada por outra, o que acontece com o endereço MAC do host?

Como já dissemos, o MAC acompanha a placa de rede, ou adaptador. Se ela for retirada, o MAC é retirado junto, e ao inserir uma nova placa, consequentemente o host terá um novo endereço MAC.

Em algumas redes, o administrador cadastra e gerencia os endereços MAC dos computadores, para que somente os MACs cadastrados possam ter acesso à rede, evitando o acesso de intrusos com outros computadores.

Assim como o DNS resolve nomes em IPs para um host, os endereços MAC também tem que ser resolvidos em IPs e o responsável por fazer tudo isto é o protocolo **ARP – Address resolution Protocol**, ou protocolo de Resolução de Endereços.

O ARP faz um mapeamento na rede de todos os endereços MAC à medida que eles vão enviando ou recebendo dados na rede e coloca estes endereços em uma tabela, chamada de **tabela ARP**.



Exercícios

1. O que é um enlace?

_____

_____

_____

_____

2. O que é um Endereço MAC?

_____

_____

_____

3. Relacione os PDUs com as camadas:

(1) Camada de Aplicação.

(2) Camada de Transporte.

(3) Camada de Rede.

(4) Camada de Enlace.

( ) quadro

( ) segmento

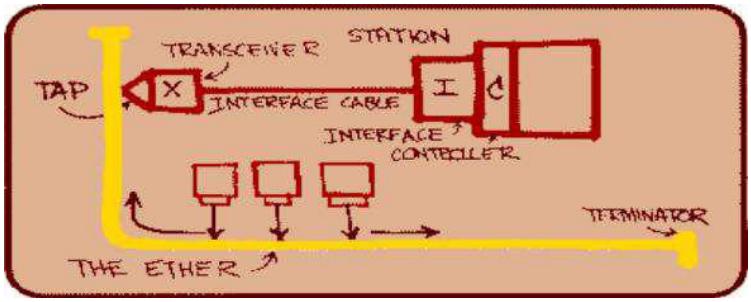
( ) dados

( ) datagrama

5.5.2. Ethernet

Existem muitas tecnologias de rede, mas de longe, a mais conhecida e usada de todas é a **Ethernet**, que surgiu dos termos ether: cabo coaxial e net: rede. Pode-se dizer então que o padrão Ethernet é usado em redes cabeadas, já que se estendeu também aos outros tipos de cabo além do coaxial, como o par trançado e a fibra óptica. Alguns autores afirmam que as redes wireless também fazem parte do padrão Ethernet, mas como a maioria discorda, não vamos entra nessa discussão neste momento.

Este padrão começou a ser desenvolvido em meados da década de 70 por Bob Metcalfe que fez o seguinte desenho de seu projeto:



O padrão original da Ethernet possuía 2.94 Mbps e usava cabos coaxias. Este padrão deu origem a outros dois: o 10BASE-5 e o 10BASE-2. Logo em seguida surgiram os padrões 10BASE-T e o 10BASE-F.

O que todos estes padrões têm em comum?

A velocidade. Todos eles transmitiam dados a 10 Mbps, daí o significado do número 10 no início dos nomes. O termo BASE vem de *baseband* modulation, o que significa que o sinal é percorrido de forma digital e não mais de forma analógica, dispensando o uso de modems telefônicos. Vejamos as características:

- 10BASE-5: usava cabos coaxiais pesados e pouco flexíveis do tipo *thicknet*, transmitia a 10 Mbps e o sinal poderia chegar a até 500 metros de comprimento.
- 10BASE-2: surgiu em seguida, usando cabos coaxiais mais leves e flexíveis do tipo *thinnet*, transmitia a 10 Mbps e o sinal poderia percorrer uma distância de até 185 metros pelo cabo.
- 10BASE-T: é a evolução do Ethernet do cabo coaxial para o cabo de par trançado. A letra T no fim do nome vem de *twisted pair*, ou par trançado. Este padrão também transmite a 10 Mbps e o sinal percorre até 100 metros.
- 10BASE-F: neste padrão já é utilizada a fibra óptica, indicada pela letra F de *fiber optic*. É um padrão com custo muito elevado, portanto não foi muito utilizado. O sinal podia chegar a 2000 metros de distância.

Todos estes padrões de 10 Mbps tornaram-se obsoletos e não são mais utilizados. A grande evolução dos padrões Ethernet fez surgir o **Fast Ethernet**, um padrão que aumentava em 10 vezes a velocidade da transmissão. Dentre os padrões Fast Ethetnet lançados os principais são:

- 100BASE-TX: É o padrão mais popular entre todos. Possui taxa de transmissão de 100 Mbps, uma boa evolução em relação ao 10BASE-T, seu correspondente Ethernet. Ele usa o cabo de par trançado e nele o sinal percorre até 100 metros. O cabo UTP mais utilizado no 100BASE-TX é o de categoria 5, onde dos 4 pares apenas dois são utilizados, um para enviar e outro para receber. [MORIMOTO, 2010]. Os outros dois

pares não utilizados para transmissão ficam fazendo o papel de isolamento contra interferências eletromagnéticas, uma grande vantagem neste padrão.

- 100BASE-FX: é o Fast Ethernet para uso com fibra óptica e transmite a 100 Mbps.

No caminho da evolução surgiu o padrão **Gigabit Ethernet** que eleva a velocidade de transmissão de 100 Mbps (Fast Ethernet) para 1000 Mbps, ou 1 Gbps, daí o nome Gigabit.

- 1000BASE-LX: padrão para cabos de fibra óptica, utiliza lasers que são mais rápidos que leds, porém muito mais caros. Seu alto nível qualidade oferece um alcance de sinal de até 10 km, portanto é um padrão muito utilizado para redes de longa distância.
- 1000BASE-SX: também feito para uso com fibra óptica, porém usa lasers de curta distância, barateando os custos, o que leva a uma redução do alcance para no máximo 275 metros.
- 1000BASE-CX: este padrão já passa a usar cabos de par trançado, porém apenas os STPs ou SSTPs, ou seja, cabos blindados. Chagou a ser mais utilizado logo após seu lançamento, por ser mais barato que a fibra óptica, mas com o aparecimento do 1000BASE-T, ele praticamente caiu em desuso.
- 1000BASE-T: é o padrão para cabos de par trançado e ainda por cima, UTPs, ou seja, sem blindagem. Este padrão fez o Gigabit Ethernet começar a se popularizar, pois além de diminuir e muito os custos, seu complexo sistema de transmissão permitiu manter a distância de propagação do sinal em 100 metros, os mesmos usados no 10BASE-T e no 100BASE-FX.

Por último, mas não menos importante, temos o surgimento do mais atual padrão Ethernet: o **10 Gigabit Ethernet**. É isso mesmo que você está pensando, ele multiplica por 10 o Gigabit Ethernet. Possui taxa de transmissão de 10Gbps (10 gigabits por segundo), ou 10.000 Mbps. É de longe o padrão mais veloz, porém ainda não muito popular. Para uso com fibras ópticas temos

vários padrões como os 10GBASE-LR, 10GBASE-ER, 10GBASE-ZR, 10GBASE –SR e 10GBASE-LRM. A princípio imaginou-se que com este padrão não seria possível o uso de cabos de par trançado e que obrigatoriamente, quem quisesse aumentar a velocidade de transmissão usando este padrão teria que migrar para a fibra óptica, mas como podíamos prever, os pesquisadores estudaram várias formas até conseguir criar um padrão que usasse o par trançado, foi então que surgiu o 10GBASE-T, onde o cabo ideal para uso é o categoria 6.

No 10GBASE-T, surgiram algumas condições para que fosse possível usar os cabos categoria 6: os 4 pares do cabo são utilizados para transmissão de dados, extinguindo assim os cabos que faziam o isolamento contra interferências eletromagnéticas. A distância percorrida pelo sinal passou de 100 para 55 metros, pois a partir daí o sinal começa a atenuar. Ao utilizar o 10GBASE-T, deve haver um cuidado especial com a crimpagem dos cabos e evitar ao máximo os ruídos que gerem interferências, como antenas e cabos elétricos próximos aos cabos de dados.

PESQUISA

Pesquise na rede de sua escola se é usado algum padrão Ethernet. Qual deles é utilizado?

Hino Nacional

Ouviram do Ipiranga as margens plácidas
De um povo heróico o brado retumbante,
E o sol da liberdade, em raios fúlgidos,
Brilhou no céu da pátria nesse instante.

Se o penhor dessa igualdade
Conseguimos conquistar com braço forte,
Em teu seio, ó liberdade,
Desafia o nosso peito a própria morte!

Ó Pátria amada,
Idolatrada,
Salve! Salve!

Brasil, um sonho intenso, um raio vívido
De amor e de esperança à terra desce,
Se em teu formoso céu, risonho e límpido,
A imagem do Cruzeiro resplandece.

Gigante pela própria natureza,
És belo, és forte, impávido colosso,
E o teu futuro espelha essa grandeza.

Terra adorada,
Entre outras mil,
És tu, Brasil,
Ó Pátria amada!
Dos filhos deste solo és mãe gentil,
Pátria amada,Brasil!

Deitado eternamente em berço esplêndido,
Ao som do mar e à luz do céu profundo,
Fulguras, ó Brasil, florão da América,
Iluminado ao sol do Novo Mundo!

Do que a terra, mais garrida,
Teus risonhos, lindos campos têm mais flores;
"Nossos bosques têm mais vida",
"Nossa vida" no teu seio "mais amores."

Ó Pátria amada,
Idolatrada,
Salve! Salve!

Brasil, de amor eterno seja símbolo
O lábaro que ostentas estrelado,
E diga o verde-louro dessa flâmula
- "Paz no futuro e glória no passado."

Mas, se ergues da justiça a clava forte,
Verás que um filho teu não foge à luta,
Nem teme, quem te adora, a própria morte.

Terra adorada,
Entre outras mil,
És tu, Brasil,
Ó Pátria amada!
Dos filhos deste solo és mãe gentil,
Pátria amada, Brasil!

Hino do Estado do Ceará

Poesia de Thomaz Lopes
Música de Alberto Nepomuceno
Terra do sol, do amor, terra da luz!
Soa o clarim que tua glória conta!
Terra, o teu nome a fama aos céus remonta
Em clarão que seduz!
Nome que brilha esplêndido luzeiro
Nos fulvos braços de ouro do cruzeiro!

Mudem-se em flor as pedras dos caminhos!
Chuvas de prata rolem das estrelas...
E despertando, deslumbrada, ao vê-las
Ressoa a voz dos ninhos...
Há de florar nas rosas e nos cravos
Rubros o sangue ardente dos escravos.
Seja teu verbo a voz do coração,
Verbo de paz e amor do Sul ao Norte!
Ruja teu peito em luta contra a morte,
Acordando a amplidão.
Peito que deu alívio a quem sofria
E foi o sol iluminando o dia!

Tua jangada afoita enfune o pano!
Vento feliz conduza a vela ousada!
Que importa que no seu barco seja um nada
Na vastidão do oceano,
Se à proa vão heróis e marinheiros
E vão no peito corações guerreiros?

Se, nós te amamos, em aventuras e mágoas!
Porque esse chão que embebe a água dos rios
Há de florar em meses, nos estios
E bosques, pelas águas!
Selvas e rios, serras e florestas
Brotem no solo em rumorosas festas!
Abra-se ao vento o teu pendão natal
Sobre as revoltas águas dos teus mares!
E desfraldado diga aos céus e aos mares
A vitória imortal!
Que foi de sangue, em guerras leais e francas,
E foi na paz da cor das hóstias brancas!

GOVERNO DO
ESTADO DO CEARÁ

Secretaria da Educação