

DlteC do Brasil®

[www.dltec.com.br](http://www.dltec.com.br)  
info@dltec.com.br | 41 3045.7810



DLTEC DO  
BRASIL

APOSTILA/E-BOOK DO CURSO DE REDES  
COMPLETO

Apostila/E-Book do Curso de Redes Completo

DlteC do Brasil®  
Todos os direitos reservados©

## Sobre o E-book/Apostila

O conteúdo desse documento é uma adaptação da **matéria online de leitura** do curso.

O presente material traz conteúdo teórico do curso online, porém temos que deixar claro que **não é um curso e sim uma adaptação do nosso material online para e-book/apostila**. Portanto recursos como exercícios, simulados, tutoria (tira dúvidas com professores) e vídeo aulas não fazem parte desse e-book, pois são exclusivos para alunos devidamente matriculados em nosso site oficial.

Para maiores informações sobre nossos treinamento visite o site:

>>> [<<<](http://www.dltec.com.br)

## Direitos Autorais

### Aviso Importante!

Esse material é de propriedade da **DLTEC do Brasil Ltda** e é protegido pela **Lei de direitos autorais 9610/98**.

É expressamente proibida cópia física ou em meio digital, reprodução parcial, reprografia, fotocópia ou qualquer forma de extração de informações deste sem prévia autorização da **DLTEC do Brasil** conforme legislação vigente.

Seu uso pessoal e intransferível é somente para o cliente que adquiriu o referido e-book/apostila.

A cópia e distribuição são expressamente proibidas e seu descumprimento implica em processo cível de danos morais e materiais previstos na legislação contra quem copia e para quem distribui, sejam cópias físicas e/ou digitais.

**Copyright © 2016.**

## Índice

<i>Capítulo 01 - Introdução.....</i>	<b>5</b>
<i>Capítulo 02 - Conceitos Básicos de Rede.....</i>	<b>15</b>
<i>Capítulo 03 - Dispositivos de Redes.....</i>	<b>31</b>
<i>Capítulo 04 - Modelos OSI e TCP-IP .....</i>	<b>57</b>
<i>Capítulo 05 - Endereçamento IPv4, Sub-redes e Noções de IPv6.....</i>	<b>142</b>
<i>Capítulo 06 - Switching e VLANs .....</i>	<b>181</b>
<i>Capítulo 07 - Infraestrutura de Redes e Cabeamento Estruturado .....</i>	<b>214</b>
<i>Capítulo 08 - Implementando Redes sen Fio.....</i>	<b>252</b>
<i>Capítulo 09 - Intranet, Internet e Roteadores.....</i>	<b>312</b>
<i>Capítulo 10 - Tópicos de Segurança e Gerenciamento de Redes.....</i>	<b>327</b>
<i>Capítulo 11 - Protocolo IP versão 6 .....</i>	<b>363</b>
<i>Capítulo 12 - Estudo de Caso - Projeto e Implementação de Rede.....</i>	<b>396</b>

*Nesse capítulo iremos estudar o histórico e a evolução dos sistemas computacionais, os quais tornaram a necessidade da evolução das redes de computadores uma constante até os dias de hoje.*

*Portanto, em paralelo aos avanços da computação as redes de computadores, assim como outras tecnologias de comunicação de dados, evoluíram para acompanhar as necessidades de troca de informações, armazenamento e processamento de dados remotamente partindo de sistemas isolados, onde para se trocar informações os operadores eram obrigados a carregar rolos de fitas magnéticas de um computador para outro, para uma realidade que migra para a computação em nuvem ou em inglês “Cloud Computing”.*

*Ao longo do curso veremos diversos conceitos e tecnologias com foco na implementação de uma rede de maneira estruturada e segura.*

*Desejamos a todos bons estudos.*

## Capítulo 01 - Introdução

### Objetivos do Capítulo

Ao final desse capítulo você deverá ser capaz de:

- Entender o histórico do avanço dos sistemas computacionais
- Entender o histórico do avanço das redes de computadores
- Entender e descrever os objetivos de uma rede de computadores

### Sumário do Capítulo

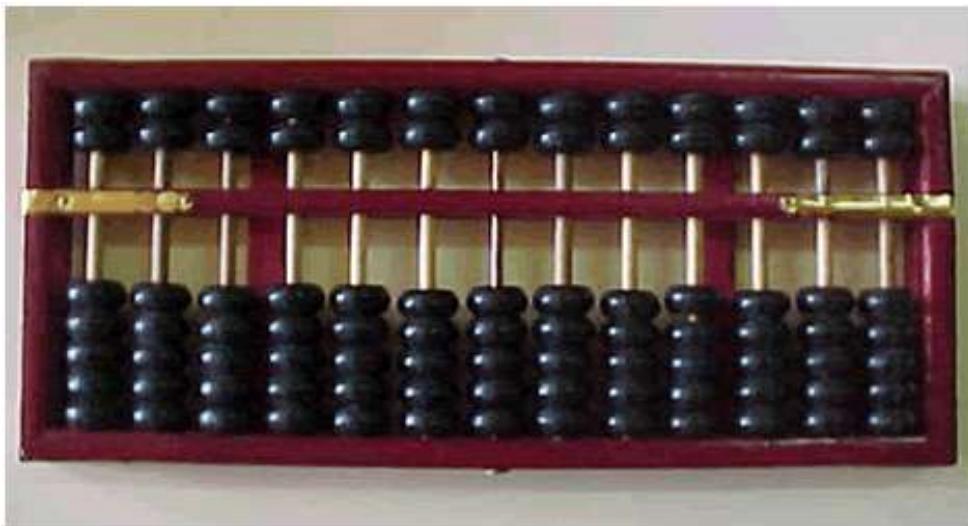
<b>1 Histórico e Evolução dos Sistemas Computacionais</b>	<hr/> <b>6</b>
<b>2 Histórico e Evolução das Redes de Computadores</b>	<hr/> <b>11</b>
<b>3 Objetivo e Desafios das Redes de Computadores</b>	<hr/> <b>14</b>

## 1 Histórico e Evolução dos Sistemas Computacionais

Porque iniciar um curso de redes de computadores estudando a evolução dos sistemas computacionais? A resposta é simples, porque sem computadores não há rede. Portanto precisamos entender a evolução histórica dos computadores para podermos também compreender a origem da necessidade da comunicação em rede desses dispositivos.

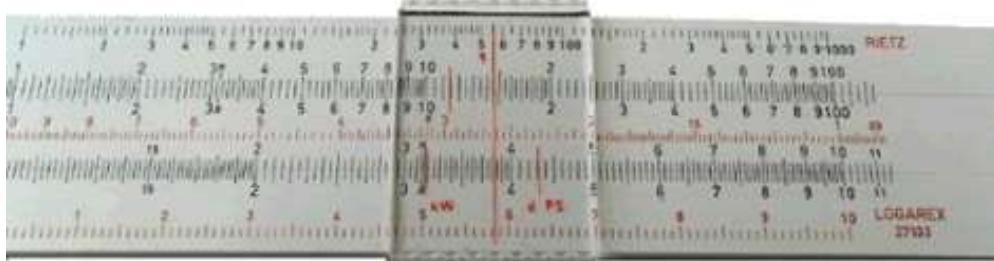
Atualmente os computadores fazem parte da nossa vida de uma forma nunca vista anteriormente. Seja em casa, na escola, na faculdade, na empresa ou em qualquer outro lugar eles estão sempre entre nós, ainda mais se considerarmos o avanço dos smartphones e tablets que permitem uma convivência quase que total do ser humano com o ambiente computacional na atualidade.

Mas ao contrário do que parece, a computação não surgiu nos últimos anos ou décadas, mas sim há alguns mil anos atrás. Dependendo da bibliografia essa realidade surge entre 3.500 e 7 mil anos atrás com a criação do ábaco, a primeira calculadora da história, veja uma foto na figura a seguir.



Após o ábaco a próxima ferramenta para auxiliar em cálculos matemáticos foi a régua de cálculos, desenvolvida em meados de 1638 por William Oughtred, baseando-se na tábua de logaritmos que havia sido inventada por John Napier em 1614.

O mecanismo do William era consistido de uma régua que já possuía uma boa quantidade de valores pré-calculados, organizados em forma que os resultados fossem acessados automaticamente. Uma espécie de ponteiro indicava o resultado do valor desejado.



Após a régua de cálculo tivemos outros inventos como a máquina de Pascal, conhecida como a primeira calculadora mecânica da história, inventada nos idos de 1642. Tivemos também o advento da programação funcional por volta dos anos de 1801, depois a máquina de diferenças e o engenho analítico no ano de 1822, a teoria de Boole com a introdução de um sistema lógico utilizando os algarismos zero e um, o que deu origem à lógica moderna, isso ocorreu no ano de 1847.

Já em 1890 temos o advento da máquina de Hollerith com o conceitos dos cartões perfurados e então na primeira metade do século 20 nascem os primeiros computadores mecânicos.

Já a computação moderna nasce em torno de 1946 com a primeira geração de computadores, onde seu principal representante foi o ENIAC (veja a figura abaixo). Ele foi criado no ano de 1946 e era 1000 vezes mais rápido que qualquer um dos seus antecessores, foi desenvolvido pelos cientistas norte-americanos John Eckert e John Mauchly.



Outro marco da computação moderna foi o IBM 7300 (veja figura abaixo), conhecido por Strech, o qual marcou a segunda geração de computadores que vai de 1959 até aproximadamente 1964. Apesar de atualmente ser um “monstro” para sua época era pequeno em relação aos seus concorrentes e chegou a custar 13 bilhões de dólares americanos!



Porém, além do IBM 7300 tivemos alguns mini computadores na segunda geração, dos quais o que mais se destacou foi o PDP-8, apesar de menores que os supercomputadores ainda custava centenas de milhões de dólares!



Os computadores da segunda geração já efetuavam cálculos em microssegundos, eram mais confiáveis e com seus principais representantes clássicos, o IBM 1401 e seu sucessor o IBM 7094, já totalmente transistorizado. Entre os modelos 1401 e 7094, a IBM vendeu mais de 10.000 computadores!

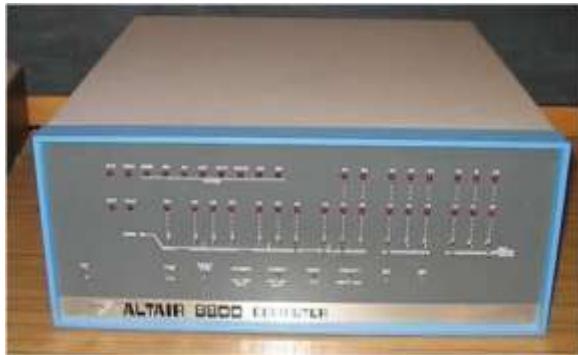
Após a segunda geração, entre 1964 e 1970 temos então a terceira geração, a qual foi marcada pelo início do uso dos circuitos integrados, permitindo que vários componentes e circuitos fossem armazenados em uma mesma placa, aumentando a velocidade de processamento e também reduzindo o custo dos dispositivos.

Um dos representantes mais marcantes dessa época foi o IBM 360/91, lançado em 1967. Este modelo foi um dos primeiros a permitir a programação da CPU por microcódigos e não precisava ter suas operações projetadas em hardware. Além disso, ele permitia o uso de dispositivos modernos para a época como discos de fita e impressoras simples.



Após a terceira geração de computadores vem a quarta geração, a qual é localizada entre os anos de 1970 ou 1971 até hoje, considerando a importância de uma maior escala de integração alcançada pelos circuitos integrados e o advento dos microprocessadores e dos microcomputadores.

Um dos representantes do início da quarta geração foi o Altair 8800 (veja a figura abaixo), o qual foi um dispositivo revolucionário para sua época, tanto que um jovem programador chamado Bill Gates se interessou pela máquina e criou sua linguagem de programação chamada Altair Basic.



Após o Altair, figuras importantes do mundo da informática começaram a surgir, como o Steve Jobs (fundador da Apple) e o "Apple I" (lançado em 1976), o qual pode ser considerado como o primeiro computador pessoal, pois acompanhava um pequeno monitor gráfico que exibia o que estava acontecendo no PC. Como o sucesso da máquina foi muito grande, em 1979 foi lançado o Apple II, que seguia a mesma ideia.



Seguindo na mesma linha, com os computadores Lisa (1983) e Macintosh (1984), foram os primeiros a utilizar o Mouse e possuírem a interface gráfica como nós conhecemos hoje em dia, com pastas, menus e área de trabalho.

Nessa mesma época Bill Gates fundou a Microsoft, que também desenvolvia computadores pessoais. No começo de sua existência, no final dos anos 70 e até meados dos anos 80, Bill Gates usou as ideias contidas em outras máquinas para construir a suas próprias, utilizando processadores 8086 da Intel. Seu primeiro sistema operacional da Microsoft foi o "MS-DOS".

Nessa mesma época, visando a melhoria do seu sistema operacional, Bill Gates acabou criando uma parceria com Steve Jobs, e após algum tempo, programou toda a tecnologia gráfica do Macintosh para o seu novo sistema operacional, o Windows.

Desta época para cá a história já é mais conhecida, pois tivemos vários processadores lançados, acompanhados de várias versões de sistemas operacionais. Entre os modelos da Intel, podemos citar: 8086, 286, 386, 486, Pentium, Pentium 2, Pentium 3, Pentium 4, Core 2 Duo, i5 e i7. Também temos a AMD, que entrou no ramo de processadores em 1993, com o K5, lançando posteriormente k6, k7, Atlhon, Duron, Sempron, dentre outros.

Atualmente qualquer smartphone (celulares) tem a capacidade de processamento muito superior aos supercomputadores da segunda ou terceira gerações. Além disso, a variedade de equipamentos criada para os computadores é bastante variada, pois temos desktops, laptops, tablets, os já falados smartphones e a cada dia a evolução tecnológica permite mais dispositivos e possibilidades de inovação nessa área.

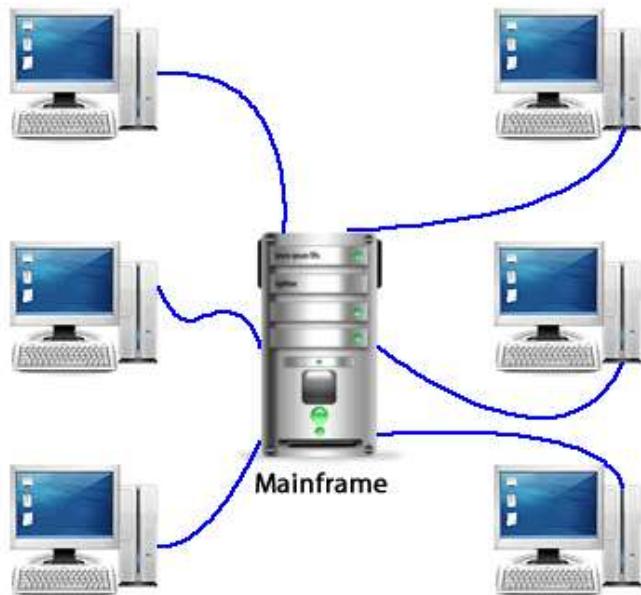
Porém, com toda essa evolução dos computadores também veio a necessidade de comunicação, da integração entre os diversos computadores, serviços mais avançados para os usuários, necessidade de guardar as informações em banco de dados, e assim por diante, por isso fizemos questão de mostrar a evolução histórica dos sistemas computacionais antes de entrarmos realmente na área das redes de computadores.

## 2 Histórico e Evolução das Redes de Computadores

Durante as primeiras décadas da utilização dos computadores na área corporativa (em ambiente empresarial), inicialmente os computadores foram utilizados principalmente com finalidade científica e/ou militar e os sistemas computacionais eram altamente centralizados.

O ambiente onde os computadores ficavam localizados era chamado CPD (Centro de Processamento de Dados) e pelo fato dos sistemas estarem centralizados implicava que existia uma máquina que concentrava todos os dados, ou seja, um dispositivo que fornecia todo processamento e todas as informações necessárias. Esse dispositivo era tipicamente um computador de grande porte para a época, conhecido como **mainframe**, o qual o maior fabricante de computadores da época era a IBM, empresa já citada no tópico anterior.

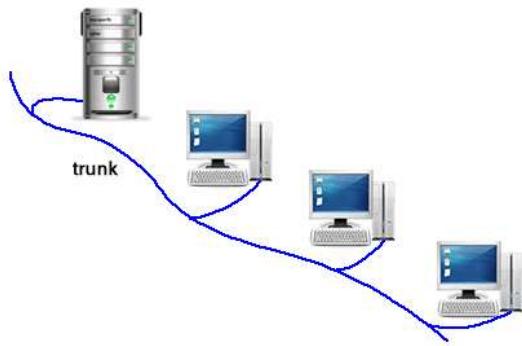
Além dos mainframes, existiam diversas máquinas, chamadas de terminais, para acesso aos dados e como o processamento não estava nelas, elas eram chamadas de terminais burros.



Apesar de sua capacidade de processamento, este modelo centralizado acabou perdendo força com a evolução dos computadores pessoais (PCs – Personal Computers), pois o custo elevado e características de manutenção (quando o computador central falha todo o sistema é comprometido) acabaram tornando os PCs a solução mais adotada com o passar do tempo. Além disso, os terminais burros podiam apenas fazer tarefas pré-determinadas, limitando as possibilidades dos usuários.

Com o crescimento da variedade e oferta dos computadores pessoais vem também a necessidade de integrá-los de alguma forma, pois a necessidade de trocar informações ou então interagir com outros usuários da rede foi naturalmente surgindo. Até certo ponto essa troca de dados entre os computadores pessoais tinha que ser feita gravando os dados em um disco (disquete ou fita) e levando até o outro computador para o processamento. Em redes até existe uma piada que esse foi o primeiro protocolo de rede chamado **DPL-DPC** ou “**disquete pra lá – disquete pra cá**”. Portanto, essa necessidade de comunicação entre dois ou mais computadores surge primeiramente no ambiente corporativo, mas quase ao mesmo tempo para os usuários domésticos.

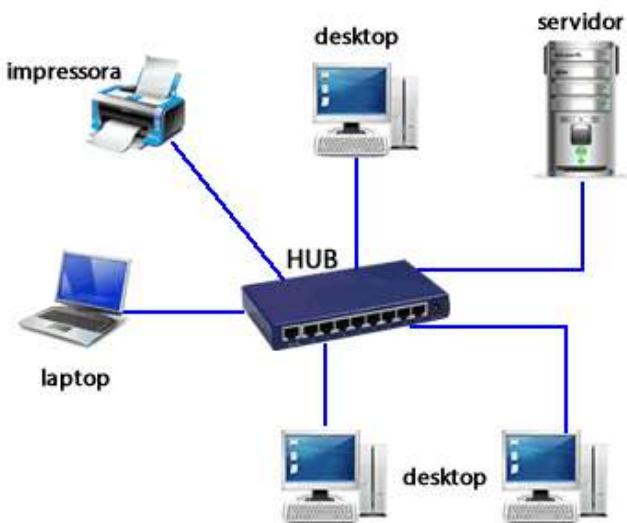
Nesse momento vários fabricantes iniciaram o desenvolvimento de redes proprietárias, como a Novell e o IPX, o que dificultava a vida das empresas, pois elas ficavam presas a um determinado padrão ou fabricante, o que gerou a necessidade de padronização e o nascimento de modelos de referência como o **OSI (Open Systems Interconnection)**, o qual estudaremos posteriormente. Veja na figura a seguir um exemplo de uma rede de computadores pessoais.



As redes tornam-se populares e praticamente indispensáveis a partir dos anos 90 com o surgimento da Internet e a massificação do uso do protocolo TCP/IP, atual protocolo de rede utilizado na Internet e nas redes internas das empresas (Intranet).

Em termos físicos, as redes iniciam com os cabos coaxiais, conforme figura anterior, depois tem uma evolução para o uso do UTP, com as redes Ethernet 10baseT. Os cabos coaxiais foram substituídos por pares metálicos após algum tempo devido ao custo, espaço (eles são mais grossos), conectores mais caros e também devido ao fato de que quando o cabo tinha um problema todos os computadores para trás perdia conexão com a rede.

Atualmente maioria das redes utiliza uma velocidade de 100Mbps ou 1Gbps em suas LANs (Local Area Network) utilizando cabos metálicos UTP (Unshield Twisted Pair – pares trançados não blindados) e são interligados através de equipamentos chamados switches ou hubs (atualmente em desuso).



Também não podemos esquecer a evolução das redes sem fio, chamadas de wireless ou WiFi, que nasceram com velocidades de 11Mbps e atualmente suas versões em desenvolvimento prometem velocidades acima de 400Mbps. Em uma rede sem fio temos um elemento chamado Access Point (AP) ou Ponto de Acesso que faz a distribuição do sinal de rede para as diversas placas de rede sem fio que estão nos dispositivos dos usuários.



Outro meio muito utilizado em redes, porém principalmente para interligar os diversos dispositivos de redes, como os switches, é a fibra ótica. Apesar do seu custo, tanto de instalação como manutenção, ser mais alto que do par metálico, ela é muito utilizada para interligar os diversos switches ou servidores de alta capacidade dentro de uma rede de computadores. A grande vantagem da fibra é sua imunidade às interferências eletromagnéticas e maior largura de banda que o par metálico. Veja a figura a seguir com um switch e suas conexões ópticas.



Ao longo do curso vamos estudar a teoria de redes e as diversas opções para montarmos redes com e sem fio.

### **3 Objetivo e Desafios das Redes de Computadores**

O uso das redes de computadores em corporações tem o objetivo de gerar economia de tempo e maior controle dos processos, ou seja, tornar a organização mais eficiente. Outro ponto importante é a necessidade que as corporações possuem em manter informações em tempo real, tornando a rede não apenas um "artigo de luxo" e sim uma necessidade real para seus negócios poderem fluir da melhor maneira possível.

A maioria das empresas já reconhece que para ter sucesso nos negócios é preciso compartilhar informação e manter uma boa comunicação não apenas internamente, mas também com todo o ambiente externo (clientes, parceiros, governo, etc.). Uma empresa que utiliza redes acaba se tornando mais competitiva, uma vez que sua eficiência interna aumenta.

O uso das redes, em especial da Internet, tem proporcionado novas oportunidades para as empresas e novos mercados são alcançados, permitindo que a empresa ultrapasse barreiras geográficas, atuando não apenas em sua região, mas de forma nacional, regional ou até global.

O avanço das redes permitiu o desenvolvimento de diversas aplicações que atualmente fazem parte do nosso cotidiano, tais como o acesso a banco de dados via Internet como. Por exemplo, o acesso a contas bancárias via InternetBanking, realização de compras de diversos tipos de produtos e serviços através de sites de e-commerce (Comércio Eletrônico), ferramentas de comunicação online como as de chat (Skype, MSN, googletalk, Yahoo messenger), envio e recebimento de correio eletrônico (e-mail) com ferramentas como o Gmail e muitas outras opções e serviços são cada vez mais comuns.

Em um ambiente corporativo a rede permite acesso à cadastros de clientes e fornecedores, banco de dados com os produtos disponíveis, diversos controles de processos como estoque, pedidos de compra, logística e muito mais. Esses sistemas têm diversos nomes padronizados pelas indústrias como ERP, CRM e assim por diante, os quais são os diversos sistemas que podem ser utilizados para administrar os processos de uma corporação de maneira única e muito mais eficiente.

Além disso, em um ambiente corporativo existe ainda o grande desafio da convergência entre os dados e serviços de multimídia, como voz e vídeo, pois atualmente essa é a realidade de uma rede em uma grande corporação e não mais uma tendência, ou seja, ambientes de rede complexos e com cada vez mais dispositivos, diferentes tipos de tráfego e necessidades para serem tratadas pelos elementos de rede.

Uma dica importante para você que está iniciando o curso e também na área de redes é que não adianta apenas entender os dispositivos de rede, como roteadores e switches, também temos que entender as diversas aplicações, suas necessidades em relação à rede e claro, o mais importante, as necessidades dos usuários e do negócio de cada empresa, pois sem pessoas utilizando a rede ela não existe!

*Nesse capítulo iremos estudar os conceitos básicos de redes e suas terminologias.*

*Podemos classificar as redes pela sua abrangência geográfica ou pela sua finalidade e esses termos são frequentemente utilizados por profissionais que atuam na área, portanto estude muito bem esse capítulo.*

*Além disso, faremos uma breve introdução ao modelo de referência OSI e arquitetura TCP/IP.*

*Desejamos a todos bons estudos.*

*Desejamos a todos bons estudos.*

## **Capítulo 02 - Conceitos Básicos de Rede**

### **Objetivos do Capítulo**

Ao final desse capítulo você deverá ser capaz de:

- Definir redes de computadores e protocolos de rede
- Entender a terminologia e classificação das redes de computadores
- Habituar-se à terminologia e camadas do modelo OSI e arquitetura TCP/IP

### **Sumário do Capítulo**

<b>1 Definição de Redes de Computadores e Protocolos de Rede</b>	<b>16</b>
<b>2 Classificação e Terminologia de Redes de Computadores</b>	<b>17</b>
<b>2.1 Classificação das Redes pela Finalidade</b>	
<b>21</b>	
<b>3 Introdução ao Modelo de Referência OSI e TCP/IP</b>	<b>23</b>
<b>3.1 Arquitetura TCP/IP</b>	<b>29</b>

## 1 Definição de Redes de Computadores e Protocolos de Rede

Como já vimos no capítulo anterior, uma Rede de Computadores é um conjunto de dispositivos processadores capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação.

Este sistema de comunicação é composto por elementos ou dispositivos que tem funções bem específicas na rede, tais como os switches que têm a função de dar acesso à rede para os computadores, já os roteadores possuem a função de encaminhar os pacotes IP para os destinos corretos e assim por diante.

Toda essa troca de informação é realizada através de **protocolos**, mas afinal o que é um protocolo? Na ciência da computação ou informática, um protocolo é uma **convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais**. De maneira simples, um protocolo pode ser definido como "as regras que governam" a **sintaxe, semântica e sincronização** da comunicação, ou seja, que controlam essa "**conversa**" entre os dispositivos. Os protocolos podem ser implementados pelo hardware, software ou por uma combinação dos dois.

É bem simples de visualizar a importância dos protocolos de comunicação em rede, imagine você em uma reunião onde diversas pessoas estão sentadas ao redor da mesa querendo expor seus problemas e pontos de vista. Se não houver uma **regra ou protocolo** fica impossível de haver a **comunicação**, concorda? Pois é simples de visualizar que se todos falarem ao mesmo tempo ninguém irá se entender. A função dos protocolos de rede é bem semelhante, porém muito mais complexa e com uma variedade de padrões, os quais vamos estudar os principais.

Falando em termos simples, uma rede precisa dos seguintes protocolos:

1. Que regulem o acesso aos meios físicos (como a família Ethernet com CSMA/CD, PPP, Frame-relay);
2. Que regulem o envio pela rede e endereçamento lógico da rede (representado pelo protocolo IP);
3. Que regulem o envio das informações dentro dos computadores e separem as diversas comunicações (representado pelo TCP e UDP) e
4. Protocolos que forneçam os serviços de rede aos usuários (representado pelo HTTP, FTP, Telnet, DNS e demais serviços que estamos habituados a utilizar).

Você verá ao longo do curso que cada um desses protocolos forma uma pilha que juntos possibilitam a comunicação em rede.

Lembre que o que queremos em uma rede é que uma determinada informação que está em nosso computador atravesse um meio de comunicação e chegue a outro computador ou servidor para ser processado, como isso será realizado são os protocolos que definem.

É muito importante que você entenda esse fluxo de informações e os diversos dispositivos que os pacotes irão passar, veremos isso ao longo do curso.

## 2 Classificação e Terminologia de Redes de Computadores

As redes de computadores podem ser classificadas basicamente de duas maneiras (porém não são as únicas):

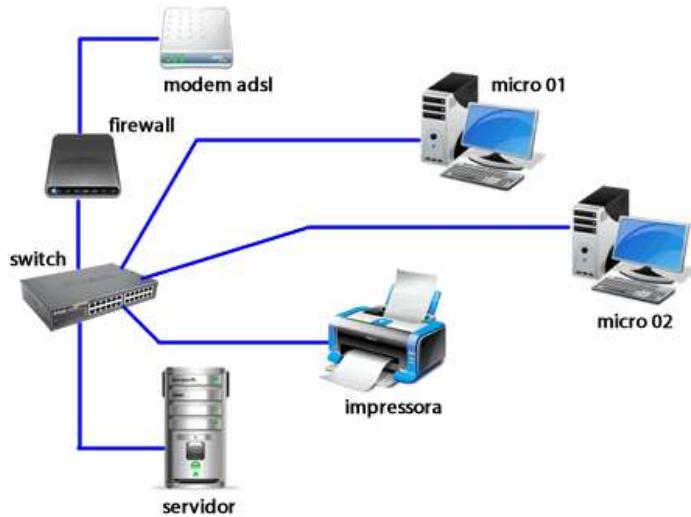
- Quanto a sua abrangência geográfica
- Quanto a sua finalidade

A classificação quanto à abrangência geográfica é a mais comum e que utilizamos em nosso dia a dia de administradores de redes, quem nunca ouviu falar de redes LAN, MAN e WAN? Se você não ouviu fique tranquilo, vamos estudar esses termos e muitos outros na sequência.

### Local Area Network (LAN)

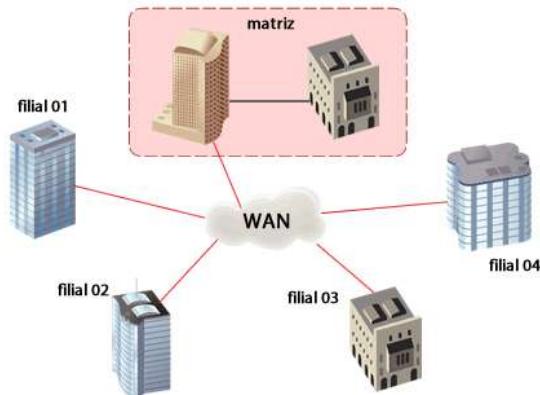
Rede de Área Local (LAN – Local Area Network), ou simplesmente Rede Local, é um grupo de dispositivos processadores interligados em uma rede em um mesmo ambiente. Por exemplo, uma empresa que está situada em duas salas do mesmo prédio, todos os micros e dispositivos de rede interligados formam a LAN dessa empresa.

A LAN é a região onde os usuários finais e seus dispositivos tem acesso aos recursos de rede, normalmente temos computadores, telefones IP, laptops, câmeras IP, catracas biométricas, impressoras de rede, servidores locais como dispositivos de cliente e switches fazendo a conexão deles com a rede.



### Wide Area Network (WAN)

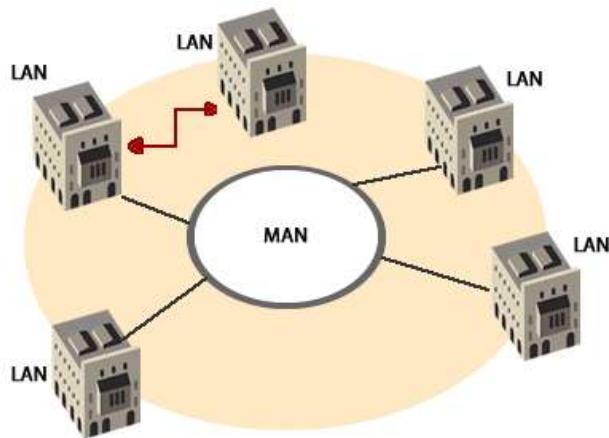
Rede de Longa Distância (WAN – Wide Area Network) é a rede de interligação de diversos sistemas de computadores, ou redes locais, localizados em regiões fisicamente distantes. Normalmente a rede WAN é composta por circuitos ou links adquiridos de uma operadora ou prestadora de serviços de telecomunicações e utilizam os roteadores para fazer a interligação das diversas localidades remotas das empresas.



### Metropolitan Area Network (MAN)

Rede Metropolitana (MAN – Metropolitan Area Network) é uma rede dentro de uma determinada região (normalmente dentro de uma mesma cidade) onde os dados são armazenados em uma base comum, por exemplo, uma rede de um determinado banco ou farmácia dentro de uma mesma cidade.

Normalmente o conceito de WAN e MAN se confundem na prática, pois muitas vezes para interligar escritórios em uma mesma cidade precisamos de links de prestadores de serviços de telecom e esses links são muitas vezes chamados de "links WAN", porém você deve tomar cuidado com essa terminologia e analisar o cenário que você se encontra.

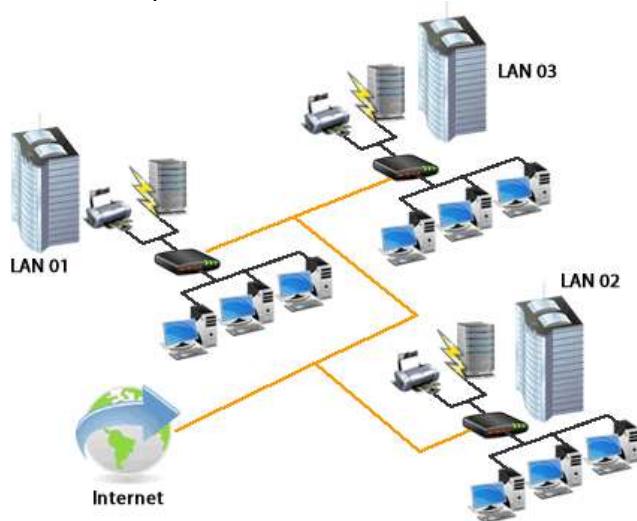


**Campus Area Network (CAN)**

Rede de Campus (CAN – Campus Area Network) é uma rede que compreende uma área mais ampla que uma rede local (porém mesmo assim muitas bibliografias tratam as redes campus como uma LAN), a qual pode conter vários edifícios próximos interligados entre si. O exemplo mais conhecido desse tipo de rede é um Campus Universitário.

Muitas vezes a rede de um campus é tratada tecnicamente como uma LAN por estarem em um mesmo ambiente ou terreno e não utilizarem links de terceiro para fazer a interligação dos prédios ou ambientes.

Veja a figura a seguir onde temos uma empresa com três prédios no mesmo terreno compondo uma rede campus.

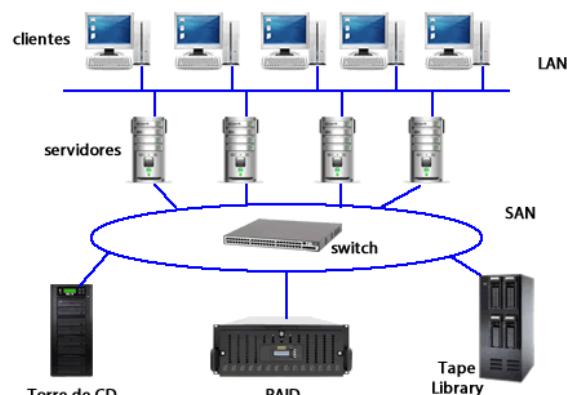


### Storage Area Network (SAN)

Rede de Armazenamento (SAN - Storage Area Network) é uma rede que compartilha uma base de dados comum em um determinado ambiente, normalmente em um **Data Center**. O **Data Center** é um ambiente projetado para abrigar servidores e outros componentes como sistemas de armazenamento de dados (storages) e ativos de rede (switches, roteadores).

O objetivo principal de um Data Center é garantir a disponibilidade de equipamentos que rodam sistemas cruciais para o negócio de uma organização, tal como o ERP ou CRM, garantindo assim a continuidade do negócio.

Veja as figuras abaixo com um exemplo de ambiente de Data Center e com a ilustração de uma rede SAN.



### Personal Area Networks (PAN)

Uma rede PAN, também designadas de redes de área pessoal, são redes que usam tecnologias de rede sem fios para interligar os mais variados dispositivos (computadores, smartphones, etc) numa área muito reduzida.

Veja o exemplo abaixo que ilustra a interligação de um laptop com vários dispositivos via Bluetooth.



## 2.1 Classificação das Redes pela Finalidade

A classificação das redes pela finalidade trata do uso dela, pois uma rede local normalmente faz parte da rede interna da empresa, já quando vamos acessar ao ambiente público ou Internet estamos em outra área da rede, a qual normalmente não pertence mais à empresa, portanto é preciso classificar o uso de cada ambiente.



### Internet

É o conjunto de redes de computadores interligadas pelo mundo inteiro, portanto é uma rede pública. A Internet utiliza a arquitetura TCP/IP e disponibiliza o acesso a serviços de rede disponibilizados ao redor do globo, permitindo a comunicação e troca de informação aos usuários de todo planeta.

### Intranet

É a rede de computadores de uma determinada empresa, baseada também na arquitetura TCP/IP. Fornece serviços aos empregados e permite a comunicação interna da empresa de forma controlada. Normalmente é interligada ao ambiente externo (à Internet) de maneira segura. Também é conhecida como Rede Corporativa.

### Extranet

É um conceito que permite o acesso de funcionários e fornecedores de uma organização aos recursos disponibilizados pela Intranet da empresa. Podemos dizer que é uma extensão da Intranet. Dessa maneira, podemos disponibilizar um padrão unificado entre as diversas empresas, filiais ou parceiros de negócio da corporação.

### VPN (Rede Privada Virtual)

VPN é uma rede virtual estabelecida entre dois ou mais pontos, a qual oferece um serviço que permite o acesso remoto de funcionários ou fornecedores a uma determinada rede, a fim de executarem suas tarefas como se estivessem na rede local da empresa. Este tipo de conexão é utilizada para que funcionários remotos tenham acesso aos e-mails corporativos via Intranet ou para as equipes de suporte técnico solucionarem problemas em seus sistemas de maneira remota. As VPNs são utilizadas também para criar uma rede WAN através da Internet de maneira segura, pois normalmente esse tipo de conexão entre dois pontos é protegido por uma técnica de criptografia, ou seja, mesmo que um hacker capture as informações trocadas entre as duas pontas ele não irá conseguir ler essas informações.

Além das classificações dadas anteriormente você pode ouvir falar de alguns outros termos como:

- **Home-office**: trata-se de um funcionário que trabalha em casa e tem acesso à todos os recursos da Intranet (rede corporativa) através de uma conexão do tipo VPN realizada pela Internet.
- **SOHO ou Small-office / Home-Office**: termo que designa um pequeno escritório ou como já vimos anteriormente um funcionário que trabalha em casa. A rede de uma pequena empresa pode ser muito semelhante a um home-office, pois tem poucos computadores e apenas acesso à Internet. Normalmente envolve de um a dez funcionários.
- **Computação em Nuvem**: Até poucos anos atrás, a computação em nuvens (do inglês “**cloud computing**”) era tida como uma tendência e hoje é uma realidade. A aposta era a de que ninguém mais precisaria instalar programa algum em seu computador para realizar desde tarefas básicas (como mexer com planilhas eletrônicas) até trabalhos mais complexos (edição de imagens e vídeos), pois tudo seria feito pela internet. Um exemplo perfeito de computação em nuvens são os serviços de sincronização de arquivos, como o Dropbox. Com ele, tudo o que você precisa fazer é reservar um espaço do disco rígido, o qual será destinado para o sincronismo nas nuvens, ou seja, ao copiar ou mover um arquivo nesse espaço, ele será duplicado no servidor do aplicativo e também em outros computadores que tenham o programa instalado e nos quais você acesse a sua conta.

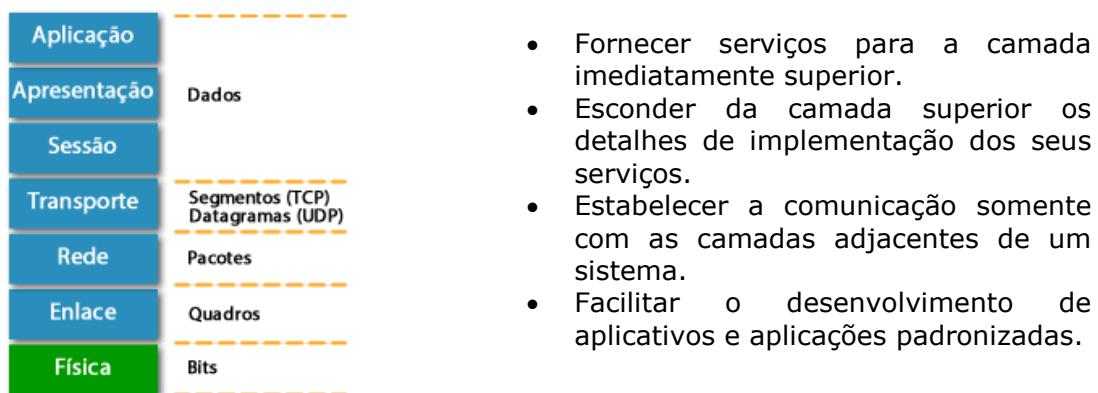
### 3 Introdução ao Modelo de Referência OSI e TCP/IP

Lembre-se do início desse capítulo que toda essa comunicação entre as LANs, WANs, MANs, Internet e demais redes que você deseja interligar é realizada com base em diversos **protocolos de rede** seguindo a arquitetura TCP/IP. Mas de onde surgiram os protocolos de rede? Por que eles foram criados?

Os protocolos surgiram para que a comunicação pudesse ser realizada de maneira eficaz e padronizada, porém no início das redes cada fabricante estava implementando sua comunicação em rede de uma maneira própria, ou seja, com protocolos “proprietários”. Você vai ouvir muito na área de TI a palavra “proprietário”, a qual significa que é de um determinado fabricante e normalmente não consegue interoperar com outros fabricantes diferentes. O oposto são os protocolos abertos, os quais são padronizados por órgãos internacionais como a IETF (Internet Engineering Task Force). Portanto, esse desenvolvimento proprietário causava um problema sério para as empresas e usuários, pois eles ficavam “amarrados” a um determinado fabricante.

Para resolver esse problema foi criado o modelo de referência OSI (Open Systems Interconnection), o qual foi desenvolvido pela ISO (International Standard Organization) com o objetivo de criar uma **estrutura para definição de padrões** para a conectividade e interoperabilidade de sistemas diferentes, ou seja, para que diferentes fabricantes pudessem montar protocolos que fossem **interoperáveis**.

Esse modelo define um conjunto de **7 camadas** (em inglês *layers*) e os serviços atribuídos a cada uma, porém o modelo OSI é uma **referência** e não uma **implementação!** O objetivo resumido de cada camada é:



Agora vamos ver de maneira resumida a função de cada camada. Não se preocupe com o funcionamento e detalhes agora, o objetivo aqui é que você se acostume com a nomenclatura, pois veremos os detalhes mais para frente.

**Camada 1 – Física**

Trata da transmissão transparente de sequências de bits pelo meio físico, sendo a parte final da comunicação, ou seja, onde a transmissão pelo meio de comunicação realmente acontece. Contém padrões mecânicos (conectores, painéis de conexão, cabos, etc.), funcionais, elétricos e procedimentos para acesso a esse meio físico. Nessa camada temos as especificações dos meios de transmissão (satélite, coaxial, radiotransmissão, par metálico, fibra óptica, etc.).

Nas redes mais antigas era aqui na camada física que os computadores eram interconectados utilizando os HUBs, os quais são dispositivos simples que encaminham os bits recebidos para todas as portas simultaneamente. Apesar de não recomendado eles ainda são encontrados no mercado e utilizados em redes domésticas e de pequeno porte pelo seu custo ser extremamente baixo.



**Camada 2 – Enlace**

Esconde características físicas do meio de transmissão para as camadas superiores, pois ele transforma os bits em quadros (frames). Sua principal função é fornecer um meio de transmissão confiável entre dois sistemas adjacentes. Funções mais comuns da camada 2:

- Delimitação e formato dos quadros de bits
- Detecção de erros
- Sequenciamento dos dados
- Controle de fluxo de quadros
- Endereçamento físico (endereço MAC)
- Controle de acesso aos meios físicos

Para redes locais a camada de enlace é dividida em dois subníveis: **LLC (Logical Link Control)** e **MAC (Media Access Control)**, sendo que a LLC faz interface com a camada de rede e o MAC com a camada física.

Os representantes da camada de enlace são as placas de rede, switches e bridges. Nas redes atuais recomenda-se o uso de switches no lugar dos HUBs por questões de desempenho e segurança, pois os switches ao invés de enviar uma informação recebida para todas as portas ele cria um caminho virtual ponto a ponto entre os computadores que estão se comunicando, o que melhora sensivelmente o desempenho e a segurança da rede, pois impede que terceiros consigam espiar o tráfego de rede, **técnica chamada de "sniffing"**.

As informações trocadas pelos protocolos de **camada 2**, tais como o ethernet, fastethernet, PPP, HDL e demais são chamadas de **quadros**.



**Camada 3 – Rede**

Tem a função de fornecer um canal de comunicação independente do meio, pois ela transmite pacotes de dados através da rede utilizando um esquema de endereçamento lógico que pode ser “roteado” através de diversas redes até chegar ao seu destino. As funções características da camada 3 são:

- Tradução de endereços lógicos em endereços físicos (protocolo ARP)
- Esquema de endereçamento lógico
- Roteamento de pacotes
- Não possuem garantia de entrega dos pacotes

Os protocolos de camada 3 utilizados atualmente tanto na Internet como nas Intranets são o IP versão 4 e o IP versão 6 (o IPv6 está sendo aos poucos implementado em diversas redes e na Internet).

As informações trocadas pelos protocolos de camada 3, tais como o IP, são chamadas de **pacotes**.



É importante ressaltar aqui que a comunicação em rede propriamente dita é realizadas pelas camadas 1, 2 e 3. A partir da camada 4 estamos tratando de uma comunicação mais interna dos computadores, pois elas não são utilizadas na rede para o roteamento e envio das informações.

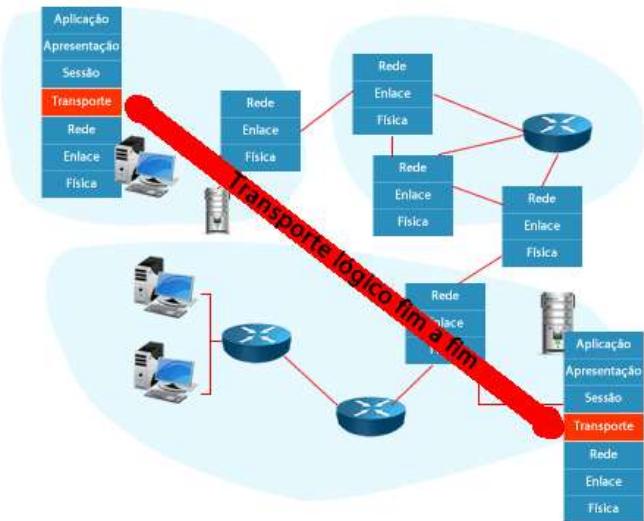
#### Camada 4 – Transporte

Nesta camada temos o conceito de comunicação fim-a-fim. A camada 4 possui mecanismos que fornecem uma comunicação confiável e transparente entre dois computadores, isto é, assegura que todos os segmentos cheguem corretamente ao destino e na ordem correta. Funções da camada 4:

- Controle de fluxo de segmentos
- Correção de erros
- Multiplexação

A camada 4 normalmente é caracterizada pelas especificações do protocolo chamado TCP, o qual é utilizado em aplicações que necessitam de garantia na entrega e controle de fluxo, pois ele é orientado a conexão. Porém existe um segundo protocolo chamado UDP, o qual não é orientado a conexão e utilizado em aplicações que necessitam de velocidade, pois sem tantos controles como o TCP ele acaba sendo naturalmente mais veloz.

Na camada 4 quando falamos do fluxo TCP chamamos as informações de **segmentos**, já o fluxo UDP é chamado de **datagrama**.



#### Camada 5 – Sessão

A camada de sessão tem a função de disponibilizar acessos remotos, estabelecendo serviços de segurança, verificando a identificação do usuário, sua senha de acesso e suas características, por exemplo, seus perfis de usuário. Atua como uma interface entre os usuários e as aplicações de destino, podendo inclusive fornecer sincronização entre as tarefas dos usuários.

#### Camada 6 – Apresentação

A camada 6 é responsável pelas transformações ou traduções adequadas nos dados antes do seu envio a camada de sessão, sendo que essas transformações podem ser referentes à compressão de textos, criptografia, conversão de padrões de terminais e arquivos para padrões de rede e vice-versa. Portanto tem o objetivo de fazer com que os dois lados "falem a mesma língua". Suas funções típicas são:

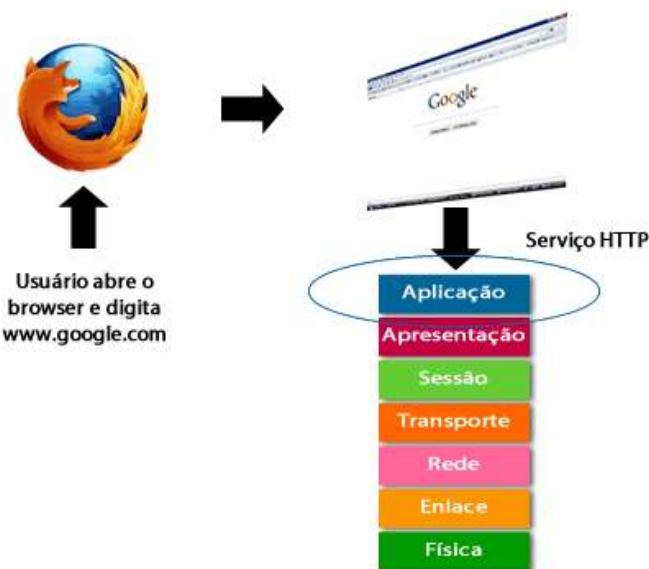
- Formatação de dados
- Compressão e criptografia
- Compatibilização entre aplicações (sintaxe)

### Camada 7 - Aplicação

Esta camada é a mais superior e é responsável pela interface com as aplicações dos computadores (hosts), ou seja, a camada de aplicação tem a função de dar acesso à rede aos aplicativos dos usuários que estão instalados nos computadores. Nessa camada temos os serviços de rede, tais como:

- Serviço de tradução de nomes de Internet: DNS
- Serviços de e-mail: SMTP, POP3 e IMAP
- Serviços de terminal: Telnet e SSH
- Serviços de web: HTTP e HTTPS (seguro)
- Gerenciamento de redes: SNMP
- Acesso a arquivos em rede: FTP e TFTP
- Fornecimento de endereços IP dinâmicos: DHCP

Veja a figura a seguir onde temos um exemplo em que o usuário abre seu web browser e digita [www.google.com](http://www.google.com), portanto a camada que vai fazer interface com o aplicativo é a 7, ou seja, a camada de aplicação vai pegar os dados do usuário e prepará-los para que eles sejam enviados através das camadas e tenham acesso à rede.

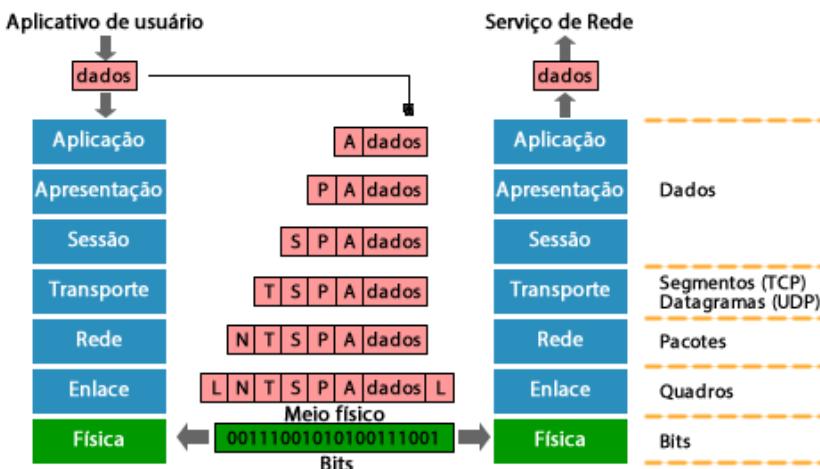


As informações trafegadas entre as camadas de sessão, apresentação e aplicação são chamadas de **dados**.

Portanto, o modelo de referência OSI quebra a rede em pedaços ou fatia a rede para que o desenvolvimento seja mais simples e modular. Cada camada é independente da outra e é como se entre dois hosts houvesse uma conexão camada a camada independentemente uma das outras.

O controle das informações de cada camada é realizado através de uma unidade de protocolo chamada PDU (protocol data unity), as quais são inseridas no início, chamada de "cabeçalho" (em inglês header). Esses cabeçalhos são lidos no destino para que o computador saiba o que fazer com a informação. Nele estão contidos instruções, endereços e demais controles necessários para que a comunicação flua entre os dois computadores.

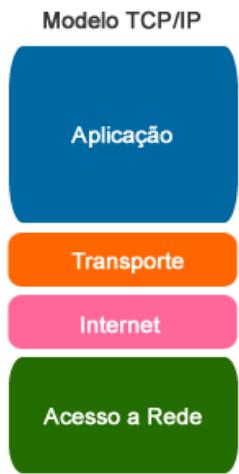
O processo de recebimento dos dados do usuário pela camada 7 até sair em bits na camada 1 é chamado de “encapsulamento”.



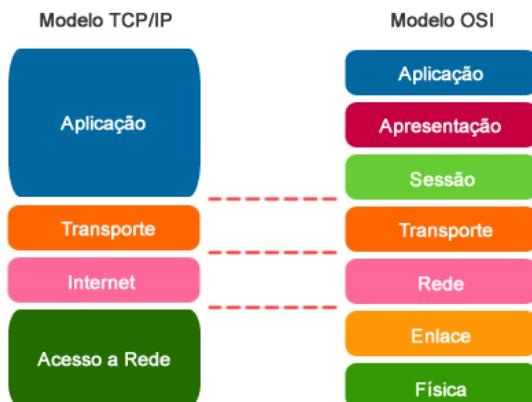
### 3.1 Arquitetura TCP/IP

Apesar do modelo OSI ser uma referência para as redes, pois todos os dispositivos são caracterizados pela sua camada no modelo OSI, a arquitetura TCP/IP é a que foi realmente implementada e está em uso até os dias de hoje, tanto nas redes internas como na Internet.

A arquitetura TCP/IP é composta por 4 camadas (formando a pilha da estrutura do protocolo) conforme mostra a figura abaixo.



Na prática, as camadas 5, 6, e 7 do modelo OSI foram mescladas para formar a camada de Aplicação do TCP/IP. Já as camadas 3 e 4 dos dois modelos são similares, porém a camada 3 do TCP/IP é chamada de Internet. Já as camadas 1 e 2 do modelo OSI foram mescladas no TCP/IP para formar a camada de acesso aos meios ou acesso à rede.



Vamos agora a uma descrição breve de cada camada da arquitetura TCP/IP.

#### **Camada de Acesso à Rede ou Acesso aos Meios**

Esta é a camada inferior da arquitetura TCP/IP tem as funcionalidades referentes às camadas 1 e 2 do Modelo OSI.

#### **Camada Internet**

A camada Internet, também conhecida como de Rede ou Internetwork, é equivalente a camada 3 do Modelo OSI. Os protocolos IP e ICMP (ping) estão presentes nesta camada.

#### **Camada de Transporte**

A camada de Transporte equivale à camada 4 do Modelo OSI. Seus dois principais protocolos são o TCP e o UDP.

#### **Camada de Aplicação**

A camada superior é chamada de camada de aplicação equivalente às camadas 5, 6 e 7 do Modelo OSI. Os protocolos mais conhecidos são: HTTP, FTP, Telnet, DNS e SMTP.

Para finalizar, aqui é importante você entender e se acostumar com a nomenclatura de rede, pois iremos abordar tanto o modelo OSI como o TCP/IP posteriormente. Mas por que é tão importante saber o OSI e TCP/IP? A resposta é simples, para que você conheça os equipamentos de rede e principalmente entenda o fluxo de informações que são trocados entre dois hosts. Somente assim você terá condições de projetar e resolver problemas reais de rede!

*Nesse capítulo iremos estudar os diversos dispositivos e componentes de uma rede de computadores.*

*Lembre que temos os computadores querendo acessar serviços de rede, que estão em diversos servidores, através de um meio de transmissão. Toda essa informação é encaminhada pela rede através dos dispositivos de rede, portanto aqui nesse capítulo vamos nos acostumar com essa nomenclatura e a diversidade de equipamentos de rede.*

*Desejamos a todos bons estudos!*

## **Capítulo 03 - Dispositivos de Redes**

### **Objetivos do Capítulo**

Ao final desse capítulo você deverá ser capaz de:

- Conhecer a terminologia dos diversos dispositivos de redes de computadores;
- Descrever os clientes e servidores de rede;
- Descrever os dispositivos da infraestrutura de redes;
- Descrever os dispositivos que são utilizados para encaminhar as informações em uma rede.

## Sumário do Capítulo

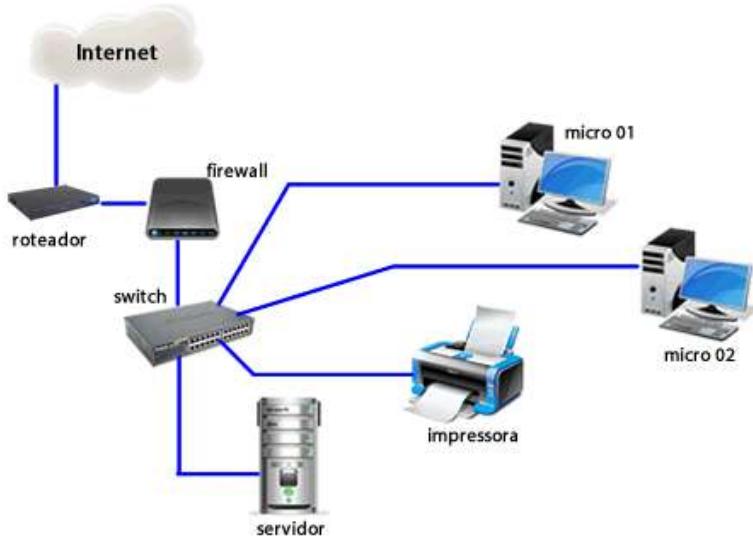
<b>1</b>	<i>Componentes de uma Rede de Computadores</i>	<b>33</b>
<b>2</b>	<i>Dispositivos Finais (Endpoints) – Clientes e Servidores</i>	<b>34</b>
2.1	Computadores	34
2.2	Servidores	37
2.3	Outros Dispositivos Finais	39
<b>3</b>	<i>Componentes da Infraestrutura de Redes</i>	<b>41</b>
<b>4</b>	<i>Dispositivos de Rede</i>	<b>45</b>
4.1	Repetidores	45
4.2	Hub	45
4.3	Conversor de Mídia	46
4.4	Bridge	46
4.5	Switch	48
4.6	Access Point (AP)	49
4.7	Roteador (Router)	50
4.8	Modem e CSU/DSU	51
<b>5</b>	<i>Dispositivos de Segurança de Redes</i>	<b>53</b>
5.1	Firewall	53
5.2	IDS – Sistemas de Detecção de Intrusão	54
5.3	IPS – Sistemas de Prevenção de Intrusão	55
5.4	Aplicativos para Desktops	56

## 1 Componentes de uma Rede de Computadores

Basicamente podemos dizer que temos os dispositivos finais ou endpoints (terminais), os quais são os hosts da rede e podem ser computadores, laptops, telefones IP e muitos outros mais, e o que queremos fazer é interconectá-los entre si ou então com um determinado serviço de rede localizado em um servidor (que também não deixa de ser endpoint).

Um meio de transmissão será utilizado para conectar esses diversos dispositivos e a informação trafegada será encaminhada até seu destino através de dispositivos de redes, tais como Hubs, Switches e Roteadores.

Veja na figura a seguir uma topologia de rede típica de uma empresa de pequeno porte, onde temos dois computadores, uma impressora de rede e um servidor local onde as aplicações e arquivos de rede são armazenados. Eles são interligados entre si por um switch e tem sua saída para Internet através de um serviço de banda larga do tipo DSL (por exemplo, um ADSL). Além disso, temos um firewall para fazer a proteção contra ataques externos.

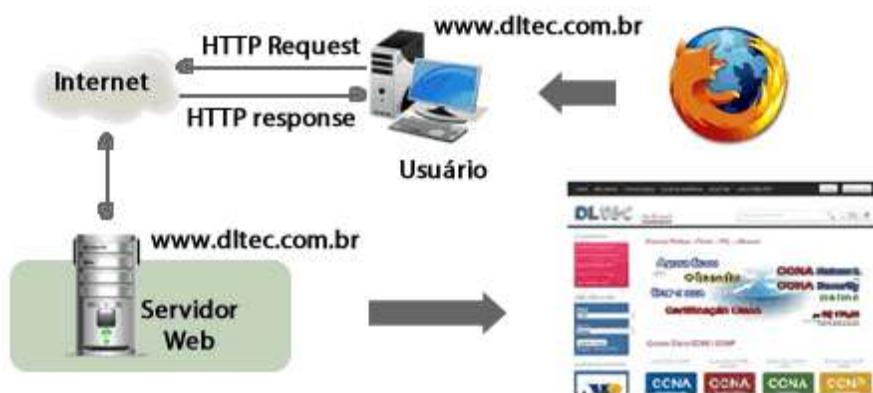


Ao longo desse capítulo estudaremos os diversos equipamentos que podem ser encontrados em uma rede e suas principais funções.

## 2 Dispositivos Finais (Endpoints) – Clientes e Servidores

As redes de computadores têm como dispositivos finais os **hosts**, o qual é um termo genérico assim como **endpoint** (dispositivo final em inglês).

Mais para frente você verá que as redes TCP/IP utilizam uma arquitetura cliente/servidor, ou seja, temos dispositivos clientes (que desejam utilizar serviços de rede) e servidores, os quais prestam os serviços de rede. Um exemplo que utilizamos todos os dias é o serviço de Web (WWW), em nossos micros temos programas chamados **browsers** (como o IE, Mozilla, Google Chrome, dentre outros) e digitamos um nome de site para acessar as informações na tela do nosso computador. Essa informação está contida em um servidor web, máquina com um determinado serviço de rede instalado, nesse caso o HTTP, que provê o conteúdo da página solicitada.



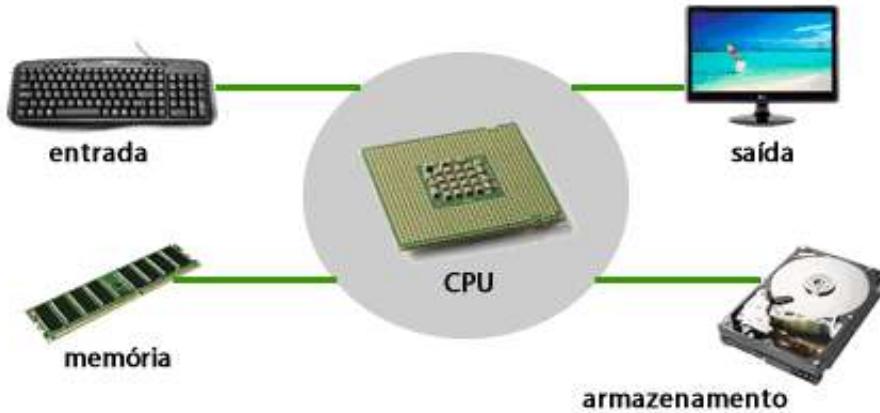
### 2.1 Computadores

Equipamentos utilizados para o processamento de dados que, na visão de rede, podem ser classificados como **estações de trabalho** (clientes ou desktops) e **servidores**, os quais estudaremos em um tópico a parte.

Aqui é importante frisar que o conceito sobre quem é o cliente e quem é o servidor não é fixo, ou seja, em um determinado momento para uma determinada aplicação o computador pode ser considerado como servidor e para outra aplicação ele pode ser considerado como cliente. Mais para frente vamos estudar o assunto sobre aplicações que usam a arquitetura cliente-servidor no capítulo específico sobre TCP/IP.

Mas nesse caso vamos falar mais especificamente sobre os computadores, desktops, laptops e netbooks, os micros utilizados em casa ou nas empresas para as tarefas diárias envolvendo acesso a programas, aplicativos e à Internet e seus mais variados serviços.

Um computador é basicamente composto por **Hardware**, **Software** e **Firmware**. O Hardware de um computador é formado pelos seguintes componentes básicos:



- **Unidade de Processamento:** Composto pelo Processador ou UCP (Unidade Central de Processamento ou CPU – Central Processing Unit - em inglês). A CPU tem papel parecido ao **cérebro** no computador.
- **Unidades de Armazenamento:** Compostas pelas memórias (RAM, ROM, etc.), unidades de disco (Unidades de Disco Rígido ou HD – Hard Disk, também conhecido como Winchester, Unidades de Disco Flexível ou Floppy Disk, Unidades de CD – Compact Disk, Unidades de DVD, etc.).
- **Dispositivos de Entrada e Saída:** Monitor, Teclado, Impressora, Mouse, Plotter, etc.
- **Interface de Rede:** Atualmente podemos ter placas de redes para cabeamento físico ou placas de rede sem fio (wireless). A interface de rede pode ser onboard, ou seja, está integrada na placa mãe ou em uma placa externa USB, PCI ou PCMCIA.

Normalmente as unidades de processamento, armazenamento e muitas vezes a própria interface de rede estão integradas em uma **Placa Mãe**. A placa mãe é a parte do computador responsável por conectar e interligar todos os componentes do computador entre si, ou seja, processador com memória RAM, disco rígido, entre outros. É nela que são conectados todos estes componentes. Existem diversos padrões de placas mãe, cada qual com seu tamanho específico e quantidade de barramentos e conectores.



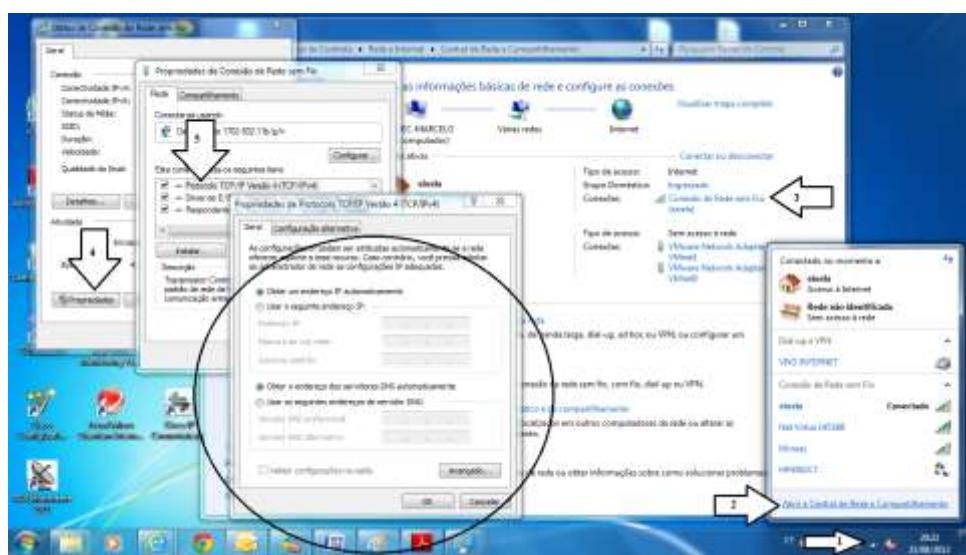
Sobre o **Software** temos basicamente o **Sistema Operacional** e os **Aplicativos**.

O **Sistema Operacional** (OS – Operational System) é um software que permite a utilização da máquina como um todo por outros programas, ativando-a e gerenciando a memória e os dispositivos de entrada e saída, por exemplo. Além disso, ele define o ambiente de trabalho do usuário no computador. É na realidade um conjunto de programas (rotinas) executado pelo processador que estabelece uma interface de contato do usuário com o computador e do computador com o usuário. Exemplos de sistemas operacionais utilizados em computadores de clientes são as diversas distribuições de Linux, Windows e MacOS.

Já o **Firmware** é o programa instalado na memória de inicialização do computador, contendo as instruções básicas para inicialização do computador (BIOS – Basic Input/Output System).

Em termos de redes, que é o nosso foco, a configuração se dá na placa ou interface de rede. A placa de rede é instalada através de um driver e normalmente vem configurada para buscar sua configuração através de um servidor DHCP (Dynamic Host Configuration Protocol), o qual configura dinamicamente os endereços IPs dos clientes em uma rede. Apesar disso, podemos configurar nossas placas de rede manualmente.

Em ambiente Windows 7 você pode clicar no ícone que indica a conexão de rede na barra inferior (1), depois em Abrir a Central de Rede e Compartilhamento (2), logo após clique na conexão de rede desejada (3), depois em Propriedades (4), duplo clique no protocolo TCP/IP versão 4 e pronto, você está na tela de configuração de rede. Essa é uma das maneiras, existem outras formas de chegar à mesma tela. No capítulo de TCP/IP veremos como fazer a configuração de um host de forma manual.



## 2.2 Servidores

Os servidores não são nada mais que computadores normalmente mais “poderosos” que os utilizados em nossas casas, tanto é que você pode instalar aplicações específicas ou ativar recursos do seu sistema operacional e transformar seu computador em um servidor também! Então por que tratar dos servidores separadamente dos computadores?

Porque dependendo do porte da empresa ou do perfil da aplicação a ser utilizada, um computador normal não aguentaria a exigência de processamento e de memória RAM que esse serviço de rede precisaria para operar. Por exemplo, imagine você pegar um computador comum e colocar na Internet hospedando um site famoso como o Google.

Com certeza serão milhares e até milhões de acessos simultâneos que esse site irá receber diariamente e ele, um computador, comum não aguentaria essa carga de solicitações, pois ele não foi projetado para esse fim. Na realidade um serviço desse porte normalmente está espalhado por diversos servidores **virtualizados** em máquinas que compartilham recursos em rede para melhorar a performance do serviço como um todo.

Falando genericamente, um servidor terá um sistema operacional mais poderoso ou preparado para tal finalidade, por exemplo, no caso do Windows existe uma versão para servidor, o **Windows Server**. Já para o Linux existem distribuições que são mais utilizadas em servidores de rede, por exemplo, o **Red Hat** e o **Debian**.

Portanto, apesar da estrutura básica de um computador e um servidor serem as mesmas, o que difere é a **capacidade**. Normalmente o servidor terá um ou mais processadores mais poderosos, uma quantidade de memória RAM maior, capacidade de armazenamento maior ou até utilizar o armazenamento externo através de uma rede SAN utilizando Storages. Além disso, também terá um sistema operacional mais adequado e serviços de rede ou aplicações corporativas instaladas, como por exemplo, serviço de e-mail, web, FTP, sistema de arquivos (file system), serviços corporativos como os ERPs, Bancos de Dados e CRMs, podendo estes serviços estarem em um mesmo servidor ou espalhados em diversos servidores. Essa escolha de **agregar** ou **consolidar** os serviços em apenas um servidor depende do volume de processamento exigido pelas aplicações ou pelo volume de solicitações aos serviços que os clientes irão realizar.

Quando falamos de servidores estamos acostumados a visualizar **máquinas físicas**, porém uma grande parte dos servidores atualmente está em um ambiente **virtualizado**. A **virtualização** é a técnica de **separar aplicação e sistema operacional dos componentes físicos**. Por exemplo, uma máquina virtual possui aplicação e sistema operacional como um servidor físico, mas estes não estão vinculados ao hardware e podem ser disponibilizados onde for mais conveniente.

Com a **virtualização** um dos maiores ganhos é que normalmente muitos servidores implantados pelas organizações são subutilizados e implantando múltiplos servidores em um número menor de servidores físicos, é possível aumentar a utilização média de recursos dos servidores, sendo que ao mesmo tempo diminuindo o número de máquinas. Na maioria das organizações, **consolidar** os servidores com **virtualização de servidores** diminui os gastos com eletricidade, consumo de espaço e etc. O termo **consolidar** aqui significa unificar os serviços em um mesmo ambiente de servidores virtualizados.

Além disso, lembre que quando temos um problema em nosso micro e perdemos nosso HD, por exemplo, temos que reinstalar um sistema operacional, reinstalar os programas, configurá-los e voltar nossos dados, isso se fizemos um backup! Com a virtualização, basta você subir a sua máquina virtual em outro hardware, simples assim.

Em termos físicos, os servidores podem ser gabinetes como os que estamos acostumados com os desktops (chamados de **torre**), de rack ou então em blades (se pronuncia "bleide").

As soluções em torre têm problemas de espaço limitado e precisam de processamento centralizado. Este modelo é recomendado para empresas pequenas que necessitam de apenas um servidor.



Já os servidores em rack já são recomendados para empresas que necessitam de mais de um servidor e tem problemas de espaço ou então precisam de maior capacidade de armazenamento interno.



Os Servidores blade são recomendados para empresas que necessitam de uma capacidade de computação bastante elevada ou para empresas que planejam desenvolver um data center próprio. Com esse tipo de servidor há ganho de espaço, processamento e consumo de energia, porém o custo é bem mais elevado.

Acompanhe na figura abaixo que cada espaço do sub-bastidor você tem uma lâmina ou blade que é na realidade um servidor.



### 2.3 Outros Dispositivos Finais

Além dos computadores e servidores podemos ter vários outros dispositivos que necessitam de acesso aos recursos de rede, pois até os telefones celulares, mais especificamente os smartphones, têm possibilidade de acesso à rede através de uma interface sem fio (wireless).

Portanto abaixo seguem outros dispositivos que vocês podem encontrar como endpoints em uma rede de computadores:

- **Câmeras de segurança IP:** utilizadas para monitorar e gravar o ambiente residencial ou corporativo e tanto a monitoração como o controle é realizado via rede.
- **Dispositivos de VoIP (Telefones IP, ATAs e softphones):** cada vez mais comuns são os sistemas de telefonia IP, onde agora a voz é transmitida pela rede e um PABX ou Central Telefônica IP é que faz a interface e comutação das chamadas internas e externas. Nesses tipos de sistemas temos a central instalada em um servidor ou em um dispositivo proprietário e os endpoints podem ser telefones IP, adaptadores que interligam o mundo convencional com o mundo IP (chamados de ATAs) ou então o telefone IP pode estar instalado nos computadores dos usuários através de um aplicativo, o qual recebe o nome de softphone ou telefone por software.
- **Smartphones e Tablets:** cada vez mais utilizados no mundo corporativo são os smartphones e os tablets, os quais permitem o uso pessoal ou então acesso aos recursos da empresa, tais como serviços de e-mail, banco de dados e sistemas corporativos. Aqui normalmente o acesso é realizado através da rede sem fio (wireless).

- **Thin Clients:** em português, o "cliente magro" é um computador cliente em uma rede de modelo cliente-servidor de duas camadas o qual tem pouco ou nenhum aplicativo instalado, ou seja, ele depende primariamente de um servidor central para o processamento de atividades. A palavra "thin" (magro) se refere a uma pequena imagem de boot que tais clientes tipicamente requerem - talvez não mais do que o necessário para fazer a **conexão com a rede** e **iniciar um navegador web** dedicado ou uma conexão de "**Área de Trabalho Remota**" tais como X11, Citrix ICA ou Microsoft RDP.
- **Aparelhos de Vídeo Conferência:** utilizados para comunicação de voz e áudio entre diferentes localidades de uma mesma empresa ou até entre empresas parceiras. Tanto a telefonia IP ou VoIP como a vídeo conferência necessitam de recursos e configurações especiais na rede, tanto no que se refere à largura de banda suficiente como aos requisitos de qualidade de serviços (QoS).
- **Sistemas de Catracas Eletrônicas ou Biométricas:** muitas empresas utilizam um sistema de liberação de acesso a determinadas áreas, assim como ponto eletrônico com cartões magnéticos ou até mesmo com recursos de biometria (leitura de impressão digital, por exemplo). Para isso, na maioria dos casos, essas catracas estão interligadas via rede IP com um sistema de autorização e registro de entrada e saída dos funcionários a um servidor.



Citamos aqui os mais relevantes, porém com o avanço tecnológico mais e mais dispositivos surgem, os quais com necessidades específicas de acesso à rede e seus serviços. Esse é o maior desafio de uma rede, o de manter-se atualizada e suportar os diferentes requisitos de cada sistema, aplicação ou dispositivo!

Aqui vamos abrir um parêntese para outra questão que tem se tornado um desafio constante que é a **segurança**. A cada dia surgem novos dispositivos e os usuários acabam trazendo para a empresa esses equipamentos. É muito comum funcionários terem um computador corporativo e trazerem também seu iPad, por exemplo, ou então um smartphone com capacidades de rede.

Como dar acesso à rede ou à Internet para esses dispositivos de maneira segura é o grande desafio. Esta é uma prática que está se tornando cada vez mais comum nas empresas e foi até criado um termo para designá-la no mundo corporativo: “**BYOD**”, que significa “**Bring Your Own Device**”, traduzindo “**Traga seu próprio equipamento**”. Tem-se notado que com o avanço dessa prática, a produtividade dos funcionários aumentou, porém ela também pode trazer vários riscos de segurança que devem ser avaliados e tratados antes da sua adoção no dia a dia de grandes corporações.

### 3 Componentes da Infraestrutura de Redes

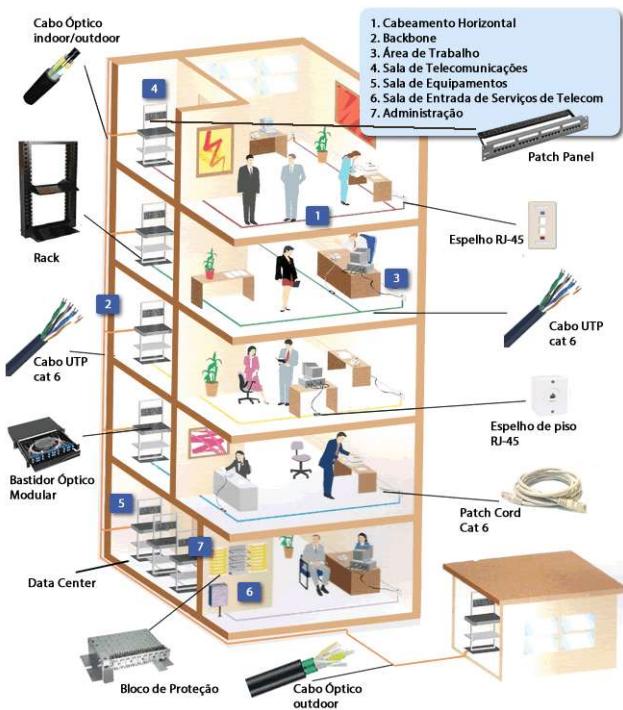
Agora que já vimos os principais dispositivos que necessitam de acesso às redes temos que conectá-los, plugá-los, dar acesso a esses dispositivos a essa rede, para isso precisamos de uma **infraestrutura** de redes.

Portanto, a infraestrutura é o recurso básico para **utilização** e **interligação** dos componentes de uma rede.

O primeiro aspecto de uma infraestrutura é o **meio físico** que você irá utilizar para que os dispositivos se conectem na rede, pois é através dele que iremos estabelecer a forma de interconexão entre os componentes da rede. Podemos dividir os meios físicos de rede entre físico, feito através de um cabeamento metálico ou óptico, ou através do ar, ou seja, transmissão sem fio ou wireless.

Normalmente você irá ouvir para o cabeamento físico o termo “**cabeamento estruturado**”, pois existem normas e recomendações para a montagem e organização da infraestrutura física de uma rede que devem ser seguidas para que você tenha o máximo desempenho e qualidade para interligar os diversos equipamentos.

Basicamente nessa rede temos um cabeamento que vai dos endpoints até os switches e Hubs nas salas de telecomunicações chamado de “**cabeamento horizontal**” e também a interligação entre os equipamentos de rede chamado “**cabeamento vertical**” ou “**backbone**”.

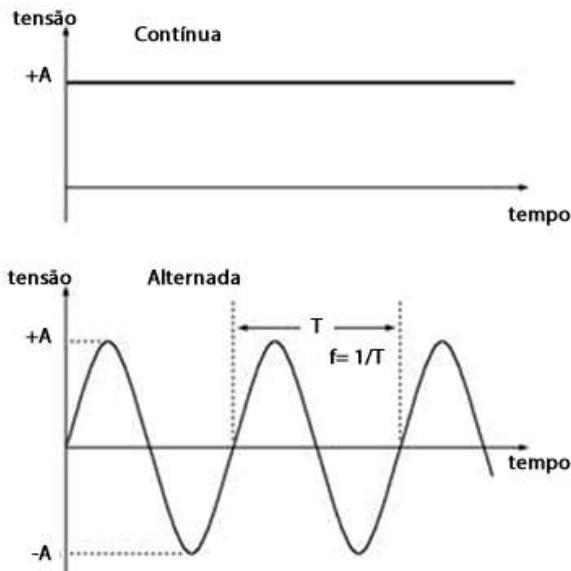


Na infraestrutura física não temos somente os cabos e seus conectores, mas para frente ainda nesse curso iremos estudar que para montar a rede física podemos precisar também de:

- **Guias e Canaletas:** para passar os cabos de maneira organizada e deixá-los fixos.
- **Patch Panel:** para fazer a terminação dos cabos e possibilitar a interligação mais fácil dos cabos de rede com os switches e hubs. Normalmente podem ser de 12, 24 ou 48 portas.
- **Tomadas de Telecomunicações:** para que os cabos não fiquem soltos na mesas e com risco de quebrar. As tomadas de telecom também podem ser chamadas de espelhos.
- **Racks:** para afixar e acomodar os dispositivos de rede ou servidores em salas de telecomunicações ou data centers.
- **Cabos:** podemos ter par metálico (UTP e STP) ou fibra óptica. Os cabos UTP são utilizados tanto para conectar os usuários como os dispositivos de rede, já as fibras ópticas são mais utilizadas na interligação dos equipamentos de rede, chamado de backbone. O cabeamento dos usuários é chamado de cabeamento horizontal.
- **Patch cords ou patch cables:** os cabos utilizados para ligar das tomadas de telecomunicações para os desktops ou então dos patch panels aos switches ou roteadores.
- **Organizadores de Cabos:** utilizados para evitar o “emaranhado” de cabos soltos entre os dispositivos de rede, tais como switches, e os patch panels.

Já em uma rede sem fio precisamos de um equipamento que converta o sinal elétrico em um sinal eletromagnético que será enviado pelo ar através de uma antena, esse equipamento recebe o nome de **ponto de acesso** ou **Access Point** (AP). Trataremos posteriormente as redes sem fio e suas características.

A alimentação é outro ponto importante em um projeto de redes, pois precisamos energizar os equipamentos de rede. Essa energização pode ser realizada por corrente contínua, através de baterias ou pilhas, ou então por corrente alternada, através da rede elétrica, o que é o mais comum em redes domésticas ou corporativas. A corrente alternada é mais comum em ambientes de prestadores de serviço de telecomunicações.



Além disso, quando falamos de alimentação temos que pensar em o que iremos fazer se cair a energia elétrica do prédio?

Para isso existem os nobreaks ou UPS (Uninterruptible Power Supplies – Fonte de Alimentação Ininterrupta) que fornecem energia por um tempo limitado, ou seja, enquanto durar sua bateria.

Existem sistemas de vários portes, desde para o uso doméstico até sistemas de proteção que utilizam bancos de baterias gigantescos para garantir o funcionamento de redes em grandes empresas.

Outra opção, porém muito mais cara e mais utilizada em Data Centers são os geradores a diesel. Veja na figura a seguir a foto de um nobreak, note que você irá ligar a rede elétrica nele e os dispositivos de rede nessas tomadas que estão na parte traseira, portanto enquanto houver uma queda na energia elétrica os dispositivos ligados às tomadas do nobreak serão alimentados pela energia das baterias contidas neles por um tempo limitado.



Vale ressaltar aqui a tecnologia chamada Power over Ethernet ou simplesmente PoE, a qual permite que a alimentação seja enviada no mesmo cabo de rede que chega até um endpoint (por exemplo, um telefone IP) ou dispositivo de rede como um Access Point (ponto de acesso wireless). Assim você não precisa se preocupar em ter um ponto de alimentação para esses tipos de dispositivos, economizando com a infraestrutura elétrica e melhorando o aspecto visual, pois é menos uma tomada e fonte de alimentação para esconder. O PoE pode ser fornecido diretamente pelos switches com suporte à essa tecnologia ou então por patch panels PoE.

Outro ponto importante é a temperatura e a umidade do ar do ambiente onde os dispositivos serão instalados. Todos os fabricantes informam em seus prospectos (data sheet) os limites de temperatura e umidade do ar que os equipamentos suportam e isso deve ser levado em conta ao montar a sua infraestrutura.

Outros recursos e tecnologias que podem ser utilizadas na montagem de uma infraestrutura física são:

- **Piso elevado:** a montagem do piso com placas elevadas em uma estrutura metálica para que o cabeamento seja passado de maneira escondida por debaixo dessa estrutura. O piso elevado é muito comumente encontrado em salas de telecomunicações ou nos CPDs das empresas, apesar de que pode ser utilizado no ambiente corporativo para melhorar o aspecto visual das salas.



- **Sistemas Supressores de Incêndio:** realizado por meio de descarga de gás ou aerossol que possui efeito supressor de combustão ou redução de oxigênio, recomendado para o interior de ambientes críticos.
- **Sistemas de Ar-Condicionado:** para garantir a temperatura e umidade relativa do ar.
- **Sistemas de Controle de Acesso:** tais como catracas biométricas ou com cartões para controlar o acesso de pessoas aos ambientes de rede.

Portanto, em um projeto da estrutura física para acomodar os computadores e os dispositivos de rede, devemos planejar e adequar o ambiente de acordo com as funções dos equipamentos, levando em consideração diversos pontos, dentre eles podemos destacar:

- Espaço físico que será ocupado?
- Onde os dispositivos de rede serão acomodados? O aspecto visual atualmente é importante.
- Qual o mobiliário adequado (bastidores / racks, móveis de escritório, como o cabeamento será passado – canaletas aparentes ou embutidas, etc.)?
- Quais as exigências de temperatura e umidade para a sala onde os dispositivos de rede irão ser acomodados?
- Como será o acesso físico aos equipamentos?
- Como será realizada a energização dos equipamentos?
- Proteção contra falha no fornecimento de energia será necessária?
- Será necessário acesso sem fio? Se sim, qual a cobertura necessária?

Aqui nesse tópico procuramos citar a maioria dos componentes de uma rede física e suas tecnologias, porém existem mais opções dependendo do ambiente e porte da sua rede. Por exemplo, para Data Centers existem soluções de mercado muito específicas para tratar da infraestrutura. Vale lembrar que voltaremos a tratar do assunto no capítulo 9, porém com mais detalhes de projeto e instalação de ambientes de pequeno e médio porte, aqui é apenas uma introdução.

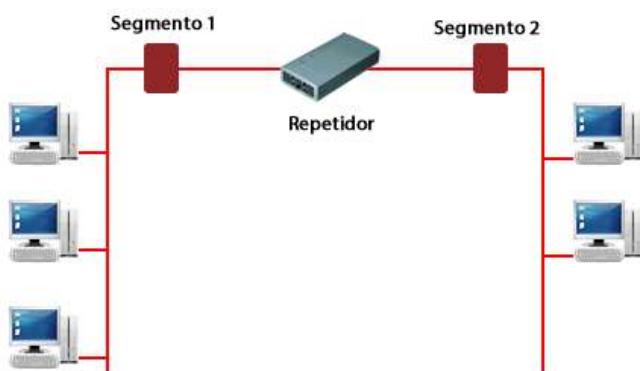
## 4 Dispositivos de Rede

Agora que nossos computadores, servidores, telefones IP e demais endpoints estão conectados à rede via cabo ou então pela rede sem fio (wireless) precisamos encaminhar as informações que eles desejam trocar através da rede e isso é realizado pelos “**dispositivos de rede**”.

Os dispositivos de rede são classificados de acordo com a sua funcionalidade e pela camada do modelo OSI que ele atua. Abaixo seguem os elementos de rede mais importantes:

### 4.1 Repetidores

Os repetidores (repeater) são dispositivos usados para estender as redes locais além dos limites especificados para o meio físico utilizado nos segmentos. Por padrão o limite de um cabo UTP a 10 ou 100Mbps é de 100 metros. Os repetidores operam na camada 1 (Física) do modelo OSI e copiam bits de um segmento para outro, regenerando os seus sinais elétricos.



### 4.2 Hub

Os Hubs (concentradores) são os dispositivos que trabalham na camada 1 (Física) do modelo OSI e substituem os repetidores, pois são repetidores com múltiplas portas. Eles são dispositivos usados para interligar vários equipamentos em rede. Assim como os repetidores os hubs replicam os bits para todas as portas, sendo muitas vezes comparado a um “curto circuito”, pois quando um micro envia uma informação todos os demais recebem, mesmo não sendo o destino daquela informação.



Atualmente tanto os hubs como os repetidores caíram em desuso e foram substituídos pelos switches.

#### 4.3 Conversor de Mídia

Atualmente para estender uma rede em uma distância acima do padrão utilizamos os conversores de mídia ao invés dos repetidores, os quais transformam o sinal elétrico em um sinal óptico que tem a capacidade de ir bem mais longe que o cabo metálico.

Veja a figura a seguir e note que o conversor de mídia possui uma entrada UTP em RJ-45 para você conectar a rede e do outro lado uma interface óptica com um ou dois conectores, dependendo do modelo do equipamento. Na outra ponta você conecta a fibra e retira o sinal elétrico como se estivesse conectado diretamente ao seu switch local.



#### 4.4 Bridge

São dispositivos que operam na camada 2 (Enlace) do modelo OSI e servem para conectar duas ou mais redes formando uma única rede lógica e de forma transparente aos dispositivos da rede. As redes originais passam a ser referenciadas por segmentos. As bridges foram criadas para resolver problemas de desempenho das redes. Elas resolveram os problemas de congestionamento nas redes de duas maneiras:

- Reduzindo o número de colisões na rede, com o domínio de colisão.
- Adicionando banda à rede, pois como são menos computadores disputando o meio sobra mais banda para todos.

Como as bridges operam na camada de enlace, elas "enxergam" a rede apenas em termos de endereços de dispositivos (MAC Address), ou seja, elas tomam suas decisões "aprendendo" o endereço MAC dos dispositivos que estão em cada um dos segmentos de rede. Uma vez aprendido os endereços MAC, quando um dispositivo do segmento A quer falar com outro do segmento B a bridge deixa o quadro cruzar de um segmento para o outro. Agora, quando dois dispositivos do segmento A querem se comunicar ele filtra essa informação e não envia para o segmento B.



As bridges são transparentes para os protocolos de nível superior, o que significa que elas transmitem os "pacotes" de protocolos superiores sem transformá-los. As bridges são dispositivos que utilizam a técnica de store-and-forward (armazenar e encaminhar), ou seja, ela armazena o quadro (frame) em sua memória, compara o endereço de destino em sua lista interna e direciona o quadro para uma de suas portas. Se o endereço de destino não consta em sua lista o quadro é enviado para todas as portas, exceto a que originou o quadro, isto é o que chamamos de flooding (inundação), no caso da bridge conhecer o endereço MAC de destino ela faz o processo mencionado no parágrafo anterior.

#### 4.5 Switch

Os switches (comutadores) também operam na camada 2 (Enlace) do modelo OSI e executam as mesmas funções das bridges, com algumas melhorias.

Os switches possuem um número mais elevado de portas, por isso são consideradas bridges multiporta. Além disso, os switches podem operar em outras camadas do modelo OSI além da camada 2, por exemplo, existem switches layer 3 que atuam ao mesmo tempo como roteador e switch, fazendo além da comutação dos quadros de camada 2 também o roteamento dos pacotes IP através da rede.

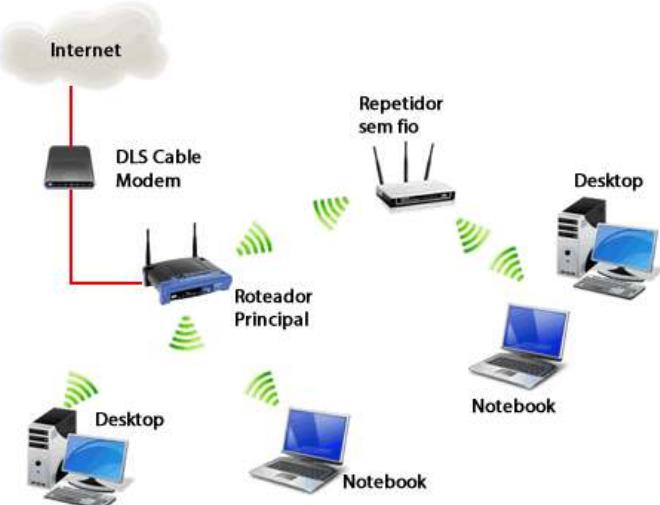


Uma diferença básica entre os switches e as bridges é que eles fazem o encaminhamento baseado em hardware e as bridges são baseadas em software, o que as tornam mais lentas que os switches.

#### 4.6 Access Point (AP)

Um Access point ou ponto de acesso é um dispositivo que permite interligar duas redes sem fio entre si ou uma rede a vários dispositivos em um mesmo ambiente. Em geral, o access point se conecta a uma rede cabeada e fornece acesso sem fio a esta rede para dispositivos móveis no raio de alcance do sinal de rádio.

Portanto, o AP se conecta a rede cabeada e serve de interface entre os dispositivos com placa de rede sem fio até os demais dispositivos de rede. Existem vários padrões de rede sem fio, chamadas também de wifi, que são baseadas nas recomendações do 802.11. Temos atualmente o 802.11a, 802.11b, 802.11g e 802.11n, sendo que cada uma dessas tecnologias tem uma característica de velocidade, alcance e tecnologia. Veja a figura abaixo onde temos um roteador sem fio e um repetidor fornecendo acesso wireless aos computadores de um pequeno escritório.



#### 4.7 Roteador (Router)

O Roteador é o equipamento que opera na camada 3 (Rede) do modelo OSI e permite a conexão entre diferentes redes locais (LAN) ou entre duas ou mais redes locais que estão distantesumas das outras através de uma rede de longa distância (WAN). Suas principais funções são:

- Filtrar e encaminhar os pacotes IP
- Determinar as melhores rotas para redes de destino
- Servir como interface entre diferentes tipos de redes, atuando como um gateway



Quanto a sua forma de operação, as rotas são determinadas a partir do endereço de rede do computador de destino através da consulta de uma **tabela de roteamento**. Essas tabelas são atualizadas utilizando-se informações de roteamento e por meio de algoritmos de roteamento (protocolos de roteamento dinâmicos) ou mantidas através de rotas criadas pelos próprios administradores de redes, chamadas rotas estáticas. Essa é a função principal de um roteador, ou seja, **rotear** ou **encaminhar os pacotes** através da rede.

Estamos acostumados em nossas casas com os roteadores ADSL ou roteadores sem fio, os quais são dispositivos de pequeno porte e que apenas servem para conectar a nossa LAN à Internet.

Já em ambientes corporativos os roteadores podem assumir outros papéis, atuando como gateways e servindo como ponto de conexão de diferentes tipos de interfaces e tecnologias. Por exemplo, uma empresa que utiliza telefonia IP normalmente precisa, além dos canais de voz que trafega via rede, de uma conexão com a rede pública de telefonia convencional (POTS). Isso pode ser realizado por um roteador, que nesse caso recebe o nome de gateway de voz. Nesse mesmo roteador iremos conectar a LAN, a WAN e a rede de telefonia pública através de diferentes interfaces!



Os roteadores desse tipo são chamados também de “**multisserviço**”, pois além de rotear podem fornecer outros tipos de serviço de rede, tais como Voz, Vídeo, atuar como um AP através de uma interface sem fio, ter possibilidade de conexão de placas para servidores virtualizados, correio de voz e muito mais, tudo isso em apenas um equipamento.

#### 4.8 Modem e CSU/DSU

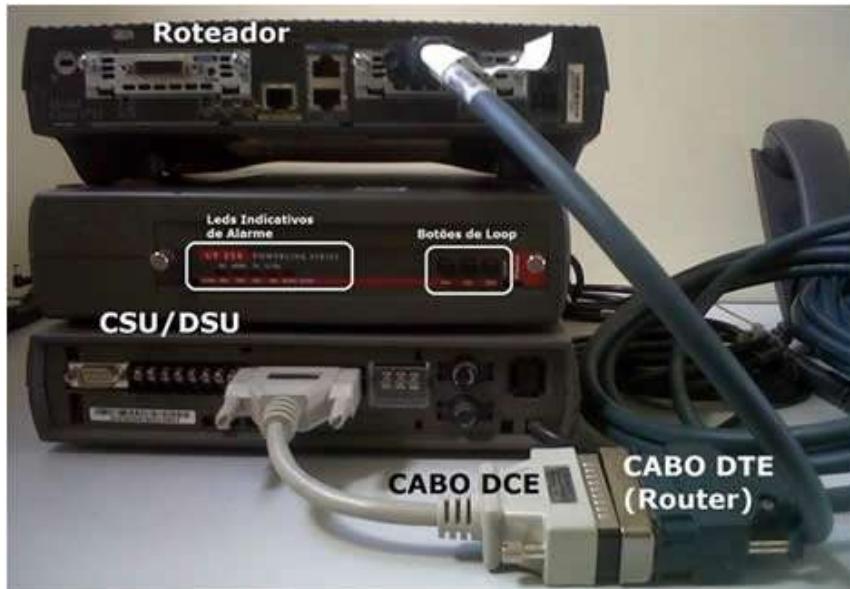
O modem é o dispositivo eletrônico utilizado para a conversão entre sinais analógicos e digitais. A palavra tem como origem as funções de **modulação** e **demodulação**. São geralmente utilizados para estabelecer a conexão entre computadores e redes de acesso através de linhas discadas, ou seja, utilizando a linha telefônica convencional.



Os modems analógicos atualmente são utilizados para acesso remoto a dispositivos de rede ou então como backup discado de redes remotas para serviços essenciais e de baixa velocidade, muito utilizado até os dias de hoje em caixas automáticos de bancos (ATMs).

No Brasil utilizamos também a palavra modem para designar os **modems digitais** que as operadoras de telecom utilizam para entregar seus circuitos de dados. Esses modems utilizam tecnologias da família xDSL tais como HDSL, SHDSL, MSHDSL e outras tecnologias que diferente do ADSL são simétricas, ou seja, tem a mesma velocidade de upload e download de dados.

Você vai encontrar em algumas bibliografias o modem digital desse tipo chamado de CSU/DSU (Channel Service Unit/Data Service Unit - Unidade de Serviço de Canal/Unidade de Serviço de Dados). Veja a figura abaixo onde temos um CSU/DSU conectado a um roteador.



## 5 Dispositivos de Segurança de Redes

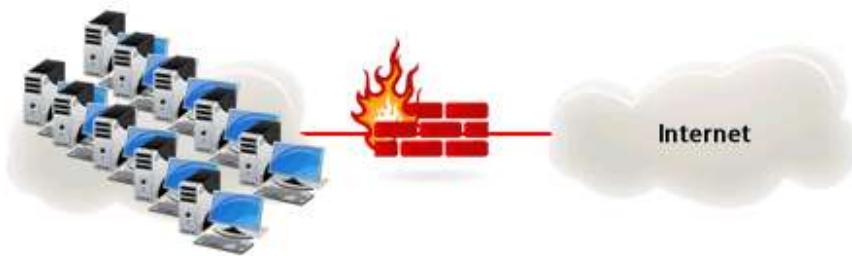
Os dispositivos de segurança de rede visam não somente evitar ataques externos como também podem evitar que ameaças internas aconteçam nas redes. Por exemplo, limitando acesso a sites da web que sejam de conteúdo suspeito ou que um vírus entre na sua rede.

O dispositivo mais conhecido e que já está presente em muitos dos sistemas operacionais dos computadores atualmente são os firewalls. O IDS e IPS são sistemas mais avançados que os firewalls e acabam trabalhando em conjunto com eles para minimizar as ameaças de rede.

Além disso, é aconselhável que os computadores dos usuários e servidores tenham aplicativos especiais para evitar ataques, invasões e vírus. Vamos agora estudar um pouco mais de cada um dos dispositivos.

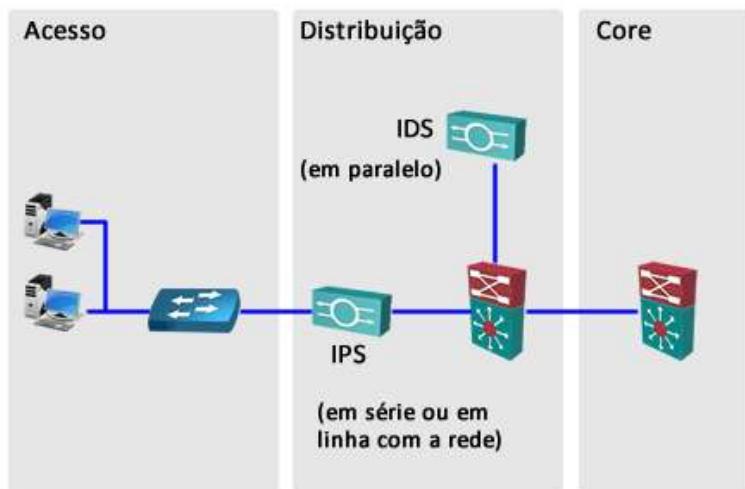
### 5.1 Firewall

Firewall (em português: muro corta-fogo) é o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.



## 5.2 IDS – Sistemas de Detecção de Intrusão

O IDS (em inglês: Intrusion Detection System) é uma ferramenta utilizada para detectar ataques ou invasões, o qual pode ser um software ou dispositivo que utiliza meios técnicos de descobrir quando uma rede está sofrendo acessos não autorizados que podem indicar a ação de um cracker ou até mesmo funcionários mal intencionados. Ele se baseia em “assinaturas” de ataque para detectar uma intrusão.

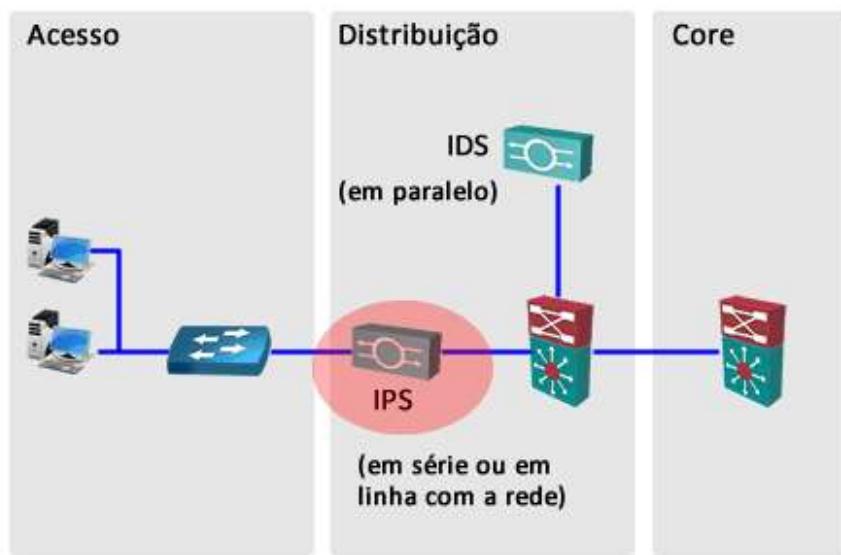


Os IDSs são ligados em paralelo com a rede, escutando todo o tráfego e emitindo alertas para os administradores de rede. Aqui vem “o segredo”, descobrir o que é realmente uma invasão ou não. Pode ocorrer uma invasão e ela não ser detectada, o que é chamado de um falso negativo ou então um determinado tráfego ser considerado perigoso e na realidade ser normal, o que é chamado de falso positivo. Esses princípios são válidos tanto para o IDS como para o IPS.

### 5.3 IPS – Sistemas de Prevenção de Intrusão

Em linhas gerais a função do IPS é ser um dispositivo de segurança de rede que monitora o tráfego e/ou atividades dos sistemas em busca de comportamentos maliciosos ou não desejáveis em tempo real, com a finalidade de bloquear ou prevenir essas atividades. Um IPS baseado em rede, por exemplo, vai operar em linha para monitorar todo o tráfego em busca de códigos maliciosos ou ataques.

Quando um ataque é detectado, é possível bloquear os pacotes danosos enquanto o tráfego normal continua seu caminho.



As tecnologias IDS e IPS utilizam **assinaturas** para detectar desvios de padrões de tráfego na rede. Uma assinatura é um conjunto de regras que um IDS ou IPS utiliza para detectar uma atividade intrusiva, ou seja, cada ataque tem uma característica as quais são mapeadas e armazenadas em um banco de dados de assinaturas e comparadas com o tráfego entrante. Caso o tráfego malicioso tente entrar na rede e será detectado e o IPS pode tomar uma ação conforme configurado pelo administrador de rede, sendo desde emitir um alarme até bloquear aquele tráfego.

Os IPSs e IDSs de grande porte são equipamentos caros e de difícil operação, porém atualmente vários fabricantes estão desenvolvendo soluções de IPS/IDS para empresas de pequeno porte, os quais são uma opção bastante interessante pela possibilidade de evitar que os usuários baixem arquivos com vírus e trojans para dentro da rede.

#### 5.4 Aplicativos para Desktops

Este é um assunto “manjado”, mas vale a pena repetir! Nos computadores dos usuários, assim como em servidores, é importante que tenhamos instalados e sempre atualizados softwares antivírus e antispyware. Além disso, em sistemas operacionais como o Windows deixar habilitado o firewall nativo da máquina.

O **antivírus** é um software responsável pela detecção, desinfecção e remoção de pragas digitais como vírus, trojans (cabalos de tróia), worms e qualquer outro tipo de código malicioso, não se limitando somente aos vírus como o nome sugere. Alguns antivírus também removem adwares e spywares, tarefa antes reservada apenas aos antispywares.

Um **antispyware** é um software de segurança que tem o objetivo de detectar e remover adwares e spywares. A principal diferença de um antispyware de um antivírus é a classe de programas que eles removem. Adwares e spywares são consideradas áreas “cinza”, ou seja, nem sempre é fácil determinar o que é um adware e um spyware. Adwares são desenvolvidos por empresas de publicidade que geram milhões de lucro e que já processaram empresas que fabricam antispyware por removerem seus softwares das máquinas dos usuários.

Existem vários exemplos dos dois softwares, tais como Norton, Symantec, Trend Micro e muitos outros com versões pagas e gratuitas.



*Nesse capítulo iremos estudar com mais detalhe o modelo de referência OSI e arquitetura TCP/IP.*

*Lembre que apesar da implementação prática ter sido realizada com o TCP/IP, o modelo OSI acaba sendo uma referência para a classificação e posicionamento dos equipamentos em uma rede. Além disso, o modelo de referência OSI ele serve como referência para os testes e resolução de problemas em ambientes de rede.*

*Nesse capítulo você também irá estudar os principais integrantes da pilha de protocolos do TCP/IP e entender como se dá o fluxo de informações em uma rede IP, pois isso é fundamental para qualquer estudante que deseja seguir uma carreira na área de redes!*

*Desejamos a todos bons estudos.*

## **Capítulo 4 - Modelos OSI e TCP-IP**

### **Objetivos do Capítulo**

Ao final desse capítulo você deverá ser capaz de:

- Compreender cada camada do modelo OSI, sua aplicação e dispositivos;
- Entender e descrever o processo de encapsulamento de dados tanto no OSI como no TCP/IP;
- Compreender cada camada da arquitetura TCP/IP, sua aplicação e dispositivos;
- Descrever o fluxo de informações dentro de uma rede da origem ao seu destino através de redes LAN e WAN.

## Sumário do Capítulo

<b>1</b>	<b>Modelo de Referência OSI</b>	<b>59</b>
1.1	Camada 1 – Física	59
1.2	Camada 2 – Enlace	63
1.3	Camada 3 – Rede	69
1.4	Camada 4 – Transporte	73
1.5	Camadas 5, 6 e 7 – Sessão, Apresentação e Aplicação	74
1.6	Processo de Encapsulamento e Desencapsulamento de Dados	76
<b>2</b>	<b>Arquitetura TCP/IP</b>	<b>79</b>
2.1	Camada de Acesso à Rede ou Acesso aos Meios	79
2.1.1	Ethernet 10BASE-T	80
2.1.2	Fastethernet – 100 Mbps	81
2.1.3	Gigabit Ethernet – 1.000 Mbps	82
2.1.4	Ethernet 10 Gigabit	83
2.2	Camada Internet	83
2.2.1	ICMP (Internet Control Message Protocol)	86
2.2.2	ARP e RARP	88
2.2.3	Protocolos de Roteamento	92
2.3	Camada de Transporte	93
2.3.1	Protocolo TCP	98
2.3.2	Protocolo UDP	101
2.4	Camada de Aplicação	102
2.4.1	Serviços de Acesso a Páginas de Web – HTTP e HTTPS	103
2.4.2	Serviço de Resolução de Nomes da Internet – DNS	107
2.4.3	Serviços de Compartilhamento de Arquivos na Web – FTP, TFTP e SFTP	112
2.4.4	Serviços de E-mail – SMTP, POP3 e IMAP	115
2.4.5	Serviço de Alocação Dinâmica de IPs – DHCP	117
2.4.6	Serviços de Acesso via Terminal Virtual – Telnet e SSH	120
2.4.7	Serviço de Sincronização dos Relógios dos Computadores – NTP	122
2.4.8	Serviço de Gerenciamento Remoto de Dispositivos de Redes – SNMP	123
2.4.9	Outros Serviços de Rede	125
2.5	Fluxo de Informações em Redes TCP/IP	126

<b>3</b>	<b>Topologias de Rede</b>	<b>130</b>
<b>4</b>	<b>Largura de Banda e Throughput</b>	<b>135</b>
4.1	Medidas de Largura de Banda Digital	135
4.2	Diferença da Largura de Banda dos Meios	137
4.3	Throughput de Dados em relação à Largura de Banda Digital	138
<b>5</b>	<b>Utilizando o Modelo OSI para Auxiliar na Resolução de Problemas de Rede (Troubleshooting)</b>	<b>140</b>

## 1 Modelo de Referência OSI

Devido à importância do modelo de referência OSI vamos iniciar o capítulo fazendo uma revisão de cada camada, suas funções e que dispositivos estão envolvidos em cada uma delas. Apesar de você já ter estudada esse assunto no capítulo anterior pedimos que você faça essa revisão para reforçar sua compreensão e fixar a terminologia, além disso, agora vamos vincular os dispositivos com cada camada, portanto não é somente uma repetição!

Vamos iniciar analisando a figura abaixo com as camadas do modelo OSI. Lembre que a camada 7 é a que dá acesso aos aplicativos do usuário à rede e a camada 1 é a que realmente irá transmitir os bits do usuário para na rede.



### 1.1 Camada 1 – Física

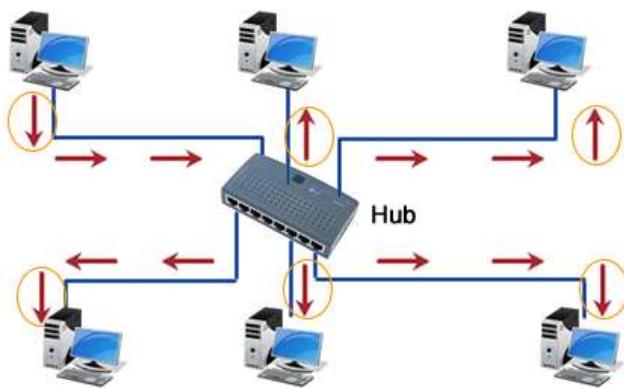
Trata da **transmissão transparente de sequências de bits pelo meio físico**, sendo a **parte final da comunicação**, ou seja, onde a transmissão pelo meio de comunicação **realmente** acontece.

Nessa camada estão definidos os padrões mecânicos (conectores, painéis de conexão, cabos, etc...), funcionais (DCE ou DTE, por exemplo), elétricos (voltagens, codificação de linha, etc...) e procedimentos para acesso a esse meio físico. Nessa camada também temos as especificações dos meios de transmissão, como por exemplo: transmissão via satélite, cabo coaxial, radiotransmissão (rádios digitais ponto a ponto, Wifi, espalhamento espectral, etc.), par metálico (UTP e STP), fibra óptica (monomodo ou multimodo), etc...

Os dispositivos que estão situados na camada física são os componentes do cabeamento estruturado, tais como conectores, transceiver, patch panels, cabos e também os HUBs e repetidores. Veja a figura a seguir.

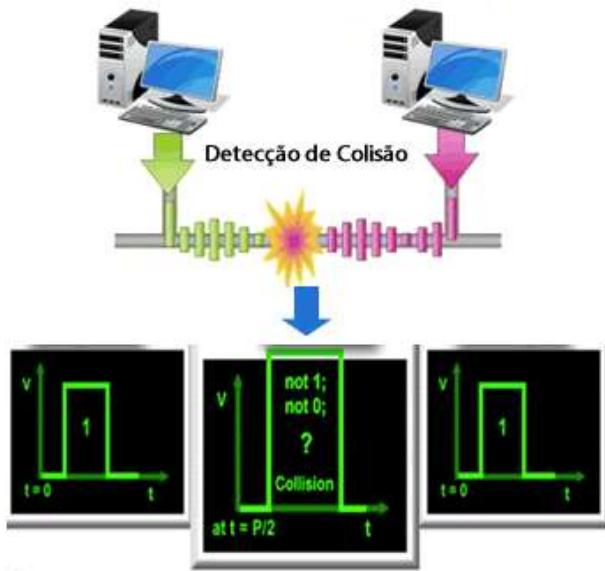


Lembre que os Hubs e Repetidores são dispositivos simples que encaminham os bits recebidos para todas as **portas simultaneamente**. São equipamentos que não tem “inteligência”, isto é, eles não têm a capacidade de ler endereços ou tomar decisões baseadas em quaisquer tipos de informações, eles simplesmente atuam como um “curto-circuito” ou um “barramento” encaminhando a informação recebida em uma porta para todas as outras.



Essa transmissão realizada pelos Hubs e Repetidores é realizada com apenas um par metálico, sendo realizada tanto a transmissão quanto a recepção dos dados pelo mesmo par. Como os bits são sinais elétricos (ondas eletromagnéticas), por exemplo -5 Volts seria o bit zero e +5 Volts o bit 1, se houver a transmissão de dois deles ao mesmo tempo ocorrerá um problema chamado “**colisão**”.

Uma colisão é no “popular” uma “batida” e é isso mesmo, as ondas colidem ou batem uma na outra e o resultado dessa colisão vai ser uma coisa que nem é um bit zero nem um bit 1, ou seja, um sinal que não pode ser interpretado e deve ser descartado. Se o computador detecta uma colisão, toda transmissão é interrompida e é emitido um sinal (“jam” de 48 bits) para anunciar que ocorreu uma colisão, o qual tem o objetivo de evitar colisões sucessivas.



Quando isso ocorre os computadores devem parar de transmitir e tomar uma ação, a qual é assumir um tempo aleatório randômico e quem acabar o contador antes inicia a transmitir novamente. Tecnicamente essa ação é chamada “**algoritmo de backoff**”.

Todo esse procedimento acima está programado nas placas de rede dos computadores que estão conectados aos hubs e é chamado de protocolo CSMA/CD (Carrier Sense Multiple Access with Collision Detection). A tradução da sigla em português diz bem o que é esse protocolo:

- **CS (Carrier Sense)**: Capacidade de identificar se está ocorrendo transmissão, ou seja, o primeiro passo na transmissão de dados em uma rede Ethernet com hub ou repetidor é verificar se o cabo está livre.
- **MA (Multiple Access)**: Capacidade de múltiplos nós concorrerem igualmente pelo meio de transmissão, ou seja, o protocolo CSMA/CD não gera nenhum tipo de prioridade (daí o nome de Multiple Access, acesso múltiplo). Como o CSMA/CD não gera prioridade pode ocorrer de duas placas tentarem transmitir dados ao mesmo tempo e quando isso ocorre há uma colisão, resultando em que nenhuma das placas consegue transmitir dados.
- **CD (Collision Detection)**: Capacidade de detectar a colisão quando ela ocorrer, ou seja, reconhecer quando um sinal diferente do que foi projetado para os bits zero e um e acionar o algoritmo de backoff.

Devido a transmissão e recepção não poder ocorrer simultaneamente, pois temos apenas um meio físico, ela é chamada de “**half-duplex**”, o half em português quer dizer metade, o que é a pura realidade do que ocorre na prática. Se você tem que transmitir e somente em outro período de tempo o receptor responde, ou seja, ocorre metade do processo de cada vez, por isso o nome “**half-duplex**”.

Outro termo utilizado quando temos redes com Hub e repetidores é o “**Domínio de Colisão**”. Esse termo nada mais é que todas as portas que estão ligadas por Hub ou repetidores que podem ter seus bits colididos, por exemplo, se temos um hub de 24 portas todos os micros que estão conectados nessas 24 portas estão em um mesmo domínio de colisão.

Agora, se conectarmos uma das portas desse hub em outro hub de 24 portas, teremos então um domínio de colisão de 48 portas com 46 hosts que podem ter suas informações colidindo entre si (46 porque gastamos 2 portas, uma de cada hub, para interligá-los), e assim por diante. Portanto **quanto maior esse domínio de colisão mais problemas sua rede vai ter**, pois temos mais hosts com probabilidade de transmitir simultaneamente e ter seus bits colidindo!



Agora que os hubs foram  
conectados entre si  
temos um domínio de  
colisão maior, com  
48 portas

Para fechar o assunto, temos então que os hubs são dispositivos para conectarmos os hosts em uma LAN utilizando apenas um par metálico, por isso eles utilizam a transmissão “half-duplex” e estão sujeitos a colisões, portanto as placas de rede precisam ativar o protocolo CSMA/CD. Aqui temos a explicação do porque os hubs apresentam uma performance baixa em redes grandes, imagine 50 micros ligados a vários hubs cascataeados (ligados uns nos outros), todos tentando acessar a rede, o número de colisões será grande (pois todos estarão em um único domínio de colisão) e a rede ficará naturalmente mais lenta.

Você verá na camada de enlace que os equipamentos de camada 2 conseguem “segmentar” os domínios de colisão e melhorar a performance da rede.

Outro ponto negativo dos hubs é a questão de segurança, pois como a informação trocada entre dois hosts é copiada para todos os outros, se instalarmos em um micro dessa rede um programa que abra essa comunicação, chamado sniffer, poderemos capturar os pacotes trocados e “espiar” essa comunicação. Assim os atacantes (hackers) conseguiriam descobrir usuários e senhas de rede que sejam trocadas em modo texto, ou seja, sem nenhum mecanismo de proteção como a criptografia.

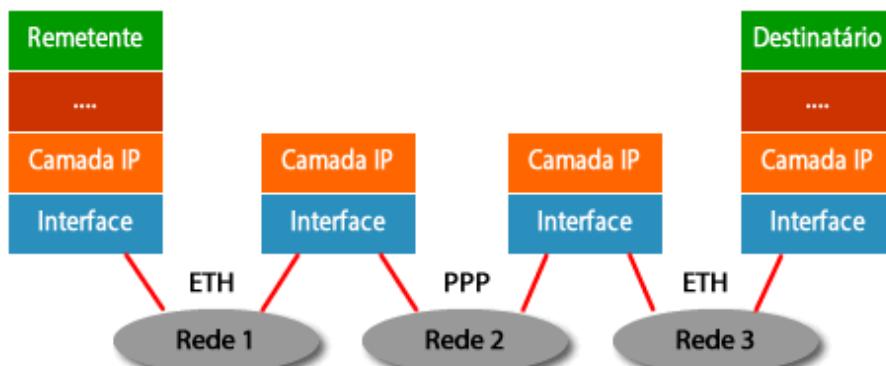
## 1.2 Camada 2 – Enlace

A camada de enlace tem a função de preparar os pacotes que vem da camada de rede para que eles possam ser enviados corretamente pelos diferentes tipos de meios físicos, esse processo é chamado enquadramento (framing), ou seja, ao pacote que está vindo da camada de rede serão inseridas informações de controle e será gerado um quadro (frame) de camada 2 apropriado para cada meio de transmissão que estiver sendo utilizado.

Point-to-Point Protocol					
Quadro					
Nome do campo	Flag	Endereço	Controle	Protocolo	Dados
Comprimento (bytes)	1 byte	1 byte	1 byte	2 bytes	variável
Protocolo Ethernet					
Quadro					
Nome do campo	Preâmbulo	Endereço de Destino	Endereço de Origem	Tipo	Dados
Comprimento	8 bytes	6 bytes	6 bytes	2 bytes	46 - 1500 bytes
Seqüência de Verificação do Quadro					
4 bytes					

Portanto, teremos um quadro diferente para cada tipo de tecnologia de transmissão e meio físico que formos utilizar. Por exemplo, em uma rede LAN podemos utilizar as tecnologias Ethernet, as quais utilizam um determinado tipo de quadro, com suas características. Já ao transmitir esse mesmo pacote através de uma WAN ele será enquadrado novamente conforme o protocolo de WAN daquele determinado link.

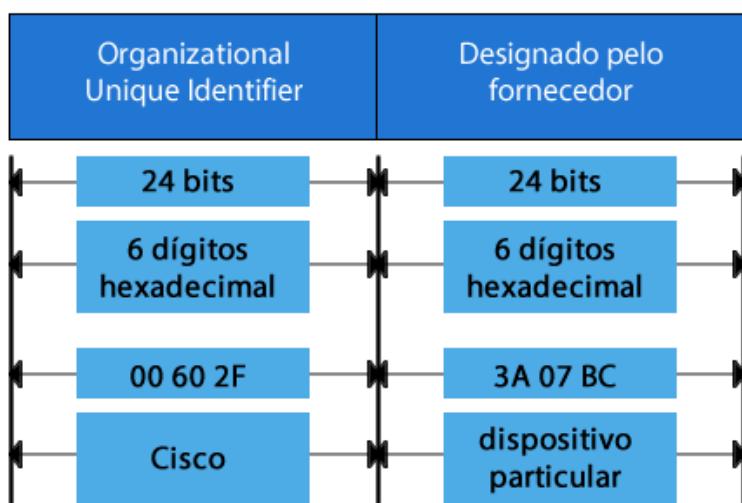
Então, quando um pacote cruza uma rede ele irá passar por diversas LANs e WANs, cada uma podendo ser composta por um tipo diferente de protocolo, e nessa “navegação” o pacote sempre continua o mesmo, ele nunca é alterado, apenas os quadros de camada 2 são desmontados e montados conforme a tecnologia utilizada. Veja a figura abaixo onde a cada nó de rede os quadros de camada 2 são trocados conforme a tecnologia utilizada e a informação da camada 3 (no exemplo estamos utilizando o protocolo IP) nunca é alterada.



Na camada 2 também são realizados controle de erro e controle de fluxo para uma comunicação segura entre os dois pontos.

Outro ponto importante é que na camada de enlace vem o primeiro nível de endereçamento que utilizamos nas redes, o “**endereço físico**”. Esse endereçamento é utilizado apenas localmente naquele link físico, sendo utilizado para que os dois endpoints ou dispositivos de rede formem a comunicação ponto a ponto e possam enviar as informações entre si. Cada protocolo de camada 2 tem seu tipo de endereçamento, por exemplo, a família Ethernet utiliza o endereço MAC (MAC address) para identificar cada host em uma rede LAN. Outro exemplo é o DLCI (Data Link Connection Identifier) utilizado pelo protocolo de WAN Frame-relay para identificar suas conexões.

O mais famoso e estudado endereço de camada 2 é o MAC, pois ele é fundamental para comunicação em uma rede LAN que utilize tecnologias da família de protocolos ethernet, tais como o próprio ethernet, fastethernet e gigabit ethernet. Ele é composto por 48 bits, os quais estão divididos em duas porções: o OUI (Organizational Unique Identifier) e um serial. Portanto, 24 bits representam o fabricante, chamado de OUI, e os outros 24 bits representam o número de série que deve ser único mundialmente falando, pois esses valores são administrados pelo IEEE (Institute of Electrical and Electronic Engineers).



Note na figura que os endereços MAC são escritos com caracteres hexadecimais, os quais cada um deles é escrito com 4 bits, portanto temos 48 bits divididos por 4 em um total de 12 algarismos hexadecimais. O Hexadecimal utiliza os algarismos de 0 a 9 e a partir do 10 são representados pelas letras A, B, C, D, E e F, o que dá em decimal de 0 a 15, totalizando 16 tipos de caracteres. Normalmente o MAC pode ser escrito das seguintes maneiras abaixo, dependendo do sistema operacional do dispositivo:

- **0000.0c00.1234** → pontuado de 4 em 4 caracteres.
- **08:00:20:AB:CD:09** → separado por dois pontos de dois em dois caracteres.
- **01-00-0C-CC-CC-CC** → o mesmo do anterior, porém separado com traço.

Você pode pesquisar na Internet quem é o fabricante da sua placa de rede entrando no prompt de comando, digitando o comando "ipconfig /all", procure pelo endereço MAC e vá até o website abaixo, copie e cole seu MAC para ver o fabricante (veja as figuras abaixo). Note que no campo de resultado (Results) o OUI **C0:18:85** pertence ao fabricante **Hon Hai Precision Ind. Co.,Ltd.**

<http://www.wireshark.org/tools/oui-lookup.html>

```
C:\Users\dltec>ipconfig /all

Configuração de IP do Windows

Nome do host . . . . . : dltec-marcelo
Sufixo DNS primário . . . . . :
Tipo de nó . . . . . : desconhecido
Roteamento de IP ativado. . . . . : não
Proxy WINS ativado. . . . . : não

Adaptador de Rede sem Fio Conexão de Rede sem Fio:

Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : Dell Wireless 1702 802.11b/g/n
Endereço Físico . . . . . : C0-18-85-E5-EE-DB
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv6 de link local . . . . . : fe80::9db:ae76:db9:bccd%12(Pref
Endereço IPv4. . . . . : 10.0.0.102(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : quinta-feira, 23 de agosto de 2
Concessão Expira. . . . . : quinta-feira, 23 de agosto de 2
```

### OUI Lookup Tool

The Wireshark OUI lookup tool provides an easy way to look up **OUIs** and other MAC address prefixes. It uses the [Wireshark manufacturer database](#), which is a list of OUIs and MAC addresses compiled from a number of sources.

#### Directions:

Type or paste in a list of OUIs, MAC addresses, or descriptions below. OUIs and MAC addresses may be colon-, hyphen-, or period-separated.

#### Examples:

0000.0c  
08:00:20  
01-00-0C-CC-CC-CC  
missouri

#### OUI search

C0-18-85-E5-EE-DB

Find

#### Results

C0:18:85 Hon Hai Precision Ind. Co.,Ltd.

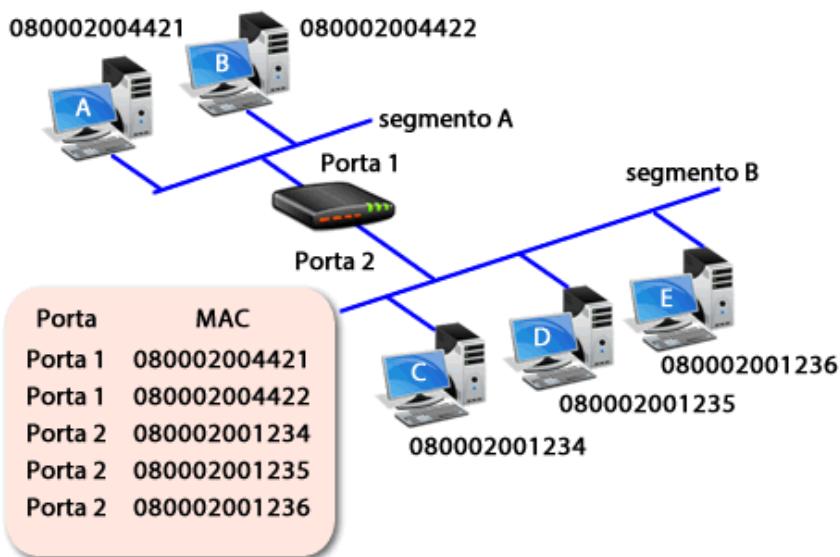
Quando um micro em uma rede LAN ethernet deseja se comunicar com outro na mesma rede, ele precisa saber o endereço MAC do computador remoto. Normalmente esse endereço MAC de destino (do micro remoto) não é conhecido, porém é necessário. Para resolver esse problema o TCP/IP possui um protocolo chamado ARP (Address Resolution Protocol), o qual tem a função de descoberta do MAC de destino dado um endereço IP conhecido. Perceba na figura anterior (primeira figura) que existem dois campos no quadro ethernet chamados MAC de destino (destination address) e MAC de origem (source address).

O que caracteriza os dispositivos de camada 2 é a capacidade de "ler" esses endereços MAC e tomar decisões baseado nessa informação. Por exemplo, um switch sabe para que porta encaminhar determinado quadro através do endereço MAC de destino do quadro que ele recebe em uma interface.

Como já estudamos anteriormente, os representantes da camada de enlace são as placas de rede, switches e bridges. Mas como foi a evolução? Por que os hubs deixaram de ser utilizados?

Se você lembrar do tópico anterior, os hubs ligados uns com os outros acabam gerando um grande domínio de colisão, o que causa lentidão na rede pelo alto número de computadores disputando o mesmo meio, pois quanto mais hosts em uma LAN conectada via hubs maior a probabilidade de ocorrer colisões! Foi então que nessa época surgem as bridges (pontes), equipamentos de camada 2 que tem a capacidade de aprender os endereços MAC dos micros que estão conectados nas suas portas e tomar decisões baseadas nesses endereços.

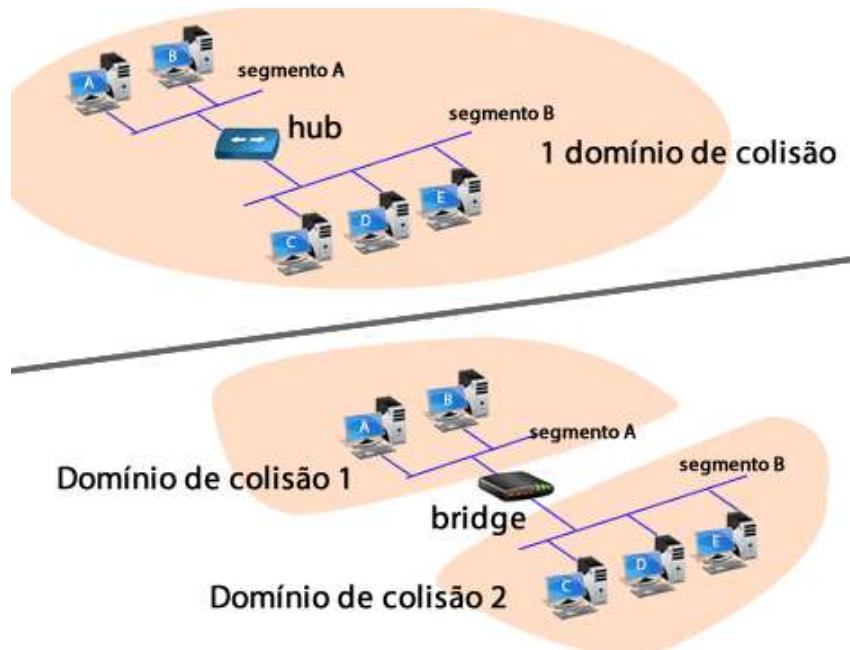
Mas como as bridges fazem isso? As bridges tem uma tabela interna que é capaz de guardar que endereço ou endereços MAC estão conectados a cada uma de suas portas. Ela aprende os MACs ao longo do tempo, pois enquanto os computadores estão trocando informações entre si os hubs encaminham os quadros para todas as suas portas e assim a bridge pega o endereço MAC de origem e mapeia com a porta que ele recebeu aquele quadro.



Agora que a bridge sabe os endereços MAC que estão conectados a cada uma de suas portas, quando um computador que está no segmento A deseja se comunicar com um que está no segmento B a bridge encaminha essa quadro da porta 1 para a porta 2. Mas quando dois micros do mesmo segmento, por exemplo, o micro C deseja falar com o micro E, a bridge irá filtrar essa informação, pois ela sabe que o MAC de C e E estão nos mesmos segmento e seria inútil encaminhar para o segmento 1. Isso é a segmentação de rede, o que significa que agora

temos dois domínios de colisão separados pela bridge, um domínio de colisão formado pelos micros A e B e um segundo domínio de colisão formado pelos micros C, D e E.

Então podemos notar que as bridges foram inseridas nas LANs para diminuir o número de computadores em um domínio de colisão, ou seja, aumentando a quantidade de domínios de colisão. Achou confuso? Este é um jogo de palavras que pode parecer complicado mas não é, basta você lembrar que quanto mais micros compartilhando o mesmo meio pior é, pois são mais dispositivos para colidir e quando diminuímos esse número de micros melhoramos essa situação. Portanto, quanto mais domínios de colisão com menos computadores em cada domínio melhor será a rede. Veja a figura abaixo.



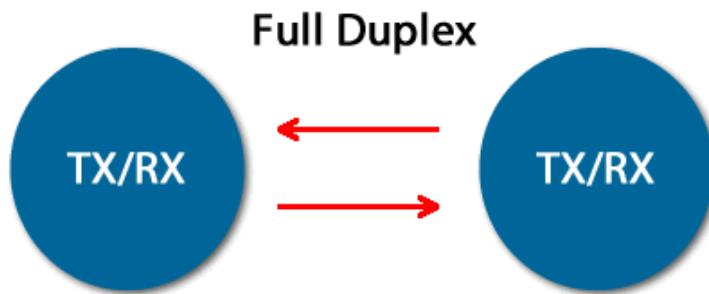
Na realidade a coisa é um pouco mais complicada sobre o aprendizado, pois a bridge lê os quadros inteiros, analisa o campo FCS, o qual indica se o quadro foi corrompido ou não através de uma operação matemática, e caso não houver erro com o quadro é que a bridge irá fazer o encaminhamento. Lembre que estamos em uma rede com hubs e podem haver colisões e dependendo do caso a colisão pode ocorrer após os endereços de origem e destino, sendo assim se a bridge não verificar a integridade do quadro ela pode acabar encaminhando "lixo" entre as portas, por isso ela precisa ler o quadro ethernet inteiro, verificar se ele está sem erros para aí sim fazer o encaminhamento para a outra porta. Esse processo é chamado de "**store and forward**" ou "**armazena e encaminha**". Esse processo torna a bridge mais lenta que os hubs e é realizado por software, ou seja, por um programa que está dentro da bridge.

Portanto, devido a essa latência que a bridge traz para as redes ela acabava se tornando um gargalo, basta verificar na figura 6 que um dispositivo apenas entre duas redes repletas de hubs acaba realmente se tornando um ponto de "estrangulamento" do tráfego. Porém, essa segmentação dos domínios de colisão realmente melhorava a rede, por isso pensaram em fazer uma bridge com mais de duas portas e foi aí que nasceram os **switches**.

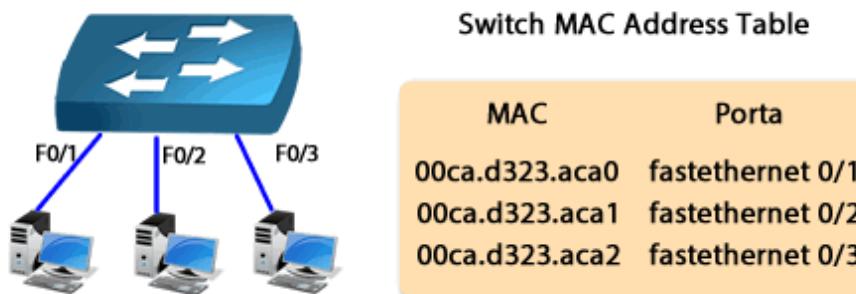
Os switches são basicamente bridges multiportas, porém com algumas melhorias, pois agora eles tomam decisão por hardware e não mais por software, o que os torna mais rápidos que as bridges. Além disso, foram criados outros tipos de encaminhamento mais eficientes que o store and forward, os quais veremos na sequência.

No início os switches, assim como as bridges, faziam a segmentação das redes onde já existiam hubs, porém com muito mais portas do que as bridges. No entanto, ao longo do tempo houve um barateamento dos equipamentos e os administradores de rede partiram para conectar os computadores direto nos switches, ao invés de conectar os computadores em hubs e segmentar com switches. Isso trouxe um ganho muito grande, porque agora não existe mais colisão na rede, pois cada porta do switch é um domínio de colisão com apenas um computador!

Outra vantagem é que os switches permitem a comunicação full-duplex, utilizando dois pares metálicos para se conectar com os computadores, um para transmissão (tx) e outro para recepção (rx), aumentando a banda disponível para os computadores. Quando dois computadores se comunicam através de um switch um caminho livre de colisões é formado internamente e a comunicação se torna mais rápida e segura, porque agora os quadros trocados entre origem e destino não são mais copiados para as demais portas, como era o caso dos hubs, a comunicação fica isolada entre os dois dispositivos que estão se comunicando. Veja a figura abaixo.



Assim como as bridges, os switches mantêm uma tabela de endereços MAC aprendida por porta, para permitir o encaminhamento dos quadros entre as portas. Essa tabela é chamada SAT (Source Address Table) ou CAM (Content Addressable Memory). Veja a figura ao lado.



Quando um host envia quadros para outro e o switch conhece o MAC de destino, ou seja, o endereço MAC para quem a origem está mandando os quadros, e então ele cria um micro-segmento entre os dois computadores livre de colisões. Porém, quando o switch não conhece o MAC de destino ele copia esse quadro para todas as demais portas, menos para quem enviou o quadro.

Esse processo é chamado de flooding, ou inundação, e é o momento de vulnerabilidade do switch, pois todo switch tem um limite na tabela de endereços MAC e é assim que é realizado o ataque chamado MAC flooding. Um programa gera vários MACs falsos em uma porta até lotar a

tabela CAM e o switch atua como um hub, copiando todos os quadros para todas as portas e possibilitando que o atacante "escute" a rede, ou seja, instale um sniffer em seu computador e "espie" a comunicação que está passando por aquele determinado switch.

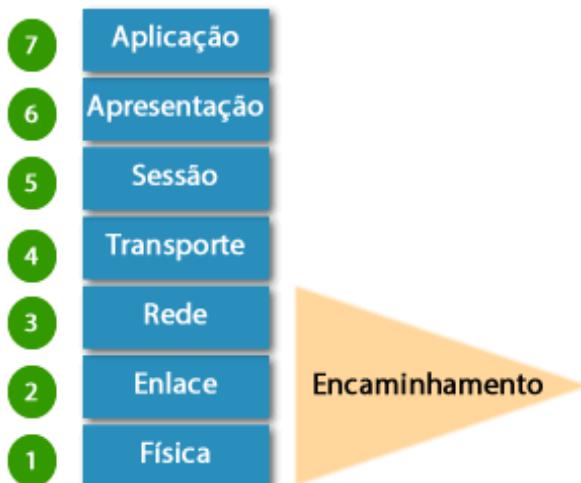
Vamos a um exemplo de flooding. Imagine que o switch aprendeu os endereços MAC dos micros B, C e D, mas não tem em sua tabela de endereços MAC o micro A. Portanto, quando B, C ou D enviar um quadro para o computador A o switch terá que fazer um flooding, copiando esse quadro para todas as portas menos para quem enviou o quadro, na tentativa de encontrar o MAC que ele não conhece. Quando o micro A receber o quadro ele irá responder e o switch irá completar sua tabela de endereços vinculando o MAC do micro A com a porta fastethernet de número 0/3.

Apesar de ainda não termos visto o conceito de broadcast é importante saber que os switches não conseguem evitar ou segmentar broadcasts, pois eles segmentam domínios de colisão. Se um switch receber um quadro de broadcast como endereço de destino, o qual tem o endereço MAC ffff.ffff.ffff (todos os 48 bits em 1), esse quadro será copiado para todas as portas.

No capítulo 6 estudaremos mais alguns detalhes sobre as redes LAN e switches, pois podemos dividir uma rede com switches em diversos domínios de broadcast e melhorar ainda mais o desempenho geral para os usuários, melhorando inclusive a segurança de rede.

### 1.3 Camada 3 – Rede

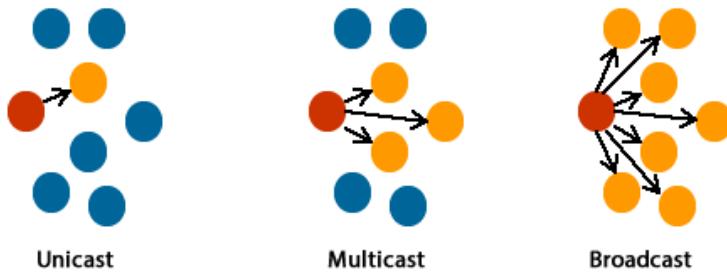
As camadas 1, 2 e 3 do modelo OSI são as camadas que realmente fazem que a informação seja encaminhada através de uma rede e cheguem ao seu destino. As camadas 1 e 2 permitem que vários tipos de interfaces e tecnologias de transmissão sejam utilizadas de maneira independente e a camada 3 fornece o esquema de endereçamento lógico utilizado para identificar os dispositivos de maneira única dentro das diversas redes existentes. Veja a figura abaixo.



Falando mais especificamente da camada 3 ou rede, ela é responsável pelo **esquema de endereçamento** global de uma rede, ou seja, o endereçamento que permite identificar um dispositivo a **longa distância**, e também pelo **roteamento dos pacotes** através dessas diversas redes. Além disso, na camada 3 temos protocolos auxiliares que fornecem mensagens de controle e erro para auxiliar protocolo roteado, por exemplo, o ICMP (Internet Control Message Protocol).

Em uma rede temos basicamente três tipos de comunicação possíveis em camada 3 (veja a figura abaixo):

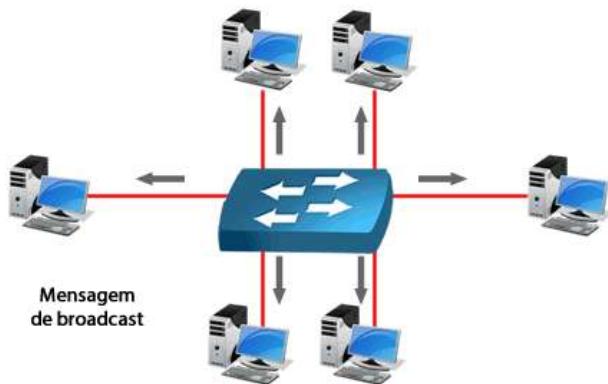
- **Unicast:** um host se comunicando diretamente com outro. **Um para um.**
- **Broadcast:** um endereço especial que faz com que todos os hosts ou um conjunto que pertence a uma mesma rede sejam alcançados. **Um para todos.**
- **Multicast:** permite que um grupo selecionado através de um endereço de multicast se comunique. **Um para um grupo (alguns).**



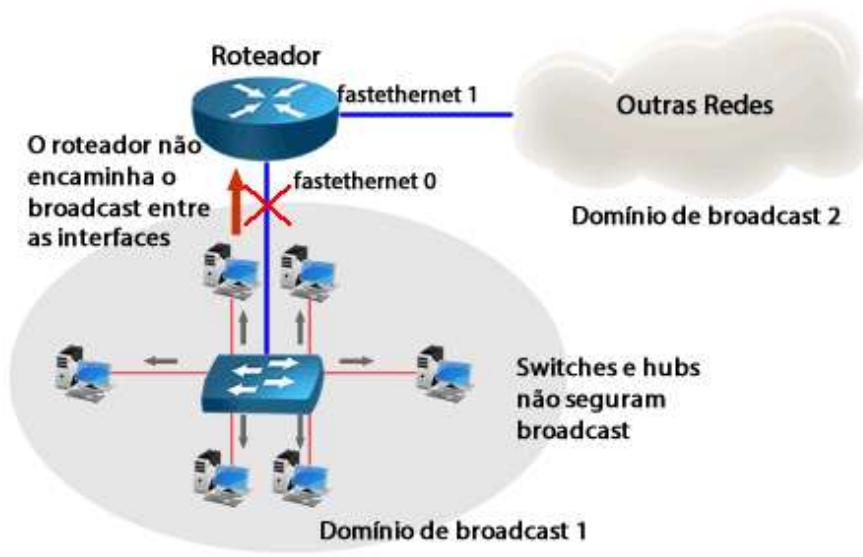
Os dispositivos de rede que representam a camada 3 são os roteadores e os switches de camada 3 (switches que podem fazer tarefas de roteador), porém você verá nas bibliografias tradicionais o **roteador** como representante principal da camada de rede.

A principal característica de um roteador, que é o que faz o posicionamento dele na camada 3, é que cada interface dele é um domínio de broadcast. Isso quer dizer que se um roteador tem duas interfaces, cada uma delas deve estar em uma rede própria e se um host de uma delas enviar um broadcast o roteador não irá encaminhá-lo para a outra interface. Por isso os roteadores conseguem segmentar “**domínios de broadcast**”. Semelhante à definição de domínio de colisão, o domínio de broadcast é a região onde um broadcast consegue se propagar.

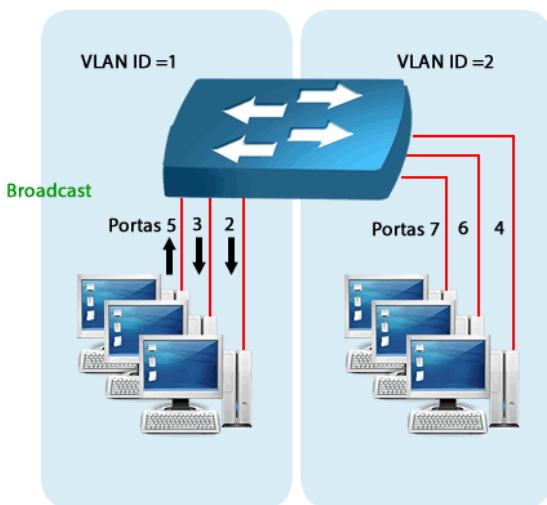
Acompanhe na figura abaixo que em um switch, quando uma porta recebe uma mensagem de broadcast ela é encaminhada para as demais portas, pois switches segmentam domínios de colisão!



Agora analise a próxima figura e note que ao roteador receber essa mesma mensagem de broadcast ele não repassará para suas demais portas, pois cada porta do roteador é um domínio de broadcast.

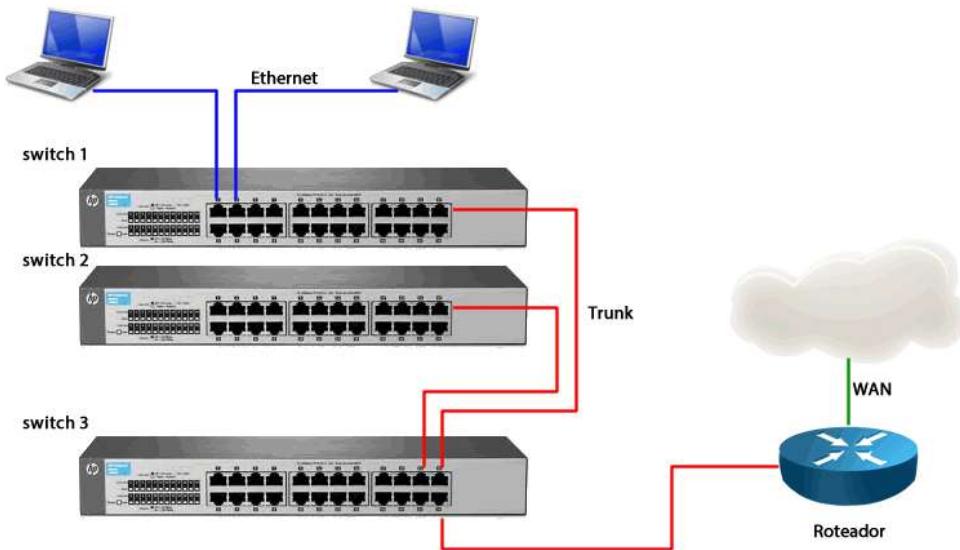


Além de um roteador ou switch de layer 3, podemos fazer com que switches normais de camada 2 segmentem domínios de broadcast utilizando LANs virtuais ou VLAN (virtual LAN). As VLANs são grupos de portas dos switches que podemos agrupar e isolá-las das demais portas. Na prática criamos um número ou identificador de VLAN (como 1, 2, 3 e assim por diante) e vinculamos as portas nessas VLANs criadas. Por exemplo, se eu tenho um switch de 12 portas e crio 3 VLANs (vlan1, vlan2 e vlan3, por exemplo) e escolho que as portas de 1 a 4 pertencem à VLAN 1, de 5 a 8 à VLAN 2 e as demais à VLAN 3, agora se um micro que está na porta 1 enviar um broadcast somente os micros das portas 2, 3 e 4 receberão essa mensagem, porque cada VLAN é um domínio de broadcast! Veja a figura abaixo.



O broadcast recebido pela porta 5 do switch é encaminhado somente para as portas 2 e 3, pois essas estão na mesma VLAN.

Para que duas VLANs se comuniquem será necessário um roteador ou um switch que trabalhe também na camada 3 para que seja realizado o roteamento entre as diferentes VLANs. Veremos no capítulo 6 que esse entroncamento entre switches que possuem VLAN ou então com o roteador é feito por links especiais chamados "trunks" ou troncos, os quais utilizam um protocolo chamado 802.1Q, o qual faz a marcação ou tagging dos quadros, para que várias VLANs possam compartilhar o mesmo link e os switches reconheçam a quem pertence o quadro que ele está recebendo.

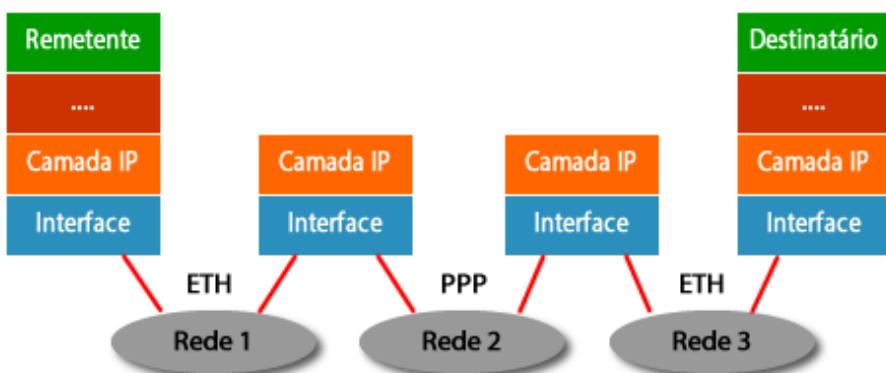


O que ocorre quando temos VLANs é que os quadros enviados entre dois hosts que estão em VLAN IDs diferentes chegam até o roteador pelos trunks, permitindo que o roteador faça seu papel e roteie a informação entre as diferentes VLANs, permitindo que os hosts se comuniquem.

Na prática, ser um domínio de broadcast significa que você precisa de uma rede própria para aquela interface e seus hosts que estão plugados nela, veremos isso com mais detalhes no capítulo 5.

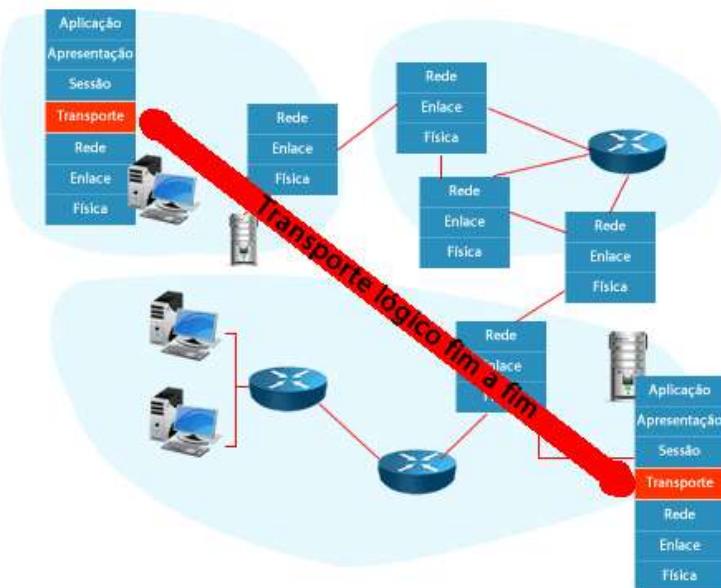
Relembrando e resumindo, o que vem da camada 4 é passado para a camada de redes como os "dados de entrada" ou "payload" que ela deve enviar para um host remoto. Esse dado vai receber um cabeçalho da camada 3, o qual contém endereço lógico de origem e destino e vários bits de controle e será enviado para a camada de enlace (camada 2). A camada de enlace irá montar o quadro para envio na camada física (camada 1) e também irá inserir os endereços físicos de origem e destino para que a comunicação local ocorra. Após o quadro montado ele é enviado para a camada física enviar os bits através do meio físico.

Esse processo de montagem e desmontagem dos quadros de camada 2 e envio dos bits pelo meio físico é repetido até o pacote de camada 3 chegar ao seu destino, mas como isso ocorre? No meio do caminho temos vários roteadores que analisam o **endereço de destino** do pacote e retransmitem esse pacote para a interface de saída mais apropriada (**esse é o processo de roteamento e comutação**). O roteamento entre as diversas interfaces de diversos roteadores então é feito até que o pacote cruze a rede e chegue a seu destino, onde será passado para o computador ou servidor que aí sim irá processar a informação até extrair o dado que deve ser enviado para o aplicativo de destino. Veja a figura abaixo.



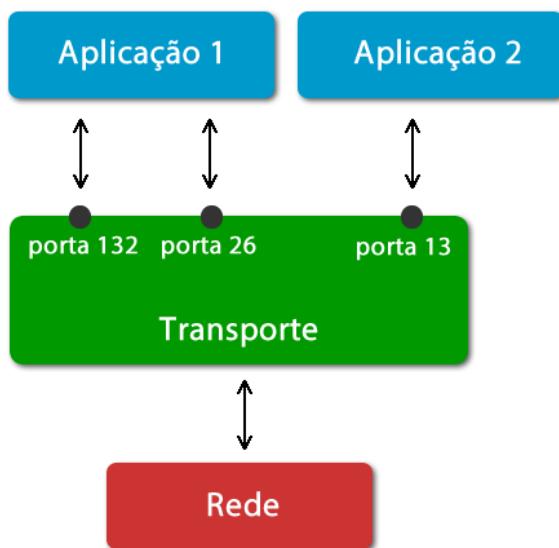
#### 1.4 Camada 4 – Transporte

Lembre que nessa camada temos o conceito de comunicação fim-a-fim.



É na camada de transporte que os dados dos aplicativos realmente são preparados para o transporte dentro da rede. As principais características dessa camada é que os vários fluxos abertos pelos aplicativos são identificados, ou seja, recebem um endereçamento chamado de “porta” para que possam ser multiplexados (compartilhados) e enviados para as camadas inferiores.

Esse “endereçamento” que a camada de transporte utiliza tem a finalidade de distinguir para que programa ou aplicação que está instalada nos computadores de origem e destino os dados devem ser enviados. Além disso, imagine que não pudéssemos compartilhar o meio, aí você teria que abrir uma página web, por exemplo, finalizar a sessão para depois enviar ou receber um e-mail, porém não é assim que funciona, pois cada fluxo aberto por um aplicativo recebe um endereço único de camada 4 fazendo com que o seu computador possa acessar vários serviços de rede simultaneamente, isso é a multiplexação dos serviços. Veja a figura abaixo.



Além disso, a camada de transporte desempenha outras importantes funções, tais como a segmentação dos dados (quebra os dados das camadas superiores em segmentos menores), controle de fluxo, transporte confiável de dados não importando o meio físico, etc.

Portanto a camada de transporte recebe um dado da camada de sessão, faz a segmentação (quebra esses dados em pedaços menores), coloca o endereçamento (portas de origem e destino) e envia o segmento para a camada de rede para que ele possa ser roteado pela rede.

Genericamente chamamos o PDU da camada 4 de **segmento**.

No capítulo de arquitetura TCP/IP você estudará os protocolos TCP e UDP, os quais estão na camada 4, e normalmente as descrições da camada de transporte são as características do protocolo TCP.

### 1.5 Camadas 5, 6 e 7 – Sessão, Apresentação e Aplicação

As camadas de 4 a 7 estão mais internas à cada host, ou seja, não são utilizadas pela rede para tomada de decisões ou encaminhamento de informações. Nessas camadas atuam os firewalls e proxies, ou seja, dispositivos de segurança ou de um nível superior que tratam das informações nas camadas superiores para apenas verificar a parte de segurança ou itens de alto nível.

Temos aqui outros dispositivos como os filtros de conteúdo e switches de conteúdo, os quais analisam a informação da camada 7 para tomar decisões de encaminhamento do serviço como um todo. Por exemplo, um switch de conteúdo pode analisar as informações das camadas 4 a 7 para fazer balanceamento de carga entre servidores. Mas no geral um dispositivo que trata da camada 4 para cima nas bibliografias tradicionais são os hosts (servidores e computadores). Vamos agora relembrar o que faz cada camada.

A camada de sessão tem a função de disponibilizar acessos remotos, estabelecendo serviços de segurança, verificando a identificação do usuário, sua senha de acesso e suas características, por exemplo, seus perfis de usuário. Atua como uma interface entre os usuários e as aplicações de destino, podendo inclusive fornecer sincronização entre as tarefas dos usuários.

A camada 6 é responsável pelas transformações ou traduções adequadas nos dados antes do seu envio a camada de sessão, sendo que essas transformações podem ser referentes à compressão de textos, criptografia, conversão de padrões de terminais e arquivos para padrões

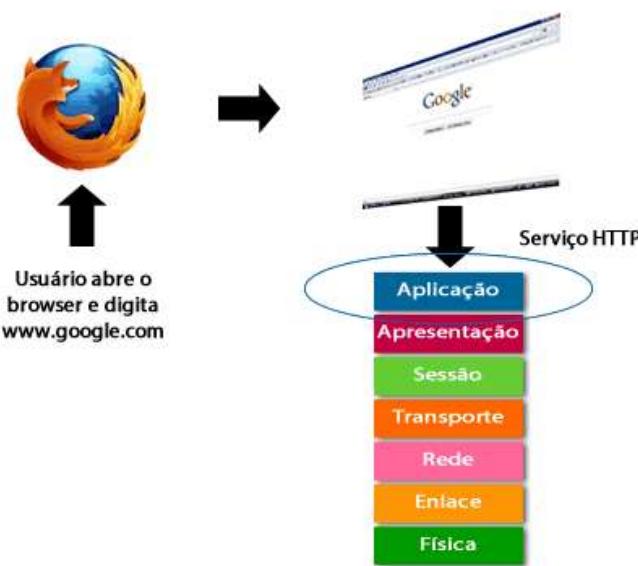
de rede e vice-versa. Portanto tem o objetivo de fazer com que os dois lados "falem a mesma língua". Suas funções típicas são:

- Formatação de dados
- Compressão e criptografia
- Compatibilização entre aplicações (syntaxe)

A camada 7 é a mais superior e é responsável pela interface com as aplicações dos computadores (hosts), ou seja, a camada de aplicação tem a função de dar acesso à rede aos aplicativos dos usuários que estão instalados nos computadores. Nessa camada temos os serviços de rede, tais como:

- Serviço de tradução de nomes de Internet: DNS
- Serviços de e-mail: SMTP, POP3 e IMAP
- Serviços de terminal: Telnet e SSH
- Serviços de web: HTTP e HTTPS (seguro)
- Gerenciamento de redes: SNMP
- Acesso a arquivos em rede: FTP e TFTP
- Fornecimento de endereços IP dinâmicos: DHCP

Lembre-se da figura ao lado, a qual já estudamos anteriormente, onde temos um exemplo em que o usuário abre seu web browser e digita [www.google.com](http://www.google.com), portanto a camada que vai fazer interface com o aplicativo é a 7, ou seja, a camada de aplicação vai pegar os dados do usuário e prepará-los para que eles sejam enviados através das camadas e tenham acesso à rede.



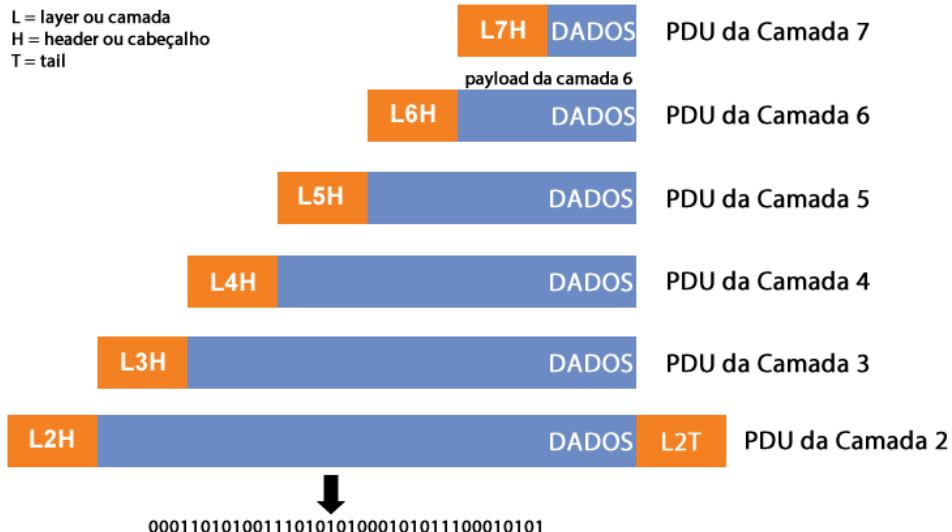
É também importante lembrar que as informações trafegadas entre as camadas de sessão, apresentação e aplicação são chamadas de **dados**.

## 1.6 Processo de Encapsulamento e Desencapsulamento de Dados

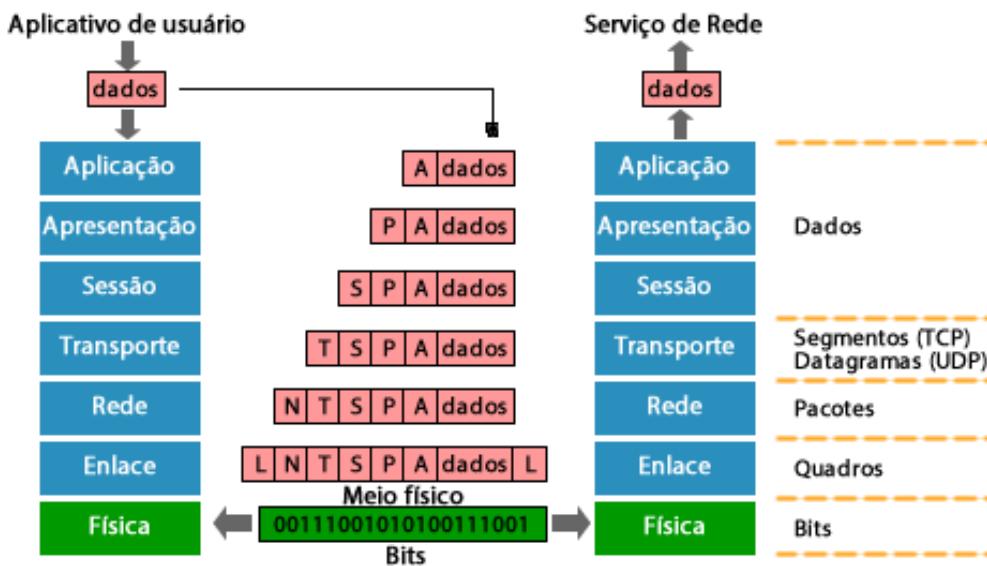
Como vimos, o modelo de referência OSI quebra as diversas tarefas necessárias para que um dado seja enviado pela rede em pedaços ou fatias para que o desenvolvimento seja mais simples e modular.

Lembre que cada camada vai possuir um formato específico contendo informações de controle, sendo chamado de Unidade de Dados de Protocolo ou **PDU** (Protocol Data Unity), os quais são inseridos no início, na parte chamada de "cabeçalho" (em inglês header) e em algumas vezes no final, chamado de Trailer ou Tail. Esses cabeçalhos e tails são lidos no destino para que cada camada saiba o que fazer com a informação. Nele estão contidos instruções, endereços e demais controles necessários para que a comunicação flua entre os dois computadores. Veja a figura abaixo.

Note que cada camada ou layer será inserida na camada inferior como dados, chamado em inglês muitas vezes de payload. Quando o host de destino recebe a informação ela tem seu cabeçalho/tail lido, depois removido e passado para a camada superior, no processo inverso até os dados que foram enviados pela camada de aplicação serem recebidos pelo aplicativo do host de destino.



Portanto, esse processo de recebimento dos dados do usuário pela camada 7 até sair em bits na camada 1 é chamado de "encapsulamento".



**Obs: Recurso disponível somente na matéria online**

Veja a animação sobre o processo de encapsulamento e desencapsulamento do Modelo de Referencia OSI desenvolvido pelo LARC (Laboratório de Arquitetura e Redes de Computadores da Escola Politécnica da USP) para que o conceito fique mais claro.

<http://www.youtube.com/watch?v=DNO37Ah4rKE>

Além disso, assista também a animação sobre o modelo OSI no link abaixo:

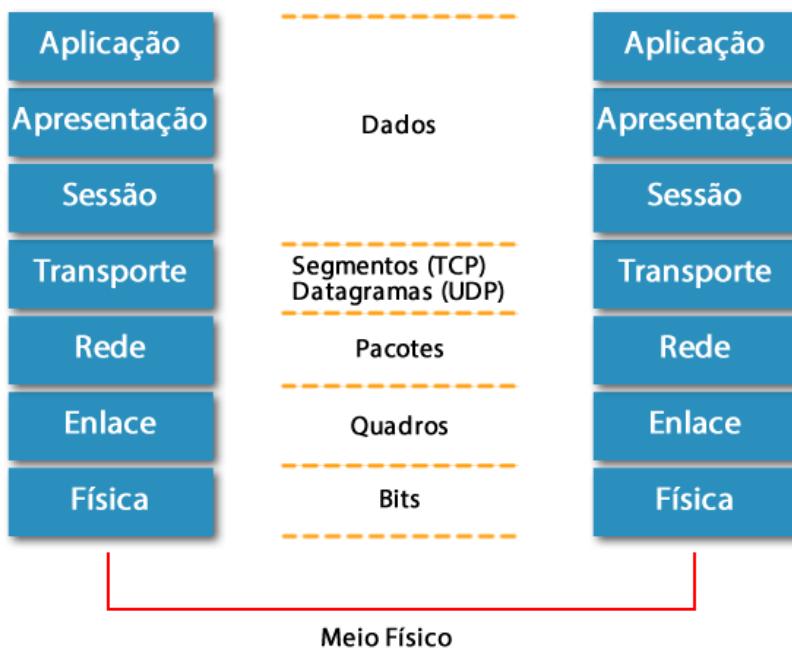
<http://www.youtube.com/watch?v=fiMswfo45DQ&feature=related>

Fica bem claro nas duas animações que tudo inicia no aplicativo do host (computador do usuário). A partir desse momento, quando um aplicativo quer acessar a rede para comunicar-se com um host remoto, ocorrem os seguintes passos:

1. A camada de aplicação (camada ou layer 7) recebe os dados da aplicação, insere seu cabeçalho e essas informações (cabecalho de aplicação + dados do aplicativo) são passados para a camada de apresentação.
2. Em seguida a camada de apresentação recebe esses dados, insere suas informações de controle, ou seja, seu cabeçalho e envia esses dados para camada de sessão.
3. Os dados vindos da camada de apresentação recebidos pela camada de sessão, a qual também insere seus dados de controle (seu cabeçalho) e esses dados são enviados à camada de transporte.
4. Os dados recebidos da camada de sessão pela camada de transporte serão agora segmentados (quebrados em pedaços menores) e enviados à camada de rede.
5. A camada de rede recebe os **segmentos** da camada de transporte, insere seus dados de controle (incluindo os endereços de origem e destino de rede) e envia seus **pacotes** para a camada de enlace prepará-los para que eles sejam enviados através do meio físico.

6. Na camada de enlace os pacotes são **enquadados** recebendo as informações de controle e normalmente um **endereçamento físico** em seu cabeçalho, podem ter inserido também um **tail** contendo informações para controle de erros e são finalmente enviados para a camada física.
7. Na camada física os **quadros** recebidos da camada de enlace são convertidos no padrão físico que estiver sendo utilizado (elétrico, óptico, sinal de rádio, ECT) e enviado pelo meio de transmissão até o destino ou então para o próximo salto responsável pelo roteamento da informação até o destino final.

É importante ficar atendo ao nome “técnico” dado a cada PDU conforme figura ao lado.



Você pode encontrar também bibliografias que utilizam a palavra **datagrama** para descrever os PDUs da camada de rede do protocolo **IP** e também da camada de transporte quando utilizando o protocolo **UDP**, isso porque ambos os protocolos são **“Best effort”** (melhor esforço), ou seja, não são orientados a conexão como o protocolo de transporte TCP.

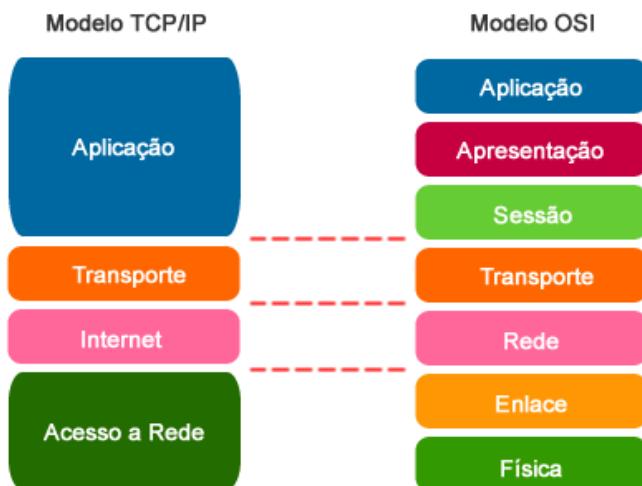
Analise ainda a figura anterior e veja que ao ser recebido pela Máquina B ou Host B a informação passará pelo processo inverso do encapsulamento até chegar ao aplicativo que deve recebê-la, esse processo é o **desencapsulamento**. Ou seja, a camada física passa os bits para a camada de enlace, a qual verifica se os endereços físicos e demais informações de controle são realmente para aquele host, retira seu cabeçalho e passa para a camada de rede. A camada de rede lê o cabeçalho, verifica se o endereço de destino contido nele é realmente o seu e depois retira todo seu cabeçalho e passa a informação para a camada de transporte. Isso se repete até a camada de aplicação da Máquina B enviar os dados para o aplicativo de destino para que ele seja processado e uma ação seja tomada, a qual pode ser, por exemplo, inserir um novo e-mail em sua caixa de entrada.

Então chegamos ao fim do estudo do modelo OSI e você deve aqui ter aprendido a nomenclatura de cada camada, o que cada uma delas faz, quais os dispositivos que estão em cada uma delas e o processo de encapsulamento. Na sequência veremos o TCP/IP, o qual é a pilha de protocolos de rede que realmente foram implementadas nas redes, porém toda a referência do mundo de redes é sobre o modelo OSI, por isso é tão importante entender ambos!

## 2 Arquitetura TCP/IP

Como já foi estudado tanto no capítulo 2 como aqui nesse capítulo, apesar do modelo OSI ser a referência para as redes e toda sua nomenclatura, a arquitetura TCP/IP é a que foi realmente implementada e está em uso até os dias de hoje tanto nas redes internas (Intranets) como na Internet.

A arquitetura TCP/IP é composta por apenas 4 camadas (formando a pilha da estrutura do protocolo), sendo que na prática, as camadas 5, 6, e 7 do modelo OSI foram mescladas para formar a camada de **Aplicação** do TCP/IP. Já as camadas 3 e 4 do modelo OSI são similares às camadas 2 e 3 do TCP/IP, inclusive a camada de transporte do TCP/IP tem o mesmo nome, porém a camada 3 do modelo OSI (rede) no TCP/IP é chamada de **Internet**. Já as camadas 1 e 2 do modelo OSI foram mescladas no TCP/IP para formar a camada de **acesso aos meios** ou **acesso à rede**. Veja a figura abaixo.



No TCP/IP não costumamos nos referir por camadas e sim pelos nomes delas, pois quando nos referimos pelo número da camada estamos falando do OSI.

### 2.1 Camada de Acesso à Rede ou Acesso aos Meios

Esta é a camada inferior da arquitetura TCP/IP tem as funcionalidades referentes às camadas 1 e 2 do Modelo OSI. Nela temos os diversos protocolos, tecnologias e dispositivos utilizados nas redes LAN e WAN. É a responsável pelo envio dos pacotes através do meio físico.

Atualmente as principais tecnologias de acesso para redes LAN são as que utilizam cabos metálicos (UTP e STP) ou fibra ótica da família Ethernet e os meios sem aéreos, ou seja, tecnologia sem fio (wireless ou Wi-Fi) através da família IEEE 802.11.

O funcionamento da família ethernet é similar entre os padrões e foi explicado nesse capítulo quando falamos das camadas 1 e 2 do modelo OSI, com o CSMA/CD e a comunicação full-duplex feita pelas bridges e switches. Normalmente as diversas opções desse família de tecnologias recebem um nome que contém a velocidade, o termo "base" e um sufixo que significa a tecnologia de transmissão utilizada (par metálico, fibra, etc.).

Por exemplo, 10Base-T representa o padrão 802.3i, o qual utiliza par metálico (T – twisted pair ou par trançado), com uma velocidade de 10Mbps (10.000.000 – dez milhões bits por segundo) enviado em banda base, ou seja, o "Base"(Baseband/banda base) indica transmissão de apenas um sinal digital por vez na linha. Toda essa família utiliza switches ou hubs como dispositivos de rede de acesso, ou seja, onde os hosts se conectam.

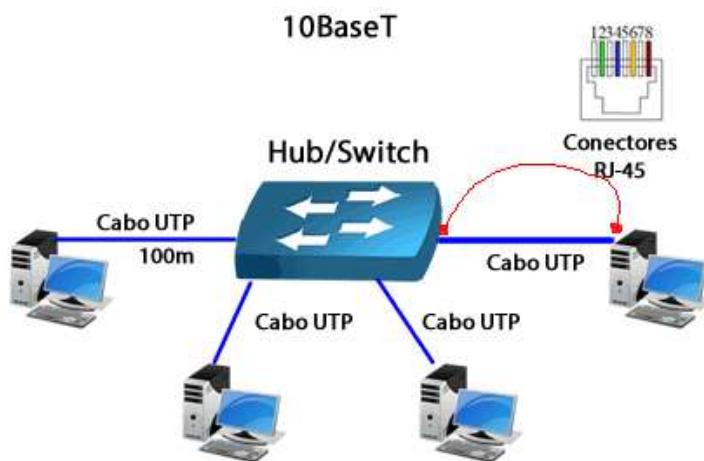
Vamos ver os principais padrões utilizados até os dias de hoje nas redes LAN cabeadas.

### 2.1.1 Ethernet 10BASE-T

O padrão 10BASE-T foi introduzido em 1990 e possui as seguintes características:

- Padrão 802.3i.
- Taxa de transmissão de 10 Mbps com sinalização em banda base.
- Usa cabo de par-trançado UTP e pode ser conectado a uma distância máxima de 100 metros.
- Utiliza nas pontas o conector RJ-45.
- Pode operar nos modos half-duplex (hub) ou full-duplex (switch).
- Utiliza o procedimento CSMA/CD quando em modo half-duplex.
- Utiliza topologia em estrela ou estrela estendida com um hub central.
- Sua grande vantagem refere-se ao fato de que uma falha no cabo afeta somente uma estação.
- Apesar de estar caindo em desuso ainda pode ser encontrada em casos específicos.

A mesma topologia física e tipo de cabeamento serão utilizados para as demais tecnologias, tais como fastethernet e gigabitethernet, podendo variar apenas o tipo de cabo (categoria).



### 2.1.2 Fastethernet – 100 Mbps

A Ethernet 100 Mbps é conhecida por FastEthernet e está no padrão IEEE 802.3u. A principal característica da Ethernet 100 Mbps é sua taxa de transmissão, dez vezes maior que o padrão 10BASE-T visto anteriormente. Suas principais representantes são:

#### **100BASE-TX**

- Taxa de transmissão de 100 Mbps.
- Sinalização em banda base, utilizando também o cabo de par trançado UTP (cat5 ou cat5e – categoria do cabo). Comprimento máximo de 100 metros.
- Conector RJ-45.
- Pode operar nos modos half-duplex ou full-duplex.
- Pode utilizar Hubs com o procedimento CSMA/CD.
- Utiliza topologia em estrela ou estrela estendida.

Atualmente é o padrão mais difundido devido a quantidade de redes 10/100 instaladas. Aos poucos tendem a serem substituídas por redes Giga ou até mesmo pelos novos padrões de redes sem fio.

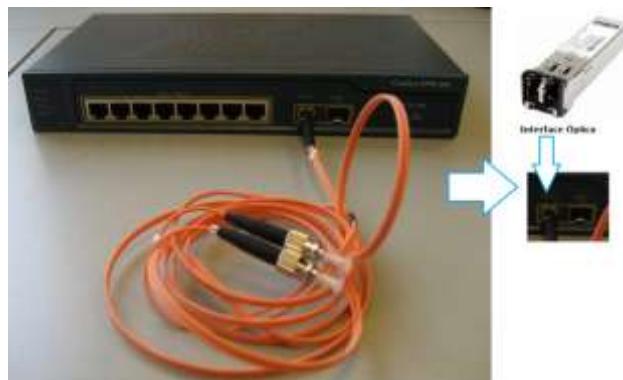
#### **100BASE-FX**

- Taxa de transmissão de 100 Mbps com sinalização em banda base.
- Usa cabo de fibra óptica de duas vias (uma fibra para transmissão e outra para recepção – TX/RX).
- Conector do tipo ST ou SC (veja a figura abaixo).



O 100BASE-FX pode chegar a 400 metros e pode ser encontrado como interfaces de switches ou em conversores ópticos, os quais são utilizados em conjunto com switches que não tem opção de interface óptica.

Nos switches as interfaces de fibra normalmente estão disponibilizadas em pequenos módulos conversores eletro/ópticos. Veja as figuras 1 (conversor de mídia) e 2 (switch) ao lado. Note na figura a seguir que o switch não vem com a interface óptica, ela é um módulo que pode ser inserido conforme necessidade de cada projeto, os quais são chamados de GLCs ou GBICs.



### 2.1.3 Gigabit Ethernet – 1.000 Mbps

A Ethernet 1.000 Mbps ou Gigabit Ethernet (1 Gbps) utiliza cabeamento de cobre (par trançado) e/ou fibra óptica. Suas principais tecnologias são:

#### **1000BASE-T**

Especificação IEEE 802.3ab, usa cabo de par trançado (categoria 5e ou 6) e pode chegar a uma distância de 100m. Normalmente é utilizada para conectar servidores ou dispositivos de rede, porém com a disseminação e constante redução do custo da tecnologia ela vem sendo cada vez mais adotada para conectar os computadores dos usuários finais, principalmente em ambientes que necessitam de alta taxa de dados.

Os equipamentos que disponibilizam essa taxa na rede normalmente são chamados de 10/100/1000 por suportarem as três velocidades, de 10Mbps, 100Mbps e 1000Mbps em suas portas. Veja a figura abaixo com um switch 10/100/1000 Cisco modelo SR2024.



Além disso, é bem comum encontrarmos switches com 24 portas 10/100 e uma ou duas portas a Gigabit chamadas de "Uplink", ou seja, portas de maior velocidade para fazer o entroncamento com outros switches ou roteadores.

#### **1000BASE-SX e LX**

As especificações 1000BASE-SX e 1000BASE-LX usam os mesmos parâmetros de temporização e um tempo de bit de 1 nanosegundo, porém utilizando fibra óptica como meio físico. Assim como para o padrão 100Base-FX, as tecnologias em fibra a Giga podem ser encontradas em dispositivos ponto a ponto, como os conversores de fibra, ou como uma interface para uso em switches (GLC ou GBIC).

A diferença entre os três padrões é o tipo de fibra utilizada e a distância que o link pode alcançar. O padrão 1000BASE-SX é recomendado nas redes de até 550 metros, enquanto o 1000Base-LX é capaz de atingir até 5km com o uso de fibras ópticas monomodo.

#### 2.1.4 Ethernet 10 Gigabit

O novo padrão Ethernet de 10 gigabits abrange 7 tipos diferentes de mídias para redes LAN, MAN e WAN. Ele está atualmente especificado por um padrão suplementar (IEEE 802.3ae) e será incorporado numa versão futura do padrão IEEE 802.3. Normalmente usam conexão ponto a ponto, interligando apenas dois equipamentos. Seus principais padrões são:

- **10GBASE-SR**: destinado a curtas distâncias através de fibras multimodo já instaladas, suportando distâncias entre 26 m e 82 m.
- **10GBASE-LX4**: utiliza WDM (Wavelength Division Multiplexing – divisão por comprimento de onda) e suporta distâncias de 240 m a 300 m através das fibras multimodo já instaladas, e 10 km através de fibras monomodo.
- **10GBASE-LR e 10GBASE-ER**: suporta de 10 km a 40 km através de fibra monomodo.
- **10GBASE-SW, 10GBASE-LW e 10GBASE-EW**: conhecidos de forma genérica como 10GBASE-W são destinados a funcionar com equipamentos OC-192 STM (Synchronous Transport Module) SONET/SDH utilizados em redes MAN e WAN.

## 2.2 Camada Internet

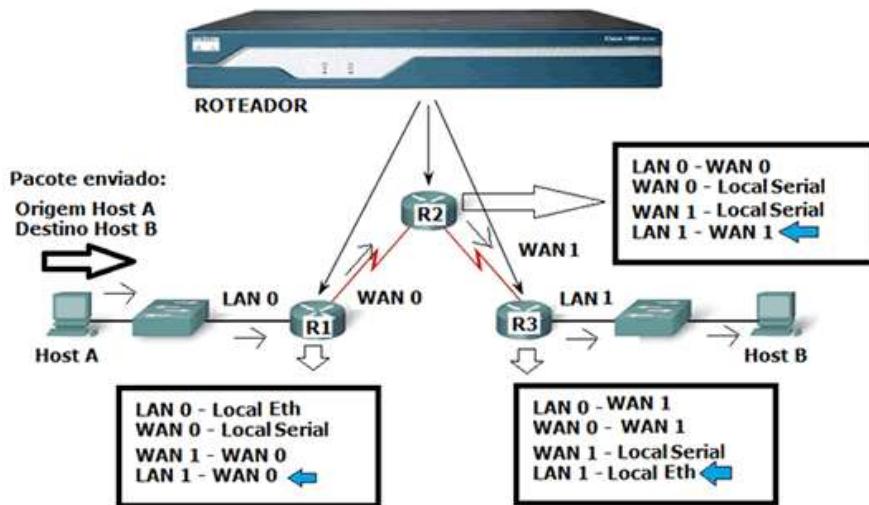
A camada de Internet do TCP/IP é equivalente a camada 3 do Modelo OSI (Rede). Ela tem as funções de fornecer o **endereçamento lógico** dos endpoints e dispositivos de rede, assim como fazer o **roteamento dos pacotes** entre as diversas redes. Na camada de Internet que os **roteadores** atuam.

Para entender a camada de Internet e como os pacotes são encaminhados temos que ter em mente que ela nada mais é que um conjunto de redes interligadas, ou seja, várias LANs interligadas por diversas WANs através de roteadores.



Mas como isso é feito? Quando um pacote é enviado para um destino remoto, um roteador em sua rede o recebe, lê o endereço de destino (o endereço do host remoto que vai receber o pacote enviado) que está no cabeçalho do pacote, escolhe uma interface de saída baseado em sua **"tabela de roteamento"** e faz a comutação do pacote para essa interface de saída.

Acompanhe um exemplo na figura abaixo, onde um computador (Host A) da rede LAN 0 envia um pacote para um computador (Host B) que está em uma rede remota chamada LAN 1. Esse pacote quando enviado é recebido pelo roteador local R1 que está conectado com a rede **LAN 0**, o qual consulta sua tabela de roteamento e verifica que para alcançar a rede **LAN 1** deve **comutar** o pacote (**rotear**) para a rede **WAN 0**. Quem recebe o pacote em seguida é o roteador R2, o qual também consulta sua tabela de roteamento e verifica que a rede LAN 1 não está diretamente conectada a uma de suas interfaces e por isso precisa encaminhar (rotear ou comutar) o pacote para a interface **WAN 1**. Agora o roteador R3 recebe o pacote, verifica o endereço de destino, o qual pertence à rede **LAN 1** que está conectada à sua interface local, e encaminha para sua rede Ethernet para que o Host B possa receber o pacote enviado pelo Host A.



Este exemplo é uma representação macro e simplificada do que ocorre na Internet ou nas Intranets que utilizam o protocolo IP como protocolo roteado, portanto os pacotes são enviados rede a rede, roteador a roteador até que encontrem seus destinos. É importante lembrar aqui que o protocolo IP não tem garantia de entrega, pois ele é um protocolo de melhor esforço (best effort), ou seja, não se preocupa com erros ou retransmissões se um pacote não chegar ao seu destino.

Temos diversos protocolos que atuam na camada de Internet, sendo que o principal deles é o **IP** (Internet Protocol), o qual é a base da comunicação em rede atual. O IP existe em duas versões: versão 4 (**IPv4**) e versão 6 (**IPv6**). A internet ainda funciona baseada no **IPv4**, porém tudo tende a migrar para a **versão 6** do protocolo IP (processo que já está em andamento), pois o IPv6 tem muito mais endereços disponíveis e melhorias em relação ao IP versão 4.

O cabeçalho do protocolo IP versão 4 tem o formato conforme mostrado abaixo.

0	4	8	15 16	32		
Versão	Tamanho Cabeçalho	Tipo Serviço (TOS)	Tamanho Total (bytes)			
Identificação		Flag	Offset de fragmentação			
Tempo de Vida (TTL)	Protocolo		Checksum			
Endereço IP Origem						
Endereço IP Destino						
Opções						
Dados						

Veja o que significa cada um dos campos:

- **Versão:** indica a versão do protocolo a que o pacote pertence, que nesse caso estamos vendo o cabeçalho do IPv4.
- **Tamanho do Cabeçalho:** indica o tamanho do cabeçalho, informando seu tamanho em palavras de 32-bits.
- **Tipo de Serviço:** permite que o host informe à sub-rede o tipo de rede que deseja (confiável ou veloz).
- **Tamanho Total:** inclui tudo o que há no pacote (cabeçalho + dados).
- **Identificação:** é necessário para permitir que o host destino determine a qual pacote pertence um fragmento recém-chegado. Todos os fragmentos de um pacote contêm o mesmo valor de identificação.
- **Flag:** campo que indica se o pacote dever ser fragmentado ou não. Existem alguns hosts que não aceitam pacotes fragmentados.
- **Offset de Fragmentação:** informa a que ponto do pacote atual o fragmento pertence;
- **Tempo de Vida:** é um contador usado para limitar a vida útil do pacote. Esse campo conta o número de saltos que um pacote pode dar, permitindo uma vida útil máxima de 255 saltos. A cada salto que o pacote dá esse campo é decrementado. Quando o contador chegar a zero, o pacote é descartado e um pacote de advertência é enviado para o host de origem. Este é o princípio do traceroute, teste que permite que você descubra qual o caminho que um pacote segue até seu destino.
- **Protocolo:** quando um pacote estiver completamente montado, a camada de rede precisa saber o que fazer com ele. Este campo informa a ela o processo de transporte que deverá ser aplicado ao pacote, como TCP ou UDP.
- **Checksum:** campo que confere apenas o cabeçalho, utilizado para detecção de erros.
- **Endereço IP Origem e Endereço IP Destino:** indicam o número da rede e o número do host de quem está enviando os pacotes (origem) e do host que deve receber esses pacotes (destino).
- **Opções:** este campo foi projetado para permitir que versões posteriores do protocolo incluam informações inexistentes no projeto original, possibilitando a experimentação de novas ideias e evitando a alocação de bits de cabeçalho para informações raramente necessárias.
- **Dados:** contém os dados a serem transmitidos, os quais são normalmente os segmentos TCP ou Datagramas UDP vindos da camada de transporte.

Juntamente com o IP outros protocolos atuam na camada 3 para auxiliar a comunicação em rede e complementar funções necessárias tais como a descoberta de endereços físicos em redes LAN, envio de mensagens e notificações de erros, etc. Basicamente temos ainda na camada 3 os protocolos **ICMP** (Internet Control Message Protocol), **ARP** (Address Resolution Protocol), **RARP** (Reverse Address Resolution Protocol) e os **protocolos de roteamento dinâmico**. Vamos ver na sequência cada um desses protocolos.

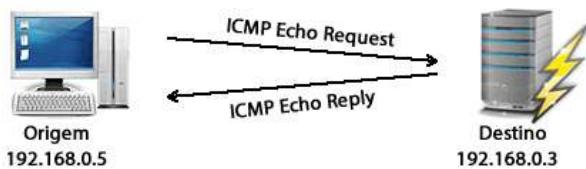
### 2.2.1 ICMP (Internet Control Message Protocol)

O ICMP é um protocolo integrante do Protocolo IP, definido pela RFC 792, e utilizado para fornecer relatórios de erros ao host que deu origem aos pacotes enviados na rede. Qualquer computador que utilize IP precisa aceitar as mensagens ICMP e alterar o seu comportamento de acordo com o erro relatado. Os gateways (roteadores) devem estar programados para enviar mensagens ICMP quando receberem pacotes que provoquem algum tipo de erro.

As mensagens ICMP geralmente são enviadas automaticamente em uma das seguintes situações:

- Um pacote IP não consegue chegar ao seu destino, por exemplo, quando o tempo de vida (TTL) do pacote está expirado (o contador chegou à zero). Esta mensagem é o destino inalcançável ou “destination unreachable”.
- O roteador não consegue retransmitir os pacotes na frequência adequada, ou seja, o roteador está congestionado.
- O roteador indica uma rota melhor para o host que está enviando pacotes (redirecionamento de rota).

Além disso, o ICMP fornece ferramentas comumente usadas para testes de rede como o Ping e Traceroute. O Ping é baseado em duas mensagens, o echo request e echo reply. Quando você entra no prompt de comandos do Windows, por exemplo, e digita “ping www.dltec.com.br”, na realidade seu computador está enviando mensagens de “echo request” ao servidor onde a página da DLTEC está hospedada e ao receber essa mensagem nosso servidor responde com um “echo reply”. Caso o servidor não responda seu computador indicará um timeout (tempo de resposta expirado), indicando que não houve resposta.



Veja a tela a seguir com dois exemplos de ping, o primeiro obteve resposta (0% de perda) e o segundo não (100% de perda).

```
C:\Windows\system>ping www.dltec.com.br

C:\Users\dltec>ping www.dltec.com.br

Disparando www.dltec.com.br [96.125.170.182] com 32 bytes de dados:
Resposta de 96.125.170.182: bytes=32 tempo=159ms TTL=48
Resposta de 96.125.170.182: bytes=32 tempo=157ms TTL=48
Resposta de 96.125.170.182: bytes=32 tempo=157ms TTL=48
Resposta de 96.125.170.182: bytes=32 tempo=157ms TTL=48

Estatísticas do Ping para 96.125.170.182:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
              perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 157ms, Máximo = 159ms, Média = 157ms

C:\Users\dltec>ping 172.16.1.1

Disparando 172.16.1.1 com 32 bytes de dados:
Esgotado o tempo limite do pedido.

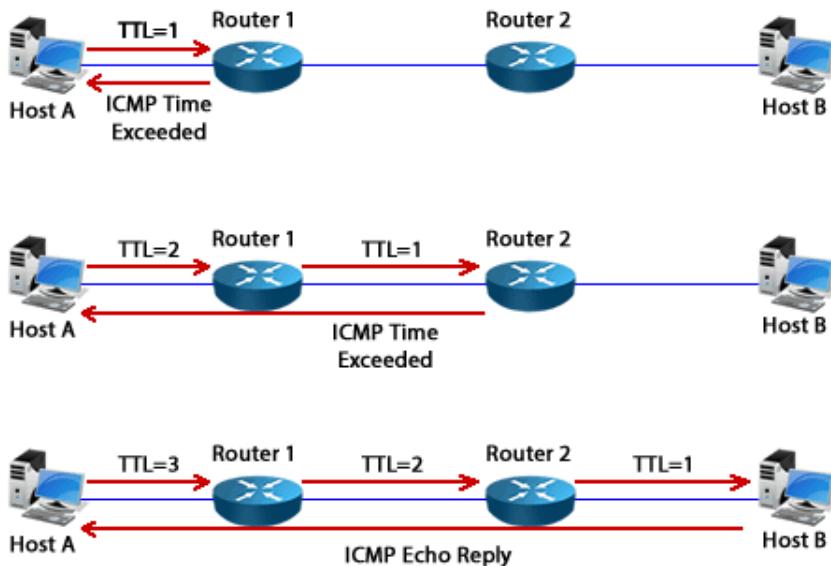
Estatísticas do Ping para 172.16.1.1:
    Pacotes: Enviados = 4, Recebidos = 0, Perdidos = 4 (100% de
              perda),

C:\Users\dltec>
```

O teste de ping é utilizado para verificar se há comunicação fim a fim, ou seja, entre origem e destino, sem se importar com os dispositivos (roteadores e switches) que estão no meio do caminho. Vale a pena lembrar que as mensagens de ping podem ser bloqueadas por firewalls e IPSs, portanto nem sempre não obter uma resposta a um ping significa necessariamente um erro, pode ser que esse teste esteja bloqueado por motivos de segurança.

Já o trace ou traceroute tem a função de testar o **caminho** que o pacote está seguindo até seu destino, ou seja, ele é um **teste ponto a ponto**. O trace está baseado no funcionamento do campo TTL do protocolo IP, pois quando um pacote IP tem seu tempo de vida expirado o roteador deve enviar uma mensagem ICMP à origem do pacote indicando esse problema. Nessa mensagem vem o IP do roteador e com isso o computador consegue saber por onde o pacote está passando.

Resumindo, o host onde foi originado o trace manda um pacote com TTL igual a 1, no primeiro salto o pacote expira e o roteador responde. Depois envia um pacote com TTL igual a 2, aí ele conhece o roteador que está no segundo salto, sendo que esse processo se repete até que o pacote atinja seu destino e o caminho é traçado. Veja a figura abaixo, onde o host de destino está a 3 saltos da origem.



Acompanhe na tela mostrada a seguir onde temos um exemplo do “tracert” que é o comando do Windows para o traceroute (Cisco e Linux). Note que no décimo oitavo salto o computador não obteve resposta, pois provavelmente existe um bloqueio por motivos de segurança nesse roteador. Para alcançar o destino nosso pacote teve que percorrer 19 saltos, ou seja, passou por 19 roteadores entre a origem e o destino.

```
C:\Windows\system32\cmd.exe
C:\Users\dltec>tracert www.dltec.com.br

Rastreando a rota para dltec.com.br [96.125.170.182]
com no máximo 30 saltos:

 1  2 ms   2 ms   2 ms  192.168.1.1
 2  2 ms   2 ms   2 ms  192.168.1.1
 3  11 ms   9 ms   9 ms  gvt-10.b3.cta.gvt.net.br [177.42.96.1]
 4  11 ms   9 ms   9 ms  177.99.179.static.host.gvt.net.br [177.99.179.129]
 5  13 ms   15 ms  14 ms  gvt-te-0-2-4-0-rc01.cta.gvt.net.br [187.115.212.26]
 6  12 ms   11 ms  15 ms  gvt-te-0-5-0-0-rc03.cta.gvt.net.br [189.59.247.206]
 7  19 ms   37 ms  22 ms  187.115.214.233.static.host.gvt.net.br [187.115.214.233]
 8  24 ms   23 ms  23 ms  gvt-te-0-0-0-4-rt02.spo.gvt.net.br [187.115.214.194]
 9  171 ms  179 ms  184 ms  Xe0-1-1-0-grtsaosi2.red.telefonica-wholesale.net [84.16.10.201]
10  191 ms  285 ms  226 ms  176.52.249.197
11  171 ms  165 ms  163 ms  Xe2-0-0-0-grtmiana2.red.telefonica-wholesale.net [94.142.118.250]
12  174 ms  186 ms  181 ms  softlayer-AE-0-0-grtmiana2.red.telefonica-wholesale.net [213.148.51.19
0]
13  128 ms  129 ms  171 ms  ae7.bbr01.tm01.mia01.networklayer.com [173.192.18.174]
14  152 ms  154 ms  153 ms  ae1.bbr01.sr02.hou02.networklayer.com [173.192.18.162]
15  157 ms  200 ms  158 ms  ae3.bbr01.eq01.dal03.networklayer.com [173.192.18.218]
16  158 ms  159 ms  159 ms  ae5.dar01.sr01.dal07.networklayer.com [173.192.18.179]
17  159 ms  159 ms  162 ms  po1.fcr01.sr01.dal07.networklayer.com [50.22.118.131]
18  *       *       *       Esgotado o tempo limite do pedido.
19  157 ms  159 ms  159 ms  web.dltec.com.br [96.125.170.182]

Rastreamento concluído.
```

## 2.2.2 ARP e RARP

O **ARP** (Address Resolution Protocol – protocolo de resolução de endereços) e o **RARP** (Reverse Address Resolution Protocol – protocolo de resolução de endereços reverso) são dois protocolos utilizados para resolução de endereços físicos, isto é, eles têm a função de mapear qual endereço físico está vinculado a um determinando endereço IP de um host remoto. Isto é necessário em redes da família Ethernet para que o quadro de camada 2 possa ser montado e enviado localmente até seu destino ou então até o roteador que tem a saída para a rede de destino (que pode ser a Internet, por exemplo). Lembre-se que para que dois hosts se comuniquem, no quadro da camada 2 deve estar indicado os endereços MAC de origem e destino. Sem isso não tem como a rede local, por exemplo, um switch determinar para que porta ele deve encaminhar o quadro e também quando o quadro chegar ao destino este host não conseguiria saber que o quadro é para ele. Veja a figura ao lado com o quadro da camada 2 genérico para a família Ethernet.

Protocolo Ethernet (Quadro)

Preâmbulo	Endereço de Destino	Endereço de Origem	Tipo	Dados	Sequência de Verificação do Quadro
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

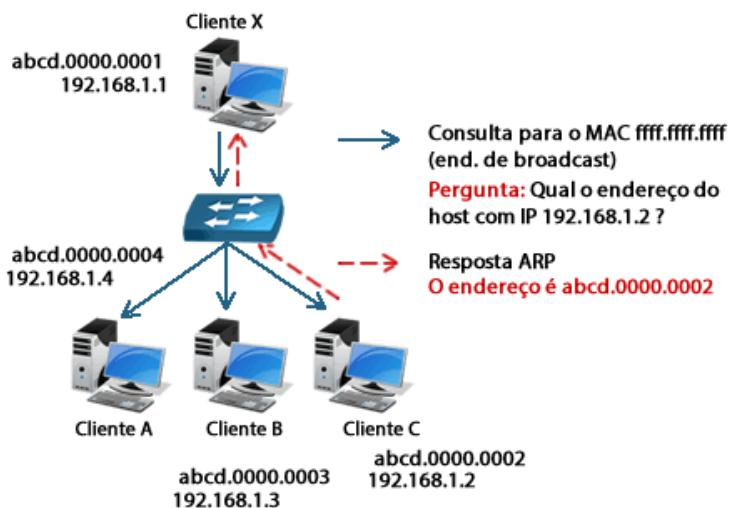
Note que no segundo campo temos o MAC do destino (computador que vai receber os dados) e no terceiro campo do quadro o MAC de origem, ou seja, de quem está enviando os quadros.

Quando a comunicação se dá entre dois computadores na mesma LAN, por exemplo, na sua casa você quer fazer um ping do seu computador para o computador de seu Pai ou Irmão, nesse caso eles estão na mesma rede que você e normalmente você sabe os endereços IP, portanto você digita "ping 192.168.1.2".

Com isso o seu computador tem o seu próprio IP, pois ele está configurado na placa de rede, seu endereço MAC que também está gravado na placa de rede, conhece o IP remoto, porque você o digitou e falta o endereço MAC do computador remoto.

É aí que entra o protocolo chamado ARP, pois ele envia uma requisição na rede em broadcast, ou seja, todos os micros da mesma rede irão receber essa requisição, solicitando o endereço MAC do IP que você digitou no ping. Todos os micros recebem a requisição, mas quem responde é aquele que tem o IP 192.168.1.2. Ao receber a informação o computador de origem consegue montar o quadro e enviar as informações.

Acompanhe na figura abaixo a ilustração do funcionamento do protocolo ARP. Logo abaixo da figura para ver como é o formato do quadro do ARP com a resposta do host com IP 192.168.1.2 informando seu MAC ao host de origem, note que a resposta do ARP é enviada diretamente para o solicitante, ou seja, não mais em broadcast e sim em unicast. Na sequência você verá a figura com quadro já finalizado e que será enviado entre o host ClienteX e o ClienteC.



bits 0-7	bits 8-15	bits 16-31
Hardware Type (HTYPE) 0x0001 (ethernet)	Protocol Type (PTYPE) 0x0806 (ARP)	
Hardware Length (HLEN) 0x06	Protocol Length (PLEN) 0x04	Operation (OPER) 0x0002 (REPLY)
Sender Hardware Address (SHA) abcd.0000.0002		
Sender Protocol Address (SPA) 192.168.1.2		
Target Hardware Address (SHA) abcd.0000.0001		
Target Protocol Address (SPA) 192.168.1.1		

Quadro entre ClienteX e Cliente C

Preâmbulo	Endereço de Destino	Endereço de Origem	Tipo	Dados	Sequência de Verificação do Quadro
01010101 (x8)	abcd.0000.0002	abcd.0000.0001	0x0800	IP	CRC
8 bytes	6 bytes	6 bytes	2 bytes		4 bytes

No seu computador a tabela ARP pode ser visualizada abrindo o prompt de comando e digitando "arp -a".

```

C:\Windows\system32\cmd.exe
Microsoft Windows [versão 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.

C:\Users\dltec>arp -a

Interface: 192.168.1.55 --- 0xc
Endereço IP      Endereço físico      Tipo
192.168.1.1     28-93-fe-6c-e1-63  dinâmico
192.168.1.11    e0-cb-4e-cc-9b-9b  dinâmico
192.168.1.18    1c-c1-de-f9-3f-53  dinâmico
192.168.1.52    00-18-e7-61-77-a8  dinâmico
192.168.1.54    c0-18-85-e5-ec-bf  dinâmico
192.168.1.255   ff-ff-ff-ff-ff-ff  estático
224.0.0.22       01-00-5e-00-00-16  estático
224.0.0.252     01-00-5e-00-00-fc  estático
224.0.1.60       01-00-5e-00-01-3c  estático
239.255.255.250 01-00-5e-7f-ff-fa  estático
255.255.255.255 ff-ff-ff-ff-ff-ff  estático

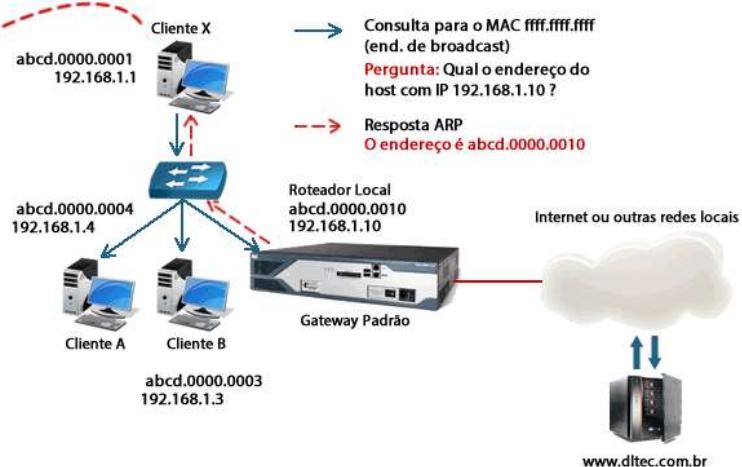
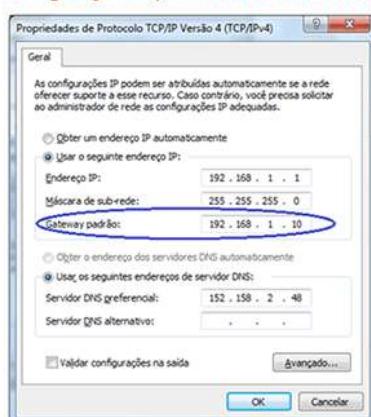
```

Na tabela ARP ficam apenas os endereços MAC dos computadores que estão na mesma rede local e alguns endereços especiais que são configurados nos dispositivos, como os de broadcast (255.255.255.255 – ffff.ffff.ffff) e multicast (veremos no capítulo de endereçamento IP mais detalhes sobre a faixa de endereços IP).

Quando a comunicação é realizada com um host que não pertence à mesma LAN o roteador local entra em cena servindo de intermediário, pois como já vimos anteriormente é o roteador que conhece as rotas para demais redes. Nesse caso o computador que deseja enviar as informações para fora da rede consegue distinguir que o destino não pertence à mesma rede e envia uma requisição ARP solicitando o endereço MAC do roteador local, o qual está configurado em sua placa de rede como "roteador padrão" ou "gateway padrão".

Quando o roteador recebe a solicitação ele envia seu MAC ao solicitante e a partir daí serve como intermediário da comunicação. Portanto, o quadro terá o MAC de origem do computador solicitante e o MAC de destino será o endereço do roteador local. Porém, no protocolo IP, o endereço de destino não será o do roteador local, e sim o endereço IP do computador de destino, senão não haveria comunicação, pois o roteador não saberia para que interface encaminhar aquele pacote! Veja a figura com a ilustração do funcionamento do ARP quando os hosts comunicantes estão em LANs distintas.

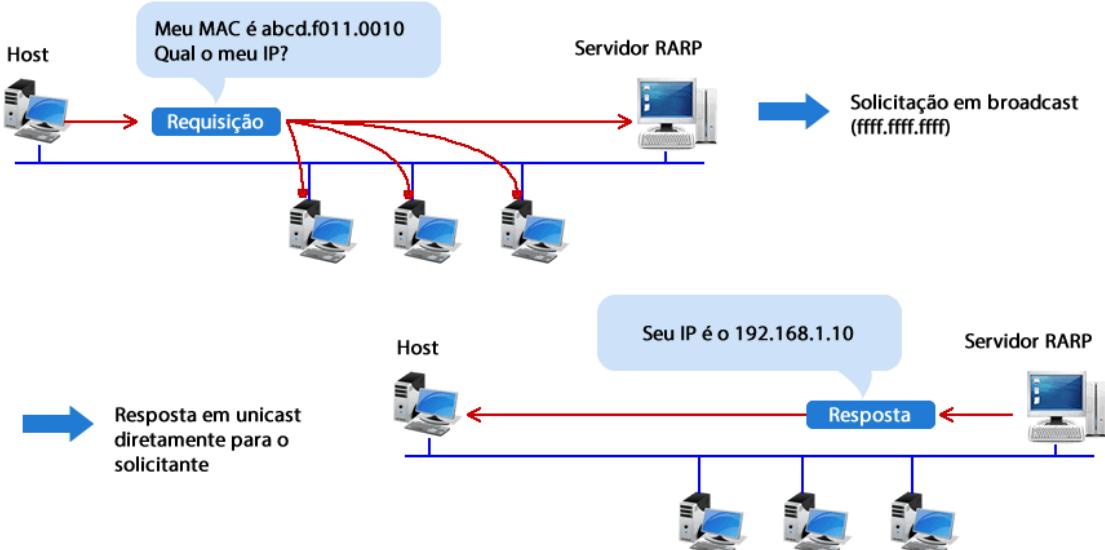
Configuração da placa de rede do ClienteX



Mais para frente você verá que para o computador descobrir o IP do website [www.dltec.com.br](http://www.dltec.com.br) ele precisará utilizar primeiro o protocolo de resolução de nomes de Internet, chamado DNS.

Já o Reverse Address Resolution Protocol (RARP) ou Protocolo de Resolução Reversa de Endereços associa um **endereço MAC conhecido a um endereço IP**. Permite que os dispositivos de rede encapsulem os dados antes de enviá-los à rede. Um dispositivo de rede, como uma estação de trabalho sem disco, por exemplo, pode conhecer seu endereço MAC, mas não seu endereço IP.

O RARP permite que o dispositivo faça uma solicitação para saber seu endereço IP. Os dispositivos que usam o RARP exigem que haja um **servidor RARP** presente na rede para responder às solicitações RARP. O RARP caiu em desuso devido a sua função ser praticamente a mesma que a dos servidores de DHCP (atribuição dinâmica de endereços IP para hosts). Veja a figura abaixo com uma ilustração do funcionamento do RARP.



No servidor RARP o administrador de rede deve ter pré-configurado todos os MACs dos micros que participam desse processo de inicialização e vinculado IPs a essas máquinas.

### 2.2.3 Protocolos de Roteamento

Uma das funções da camada de Internet, assim como a camada de rede do modelo OSI, é fornecer a conectividade através do roteamento dos pacotes por entre as diversas redes que compõe uma Intranet ou até mesmo na Internet.

Quem cumpre esse papel de descobrir as rotas e inseri-las nas tabelas de roteamento são os administradores de rede ou então os protocolos de roteamento dinâmicos. Quando o próprio administrador configura as rotas em um roteador ou endpoint chamamos esse processo de roteamento estático, pois a parte “inteligente” de descoberta de rotas é feita por um ser humano e no roteador serão inseridas rotas manuais definidas pelo administrador de rede para as diversas redes que compõe a Intranet e também a saída para a Internet. Esse processo manual é mais econômico para os dispositivos, pois quem pensa é o administrador, porém mais complicado de administrar.

Os protocolos de roteamento dinâmicos tem a função de analisar os endereços de rede de cada roteador e descobrir sozinho os melhores caminhos para as diversas redes que compõe a infraestrutura de uma empresa.

Temos protocolos de roteamento específicos para as Intranets, chamados de IGP (Interior Gateway Protocol), tais como o RIP, OSPF, IS-IS e EIGRP. Na Internet com o protocolo IP versão 4 o protocolo de roteamento utilizado entre os diversos provedores de serviço, operadoras de Telecomunicação e empresas com Sistemas Autônomos (que possuem sua própria faixa de endereços de Internet) é o BGP-4 (Border Gateway Protocol versão 4).

Portanto, um protocolo de roteamento dinâmico tem um processo que roda nos roteadores, coletando e trocando informações sobre rotas entre eles. Essas informações são processadas em cada roteador e uma decisão sobre a melhor rota é tomada para que a tabela de roteamento seja alimentada.

Os computadores também tem tabela de roteamento, não somente os roteadores. Para você visualizar a tabela de rotas do seu computador com sistema operacional Windows, basta entrar mais uma vez no prompt de comando e digitar “route print”. Veja a saída do comando na tela da figura abaixo. Note logo abaixo da frase “Tabela de rotas IPv4” temos uma rota para a rede 0.0.0.0, esta é a rede que representa a Internet e está vinculada ao seu roteador local padrão, chamado de default gateway. Esta rota tem a propriedade de encaminhar os pacotes com destinos desconhecidos para um dispositivo que servirá como ponte entre o computador e a Internet ou demais redes LAN e WAN da sua Intranet.

```
C:\Windows\system32\cmd.exe
C:\Users\dltec>route print
=====
Lista de interfaces
12...c0 18 85 e5 ee db .....Dell Wireless 1702 802.11b/g/n
 1.....Software Loopback Interface 1
24...00 00 00 00 00 00 e0 Adaptador do Microsoft ISATAP
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
26...00 00 00 00 00 00 e0 Adaptador do Microsoft ISATAP #2
28...00 00 00 00 00 00 e0 Adaptador do Microsoft ISATAP #5
=====

Tabela de rotas IPv4
=====
Rotas ativas:
Endereço de rede      Máscara    Ender. gateway      Interface   Custo
  0.0.0.0          0.0.0.0    192.168.1.1      192.168.1.55     25
  127.0.0.0        255.0.0.0  No vínculo       127.0.0.1      306
  127.0.0.1        255.255.255.255  No vínculo       127.0.0.1      306
  127.255.255.255 255.255.255.255  No vínculo       127.0.0.1      306
  192.168.1.0      255.255.255.0  No vínculo       192.168.1.55     281
  192.168.1.55      255.255.255  No vínculo       192.168.1.55     281
  192.168.1.255     255.255.255.255  No vínculo       192.168.1.55     281
  224.0.0.0          240.0.0.0  No vínculo       127.0.0.1      306
  224.0.0.0          240.0.0.0  No vínculo       192.168.1.55     281
  255.255.255.255  255.255.255.255  No vínculo       127.0.0.1      306
  255.255.255.255  255.255.255.255  No vínculo       192.168.1.55     281
=====

Rotas persistentes:
Nenhuma
```

Quando estamos em um roteador a tabela de roteamento fica um pouco diferente, porém o princípio é o mesmo para o processo de roteamento de um pacote. O roteador irá analisar o endereço IP de destino, verificar se existe uma rota explícita para essa rede e se tiver encaminhar o pacote para a interface de saída.

Caso o roteador não encontre uma rota explícita para a rede de destino existem duas possibilidades, ou ele tem um gateway padrão configurado e encaminha os pacotes para esse gateway ou então descarta esses pacotes, ou seja, joga fora os pacotes (chamado de "drop", muitas vezes pessoas da área falam "pacotes dropados" o que significa que foram descartados pelo roteador).

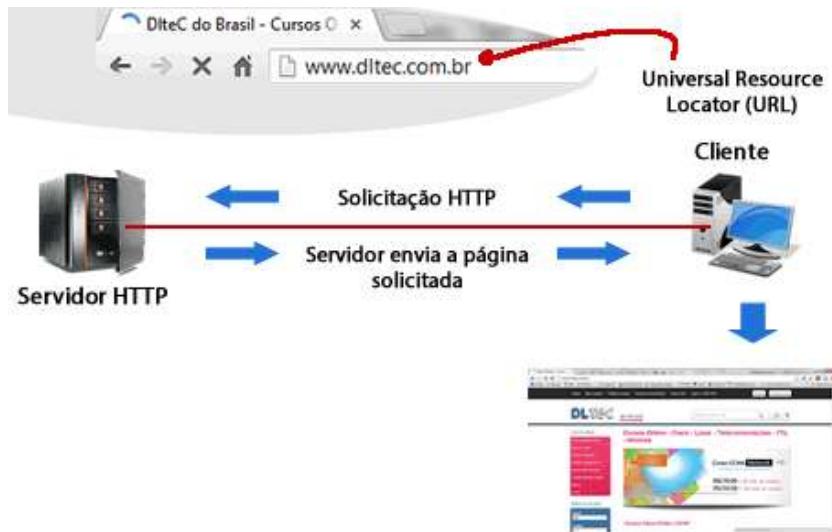
Sempre tenha em mente ao configurar um host manualmente que você precisará do seu endereço IP e máscara (veremos em outro capítulo com detalhes), seu gateway ou roteador padrão e pelo menos um servidor de resolução de nomes de Internet (DNS).

### 2.3 Camada de Transporte

Vimos anteriormente que nas camadas de acesso aos meios e Internet que os pacotes e quadros são transmitidos por uma rede TCP/IP. É nessas camadas que o transporte da informação de um ponto a outro realmente se dá através da rede. Já na camada de transporte, a qual equivale à camada 4 do Modelo OSI, é onde o aplicativo do usuário irá escolher o tipo de serviço de rede que ele deseja, se confiável ou mais rápido (não confiável).

Os dois protocolos utilizados pelo TCP/IP são o **TCP** (confiável e orientado a conexão) e o **UDP** (não orientado a conexão, porém mais veloz). Além disso, os protocolos TCP e UDP também tem a função de identificar cada fluxo que os aplicativos abrem com a rede para que possamos utilizar várias conexões simultâneas de rede, multiplexando (compartilhando) o meio entre os diversos programas do seu computador que precisam acessar as redes.

Para entender o funcionamento de uma rede com protocolo TCP/IP devemos ter em mente que a grande maioria das aplicações e serviços de rede são arquiteturas **Cliente/Servidor**. Você pode até não ter ouvido esse termo ainda, mas usa diariamente quando acessa uma página de web, pois seu micro utiliza um browser (IE, Mozilla, Google Chrome) que é um **cliente** para o serviço de web (protocolo HTTP ou HTTPS) e a página que você acessa está hospedada (instalada ou guardada) em um **servidor** web (servidor HTTP ou HTTPS).



É claro que muitas vezes o seu micro pode se tornar um servidor também, por exemplo, quando você compartilha uma impressora ou arquivos em rede através do seu micro ele estará atuando como servidor quando outro usuário de rede estiver imprimindo ou puxando arquivos das suas pastas.

Resumindo o assunto, os servidores sempre estão prontos para receber uma conexão de rede e fornecer um determinado serviço, já os clientes são os solicitantes que irão utilizar esses serviços.

Mas se temos dois tipos de entregas na camada de transporte através do TCP ou UDP o que determina qual deles utilizar? Na realidade o que determina essa escolha é o tipo de aplicação a ser utilizada. Cada desenvolvedor deve escolher entre um protocolo mais confiável, porém mais lento, ou um protocolo de transporte mais rápido, porém sem controle de fluxo ou erros, ficando para a sua aplicação essa tarefa. Existe já uma gama de protocolos utilizados e já bem conhecidos que utilizam TCP ou UDP, os quais foram identificados através de um endereçamento, aqui chamado de número de porta, padronizado globalmente.

Esses endereços ou portas TCP e UDP tem um máximo de 16 bits, o que nos dá um máximo de 65536 possíveis portas. O órgão internacional chamado "Internet Assigned Numbers Authority" (IANA) é o responsável por manter a alocação oficial do número de portas TCP e UDP em uso atualmente, porém muitas empresas acabam fazendo o uso de endereços bem conhecidos ou registrados para outros protocolos na prática. Esse endereçamento está atualmente dividido da seguinte maneira:

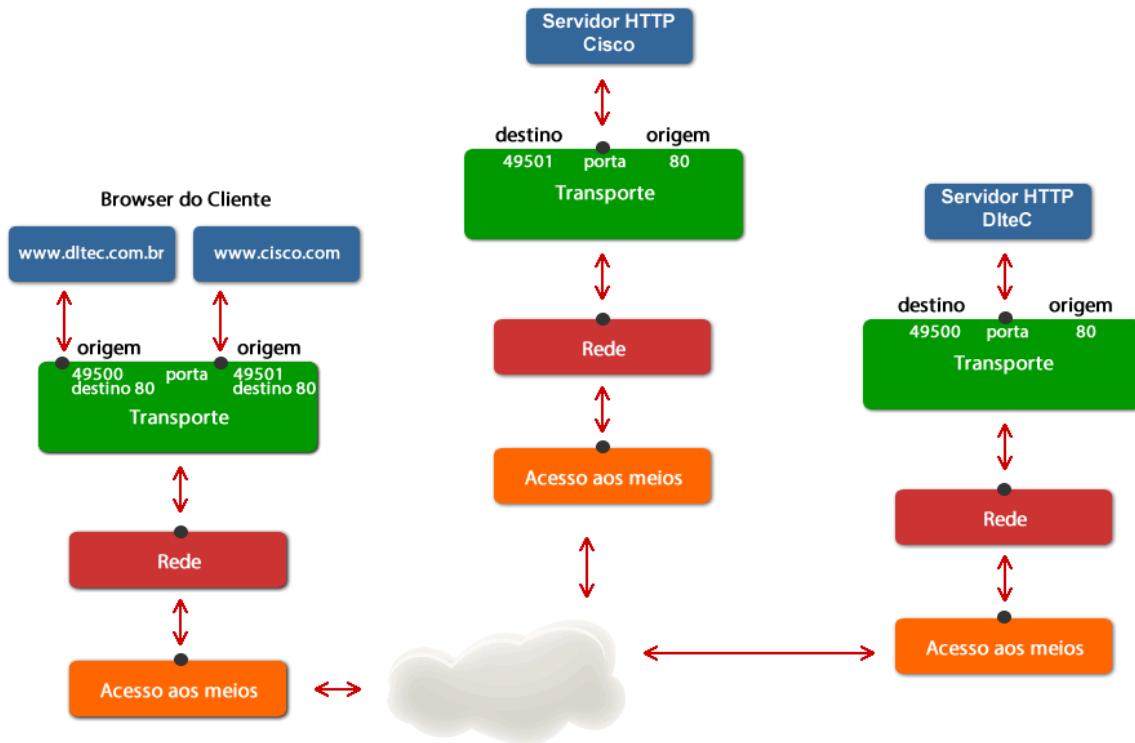
- As portas TCP mais usadas (também chamadas de "**well known ports**") são as portas de **0 a 1023**, que são reservadas para serviços mais conhecidos e utilizados, tais como servidores web, FTP, servidores de e-mail, compartilhamento de arquivos, etc. A porta 80, por exemplo, é reservada para uso de servidores web, enquanto a porta 21 é a porta padrão para servidores FTP. A porta "0" é reservada, por isso não entra realmente na lista.
- As portas de **1024 até 49151** são as portas registradas, normalmente utilizadas por aplicativos conhecidos no mercado, mas podem ser utilizadas para outras finalidades, o que não ocorre com a faixa de portas bem conhecidas vistas anteriormente.
- As portas entre os valores de **49152 a 65535** são chamadas portas para uso de clientes ou de uso efêmero. Não podem ser registradas oficialmente como a faixa anterior das portas registradas.

Essa numeração das portas TCP e UDP de origem e destino estão no quadro de ambos protocolos e é utilizada para identificar um processo ou um fluxo trocado entre um aplicativo cliente de um determinado host e um servidor remoto. Tanto no TCP como no UDP, quando um aplicativo do usuário do computador solicita acesso à determinado serviço de rede, uma porta de origem é criada para vincular aquele fluxo de informações recebidas com o aplicativo do usuário. Essa porta de origem pega um valor da faixa entre 49152 a 65535.

Já a porta de destino que o protocolo vai selecionar depende do serviço que o aplicativo cliente deseja acessar, por exemplo, se você está tentando acessar a Internet será utilizado o protocolo TCP, a porta de origem entre 49152 a 65535 e a porta de destino a 80, pois o serviço de web (HTTP) está em uma porta bem conhecida. Esse número escolhido como porta de origem nunca irá se repetir dentro de um mesmo computador, pois é ele que identifica a conexão com um determinado aplicativo.

Por exemplo, você abriu o browser e digitou [www.dltec.com.br](http://www.dltec.com.br), com isso seu computador escolheu a porta de origem aleatoriamente como 49500 e o destino como porta 80 (padrão para serviço de web). Em seguida você clica para abrir uma nova aba em seu browser e digita [www.cisco.com](http://www.cisco.com), o que vai acontecer?

Provavelmente seu computador irá identificar esse fluxo TCP com a porta de origem 49501 e a porta de destino como 80. Quando o servidor da DLTEC responder para você, ele responde na porta 49500 e quando o da Cisco responder ele irá enviar suas informações na porta 49501, portanto você está acessando duas páginas diferentes, com o mesmo serviço de rede sem problema algum, porque o TCP, ou melhor, a camada de transporte fez a identificação dos fluxos através do número de porta! Veja a ilustração a seguir.



Quando você instala uma aplicação com a função de servidor ela irá utilizar então uma porta fixa para prestar o serviço de rede escolhido, por exemplo, você habilita o serviço HTTP para fazer uma página interna da sua empresa (Intranet), ao final da instalação ou ativação do serviço uma porta TCP com o número ou endereço 80 será aberta em seu computador ou servidor.

A partir desse momento nenhum outro programa pode mais utilizar essa porta TCP. Além disso, essa porta fica “aberta”, o que quer dizer que ela fica esperando conexões de clientes que venham a solicitar sua página (seu serviço). No TCP dizemos que a porta fica em um estado chamado “listening” ou “escutando”. Se você instalou um programa que utiliza o UDP como serviço de transporte ela fica aberta, porém a porta não tem um estado definido no UDP por ele não ser um serviço orientado a conexão.

No Windows e no Linux você pode utilizar no prompt de comando o “Netstat” para verificar o estado das portas e conexões TCP ou UDP. Com o comando “netstat -a” você consegue ver todas as portas que estão em modo de escuta, ou seja, portas abertas para conexões externas.

As portas TCP aparecerão como “escutando” ou “listening” e as UDP como “\*.\*”. Muitos serviços dos próprios sistemas operacionais podem abrir uma porta de servidor em seu computador, assim como vírus e Cavalos de Tróia, portanto cuidado com o que você instala em seu computador. Veja um exemplo do comando na figura abaixo.

Proto	Endereço local	Endereço externo	Estado
TCP	0.0.0.0:135	dltec-marcelo:0	LISTENING
TCP	0.0.0.0:445	dltec-marcelo:0	LISTENING
TCP	0.0.0.0:554	dltec-marcelo:0	LISTENING
TCP	0.0.0.0:912	dltec-marcelo:0	LISTENING
TCP	0.0.0.0:2869	dltec-marcelo:0	LISTENING
TCP	0.0.0.0:5357	dltec-marcelo:0	LISTENING
TCP	0.0.0.0:10243	dltec-marcelo:0	LISTENING
TCP	0.0.0.0:49152	dltec-marcelo:0	LISTENING
TCP	0.0.0.0:49153	dltec-marcelo:0	LISTENING
TCP	0.0.0.0:49154	dltec-marcelo:0	LISTENING
TCP	0.0.0.0:49155	dltec-marcelo:0	LISTENING
TCP	0.0.0.0:49157	dltec-marcelo:0	LISTENING
TCP	127.0.0.1:5939	dltec-marcelo:0	LISTENING
TCP	127.0.0.1:6999	dltec-marcelo:0	LISTENING
TCP	127.0.0.1:37848	dltec-marcelo:0	LISTENING
TCP	127.0.0.1:62514	dltec-marcelo:0	LISTENING
TCP	192.168.1.55:139	dltec-marcelo:0	LISTENING
TCP	192.168.1.55:55389	HP1CC1DEF93F53:microsoft-ds	ESTABLISHED
TCP	192.168.1.55:56874	channel-ig-12-01-snc7:https	ESTABLISHED
TCP	192.168.1.55:56913	web:imap	ESTABLISHED
TCP	192.168.1.55:57022	64.212.172.139:http	CLOSE_WAIT
TCP	192.168.1.55:57859	64.212.172.139:http	CLOSE_WAIT
TCP	192.168.1.55:57126	64.212.172.139:http	CLOSE_WAIT
TCP	192.168.1.55:57249	64.212.172.139:http	CLOSE_WAIT
TCP	192.168.1.55:57250	64.212.172.139:http	CLOSE_WAIT
TCP	192.168.1.55:57251	64.212.172.139:http	CLOSE_WAIT

O proto é o tipo de protocolo, o endereço local é o IP e porta que estão listados, o endereço externo indica um IP remoto caso haja uma conexão estabelecida naquele momento e o estado é o status da porta, se estiver em **listening**, **escuta** ou **\*.\*** significa que a porta está aberta e existe um serviço em modo servidor esperando conexões por ela. Por exemplo, analisando a figura 3 você verá bem no início que as portas 135, 445 e 912, as quais são portas bem conhecidas (abaixo de 1023), estão abertas. Você agora pode ir até o site abaixo e consultar o que fazem esses serviços:

<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>

Ao entrar com esse comando podem aparecer outros estados de porta relativos ao TCP que veremos na sequência quando estudarmos os dois protocolos mais detalhadamente. Com o comando "netstat -n" você pode analisar as conexões que estão em andamento do TCP/IP no seu computador.

Os firewalls normalmente tem sua atuação sobre os endereços IP e principalmente as portas TCP e UDP, pois elas que indicam que serviços podem ou não ser acessados em uma rede.

Vamos agora ver mais características e funcionamento específico dos protocolos TCP e UDP.

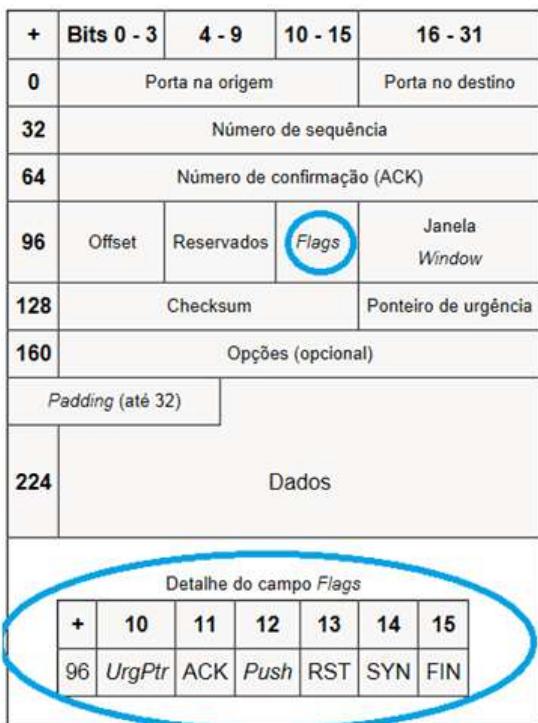
### 2.3.1 Protocolo TCP

O protocolo TCP (Transmission Control Protocol) é um protocolo de transporte confiável, pois ele é orientado a conexão, ou seja, primeiro ele verifica a disponibilidade do destino para depois fazer uma conexão e enviar os dados. O TCP possui controle de fluxo, sequenciamento dos segmentos enviados (o que permite fazer a reordenação dos segmentos no destino antes de enviar os dados à camada de aplicação), retransmissão de segmentos (caso haja perda no caminho entre a origem e o destino), ou seja, é um protocolo que tem entrega garantida e tira da aplicação a preocupação e tarefas relacionadas a esse tema.

Sua vantagem é essa confiabilidade, porém isso tudo tem um custo: "a velocidade". Devido a todos esses controles o TCP acaba se tornando mais lento que o UDP, portanto ele é recomendado para aplicações que não sejam em tempo real. Por exemplo, no caso da transmissão de voz sobre o protocolo IP (VoIP), imagine o atraso e complicações que todo esse controle traria para a comunicação? Até todas as confirmações serem realizadas as duas pessoas que estão falando ao telefone já desistiram de falar!

Porém, para serviços como o de páginas de web (HTTP e HTTPS), e-mail (SMTP, POP3 e IMAP), terminais virtuais (SSH e Telnet), acesso a arquivos via Internet (FTP e SFTP) o TCP se aplica perfeitamente, pois é muito melhor esperar um pouco para ter sua página de web impressa na tela corretamente que ter figuras faltando pedaços ou letras trocadas. Esses tipos de serviço suportam bem os atrasos causados pelas confirmações.

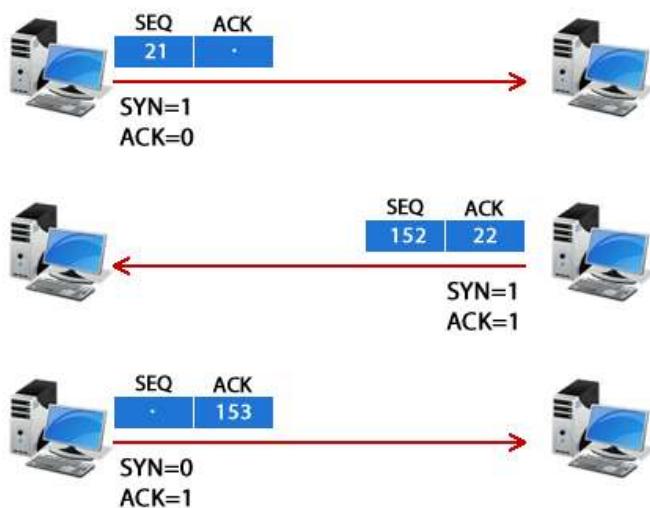
Mas como o TCP opera? Conforme já mencionado, o TCP é um protocolo orientado a conexão, por isso antes de iniciar a transmissão dos segmentos entre as duas pontas ele precisa verificar a disponibilidade do destino e também abrir uma conexão entre os dois. Esse processo é chamado de processo de sincronização, através do **Handshake de Mão Tripla** ou de **Três Vias**. Veja na figura 1 ao lado, onde mostramos o cabeçalho do protocolo TCP. Note o campo "Flags" que no detalhe abaixo mostra que são 6 bits e temos um deles chamado SYN (sincronizar) e outro ACK (reconhecimento).



Quando um host está abrindo uma sessão TCP com o servidor ele envia o quadro do TCP com o SYN setado em 1, o ACK em zero e no campo número de sequência ele envia um valor que será utilizado como numeração dos bytes dos seus segmentos.

Quando o destino recebe esse segmento ele automaticamente responde com o ACK setado 1 e com um valor no campo de confirmação que é o número enviado no campo do número de sequência somado 1, significando que ele recebeu a sequência enviada e reconheceu. Além disso, o destino coloca seu SYN em 1 e no campo do número de sequência ele insere seu valor inicial.

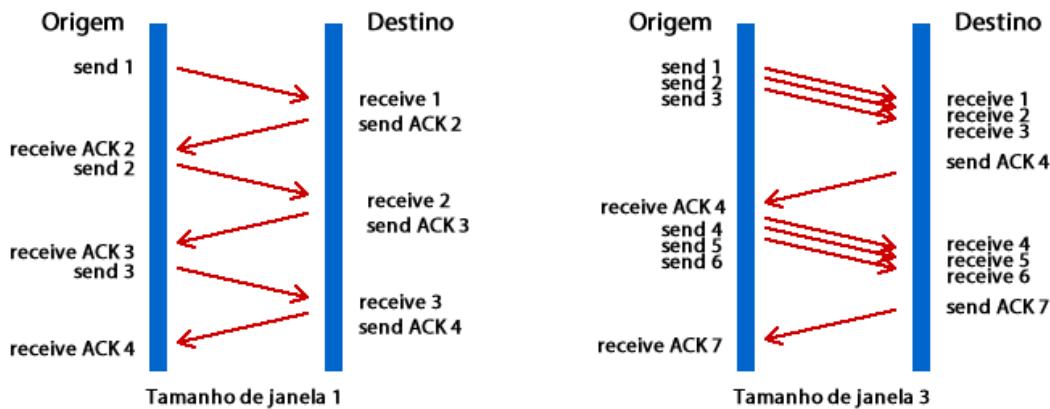
Agora a origem recebe esse segmento, responde com um ACK setado em um e seu número de confirmação como o número de sequência enviado pelo destino mais 1. Agora o handshake foi finalizado e os dois computadores iniciarão a troca de informações. Veja na figura abaixo a ilustração do que foi lido até o momento do handshake triplo.



O número de sequência passado entre o host e o servidor é chamado de ISN (Initial Sequence Number) ou número inicial de sequenciamento. É com esse valor que os bytes que serão trocados após a abertura da conexão serão numerados.

Uma vez estabelecida a sessão, agora os segmentos com informação útil serão trocados, aí entra em ação o “Slow start” ou algoritmo de início-lento, o qual visa iniciar transmitindo poucos bytes até chegar a um valor otimizado, o qual pode variar durante a transmissão de acordo com as condições da rede. O processo de definir quantos bytes será trocado entre a origem e o destino é chamado “janelas deslizantes” ou “janelamento”.

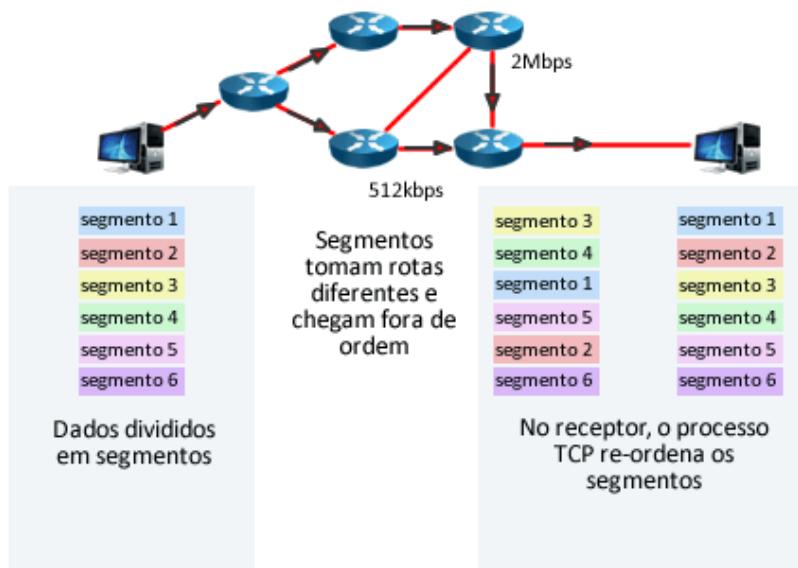
O termo janela foi utilizado porque você pode aumentar (abrir a janela) ou diminuir (fechar a janela) o tamanho em bytes que será inserido no campo de dados do quadro TCP. Veja os exemplos da figura abaixo onde temos uma janela de 1 Byte e outra com 3 Bytes.



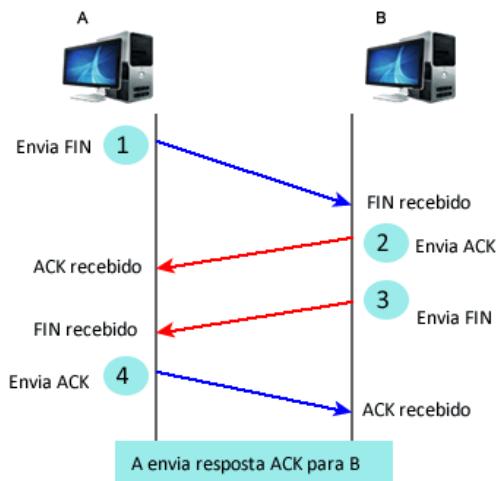
O cabeçalho TCP possui um parâmetro que permite indicar o espaço livre atual do destino: a janela (ou window). Assim, a origem fica sabendo que só poderá ter em trânsito aquela quantidade de informação até esperar pela confirmação (ACK) de um dos pacotes - que por sua vez trará, com certeza, uma atualização da janela.

Caso seja recebido um número de confirmação (ACK) menor que o esperado quer dizer que houve perda de pacotes e esses deverão ser retransmitidos, porém se a confirmação continuar a vir menor que a esperada pode significar um congestionamento na rede e uma nova janela, agora menor, terá que ser negociada. Esse processo de reconhecimento dos bytes recebidos e retransmissão em caso de perda garantem a confiabilidade na entrega das informações.

Outro recurso do TCP é o sequenciamento, o qual foi iniciado com a troca dos números iniciais de sequenciamento ou ISN durante o handshake. Com essa numeração dos segmentos o destino pode verificar se os pacotes chegaram na ordem correta e caso tenham chegado fora de ordem, reordená-los antes de enviar para a camada de aplicação.



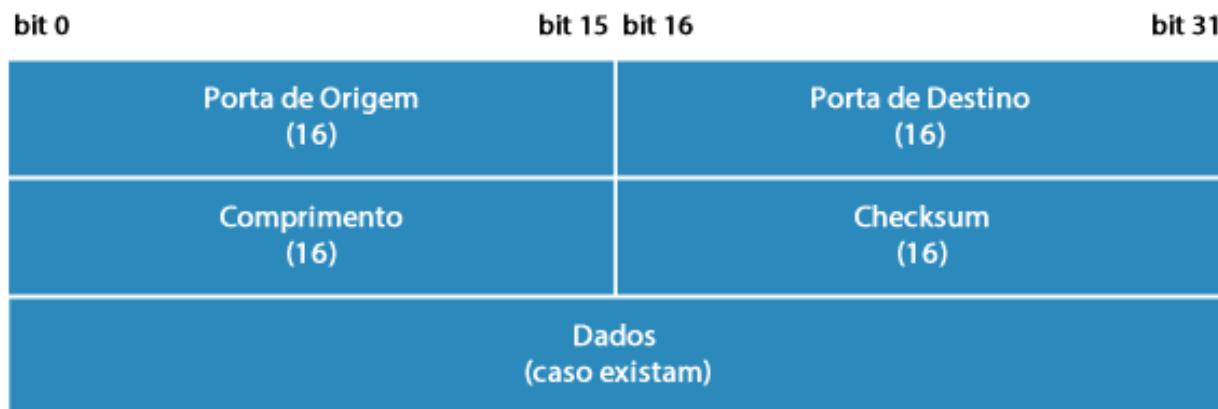
Assim como o TCP abre uma conexão ele também pode fechá-la com o sinal FIN, veja a sequência de fechamento de uma sessão TCP.



Chegamos ao final do estudo do TCP e podemos chegar a conclusão que sua palavra chave é “confiabilidade”!

### 2.3.2 Protocolo UDP

O protocolo UDP (User Datagram Protocol) é um protocolo simples da camada de transporte, o qual permite que a aplicação envie um datagrama encapsulado em um pacote IPv4 ou IPv6, que então é enviado ao destino, porém sem qualquer tipo de garantia de entrega do pacote. Veja na figura abaixo como o datagrama UDP é muito mais simples que o segmento TCP.



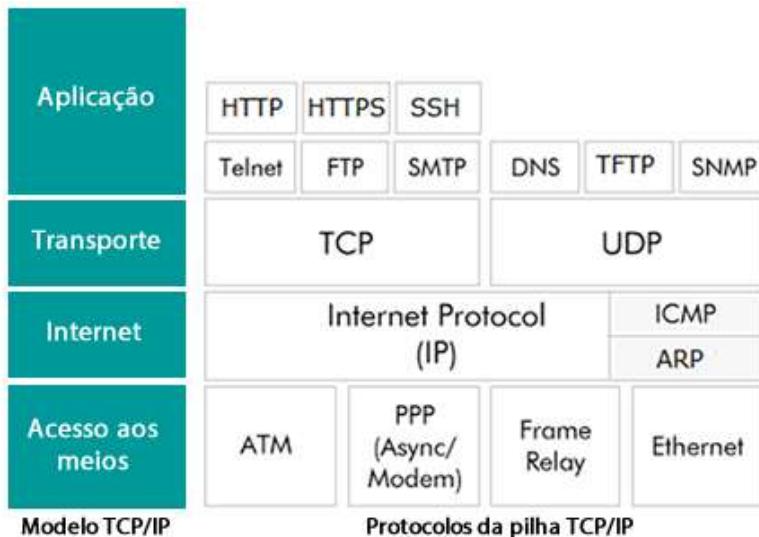
Por esse motivo o protocolo UDP é dito não é confiável. Caso garantias sejam necessárias, é preciso implementar uma série de estruturas de controle, tais como timeouts, retransmissões, acknowledgments, controle de fluxo, etc. no aplicativo do usuário (tanto no cliente como no servidor).

Também dizemos que o UDP é um serviço **sem conexão**, pois não há necessidade de manter um relacionamento entre cliente e o servidor, como é o caso do TCP. Assim, um cliente UDP pode enviar um datagrama para um servidor sem a necessidade de qualquer tipo de inicialização.

O UDP é utilizado em protocolos de tempo real, por exemplo, o RTP (Real Time Protocol) utilizado para transportar voz sobre o protocolo IP, devido à sua velocidade. Outros exemplos de protocolos que utilizam o UDP são as redes virtuais privadas ou VPNs e o serviço de TFTP (Trivial FTP).

## 2.4 Camada de Aplicação

A camada superior é chamada de camada de aplicação equivalente às camadas 5, 6 e 7 do Modelo OSI. Os protocolos mais conhecidos na camada de aplicação são: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, DNS, DHCP, POP3, IMAP, SMTP e SNMP, os quais iremos estudar com mais um pouco de detalhe na sequência.



A camada de aplicação é a porta de entrada para que os aplicativos possam acessar a rede e chegarem até os servidores para a utilização dos serviços. Ela é quem define se utilizaremos TCP ou UDP, por exemplo.

O método mais simples para testar a camada de aplicação é acessando um serviço, por exemplo, ao instalar uma rede tente acessar uma página da web, assim você terá certeza que todas as camadas estão funcionando.

Vale a pena aqui ressaltar que a camada de aplicação está em contato com os programas instalados nos servidores e clientes. Por exemplo, o serviço de web HTTP e HTTPS (versão segura do HTTP) são acessados via um browser, como por exemplo, o Mozilla. Já o servidor HTTP/HTTPS onde as páginas serão hospedadas pode ser um Apache ou um IIS (Internet Information Services) da Microsoft.

#### 2.4.1 Serviços de Acesso a Páginas de Web – HTTP e HTTPS

O HTTP (Hypertext Transfer Protocol - Protocolo de Transferência de Hipertexto) é um protocolo da camada de aplicação que utiliza como transporte o TCP e fica disponível na porta 80 nos servidores. Trata-se do serviço básico utilizado pelos navegadores de Internet ou browsers para acessar o conteúdo das páginas web normalmente escritos na linguagem HTML (HyperText Markup Language - Linguagem de Marcação de Hipertexto). Contudo, para haver comunicação com o servidor onde o site da web está hospedado é necessário utilizar comandos adequados, que não estão em linguagem HTML.

Este serviço pode ser organizado em uma arquitetura two-tier, onde são servidas páginas web estáticas, ou three-tier, onde o servidor web busca informações de outras fontes (bancos de dados ou outros serviços) para construir as páginas solicitadas de maneira dinâmica.

Sua versão segura (com criptografia) é o HTTPS (HyperText Transfer Protocol Secure) que também utiliza o protocolo TCP como transporte, porém nos servidores é disponibilizado na porta 443. O HTTPS é uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS. Essa camada adicional permite que os dados sejam transmitidos através de uma **conexão criptografada** e que se verifique a autenticidade do servidor e do cliente através de **certificados digitais**.

Os clientes utilizados para acessar as páginas de web via HTTP são os navegadores de Internet, conhecidos como "Browsers", os quais os mais conhecidos são o Internet Explorer, Mozilla Firefox, Google Chrome, Safari e Opera.

Já os servidores web (HTTP Servers ou Web Servers) mais utilizados são o Apache e IIS (Internet Information Services), porém na tabela abaixo você encontra a mais recente estatística de servidores de web atualmente utilizados no mercado realizada em julho de 2012 pela empresa de pesquisas Netcraft.

Produto	Fabricante	Número de Websites Postados	Percentual de Uso
Apache	Apache	409,185,675	61.45%
IIS	Microsoft	97,385,377	14.62%
nginx	NGINX, Inc.	73,833,173	11.09%
GWS	Google	22,931,169	3.44%

O funcionamento das páginas de web está intimamente ligado com o serviço de resolução de nomes ou DNS que veremos a seguir, pois na Internet os roteadores reconhecem os endereços IP e não os nomes de página, porém ficaria impraticável decorar os endereços IP das páginas, por isso os websites recebem um "nome de domínio" ou URL (Universal Resource Locator ou Localizador Universal de Recurso), por exemplo, <http://www.dltec.com.br>, para acessar o HTTPS basta digitar <https://www.exemplo.com.br>.

Ao digitar no seu browser <http://www.exemplo.com.br> na realidade ele está enviando ao servidor um comando GET para o endereço IP que o servidor DNS enviou da página e direcionado para a porta 80 do protocolo TCP, como o exemplo abaixo:

```
GET /index.html HTTP/1.1  
Host: www.exemplo.com
```

A resposta do servidor (seguida por uma linha em branco e o texto da página solicitada) pode ser conforme o exemplo abaixo, contendo o código em HTML da página solicitada, a qual será mostrada na tela do seu browser conforme mostrado a seguir.

```
HTTP/1.1 200 OK  
Date: Mon, 23 May 2005 22:38:34 GMT  
Server: Apache/1.3.27 (Unix) (Red-Hat/Linux)  
Last-Modified: Wed, 08 Jan 2003 23:11:55 GMT  
Etag: "3f80f-1b6-3e1cb03b"  
Accept-Ranges: bytes  
Content-Length: 438  
Connection: close  
Content-Type: text/html; charset=UTF-8
```

```
<html>  
<body>  
<h1> Teste de Funcionamento OK! </h1>  
</body>  
</html>
```

```
<img>funcionando.png</img>
```



Lembre que a resposta do servidor terá o IP do servidor e a porta TCP 80 como origem, porém o destino agora será o IP do computador solicitante e sua porta de cliente. Existem diversos outros comandos, porém não vamos entrar em detalhes, pois aqui o intuito é entender a comunicação em rede. Essa transmissão irá continuar até que a página seja toda carregada no browser do computador do cliente.

Outro ponto importante de se observar é que a resposta do servidor é dividida em duas seções, separadas por uma linha vazia:

1. A primeira seção é denominada cabeçalho (header) e contém informações do servidor sobre a URL solicitada: status da resposta, tipo e tamanho da resposta, configuração do servidor, etc.
2. A segunda seção, denominada corpo (body), contém o recurso propriamente dito, solicitado pelo navegador. Está a partir do campo <html>.

Para identificar o tipo do conteúdo da resposta do servidor web temos na linha **Content-type** do cabeçalho da resposta o tipo MIME (Multipurpose Internet Mail Extension) usado, os quais seguem um padrão especificado nas RFCs 2045 a 2048. Alguns exemplos de tipos MIME comuns seguem na tabela abaixo:

Tipo MIME	Significado
text/plain	arquivo de texto puro
text/html	arquivo de texto em formato HTML
image/gif	arquivo de imagem em formato GIF
image/jpeg	arquivo de imagem em formato JPEG
application/pdf	arquivo de aplicação em formato PDF
video/quicktime	arquivo de vídeo em formato QuickTime

Quando utilizamos o HTTPS, antes da realização dos passos acima são trocadas chaves criptográficas e os dados entre o servidor e o cliente serão enviados "criptografados", ou seja, se você capturar os pacotes trocados entre um cliente e um servidor HTTP você poderá ler os dados, porém entre um servidor HTTPS e um cliente esses dados estão "descaracterizados" pelo algoritmo de criptografia utilizado entre o servidor e o cliente.

Para fazer testes de conexão e aprender mais sobre o protocolo HTTP você pode ativar o serviço no seu computador ou o mais recomendado é instalar um programa que atua como webserver, pois depois é mais fácil de desinstalar. Nós utilizamos em nosso laboratório de redes o programa Abyss Web Server X1 Personal Edition, pois ele é gratuito e funciona muito bem para testes. Você pode fazer o download na página do fabricante na URL abaixo:

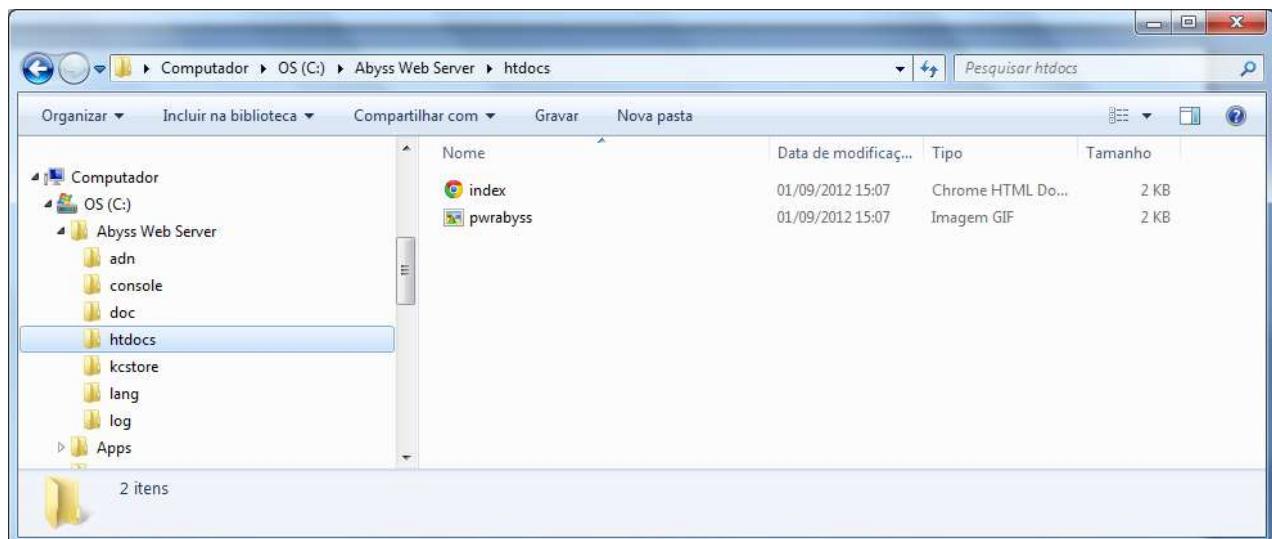
<http://www.aprelium.com/abyssws/download.php>

No momento de instalar, antes de finalizar o programa fará um pergunta conforme mostrado abaixo, escolha inicialização manual (manual startup) para que ele não inicialize sozinho ao ligar o computador, dessa maneira você controla quando utilizar o programa.



Feche a página de configuração que será oferecida a seguir e simplesmente utilize o comando "netstat -a" para verificar se a porta 80 agora está aberta. Para acessar a página padrão do servidor digite <http://localhost> ou <http://127.0.0.1> e utilize o comando "netstat -n" para verificar a conexão local com o servidor. Caso tenham mais computadores na rede você pode verificar seu IP indo no prompt de comando e digitando "ipconfig", vá até o outro computador e digite "http://" seguido do seu endereço IP.

Você pode ainda editar e alterar a página mostrada se desejar, basta ir à pasta de instalação e procurar o "índex.html" dentro da pasta "htdocs", conforme figura a seguir. Para editar o arquivo HTML você pode utilizar o próprio Word ou um bloco de notas.



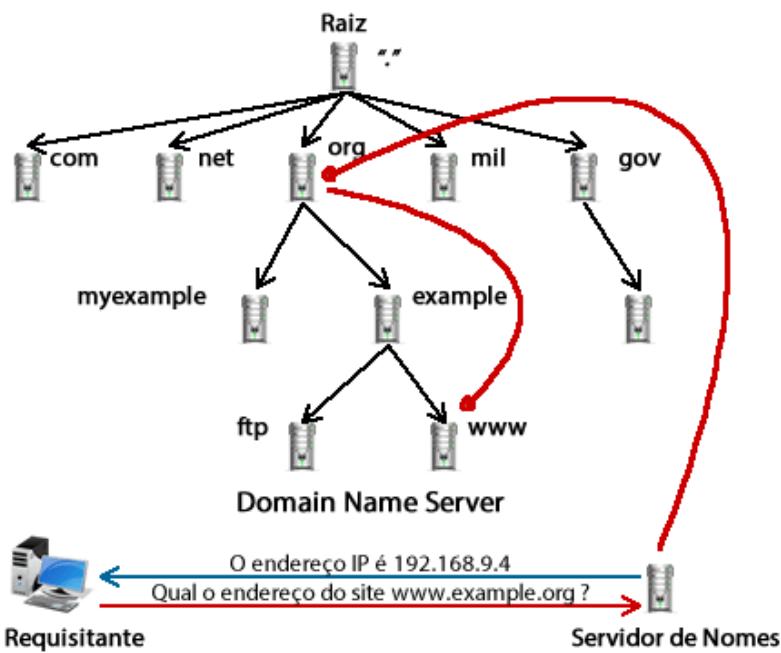
Em um ambiente corporativo o serviço de HTTP é utilizado amplamente e das mais variadas formas. Por exemplo, para publicar sua página institucional ou um comércio eletrônico (e-commerce), para ter uma página de uso interno conhecida como Intranet, onde os funcionários podem ter acesso à arquivos padrões da empresa, informações sobre plano de saúde ou uso dos recursos da corporação, acesso à sistemas de helpdesk e de RH, ou seja, para facilitar o dia a dia dos funcionários.

Além disso, um servidor HTTP pode ser utilizado em conjunto com os sistemas corporativos e servir para acesso a cadastro de clientes, listas de estoque, fazer pedidos de compra, etc. Portanto, esse com certeza é um serviço de alto valor agregado e muito importante para o mundo corporativo em redes!

#### 2.4.2 Serviço de Resolução de Nomes da Internet – DNS

O DNS (Domain Name System – Sistema de Nomes de Domínio) é um sistema usado na Internet para converter os nomes de domínios e seus respectivos nós de rede divulgados publicamente em endereços IP e podemos dizer que ele é o coração da Internet atual! Seu serviço utiliza como transporte o UDP para requisições de cliente e TCP para requisições entre servidores, porém ambos na porta 53.

O serviço de DNS é formado por um conjunto de servidores operando de forma descentralizada, isto é, cada servidor é responsável por um **domínio** ou **sub-domínio** de nomes na Internet.



O que faz o serviço funcionar é o fato dos domínios serem organizados hierarquicamente. Primeiramente temos o servidor raiz (root server), que pode ser entendido como o principal serviço de DNS e é representado por um ponto no final do endereço. A internet conta pelo menos com treze servidores raiz, sendo que dez se localizam nos Estados Unidos, dois na Europa (Estocolmo e Amsterdam) e um na Ásia (Tóquio). Quando há uma falha, os demais conseguem manter o funcionamento da rede.

A hierarquia é seguida com domínios que conhecemos como .com, .net, .org, .info, .edu, .br, .me e várias outros. Estas são chamadas de gTLDs (Generic Top Level Domains - algo como Domínios Genéricos de Primeiro Nível).

Há também terminações orientadas a países, chamadas de ccTLDs (Country Code Top Level Domains - algo como Código de País para Domínios de Primeiro Nível), como por exemplo o ".br" para o Brasil e ".fr" para a França. Além disso, há combinações também como .com.br e .blog.br.

Seguindo a hierarquia vem os servidores de nomes que as empresas e pessoas podem registrar como os domínios com palavras como dltec em dltec.com.br ou google em google.com.br.

Voltando à figura anterior, note que quando o solicitante procurou pelo domínio example.org para seu servidor DNS local esse servidor não sabia como resolver o nome e, portanto, o servidor local fez uma consulta para o .org que chegou ao example.

Se formos olhar dentro de uma determinada rede, um servidor DNS pode estar colocado basicamente com três tipos de função:

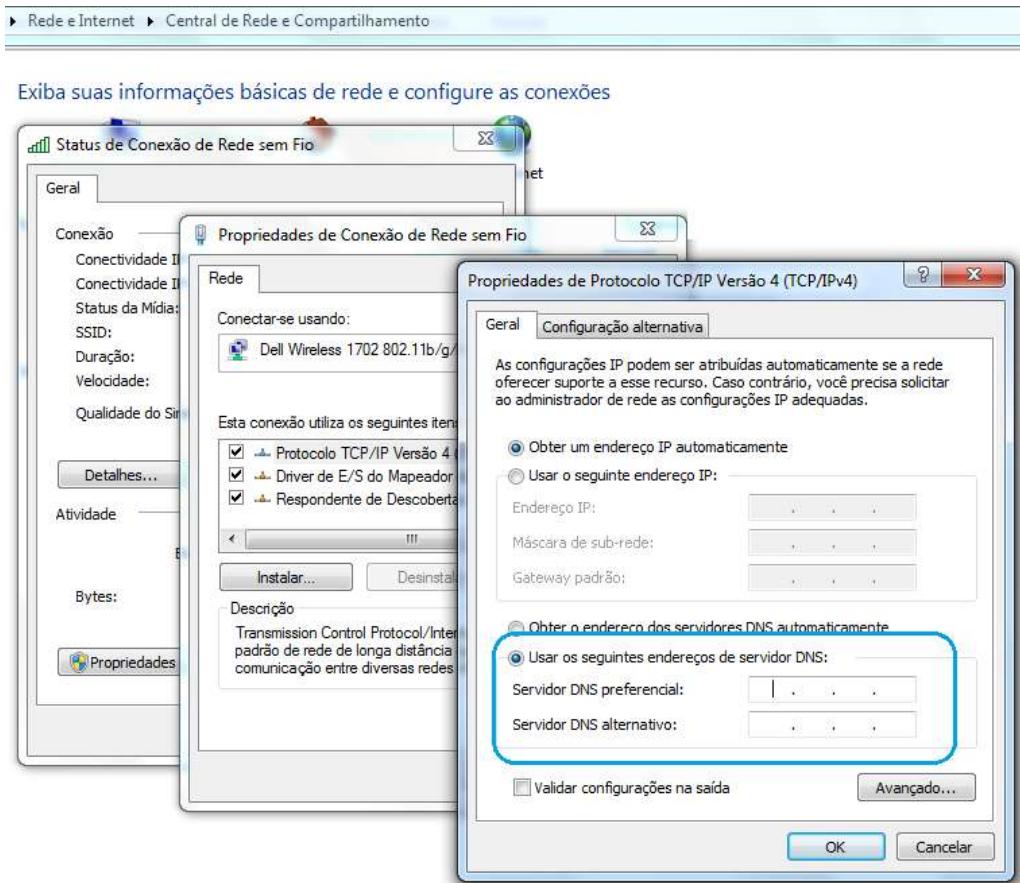
- **DNS Primário:** É o servidor responsável por um domínio, pois toda inclusão, alterações ou exclusão dos registros do domínio são feitas neste servidor.
- **DNS Secundário:** O servidor DNS secundário é uma espécie de cópia de segurança do servidor DNS primário, porém ele também responde às requisições dos clientes quando requisitado.
- **Caching-only:** servidor DNS que apenas efetua consultas e retorna resultados, mantendo um cache local, ou seja, armazena temporariamente os nomes que foram consultados pelos clientes para acelerar o processo de busca. Ele não é responsável por nenhum domínio, sua única função é melhorar o desempenho das resoluções de nome para os clientes locais usando seu cache.

Nos computadores e outros hosts de rede o DNS é um dos parâmetros necessários para o acesso à Internet e muitas vezes também para os servidores internos da rede corporativa. Sua configuração está na placa de rede dos clientes e pode ser feita de maneira estática ou dinâmica através do serviço de DHCP, o qual estudaremos mais tarde.

Para verificar a configuração atual você pode utilizar o comando do Windows "ipconfig /all", veja um exemplo na tela da figura a seguir.

```
C:\Windows\system32\cmd.exe  
Microsoft Windows [versão 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.  
C:\Users\dltec>ipconfig /all  
Configuração de IP do Windows  
Nome do host . . . . . : dltec-marcelo  
Sufixo DNS primário . . . . . :  
Tipo de nó. . . . . : híbrido  
Roteamento de IP ativado. . . . . : não  
Proxy WINS ativado. . . . . : não  
  
Adaptador de Rede sem Fio Conexão de Rede sem Fio:  
Sufixo DNS específico de conexão. . . . . :  
Descrição . . . . . : Dell Wireless 1702 802.11b/g/n  
Endereço Físico . . . . . : C0-18-85-E5-EE-DB  
DHCP Habilitado . . . . . : Sim  
Configuração Automática Habilitada. . . . . : Sim  
Endereço IPv6 de link local . . . . . : fe80::9db:ae76:db9:bccdk12(Preferencial)  
Endereço IPv4. . . . . : 10.0.0.102(Preferencial)  
Máscara de Sub-rede . . . . . : 255.255.255.0  
Concessão Obtida. . . . . : sexta-feira, 31 de agosto de 2012 19:18:48  
Concessão Expira. . . . . : sábado, 1 de setembro de 2012 20:19:02  
Gateway Padrão. . . . . : 10.0.0.1  
Servidor DHCP . . . . . : 10.0.0.1  
IAID de DHCPv6. . . . . : 230692997  
GUID do Cliente DHCPv6. . . . . : 00-01-00-01-15-FB-ED-2F-24-B6-FD-06-DC-17  
Servidores DNS. . . . . : 192.168.1.1  
                          10.0.0.1  
NetBIOS em Tcpip. . . . . : Habilitado
```

A configuração manual do DNS nos clientes é na mesma localização onde configuramos o endereçamento IP. Em ambiente Windows você pode acessar via **Painel de Controle > Central de Rede e Compartilhamento > Exibir o status e as tarefas de rede** e clique na interface de rede que você estiver utilizando. Uma vez na interface clique em Propriedades e procure o **Protocolo TCP/IP versão 4**, onde você verá a tela da figura mostrada abaixo.



Você pode inserir nos clientes mais de um servidor DNS, pois caso o preferencial caia ou fique indisponível seu computador poderá ter um DNS alternativo como backup.

No mundo corporativo muitas empresas têm seus próprios domínios e servidores DNS para resolução de nomes. Em nossas residências utilizamos os servidores DNS disponibilizados pelos provedores de serviço de Internet. Existem também alguns servidores que você pode utilizar de maneira estática caso desconfie que seu servidor DNS não esteja respondendo, um deles é do Google com o endereço primário 8.8.8.8 e secundário 8.8.4.4. Caso seu micro indique uma falha de comunicação com o DNS você pode configurar esses DNSs e se ele responder você terá certeza que o DNS do seu provedor de Internet está com problemas.

Além dos IPs acima do Google Public DNS também existem endereços de servidores de nome em **IPv6**, os quais são primário 2001:4860:4860::8888 e como secundário 2001:4860:4860::8844. Para o IPv6 o serviço de DNS será muito mais importante, pois o endereçamento será mais complexo de você decorar que o IPv4. Basta lembrar que para o IPv4 temos quatro conjuntos de no máximo três algarismos que vão de 0 a 255, por exemplo, 8.8.8.8, já no IPv6 são 8 conjuntos de no máximo quatro algarismos em hexadecimal, ou seja, com letras e números que vão de 0 a 9 e de A a F, por exemplo, 2001:4860:4860::8888. Veremos mais a frente detalhes sobre como escrever e interpretar os endereços de rede tanto em IPv4 como em IPv6.

O comando “**nslookup**” permite efetuar consultas a servidores DNS via linha de comando. Ele é muito utilizado para verificar configurações e diagnosticar problemas no serviço DNS, além de ser utilizado para descobrir o domínio de endereços suspeitos. Veja um exemplo abaixo.

```
C:\Windows\system32\cmd.exe
C:\Users\dltec>nslookup www.google.com
Servidor: UnKnown
Address: 192.168.1.1

Não é resposta de autorização:
Nome: www.l.google.com
Addresses: 2800:3f0:4001:803::1012
          74.125.234.114
          74.125.234.112
          74.125.234.113
          74.125.234.115
          74.125.234.116
Aliases: www.google.com

C:\Users\dltec>nslookup 8.8.8.8
Servidor: UnKnown
Address: 192.168.1.1

Nome: google-public-dns-a.google.com
Address: 8.8.8.8

C:\Users\dltec>
```

Note que na primeira busca utilizamos um nome de domínio para descobrir o IP que está mapeado a ele, já no segundo exemplo utilizamos um endereço IP para descobrir qual o nome de domínio. É interessante aqui que para o site Google.com foram descobertos cinco diferentes endereços IP, pois devido ao número de requisições o serviço do Google está espalhado em nuvem e em diversos servidores virtualizados.

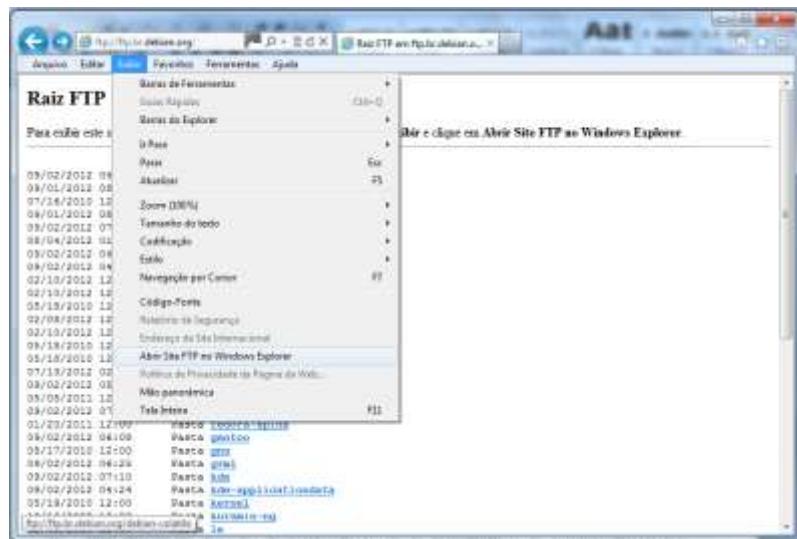
#### 2.4.3 Serviços de Compartilhamento de Arquivos na Web – FTP, TFTP e SFTP

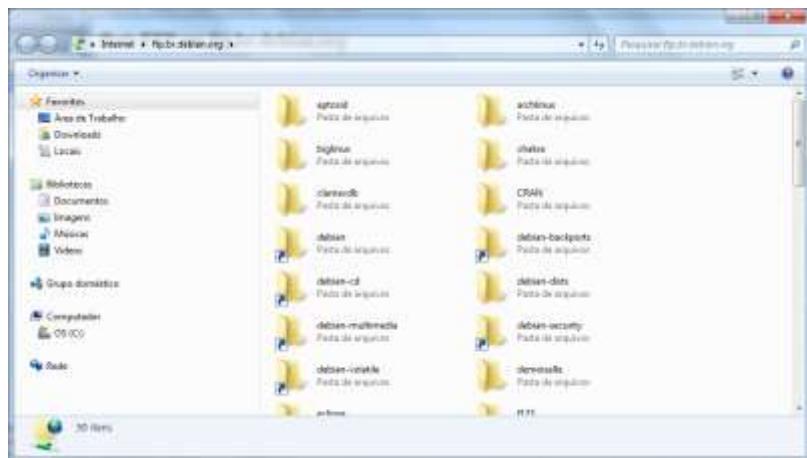
O serviço FTP (File Transfer Protocol – Protocolo de Transferência de Arquivos) é um serviço confiável e orientado a conexões, pois usa o TCP como protocolo de transporte nas portas 20 e 21. Suporta transferências bidirecionais de arquivos binários e ASCII.

O serviço de FTP faz uso de duas portas TCP, ou seja, na portas 20/TCP temos o fluxo de dados e na 21/TCP são passados os comandos de controle da conexão, mas também ele pode utilizar outras portas acima de 1024, tudo depende da configuração dos servidores. Na prática isso quer dizer que quando você deseja, por exemplo, baixar um arquivo FTP o comando (get) para baixar o arquivo é passado pela porta 21 e assim que o servidor aceita ele envia os dados do arquivo pela porta 20.

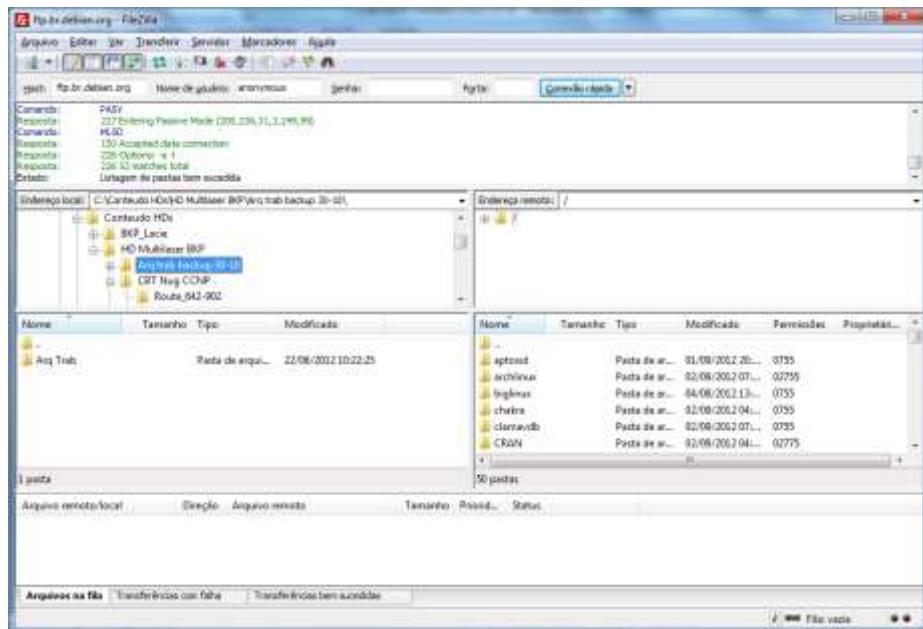
O FTP é um dos serviços mais usados na Internet. Ele pode ser usado para transferência de arquivos privados de usuários, usando autenticação (via nome de usuário e senha) e também para acesso a repositórios públicos, com acesso anônimo. Os servidores de FTP podem ser acessados através de clientes em linha de comando, clientes gráficos específicos ou navegadores Web. A maioria dos sistemas operacionais dispõe de um cliente FTP em modo texto, acessível através do comando ftp via terminal ou prompt de comando.

Normalmente o acesso aos repositórios de arquivos FTP pode ser feito diretamente via browser digitando "ftp://" seguido da URL desejada, por exemplo, [ftp://ftp.br.debian.org/](http://ftp.br.debian.org/). Mais especificamente no Internet Explorer você deve ir depois de abrir o site FTP como se fossem arquivos do seu computador na opção "Exibir" e clicar em "Abrir Site FTP no Windows Explorer", pois senão você poderá visualizar e copiar os arquivos, mas não poderá enviar arquivos ao servidor FTP. Veja as telas nas figuras seguintes.





Existem também clientes FTP específicos em modo gráfico que podem ser gratuitos ou pagos e com diversas funcionalidades interessantes em relação à navegação FTP via Browser. Um exemplo de cliente FTP gráfico gratuito é o FileZilla, disponível em <http://filezilla-project.org/>, veja a tela do programa na tela da figura 3 ao lado. Note que ele traz uma interface mais simples de se administrar, pois do lado esquerdo temos as pastas do nosso computador e do lado direito as pastas do computador remoto, bastando arrastar para fazer as transferências. Além disso, podemos apagar ou renomear os arquivos de maneira simplificada.



Vários servidores de FTP estão disponíveis gratuitamente em ambiente UNIX e Linux, dentre eles são muito usados o VSFTP, o WU-FTP, o ProFTPD e o PureFTP. Cada um deles possui seus próprios arquivos de configuração. Existem diversos servidores FTP para várias plataformas, segue abaixo uma lista dos principais para ambiente Linux/Unix e Windows.

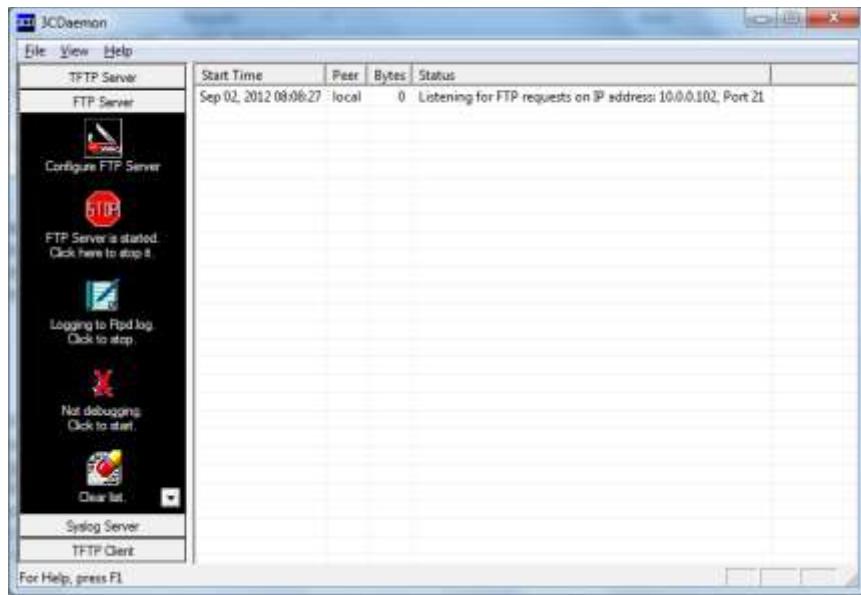
Exemplos de servidores FTP para Linux/Unix/BSD são:

- ftpd
- glftpd
- ProFTPD
- Pure-FTPd
- VsFTPD
- Wu-ftpd
- wzdftpd

Para Windows podemos citar:

- WarFTPD Server (open source),
- FileZilla Server (open source),
- Pure-FTPd (BSD),
- Typsoft FTP server (GPL),
- wzdftpd (open source)
- Internet Information Services (Proprietário, acompanha várias versões do Windows)

Outro servidor FTP e TFTP interessante e bem simples para Windows é o **3ComDaemon**, o qual você encontra para download na área do aluno dentro da pasta Biblioteca. Ele é muito simples de se utilizar e você pode tê-lo instalado em seu computador para facilitar a transferência de arquivos em sua rede local ou em casa entre seus computadores.



A configuração é bastante simples, clique em Configure FTP ou TFTP Server, defina o caminho das pasta que será compartilhada e você já pode utilizá-lo. Para cessar os arquivos utilize um cliente FTP digitando "ftp://localhost" ou "ftp://127.0.0.1". Depois você pode utilizar o comando "netstat -a" e "netstat -n" para visualizar as portas TCP abertas e as conexões que você fizer com o servidor.

O serviço de FTP é utilizado na prática para disponibilização de arquivos em uma rede local ou via Internet e também para administração de websites, pois o desenvolvimento e criação de um website é realizada em máquinas locais e depois de devidamente testado os webdesigners e programadores fazem o upload do site para o servidor de Internet utilizando o serviço de FTP.

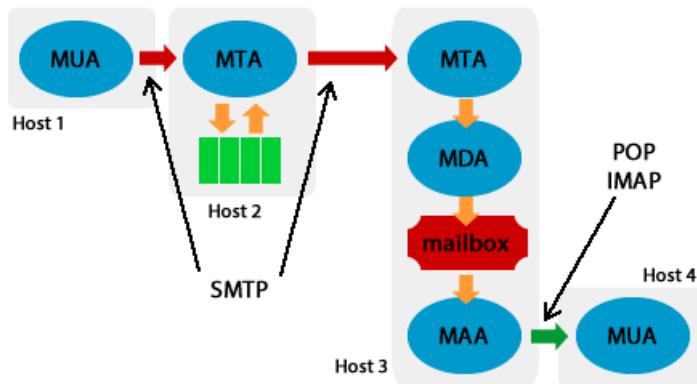
Já o TFTP (Trivial File Transfer Protocol – Protocolo de Transferência de Arquivos Simples) é também utilizado para transferência de arquivos, porém é um serviço sem conexão e usa o UDP (User Datagram Protocol – Protocolo de Datagrama de Usário) como protocolo de transporte na porta 69. É usado por dispositivos de rede, tais como roteadores switches e telefones IP para transferir arquivos de configuração, imagens IOS e firmwares. É útil em algumas redes locais porque opera mais rápido do que o FTP em um ambiente estável, porém não recomendado para utilizar em redes públicas, como a Internet, pois ele não suporta autenticação. O programa visto anteriormente também disponibiliza o serviço de TFTP.

O SFTP (Secure File Transfer Protocol) é semelhante ao FTP convencional, porém em função do uso de criptografia nas conexões (através do estabelecimento de um túnel SSH) o tráfego de informações possui um incremento de segurança, tornando o serviço mais confiável que o FTP, pois se as informações trocadas entre o cliente e o servidor forem capturadas não poderão ser lidas tão facilmente. O SFTP roda como o SSH utilizando a porta 22 TCP por padrão.

Para transferir arquivos usando o protocolo SFTP, precisará de um servidor que esteja configurado para SFTP e um cliente que o suporte. Os servidores populares de SFTP incluem FileZilla, WinSCP e DataFreeway. O cliente de SFTP mais comumente usado é PuTTY, o qual é gratuito e você pode encontrar na Biblioteca dentro da área do aluno. Os usuários que desejarem uma interface mais intuitiva podem optar por um cliente mais amigável, como o PASSPORT da Zephyr.

#### 2.4.4 Serviços de E-mail – SMTP, POP3 e IMAP

O E-Mail ou Correio Eletrônico é um serviço disponível na Internet que possibilita o envio e o recebimento de mensagens ("mails") em meio eletrônico. A infraestrutura de transporte de e-mail na Internet funciona através da interação entre diversos agentes, conforme a figura abaixo.



O MUA (Mail User Agent) é o programa que o usuário acessa para compor seu e-mail, como por exemplo, o Outlook, Netscape, Eudora, Pine, Kmail, etc. Nele iremos ler os e-mails ou enviar essas mensagens de correio eletrônico.

O MTA (Mail Transport Agent) tem a função de receber o e-mail do MUA e o enviar a outros MTAs, até que seja entregue ao destinatário. O principal MTA em UNIX e Linux é o SendMail, mas existem também o QMail , Postfix, Exim e outros. Na Internet, os MTAs se comunicam entre eles graças ao protocolo SMTP que é chamado logicamente de servidor SMTP (às vezes servidor de correio de saída).

O MDA (Mail Delivery Agent) tem a função de receber o e-mail do MTA e o depositar na caixa de correio do usuário. O MDA default do Linux é o procmail, mas existem diversos outros.

E para finalizar a estrutura de e-mail temos o MAA (Mail Access Agent), o qual permite ao MUA acessar aos e-mails que estão na caixa de correio do usuário. Na prática, esta função é exercida pelos servidores POP3 e/ou IMAP.

O serviço de e-mail usa vários protocolos para o transporte das mensagens entre remetentes e destinatários. O protocolo SMTP - Simple Mail Transfer Protocol é o protocolo responsável pelo envio do e-mail do cliente (MUA) ao servidor (MTA) e deste para outros servidores, até chegar ao servidor de destino. O protocolo SMTP utiliza o TCP como transporte na porta 25 por padrão.

Para consultar os e-mails armazenados no servidor, o cliente (MUA) utiliza os protocolos POP3 (Post-Office Protocol v3) e IMAP (Internet Message Access Protocol).

Normalmente o uso de POP3 é mais indicado quando os usuários são estáticos, ou seja, cada um possui seu computador e só acessa seu e-mail a partir dele. POP3 é um protocolo leve e que não mantém conexão constante com o servidor, ou seja, você ao enviar e receber e-mails ele estabelece a conexão, baixa os e-mails para seu computador ou envia os e-mails que estão em sua caixa de saída e fecha a conexão. O POP3 utiliza o TCP como transporte na porta 110 por padrão. Existe também a versão segura chamada POP3S que utiliza a porta 995 do TCP.

O uso de IMAP é indicado quando os usuários são “nômades”, ou seja, quando usam vários computadores diferentes. O IMAP exige mais recursos de CPU, disco e memória do servidor que o POP3. A conexão IMAP normalmente é mantida enquanto durar a sessão de trabalho do usuário, pois seu cliente de e-mail fica sincronizado com o servidor e uma cópia dos e-mails é mantida nele, assim você pode ler seus e-mails de qualquer host. Este protocolo é muito usado em ambientes de WebMail, para os acessos do servidor Web ao servidor de e-mail, normalmente sendo realizada através de seu browser, e por isso é o mais utilizado em ambientes corporativos, pois assim os funcionários podem acessar suas caixas de e-mail em qualquer computador, mesmo estando fora de sua rede local ou longe de seu computador. O IMAP utiliza também o TCP como protocolo de transporte na porta 143 por padrão. Existe também a versão segura chamada IMAPS que utiliza a porta 993 do TCP.

As portas informadas acima são as portas padrões, porém muitos provedores de e-mail utilizam outras portas por motivos de segurança ou então para compatibilizar sua infraestrutura.

Os servidores de e-mail (MTAs) funcionam segundo um princípio “store and forward”, o que significa que um MTA recebe cada mensagem integralmente e a deposita em um diretório temporário, para somente então passá-la adiante, seja a outro MTA ou ao MDA, se o destinatário for um usuário local. Cada transmissão fica registrada em uma linha Received do cabeçalho do e-mail. Esse procedimento garante a entrega da mensagem ao destinatário, sem possibilidade de perdas na transmissão.

Para identificar os usuários os servidores utilizam o **endereço de e-mail**. Um endereço de email é emitido por um provedor de serviços de Internet e ele contém dois componentes de informações importantes que permitem a um email enviado pela Internet chegar até seu destinatário:

1. O primeiro componente é o **nome do usuário**, ou a parte que aparece antes do sinal de @, como "joao" no endereço de email joao@example.com.br.
2. Após o sinal de @ vem o **nome do domínio** ou do **host**. Esse nome é semelhante à rua ou cidade de seu endereço. Ele identifica o local para onde o email deve ser encaminhado.

Depois que a mensagem chega ao domínio, o nome do usuário é semelhante ao seu endereço residencial específico. Ele permite que o provedor de serviços de Internet encaminhe a mensagem para sua própria caixa de correio.

Em ambiente Windows o servidor de e-mails é o **Microsoft Exchange Server**.

#### 2.4.5 Serviço de Alocação Dinâmica de IPs – DHCP

O DHCP (Dynamic Host Configuration Protocol - Protocolo de Configuração Dinâmica de Host) é um protocolo de serviço TCP/IP que oferece configuração dinâmica de hosts, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede, assim os administradores de rede não precisam configurar manualmente os parâmetros das placas de rede nos computadores dos usuários.



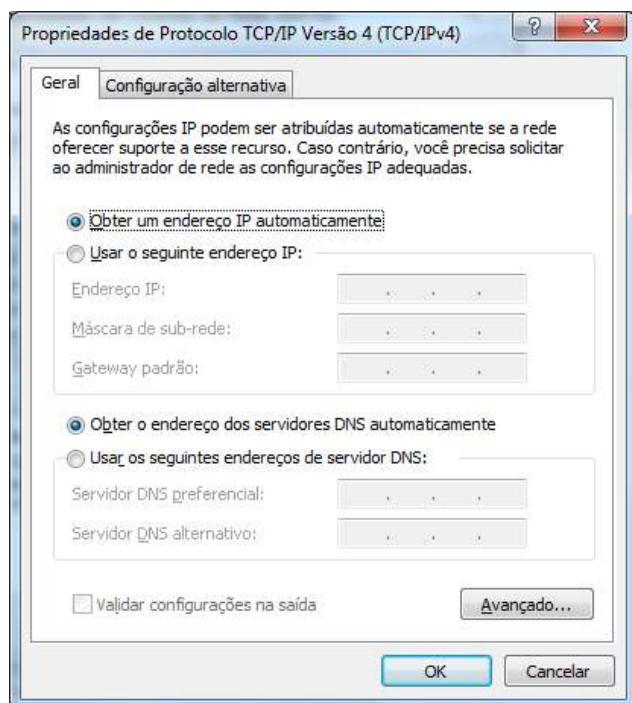
O DHCP surgiu como padrão em Outubro de 1993 e a RFC 2131 contém as especificações mais atuais (março de 1997). O último padrão lançado para a especificação do DHCP sobre IPv6 (DHCPv6) foi publicado em Julho de 2003 com a RFC 3315.

Resumidamente, o DHCP opera da seguinte forma (veja a figura 1 ao lado):

- Um cliente envia um pacote UDP em broadcast (destinado a todas as máquinas) com um pedido DHCP.
- Os servidores DHCP que receberem esta requisição irão responder com um pacote com configurações onde constará pelo menos um endereço IP, uma máscara de rede, o gateway padrão e os servidores de DNS, porém outras opções podem ser fornecidas.

O DHCP usa um modelo cliente-servidor, no qual o servidor DHCP mantém o gerenciamento centralizado dos endereços IP usados na rede, normalmente chamado de **escopo** (cada rede é um escopo de DHCP).

O padrão da maioria dos sistemas operacionais atualmente é deixar a placa de rede com o cliente DHCP habilitado, pois a maioria dos equipamentos de acesso à Internet, como os roteadores ADSL ou os Cable Modems, já fornecem os dados para os clientes via DHCP, não sendo necessária a configuração manual do IP nos computadores clientes. Na placa de rede dos computadores a configuração do DHCP ou IP estático (manual) é realizada no mesmo local em ambiente Windows, o qual já vimos anteriormente. Veja na figura ao lado a configuração de uma placa de rede com DHCP, onde as opções de obter um endereço IP e DNS automaticamente estão habilitadas.



Para visualizar a configuração passada pelo servidor DHCP você pode utilizar o comando "ipconfig" ou "ipconfig /all" no prompt de comando. Com o **ipconfig** você verá um resumo dos IPs configurados em suas interfaces de rede, já com o complemento **/all** você verá as opções completas. Veja um exemplo na tela da figura abaixo. Aprenda bem esse comando, pois ele será muito utilizado se você for trabalhar em uma empresa com ambiente Windows.

```
C:\Windows\system32\cmd.exe
C:\Users\dltec>ipconfig

Configuração de IP do Windows

Adaptador de Rede sem Fio Conexão de Rede sem Fio:

Sufixo DNS específico de conexão . . . . . : 
Endereço IPv6 de link local . . . . . : fe80::9db:ae76:db9:bcc0%12
Endereço IPv4 . . . . . : 10.0.0.102
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . : 10.0.0.1

Adaptador de túnel isatap.{C8888380-8AA9-4243-AA04-03297B37015C}:

Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão . . . . . : 

Adaptador de túnel Conexão Local* 9:

Sufixo DNS específico de conexão . . . . . : 
Endereço IPv6 . . . . . : 2001:0:4137:9e76:28a1:2797:f5ff:ff99
Endereço IPv6 de link local . . . . . : fe80::28a1:2797:f5ff:ff99%13
Gateway Padrão. . . . . : 11

C:\Users\dltec>
```

```
C:\Windows\system32\cmd.exe
C:\Users\dltec>ipconfig /all

Configuração de IP do Windows

Nome do host. . . . . : dltec-marcelo
Sufixo DNS primário . . . . . : 
Tipo de nó. . . . . : híbrido
Roteamento de IP ativado. . . . . : não
Proxy WINS ativado. . . . . : não

Adaptador de Rede sem Fio Conexão de Rede sem Fio:

Sufixo DNS específico de conexão. . . . . : 
Descrição . . . . . : Dell Wireless 1782 802.11b/g/n
Endereço Físico . . . . . : 08-18-85-E5-EE-00
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv6 de link local . . . . . : fe80::9db:ae76:db9:bcc0%12(Preferencial)
Endereço IPv4. . . . . : 10.0.0.102(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : sexta-feira, 31 de agosto de 2012 19:18:48
Concessão Expira. . . . . : domingo, 2 de setembro de 2012 11:19:03
Gateway Padrão. . . . . : 10.0.0.1
Servidor DHCP . . . . . : 10.0.0.1
IAID de DHCPv6. . . . . : 238692997
UUID de Cliente DHCPv6. . . . . : 00-01-00-01-16-FB-ED-2F-24-B6-FD-06-DC-17
Servidores DNS. . . . . : 192.168.1.1
NetBIOS em Tcpip. . . . . : Habilitado

Adaptador de túnel isatap.{C8888380-8AA9-4243-AA04-03297B37015C}:

Estado da mídia. . . . . : mídia desconectada
```

O serviço de DHCP pode estar instalado em servidores locais descentralizados ou então em uma infraestrutura centralizada. Além disso, muitos roteadores permitem a configuração de um servidor DHCP para facilitar a administração de localidades remotas e evitar a necessidade da configuração de vários servidores locais um por unidade remota.

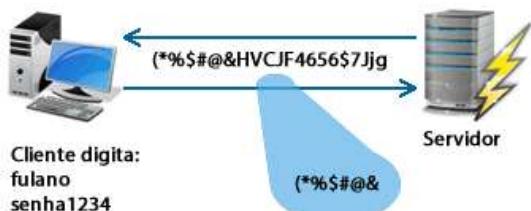
#### 2.4.6 Serviços de Acesso via Terminal Virtual – Telnet e SSH

Estes dois protocolos permitem o acesso remoto à linha de comando de outro computador, servidor ou dispositivo de rede, permitindo que um usuário efetue logon em um dispositivo da rede e execute comandos. Eles são utilizados para a administração remota de servidores, roteadores e switches. A diferença básica entre os dois serviços é a questão da segurança, pois o Telnet é enviado em modo texto claro através da rede, enquanto o SSH troca as informações entre os dispositivos de maneira segura e criptografada.

Telnet - seção de login sem criptografia



SSH- seção de login com criptografia

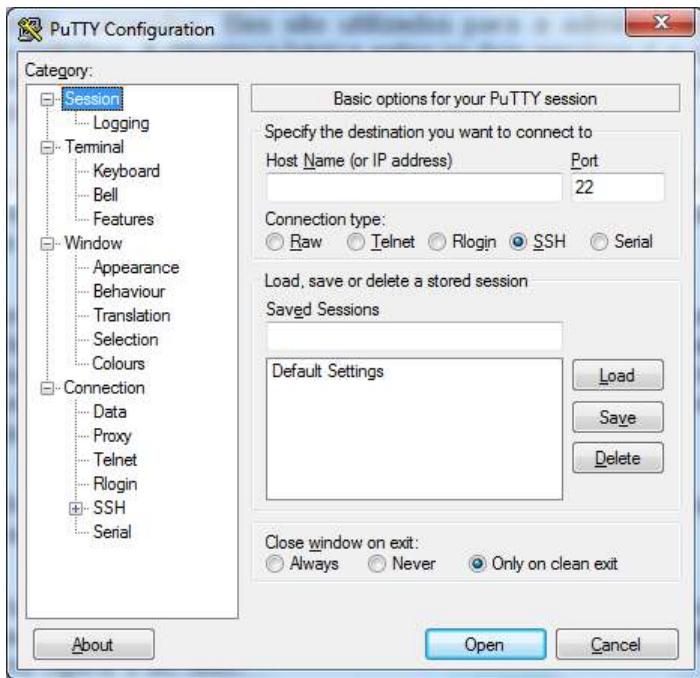


O Telnet é um protocolo cliente-servidor usado para permitir a comunicação entre computadores ligados numa rede (exemplos: rede local / LAN, Internet), baseado em TCP, o qual utiliza a porta 23 como padrão.

O Telnet vem sendo gradualmente substituído pelo SSH, cujo conteúdo é criptografado antes de ser enviado. O uso do protocolo Telnet tem sido desaconselhado, à medida que os administradores de sistemas vão tendo maiores preocupações com segurança. Com o Telnet todas as comunicações entre o cliente e o servidor podem ser vistas, inclusive usuários e senhas, já que é somente texto aberto.

O Secure Shell ou SSH utiliza também o transporte TCP, porém na porta 22, e possibilita a transferência de informações criptografadas pela rede. Conforme já mencionado ele foi desenvolvido para substituir as ferramentas inseguras de login e execução de comandos remotos como telnet, rlogin e rsh. Acessar um sistema através de algum método como o telnet coloca em risco tudo que você enviar e receber, pois os dados são enviados através de texto puro e sua sessão é completamente visível para qualquer outro na sua rede e na rede da máquina que você estiver acessando. Isso faz com que qualquer um possa monitorar e roubar ("sniffing") qualquer dado transmitido nessa conexão, como nome de usuário, senha, emails que você ler, comandos enviados, etc. Por essas razões, você precisa de algum sistema mais sofisticado para realizar a conexão remota aos dispositivos de redes.

Existem vários clientes telnet e SSH disponíveis, porém o mais famoso deles é o Putty, o qual já mencionado anteriormente e está disponível para download na Biblioteca da área do aluno.



Veja que você pode selecionar a conexão via Telnet ou SSH, no campo Host Name insira o IP ou nome do host e na porta insira a porta utilizada, apesar do campo da porta (Port) já vir preenchido alguns administradores de rede mudam as portas padrões por questões de segurança, por isso o programa dá a possibilidade de mudar essa porta.

Além do telnet e SSH existem outros protocolos utilizados para acesso remoto, tais como o rlogin, rsh, terminal services e RDP (remote desktop), porém muitos deles permitem mais que acesso a um terminal virtual. Por exemplo, com o RDP e terminal services você tem acesso completo e gráfico ao desktop de um computador ou servidor remoto, possibilitando a administração de servidores ou suporte remoto a usuários. Em capítulos posteriores, quando formos tratar da administração de redes, vamos voltar a esse assunto de como administrar remotamente computadores, servidores e dispositivos de rede.

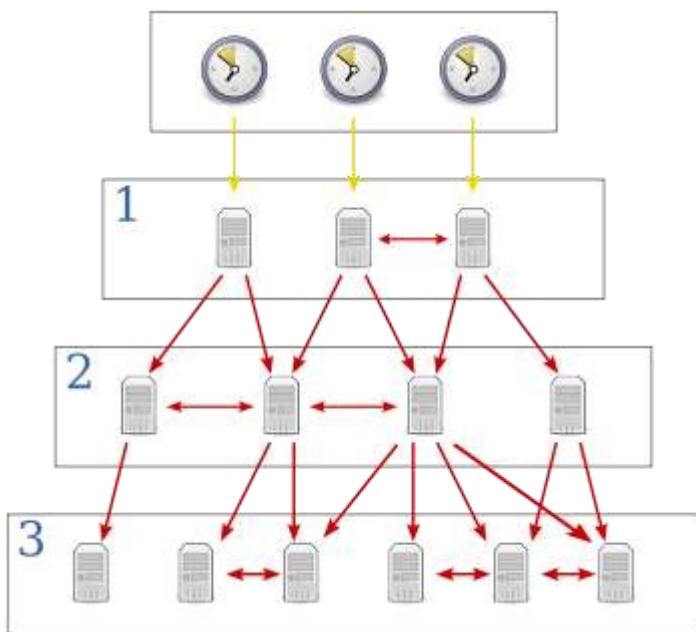
#### 2.4.7 Serviço de Sincronização dos Relógios dos Computadores – NTP

O NTP (Network Time Protocol) é um protocolo para sincronização dos relógios dos computadores baseado no protocolo de transporte UDP (porta 123) para sincronização do relógio de um conjunto de computadores em redes de dados com latência variável, permitindo manter o relógio dos computadores da rede com a hora sempre certa e com grande precisão.

Portanto, utilizando o protocolo NTP teremos uma informação de data/hora mais precisa e também teremos a garantia que todos os dispositivos fiquem sincronizados, ou seja, com a mesma informação de data/hora. Isso é muito importante em uma rede, pois em caso de problemas teremos nos logs (registros) dos equipamentos a data e hora correta que eles ocorreram, possibilitando uma melhor auditoria e correlação de eventos.

Os servidores NTP formam uma topologia hierárquica, dividida em camadas ou estratos (em inglês: strata) numerados de 0 (zero) a 16 (dezesseis). O estrato 0 (stratum 0) na verdade não faz parte da rede de servidores NTP, mas representa a referência primária de tempo, que é geralmente um receptor do Sistema de Posicionamento Global (GPS) ou um relógio atômico. O estrato 16 indica que um determinado servidor está inoperante.

O estrato 0, ou relógio de referência, fornece o tempo correto para o estrato 1, que por sua vez fornece o tempo para o estrato 2 e assim por diante. O NTP é então, simultaneamente, servidor (fornecer o tempo) e cliente (consulta o tempo), formando uma topologia em árvore.



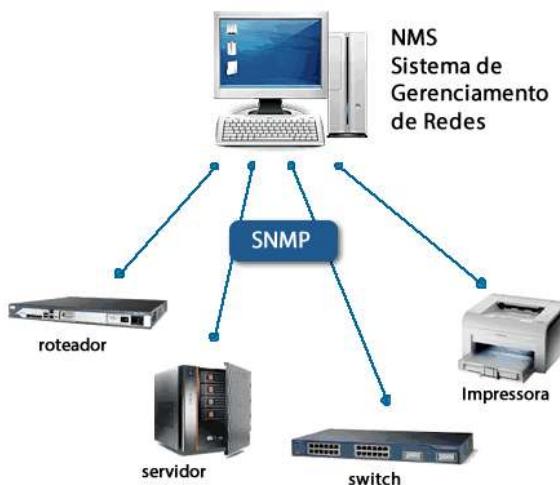
Na Internet você pode encontrar diversos servidores públicos estratos 2 ou 3 (e até mesmo alguns estrato 1) para utilizar. Uma lista dos servidores NTP disponíveis na Internet pode ser encontrada no endereço <http://support.ntp.org/bin/view/Servers/WebHome>.

#### 2.4.8 Serviço de Gerenciamento Remoto de Dispositivos de Redes – SNMP

O SNMP (Simple Network Management Protocol – Protocolo Simples de Gerenciamento de Rede) oferece uma forma de monitorar, controlar e gerenciar configurações, coleta de dados estatísticos, desempenho e segurança em dispositivos de rede. Ele utiliza como transporte o UDP na porta 161.

Uma rede gerida pelo protocolo SNMP é formada por três componentes chaves (veja a figura a seguir):

- Dispositivos Gerenciados ou Geridos
- Agentes
- Sistema de Gerenciamento de Redes (NMS - Network-Management Systems)



Um Dispositivo Gerido ou Gerenciado é um nó de rede que possui um **agente SNMP** instalado e se encontra numa rede gerenciada. Estes dispositivos coletam e armazenam informações de gerenciamento e mantém estas informações disponíveis para sistemas NMS em bancos de dados chamados **MIB** (Management Information Base), as quais podem ser acessadas através do protocolo SNMP. Os dispositivos gerenciados, também às vezes denominados de dispositivos de rede, podem ser roteadores, servidores de acesso, impressoras, computadores, servidores de rede, switches, dispositivos de armazenamento, dentre outros.

As variáveis acessíveis via SNMP são organizadas hierarquicamente. Estas hierarquias e outras informações secundárias (como o tipo e a descrição das variáveis) são definidas nas Management Information Bases (MIBs).

Um **Agente** é um módulo de software de gerenciamento de rede que fica armazenado em um Dispositivo Gerenciado. Um agente tem o conhecimento das informações de gerenciamento locais e traduz estas informações para um formato compatível com o protocolo SNMP.

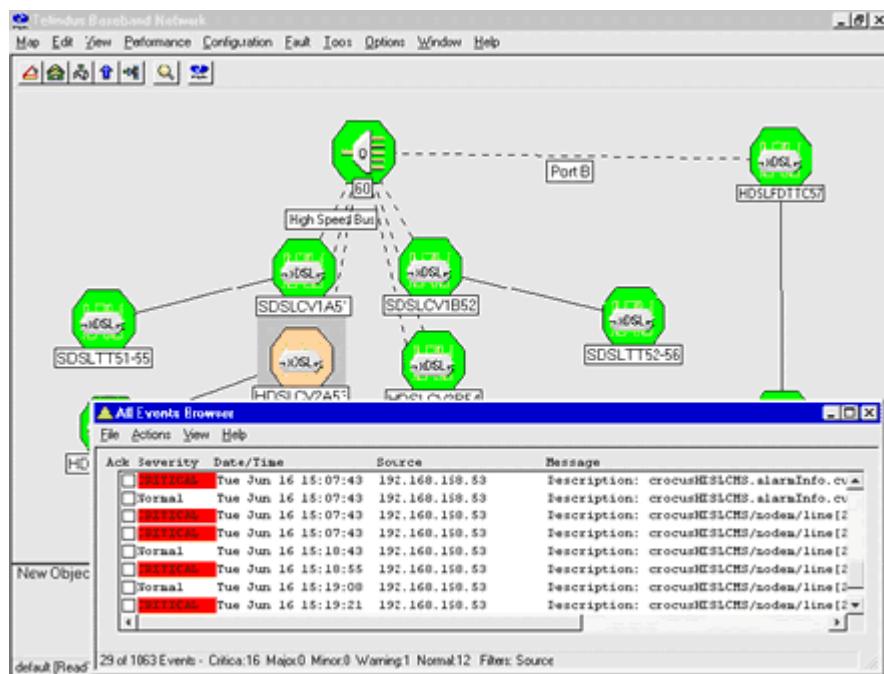
Um sistema **NMS** é responsável pelas aplicações que monitoram e controlam os dispositivos gerenciados. Normalmente é instalado em um ou mais servidores de rede dedicados a estas operações de gestão, que recebe informações (pacotes SNMP) de todos os dispositivos gerenciados daquela rede.

Temos as versões 1, 2 e 3 do SNMP. A versão 2 do SNMP é uma evolução do protocolo inicial, a qual oferece uma boa quantidade de melhorias em relação ao SNMPv1, incluindo operações adicionais do protocolo, melhoria na performance, segurança, confidencialidade e comunicações Gerente-para-Gerente. A SNMPv3 inclui melhorias relativas à segurança do protocolo, tais como privacidade, autenticação e controle de acesso. Na prática, as implementações do SNMP oferecem suporte para as múltiplas versões baseadas na RFC 3584.

Via SNMP podemos monitorar diversas informações dos dispositivos de rede, tais como utilização de memória RAM ou HD, utilização da CPU, nível de utilização das interfaces de rede, dentre outros. Além disso, também podemos monitorar os TRAPs, os quais são utilizados para comunicar um evento pré-determinado. O agente comunica ao gerente o acontecimento de um evento, previamente determinado, através do TRAP, e um alarme é gerado na tela do NMS, por exemplo.

Em grandes empresas programas NMS como Tivoli da IBM e HP OpenView são utilizados para monitoração dos diversos dispositivos de rede. Existem outras opções mais baratas ou até gratuitas que utilizam o SNMP, tais como o WhatsUp e o Nagios. Esses programas são utilizados nos NOCs (Network Operations Center), onde uma equipe de suporte técnico pode analisar as condições dos dispositivos de rede e agir de maneira proativa na resolução de problemas.

Veja na tela da figura abaixo um mapa de rede com vários alarmes fornecidos por um NMS SNMP.



#### 2.4.9 Outros Serviços de Rede

Estudamos nesse tópico da camada de aplicação do TCP/IP que existem diversos serviços de rede e cada um deles tem uma característica. Qualquer profissional ou estudante que deseja progredir em uma carreira na área de redes precisa conhecer essas aplicações, suas características e necessidades de rede, pois cada vez mais uma rede IP vem sendo utilizada para a chamada "convergência" de redes, ou seja, ao invés de trafegar somente os serviços tradicionais de dados outros serviços, principalmente os multimídia, estão sendo agregados às redes.

Você verá que em um ambiente corporativo podemos ter uma central telefônica ou PABX baseado no protocolo IP com o serviço de voz sobre o protocolo IP, chamado de VoIP. Nesse serviço temos servidores ou dispositivos onde os telefones IP, sejam físicos ou softwares instalados nos computadores dos usuários, irão se registrar para fazer suas ligações.

Outro serviço muito comum em empresas de todos os portes é a vídeo conferência através da rede IP, seja feita através de equipamentos específicos ou então diretamente entre os computadores.

Também temos o armazenamento de arquivos, os quais podem ser realizados nos discos dos servidores de arquivos ou então distribuídos em storages, dispositivos que possuem diversos discos para armazenamento de grandes volumes de dados.

Outro serviço comum e agregado aos sistemas de arquivo são os sistemas de backup, pois caso haja problema com os dados dos usuários ou então de um determinado sistema os administradores de rede podem recuperar parcialmente ou totalmente os dados dos usuários.

Portanto, os tipos de serviços, servidores e clientes em uma rede vai depender do porte e das necessidades de cada empresa ou ambiente de rede.

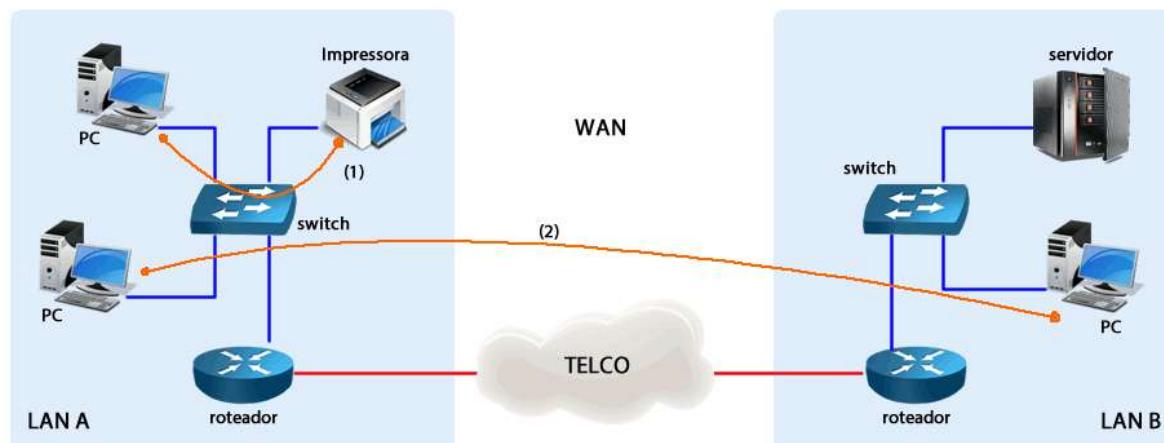
## 2.5 Fluxo de Informações em Redes TCP/IP

Em uma rede TCP/IP temos basicamente dois tipos de troca de informação entre hosts ou entre clientes e servidores:

- Dentro da mesma rede local (LAN) ou
- Em redes locais diferentes, seja em redes ou subredes diferentes ou um acesso à Internet ou Intranet via WAN.

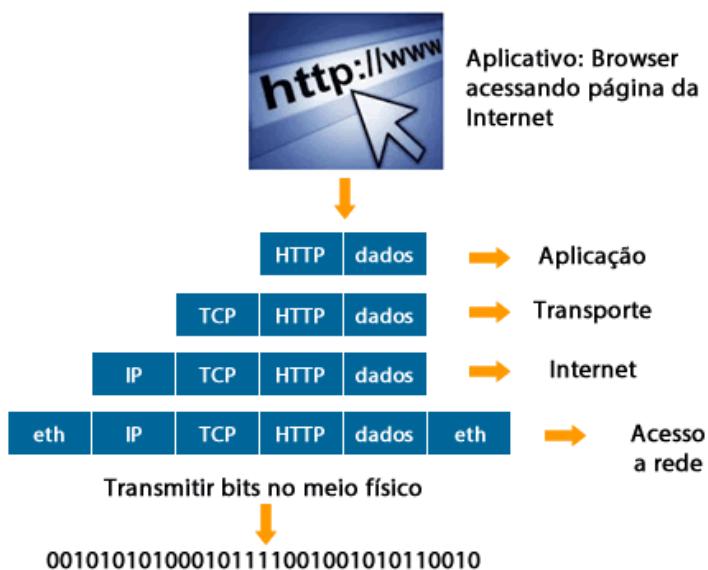
Quando os dois dispositivos que desejam se comunicar estão na mesma LAN a comunicação se dá diretamente entre os dois, porém quando os dispositivos estão em redes diferentes um roteador (ou vários) será utilizado como "intermediário" (gateway), roteando os pacotes até que eles cheguem à rede de destino e, por conseguinte ao host de destino.

Veja a figura a seguir, onde temos em (1) uma comunicação local entre um PC e uma impressora e em (2) temos dois PCs em redes LAN diferentes querendo se comunicar através de uma rede WAN.



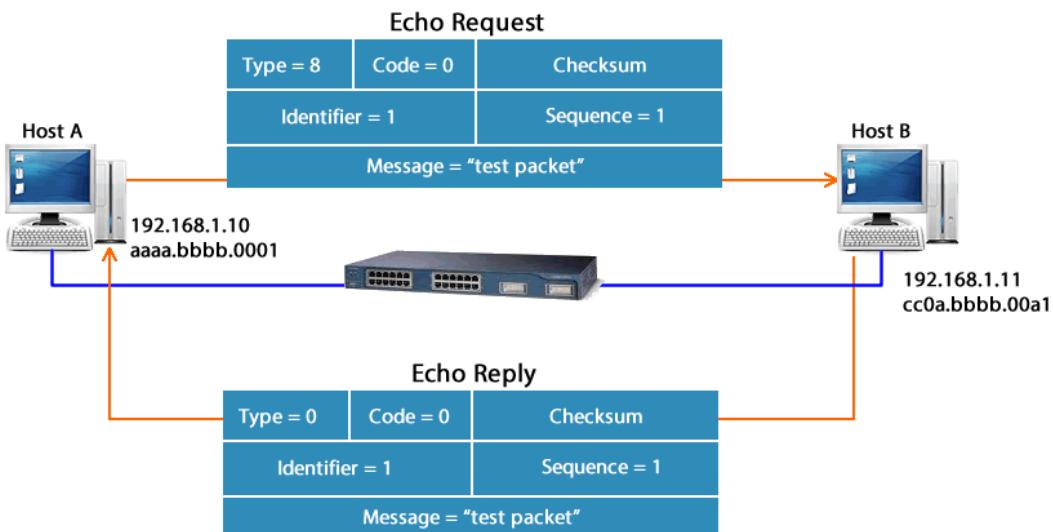
Resumindo, tudo nasce no aplicativo do usuário querendo acessar um servidor de rede ou outro host e a camada de aplicação recebe esses dados. Após a camada de aplicação tratar os dados e inserir seu cabeçalho ela passará os dados à camada de transporte, onde a aplicação pode escolher entre utilizar os serviços do TCP ou UDP. Na camada de transporte os dados da camada de aplicação são inseridos no campo de "dados" do PDU, o cabeçalho de transporte é inserido e depois enviado para a camada de Internet.

Na camada de Internet os segmentos TCP ou datagramas UDP são recebidos, colocados dentro do pacote IP, juntamente com o endereço de IP origem (local) e o endereço do host de destino e enviados para a camada de acesso aos meios criar o quadro referente à tecnologia de LAN que está sendo utilizada e transmitir as informações no meio físico bit a bit. Veja a figura abaixo.



Mas agora vamos incluir os conceitos adicionais e verificar que bem mais coisas acontecem para que o processo de encapsulamento possa ser completado. Vamos ao primeiro tipo de comunicação em uma LAN, onde queremos, por exemplo, acessar arquivos compartilhados em um micro na mesma rede ou então fazer um teste de conectividade através do ICMP, mais especificamente utilizando o comando “ping”.

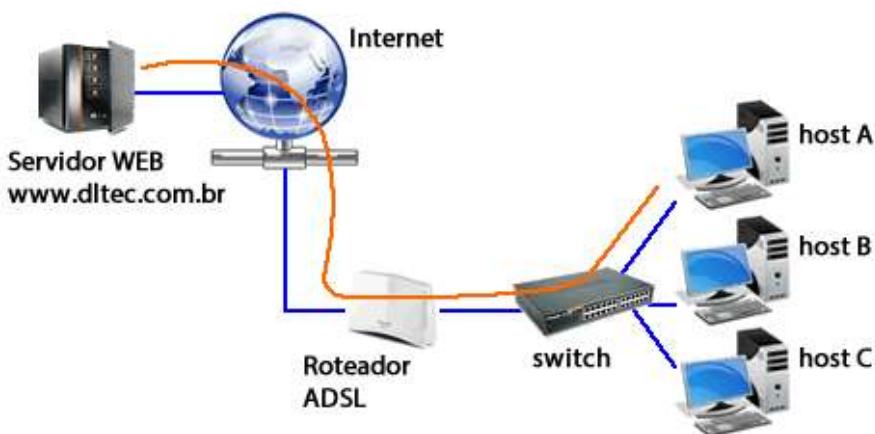
Vamos supor que temos dois computadores, o Host-A e o Host-B a uma LAN conectados através de um switch. Sabemos que o IP do Host-A é o 192.168.1.10 e do Host-B 192.168.1.11, com isso abrimos o prompt de comando no Host-A e digitamos “ping 192.168.1.11”. Com isso o protocolo ICMP precisa montar um pacote IP contendo o IP 192.168.1.10 como origem e o destino será o IP 192.168.1.11, mas as informações específicas do ICMP com o comando **echo request**.



Porém, como estamos em uma rede do tipo ethernet antes do pacote poder ser enviado é necessário que o Host-A conheça o endereço MAC (endereço físico) do Host-B. Para isso o Host-A envia uma mensagem de requisição ARP solicitando o endereço MAC do Host-B. Nessa requisição temos os endereços IP e MAC do Host-A como origem e no destino temos o IP do Host-B e queremos saber o MAC do Host-B, sendo que a mensagem é enviada em broadcast para a rede. Quando o Host-B recebe essa mensagem ele responde diretamente para o Host-A informando qual o seu MAC, com isso o computador Host-A consegue montar o quadro ethernet e enviar os pacotes do ping para o Host-B.

Quando o Host-B recebe os pacotes ICMP com o echo request ele responde para o Host-A com pacotes de echo-reply.

Portanto, em uma rede local temos apenas a resolução de endereço IP para MAC do host de destino, porém se formos pensar em um acesso à Internet, onde o host remoto normalmente é um servidor que está em uma rede remota outros processos irão entrar em cena, pois não sabemos o IP do servidor remoto e nem estamos na mesma rede local. Veja o cenário na figura seguinte, onde o computador Host-A deseja acessar o site da DlteC através da Internet via uma conexão ADSL.

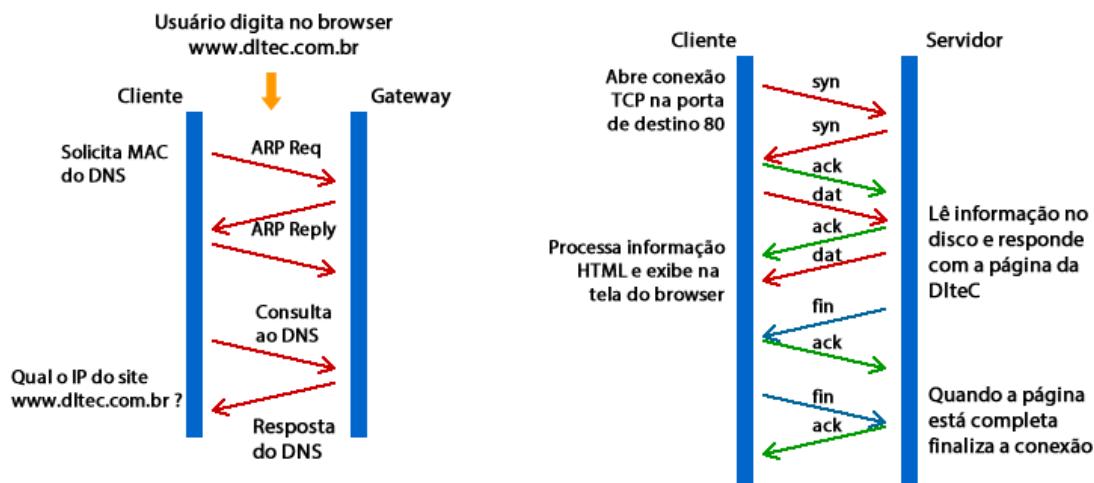


Mas o que terá de diferente entre o acesso local entre dois hosts visto anteriormente e agora no cenário da figura 4? Além do serviço ser diferente, pois no primeiro cenário tínhamos um simples ping e agora estamos tentando acessar um servidor web, temos dois Hosts em redes diferentes e não sabemos o endereço IP do servidor, temos somente a URL do website. Vamos então descrever os passos resumidamente que ocorrerão nesse acesso à Internet:

1. O usuário abre o browser e digita <http://www.dltec.com.br>, com isso o computador precisa encontrar qual o endereço IP da URL digitada utilizando o serviço de DNS;
2. O computador verifica o endereço IP do servidor DNS configurado em sua interface de rede e verifica que é o IP do roteador ADSL, o qual está na mesma rede que o computador;
3. Com isso o computador cria uma requisição ARP para verificar o endereço MAC do roteador ADSL e depois que recebe a resposta cria uma solicitação ao servidor DNS;
4. Uma vez recebida a resposta do servidor DNS o Host-A verifica que o IP do servidor da DlteC está em uma rede diferente da sua LAN e com isso precisaria montar uma requisição ARP solicitando o endereço MAC do dispositivo configurado como seu gateway padrão em sua interface de rede, porém como o DNS é o mesmo IP, pois está configurado dentro do roteador ADSL o computador já possui esse MAC e cria a solicitação HTTP para o IP do servidor da DlteC conforme vimos no item 4.4.1;

5. O roteador local irá receber esse pacote e encaminhar para o endereço IP que está configurado em sua tabela de roteamento como roteador padrão e os roteadores de Internet irão, através do endereço IP de destino do pacote, roteá-lo até que o servidor web da DLTEC seja encontrado;
6. Uma vez que o servidor recebe essa solicitação na porta 80 TCP, ele processa a solicitação e inicia o envio da página para o Host-A até que todo conteúdo seja enviado e a conexão seja finalizada.

Veja o fluxo de informações descrita anteriormente em modo gráfico na figura abaixo.



Lembre que na camada de transporte o segmento TCP criado no Host-A terá como origem uma porta acima de 49152 e como destino a porta 80, a qual é a porta padrão do HTTP. Quando o servidor responder à requisição ele terá como origem a porta 80 e o destino a porta que o Host-A enviou como origem, ou seja, ao contrário do enviado pelo Host-A. O mesmo se dá para o endereçamento IP, o que é origem vira destino e o que era destino vira origem na resposta à requisição do solicitante. Essas informações criadas nas camadas de aplicação, transporte e Internet não variam durante o roteamento através da rede.

Já os quadros da camada de acesso aos meios serão montados e desmontados de acordo com o meio físico utilizado.

Os exemplos utilizados aqui estão simplificados, pois muitos outros processos podem entrar no meio do caminho dependendo da arquitetura da rede ou serviço que está sendo acessado, porém o que tratamos aqui são os princípios básicos e fundamentais para o bom entendimento da rede e para que você futuramente possa realizar análises e troubleshootings (resolução de problemas) na rede de sua casa ou empresa onde trabalha.

Para finalizar os estudos sobre o TCP/IP assista o vídeo Guerreiros da Internet no link abaixo, o qual mostra o fluxo dos pacotes IP através de uma rede.

[http://www.youtube.com/watch?v=fmiC5lyc\\_X4](http://www.youtube.com/watch?v=fmiC5lyc_X4)

### 3 Topologias de Rede

Quando queremos interligar as diversas redes que devem se comunicar entre si - as linhas de comunicação e os pontos de conexão - temos que escolher como vamos fazer essas conexões, ou seja, como vamos interligar esses dispositivos para que todos os terminais (endpoints) possam se comunicar? A forma (física e lógica) que representa essa rede é chamada de **topologia de rede**.

A ligação mais simples é utilizar uma ligação ponto-a-ponto, ou seja, um dispositivo diretamente conectado a outro. Esta é a topologia utilizada na maioria das redes WAN quando utilizamos interfaces seriais e também nas conexões de Internet residenciais, pois nosso Modem ADSL ou Cable Modem está conectado com apenas um ponto ao equipamento de transmissão do provedor de Internet. Veja a figura abaixo com o exemplo de dois computadores ligados diretamente um no outro.



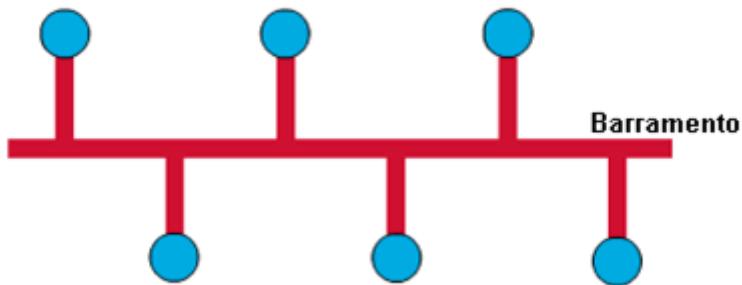
Em uma rede TCP/IP temos a maioria das redes LAN com tecnologia da família Ethernet, a qual utiliza uma topologia em estrela ou estrela estendida, ou então via redes sem fio que utilizam topologias celulares. Já nas redes WAN a maioria são redes ponto a ponto através de interfaces seriais síncronas.

Uma boa adaptação entre a topologia da rede, os serviços a serem prestados, a rede lógica a ser implantada e tipos de usuários são detalhes fundamentais para a criação de um projeto de qualidade. Nesse tópico apresentaremos algumas topologias com suas vantagens e desvantagens.

**Topologia Barramento Linear**

Na topologia de barramento todos os nós são conectados diretamente a um link e não existem outras conexões entre os nós.

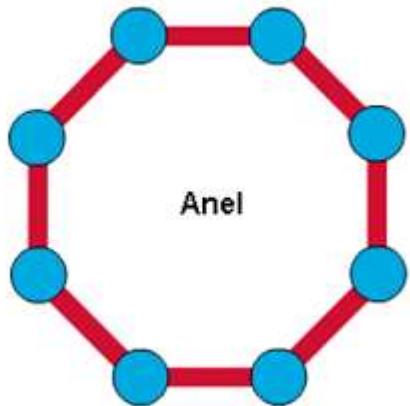
Cada elemento é conectado a um fio comum. Uma vantagem dessa topologia é que todos os elementos estão conectados uns aos outros e, portanto, podem comunicar-se diretamente. Uma desvantagem dessa topologia é que um rompimento no cabo desconecta os elementos uns dos outros.

**Topologia em Anel**

A topologia em anel é um único anel fechado que consiste em nós e links, com cada nó conectado a apenas dois nós adjacentes.

A topologia mostra todos os dispositivos conectados diretamente uns aos outros, que é chamado de interligação de equipamentos em cascata.

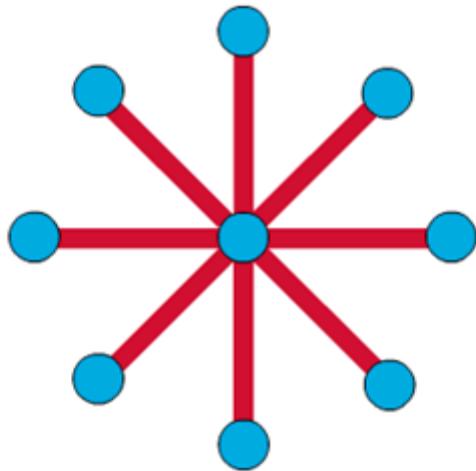
Para que as informações fluam, cada estação tem de passar as informações à sua estação adjacente.



**Topologia em Estrela**

A topologia em estrela tem um nó central do qual todos os links ligados aos outros nós se irradiam e não permitem outros links.

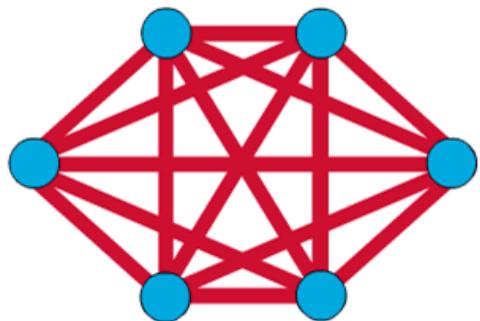
Sua vantagem principal é permitir que todos os outros nós se comuniquem uns com os outros, convenientemente. Sua principal desvantagem é que se o nó central falhar, a rede inteira fica desconectada.

**Topologia em Malha ou Completa**

Em uma topologia completa ou em malha, cada nó é vinculado diretamente a todos os outros nós.

Essa topologia tem vantagens e desvantagens muito distintas. Uma vantagem é que todos os nós estão fisicamente conectados a todos os outros nós (criando uma conexão redundante). Se algum link falhar, as informações poderão fluir através de muitos outros links para atingir seu destino. Outra vantagem dessa topologia é que ela permite que as informações sejam transmitidas por muitos caminhos de volta através da rede.

A principal desvantagem física é que, para um pouco mais que um número pequeno de nós, a quantidade de meios para os links e a quantidade de conexões feitas aos links serão esmagadoras.



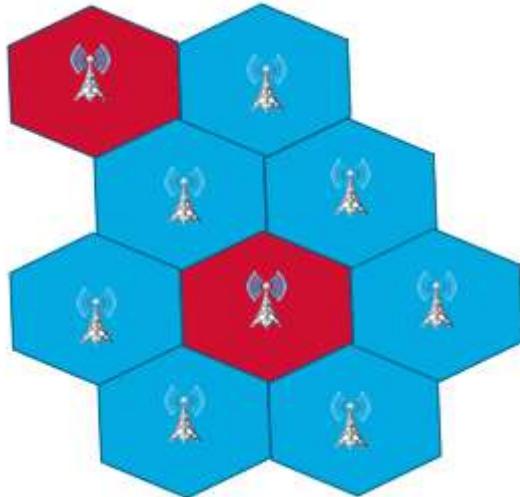
### Topologia de Rede Celular

A topologia celular consiste em áreas circulares ou hexagonais, cada uma tendo um nó individual no centro.

A topologia celular é uma área geográfica dividida em regiões (células) para fins de tecnologia sem-fio, uma tecnologia que se torna cada vez mais importante. Não há links físicos em uma topologia celular, apenas ondas eletromagnéticas. Às vezes, os nós de recepção (por exemplo, o telefone celular em um carro) se movem e, às vezes, os nós de envio se movem (por exemplo, os links de comunicação por satélites).

A vantagem óbvia de uma topologia celular (sem fio) é que não há outros meios tangíveis que não a atmosfera terrestre ou o vácuo do espaço (satélites). As desvantagens são que os sinais estão presentes em todos os lugares de uma célula e, assim, são suscetíveis a interferências (provocadas pelo ser humano e pelo meio ambiente) e às violações na segurança (por exemplo, o monitoramento eletrônico e roubo de serviço).

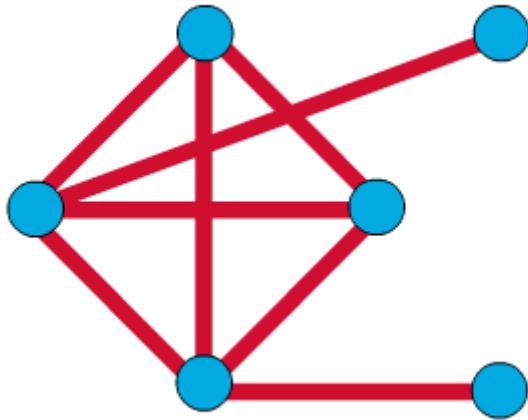
As tecnologias celulares comunicam-seumas com as outras diretamente (embora as limitações impostas pela distância e a interferência às vezes tornem essa comunicação extremamente difícil) ou comunicam-se apenas com suas células adjacentes, o que é muito ineficiente. Como regra, as topologias baseadas em celular são integradas a outras topologias, independentemente de usarem a atmosfera ou satélites.



**Topologia Irregular**

Na topologia de rede irregular não há nenhum padrão óbvio para os links e nós.

O cabeamento é inconsistente. Os nós têm números variáveis de fios que partem deles. Essa é a forma como as redes que estão nas etapas iniciais de construção, ou que foram mal planejadas, são freqüentemente cabeadas.



## 4 Largura de Banda e Throughput

A largura de banda é um conceito um pouco abstrato, mas extremamente importante em telecomunicações e principalmente em redes de computadores.

Nesse capítulo do curso vamos apresentar esse conceito para que posteriormente possa ser usado em diversas discussões.

Na sequência veremos os seguintes tópicos:

- Medidas de largura de banda digital
- Diferença da largura de banda dos meios
- Throughput de dados em relação a largura de banda digital

### 4.1 Medidas de Largura de Banda Digital

A largura de banda é a medida da quantidade de informação que pode ser transferida de um lugar para o outro em um determinado período de tempo.

Sabemos que o termo da unidade de informação mais básica é o bit. Também sabemos que a unidade básica de tempo é o segundo. Então, se estivermos tentando descrever a quantidade de fluxo de informações em um intervalo de tempo específico, poderíamos usar as unidades "bits por segundo" para descrever esse fluxo.

Logo, bits por segundo é uma unidade de largura de banda. A tabela ao lado resume as várias unidades de largura de banda.

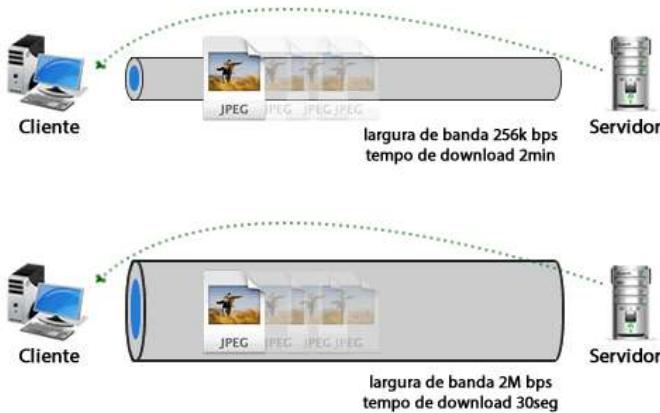
A largura de banda é um elemento muito importante da rede, ainda que seja um pouco abstrato e difícil de entender. Para podermos entender melhor esse conceito vamos ver duas analogias que podem nos ajudar a compreender o que é a largura de banda.

Unidade de Largura de Banda	Abreviatura	Equivalência
Bits por segundo	bps	Unidade básica de largura de banda
Quilobits por segundo	kbps	$1 \text{ kbps} = 1000 \text{ bps} = 10^3 \text{ bps}$
Megabits por segundo	Mbps	$1 \text{ Mbps} = 1000 \text{ kbps} = 10^6 \text{ bps}$
Gigabits por segundo	Gbps	$1 \text{ Gbps} = 1000 \text{ Mbps} = 10^9 \text{ bps}$

### A largura de banda é como o diâmetro de um cano

Pense na rede de canos que traz água até sua casa. Esses canos têm diferentes diâmetros: o principal cano de água da cidade pode ter 2 metros de diâmetro, enquanto a torneira da cozinha pode ter 2 centímetros.

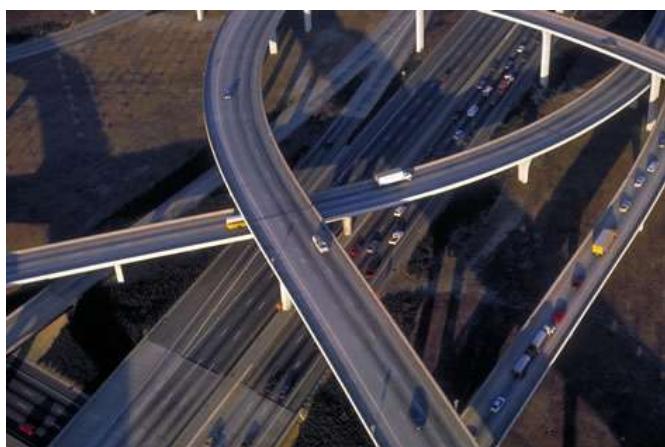
O diâmetro do cano mede a capacidade do cano levar água. Nessa analogia, a água é como a informação, e o diâmetro do cano é como a largura de banda. Na verdade, muitos especialistas em rede falam em termos de "colocar canos maiores", o que significa mais largura de banda, ou seja, mais capacidade de transmitir informações.



### Largura de banda é como o número de pistas de uma rodovia

Pense em uma rede de estradas que atenda à sua cidade ou município. Pode haver rodovias com oito pistas, com saídas para estradas de 2 e 3 pistas, que podem, por sua vez, levar a ruas com duas pistas não divididas e, finalmente, à garagem da sua casa. Nessa analogia, o número de pistas é como a largura de banda, e o número de carros é como a quantidade de informação que pode ser transportada.

Lembre-se de que o significado de largura de banda verdadeiro e real, no nosso contexto, é o número máximo de bits que podem passar teoricamente através de uma área determinada por um tempo específico (sob dadas condições). As analogias usadas são apenas para tornar mais fácil entender o conceito de largura de banda.



#### 4.2 Diferença da Largura de Banda dos Meios

A largura de banda é um conceito muito útil. Porém, ela tem limitações. Não importa como você envia mensagens ou que meio físico você utiliza, a largura de banda é limitada. Isso se deve tanto às leis da física quanto aos atuais avanços tecnológicos.

Os diferentes meios e as diferentes tecnologias têm diferentes larguras de banda. Isso se deve à física e à engenharia. Há diferenças físicas no modo como os sinais trafegam pelos meios de par trançado, coaxial, sem fio e de fibra óptica, que impõem limites fundamentais à capacidade de carregar as informações, ou na largura de banda, desses meios.

Mas a largura de banda real é determinada pelas tecnologias escolhidas para a sinalização e detecção dos sinais de rede. Por exemplo, a limitação física no cabo de par trançado não-blindado é de até 1 gigabit por segundo. No entanto, dependendo da tecnologia usada, por exemplo, 10Base-T ou Fast Ethernet (100Base-TX), a largura de banda é estabelecida pelas placas de rede e a sinalização utilizada, e não pelas limitações reais do meio.

A memorização das larguras de banda dos diferentes meios e das diferentes tecnologias não é crucial, mas devemos ter sempre em mente que a fibra óptica tem teoricamente a maior largura de banda e aqueles simples e antigos cabos de telefone têm a menor, com as tecnologias UTP, STP, sem fio (wireless) e coaxiais entre elas.

A tabela abaixo ilustra a largura de banda digital máxima possível, com as limitações de comprimento, para alguns meios de rede comuns. Já na tabela seguinte mostramos um resumo dos diferentes serviços e a largura de banda associada a cada serviço.

Lembre-se sempre de que os limites são físicos e tecnológicos.

Meios Típicos	Largura de Banda	Distância Física Máxima
Cabo coaxial de 50 ohm (Ethernet 10Base2)	10 - 100 Mbps	185m
Cabo coaxial de 50 ohm (Ethernet 10Base5)	10 - 100 Mbps	500m
Par trançado não blindado (UTP) Cat. 5 (Ethernet 10BaseT, 100Base-TX)	10 Mbps - 1 Gbps	100m
Multimodo (núcleo de 62,5/125mm) Fibra óptica 100Base-FX, 1000Base-SX	100 Mbps	2.000m
Monomodo (núcleo de 9/125mm) Fibra óptica 1000Base-LX	1 - 10 Gbps	3.000m
Sem fio	300 Mbps	Alguns 100 metros

Tipos de Serviços	Usuário Típico	Largura de Banda
Modem	Pessoas	56 kbps
RDSI	Usuários em trânsito, pequenas empresas	128 kbps
Frame-Relay	Pequenas instituições	56 kbps – 1544 kbps
E1	Entidades maiores	2048 kbps
E3	Entidades maiores	34368 kbps
STM-1 (OC-3 ou STS-3)	Empresas telefônicas, backbone de empresas de comunicação de dados	155,251 Mbps
STM-16 (OC-48 ou STS-48)	Empresas telefônicas, backbone de empresas de comunicação de dados	2,488320 Gbps

#### 4.3 Throughput de Dados em relação à Largura de Banda Digital

Um fato importante em redes é que o desempenho real de uma rede é geralmente menor do que o desempenho máximo da tecnologia. Esse desempenho real é chamado de throughput e depende de muitas variáveis.

Imagine que você tenha muita sorte e tenha um cable modem do último tipo, ou que você tenha recentemente contratado o serviço ADSL para acesso à internet. E mesmo assim imagine que aquele filme que você quer ver, ou a página da Web que deseja carregar, ou o software do qual deseja fazer download ainda leve um tempo enorme para ser recebido.

Você acreditou que estava usando toda a largura de banda anunciada? Há outro conceito importante que você devia ter levado em conta, ele se chama throughput.

Throughput se refere à largura de banda real, medida a uma determinada hora do dia, com o uso de rotas específicas da Internet, enquanto se faz o download de um determinado arquivo. Infelizmente, por muitas razões, o throughput é muito menor que a largura de banda digital máxima possível do meio que está sendo usado. Alguns dos fatores que determinam o throughput e a largura de banda estão listados abaixo:

- Dispositivos de internetworking
- Tipos de dados sendo transferidos
- Topologia da rede
- Número de usuários
- Computador do usuário
- Computador servidor
- Hora do dia
- Falhas de energia ou induzidas pelo tempo

Ao se projetar uma rede, é importante que se leve em conta a largura de banda teórica. A rede nunca será mais veloz do que o seu meio permitir.

A fórmula abaixo representa o tempo mais rápido que os dados poderiam ser transferidos. Ela não leva em conta nenhuma das questões previamente discutidas que afetam o throughput, mas fornece uma estimativa aproximada do tempo que levará para enviar as informações através desse aplicativo/meio específico.

$$\text{Melhor download } T = \frac{S}{BW}$$

$$\text{Download típico } T = \frac{S}{P}$$

**BW** = Largura de banda máxima teórica do "link mais lento" entre a origem e o destino. (medida em bits por segundo)

**P** = Throughput real no momento da transferência. (medido em bits por segundo)

**T** = Tempo de duração da transferência de arquivos. (medido em segundos)

**S** = Tamanho do arquivo em bits.

### **A Importância da Largura de Banda:**

Nesse capítulo tivemos a oportunidade de conhecer um pouco sobre os conceitos que envolvem o tema largura de banda. Vamos agora resumir alguns dos motivos pelos quais devemos aprender esse conceito.

Primeiro, a largura de banda é finita. Independentemente dos meios, a largura de banda é limitada pelas leis da física.

Por exemplo, as limitações da largura de banda, devido às propriedades físicas dos fios telefônicos de par trançado, que existem em muitas casas, é o que limita a 56 kbps o throughput dos modems convencionais. A largura de banda do espectro eletromagnético é finita. Há somente tantas freqüências na onda do rádio, nas microondas e no espectro infravermelho. A fibra óptica tem largura de banda virtualmente ilimitada. Entretanto, o resto da tecnologia para fazer redes de largura de banda extremamente alta, que usem inteiramente o potencial da fibra óptica, está apenas sendo desenvolvida e implementada agora.

É possível economizar muito dinheiro se soubermos como a largura de banda funciona e que ela é finita. Por exemplo, o custo de várias opções de conexão de provedores de serviços de Internet depende, em parte, de quanta largura de banda você requer - em média e no pico de uso. De certa forma, o que você paga é a largura de banda.

É importante que os profissionais do meio tenham conhecimento sobre largura de banda e throughput. Esses são fatores importantes na análise do desempenho de uma rede.

## 5 Utilizando o Modelo OSI para Auxiliar na Resolução de Problemas de Rede (Troubleshooting)

Agora que já conhecemos a teoria do modelo OSI vamos conectar essa teoria com o dia-a-dia de um profissional de redes e com as tarefas diárias e resolução de problemas.

Você pode enxergar o modelo OSI como algo somente teórico, que deve ser decorado para passar em alguma prova de certificação e depois pode ser esquecido, pois não é utilizável na prática, porém esse é um erro grave, cometido por muitos, mas que pode ser facilmente reparado. Vamos agora ver como o modelo OSI pode ajudar um administrador de rede, facilitando seu dia-a-dia.

É bem comum encontrarmos no mercado de trabalho técnicos que são capazes de bloquear uma porta do switch, configurar um endereço IP em uma interface e etc. Mas nem todos conseguem realmente visualizar como rede funciona, com uma visão macro.

O entendimento do modelo OSI, lhe dá a capacidade de entender como os bits são enviados como sinais elétricos através de fios de cobre; como esses bits são remontados em quadros pelo Ethernet na camada 2; como esses quadros são comutados para o destino certo, como o PC desmonta os quadros e pacotes para verificar se ele é o IP de destino; como ele quebra o segmento da camada de transporte, responde com um reconhecimento (ACK), e envia os dados para a camada sessão, apresentação e de aplicação, e como toda comunicação, por menor que seja, exige que todo esse processo aconteça muitas e muitas vezes por segundo.

Através do entendimento do modelo OSI você poderá entender os conceitos de configuração de firewalls e dispositivos mais avançados com mais facilidade. Tendo o conhecimento de que o protocolo TCP está na camada de transporte e que os números de portas são utilizados para identificar aplicações, você poderá entender com maior clareza a criação de regras de filtragem em firewalls que definem o tráfego desejado.

Portanto, uma vez que você entende o modelo OSI, você será capaz de realizar troubleshooting muito mais facilmente e de maneira mais eficaz.

Na hora de realizar o troubleshooting, ou seja, de resolver um problema tenha em mente como o modelo OSI trabalha: o tráfego flui da camada de aplicação para baixo, em direção a camada física e então trafegam no meio físico (cabos ethernet, por exemplo) até a camada física do receptor. Uma vez no receptor, flui da camada física em direção a camada de aplicação.

Do ponto de vista do receptor, ele agora agirá como emissor, os dados seguirão o caminho inverso, indo da camada 7 até a 1, trafegando pelo meio físico até a outra ponta e assim sucessivamente.

Então se uma das camadas do modelo OSI não está funcionando, o tráfego não flui nesse processo. Por exemplo, se a camada de enlace não funciona o tráfego nunca irá conseguir ir da camada de aplicação para a física, pois no meio do caminho a camada de enlace não funcionou.

Uma das abordagens mais utilizadas é realizar o troubleshooting indo de baixo para cima, ou seja, da camada 1 (física) em direção a camada 7 (aplicação). Inicie investigando a camada física (cabos e conectores, por exemplo). Se encontrar algum problema, conserte-o, teste novamente e se a comunicação falhar passe para a camada de enlace.

Ao investigar a camada 2 verifique por exemplo se não existe nenhum endereço MAC duplicado investigando a tabela MAC dos switches de acesso. Ou então as placas de rede podem estar com velocidades fixas, porém diferentes em cada ponta, ou então um lado configurado como half-duplex e outro como full-duplex.

Depois passe para a camada 3 e verifique o endereçamento IP, máscaras de rede e etc... e assim sucessivamente.

Nos hosts lembre que precisamos de um IP, máscara, gateway e um servidor DNS, pelo menos. Caso você tenha testado da camada física até a camada 3 e tudo funcionou, verifique se o IP do DNS configurado nas placas de redes dos hosts está realmente respondendo.

Lembre que para fazer os testes você pode utilizar o ping e o trace, os quais podem auxiliar a detectar problemas da camada física até a camada de rede. Para testar as camadas superiores utilize o acesso a uma aplicação, como telnet, por exemplo.

*Nesse capítulo vamos estudar melhor o protocolo IP e como podemos endereçar os diversos dispositivos de rede.*

*Estudaremos o endereçamento IP versão 4 e noções sobre o endereçamento IP versão 6, assim como dividir esses endereços de forma hierárquica para melhorar o desempenho das redes.*

*Este é um capítulo muito importante e quem aprende e entende como endereçar uma rede consegue ter um diferencial que pode ajudar muito em sua vida profissional.*

*Bons estudos.*

## **Capítulo 5 - Endereçamento IPv4, Sub-redes e Noções de IPv6**

### **Objetivos do Capítulo**

Ao final desse capítulo você deverá entender os seguintes assuntos:

- A estrutura do endereço IP versão 4 e as diversas classes de endereçamento;
- Como dividir as redes IP em sub-redes;
- A estrutura e funcionamento básico do IP versão 6;
- Explicar o processo de roteamento em redes IP.

## Sumário do Capítulo

<b>1</b>	<i>Introdução ao Endereçamento IP</i>	<b>144</b>
<b>2</b>	<i>Sistemas Numéricos Decimal, Binário e Hexadecimal com Foco em Redes</i>	<b>146</b>
<b>3</b>	<i>Entendendo o Endereçamento IP Versão 4</i>	<b>146</b>
3.1	Introdução e Histórico	146
3.2	Endereçamento IPv4 na Prática	149
<b>4</b>	<i>Dividindo as Redes IP em Sub-redes</i>	<b>152</b>
4.1	Sub-redes Válidas, Sub-rede Zero e Sub-rede de Broadcast	156
4.2	RFC 3021 – Uso de Máscaras /31 para Links Ponto a Ponto	157
4.3	VLSM – Máscaras de Sub-rede com Comprimento Variável	159
4.4	Exemplos Práticos e Macetes para Cálculo de Sub-redes e VLSM	162
4.4.1	Analisando um endereço IP e Máscara de Sub-rede	163
4.4.2	Projeto de rede IP pela quantidade de sub-redes	164
4.4.3	Projeto de rede IP pela quantidade de hosts	166
4.4.4	Exemplo de VLSM	167
<b>4.5</b>	CIDR e Sumarização de Rotas	<b>170</b>
<b>5</b>	<i>Tópicos sobre Projeto Lógico de Redes IP</i>	<b>171</b>
<b>6</b>	<i>Tópicos sobre Roteamento IP</i>	<b>173</b>
6.1	Introdução ao Roteamento Estático e Dinâmico	174
<b>7</b>	<i>Acesso à Internet – Proxy e NAT</i>	<b>177</b>
<b>8</b>	<i>IPv6 – Introdução e Características</i>	<b>180</b>

## 1 Introdução ao Endereçamento IP

A camada de Internet, como já estudado anteriormente, é responsável pelo endereçamento lógico e escolha do melhor caminho entre as redes.

O endereço **IP versão 4** ou **IPv4** é um número de **32 bits** escrito com **quatro octetos** (8 bits ou um byte) representados no formato **decimal** como, por exemplo, "10.0.0.1". Os números em cada um dos octetos em decimal podem ir de 0 a 255, portanto os endereços IP têm seu valor mais baixo em **0.0.0.0** e o mais alto em **255.255.255.255**.

Os endereços IP são divididos em duas partes, onde a primeira parte do endereço identifica uma **rede** (conjunto de hosts) e a segunda parte identifica um **host** individual dentro dessa rede. Para identificar a porção de rede e de host é utilizada uma "**máscara de rede**", onde os bits 1 na máscara representam a porção de rede e os bits zero a porção de host no endereço IP. Por exemplo, o IP anterior 10.0.0.1 com uma máscara 255.0.0.0 (11111111.00000000.00000000.00000000) tem o "10" como porção de rede e "0.0.1" como porção de host.

No início do desenvolvimento das redes IP os endereços foram divididos em cinco classes de endereços (A, B, C, D e E), sendo que três dessas classes (A, B e C) podem ser utilizadas como endereços de host. Veja abaixo um resumo sobre as classes de endereços IPv4:

- **Classe A:** Primeiro bit do primeiro octeto é 0 (zero), utiliza o primeiro octeto para definir as redes e os três últimos para endereçar os hosts. Vão das redes 1.0.0.0 a 126.0.0.0.
- **Classe B:** Primeiros dois bits do primeiro octeto são 10 (um, zero), utiliza o primeiro e segundo octetos para definir as redes e os dois últimos para endereçar os hosts. Vão de 128.0.0.0 a 191.255.0.0.
- **Classe C:** Primeiros três bits do primeiro octeto são 110 (um, um, zero), utiliza os três primeiros octetos para definir as redes e o último para endereçar os hosts. Vão de 192.0.0.0 a 223.255.255.0.
- **Classe D:** Esta classe é destinada a endereços de multicast e seus primeiros quatro bits do primeiro octeto são 1110 (um, um, um, zero). Todos os endereços de Multicast são endereços de Host, não existem redes com endereços de Multicast. Sua faixa de endereçamento vai de 224.0.0.0 até 239.255.255.255.
- **Classe E:** Esta é uma classe de endereço especial e reservada, sendo que os primeiros quatro bits do primeiro octeto são 1111 (um, um, um, um). Não são utilizadas para endereçamento, atualmente está reservada a testes pela IETF. Sua faixa de endereçamento vai de 240.0.0.0 até 255.255.255.254.

Existem também endereços IP reservados para uso especial, os quais são:

- A rede **0.0.0.0** é reservada para representação da Internet em rotas IP;
- A rede **127.0.0.0** (127.0.0.1 até 127.255.255.255) está reservada para o endereçamento de loopback, ou seja, se você fizer em seu computador um ping para o IP 127.0.0.1 você está pingando sua própria placa de rede;
- O endereço **255.255.255.255** é reservado para o broadcast local, ou seja, um ping para esse endereço IP e todas as redes IP (classes A, B e C) responderiam ao ping.

Além disso, iremos ver que existe uma abordagem mais atual que não leva em consideração as classes, essa abordagem é chamada de roteamento classless (sem classe) ou **CIDR** (Classless Inter-Domain Routing), a qual visa a melhor utilização de todas as faixas de IP e prolongar o uso do IPv4, pois justamente devido ao esgotamento do IPv4 é que veio a necessidade da criação de uma nova versão de endereçamento IP, o IPv6.

A versão 6 dos endereços IP ou IPv6 utiliza um número de **128 bits** ao invés de 32 como no IPv4. Outra diferença é que o IPv6 é composto por oito blocos de quatro algarismos em hexadecimal e não mais em decimal, ou seja, utiliza dos algarismos de 0 a 9 e A a F (A-10, B-11, C-12, D-13, E-14, F-15).

Para se ter uma ideia da diferença numérica entre o IPv6 e o IPv4, no IPv4 temos um endereço de 32 bits, o que nos dá  $2^{32}$  endereços, ou seja, 4.294.967.296 mais de quatro bilhões de endereços IP. No IPv6 temos  $2^{128}$  possíveis endereços, ou seja, 340.282.366.920 seguido por mais 27 casas decimais, ou seja, **340 bilhões multiplicados por 10 elevado a 27** endereços IP versão 6!

Antes de iniciarmos em como interpretar e realizar os cálculos relativos ao endereçamento IP temos que aprender como funcionam algumas operações matemáticas com números binários e também como interpretar os números em hexadecimal, pois essa é a base para entender as versões 4 e 6 dos endereços IP. Se você julga que já tem essa base pode pular diretamente para o tópico 5.

## 2 Sistemas Numéricicos Decimal, Binário e Hexadecimal com Foco em Redes

Antes de continuarmos você deverá ler a apostila disponibilizada para download na Área do Aluno. É muito importante que você comprehenda como funcionam os sistemas de numeração, pois só assim irá conseguir compreender os conceitos que apresentaremos nos próximos capítulos.

Se você ainda não tem domínio sobre o cálculo binário e o sistema hexadecimal invista um bom tempo estudando a apostila. Caso já tenha esse domínio dê um uma lida rápida para reforçar o seu conhecimento. Em seguida, prossiga para o capítulo 5.

## 3 Entendendo o Endereçamento IP Versão 4

### 3.1 Introdução e Histórico

No início da Internet não era prevista essa taxa de adesão tanto de empresas como do setor público em geral, por isso os IP utilizados para endereçar as redes foram divididos em três classes de tamanhos fixos da seguinte forma (veja a tabela abaixo):

- **Classe A:** definia o bit mais significativo como 0, utilizava os 7 bits restantes do primeiro octeto para identificar a rede, e os 24 bits restantes (3 últimos octetos) para identificar o host. Esses endereços utilizavam a faixa de 1.0.0.0 até 126.0.0.0.
- **Classe B:** definia os 2 bits mais significativo como 10, utilizava os 14 bits seguintes para identificar a rede, e os 16 bits restantes (2 últimos octetos) para identificar o host. Esses endereços utilizavam a faixa de 128.1.0.0 até 191.254.0.0.
- **Classe C:** definia os 3 bits mais significativo como 110, utilizava os 21 bits seguintes para identificar a rede, e os 8 bits restantes (último octeto) para identificar o host. Esses endereços utilizavam a faixa de 192.0.1.0 até 223.255.254.0.

Classe	Formato	Qtdade de Redes	Qtdade de Hosts	Faixa de Endereços IP	Máscara de Rede Padrão
A	7 bits Rede, 24 bits Host	128	16.777.216	1.0.0.0 a 126.255.255.255	255.0.0.0 (/8)
B	14 bits Rede, 16 bits Host	16.384	66.536	128.0.0.0 a 191.255.255.255	255.255.0.0 (/16)
C	21 bits Rede, 8 bits Host	2.097.152	256	192.0.0.0 a 223.255.255.255	255.255.255.0 (/24)

Com o crescimento da Internet esse tipo de classificação passou a não ser mais eficiente, pois as classes acabaram ficando muito limitadas em termos de tamanho de rede e flexibilidade. Atualmente o mundo está vivendo uma fase em que os endereços IP versão 4 disponíveis estão com seus dias contados e já foi dado o início à implementação do IP versão 6, porém como os dois ainda irão conviver por algum tempo temos que saber sobre as duas versões.

Note os seguintes pontos negativos dessa divisão inicial dos endereços IP:

- A classe A atendia um número muito pequeno de redes e ocupava metade de todos os endereços disponíveis, portanto poucas redes com muitos endereços.
- A classe B ainda assim possuía um número muito grande de hosts por rede.
- A classe C permitia criar muitas redes só que com poucos endereços disponíveis.
- Ao mesmo tempo em que as classes A e B traziam muitas vezes desperdícios de endereços IP, a classe C muitas não supria a necessidade de endereços necessários disponíveis.

Outro ponto importante de se ressaltar foi a forma que as faixas classe A foram distribuídas entre grandes instituições como AT&T, IBM, Xerox, HP, Apple, MIT, Ford, dentre outras. É isso mesmo que você está pensando, uma empresa apenas com uma classe A inteira, ou seja, mais de dezesseis milhões de hosts!

Alguns outros fatos históricos interessantes sobre o crescimento da Internet:

- Em 1990 já existiam 313.000 hosts conectados à Internet.
- Em maio de 1992 38% das faixas de endereços classe A, 43% da classe B e 2% da classe C já estavam alocados, sendo que a rede já possuía 1.136.000 hosts conectados.
- Em 1993, com a criação do protocolo HTTP e a liberação por parte do Governo estadunidense para a utilização comercial da Internet, a quantidade de hosts na Internet passou de 2.056.000 em 1993 para mais de 26.000.000 em 1997.

Tendo essa explosão no uso da Internet e requisições de novos endereços IP de uma maneira muito acima da esperada, a IETF (Internet Engineering Task Force) foi obrigada a elaborar estratégias para solucionar a questão do esgotamento dos endereços IP e do aumento da tabela de roteamento, pois com o crescimento do uso da Internet os roteadores também começaram a ficar sobrecarregados.

Em novembro de 1991 é formado o grupo de trabalho ROAD (Routing and Addressing), que apresenta como solução a estes problemas, a utilização do CIDR (Classless Inter-domain Routing). Basicamente o CIDR tem como ideia central o **fim do uso das classes de endereços**, por isso o nome classless ou "sem classes", possibilitando a alocação de blocos de tamanho apropriado conforme a real necessidade de cada rede.

Além disso, o CIDR possibilita a agregação de rotas, ou seja, representar os IPs que uma determinada rede possui com uma rota que representa várias redes de uma vez só, reduzindo o tamanho das tabelas de roteamento. Com o CIDR os blocos de endereços são referenciados como prefixo de redes e ao invés de utilizarmos a máscara passamos a utilizar a notação do endereço com um prefixo, ou seja, endereço barra a quantidade de bits 1 da máscara de rede (a.b.c.d/x - onde os x indicam os bits 1 da máscara de rede). Por exemplo, a máscara 255.0.0.0, que é a padrão da classe A, pode ser representada por um prefixo /8, a da classe B que é 255.255.0.0 como /16 e da classe C que é 255.255.255.0 como /24.

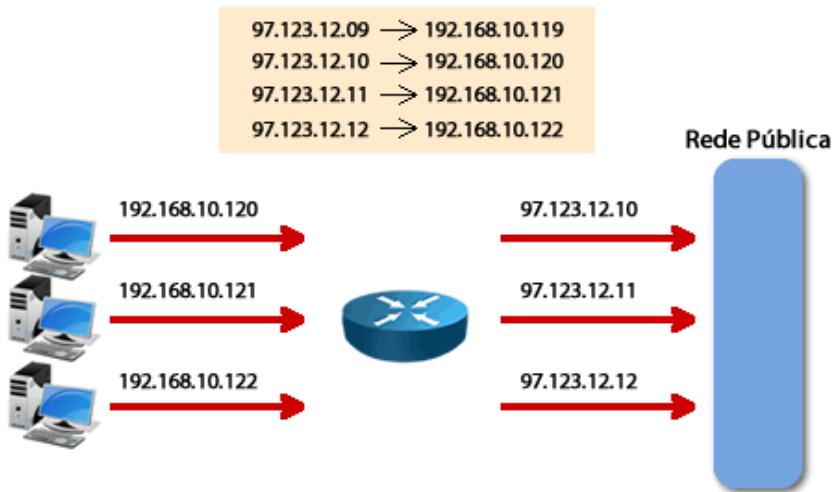
Na prática o CIDR permite a criação de uma rede que era classe C, por exemplo, 192.168.0.0 /24 (255.255.255.0) como 192.168.0.0 /16 (255.255.0.0), onde dentro dela temos as redes /24 de 192.168.0.0 a 192.168.255.0.

Outras duas técnicas que foram desenvolvidas para desacelerar o esgotamento de IPs válidos da Internet foi a introdução dos **endereços IP privados** (RFC 1918) e o uso do **NAT** (Network Address Translation).

Como a maioria das empresas precisam acessar a Internet para utilizar os serviços disponibilizados na rede mundial de computadores, não é necessário que todos os seus hosts estejam com endereços válidos, ao invés disso foram definidos os três intervalos de endereços IP declarados como **privados na RFC 1918**, sendo que a única regra de utilização é que nenhum pacote contendo estes endereços pode trafegar na Internet pública, por isso o nome de privado, pois eles são de uso na Intranet. As três faixas reservadas são:

- 10.0.0.0 a 10.255.255.255 /8 (16.777.216 hosts)
- 172.16.0.0 a 172.31.255.255 /12 (1.048.576 hosts)
- 192.168.0.0 a 192.168.255.255 /16 (65.536 hosts)

Mas se esses endereços não podem trafegar na Internet como um computador com esse endereço poderá acessar a Internet? Através de uma tradução do endereço privado para um endereço público de Internet, o qual é realizado pelo NAT (Network Address Translation - Tradução de Endereço de Rede). O NAT tem como ideia básica permitir que com um único ou poucos endereços IP, vários hosts possam trafegar na Internet. Dentro de uma rede, cada computador recebe um endereço IP privado único, que é utilizado para o roteamento do tráfego interno, e quando ele precisa acessar a Internet uma tradução de endereço é realizada, convertendo endereços IP privados em endereços IP públicos únicos na Internet.



Se você utiliza um serviço ADSL ou Cable Modem em sua casa e tem acesso às configurações dos equipamentos de acesso à Internet pode verificar na que Interface WAN, a que está conectada à Internet, normalmente terá um IP válido de Internet. Já no seu computador ou computadores, você terá um endereço de alguma das faixas da RFC 1918, normalmente uma rede pertencente à faixa do 192.168.0.0 /16. Utilize o comando ipconfig para verificar o IP do seu computador e o depois clique no link abaixo para verificar qual IP que você está utilizando para acessar a Internet:

<http://www.meuip.com.br> ou <http://www.ip-adress.com/>

No segundo link você terá inclusive sua localização e qual seu provedor de serviços de Internet, pois como os endereços IP de Internet são administrados por entidades reguladoras existe um registro das faixas de IP fornecidas a todas instituições, por região, país e tipo de uso (empresa, ONG, pessoal, etc). No Brasil quem administra os endereços IP é o RegistroBr (<http://registro.br>), nesse link você pode registrar domínios e também verificar a disponibilidade de domínios.

Além do NAT, a tradução de endereços IP privados para acesso à Internet pode ser realizada por um servidor chamado **Proxy**. A diferença entre os dois é que o Proxy trabalha na camada de aplicação e permite mais recursos de filtragem que o NAT, pois ele é apenas um tradutor de endereços e não consegue "ler" a camada de aplicação.

Essas e algumas outras soluções diminuíram o problema da escassez de endereços IP, porém não solucionaram definitivamente. Por isso a criação de um novo protocolo de Internet fez-se necessária, porém nesse tópico e no próximo estudaremos apenas a versão 4 do endereçamento IP. Deixaremos o IPv6 para o final do curso.

### 3.2 Endereçamento IPv4 na Prática

Como já comentamos, na prática um endereço IP versão 4 possui 32 bits e é dividido em quatro “**octetos**”, ou seja, quatro conjuntos de oito bits e escritos em formato decimal. O que define que parte do endereço é rede ou host é a “**máscara de rede**” ou “**máscara de sub-rede**”. Por exemplo, se tivermos o endereço 192.168.10.65 e não dermos mais nenhuma característica não seria nada mais que um número qualquer, pois se não pudéssemos dividir os endereços IPs em redes não teríamos uma “**hierarquia**” e não poderíamos dividir as redes entre as diversas empresas e corporações.

Tenha em mente que a “rede IP” representa um conjunto de endereços, assim como no endereçamento postal de um país se não tivéssemos os Estados, Cidades, Ruas e números das casas não conseguíramos enviar cartas. Imagine se tivéssemos apenas o País Brasil e você deseja enviar uma carta para uma pessoa, como seria possível encontrar o João da Silva que tem seu endereço “Brasil”? Precisamos de uma hierarquia, ou seja, vamos mandar uma carta para o Sr João da Silva, que mora no Brasil, na cidade de São Paulo, na rua tal, número tal apartamento 100, agora sim faz sentido concorda? A mesma coisa acontece com as redes IP, para que possamos encontrar um host, que é relativo à uma pessoa ou casa no endereçamento postal, precisamos saber onde ele está e isso quem nos diz é a rede ou sub-rede IP e quem nos mostra isso é a máscara de rede ou de sub-rede.

Vamos completar agora o endereço 192.168.10.65 com a máscara padrão de um endereço de classe C que é o 255.255.255.0. Veja que cada octeto da máscara corresponde ao octeto do endereço, portanto onde temos o bit um (1) na máscara indica que o número que está no endereço IP representa uma rede, convertendo a máscara em binário (que estudamos no capítulo anterior) temos 11111111.11111111.11111111.00000000, ou seja, os três primeiros octetos representam a rede e o último octeto o host. Isso significa que temos um conjunto de micros dentro da rede 192.168.10 e o que procuramos é o que tem o final 65.

Na prática uma rede é quando todos os bits de host estão zerados, portanto representamos a rede que o host final 65 pertence como: 192.168.10.0, pois é no último octeto que estão os bits de host. Os Hosts, ou seja, os endereços que posso configurar em um computador, lap-top, impressora, switch ou interface de um roteador vão do primeiro IP após o endereço de rede até o penúltimo número da sequência. Em nosso exemplo, os endereços de hosts iriam de 192.168.10.1 até 192.168.10.254. Os endereços de host são também chamados de endereços de **Unicast**, para utilização de comunicação entre dois terminais apenas. Já o último valor, em nosso exemplo seria 192.168.10.255, representa o **broadcast direcionado** daquela rede, ou seja, se enviarmos um ping para o último valor da sequência de IPs de uma rede todos os hosts que estiverem ativos dessa rede deveriam responder. Colocamos a palavra “deveriam” porque essa ação pode ser bloqueada em algumas redes por questões de segurança.

Vamos então entender o que é uma rede IP finalizando a análise do endereço 192.168.10.65 com a máscara 255.255.255.0. Já sabemos que sua rede é o 192.168.10.0, que o broadcast é o último valor da sequência (quando todos os bits de host estão em um) e os hosts válidos estão entre a rede e o broadcast, portanto teremos:

- Rede: 192.168.10.0 (quando todos os bits de host estão zerados).
- Broadcast (último valor): 192.168.10.255 (192.168.10.11111111 → o último valor é quando todos os bits de host estão setados em um).
- Endereços que podemos utilizar nos hosts: 192.168.10.1 (o próximo após a rede) até 192.168.10.254 (um a menos que o endereço de broadcast).

Portanto, essa é a definição de uma rede IP, ou seja, ela possui um endereço de rede (todos os bits de host estão zerados), os hosts válidos (um após a rede até um antes do broadcast) e um endereço de broadcast (todos os bits de host estão em 1 – último IP antes da próxima rede).

Uma outra maneira de encontrar a rede que um endereço pertence, a qual é utilizada pelos roteadores e computadores, é fazendo o AND lógico entre o IP e a máscara. Um AND lógico é uma conta em binário que diz que qualquer valor AND zero dá zero e um AND um dá um. Vamos fazer a conta com o endereço 192.168.10.65 AND 255.255.255.0

Onde temos 255 é tudo 1 e onde temos zero é tudo zero, ou seja, temos oito bits um no número 255 e oito bits zero no ponto zero. Fazendo o AND temos que:

- 192 AND 255 = 192
- 168 AND 255 = 168
- 10 AND 255 = 10
- 65 AND 0 = 0

Portanto a rede é a 192.168.10.0 com a máscara 255.255.255.0.

Outro ponto importante é que no tópico anterior foram mostrados vários números em relação a quantidade de redes e hosts por rede, como isso tudo pode ser calculado? Se você conhecer bem o binário conseguirá responder essa pergunta sozinho, senão vamos aprender na sequência.

Quem dá a quantidade de redes ou hosts que teremos são quantos bits vamos utilizar para fazer as redes e hosts, ou seja, os bits um da máscara que podemos utilizar dão a quantidade de redes e os bits zero dão a quantidade de hosts. Por exemplo, foi citado que uma classe C tem sempre os três primeiros bits fixos em "110" e como ela utiliza os três primeiros octetos para rede e somente o quarto octeto para host temos o seguinte cenário:

- 21 bits 1 (r) para redes (24 menos 3 que são fixos) e 8 bits (h) para fazer os hosts.
- 110rrrrr.rrrrrrr.rrrrrrr.hhhhhhhh

Para calcular as redes basta você fazer dois (base do binário) elevado à quantidade de bits de rede que sobraram, nesse caso 21, ou seja,  $2^{21}$  será igual a 2.097.152 de redes classe C.

Já para os hosts temos um detalhe importantíssimo, pois o primeiro IP é utilizado para dar o endereço rede e o último o broadcast, portanto temos que descontar dois IPs da conta, por isso a fórmula para hosts é dois elevado ao número de bits zero da máscara, menos dois, pois temos que descontar a rede e o broadcast que não são utilizados para endereçar hosts. No caso da classe C temos  $(2^8 - 2) = (256 - 2) = 254$  IPs.

Seguindo o mesmo princípio, se tivermos que escolher redes Classe A e B o que variam são as quantidades de redes e hosts que temos por classe. Por exemplo, se fossemos endereçar uma LAN com a rede 172.16.0.0 classe B, a qual tem a máscara padrão 255.255.0.0 ou /16 temos as seguintes características:

- 172.16.0.0 é o endereço de rede, ou seja, quando todos os bits de host estão em zero.
- Como máscara é 255.255.0.0 temos os dois últimos octetos variando como host, pois ela é uma classe B (10rrrrr.rrrrrrr.hhhhhhhh.hhhhhhhh).
- O último endereço IP é o broadcast dessa rede (todos os bits de host estão em um), o qual será 172.16.1111111.1111111 ou 172.16.255.255.
- Tudo que está entre 172.16.0.0 e 172.16.255.255 você pode utilizar para endereçar hosts.
- Portanto temos os endereços válidos iniciando em 172.16.0.1 e o último 172.16.255.254 (um a menos que o broadcast).

Em termos quantitativos, para uma classe B temos 14 bits (pois os dois primeiros do primeiro octeto são sempre 10) de rede e 16 bits de host. O que nos dá  $2^{14}$  redes (16.384) e " $2^{16} - 2$ " endereços de host (65.534 hosts válidos).

Agora vamos a um exemplo com a classe A, endereçando uma LAN com a rede 10.0.0.0, a qual tem a máscara padrão 255.0.0.0 ou /8 temos as seguintes características:

- 10.0.0.0 é o endereço de rede, ou seja, quando todos os bits de host estão em zero.
- Como máscara é 255.0.0.0 temos os três últimos octetos variando como host, pois ela é uma classe A (10rrrrrr.hhhhhhhh.hhhhhhhh.hhhhhhhh).
- O último endereço IP é o broadcast dessa rede (todos os bits de host estão em um), o qual será 10.1111111.1111111.1111111 ou 10.255.255.255.
- Tudo que está entre 10.0.0.0 e 10.255.255.255 você pode utilizar para endereçar hosts.
- Portanto temos os endereços válidos iniciando em 10.0.0.1 e o último 10.255.255.254 (um a menos que o broadcast).

Em termos quantitativos, para uma classe A temos 7 bits de rede (pois o primeiro octeto é sempre 0 na classe A) e 24 bits de host. O que nos dá  $2^7$  redes (128) e " $2^{24} - 2$ " endereços de host (16.777.214 hosts válidos). Porém ao invés de termos 128 temos 126 redes na classe A, pois temos que descontar as redes iniciadas com zero (0.0.0.0) e com 127 (127.0.0.0). Lembre que elas são redes especiais, sendo que a zero é reservada para representar todas as redes ou a Internet e a 127 é reservada para loopback.

Na prática cada rede LAN, VLAN ou WAN precisa de uma rede IP própria, portanto endereçar é atribuir uma rede a uma interface de um roteador ou a uma VLAN e distribuir os endereços de host para essas interfaces e demais terminais. Vamos mais para frente no tópico 8 desse capítulo abordar o projeto lógico de redes e você irá aprender o endereçamento com exemplos e topologias práticas.

Agora você pode aplicar os mesmos conceitos para refazer as contas para as classes A e B, além disso, o que estudamos aqui são as redes baseado em classes ou **classfull**, na sequência iremos dividir essas redes em sub-redes e analisar o cálculo de redes classless, ou seja, como a Internet funciona atualmente, desconsiderando as classes de IP e utilizando prefixos ao invés de máscaras de sub-rede.

#### 4 Dividindo as Redes IP em Sub-redes

Estudamos no tópico anterior que a Internet e as redes IP nasceram baseadas em classes, nas quais apenas 3 tamanhos de rede foram criados através das classes A, B e C, mas e se minha rede não se adequar a esse modelo? Com certeza os valores padrões das classes de 254, 65.534 e 16.777.214 hosts por rede não irão se adequar a todas às necessidades nem das Intranets ou da Internet, por isso várias técnicas foram criadas para dividir as redes e ocupar melhor todos os endereços disponíveis. Já citamos as principais anteriormente e agora vamos aprender como fazer realmente a divisão dessas redes em tamanhos diferentes.

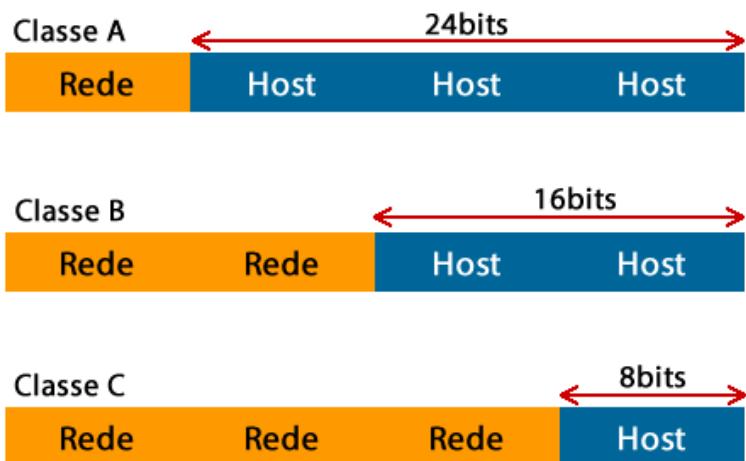
Vamos iniciar com dois conceitos muito parecidos que são a divisão das redes em sub-redes (em inglês subnetting) e o **VLSM (Variable Length Subnet Mask – Máscaras de Sub-rede com Comprimentos Variáveis)**. Dizemos aqui que os conceitos são muito semelhantes porque uma VLSM são várias sub-redes, cada uma com um comprimento diferente, ou seja, é fazer a "sub-rede da sub-rede".

Se você for analisar mais de perto cada uma das classes o que muda entre elas além do primeiro octeto que dá o tamanho da rede? Se você não conseguiu responder sozinho não fique preocupado, mas a resposta certa é a **máscara**. Isso mesmo, a máscara que diz **quantos hosts vamos ter naquela rede**, certo? Mais especificamente são os bits zero da máscara que determinam a quantidade de hosts e os bits um determinam as redes. Então o que vai acontecer se pegarmos um endereço de classe A e utilizarmos uma máscara de classe C nele? Simplesmente vamos dividir essa rede em 65.536 sub-redes de 254 hosts cada uma com apenas um endereço de classe A! Acompanhe abaixo um exemplo com a rede 10.0.0.0:

- Se utilizarmos a rede 10.0.0.0 com máscara /24 ou 255.255.255.0 a diferença básica entre a original da classe A é que pegamos o segundo e terceiro octeto para fazer "sub-redes": antes 255.**0.0.0** → depois 255.**11111111.11111111.00000000**.
- Portanto emprestamos nesse caso 16 bits de host (marcados em amarelo) para fazer "sub-redes", sobrando apenas 8 bits zero para endereçar hosts.
- Com 16 bits emprestados para fazer sub-redes vamos ter  $2^{16}$  sub-redes, ou seja, 65.536 sub-redes. Como sobraram 8 bits zero vamos ter " $2^8 - 2$ " hosts, por isso 254 hosts por sub-rede.
- Originalmente tínhamos uma rede classe A com " $2^{24} - 2$ " hosts, ou seja, 16.777.216 hosts válidos e agora temos "254 (hosts) \* 65.536 (sub-redes)" hosts apenas, que dá 16.646.144 hosts válidos, você consegue explicar por que essa diferença? Porque agora pegamos de cada sub-rede criada 2 IPs que eram válidos e transformamos em "**sub-rede e broadcast**". Veja na sequência abaixo com as sub-redes.
- Agora teremos as sub-redes:
  - 10.0.0.0 /24 → hosts 10.0.0.1 até 10.0.0.254 com broadcast 10.0.0.255
  - 10.0.1.0 /24 → hosts 10.0.1.1 até 10.0.1.254 com broadcast 10.0.1.255
  - 10.0.2.0 /24 → hosts 10.0.2.1 até 10.0.2.254 com broadcast 10.0.2.255
  - E assim por diante até
  - 10.255.254.0 /24 → hosts 10.255.254.1 até 10.255.254.254 com broadcast 10.255.254.255
  - 10.255.255.0 /24 → hosts 10.255.255.1 até 10.255.255.254 com broadcast 10.255.255.255

Note que todos os IPs da classe A 10.0.0.0 /8 continuam presentes, porém com a máscara /24 alguns que eram válidos passaram a ser "sub-redes" e broadcast. Portanto dividir em sub-redes sempre traz uma perda, porém ela é tolerada, pois a perda de usar, por exemplo, uma classe A para endereçar uma rede de 200 hosts é muito maior!

Resumindo, fazer sub-rede nada mais é que “**emprestar**” bits que eram de “**host**” para fazer **novas redes**, a qual é chamada de sub-rede por respeitar a máscara de classe, portanto uma sub-rede de classe A você vai emprestar bits a partir do segundo octeto, na classe B a partir do terceiro octeto e na classe C do quarto octeto. Veja a figura abaixo com as redes classe A, B e C e suas máscaras padrões.



Portanto, analisando ainda a figura acima, na classe A temos teoricamente 24 bits para emprestar para sub-rede, na classe B 16 e na classe C apenas 8. A palavra “**teoricamente**” foi utilizada porque uma rede ou sub-rede precisa ter um endereço de rede, endereços de host e um endereço de broadcast, correto? Isso nos leva a um valor máximo de empréstimo de bits, pois imagine se emprestarmos todos os bits da máscara para fazer sub-rede, teríamos uma máscara de sub-rede com tudo 1, ou seja, 255.255.255.255 que não tem nenhum bit zero, aí a fórmula de hosts seria “ $2^0 - 2$ ” que dá “-1” hosts. Se deixarmos apenas um bit zero temos a máscara em binário 11111111.11111111.11111111.11111110 que é 255.255.255.254, se colocarmos na fórmula de hosts dá “ $2^1 - 2$ ” que vai dar zero como respostas, ou seja, zero hosts porque vamos ter apenas dois IPs, mais tarde você vai ver que aqui tem uma exceção, mas por enquanto vamos deixar assim. Agora se deixarmos 2 bits na máscara já vamos ter “ $2^2 - 2$ ” que dão 2 hosts válidos, agora chegamos ao valor mínimo para a máscara que são pelo menos dois bits de host que em binário temos 11111111.11111111.11111111.11111100, ou seja, a máscara 255.255.255.252 que é o prefixo /30 (pois temos 30 bits um na máscara).

Então, agora chegamos aos valores de empréstimo por classe, pois se temos que deixar pelo menos dois bits zero para a classe A podemos emprestar de 1 a 22 bits, para a classe B vai de 1 a 14 bits e para a classe C de 1 a 6 bits na máscara.

Lembre que apesar de representarmos as máscaras e os IPs em decimal eles são números binários, portanto variam em potências de 2. Isso nos leva que a cada bit de host emprestado dividimos a rede em múltiplos de 2. Vamos a um exemplo utilizando uma classe C 192.168.0.0, a qual tem a máscara padrão 255.255.255.0, e vamos emprestar 1 bits da máscara para fazer sub-rede.

Com isso vamos ter a máscara de sub-rede em binário 11111111.11111111.11111111.10000000 ou 255.255.255.128 em decimal. Veja que a parte original até o terceiro octeto não pode variar, sempre vai ser 192.168.0 e o bit que emprestamos para a máscara torna possível a variação em binário das redes: 00000000 e 10000000, ou seja, temos as seguintes sub-redes possíveis:

1. 192.168.0.00000000 que em decimal é 192.168.0.0
2. 192.168.0.10000000 que em decimal é 192.168.0.128

Veja que na rede original tínhamos os valores de 192.168.0.0 até 192.168.0.255 e agora quebramos esse conjunto de IPs em 2 subconjuntos, um que vai de 192.168.0.0 até 192.168.0.127 e um segundo que inicia em 192.168.0.128 e vai até 192.168.0.255. Veja que os 256 IPs originais estão divididos em dois conjuntos de 128 IPs.

Agora vamos emprestar 2 bits e ver o que acontece com a mesma rede classe C 192.168.0.0. Teremos então a máscara 255.255.255.0 com dois bits emprestados em binário 11111111.11111111.11111111.11000000 ou 255.255.255.192 em decimal. Com isso agora temos dois bits que eram hosts que podem ser variados em 4 sub-redes, que fica em binário 00, 01, 10 e 11, veja abaixo:

1. 192.168.0.00000000 em decimal 192.168.0.0
2. 192.168.0.01000000 em decimal 192.168.0.64
3. 192.168.0.10000000 em decimal 192.168.0.128
4. 192.168.0.11000000 em decimal 192.168.0.192

Veja que da mesma forma do exemplo anterior os 256 IPs originais foram divididos, mas estão todos presentes, porém agora como pegamos 2 bits emprestados temos 4 sub-redes ( $2^2$ ). Com isso os 256 IPs foram quebrados em quatro sub-redes de 64 IPs totais. A sub-rede 192.168.0.0 vai até o IP 192.168.0.63, depois temos uma faixa que vai de 192.168.0.64 até 192.168.0.127, outra que vai de 192.168.0.128 até 192.168.0.191 e a última vai de 192.168.0.192 até 192.168.0.255. Nesse caso então temos 4 sub-redes com 62 IPs válidos para endereçar hosts cada uma ( $2^6 - 2$ ), pois ficaram 6 bits zero na máscara para endereçarmos os hosts.

Note que o número de bits que emprestamos para fazer sub-rede dá a quantidade de sub-redes e os bits zero que sobraram o número de hosts, lembrando-se das fórmulas " $2^n$ " (onde o n são os bits emprestados ou os uns da sub-rede) para as sub-redes e " $2^n - 2$ " para os hosts (onde o n agora são os bits zero que sobraram na máscara).

Para finalizar esse tópico, com o que estudamos até o momento podemos concluir que para classe A temos a máscara padrão 255.0.0.0 ou /8 e podemos fazer sub-redes emprestando bits a partir do segundo octeto, iniciando com a máscara 255.128.0.0, onde emprestamos 1 bit e dividimos a rede em duas novas sub-redes ( $2^1 = 2$ ) com 8.388.606 hosts cada sub-rede, pois sobram 23 bits zero na máscara ( $2^{23} - 2$ ). Podemos chegar a emprestar no máximo 22 dos 24 bits de host da máscara de classe A para criar sub-redes e se pegarmos o último valor possível temos a máscara 255.255.255.252, onde temos apenas 2 hosts válidos ( $2^2 - 2$ ) por sub-rede e um total de 4.194.304 sub-redes ( $2^{22}$ ).

0	8	16	24	32	
11111111	00000000	00000000	00000000		Máscara padrão da classe A (255.0.0.0)
255	0	0	0		

← Onde podemos emprestar bits →

Já para a classe B temos a máscara padrão 255.255.0.0 ou /16 e podemos fazer sub-redes emprestando bits a partir do terceiro octeto, iniciando com a máscara 255.255.128.0, onde emprestamos 1 bit e dividimos a rede em duas novas sub-redes ( $2^1=2$ ) com 32.766 hosts cada sub-rede, pois sobram 15 bits zero na máscara ( $2^{15}-2$ ). Podemos chegar a emprestar no máximo 14 dos 16 bits de host da máscara de classe B para criar sub-redes e se pegarmos o último valor possível temos a máscara 255.255.255.252, onde temos apenas 2 hosts válidos ( $2^2-2$ ) por sub-rede e um total de 16.384 sub-redes ( $2^{14}$ ).

0	8	16	24	32	
11111111	11111111	00000000	00000000		Máscara padrão da classe B (255.255.0.0)
255	255	0	0		← Onde podemos emprestar bits →

Por último, na classe C temos a máscara padrão 255.255.255.0 ou /24 e podemos fazer sub-redes emprestando bits a partir do quarto octeto, iniciando com a máscara 255.255.255.128, onde emprestamos 1 bit e dividimos a rede em duas novas sub-redes ( $2^1=2$ ) com 126 hosts cada sub-rede, pois sobram 6 bits zero na máscara ( $2^6-2$ ). Podemos chegar a emprestar no máximo 6 dos 8 bits de host da máscara de classe C para criar sub-redes e se pegarmos o último valor possível temos a máscara 255.255.255.252, onde temos apenas 2 hosts válidos ( $2^2-2$ ) por sub-rede e um total de 64 sub-redes ( $2^6$ ).

0	8	16	24	32	
11111111	11111111	11111111	00000000		Máscara padrão da classe C (255.255.255.0)
255	255	255	0		← Onde podemos emprestar bits →

Baixe na área do aluno, na parte referente a esse capítulo, a planilha com as sub-redes possíveis classes A, B e C em pdf e analise toda a faixa de IPs e quantidades por bits emprestados para fazer sub-redes.

Uma dica, a máscara /32 é utilizada para identificar um host específico ou até criar rota para um host apenas. Veja na tabela de roteamento do seu computador, caso ele seja Windows, com o comando "route print" que seu próprio IP está configurado como uma /32. Note da saída do comando na figura abaixo.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [versão 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.

C:\Users\dltec>route print

Lista de interfaces
12...c8 85 e5 ee db .....Dell Wireless 1702 802.11b/g/n
11...24 b6 fd 06 dc 17 .....Realtek PCIe GBE Family Controller
 1.....Software Loopback Interface 1
25...00 00 00 00 00 00 e0 Adaptador do Microsoft ISATAP
24...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
35...00 00 00 00 00 00 e0 Adaptador do Microsoft ISATAP #2

Tabela de rotas IPv4

Rotas ativas:
Endereço de rede  Máscara Ender. gateway Interface Custo
  0.0.0.0      0.0.0.0   192.168.1.1 192.168.1.4    25
  127.0.0.0     255.0.0.0  No vínculo       127.0.0.1    306
  127.0.0.1     255.255.255,255  No vínculo       127.0.0.1    306
127.255.255.255 255.255.255,255  No vínculo       127.0.0.1    306
  192.168.1.0     255.255.255,0  No vínculo       192.168.1.4    281
  192.168.1.4     255.255.255,255  No vínculo       192.168.1.4    281
  192.168.1.255 255.255.255,255  No vínculo       192.168.1.4    281
  224.0.0.0      240.0.0.0  No vínculo       127.0.0.1    306
  224.0.0.0      240.0.0.0  No vínculo       192.168.1.4    281
  255.255.255.255 255.255.255,255  No vínculo       127.0.0.1    306
  255.255.255.255 255.255.255,255  No vínculo       192.168.1.4    281

Rotas persistentes:
Nenhuma

```

#### 4.1 Sub-redes Válidas, Sub-rede Zero e Sub-rede de Broadcast

No início da implantação dos endereços IP nos roteadores as redes IP foram implementadas levando em consideração a RFC 950, a qual tinha a seguinte recomendação:

"É recomendado preservar e estender a interpretação dessas redes especiais (rede e broadcast) em sub-redes. Isto significa que as subnets com valores todos zero ou uns no campo de sub-rede não devem ser alocadas em interfaces de rede."

Na prática significa descartar a primeira e a última sub-rede, chamadas sub-rede zero e sub-rede de broadcast ou sub-rede all-ones (todos os bits de sub-rede em um). Por exemplo, se emprestamos três bits para fazer sub-rede ao invés de termos 8 sub-redes ( $2^3$ ) teríamos apenas 6 sub-redes ( $2^3-2$ ), ou seja, não utilizariammos a subnet zero e a de broadcast (all-ones) nessa visão tradicional.

Algumas bibliografias chamam essa metodologia convencional de fazer sub-redes como "sub-redes úteis" ou "válidas". Vamos ver um exemplo prático utilizando a rede 172.16.0.0, conforme tabela 1 ao lado. Note que se utilizamos a abordagem tradicional não utilizamos as sub-redes 172.16.0.0 nem a 172.16.224.0.

Sub-rede	Máscara de Sub-rede	Broadcast	Faixa de Ips Válidos	Nomenclatura Tradicional
<b>172.16.0.0</b>	<b>255.255.224.0</b>	<b>172.16.31.255</b>	<b>172.16.0.1 até 172.16.31.254</b>	<b>Sub-rede zero</b>
172.16.32.0	255.255.224.0	172.16.63.255	172.16.32.1 até 172.16.63.254	Sub-redes Válidas
172.16.64.0	255.255.224.0	172.16.95.255	172.16.64.1 até 172.16.95.254	
172.16.96.0	255.255.224.0	172.16.127.255	172.16.96.1 até 172.16.127.254	
172.16.128.0	255.255.224.0	172.16.159.255	172.16.128.1 até 172.16.159.254	
172.16.160.0	255.255.224.0	172.16.191.255	172.16.160.1 até 172.16.191.254	
172.16.192.0	255.255.224.0	172.16.223.255	172.16.192.1 até 172.16.223.254	
<b>172.16.224.0</b>	<b>255.255.224.0</b>	<b>172.16.255.255</b>	<b>172.16.224.1 até 172.16.255.254</b>	<b>Sub-rede de Broadcast ou All-ones</b>

Porém, atualmente essa recomendação não tem mais validade, com a RFC 1878 essa recomendação anterior foi revogada, pois essa recomendação tem sentido para os endereços de rede e broadcast, porém ter uma sub-rede de rede e uma sub-rede de broadcast além de não ter sentido ainda representa o desperdício de vários IPs que podem ser necessários em um projeto de rede IP.

É importante saber que em alguns exames de certificação ou questões de concurso público esse conceito pode ser cobrado, portanto essa nomenclatura e forma de cálculo devem ser bem conhecidas por todos os administradores de rede.

Nos sistemas operacionais dos principais roteadores como os dos fabricantes Cisco, Juniper e Huawei o comando "ip subnet-zero" ativa a maneira atual de cálculo das redes com a fórmula  $2^n$  (onde o n são os bits emprestados para sub-rede), ou seja, permitindo a configuração das sub-redes zero e de broadcast nos roteadores.

#### 4.2 RFC 3021 – Uso de Máscaras /31 para Links Ponto a Ponto

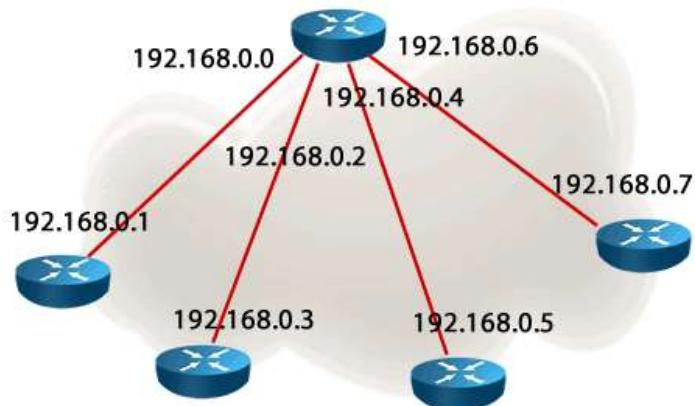
A máscara /31 foi introduzida na RFC 3021 e fornece a opção de aumentar a utilização do espaço de endereçamento IP em links ponto a ponto. Desde então, a maioria dos fabricantes fizeram um movimento para suportar esse padrão. Portanto, essa é uma configuração que não é suportada por todos os fabricantes ou sistemas operacionais e para ser utilizado esse tipo de máscara você precisará consultar se essa máscara é suportada, caso contrário haverá um erro no momento de configurar o IP com a máscara /31.

Em decimal a /31 é 255.255.255.254 e nos dá apenas 2 IPs. Com a filosofia tradicional, anterior à RFC 3021, essa configuração não seria possível, porque com apenas dois IPs teríamos um endereço de rede e um broadcast, portanto, nenhum endereço de host. O que essa recomendação faz é com que os equipamentos de rede entendam esse endereço de rede e de broadcast como sendo um endereço de host.

Isso traz uma vantagem sobre a máscara que tradicionalmente utilizamos com redes WAN (máscara /30 ou 255.255.255.252), pois ela tem 4 IPs, sendo o endereço de rede, dois IPs válidos e um broadcast.

Por exemplo, a rede 192.168.0.0 /30 tem a rede 192.168.0.0, os IPs válidos 192.168.0.1 e 192.168.0.2, sendo o broadcast o IP 192.168.0.3. Com essa mesma rede se utilizarmos o /31 temos duas sub-redes, pois podemos ter a rede 192.168.0.0 /31 com os IPs 192.168.0.0 e 192.168.0.1 e a sub-rede 192.168.0.2 /31 com os IPs 192.168.0.2 e 192.168.0.3. Veja a topologia na figura abaixo.

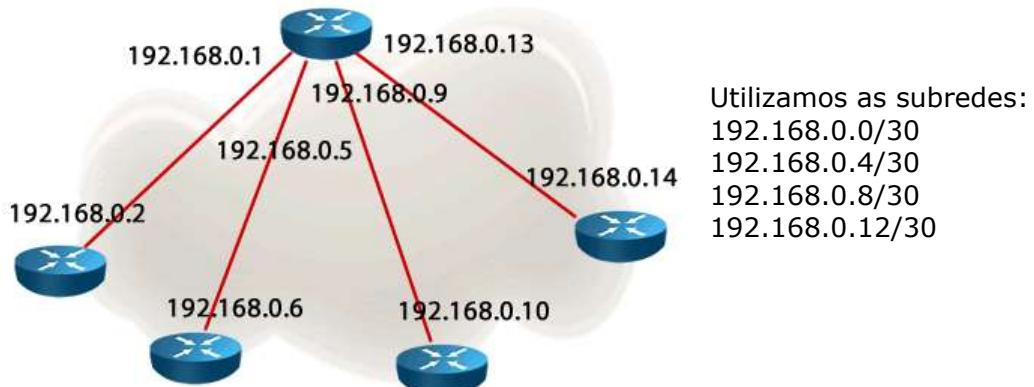
Redes WAN ponto a ponto com máscara /31



Com isso uma operadora pode ganhar vários IPs para endereçar redes WAN ponto a ponto de Internet, por exemplo. Com redes /30 uma classe C ou máscara /24 pode ser dividida em 64 sub-redes, pois temos 256 IPs divididos de 4 em 4. Já com a mesma rede e com a máscara /31 temos as redes divididas de 2 em 2 IPs, totalizando 128 sub-redes, economizando o dobro de IPs para redes ponto a ponto.

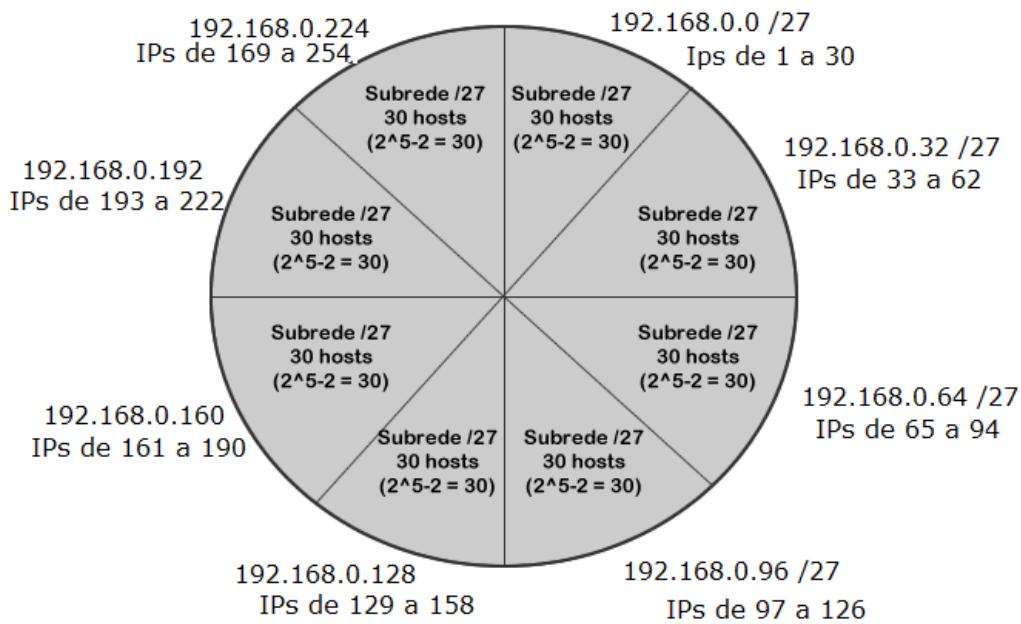
Lembre que se não for citada a RFC 3021 uma rede WAN ou ponto a ponto deve utilizar uma máscara /30 ou 255.255.255.252, além disso, devido a ser uma recomendação muito específica é importante verificar a disponibilidade antes de planejar e configurar uma rede com esse tipo de IP. Veja a figura abaixo a mesma topologia endereçada com redes /30.

Redes WAN ponto a ponto com máscara /30



#### 4.3 VLSM – Máscaras de Sub-rede com Comprimento Variável

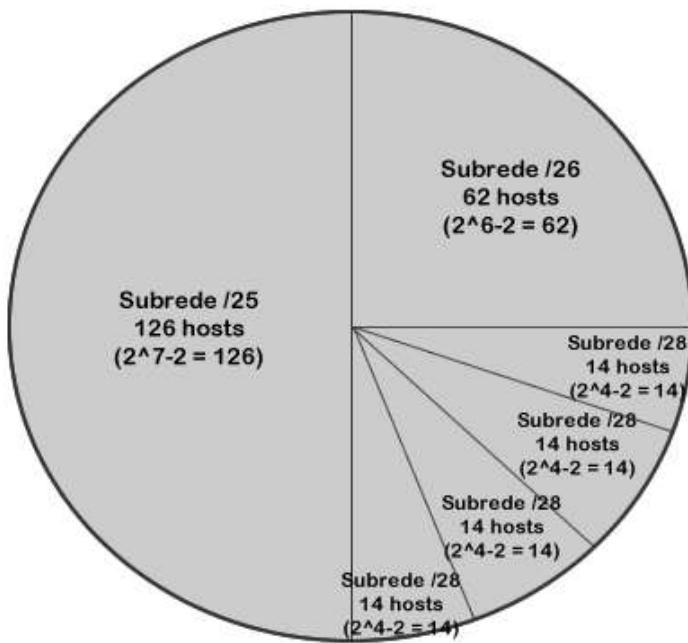
O VLSM (Variable Length Subnet Masking) pode parecer complicado a primeira vista, mas é fácil de entender se você tiver um bom entendimento do conceito de sub-redes. Com a utilização de sub-redes nós dividimos uma rede (classe A, B ou C) em várias sub-redes, cada uma delas com um tamanho fixo. Por exemplo, podemos dividir uma rede classe C em 08 sub-redes com a máscara /27. Veja o exemplo na figura abaixo.



**Rede Classe C /24 (254 hosts)**

Agora com o conceito de VLSM basicamente o que fazemos é **dividir as sub-redes em outras sub-redes**, cada uma com o tamanho necessário para satisfazer os requisitos de projeto de cada rede. Simplificadamente podemos dizer que fazemos sub-redes das sub-redes. Acompanhe na figura abaixo, onde podemos pegar a mesma rede classe C da figura anterior e agora dividir as sub-redes em outras sub-redes, cada uma delas com um tamanho específico. Por isso o termo VLSM (Variable Length Subnet Masking), ou seja, Sub-Redes de Tamanhos Variáveis.

Veja um exemplo de divisão de uma rede classe em VLSM na figura seguinte, onde ela foi dividida em duas sub-redes /25 e uma das /25 foi dividida em outras sub-redes menores. Mais especificamente em uma /26 e quatro /28.



**Rede Classe C /24 (254 hosts)  
dividida com o uso do VLSM**

Colocando em termos numéricos o exemplo anterior vamos utilizar a mesma rede classe C 192.168.0.0 /24 e fazer as VLSMs conforme o gráfico da primeira figura. Quando dividimos a rede com duas /25 temos as seguintes sub-redes:

1. 192.168.0.0 /25 (IPs válidos de 192.168.0.1 até 192.168.0.126 e broadcast 192.168.0.127)
2. 192.168.0.128 (IPs válidos de 192.168.0.129 até 192.168.0.254 com broadcast 192.168.0.255)

Mas agora vamos quebrar a rede com final 128 primeiro em uma rede /26, onde temos uma máscara em binário 11111111.11111111.11111111.11100000, como o último bit da máscara vale 64 essa sub-rede varia de 64 em 64 IPs, portanto ela irá de 192.168.0.128 até 192.168.0.191 e a próxima sub-rede seria a 192.168.0.192. Portanto temos para a sub-rede /26 a sub-rede 192.168.0.128 com IPs válidos de 192.168.0.129 até 192.168.0.190 e broadcast o final 191.

Agora temos livre a faixa de 192 até 255 e vamos quebrar em quatro /28. Uma /28 em binário é 11111111.11111111.11111111.11110000 e como seu último bit vale 16 essa sub-rede vai variar de 16 em 16, portanto a próxima sub-rede tem início no IP 192.168.0.192 e as demais irão variar de 16 em 16, vamos fazer essas sub-redes abaixo:

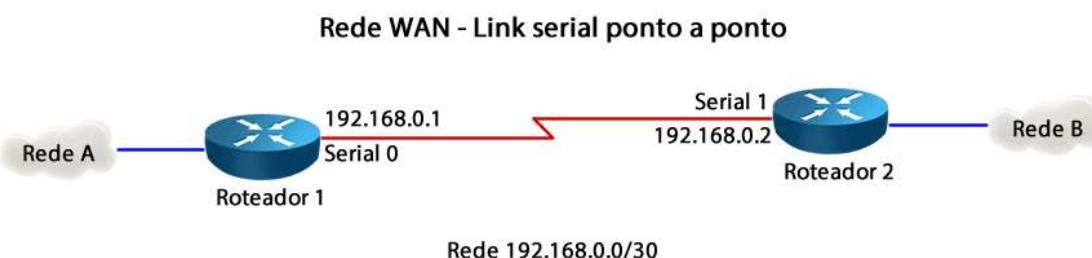
1. 92.168.0.192 → IPs válidos de 193 a 206 com broadcast no final 207
2. 192.168.0.208 → IPs válidos de 209 a 222 com broadcast no final 223
3. 192.168.0.224 → IPs válidos de 225 a 238 com broadcast no final 239
4. 192.168.0.240 → IPs válidos de 241 a 254 com broadcast no final 255

O grande segredo de uma VLSM é respeitar ou prestar atenção para não fazer a sobreposição das faixas de IP. Por exemplo, se alguém fizesse a primeira sub-rede utilizando uma /27, no lugar da /28 o que aconteceria?

Uma /27 tem a máscara 11111111.11111111.11111111.11**1**00000 como o último bit da máscara vale 32 ela varia de 32 em 32 IPs, ou sejam a sub-rede 192.168.0.192 iria de 192 até 223 e iria sobrepor a faixa que planejamos utilizar a rede 192.168.0.208, causando um conflito de IPs entre duas sub-redes.

Quando isso é realizado em um mesmo roteador ele não permite a configuração, porém se as sub-redes estão em roteadores diferentes você terá um sério problema e de difícil resolução prática caso sua documentação não esteja muito bem escrita.

Uma máscara VLSM muito utilizada e “manjada” é a utilizada em redes WAN ponto a ponto /30 ou 255.255.255.252. Ela permite a criação de sub-redes com quatro endereços, onde dois deles são os endereços válidos para configuração das interfaces. Normalmente a topologia de uma rede ponto a ponto é simples e segue o exemplo da figura abaixo.



#### 4.4 Exemplos Práticos e Macetes para Cálculo de Sub-redes e VLSM

Nesse tópico vamos resolver vários modelos de exercícios que você pode encontrar em provas de certificação ou concursos relativos a endereçamento IP, divisão em sub-redes e VLSM. Essa base de cálculo irá ajudar em seu dia a dia como administrador de redes, pois engloba nada mais do que precisamos para entender uma rede e seu projeto.

Antes de irmos para os exemplos práticos vamos passar alguns conceitos que serão utilizados.

Primeiro você deve lembrar-se de quanto vale cada bit em um octeto, conforme figura 1 ao lado. Com esses valores em mente temos como saber, por exemplo, que se emprestarmos 2 bits para sub-rede temos 4 sub-redes ( $2^2=4$ ) ou então que se deixarmos 6 bits zero na máscara de sub-rede temos um total de 62 hosts ( $2^6 - 2 = 64 - 2$ ).

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

Acima desses valores é só multiplicar por 2, por exemplo,  $2^8$  é igual a 256,  $2^9$  dá 512 e  $2^{10}$  dá 1024. Por exemplo, se um exercício pedir que uma rede tenha 1000 hosts devemos deixar 10 bits zero na máscara, pois  $2^{10}$  é igual a 1024, menos dois da fórmula de hosts para descartar a sub-rede e o broadcast temos 1022 hosts, portanto a máscara ficaria 11111111.11111111.11111111**00.00000000** ou 255.255.252.0. Perceba que se emprestássemos apenas 9 bits, teríamos  $2^{9-2}=510 < 1000$ , logo não atenderia ao requisito do projeto.

Outro ponto importante é que as máscaras podem ter apenas alguns valores fixos, pois o empréstimo de bits deve ser feito da esquerda para a direita, portanto podemos ter os valores:

- 0 - 00000000
- 128 - 10000000 (varia de 128 em 128: sub-redes 0 e 128)
- 192 - 11000000 (varia de 64 em 64: sub-redes 0, 64, 128, ...)
- 224 - 11100000 (varia de 32 em 32: sub-redes 0, 32, 64, 96, ...)
- 240 - 11110000 (varia de 16 em 16: sub-redes 0, 16, 32, 48, ...)
- 248 - 11111000 (varia de 8 em 8: sub-redes 0, 8, 16, 24, ...)
- 252 - 11111100 (varia de 4 em 4: sub-redes 0, 4, 8, 12, ...)
- 254 - 11111110 (varia de 2 em 2: sub-redes 0, 2, 4, 6, ...)
- 255 - 11111111 (varia de 1 em 1: sub-redes 0, 1, 2, 3, 4, ...)

Por exemplo, uma máscara 255.222.0.0 não é válida, assim como 255.128.255.0 não pode existir. Lembre-se da folha com as sub-redes possíveis, pois lá mostramos todas as máscaras válidas por classe.

Lembre também que uma rede IP, assim como uma sub-rede, tem um endereço de rede, os IPs válidos e um endereço de broadcast. O endereço de sub-rede é o primeiro valor de IP ou então quando todos os bits de host estão em zero. Já o broadcast é o último IP da sequência ou quando todos os bits de host estão em um. Já os IPs válidos são aqueles que estão entre o endereço de sub-rede e o de broadcast. Para termos esses valores de maneira mais simples basta você lembrar que uma sub-rede é uma rede dividida e o que dá de quanto em quanto essa rede foi dividida é o último bit da máscara de sub-rede.

Por exemplo, uma rede classe B 172.16.0.0 foi dividida em sub-redes utilizando a máscara /28 ou 255.255.255.240, essa máscara em binário é 11111111.11111111.11111111.11110000 e seu último bit 1 (grifado) vale 16, portanto as redes variam de 16 em 16 IPs, sendo que teremos as seguintes sub-redes então: 172.16.0.0, 172.16.0.16, 172.16.0.32, 172.16.0.48, e assim por diante até a última sub-rede 172.16.255.240. Portanto a sub-rede 172.16.0.32 tem o broadcast 172.16.0.47 (um a menos que a próxima sub-rede) e, portanto, os IPs válidos vão de 172.16.0.33 até 172.16.0.46.

Por último lembre que o número de hosts de uma sub-rede é dois elevado ao número de bits zero da máscara menos dois, pois temos que descontar o endereço da sub-rede e o de broadcast. Já o número de sub-redes normalmente é dois elevado ao número de bits emprestados para fazer a sub-rede.

Lembre-se da exceção das sub-redes válidas, as quais foram implementadas no início das redes IP e descontam a primeira e última sub-redes (subnet zero e de broadcast).

Sub-redes válidas	$2^n - 2$
Sub-redes	$2^n$

Com esses conceitos vamos aos exemplos com os principais tipos de exercícios e situações práticas que você pode encontrar em provas de certificação, concursos públicos, entrevistas de emprego ou no dia a dia de um administrador de redes.

#### 4.4.1 Analisando um endereço IP e Máscara de Sub-rede

Nesse tipo de exercício a questão normalmente traz um IP e uma máscara e pode pedir para que você dê informações sobre a sub-rede que ele pertence ou então perguntas relacionadas às sub-redes que podem ser criadas com a mesma máscara do IP de exemplo.

O que pode ser pedido? As questões podem pedir em que sub-rede aquele endereço se encontra, o endereço de broadcast ou faixa de IPs válidos daquela sub-rede, endereços válidos ou de host dentre uma lista de IPs ou então todas as informações anteriores, mas relativas a quaisquer sub-redes criadas com aquela máscara.

Para resolver esse tipo de exercício utilizamos uma metodologia bem simples, baseada na variação que cada sub-rede tem, que é o valor do último bit da máscara de sub-rede. Vamos a alguns exemplos.

**Questão 1** – Dado o IP 172.31.144.16 com a máscara 255.255.224.0 assinale abaixo **dois** endereços IP da mesma sub-rede que são válidos para endereçar hosts.

- a) 172.31.128.0
- b) 172.31.129.200
- c) 172.32.0.1
- d) 172.31.159.255
- e) 172.31.130.1

Para resolver primeiro temos que saber a classe, se você não decorou basta converter o primeiro octeto em binário e classe A inicia em 0, B em 10 e C em 110. Nesse caso temos uma classe B e a sub-rede está a partir do terceiro octeto. Portanto a rede base é 172.31.0.0 /16 e podemos descartar a resposta C.

Agora vamos ver a máscara que é 255.255.224.0 em binário temos 11111111.11111111.11**1**00000.00000000, portanto o último bit da máscara vale 32 e as sub-redes irão variar de 32 em 32, vamos agora ver a que sub-rede aquele IP pertence escrevendo elas abaixo:

- 172.31.0.0, 172.31.32.0, 172.31.64.0, 172.31.96.0, 172.31.128.0, 172.31.160.0, ...

Veja que as sub-redes basta ir somando o octeto utilizando a variação. Note que o 172.31.**144**.16 está entre a sub-rede 172.31.128.0 e 172.31.160.0, por isso ela pertence à sub-rede 172.31.128.0, a qual tem o seu broadcast um a menos que a próxima sub-rede e por isso é 172.31.159.255. Os IPs válidos estão entre a sub-rede e o broadcast, portanto vão de 172.31.128.1 até 172.31.159.254.

Agora fica fácil de analisar as alternativas:

- 172.31.128.0 → Não está correto, é a sub-rede
- 172.31.129.200 → Está correto, é um IP válido
- 172.32.0.1 → Pertence à outra sub-rede, não está correto
- 172.31.159.255 → É o broadcast da sub-rede, não está correto
- 172.31.130.1 → Está correto

Portanto as respostas certas são B e E.

Note que com essa mesma resolução você poderia encontrar endereços de broadcast, endereço de rede da mesma sub-rede ou então endereços válidos de host, redes ou broadcasts de quaisquer sub-redes feitas com a máscara 255.255.224.0!

#### 4.4.2 Projeto de rede IP pela quantidade de sub-redes

Outro modelo de exercício que pode ser cobrado no CCNA é relacionado ao projeto de uma rede IP baseado na quantidade de sub-redes, hosts ou um conjunto de requisitos entre hosts e sub-rede. A resposta esperada geralmente é uma máscara de sub-rede.

Para fazer esse cálculo lembre que existem duas filosofias para cálculo de sub-redes, a tradicional que desconta a sub-rede zero e a de broadcast (primeira e última) e a atual que considera todas as sub-redes, por isso cuidado com o enunciado quando ele citar o termo "sub-redes válidas" ou "sub-redes úteis", pois isso é um indicativo de que está sendo considerada a filosofia tradicional. Se o exercício não citar nada utilize a fórmula  $2^n$ , onde n são os bits emprestados para sub-rede. Vamos agora a um exemplo.

**Questão 1** – Você trabalha em uma empresa como administrador de redes e recebeu a rede 192.168.0.0 para dividir em vinte novas sub-redes. Qual a máscara que melhor se encaixa a essa quantidade solicitada de sub-redes?

- 255.255.240.0
- 255.255.255.252
- 255.255.255.0
- 255.255.255.248
- 255.255.255.128

Como sempre iniciamos com a classe, como o IP é classe C sabemos que o empréstimo de bits é feito no quarto octeto, por isso eliminamos a alternativa A. Além disso, a alternativa C é a máscara padrão da classe C.

Como o exercício pede 20 sub-redes e não fala nada de "redes válidas ou úteis" vamos utilizar a fórmula  $2^n$ , veja na figura 1 ao lado que o empréstimo que melhor se encaixa é o  $2^5$  que dão 32 sub-redes, pois  $2^6$  passa muito do valor e  $2^4$  faltam 4 sub-redes para dar as 20.

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

Como a classe C padrão tem a máscara 255.255.255.0, emprestando 5 bits temos 255.255.255.**11111**000 ou 255.255.255.248, sendo a resposta certa a alternativa D.

Ainda podemos tirar mais conclusões que poderiam ser pedidas no exercício, por exemplo, temos 32 sub-redes com quantos hosts por sub-rede? Basta fazer a conta " $2^n - 2$ ", sendo que o "n" são os bits zero que sobraram na máscara, o que nos dá " $2^3-2=6$ " ou seis hosts válidos por sub-rede.

As sub-redes de uma máscara /29, que é o nosso caso, variam de 8 em 8 IPs, pois o último bit da máscara vale 8, portanto teremos as sub-redes:

1. 192.168.0.0
2. 192.168.0.8
3. 192.168.0.16
4. 192.168.0.24
5. 192.168.0.32
6. ...
7. 192.168.0.248

Lembre que para saber os hosts válidos e o broadcast você deve pegar um valor a menos que a próxima sub-rede e temos o broadcast, já os hosts válidos estão entre o primeiro IP após o endereço de sub-rede e um antes do broadcast (penúltimo IP), veja abaixo:

1. 192.168.0.0 → broadcast 192.168.0.7 → IPs válidos de 192.168.0.1 até 192.168.0.6
2. 192.168.0.8 → broadcast 192.168.0.15 → IPs válidos de 192.168.0.9 até 192.168.0.14
3. 192.168.0.16 → broadcast 192.168.0.23 → IPs válidos de 192.168.0.17 até 192.168.0.22
4. 192.168.0.24 → broadcast 192.168.0.31 → IPs válidos de 192.168.0.25 até 192.168.0.30
5. E assim por diante...

Outro jeito de resolver esse exercício é transformar os octetos de sub-rede das máscaras dadas e verificar a quantidade de sub-redes possíveis, fica bem mais simples, porém mostramos o primeiro método porque para um projeto real ele é mais correto de ser utilizado.

#### 4.4.3 Projeto de rede IP pela quantidade de hosts

Este modelo é bem parecido com o anterior, porém agora você deve pensar não em empréstimo, mas sim em “**quantos bits zero eu devo deixar na máscara**” para suportar a quantidade de hosts solicitada, pois são os bits zero que determinam a quantidade de hosts que uma sub-rede terá.

Para a quantidade de hosts a fórmula é uma só “ **$2^n - 2$** ” onde o “**n**” são os bits zero que restaram na máscara de sub-rede para endereçar os hosts. Vamos ao exemplo.

Questão 1 – Você trabalha em uma empresa como administrador de redes e recebeu a rede 172.16.0.0 para dividir pelo menos vinte novas sub-redes que suportem obrigatoriamente no mínimo 500 hosts. Qual a máscara que melhor se enquadra a essa quantidade solicitada de hosts por sub-redes? Resposta: \_\_\_\_ . \_\_\_\_ . \_\_\_\_ . \_\_\_\_

Quando temos um projeto por número de hosts temos que pensar em “quantos bits zero eu deixo na máscara para os hosts?”. Se precisamos de 500 host precisamos encontrar um valor de “ $2^n - 2$ ” que seja próximo de 500. Lembre dos principais valores na figura abaixo.

2 <sup>10</sup>	2 <sup>9</sup>	2 <sup>8</sup>	2 <sup>7</sup>	2 <sup>6</sup>	2 <sup>5</sup>	2 <sup>4</sup>	2 <sup>3</sup>	2 <sup>2</sup>	2 <sup>1</sup>	2 <sup>0</sup>
1024	512	256	128	64	32	16	8	4	2	1

Portanto, o valor que mais se aproxima de 500 é o  $2^9$  que dá 512, menos dois ficamos com 510 hosts por sub-rede. Agora vem o segredo, começamos a deixar os bits zero a partir do último octeto em direção ao primeiro, como precisamos de 9 bits zero teremos:

00.00000000 (o último octeto todo em zero e mais dois bits do terceiro octeto em zero)

Agora basta completar com bits “1”: **11111111.11111111.11111111.00000000**. Temos então uma máscara 255.255.254.0 ou /23.

Lembre também que o enunciado pede pelo menos 20 sub-redes, será que temos esse valor com essa máscara? Como temos uma classe B o empréstimo de bits para sub-rede foi realizado no terceiro octeto em um total de sete bits uns, portanto temos  $2^7$  sub-redes que dá um total de 128 sub-redes, portanto a máscara atende os requisitos do exercício.

Fazendo a mesma análise do tópico anterior, para a rede 172.16.0.0 com a máscara /23 temos um total de 128 sub-redes que variam de 2 em 2, ou seja, temos a sub-rede zero como 172.16.0.0 e a sequência somando dois no terceiro octeto o que nos dá 172.16.2.0, 172.16.4.0, 172.16.6.0, 172.16.8.0, ... , até a última que é 172.16.254.0.

Portanto para cada sub-rede temos a seguinte faixa de IPs válidos e broadcast:

1. 172.16.0.0 → broadcast 172.16.1.255 → IPs válidos 172.16.0.1 até 172.16.1.254
2. 172.16.2.0 → broadcast 172.16.3.255 → IPs válidos 172.16.2.1 até 172.16.3.254
3. 172.16.4.0 → broadcast 172.16.5.255 → IPs válidos 172.16.4.1 até 172.16.5.254
4. E assim por diante...

Note que com essa máscara temos IPs final zero e 255 válidos! Muito cuidado com máscaras menores que /24, ou seja, /23 até /8, pois com elas vocês terão IPs final zero e 255 que são válidos, portanto não marquem respostas que perguntam sobre IPs válidos, endereços de rede ou broadcast sem antes ter certeza da faixa de IPs com a metodologia aqui mostrada.

Esse é um erro muito comum de se cometer em uma prova ou exame, pois acabamos nos acostumando a treinar muito máscaras de classe C ou maiores que /24, porém lembre-se dessa dica, ela pode ser útil tanto em provas como em seu dia a dia.

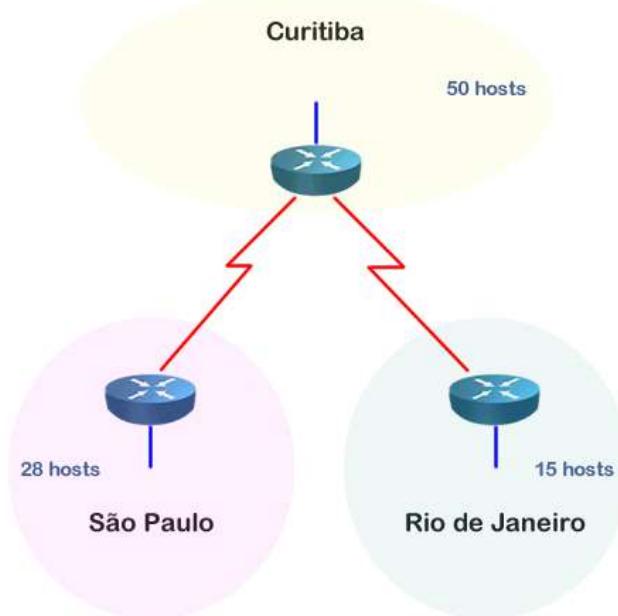
Por exemplo, para a rede 172.16.4.0 temos os IPs 172.16.4.255, 172.16.5.0, 172.16.5.255, 172.16.6.0, 172.16.6.255 e 172.16.7.0 válidos, ou seja, você pode configurar esses IPs em hosts ou interfaces de roteadores que irão funcionar!

#### 4.4.4 Exemplo de VLSM

Como já mencionado anteriormente, uma VLSM nada mais é que quebrar uma sub-rede em sub-redes menores, ou seja, todos os cálculos que fizemos até agora continuam valendo. O grande cuidado ao utilizar VLSMs é de não sobrepor sub-redes, ou seja, acabar utilizando máscaras que ultrapassam os limites de outras sub-redes e podem causar conflitos de IP entre essas sub-redes, pois alguns IPs podem estar presente em ambas sub-redes.

Para fixarmos o conceito de VLSM vamos a um exemplo prático. Suponha que você trabalhe como administrador de rede em uma empresa que tenha recebido o bloco de endereço IP 195.125.5.0/24 para endereçar três escritórios, conforme dados abaixo e topologia na figura seguinte.

- 1 escritório com 50 hosts em Curitiba
- 1 escritório com 28 hosts em São Paulo
- 1 escritório com 15 hosts no Rio de Janeiro



Vamos começar a resolução calculando as faixas de endereços para cada escritório, começando por Curitiba por ser o maior. Como precisamos de 50 hosts, temos que utilizar 6 bits para hosts ( $2^6=64 > 50$ ). Utilizando 6 bits para hosts temos 2 bits para sub-rede, ou seja, teremos uma máscara /26.

A alocação de uma sub-rede e dos IPs que utilizaremos em Curitiba segue abaixo:

- Sub-rede 195.125.5.0/26
- Endereço de rede é 195.125.5.0
- Endereço de broadcast é 195.125.5.63
- Endereço de hosts 195.125.5.1 a 195.125.5.62

O próximo passo é fazer o mesmo procedimento para São Paulo. Ou seja, precisamos de 28 hosts ( $2^5 - 2 = 30 > 28$ ). Utilizamos 5 bits para hosts e 3 para rede, ficando uma máscara /27. Como a sub-rede de Curitiba parou no endereço "63" vamos iniciar a sub-rede de São Paulo com o "64", porém ele deve estar na faixa de endereços de rede da máscara /27, que no caso está.

A alocação de uma sub-rede e dos IPs que utilizaremos em São Paulo segue abaixo:

- Sub-rede 195.125.5.64/27
- Endereço de rede é 195.125.5.64
- Endereço de broadcast é 195.125.5.95
- Endereço de hosts 195.125.5.65 a 195.125.5.94

De forma análoga no Rio de Janeiro teremos 15 hosts. Ou seja, 5 bits para hosts ( $2^5 - 2 = 30 > 15$ ) e 3 bits para rede. Como já utilizamos a rede 195.125.5.64/27 para São Paulo e ela vai até o IP "95", utilizaremos a próxima para o Rio de Janeiro que inicia em "96", ficando da seguinte forma a alocação para o Rio de Janeiro:

- Sub-rede 195.125.5.96/27
- Endereço de rede é 195.125.5.96
- Endereço de broadcast é 195.125.5.127
- Endereço de hosts 195.125.5.97 a 195.125.5.126

Nesse ponto já temos o cálculo das sub-redes para a LAN de cada escritório, mas como em nossa topologia exemplo estamos utilizando enlaces seriais, precisaremos também de sub-redes para endereçar os links ponto-a-ponto entre as unidades. Primeiramente vamos calcular os endereços do enlace entre Curitiba-São Paulo.

Precisamos apenas de 2 endereços de hosts (um para cada interface serial de cada roteador). Logo, 2 bits para hosts é o suficiente e ficamos uma máscara /30, ficando da seguinte forma. Lembre-se também que o último IP utilizado foi o final "127", por isso vamos iniciar as redes WAN com o "128".

Enlace Curitiba-São Paulo:

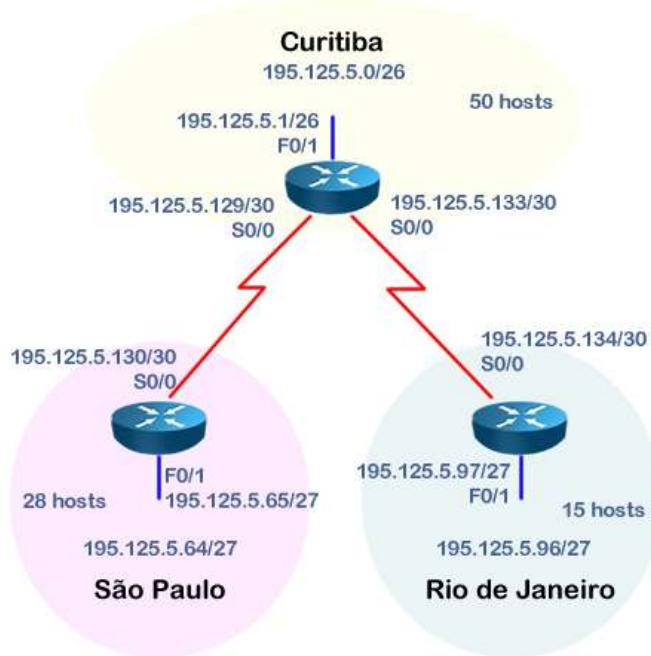
- Sub-rede 195.125.5.128/30
- Endereço de rede é 195.125.5.128
- Endereço de broadcast é 195.125.5.131
- Endereço de hosts 195.125.5.129 e 195.125.5.130

Enlace Curitiba-Rio de Janeiro:

- Sub-rede 195.125.5.132/30
- Endereço de rede é 195.125.5.132
- Endereço de broadcast é 195.125.5.135
- Endereço de hosts 195.125.5.133 e 195.125.5.134

Nesse ponto já temos todo o nosso esquema de endereçamento calculado e você poderá notar que a partir de um bloco contínuo de endereços classe C padrão (195.125.5.0) conseguimos fazer a divisão em blocos de endereços variáveis, otimizando a utilização dos endereços IP. Isso graças ao conceito de VLSM.

Veja a figura abaixo com a topologia completa já com os endereços calculados.



#### 4.5 CIDR e Sumarização de Rotas

No tópico anterior aprendemos a calcular sub-redes e utilizar o conceito de máscaras de comprimento variável (VLSM) para dividir e otimizar as sub-redes feitas a partir de máscaras classe A, B ou C, portanto ainda estávamos respeitando o conceito de classe ou classfull.

Agora imagine que você é um provedor de Internet e troca anúncios de rotas com outros provedores vizinhos e recebe da entidade que administra a alocação de IPs públicos todas redes classe B 160.0.0.0 até 160.255.0.0, um total de 256 sub-redes IP que podem gerar milhares ou até milhões de sub-redes IP. Você pode anunciar as 256 redes ou suas sub-redes para seus vizinhos ou então economizar anúncios utilizando o conceito do roteamento classless, ou CIDR, com a sumarização de rotas.

Vamos ver na prática utilizando a faixa de IPs acima. Como uma classe B normalmente você teria as seguintes redes:

- 160.0.0.0
- 160.1.0.0
- 160.2.0.0
- ... até
- 160.255.0.0

Porém, note que no segundo octeto temos uma variação completa dos oito bits daquele octeto, eles podem variar de 0 até 255, portanto podemos utilizar um anúncio resumido (sumarizado) com o seguinte prefixo: 160.0.0.0 /8.

Se formos analisar mais a fundo, a rede 160.0.0.0 /8 vai dos IPs 160.0.0.1 até 160.255.255.254 e tem o broadcast 160.255.255.255, ou seja, os IPs individuais de cada sub-rede estão contidos nesse anúncio, portanto podemos ao invés de anunciar as 256 redes, anunciar somente o bloco CIDR 160.0.0.0/8 que dá no mesmo!

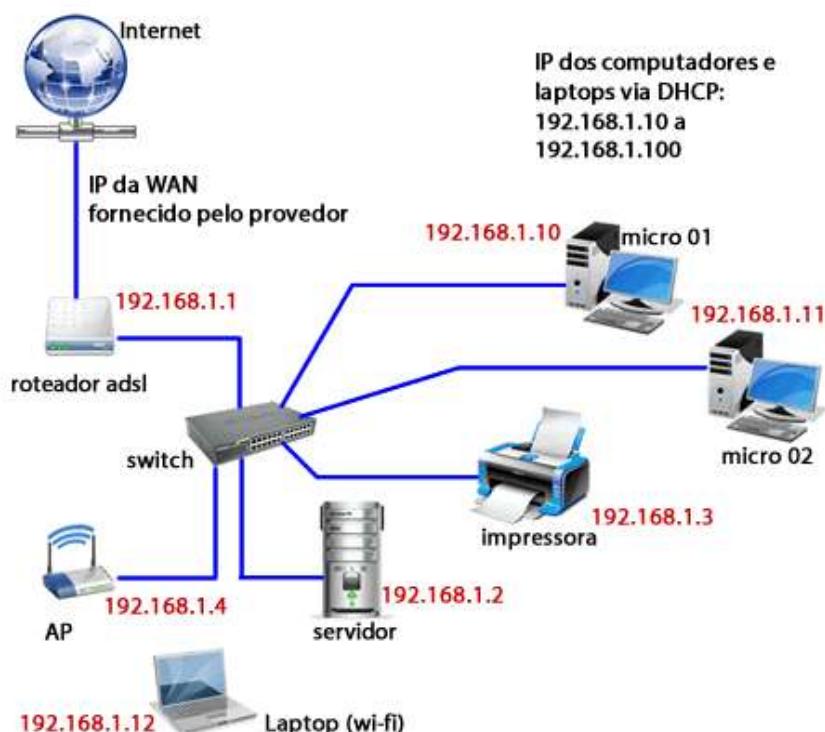
Portanto, o CIDR é utilizar máscaras “menores” que a padrão de cada classe e a sumarização é criar uma nova rede ou bloco CIDR com várias redes ou sub-redes que deveriam ser anunciadas, economizando anúncios trocados entre os roteadores.

Com isso finalizamos os conceitos do IP versão 4. Nos próximos tópicos desse capítulo você ainda verá outros assuntos importantes relacionados ao IPv4 e os conceitos e funcionamento básico do IP versão 6.

## 5 Tópicos sobre Projeto Lógico de Redes IP

Com o que aprendemos até o momento sobre endereçamento IP versão 4, dispositivos de rede e acesso à Internet podemos utilizar esses conhecimentos para elaborar a topologia lógica de uma rede IP.

Vamos imaginar uma rede simples, de uma pequena empresa com no máximo 20 computadores, um servidor e acesso à Internet. Nesse caso precisaremos de um switch e/ou um Access Point, assim podemos conectar o servidor e alguns micros via cabo UTP e os demais via interface aérea, além disso, precisaremos de um dispositivo que faça a conexão via Internet. Vamos supor aqui que a conexão utiliza serviço banda larga ADSL. Veja a topologia lógica na figura abaixo.



Como o serviço de ADSL é fornecido por um provedor de Internet o endereço IP da interface WAN (que conecta diretamente ao serviço de ADSL) é fornecido pelo provedor. Normalmente no serviço ADSL esse IP é um endereço válido de Internet e é trocado de tempos em tempos, se a empresa precisa que o IP seja fixo deverá pagar uma tarifa adicional.

Na rede interna (intranet) temos que escolher uma rede IP para distribuir os endereços aos computadores, servidores, laptops, impressoras e para a interface LAN do roteador ADSL. Nesse caso escolhemos a rede 192.168.0.0/24. Para atribuir os IPs aos computadores utilizaremos o serviço de DHCP, liberando dos IPs 192.168.0.10 a 192.168.0.100 para os computadores que pegam IP dinâmico. Dos IPs 192.168.0.1 até 192.168.0.9 vamos reservar para configurar os IPs fixos, conforme abaixo:

- O IP 192.168.0.1 configuramos na interface LAN do roteador;
- O IP 192.168.0.2 para o servidor local;
- O IP 192.168.0.3 para uma impressora de rede;
- O IP 192.168.0.4 para o Access Point (AP).

Além disso, se o switch for gerenciável, ou seja, permitir acesso remoto via IP você pode atribuir um IP para ele também. Com relação ao AP, normalmente ele pode funcionar como roteador ou como bridge, ou seja, você configura um IP da interface WAN, que seria nesse caso o 192.168.0.4, e os micros sem fio precisariam de outra rede IP interna para sair. No caso dele funcionar como bridge, aí o servidor DHCP que está configurado no roteador ADSL irá fornecer também os IPs dos terminais sem fio. Nesse exemplo consideramos um AP como bridge.

Lembre-se também que para o acesso à Internet você deve configurar o endereço de pelo menos um servidor DNS em seus hosts. Em redes pequenas o DNS é o IP do próprio roteador ADSL, sendo que ele pega automaticamente um ou mais IPs de DNS passados pelo provedor de serviços, portanto o roteador ADSL nesse caso acaba servindo como cache e também um intermediário entre os micros internos e o servidor DNS do provedor de serviços.

Note que nossa rede interna utiliza uma faixa de endereço privativo (RFC 1918), portanto para acesso à Internet o roteador ADSL deve suportar o NAT (Network Address Translation) para que os IPs privativos sejam convertidos no IP válido que está configurado na interface WAN dele. Em um tópico posterior, sobre Acesso à Internet, o funcionamento do NAT será explicado.

Basicamente em uma rede de pequeno porte de até 25 computadores, essa topologia se encaixa perfeitamente, porém tudo depende de cada projeto e do segmento de cada empresa, pois em empresas onde a propriedade intelectual ou movimentações financeiras de grande porte estão envolvidas, independentemente do número de computadores o uso de segmentação com VLANs, firewalls, IPS e topologias redundantes podem ser adotadas.

## 6 Tópicos sobre Roteamento IP

Como estudamos nesse capítulo, as redes IP são conjuntos de hosts que compartilham um domínio de broadcast e podem ser redes internas (Intranet) ou estarem conectadas à rede pública (Internet).

Para que os dispositivos possam se comunicar entre as diferentes redes em uma Intranet ou na Internet um dispositivo de camada 3 (Rede ou Internet) deve fazer o roteamento dos pacotes, ou seja, encaminhar os pacotes recebidos em uma interface para outra interface de saída que “conheça” a rede de destino para qual o pacote está sendo enviado. Esse processo pode ser chamado também de “comutação” ou “chaveamento” em algumas bibliografias, pois o pacote é comutado ou chaveado para uma interface de saída.

Essa análise sobre as redes que um roteador ou até mesmo um terminal (endpoint) tem conhecimento é realizada através da consulta à “**tabela de roteamento**” IP de cada dispositivo. Portanto, nos equipamentos que atuam na camada 3 do modelo OSI (como por exemplo, roteadores, switches camada 3 e até nos computadores) existe uma tabela que contém as redes que cada dispositivo conhece, as entradas nessa tabela chamamos de “rotas”. Uma rota deve conter pelo menos três informações básicas: rede de destino, máscara ou prefixo e a interface ou IP de saída, a qual tem alcance à rede de destino. Veja um exemplo na tela da figura abaixo da tabela de roteamento de um computador com sistema operacional Windows (comando route print).

```
C:\Windows\system32\cmd.exe
C:\Users\dltec>route print
=====
Lista de interfaces
12...c0 18 85 e5 ee db .....Dell Wireless 1702 802.11b/g/n
11...24 b6 fd 06 dc 17 .....Realtek PCIe GBE Family Controller
43...08 00 27 00 d0 3c .....VirtualBox Host-Only Ethernet Adapter
1.....Software Loopback Interface 1
25...00 00 00 00 00 00 e0 Adaptador do Microsoft ISATAP
24...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
26...00 00 00 00 00 00 e0 Adaptador do Microsoft ISATAP #2
47...00 00 00 00 00 00 e0 Adaptador do Microsoft ISATAP #3
=====

Tabela de rotas IPv4
=====
Rotas ativas:
Endereço de rede      Máscara    Ender. gateway      Interface   Custo
          0.0.0.0        0.0.0.0       192.168.1.1     192.168.1.66    25
          127.0.0.0       255.0.0.0      No vínculo       127.0.0.1     306
          127.0.0.1       255.255.255.255  No vínculo       127.0.0.1     306
        127.255.255.255 255.255.255.255  No vínculo       127.0.0.1     306
          192.168.1.0     255.255.255.0  No vínculo       192.168.1.66    281
          192.168.1.66     255.255.255.255  No vínculo       192.168.1.66    281
          192.168.1.255    255.255.255.255  No vínculo       192.168.1.66    281
          192.168.56.0     255.255.255.0  No vínculo       192.168.56.1    276
          192.168.56.1     255.255.255.255  No vínculo       192.168.56.1    276
        192.168.56.255    255.255.255.255  No vínculo       192.168.56.1    276
          224.0.0.0        240.0.0.0      No vínculo       127.0.0.1     306
          224.0.0.0        240.0.0.0      No vínculo       192.168.1.66    281
          224.0.0.0        240.0.0.0      No vínculo       192.168.56.1    276
        255.255.255.255  255.255.255.255  No vínculo       127.0.0.1     306
        255.255.255.255  255.255.255.255  No vínculo       192.168.1.66    281
        255.255.255.255  255.255.255.255  No vínculo       192.168.56.1    276
=====
```

Note que a saída do comando inicia com uma lista de interfaces de rede (físicas ou virtuais) configuradas no computador com seu endereço MAC no campo "Lista de Interfaces". Logo abaixo temos a "tabela de rotas IPv4" onde estão as redes conhecidas pelo computador.

Na tabela de roteamento do Windows são mostradas redes IP, os endereços IPs configurados com a máscara /32 (255.255.255.255) e também endereços de Multicast e de Broadcast. Vamos analisar abaixo um resumo das principais entradas conforme tabela seguinte.

Endereço de Rede	Máscara	Gateway	Interface Local	Custo
192.168.1.0	255.255.255.0	No Vínculo	192.168.1.66	281
192.168.56.0	255.255.255.0	No Vínculo	192.168.56.1	276
127.0.0.0	255.0.0.0	No Vínculo	127.0.0.1	306
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.66	25

Vamos analisar cada linha, a primeira linha significa que o computador tem uma rota para a rede 192.168.1.0 /24 em sua interface local, que possui o IP 192.168.1.66. O "No Vínculo" no campo gateway significa que o pacote é roteado localmente e não precisa de um gateway para ser encaminhado, pois a interface está diretamente conectada a essa rede LAN. O mesmo ocorre na linha 2 para a rede 192.168.56.0 que está conectada diretamente a uma interface local com IP 192.168.56.1.

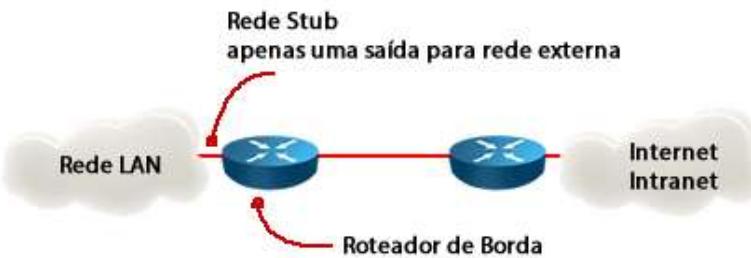
Na linha 3 temos a rede de loopback, a qual é um IP interno da placa de rede, ou seja, se você pingar o IP 127.0.0.1 você estará pingando sua própria placa de rede. Ele é utilizado para processos internos do host.

Por último, temos a saída para Internet com a rota 0.0.0.0 e máscara 0.0.0.0, a qual aponta para o IP 192.168.1.1 como gateway. Essa rota é chamada de rota padrão ou default e sempre é a última a ser utilizada pelo dispositivo, significa que se nenhuma rota explícita (direta) para a rede de destino for encontrada o pacote deve ser encaminhado para a interface ou IP de gateway configurado na tabela de roteamento. Se não houvesse essa rota instalada na tabela de roteamento esse computador poderia enviar pacotes apenas para as redes 192.168.1.0, 192.168.56.0 e 127.0.0.0, sendo que quaisquer outras redes não conhecidas não poderiam ser alcançadas.

## 6.1 Introdução ao Roteamento Estático e Dinâmico

Em um roteador ou switch layer 3 o processo é semelhante ao que vimos anteriormente, porém um pouco mais complexo, pois é preciso que os dispositivos de camada 3 normalmente conheçam mais rotas que apenas suas redes diretamente conectadas e um IP de gateway. Quando falamos no roteamento de uma rede de médio ou grande porte podemos escolher entre criar rotas estáticas (manuais), utilizar um protocolo de roteamento dinâmico para criar e manter as entradas na tabela de roteamento ou então uma mistura desses dois tipos.

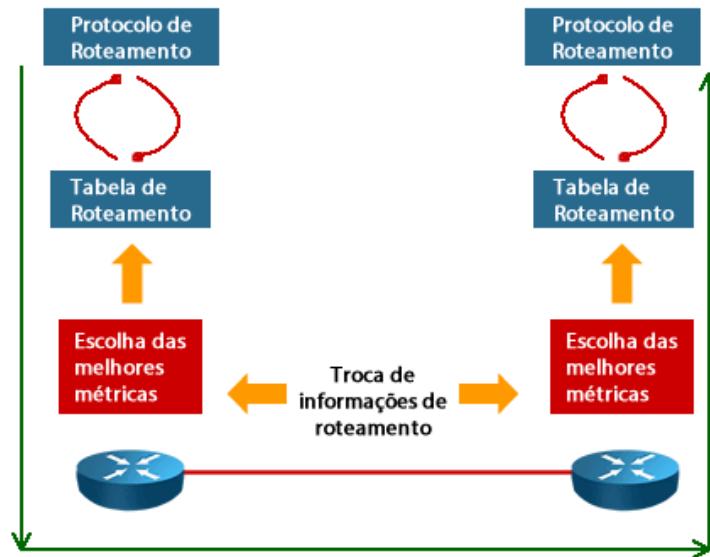
As rotas estáticas são entradas manuais realizadas pelos administradores de rede nos dispositivos de camada 3, portanto não são recomendadas para redes muito grandes, pois cada alteração ou inserção de um novo dispositivo o trabalho para reconfigurar as tabelas de roteamento pode ser muito grande. Uma rota estática é recomendada para os casos onde você tem apenas um caminho possível, chamada de rede stub, veja a figura abaixo.



Como o roteador de borda possui apenas uma conexão serial com a Internet ou demais redes da Intranet é mais fácil criar apenas uma rota padrão de saída apontando para as demais redes do que habilitar um protocolo de roteamento dinâmico nesse roteador.

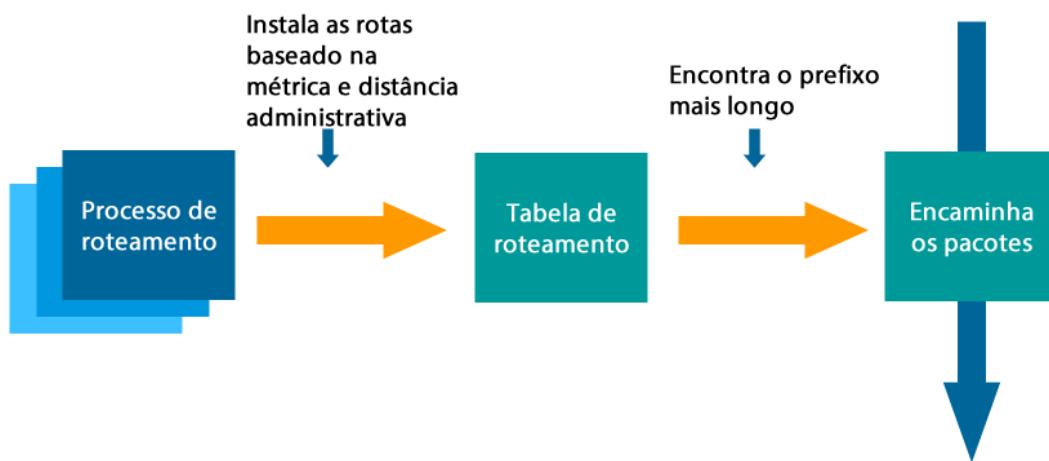
Quando temos uma topologia mais complexa o uso de protocolos de roteamento dinâmico é mais aconselhável, pois a inserção ou alteração dos elementos de rede são bem mais simples e repassadas automaticamente para os demais dispositivos pelo elemento que sofreu a alteração, portanto, o que você muda em um é repassado dinamicamente para todos os outros.

O funcionamento macro dos protocolos de roteamento é bem semelhante, pois eles são processos habilitados nos roteadores que coletam informações das suas redes diretamente conectadas e repassam essas informações aos outros roteadores. Com isso, um banco de dados é criado, analisado e através de um parâmetro de decisão chamado “**métrica**” a melhor rota é inserida na tabela de roteamento. Além disso, os protocolos de roteamento devem atuar sobre alterações na rede por motivos de problemas, tais como a queda de um link de uma operadora ou um dispositivo que saiu do ar por falta de energia elétrica. Nesses casos, a indisponibilidade daquelas redes deve ser refletida para todos os dispositivos.



Atualmente na Internet o protocolo de roteamento utilizado entre os sistemas autônomos é o BGP. Já nas Intranets utilizamos o RIP, OSPF ou IS-IS que são protocolos abertos, ou seja, funcionam entre fabricantes diferentes, e existe também um protocolo proprietário do fabricante Cisco que é muito famoso chamado EIGRP.

Para resumir o funcionamento geral dos protocolos de roteamento veja a figura 3 ao lado. Um ou mais processos de roteamento podem ser ativados em um roteador, sendo que eles irão trocar informações e escolher internamente suas melhores rotas para cada destino baseado em uma "métrica" padrão que depende de cada protocolo. Por exemplo, no RIP a melhor rota é a que tem menos saltos até o destino, já para o OSPF a melhor rota é a que tem menor custo (conta baseada no somatório da velocidade de cada link até o destino) sendo que a rota que tem a menor métrica (menor valor calculado) é considerada vencedora. Caso tenhamos apenas um protocolo de roteamento habilitado essa rota, a que tem a menor métrica, é instalada na tabela de roteamento.



Quando temos mais de um protocolo de roteamento, ou seja, várias fontes de entrada para uma mesma rota vinda de diferentes protocolos, a distância administrativa ou custo é utilizado como critério de desempate. Por exemplo, vamos supor que o RIP tem distância administrativa 120 e o OSPF 110 e ambos aprendem uma rota para a rede 192.168.0.0, qual delas o roteador instala na tabela de roteamento? Será a aprendida via OSPF porque ela tem menor distância administrativa.

Na tabela de roteamento podemos ter várias rotas parecidas com prefixos diferentes, por exemplo, uma rota para a rede 192.168.0.0 com o prefixo /16 apontando para a interface 1 e outra rota para a rede 192.168.0.0 com o prefixo /24 apontando para a interface 2. Se calcularmos os IPs que cada prefixo possui teremos que:

- Dentro do /16 temos os IPs de 192.168.0.0 até 192.168.255.255
- Dentro do /24 temos os IPs de 192.168.0.0 até 192.168.0.255

Note que a faixa de 0.0 até 0.255 está dentro das duas rotas, mas qual o roteador irá escolher quando um IP de destino for, por exemplo, 192.168.0.1?

Essa decisão sempre é tomada pelo prefixo mais longo, em inglês "longest prefix match", ou seja, quanto maior o prefixo maior é a probabilidade daquela faixa de IP ser encontrada naquela interface saída, por ele ser **mais específico**.

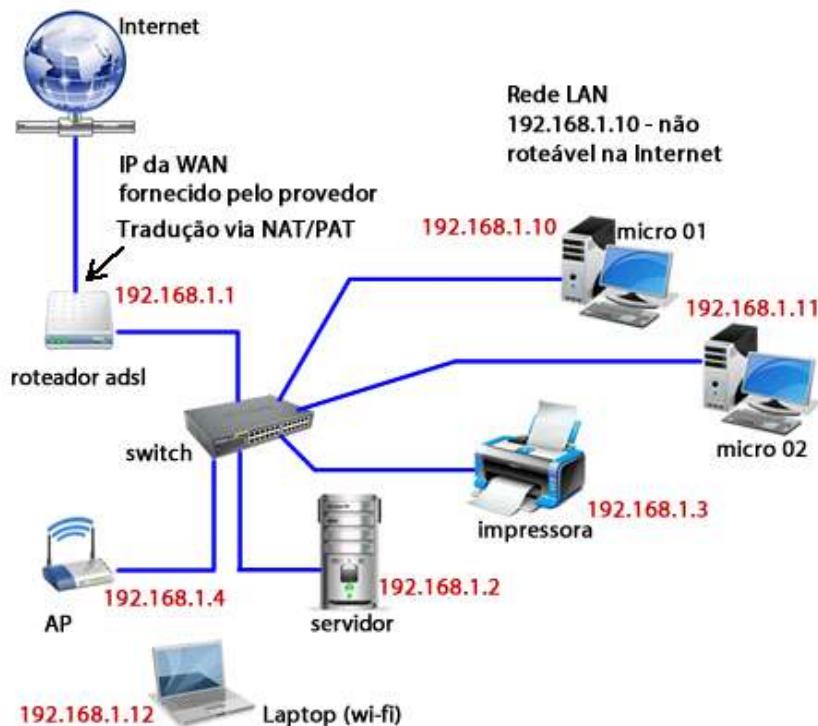
Portanto, no exemplo acima os pacotes serão enviados para a Interface 2! Em outras palavras para clarear as coisas, quando falamos em prefixo mais longo estamos falando de máscara de subrede, ou seja, a interface 2 tem uma máscara de subrede /24 que é mais longa que a /16

da interface 1. Isso quer dizer que a rede /24 será mais específica do que a /16, como temos menos hosts nessa subrede a probabilidade de se encontrar o host nessa rede será maior.

Para maiores detalhes sobre o roteamento IP e a configuração desses protocolos recomendamos o curso **CCNA Network** da DLteC, nele toda a teoria dos principais protocolos de roteamento é abordada, além disso, você poderá praticar em equipamentos ou simuladores de roteadores e switches Cisco, indo além da teoria e vendo como as coisas funcionam na prática.

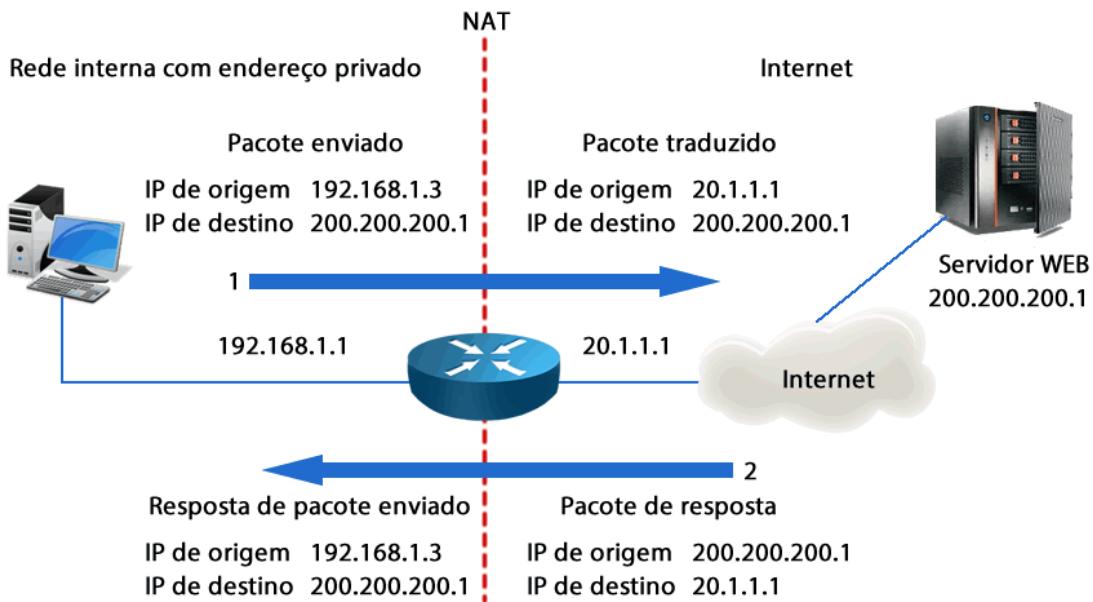
## 7 Acesso à Internet – Proxy e NAT

Quando estudamos anteriormente o projeto lógico de Redes IP foi citado que para acesso à Internet nossos micros precisariam de uma “**tradução**” do seu endereço IP interno, o qual normalmente pertence a uma faixa de IPs privativos, para um IP válido de Internet.



Essa tradução pode ser feita basicamente de três maneiras, através do NAT (Network Address Translation), PAT (Port Address Translation), também chamado de NAPT (Network Address and Port Translation), ou com o uso de um servidor Proxy.

O NAT faz apenas uma tradução direta de um IP interno para um IP externo, mantendo uma tabela que relaciona o host interno com o endereço IP externo utilizado na tradução, pois assim quando o pacote de retorno for enviado pelo host remoto o roteador poderá identificar para qual dos hosts internos enviar aquela informação. Veja a figura 2 ao lado onde o host com IP privativo 192.168.1.3 envia um pacote para o servidor que está na Internet com o IP 200.200.200.1.

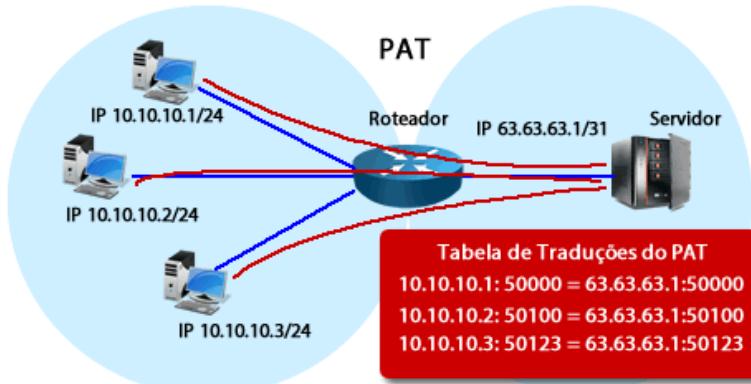


Note que quando o pacote com IP privativo chega no roteador que tem o NAT habilitado, há uma tradução do IP privativo por um IP público, o qual nesse exemplo é o 20.1.1.1. O roteador guarda em uma tabela essa tradução para que no passo 2, quando o servidor responder ao host, o pacote de resposta seja encaminhado para o host correto.

Mas com o NAT o que acontece se precisarmos de vários acessos simultâneos à Internet? Por exemplo, 500 micros tentando acessar vários serviços simultaneamente. Como a tradução é um para um, ou seja, para cada IP privativo preciso de um IP público seria quase a mesma coisa que termos os computadores com IPs válidos, pois precisaríamos de tantos IPs que não teríamos vantagem alguma.

Na realidade o NAT atualmente é mais utilizado para o acesso contrário, ou seja, permitir o acesso a um host interno a partir da Internet, processo chamado **NAT Reverso**. Com o NAT Reverso você configura um micro interno e quando um pacote chega para se conectar com o IP do roteador ele é automaticamente encaminhado para um computador interno, é como se colocássemos o IP válido do roteador na placa de rede do micro.

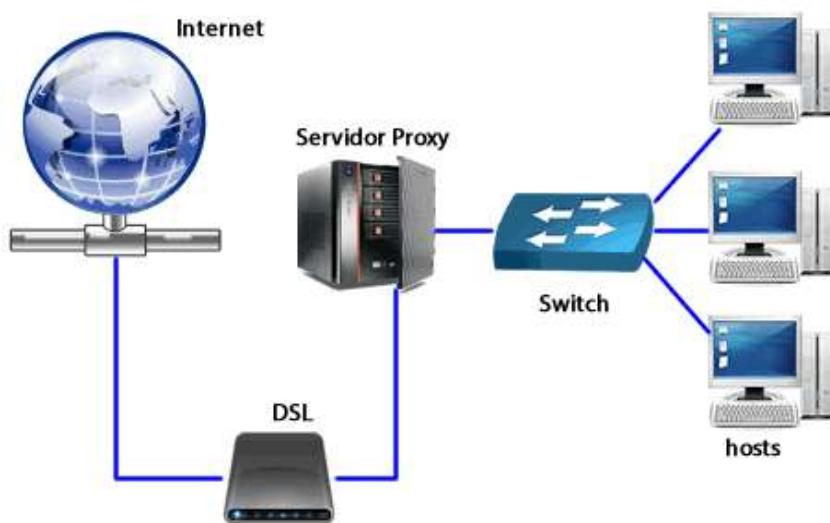
Na prática, para acesso à Internet os roteadores utilizam o PAT, o qual utiliza a tradução do endereço IP e também faz uso das portas TCP ou UDP para identificar as conexões. Portanto, cada IP válido tem a possibilidade de traduzir mais de 65000 conexões, ou seja, a quantidade de portas TCP e UDP disponíveis no cabeçalho de transporte.



Note que no caso do PAT o roteador possui apenas o IP 63.63.63.1 como válido e quando os três micros acessam ao servidor de WEB cada conexão é identificada pela porta TCP utilizada, por isso que com apenas um IP o PAT pode traduzir várias conexões simultâneas. Quando o servidor devolver suas respostas ele irá colocar o IP 63.63.63.1 como destino e a porta TCP 50000, isso significa que a resposta deve ser enviada ao host com IP 10.10.10.1. Por isso o nome é NAPT, ou seja, tradução utilizando o endereço de rede e a porta!

Na maioria dos equipamentos para uso residencial ou em empresas de pequeno porte o PAT já vem habilitado para facilitar a vida dos usuários e administradores de rede. Em redes maiores a ativação desse serviço pode ser uma tarefa um pouco mais complexa.

Outra opção que existe para as traduções e acesso à Internet são os servidores Proxy. A diferença básica entre o NAT/PAT e o servidor Proxy é que ele pode atuar entre as camadas de 4 a 7 do modelo OSI, portanto podemos validar, por exemplo, se um determinado usuário de rede pode acessar determinados serviços, web sites, conteúdos, determinar horários e tipos de acesso, etc.



Note que na topologia da figura 4 os dois serviços serão utilizados, pois o servidor de Proxy não está conectado diretamente à Internet. Você pode perguntar qual a vantagem dessa arquitetura se vou usar o NAT? A resposta é pelo controle adicional que você pode ter sobre o que os usuários irão ou não acessar na Internet. Como o NAT/PAT é puramente tradução, o máximo que você consegue limitar são os IPs que irão utilizar esse serviço. Já com Proxy, por atuar até a camada 7, você consegue inserir mais filtros, como por exemplo limitar acesso a determinadas páginas pelo nome ou pedaços de palavras, por exemplo, proibindo quaisquer páginas que iniciem com xxx ou hacker, portanto um Proxy pode aumentar o controle.

## 8 IPv6 – Introdução e Características

O protocolo IP versão 6 ou simplesmente IPv6 é a versão mais atual do Protocolo de Internet. Sua principal especificação encontra-se na RFC 2460.

Na data de 6 de junho de 2012, a Internet Society promoveu o **IPv6 World Launch**, o dia em que grandes provedores de Internet (ISPs), fabricantes de equipamentos de rede e empresas da Web ao redor do mundo habilitaram permanentemente o IPv6 em seus produtos e serviços.

Portanto, o IPv6 vem sendo implantado gradativamente na Internet e deve funcionar em conjunto com o IPv4 por um longo período. O termo técnico utilizado para essa convivência de ambos os protocolos em uma mesma interface é denominado "pilha dupla" ou "dual stack".

Em longo prazo, o IPv6 tem como objetivo substituir o IPv4, que só suporta aproximadamente 4 bilhões de endereços IP, ao passo que o IPv6 suporta aproximadamente  $3,4 \times 10^{38}$  endereços, sendo esse o principal motivo para a implantação do IPv6 na Internet: "a necessidade de mais endereços", pois os endereços livres IPv4 acabaram.

Uma das razões desse esgotamento é que a Internet não foi projetada para uso comercial, pois no início da década de 80 ela poderia ser considerada uma rede predominantemente acadêmica, com poucas centenas de computadores interligados. Com a criação da Internet pública e a explosão do uso dos serviços online e cada vez mais dispositivos com suporte ao protocolo IP sendo criados foi inevitável essa necessidade de uma atualização do protocolo IP.

Um endereço IPv6 é escrito não mais em decimal pontuado, como no IPv4, agora ele é escrito em oito conjuntos de quatro caracteres em hexadecimal separados por dois pontos. Como cada algarismo em hexa tem 4 bits temos 4 bits vezes 4 algarismos vezes 8 conjuntos, o que nos dá um endereço de 128 bits. Lembre-se que estamos falando em algarismos em hexadecimal, portanto, os algarismos que vamos encontrar em um endereço IPv6 serão de 0 a 9 e de A a F. Veja abaixo um exemplo de um endereço IPv6:

### **2001:0db8:85a3:08d3:1319:8a2e:0370:7344**

Um endereço padrão IPv6 deve ser formado por um campo provider ID, subscribe ID, subnet ID e node ID. O node ID (ou identificador de interface) deve ter 64bits, e pode ser formado a partir do endereço físico (MAC) no formato EUI 64. O que define a porção de rede e host de um endereço continua sendo o prefixo, como no CIDR do IPv4, porém agora o prefixo pode ir até /128.

Com o IPv6 todas as redes locais devem ter prefixos /64. Isso é necessário para o funcionamento da autoconfiguração e outras funcionalidades. Usuários de qualquer tipo receberão de seus provedores de Internet um /48, ou seja, terão a seu dispor uma quantidade suficiente de IPs para configurar aproximadamente **65 mil redes**. Alguns provedores cogitam entregar aos usuários domésticos redes com tamanho /56, permitindo sua divisão em apenas 256 redes /64.

Além disso, no Ipv6 não existe mais broadcast, temos ainda a comunicação Unicast (um para um), Multicast (um para um grupo) e agora um novo tipo que não existia no IPv4 chamado Anycast. O Anycast corresponde a múltiplas interfaces que partilham um prefixo comum, onde os dados são distribuídos "ao destino o mais próximo" ou "melhores" conforme definido pelo roteamento da rede.

Não se preocupe que ainda nesse curso voltaremos a falar com mais detalhes sobre o protocolo IPv6, aqui fizemos apenas uma introdução.

*Nesse capítulo estudaremos os principais conceitos relacionados à camada 2 referente às tecnologias e equipamentos que trabalham com conexões da família Ethernet (ethernet, fast ethernet e gigabit ethernet), ou seja, os switches.*

*Este é um assunto muito importante para quem deseja seguir na área de redes como profissional, pois em redes de todos os portes os switches desempenham uma função vital: "dar acesso aos usuários e também aos demais dispositivos de rede".*

*Aproveite bem esse capítulo e bons estudos!*

*Desejamos a todos bons estudos.*

## **Capítulo 06 - Switching e VLANs**

### **Objetivos do Capítulo**

Ao final desse capítulo você deverá ter estudado e aprendido os seguintes assuntos:

- Modelo de projeto em três camadas;
- As características e funcionamento de um switch;
- O que é e para que serve uma VLAN;
- A importância e funcionamento do protocolo Spanning-Tree;
- O que é uma agregação de link e empilhamento de switches;
- O funcionamento básico de um switch layer-3;
- As opções de switches e suas interfaces disponíveis no mercado.

## Sumário do Capítulo

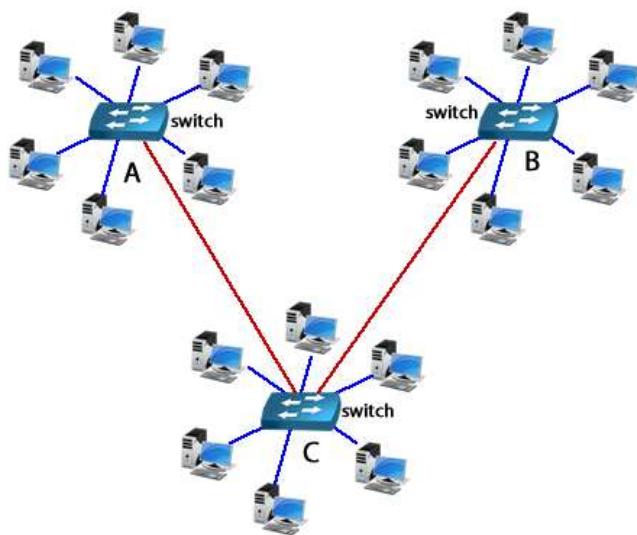
<b>1</b>	<b><i>Topologias de Redes LAN</i></b>	<b>183</b>
<b>2</b>	<b><i>Switches – Características e Funcionamento</i></b>	<b>187</b>
2.1	Aprendendo Endereços MAC	187
2.2	Filtragem de Quadros	191
2.3	Tipos de Switches – Encaminhamento	
	191	
2.4	Loops de Camada 2 e Redes Redundantes	193
2.5	Power Over Ethernet (PoE)	195
<b>3</b>	<b><i>VLAN – Redes Locais Virtuais</i></b>	<b>196</b>
3.1	Criando VLANs e Alocando Portas	199
3.2	VLAN Nativa e IP de Gerenciamento	200
3.3	Entroncando Switches via Protocolo 802.1Q	201
<b>4</b>	<b><i>Protocolo Spanning-Tree – STP, RSTP e MSTP</i></b>	<b>203</b>
<b>5</b>	<b><i>Recursos Avançados – Agregação de Links, Empilhamento e Espelhamento de Portas</i></b>	<b>205</b>
5.1	Agregação de Links	205
5.2	Empilhamento de Switches (Stacking)	
	206	
5.3	Espelhamento de Porta	207
<b>6</b>	<b><i>Outros Modelos de Switches (Camadas 3 a 7)</i></b>	<b>209</b>
<b>7</b>	<b><i>Modelos de Switches e suas Interfaces</i></b>	
	210	

## 1 Topologias de Redes LAN

Em uma rede LAN os switches desempenham papel fundamental servindo de ponto de entrada para que os demais dispositivos e terminais possam acessar os recursos de rede e compartilhar informações.

Para que essa comunicação flua de maneira adequada devemos, além de dimensionar a capacidade de portas e tráfego dos switches, definir uma topologia de rede adequada para acomodar os terminais e também interligar os demais dispositivos de rede.

Basicamente uma rede da família ethernet é chamada de “broadcast multiacesso”, ou seja, ela forma um domínio de broadcast onde vários dispositivos podem se comunicar ao mesmo tempo, pois é assim que uma LAN tradicional funciona. Lembre-se do que estudamos até agora sobre os HUBs, Bridges e Switches, onde eles formam um único domínio de broadcast e os hosts ligados a esses equipamentos podem se comunicar entre si. Veja a figura abaixo onde temos uma rede ethernet em estrela estendida interligando três switches e diversos hosts.



O projeto de uma rede LAN pode ser simples, assim como na figura mostrada acima, onde temos os switches interligados por apenas um link (cabô) e todos os computadores no mesmo domínio de broadcast.

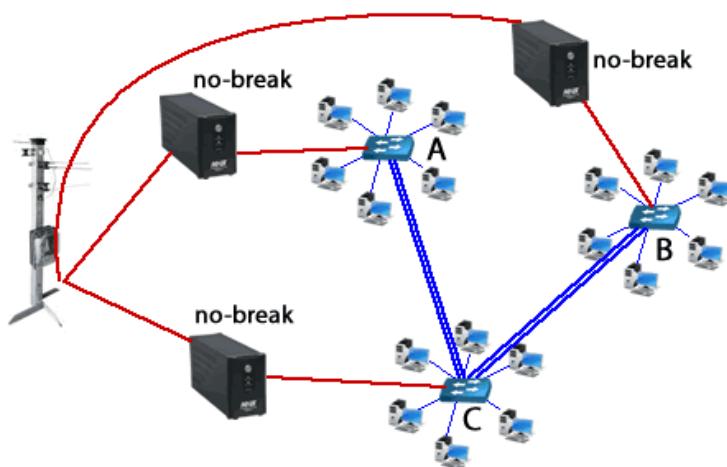
Porém, ao montar uma topologia de LAN ou até mesmo uma WAN em um ambiente corporativo devemos pensar nos seguintes pontos para o projeto:

- **Tolerância a falhas** – as redes devem prever redundância (física lógica e energia).
- **Escalabilidade** – propriedade de aumentar ou expandir a rede sem precisar construir uma nova rede, ou seja, simplesmente adicionando dispositivos.
- **Qualidade de Serviços (QoS)** – propriedade de suportar diversos tipos de tráfego priorizando cada um de acordo com suas características e necessidades. Por exemplo, pacotes de voz devem ter prioridade sobre pacotes de acesso à Internet via HTTP, pois a voz precisa de um fluxo em tempo real, enquanto o acesso web tolera melhor o atraso e perda de pacotes, portanto uma das funções do QoS é de tratar os diferentes tráfegos e priorizar os fluxos conforme suas necessidades de largura de banda, atraso e demais especificações de qualidade.

- **Segurança** – evitar ataques, invasões, espionagem industrial, destruição de dados, quebra de privacidade, etc.

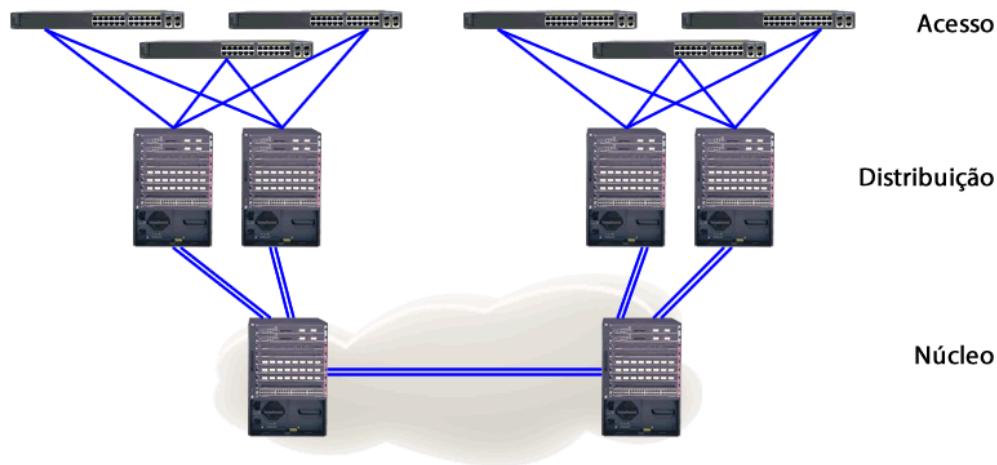
Voltando à figura anterior, o que irá ocorrer se o cabo entre os switches A e C for rompido ou desligado? Da maneira que está o switch A ficará isolado e somente os equipamentos entre B e C irão se comunicar. Outra possibilidade de problema é, por exemplo, o ponto de energia onde o switch C está conectado fica com problemas ou simplesmente a rede elétrica parou de fornecer energia para o switch C, o que irá ocorrer? Os hosts do switch C não irão mais ter comunicação com a rede, assim como os switches A e B ficarão isolados.

Os dois exemplos citados anteriormente podem ser resolvidos construindo uma rede redundante, sendo que para o problema de link basta conectar mais de um cabo e para o de energia basta ter uma fonte extra, tal como um No-break. Veja na figura seguinte um exemplo simples do complemento da rede da figura 1 com redundância, onde cada switch agora recebeu uma segunda conexão de backbone e estão conectados a um no-break para evitar problemas com relação à falta de energia elétrica.

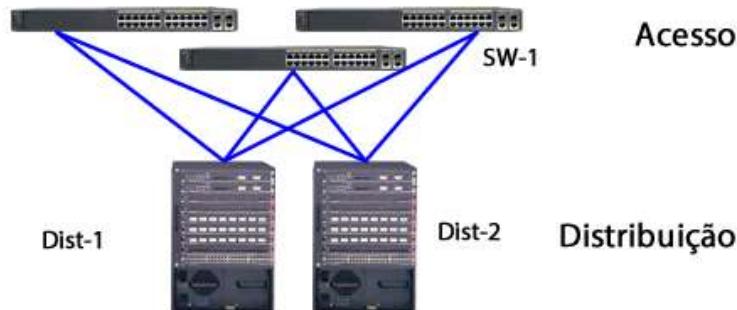


A topologia mostrada na figura acima, onde ligamos os switches em cascata (um conectado ao outro) através de dois cabos ainda é muito utilizada em empresas de pequeno porte, pois é uma topologia simples e relativamente segura pelo seu custo benefício.

Já em redes de médio e grande porte a topologia mais utilizada é a que segue o modelo de projeto em três camadas, onde a rede local é dividida em **Acesso** (Access), **Distribuição** (Distribution) e **Núcleo** (Core). Inclusive, a maioria dos fabricantes classificam seus switches de acordo com essa nomenclatura, ou seja, eles possuem linhas de produtos divididos entre Switches de Acesso, Switches de Distribuição e Switches de Core (Núcleo). Veja a figura seguinte com um exemplo de topologia em 3 camadas.



A camada de acesso, como o nome diz, dá acesso aos terminais, sejam eles computadores, telefones IP, Servidores, Impressoras e assim por diante. Normalmente nela temos switches layer 2 puros com capacidade de recursos tais como QoS, para dar início à marcação dos pacotes, PoE (Power over Ethernet) para alimentar telefones IP e Access Points, suporte a configuração de VLANs e empilhamento (stacking). Note que a conexão entre os switches de acesso e de distribuição é feita de maneira cruzada, ou seja, eles se conectam a dois switches de distribuição, pois isso garante redundância de link e também de equipamento, pois se um dos switches de distribuição ficar indisponível o outro permitirá a comunicação. Veja o detalhe na figura abaixo. Note que o switch de acesso SW-1 tem um link com o switch de distribuição Dist-1 e uma segunda porta conectada ao Dist-2.



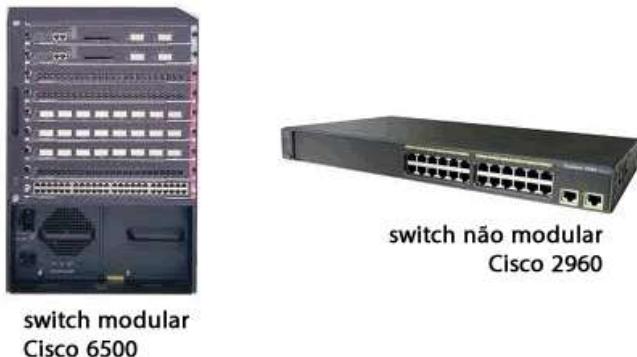
Já os switches de distribuição normalmente suportam recursos de camada 3, ou seja, são switches layer 3, e tem a função de servir como gateway para os switches de acesso. A camada de distribuição também garante a redundância para os switches de acesso, assim como evita possíveis problemas de rede na camada de acesso, pois ela provê o acesso à camada de núcleo normalmente com links layer 3 (como se fossem roteadores). Outras funções que podem ser inseridas nos switches de distribuição é aplicação de regras de filtragem para implementar segurança entre as redes.

Por exemplo, em uma escola onde você pode ter uma rede corporativa ou administrativa em conjunto com uma rede educacional (onde os alunos têm acesso), nos switches de distribuição o administrador de redes pode implementar regras onde os alunos podem somente acessar à Internet, prevenindo invasões ou acessos indesejados à rede corporativa da escola.

Já a camada de núcleo é dedicada à comutação dos pacotes entre os diversos equipamentos de distribuição, fornecendo um encaminhamento de pacotes o mais rápido possível e normalmente trabalhando interligada com velocidades altas, por exemplo, links de 10 Gbps.

Note na figura anterior que na conexão entre a camada de distribuição e núcleo, assim como entre os dispositivos da camada central (núcleo), temos pelo menos dois links entre os equipamentos, garantindo também a redundância de circuito.

Mais tarde você verá que o que difere os equipamentos de acesso, distribuição e central é o porte do equipamento. Normalmente os equipamentos de acesso são mais simples, montados em uma "caixa", ou seja, uma placa mãe (backplane) que já vem conectada às portas. Já os equipamentos de distribuição e core são compostos de um chassi e precisam ser equipados com diversas placas, pois o chassi é apenas um gabinete metálico com um circuito que permite a conexão dos diversos módulos que compõe o switch.



Mas então qual topologia devemos utilizar? Não existe uma recomendação fixa para isso, pois cada empresa tem uma necessidade e um porte. Como já citado, se sua empresa é pequena e possui poucos switches uma topologia em cascata pode ser uma boa solução. Porém, mesmo sendo pequena, se você deseja uma garantia que o serviço esteja sempre disponível para os usuários a topologia em três camadas já é a mais recomendada. Já para empresas de médio e grande porte a topologia em três camadas é a mais recomendada sem sombra de dúvidas.

## 2 Switches – Características e Funcionamento

Os switches são dispositivos de camada 2, ou seja, atuam na camada de enlace do modelo OSI, e sua principal característica é a de utilizar os endereços de camada 2 do padrão ethernet (o endereço MAC) para tomar suas decisões de encaminhamento entre as portas.



Basicamente um switch tem três funções principais para executar:

- Aprender endereços MAC
- Encaminhar ou filtrar os quadros recebidos
- Evitar loops (protocolo spanning-tree)

Vamos a seguir ver cada um desses processos.

Normalmente um switch também pode ser gerenciável ou não. Em um switch não gerenciável você conecta os computadores nele e nada mais, pois ele não possui uma interface de gerenciamento que permita que você o acesse para fazer configurações adicionais ou por motivos de manutenção. Já os switches gerenciáveis, mesmo sendo layer 2, possuem a capacidade da configuração de um IP de gerenciamento para acesso remoto via Web, Telnet ou SSH, sendo que alguns modelos também possuem uma interface local via RS-232 (porta serial) para realização de uma configuração inicial ou em caso do acesso remoto ser perdido por qualquer motivo.

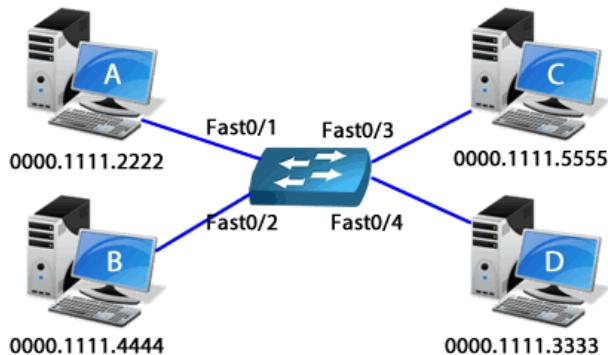
### 2.1 Aprendendo Endereços MAC

Um switch deve aprender os endereços MAC dos computadores conectados às suas portas e montar uma tabela de encaminhamento, possibilitando a criação de diversos caminhos virtuais livres de colisão entre esses computadores.

Veja a figura a seguir, onde temos os computadores A, B, C e D conectados às portas fast 0/1 até a fast 0/4 respectivamente a um switch. Ao longo do tempo, com a comunicação entre os computadores, o switch aprende através dos **endereços MAC de origem** enviados pelos computadores, o MAC de cada um deles e vincula esse MAC com a porta que recebeu esse quadro ethernet.

Tabela de endereços MAC

Porta	MAC
Fast 0/1	0000.1111.2222
Fast 0/2	0000.1111.4444
Fast 0/3	0000.1111.5555
Fast 0/4	0000.1111.3333



Na próxima figura temos o quadro ethernet para você relembrar dos campos que o switch utiliza para o aprendizado de endereços (MAC de origem), para o encaminhamento dos quadros (MAC destino) e verificação de erros.

Protocolo Ethernet (Quadro)

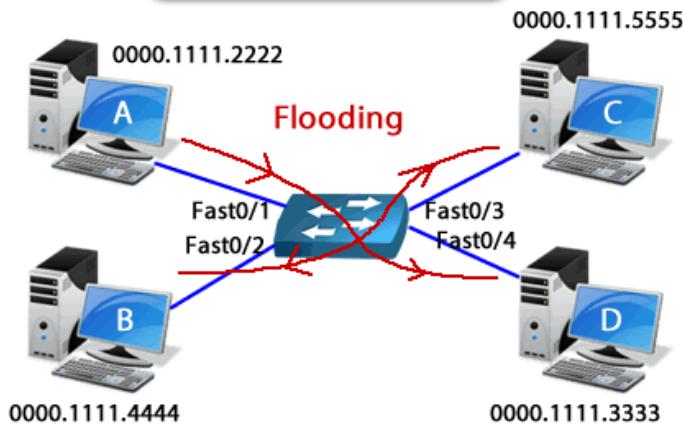
Preâmbulo	Endereço de Destino	Endereço de Origem	Tipo	Dados	Sequência de Verificação do Quadro
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

Até o momento supomos que o switch já conhecesse todos os MACs conectados às suas portas. Mas o que acontece se o switch não conhecer ainda todos os MACs que estão conectados às suas portas e um computador enviar um quadro para esse MAC desconhecido? Como o switch não sabe para onde enviar ele envia uma cópia desse quadro para todas as suas portas, menos para àquela que enviou o quadro. Assim, com certeza o computador de destino irá receber esse quadro e responder a essa requisição. Quando isso ocorrer o switch irá inserir uma nova entrada em sua tabela de endereços MAC, adicionando em sua tabela uma entrada com o endereço do micro que antes era desconhecido e que agora passa a ser conhecido. Lembre-se que esse processo é chamado de flooding.

Acompanhe na figura seguinte uma ilustração do processo de flooding onde o computador A envia um quadro para o computador C, o qual ainda não era conhecido pelo switch. Note que quando o switch recebe esse quadro ele constata que não conhece aquele MAC e envia uma cópia do quadro para todas as portas (flooding), menos para a porta do computador A.

Tabela de endereços MAC

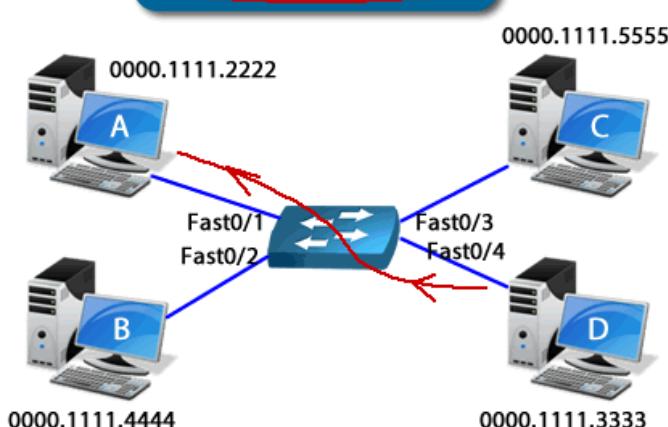
Porta	MAC
Fast 0/1	0000.1111.2222
Fast 0/2	0000.1111.4444
Fast 0/3	?
Fast 0/4	



Quando o computador C recebe o quadro ele responde e o switch vincula seu MAC de origem com a porta fast 0/3. Apesar dos computadores B e D receberem o mesmo quadro eles compararam internamente o MAC de destino com seus MACs gravados na placa de rede e verificam que aquele quadro não é para eles, portanto o quadro é descartado por B e D.

Tabela de endereços MAC

Porta	MAC
Fast 0/1	0000.1111.2222
Fast 0/2	0000.1111.4444
Fast 0/3	0000.1111.5555
Fast 0/4	0000.1111.3333



Não confunda o flooding com o ARP, o ARP é uma ferramenta de camada 3 e utilizada para descobrir um MAC que está vinculado a um endereço IP que é conhecido. Aqui no flooding não entramos na camada 3, pois o switch faz somente uma cópia simples do quadro para todas as portas. O flooding pode ser traduzido para o português por algumas bibliografias como "inundação de quadros".

Com isso aprendemos como os switches aprendem endereços MAC e fazem o encaminhamento dos quadros de Unicast, ou seja, comunicação direta entre dois dispositivos. Mas e se um computador enviar um quadro com um endereço de broadcast como destino? Ou seja, com o endereço MAC ffff.ffff.ffff no campo de MAC de destino do quadro ethernet? Lembrem-se do que já foi citado em capítulos anteriores, um switch é um dispositivo de camada 2, por isso ele irá encaminhar o broadcast para todas as portas menos para a porta de onde ele recebeu o quadro. Por exemplo, considerando a figura 4 se o micro A envia um broadcast que portas irão receber esse quadro? Serão as portas fast 0/2, fast 0/3 e fast 0/4. Portanto o switch consegue segmentar domínios de colisão, porém não segmenta domínios de broadcast.

Podemos também dizer que os pacotes com MAC de destino apontando para um endereço de broadcast passam por um processo idêntico ao de flooding, pois o switch inunda todas as portas com esse quadro. O mesmo ocorre com um quadro de Multicast, ou seja, os quadros de comunicações multicast recebem um endereço MAC especial iniciado em **0100.5E** (com uma faixa de 0100.5e00.0000 até 0100.5e7f.ffff) e são encaminhados para todas as portas do switch, menos para a porta que enviou o quadro, assim como o broadcast. Os endereços de broadcast e multicast não são guardados na tabela de endereços MAC do switch, eles sempre são tratados como endereços não conhecidos e sofrem o processo de flooding.

Vale a pena também ressaltar que os quadros aprendidos pelos switches também recebem um "time stamp", ou seja, uma etiqueta de tempo, pois se o computador for desconectado da porta ou ficar muito tempo sem se comunicar, a entrada da tabela de endereços MAC deve ser apagada para liberar espaço da memória. Todos os switches tem um limite de endereços MAC que podem ser aprendidos, além disso, manter um MAC aprendido sem apagá-lo pode criar entradas erradas, por exemplo, você troca a placa de rede de um micro que está conectada a uma porta de um switch, se ele não apagasse a entrada após um tempo você acumularia dois MACs naquela porta, mas na realidade somente um é válido. Esse tempo é chamado "aging time" ou tempo de envelhecimento do MAC. A maioria dos fabricantes utilizam 300 segundos como aging time padrão das interfaces.

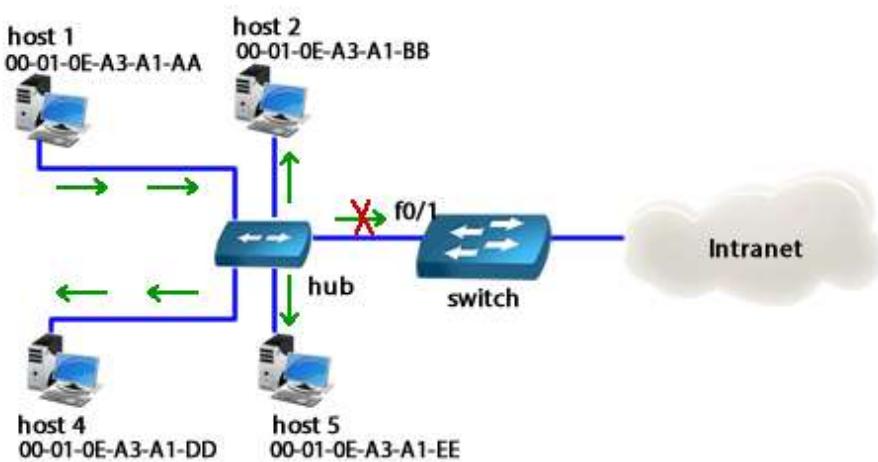
Além disso, se o switch suporta VLANs a tabela de endereços MAC guarda também a que VLAN aquele MAC pertence, portanto a tabela MAC irá manter por porta os seguintes itens:

- Número da porta
- MAC ou MACs de origem aprendidos
- A quanto tempo ele foi aprendido (contador do aging time)
- A VLAN que a porta está vinculada

O conceito de VLAN veremos em um tópico posterior ainda nesse capítulo.

## 2.2 Filtragem de Quadros

A filtragem dos quadros ocorre quando um switch tem mais de um endereço MAC vinculado à mesma porta, por exemplo, quando temos um HUB conectado a uma porta e dois micros conectados a esse HUB. Quando esses dois micros que estão conectados no HUB se comunicam os quadros trocados entre eles não precisam ser enviados para as demais portas do switch, portanto o switch “filtra” essa comunicação mantendo ela restrita ao HUB. Veja a figura abaixo onde o Host1 está se comunicando com o Host4 que está conectado ao mesmo HUB.



Na tabela de endereços MAC do switch os endereços MAC dos Hosts1, 2, 4 e 5 estarão vinculados à mesma porta do switch, ou seja, à porta fast 0/1. Porém, se o switch não tiver vinculado ainda o MAC do Host4 à porta fast 0/1 ele fará o flooding normalmente, como mostrado no tópico anterior.

## 2.3 Tipos de Switches – Encaminhamento

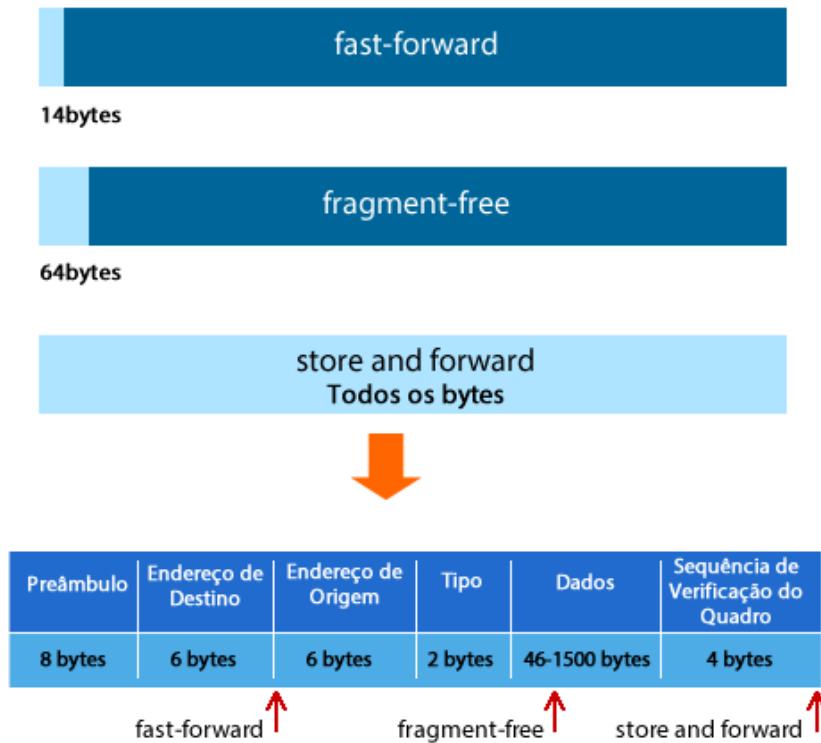
Após o processo de aprendizagem, a maneira que o switch irá encaminhar os quadros pode ser realizada de três formas diferentes, através do “armazena e encaminha”, fast-forward (encaminhamento rápido) e fragment-free (livre de fragmentos).

Essas três formas de encaminhar foram criadas para se adequarem à realidade de cada rede e seus dispositivos. A primeira delas que surgiu foi a “armazena e encaminha”, em inglês “store and forward”, com as bridges. Como as bridges estavam em um ambiente de HUBs, onde as colisões eram frequentes e o “lixo” na rede provocado por elas era muito grande, esse método de encaminhamento fazia a leitura de todo o quadro e a avaliação do FCS, pois nesse campo é onde verificamos os erros, para aí sim encaminhar apenas os quadros íntegros, ou seja, sem erro no FCS.

Com a entrada dos switches nas redes elas se tornaram mais confiáveis, portanto um método mais rápido poderia ser criado para o encaminhamento dos quadros. Com isso surge o Fragment-free, ou seja, um encaminhamento que garante apenas que está encaminhando quadros que não são fragmentos de colisões, pois ainda existe HUBs na rede. Esse método se baseia em que estatisticamente as colisões acontecem até o byte 64 dos quadros ethernet, portanto para encaminhar o switch precisa ler até o byte 64 apenas e não precisa mais verificar o FCS, o que acelerou bastante o encaminhamento.

Nos dias atuais, com as redes sendo implantadas 100% com switches um novo método de encaminhamento pode ser utilizado, chamado fast-forward, ou seja, um encaminhamento rápido em que o switch lê apenas o MAC de destino e já faz o encaminhamento, pois uma vez que a rede não tem mais HUBs não haverão fragmentos de colisão!

Os métodos fragment-free e fast-forward são considerados dois tipos de encaminhamento “**cut-through**”. Veja a figura abaixo com uma relação do quadro ethernet e até onde cada método precisa ler para fazer o encaminhamento.



Na maioria dos fabricantes da atualidade o cut-through do tipo fast-forward é o padrão estabelecido para encaminhamento dos quadros pelos switches.

## 2.4 Loops de Camada 2 e Redes Redundantes

Ao criar caminhos redundantes entre switches estamos criando também loops de camada 2. Um loop é um caminho onde o mesmo quadro pode ficar circulando indefinidamente por ele, sendo copiado e enviado entre as portas gerando consumo de banda desnecessária e outros problemas. Porém, os caminhos redundantes são desejáveis e até recomendados para uma rede de camada 2. Logo, os switches devem ser capazes de tratar esse problema e isso normalmente é feito com a utilização do protocolo chamado **spanning-tree** ou **STP**, o qual estudaremos com mais detalhes posteriormente.

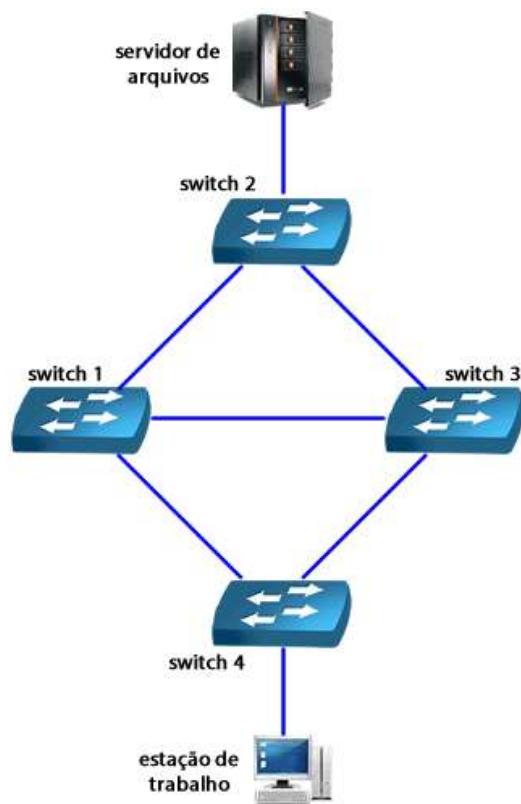
Vamos aqui nesse tópico analisar quais problemas os loops de camada 2 podem gerar em uma rede comutada por switches, os quais são:

- Múltiplas transmissões de quadros
- Instabilidade em bancos de dados e
- Tempestades de broadcast (broadcast storm)

Analise a topologia da figura seguinte. Suponha que um quadro originado pela Workstation é enviado ao "File Server" (servidor de arquivos), note que esse quadro vai chegar primeiro no Switch 4. Ao receber o quadro, o Switch 4 irá analisar sua tabela de endereços MAC e suponha que ele não conhece o MAC do "File Server" (o servidor está em outro switch e provavelmente é o que acontecerá na prática), portanto ele irá encaminhar o quadro para todas as portas, com exceção da porta de origem.

Agora ambos, Switch 1 e Switch 3, receberão o quadro. Como o file Server também não está diretamente conectado à esses switches vamos supor que eles não irão conhecer o MAC de destino e também farão o flooding do quadro para todas as suas portas, com exceção da porta que eles receberam o quadro. Isso vai causar o envio do quadro novamente para o Switch 4 via o link Switch 1 – Switch 3 – Switch 4 ou Switch 3 – Switch 1 – Switch 4. Com isso teremos um loop de camada 2 e o quadro irá circular indefinidamente por essas interfaces.

Este é o processo que leva ao File Server provavelmente receber várias cópias do mesmo quadro por caminhos diferentes, o que traz uma sobrecarga na rede e no processamento do servidor. Além disso, se ao invés de um servidor de arquivos tivéssemos um servidor de banco de dados você poderia causar uma instabilidade nesse banco de dados, pois ele receberia várias entradas iguais através dessas diversas cópias que seriam enviadas devido ao loop de camada 2.



A tempestade de broadcast tem o mesmo princípio, porém ela tem um efeito muito mais nocivo à rede, pois um broadcast é processado por todos os hosts que o recebem e esses pacotes são multiplicados até uma degradação séria da performance da rede.

Os resultados dessa tempestade de broadcasts, seja por um loop ou outros motivos, são terríveis, como por exemplo, a parada total da rede com todos os servidores tendendo a 100% de CPU utilizada. E como qualquer estação pode gerar broadcasts, esse problema pode acabar sendo muito difícil de se localizar.

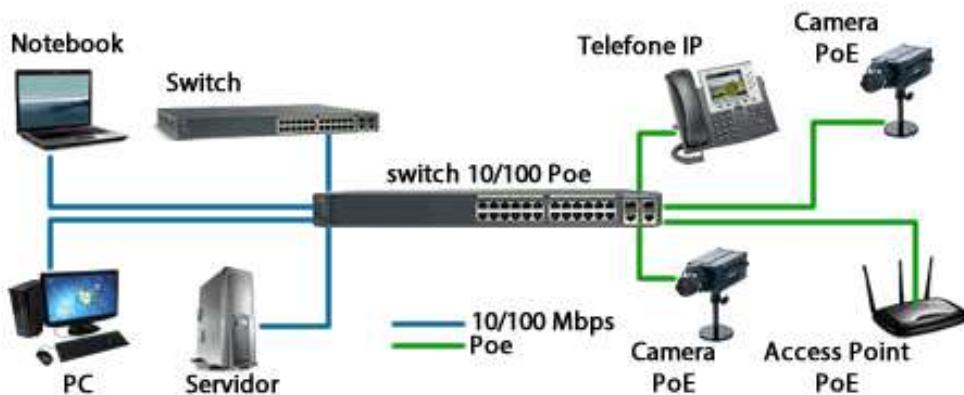
Na prática devemos habilitar um protocolo que permita os caminhos redundantes, porém livres de loop. O nome desse protocolo é Spanning-tree, ele envia quadros chamados BPDU para calcular um caminho livre de loops na rede comutada por switches.

## 2.5 Power Over Ethernet (PoE)

O PoE é uma tecnologia que possibilita o envio da alimentação pelo mesmo cabo que utilizamos para trafegar os dados. O envio da alimentação pode ser tanto pelos mesmos pares utilizados para trafegar os dados (conhecida como tipo A) ou pelos pares de fios livres (conhecida como tipo B).

PADRÃO	PINAGEM								OBS	
	Conector Ethernet RJ-45 connector									
	1	2	3	4	5	6	7	8		
IEEE 802.3af utilizando pares de dados	RX DC+	RX DC+	TX DC-	livre	livre	TX DC-	livre	livre	Industry Standard for Embedded POE (utilizado pelos Switches Cisco Catalyst)	
IEEE 802.3af utilizando pares livres	RX	RX	TX	DC+	DC+	TX	DC-	DC-	Padrão Industrial para Alimentação PoE	

Hoje em dia, muitos dispositivos de redes já suportam a alimentação PoE, como por exemplo, telefones IP, access points, câmeras de vídeo para segurança e por aí vai. Veja a figura 1 ao lado.



Agora imagine as vantagens obtidas através dessa tecnologia de alimentação! Utilizamos o mesmo cabo de rede para passar tanto os dados, quanto a alimentação necessária para manter funcionando um telefone IP ou para alimentar um Access Point, sem precisar a infraestrutura local de cabos de eletricidade e tomada para alimentar esses aparelhos. Fica fácil perceber algumas vantagens:

- Fonte de alimentação centralizada (no caso o switch PoE)
- Possibilidade de alimentar dispositivos que estão distantes da tomada (câmeras de vigilância ou access point, por exemplo)
- Eliminação do emaranhado de fios na sua mesa de trabalho (realmente isso é algo que incomoda)

É importante ressaltar que o PoE se tornou um padrão oficial em 2003 com o 802.3af. No entanto, nessa época já havia muitos fabricantes desenvolvendo equipamentos PoE e utilizando seus próprios métodos, dentre os quais temos o Cisco Inline Power.

Outro ponto que não podemos esquecer é que recentemente o IEEE criou o padrão PoE 802.3at, chamado de PoE Plus, cujo objetivo foi aumentar a potência utilizada de 15.4W para 25.5W.

Outro detalhe é que os switches PoE podem suportar um determinado número de dispositivos dependendo do consumo de energia total suportado por ele, porém é importante saber que alguns switches suportam apenas algumas portas com PoE, portanto em um projeto é bom prestar atenção nesses detalhes para fazer a escolha do modelo correto.

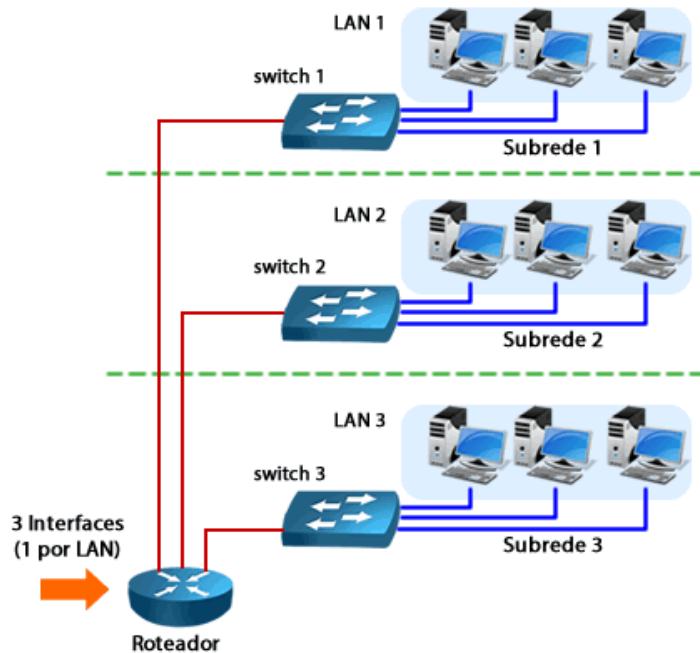
### **3 VLAN – Redes Locais Virtuais**

Como já estudamos os switches fazem a divisão ou segmentação dos domínios de colisão, pois cada porta do switch é um domínio de colisão. Também já vimos que eles não dividem domínios de broadcast, pois são os roteadores que tem essa capacidade. Mas vamos imaginar uma rede de grande porte, por exemplo, uma LAN com 1000 computadores ligados a uma rede de switches de 48 portas. Se dividirmos 1000 por 48 vamos chegar à conclusão que precisaremos de mais de 21 switches, pois ainda temos que pensar em conectar uns aos outros. Mas será que a performance dessa rede com 1000 computadores trocando informações na mesma subrede será razoável?

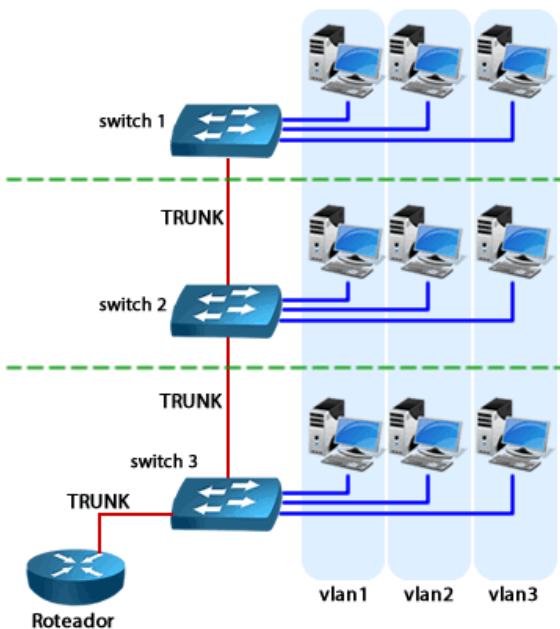
Em uma rede baseada em IPv4 temos muitos pacotes de broadcast sendo enviados devido ao ARP e muitos dos protocolos utilizarem o broadcast, por exemplo o DHCP, onde o cliente envia a solicitação em broadcast. Portanto, o ideal seria dividirmos essa rede em vários domínios de broadcast, assim poderíamos ter os computadores divididos por setor, andar, função dos usuários ou da maneira que for melhor para sua administração.



Se utilizarmos roteadores para fazer essa divisão precisaremos de uma interface de LAN para cada subrede a ser criada, o que faria com que o projeto ficasse com um custo muito elevado, pois o custo por porta de um roteador é muito mais elevado quando comparamos com um switch. Veja a figura seguinte onde queremos ter 3 domínios de broadcast, ou seja, dividir a LAN em três subredes, uma por andar. Para isso precisaríamos de um roteador com três interfaces, uma para cada subrede (uma subrede é o mesmo que um domínio de broadcast).



É aí que entram em cena as VLANs ou “LANs Virtuais” que permitem você alocar portas em um domínio de broadcast e segregar a comunicação entre essas “LANs Virtuais”. O recurso de VLAN é uma facilidade que a maioria dos switches layer 2 e 3 possuem. Veja a mesma topologia agora feita com switches que suportam VLAN.



Note na figura anterior que além de segregar os domínios de broadcast de uma maneira mais simples, o uso de VLANs permite que o administrador de redes estenda as VLANs entre os switches, possibilitando uma alocação flexível das portas. Para que seja possível a interligação dos switches entre eles ou com outros dispositivos existe o protocolo chamado 802.1Q. Esse protocolo permite o entroncamento entre os diversos switches e o compartilhamento das informações de VLAN entre os switches ou entre um switch e um roteador ou servidor com placa de rede que tenha suporte ao 802.1Q. Esses links que interligam os switches com o 802.1Q são chamados de "trunks" ou troncos e formam o backbone da rede (espinha dorsal) servindo como links de infraestrutura.

Nós vamos estudar posteriormente que os trunks ou troncos com o protocolo 802.1Q conseguem trafegar informações de todas as VLANs por um único link "**marcando**" os quadros com um identificador (VLAN ID). Essa marcação é chamada de "**tag**" e o processo de "**frame tagging**". Portanto, um trunk não utiliza o quadro padrão ethernet, pois ele insere um "tag" com informações relativas à VLAN que o quadro pertence.

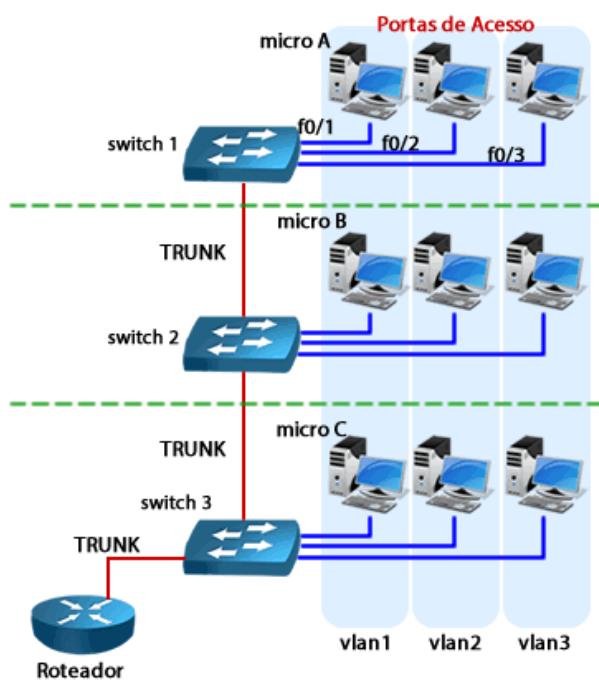
Além das vantagens de segregar a rede em diversos domínios de broadcast e melhorar a performance em termos de tráfego, as VLANs também ajudam a melhorar a segurança da rede, pois ela permite que você crie regras entre as diversas subredes, permitindo ou bloqueando acesso a determinados serviços ou IPs.

### 3.1 Criando VLANs e Alocando Portas

No capítulo anterior estudamos que uma VLAN possibilita dividirmos as portas dos switches layer 2 ou 3 em domínios de broadcast, mas na prática o que isso significa? Como isso é feito nos switches?

O processo de adição de VLANs e alocação das portas nas VLANs são bem semelhantes em todos os fabricantes. Basicamente você precisa criar a VLAN, que nada mais é que definir os VLAN-IDs que você vai utilizar, e depois entrar via sistema de gerenciamento nas portas do switch e vinculá-las a um dos VLAN-IDs criados.

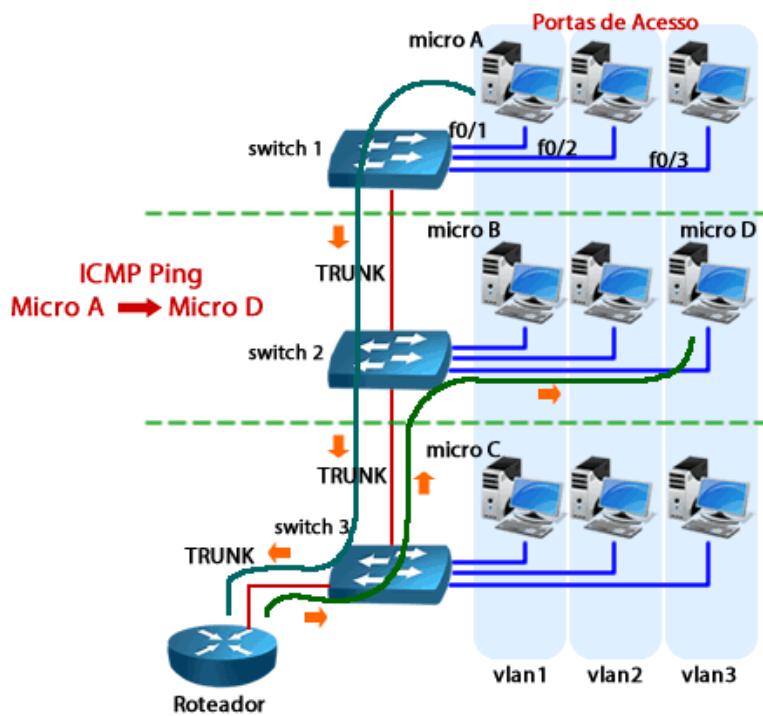
Veja o exemplo na figura seguinte, note que em todos os switches deveriam ser criadas as VLANs com IDs 1, 2 e 3. No Switch 3 teríamos que entrar no sistema de gerenciamento e definir que a porta Fast 0/1 pertence à VLAN1, a porta Fast 0/2 pertence à VLAN2 e a Fast 0/3 pertence à VLAN3.



Agora a regra de encaminhamento de quadros de broadcast no switch muda com relação ao que estudamos no capítulo anterior, pois quando o computador que está na Fast 0/1 enviar um broadcast somente as portas alocadas na VLAN1 receberão esse quadro. Além disso, o trunk também recebe uma cópia desse quadro para poder encaminhar aos demais switches interligados, pois a VLAN pode ser estendida pela rede de switches e esse quadro pode ter importância para um equipamento que está nos switches 1 ou 2. Portanto, analisando a figura 1 chegamos à conclusão que os hosts "Micro B" e "Micro C", que estão conectados aos switches 1 e 2 e pertencem à VLAN 1, também receberão esse quadro enviado pelo "Micro A" através dos links de trunk.

Lembre-se que nesse caso temos três domínios de broadcast e portanto precisamos de três subredes IP, uma para cada VLAN criada. Os switches de layer 2 não conseguem encaminhar quadros entre as VLANs, por exemplo, suponha que o Micro A, que está na VLAN 1 tem o IP 192.168.1.10/24 e quer se comunicar com um micro que está na VLAN 3 com o IP 192.168.2.10/24. Nesse caso os switches precisarão do apoio de um equipamento de camada 3, por exemplo, um roteador ou switch camada 3, para executar o roteamento entre essas duas VLANs. Considerando nossa topologia, esse pacote chegaria até o roteador via os links de trunk e seria roteado entre as duas VLANs, ou seja, o roteador faria o encaminhamento entre as duas

subredes IP. Veja a figura abaixo. Esse processo é conhecido como “roteamento entre VLANs” e pode ser executado tanto por um roteador como por um switch de layer 3.



### 3.2 VLAN Nativa e IP de Gerenciamento

Normalmente um switch que tem o recurso de VLAN, ou seja, suporta a criação de VLANs, já vem com todas as portas alocadas em uma VLAN chamada “**VLAN Nativa**”, a qual normalmente tem o identificador (VLAN ID) “1”.

Portanto, todas as portas do switch sem configuração, ou seja, com a configuração de fábrica, estão vinculadas a VLAN Nativa, a qual tem duas propriedades especiais:

1. É utilizada para configurar o IP de gerenciamento do switch e
2. Não possui marcação do quadro quando passa por um trunk (seus quadros passam sem marcação, o que chamamos em inglês de “untagged”).

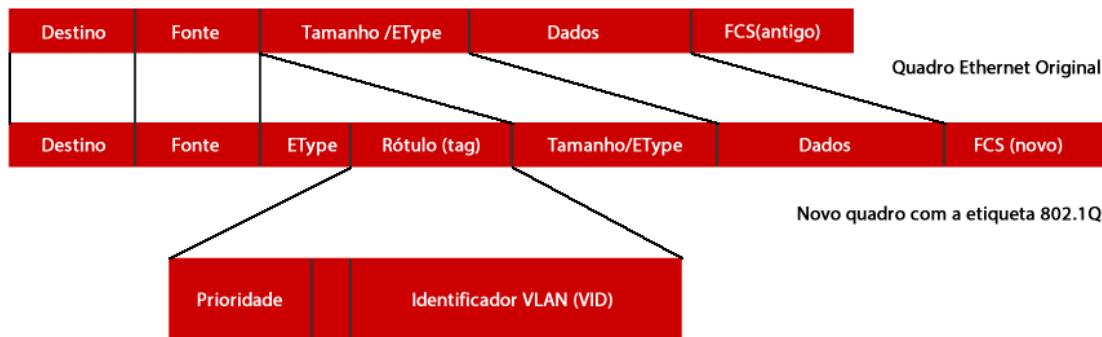
Com essas propriedades um switch sem configuração pode ser desembalado e já colocado em produção em um pequeno escritório que não necessite do recurso de VLANs.

Uma recomendação de segurança dada por muitos fabricantes é não utilizar a VLAN nativa padrão que vem configurada nos switches, como a VLAN1 para o fabricante Cisco, e configurar outra VLAN como nativa e de gerenciamento. Isso porque qualquer hacker ou atacante já tem pleno conhecimento da fragilidade da VLAN1 e de como efetuar um ataque usando esse VLAN-ID para invadir um switch.

### 3.3 Entroncando Switches via Protocolo 802.1Q

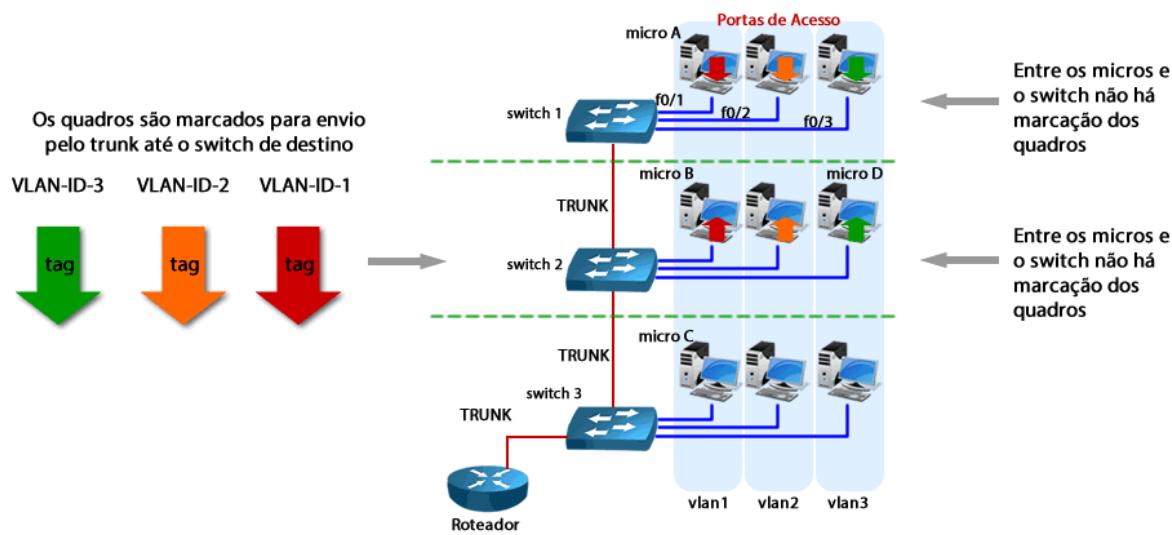
Conforme já vimos somente as portas que estão na mesma VLAN ou com o mesmo VLAN-ID podem se comunicar e todas as portas que estão em VLANs distintas não se comunicam entre si. Logo, faz necessário uma forma de transmitir todas ao mesmo tempo para que um equipamento de camada 3 faça essa comunicação entre elas via roteamento.

É isso que os trunks com o protocolo 802.1Q fazem. Um trunk 802.1Q é um link reservado para a comunicação entre switches ou quaisquer outros equipamentos que precisam receber a informação de várias VLANs ao mesmo tempo. O 802.1Q faz isso marcando os quadros antes deles saírem do switch de origem para o destino, ou seja, cada quadro recebe uma "etiqueta" (chamado também de tag, marcação ou rótulo) com sua VLAN, pois assim, quando o switch de destino receber os quadros ele pode ler essa marcação e distribuir os quadros para as portas corretas (para as VLANs corretas). Veja o quadro do 802.1Q na figura abaixo.



Note ainda na figura acima que o campo do FCS que faz a verificação de erros via CRC (check de redundância cíclica) é recalculado após a colocação da etiqueta do 802.1Q, pois como o tamanho do quadro varia, ou seja, novos bits são inseridos, o cálculo do FCS deve ser refeito antes do envio.

Portanto, quando um computador envia quadros de broadcast, flooding ou para micros com MAC de destino que não pertencem ao switch de origem, o switch enviará os quadros também pelo entroncamento (trunk) e marcará cada um deles com o rótulo 802.1Q (etiqueta ou tag) para que no destino esses quadros sejam encaminhados para as portas corretas. O switch de destino ao receber esses quadros marcados em seu link de trunk retira o rótulo antes de enviar o quadro para o computador de destino, isso porque o computador de destino está esperando um quadro padrão ethernet e não entenderia o quadro 802.1Q.



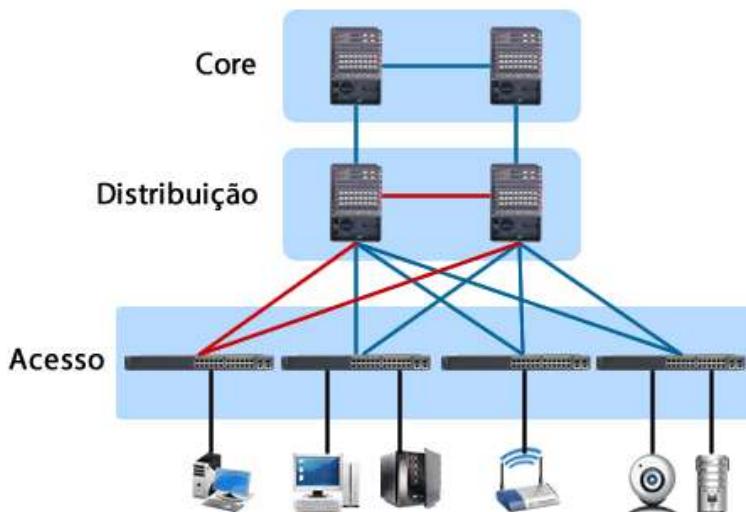
Lembre-se que nos switches que suportam VLANs temos dois tipos de portas, as de acesso ou Access onde ligamos os terminais (computadores, servidores, telefones IP e demais endpoints) e as portas de trunk ou tronco, as quais utilizamos para fazer as conexões de backbone entre os switches ou então entre um switch e um roteador. Você pode ainda encontrar no mercado e nas empresas servidores com placas de rede que suportam o 802.1Q entroncados com os switches e em alguns casos até fazendo o roteamento entre as VLANs.

Outro dispositivo que podemos entroncar com um switch via 802.1Q são os Access Point (pontos de acesso sem fio), assim você pode transmitir via rede aérea os pacotes de mais de uma subrede com apenas um aparelho.

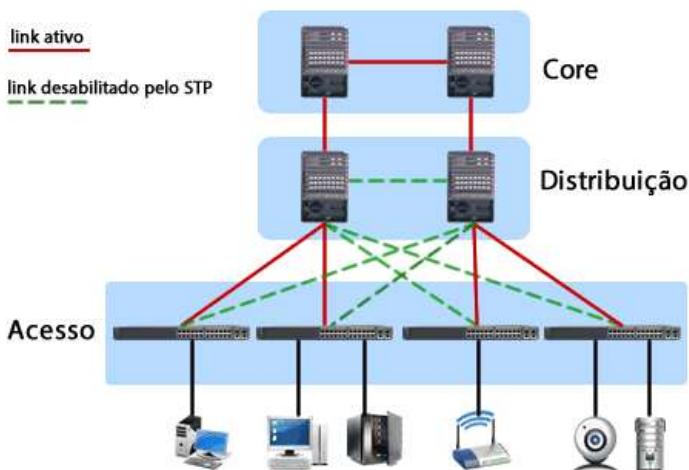
#### 4 Protocolo Spanning-Tree – STP, RSTP e MSTP

Vimos anteriormente que em uma rede LAN da família Ethernet utilizando switches os caminhos redundantes eram recomendados para que no caso da queda de um link outro pudesse assumir o tráfego entre os switches. Porém, também estudamos que essa redundância traz problemas na camada 2, chamados de loops de camada 2, os quais podem ser muito prejudiciais à rede.

Veja a figura abaixo com uma topologia em três camadas onde temos vários loops, porém destacamos um que ocorre entre as conexões redundantes do switch Acc-1 e os dois switches de distribuição (linhas pintadas em vermelho).



Para que essa conexão física seja possível em redes comutadas o protocolo spanning-tree (STP – Spanning-Tree Protocol) envia quadros especiais e calcula uma topologia livre de loops. Ele faz isso desabilitando algumas portas e no caso de queda de um link ativo ele recalcula a topologia e habilita o caminho redundante. Veja na figura seguinte a topologia lógica final após o cálculo do spanning-tree. Perceba que temos apenas um caminho possível entre os switches e as demais interfaces ficam desabilitadas até que um problema em algum dos links principais ocorra.



Atualmente existem três versões do protocolo Spanning-tree definidos pela IEEE:

- 802.1d ou Per-VLAN Spanning Tree Protocol (PVST);
- 802.1w ou Rapid Spanning Tree Protocol (RSTP ou Rapid Per-VLAN Spanning Tree - RPVST);
- 802.1s ou Multiple Spanning Tree Protocol (MSTP).

Os protocolos 802.1d e 802.1w tem a operação bastante semelhante, porém o RSTP tem a convergência muito mais rápida que o PVST. Enquanto o PVST pode levar até 50 segundos para convergir a rede (calcular o caminho livre de loops e iniciar o encaminhamento de quadros) o RSTP pode levar entre 3 e 5 segundos apenas. Isso é possível devido a melhorias na quantidade de estado de portas e simplificação dos contadores internos.

O Multiple STP (MSTP - IEEE 802.1s) possibilita o uso do RSTP em ambientes com múltiplas VLANs, tornando possível mapear um conjunto de VLANs que compartilham a mesma topologia lógica em uma mesma instância de RSTP. O MSTP reduz o número total de instâncias RSTP gerada pelo cálculo de uma instância para cada VLAN através do agrupamento de múltiplas VLANs em uma única instância RSTP. Com isso o switch tem o seu overhead (sobrecarga de trabalho) gerado pelo envio de BPDU para cada instância de STP criada reduzido, assim como o tempo de convergência da rede como um todo também é reduzido.

A maioria dos switches de mercado utiliza por padrão o PVST (Spanning Tree por VLAN – 802.1d), o qual automaticamente quando fazemos a criação de uma VLAN também cria uma instância de STP para ela, ou seja, ao criar a VLAN 2 uma instância de STP para essa VLAN também é criada para evitar loops de camada 2.

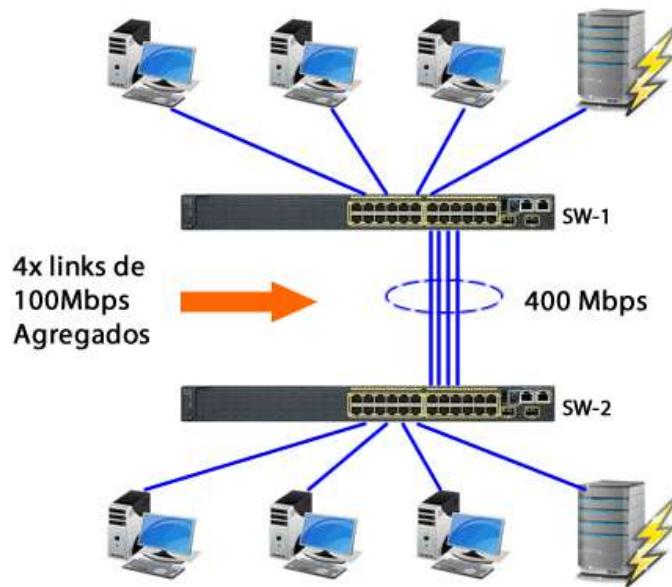
Para utilizar o RSTP ou o MSTP é necessário verificar se o switch suporta os recursos e inserir as configurações necessárias, as quais variam de fabricante para fabricante.

## 5 Recursos Avançados – Agregação de Links, Empilhamento e Espelhamento de Portas

### 5.1 Agregação de Links

A agregação de links ou Ethernet bonding segue a norma IEEE 802.3ad com o título **Link Aggregation**. Trata-se de uma técnica usada para o acoplamento de dois ou mais canais Ethernet em paralelo para produzir um **único canal de maior velocidade** e/ou **aumentar a disponibilidade e redundância** desse canal.

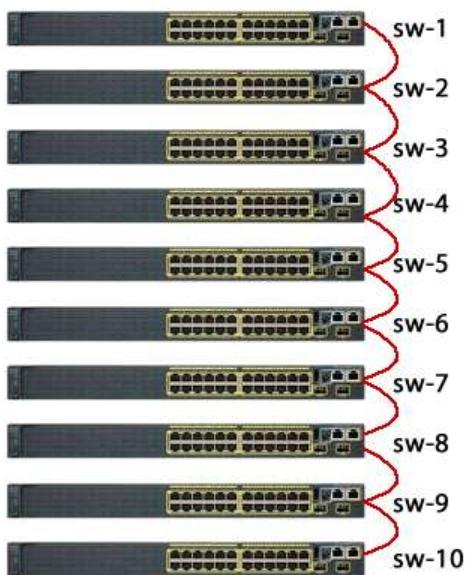
A vantagem do uso do link aggregation é a de manter os dois links ativos, pois o spanning tree encara dois links agregados como se fosse uma só conexão. Dessa forma você ganha largura de banda entre os switches, pois ao invés de ter uma porta funcionando com o link aggregation serão duas. Também tem a redundância, pois se uma porta cair a outra continua operando normalmente. Veja a figura abaixo com um exemplo de agregação de quatro links fastethernet em um link de 400Mbps. No caso de um dos links ficar inoperante a banda cai para 300Mbps, porém a conexão continua operando normalmente.



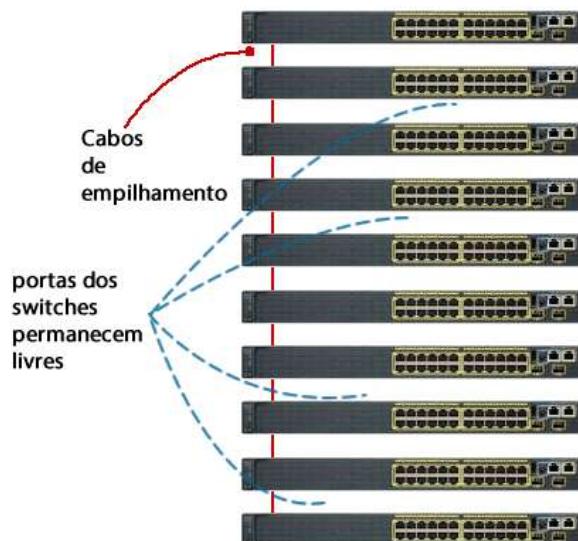
O link aggregation pode ser utilizado entre dois switches, ou então entre um switch e um roteador, entre um switch e um servidor, entre dois servidores ou em uma rede de switches Metroethernet para aumentar a largura de banda e inserir redundância do link.

## 5.2 Empilhamento de Switches (Stacking)

Outro recurso que alguns switches possuem é o empilhamento ou stacking, porém nesse caso precisamos de switches que suportem o empilhamento chamados de **switches stackable** ou "empilháveis". Para entender o empilhamento vamos a um exemplo onde uma empresa precisa de 230 portas para conectar computadores e demais terminais de rede e decide adquirir 10 switches de 24 portas. Ficam sobrando aqui 10 portas, correto? Os switches precisam ser interligados, pois ficam no mesmo ambiente, então quantos pontos precisaremos para essa conexão? Tudo depende da topologia usada, porém se formos conectá-los em cascata utilizando apenas uma porta precisaremos de uma porta no primeiro e último switch e duas portas do segundo ao nono switch, ou seja, um total de pelo menos 18 portas.



Com o empilhamento não precisamos utilizar portas dos switches para fazer essas conexões, pois ele é realizado com um cabo especial que interliga diretamente o backplane dos switches e em termos de gerenciamento é como se criássemos um switch novo com 240 portas.



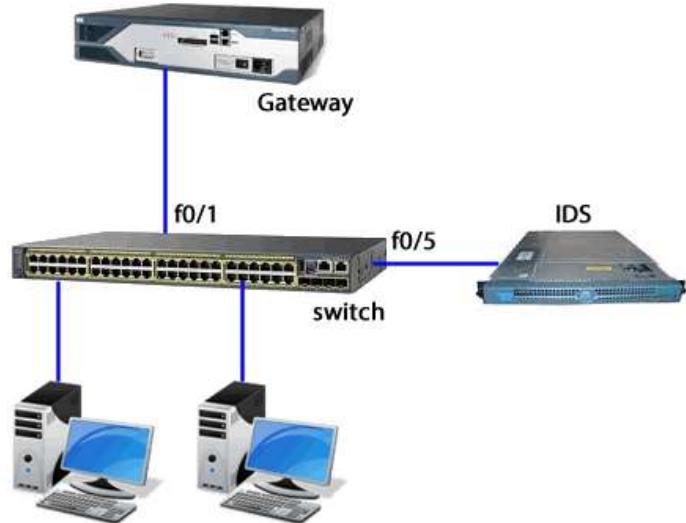
Conforme já citado não são todos os switches que suportam esses recursos de agregação de links ou empilhamento. Em seu projeto você precisará consultar o fabricante escolhido sobre qual o melhor modelo para utilizar esse tipo de recurso. Além disso, as figuras e quantidades de conexões utilizadas em ambos os exemplos são meramente ilustrativas, pois cada fabricante ou modelo de switch tem uma especificação própria.

### 5.3 Espelhamento de Porta

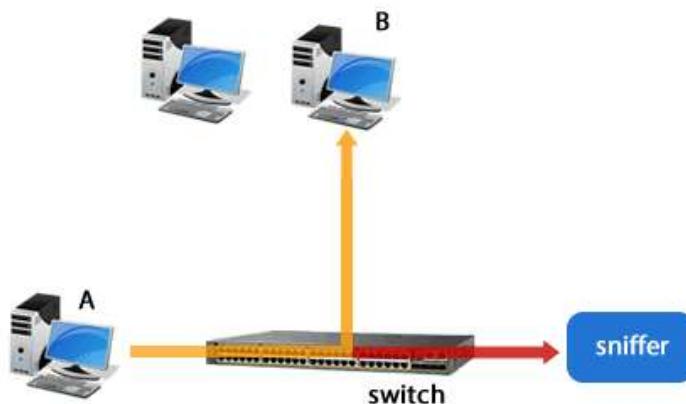
O espelhamento de portas é utilizado para fins de gerenciamento e monitoração de uma rede. Lembre que a principal característica das portas de um switch é que cada uma delas é um domínio de colisão, ou seja, a troca de quadros entre duas portas fica restrita somente à essas portas.

Em um HUB tudo o que é enviado é recebido por todos os hosts conectados à ele, portanto um HUB permite que você monitore o tráfego da rede relativo à todos os elementos conectados ao HUB. Porém um switch não, pois os quadros não são copiados para todas as portas, com exceção do processo de flooding, broadcasts e multicasts. Mas então se precisarmos monitorar o tráfego das portas como faremos? Uma opção é colocar um HUB na porta e conectar um segundo micro com um sniffer ou analisador de protocolo com sua placa de rede em modo promiscuo (lendo quaisquer quadros mesmo que não sejam para a própria máquina). Porém não parece uma solução muito viável, correto?

A solução é o espelhamento de portas dos switches, o qual permite que você envie uma cópia de todo tráfego de todas as portas para uma determinada porta. Por exemplo, posso espelhar o tráfego do switch na porta Fast 0/5 e conectar um IDS (Sistema de Detecção de Intrusão) para verificar se minha rede não está sendo invadida, assim todos os quadros trocados pelas portas daquele switch serão enviados para o IDS analisar, via porta Fast 0/5.



Outra aplicação para o espelhamento de porta é conectar um sniffer com capacidade de análise de protocolos para verificar o que está passando na rede e saber qual o nível de broadcast está passando por aquele switch, por exemplo.



Em switches Cisco o espelhamento de porta é geralmente chamado de Switched Port Analyzer (SPAN), já em switches 3Com é denominado Roving Analysis Port (RAP).

## 6 Outros Modelos de Switches (Camadas 3 a 7)

Ao utilizar VLAN em uma rede com switches normais de camada-2 precisamos de um equipamento de camada 3 para fazer o roteamento entre essas VLANs, no início eram utilizados roteadores para realizar esse papel, nada mais comum, pois se é preciso **rotear** entre as VLANs que sejam utilizados **roteadores**.

O fabricante de equipamentos Cisco Systems recomenda que os domínios de broadcast separados por uma porta de um dispositivo de camada 3 (switch layer 3 ou roteador) não ultrapassem 500 hosts quando utilizamos o protocolo IP. Porém existem outras recomendações para dimensionamento e muitas delas de diferentes fabricantes de equipamentos.

Porém, como o preço dos roteadores é elevado, normalmente mais elevado que o dos switches, foram criados os **switches de camada três** também conhecidos como "**switch-router**" ou "**switches layer 3**". Esses switches fazem o roteamento entre VLANs e outras tarefas que os roteadores normalmente desempenham, tais como listas de controle de acesso, DHCP, roteamento dinâmico, etc. A diferença básica entre um switch de camada 3 e um de camada 2 é que nos layers 3 podemos habilitar o protocolo IP e o roteamento IP, possibilitando configurar IP nas interfaces e também fazer o roteamento entre as VLANs. Já nos layer 2 as portas somente trabalham lendo endereços MAC, não podemos atribuir IP nelas ou fazer roteamento.

Não confunda o IP de gerenciamento do switch camada 2 com os recursos de um switch camada 3, pois o IP de gerenciamento é apenas um IP virtual que é inserido para acesso remoto via Web, Telnet ou SSH para fins de configuração e gerenciamento.

Apesar dessas diferenças, se você não habilitar o roteamento IP em um switch camada 3 ele se comporta como um de camada 2. Ou seja, via de regra, para que o switch layer 3 trabalhe na camada 3 é necessário que você habilite o roteamento IP nesse switch, caso contrário ele irá atuar como um switch layer 2 comum. Já a diferença entre um roteador e um switch de camada 3 é que na maioria dos roteadores o encaminhamento de pacotes se dá utilizando um **software** que roda em sua CPU, já nos switches camada 3 esse encaminhamento de pacotes (roteamento) se dá através de **hardware**, utilizando ASICs (Application-specific Integrated Circuit).

Outro modelo de switch (não muito comum de ser encontrado isoladamente) é o de **camada 4** (transporte), o qual permite que o switch tome decisões de encaminhamento baseado no tipo de protocolo (TCP ou UDP) e portas. Esse modelo de switch é utilizado normalmente para criar listas de acesso e melhorar a segurança da rede ou fazer balanceamento de carga. Muitos dos switches ditos layer 3 possuem também capacidades de layer 4, porém como essa denominação de "switch camada 4" não é muito comum os fabricantes acabam chamando esse equipamentos de switches de camada 3 mesmo.

Já um **switch camada 7** permite o roteamento de pacotes de acordo com as aplicações. Ele é utilizado em alguns casos no balanceamento de carga entre servidores de Internet, por exemplo. Alguns fabricantes os denominam como **Switch de Conteúdo** (Content Switch) ou **Web-Switch**.

## 7 Modelos de Switches e suas Interfaces

Como você já pode perceber a classificação dos switches pode ser uma tarefa complicada, mas vamos tentar agregar aqui por algumas características principais. A primeira delas é referente ao modelo de hardware, temos dois tipos de hardware de switch:

- **Modular:** nesse modelo de switch temos um chassi que não tem inteligência e devemos equipar com placas, por exemplo, uma controladora (CPU), placas de tributário (portas RJ-45, fibra, etc.), ventiladores (Fans), etc.
- **Configuração fixa:** nesse caso o switch é uma "caixa preta", ou seja, já vem com um chassi e o número de portas fixas, você não pode expandir e nem remover portas. Por exemplo, um switch 24 portas virá com as 24 portas e se você precisar de mais portas tem que comprar um novo switch, não há como inserir módulos nele.

Veja as figuras abaixo com modelos de switches de configuração fixa e modular respectivamente. Note que no switch modular você tem um chassi ou sub-bastidor vazio e precisa inserir as placas para que ele funcione. Normalmente os switches modulares são de maior porte (distribuição e core) e mais caros que os de configuração fixa.



Outra classificação que podemos utilizar é relativa a posição da rede que esse switch será inserido, se de **Acesso, Distribuição** ou **Core**. Vamos nesse curso focar nos switches de acesso, pois os switches de maior porte são muito flexíveis e com recursos que variam muito entre fabricantes, tornando muito difícil fazer um curso não vinculado a uma marca, como é o propósito desse curso.

Os switches de acesso são os que estamos mais acostumados a trabalhar, são normalmente de configuração fixa e podem ter de 4 a 48 portas, sendo que os mais comuns são os de 8, 16, 24 e 48 portas. Alguns ainda possuem duas portas a mais para o entroncamento (trunk) com outros switches ou com um roteador.

Na figura anterior temos dois switches de 24 portas e um de 48 portas do fabricante Extreme. Note ainda que do lado direito dos switches existem mais duas portas extras, que antigamente eram chamadas de Uplink, destinada ao entroncamento entre switches ou com roteadores. Veja um zoom abaixo com essas portas.



Com o conteúdo estudado até o momento você já poderia iniciar o processo de escolha de um switch para um determinado projeto, primeiro pela topologia a ser utilizada no backbone (como os switches serão interligados? Cascata ou em três camadas?) e número de portas que iremos precisar (quantos hosts precisarão acesso à rede?).

Lembre-se que além dos computadores temos que prever portas para os seguintes casos:

- Interligação entre os switches (trunk) da mesma LAN;
- Conexão com um roteador, caso não sejam utilizados switches de camada-3;
- Conexão com outros pontos, como saída para Internet ou outras redes;
- Portas reservas para o caso de expansão ou monitoração da rede.

Dependendo do número de hosts que precisam ser conectados à rede, será necessário também fazer a divisão lógica dos domínios de broadcast em VLANs e, portanto, a rede precisará de um dispositivo de camada 3 (roteador ou switch camada 3) para fazer o roteamento entre as VLANs. Essa é uma característica que você precisará definir em um projeto, o de utilizar switches camada 2 ou camada 3. Lembre-se que você pode utilizar os switches camada 3 apenas na distribuição e os de acesso podem ser camada 2, isso ajuda a reduzir o custo final do projeto, pois os switches de camada 3 são normalmente mais caros que os de camada 2.

Existem outros recursos ainda, como o empilhamento, agregação de portas, suporte a protocolos de roteamento mais avançados que precisam ser avaliados. Tenha a certeza de quanto mais recursos o switch possuir mais caro será o modelo que irá se adequar a todas as necessidades.

Por último vamos analisar os tipos de interface que podemos utilizar para o backbone da rede, ou seja, para fazer a interligação dos switches. O tipo de interface a ser utilizada depende basicamente da distância e/ou padrão que a empresa utiliza. Por exemplo, links maiores que 100m precisarão de uma conexão de fibra, este é um requisito do padrão ethernet, ou então por determinação da empresa todos os links de backbone que não ficam no mesmo ambiente devem ser realizados com fibra óptica. Nesse ponto você terá que definir esses links, o tipo de fibra a ser utilizado e a conectorização, pois existem alguns modelos de conectores e interfaces de fibra diferentes, muitas vezes serão necessários adaptadores para fazer o casamento de padrões. Veremos melhor os tipos de conectores e fibras em um capítulo posterior, dedicado a esse assunto.

Para conexão via RJ-45 com cabos UTP normalmente é só utilizar uma ou mais portas do switch com um cabo cruzado, caso a porta do switch não suporte o Auto-MDIX, ou seja, a detecção automática do tipo de cabo. Quando o switch possui o recurso de detecção automática do tipo de cabo não importa para o switch se o cabo é direto ou cruzado.

Já no caso do uso de um link de fibra podemos optar por utilizar um conversor de mídia ou então um switch com suporte a interfaces de fibra. Na prática o recomendado é reduzir os pontos de falha de uma rede, por isso é preferível utilizar a saída de fibra no próprio switch.

Os switches podem suportar diversos tipos de conexão de fibra, porém alguns são mais limitados, por isso você deve ter em mente as especificações do projeto para escolher o tipo correto de padrão a ser utilizado. As interfaces de fibra também são conhecidas como Transceiver, os quais geralmente são agrupados pela velocidade de transmissão de 1Gbps e 10Gbps.

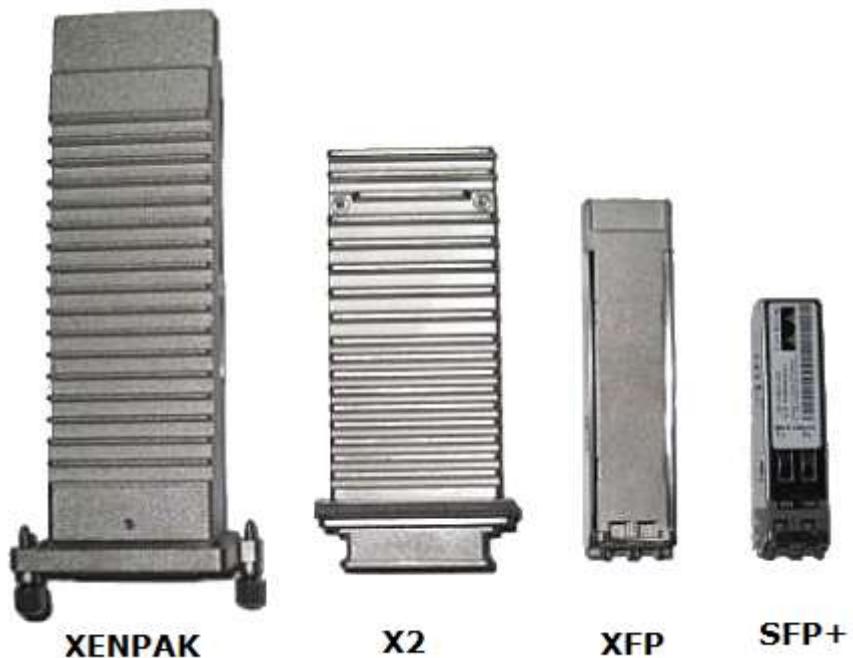
Os transceivers de 1Gbps são conhecidos como GBIC (gigabit interface converter) e SFP (small form-factor pluggable), porém alguns deles também suportam a velocidade de transmissão de 100Mbps (Fast Ethernet). A maioria das GBICs tem uma terminação óptica do tipo SC (veja figura 4) e as SFPs utilizam conectores LC.



Os transceivers de 10Gbps podem ser dos tipos XFP, X2, XENPAK e SFP+, segue uma breve descrição sobre cada uma das interfaces abaixo:

- **XENPAK** – a primeira interface óptica de 10GbE. Utiliza conector SC.
- **X2** – Sucessor da XENPAK. Utiliza conector SC.
- **XFP** – primeira "small form factor" 10GbE. Utiliza conector LC.
- **SFP+** – interface óptica de 10GbE que utiliza o mesmo formato físico da gigabit SFP. Utiliza conector LC.

Normalmente a taxa de 10Gbps não é suportada por switches de pequeno porte, somente por switches modulares, porém com a evolução das tecnologias é bem provável que em um futuro próximo essa realidade mude. Veja a figura abaixo com alguns modelos de transceivers de 10Gbps do fabricante Cisco.



A última classificação que pode ser realizada para dividir as linhas de switch de um fabricante é por segmento industrial ou corporativo que os switches se destinam. Por exemplo, o fabricante Cisco tem uma linha de switches para pequenos escritórios, mais baratos, chamada Small Business. Outras denominações são switches "Enterprise", ou seja, para corporações de todos os portes, das pequenas até as grandes empresas.

Com isso fechamos esse módulo do curso e até o próximo!

*Nos capítulos anteriores estudamos os dispositivos, protocolos e topologias utilizadas em redes LAN, agora vamos estudar como conectar fisicamente esses dispositivos de maneira estruturada. Além disso, será abordada a questão da energização dos equipamentos e cuidados que devemos ter com a rede elétrica.*

*Bons estudos.*

## **Capítulo 07 - Infraestrutura de Redes e Cabeamento Estruturado**

### **Objetivos do Capítulo**

Ao final desse capítulo você deverá ter estudado e compreendido os seguintes conceitos:

- Visão geral da infraestrutura necessária para montagem de uma rede;
- Tipos de cabos e conectores disponíveis;
- O que é um cabeamento estruturado e seus componentes;
- Os conceitos sobre a rede elétrica e cuidados para a energização dos equipamentos.

## Sumário do Capítulo

<b>1</b>	<i>Infraestrutura Física de Redes</i>	<b>216</b>
<b>1.1</b>	<i>Cabos metálicos</i>	<b>216</b>
1.1.1	Montagem e Testes dos Cabos de Pares Trançados	219
<b>1.2</b>	<i>Cabos Coaxiais</i>	<b>221</b>
<b>1.3</b>	<i>Fibras Ópticas</i>	<b>222</b>
1.3.1	Principais Tipos de Conectores Ópticos	224
<b>2</b>	<i>Cabeamento Estruturado</i>	<b>228</b>
<b>2.1</b>	<i>Cabeamento Horizontal / Rede Secundária</i>	<b>229</b>
<b>2.2</b>	<i>Cabeamento Vertical / Rede Primária</i>	<b>232</b>
<b>2.3</b>	<i>Área de Trabalho</i>	<b>233</b>
<b>2.4</b>	<i>Sala de Telecomunicações</i>	<b>234</b>
<b>2.5</b>	<i>Sala de Equipamentos</i>	<b>237</b>
<b>2.6</b>	<i>Sala de Entrada de Serviços de Telecomunicações</i>	<b>239</b>
<b>2.7</b>	<i>Administração do Cabeamento</i>	<b>239</b>
<b>3</b>	<i>Conceitos Básicos sobre Infraestrutura Elétrica de Redes</i>	<b>240</b>
<b>3.1</b>	<i>Cuidados ao Energizar os Equipamentos – 127V ou 220V?</i>	<b>241</b>
<b>3.2</b>	<i>Principais Problemas da Rede Elétrica</i>	<b>243</b>
<b>3.3</b>	<i>Aterramento</i>	<b>246</b>
<b>3.4</b>	<i>Filtros de Linha</i>	<b>246</b>
<b>3.5</b>	<i>No-break ou UPS</i>	<b>248</b>
3.5.1	Tipos de No-Break	249

## 1 Infraestrutura Física de Redes

A infraestrutura física de redes de uma maneira genérica visa a conexão física e energização dos diversos dispositivos de rede.

A conexão física dos equipamentos é realizada através do cabeamento, o qual deve seguir normas e padrões industriais chamados normalmente de "Cabeamento Estruturado" (CE), o qual é uma infraestrutura única de cabeamento metálico ou óptico não proprietária, capaz de atender a diversas aplicações e proporcionar flexibilidade de layout, facilidade de gerenciamento, administração e manutenção.

Além do cabeamento propriamente dito existem diversos outros materiais e recursos de infraestrutura utilizados para facilitar a instalação e organização do cabeamento, tais como conectores, guias, caneleiras, caixas de passagem, piso elevado, racks, etc.

### 1.1 Cabos metálicos

O principal cabo metálico utilizado nas redes é o par trançado, os quais podem ser blindados ou não blindados e possuem 4 pares por cabo. Cada par é separado por cores para facilitar a conectorização. As principais vantagens de uso do cabo par trançado são taxa de transmissão, baixo custo do cabo e baixo custo de manutenção de rede. As taxas usadas nas redes com o cabo par trançado são:

- 10 Mbps (Ethernet)
- 100 Mbps (Fast Ethernet)
- 1000 Mbps (Gigabit Ethernet)
- 10000 Mbps ou 10Gbps (10Gigabit Ethernet)

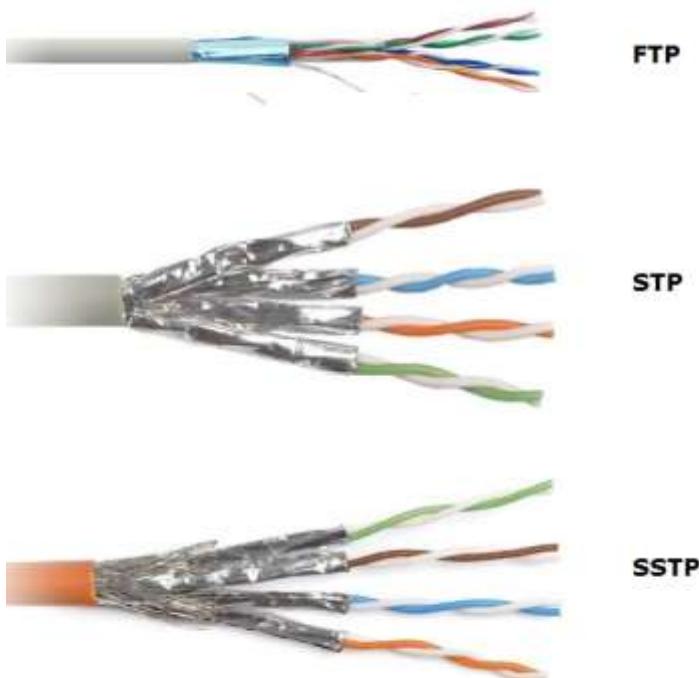
O mais utilizado na prática é o cabo não blindado denominado UTP (Unshielded Twisted Pair ou Par Trançado sem Blindagem), o qual pode ser utilizado para transmissão tanto de dados como voz.



Para a conexão dos cabos UTP são utilizados os conectores RJ-45 macho ou fêmea. Os conectores macho são utilizados como terminação das conexões e os fêmeas, conhecidos como keystone jacks, são utilizados nos painéis de distribuição (de patch-panels), nas tomadas de telecomunicações (utilizadas nas mesas e paredes), placas de rede e assim por diante.



Os cabos blindados dividem-se em três categorias: FTP, STP e SFTP. O mais utilizado deles é o STP (Shield Twisted Pair ou Par Trançado Blindado), o qual é semelhante ao UTP com a diferença de possuir uma blindagem feita com uma malha metálica em cada par. Veja a figura abaixo com os blindados.



Note na figura que os cabos FTP (Foiled Twisted Pair) são os que utilizam a blindagem mais simples com apenas uma blindagem que envolve todos os pares. Já os cabos SSTP (Screened Shielded Twisted Pair), também chamados de SFTP (Screened Foiled Twisted Pair), combinam a blindagem individual para cada par de cabos com uma segunda blindagem externa, envolvendo todos os pares, o que torna os cabos especialmente resistentes a interferências externas. Para os cabos blindados existem os conectores blindados do padrão RJ-45.

Os cabos UTP foram padronizados pelas normas da EIA/TIA-568-B, sendo divididos em 10 categorias, levando em conta o nível de segurança e a bitola do fio, onde os números maiores indicam fios com diâmetros menores.

Em todas as categorias, a distância máxima permitida é de 100 metros (com exceção das redes 10G com cabos categoria 6, onde a distância máxima cai para apenas 55 metros). Veja abaixo um resumo das principais características de cada categoria.

- **Categoria 1 (CAT1):** Consiste em um cabo blindado com dois pares trançados compostos por fios 26 AWG. São utilizados por equipamentos de telecomunicação e rádio. Foi usado nas primeiras redes Token-Ring, mas não é aconselhável para uma rede par trançado atualmente.
- **Categoria 2 (CAT2):** É formado por pares de fios blindados (para voz) e pares de fios não blindados (para dados). Também foi projetado para antigas redes token-ring e ARCnet chegando a velocidade de 4 Mbps, não sendo mais utilizados atualmente.
- **Categoria 3 (CAT3):** É um cabo não blindado (UTP) usado para dados de até 10Mbps com a capacidade de banda de até 16 MHz. Foi muito usado nas redes Ethernet criadas nos anos noventa (10BASET).
- **Categoria 4 (CAT4):** É um cabo par trançado não blindado (UTP) que pode ser utilizado para transmitir dados a uma frequência de até 20 MHz e dados a 20 Mbps. Foi usado em redes que podem atuar com taxa de transmissão de até 20Mbps como token-ring, 10BASET e 100BASET4. Não é mais utilizado, pois foi substituído pelos cabos CAT5 e CAT5e.
- **Categoria 5 (CAT5):** usado em redes fast ethernet em frequências de até 100 MHz com uma taxa de 100 Mbps. Não utilizado mais atualmente, pois foi substituído pela categoria 5e.
- **Categoria 5e (CAT5e):** é uma melhoria da categoria 5. Pode ser usada para frequências até 125 MHz em redes 1000BASE-T gigabit ethernet. Ela foi criada com a nova revisão da norma EIA/TIA-568-B. Esse padrão é utilizado até os dias de hoje.
- **Categoria 6 (CAT6):** definido pela norma ANSI EIA/TIA-568-B-2.1 possui bitola 24 AWG e banda passante de até 250 MHz e pode ser usado em redes gigabit ethernet com velocidade de 1Gbps.
- **Categoria 6a (CAT 6A):** é uma melhoria dos cabos CAT6. O a de CAT6a significa augmented (ampliado). Os cabos dessa categoria suportam até 500 MHz e podem ter até 55 metros no caso da rede ser de 10Gbps, caso contrário podem ter até 100 metros para as velocidades de 10/100/1000 Mbps. Para que os cabos CAT 6a sofressem menos interferências os pares de fios são separados uns dos outros, o que aumentou o seu tamanho e os tornou menos flexíveis. Essa categoria de cabos tem os seus conectores específicos que ajudam evitar interferências.
- **Categoria 7 (CAT7):** está sendo criada para permitir a criação de redes de 40Gbps em cabos de 50m usando fio de cobre. Esta norma baseia-se na Classe F que ainda não é reconhecida pela TIA/EIA.
- **Categoria 7a (CAT7a):** está sendo criada para permitir a criação de redes de 100Gbps em cabos de 15m usando fio de cobre. Esta norma baseia-se na Classe Fa que ainda não é reconhecida pela TIA/EIA, assim como a CAT7. Os conectores da CAT7 e 7a são

diferentes dos RJ-45, serão utilizados nesse caso os conectores TERA, padrão desenvolvido pela Siemon. Veja a figura abaixo.



Portanto as categorias de cabos utilizadas atualmente são a CAT5e, CAT6, CAT6a e as CAT7 e CAT7a, porém estas duas últimas não são reconhecidas ainda pela EIA/TIA.

#### 1.1.1 Montagem e Testes dos Cabos de Pares Trançados

A montagem dos cabos é realizada com ferramentas especiais chamadas crimpadores ou alicate de crimpar, os quais são feitos para fixar o conector macho na ponta dos patch cords e patch cables (nome dado aos cabos com duas pontas macho), e punch downs utilizados para fixar os fios nos conectores fêmea. Além disso, existem também os descascadores de cabo para facilitar a confecção dos mesmos.

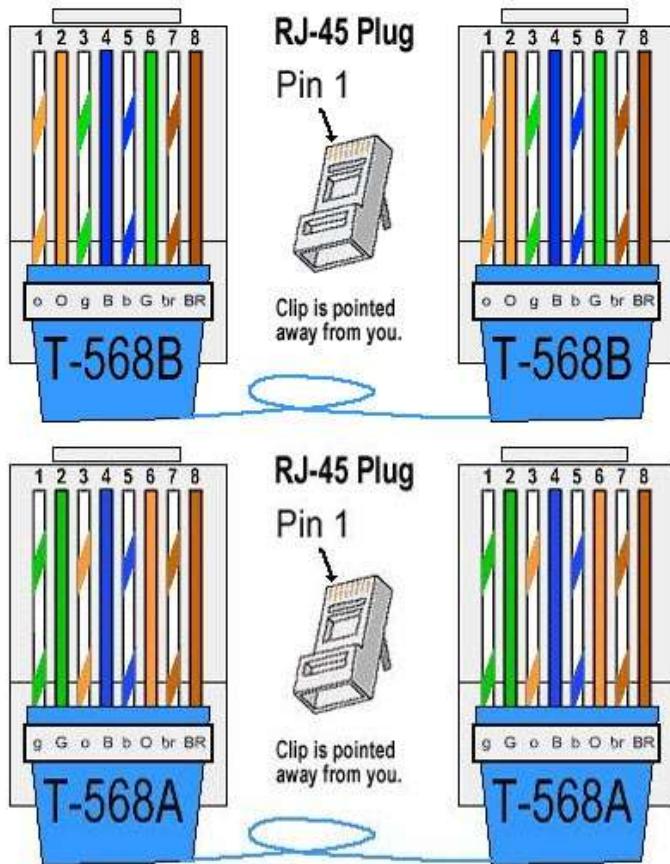


Essa montagem pode ser basicamente de dois tipos cabos, um chamado cabo direto e outro chamado cabo cruzado (cross), as quais estão baseadas nos padrões T568A e T568B. Antes de vermos os padrões vamos conhecer as cores dos fios, que são:

- Laranja e branco
- Laranja
- Verde e branco
- Azul
- Azul e branco
- Verde
- Castanho (ou marrom) e branco
- Castanho (ou marrom)

A norma EIA/TIA-568-B prevê duas montagens para os cabos, denominadas T568A e T568B. A montagem T568A usa a sequência branco e verde, verde, branco e laranja, azul, branco e azul, laranja, branco e castanho, castanho. A montagem T568B usa a sequência branco e laranja, laranja, branco e verde, azul, branco e azul, verde, branco e castanho, castanho.

Um cabo cujas duas pontas usam a mesma montagem é denominado "Cabo Direto" (T568B-T568B), e serve para ligar estações de trabalho e roteadores a switches ou hubs. Um cabo em que cada ponta é usado um padrão diferente (T568A-T568B) é denominado "Cabo Crossover", e serve para ligar equipamentos do mesmo tipo entre si. Veja na figura 2 ao lado os padrões de montagem de cada cabo.



Para testar os cabos podem ser utilizado testadores simples, os quais apenas validam a continuidade dos fios e a sequência da pinagem, ou então testadores mais avançados que possibilitam a certificação do cabeamento. Certificar um cabeamento é testar as especificações elétricas dos cabos montados, como por exemplo, ruído, interferências, atenuação e outros parâmetros definidos pelas normas EIA/TIA. Os equipamentos mais avançados ou certificadores de rede são bem mais caros e normalmente as empresas contratam outras empresas para fazer a certificação do seu cabeamento devido ao custo desses equipamentos. O fabricante mais conhecido na área dos certificadores de rede é a Fluke Networks.

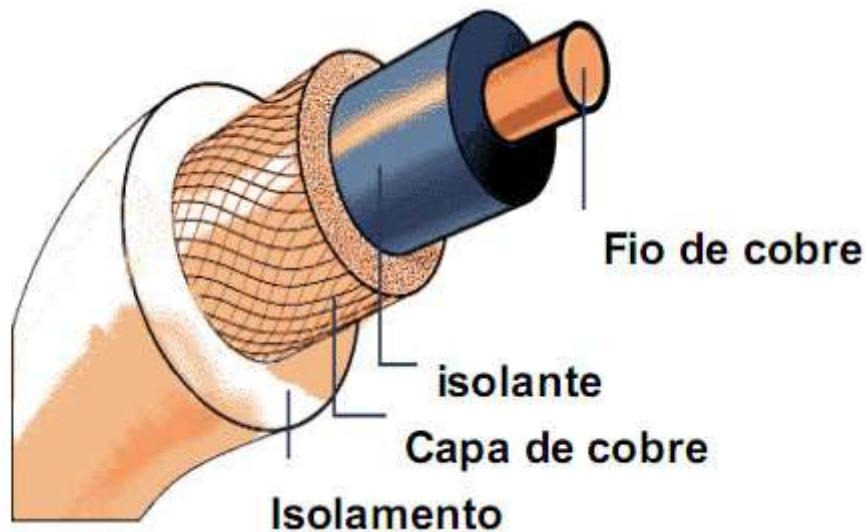
Veja a figura abaixo com um testador simples. Note que ele é composto de duas partes, onde você conecta as duas pontas do cabo e pressiona um botão para iniciar o teste, os leds irão indicar a pinagem e problemas de continuidade nos pares.



## 1.2 Cabos Coaxiais

Apesar dos cabos coaxiais terem caído em desuso nas redes de computadores, eles ainda são utilizados em um ambiente corporativo para conexão de sistemas de monitoração (CFTV - Circuito Fechado de Televisão), conexão de banda larga via cable modems (Internet provida por operadoras de TV a cabo) e conexão de links de voz digital E1 (link com 30 canais de voz agregados em apenas um circuito) utilizado em PABX e Centrais Telefônicas.

O cabo coaxial é constituído por um fio de cobre condutor revestido por um material isolante e rodeado duma blindagem.



Para a terminação dos cabos coaxiais o conector mais comum é o BNC, o qual existe uma terminação do tipo macho e outra fêmea, veja a figura abaixo.



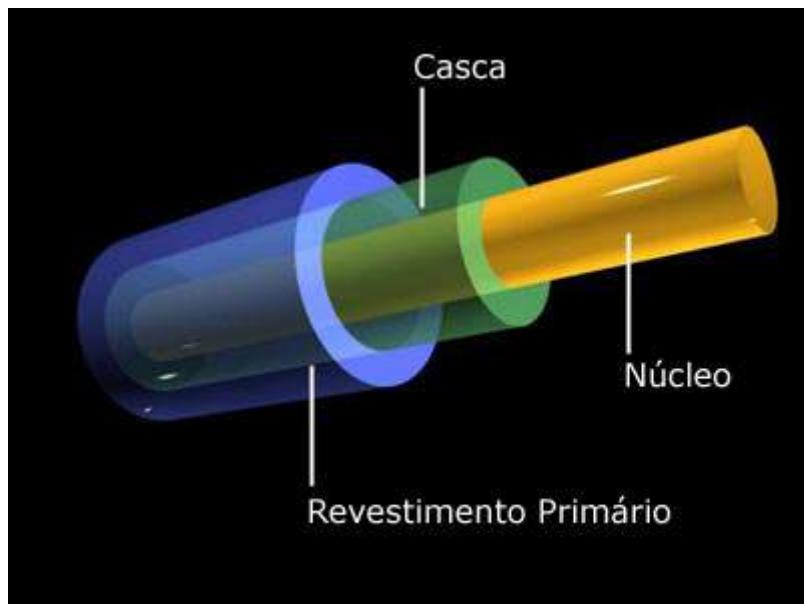
### 1.3 Fibras Ópticas

As fibras ópticas em redes de computadores são utilizadas para conectar equipamentos que estão distantes uns dos outros, em ambientes de muita interferência eletromagnética e principalmente no backbone das redes, ou seja, para interligar os diversos switches da rede. Além disso, nos Data Centers os servidores e storages também utilizam fibras ópticas para suas conexões de rede por sua velocidade e alta disponibilidade.

Isto se explica porque o sinal transmitido pelas fibras é um feixe de luz ou laser, portanto ela não é suscetível às interferências eletromagnéticas. Além disso, a banda passante em fibras ópticas é muito superior aos demais meios.

O foco desse capítulo será mais técnico para ajudar a você entender as fibras que estão disponíveis no mercado e as opções de conectores, sem aprofundar a teoria.

Lembre que uma fibra óptica utiliza como princípio a reflexão total da luz em dois meios com índice de refração diferentes, um núcleo e uma casca com índices diferentes que fazem a luz refletir dentro da fibra, veja a figura abaixo. As fibras ópticas são divididas em dois tipos: monomodo e multimodo.



Abaixo seguem as características das fibras Monomodo.

- Permite o uso de apenas um sinal de luz pela fibra, ou seja, um modo e por isso o nome "monomodo".
- Dimensões menores que os outros tipos de fibras.
- Maior banda passante por ter menor dispersão (o sinal óptico fica menos distorcido na recepção).
- Geralmente é usado um laser como fonte de geração de sinal.
- Pode ser utilizada para longas distâncias.
- Seu núcleo pode ter núcleo de 8 a 10 µm (micrometros ou micron) de diâmetro.

Atualmente as fibras monomodo podem ser classificadas em três grupos:

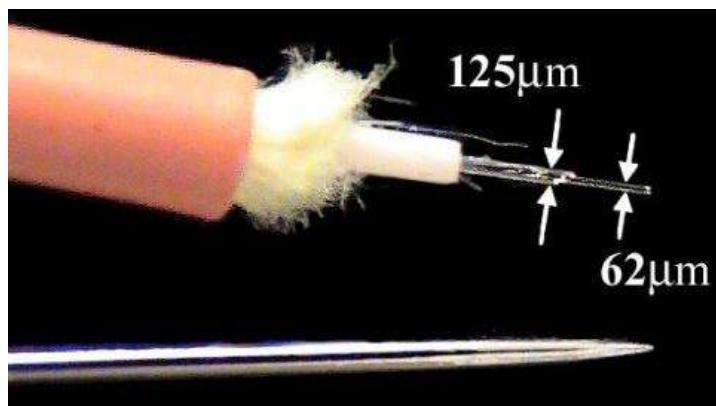
- Fibras monomodo convencionais ITU-T G.652 (Standard Monomode Fiber - SMF)
- Fibras de dispersão deslocada ITU-T G.653 (Dispersion Shifted Fiber - DSF)
- Fibras de dispersão deslocada não nula ITU-T G.655 (Non Zero Dispersion Shifted Fiber - NZDF).

Agora vamos ver as características de uma fibra Multimodo.

- Permite o uso de fontes luminosas mais simples como LEDs, as quais são mais baratas.
- Diâmetros grandes facilitam o acoplamento de fontes luminosas e requerem pouca precisão nos conectores, ou seja, o encaixe dos conectores é mais simplificado quando comparamos com as fibras monomodo.
- Mais usado para curtas distâncias pelo preço e facilidade de implementação.

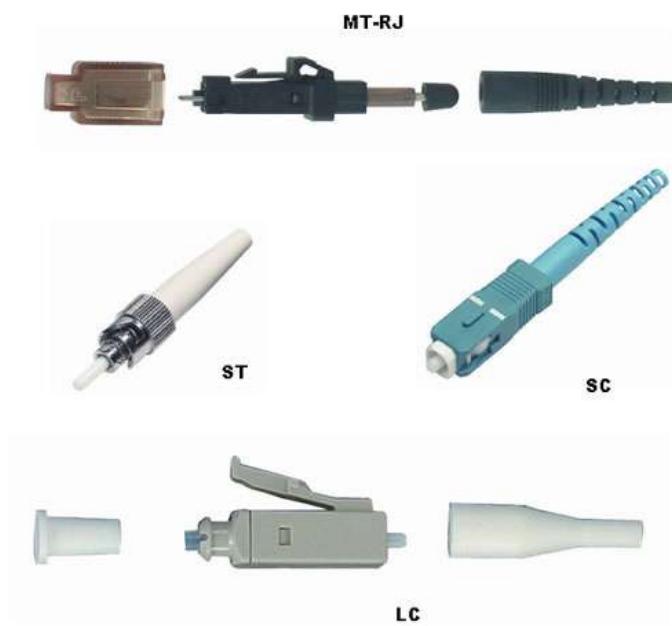
- Podemos encontrar no mercado dois tipos de fibras multimodo (MM), com núcleo de 50  $\mu\text{m}$  de diâmetro ou com núcleo de 62.5  $\mu\text{m}$  de diâmetro.
- Os sistemas que utilizam fibras multimodo, geralmente possuem LEDs (emissão com comprimento de onda entre 600 - 850 nm) ou VCSELs (tipo de laser mais simples e barato com operação em comprimentos de onda de 850 nm ou 1300 nm) como fonte luminosa.

Para você ter uma ideia das dimensões de uma fibra veja a figura 2 ao lado, trata-se de uma fibra multimodo em que a casca tem 125 mícrons e o núcleo 62,5 mícrons, abaixo tem uma agulha para comparação das dimensões.



### 1.3.1 Principais Tipos de Conectores Ópticos

Os conectores ópticos tem a função de deixar a fibra perfeitamente alinhada nos pontos de conexão para que o sinal luminoso possa ser transmitido sem grandes perdas. Os quatro tipos de conectores mais comuns são LC, SC, ST e MT-RJ, veja a figura abaixo.



Os conectores ST e SC eram os mais populares até pouco tempo atrás, mas os LC têm crescido bastante em popularidade e podem vir a tornar-se o padrão dominante.

Os conectores MT-RJ também têm crescido em popularidade devido ao seu formato compacto, mas ainda estão restritos a alguns nichos. Como cada conector oferece algumas vantagens sobre os concorrentes e é apoiada por um conjunto diferente de empresas, a escolha recai sobre o conector usado pelos equipamentos que pretender usar.

O LC (Lucent Connector) é um conector miniaturizado que, como o nome sugere, foi originalmente desenvolvido pela Lucent. Ele tem bastante popularidade, sobretudo no uso de fibras monomodo. Ele é o mais comumente usado em transceivers 10 Gigabit Ethernet.

É possível também utilizar conectores diferentes dos dois lados do cabo, usando conectores LC de um lado e conectores SC do outro, por exemplo. Além disso, existem adaptadores para que você possa conectar fibras do mesmo tipo ou de tipos diferentes. Veja a figura a seguir com um cordão com conector MT-RJ em uma ponta e outra com conector LC. O cordão óptico também é conhecido como "pigtail".



Além do uso de conectores, também é possível unir as fibras ou reparar um fio partido usando dois métodos, conforme abaixo.

- **Processo de fusão (fusion splicing)**: nesse processo é utilizado um arco elétrico para soldar as duas fibras, criando uma junção permanente. Os aparelhos de fusão atuais fazem a junção de forma semi-automatizada, o problema é que eles são muito caros e acessíveis apenas a empresas especializadas.
- **Processo mecânico (mechanical splicing)**: no processo mecânico é utilizada uma emenda de aplicação manual, onde os dois fios são unidos usando um suporte e colados através de uma resina especial, a qual foi desenvolvida para não obstruir a passagem da luz. Como a junção é bem mais frágil que o fio original, o trecho deve ser reforçado externamente para evitar uma nova ruptura.

Para testes em redes ópticas utilizamos um instrumento chamado OTDR (optical time domain reflectometer), que significa refletômetro óptico no domínio do tempo. Muitas vezes os mesmos medidores de cabos UTP podem servir como OTDRs apenas trocando-se o adaptador de entrada.



Várias medidas podem ser feitas com esse equipamento, de atenuações e perdas até verificar a distância que uma fibra foi rompida em um determinado trecho.

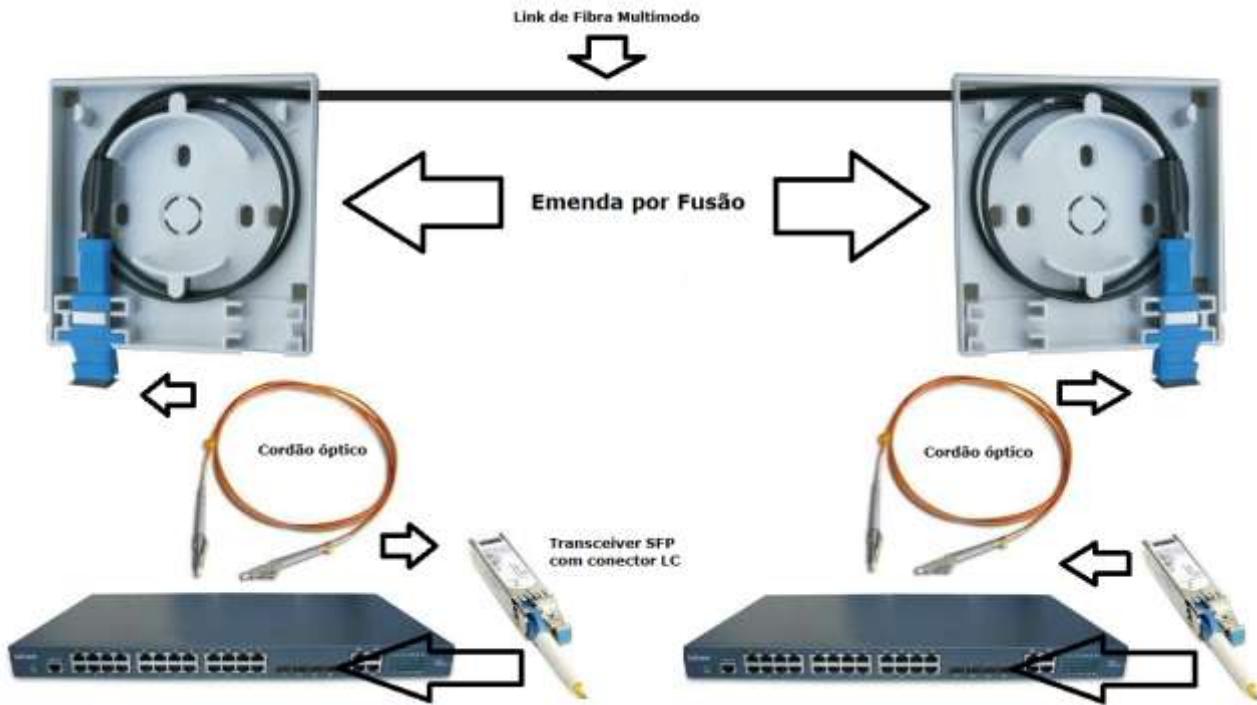
Muitas vezes a atenuação pode ser causada por sujeira no conector óptico e para limpá-los deve ser utilizado um álcool sem água chamado álcool isopropílico.

Outro equipamento muito comum de ser encontrado em redes que utilizam fibras ópticas são as caixas de distribuição ópticas (que podem ser também caixas de emendas ópticas ou caixas de terminações ópticas), utilizadas para acomodar as conexões de fibra e é onde normalmente fica terminado um circuito de fibra.

Elas são utilizadas para conectar do equipamento, como um switch ou conversor óptico à fibra de maneira segura, pois como a fibra é mais sensível que um cabo óptico deixá-la solta seria muito arriscado, seria similar ao patch panel de uma rede metálica. Veja a figura seguinte com uma caixa de terminações ópticas.



Vamos agora montar um circuito simples com uma conexão óptica entre switches de uma empresa. Por exemplo, temos dois switches com interface SFP com conectores do tipo LC que utiliza fibra multimodo (MM). Portanto, vamos precisar de um cabo de fibra multimodo e duas caixas de terminação ópticas com conectores do tipo LC, lançar um cabo com fibras entre os dois pontos e fazer emendas nas caixas de terminação óptica. Uma vez o circuito montado o caminho precisa ser testado e depois precisaremos de cordões ópticos para ligar das portas dos switches para a caixa de terminação óptica.



Baixe na área do aluno (dentro desse capítulo) o documento “**Padrões e Distâncias em Links de Fibra**” com vários padrões, tipos de fibra e distâncias suportadas para ajudar em seus futuros projetos.

## 2 Cabeamento Estruturado

O sistema de cabeamento estruturado baseia-se na padronização de interfaces e meios de transmissão, de maneira que o cabeamento seja independente ao design do ambiente e permita o tráfego de todos os tipos de sinais que uma empresa utilize, tais como voz analógica e digital, sistemas digitais de alta velocidade e comunicações de dados (LANs), vídeo e imagens, sistemas de automação predial (BAS) – incêndio, segurança, aquecimento, ventilação e ar condicionado (HVAC).

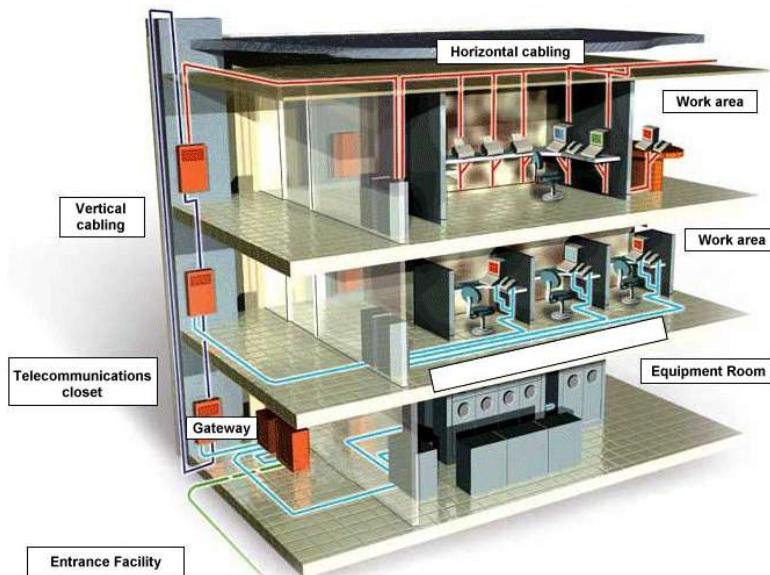
Com o objetivo de padronizar o conceito de Cabeamento Estruturado, foram desenvolvidas normas nacionais e internacionais que tratam do assunto, sendo as principais delas a NBR 14565, TIA/EIA-568-B, TIA/EIA-569-A, TIA/EIA-606-A, TIA/EIA-862, dentre outras.

O cabeamento estruturado permite mudanças, manutenções e implementações de maneira bastante rápida, segura, eficiente e controlada. Tanto que é obrigatório seguir o padrão de identificação elaborado para administrar e documentar qualquer mudança de ocupação em um edifício comercial. O objetivo da padronização é evitar erros ou dúvidas relativas aos cabos, tomadas e posição de usuários.

O sistema de cabeamento estruturado pode ser instalado por baixo de pisos, utilizando canaletas ou dutos, dentre outros. A vida útil destes sistemas, quando seguem as especificações das normas e recomendações dos fabricantes, é de no mínimo 10 anos. Esse período equivale à média da vida útil de ambientes comerciais.

No total, o sistema de cabeamento estruturado é composto por 7 subsistemas, cada um com suas próprias especificações de instalação, desempenho e teste. Seguem abaixo os subsistemas que compõe o cabeamento estruturado (veja a próxima figura):

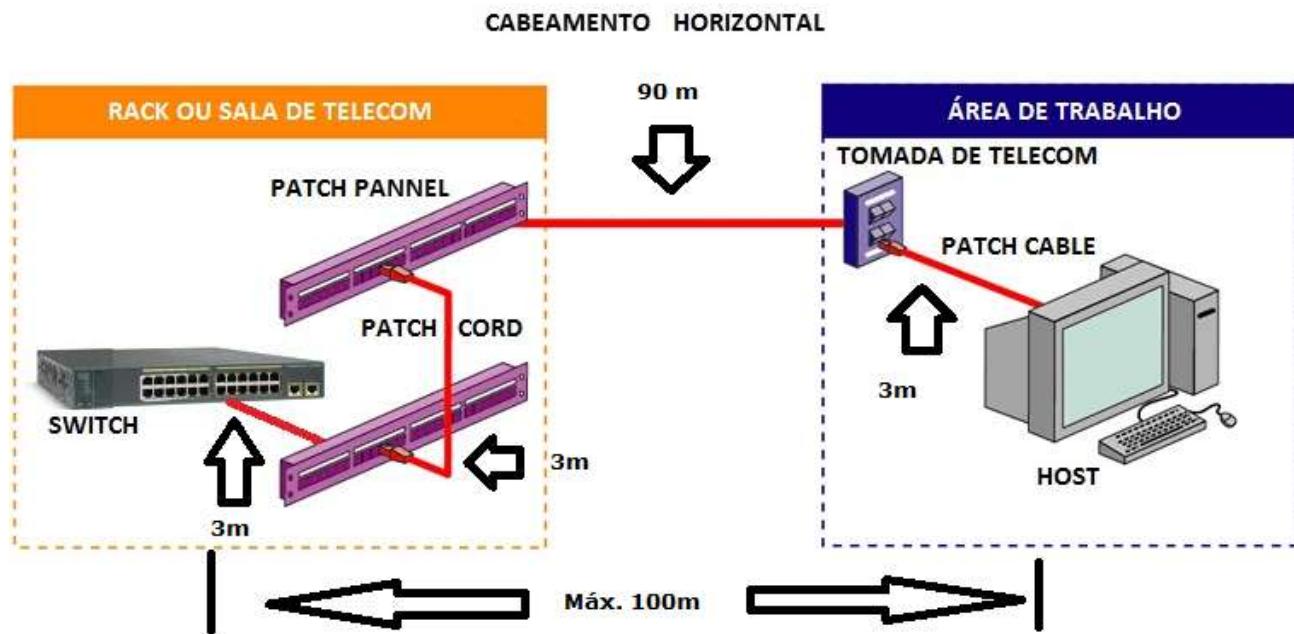
1. **Cabeamento Horizontal** (Horizontal Cabling)
2. **Área de Trabalho** (Work Area)
3. **Cabeamento Vertical** (Back Bone ou Vertical Cabling)
4. **Sala de Telecomunicações** (Telecommunications Closet)
5. **Sala de Equipamento** (Equipment Room)
6. **Entrada de Serviços de Telecomunicações** (Entrance Facilities)
7. **Administração do Cabeamento** (Cabling Administration)



Vamos a seguir estudar os principais conceitos de cada um dos subsistemas.

## 2.1 Cabeamento Horizontal / Rede Secundária

O cabeamento horizontal é todo cabeamento entre a tomada de telecomunicações (Telecommunications Outlet - TO - ou Tomadas Multi-Usuários de Telecomunicações - MUTOA) na área de trabalho e a conexão cruzada do cabeamento horizontal (patch panel) na sala de telecomunicações, incluindo a tomada de telecomunicações e a conexão cruzada horizontal.

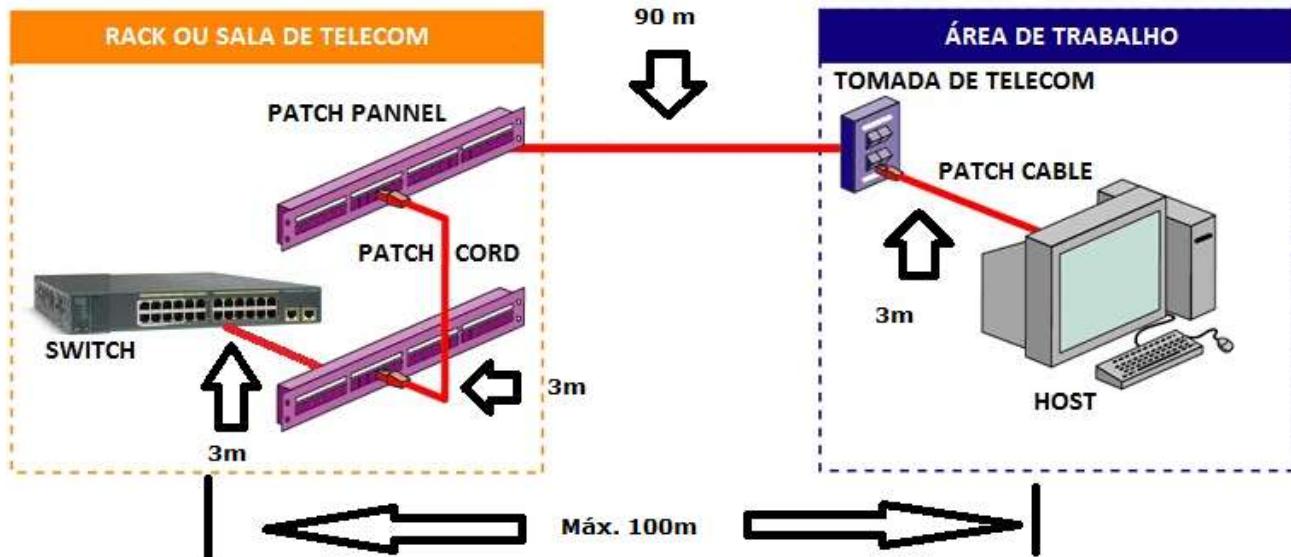


O cabeamento horizontal, como o próprio nome sugere, é passado na horizontal (por exemplo, suspenso pelo teto ou por baixo de um piso elevado) e não vai nem para baixo nem para cima entre os andares do prédio. O uso de pisos elevados ou tetos falsos ajudam na parte visual da instalação da rede, permitindo esconder o cabeamento e também uma melhor organização. Apesar disso, existem dutos feitos especialmente para instalação aparente, ou seja, dutos metálicos ou de materiais plásticos que podem ficar à mostra, porém tudo depende do requisito de cada empresa com relação à estética do ambiente da área de trabalho. Veja a figura abaixo com uma foto de um piso elevado.



A distância máxima permitida entre a tomada de telecomunicações e a sala de telecomunicações é de 90 metros, independente do tipo da categoria do cabeamento, além disso, são permitidos mais 6 metros adicionais para conexão via patch cables na sala de telecomunicações e na área de trabalho, entre os computadores e as tomadas de telecomunicação, porém combinados esses cabos não podem ultrapassar 10 metros (recomendo 3 metros no máximo para cada patch cable ou patch cord). Veja novamente a figura e repare nas distâncias indicadas.

#### CABEAMENTO HORIZONTAL

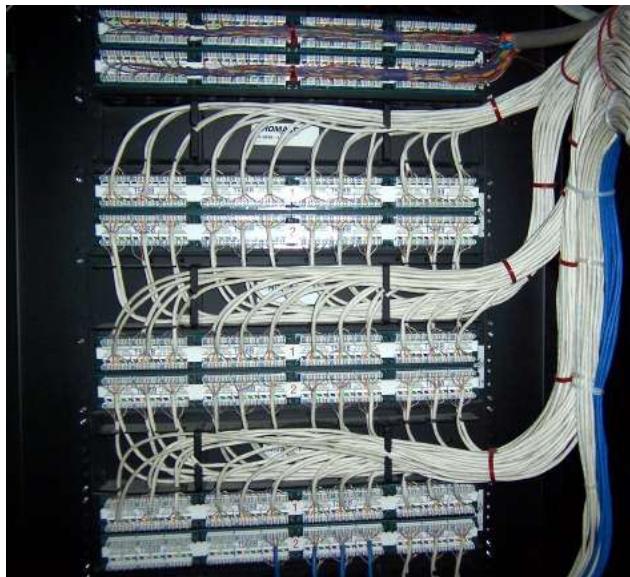


Os patch panels ou painéis de conexões (conhecidos como jackfield ou patch bay) são os elementos utilizados para a terminação do cabeamento horizontal ou nas conexões cruzadas dentro das salas de telecomunicações. Estes painéis são compostos por um conjunto de conectores RJ-45 fêmea e podem ter diversas capacidades, sendo que as mais comuns no mercado são as 24 ou 48 portas. Acompanhe na figura seguinte onde temos a foto de um patch panel de 48 portas com as vistas frontal e traseira.



A ideia de utilizar patch panels e não conectar as terminações de cabos diretamente nos switches é ter todos os seus pontos de rede espelhados no patch panel e conforme a necessidade são usados patch cords para interligar os pontos aos switches e demais ativos de rede, sem a necessidade de ficar inserindo e retirando cabos diretamente nos equipamentos.

Isso torna a rede mais flexível e a porta de um switch tem sua vida útil estendida, pois existe um limite mecânico de retirar e recolocar o cabo na porta, e ter um patch panel para fazer as manobras dos cabos evita o desgaste direto na porta do switch, pois a conexão entre o switch e o patch panel fica fixa e você irá movimentar os cabos apenas no patch panel.



Outro elemento que você pode encontrar na prática, logo abaixo ou acima de um patch panel, é o organizador de cabos (chamado também de guia ou passador de cabos). Esse organizador é utilizado para melhorar a organização da saída dos cabos na parte frontal do rack. Os organizadores podem ser frontais, o que possibilita esconder os cabos que saem dos patch panels e switches, ou laterais, os quais ajudam a passagem dos cabos pelo lado do rack.

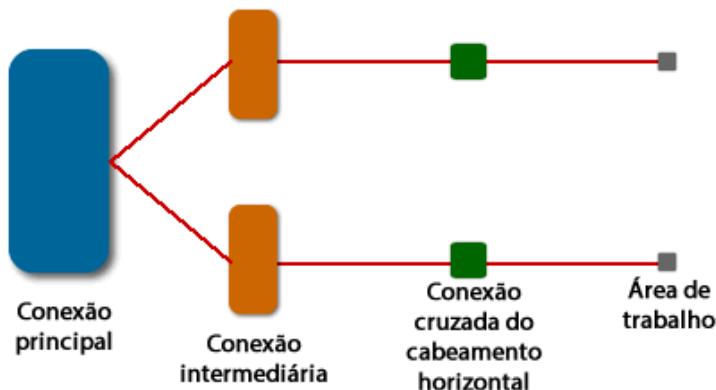


O cabo horizontal deve seguir o padrão UTP (quatro pares de  $100\Omega$ , no mínimo Categoria 5E) e pelo menos duas fibras multimodo de 62.5/125 micrões ou fibras de 50/125 micrões.

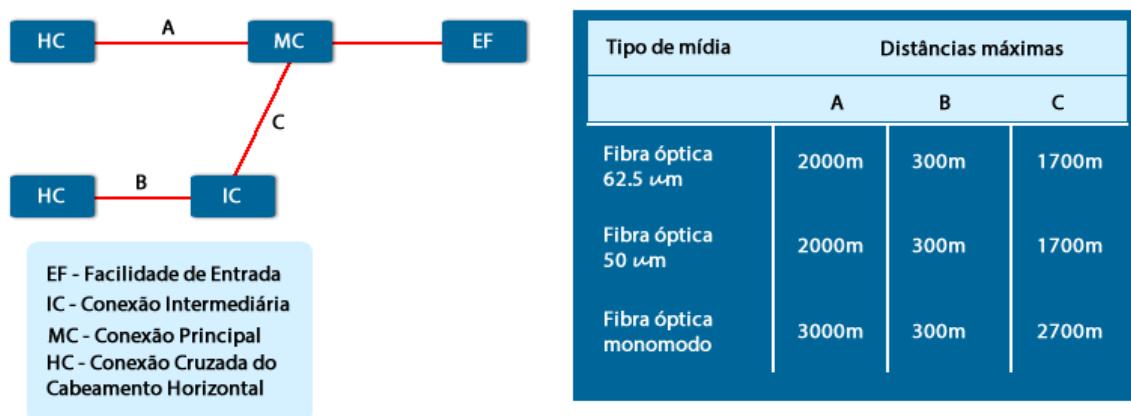
## 2.2 Cabeamento Vertical / Rede Primária

O cabeamento vertical é aquele realizado entre os andares ou edificações de uma empresa e são os cabos utilizados entre as salas de telecomunicações, entrada de serviços de telecomunicações (EF), salas de equipamentos, incluindo todos os cabos, terminações de cabos e conexões cruzadas de cabeamento horizontal (HC), conexões intermediárias (IC) e conexões principais (MC).

Os padrões normalmente especificam uma topologia hierárquica em estrela para o cabeamento de backbone, onde todo cabeamento irradia de um ponto central chamado "main cross-connect" ou conexão principal, normalmente uma sala de telecomunicações. Toda sala de telecomunicações ou entrada de serviços de telecomunicações é cabeada diretamente à conexão principal ou via uma conexão intermediária.

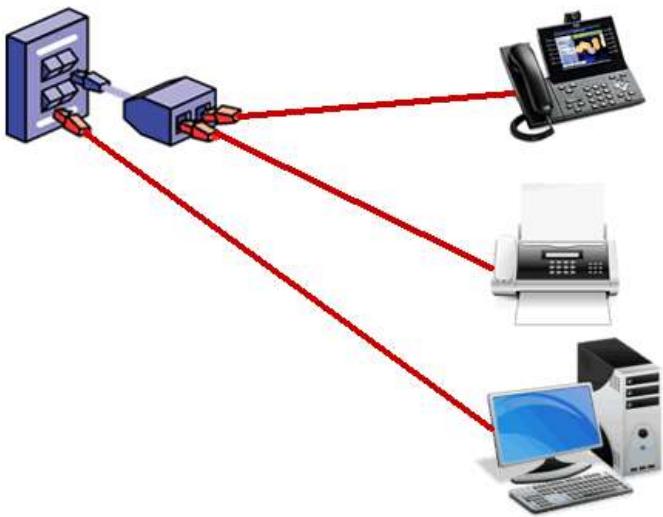


O limite de distância do cabeamento depende do tipo de cabo e facilidades de conexão, por exemplo, o UTP (par trançado) tem uma limitação de 100m, porém pela norma recomenda-se um limite de 90 metros.



## 2.3 Área de Trabalho

A área de trabalho, como o nome sugere, é a área onde os funcionários da empresa interagem com seus equipamentos de informática com acesso à rede e telecomunicações, incluindo todos os cabos e componentes entre as tomadas de telecomunicações e os equipamentos dos usuários, como por exemplo, telefones, aparelhos de fax, impressoras, computadores e a própria tomada de telecomunicação.



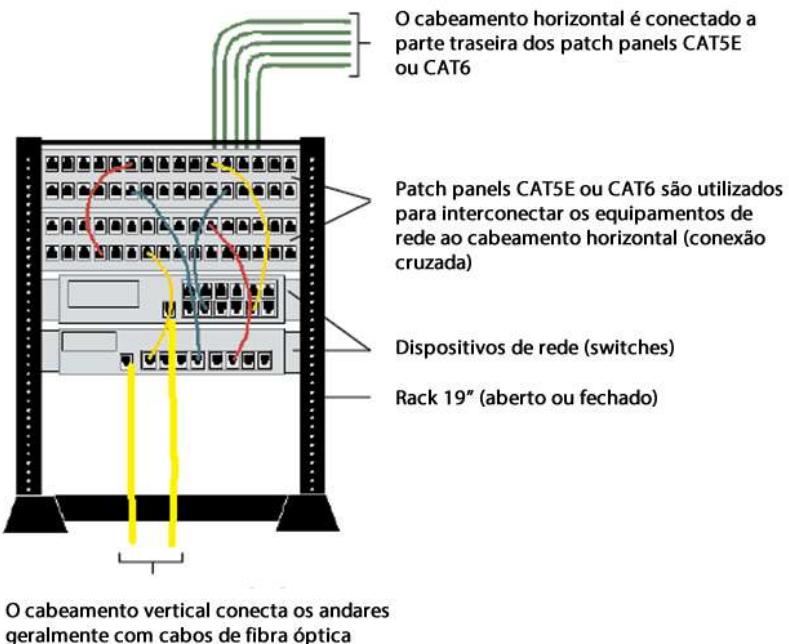
O cabeamento da área de trabalho deve ser projetado para ser flexível, porém requer um cuidado especial. O padrão T568B é o mais comum para aplicações de dados e no caso da utilização de voz convencional (análogica) é necessário dedicar dois pontos de rede na tomada de telecomunicações, uma para voz e outro para dados.

Com a tendência crescente da convergência de redes e o uso da telefonia IP, muitas vezes apenas um ponto de rede por tomada de telecomunicações é necessário. Isso é possível porque a maioria dos modelos de telefone IP possuem um switch interno capaz de separar a voz sobre IP (que vem em uma VLAN de voz) da parte de dados (que vem em uma VLAN de dados). Nesse telefones teremos dois conectores RJ-45, onde em um deles o switch é conectado e no outro conectamos o computador.



## 2.4 Sala de Telecomunicações

A sala de telecomunicações é um ambiente fechado, o qual pode ser uma sala ou apenas um rack, onde os equipamentos de telecomunicações, quadros de distribuição, terminações de cabos e conexões cruzadas serão acondicionados. Em outras palavras, onde ficará todo hardware para conectar o cabeamento horizontal ao cabeamento vertical. Em inglês esta área também pode receber o nome de “wiring closet”.



Além dos equipamentos de rede, na sala de telecomunicações podem estar instalados equipamentos auxiliares, por exemplo, servidores locais de arquivo.

É recomendado que as edificações tenham pelo menos uma sala de telecomunicações e a recomendação da norma do cabeamento estruturado diz que é necessário um por andar. Existem também recomendações sobre a área necessária para a sala de telecomunicações dependendo da área de serviço a ser atendida, além disso, essa sala deve ter espaço suficiente para que o pessoal técnico realize manutenções ou suas tarefas relacionadas ao gerenciamento desse cabeamento assim como espaço para todo hardware que será instalado. Veja a tabela seguinte com algumas especificações de tamanho de sala de telecomunicações.

Área a ser servida	Tamanho mínimo da sala de telecomunicações
até 500m <sup>2</sup>	3.0m x 2.2m
de 500m <sup>2</sup> a 800m <sup>2</sup>	3.0m x 2.8m
de 800m <sup>2</sup> a 1000m <sup>2</sup>	3.0m x 3.4m

Outros itens que devem ser considerados são a iluminação do ambiente, alimentação e condições de temperatura e umidade relativa do ar para que os equipamentos de rede e o cabeamento consigam operar corretamente e o ambiente esteja de acordo com os padrões estabelecidos pelas normas.

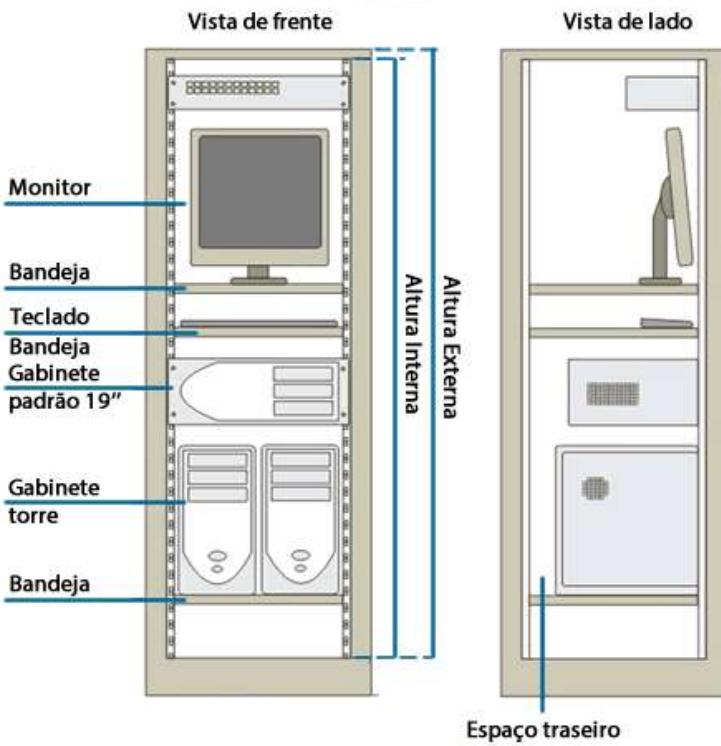
Voltando a primeira figura desse tópico, onde temos o rack 19" (dezenove polegadas) note que os equipamentos de rede e patch panels estão afixados nele. Os racks são estruturas metálicas utilizadas tanto nas salas de telecomunicações como na sala de equipamentos e entrada de facilidades para que os dispositivos de rede, servidores, nobreaks e equipamentos possam ser fixados de maneira segura e organizada. Os racks podem ser abertos, podendo ser em colunas, ou fechados e que possibilitam a restrição de acesso aos equipamentos com chaves, como mostrado abaixo.



O termo dezenove polegadas se refere à largura do rack, existem outras larguras como o de 23 polegadas, mas a medida de dezenove é a mais comum para equipamentos de rede.

Para dimensionar os racks deve-se escolher a largura correta (depende do padrão de equipamento de rede ser de 19" ou 24", por exemplo) e a altura do rack é dimensionada pela soma da altura dos equipamentos de rede. A altura dos equipamentos (distância entre os furos de fixação do rack) é chamada de "U" ou "Unidade de Rack" (Rack Unity – RU). A altura de 1U tem aproximadamente 4,5cm e praticamente todos os equipamentos de redes estruturadas são construídos de acordo com estas medidas.

Por exemplo: você irá instalar uma régua de tomadas de 1U, um patch panel de 2Us, uma guia de cabos horizontal de 1U, um switch de 1U e uma bandeja fixa de 1U, portanto o rack precisará de no mínimo 6 Us de altura. Veja a figura seguinte com um projeto de ocupação de rack.



A fixação dos equipamentos no rack é feita com as "porcas gaiolas" e parafusos para fixação dos dispositivos, veja o detalhe abaixo.



Os equipamentos que são menores que 19 polegadas podem ser acomodados em bandejas que podem ser fixas ou deslizantes (possuem um trilho e você pode puxá-la para fora do rack).



## 2.5 Sala de Equipamentos

A sala de equipamentos é o local onde ficam armazenados os sistemas de telecomunicações como PABX, servidores, roteadores, switches de distribuição/core, sistemas de monitoração de vídeo e alarmes, bem como as terminações do cabeamento vertical.

Apesar de soar semelhante a uma sala de telecomunicações, a sala de equipamentos é considerada diferente pela complexidade dos equipamentos de telecomunicações e redes que ficam alocados nela.

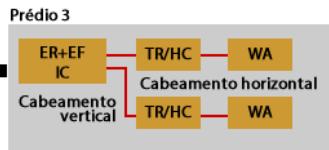
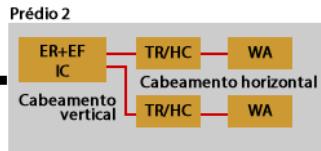
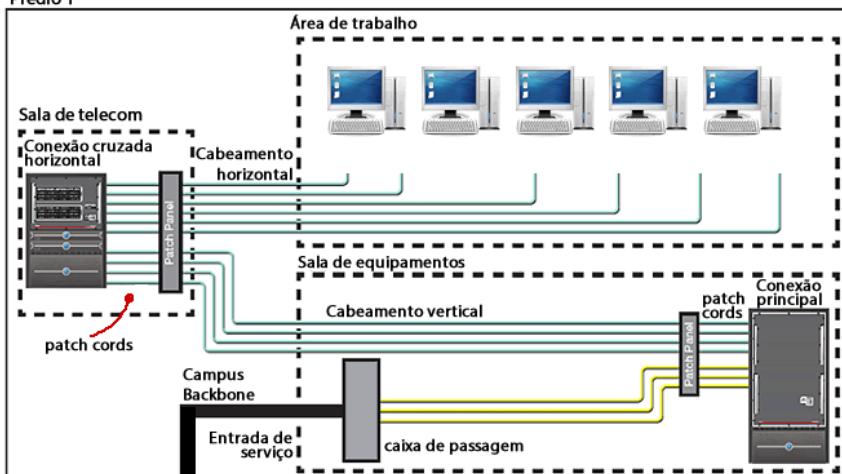


A sala de equipamentos pode estar acomodada juntamente com uma sala de telecomunicações, em um mesmo andar, por exemplo, ou estar em um ambiente separado. A sala de equipamentos fornece o ponto de terminação para o cabeamento vertical (backbone) que está conectado a uma ou mais salas de telecomunicações, podendo ser também a conexão principal (main cross-connect) para todos os andares de uma edificação.

Em um ambiente de Campus (vários prédios) cada prédio deve ter sua própria sala de equipamentos, na qual as salas de telecomunicações locais serão interconectadas, sendo que esta sala de equipamentos deve ser conectada a uma entrada de serviços central do campus que terá a função de conexão principal para todos os prédios desse ambiente.

Veja a figura seguinte onde temos três prédios, sendo que o Prédio 1 é o que tem a conexão central do backbone do Campus. Temos algumas siglas que significam: ER – Equipment Room ou sala de equipamentos, TR – Telecom Room ou sala de telecomunicações, WA – Work Area ou área de trabalho. Os demais termos já foram apresentados nos tópicos anteriores desse capítulo. A caixa de passagens é onde as fibras ópticas que ligam os prédios do campus estão sendo conectadas (emendadas ou fundidas). Note que nos prédios 2 e 3 a sala de telecomunicações e a sala de equipamentos estão sendo colocadas em um mesmo ambiente.

Prédio 1



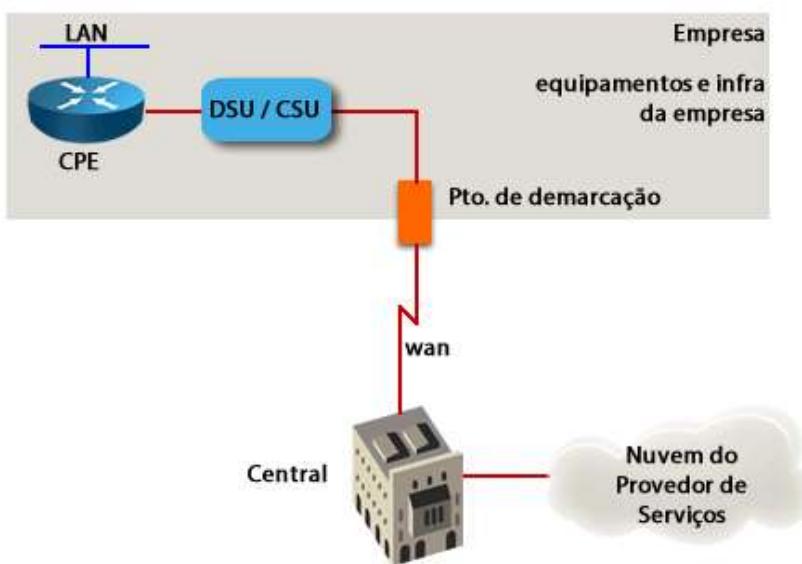
O tamanho mínimo de uma sala de equipamentos deve ser de 14 m<sup>2</sup> e a tabela abaixo mostra os padrões de dimensões baseados no padrão vigente.

Quantidade de área de trabalhos	Área (m <sup>2</sup> )
até 100	14
de 101 a 400	37
de 401 a 800	74
de 801 a 1200	111

## 2.6 Sala de Entrada de Serviços de Telecomunicações

A sala de entrada de serviços de telecomunicações é onde fica o ponto de conexão dos equipamentos e cabos das prestadoras de serviço de telecomunicações e também pode acomodar as conexões que vêm dos demais prédios do Campus, servindo como ponto central para interconexão entre os diversos prédios do campus.

O ponto onde as empresas provedoras de serviço de Telecom entregam seus links, circuitos e demais produtos de comunicação é chamado de “ponto de demarcação” ou “demarcation point”. Normalmente o ponto de demarcação deve seguir padrões mínimos estabelecidos pelos provedores de serviços de telecomunicações com relação a espaço, tipo de entrada dos cabos no prédio, etc. Além disso, a parte interna é na grande maioria das vezes responsabilidade da empresa, sendo que a provedora de serviços de Telecom se responsabiliza pela infraestrutura até o ponto de demarcação.



Normalmente nessa sala são entregues os circuitos de voz, que podem ser analógicos (2 fios) ou digitais (E1 – cabo coaxial), links de Internet (UTP RJ-45 ou cabos seriais V.35), links seriais para outras unidades (cabos V.35) ou até Data Centers onde servidores da empresa (alguns ou em muitas vezes todos) estão hospedados.

Em alguns casos, a sala de equipamentos e a sala de entrada de serviços de Telecom podem estar compartilhando o mesmo ambiente para facilitar a conexão com os equipamentos de voz (PABX e Gateways de Voz) e dados (roteadores e switches).

## 2.7 Administração do Cabeamento

O processo de administração inclui todos os aspectos relacionados ao cabeamento e sua infraestrutura, tais como documentação, gerenciamento e testes no sistema, assim como elaborar e manter diagramas (plantas) com a arquitetura do sistema de cabeamento como um todo.

A documentação é parte fundamental e deve iniciar no projeto do sistema de cabeamento e ser atualizado ao final da instalação com possíveis alterações e adaptações que foram realizadas durante o processo de instalação do cabeamento. É importante utilizar uma nomenclatura padrão, assim como identificar equipamentos, cabos, pontos de rede e assim por diante, para que a manutenção ou ampliação do sistema seja simplificada.

### 3 Conceitos Básicos sobre Infraestrutura Elétrica de Redes

A norma brasileira **ABNT NBR 5410:2004 Versão Corrigida:2008** - "Instalações Elétricas de Baixa Tensão", fixa as condições que as instalações de baixa tensão devem atender, a fim de garantir seu funcionamento adequado, a segurança das pessoas e animais domésticos e a conservação de bens. Portanto, esta norma deve ser observada também para a parte elétrica de redes de computadores, informática e telecomunicações nas empresas comerciais.

Esta norma é aplicada desde instalações novas até reformas em instalações existentes - considerando como "reforma" qualquer ampliação de instalação existente (criação de novos circuitos, alimentação de novos equipamentos e etc.), bem como qualquer substituição de componentes que implique alteração de circuitos.

O objetivo desse tópico não é ensinar conceitos básicos de eletricidade, corrente contínua ou alternada e sim mostrar uma visão bastante prática sobre os dispositivos que utilizamos na infraestrutura elétrica das redes e alguns dispositivos que usamos em nossas residências para manter nossos computadores e demais dispositivos de redes energizados de maneira segura.

Mesmo em empresas de pequeno porte, o investimento em equipamentos de rede, servidores, computadores instalados, além do valor de toda informação contida nesses computadores, banco de dados e demais sistemas de informação, normalmente são valores altos e muitas vezes até difíceis de mensurar.

Por isso, o cuidado com a energização dos equipamentos de redes e TI em geral deve ser tão grande, pois a rede elétrica, salvo raras exceções, pode apresentar flutuações nos níveis de energia, quedas, sobretensões, surtos causados por descargas atmosféricas (raios) e tudo isso pode danificar os equipamentos de telecomunicações, de redes e os próprios endpoints.

Por exemplo, separar os circuitos das tomadas elétricas dos circuitos de iluminação, do circuito de sistemas de ar condicionado, e assim por diante, é uma medida útil para prevenir que comportamentos de carga diferentes influenciem o funcionamento dos equipamentos de transmissão. Além disso, para tudo isso estar funcionando adequadamente, o aterramento de todo o sistema deverá estar devidamente instalado e testado, respeitando valores padrões de segurança.

Lembre-se que a transmissão de dados em meios metálicos se dá através de zeros e uns, que nada mais são que níveis elétricos de tensão, os quais podem ser facilmente "distorcidos" por um ruído provocado por uma instalação elétrica mal planejada ou um aterramento mal feito.

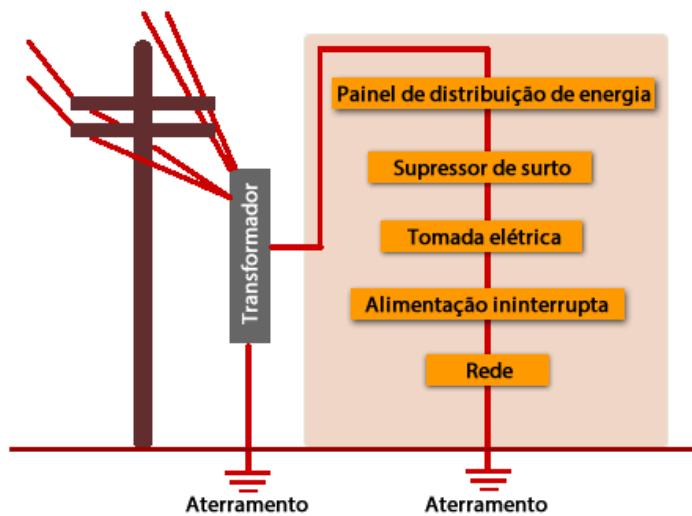
Basicamente, para instalação da parte elétrica de telecomunicações e informática de uma empresa deve-se ter cuidado com a alimentação de entrada da companhia de energia elétrica, pois ela pode variar ou faltar em determinados períodos do dia.

Além disso, as redes elétricas podem contar com protetores contra surtos de tensão, disjuntores e filtros de linha para proteger sua rede contra os problemas nas redes de distribuição elétrica.

Veja a figura seguinte com uma entrada elétrica típica de uma empresa com dispositivos de rede e telecomunicações. Nesse exemplo temos a nossa rede interna conectada à rede elétrica por um painel de distribuição de energia, o qual se conecta a um supressor de surtos, em seguida é ligado a uma tomada que se conecta a uma fonte estabilizada de energia, que pode ser um no-break, para daí ser distribuído aos dispositivos de rede e demais elementos que devem ser conectados à mesma fonte de energia.

É importante notar o aterramento, o qual veremos a seguir que deve seguir padrões e medidas para que o ruído gerado e muitos outros problemas sejam minimizados. Nesse exemplo foi

utilizado um circuito ou ramal separado para a parte dos dispositivos de rede, telecomunicações e informática.



A maioria dos fabricantes de equipamentos de rede, tais como roteadores e switches, permitem a escolha de corrente contínua (DC) ou corrente alternada (AC), porém a maioria das empresas opta pela corrente alternada por necessitar de menos equipamentos e ser mais usual, reduzindo custo de operação e manutenção da rede elétrica como um todo.

### 3.1 Cuidados ao Energizar os Equipamentos – 127V ou 220V?

Lembrem que a tensão alternada na maioria dos estados brasileiros pode ser de 127 Volts (127V) ou 220V.

Nota: muitas vezes a tensão de 127V é denominada de 110V, mas isso é um erro, pois este nível de tensão não é normatizado.

Aqui vem um ponto de atenção importante, ao ligar os equipamentos na rede elétrica devemos ficar atentos para a tensão correta, pois um equipamento de 127V ligado em uma tomada de 220V será danificado. O dano causado poderá ser de apenas ter um fusível de proteção queimado, uma fonte de alimentação queimada ou até mesmo circuitos internos importantes que podem levar a perda total do equipamento.

Muitos equipamentos de rede já são bivolts, ou seja, suportam de 127V a 220V, não importando o tipo de tomada que você o conecte. Normalmente essa informação estará atrás ou embaixo do equipamento, se ele utilizar fonte externa a informação estará na fonte. Veja as fotos onde mostramos a indicação das voltagens permitidas por um switch Catalyst 2950 do fabricante Cisco.



Por esse motivo é importante que se múltiplas tensões forem ser utilizados em uma instalação elétrica as tomadas devem ser identificadas. Na dúvida, utilize um multímetro para fazer a medição da tensão da tomada.



Para realizar a medição, em primeiro lugar você deve identificar no multímetro a escala de Tensão Alternada (AC), a qual pode ser identificada através das siglas VCA, ACV ou VAC. Além disso, pode aparecer através do símbolo V~ como encontramos na foto anterior.

Dentro da Escala de Tensão Alternada (AC) teremos os números 200 que mede até 200V e 500 que mede até 500V. Se estiver na dúvida de qual tensão se encontra na sua tomada posicione o multímetro em 500, pois caso seja 220V você corre o risco de danificar o multímetro. Para realizar a medição basta fazer como na figura abaixo, inserindo as pontas de prova nos pinos vivos da tomada e verificando o valor mostrado no display.



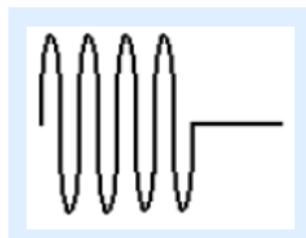
### 3.2 Principais Problemas da Rede Elétrica

Devemos ter em mente que a rede elétrica fornece energia para a utilização de qualquer tipo de carga, seja ela doméstica ou industrial. Tal integração de cargas de pequeno e grande porte pode produzir oscilações e instabilidades na rede elétrica, gerando distúrbios que podem provocar danos muitas vezes irreversíveis a equipamentos e cargas sensíveis.

Aqui o termo **carga** utilizado refere-se aos dispositivos elétricos e eletrônicos que serão conectados à rede, tais como os computadores, roteadores, switches, uma televisão ou um forno de micro-ondas, ou seja, qualquer dispositivo de uso residencial, comercial ou industrial.

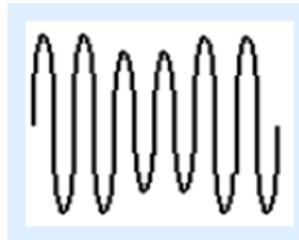
Vamos agora estudar os seis principais tipos de distúrbios presentes na rede elétrica que frequentemente afetam cargas críticas como, por exemplo, equipamentos de informática, hospitalares, industriais e eletrônicos em geral.

- **TIPO 1- Falta de Rede:** Nessa situação a energia é totalmente interrompida, produzindo o desligamento da carga. Geralmente provocada pela atuação nas proteções do sistema de distribuição em função de sobrecargas, descargas atmosféricas, dentre outros motivos, até mesmo acidentes de trânsito. Note na figura a seguir a tensão alternada é formada por uma onda senoidal que desaparece quando a energia é interrompida. A interrupção da energia em uma rede de computadores pode provocar desde a perda de informações até corrupção de bancos de dados.



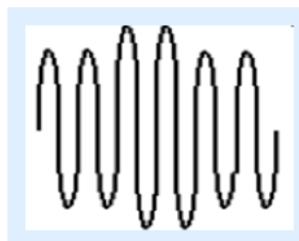
Tipo 1

- **TIPO 2 - Subtensão:** Queda momentânea no valor da tensão da rede elétrica, ou seja, a tensão fica menor que a esperada. É o distúrbio mais comum encontrado nos sistemas de distribuição, correspondendo a aproximadamente **85% das falhas**. Provocado basicamente pela partida de cargas de grande porte, por exemplo, quando um grande motor elétrico ou dispositivo de grande porte é ligado.



Tipo 2

- **TIPO 3 - Sobretensão:** É a situação oposta da anterior, nessa situação ocorre a elevação momentânea no valor da tensão da rede elétrica, ou seja, a tensão fica maior que a esperada. Pode ocorrer no retorno da energia após uma interrupção, ou seja, quando a energia volta após uma queda, ou também por descargas atmosféricas (raios).



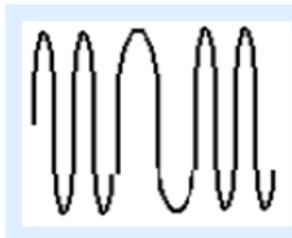
Tipo 3

- **TIPO 4 - Surto de Tensão:** São transientes (picos) rápidos e de elevada energia, podendo atingir valores na ordem dos **kiloVolts** (maior que 1000 Volts), esse é o distúrbio potencialmente mais perigoso para a carga. Ocorre com maior frequência no verão, devido ao aumento na ocorrência de descargas atmosféricas próximas a rede elétrica, não sendo suprimidos pelas proteções do sistema de distribuição.



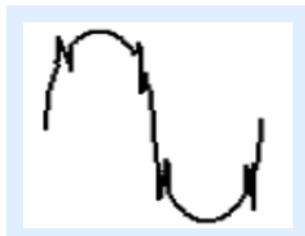
Tipo 4

- **TIPO 5 - Variação de Frequência:** Variações de frequência na rede elétrica também são comuns e provocadas por variações bruscas de cargas de grande porte ou mesmo curto-circuito na rede elétrica. A variação de frequência pode provocar mau funcionamento, superaquecimento e até mesmo a queima de equipamentos e componentes eletrônicos. Nota: Na maioria dos países da América, inclusive Brasil e EUA, a frequência da rede elétrica é de 60 Hz. Na Europa, inclusive em Portugal, é usada a frequência de 50 Hz. A frequência de 50 Hz também é usada em alguns países da América do Sul, como por exemplo a Argentina, a Bolívia, o Chile e o Paraguai.



Tipo 5

- **TIPO 6 - Ruído:** A presença de ruídos de alta frequência na rede elétrica pode provocar interferência e mau funcionamento em equipamentos eletrônicos, industriais e também em sistemas de telecomunicação. São produzidos por geradores, fontes chaveadas, motores, sistemas de controle antiquados e de baixa qualidade, entre outros.



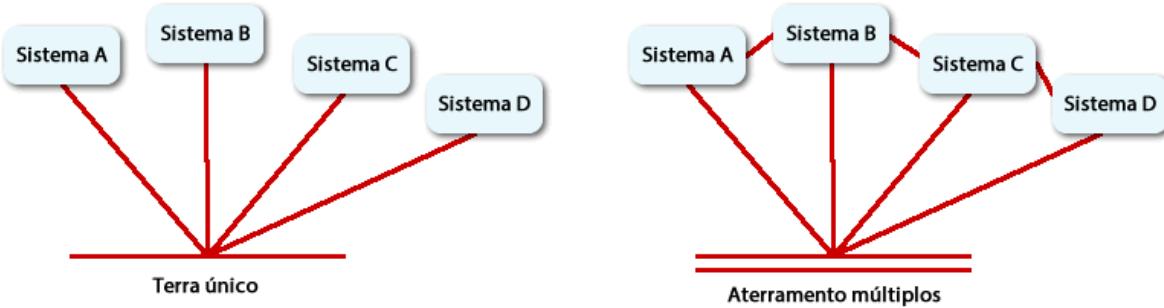
Tipo 5

### 3.3 Aterramento

Todas as tomadas elétricas de um sistema de alimentação de rede devem possuir um único ponto de terra comum. Os sistemas elétricos para redes de computadores utilizam três fios com cores padronizadas:

- Fase (Branco / Vermelho / Preto)
- Neutro (Azul)
- Terra (Verde)

Um aterramento bem feito é crucial para as instalações elétricas de redes, informática e telecomunicações, pois vários problemas em transmissão de dados são decorrentes de correntes elétricas espúrias, ou seja, correntes elétricas geradas por diferenças de potenciais quando são utilizados diversos pontos de **aterramento** isolados na rede. Por isso, o terra deve ser único ou ligados em multiponto, porém com a mesma referência de terra.



Outra finalidade do aterramento nos equipamentos eletrônicos em geral é evitar que estruturas metálicas expostas, tais como os gabinetes de computadores, chassi de roteadores e switches, até mesmo os racks, se energizem com uma tensão que gere risco aos usuários e administradores de rede, o que pode ocorrer devido a uma falha interna desses dispositivos.

### 3.4 Filtros de Linha

Filtro de linha é o nome que se dá ao protetor contra surtos (problema tipo 4 analisado anteriormente) no Brasil e em muitos países de língua portuguesa, em inglês é chamado de "**surge protector**". Sua função é a proteção de computadores e equipamentos eletrônicos em geral através do uso de componentes como varistores, fusíveis térmicos, bobinas, etc.

Os MOVs (varistores) são os componentes principais de proteção. Sua função é direcionar os surtos de tensão para o aterramento.

Uma proteção contra surtos tem dois modos de operação:

1. **Modo Diferencial:** é o mais importante por lidar com surtos entre fase e neutro, que são aqueles que estão presentes na rede elétrica o tempo todo. Nenhuma necessidade de aterramento se faz nesse tipo proteção. Tais surtos ocorrem quando o liquidificador é ligado, quando a batedeira de bolo é ligada, quando a madeireira da esquina aciona seus motores, etc., podendo danificar equipamentos eletrônicos quando atingem um patamar elevado ou de maior duração.

**2. Modo Comum:** atua contra as descargas elétricas e apenas nesse caso deve ter uma via de escoamento da energia extra, que é o fio terra. Nem o protetor sozinho dá proteção eficiente contra raio, nem o aterramento dará proteção sem o protetor contra surtos.

Além de remover ruídos e picos de tensão, os filtros de linha têm outras finalidades básicas. Por exemplo, ele expande o número de tomadas disponíveis perto de um computador ou de equipamentos de áudio/vídeo e protege contra curtos-circuitos e sobrecarga de tensão. Isso é possível porque a maioria dos filtros de linha possui um disjuntor (ou fusível) responsável por desligar a alimentação elétrica, caso a corrente total exigida pelo equipamento seja maior do que a corrente rotulada. No caso de dispositivos protegidos por fusível, em caso de sobretensão, esse se funde, sendo necessária sua substituição para que o filtro de linha volte a funcionar corretamente.

Procure adquirir os filtros de linha que possuem varistores, pois eles são mais eficientes na proteção contra surtos de tensão (picos). Se na caixa do produto ou em suas especificações técnicas estiver escrito algo como "L-N, L-G, N-G", isso significa que o filtro de linha tem pelo menos três varistores, ou peça para seu fornecedor filtros com varistores. Lembre que quanto melhor o filtro de linha, ou seja, quanto mais recursos de proteção mais caro ele será.

Veja abaixo a foto de um filtro de linha do fabricante APC, porém no modelo de tomada com pinagem antiga, e ao lado temos um filtro de linha do fabricante Clone com tomadas no modelo atual de pinagem.



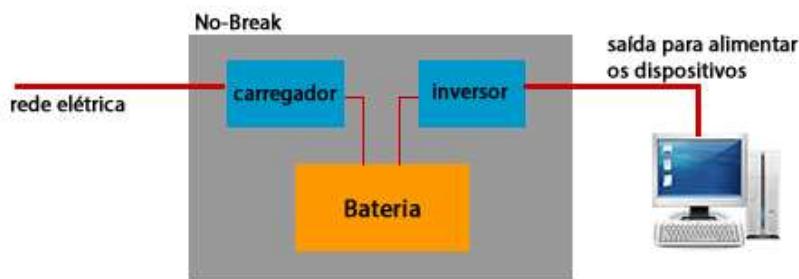
No momento de adquirir um filtro de linha ou régua de tomadas (PDU) para um rack é importante lembrar-se dos padrões de tomadas e muitas vezes serão necessários adaptadores para que os equipamentos possam ser conectados à rede elétrica.

### 3.5 No-break ou UPS

O No-Break ou UPS (Uninterruptible Power Supply ou Fonte Ininterrupta de Energia) tem a função de proteger e manter os equipamentos eletrônicos alimentados quando ocorrerem falhas no fornecimento rede de distribuição elétrica, permitindo que os usuários de redes de computadores possam salvar e fechar os arquivos e programas em utilização.

Alguns tipos de no-break conseguem manter os dispositivos energizados por 15 a 20 minutos, porém, existem modelos que possibilitam uso por algumas horas ininterruptas no caso de falta da energia elétrica.

Um no-break é formado de maneira geral por baterias, um carregador de baterias e um inversor/retificador de energia.

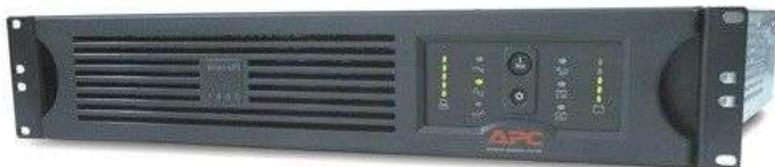


O Inversor é um circuito interno que transforma a tensão das baterias, a qual é contínua, em tensão alternada. Já o Retificador transforma a tensão alternada da rede elétrica em tensão contínua, com finalidade de alimentar o inversor.

O carregador de bateria é projetado para manter as baterias em condição de pico durante os períodos em que o sistema da linha de alimentação estiver funcionando normalmente, pois assim teremos a garantia que na falta de energia tenhamos as baterias em perfeito estado para manter os dispositivos energizados pelo tempo esperado. É importante lembrar que as baterias têm uma vida útil portanto, no caso do uso de no-breaks é importante verificar o estado de conservação das baterias e respeitar o prazo de validade delas.

O UPS (no-break) pode possuir uma ou várias baterias, que são utilizadas quando um circuito eletrônico identifica a interrupção de energia e começa a alimentar automaticamente o equipamento. Geralmente, quanto maior for a capacidade da bateria em um UPS, maior o período de tempo em que ela poderá suportar os dispositivos de rede durante faltas de energia.

Veja a figura abaixo com o exemplo de um no-break de rack do fabricante APC. Existem modelos de no-break tanto para rack padrão 19 polegadas, como no-breaks do tipo torre, conforme figura 3 ao lado. Além disso, alguns modelos podem ser rack ou torre, podendo ser montado conforme necessidade do projeto.



### 3.5.1 Tipos de No-Break

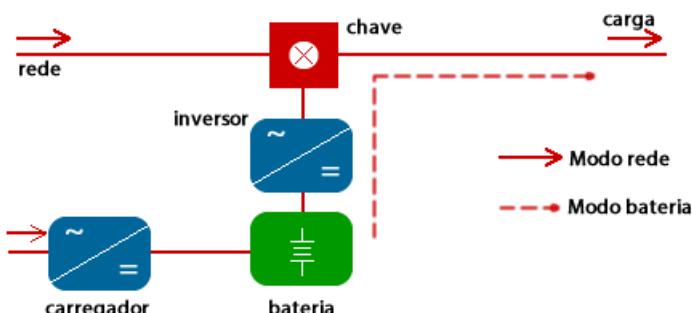
A norma que regulamenta os tipos de no-breaks no Brasil é a **NBR 15014** "Conversor e semicondutor – Sistema de alimentação de potência ininterrupta, com saída em corrente alternada (*no-break*) – Terminologia" foi editada em Dezembro de 2003, porém somente entrou em vigor a partir de 30.01.2004 em substituição a norma NBR 11875:1991.

Seu principal objetivo é definir os termos e definições para sistemas de alimentação de potência ininterrupta, os *no-breaks*. Além de apresentar as topologias, essa norma também apresenta os principais termos que descrevem as características técnicas dos *no-breaks*, como por exemplo, as definições de retificador, inversor, tempo de transferência, tempo de recarga, entre outros.

Hoje em dia, existem muitos fabricantes que, por não atenderem às normas vigentes, criam terminologias próprias para os seus equipamentos. Podemos citar os termos "tripla conversão", "Semi On-Line", "Semi-Senoidal" entre outros.

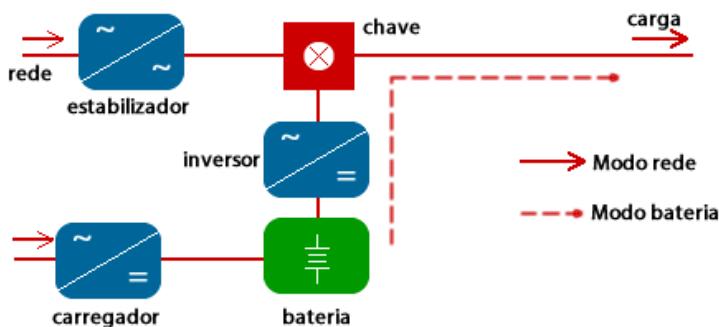
De acordo com a **NBR 15014**, os no-breaks são classificados três classes distintas:

1. **No-break Stand-By**: Existem duas condições de operação, definidas pela situação da rede de alimentação. A primeira enquanto a rede está presente, a chave é mantida fechada, ou seja, a carga (equipamentos conectados ao no-break) permanece alimentada pela rede elétrica, onde a tensão e a frequência de saída são totalmente dependentes da tensão e frequência de entrada. Essa topologia fornece proteção à carga para os três primeiros distúrbios da rede elétrica apresentados, porém por não possuir capacidade de estabilização, gera frequentes processos de carga e descarga das baterias, reduzindo drasticamente a sua vida útil. Para os outros três distúrbios, essa topologia não oferece proteção, expondo a carga a um risco muito elevado.



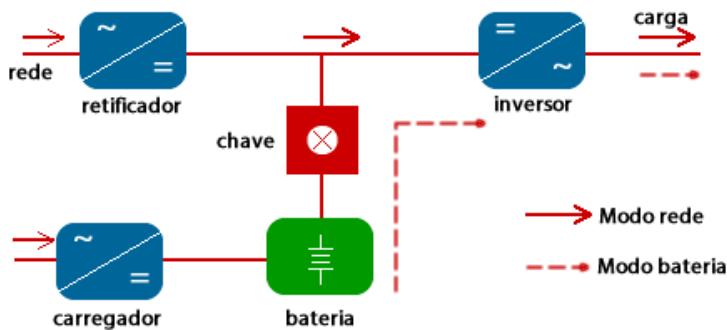
Topologia Stand-By

2. **No-break Interativo**: nesse modelo de no-break a estrutura interna é muito semelhante à topologia Stand-By, existindo forte dependência da saída em relação a entrada. Essa topologia oferece proteção não só contra a falta de rede, mas também às variações de amplitude da tensão de entrada, abrangendo os três primeiros distúrbios apresentados. Mesmo a tensão de saída sendo estabilizada, o processo de estabilização demanda certo tempo mantendo a carga exposta a variações bruscas da rede elétrica e também permanecendo vulnerável a variações de frequência, ruídos e surtos de tensão. Enquanto a rede está presente a chave permanece fechada, sendo a carga alimentada pela rede elétrica. Dessa forma, cargas com baixo fator de potência poderão produzir tarifações e multas, além de provocar distorções na rede elétrica e interferência em outros equipamentos. Existem três tipos de no-break interativos, o Interativo Convencional (veja figura abaixo), Interativo Ferroresonante e Interativo de Simples Conversão.



Topologia Interativo Convencional

3. **No-Break On-line:** chamado também de UPS Contínuo, é ligado em série com a rede elétrica, atuando não somente como uma proteção contra a falta de energia, mas também como um "estabilizador" para a tensão de saída que é fornecida aos dispositivos eletrônicos nele conectado. Esta é a única topologia de no-break que protege a carga contra os seis principais distúrbios da rede elétrica estudados anteriormente, sempre fornecendo uma tensão senoidal na saída, além de não apresentar interrupção nas transferências de carga, ou seja, na topologia On-Line o inversor é responsável por 100% da potência fornecida à carga por 100% do tempo de operação.



Topologia On-Line de Dupla Conversão

Os no-breaks do tipo Interativo e Stand-by muitas vezes são chamados de off-line, pois o inversor somente entra em ação se a rede elétrica principal ficar indisponível.

A escolha do modelo de no-break a ser utilizado depende de questões financeiras e da quantidade de equipamentos que devem ser conectados a ele. Os no-breaks off-line são mais baratos que o on-line, porém os on-line protegem melhor os dispositivos nele conectados. Portanto a questão custo deve ser analisada levando-se em conta "**Que dispositivos devem ser protegidos?**", pois dependendo do custo total da danificação dos dispositivos a serem protegidos o custo do no-break on-line pode se tornar razoável.

Outro fator que determina não somente o tipo, mas também o tamanho do no-break, ou seja, é a soma da potência dos dispositivos que ele deve proteger, pois o dimensionamento da carga que um no-break deve suportar depende de quantos equipamentos iremos conectar ao no-break e da soma potência de cada dispositivo.

Nesse ponto do dimensionamento da potência cuidado com as unidades utilizadas, pois o no-break tem sua potência calculada em VA (Volt-Ampere) e maioria dos equipamentos tem sua potência calculada em Watts (W), as quais não são totalmente compatíveis. A capacidade em VA é igual ao fornecimento em watts apenas em situações onde são ligados dispositivos com carga 100% resistiva, como por exemplo, as lâmpadas incandescentes e aquecedores. Sempre que são incluídos componentes indutivos ou capacitivos, como no caso das fontes de computadores e dispositivos de rede, a capacidade em watts é calculada multiplicando a capacidade em VA pelo **fator de potência da carga**, sendo que a maioria das fontes de alimentação trabalha com fator de potência de 0.65 ou 0.7.

Em dispositivos de rede muitas fontes de alimentação tem um dispositivo chamado "power factor correction" (PFC – circuito de correção de fator de potência), o qual faz a correção do fator de potência para muito próximo de 1, portanto fazendo com que o valor em VA seja praticamente o mesmo fornecido pelo fabricante em Watts nas especificações dos equipamentos. O fabricante Cisco, por exemplo, cita que fontes de seus equipamentos que tenham consumo 75W ou acima possuem o PFC já embutido (built-in) em suas fontes de alimentação.

*Nesse capítulo vamos estudar as tecnologias sem fio utilizadas em redes LAN para permitir que computadores accessem a rede via interface aérea, independente de localização física ou cabos.*

*As tecnologias sem fio utilizadas em redes LAN fazem parte da família 802.11, sendo que vários padrões foram criados e outros devem vir no futuro para atender à crescente demanda por largura de banda que os acessos às redes locais exigem.*

*Bons estudos.*

## **Capítulo 08 - Implementando Redes sem Fio**

### **Objetivos do Capítulo**

Ao final desse capítulo você deve ter estudado e estar familiarizado com os seguintes assuntos:

- Descrever os fundamentos de wireless;
- Descrever as topologias de wireless possíveis de serem utilizadas;
- Conhecer os princípios de RF e suas métricas;
- Descrever e saber a diferença dos tipos de antenas utilizadas em LANs sem fio;
- Descrever o funcionamento das tecnologias spread spectrum;
- Conhecer os órgãos reguladores, normas, certificações e tecnologias wireless da família 802.11.

## Sumário do Capítulo

<b>1 Fundamentos de Wireless</b>	<b>254</b>
<b>2 Tipos de Redes Sem Fio</b>	<b>257</b>
2.1 Wireless Personal Area Network	258
2.2 WLAN (Wireless Local Area Network)	258
2.3 WMAN (Wireless Metropolitan Area Network)	259
2.4 WWAN (Wireless Wide Area Network)	259
<b>3 Modos de Operação de uma WLAN – Ad-hoc e Infraestrutura</b>	<b>260</b>
3.1 Arquiteturas WLAN Ad-Hoc	260
3.2 Arquiteturas WLAN Infraestrutura	261
3.2.1 BSS - Basic Service Area	262
3.2.2 ESS - Extended Service Areas	262
3.2.3 Outros Modos de Operação dos APs	266
<b>4 Princípios de Funcionamento de uma Rede Wireless</b>	<b>267</b>
4.1 Técnicas de Modulação – Enviando um Bit via RF	267
4.2 Problemas Típicos das Transmissões em Redes sem Fio	270
4.2.1 Perda no Espaço Livre	271
4.2.2 Perda por Penetração ou Absorção	271
4.2.3 Reflexão	272
4.2.4 Refração	272
4.2.5 Espalhamento do sinal	273
4.2.6 Propagação Multicaminhos ou Multipercursos	274
4.2.7 Linha de Visada e Zona de Fresnel	275
4.2.8 Relação Sinal Ruído (SNR) e Força do Sinal Recebido (RSSI)	276
4.3 Principais Tipos de Antenas	278
4.3.1 Antenas Omnidirecionais	280
4.3.2 Antenas Direcionais	281
4.3.3 Conectores e Cabos	284
4.4 Tecnologia MIMO	285
4.5 Funcionamento Básico do CSMA-CA	286
4.6 Descobrindo uma Rede sem Fio (Scan)	286
4.7 Autenticação, Criptografia e Associação de Clientes	288

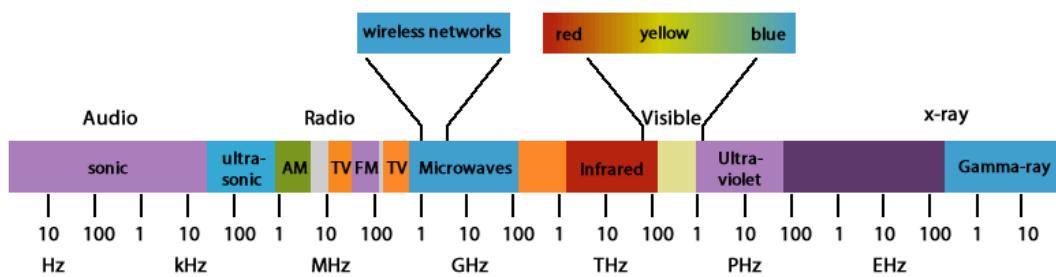
4.7.1 Associação	289
<b>5 Tecnologias Wireless da Família 802.11</b>	<b>290</b>
5.1 Padrão 802.11b	291
5.2 Padrão 802.11a	291
5.3 Padrão 802.11g	292
5.4 Padrão 802.11n	292
5.5 Padrão 802.11ac	293
5.6 Padrão 802.11ad	293
<b>6 Segurança em Redes sem Fio</b>	<b>293</b>
6.1 Ferramentas para Prevenção Contra Ataques a WLANs	294
6.2 Padrões de Segurança Wireless	296
6.2.1 WEP - Wired Equivalent Privacy	296
6.2.2 WPA Versão 1 - Wi-Fi Protected Access	296
6.2.3 WPA2 ou IEEE 802.11i	297
6.2.4 Criptografia: TKIP, AES e RC4	297
6.3 Outros Mecanismos de Segurança em Redes sem Fio	298
<b>7 Configurando um AP e um Cliente em Windows 7</b>	<b>300</b>
7.1 Alterando os Parâmetros de Gerenciamento do AP	302
7.2 Configurando as Redes LAN e WAN do AP	303
7.3 Configurando o SSID e Parâmetros da Rede Wireless	305
7.4 Configurando a Autenticação e Criptografia	307
7.5 Configurando o Filtro de Endereços MAC	308
7.6 Configurando os Clientes e Testando a Conectividade	310

## 1 Fundamentos de Wireless

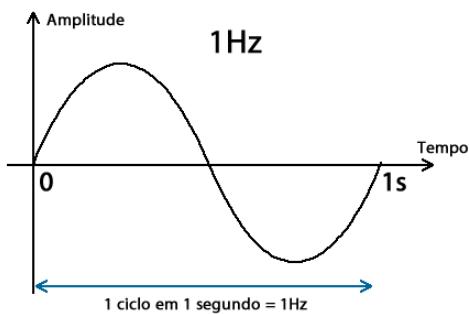
O uso de tecnologias de transmissão sem fio em redes de computadores não é tão nova como se pensa. As primeiras transmissões sem fio aconteceram na década de 70 com redes ponto a ponto utilizando a frequência de 900MHz, porém através de protocolos proprietários e bastante lentas em relação aos padrões atuais.

Para que as redes que conhecemos atualmente do padrão 802.11 fossem desenvolvidas foi necessária a padronização da tecnologia e regulamentação do uso das frequências, pois as frequências de rádio disponíveis são utilizadas por diversos serviços essenciais, tais como polícia e bombeiros, assim como para transmissão de rádio (AM/FM), televisão, telefonia celular e muitas outras aplicações. Essa padronização nasce com a definição do uso de frequências para Aplicações Industriais, Científicas e Médicas (ou ISM) nas décadas de 80 e 90. Em paralelo a IEEE em 1997 define a primeira norma 802.11 que descreve como o sinal deve ser enviado utilizando a faixa de frequências ISM, portanto a maioria dos protocolos que utilizamos atualmente foram desenvolvidos entre 1997 e 2003.

Para entender melhor a transmissão sem fio, vamos analisar a figura abaixo com as faixas de frequência que podem ser transmitidas em meio aéreo ou em "espaço livre".



**Hertz – Hz:** A medida de frequência dos sinais é medida em Hz (Hertz), que representa a unidade de frequência derivada do SI (Sistema Internacional de Medidas) para frequência, a qual é expressa, em termos de **ciclos por segundo**, a frequência de um evento periódico, oscilações (vibrações) ou rotações por segundo. Um de seus principais usos é descrever ondas senoidais, como as de rádio ou sonoras.

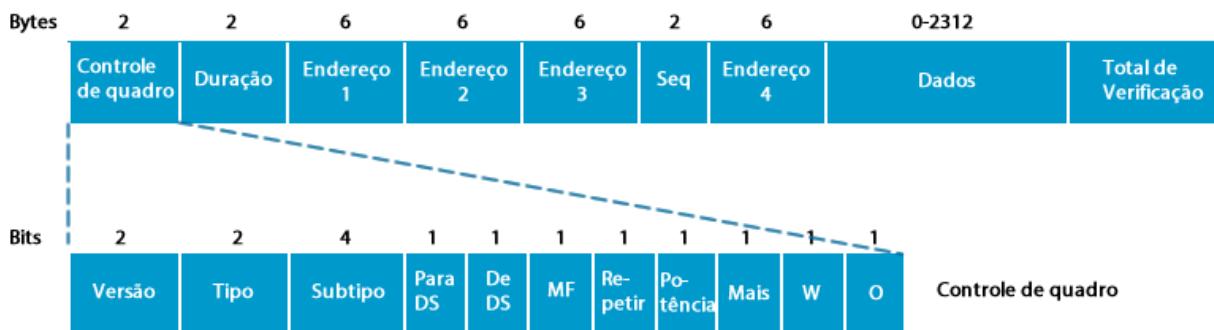


Note que as frequências mais baixas são as de áudio, sendo que as audíveis pelo ouvido humano estão entre 20Hz e 20.000Hz (20.000Hz). Depois temos o ultrassom, frequências da rádio AM, FM, sinais de televisão, as quais estão na faixa de KHz (Quilo Hertz - 1.000Hz) e MHz (Mega Hertz - 1.000.000Hz) e então vem as micro-ondas que estão na faixa do GHz (Giga Hertz - 1.000.000.000Hz).

Os sinais das redes 802.11 estão na faixa de frequência entre 1GHz e 5GHz, ou seja, entre um bilhão e cinco bilhões de ciclos por segundo! Acima disso começamos a entrar no infravermelho, o qual também foi e é utilizado até hoje para transmissão de curtas distâncias com velocidade mais baixa, depois temos a luz visível, passando para o ultravioleta, raios-X e raios-gama.

Se compararmos uma rede sem fio com a rede cabeada poderemos entender melhor o que uma rede sem fio é e suas características. Veja abaixo algumas semelhanças e diferenças entre estes dois tipos de redes LAN:

- Ambas são IEEE 802, sendo que as redes com fio fazem parte da família 802.3 e as redes sem fio da 802.11. Isso significa que, para o usuário, se ele estiver acessando uma rede LAN com ou sem fio o acesso será transparente. Tirando a placa de rede que uma tem um conector para plugar o cabo e outra não, o acesso aos dados em uma rede LAN com ou sem fio é transparente para os usuários finais. Veja uma topologia com redes wireless na figura abaixo.
- As redes 802.3 e 802.11 definem o acesso das camadas física e de enlace, sendo que ambos padrões utilizam endereços MAC no mesmo padrão de 48 bits divididos em 12 algarismos Hexadecimais. Veja a figura 3 ao lado.
- Os mesmos tipos de protocolos das camadas 3 a 7 continuam sendo suportados, pois o 802.11 é apenas um meio de transporte dentro de uma rede LAN sem fio, sendo transparente seu uso para as camadas superiores. Continuamos podendo utilizar o IP, ICMP, HTTP, IPSec, FTP, ou seja, quaisquer protocolos que são utilizados em uma rede com fio continuam valendo para as redes sem fio.
- A principal diferença é que o meio de transmissão utilizado em uma rede sem fio do tipo 802.11 é o ar e não mais cabos metálicos ou fibras ópticas como no padrão 802.3. A transmissão dos dados digitais é realizada por RF (rádio frequência) utilizando a faixa das micro-ondas, conforme já estudamos anteriormente. Portanto a primeira e mais gritante diferença está na camada 1 do modelo OSI que utiliza o ar como meio de transmissão para as redes sem fio.
- As redes com fio utilizam o CSMA/CD para transmitir os dados, porém como em uma rede sem fio não há como detectar uma colisão ela precisa de um novo protocolo de acesso aos meios, chamado de CSMA/CA ou "Carrier Sense Multiple Access with Collision Avoidance". Nas redes com fio tínhamos a detecção da colisão, porém nas redes sem fio temos que "evitar uma colisão", por isso o termo "CA – Collision Avoidance". Portanto, ambos tipos de redes (com e sem fio) utilizam a detecção de portadoras ou "Carrier Sense", a diferença é que nas redes com fio as colisões são detectadas e nas redes sem fio são evitadas com o uso do protocolo RTS (Request to Send – requisição para enviar) e CTS (Clear to Send – Pronto para enviar). Como em uma rede sem fio não é possível que a estação transmita e receba ao mesmo tempo fica impossível de detectar uma colisão.
- Os quadros do 802.3 e do 802.11 também são diferentes, pois as comunicações sem fio precisam de protocolos adicionais para funcionar, porém os dois utilizam os MACs de origem e destino para montar seus quadros. Veja a figura abaixo, note que o quadro tem quatro campos de endereço, pois deve conter origem e destino para a transmissão e origem e destino para envio até o Access Point.



- As redes sem fio enfrentam mais problemas de conectividade e de privacidade (segurança) que uma rede cabeada. Podemos citar problemas como refração, reflexão, absorção, caminhos múltiplos do sinal (multipath), etc. Além disso, como é muito difícil evitar que o sinal saia dos domínios da empresa, ou seja, que não vaze para fora de um edifício, por exemplo, a parte de segurança é um aspecto fundamental da implementação de uma rede sem fio. Caso contrário, uma invasão ou até mesmo o uso dos recursos da rede por pessoas não autorizadas seria muito simples de se fazer.
- As redes sem fio suportam mobilidade (mobility), facilidade parecida com o **roaming** dos telefones celulares, onde ao cruzar células de rádio sua ligação não cai e sim é "transferida" para a nova célula que você está entrando. Isso possibilita o uso de diversas facilidades em redes corporativas, tais como telefonia IP sem fio.
- As redes sem fio dependem da regulamentação do uso do espectro de frequência de cada País.

Em uma rede cabeada nosso sinal é convertido em impulsos elétricos ou ópticos para serem transmitidos no meio físico, essa é a característica das tecnologias da família 802.3 (Ethernet). Já nas redes sem fio, que pertencem à família 802.11, os bits a serem transmitidos são convertidos em ondas de RF e os bits são codificados ou modulados utilizando diversas tecnologias de espalhamento espectral ou Spread Spectrum.

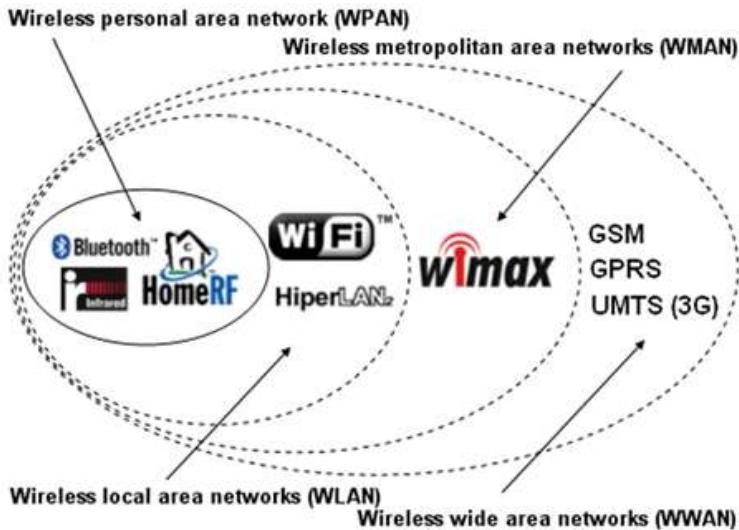
Algumas empresas fabricantes de equipamentos de rede e placas de rede, tais como 3Com, Nokia, Lucent Technologies (atualmente Alcatel-Lucent) e Symbol Technologies (adquirida pela Motorola) se uniram para criar um grupo para lidar com este tema em meados de 1999, nascendo assim a Wireless Ethernet Compatibility Alliance (WECA), que passou a se chamar Wi-Fi Alliance em 2003. Assim como acontece com outros consórcios de padronização de tecnologias, o número de empresas que se associam à Wi-Fi Alliance aumenta constantemente. Até Janeiro de 2012, o grupo contava com a participação de mais de 300 empresas e entidades. Por isso muitas vezes as tecnologias da família 802.11 são chamadas de **Wi-Fi**.

Lembre-se que no Brasil o órgão que regulamenta o uso das frequências é a **Anatel** (Agência Nacional de Telecomunicações).

## 2 Tipos de Redes Sem Fio

As redes sem fio podem ser divididas em quatro tipos principais (veja a figura abaixo):

- Redes pessoais ou curta distância (**WPAN**)
- Redes locais (**WLAN**)
- Redes metropolitanas (**WMAN**)
- Redes geograficamente distribuídas ou de longa distância (**WWAN**).



Veja a seguir as principais características de cada um dos tipos de rede sem fio.

## 2.1 Wireless Personal Area Network

A **Wireless Personal Area Network** (rede pessoal sem fio) é normalmente utilizada para interligar dispositivos que estão fisicamente próximos. Este tipo de rede é ideal para eliminar os cabos usualmente utilizados para interligar teclados, impressoras, telefones móveis, agendas eletrônicas, computadores de mão, câmeras fotográficas digitais, mouses dentre outros.

Nos equipamentos mais recentes é utilizado o padrão **Bluetooth** para estabelecer este tipo de comunicação, mas também pode ser empregado o **infravermelho** ou **IrDA - Infrared Data Association** (semelhante ao utilizado nos controles remotos de televisores), o qual foi muito utilizado na década de 90 para estabelecer conexão entre os telefones celulares e computadores ou entre calculadoras científicas para transferência de arquivos a curtíssima distância. Veja a figura abaixo com exemplos de utilização do Bluetooth.



Normalmente estas redes estão limitadas a apenas alguns metros de distância de alcance.

## 2.2 WLAN (Wireless Local Area Network)

Uma Wireless LAN ou WLAN (Wireless Local Area Network – Rede local sem fio) é uma rede local (LAN) que usa ondas de rádio para fazer uma conexão física entre um dispositivo cliente, geralmente com uma placa de rede sem fio, e um ponto de acesso ou Access Point (AP), o qual tem a função semelhante a um switch, porém sem a utilização de cabos para a comunicação com seus clientes de rede. As redes WLAN estão limitadas a algumas centenas de metros de distância, pois quanto mais longe ela se estender maior o risco da captura do sinal por pessoas não autorizadas.

Aqui é onde estão os padrões 802.11 e o foco desse capítulo.

## 2.3 WMAN (Wireless Metropolitan Area Network)

Uma Wireless Metropolitan Area Network (WMAN) é uma rede de área metropolitana sem fio (wireless). As WMAN baseiam-se na norma **IEEE 802.16** e tem de 4 a 5 quilômetros de alcance.

A principal tecnologia WMAN é o **WiMAX**, a qual pode chegar a taxas de transmissão de aproximadamente 70 Mbps em um raio de vários quilômetros. O padrão WiMAX tem como objetivo estabelecer a parte final da infraestrutura de conexão de banda larga (last mile ou última milha) oferecendo conectividade para uso doméstico, empresarial e em hotspots.



## 2.4 WWAN (Wireless Wide Area Network)

As redes WWAN são basicamente as tecnologias utilizadas pelos sistemas de telefonia celular de voz e para serviços de dados (Wireless Data Services). Abaixo alguns dos padrões utilizados:

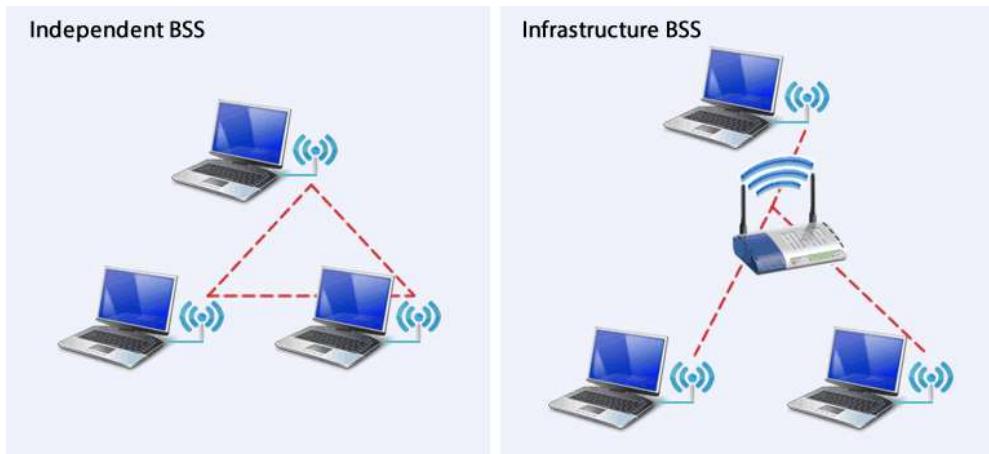
- GSM (Global System for Mobile Communication) - 2G
- GPRS (General Packet Radio Service) - 2.5G
- UMTS (Universal Mobile Telecommunication System) - 3G
- LTE (Long Term Evolution) - 4G

Além das tecnologias citadas nesse tópico sobre tipos de redes sem fio, temos ainda os links de micro-ondas ponto a ponto que podem ser utilizadas nas redes MAN e WAN por operadoras de telecomunicações, assim como as comunicações via satélites são outros tipos de comunicação sem fio que podem ser utilizadas.

A seguir vamos estudar alguns conceitos sobre a teoria de RF e transmissão de sinais em espaço aberto, para aí sim estudar cada um dos padrões de redes LAN sem fio que você poderá encontrar em seu dia a dia como profissional de redes e tratar de alguns aspectos importantes de projeto de redes sem fio.

### 3 Modos de Operação de uma WLAN – Ad-hoc e Infraestrutura

As redes sem fio locais podem operar de dois modos, sendo o primeiro chamado **Ad-hoc** ou **IBSS** (Independent Basic Service Set), e o segundo de Infraestrutura (Infrastructure), a qual pode ser dividida em dois tipos de operação: **BSS** (Basic Service Set) e **ESS** (Extended Service Set). Estes modos definem como a comunicação entre os diversos dispositivos de uma rede local vai ser estabelecida.



#### 3.1 Arquiteturas WLAN Ad-Hoc

Em uma rede Ad-hoc ou IBSS, temos a comunicação direta entre os equipamentos sem fio, sem a necessidade de um intermediário. É como se criássemos um domínio, ou grupo de trabalho, onde os componentes podem trocar informação direta entre si.



As redes Ad-hoc também são conhecidas como redes sem fio P2P (Peer to Peer) ou IBSS (Independent Basic Service Set – Grupo ou Conjunto de Serviço Básico Independente).

Nesse modo de operação redes com poucos dispositivos podem ser criadas diretamente utilizando os computadores de algumas pessoas e suas placas de rede sem fio para compartilhar informações, por exemplo. Como cada computador em uma rede Ad-hoc está utilizando apenas um rádio, a comunicação feita entre os dispositivos será do tipo half-duplex, assim como estudamos anteriormente para os HUBs em uma rede cabeada.

A maior dificuldade desse tipo de rede é a organização das redes. Imagine como você conseguirá identificar os integrantes de várias redes Ad-hoc situadas no mesmo ambiente? Podem até ser criados grupos de trabalho para identificar essas redes, mas mesmo assim a identificação de cada integrante seria difícil, por isso em LANs o Ad-hoc não é tão utilizado.

### 3.2 Arquiteturas WLAN Infraestrutura

As redes em modo Infraestrutura tem sua principal diferença das redes Ad-hoc pela utilização obrigatória de um **ponto de acesso** ou **Access Point (AP)**.

O AP tem duas funções principais, a de funcionar como uma “ponte” entre a rede cabeada 802.3 e a rede sem fios 802.11, assim como fornecer a interface aérea para comunicação entre os dispositivos sem fio (clientes) e a rede. Portanto, no modo infraestrutura não há comunicação direta entre dois clientes de rede sem fio, pois eles obrigatoriamente precisarão passar pelo AP para falar entre si ou com o restante dos dispositivos da rede cabeada ou com dispositivos que estejam em outras células sem fio distantes.



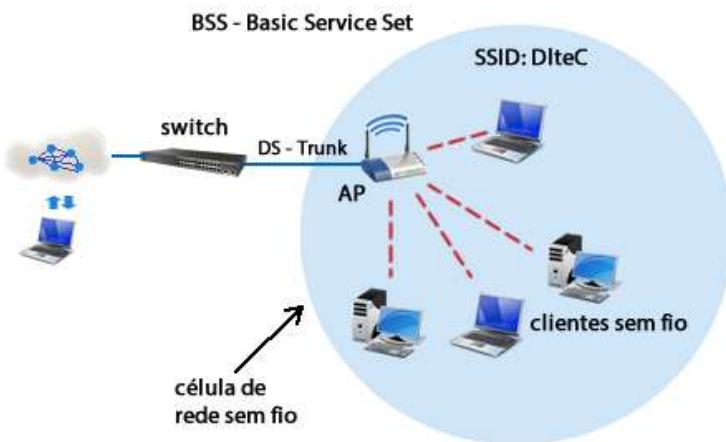
O link ou entroncamento entre o switch e o AP é denominado **DS** (Distribution System ou Sistema de Distribuição), o qual permite que os computadores dessa célula de rede sem fio possam acessar os demais recursos da rede. Este link pode ser, por exemplo, um tronco 802.1Q como vimos no capítulo relacionado às VLANs e switching, o qual seria utilizado para passar uma ou mais VLANs (subredes) da rede física para a rede sem fio.

Os APs não necessariamente terão apenas uma rede vinculada a sua interface aérea, pois existem modelos de AP que possuem mais de uma interface de rádio e permitem a configuração de múltiplas redes LAN sem fio (WLANs) em um mesmo dispositivo. Esta facilidade é utilizada, por exemplo, para fornecer acesso à rede conhecida como **Guest**, ou seja, uma rede disponibilizada para visitantes ou parceiros poderem acessar a Internet com segurança, sem precisar passar pela rede corporativa da empresa.

Agora vamos analisar os dois modos de Infraestrutura sem fio que podemos encontrar na prática: **BSS** e **ESS**.

### 3.2.1 BSS - Basic Service Area

A **Basic Service Area** é um modo de operação onde os APs trabalham de forma independente uns dos outros na rede ou temos apenas **um AP isolado**. Este tipo de arquitetura é a que utilizamos em nossas residências ou pequenos escritórios.



Em uma rede de infraestrutura, as estações devem efetuar a **associação a um AP** para ter acesso aos serviços de rede, a qual é semelhante à função de ligar o cabo ethernet. Um terminal sem fio pode tentar se conectar a qualquer AP, porém é o AP quem decide se permite ou não o seu registro. A função de solicitar a associação é exclusiva do terminal, o qual pode estar associado a um AP por interface sem fio.

Os APs seguem o mesmo conceito de célula da telefonia celular, pois cada AP tem uma área de cobertura e a célula está delimitada pela região que o AP consegue dar cobertura de sinal aos seus clientes. Esta área de cobertura é o BSS ou Grupo de Serviços Básico que o AP irá fornecer aos seus clientes, sendo que a identificação da rede sem fio se dá através do **identificador do grupo de serviços**, conhecido como **SSID** ou **Service Set Identifier**. Veja o detalhe na figura anterior, onde o AP divulga sua rede com o SSID "DlteC".

O padrão 802.11 não impõe nenhuma limitação ao número de terminais que podem estar associados a um AP, porém esta limitação é normalmente baseada nos requisitos de taxa de transmissão necessária para os clientes e também por recomendações dos fabricantes. Por exemplo, APs do fabricante Cisco conseguem suportar até 2048 endereços MAC em sua tabela de endereços MAC, porém o fabricante não recomenda mais que 24 usuários por AP para não afetar o throughput da rede.

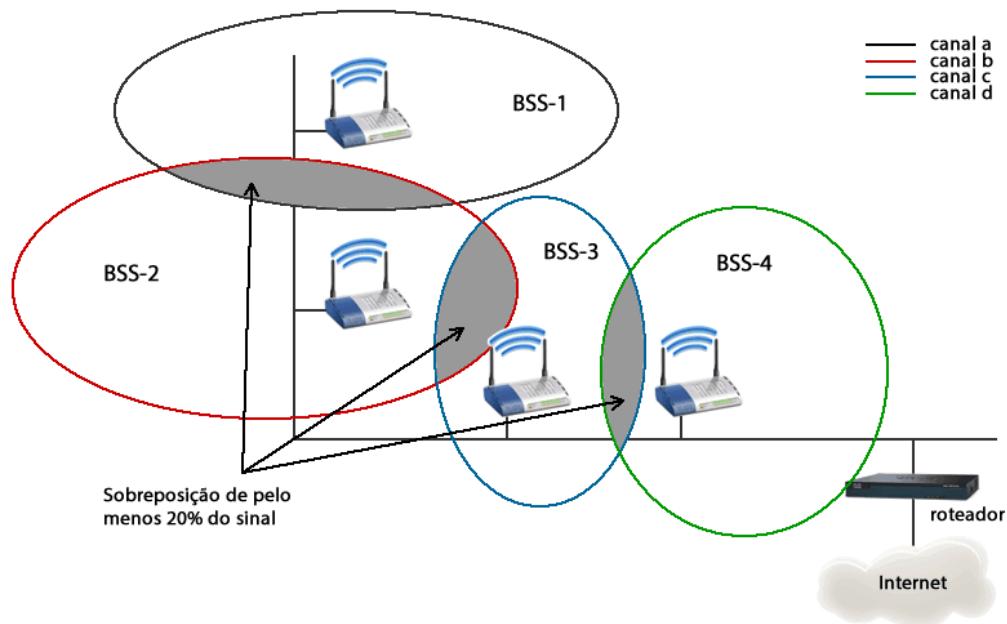
### 3.2.2 ESS - Extended Service Areas

A BSS (rede com 1 AP ou APs isolados) tem apenas a capacidade de cobertura para pequenos escritórios ou instalações pessoais, conforme estudamos anteriormente. Porém, o padrão 802.11 permite a criação de redes wireless de área estendida a partir do **agrupamento de várias BSSs** em uma **ESS** (Extended Service Set – Grupo ou Conjunto de Serviço Estendido).

As ESSs são criadas agrupando todas as BSSs utilizando uma rede backbone, sendo que todos os AP na ESS tem configurado **o mesmo SSID** (Service Set Identifier), que funciona como o nome da rede do ponto de vista dos clientes. Um detalhe é que essa tecnologia utilizada na rede backbone não é especificada pelo padrão 802.11, o qual define apenas uma série de serviços obrigatórios que a ESS deve fornecer a seus clientes.

A principal vantagem do uso do modo ESS em rede sem fio é a possibilidade do **Roaming**, ou seja, trocar de célula (trocar de AP) sem perder a conexão de rede. Esse roaming é semelhante ao de uma rede de telefonia celular, onde não há queda da chamada quando você passa de uma célula para outra, pois senão não seria possível falar ao celular quando nos deslocamos de carro ou ônibus. O roaming possibilita implementar recursos de “**mobilidade**” na WLAN com ESS, permitindo que recursos como a telefonia IP sem fio seja possível.

Na figura abaixo temos uma Infraestrutura sem fio ESS formada pela união de 4 BSSs, onde cada AP é configurado com o mesmo SSID. Nessa arquitetura, um cliente pode movimentar-se na área de cobertura do ESS sem ter que se preocupar com os diferentes APs que irá se conectar ao longo do caminho.

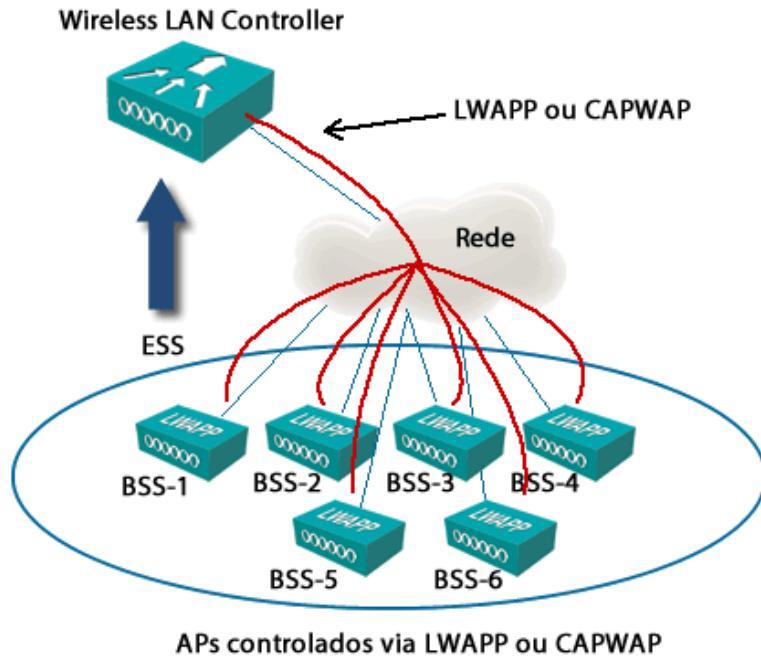


Para que uma ESS seja construída, nas áreas limites entre as células deve haver uma sobreposição de sinal de pelo menos 20%, conforme mostra as áreas em cinza da figura. Além disso, para que haja sobreposição de célula e não interferência, cada célula deve estar em um canal distinto, ou seja, cada célula que se sobreponha deve trabalhar em uma faixa de frequência distinta. Ao logo desse capítulo você estudará que cada padrão da recomendação 802.11 tem uma faixa de frequências ou canais para operar. Se colocarmos dois APs próximos operando no mesmo canal, ou seja, na mesma faixa de frequências haverá uma interferência.

Normalmente não nos preocupamos muito com esse assunto porque os APs residenciais alocam a frequência automaticamente. No entanto, muitas vezes as áreas que temos problemas com sinal podem ser células que estão operando na mesma frequência que o AP de um vizinho, por exemplo.

Para a implementação do ESS a maioria dos fabricantes exige o uso de controladoras de redes sem fio, chamadas de **Wireless LAN Controllers** ou simplesmente **WLC**. No caso do uso das controladoras, os APs que fazem parte de uma ESS se conectam e são controladas por uma WLC. Caso existam várias WLCs na rede elas podem se conectar para estender os domínios da ESS criada, pois cada WLC tem suporte a um determinado número limitado de APs.

Este gerenciamento com WLCs é feito de maneira centralizada e utilizando um protocolo especial chamado **Lightweight Access Point Protocol** ou **LWAPP**. Alguns fabricantes estão optando por gerenciar seus APs de maneira centralizada utilizando também o protocolo **Control and Provisioning of Wireless Access Points** ou simplesmente **CAPWAP**.

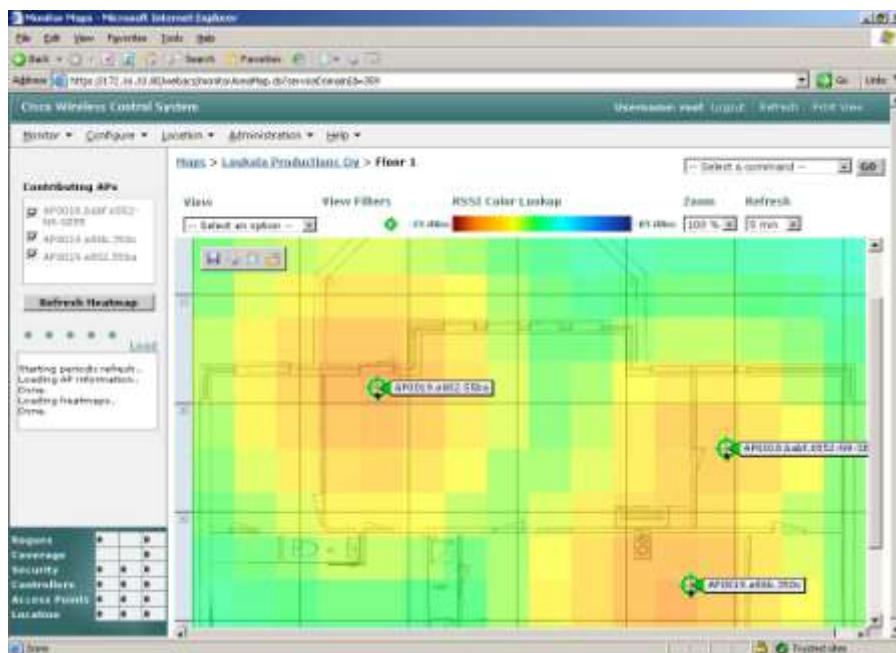


Além das controladoras, muitos fabricantes possuem **softwares de gerenciamento da rede sem fio**, os quais permitem configurações de maneira mais amigável das controladoras e APs da rede, assim como o uso de recursos avançados de gerenciamento e monitoração, tais como inserir a planta baixa da empresa e posicionar os APs para uma visualização gráfica simplificada, determinar a posição de clientes sem fio nessas plantas, calibragem automática do sinal wireless para maximizar a área de cobertura, dentre outros.

Veja na figura seguinte uma tela da sessão “3D RF PLANNING” do software RingMaster do fabricante Juniper, o qual é um software de gerenciamento utilizado no planejamento, configuração, implantação, monitoração e otimização de redes wireless corporativas. Perceba que nessa tela temos a planta baixa da localidade, com os APs posicionados e a cobertura de cada um deles mostrada em cores diferentes.



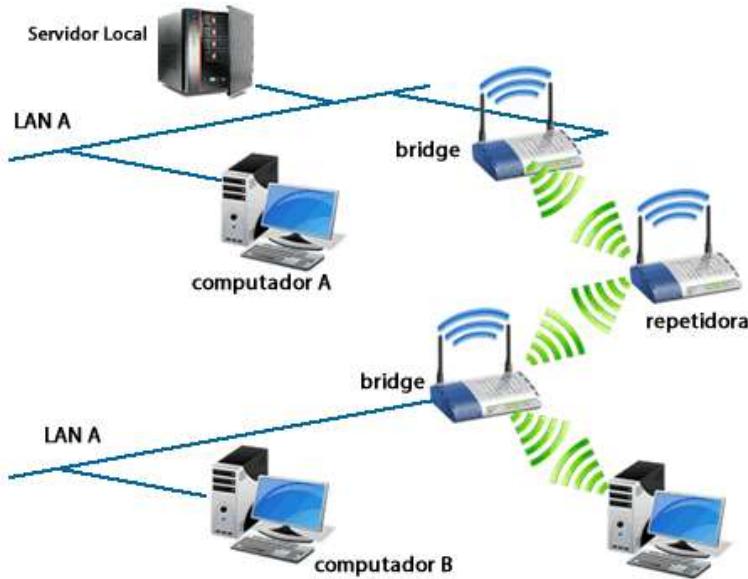
O fabricante Cisco, possui o software Wireless Control System (WCS), veja uma tela do software abaixo.



Nesse ponto deve estar claro para você que uma rede sem fio pode ser muito mais que colocar um AP e acessar a Internet sem fio. Tenha em mente que as soluções corporativas podem ser tão complexas e caras conforme as necessidades de cada projeto.

### 3.2.3 Outros Modos de Operação dos APs

Além do que já vimos, os APs podem operar com **bridges**, ou seja, apenas uma ponte entre duas redes ou uma extensão para a rede cabeada, porém agora sem fio. Em modo bridge o AP também pode funcionar como uma estação repetidora para aumentar o alcance de uma rede sem fio.



Existem modelos de AP que podem também atuar como um link ponto a ponto em modo bridge, bastando conectar uma antena correta para essa aplicação. Dessa forma, empresas podem estender a comunicação entre suas edificações que está em linha de visada (que dá para enxergar sem obstáculos) sem o uso de cabos metálicos ou fibras ópticas.

#### 4 Princípios de Funcionamento de uma Rede Wireless

Vamos agora estudar os conceitos teóricos que irão permitir uma maior compreensão do que é uma transmissão sem fio, suas características, principais dificuldades e também recursos de segurança.

Lembre-se que em uma rede sem fio simples temos dois dispositivos principais: o ponto de acesso sem fio (Access Point ou AP) e um cliente de rede sem fio (Computador ou Laptop com placa de rede sem fio, Tablet, Smartphone, etc.).

Quando estávamos tratando de redes cabeadas bastava conectar um switch à placa de rede do computador para ter acesso à rede e aos demais protocolos que dão acesso aos serviços de rede. Mas e agora o que muda com uma WLAN? A resposta é simples, não temos mais o cabo e o AP faz o papel do switch para os computadores, porém ao invés de termos um link com par metálico temos um link através de uma interface aérea, concorda? No geral a descrição de uma rede sem fio está correta, no entanto algumas perguntas não foram respondidas, como por exemplo:

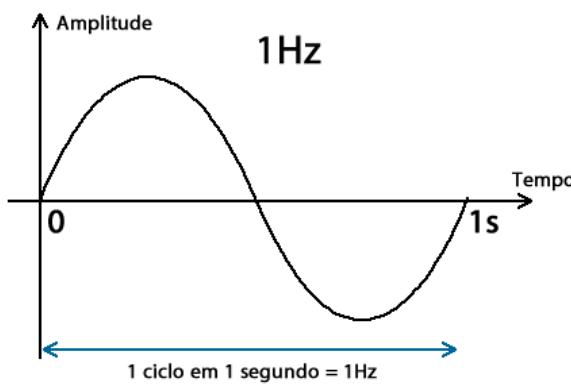
- Como os bits que eram sinais elétricos são agora transmitidos nesse meio sem fio se não dá para fazer um bit 1 ser +5V e o bit zero -5V? Como esses bits são convertidos para uma onda eletromagnética?
- Porque meu sinal tem uma limitação de distância e em algumas áreas da minha casa não consigo ter um sinal com qualidade e em outras, mesmo que próximas o sinal tem qualidade?
- Qual a diferença de transmitir usando o CSMA-CD (das redes com fio) para o CSMA-CA? Porque eu não posso utilizar o mesmo protocolo das redes com fio?
- Como eu identifico qual é a minha rede sem fio e como meu AP dá acesso à rede a meu computador? E se outra pessoa tentar se conectar na minha rede sem fio o que vai acontecer?
- Como eu faço para ter mais privacidade (segurança) na minha rede sem fio e evitar virar um "provedor de Internet" para meus vizinhos?

Provavelmente muitas das perguntas ou até todas você sabe responder, porém recomendamos a leitura desse tópico, pois ele é muito importante para entender o funcionamento básico de uma rede sem fio e suas características.

##### 4.1 Técnicas de Modulação – Enviando um Bit via RF

Como já estudamos anteriormente, em uma rede 802.3 podemos ter as interfaces físicas metálicas e ópticas. Com pares metálicos os bits são transmitidos através de níveis de tensão, por exemplo, +5V para o bit 1 e -5V para o bit zero. Já para uma transmissão óptica é ligando e desligando o laser ou led que representamos os bits um e zero respectivamente. Mas e com uma rede sem fio, como os bits são representados?

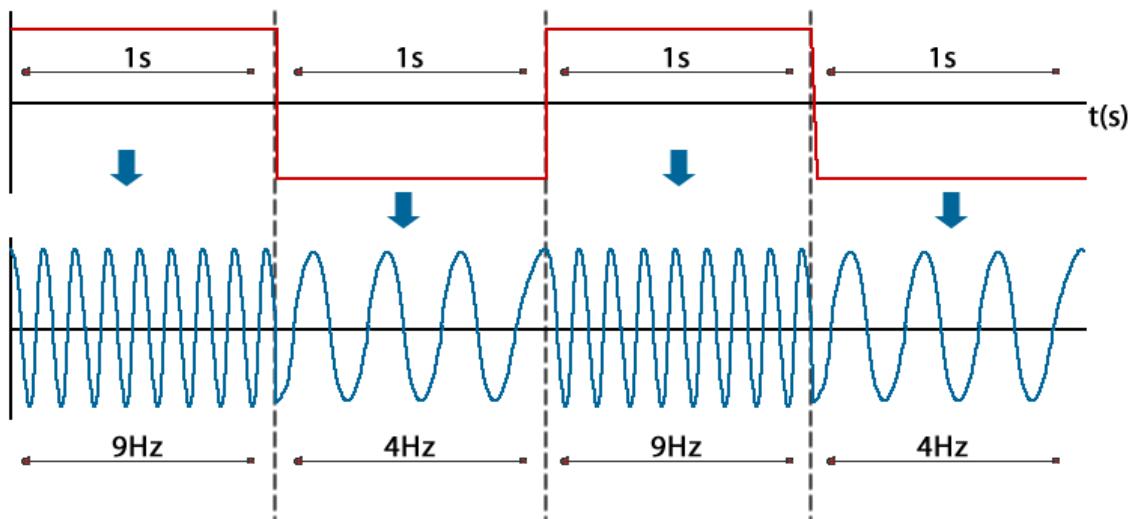
Vamos primeiro analisar o que é uma onda. Veja na figura ao lado que a onda eletromagnética é um sinal que varia com o tempo e tem duas características básicas: Amplitude e Frequência.



A amplitude está na vertical do gráfico e representa a altura da onda eletromagnética, ou seja, quanto menor a amplitude mais difícil de um receptor perceber aquela onda. Em outras palavras, a onda com uma amplitude muito baixa pode ser tão fraca que será impossível do receptor perceber ou ler aquela informação. O oposto é que a amplitude pode ser tão grande que pode ser demais para o receptor e pode danificá-lo ou simplesmente ficar irreconhecível para leitura.

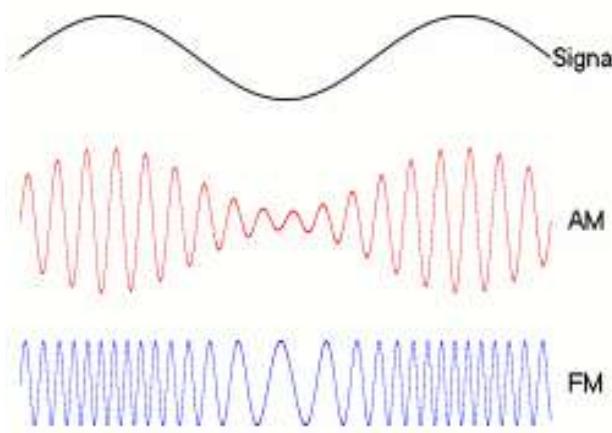
A variação dessa amplitude no tempo é cíclica e a cada ciclo completado em um determinado período tempo representa a frequência que essa onda tem, a qual é medida em Hertz. No exemplo da figura a onda completa um ciclo em um segundo, o que caracteriza um Hertz ou 1Hz. Quanto mais ciclos por segundo a onda completar maior a frequência dela, por exemplo, se ela completar 10 ciclos em 1 segundo ela tem 10 Hz. Lembre-se do início desse capítulo onde vimos que os sinais sem fio estão entre 1 e 5 Giga Hertz, isso quer dizer que os sinais completam cinco bilhões de ciclos em um segundo!

Agora podemos utilizar estes dois parâmetros básicos para criar exemplos de modulação, ou seja, representar um sinal elétrico através de uma onda eletromagnética. Por exemplo, podemos utilizar a frequência para representar dois níveis de um sinal elétrico, veja o exemplo na figura ao lado onde temos um sinal elétrico quadrado que varia de um em um segundo (1Hz) em um nível de tensão positivo e outro negativo. Nesse exemplo de modulação do sinal elétrico utilizamos a frequência de 9Hz para representar o sinal positivo e de 4Hz para representar o sinal negativo.



Quando o receptor captar o sinal de 9Hz ele irá converter para a tensão positiva e o sinal de 4 Hz para a negativa. Note que esse é um exemplo apenas ilustrativo, pois as modulações que são utilizadas nos padrões 802.11 são muito mais complexas, porém este é o princípio básico de uma modulação de um sinal em redes sem fio.

Além da frequência, podemos utilizar a amplitude e a fase do sinal para implementar técnicas de modulação, podendo ainda fazer técnicas compostas que utilizam mais de uma característica para compor a técnica de modulação. Veja a figura abaixo (na matéria online temos uma animação sobre isso) comparando a modulação em frequência e amplitude de uma onda senoidal.

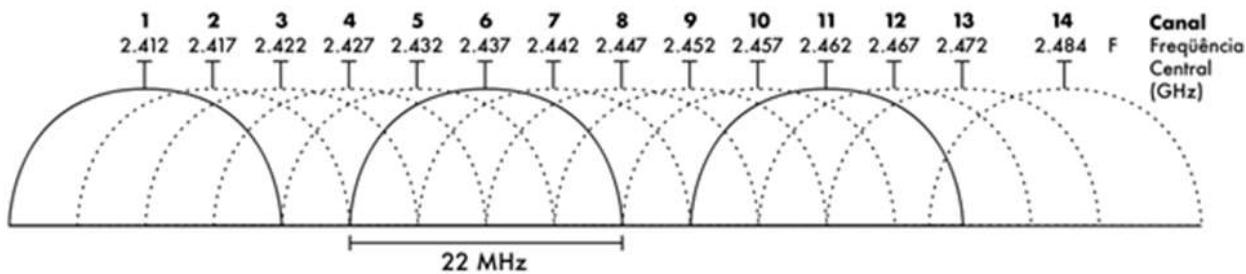


Na prática os padrões 802.11 utilizam basicamente técnicas de espalhamento espectral (Spread Spectrum) para transmitir o sinal com as modulações do tipo:

- **Frequency-hopping Spread Spectrum (FHSS)**: foi utilizado pela primeira versão de 802.11 (versão original) e não é utilizado atualmente.
- **Direct-sequence Spread Spectrum (DSSS)**: utilizado pelos padrões 802.11b e 802.11g.
- **Orthogonal Frequency-division Multiplexing (OFDM)**: utilizado pelos padrões 802.11a, 802.11g, 802.11n e 802.11ac.

O espalhamento espectral consiste em codificar e modificar o sinal de informação executando o seu espalhamento no espectro de frequências, ou seja, ao invés de utilizar uma frequência específica o sinal passa em várias faixas de frequência ou canais. Portanto, o sinal espalhado ocupa uma banda maior que a informação original, porém acaba utilizando menos potência e baixa relação sinal/ruído. O receptor deve estar sincronizado com o transmissor, ou seja, deve saber previamente a sequencia de canais onde o transmissor vai saltar para poder sintonizar estes canais e receber os pacotes transmitidos.

Ainda nesse capítulo, quando estudarmos os padrões 802.11, você poderá visualizar os canais que cada tecnologia utiliza. Veja agora o exemplo dos canais que o 802.11g pode utilizar na figura abaixo. Note que o padrão 802.11g utiliza 14 canais e cada um deles ocupa 22MHz de largura de banda de RF, isso significa que se utilizarmos dois APs 802.11g próximos um do outro precisaremos escolher canais que não interferem entre si. Por exemplo, em um deles podemos utilizar o canal 1 e no outro o canal 6, conforme destacado na figura. Note que os canais de 2 a 4 utilizam uma faixa de frequências que podem interferir no canal 1 e o canal 5 está no limite, ou seja, "colado" com o canal 1. Por isso a escolha dos canais 1 e 6, porque há um espaço de frequências seguro entre os dois, evitando possíveis interferências.



No projeto de redes sem fio de maior porte, onde são utilizados diversos APs e até o modo ESS de Infraestrutura sem fio, a escolha dos canais para garantir a sobreposição segura entre as células é fundamental. Na prática os engenheiros e técnicos de campo costumam chamar a atividade de escolha dos canais de “canalização”.

Além disso, existe uma recomendação para camada física baseada em infravermelho, a qual não foi muito difundida e por isso seu uso atualmente é extremamente restrito. Algumas vezes não sendo nem mencionado, sendo a camada física menos utilizada em redes 802.11.

#### 4.2 Problemas Típicos das Transmissões em Redes sem Fio

Como o sinal de RF trafega em espaço aberto, ou seja, via ondas eletromagnéticas pelo ar, ele está sujeito a muito mais tipos de interferências, atenuações e problemas que um sinal elétrico que passa por um cabo UTP ou um sinal óptico através de um cabo de fibra. Portanto, esse tópico é dedicado ao estudo dos principais problemas que um sinal sem fio enfrenta e suas consequências.

Basicamente os sinais sem fio estão sujeitos aos seguintes efeitos que podem atenuar (diminuir a potência do sinal), distorcer, interferir ou afetar as transmissões sem fio:

- Perda no espaço livre
- Absorção (Penetração)
- Reflexão
- Refração
- Espalhamento do sinal
- Propagação multicaminhos

Os problemas que serão apresentados a seguir causam distorções, atenuações, degradação e até em alguns casos o cancelamento do sinal na recepção. Esses problemas podem ser avaliados e minimizados com o “**site survey**”. O sitesurvey é uma visita técnica onde pessoas qualificadas irão analisar o ambiente, inserindo APs de prova para coletar informações sobre o sinal e ao final do processo se tem um relatório com o posicionamento que cada AP deve ter para garantir o sinal na área de cobertura escolhida pelo administrador de redes. Além do posicionamento, muitas vezes teremos também recomendações de tipos de antenas a serem utilizadas, potência dos equipamentos e demais requisitos para que o modelo de AP possa ser especificado.

#### 4.2.1 Perda no Espaço Livre

Apenas parte da energia transmitida através das ondas eletromagnéticas é captada pela antena receptora, sendo que a perda é maior quanto maior for a distância percorrida pelo sinal. Esta perda é denominada **Perda no Espaço Livre** ou **Free Path Loss**. Nesse caso não estamos considerando nenhum anteparo entre o emissor e o receptor, por isso o nome “espaço livre”. Depois veremos que ao inserir anteparos ou obstáculos outros problemas são adicionados à perda em espaço livre, causando mais atenuações e distorções no sinal original emitido pelo transmissor.

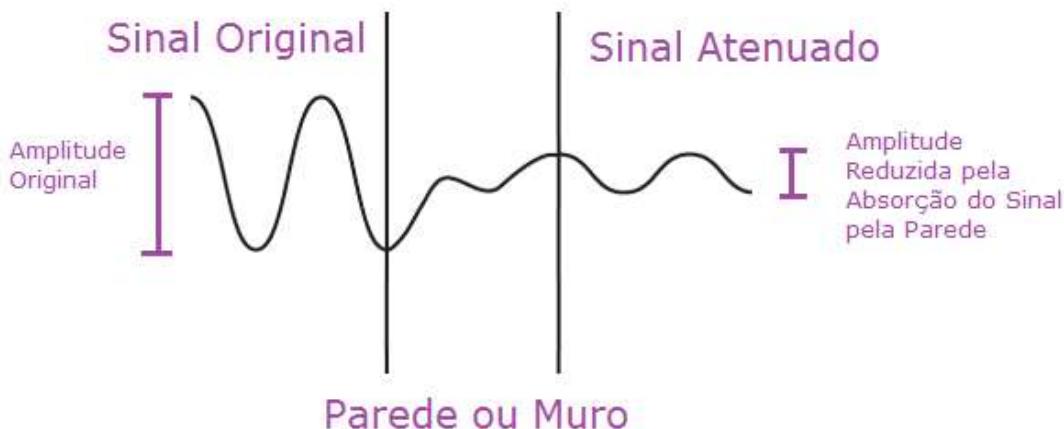
Imagine uma pedra jogada no meio de um lago sem ondulações, do ponto onde a pedra foi jogada para a margem as cristas das ondas vão ficando menores, ou seja, quanto mais perto de onde jogamos a pedra maior será a crista da onda ou sua amplitude. Esta mesma analogia podemos fazer para as emissões de uma antena de um AP, quanto mais perto do AP mais forte será o sinal, ou seja, a onda eletromagnética emitida pelo AP diminui de potência a medida que nos afastamos dele.



#### 4.2.2 Perda por Penetração ou Absorção

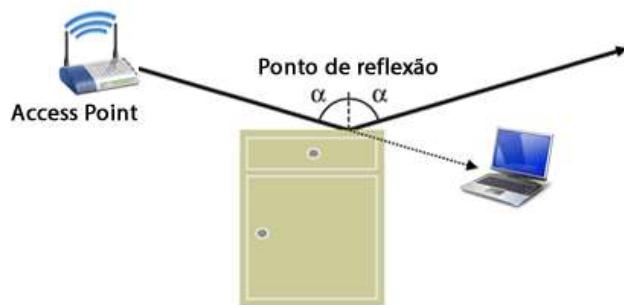
Quando um sinal atravessa um objeto, ou seja, um obstáculo entre a origem e destino da comunicação, este sinal sofre com uma redução do seu nível de potência (atenuação). Esta perda da potência do sinal ao cruzar os objetos é chamada de perdas de penetração ou absorção.

A perda de penetração depende do material o qual compõe o objeto. Obstáculos como paredes e janelas, por exemplo, apresentam valores diferentes de perdas de penetração. Quanto mais metal estiver presente no obstáculo, maior será a perda por absorção.



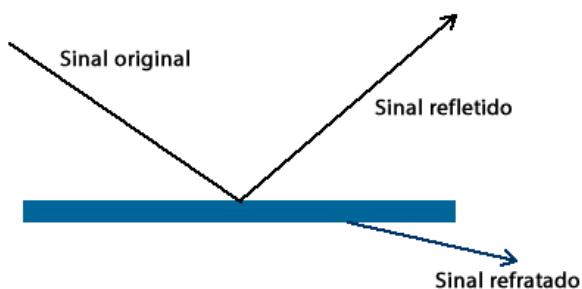
#### 4.2.3 Reflexão

A reflexão é um fenômeno que ocorre quando a onda de rádio incide sobre um objeto de proporções maiores que seu comprimento da onda, sendo que o sinal pode ser refletido em várias direções. A reflexão depende do comprimento de onda e do ângulo de incidência. Além disso, dependendo do material que o obstáculo é composto, parte do sinal pode ser refletido e parte absorvido, portanto a reflexão também depende do material em que a onda está incidindo.



#### 4.2.4 Refração

A refração é o desvio que uma onda eletromagnética, como um sinal de RF, sofre ao passar através de um meio de densidade diferente, conforme abaixo.



O exemplo mais utilizado para ilustrar a refração é o do lápis em um copo d'água, veja na foto da figura abaixo o efeito da refração na prática.

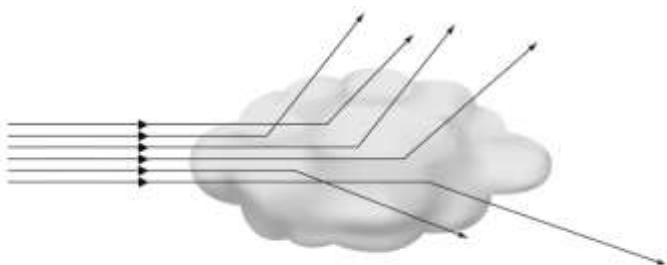


Na realidade quando uma onda de rádio atravessa um meio de densidade diferente, parte da onda é refletida e parte sofre um desvio em outra direção. Especialmente em links de longa distância esse desvio pode tornar-se um problema. Tenha em mente que um link de longa distância pode passar por áreas com condições atmosféricas variadas, cada uma com um valor de densidade diferente, sofrendo o efeito da refração ao longo do percurso. E isso pode fazer com que o sinal sofra um desvio tão acentuado que não seja capaz de chegar ao receptor.

#### 4.2.5 Espalhamento do sinal

O espalhamento parece muito com a reflexão, porém a reflexão ocorre quando o sinal encontra um obstáculo como um espelho ou a tampa de uma mesa, já o espalhamento ocorre quando o sinal encontra um obstáculo de grandeza igual ou menor que seu comprimento de onda, por exemplo, grãos de poeira, uma região de maior umidade (vapor ou gotículas de água), superfícies rugosas como as folhas de uma árvore, água da chuva, de um lago ou do oceano e assim por diante.

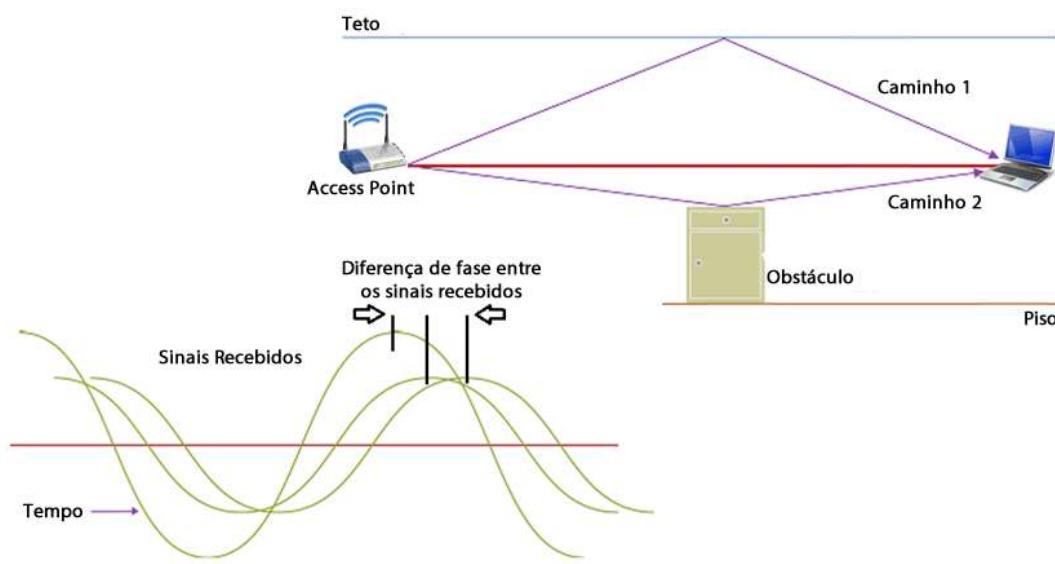
O espalhamento do sinal ou, em inglês, **scattering** pode causar dois efeitos negativos a rede sem fio. O primeiro deles é a degradação do sinal original (enfraquecimento ou atenuação), podendo até chegar à queda do sinal, e o segundo, é o próprio nome desse efeito, ou seja, o espalhamento do sinal em diversas direções, o que pode trazer efeitos imprevisíveis para o receptor.



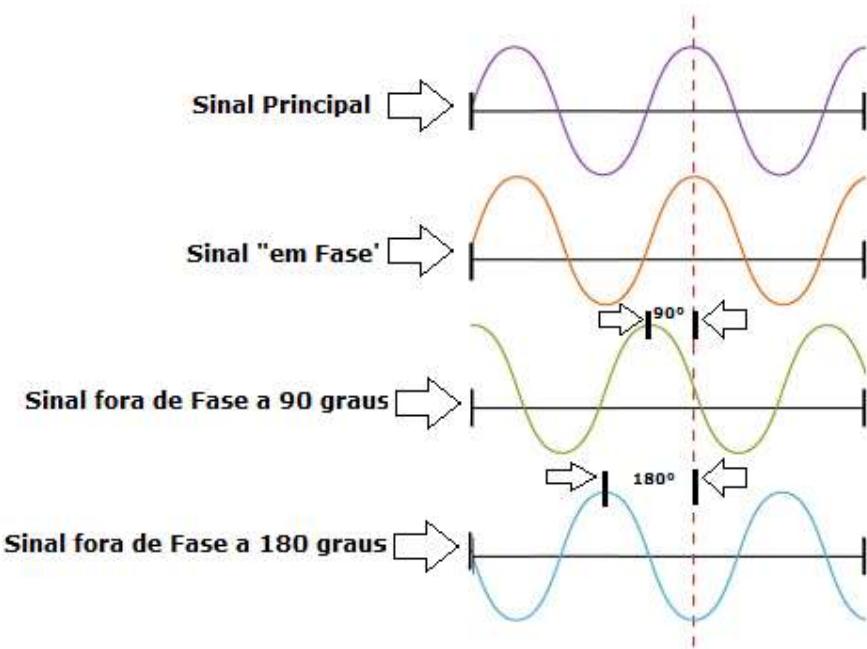
#### 4.2.6 Propagação Multicaminhos ou Multipercursos

O multipercuso ou multicaminhos (em inglês, multipath) é originado pela combinação de diversos fenômenos de propagação, tais como reflexão, difração, refração e espalhamento do sinal enviado. Ou seja, quando combinados estes fenômenos de propagação podem fazer com que o sinal original percorra caminhos diferentes da origem até o destino, sendo que cada um deles acaba levando um tempo diferente para chegar ao receptor.

Portanto, o sinal recebido pelo receptor depende da posição do receptor e dos objetos que esse sinal acabou refletindo. Por exemplo, podem chegar dois sinais em tempos diferentes, causando uma defasagem entre as fases desses sinais, o que pode causar atenuação do sinal e até mesmo o cancelamento dele. Veja na figura seguinte a ilustração do problema.

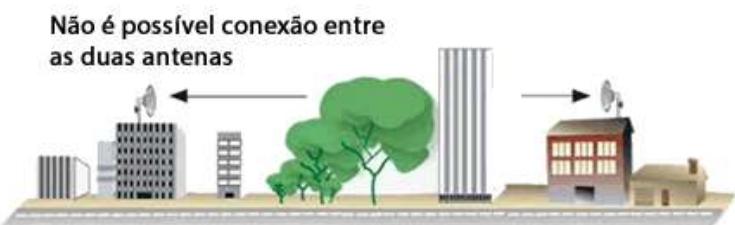


Para entender melhor o que é a fase do sinal, o que gera o problema dos multicaminhos por fases diferentes, veja a figura a seguir. Repare que temos o sinal principal, depois um segundo sinal que está "em fase" com o principal, ou seja, não há deslocamento entre a fase dos dois, depois abaixo temos um sinal  $90^\circ$  e na sequência um sinal  $180^\circ$  defasado em relação ao principal.



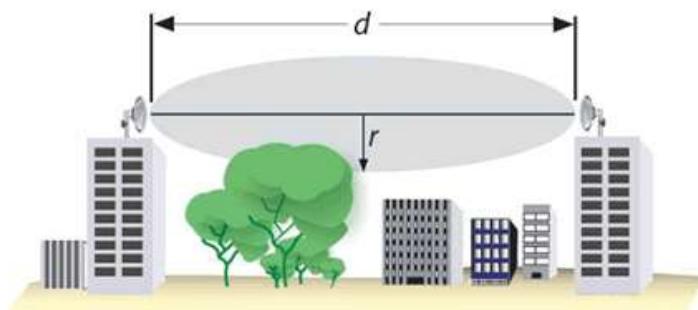
#### 4.2.7 Linha de Visada e Zona de Fresnel

Para transmitir um sinal entre dois pontos a uma distância razoável através do espaço livre é necessário que haja uma **linha de visada** entre as duas antenas utilizadas para a transmissão do sinal. Em outras palavras, de uma antena temos que enxergar a outra. Caso contrário, se tivermos obstáculos no meio do caminho, o sinal será interrompido e não chegará ao seu destino. Veja a figura abaixo com o exemplo de uma transmissão ponto a ponto utilizando linha de visada, em inglês, **Line of Sight** ou **LOS**.



Mas não basta somente enxergarmos de uma antena a outra antena, é preciso enxergar também uma área pré-determinada que deve ser maior à medida que a distância entre antenas aumente, pois é dentro desta área pré-determinada que encontramos a **Zona de Fresnel**.

Na realidade o físico Augustin Fresnel descobriu que a transmissão não se dá em linha reta, mas sim em um formato de bola de futebol americano (elipsoidal), sendo que essa forma tridimensional é dividida em regiões onde os sinais estão em fases diferentes. Quando não temos obstáculos dentro da zona de Fresnel o sinal é recebido sem problemas, porém quando essa zona é obstruída, partes dos sinais fora de fase acabam interferindo na recepção, podendo até cancelar totalmente o sinal recebido. Veja na figura seguinte que a zona de Fresnel é caracterizada pela distância e um raio, o qual determina a área total.



d: Distância

r: Raio

Portanto, mesmo com linha de visada uma comunicação de rádio ponto a ponto pode ser prejudicada, pois a transmissão do sinal no meio não é exatamente uma linha reta, como mostra a zona de Fresnel. A recomendação geral sobre esse tipo de conexão de rádio é que para que ela seja realizada com segurança pelo menos 60% da Zona de Fresnel deve estar livre de obstáculos.

#### 4.2.8 Relação Sinal Ruído (SNR) e Força do Sinal Recebido (RSSI)

A energia elétrica das ondas de rádio (RF) e outros sinais elétricos normalmente é medida na unidade de potência "Watts", no caso do padrão 802.11 em miliWatts (mW). Por exemplo, o sinal do padrão 802.11b deve ser capaz de transmitir com a potência de 32 mW. Já a quantidade de energia da onda que o receptor capta em sua antena será menor que o valor original, pois como vimos temos diversos tipos de propagação que atenuam e degradam o sinal original, reduzindo sua potência ao longo do caminho até o receptor.

Porém, se você notar, a maioria dos fabricantes não indicam a potência de suas antenas em Watts ou mW e sim utilizam uma unidade chamada **decibel-miliWatt** ou **dBm**. O decibel é simplesmente a relação entre duas medidas de potência, ou seja, é na realidade um décimo da potência de dez. Os cálculos e conversões de dBm para Watts e o contrário são baseados em escalas logarítmicas e não muito simples, por isso vamos colocar alguns valores padrões abaixo e logo em seguida mostrar algumas dicas práticas sobre conversão.

Por definição "**0 dBm = 1 mW**", sendo que potências maiores que 1 mW são representadas por números positivos e menores com números negativos. Um limite teórico para a recepção de uma antena que usa padrão 802.11b em uma placa de rede é de -83 dBm, porém na prática esse limite deve ser considerado -50 dBm, que em Watts representa 0,00001 mW. Veja os valores abaixo e depois vamos entender como chegamos no valor em Watts para o -50dBm:

- 0 dBm = 1 mW
- 10 dBm = 10 mW
- 20 dBm = 100 mW
- 30 dBm = 1000 mW ou 1 W
- 40 dBm = 10 W

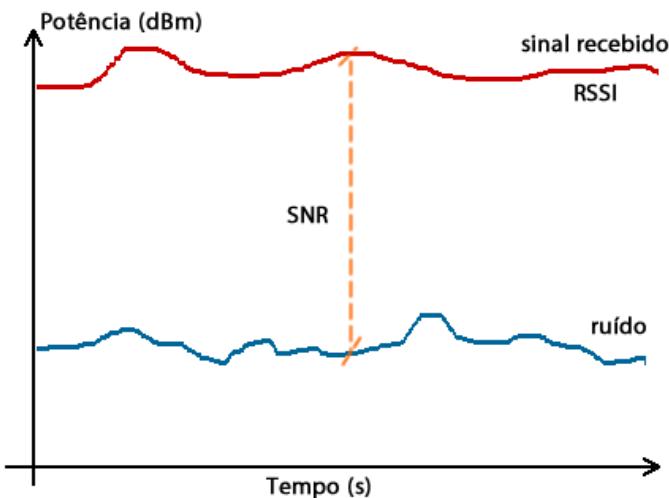
Note que a cada 10 dBm multiplicamos o valor em Watts por 10, portanto, o contrário também é verdade, se temos -50dBm ele é 50 vezes menor que o 0dBm, por isso a cada 10 dBm a menos dividimos por 10 o que dá:

- 0 dBm = 1 mW
- -10 dBm = 0,1 mW
- -20 dBm = 0,01 mW
- -30 dBm = 0,001 mW
- -40 dBm = 0,0001 mW
- -50 dBm = 0,00001 mW

Existe outra regra que diz que a cada 3 dBm o valor anterior dobra, por exemplo, 23dBm em Watts será 200mW, pois o valor de 20dBm era 100mW e se a cada 3 dBm a mais ele dobra o valor final será 100mW vezes 2, ou seja, 200mW de potência. Os valores aqui são aproximados para que você não precise se preocupar com fórmulas e funcionam bem na prática.

Porém nem todos os fabricantes expressam a potência do sinal em dBm, alguns reportam através de escalas que fornecem um indicador de potência do sinal recebido (Received Signal Strength Indicator - RSSI) através de cálculos complexos. Alguns fabricantes utilizam uma escala que vai de 0-31 e outros de 0-63. Portanto, o RSSI é utilizado para indicar quanto forte um sinal é para o receptor, normalmente é um valor negativo em dBm e quanto mais perto de zero melhor será o RSSI.

O ruído é também uma forma de energia elétrica e pode ser reportada em dBm ou através de porcentagem em relação ao sinal recebido. A relação sinal ruído (signal to noise ratio ou SNR) é a diferença simples entre o sinal recebido e o ruído e representa quanto o ruído está interferindo sobre o sinal recebido. Quanto maior o SNR melhor é o sinal. Veja a figura abaixo.



Existem outras medidas que podem ser utilizadas quando falamos de transmissão em RF, tais como dBi (decibel isotrópico), dBd e EIRP, abaixo segue uma descrição rápida sobre cada uma delas, pois não vamos nos aprofundar nesse assunto, uma vez que maioria dos equipamentos do padrão 802.11 tratam sua potência em mW ou dBm:

- **dB<sub>i</sub> (Decibel Isotrópico)** : usado para expressar o ganho de uma antena em relação a antena ISOTRÓPICA. A antena isotrópica tem um diagrama de irradiação esférico, ou seja, irradia igualmente o sinal em todas as direções. O dB<sub>i</sub> é muito usado em cálculos de enlaces de **telecomunicações**, pois a atenuação de propagação é sempre calculada entre antenas isotrópicas. A antena isotrópica é uma referência teórica, sendo de difícil construção prática.
- **dB<sub>d</sub>** : usado para expressar o ganho de uma antena em relação ao DIPOLO de meia onda. O dipolo de meia onda é a antena ressonante mais simples e fácil de ser construída e por isso é muito usada como referência. Em espaço livre, o ganho do dipolo de meia onda é de 0 dB<sub>d</sub> = 2,15 dB<sub>i</sub>.
- **EIRP (Equivalent Isotropically Radiated Power)**: o EIRP de um sistema é simplesmente a conta de chegada da potência na antena de saída.

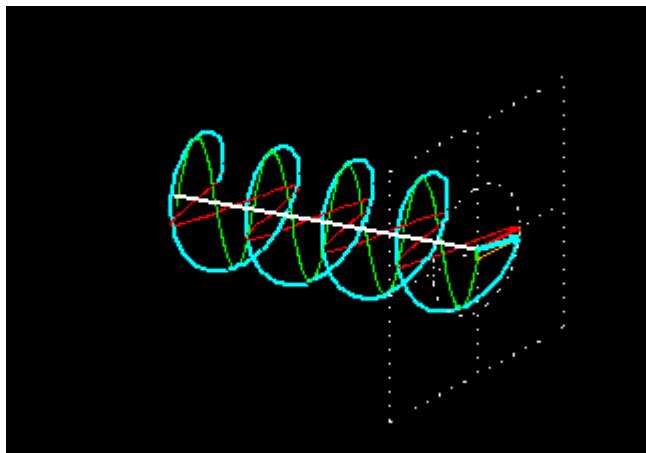
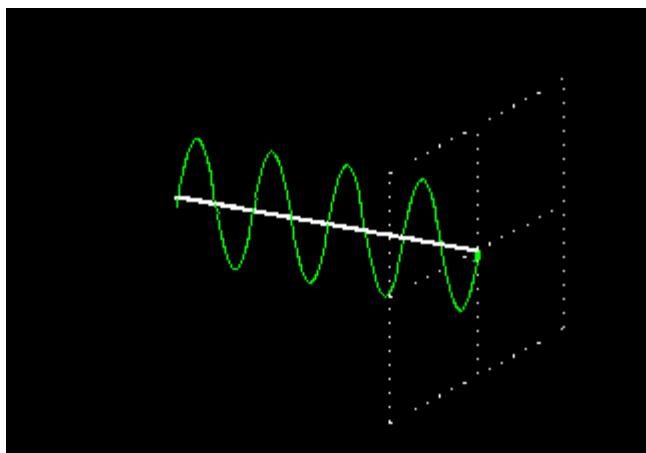
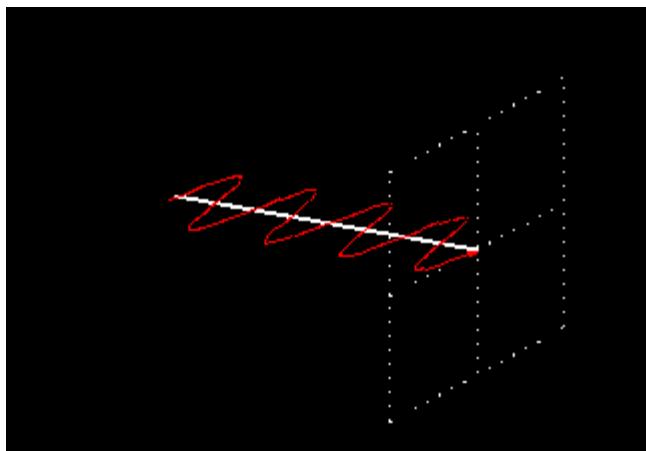
Esses parâmetros de medida são utilizados para especificar as antenas e também para calcular distâncias máximas, tamanhos de antena, etc.

#### 4.3 Principais Tipos de Antenas

Este é um ponto muito importante para uma transmissão sem fio, tanto que muitos técnicos e engenheiros diriam que é o principal ponto, pois sem uma antena o seu AP não seria nada mais que um ponto de distribuição conectado a um switch e o sinal sem fio irradiado por ele não passaria de 3 metros.

De maneira bem simplificada, uma antena é um dispositivo cuja função é transformar energia eletromagnética guiada pela linha de transmissão (sinal elétrico) em energia eletromagnética **irradiada** (sinal de RF – Rádio Frequência). Pode-se também dizer que esta lei serve no sentido inverso, ou seja, transformar energia eletromagnética irradiada em energia eletromagnética guiada para a linha de transmissão. Em outras palavras, é a responsável pela transmissão e recepção do sinal de RF e conversão para um sinal elétrico.

Quando falamos de antena você pode ouvir alguns termos que não estudamos até o momento como diversidade e polarização. Começando pela polarização, ela descreve como a onda irá ser enviada pelo espaço, ou seja, a orientação da onda no espaço. Podemos ter basicamente uma polarização linear, a qual pode ser vertical ou horizontal, e ainda podemos ter uma polarização circular. Este termo é o mesmo utilizado para a polarização da luz e também das antenas de TV, ou seja, tem o mesmo significado. Portanto a polarização indica como a onda eletromagnética irá se propagar no espaço. Veja as figuras seguinte (na matéria online são mostradas animações) com exemplo das polarizações horizontal, vertical e circular respectivamente.



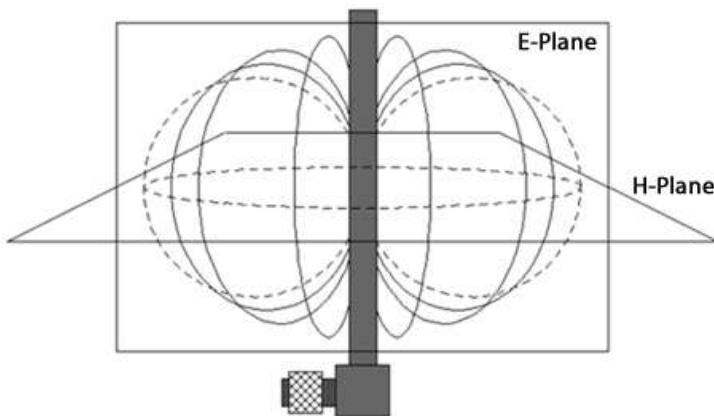
As antenas dos equipamentos WLAN podem utilizar qualquer uma das polarizações mostradas aqui, porém as mais comuns em campo são antenas com polarização vertical. Em ambientes internos (indoor), o fato das antenas estarem um pouco fora da posição, como por exemplo, uma antena com polarização vertical estar deitada, pode não causar muitos problemas, pois como são ambientes pequenos a degradação do sinal acaba sendo suportada pelos APs. No entanto, em ambientes externos (outdoor) isso pode ser um grande problema, por isso preste atenção ao posicionar as antenas dos APs.

Já a diversidade da antena visa tratar os problemas relacionados ao multicaminho. Isto pode ser feito utilizando diferentes tipos de antena ou então inserindo mais uma antena no AP distanciadas por um comprimento de onda entre si (as duas devem ser iguais), assim o AP pode "escolher" qual antena tem o melhor sinal recebido, por exemplo.

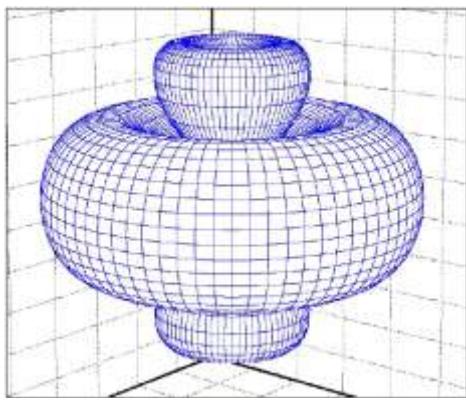
Agora vamos analisar os dois tipos mais comuns de antena que utilizamos em ambientes WLAN: as antenas **Omnidirecionais** e as **Direcionais**.

#### 4.3.1 Antenas Omnidirecionais

As antenas Omnidirecionais são antenas que irradiam sinal em **todas as direções**, normalmente são chamadas de dipolo (em inglês **dipole**). Na realidade, o termo "**em todas as direções**" é uma figura de linguagem, pois as antenas concentram o sinal na horizontal, em um raio de 360 graus, irradiando pouco sinal na vertical. O sinal emitido pelo ponto de acesso com uma antena desse tipo tem uma área de cobertura em formato de um **donut** (rosquinha), conforme figura abaixo.

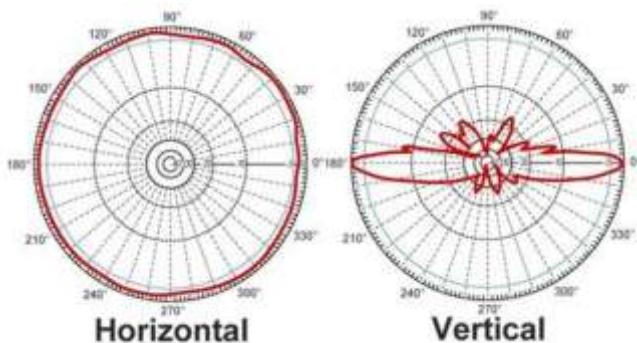


Na figura temos que **H-Plane** (H-Plano ou eixo "x") é a irradiação da antena na horizontal, já o **E-Plane** (E-Plano ou eixo "y") é a irradiação da antena na vertical. Veja a representação 3D de uma antena do tipo dipolo na figura abaixo.



As antenas omnidirecionais comuns são também chamadas de **antena dipolo 2.2 dBi**, a qual é a mais comum utilizada em ambientes indoor e são bastante fracas. Por isso que a antena de um AP que utiliza esse tipo de antena deve ficar sempre na posição vertical, além disso, o ideal é que o AP fique em uma posição central e um pouco mais alto que os móveis e demais obstáculos, possibilitando que o sinal trafegue até os clientes sem muitos desvios.

Existem outras opções de antenas omnidirecionais mais potentes que a de 2.2 dBi, podendo ir de 3 a 12 dBi ou mais, com diferentes tamanhos de área de coberturas na horizontal. Por exemplo, temos antenas omnidirecionais maiores para uso externo que podem oferecer ganhos de 10 a 15 dBi. Utilizando essas antenas, o sinal continua sendo transmitido em todas as direções na horizontal, porém o ângulo vertical se torna muito mais estreito em relação ao oferecido pelas antenas padrão, ou seja, o maior ganho da antena não faz com que ela transmita mais sinal, mas apenas com que concentre a transmissão em uma faixa mais estreita, veja a figura ao lado.



Na figura acima, o gráfico da esquerda (escrito **Horizontal**) é o sinal visto de cima, com a antena bem no centro do círculo e se fosse tirada uma foto da energia eletromagnética por cima da antena. Note que a irradiação em vermelho não é um círculo perfeito, nas bordas existem algumas irregularidades.

Já no gráfico da direita (escrito **Vertical**) é como se fosse tirada uma foto da antena vista de lado e o fotógrafo estando de pé apontando para o topo da antena. Assim como no primeiro caso a antena está no centro da foto e você pode notar que ela irradia o sinal quase todo na horizontal, bem pouco sinal é irradiado na vertical.

Estas figuras são chamadas de **Gráficos de Irradiação** e os fabricantes das antenas fornecem para que você saiba como essa antena irá irradiar o sinal, e dessa forma, você poderá escolher o melhor modelo para seu projeto. Com esse gráfico e a potência da antena o projetista tem como estimar a distância que o sinal pode alcançar teoricamente.

#### 4.3.2 Antenas Direcionais

As antenas direcionais irradiam o sinal em uma única direção. Podemos também dizer que as antenas direcionais não irradiam mais em um ângulo de 360 graus como as omnidirecionais, as direcionais **irradiam em ângulos de 90 graus ou menores, concentrando o sinal irradiado em uma determinada direção**.

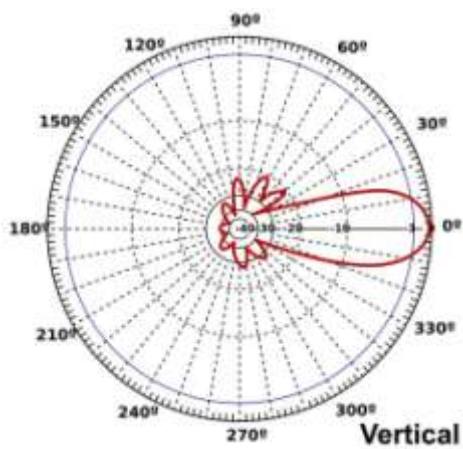
Existem diversos modelos de antenas direcionais, as principais seguem abaixo:

- Antenas setoriais, divididas em patch antennas (antenas de painel) e round patch antennas (antenas circulares).
- Antenas yagi.
- Antenas parabólicas.



As antenas setoriais concentram o sinal em um ângulo de aproximadamente 90 graus, ou seja, um quarto de um círculo completo. Se instaladas no canto de uma sala ou cômodo, elas distribuem o sinal em todo o ambiente, deixando pouco sinal vazar em outro sentido.

As antenas yagi oferecem um ganho maior que as setoriais, porém são capazes de cobrir uma área menor, e normalmente precisam estar diretamente apontadas com um raio entre 24 a 30 graus (ou menor) entre si. Uma antena yagi emite o sinal em um ângulo similar ao de um cone e são úteis para cobrir alguma área específica (longe do ponto de acesso) ou interligar duas redes distantes. Usando duas antenas yagi de alto ganho é possível criar links de até 25 km. Veja o gráfico de irradiação de uma antena yagi na figura abaixo.



Um tipo de antena yagi interessante é feita com lata de batata Pringle's, chamada de Cantenna. Veja a foto na figura ao lado. É possível a construção de antenas caseiras como mostra a figura, porém o grande problema é que para utilizá-las devem-se seguir os padrões estabelecidos pelos órgãos reguladores, como o FCC dos EUA e a Anatel no Brasil.



Por último temos as antenas parabólicas, as quais também captam o sinal em apenas uma direção, porém de forma ainda mais concentrada que as antenas do tipo yagi. Isto permite que sejam atingidas distâncias ainda maiores que 25 km.

A maioria das antenas parabólicas destinadas a redes WI-FI utiliza uma **grelha metálica** no lugar de um disco sólido, o que reduz o custo e evita que a antena seja balançada pelo vento, saindo de sua posição ideal. Por causa disso, elas são também chamadas de **antenas de grelha**, ou **grid antennas**, em inglês.



#### 4.3.3 Conectores e Cabos

Para conectar as antenas aos APs existem diversos tipos de conectores e cabos, principalmente quando utilizamos antenas de uso externo.

O conector mais utilizado em APs e placas sem fio PCI são chamados **RP-SMA** (Reverse Polarity SMA, também chamado de SMA-RP, RSMA ou Conector SMA Reverso), onde o conector macho fica no dispositivo (AP ou placa PCI) e a fêmea fica na antena. Veja as fotos abaixo.



Um conector menos comum, porém utilizado por um grande número de APs, tais como Linksys WRT54GS e o Cisco Aironet 1200, é o RP-TNC. Ele é um pouco maior e mais robusto que o RP-SMA. Veja a foto da figura ao lado a comparação de um AP com conector SMA e embaixo um AP com conector TNC.



Os conectores SMA e TCN são recomendados para antenas indoor, já para antenas de uso externo, os conectores mais utilizados são os do tipo N (N-Type). Os conectores N-Type são próprios para cabos coaxiais e são utilizados desde a década de 1940 até os dias de hoje. Com a evolução nas técnicas de fabricação esses tipos de conectores são cada vez mais precisos e com menos perda de sinal. Veja uma foto do conector, onde temos um cabo adaptador de SMA para N-type.

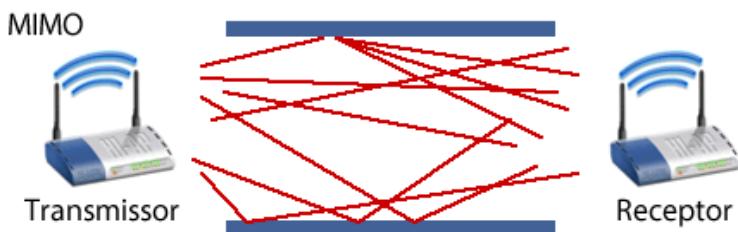


Existem ainda outros tipos de conectores como os MC e MMCX ou os miniaturizados MHFs, porém os principais são os três citados anteriormente. O importante é você saber que ao comprar um AP podem haver vários tipos de conectores para suas antenas e algumas vezes adaptações serão necessárias quando não houver opção de casar o conector da antena com o ponto de acesso.

#### 4.4 Tecnologia MIMO

O MIMO ou Multiple-input and multiple-output é o conjunto de técnicas de transmissão para sistemas de comunicação sem fio com múltiplas antenas na transmissão e na recepção, as quais foram incorporadas em diversos padrões de comunicação devido ao grande ganho de desempenho que elas proporcionam, como por exemplo, no LTE (Long Term Evolution), WiMax, HSPA, **802.11n** e **802.11ad**.

O MIMO permite que a placa utilize diversos fluxos de transmissão, utilizando vários conjuntos transmissores, receptores e antenas, transmitindo os dados de forma paralela.



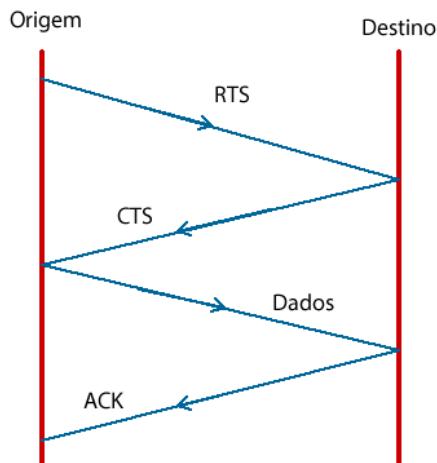
Note na figura que a tecnologia MIMO utiliza o que era um problema, chamado multicaminhos, para aumentar a velocidade de transmissão, utilizando os fluxos que estão em caminhos diferentes para transmitir dados.

#### 4.5 Funcionamento Básico do CSMA-CA

O CSMA/CA ou “Carrier Sense Multiple Access with Collision Avoidance” (Acesso múltiplo com verificação de portadora com prevenção de colisão) é um método de controle de acesso ao meio sem fio que, ao contrário do CSMA/CD, antes de transmitir efetivamente um pacote (dados), a estação transmissora **avisa sobre a transmissão e em quanto tempo** irá realizar a tarefa para **prevenir** (evitar) que uma colisão ocorra.

Por isso o termo “**Collision Avoidance**” (prevenção de colisão) substituiu o termo “**Collision Detection**” (detecção de colisão) nas redes sem fio em relação às redes cabeadas. Nas redes cabeadas existem meios de detectar uma colisão, enquanto em uma rede sem fio não é possível.

Os dispositivos de uma rede (WLAN) devem sentir (ouvir) o meio para verificar alimentação (estímulo de RF acima de certo limite) e esperar até que o meio esteja livre antes de transmitir, ou seja, verificar a portadora. Para evitar as colisões no ambiente sem fio é utilizado um recurso chamado "solicitar para enviar" e "livre para enviar" (Request to Send - RTS / Clear to Send - CTS).



Portanto, o RTS/CTS do CSMA/CA lembra muito o handshake triplo realizado pelo TCP para estabelecer uma conexão antes de iniciar o envio dos segmentos, porém aqui estamos em camada 2.

#### 4.6 Descobrindo uma Rede sem Fio (Scan)

Pela natureza das redes sem fio, o ponto de acesso precisa **anunciar** a existência da rede para que os clientes possam se conectar e utilizar os serviços e recursos de rede. Uma rede sem fio é reconhecida pelo seu identificador chamado **SSID**. O SSID é um valor único, normalmente alfa-numérico, com comprimento que varia de 2 a 32 caracteres.

Para este “anúncio” da rede, o AP utiliza quadros especiais chamados de **beacons** (em português, balizas), os quais são enviados periodicamente para facilitar a descoberta de uma rede sem fio e informar as capacidades que os APs têm, como o próprio SSID, taxa de dados, etc.

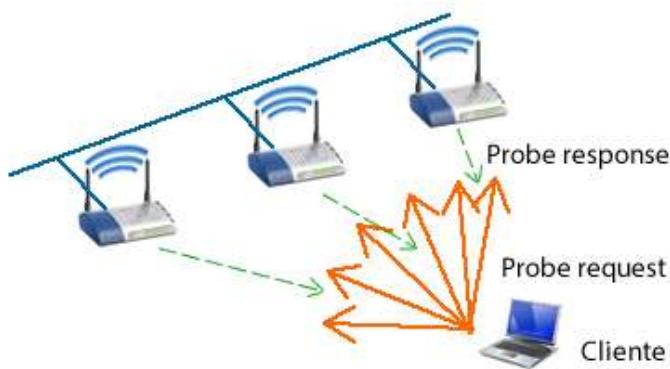
Portanto, quando instalamos, configuramos e iniciamos um cliente de rede sem fio, o primeiro passo que será executado por ele, será verificar a existência de alguma rede sem fio ao seu alcance. Caso haja, o cliente deverá verificar se há possibilidade de associação com a rede sem fio em questão. Este processo é chamado de **scanning** (varredura).

O scanning da rede pode ser feito de duas maneiras: **Ativo** e **Passivo**. No modo passivo os clientes procuram por beacons em cada canal por um determinado período de tempo assim que ele é inicializado. Os beacons, portanto, são enviados pelo AP e as estações procuram nesses beacons o SSID da rede que eles desejam se conectar. Se estiver, a estação então tenta entrar na rede através do AP que enviou o beacon.



Em configurações em que há vários APs, vários beacons serão enviados e, nesse caso, a estação tenta entrar na rede através do AP que tiver o **sinal mais forte**.

No modo ativo são as estações que iniciam o processo, tornando-se, portanto, parte ativa do processo de descoberta de redes. Quando a estação está procurando por uma rede, ela envia um frame chamado **probe request**, contendo o SSID da rede que ela. O AP que tiver o SSID em questão envia um **probe response**.



Se houver vários APs, somente aquele que tiver aquele SSID envia o probe response. Por outro lado, se o SSID de broadcast (que indica "qualquer rede") for enviado no probe request, **todos os APs** enviarão um probe response.

Uma vez que o AP com o SSID específico tenha sido encontrado, a estação inicia os passos de **autenticação** e **associação** para entrar na rede através daquele AP.

#### 4.7 Autenticação, Criptografia e Associação de Clientes

A autenticação é a primeira etapa do processo e serve para o cliente estabelecer a sua identidade com um ponto de acesso. Existem dois tipos de autenticação: Sistema de autenticação aberta ou Autenticação com Chave Compartilhada (shared key).

O sistema de autenticação aberto consiste em duas etapas. A primeira é uma solicitação de autenticação pelo cliente, a qual é seguida de uma resposta de autenticação por parte do AP contendo uma mensagem de sucesso ou falha. Veja a figura ao lado com a troca de mensagens até a associação do cliente ao AP com autenticação aberta.



Já no processo de autenticação e criptografia com chaves compartilhadas, uma chave ou senha é definida manualmente em ambos os equipamentos (AP e Cliente). Há vários tipos de autenticação de chave compartilhada disponíveis para usuários residenciais ou de pequenas empresas, sendo que as principais são:

- **WEP (Wired Equivalent Privacy)**: WEP não é recomendado mais para uso em redes sem fio, pois possui diversas vulnerabilidades. Um dos principais riscos de segurança é a possibilidade de um hacker capturar quadros que são trocados no início do processo (usando softwares específicos) e usar as informações para quebrar criptografia.
- **WPA (Wi-Fi Protected Access)**: WPA já é um protocolo considerado seguro e aumenta significativamente o nível de proteção de dados e de controle de acesso (autenticação) para uma rede sem fio. WPA utiliza a autenticação 802.1X e a troca de chaves só funciona com chaves de criptografia dinâmicas, já no WEP as chaves são estáticas. Existem alguns tipos de WPA, os mais utilizados são o WPA-Pessoal, WPA-PSK (Pre-shared key - chave pré-compartilhada) e WPA-Home.
- **Wi-Fi Protected Access 2 (WPA2)**: WPA2 implementa uma melhoria de segurança para o WPA, sendo que os dois não são interoperáveis. Normalmente o WPA e o WPA-2 suportam as criptografias via TKIP e AES.

Veja na figura abaixo a troca de mensagens de autenticação quando utilizamos chaves compartilhadas. Note que ao invés de enviar os dados abertos da autenticação, é enviando um challenge ou desafio, que significa que aquela informação está criptografada.

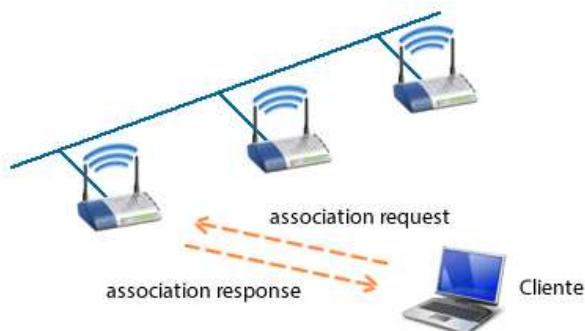


A vantagem do uso da criptografia na transmissão dos dados é que as informações trocadas entre o cliente e o AP são protegidas (codificadas com um protocolo de criptografia). Assim, caso as informações sejam capturadas por um hacker elas não conseguirão ser decodificadas, a não ser que ele consiga descobrir chave utilizada (configuradas no AP e nos clientes), porém utilizando sistemas de criptografias fortes isto é praticamente impossível ou pelo menos muito difícil.

#### 4.7.1 Associação

Assim que a autenticação termina os clientes podem se associar (registrar) com o AP para ter acesso completo aos recursos de rede. Somente APs em modo infraestrutura fazem a associação de clientes, em redes Ad-Hoc não há associação. Na associação o AP vincula o cliente com um identificador de associação (ID), vinculado ao endereço MAC daquela estação.

Veja a figura abaixo que o cliente envia uma requisição de associação ao AP (association request) e o AP responde informando se o cliente está ou não associado (association response).



Ao final do processo de associação os clientes podem estar nos seguintes estados:

- **Não autenticado e não associado** – Nesta fase inicial o nó wireless está desconectado da rede e incapaz de encaminhar seus quadros através do AP. Os APs geralmente mantêm uma tabela de status de conexão de clientes conhecida como tabela de associação.
- **Autenticado e não associado** – Nessa segunda fase, o cliente está autenticado, mas não associado com o AP. O status da tabela de associação do AP mostrará AUTENTICADO, mas o cliente ainda não pode passar dados através do AP.
- **Autenticado e associado** – Esta é a última fase, o cliente por estar associado já pode encaminhar seus dados através do AP, ou seja, está totalmente conectado à rede. A tabela de associação agora mostrará o status ASSOCIADO.

## 5 Tecnologias Wireless da Família 802.11

A primeira versão do padrão 802.11 foi lançada em 1997, após aproximadamente 7 anos de estudos. Com o surgimento de novas versões, a versão original passou a ser conhecida como 802.11-1997 ou 802.11 Legacy. Atualmente temos os padrões 802.11 "a", "b", "g" e "n" no mercado, além disso, existem os padrões 802.11ac e 802.11ad em desenvolvimento. Veja a tabela abaixo com as principais características de cada padrão.

Protocolo 802.11	Ano de Lançamento	Freq. (GHz)	Largura de Banda do Canal (MHz)	Taxa de dados por Stream (Mbps)	Número de Streams MIMO Permitidos	Modulação	Distância Indoor (m)	Distância Outdoor (m)	
Legacy	jun/97	2.4	20	1, 2	1	DSSS, FHSS	20	100	
a	set/99	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	120	
		3.7					—	5.000	
b	set/99	2.4	20	1, 2, 5.5, 11	1	DSSS	35	140	
g	jun/03	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	140	
n	out/09	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM	70	250	
			40	15, 30, 45, 60, 90, 120, 135, 150			70	250	
ac (DRAFT)	nov/11	5	20	Até 87.6	8		A definir		
			40	Até 200					
			80	Até 433.3					
			160	Até 866.7					

Um detalhe importante é que ao escolher uma tecnologia ou padrão 802.11 para o ponto de acesso sem fio (AP), deve-se verificar também se a placa de rede sem fio do cliente suporta o mesmo padrão, ou então, se pelo menos há compatibilidade entre os padrões.

Deve-se tomar muito cuidado ao misturar padrões, pois, em alguns casos a velocidade do AP acaba sendo limitada pela menor suportada entre dois padrões, acabando por diminuir a velocidade que seus clientes se conectam com sua rede sem fio. Seria similar a montar uma estrutura de cabeamento categoria 6 e utilizar nos clientes placas Ethernet a 10Mbps!

A partir desse primeiro modelo de WLAN foram lançados vários outros padrões e provavelmente muitos outros virão no futuro. Na sequência você estudará as principais características de cada um dos padrões de wireless, os quais estão em uso em diversas redes até os dias de hoje.

### **5.1 Padrão 802.11b**

Em 1999, foi lançada uma atualização do padrão 802.11 que recebeu o nome **802.11b**. A principal característica desta versão é a possibilidade de estabelecer conexões nas seguintes velocidades de transmissão: 1 Mbps, 2 Mbps, 5.5 Mbps e 11 Mbps.

O intervalo de frequências é o mesmo utilizado pelo 802.11 original (entre 2,4 GHz e 2,4835 GHz), mas a técnica de transmissão se limita ao DSSS, uma vez que o FHSS acaba não atendendo às normas estabelecidas pela Federal Communications Commission (FCC) quando operada em transmissões com taxas superiores a 2 Mbps. Para trabalhar de maneira efetiva com as velocidades de 5.5 Mbps e 11 Mbps, o 802.11b também utiliza uma técnica chamada Complementary Code Keying (CCK).

A área de cobertura de uma transmissão 802.11b pode chegar, teoricamente, a 140 metros em ambientes abertos e pode atingir uma faixa de 35 metros em lugares fechados (tais como escritórios e residências). É importante frisar, no entanto, que o alcance da transmissão pode sofrer influência de uma série de fatores já estudados aqui, tais como objetos que causam interferência ou impedem a propagação da transmissão a partir do ponto em que estão localizados.

Para manter a transmissão o mais funcional possível, o padrão 802.11b (e os padrões sucessores) pode fazer com que a taxa de transmissão de dados diminua até chegar ao seu limite mínimo (1 Mbps) à medida que uma estação fica mais longe do ponto de acesso. O contrário também acontece: quanto mais perto do ponto de acesso, maior pode ser a velocidade de transmissão.

O padrão 802.11b foi o primeiro a ser adotado em larga escala, sendo, portanto, um dos responsáveis pela popularização das redes Wi-Fi.

### **5.2 Padrão 802.11a**

O padrão 802.11a surgiu quase na mesma época que a versão 802.11b. Sua principal característica é a possibilidade de operar com taxas de transmissão de dados nos seguintes valores: 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps e 54 Mbps.

O alcance do 802.11a é de aproximadamente 50 metros para ambientes indoor e até 5 km para ambientes externos, além disso, sua frequência de operação é diferente do padrão 802.11 original, passando a operar na faixa dos 5 GHz.

O uso desta frequência é conveniente por apresentar menos possibilidades de interferência, afinal, este valor é pouco usado. Por outro, pode trazer determinados problemas, já que muitos países não possuem regulamento para essa frequência. Além disso, esta característica pode fazer com que haja dificuldades de comunicação com dispositivos que operam nos padrões 802.11 original e 802.11b. Além da frequência de 5GHz, o padrão 802.11a pode operar em 3.7GHz, uma opção para países onde o 5GHz não estiver regulamentado.

O padrão 802.11a utiliza uma técnica de modulação conhecida como Orthogonal Frequency Division Multiplexing (OFDM). No OFDM a informação é dividida em vários pequenos conjuntos de dados que são transmitidos simultaneamente em diferentes frequências, com o objetivo de impedir que uma interfira na outra, fazendo com que a técnica OFDM funcione de maneira bastante eficiente.

Apesar de oferecer taxas de transmissão maiores, o padrão 802.11a não chegou a ser tão popular quanto o padrão 802.11b.

### **5.3 Padrão 802.11g**

O padrão 802.11g foi disponibilizado em 2003 e foi tido como o "sucessor natural" da versão 802.11b, pois os dois padrões são compatíveis. Isso significa que um dispositivo que opera com 802.11g pode interoperar com outro que trabalha com 802.11b sem qualquer problema, exceto o fato de que a taxa de transmissão de dados fica limitada ao máximo suportado pelo 802.11b.

A principal vantagem do padrão 802.11g é poder trabalhar com taxas de transmissão de até 54 Mbps, assim como o padrão 802.11a, porém o 802.11g opera com frequências na faixa de 2,4 GHz e possui praticamente o mesmo poder de cobertura do seu antecessor, o padrão 802.11b.

A técnica de transmissão utilizada pelo 802.11g também é o OFDM, porém quando é feita comunicação com um dispositivo 802.11b, a técnica de transmissão passa a ser o DSSS.

### **5.4 Padrão 802.11n**

O desenvolvimento da especificação 802.11n teve início em 2004 e foi finalizado em setembro de 2009.

O 802.11n tem como principal característica o uso de um esquema chamado Multiple-Input Multiple-Output (MIMO), o qual falamos anteriormente, capaz de aumentar consideravelmente as taxas de transferência de dados por meio da combinação de várias vias de transmissão em múltiplas antenas. Com isso, é possível, por exemplo, usar dois, três ou quatro transmissores e receptores para o funcionamento da rede.

Uma das configurações mais comuns neste caso é o uso de APs que utilizam três antenas (três vias de transmissão) e clientes com a mesma quantidade de receptores. Somando esta característica de combinação com o aprimoramento de suas especificações, o padrão 802.11n é capaz de fazer transmissões na faixa de 300 Mbps e, teoricamente, pode atingir taxas de até 600 Mbps.

Em relação à sua frequência, o padrão 802.11n pode trabalhar com as faixas de 2,4 GHz e 5 GHz, o que o torna compatível com os padrões anteriores, inclusive com o 802.11a (pelo menos, teoricamente). Sua técnica de transmissão padrão é o OFDM, mas com determinadas alterações, devido ao uso do esquema MIMO, sendo, por isso, muitas vezes chamado de MIMO-OFDM.

Alguns estudos apontam que sua área de cobertura pode passar de 400 metros com antenas omnidirecionais.

## 5.5 Padrão 802.11ac

O padrão 802.11ac está sendo apontado como sucessor padrão do 802.11n. Esse padrão, no momento da elaboração desse curso, ainda está em desenvolvimento mas pode ser finalizado logo. Acredita-se que esse padrão deve ser adotado de maneira massiva a partir do seu lançamento, pois sua principal vantagem está em sua velocidade que passa a ser de 450 Mbps a 1 Gbps.

O 802.11ac trabalhará na frequência de 5 GHz e possuirá técnicas mais avançadas de modulação, pois trabalhará com o esquema MU-MIMO (Multi-User MIMO), que permite transmissão e recepção de sinal de vários terminais, como se estes trabalhassem de maneira colaborativa, na mesma frequência.

## 5.6 Padrão 802.11ad

O IEEE 802.11ad ou "WiGig" é um padrão em desenvolvimento e promissor em termos de velocidade, prometendo até 7 Gbps de banda para dispositivos próximos.

A ideia central do padrão 802.11ad é permitir que notebooks, smartphones e tablets possam se conectar às redes Wi-Fi atuais para acesso à web e dos recursos da rede, e usarem o 802.11ad para transferência de arquivos e streaming de mídia a curtas de distâncias. Nesse cenário o 802.11ad funcionaria como uma espécie de **Wi-Fi direct** de nova geração.

## 6 Segurança em Redes sem Fio

Devido à característica básica de uma rede sem fio, a de **irradiar o sinal através do espaço aberto**, ela naturalmente enfrenta maiores riscos de segurança que uma rede cabeada. Como o sinal pode irradiar para fora dos domínios físicos da empresa ou residência, atacantes externos podem capturar o sinal e conseguir invadir a rede com fins obscuros.

Os principais tipos de ameaças às redes sem fio são:

- **War drivers:** O termo “war driving” se aplica à prática de usar equipamentos com antenas de alto ganho e software para captar os pacotes de identificação da rede e registrar sua localização. Os war drivers fazem anotações sobre o protocolo usado, se há criptografia ativa, qual o SSID e outras informações que possam facilitar um futuro ataque. Além disso, eles podem também fazer acesso à Internet a partir dessas redes, seja para fins pessoais maliciosos ou não.



- **Hackers:** Acessar uma rede através da rede sem fio muitas vezes significa estar conectado diretamente à rede LAN da empresa, por isso, para um hacker é uma tarefa muito mais simples que tentar invadir a rede via Internet e passar por firewalls ou outros dispositivos de segurança mais avançados.
- **Funcionários das empresas:** Empregados das empresas podem, mesmo sem querer, facilitar o trabalho de hackers ligando APs não autorizados na rede e espalhando o sinal para fora do ambiente corporativo.
- **Rogue AP(AP Clandestino ou Desonesto):** Um hacker pode espiar as redes sem fio que estão sendo anunciadas, copiar os parâmetros e configurar em um AP próximo a empresa para que os clientes se confundam e conectem-se a esse AP clandestino. Dessa forma, o hacker poderá procurar por usuários, senhas ou copiar informações dos computadores dos usuários.



Portanto, uma rede sem fio precisa ser protegida para evitar acessos indevidos. Na sequência vamos estudar as principais ferramentas para prevenção contra esses ataques.

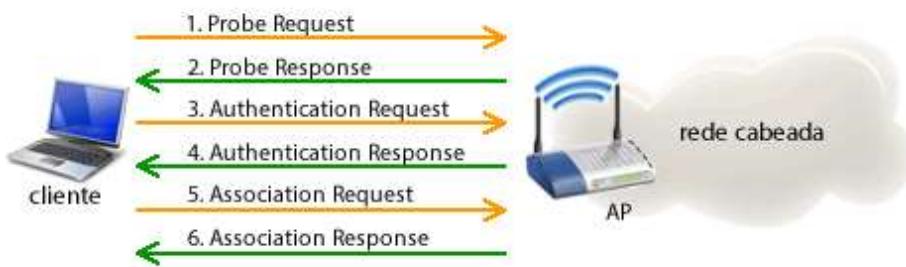
### 6.1 Ferramentas para Prevenção Contra Ataques a WLANs

As três principais ferramentas contra os ataques citados no tópico anterior são:

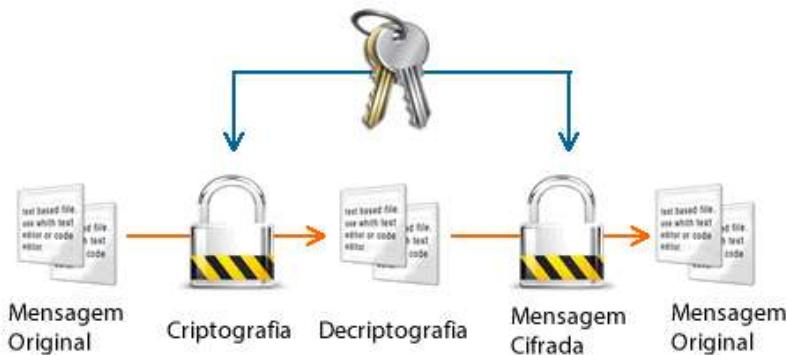
- Autenticação mútua
- Criptografia
- Prevenção contra intrusão

A autenticação mútua deve ser utilizada entre o AP e o cliente e é realizada através de uma senha secreta, chamada de Chave, que deve ser a mesma tanto no AP como no cliente.

O grande segredo aqui é que essa chave é conhecida apenas pelo AP e pelo cliente e em nenhum momento é trocada através da interface aérea, pois através de cálculos matemáticos sofisticados o AP e o cliente conseguem certificar-se que a chave é a mesma sem a necessidade de enviá-la pela rede. Portanto, mesmo que um invasor capture os quadros trocados através da interface aérea ele não conseguira descobrir essa chave.



O segundo método é a criptografia, processo que criptografa os dados na origem antes de enviá-los através da interface aérea. Quando o destino recebe esse quadro ele precisa conhecer uma chave secreta para decodificar a mensagem e enviá-la descriptografada às camadas superiores. Com isso, se um invasor capturar os quadros também não conseguirá decodificá-los sem conhecer a chave de criptografia configurada.



A terceira classe de ferramentas é a utilização de um sistema de prevenção de intrusão ou intrusos. São equipamentos conhecidos como **IPS** (Intrusion Prevention System) e **IDS** (Intrusion Detection System), os quais serão estudados no capítulo de segurança de redes desse curso, e tem a função de analisar o tráfego de rede em busca de padrões de ataques.

Veja abaixo um resumo de como proteger a rede sem fio das ameaças comuns:

- **War driver:** utilizando uma autenticação forte.
- **Hackers roubando informações através da interface aérea:** utilizando criptografia forte.
- **Evitar que funcionários instalem APs:** utilizando IDS e uma arquitetura segura.
- **AP clandestino (Rogue AP):** utilizando autenticação forte, IDS e uma arquitetura segura.

A seguir vamos estudar os padrões utilizados para segurança em redes em fio e outras ferramentas que ajudam a prevenir possíveis invasões.

## 6.2 Padrões de Segurança Wireless

Os padrões de segurança para redes sem fio iniciaram com a criação do WEP e foram avançando conforme as técnicas de criptografia e troca de chaves foram ficando mais sofisticadas. Lembre-se que o WEP é um padrão relativamente fraco e com diversas vulnerabilidades.

Vamos agora estudar as principais características de cada um dos padrões.

### 6.2.1 WEP - Wired Equivalent Privacy

Protocolo original de autenticação e criptografia definido pelo IEEE 802.11, o qual utiliza chave que varia de 40 e 128 bits (opcional). Possui um vetor de inicialização de 24 bits transmitido em **texto claro**, isso diminui consideravelmente a força do algoritmo. Utiliza o protocolo **RC4** para codificar os dados. As chaves são configuradas manualmente nos pontos de acesso e nos clientes. Além disso, não existe uma gerência de chaves.

Os principais problemas do WEP é que ele utiliza chaves pré-compartilhadas de maneira estática, ou seja, as chaves são sempre as mesmas. Dessa forma, se os administradores de rede não alterarem essas chaves constantemente, elas podem ser descobertas por hackers. O outro problema é que a chave de criptografia de 40 bits é fácil de ser quebrada com qualquer software cracker, tal como o AirSnort.



### 6.2.2 WPA Versão 1 - Wi-Fi Protected Access

Em 2001 a IEEE começou o desenvolvimento do padrão IEEE 802.11i com intuito de prover maior segurança em redes Wireless. Em 2002 a Wi-Fi Alliance optou por usar o que já estava pronto desse padrão, nesse momento ainda não estava completo o IEEE 802.11i. Assim surgiu o WPA que representa o pré-IEEE 802.11i.

O WPA permite utilizar o TKIP para troca de chaves dinâmica e padrão 802.1x (EAP) para autenticação utilizando um servidor de autenticação RADIUS.

Existe também a possibilidade de utilizar o WPA-PSK com chaves pré-compartilhadas, que traz as vantagens do WPA sem a necessidade de um servidor RADIUS e pode ser utilizado em soluções residenciais ou em pequenas empresas. A autenticação ocorre com uma chave compartilhada, parecido com o WEP, porém depois que acontece a autenticação deriva-se outra chave para a criptografia dos dados.

O WPA oferece procedimentos de criptografia significativamente mais seguros e fortes, podendo usar chaves privadas compartilhadas, chaves únicas projetadas para cada usuário da rede ou mesmo certificações SSL para autenticação no cliente e/ou no Access Point.

Para garantir a integridade dos dados o WPA-1 utiliza o **Michael Message Integrity Code** (MIC), o qual garante que a mensagem enviada não foi alterada.

#### 6.2.3 WPA2 ou IEEE 802.11i

Considerado o estado da arte em segurança para redes Wireless. Agregou vários itens do WPA, como o uso do IEEE 802.1x/EAP e adicionou novidades, como a utilização do algoritmo forte de criptografia, o AES (Advanced Encryption Standard).

O WPA2 foi introduzido pela IEEE e pela WiFi Alliance com a intenção de aproveitar os esforços de desenvolvimento do WPA e fazer uma nova certificação para as redes sem fio. A proposta do WPA2 é substituir o WEP e outras características derivadas do padrão antigo, além de suportar os recursos adicionais de segurança não disponíveis no WPA.

Uma das principais novidades do WPA2 é a utilização do algoritmo de criptografia AES junto com o TKIP, aumentando o tamanho da chave para 256 bits, enquanto que o WPA utiliza o algoritmo RC4 com TKIP. Abaixo seguem outras vantagens do WPA2:

- Interoperabilidade com clientes que utilizam outros protocolos como WPA e WEP em um mesmo ambiente de rede;
- Oferece dois modelos de operação: Enterprise e Personal;
- Possui um Vetor de inicialização de 48 bits;
- Utiliza o AES (Advanced Encryption System), o qual é o mais poderoso algoritmo de criptografia simétrica disponível atualmente.

#### 6.2.4 Criptografia: TKIP, AES e RC4

O RC4 (ou ARC4) é o algoritmo de criptografia de fluxo utilizado nos protocolos mais conhecidos, como Secure Socket Layers (SSL) (para proteger o tráfego Internet) e WEP (para a segurança de redes sem fios). O RC4 não é considerado um dos melhores sistemas criptográficos pelos adeptos da criptografia e em algumas aplicações pode converter-se em sistemas muito inseguros. No entanto, alguns sistemas baseados em RC4 são seguros o bastante num contexto prático, como o uso dele em conjunto com chaves temporárias ou TKIP, que veremos a seguir.

O TKIP (Temporal Key Integrity Protocol) é um protocolo utilizado pelo WPA e WPA2 para reforçar a troca da chave e criptografia entre o AP e seus clientes. Ele utiliza uma chave de 128 bits, o vetor de inicialização é 48 bits e também utiliza o protocolo **RC4** para criptografar os dados, porém ele utiliza uma chave diferente por pacote (per-packet key mixing). Cada estação combina a sua chave com seu endereço MAC para criar uma chave de criptografia que é única. A chave compartilhada entre o ponto de acesso e os clientes wireless é trocada periodicamente, ou seja, o TKIP utiliza chaves dinâmicas de criptografia. Dessa forma fica mais difícil para um atacante quebrar a chave, mesmo que ele consiga, a vida útil da chave será pequena.

O Advanced Encryption Standard (AES) é uma técnica de criptografia muito segura e eficiente, mas possui a desvantagem de exigir bastante processamento. O seu uso é recomendável para quem deseja alto grau de segurança, mas pode prejudicar o desempenho de equipamentos de redes não tão sofisticados (geralmente os utilizados no ambiente doméstico). O WPA2 utiliza o AES junto com o TKIP com chave de 256 bits, um método mais poderoso que o WPA, que utilizava o TKIP com o RC4.

Também existe uma versão mais segura que o AES com TKIP chamada de AES-CCMP (Protocolo Advanced Encryption Standard - Counter CBC-MAC). O novo método de proteção da privacidade das transmissões sem fio está especificado no padrão IEEE 802.11i. O AES-CCMP fornece um método de criptografia mais seguro do que o TKIP e está disponível com a autenticação de rede WPA/WPA2-Pessoal/Empresa.

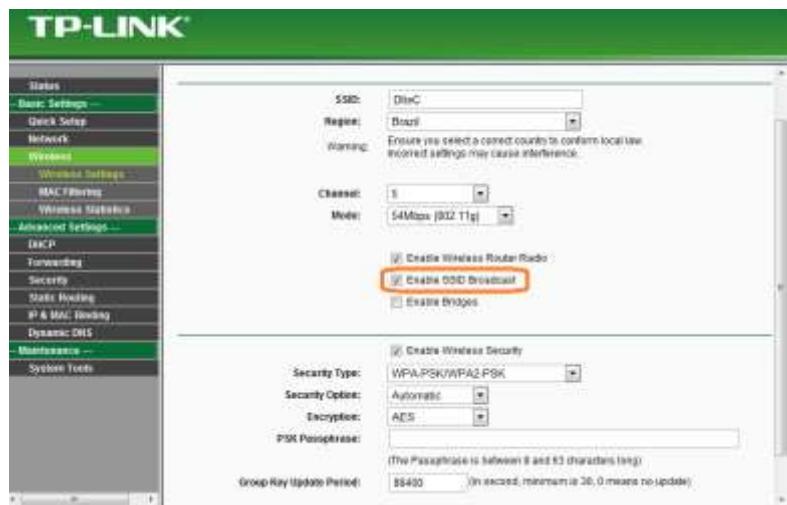
**NOTA:** É possível que algumas soluções de segurança não sejam suportadas pelo sistema operacional do computador e exijam itens de software ou hardware adicionais, além de suporte para infraestrutura de LAN sem fio dependendo de cada fabricante.

### 6.3 Outros Mecanismos de Segurança em Redes sem Fio

Além da autenticação e criptografia dos dados, é possível configurar nos APs outros recursos de segurança, como por exemplo, ocultar o SSID e a realizar a filtragem por endereços MAC.

Uma maneira simples de aumentar a segurança da rede é ocultar o SSID (Service Set Identifier) no AP. Como já vimos, o SSID é necessário para o cliente obter acesso à rede sem fio, portanto somente os computadores que conhecerem o SSID poderão acessar a rede. Ocultando o SSID ele não aparecerá na listagem de redes dos adaptadores de rede e os usuários precisarão configurar manualmente ou via script o SSID e demais informações da placa de rede. Veja na figura ao lado um exemplo das redes sem fios disponíveis em ambiente Windows. Os SSIDs ocultos não são listados nessa tela.

Na figura abaixo, você pode verificar a configuração de um AP da TP-Link, mas especificamente a configuração sobre o broadcast ou difusão do SSID. Nesse caso, ao selecionar a opção “Enable SSID Broadcast” ativamos a difusão do SSID. Quando tirarmos essa marca e salvarmos a configuração, o SSID não será mais anunciado para os clientes e precisaremos configurar manualmente na placa de rede os dados do SSID para conectar a uma rede sem fio oculta.



Outro recurso disponível na maioria dos APs é a filtragem ou liberação de clientes por Endereços MAC. Na grande maioria dos APs existe uma tabela que você pode configurar indicando o endereço MAC das placas de rede sem fios que podem completar a associação com o AP.

Portanto, somente computadores com os endereços MAC configurados nessa tabela poderão ter acesso à rede sem fio, os demais não conseguirão completar o processo de autenticação e associação com o AP e não terão acesso à rede. Veja na figura ao lado um exemplo da tela de configuração de liberação por endereços MAC em um AP da TP-Link.

ID	MAC Address	Status	Description	Modify
1	0C-...-76-75-30-AF	Enabled	PC	<a href="#">Modify</a> <a href="#">Delete</a>
2	08-...-28-12-34-56	Enabled	Cel	<a href="#">Modify</a> <a href="#">Delete</a>
3	30-...-4B-CF-9D-E1	Enabled	a Cel	<a href="#">Modify</a> <a href="#">Delete</a>
4	94-...-E5-F6-63-EB	Enabled	PC	<a href="#">Modify</a> <a href="#">Delete</a>
5	4C-...-6E-07-01-B4	Enabled	> PC	<a href="#">Modify</a> <a href="#">Delete</a>

A ideia dos mecanismos de segurança, tais como autenticação, SSID oculto e liberação de clientes por endereço MAC é evitar que computadores que não são da sua rede acessem o seu ponto de acesso sem fio e, consequentemente, acessem os recursos de rede da sua casa ou empresa. Portanto, são mecanismos que previnem o acesso indevido à sua rede sem fio, pois não temos como confinar um sinal sem fio somente nas dependências da nossa casa ou empresa, isso seria muito complexo.

Já os mecanismos de criptografia visam que uma vez autenticado e autorizado, os dados que o cliente está trocando com seu ponto de acesso não possam ser lidos caso capturados indevidamente por um hacker ou espião. O processo de criptografia codifica a informação e para decodificar é necessário saber a chave pré-configurada tanto nos clientes como no ponto de acesso. Por isso, não configure chaves óbvias ou fracas, pois seria muito fácil para um atacante descobrir por tentativa e erro, conseguindo acesso às suas informações e até à sua rede.

O problema de um acesso indevido à rede é o de roubo de informações, como usuários e senhas de e-mail ou até mesmo de acesso a um Internet Banking, acesso a arquivos dos computadores, como fotos pessoais, se for um computador corporativo o invasor pode coletar dados de clientes, produtos ou fornecedores, além do risco de um vândalo digital apagar arquivos ou danificar sistemas.

Por isso, é importante levar muito a sério a questão de segurança em redes sem fio, trocando senhas padrão de administração do ponto de acesso, utilizando chaves complexas (fortes) para autenticação e criptografia, e assim por diante. Tudo o que for executado para aumentar a segurança e evitar invasões sempre será de grande valia em uma rede sem fio!

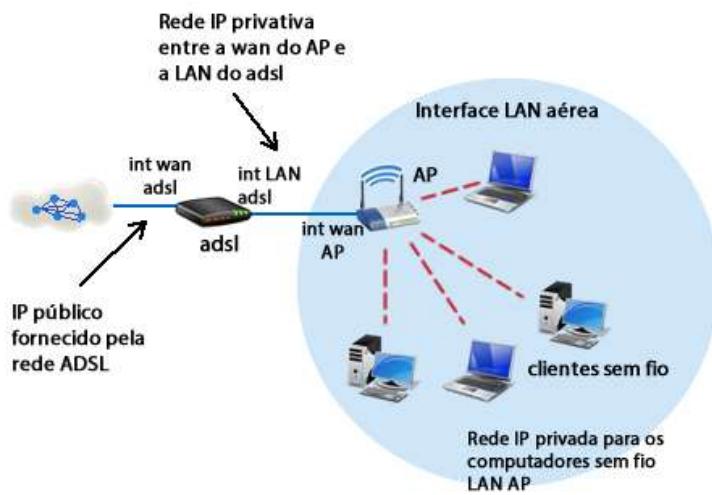
## 7 Configurando um AP e um Cliente em Windows 7

Vamos nesse capítulo focar em um modelo de ponto de acesso sem fio destinado a uso residencial ou para pequenas empresas, ou seja, APs que são modo Infraestrutura do tipo BSS.

Para instalar um AP em um ambiente residencial ou um pequeno escritório não é necessária a preocupação com o perfeito posicionamento do aparelho, pois normalmente são ambientes pequenos e colocamos o AP próximo ao equipamento que dá acesso à Internet, ao roteador ADSL ou Cable Modem. Isso quando o próprio equipamento de acesso à Internet já não tiver um AP embutido em suas funções, pois é muito comum atualmente encontrarmos roteadores ADSL já com portas RJ-45 para rede 802.3 e uma antena com padrão 802.1 a, b, g ou n.

Em empresas maiores, antes de fazer a instalação de APs recomenda-se a execução de um **"site survey"** para verificar quais os melhores pontos para instalação dos aparelhos, o tipo de antena e demais informações para a instalação dos equipamentos. No caso das soluções corporativas de maior porte, normalmente os APs são alimentados pelo cabo de rede do switch via PoE.

Voltando ao ambiente de pequeno porte, para fazer a instalação segura devemos verificar como um AP funciona na prática. Normalmente os APs possuem uma interface de WAN, uma interface de LAN (que pode ser composta de várias portas, normalmente quatro portas 10/100 Mbps) e uma interface aérea com padrão 802.11. Além disso, ele pode servir como servidor DHCP para os clientes sem fio e também como servidor DNS.



Analizando a topologia, precisaremos definir os IPs entre a Interface de LAN do modem ADSL e a Interface WAN do AP, o que pode ser deixado o padrão em ambos e essa rede será fornecida via o DHCP, normalmente habilitado por padrão nos modems ADSL. Ou então, podemos definir os IPs das interfaces e configurar IPs fixos para facilitar o gerenciamento da rede.

A segunda definição é a rede IP da interface de LAN do AP. Normalmente os APs tem um switch com algumas portas também na LAN que compartilha a mesma rede que a interface sem fio. O cuidado a ser tomado é que a rede a ser escolhida para a LAN do AP deve ser diferente da utilizada em sua WAN, pois senão haverá um conflito de IPs.

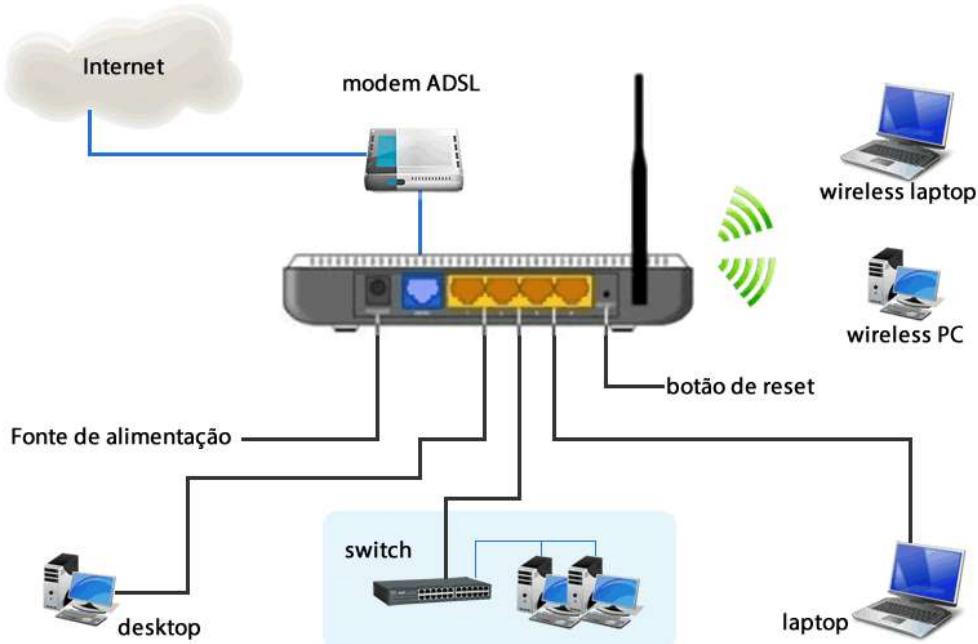
Alguns APs permitem a configuração como bridge. Nesse modo os IPs dos computadores sem fio serão passados pelo roteador ADSL, pois o AP nesse caso vira apenas uma ponte, repassando as solicitações DHCP dos clientes sem fio diretamente para o modem ADSL.

Definidas as redes IP agora temos que definir os parâmetros de gerenciamento e da interface áerea:

1. Alterar os parâmetros de gerenciamento do AP (usuário e senha de acesso administrativo);
2. Definir o SSID e seu modo de operação (oculto ou em broadcast);
3. Definir o protocolo de autenticação, de criptografia e a chave de criptografia (senha do wireless);
4. Definir se vamos fazer a liberação dos computadores clientes por endereços MAC ou não (se for utilizar esse recurso será necessário anotar os endereços MAC de todos os clientes sem fio, no Windows com o comando "ipconfig /all");
5. Implementar as configurações definidas no AP;
6. Configurar os clientes e testar a conectividade.

Alguns APs permitem várias configuração opcionais de segurança e outros recursos, tais como firewall e proteção contra DoS ou DDoS (ataque de negação de serviços). Também podemos encontrar facilidades de NAT reverso e DNS dinâmico para que seja possível acessar a partir da Internet um computador da rede interna, chamado também de configuração de DMZ (zona desmilitarizada). Alguns Access Points também possuem funções de roteador e permitem configurar rotas estáticas e até protocolos de roteamento dinâmicos simples como o RIP versão 1 e RIP versão 2, assim como gerenciamento remoto via Web e SNMP.

A seguir vamos fazer os passos de 1 a 6 definidos anteriormente para a configuração segura do roteador sem fio TP-Link modelo WR340G, o qual suporta os padrões 802.11b e 802.11g. Veja a figura abaixo com as portas e conexões do AP.



## 7.1 Alterando os Parâmetros de Gerenciamento do AP

Normalmente os APs ou roteadores sem fio vêm com um usuário e senha padrão como "admin/admin". Caso você não altere essa senha, qualquer pessoa que conseguir se conectar ao seu equipamento pode alterar as configurações ou até mesmo deixá-lo sem acesso.

Portanto, o primeiro passo é a alteração dessa senha. Para isso entre no seu web browser (IE, Mozilla ou Chrome) e digite `HTTP://IP_do_AP`, por exemplo, `HTTP://10.0.0.1`. Caso o AP seja novo, e nunca tenha sido configurado, recomenda-se conectar um cabo de rede em uma das portas de cliente e digitar o endereço informado no manual do produto (na maioria dos equipamentos é `192.168.1.1`). Ao se conectar com a tela de administração do AP pode ser solicitado um usuário e senha, se você ainda não alterou tente "admin/admin" ou leia o manual de instruções para encontrar o usuário e senha padrões do produto.

Agora vá nas ferramentas de sistema e procure o menu de alteração de senha, no caso do equipamento em questão o menu está em inglês, portanto as opções são "System Tools > Password". Veja na figura a tela de alteração de senha. Veja que você precisará inserir a senha antiga, se não foi alterada será "admin", pular o campo "New user name", ou então será criado um novo usuário de administração, digitar a nova senha duas vezes e clicar em "Save" para salvar a configuração.



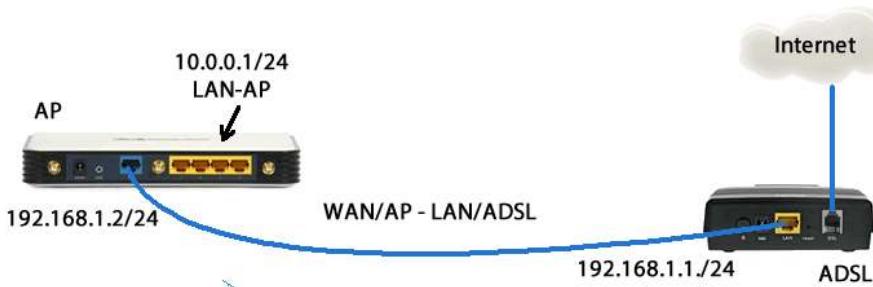
Caso você queira criar um novo usuário para administração do AP basta digitar o nome no campo "New Username" e a senha desse usuário duas vezes nos campos abaixo dele.

## 7.2 Configurando as Redes LAN e WAN do AP

Conforme já estudado no início desse tópico, a rede LAN do AP ou roteador sem fio é a utilizada na interface sem fio e também nas portas de switch que o equipamento possui.



A rede IP padrão desse modelo de equipamento é a 192.168.1.0 com a máscara 255.255.255.0. No entanto, perceba que esse é o IP padrão de vários outros modelos de equipamentos ADSL e redes sem fio também, por isso vamos alterar a rede IP da interface LAN para a classe A 10.0.0.0 com a máscara 255.255.255.0. Vamos reservar o IP 10.0.0.1 para o AP e vamos utilizar dos IPs 10.0.0.100 a 10.0.0.200 para os clientes que se conectarem via as portas RJ-45 ou interface LAN aérea. Já a rede WAN é o conector azul, o qual será conectado ao modem ADSL que já utiliza a rede 192.168.1.0 /24 e tem o IP 192.168.1.1 configurado, portanto vamos utilizar o IP fixo 192.168.1.2 com a máscara /24 para a porta WAN do AP.



Outro dado necessário para a configuração da LAN é o servidor DNS, porém, no caso dos modems ADSL podemos utilizar o IP dele como servidor DNS. No entanto, você poderia configurar os IPs passados pela operadora sem problema algum no seu AP.

Resumindo, as configurações completas das duas Interfaces do AP serão:

#### **Interface WAN:**

- IP 192.168.1.2 e máscara 255.255.255.0
- Gateway 192.168.1.1
- DNS Primário 192.168.1.1

#### **Interface LAN:**

- IP 10.0.0.1 e máscara 255.255.255.0

#### **DHCP:**

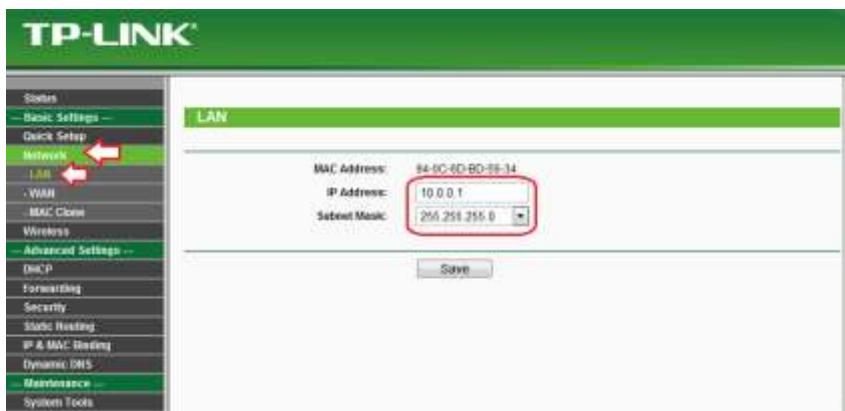
- IPs 10.0.0.100 a 10.0.0.200
- Gateway 10.0.0.1
- DNS 10.0.0.1

Normalmente o gateway e o DNS no AP são opcionais e a configuração fica como o padrão (0.0.0.0), pois o AP passa seu próprio IP como DNS e Gateway para que você não precise configurar nada se não quiser alterar as configurações.

Vamos às telas de configuração iniciando pelo IP da WAN.



Agora vamos configurar o IP da interface LAN.



Por último, vamos configurar o DHCP.



Lembre-se de clicar sempre em **Save** após finalizar a configuração da página, se você sair da página sem clicar no **Save** as configurações serão descartadas.

### 7.3 Configurando o SSID e Parâmetros da Rede Wireless

O SSID é o identificador da sua rede sem fio. Conforme já estudamos, uma opção para evitar que sua rede seja “enxergada” é a opção de “ocultar” ou “desabilitar o broadcast do SSID”, porém dessa maneira você precisará configurar manualmente a rede nos computadores cliente.

Mais um detalhe é que o SSID é uma palavra alfanumérica com no máximo 32 dígitos, sendo que ele é “case-sensitive”, isto é, diferencia letras maiúsculas e minúsculas. Portanto vamos utilizar o SSID “**DlteC-WLAN**” e também **habilitar o broadcast** do SSID (ou seja, não vamos ocultá-lo).

Além disso, vamos definir o padrão de rede a ser utilizado, lembre-se que no início falamos que o modelo do AP que estamos configurando suporta os padrões 802.11b e 802.11g, por questões de velocidade é preferível que utilizemos o 802.11g, o qual suporta até 54Mbps. Tanto o 802.11b como o 802.11g operam na faixa de frequência de 2.4GHz.

Além disso, hoje em dia a maioria das residências e prédios onde os escritórios das pequenas empresas se encontram já tem instalados diversos APs e roteadores sem fio, por isso, é interessante verificar os SSIDs já existentes, assim como os padrões de rede que estão sendo anunciados com os canais utilizados. Assim, poderemos escolher melhor o canal a ser utilizado. Normalmente os APs vêm configurados com o canal 1 como padrão e alguns até possuem o recurso de escolha automática do canal.

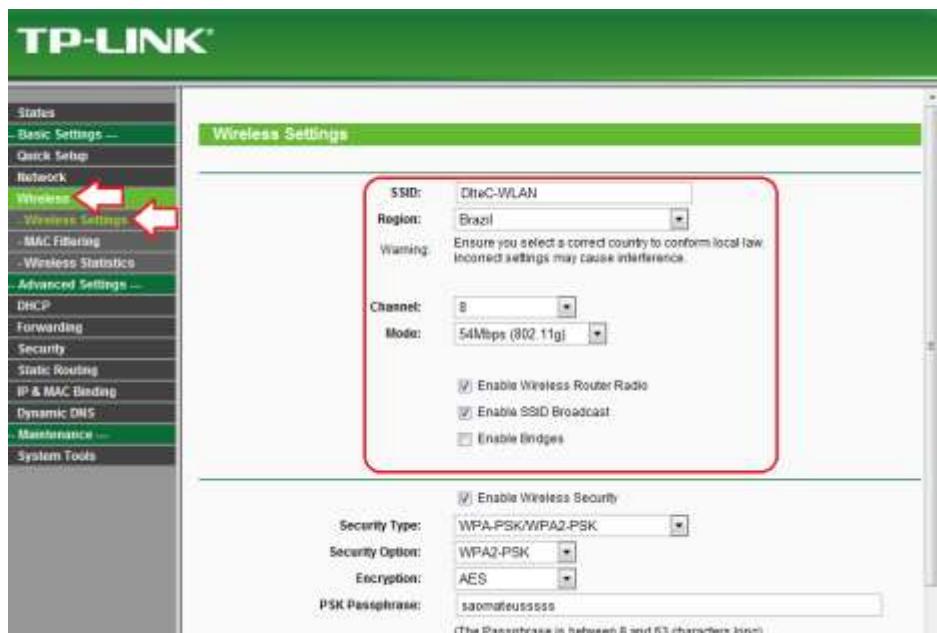
Para verificar esses dados você pode instalar em seu computador softwares que verificam as redes sem fio ao alcance do seu computador e passam de maneira gráfica ou não suas redes vizinhas. Um exemplo é o **inSSIDer**, que é gratuito e bem simples, e mostra graficamente a alocação de canais, veja a tela abaixo.



O **InSSIDer** mostra que canais estão causando interferência em quais canais (eles fazem mais coisas, porém me limitarei a estes recursos). Outra opção é utilizar o software chamado **WirelessMon**, o qual mostra as redes sem fio ao seu redor, a intensidade do sinal e também gera um gráfico dos canais mais usados nas redondezas.

Note que no exemplo mostrado será difícil de escapar de interferência, pois mesmo se utilizarmos o canal 8 ou 14 (os canais que estão livres e com um espaço em frequência entre eles) eles irão interferir com os canais vizinhos. Neste caso deveríamos utilizar o canal 14, pois a interferência será menor em relação ao canal 8, uma vez que não existe canal acima do canal 14. Se escolhermos o canal 8 haverá interferência com canais à esquerda (frequências mais baixas) e à direita (frequências mais altas). Porém, como nesta versão de equipamento, os canais do 802.11g vão de 1 a 13, teremos que escolher o canal 8.

Portanto vamos configurar o SSID “DlteC\_WLAN”, padrão 802.11g e canal 8. Veja a tela de configuração.



Marcando os checkbox "Enable Wireless Router Radio" ativamos o rádio do roteador sem fio e o "Enable SSID Broadcast" habilitamos o envio do SSID em broadcast, caso você deseje deixar o SSID oculto é só desmarcar essa opção.

Note que a configuração de segurança e criptografia está na mesma página, por isso, você pode configurar o próximo passo para depois salvar as configurações.

#### 7.4 Configurando a Autenticação e Criptografia

Na parte de segurança existe um campo "Enable Wireless Security", utilizado para habilitar a parte de segurança na comunicação sem fio. Caso você deixe desabilitado, os dados serão transmitidos entre o AP e os computadores sem criptografia, ou seja, se capturados poderão ser lidos.

Neste modelo de equipamento temos as seguintes opções de configuração:

**WEP** – Utiliza segurança baseada no padrão WEP, não recomendado por suas vulnerabilidades de segurança. O WEP pode ser configurado como:

- Automatic – Com essa opção o modo com "Shared Key" ou "Open System" é selecionado automaticamente conforme a requisição dos clientes.
- Shared Key – Força para opção de "Shared Key".
- Open System – Força para opção de "Open System".

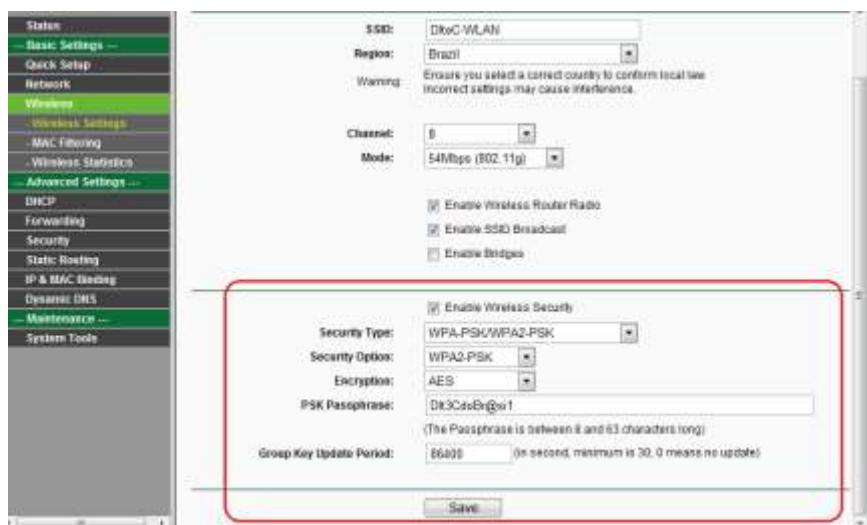
**WPA / WPA2** – Utiliza segurança baseada no padrão WPA/WPA2, porém com autenticação com servidor Radius. Esta configuração é utilizada em empresas que normalmente utilizam ambientes integrados entre os servidores de login de rede e outros sistemas, como por exemplo, o login à rede sem fio. Pode ser configurado nas seguintes maneiras:

- Automatic – Nesse padrão a configuração entre WPA ou WPA2 é baseada na requisição dos clientes.
- WPA – Força para WPA.
- WPA2 – Força para WPA versão 2.

**WPA-PSK / WPA2-PSK** – Esta é a opção mais indicada para ambientes residenciais e pequenas empresas, com o padrão WPA ou WPA2 baseado em "pre-shared passphrase" (chave ou senha pré-compartilhada). Pode ser configurada como:

- Automatic - Nesse padrão a configuração entre WPA ou WPA2 é baseada na requisição dos clientes.
- WPA-PSK – Força para o padrão WPA com chave pré-compartilhada.
- WPA2-PSK – Força o uso do WPA2 com chave pré-compartilhada.

Vamos utilizar a configuração de segurança com o WPA-PSK / WPA2-PSK, forçando para o padrão WPA2-PSK e AES como protocolo de criptografia. A "PSK Passphrase" (chave, palavra chave ou senha do wireless) deve ter entre 8 e 63 caracteres, sendo que vamos utilizar a senha como "Dlt3CdoBr@si1". Veja a tela de configuração abaixo.



Esta **PSK Passphrase** é a senha que normalmente é pedida quando selecionamos uma rede sem fio protegida, por isso é importante não utilizar sequências simples de caracteres, como "12345678" ou "abcdefgh", pois senão qualquer pessoa com algumas tentativas conseguirá se conectar a rede facilmente.

## 7.5 Configurando o Filtro de Endereços MAC

Para fazer a restrição de acesso à rede por endereços MAC primeiro é necessário anotar os endereços de todos os computadores com placa de rede sem fio que deverão ter o acesso liberado.

Em computadores com sistema operacional Windows 7 este parâmetro pode ser coletado através do comando "ipconfig /all" ou então indo na "Central de Redes e Compartilhamentos" (no caminho "Painel de Controle > Rede e Internet > Central de Rede e Compartilhamento"), clicando na conexão de redes sem fio e em detalhes, esse parâmetro é o "Endereço Físico". Veja o detalhe abaixo.



Esse mesmo procedimento deve ser feito para todos os micros e você deve tomar nota ou então copiar em um arquivo para configurar a tela do "MAC Address Filtering", conforme mostrado abaixo.

ID	MAC Address	Description	Status	Modify
1	C0-18-85-E5-EE-0B	Laptop Ditec	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

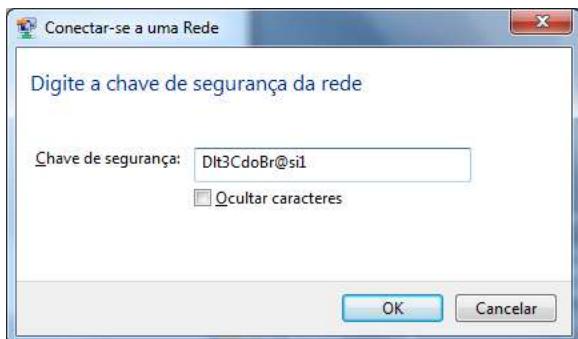
Para adicionar basta clicar em "Add New" e inserir o MAC.

## 7.6 Configurando os Clientes e Testando a Conectividade

Vamos agora fazer a configuração de um cliente sem fio baseado no sistema operacional Windows 7. Para iniciar vamos verificar se a rede sem fio configurada está sendo anunciada através do seu SSID. Para isso clicamos no ícone da interface de rede que fica no canto inferior direito do computador, ao lado do relógio do Windows.



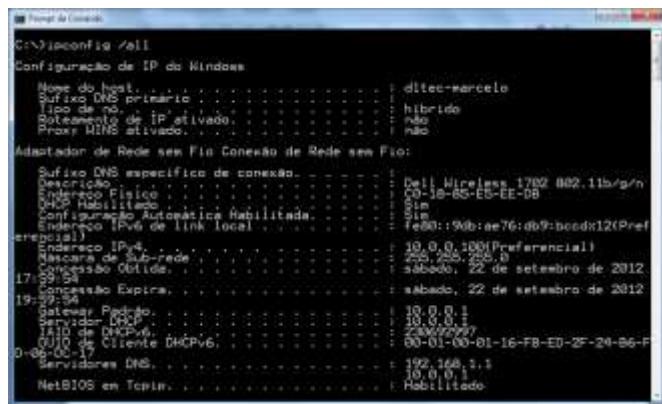
Agora basta selecionar a rede e clicar em conectar ou dar duplo clique no nome da rede sem fio DlteC-WLAN e digitar a senha (palavra passe) configura da no AP (Dlt3CdoBr@si1).



Se tudo estiver correto aparecerá uma tela sobre o tipo da rede que você está se conectando, se for na sua casa selecione rede doméstica e se em um ambiente de empresa selecione rede corporativa. A opção de rede pública deve ser selecionada quando usamos redes sem fio em um shopping center ou qualquer rede pública.



Para finalizar o teste acesse um site da Internet e com o comando “ipconfig /all” verifique se os parâmetros passados pelo DHCP estão conforme planejado e configurado. Veja a tela da figura ao lado e verifique que o endereço IPv4 passado pelo DHCP foi o 10.0.0.100 /24, o gateway é o 10.0.0.1 e o DNS 192.168.1.1, tudo conforme configurado.



No AP ou roteador sem fio você pode verificar os equipamentos conectados a rede sem fio através dos IPs alocados pelo DHCP, conforme tela mostrada ao lado, na opção “DHCP > DHCP Clients List”. Esta lista também pode ser utilizada para verificar se não existem micross não autorizados conectados ao AP indevidamente.



Até o momento o foco dos nossos estudos tem sido as LANs cabeadas ou sem fio. Nesse capítulo vamos estudar um pouco mais sobre as opções de acesso a Internet que encontraremos na prática e também como interligar as Intranets através de redes WAN.

Quando falamos de acesso a Internet e também redes WAN geralmente precisaremos utilizar roteadores para que possamos fazer a comunicação entre as diversas unidades de uma empresa.

Bons estudos.

## Capítulo 09 - Intranet, Internet e Roteadores

### Objetivos do Capítulo

Ao longo desse capítulo você deverá ter estudado e compreender os seguintes tópicos:

- O que é um roteador e suas interfaces;
- Descrever e compreender a conexão de unidades de uma empresa através de uma rede WAN;
- Entender a estrutura da Internet, opções de conexão e balanceamento de carga;
- Entender o conceito de uma VPN;
- Descrever os principais usos de uma VPN.

### Sumário do Capítulo

<b>1</b>	<b>Roteadores – Hardware e Interfaces</b>	<b>313</b>
1.1	Hardware de Roteadores	314
1.2	Principais Tipos de Interfaces WAN	316
<b>2</b>	<b>Redes Corporativas (Intranets)</b>	<b>318</b>
<b>3</b>	<b>Internet</b>	<b>319</b>
<b>4</b>	<b>VPN – Rede Virtual Privada</b>	<b>322</b>
4.1	Topologias VPN	323
4.2	Protocolo IPsec	325

## 1 Roteadores – Hardware e Interfaces

Como vamos falar de Internet e conexão de sites remotos em uma rede corporativa, muitas vezes chamada de Intranet, temos que falar um pouco mais sobre os **roteadores**. Veja as fotos abaixo.



Como já estudamos anteriormente, o roteador é um dispositivo de rede que atua na **camada 3** do modelo OSI, ou seja, na **camada de rede**. Basicamente é um dispositivo que tem a função de **interconectar as diversas redes IP** e realizar o **roteamento**, ou seja, o encaminhamento **dos pacotes IP** entre as diversas redes IP que compõe a Internet ou uma Intranet.

Como cada interface do roteador é um **domínio de broadcast**, cada interface está vinculada a uma rede ou subrede IP e através da consulta da sua **tabela de roteamento** o roteador encaminha os pacotes (analisando o endereço IP de destino) para as interfaces corretas. Veja a figura a seguir com um exemplo de tabelas de roteamento IP baseadas no protocolo RIP.



Tabela de Roteamento			Tabela de Roteamento			Tabela de Roteamento		
10.1.0.0	E0	0	10.1.0.0	S0	1	10.1.0.0	S0	2
10.2.0.0	S0	0	10.2.0.0	S0	0	10.2.0.0	S0	1
10.3.0.0	S0	1	10.3.0.0	S1	0	10.3.0.0	S0	0

O segredo da flexibilidade dos roteadores é o grande número de interfaces que eles podem suportar e, consequentemente, o grande número de protocolos de camada 2 que eles podem utilizar para se conectar com as diversas redes remotas.

Os roteadores podem ser interconectados às redes com interfaces da família Ethernet (Eth, Fast e Giga) na rede LAN. Já para rede WAN podem utilizar interfaces seriais, interfaces analógicas (dial-up), interface digital E1 ou T1, interfaces ADSL ou 3G, interfaces SDH/Sonet e muito mais, suportando protocolos de camada 2 como PPP, HDLC, Frame-relay, MPLS, ATM, dentre outros, o que os tornam equipamentos capazes de se conectar com praticamente quaisquer tipos de redes. Aqui vale uma observação, existem roteadores de todos os portes (capacidade) e quanto mais conexões, tecnologias e recursos ele suportar mais caro será o valor final do equipamento.

Portanto, os roteadores podem ser equipamentos simples, como os roteadores ADSL ou os roteadores sem fio de pequeno porte, até equipamentos complexos e suportar diversos serviços integrados em um mesmo hardware (telefonia IP, rede sem fio, Voicemail, aceleração de links, firewall, IPS e muito mais), tornando-se roteadores multisserviço chamados de **Gateways**.

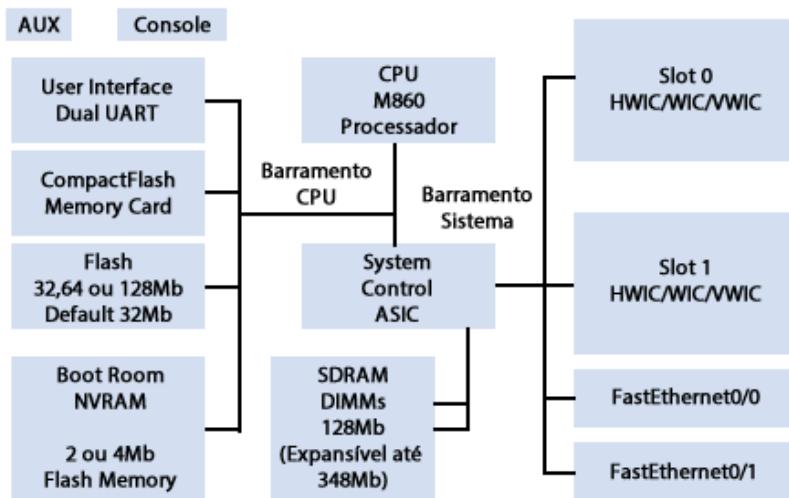
Os principais fabricantes de roteadores de uso corporativo na atualidade (até o momento que esse treinamento foi publicado) são Cisco Systems, Juniper Networks, Huawei e HP/3Com.

### 1.1 Hardware de Roteadores

A definição mais simples do hardware de um roteador é a de que ele é um computador de uso específico, ou seja, um computador customizado para a parte de roteamento e serviços de conexão de rede. Portanto, o hardware de um roteador, assim como um computador, terá:

- Placa mãe com uma CPU e Barramento
- Memórias (ROM, RAM/DRAM, Flash)
- Interfaces LAN (Ethernet, Fastethernet, Gigabit Ethernet)
- Interfaces WAN (Serial, discada, ADSL, E1, T1, T3, etc.)
- Interfaces de monitoração (local, SSH, Telnet, SNMP)

Veja na figura abaixo o esquema do hardware de um roteador do fabricante Cisco modelo 1841. Nesse modelo temos um processador M860, com dois slots para encaixar interfaces WAN (Slot 0 e Slot 1), duas interfaces de LAN onboard (Fastethernet 0/0 e Fastethernet 0/1), memórias RAM do tipo SDRAM com soquete do tipo DIMM e assim por diante.



Já na figura a seguir você pode observar alguns modelos de roteadores do fabricante Juniper Networks.



**J2320**



**J2350**



**J4350**



**J6350**

O software normalmente é um sistema operacional fechado, podendo ser proprietário, como o **IOS** da Cisco e o **Junos** da Juniper, ou aberto baseado em Linux.

Outro ponto sobre o hardware dos roteadores é que, assim como os switches, eles podem ser modulares ou não modulares. Temos roteadores formados por um chassis onde já vem uma placa mãe e normalmente as interfaces de LAN, sendo que o administrador de redes apenas insere módulos de WAN ou de serviços. Já os roteadores modulares têm um sub-bastidor sem nenhuma parte inteligente e será necessária uma placa processadora, fontes de alimentação e placas de tributário para formar o equipamento. Normalmente ambas as versões de hardware são para montagem em racks 19" ou podem ser acomodados em bandejas. Veja as fotos da abaixo com exemplos de roteadores Cisco modulares (7200 Vxr) e não modulares (Cisco 1900).

**Cisco 1900**



**Cisco 7200 Vxr**



Os roteadores de menor porte, como os ADSL ou roteadores sem fio, normalmente são bem mais simples e não possuem opções de expansão ou encaixe de módulos como os citados anteriormente. Eles possuem apenas uma interface de WAN e uma de LAN, a qual pode ser uma porta ou um pequeno switch de 4 portas para conectar mais equipamentos de LAN.

## 1.2 Principais Tipos de Interfaces WAN

Quando falamos de redes WAN (rede de longa distância) essa conexão, na maioria das vezes, depende de um **provedor de serviços de Telecomunicações (Operadora de Telecom)**. Aqui no Brasil, dependendo da sua região, podem ser utilizadas várias tecnologias para entrega dos serviços em seus clientes.

Atualmente as interfaces utilizadas nos circuitos de WAN corporativo, assim como para entrega de links de Internet dedicado, são:

- Interfaces Seriais
- Interfaces E1
- 10/100 Mbps com RJ-45
- ADSL
- 3G/4G
- Dial-up e ISDN

As interfaces seriais, muitas vezes nomeadas como links dedicados, são utilizadas em conexões ponto a ponto (via os protocolos PPP ou HDLC) ou em links que utilizam a tecnologia Frame-relay. A terminação desse tipo de circuito é feita na maioria das vezes com cabos V.35, onde uma ponta fêmea (DCE – Data Communications Equipment) fica em um modem (em inglês, CSU/DSU) da operadora e um conector macho sai do roteador (DTE – Data Terminal Equipment). Veja um exemplo na foto da figura abaixo.



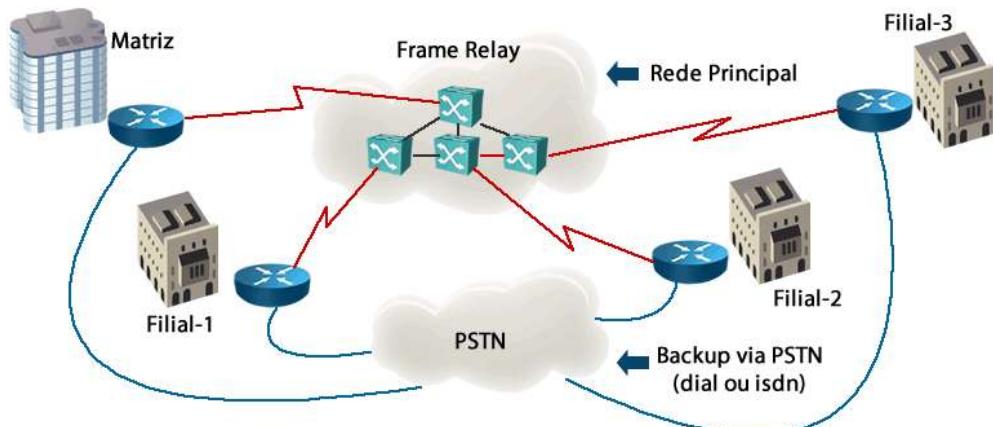
As interfaces E1 normalmente são utilizadas para conexão de canais de voz, pois ela tem a capacidade de transportar 30 canais simultâneos de voz, ideais para conexões de PABX ou gateways de voz de maneira agregada. Porém, os canais E1 também podem transportar dados com velocidades múltiplas de 64kbps e algumas operadoras entregam o link de voz e dados em um mesmo link, por exemplo, 15 canais para voz e 15 canais para dados ( $15 \times 64 = 960$ kbps). As interfaces E1 podem ser conectadas via par metálico, com uma terminação de  $120\Omega$  ou através de cabo coaxial com conectores BNC de  $75\Omega$  (opção mais utilizada).

Outra maneira das operadoras entregarem os serviços de WAN e Internet, o qual está crescendo cada vez mais, é através de rádios digitais que tem sua saída já no padrão Ethernet 10/100 Mbps com conector RJ-45 ou então utilizando fibras ópticas e conversores de mídia, também com a saída em UTP/RJ-45, o que facilita bastante a conexão dos equipamentos.

Existem outras opções de conexão, como o T3 com velocidade de 34Mbps e utiliza também cabos coaxiais com conectores RJ-45, porém não são tão usuais com as comentadas anteriormente.

Além disso, podemos utilizar interfaces ADSL com o uso de VPN (que veremos a seguir com mais detalhes) para criar uma rede WAN virtual através da Internet, pois as interfaces ADSL não podem ser utilizadas para criação de caminhos ponto a ponto entre as empresas como citado com as interfaces anteriores. Além disso, diversas empresas tem utilizado as próprias interfaces ADSL, assim como 3G/4G, com VPN para conexão à sua rede e acesso aos sistemas internos, possibilitando uma infraestrutura de conectividade mais barata e flexível. Como exemplo desses casos podemos citar bancos (para caixas automáticos – ATM) ou empresas que montam quiosques para vendas de produtos em Shopping Centers ou centros comerciais.

Estas interfaces, assim como interfaces discadas (linhas analógicas ou ISDN), podem também ser utilizadas como opção de backup de menor velocidade, mantendo apenas serviços essenciais ou um canal para entrada remota para realização de diagnóstico e resolução de problemas. Veja a topologia da figura a seguir onde temos uma rede principal de alta velocidade com tecnologia Frame-relay e conexões backup via ISDN ou Dial-up para o caso de falhas no circuito principal.

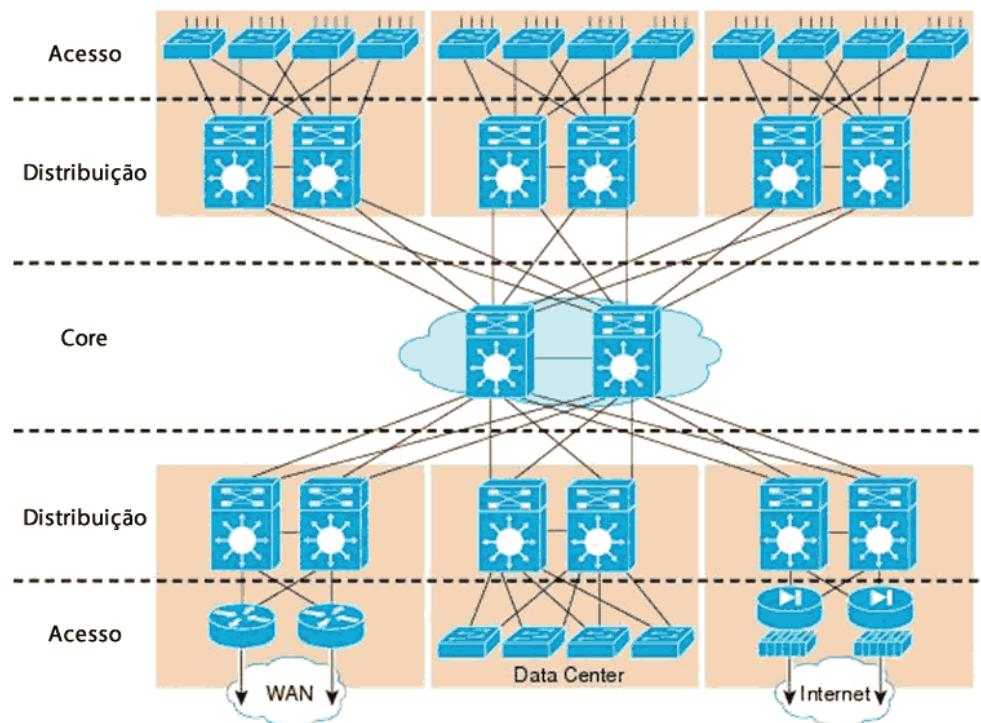


## 2 Redes Corporativas (Intranets)

Agora que já vimos o conceito das redes WAN podemos completar o conceito da Intranet ou Rede Corporativa, ou seja, a rede interna de uma empresa.

Uma empresa que tem diversas unidades distantes umas das outras terá que utilizar os serviços de conectividade de um provedor de serviços de telecomunicações para conectar a sua unidade central (matriz) às demais unidades remotas (filiais ou branch office).

Veja na figura abaixo como as conexões WAN podem entrar considerando uma infraestrutura de grande porte e o modelo de projeto em 3 camadas.



Note que os roteadores que trazem as conexões WAN com os links que ligam aos escritórios remotos estão entrando como se fossem switches da camada de acesso, ou seja, a distribuição que dará entrada aos links de WAN. O mesmo é feito com os servidores ou links de Datacenter e com as entradas de Internet (podem ser várias por questões de redundância).

Já em redes de menor porte normalmente as funções de distribuição e core estão agregadas em um só dispositivo e os links WAN chegam nesse equipamento.

O importante é que nas conexões internas de uma rede corporativa, principalmente em links WAN, sejam computados todos os tipos de tráfego necessários. Também devemos levar em conta suas características e exigências de tráfego para que não se tenha "lentidão" no acesso aos recursos corporativos centralizados, tais como acesso à bancos de dados dos sistemas corporativos.

O uso da voz sobre o protocolo IP também exige um projeto específico e que seja adicionada, além da banda necessária, a qualidade de serviços (QoS). O QoS são técnicas de marcação, priorização e enfileiramento dos pacotes IP visando dar a devida "**banda e prioridade**" conforme a necessidade de cada fluxo de rede. Por exemplo, durante um download utilizando o protocolo HTTP a tendência de ocupação da banda é para o máximo que você tenha disponível, porém imagine que ao mesmo tempo um funcionário fez uma ligação através do sistema de telefonia IP (VoIP), o que irá acontecer? Como em uma rede, por padrão, a operação é FIFO

(first in first out), ou seja, quem chega primeiro sai e os pacotes de voz terão que esperar até que o download termine para poderem ser enviados. Fica claro que essa ligação vai ter atraso ou picotes na fala, pois o fluxo de pacotes de voz não será constante e vai ficar parando no meio do caminho devido a essa “disputa de banda” com o HTTP. O QoS previne justamente esse tipo de problema, dando prioridade para os protocolos que precisam de mais velocidade e menos atraso, porém sem esquecer dos demais fluxos da rede.

### 3 Internet

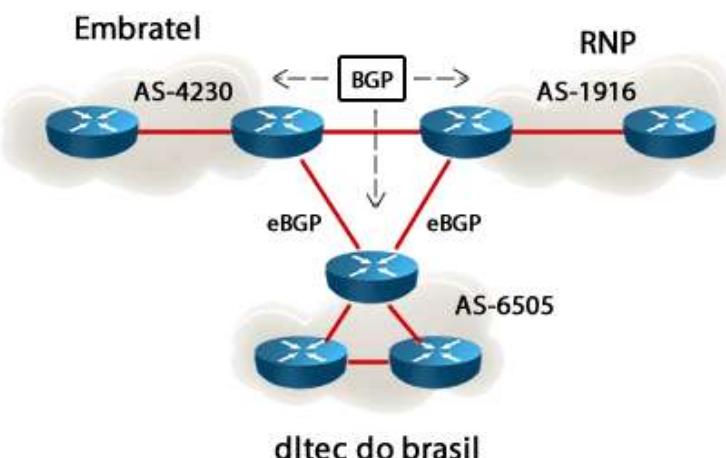
A Internet é uma rede mundial formada por diversas redes IP de empresas, provedores de serviços de Internet (ISP), entidades governamentais (como faculdades e redes de pesquisa) e outras entidades chamadas de Sistemas Autônomos (AS – Autonomous System).

Os sistemas autônomos são identificados por números de sistema autônomo ou ASN (Autonomous System Number), seguem alguns exemplos de ASNs brasileiros:

- AS 8167 Brasil Telecom
- AS 1916 RNP
- AS 10429 Telefonica
- AS 15201 UOL
- AS 18881 GVT
- AS 22055 Banco Central do Brasil

Ser um sistema autônomo significa que a entidade (pública ou privada) terá sua **própria faixa de endereços IP** e terá que se conectar com os demais sistemas autônomos através de um protocolo de roteamento chamado **BGP versão 4** (Border Gateway Protocol). Como o número de rotas que a Internet possui é bastante grande e também as interfaces que conectam os ASs normalmente são de alta velocidade, os equipamentos de borda (que estão entre dois ASs) devem suportar essa carga de processamento e memória, sendo roteadores de médio para grande porte.

Veja a figura com um exemplo de conexão hipotético de três sistemas autônomos via BGP. Dentro da rede de cada instituição podem ser utilizados protocolos de roteamento internos (IGP), tais como OSPF ou RIP, mas na conexão de Internet eles são obrigados a utilizar o BGP-4.

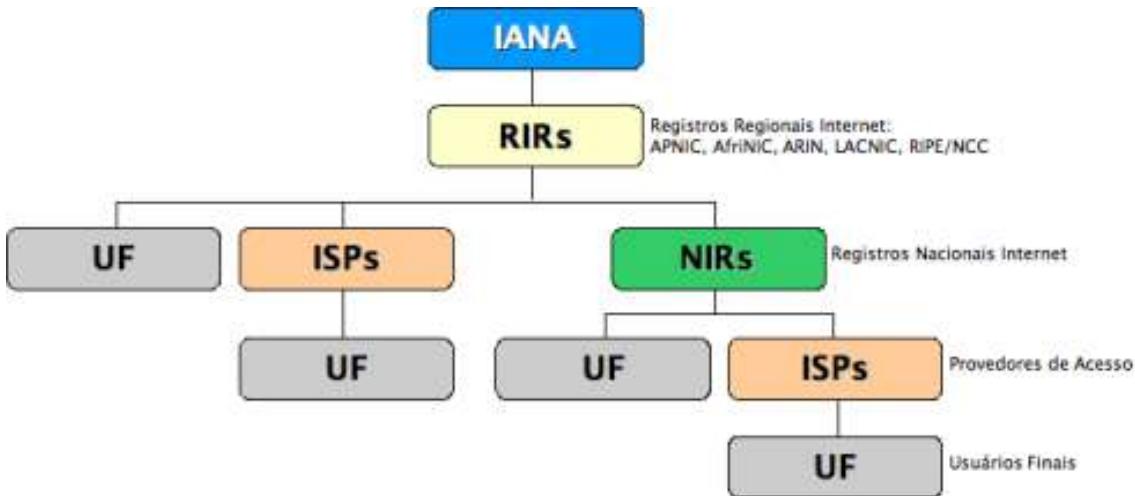


Os clientes que utilizam serviço de Internet sem ser um sistema autônomo utiliza um endereço IP da faixa alocada para o ISP a quem ele está conectado, é como se estivéssemos alugando aquele IP que utilizamos para acessar a Internet. Existem dois tipos de IPs que podemos utilizar nesse caso, o **fixo** e o **dinâmico**. O IP fixo, como o próprio nome diz, nunca muda, já o dinâmico muda conforme configuração realizada em cada provedor de Internet.

A alocação dos números de sistema autônomo, assim como a distribuição das faixas de endereçamento IP (tanto versão 4 como versão 6) é realizada por entidades não governamentais e regulada pela **IANA** (Internet Assigned Numbers Authority). A IANA divide essa administração em cinco **Regional Internet Registry (RIR)** - Registro Regional Internet conforme figura ao lado.



O Registro Regional Internet, ou RIR, para a região da América Latina e Caribe, é o LACNIC. No Brasil o Registro.br administra os Recursos de Numeração, sendo atualmente classificado como um Registro Nacional de Internet (NIR – National Internet Registry). Veja a figura abaixo com a estrutura hierárquica dessas organizações.



Portanto, no Brasil o Registro.br faz a alocação de números de sistemas autônomos e endereços IP tanto para usuários finais (UF) como para os provedores de Internet (ISP), os quais também fornecem endereço para seus usuários finais que não são sistemas autônomos.

**Informações Extras:**

Para visualizar a alocação atual das faixas de endereços IP versão 4 entre os diversos RIRs clique no link abaixo:

<http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>

Para visualizar a alocação dos endereços IP versão 6 clique no link abaixo:

<http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml>

Lembre-se que os endereços IPs de **Unicast** (utilizados para comunicação entre dois comutadores) vão de 1.0.0.0 a 223.255.255.255, sendo que as redes 10.0.0.0 /8, 172.16.0.0 /12 e 192.168.0.0 /16 são de uso privativo (RFC 1918) e não podem ser utilizadas na Internet.

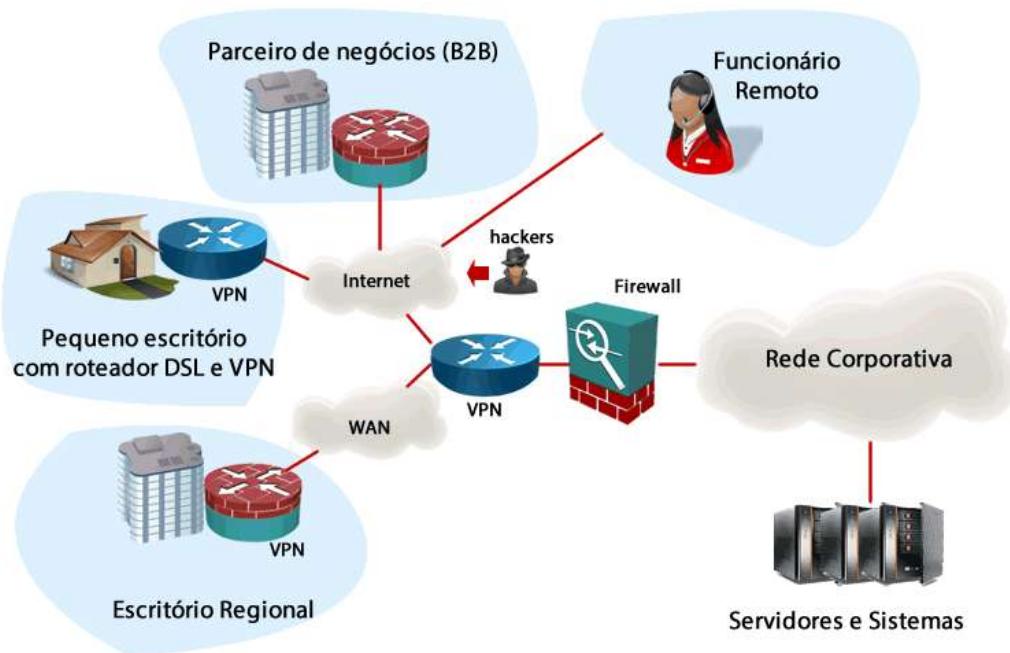
Sobre as formas de conexão com a Internet isso depende de cada provedor de serviços (ISP), mas basicamente podem ser as mesmas que citamos para links WAN, pois a Internet nada mais é que uma rede WAN, ou seja, uma rede de longa distância pública.

Quando falamos de Internet temos a distribuição de ASNs, IPs e o roteamento entre as redes, temos também o serviço de DNS Global, ou seja, o famoso "Registro de Domínios" que também é administrado por entidades globais sem fins lucrativos. No Brasil o RegistroBr acaba fazendo o papel de regulamentador e DNS raiz para as diversas extensões do nosso país, tais como ".br", ".com.br", ".org.br" e assim por diante. A lista completa de categorias de domínios disponibilizadas para o Brasil está listada no link ao lado: <http://registro.br/dominio/dpn.html>.

A entidade mundial que coordena todo o processo é a ICANN (Internet Corporation for Assigned Names and Numbers). A Internet ICANN (Corporação para Atribuição de Nomes e Números na Internet) é responsável por administrar e coordenar o **Sistema de Nomes de Domínio (DNS)** e tem a finalidade de garantir que **todo endereço seja único** e que **todos os usuários da Internet encontrem todos os endereços válidos**. Para isso, a ICANN supervisiona a distribuição de endereços IP e nomes de domínio exclusivos, assim como garante que cada nome de domínio corresponda ao endereço IP correto.

#### 4 VPN – Rede Virtual Privada

As redes virtuais privadas ou VPNs já vem sendo estudadas e implementadas a algum tempo, sendo que nos dias atuais as VPNs são frequentemente utilizadas para implementar acesso remoto e soluções site-to-site (veja a figura ao lado). VPN significa coisas diferentes para pessoas diferentes, mas em geral é um método para conectar duas redes diferentes, normalmente via Internet, através de um processo de tunelamento e criptografia.



Simplificadamente, uma VPN conecta dois pontos em uma rede pública para formar uma conexão lógica, as quais que podem ser feitas na Camada 2 ou Camada 3 do modelo OSI. As tecnologias de VPN podem ser classificados em geral como VPNs de Camada 2 (enlace) ou Camada 3 (rede).

Exemplos comuns de VPNs camada 2 são o GRE (Generic Routing Encapsulation), IPsec, L2TP e L2F. VPNs de Camada 3 podem ser conexões remotas ponto a ponto (site-to-site), como GRE em conjunto com o protocolo IPsec, ou podem estabelecer conectividade entre usuários remotos e a rede local de uma empresa através da Internet, chamado de acesso remoto.

Não podemos falar sobre VPNs sem comentar do protocolo IPsec (IP Security), o qual é baseado em uma série de RFCs (normas internacionais) que foram emitidas inicialmente durante os meados da década de 90. Estas especificações têm sido continuamente atualizadas e estão em uso no mundo inteiro. Vamos falar um pouco mais do IPsec a seguir.

Uma VPN pode garantir a segurança dos dados que estão sendo enviados pelo meio público (como a Internet) através do uso de algoritmos de criptografia. Em uma VPN os dados que devem ser protegidos são criptografados e enviados dentro de um pacote IP, garantindo que ao ser capturado por um sniffer, por exemplo, ele não possa ser decifrado.



Bem planejada, uma VPN pode trazer muitos benefícios para a empresa. Por exemplo:

- Ampliar a área de conectividade
- Aumentar a segurança
- Reduzir custos operacionais (em relação a uma rede WAN, por exemplo)
- Reduzir tempo de locomoção e custo de transporte dos usuários remotos
- Aumentar a produtividade
- Simplificar a topologia da rede
- Proporcionar melhores oportunidades de relacionamentos globais
- Prover acesso seguro ao usuário remoto externo
- Prover compatibilidade de rede de dados de banda larga
- Prover retorno de investimento mais rápido do que a tradicional WAN

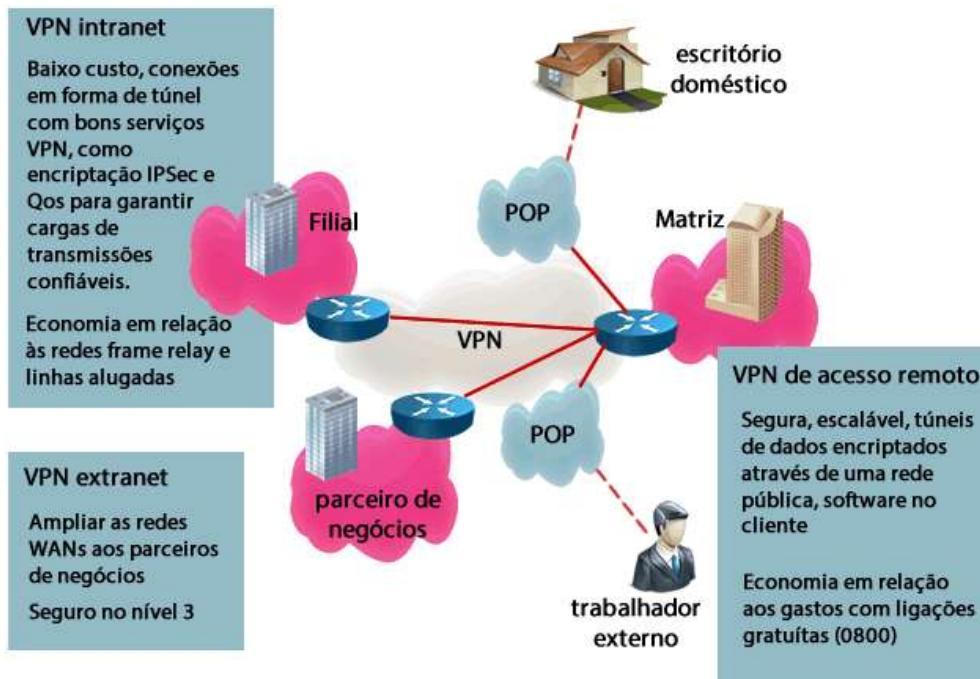
Abaixo seguem as características que um bom projeto de rede VPN deve possuir:

- Segurança (criptografia e autenticação)
- Confiabilidade
- Escalabilidade
- Gerência da rede
- Gerência de diretrizes (políticas de segurança)

#### 4.1 Topologias VPN

Falando um pouco sobre as topologias que podem ser implementadas uma VPN, geralmente temos a VPN para acesso remoto e para conectar escritórios ponto a ponto ou site-to-site.

Um dos tipos de VPN é a rede de acesso remoto, também chamada rede discada privada virtual (VPDN). Nesse tipo temos uma conexão “usuário-LAN”, ou seja, de um usuário que está normalmente na Internet à Intranet Corporativa da empresa. Comumente é utilizada por empresas cujos funcionários precisam se conectar a uma rede privada de vários lugares distantes. Quando uma empresa que precisa instalar uma grande rede VPN de acesso remoto ela pode criar sua própria estrutura ou terceirizar o processo para um provedor de serviços.



Um exemplo clássico de acesso remoto são empresas com centenas de vendedores em campo que necessitam do acesso remoto via VPN para registrar seus pedidos de vendas. O acesso remoto via VPNs permite conexões seguras e criptografadas entre redes privadas de empresas e usuários remotos por meio do serviço de provedor terceirizado. Outra aplicação é no caso de funcionários em home-office, ou seja, que trabalham sem sair de casa, ou ainda aqueles que prestam suporte em campo e necessitam acessar arquivos e sistemas da empresa de maneira segura.

No acesso remoto, o usuário acessa a rede interna da empresa do seu computador, PDA ou qualquer dispositivo que permita realizar uma VPN, através de um software cliente VPN.

Esse acesso pode ser realizado utilizando uma linha discada, seja ela através da telefonia convencional ou uma linha RDSI ou ISDN (rede digital de serviços integrados), ou através de uma Internet banda-larga, como o ADSL ou Cable Modem.

## 4.2 Protocolo IPSec

O IPSec é um framework padrão do IETF, definido pela RFC 4301, que proporciona confidencialidade, integridade e autenticação dos dados. Com o IPSec podemos criar um túnel entre dois pontos, por onde os “**dados sensíveis**” (dados que necessitam de criptografia) são enviados **protegidos**. Veja a figura abaixo com um pacote protegido pelo IPSec.



Estrutura do pacote IPSec

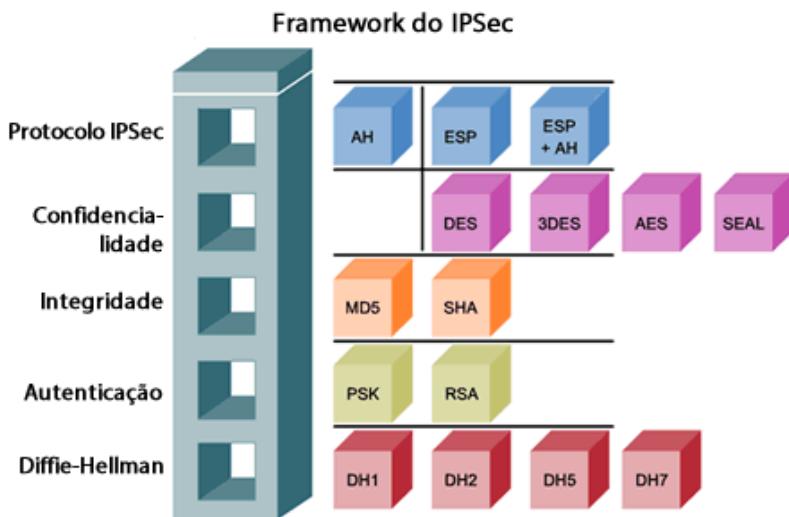
Mais especificamente, o IPsec cobre os seguintes requisitos de segurança para tráfego VPN:

- **Confidencialidade:** A confidencialidade dos dados é fornecida através da criptografia dos dados. Se um terceiro (hacker) interceptar os dados criptografados, ele não pode interpretá-lo.
- **Integridade:** A integridade de dados garante que os dados não serão modificados em trânsito. Por exemplo, roteadores em cada extremidade de um túnel podem calcular um valor de checksum, ou um valor de hash, para os dados transmitidos. Na recepção, se os dois roteadores recalculem o valor e o resultado for o mesmo, significa que os dados, muito provavelmente, não foram modificados em trânsito.
- **Autenticação:** autenticação de dados permite que as partes envolvidas na comunicação verifiquem se a outra parte é quem realmente diz ser. Existem vários métodos de autenticação possíveis com o IPSec:
  - Nomes de usuário e senhas
  - Senhas de “Um Tempo” (One-time passwords - OTP)
  - As tecnologias de biometria (como impressões digitais ou análise de exame de retina)
  - Chaves pré-compartilhada (Preshared keys)
  - Assinaturas via certificados digitais

O IPSec pode transportar as informações em dois modos, Transporte ou Túnel.

No modo transporte, somente a mensagem (payload) é criptografada, sendo que o cabeçalho IP permanece intacto. Já no modo de tunelamento, o pacote IP é criptografado por inteiro. Deve, assim, encapsular um novo pacote IP para distribuí-lo. O tunelamento é usado para comunicações de rede-a-rede (túneis seguros entre roteadores, chamadas de VPNs site-to-site) ou comunicações de host-a-rede e de host-a-host sobre a internet.

O framework IPSec, ou seja, sua estrutura, prevê dois tipos básicos de protocolos que podem ser utilizados dentro de um pacote IP. O Authentication Header (AH), que provê a autenticação e integridade dos dados, mas não a confidencialidade, e o Encapsulating Security Payload (ESP), que provê autenticação, confidencialidade dos dados e integridade da mensagem.



Na figura acima, cada funcionalidade do IPSec está em um bloco com espaços que podem ser preenchidos com os protocolos ao lado. No entanto, veja que a confidencialidade, que são os algoritmos de criptografia, não são suportados pelo AH. Para o IPSec fornecer a confidencialidade você terá que utilizar o protocolo ESP ou ESP trabalhando em conjunto com o AH (veja a linha do "Protocolo IPSec").

O segundo espaço representa o tipo de confidencialidade implementado usando um algoritmo de criptografia como DES, 3DES, AES ou SEAL. A escolha depende do nível de segurança exigido, a qual a ordem de nível de segurança (da esquerda para a direita – menos seguro para o mais seguro) segue ao lado: DES -> 3DES -> AES -> SEAL.

O terceiro espaço representa a integridade que pode ser implementada usando hashs MD5 ou SHA. Essa garantia da integridade é realizada utilizando o Hashed Message Authentication Codes (HMAC), normalmente com o MD5 ou SHA-1.

O quarto representa a forma como a chave secreta compartilhada é estabelecida. Os dois métodos são pré-compartilhada (preshared key ou PSK) ou com certificados digitais RSA. O IPSec utiliza o protocolo Internet Key Exchange (IKE) para autenticação e troca das chaves.

O último grupo representa o algoritmo Diffie-Hellman ou DH utilizado para troca segura das chaves através da Internet. Há quatro algoritmos distintos DH de troca de chaves para se escolher incluindo DH Grupo 1 (DH1), DH Grupo 2 (DH2), DH Grupo 5 (DH5) e DH Grupo 7 (DH7). O tipo de grupo selecionado depende das necessidades específicas de cada projeto. Segue abaixo uma descrição breve de cada grupo e suas aplicações práticas:

- Os grupos DH 1, 2 e 5 exponenciação de um módulo principal com um tamanho de chave de 768 bits, 1024 bits e 1536 bits respectivamente.
- Os clientes Cisco 3000 suportam grupos 1, 2 e 5. As criptografias DES e 3DES suportam grupos DH 1 e 2.
- A criptografia AES suporta os grupos DH 2 e 5.
- Os Certicom movianVPN client suportam o grupo 7.
- O grupo 7 suporta Elliptical Curve Cryptography (ECC), que reduz o tempo para geração das chaves.

Durante a configuração do túnel os pares VPN negociam o grupo DH que irão utilizar.

*Nesse capítulo vamos estudar alguns conceitos a mais sobre segurança de redes, tais como tipos de ataques e política de segurança, e também conceitos sobre gerenciamento de redes.*

*Com a constante informatização dos processos ou dos controles de determinados processos é fundamental que a rede esteja segura, não somente contra ataques, mas também contra possíveis faltas de comunicação ou corrupção de dados por acessos indevidos, por isso a segurança é um assunto cada vez mais importante para um administrador de redes.*

## **Capítulo 10 - Tópicos de Segurança e Gerenciamento de Redes**

### **Objetivos do Capítulo**

Ao final desse capítulo você deverá ter estudado e compreendido os seguintes assuntos:

- Conceitos básicos de segurança, tais como tipos de ataque e principais vulnerabilidades;
- Descrever os dispositivos e software de segurança;
- Descrever a política de segurança;
- Entender os conceitos e importância do gerenciamento de redes;
- Descrever os principais métodos de acesso remoto e de gerenciamento de equipamentos, tais como SNMP e MRTG.
- Descrever o ciclo de vida dos dispositivos de rede e os conceitos básicos da ITIL.

*Além disso, uma vez instalada uma rede ela entra em operação, ou seja, teremos que tratar de problemas que podem ocorrer devidos a infraestrutura, como cabos rompidos ou links de operadoras que ficam fora de operação, assim como mudanças na rede, tais como inclusão de novos usuários, instalação de novos equipamentos, expansões ou então desinstalação de equipamentos devido à redução de quadro, por exemplo.*

*Tudo isso exige o pleno conhecimento da rede, tanto em termos lógicos e físicos, bem como uma correta documentação.*

*Bons estudos!*

## Sumário do Capítulo

<b>1 Tópicos de Segurança</b>	<b>329</b>
1.1 Vulnerabilidades, Ameaças e Ataques	330
1.2 Tipos de Ataques	331
1.3 Termos Utilizados para Definir os Atacantes (Hackers)	334
1.4 Dispositivos de Segurança	335
1.4.1 Firewalls	336
1.4.1.1 DMZ – Zona Desmilitarizada	340
1.4.2 IDS (Intrusion Detection System) e IPS (Intrusion Prevention System)	340
1.5 Segurança nos Clientes - Softwares	344
1.6 Política de Segurança	349
1.6.1 Política de Senhas nas Empresas	349
1.7 Melhores Práticas (Best-Practices)	350
<b>2 Gerenciamento de Redes</b>	<b>351</b>
2.1 Acesso Local e Remoto – Console, Telnet, SSH e Interfaces Web	351
2.1.1 Acesso Telnet e SSH	353
2.1.2 Interface Web	355
2.2 Syslog	355
2.3 SNMP (Simple Network Management Protocol)	357
2.4 MRTG – Monitorando o Tráfego via SNMP	359
2.5 Utilizando o ICMP para Gerenciar a Rede	360
2.6 Analisadores de Protocolos e Sniffers	361

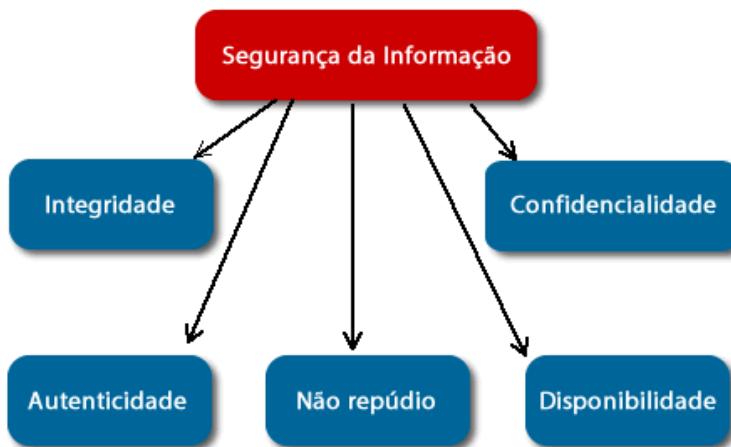
## 1 Tópicos de Segurança

Para qualquer administrador de rede na atualidade o grande desafio é “como fornecer serviços de redes de maneira segura, protegendo informações privadas, pessoais e comerciais estratégicas”.

Manter uma rede segura significa garantir a segurança dos usuários da rede e proteger os interesses comerciais das corporações. Manter uma rede segura requer vigilância por parte dos profissionais de segurança, os quais devem estar sempre cientes das novas ameaças, ataques e vulnerabilidades dos dispositivos e aplicações. Esta informação é usada para se adaptar, desenvolver e implementar técnicas de **mitigação** (investigação). No entanto, a segurança da rede é, em última análise, a **responsabilidade de todos que a utilizam**. Por esta razão, além de manter a rede segura e protegida, faz parte do trabalho do profissional de segurança de rede garantir que todos os usuários recebam treinamento de conscientização de segurança. Só assim será possível manter um ambiente de trabalho funcional para todos.

Os três principais objetivos da segurança de rede são:

- **Confidencialidade**
- **Integridade**
- **Disponibilidade**



Entende-se por **confidencialidade** a proteção da informação compartilhada contra acessos não autorizados. Podemos garantir a confidencialidade pelo controle de acesso (senhas) e controle das operações individuais de cada usuário (log). Abaixo seguem mais alguns exemplos:

- Uso de mecanismos de segurança de rede (por exemplo, firewalls e listas de controle de acesso) para impedir o acesso não autorizado aos recursos da rede.
- Exigir credenciais adequadas (por exemplo, nomes de usuário e senhas) para acesso à recursos específicos da rede.
- Criptografar o tráfego para que um atacante não consiga decifrar os dados que ele capturou a partir da rede.

A **integridade** é a garantia da veracidade da informação, que não pode ser corrompida, seja por alterações accidentais ou não autorizadas. Segue abaixo exemplos de violações de integridade:

- Modificar a aparência de um site corporativo.
- Interceptar e alterar uma transação de comércio eletrônico.
- Modificar os registros financeiros que são armazenados eletronicamente.

A **disponibilidade** é a prevenção de interrupções na operação de todo o sistema, seja ele hardware e/ou software. Por exemplo, uma quebra do sistema não deve impedir o acesso aos dados. Abaixo seguem mais alguns exemplos de como um invasor pode comprometer a disponibilidade de uma rede:

- Enviando indevidamente dados formatados para um dispositivo de rede, resultando em um erro de exceção que o dispositivo não saberia tratar, interrompendo o serviço.
- Inundando um sistema de rede com uma quantidade excessiva de tráfego ou requisições. Esta sobrecarga iria consumir recursos de processamento do sistema e impedir que o sistema responda às solicitações legítimas, fazendo com que o serviço seja negado aos usuários que realmente necessitam do serviço. Este tipo de ataque é chamado de negação de serviço (DoS – Denial of service).

### 1.1 Vulnerabilidades, Ameaças e Ataques

Em geral, analisando e simplificando o tópico segurança de rede, podemos elencar três fatores que fazem parte do assunto:

- **Vulnerabilidade:** São os **protocolos** e “**furos**” de segurança em sistemas e equipamentos que serão **explorados pelos atacantes**, por exemplo, vulnerabilidades do sistema operacional (Windows, Linux, etc.). Isso inclui roteadores, switches, desktops, servidores e até mesmo dispositivos de segurança. Além disso, as vulnerabilidades podem ser geradas pela própria tecnologia (furos de segurança nos sistemas e aplicativos), por falhas na configuração dos sistemas ou por problemas na política de segurança da corporação.
- **Ameaças:** são os indivíduos que têm interesse em realizar ataques e sempre estão procurando novas vulnerabilidades e meios para o acesso não autorizado a redes e sistemas, ou então desejam informações privilegiadas para realizar delitos. Essas ameaças podem ser tanto internas como externas à rede. Os ataques internos ainda são os que têm mais efetividade.
- **Ataques:** é a realização do que foi analisado como vulnerabilidade e colocado em prática por um atacante. Normalmente, os dispositivos de rede visados para o ataque são as extremidades, como servidores e desktops.

Além disso, podemos classificar os riscos de segurança entre físico, lógico (das redes, por exemplo) e humano (engenharia social).

Conforme mencionado anteriormente nesse curso, quando se fala de segurança vem à mente um firewall, ou seja, um dispositivo de redes, mas e o restante? E se o atacante conseguir acesso ao seu Data Center ou ao CPD da empresa? Com certeza ele está atrás do firewall e terá uma gama de ações possíveis para realizar por dentro da rede, normalmente muito mais vulnerável quando atacada por dentro!

Portanto, temos que abrir os horizontes e pensar que é importante sim a segurança de redes com firewall, IDS e IPS, porém não podemos nos esquecer da infraestrutura física e das pessoas, pois o fator humano conta muito para uma rede segura.

As ameaças à infraestrutura física podem ser resumidas em:

- **Ameaças ao hardware** – danos físicos à infraestrutura e equipamentos que fazem parte da rede.
- **Ameaças ao ambiente** – temperatura, umidade, sujeira, e outros motivos ambientais.
- **Ameaças elétricas** – sobretensão, picos de energia, descargas atmosféricas (raios), sistemas de proteção elétrica mal dimensionada, etc.
- **Ameaças à manutenção** – problemas de nomenclatura (ocasionando desligamento de equipamentos errados), janelas de manutenção mal dimensionadas, falta de manutenção preventiva, etc.

Sobre o fator humano temos que falar da **engenharia social**, que são meios de se fazer com que membros de uma corporação (até mesmo uma pessoa física) forneçam informações importantes, como o local de arquivos ou senhas, facilitando o processo de invasão.

A engenharia social pode incluir sensibilizações ao ego de um funcionário ou pode ser uma pessoa disfarçada, ou com documento falsificado, que leva uma pessoa a fornecer informações confidenciais.

Outro tema muito em foco hoje em dia são as redes sociais e não podemos esquecer que essas redes sociais também podem ser fonte de pesquisa para a **engenharia social**, permitindo que o atacante mal intencionado colete informações das pessoas de uma corporação para iniciar uma abordagem mais elaborada. O risco da engenharia social se estende para a vida pessoal, não somente para o corporativo. A cada dia cresce o número de ataques buscando informações para crimes virtuais, como roubo de senha para acesso indevido à conta bancária via Internet, clonagem de cartões de crédito e compras indevidas com os dados pessoais e de cartão de crédito de outras pessoas.

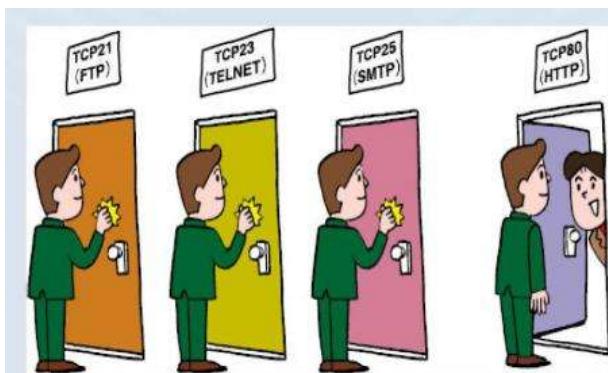
## 1.2 Tipos de Ataques

Agora vamos analisar os tipos de ataques que podem ser realizados para invadir uma rede. Podemos dividir esses ataques em três classes: **reconhecimento, acesso e negação de serviços**. Veja abaixo a definição de cada um e exemplos de ataques.

**Reconhecimento:** é a detecção não autorizada e o mapeamento de sistemas, serviços ou vulnerabilidade. Ele também é conhecido como **footprint** ou **coleta de informações** e é a **fase inicial de uma invasão**, onde o invasor está reconhecendo a rede e suas vulnerabilidades.

O invasor tenta com esses ataques descobrir uma forma mais fácil de invadir a rede, sejam equipamentos ou sistemas. Exemplos de ataques de reconhecimento:

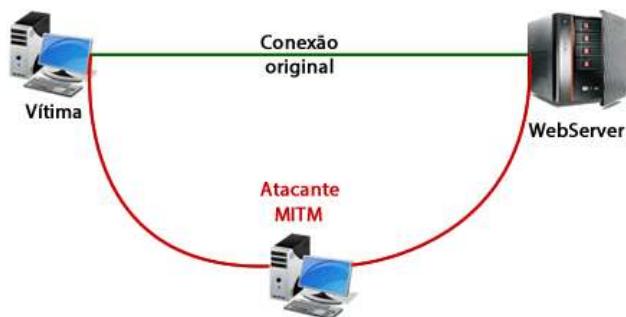
- **Consultas de informações de Internet:** utilizando ferramentas como whois e nslookup para descobrir endereços de IP de entrada para a rede.
- **Varreduras de ping:** com os endereços IP's os atacantes podem enviar pings para determinar outros IP's de outras máquinas como opções de acesso para invasão.
- **Verificações de porta (port scan):** o port scan tem o objetivo de verificar quais portas TCP e UDP estão abertas na rede (que o firewall permite acesso) para identificação das vulnerabilidades a serem exploradas (exploits).



- **Sniffers de pacote:** permitem que o atacante analise a comunicação em busca de troca de pacotes TCP e UDP não seguras para capturar usuários, senhas e outras informações úteis ao ataque. Uma VPN ou um método de criptografia pode ajudar a evitar esse tipo de ataque.

**Acesso:** é a tentativa de entrada (acesso) utilizando normalmente um script ou uma ferramenta que explore uma fraqueza conhecida do sistema, aplicativo ou dispositivo que está sendo atacado para descobrir um usuário e senha válidos, por exemplo. Exemplo de ataque de acesso:

- **Ataque de senhas:** utilização de scripts e programas para descobrir usuários e senhas para acesso a um sistema ou dispositivo. Normalmente são tentativas repetidas de login em um recurso compartilhado, como um servidor ou roteador, para identificar uma conta de usuário, senha ou ambos, também conhecido como ataque de força bruta. Um exemplo é a ferramenta L0phtCrack.
- **Exploração de confiança (Trust Exploitation):** o objetivo desse ataque é invadir um host confiável, utilizando-o para preparar ataques em outros hosts de uma rede.
- **Redirecionamento de Porta (Port Redirection):** Um ataque de redirecionamento de porta é outro tipo de ataque baseado na exploração de confiança. O atacante usa um host comprometido com acesso através de um firewall, que seriam normalmente bloqueados para um micro não confiável.
- **Man-in-the-Middle ou Ataque de Interceptação:** O ataque “man in the middle” (literalmente “ataque do homem no meio” ou “ataques do interceptor”), às vezes chamado **MITM**, é um cenário de ataque no qual um invasor “ouve” uma comunicação (utilizando um sniffer) entre dois interlocutores e falsifica as trocas a fim de fazer-se passar por uma das partes.



- **Spoofing de IP (Falsificação)** - A principal característica do Spoofing é convencer alguém de que ele é algo que ele não é, conseguindo assim, autenticação para acessar alguma parte restrita à qual ele não tem permissão, através da falsificação do seu endereço de origem.

**Negação de serviços (DoS):** Os ataques DoS são os mais temidos, é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores ou clientes. Alvos típicos são servidores web e o ataque tenta tornar as páginas hospedadas indisponíveis na WWW. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga. Exemplos de ataques de DoS:

- **DoS Distribuído (DDoS)**: Em um ataque distribuído de negação de serviço (também conhecido como DDoS, um acrônimo em inglês para Distributed Denial of Service) onde um computador mestre (denominado "Master") pode ter sob seu comando até milhares de computadores ("Zombies" - zumbis), sendo que as tarefas de ataque de negação de serviço serão distribuídas a um "exército" de máquinas escravizadas.



- **TCP SYN**: o atacante envia uma sequencia de requisições SYN para um sistema-alvo visando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação do modelo OSI. Revise o capítulo 5 sobre a abertura das conexões TCP (handshake triplo).
- **Ataque de Smurf**: o invasor envia uma rápida sequência de solicitações de ping (um teste para verificar se um servidor da Internet está acessível) para um endereço de broadcast. Usando spoofing (fazer passar por outro computador da rede para conseguir acesso a um sistema), o invasor faz com que o servidor de broadcast encaminhe as respostas não para o seu endereço, mas para o da vítima. Assim, o computador alvo é inundado pelo ping.

### 1.3 Termos Utilizados para Definir os Atacantes (Hackers)

À medida que os tipos de ameaças, ataques e meios de explorar vulnerabilidades em redes tem evoluído, vários termos foram criados para descrever os “**atacantes**”, os quais nem sempre são “do mal”. Hacker geralmente é o termo geral, historicamente utilizado para descrever um especialista em programação de computador. Mais recentemente, esse termo passou a ser utilizado de modo negativo para descrever um indivíduo que tenta obter acesso não autorizado aos recursos de rede com má intenção. Porém existe uma gama de tipos de hackers na atualidade e abaixo uma lista os termos utilizados para descrevê-los:

**White hat** – um “atacante do bem”, normalmente procura falhas nos sistemas e protocolos para informar e corrigir o risco de segurança. Traduzindo para o português chama-se hacker “chapéu branco”. Chamados também de “hackers éticos”.

**Gray hat** - Tem as habilidades e intenções de um hacker de chapéu branco na maioria dos casos, mas por vezes utiliza seu conhecimento para propósitos menos nobres. Um hacker de chapéu cinza pode ser descrito como um hacker de chapéu branco que às vezes veste um chapéu preto para cumprir sua própria agenda. Hackers de chapéu cinza tipicamente se enquadram em outro tipo de ética, que diz ser aceitável penetrar em sistemas desde que o hacker não cometa roubo, vandalismo ou infrinja a confidencialidade. Alguns argumentam, no entanto, que o ato de penetrar em um sistema por si só já é antiético (ética hacker).

**Black hat** – esse é o “**atacante do mal**”, procura invadir sistemas e redes para fins pessoais (satisfação do seu ego) ou financeiros. Cracker é um exemplo de black hat. Traduzindo para o português chama-se hacker “chapéu preto”.

**Cracker** – termo mais preciso para descrever alguém que tenta obter acesso não autorizado a recursos de rede com má intenção.

**Phreaker** – o precursor do black hat, porém utilizando normalmente telefones públicos para realizar chamadas gratuitas.

**Spammer** – esse conhecemos bem, pois recebemos uma pilha de e-mails indesejados diariamente dos spammers, os quais enviam os famosos “spams”, as propagandas, vírus e outros “lixos” eletrônicos por e-mail.

**Phisher** – utiliza email ou outros meios para levar outras pessoas a fornecer informações confidenciais, como números de cartão de crédito ou senhas. Um phisher se mascara como uma parte confiável que teria uma necessidade legítima pelas informações confidenciais.

**Script Kiddies** - subcategoria de crackers que não têm um alvo certo, vão tentando invadir tudo que vêm na frente utilizando ferramentas encontradas na Internet. Nem programar sabem, mas tem um conhecimento digital bem acima dos usuários comuns.

**Hacktivistas** - são hackers não mais preocupados em quebrar sistemas pela diversão, mas focados em questões políticas e sociais. São pessoas que dominam bits e bytes, assim como Mahatma Gandhi dominava as palavras, porém com um cunho político.

**Computer security hacker** - um hacker de que tem conhecimento sobre as técnicas e aspectos da informática e sistemas de segurança de rede. Por exemplo, esta pessoa pode tentar atacar um sistema protegido por um IPS fragmentando o tráfego malicioso de uma maneira que não são detectados pelo IPS.

**Hacker Acadêmico (Academic hacker)** - é tipicamente um trabalhador ou um estudante em uma instituição de ensino superior que utiliza os recursos de computação da instituição para escrever programas “inteligentes”. Normalmente esses hackers usam seus nomes reais (ao contrário dos pseudônimos frequentemente utilizados dos computer security hacker), e tendem a se concentrar em sistemas operacionais baseados em software livre (por exemplo, Linux).

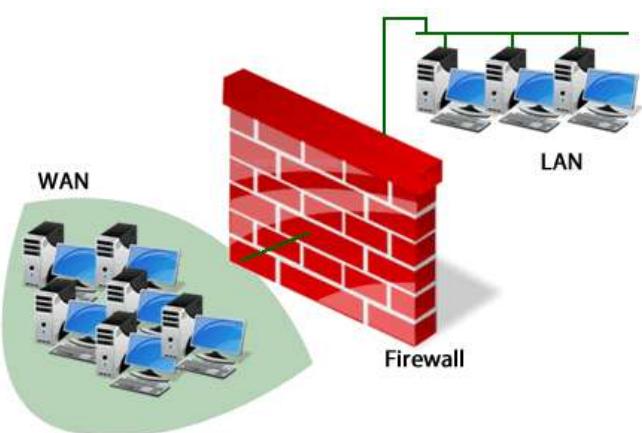
**Hacker por Hobby** - tendem a focar em computação doméstica. Eles podem modificar hardware ou software existente para uso dos mesmos sem licença legal. Por exemplo, gerar um código que “destrava” o iPhone da Apple pode ser obra de um hacker por hobby.

## 1.4 Dispositivos de Segurança

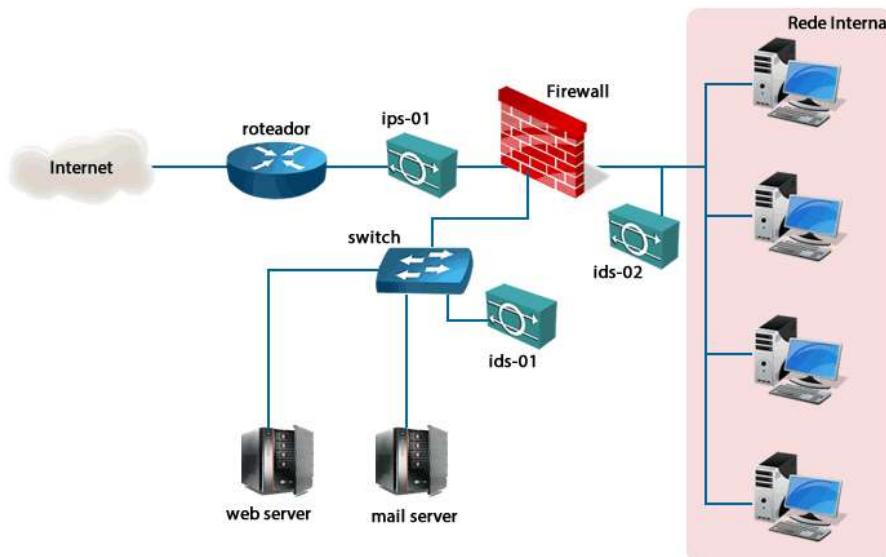
Os três principais dispositivos de segurança de redes atualmente utilizados nas corporações são:

- Firewalls
- IDS – Intrusion Detection System
- IPS – Intrusion Prevention System

Com certeza o mais falado e conhecido por qualquer pessoa que já leu ou estudou o assunto de segurança de redes ou da informação é o firewall. Estes dispositivos nasceram na década de 80 e estão presentes nas redes até os dias de hoje atuando como um filtro entre duas redes, permitindo ou negando tráfego baseado em informações das camadas 3 e 4 do modelo OSI.



Já o IDS e IPS atuam de uma forma um pouco mais ampla, analisando a aplicação e mais, indo a fundo no conteúdo dos pacotes e procurando por características (**assinaturas**) para detectar ataques mais sofisticados. Veja a figura abaixo e note que o IPS é posicionado em série com o fluxo, ou seja, ele tem condições de realmente **impedir um ataque**. Já o IDS é colocado em paralelo com o fluxo de rede, permitindo que ele analise o tráfego e apenas **informe que um ataque pode estar ocorrendo**.



#### 1.4.1 Firewalls

Os Firewalls podem ter variadas conotações para diferentes pessoas e organizações, mas todos os firewalls compartilham algumas propriedades comuns:

- Devem ser resistente a ataques
- Todos os fluxos de tráfego da Internet ou redes consideradas inseguras passam através do firewall (ponto único de acesso)
- Reforça a política de controle de acesso à rede

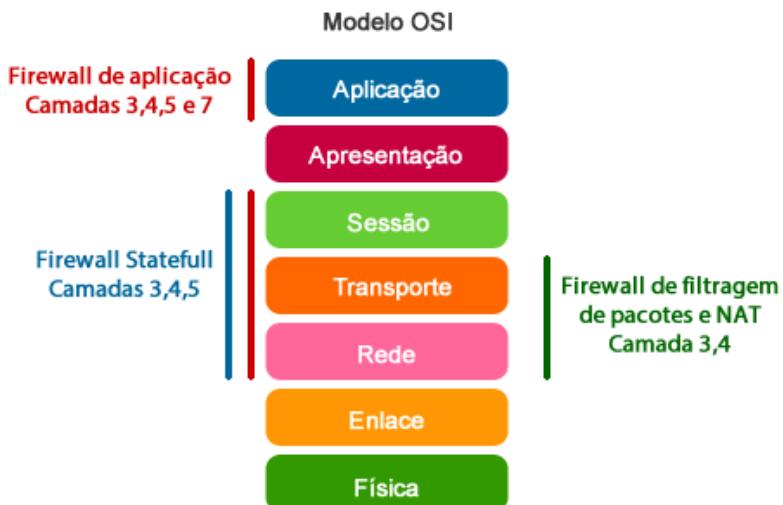
Existem várias vantagens no uso do firewall em uma rede:

- Prevenir a exposição de hosts e aplicações sensíveis para usuários/redes não confiáveis.
- O fluxo dos protocolos pode ser “higienizado”, impedindo a exploração das falhas mais conhecidas dos protocolos, normalmente exploradas no início dos ataques.
- Impedir o fluxo de dados não seguros de serem enviados a servidores e clientes.
- Facilitar a aplicação da política de segurança de maneira escalonável e robusta.
- Convergir o controle de acesso à rede em alguns pontos reduzindo a complexidade do gerenciamento de segurança.

Porém, os firewalls também têm algumas limitações:

- Se mal configurado, um firewall pode ter consequências graves (ponto único de falha – SPOF – Single Point Of Failure).
- Os firewalls não conseguem tratar certos tipos de tráfego de forma segura.
- Os usuários podem proativamente procurar maneiras de burlar as regras do firewall para receber material bloqueado e, propositalmente ou não, acabam por criar uma potencial falha de segurança.
- O desempenho da rede pode ser degradado, pois todo o tráfego passando por um único ponto pode trazer lentidão se mal projetado.
- Tráfego não autorizado pode ser encapsulado ou oculto dentro de um protocolo válido e passar através do firewall.

Existem diversas classificações e nomenclaturas para os diferentes tipos de firewalls. Veja na figura abaixo os tipos de firewall em relação ao modelo de referência OSI.



Podemos classificar os firewalls como:

- **Firewall de filtragem de pacotes (packet filtering)** - Normalmente é um roteador com a capacidade de filtrar conteúdo do pacote IP ou protocolo TCP/UDP (camadas 3 e 4), utilizando para filtragem parâmetros como endereços IP de origem e destino, portas TCP e UDP de origem e destino.
- **Stateful Firewall** - Monitora o estado de conexões (se a conexão está iniciando, realizando a transferência de dados/estabelecida ou o estado de finalização). Atua nas camadas 3, 4 e 5 do modelo OSI.
- **Firewall de Aplicação (firewall proxy ou gateway de aplicação)** - Um firewall que filtra as informações nas camadas 3, 4, 5 e 7 do modelo OSI. A maior parte do controle e filtragem é realizada em nível de software. São muitas vezes chamados de Proxy Firewall.
- **Firewall de Tradução de endereços (NAT – Network Address Translation)** - Permite o uso de endereços privativos na Internet traduzindo os IPs da rede interna por um endereço válido de Internet. Ele também acaba ocultando os endereços internos por utilizar uma faixa de IPs privativos e não válidos na Internet.
- **Personal Firewall (baseado em Host - servidor e/ou pessoal)** - Um PC ou servidor com o software de firewall em execução, por exemplo, o firewall que vem residente no Windows.
- **Firewall Transparente** - Um firewall que filtra o tráfego IP entre um par de interfaces em modo Bridge.
- **Firewall Híbrido** - Um firewall que é uma combinação de vários tipos de firewalls.

Os firewalls por filtragem de pacotes não representam uma solução completa de firewall, porém é uma parte importante da maioria das soluções disponíveis no mercado. Com a filtragem de pacotes você pode limitar o tráfego através de informações da camada-3, limitando acesso a determinadas redes IP de origem ou destino, assim como ir além e configurar filtros baseados na camada 4, ou seja, portas TCP ou UDP de origem e destino, limitando aplicações específicas.

Um exemplo é uma empresa que utiliza e-mail e que normalmente terá que liberar o uso da porta 25 do protocolo TCP para o envio dos e-mails através do protocolo SMTP (Simple Mail Transport Protocol).

As regras de um firewall baseado em filtragem de pacotes normalmente são baseadas em parâmetros das camadas 3 e 4 do modelo OSI, podendo filtrar por:

- Endereço de origem (Source IP address)
- Endereço de destino (Destination IP address)
- Protocolo
- Porta TCP/UDP de origem (Source port number)
- Porta TCP/UDP de destino (Destination port number)
- Estado da conexão (Synchronize/start – SYN)

As vantagens desse tipo de firewall são a facilidade de implementação, não gerar sobrecarga no processamento do firewall ou impacto sobre o fluxo da rede, é uma etapa inicial importante de filtragem na rede e pode ser implementado facilmente em qualquer equipamento, firewall ou roteador.

As desvantagens da filtragem de pacote tem origem em sua simplicidade, pois hackers podem enviar pacotes que passam pelas regras da ACL para realizar ataques de falsificação de IP (IP spoofing). Além disso, seguem algumas outras desvantagens da filtragem de pacotes:

- Regras muito complexas podem ser difíceis de administrar e manter.
- Não trabalham bem com pacotes segmentados.
- Não conseguem filtrar serviços que tem negociação dinâmica, por exemplo, que utilizam portas variáveis ou mudam de porta durante a negociação.
- Não mantém o estado da conexão, podendo sofrer ataques onde o contexto da conexão deve ser analisado.

No quadro abaixo temos um exemplo de regra de firewall com filtragem de pacotes:

Regra	Ação	IP de Origem	IP de destino	Protocolo	Porta de origem	Porta de destino
1	Permite	192.168.10.20	194.154.192.3	tcp	Qualquer Porta	25
2	Permite	Qualquer rede (any)	192.168.10.3	tcp	Qualquer Porta	80
3	Permite	192.168.10.0/24	Qualquer rede (any)	tcp	Qualquer Porta	80
4	Nega	Qualquer rede (any)	Qualquer rede (any)	Qualquer protocolo	Qualquer Porta	Qualquer Porta

Por exemplo, vamos analisar a regra 3, onde quaisquer pacotes vindo da rede 192.168.10.0 com a máscara 255.255.255.0 (Ips de 192.168.10.1 a 192.168.10.254) podem acessar quaisquer IP's de destino, desde que seja através da porta 80 do protocolo TCP.

A evolução da filtragem de pacotes foram os **firewalls statefull**, os quais além de filtrar por todos os parâmetros utilizados pelo antecessor, também conseguem verificar o **estado da conexão**, mantendo uma **tabela de estado**.

Sabemos que a maior parte das conexões é do protocolo TCP, o qual estabelece e gerencia uma sessão entre os dois hosts para garantir a confiabilidade das trocas de mensagem. Porém, diversos serviços (o FTP ativo, por exemplo) iniciam uma conexão sobre uma porta estática, mas abrem dinamicamente (ou seja, de maneira aleatória) uma porta para estabelecer uma sessão entre o servidor e a máquina cliente. Assim, com uma filtragem simples de pacotes fica impossível prever as portas que devemos permitir ou proibir.

Para resolver esse tipo de questão, o sistema de filtragem dinâmico de pacotes baseia-se na inspeção das camadas 3, 4 e 5 do modelo OSI, permitindo que o firewall **acompanhe as transações entre o cliente e o servidor**. O termo "stateful inspection" ou "stateful packet filtering" pode ser traduzido para "filtragem de pacotes com estado".



Dessa forma, o firewall de tipo "stateful inspection" é capaz de realizar o acompanhamento das trocas, ou seja, de monitorar o estado dos pacotes para aplicar as regras de filtragem. Quando um serviço é acessado fora, o firewall stateful mantém certos detalhes da conexão, salvando o estado da conexão na tabela de estado. Cada vez que uma conexão TCP ou UDP é estabelecida para conexões de entrada ou de saída, o firewall registra as informações em uma tabela de sessão com estado de fluxo. Quando o sistema de fora responde a um pedido, o servidor firewall compara os pacotes recebidos com o estado guardado para permitir ou negar acesso à rede.

A tabela de estado normalmente contém os endereços de origem e destino, números de porta TCP, informações de sequenciamento e sinalizadores adicionais (flags) para cada conexão TCP ou UDP que está associado a essa sessão em particular. Esta informação cria um objeto de conexão que é usado pelo firewall para comparar todos os pacotes de entrada e saída contra os fluxos de sessão na tabela de sessão stateful. O firewall permite os dados somente se existe uma conexão adequada para validar a passagem dos dados.

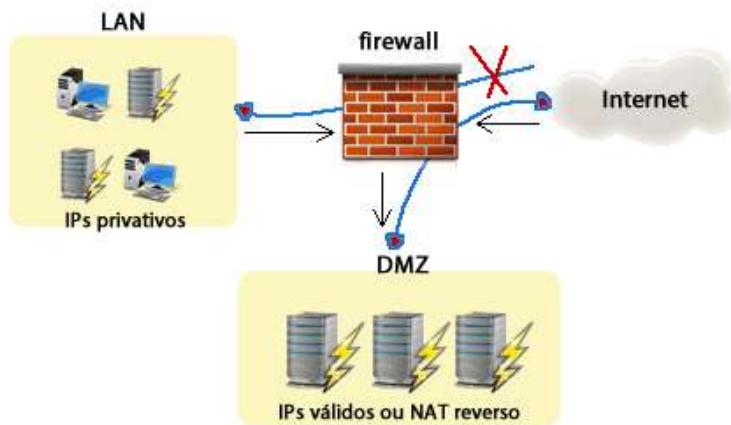
Alguns firewalls stateful mais avançados incluem a capacidade de analisar comandos do FTP e atualizar a tabela de estado para permitir que o FTP trabalhe de forma transparente através do firewall. Os stateful firewalls avançados também podem analisar número de sequência do TCP e respostas do DNS para garantir que o firewall permita somente pacotes entrantes que sejam relativos às conexões que realmente se originaram de dentro da rede, evitando o spoofing de IP. Esses recursos reduzem a ameaça de ataques de flooding de TCP/RST e DNS cache poisoning (ataques ao DNS).

Há uma desvantagem potencial da utilização de filtragem de estado. Embora a inspeção stateful proporcione rapidez e transparência, os pacotes dentro da rede devem fazer o seu caminho para a rede externa. Isso pode expor os endereços IP internos para hackers em potencial.

A maioria dos firewalls stateful podem atuar como gateways de Network Address Translation (NAT) e servidores proxy para maior segurança. Além disso, eles não protegem contra a exploração das **falhas nos aplicativos**, ligadas às vulnerabilidades das aplicações, estas vulnerabilidades representam a parte mais importante dos riscos em termos de segurança. Outras desvantagens são as de não suportar autenticação e que nem todos os protocolos, como UDP e ICMP, podem ser inspecionados utilizando esse tipo de firewall ou possuem uma inspeção limitada.

#### 1.4.1.1 DMZ – ZONA DESMILITARIZADA

Quando falamos de firewalls, um termo muito utilizado em redes e segurança é **DMZ**, o qual é a sigla para de "Demilitarized Zone" ou "Zona Desmilitarizada". A DMZ também é conhecida como **Rede de Perímetro** e de maneira simplificada ela é uma pequena rede situada entre uma **rede confiável** e **uma rede não confiável**, geralmente entre a rede local (Intranet) e a Internet.

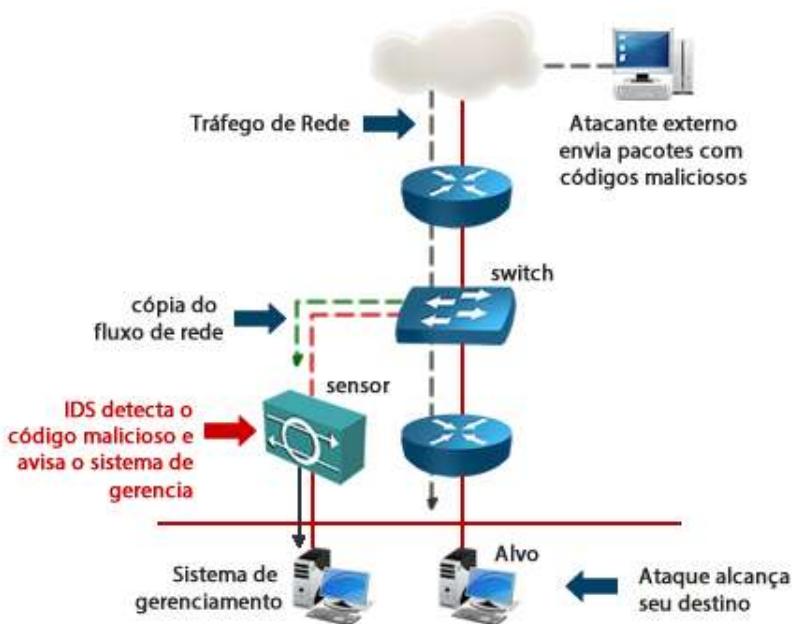


A função de uma DMZ é manter todos os serviços que possuem **acesso externo** (tais como servidores HTTP, FTP, e-mail, etc.) separados da rede local, limitando assim o potencial dano em caso de comprometimento de algum destes serviços por um invasor. Para atingir este objetivo os servidores instalados na DMZ **não devem conter nenhuma forma de acesso à rede local**. Assim, se um dos servidores da DMZ for atacado a ameaça fica restrita à DMZ e não passa para a rede interna da empresa.

#### 1.4.2 IDS (Intrusion Detection System) e IPS (Intrusion Prevention System)

Um IDS é uma ferramenta utilizada para monitorar o tráfego da rede, detectar e alertar sobre ataques e tentativas de acessos indevidos. Na grande maioria das vezes **não bloqueia uma ação**, mas **verifica** se esta ação é ou não uma ameaça para um segmento de rede, informando a um sistema de gerenciamento de falhas.

A vantagem de se utilizar um IDS é que ele não interfere no fluxo de tráfego da rede, pois ele trabalha em paralelo à rede, apenas monitorando o fluxo de dados, analisando e reportando possíveis ataques ou riscos à segurança. Um IDS é geralmente instalado em um modo que chamamos de "Promiscous-mode" ou simplesmente "Modo Promíscuo".



Podemos verificar na figura que o equipamento identificado como "**Sensor**" está conectado a uma porta do switch de camada 2 e todo o tráfego que está passando por este switch está sendo analisado. Logo, caso seja identificado algum tráfego malicioso (que vá de encontro a base de dados de assinaturas do software IDS) um alerta imediato será enviado ao sistema de gerenciamento (System Management). Este alerta pode ser, por exemplo, via e-mail ao administrador de segurança.

Com o que vimos até o momento sobre o IDS, sua maior desvantagem é não conseguir agir sozinho sobre o problema, dependendo de outros elementos de segurança para poder parar o possível ataque. Resumindo sua operação temos que, ele deve receber uma cópia de todos os pacotes enviados na rede, comparar com sua base de assinaturas de ataques (signature database) e caso seja detectado um ataque ele deve informar a uma console de gerenciamento ou enviar um log para o syslog, por exemplo.

Já um IPS – Intrusion Prevention System – surgiu como um complemento do IDS e tem a capacidade de identificar uma intrusão, analisar a relevância do evento/risco e **bloquear** determinados eventos, fortalecendo assim a tradicional técnica de detecção de intrusos.

O IPS é uma ferramenta com inteligência na maneira de trabalhar, pois reúne componentes que fazem com que ele se torne um repositório de logs e técnicas avançadas de alertas e respostas, voltadas exclusivamente a tornar o ambiente computacional cada vez mais seguro, porém, sem perder o grau de disponibilidade que uma rede deve ter.

O IPS usa a capacidade de detecção do IDS junto com a capacidade de bloqueio de um firewall, notificando e bloqueando de forma eficaz qualquer tipo de ação suspeita ou indevida e é uma das ferramentas de segurança de maior abrangência, uma vez que tem o poder de alertar e bloquear, agindo em diversos pontos de uma arquitetura de rede.

Um IPS é instalado em modo In-Line como mostrado abaixo, ou seja, em série com o fluxo de dados. Dessa forma, o equipamento consegue enxergar todo o tráfego em ambos os sentidos (In and out).

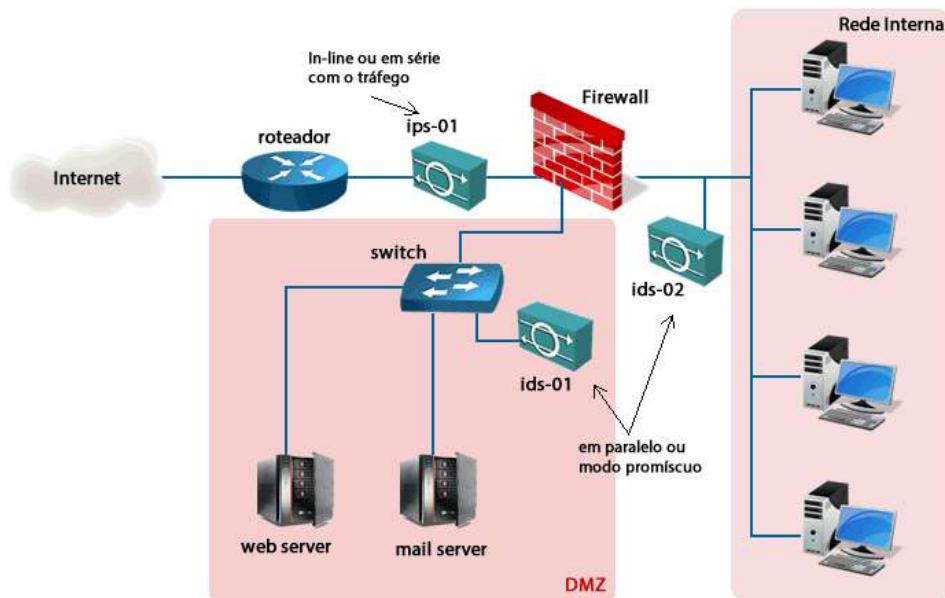


O IPS monitora as camadas 3 e 4 do tráfego, além disso, analisa também o conteúdo do payload das camadas superiores, podendo agir contra ataques mais sofisticados que podem incluir dados prejudiciais (maliciosos) nas camadas de 2 a 7 do modelo OSI.

Quando um pacote chega através de uma interface em um IPS, esse pacote não é enviado para a interface de saída até que o pacote seja analisado. Aqui está a maior desvantagem do IPS, se mal configurado ou mal dimensionado pode representar um gargalo na rede, pois todo o tráfego passará por ele.

Conforme mencionamos, as tecnologias IDS e IPS utilizam **assinaturas** para detectar desvios de padrões de tráfego na rede. Podemos definir uma **assinatura** como sendo um **conjunto de regras** que um IDS ou IPS utiliza para detectar uma atividade intrusiva. As assinaturas podem ser utilizadas para detectar falhas graves de segurança, ataques comuns à rede e coleta de informações, podendo detectar padrões de assinatura atômica ou atomic patterns (pacote único) ou padrões de assinatura composta ou composite patterns (multipacket).

Utilizar uma destas tecnologias não significa que um administrador não deve usar a outra, na verdade, as tecnologias de IDS e IPS são complementares. Por exemplo, o IDS pode ser implementado para validar a operação IPS, sendo configurado para uma inspeção de pacotes mais profunda quando estiver offline. Isso permite focar o IPS em analisar menos padrões de tráfego, ou seja, somente o que seja mais importante ou crítico para a política de segurança da empresa. Veja abaixo um exemplo de aplicação prática, onde um IPS faz a filtragem do tráfego na entrada da rede, antes do firewall e dois IDS's validam a operação dele dentro da rede Interna e na DMZ.



Veja na tabela o resumo da comparação entre um IDS e um IPS.

Comparação	IDS	IPS
Modo de operação	Modo promíscuo em paralelo com a rede.	Em série com a rede ou Inline.
Tráfego IP	Pacotes são copiados e não passam diretamente pelo IDS.	Pacotes passam pelo IDS para poderem ser analisados e filtrados.
Impacto no tráfego da rede	Sem impacto, somente monitoração.	Pode afetar o desempenho da rede se o número de pacotes for maior que a sua capacidade de processamento. Pode gerar atraso, jitter e problemas de performance.
Problemas	Mais vulnerável a ataques por não poder parar os pacotes iniciais do ataque (zero-day attacks). Facilita técnicas de evasão (fuga).	Pode afetar o desempenho da rede se houver sensores com problemas ou falhas no processo, causando atrasos no tráfego real-time sensível a atrasos, como VoIP. Além disso, sua capacidade de detecção pode ser afetada com tráfego muito intenso.

Os IDSs e IPSs podem ser instalados tanto em hosts (através de software) como funcionar como dispositivos de rede (um appliance ou caixa). Os IDSs e IPSs instalados em hosts são chamados de HIDS e HIPS (host IDS/IPS), já os instalados na rede como dispositivos são chamados de NIDS e NIPS (Network IDS/IPS).

A instalação de HIPS ou HIDS em hosts e servidores pode degradar bastante a performance dos equipamentos, pois todo pacote ou comportamento do host será analisado, o que requer uma utilização de memória e CPU razoáveis.

## 1.5 Segurança nos Clientes - Softwares

Keylogging, Virus, Trojan, Malware, Spyware – são várias palavras para denominar uma série de “vilões” dos usuários, aqueles programas mal-intencionados cujo uso vai desde roubo de senhas e informações até o mais puro caos e destruição. Mesmo assim, muitos não sabem a diferença entre uma coisa e outra, chamando tudo de “vírus”, o que pode trazer algumas confusões na hora de se defender.

**MALWARE:** programas especificamente desenvolvidos para executar ações danosas em um computador. Exemplos: worm, bots, virus, trojans...

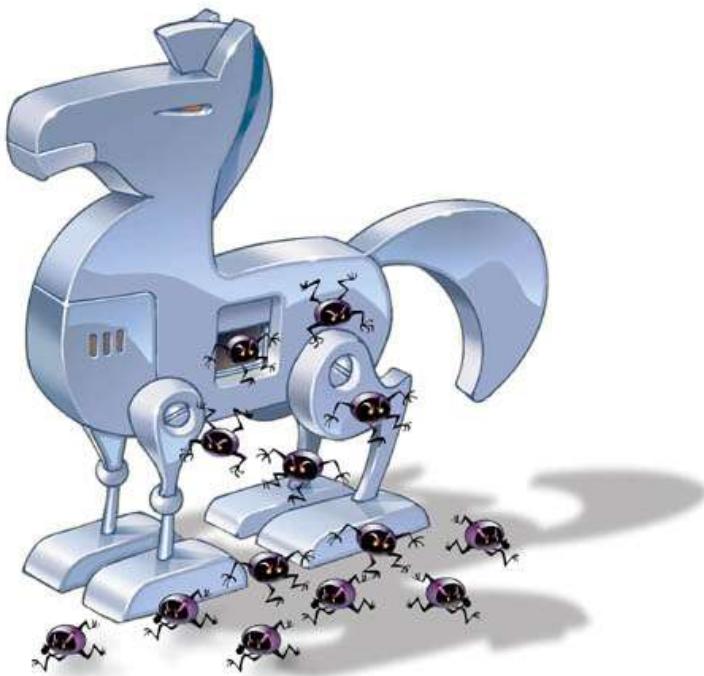
Um vírus é uma seqüência de código inserida em outro código executável, o qual tem as seguintes características:

- **Replicação:** os vírus se replicam para diversos arquivos da máquina a fim de garantir a sua sobrevivência dentro daquele sistema.
- **E ativado por uma ação externa:** pode-se dar como exemplo um arquivo anexo de e-mail que está localizado na caixa de entrada do programa gerenciador de e-mails. Se este arquivo não for executado não há como a máquina ser infectada por esse vírus.

A infecção ocorre no momento que se executa o programa com código malicioso. A partir daí esse se espalha, ou seja, ele se multiplica danificando diversos arquivos e sistemas da máquina onde ele se encontra.



Pode-se citar também um outro tipo de programa malicioso que é intitulado como **trojan**. Sua principal função é inserir um trecho de código em um programa aparentemente inofensivo, mas na verdade a intenção é colocar um hospedeiro na máquina invadida, deixando o invasor com o controle total da máquina.



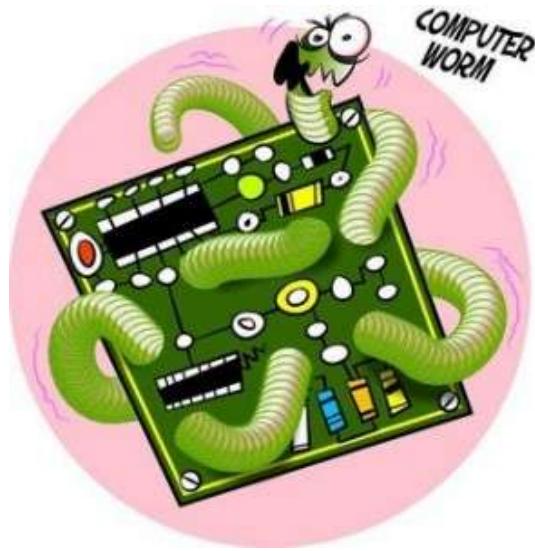
Os trojans são um tipo de ferramenta que se popularizaram na Internet a partir de 1997, quando foi lançado o famoso **Back Orifice** (uma brincadeira com o nome Back Office da Microsoft). Um **cavalo de tróia**, ou trojan, é um programa que, quando instalado no sistema de alguém, geralmente abre uma porta TCP ou UDP para receber conexões externas, fornecendo normalmente o shell (prompt de comandos) daquele sistema para um possível invasor.

Isso não é regra geral, já que alguns backdoors podem fazer também conexão reversa e outros tipos de técnicas. Um cavalo de tróia nada mais é do que um backdoor disfarçado de um programa comum, como um jogo. O termo “cavalo de tróia” faz analogia ao cavalo de madeira que os gregos deram aos troianos, no famoso episódio da guerra de Tróia.

Um **worm**, assim como um vírus, cria cópias de si mesmo de um computador para outro, mas faz isso automaticamente. Primeiro, ele controla recursos no computador que permitem o transporte de arquivos ou informações. Depois que o worm contamina o sistema, ele se desloca sozinho.

O grande perigo dos worms é a sua capacidade de se replicar em grande volume. Por exemplo, um worm pode enviar cópias de si mesmo a todas as pessoas que constam no seu catálogo de endereços de email, e os computadores dessas pessoas passam a fazer o mesmo, causando um efeito dominó de alto tráfego de rede que pode tornar mais lentas as redes corporativas e a Internet como um todo. Quando novos worms são lançados, eles se alastram muito rapidamente. Eles obstruem as redes e, provavelmente, fazem com que você (e todos os outros) tenha de esperar um tempo maior para abrir páginas na Internet.

Na prática, todos os vírus e vários worms não podem se espalhar sem que você abra um arquivo ou execute um programa infectado.



Muitos dos vírus mais perigosos foram espalhados principalmente via anexos de email, os arquivos que são enviados com as mensagens de email. Geralmente você tem como saber que um email contém um anexo, pois este é exibido como um ícone de clipe de papel que representa o anexo. Um vírus é ativado quando você abre um arquivo anexo infectado (geralmente você abre o anexo clicando duas vezes no seu ícone).

O **anti-vírus** é a ferramenta mais recomendada contra vírus, worms e trojans nos hosts, além disso os IPSs (sistema de prevenção de intrusos) e os IDSs (sistema de detecção de intrusos), em conjunto com os firewalls podem ser de grande ajuda para evitar que esses programas e códigos maliciosos entrem na rede, infectando os micros e servidores da rede.

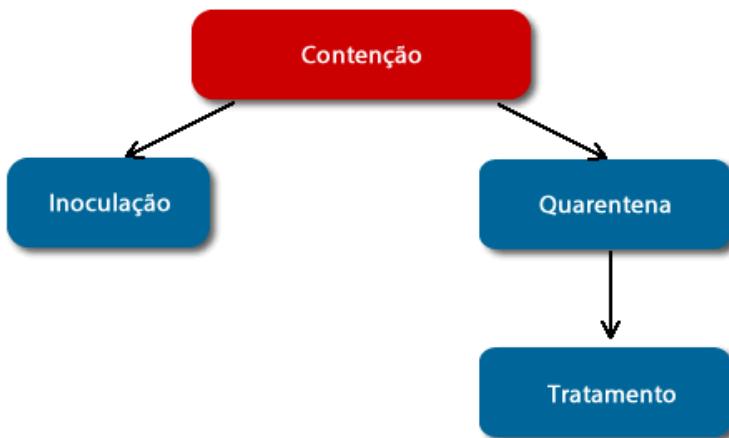
Nada pode garantir que um computador está 100% protegido. Entretanto, para continuar a melhorar a segurança do computador recomenda-se manter os programas atualizados e atualizar sempre a assinatura do software antivírus. Outras ferramentas que podem ser implementadas são os **HIPSS** ou **Host IPS**, **anti-spyware** ou **programa anti-espionagem** que protegem contra diversos tipos de infecções e cavalos de tróia. Também não se deve abrir arquivos suspeitos, e-mails que não sejam de origem confiável e nem utilizar o computador em redes suspeitas sem estar com seu micro atualizado e com o anti-vírus atualizado.

Tratando do problema com uma abordagem mais corporativa, ou seja, em como tratar um infecção de vários computadores em uma empresa, o administrador deve se preocupar com a **política de segurança nos hosts**, sejam micros ou servidores, garantindo que não saia uma máquina para um usuário final sem um anti-vírus instalado.

Existem várias opções de anti-vírus corporativas que facilitam a administração, como por exemplo, os citados na figura abaixo. Outra medida que vale a pena frisar é que os anti-vírus e sistemas devem estar sempre atualizados.



Já uma infecção por um worm exigirá mais do administrador de rede por sua característica de propagação utilizando a rede. A resposta a uma infecção do worm pode ser dividida em quatro fases: **contenção, inoculação, quarentena e tratamento**. Veja a figura abaixo como mitigar ataques de worms.



A **contenção** visa limitar a infestação que pode se espalhar na rede, o que pode ser realizado através de listas de controle de acesso ou até mesmo desligando certos segmentos de redes infestados, ou seja, isolando-os. A **inoculação** é onde o problema é resolvido, aplicando patches de segurança ou removedores de worms especificamente lançados para determinadas infestações. A **quarentena** e o tratamento serve para isolar os micros infectados e inoculá-los resolvendo o problema. Muitas vezes pode chegar ao ponto de ser necessária a **reinstalação** do sistema operacional para resolver o problema.

Existem além dos três vilões citados acima outros riscos, tais como:

- **Adware:** Tradicionalmente, o Adware é uma forma legítima de distribuição de software. Alguns desenvolvedores, principalmente aqueles independentes de grandes corporações, na hora de lucrar com suas criações, optam por um modelo de negócios alternativo: em vez de cobrar pelo programa em questão, cria-se um modelo de publicidade em programas. Ou seja, o desenvolvedor ganha uma comissão de anunciantes, que pagam para terem seus banners ou links nos programas utilizados por usuários. A prática é legal, porém existe o lado oposto, com Adwares que corrompem arquivos de usuários ou instalam Spyware. Um caso famoso era o software BonziBUDDY, um macaco roxo animado que era disponibilizado como um "companheiro" do usuário, além de prometer aprimorar a experiência de navegação. Intrusões em excesso, mudança de configurações, exibição de pop-ups sem permissão, entre outras acusações, incluindo de instalação de Trojan e uso de Backdoor, levaram o macaco a ser um dos programas mais odiados da internet.



- **Spyware:** É o "software espião". Geralmente, é um arquivo que é executado de maneira oculta, coletando dados de uso do computador e da internet do computador infectado. Alguns chegam a roubar dados, agir como keyloggers, alterar configurações e arquivos e até instalar programas.
- **Botnet:** No caso, não é uma ameaça direta, mas sim uma consequência de outros males. Uma Botnet, ou Rede de Robôs (Bots), acontece quando um hacker infecta uma série de computadores (por meio de Trojan ou Worm, geralmente), fazendo-os integrar uma rede, sem que seus donos saibam. Com esses computadores como seus "soldados", o Hacker pode disponibilizar seus serviços por dinheiro, e utilizá-los para mandar mensagens de spam em massa, assim como derrubar conexões e servidores por ataques de Denial of Service (DoS).
- **Keyloggers:** Software que realiza o Keylogging ou Keystroke Logging, é um programa oculto que registra tudo que é digitado em um computador. Geralmente instalado por meio de um Trojan, facilita a obtenção de informações e senhas. É por isso que vários sistemas de sites, como o exemplo de bancos, pedem o uso de teclados virtuais, que não necessitam que o usuário tecle suas senhas.
- **Rootkit:** Software de uso ativo, ele permite privilégios de acesso continuados a um computador, ao mesmo tempo que disfarça sua presença. Um Hacker geralmente instala um rootkit depois de passar das barreiras mais simples de um sistema, possibilitando acesso administrativo e, eventualmente, acesso total aos dados do sistema invadido.

## 1.6 Política de Segurança

De acordo com o **RFC 2196** (The Site Security Handbook), uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

As políticas de segurança devem ter um conteúdo realista, e definir claramente as áreas de responsabilidade dos usuários de sistemas de informação, do pessoal de gestão de sistemas e redes e da direção da empresa, além disso, deve também adaptar-se a alterações na organização.

O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos relacionados aos mecanismos de segurança, pois esse detalhamento pode variar ao longo do tempo. Deve ser também um documento de fácil leitura, compreensão e resumido.

Existem duas filosofias por trás de qualquer política de segurança: a **proibitiva** (tudo que não é expressamente permitido é proibido) e a **permissiva** (tudo que não é proibido é permitido), sendo que a proibitiva é a que tem mais aceitação no mundo corporativo.

Abaixo seguem os elementos da política de segurança que devem ser considerados em sua elaboração:

- **A Disponibilidade:** o sistema deve estar disponível de forma que quando o usuário necessitar possa usar. Dados críticos devem estar disponíveis ininterruptamente.
- **A Legalidade:** não se deve escrever aquilo que não está previsto nas leis vigentes de cada país.
- **A Integridade:** o sistema deve estar sempre íntegro e em condições de ser usado.
- **A Autenticidade:** o sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.
- **A Confidencialidade:** dados privados devem ser apresentados somente aos donos dos dados ou ao grupo por ele liberado.

### 1.6.1 Política de Senhas nas Empresas

Dentre as políticas utilizadas pelas grandes corporações a composição da senha ou password é uma das mais controversas. Por um lado, profissionais com dificuldade de memorizar várias senhas de acesso, por outro lado, funcionários displicentes que anotam a senha sob o teclado ou no fundo das gavetas (em casos mais graves o colaborador anota a senha no próprio monitor, por mais incrível que pareça).

Recomenda-se a adoção das seguintes regras para minimizar o problema, mas a regra fundamental é a **conscientização** dos colaboradores quanto ao uso e manutenção das senhas:

- **Senha com data para expiração:** Adota-se um padrão definido onde a senha possui prazo de validade com 30 ou 45 dias, obrigando o colaborador ou usuário a renovar sua senha.
- **Inibir a repetição:** Adota-se, através de regras predefinidas, que uma senha uma vez utilizada não poderá ter mais que 60% dos caracteres repetidos, p. ex: senha anterior "123senha" nova senha deve ter 60% dos caracteres diferentes como "456seuse", neste caso foram repetidos somente os caracteres "s" e "e" sendo os demais diferentes.
- **Obrigar a composição com número mínimo de caracteres numéricos e alfabéticos:** Define-se obrigatoriedade de 4 caracteres alfabéticos e 4 caracteres numéricos, por exemplo, 1s4e3u2s. Ou posicional, onde por exemplo, os 4 primeiros caracteres devem ser numéricos e os 4 subsequentes alfabéticos.

- **Criar um conjunto com possíveis senhas que não podem ser utilizadas:** Monta-se uma base de dados com formatos conhecidos de senhas e proíbe o seu uso. Por exemplo, o usuário chama-se Jose da Silva, logo sua senha não deve conter partes do nome como 1221jose ou 1212silv. Ou então, proibir o uso da sua data de nascimento na senha e etc. Essas regras dificultam as tentativas de descoberta de senhas vasculhando a vida de determinados funcionários, pois mesmo que o atacante descubra a data de aniversário ou nome de um deles não conseguirá utilizá-la como base para seu ataque uma vez que o sistema não permite que o usuário a utilize
- Recomenda-se ainda utilizar senhas com caracteres em maiúsculo, números e utilização de caracteres especiais como @, #, \$, %, & ou \*.

## 1.7 Melhores Práticas (Best-Practices)

Agora que você tem uma compreensão fundamental de ameaças direcionadas aos ambientes de rede e informática, vamos analisar as recomendações para ajudar a proteger a segurança de sua rede:

- Aplicar patches de sistemas operacionais e aplicativos continuamente.
- Desativar serviços desnecessários e portas não utilizadas em roteadores e switches.
- Exigir senhas fortes e forçar a expiração da senha, fazendo com que os usuários troquem suas senhas periodicamente.
- Proteger o acesso físico aos computadores demais e equipamentos de rede.
- Impor práticas seguras de programação, tais como limitar os caracteres válidos que podem ser inseridos na caixa de diálogo de um aplicativo.
- Realizar regularmente backup de dados e verificar a integridade dos backups, pois fazer o backup somente não garante que ele esteja realmente íntegro e funcional.
- Treinar os usuários sobre boas práticas de segurança e educá-los sobre táticas de engenharia social.
- Usar criptografia forte para dados importantes (sensíveis).
- Defenda-se contra ataques técnicos de implantação de sistemas de segurança de hardware e software (por exemplo, firewalls, sensores IPS e software antivírus).
- Criar uma política de segurança documentada para uso de toda a empresa.



## 2 Gerenciamento de Redes

O gerenciamento de redes pode ter várias abordagens e visão dentro de cada empresa ou área que é aplicado, por exemplo, em redes de computadores ou telecomunicações. Uma definição bem completa do tema segue abaixo:

**"Gerência de redes** ou **gerenciamento de redes** é o **controle de qualquer objeto** passível de ser monitorado numa estrutura de recursos físicos e lógicos de uma rede e que podem ser distribuídos em diversos ambientes geograficamente próximos ou não. O gerenciamento de uma rede de computadores torna-se uma atividade essencial para **garantir o seu funcionamento contínuo** assim como para **assegurar um elevado grau de qualidade dos serviços oferecidos.**" (Fonte: Wikipédia)

Se analisarmos o ciclo de vida de uma rede tudo se inicia com o levantamento de requisitos, depois passa por um projeto, a instalação e configuração dos elementos de rede, testes de validação e então a rede passa para o estágio da operação. Na operação os usuários realmente começam a utilizar a rede e, então, vem o dia a dia. Uma vez que a rede está implantada os administradores de rede deverão tratar os eventuais problemas e os MACDs (Moves, Adds, Changes and Delete – Movimentações, Adições, Alterações e Desinstalações de equipamentos de rede).

É nessa parte final que o gerenciamento de redes entra, no dia a dia, ou seja, monitorando os equipamentos de rede e os eventos (problemas, interfaces que ficam indisponíveis, características como quantidade de memória, CPU e HD utilizados e assim por diante) por eles gerados, assim como realizando as devidas alterações de maneira segura e conforme as necessidades do negócio de cada empresa.

Normalmente, nas grandes empresas o gerenciamento de redes de computadores faz parte de um processo maior de **Gerenciamento de Serviços de TI** através das melhores práticas de mercado (aquilo que dá certo nas empresas) seguindo, por exemplo, a "Information Technology Infrastructure Library" (ITIL), um conjunto de boas práticas a serem aplicadas na infraestrutura, operação e manutenção de serviços de tecnologia da informação (TI).

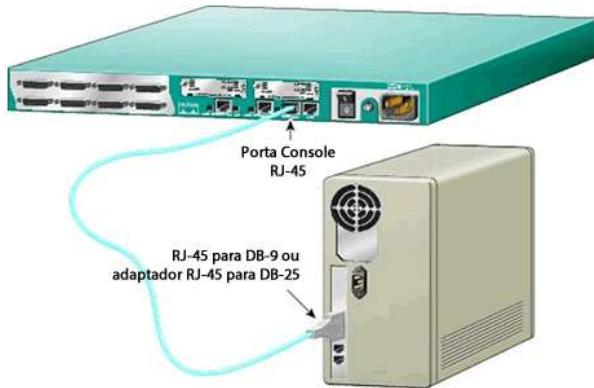
Na sequência vamos analisar algumas ferramentas e protocolos utilizados para o gerenciamento dos dispositivos de redes.

### 2.1 Acesso Local e Remoto – Console, Telnet, SSH e Interfaces Web

Normalmente os equipamentos de rede de médio e grande porte não possuem acesso Web simplificado para configuração como os roteadores sem fio ou ADSL. A configuração desses tipos de equipamentos normalmente deve ser iniciada via linha de comando (CLI – Command Line Interface) para a inserir IPs em interfaces ou habilitar determinados protocolos, permitindo assim o acesso remoto e a configuração através de aplicativos Web mais simples de se utilizar. No entanto, a maioria dos administradores de rede ainda preferem configurar equipamentos de maior porte via CLI devido à flexibilidade e maior abrangência que os comandos permitem chegar nas configurações.

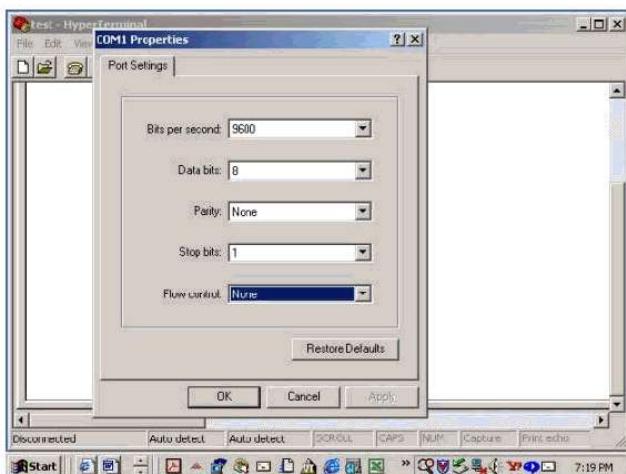
Além disso, via CLI é possível fazer "scripts", arquivos de texto com os comandos a serem aplicados nos equipamentos, o que facilita e acelera o processo de configuração.

As interfaces locais normalmente são realizadas via uma conexão serial RS-232 em uma porta nos equipamentos de rede chamada "Console". Nos computadores precisamos ter placa serial com conector DB-9 ou então um adaptador USB-Serial para fazer a conexão local. Os programas utilizados para acessar os equipamentos são os emuladores de terminal, tais como Hyperterminal, Putty ou Teraterm. Veja um exemplo de conexão local entre um computador um roteador Cisco.



A configuração para a porta de console é a mesma para os fabricantes Cisco, Huawei e Juniper (veja a tela de configuração do Hyperterminal):

- Taxa: 9600 (bits per second)
- Bits de dados: 8 (data bits)
- Paridade: none (parity)
- Bits de parada: 1 (stop bits)
- Controle de fluxo: None (flow control)



Apesar das configurações para acesso à linha de comando dos três fabricantes serem a mesma e os comandos serem parecidos, a filosofia de configuração e comandos variam entre eles.

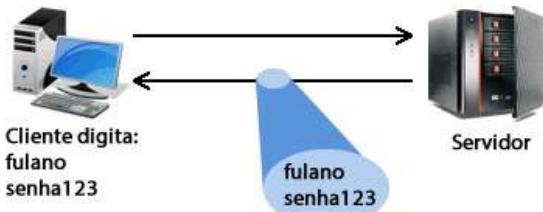
### 2.1.1 Acesso Telnet e SSH

Uma vez acessado via console e configurado, agora o equipamento deve ser preparado para o **acesso remoto**, pois normalmente os equipamentos podem estar em salas de telecomunicações distantes e ficar se deslocando toda vez que é necessário fazer uma verificação ou alteração torna a operação complicada. Por isso, você pode realizar os acessos via Telnet, SSH ou Web, porém deve-se verificar a disponibilidade de cada protocolo nas especificações dos equipamentos.

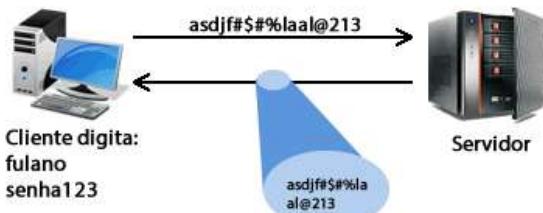
O Telnet e SSH permitirão acesso à linha de comando dos equipamentos, porém via rede IP, ou seja, não precisa estar conectado diretamente aos equipamentos como no caso da conexão local via console. Os dois métodos tem a mesma finalidade, porém o Telnet faz uma conexão "insegura" com o dispositivo de rede, ou seja, as informações trocadas entre o computador de gerenciamento e o dispositivo de rede estão em texto claro, podendo ser capturada e lida através de um sniffer de pacotes. Como já comentado, o Telnet utiliza o protocolo TCP para transporte na porta 23. Para uso interno o Telnet até pode ser utilizado, porém para acesso remoto via Internet, por exemplo, já não é recomendado o uso do Telnet.

Já com o SSH o acesso é feito de maneira segura, ou seja, ao invés dos dados entre o micro de gerenciamento e o dispositivo de rede serem enviados em texto claro, os dados são criptografados antes de serem enviados pela rede. Nesse caso, se os pacotes do SSH forem capturados não poderão ser lidos pelo atacante.

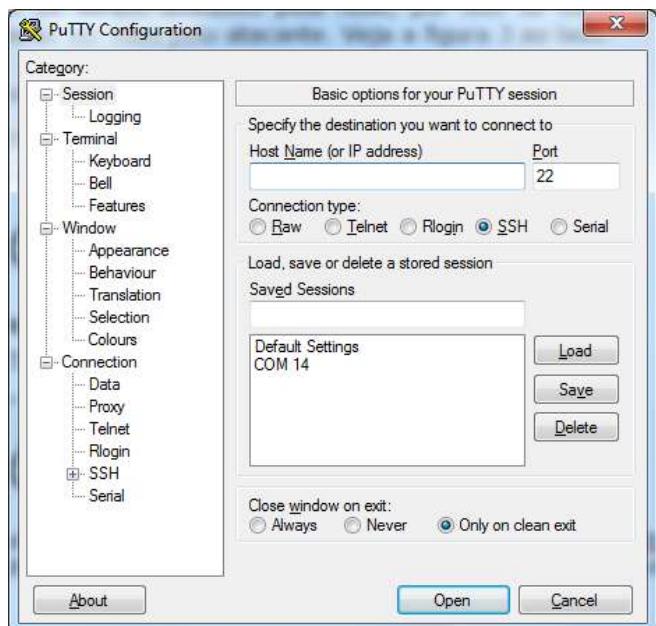
#### Sessão de login sem criptografia - Telnet



#### Sessão de login com criptografia - SSH



O programa mais utilizado para acesso remoto via Telnet e SSH é o Putty, além disso, ele também pode ser utilizado para acesso local via console. Veja a tela de configuração do Putty na figura abaixo.



Para acessar um dispositivo de rede remoto via SSH ou Telnet, basta selecionar o serviço em "Connection Type", digitar o IP do dispositivo em "Host Name (or IP address)" e opcionalmente digitar a porta em que o serviço está disponibilizado, pois alguns administradores de rede alteram as portas padrões do SSH e Telnet para dificultar a via dos invasores. Clique em Open e a sessão será aberta. Veja um exemplo de tela de uma conexão SSH via Putty.

```
iP 192.168.1.6 - PuTTY
login as: dltec
Using keyboard-interactive authentication.
Password:
Access denied
Using keyboard-interactive authentication.
Password:

dltec#
dltec#
dltec#
dltec#
```

The screenshot shows a PuTTY terminal window titled 'iP 192.168.1.6 - PuTTY'. The session is connected to the IP address 192.168.1.6. The user has typed 'dltec' as the login name. The system responds with 'Using keyboard-interactive authentication.' followed by 'Access denied'. This pattern repeats twice more. Finally, the prompt 'dltec#' appears again, indicating the user is still connected to the session.

### 2.1.2 Interface Web

As interfaces Web de gerenciamento e configuração já não são tão padronizadas como o acesso via console, Telnet e SSH. Cada fabricante tem o seu padrão, estilo de páginas e serviços que são disponibilizados via Web.

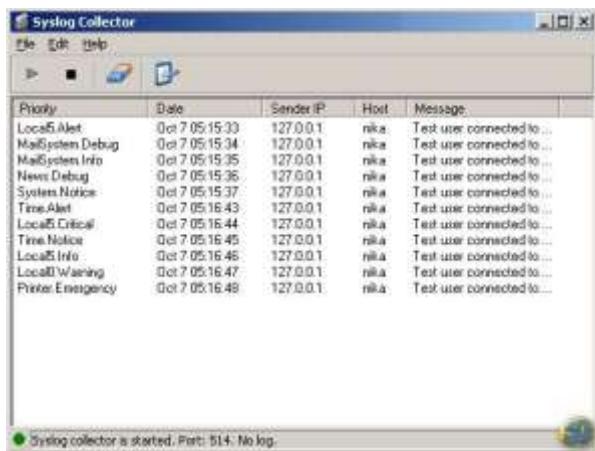
Os equipamentos de menor porte, tais como roteadores ADSL, roteadores sem fio e APs possuem sua configuração inteiramente via Web. Normalmente, eles já estão com a rede LAN pré-configurada com a rede 192.168.1.0 /24 e com o IP 192.168.1.1, porém pode variar em alguns modelos de equipamento ou fabricantes. Além disso, na maioria das vezes o login e senha inicial são "admin/admin", como este é um parâmetro amplamente conhecido recomenda-se a troca da senha de administração dos equipamentos.

Veja na figura a página inicial de administração de um roteador ADSL do fabricante Netgear.



### 2.2 Syslog

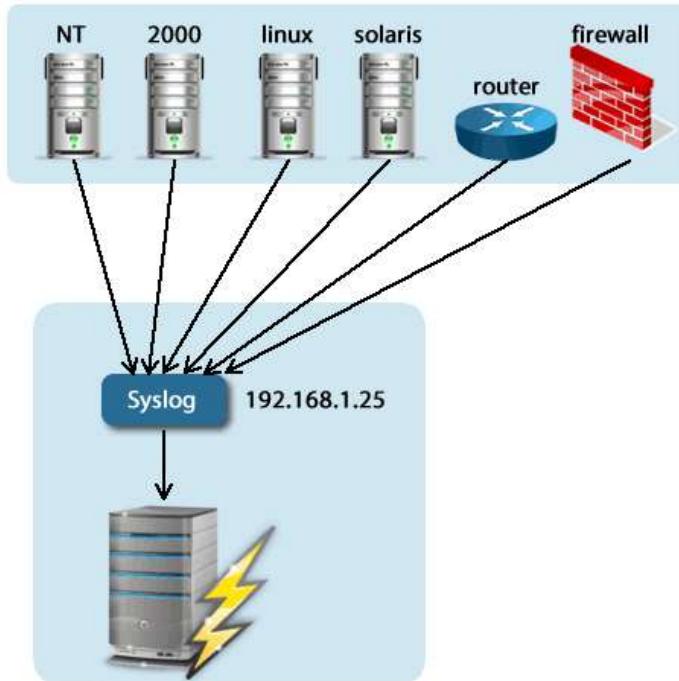
O Syslog é um padrão criado pela IETF para o envio de mensagens de log (relatório) em redes IP. O termo é geralmente utilizado para identificar tanto o protocolo de rede quanto para a aplicação ou biblioteca de envio de mensagens no protocolo Syslog.



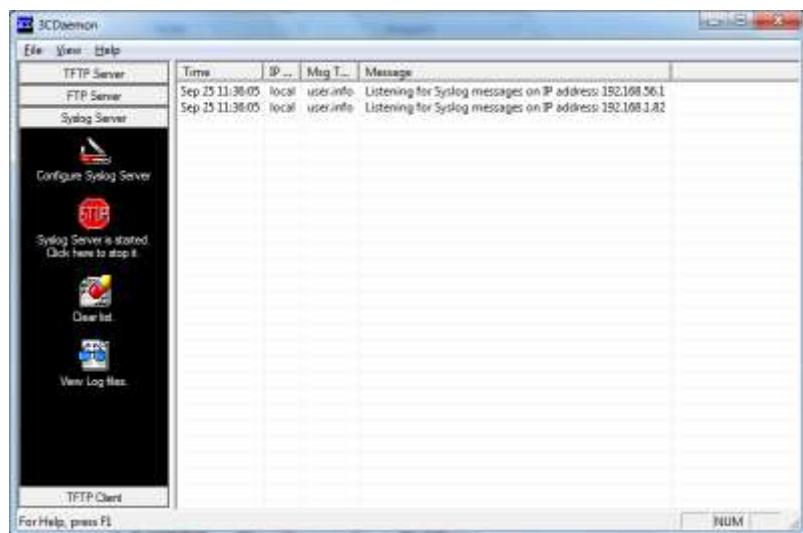
O protocolo syslog é muito simples, sendo que o remetente envia uma pequena mensagem de texto (com menos de 1024 bytes) para o destinatário (também chamado "syslogd", "serviço syslog" ou "servidor syslog"). Tais mensagens podem ser enviadas tanto por UDP quanto por TCP, além disso, o conteúdo da mensagem pode ser enviada em texto claro ou criptografada utilizando SSL (Secure Sockets Layer).

O protocolo syslog é tipicamente usado no gerenciamento de computadores e principalmente na auditoria de segurança de sistemas. Por exemplo, a empresa pode utilizar o syslog para verificar quando o acesso aos equipamentos foi realizado para verificar se acessos indevidos não estão ocorrendo em horários não permitido. O syslog também ajuda na resolução de problemas, pois o administrador de redes pode procurar mensagens de erro e correlacionar eventos utilizando diferentes sistemas e as informações do syslog.

Para que o syslog funcione você deve ter um servidor de syslog configurado em sua rede e nas máquinas ou dispositivos de rede configurar o envio das mensagens para o IP do servidor.



O serviço de syslog pode ser habilitado em um servidor Linux e também existem versões mais simples para instalação em Windows cliente e realização de testes, tais como o **3ComDaemon** e o **Kiwi Syslog Server**, ambos gratuitos. Veja a tela do 3ComDaemon na figura a seguir.



As mensagens do syslog ficam disponíveis na tela do programa e também em um arquivo de log em modo texto.

### 2.3 SNMP (Simple Network Management Protocol)

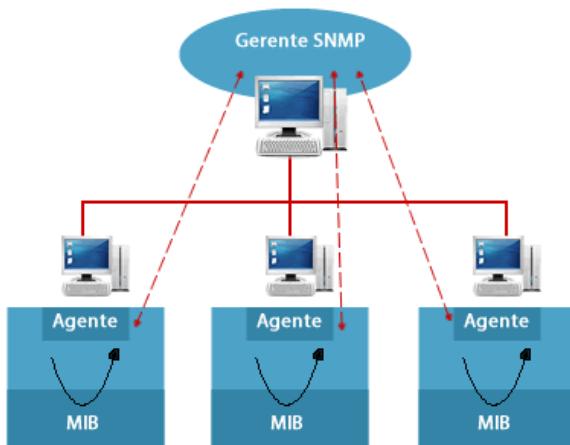
O SNMP (Simple Network Management Protocol) já foi abordado em capítulos anteriores e se trata de um protocolo que consiste em uma série de padrões para o gerenciamento de dispositivos de rede, incluindo um protocolo da camada aplicação, um programa de banco de dados e um conjunto de dados (objetos).

O SNMP é um protocolo que utiliza como transporte o UDP na porta 161. O protocolo SNMP foi ao longo do tempo sendo modificado o que levou a criação de 3 principais versões: versão 1, versão 2c (que é a mais usual) e a versão 3.

A versão 2 do SNMP é uma evolução do protocolo inicial. O SNMPv2 oferece uma boa quantidade de melhoramentos em relação ao SNMPv1, incluindo operações adicionais do protocolo, melhoria na performance, segurança, confidencialidade e comunicações gerente-para-gerente. A SNMPv3 inclui implementação na segurança ao protocolo como privacidade, autenticação e controle de acesso.

Basicamente, a ideia central do SNMP é tratar os dados de gerenciamento como variáveis do sistema a ser monitorado, sendo capaz de descrever a configuração do ambiente a ser monitorado. Essas variáveis podem ser lidas e em alguns casos até escritas pelas aplicações de gerenciamento, possibilitando a modificação de parâmetros de configuração dos dispositivos de rede.

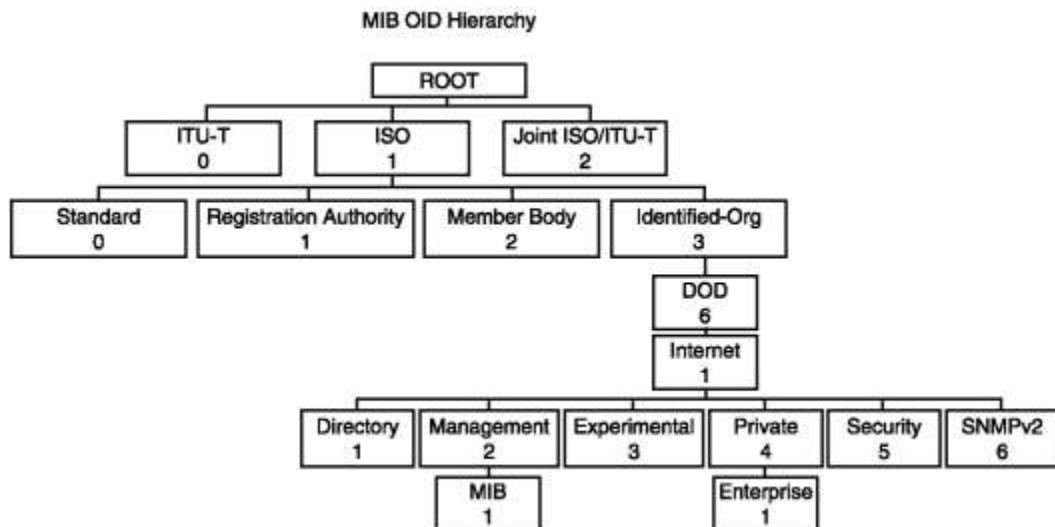
Como o SNMP consegue ler as informações do sistema? As variáveis acessíveis (informações dos dispositivos) via SNMP são **organizadas hierarquicamente**, sendo definidas nas Management Information Base (MIBs). Portanto, os equipamentos gerenciados ou agentes disponibilizam suas informações nesses bancos de dados chamados MIB e os gerentes, ou seja, um software de gerenciamento, irá ler essas informações e apresentá-las em um determinado formato, podendo ser em texto ou até mesmo em um gráfico.



Na prática, as informações que o gerente lê em uma MIB estão organizadas em tabelas que definem "índices" (chamados de OIDs) e conteúdos. Por exemplo, o OID ".1.3.6.1.2.1.1.4.0" contém como valor uma string com o contato técnico responsável pelo agente SNMP. Os OIDs são organizados em forma de árvore, e cada ramo da árvore pode receber um nome. O OID do exemplo acima também é conhecido por "SNMPv2-MIB::sysContact.0", que por sua vez é uma abreviação de ".iso.org.dod.internet.mgmt.mib-2.system.SNMPv2-MIB.sysContact.0".

Para facilitar a vida dos administradores de rede, a maioria dos softwares de gerenciamento já traz um padrão (template) que contém os modelos mais utilizados de uma maneira mais simples, para que o administrador não precise estudar como cada MIB está organizada e nem procurar o OID de cada parte do dispositivo que ele deseja monitorar.

Veja a figura com a hierarquia da MIB "Private Enterprise - 1.3.6.1.4.1", note que os números representam o caminho até chegar no campo "Enterprise" (1/ISO, 3/Identified-Org, 6/DOD, 1/Internet, 4/Private e 1/Enterprise).

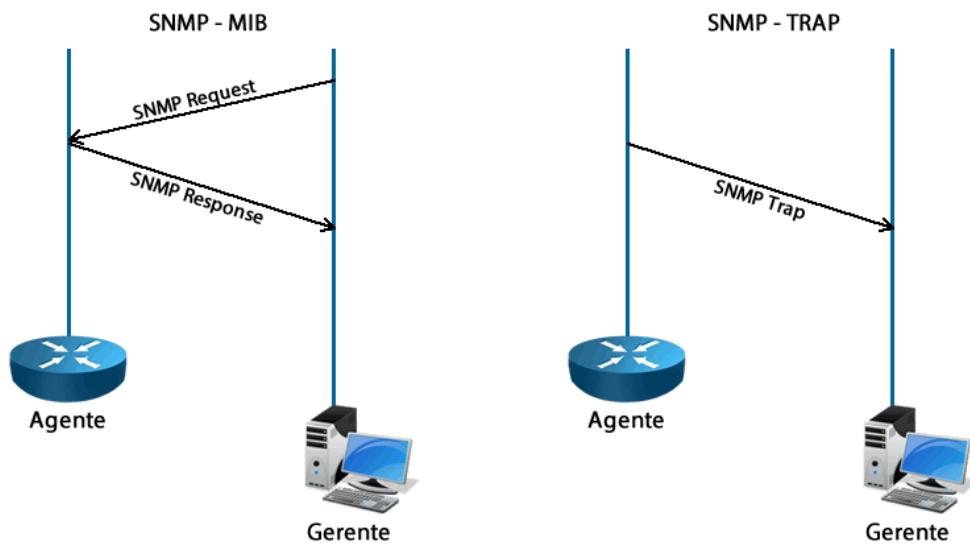


Um detalhe importante é que os dispositivos de rede, seja ele um roteador, switch, servidor ou computador, deve ter um **agente SNMP** rodando nele e também uma configuração para que os gerentes possam acessar as informações contidas nas MIBs. Para que os agentes consigam ler as MIBs são configuradas comunidades (community), as quais podem ser somente leitura ou de leitura e escrita (que permite a alteração de parâmetros via SNMP). A versão 3 do SNMP permite ainda autenticação e criptografia dos dados.

Por questões de segurança, é recomendado que nos dispositivos com agente SNMP seja restringido o endereço IP ao qual o dispositivo responde requisições SNMP através de uma lista de controle de acessos. Além disso, não se deve utilizar a community padrão que, normalmente, vem na configuração padrão de muitos dispositivos como "public" (para acesso de leitura) e "private" (para acesso leitura/escrita).

Além da leitura e escrita através de MIBs, o SNMP permite o envio de TRAPs (alarmes). A operação do TRAP ocorre no oposto do que vimos até agora, onde o gerente consulta a MIB dos agentes, pois no envio de alarmes é o dispositivo gerenciado que toma iniciativa da comunicação. Por conta disso, os sistemas de gerência de redes evitam os termos 'cliente' e 'servidor' e optam por usar "gerente" para a aplicação que roda na estação de gerenciamento e "agente" para a aplicação que roda no dispositivo de rede.

Veja na figura seguinte onde temos as duas situações ilustradas, ou seja, no modo convencional o gerente envia uma requisição ao dispositivo gerenciado, o qual responde com a informação solicitada. Já no modelo de alarmes, através do envio de TRAPs, é o contrário. O agente é que envia uma informação ao gerente, por exemplo, informando que uma determinada interface de rede ficou indisponível.



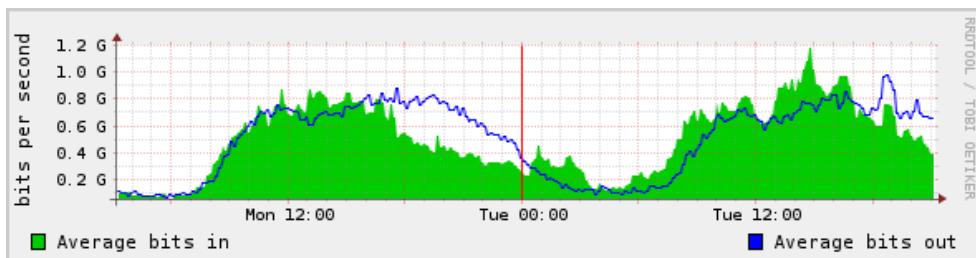
A definição dos elementos da rede a serem gerenciados varia de empresa para empresa, pois o que é importante para uma, pode não ser para outra. Além disso, o mercado dispõe de várias ferramentas para gerenciamento de redes, porém, as ferramentas mais conhecidas e de maior utilização são **Global Crossing uMonitor**, **HP Open View**, **WhatsUp**, **IBM Tivoli** e a **EITM** da Computer Associates. Além dessas, existem também ferramentas de gerenciamento gratuitas como o **Nagios**, **Cacti**, **Zabbix** e outros.

#### 2.4 MRTG – Monitorando o Tráfego via SNMP

As ferramentas de gerenciamento SNMP podem ter objetivos bastante específicos, por exemplo, verificar condições de falha, monitorar valores ou receber notificações de alarmes (traps). Um dos exemplos bastante difundido do uso do SNMP é a ferramenta chamada MRTG (Multi Router Traffic Grapher).

Inicialmente, o MRTG foi desenvolvido para monitorar o tráfego em interfaces de rede de um dispositivo gerenciado, permitindo a geração de gráficos onde é mostrada a evolução deste tráfego ao longo do tempo de diversas maneiras diferentes. Porém, suas opções de configuração o tornam uma ferramenta bastante flexível e útil para a geração de gráficos onde seja apresentada a evolução temporal de qualquer valor que possa ser monitorado via SNMP.

O MRTG pode ser configurado para a leitura de qualquer valor numérico via SNMP, armazenando o valor em um arquivo de log, no qual são mantidos registros sobre valores lidos nos dois últimos anos. Assim, a ferramenta consegue gerar gráficos com médias diárias dos valores lidos, além de gráficos correspondentes à variação do valor monitorado no período de uma semana, um mês e um ano. Veja na figura um exemplo do gráfico gerado pelo MRTG com a banda utilizada em Gbps mostrada em dias da semana.

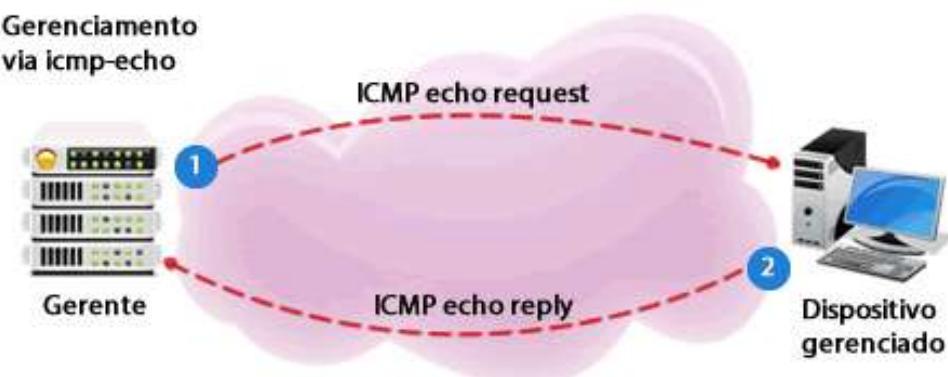


Existem versões de MRTG para Linux e Windows, porém as configurações não são triviais, mesmo assim se você desejar explorar mais o assunto o download está disponível em:

<http://oss.oetiker.ch/mrtg/download.en.html>

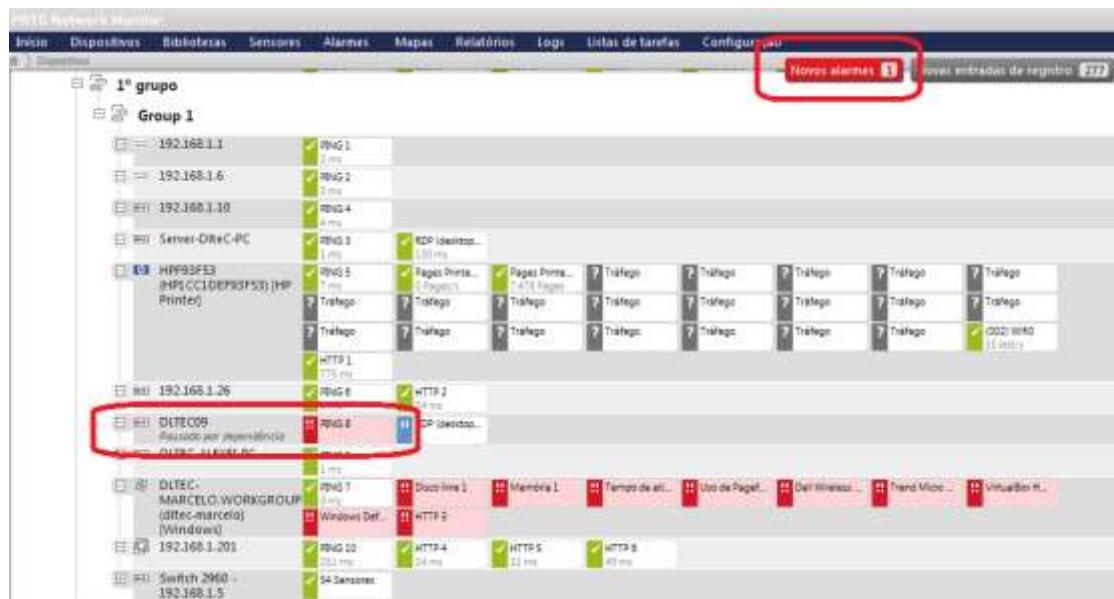
## 2.5 Utilizando o ICMP para Gerenciar a Rede

Além do SNMP, outros protocolos de rede podem ser utilizados para monitoração de dispositivos, um deles é o ICMP, mas especificamente o ping. Alguns softwares de monitoração permitem que você habilite o ping para ser realizado de tempos em tempos e mostre em forma de alarme caso o dispositivo não responda.



Essa é uma maneira simples de monitoração, a qual permite mostrar a disponibilidade dos dispositivos, assim como identificar possíveis quedas de comunicação entre localidades remotas.

Veja a tela a seguir com o exemplo de um sistema de monitoração onde o ping é utilizado para verificar a disponibilidade dos dispositivos. Note que o dispositivo DLTEC09 está alarmado, pois o dispositivo foi desligado e o sistema de gerenciamento não está mais recebendo o echo reply dessa máquina, portanto o sistema indica um problema de conexão. O software utilizado nesse exemplo é o PRTG Network Monitor, o qual possui uma versão gratuita e permite a monitoração dos dispositivos através de vários tipos de protocolos, inclusive o SNMP e ICMP.



## 2.6 Analisadores de Protocolos e Sniffers

Normalmente, quando uma placa de rede recebe um quadro ela verifica se o endereço MAC contido no campo de destino do quadro é igual ao configurado nela, caso não seja esse quadro é descartado (a não ser que o endereço seja um broadcast ou multicast, pois nesses dois casos o quadro é processado e enviado para a camada de rede).

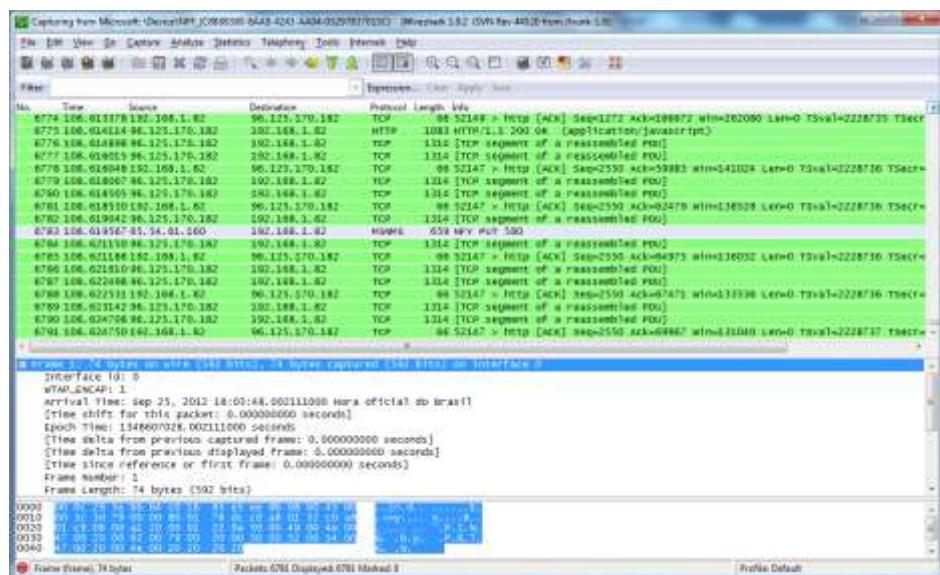
Na camada de rede acontece a mesma coisa, se o IP de destino for diferente do configurado na placa de rede quer dizer que aquele pacote não é para o seu micro, por isso ele deve descartar a informação, a não ser que seja um pacote de broadcast ou para um endereço de multicast que esteja configurado no computador. Mas existe um modo de operação nas placas de rede, chamado **"modo promíscuo"**, o qual faz com que toda a informação que chegue até ela seja repassada para cima e lida, isso se chama "sniffing".

Portanto, o sniffing é um procedimento realizado por uma ferramenta conhecida como sniffer (também conhecido como Packet Sniffer, Analisador de Rede, Analisador de Protocolo, Ethernet Sniffer em redes do padrão Ethernet ou ainda Wireless Sniffer em redes wireless), a qual pode ser um software ou hardware capaz de interceptar e registrar o tráfego de dados em uma rede de computadores. Conforme o fluxo de dados trafega na rede, o sniffer captura cada pacote e eventualmente decodifica e analisa o seu conteúdo de acordo com o protocolo definido em um RFC ou outra especificação.

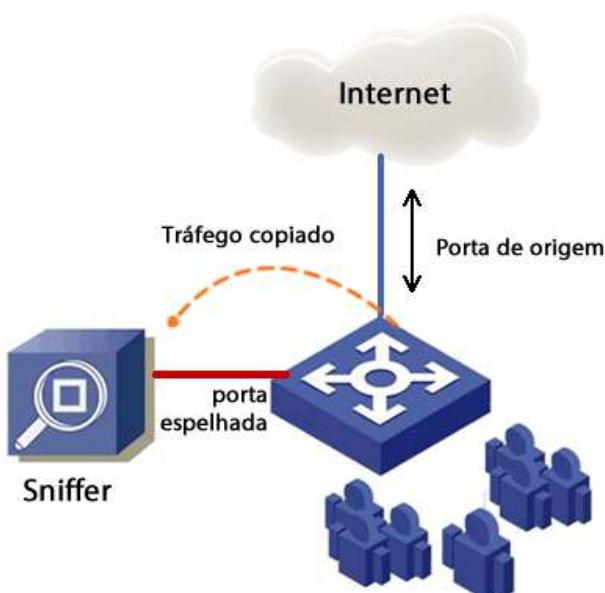
O sniffing pode ser utilizado com propósitos maliciosos por invasores que tentam capturar o tráfego da rede com diversos objetivos, por exemplo, para obter cópias de arquivos importantes durante sua transmissão ou então obter senhas que permitam acesso mais amplo ao ambiente invadido ou simplesmente monitorar as conversações em tempo real.

Porém, quando utilizado para o bem, o sniffer pode ser um aliado importante dos administradores de rede, pois eles permitem monitorar o tráfego e buscar por padrões que possam interferir no bom funcionamento da rede. Por exemplo, o administrador de redes pode, com o sniffer, analisar a quantidade de broadcast que está circulando na rede e detectar problemas de lentidão devido a tempestades de broadcast ou mau funcionamento de algum dispositivo.

Um dos sniffers mais utilizados é o Wireshark, o qual é gratuito e simples de se utilizar. Veja a tela do programa.



Lembre que em uma rede com switches não é possível de se fazer o sniffing diretamente, você precisa primeiro fazer o espelhamento de uma porta para conectar nela o equipamento que tem o sniffer. Veja na figura o exemplo de uma topologia onde uma porta que recebe o tráfego de Internet está sendo espelhada para que um sniffer possa analisar todo o tráfego de entrada e saída para a Internet.



*Nesse último capítulo vamos estudar com mais detalhe o funcionamento do IP versão 6 para entender as principais diferenças com a versão anterior (IPv4), assim como novas funcionalidades que foram introduzidas nessa nova versão do protocolo IP.*

*Lembrem-se que o lançamento oficial em nível mundial do IPv6 aconteceu no ano de 2012 e por um bom tempo as duas versões do protocolo IP devem coexistir, pois até uma total migração da comunicação pela Internet e nas redes corporativas para a versão 6 do protocolo IP teremos um longo caminho pela frente.*

*Bons estudos.*

## **Capítulo 11 - Protocolo IP versão 6**

### **Objetivos do Capítulo**

Ao final desse capítulo você deverá ter estudado e compreendido os seguintes assuntos:

- Diferença entre o IPv6 e IPv4
- Principais características do IPv6
- Principais recursos do IPv6
- Técnicas de convivência e transição entre IPv4 e IPv6

## Sumário do Capítulo

<b>1 Qual a Maior Diferença entre o IPv4 e o IPv6?.....</b>	<b>365</b>
<b>2 Campos do Pacote IPv6.....</b>	<b>366</b>
<b>3 Tipos de Comunicação e Endereços em IPv6 .....</b>	<b>368</b>
<b>4 Escrevendo e Interpretando Endereços IPv6 .....</b>	<b>370</b>
<b>5 Faixas de Endereçamento e Endereços Especiais .....</b>	<b>372</b>
5.1 IEEE EUI-64 .....	374
<b>6 Recursos e Serviços do IPv6 .....</b>	<b>375</b>
6.1 ICMPv6.....	375
6.2 NDP (Neighbor Discovery Protocol) ..	376
6.2.1 Determinando o Endereço MAC de Hosts Vizinhos.....	377
6.2.2 Encontrando Roteadores Vizinhos....	377
6.2.3 Detectando Endereços IPv6 Duplicados	
378	
6.2.4 Determinando a Acessibilidade dos Vizinhos	378
6.2.5 Redirecionamento de Pacotes .....	379
6.3 Distribuindo Endereços - Autoconfiguração e DHCPv6.....	379
6.3.1 Configuração Manual.....	379
6.3.2 Autoconfiguração Stateless .....	381
6.3.3 DHCPv6 – Stateless e Stateful .....	382
6.4 Fragmentação.....	383
6.5 Mobilidade.....	384
6.6 QoS – Qualidade de Serviços.....	385
6.7 Conceitos de Segurança em Ambiente IPv6	386
6.8 Roteamento IPv6.....	387
<b>7 Técnicas de Convivência e Transição entre o IPv4 e IPv6 .....</b>	<b>389</b>
7.1 Pilha Dupla.....	391
7.2 Tunelamento .....	392
7.3 Técnicas de Tradução.....	394
<b>8 Próximos Passos Rumo a Transição para o IPv6.....</b>	<b>395</b>

## 1 Qual a Maior Diferença entre o IPv4 e o IPv6?

A maior diferença entre o IPv4 e o IPv6 com certeza é o número de endereços IP disponíveis em cada um dos protocolos. No IPv4 temos 4,294,967,296 endereços, enquanto no IPv6 temos um total de 340,282,366,920,938,463,463,374,607,431,768,211,456 endereços IP. Note abaixo como a diferença é gritante:

**IPv4:** 4,294,967,296  
**IPv6:** 340,282,366,920,938,463,463,374,607,431,768,211,456

Esta diferença de valores entre o IPv4 e o IPv6 representa aproximadamente **79 octilhões de vezes** a quantidade de endereços IPv6 em relação a endereços IPv4, além disso, mais de **56 octilhões de endereços** por ser humano na Terra, considerando-se a população estimada em 6 bilhões de habitantes.

Tecnicamente as funcionalidades da Internet continuarão as mesmas com a introdução do IPv6 na rede e, com certeza, ambas versões do protocolo IP deverão funcionar ao mesmo tempo, tanto nas redes já implantadas em IPv4 como em novas redes que serão montadas. Atualmente as redes que suportam IPv6 também suportam o IPv4 e ambos protocolos deverão ser utilizados por um bom tempo ainda.

Acompanhe na tabela onde mostramos uma comparação simples em termos somente do formato dos endereços e quantidades.

	<b>Internet Protocol version 4 (IPv4)</b>	<b>Internet Protocol version 6 (IPv6)</b>
Publicação	1981	1999
Tamanho do Endereço	32-bit	128-bit
Notação	Decimal: 192.149.252.76	Hexadecimal: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Notação em Prefixo	192.149.0.0/24	3FFE:F200:0234::/48
Quantidade de Endereços	$2^{32} = \sim 4,294,967,296$	$2^{128} = \sim 340,282,366,920,938,463,463,374,607,431,768,211,456$

Outras diferenças importantes são a introdução dos endereços de anycast e a retirada dos endereços de broadcast. Isso mesmo, o grande vilão do IPv4, o broadcast, no IPv6 não existe mais. Agora no IPv6 temos endereços de unicast, multicast e anycast. Caso seja necessário enviar uma mensagem a todos os hosts pode-se utilizar um pacote de multicast para o endereço de link-local de destino chamado de "all nodes address" (FF02::1).

Outro ponto importante é que no IPv6 ainda temos a parte de rede, subrede e host, como no IPv4, mas não utilizamos mais o termo **máscara** e sim somente **prefixo**. O prefixo do IPv6 tem a mesma funcionalidade do prefixo do CIDR e conta a quantidade de bits de rede ou subrede que a máscara tem, sendo que os bits 1 continuam indicando a porção de redes e os bits zero os hosts. No exemplo dado na tabela anterior temos a rede 3FFE:F200:0234::/48 e o /48 representa o prefixo dessa rede, ou seja, os primeiros 48 bits do endereço são bits de rede e os demais 80 bits (128-48) são de host. Isso mesmo, temos 80 bits para hosts nesse exemplo.

## 2 Campos do Pacote IPv6

O cabeçalho do pacote IPv6 é bem mais simples que o do IPv4, contendo apenas 8 campos principais e caso serviços adicionais sejam necessários existem extensões de cabeçalho que podem ser utilizadas. O cabeçalho (header) básico está na figura abaixo.

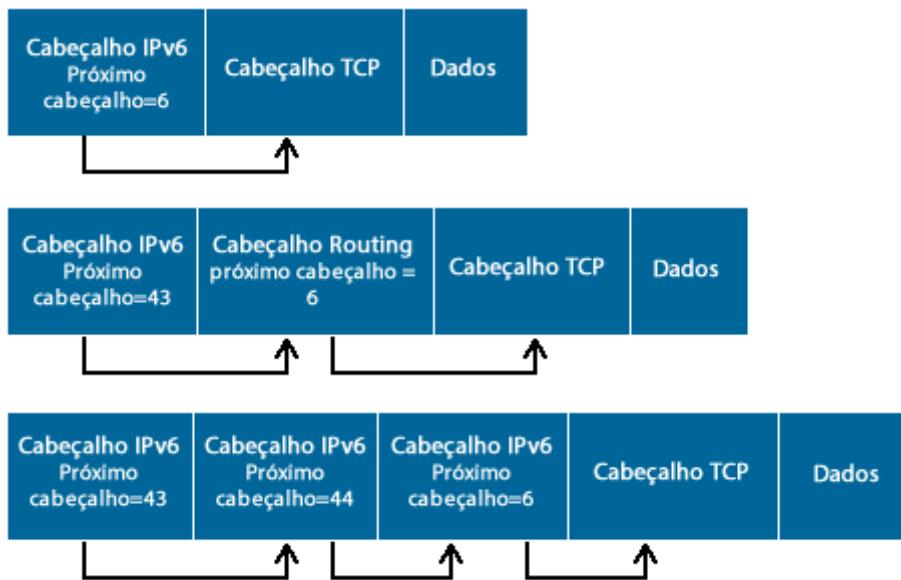


A descrição de cada campo segue abaixo:

- **Version (versão - 4 bits)**: Contém o valor para versão 6.
- **Priority ou Traffic Class (classe de tráfego - 8 bits)**: Um valor de DSCP para QoS (qualidade de serviços).
- **Flow Label (identificador de fluxo - 20 bits)**: Campo opcional que identifica fluxos individuais. Idealmente esse campo é configurado pelo endereço de destino para separar os fluxos de cada uma das aplicações e os nós intermediários de rede podem utilizá-lo de forma agregada com os endereços de origem e destino para realização de tratamento específico dos pacotes.
- **Payload Length (tamanho do payload - 16 bits)**: Tamanho do payload em bytes.
- **Next Header (próximo cabeçalho - 8 bits)**: Cabeçalho ou protocolo que virá a seguir. É utilizado para identificar que existem cabeçalhos de extensão após o principal.
- **Hop Limit (limite de saltos - 8 bits)**: Similar ao tempo de vida de um pacote IPv4 (TTL - time to live) utilizado no teste de traceroute.
- **Source Address (endereço IPv6 de origem - 128 bits)**: Endereço IP de quem está enviando os pacotes.
- **Destination Address (endereço IPv6 de destino - 128 bits)**: Endereço IP do host remoto que deve receber os pacotes.

Aqui vem mais uma diferença do IPv6, pois no IPv4 o cabeçalho base continha todas as informações principais e opcionais (mesmo que não fossem utilizadas). Já o IPv6 trata essas informações adicionais como cabeçalhos opcionais chamados de “**cabeçalhos de extensão**”.

Os cabeçalhos de extensão são inseridos entre o cabeçalho base e o cabeçalho da camada imediatamente acima (payload), não tendo nem quantidade ou tamanho fixo. Caso existam múltiplos cabeçalhos de extensão no mesmo pacote, eles serão encadeados em série formando uma “cadeia de cabeçalhos”. A figura abaixo mostra um exemplo dessa situação.



De uma maneira resumida seguem os cabeçalhos de extensão possíveis e seus identificadores:

- **Hop-by-hop Options (0)**: Transporta informações adicionais que devem ser examinadas por todos os roteadores de caminho, por isso o nome hop-by-hop que em português significa **salto a salto**.
- **Routing (43)**: Definido para ser utilizado como parte do mecanismo de suporte a mobilidade do IPv6.
- **Fragment (44)**: Indica se o pacote foi fragmentado na origem.
- **Encapsulating Security Payload (50) e Authentication Header (51)**: fazem parte do cabeçalho IPSec, utilizados para criptografia do payload.
- **Destination Options (60)**: Transporta informações que devem ser processadas apenas pelo computador de destino.

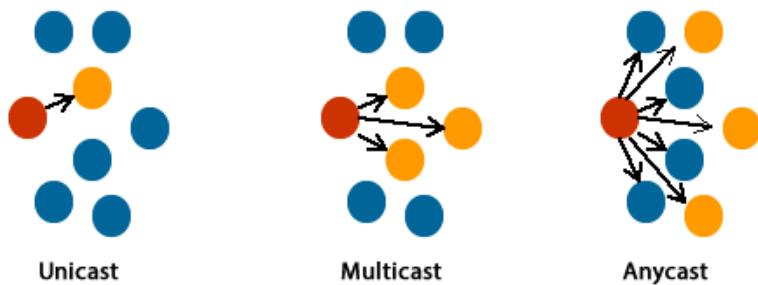
Portanto, o cabeçalho do IPv6 além de ser mais simples que o do IPv4, também trata de questões como QoS e segurança de maneira nativa, ou seja, dentro do próprio cabeçalho sem a necessidade de implementações e recursos adicionais como era necessário para o IPv4.

### 3 Tipos de Comunicação e Endereços em IPv6

Como já citado anteriormente, no IPv6 não temos mais os endereços e a comunicação via broadcast. Os endereços de unicast e multicast continuam existindo e com a mesma função em ambas versões de protocolo, porém foi criado um tipo a mais de endereçamento chamado de anycast. Veja abaixo a descrição resumida de cada um deles:

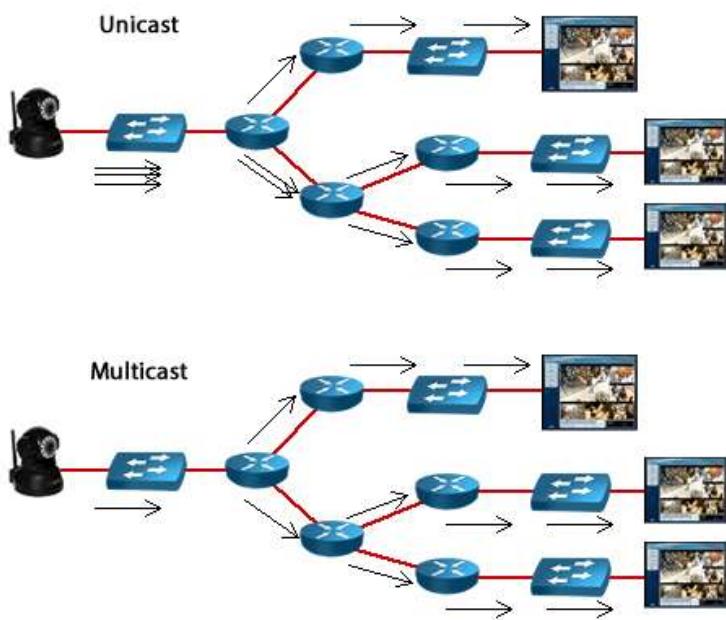
- **Unicast** → Comunicação um para um.
- **Multicast** → Comunicação um para muitos (grupo de dispositivos configurados com o mesmo endereço).
- **Anycast** → Endereço configurado em múltiplas interfaces.

Veja a figura a seguir com a representação de cada um dos três tipos de comunicação.



Para visualizar a diferença e aplicação do uso do unicast para multicast considere a figura abaixo, onde você tem um dispositivo de vídeo que irá transmitir o sinal para três hosts na rede.

Caso a transmissão seja feita utilizando unicast terão que ser criados três fluxos, um para cada host de destino, ocupando mais banda, pois a mesma informação é triplicada. Já no caso do uso do multicast o transmissor envia as informações para um único endereço que está configurado em todos os hosts que participam do mesmo “grupo de multicast” que ele, portanto a informação é transmitida utilizando apenas um fluxo até os hosts.



O endereço IP de anycast é um endereço que **podemos configurar em mais de um dispositivo**, portanto ele será anunciado em diferentes roteadores. Mas para que serve o anycast na prática? Uma das respostas e a mais utilizada é para redundância (apesar de que pode ser utilizado para balanceamento de carga).

Por exemplo, você tem três servidores DNS e configura o mesmo IP de anycast nos três, porém cada um está conectado por caminhos diferentes (roteadores distintos ou larguras de bandas diferentes). Quando o computador for realizar uma consulta ao DNS ele enviará o pacote para o IP de anycast (destino) configurado em sua placa de rede, porém quando a rede receber o pacote com o endereço de destino sendo um anycast os roteadores encaminharão esse pacote para o melhor destino em relação à origem. Ou seja, mesmo tendo três servidores com o mesmo IP de Anycast o que tiver melhor métrica em relação ao protocolo de roteamento utilizado é o que receberá a solicitação.

Por exemplo, você está utilizando OSPFv3, o qual utiliza um custo como métrica para encontrar o melhor caminho, se um dos servidores tem custo 25 (Server A), o segundo custo 40 (Server B) e o terceiro custo 20 (Server C) qual dos três irá receber a consulta enviada pelo cliente? Com certeza será o que possui menor custo (menor métrica), portanto o Server C receberá os pacotes referentes à consulta de nomes e deverá responder ao cliente.



Duas dicas importantes, o IP de anycast não é utilizado como origem em um pacote IPv6, **somente como destino** e **precisa estar anunciado** entre os roteadores (através do protocolo de roteamento) para que possa ser encaminhado conforme exemplo anterior. Portanto não é só configurar um IP, o uso do anycast exige configurações de roteamento na rede.

#### 4 Escrevendo e Interpretando Endereços IPv6

Antes de falar de como o endereçamento é dividido vamos ver como podemos escrever um endereço IPv6 (notação em hexadecimal) e também as partes que o compõe. Caso você tenha dúvidas sobre o sistema hexadecimal volte ao capítulo sobre endereçamento IP e revise a parte de **Sistemas de Numeração**.

Como já visto em capítulos anteriores, o endereço IPv6 possui 128 bits e é escrito em hexadecimal, diferente do IPv4 que eram 32 bits (4 conjuntos de 8 bits escritos em decimal pontuado). Portanto, agora cada algarismo de um IPv6 pode ter os números de 0 a 9, assim como as letras de A a F, totalizando 16 algarismos, por isso o nome hexadecimal. Veja quanto vale de A a F em decimal (*você pode escrever as letras do hexadecimal tanto em maiúsculo como em minúsculo, tanto faz!*):

- "A" vale 10 em decimal
- "B" vale 11 em decimal
- "C" vale 12 em decimal
- "D" vale 13 em decimal
- "E" vale 14 em decimal
- "F" vale 15 em decimal

Como cada algarismo em hexadecimal tem 4 bits, em 128 bits temos um total de 32 algarismos hexadecimais divididos de 4 em 4, ou seja, oito conjuntos de quatro algarismos em hexadecimal separados por dois pontos ":" (não mais pelo ponto "." como era no IPv4). Um exemplo de IPv6 é "**2000:1234:ade4:ffa0:2234:0000:0000:0012**".

Existem ainda três contrações (reduções) que podemos fazer nos endereços IPv6:

1. Zero a esquerda pode ser omitido: 2000:1234:ade4:ffa0:2234:0000:0000:**12**
2. Conjuntos de 4 zeros na mesma casa podem ser reduzidos para um zero: 2000:1234:ade4:ffa0:2234:**0:0**:12
3. Sequências de zeros podem ser substituídas por dois conjuntos de dois pontos: 2000:1234:ade4:ffa0:2234:**::**12

A única recomendação é que não haja **ambiguidade** para a terceira contração. Para entender vamos ver um exemplo com o IP 2000:1234:ade4:**0000:0000:2234:0000**:12. Se escrevermos ele com a contração 2000:1234:ade4::2234::12 nós sabemos, por visualizar o IP que deu origem, que existem dois conjuntos de 4 zeros à esquerda do 2234 e um só conjunto à direita.

No entanto, como um dispositivo (roteador ou computador) irá distinguir como ele deve completar isso na prática? Pois se pegarmos apenas o IP contraído 2000:1234:ade4:**::2234::**12 ele pode ser tanto 2000:1234:ade4:**0000:2234:0000:0000**:12 como 2000:1234:ade4:**0000:0000:2234:0000**:12.

Logo, essa notação é inválida, pois para o dispositivo ela é ambígua uma vez que ele não vai saber como preencher os espaços com os zeros. Portanto, o IP deveria ser escrito como "**2000:1234:ade4:0:0:2234::12**" ou "**2000:1234:ade4::2234:0:12**".

Outra representação importante, a qual já foi comentada anteriormente, é a dos **prefixos de rede**. No IPv6 continuamos escrevendo os endereços como no IPv4 utilizando a notação CIDR, ou seja, "**endereço-IPv6/tamanho do prefixo**", onde "**tamanho do prefixo**" é um valor decimal que especifica a **quantidade de bits contíguos à esquerda do endereço** que compreendem o prefixo, ou seja, a soma dos bits uns do prefixo.

Um endereço IPv6 pode ser dividido em um Prefixo Global (Global Prefix), Subrede (subnet ID) e endereço da Interface (Interface ID). O prefixo global normalmente é um /32, já o prefixo de subrede pode ser /48 (usuários corporativos) ou /56 a /64 (para usuários residenciais) dependendo do uso e recomendação de cada país. Já o endereço da interface utiliza os bits restantes do prefixo, ou seja, 128 bits menos o prefixo de subrede.



Vamos a um exemplo utilizando a rede **2001:db:3000:1::/64**, onde sabemos que temos 128 bits totais no endereço, porém 64 bits são utilizados para identificar a sub-rede, portanto termos:

- Prefixo 2001:db:3000:1::/64
- Prefixo global 2001:db::/32
- ID da sub-rede 3000:1
- ID de host: temos 64 bits (ou seja,  $2^{64} = 18.446.744.073.709.551.616$  endereços IP)

Da mesma maneira que mostramos no IPv4 com o CIDR e a notação em prefixos, no IPv6 podemos fazer a agregação de várias subredes de maneira hierárquica para reduzir a quantidade de redes anunciadas pelos protocolos de roteamento, além de continuar valendo o conceito de subrede e a utilização de diferentes prefixos conforme a necessidade de cada rede IPv6, similar ao VLSM.

Com relação a representação dos endereços IPv6 em URLs (Uniform Resource Locators), eles agora passam a ser representados entre **colchetes**. Deste modo, não haverá ambiguidades caso seja necessário indicar o número de uma porta juntamente com a URL, por exemplo:

- [http://\[2001:db:3000:1::22\]/index.html](http://[2001:db:3000:1::22]/index.html)
- [http://\[2001:db:3000:1::22\]:8080](http://[2001:db:3000:1::22]:8080)

## 5 Faixas de Endereçamento e Endereços Especiais

Se analisarmos a faixa total de endereços IPv6 vai de :: (0000:0000:0000:0000:0000:0000:0000) até ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff e assim como no IPv4 a IANA fez a alocação dos endereços entre os diversos tipos de endereçamento e faixas necessárias para serem distribuídas conforme explicado no capítulo sobre a Internet.

Portanto, vamos agora analisar a divisão dos endereços IPv6 e algumas faixas dedicadas a uso especial.

- **::/0** -> Rota padrão.
- **::/128** -> Endereço não especificado (Unspecified).
- **::1/128** -> Endereço de Loopback (no IPv4 é o 127.0.0.1).
- **::/96** -> Reservado para compatibilidade com IPv4, porém seu uso foi descontinuado. Seria um endereço como ::192.168.1.1, o motivo do /96 é que como temos 32 bits no IPv4 dá um total de "96+32=128 bits".
- **::FFFF:0:0/96** -> Endereço IPv4 mapeado como IPv6. É aplicado em técnicas de transição para que hosts IPv6 e IPv4 se comuniquem, por exemplo, ::FFFF:192.168.1.1.
- **2001::/32** → prefixo utilizado no mecanismo de transição Teredo. (mais para frente veremos o que é o Teredo).
- **2001:DB8::/32** -> prefixo utilizado para representar endereços IPv6 em textos e documentações.
- **2002::/16** -> Prefixo utilizado no mecanismo de transição 6to4.
- **FC00::/7** -> Unique local (ULA). Este endereço provavelmente será globalmente único, utilizado apenas para comunicações locais, geralmente dentro de um mesmo enlace ou conjunto de enlaces, portanto o endereço ULA não deve ser roteável na Internet.
- **FE80::/10** -> Link-local unicast. Este endereço é utilizado apenas na LAN onde a interface está conectada, o endereço link local é atribuído automaticamente utilizando o prefixo FE80::/64 e os outros 64 bits do ID da Interface são configurados utilizando o formato IEEE EUI-64, uma composição que utiliza o endereço MAC do host para formar o endereço da Interface.

### Link-local unicast



- **FEC0::/10** → Site-local unicast, porém sua utilização foi substituída pelos endereços ULA e ele caiu em desuso.
- **FF00::/8** → Faixa de endereços de multicast. Por exemplo, o IP FF02::9 é o endereço de multicast utilizado pelo protocolo de roteamento RIPng enviar seus anúncios de roteamento.

### Multicast



Abaixo seguem alguns outros endereços de multicast reservados:

- FF02::1 -> Todos os Hosts no Link
- FF02::2 -> Todos os Roteadores no Link
- FF02::5 -> Protocolo OSPFv3
- FF02::6 -> Protocolo OSPFv3
- FF02::A -> Protocolo EIGRP/Cisco
- FF02::1:2 -> Todos os Relay-Agents DHCP
- FF05::1:3 -> Todos os Servidores DHCP
- FF05::101 -> Todos os Servidores NTP

#### **Informações Extras sobre Multicast:**

Os flags são definidos da seguinte forma:

- **O primeiro bit** mais a esquerda é reservado e deve ser marcado com 0;
- **Flag R:** Se o valor for 1, indica que o endereço multicast “transporta” o endereço de um ponto de encontro (Rendezvous Point). Se o valor for 0, indica que não há um endereço de ponto de encontro embutido;
- **Flag P:** Se o valor for 1, indica que o endereço multicast é baseado em um prefixo de rede. Se o valor for 0, indica que o endereço não é baseado em um prefixo de rede;
- **Flag T:** Se o valor for 0, indica que o endereço multicast é permanente, ou seja, é atribuído pela IANA. Se o valor for 1, indica que o endereço multicast não é permanente, ou seja, é atribuído dinamicamente.
- **Os quatro bits** que representam **o escopo do endereço multicast (Scope)**, são utilizados para delimitar a **área de abrangência** de um grupo multicast. Os valores atribuídos a esse campo são o seguinte:
  - 1 – abrange apenas a interface local;
  - 2 – abrange os nós de um enlace;
  - 3 – abrange os nós de uma sub-rede
  - 4 – abrange a menor área que pode ser configurada manualmente;
  - 5 – abrange os nós de um site;
  - 8 – abrange vários sites de uma mesma organização;
  - E – abrange toda a Internet;
  - 0, F – reservados;
  - 6, 7, 9, A, B, C, D – não estão alocados

Para os endereços de Unicast (os roteáveis na Internet) está reservada para atribuição de endereços a faixa **2000::/3**, ou seja, dos endereços de 2000:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff. Isso representa **13% do total** de endereços possíveis com IPv6. O nome dado aos endereços de Unicast é “Global Unicast” ou endereço global unicast.

#### **Global unicast**

Prefixo Global	Subnet ID	Interface ID
----------------	-----------	--------------

A faixa 2800::/12 foi destinada à LACNIC para alocação na América Latina. No Brasil o NIC.br possui um /16 que faz parte deste /12 para distribuir entre as instituições e ISPs do nosso país.

Os endereços de Anycast são criados a partir da faixa de endereços unicast e não há diferenças de notação entre eles. O que os diferencia é a configuração realizada nos roteadores e um anúncio explícito de que aquele IP é de Anycast. Dessa maneira vai haver o roteamento e troca de informações sobre esses endereços de Anycast entre os roteadores, além disso, evita que os roteadores interpretem esse endereço como um IP duplicado e gere erros, pois o Anycast é um mesmo IP de Unicast configurado em vários hosts!

### 5.1 IEEE EUI-64

O padrão EUI-64 é utilizado para formação do endereço de Link Local, no processo de autoconfiguração e também pode ser utilizado no DHCPv6. O objetivo básico é utilizar o endereço MAC da placa de rede do host para formar um Interface ID de 64 bits.

Sabemos que um endereço MAC tem 48 bits e já é escrito em Hexadecimal, portanto para completar os 64 bits faltam apenas 16 bits, ou seja, quatro algarismos em Hexadecimal. Isto é feito com a inserção no meio do endereço MAC dos algarismos 0xffffe (FF-FE). Além disso, o sétimo bit mais a esquerda (chamado de bit U/L – Universal/Local) do endereço MAC deve ser invertido, isto é, **se for 1 será alterado para 0 e se for 0 será alterado para 1**.

Veja a figura a seguir, no meio do endereço MAC foi inserida a palavra em hexadecimal 0xffffe e como os dois primeiros algarismos do MAC são 00, que em binário é 00000000, se trocarmos o sétimo bit ele fica 00000010 ou 02 em hexadecimal (lembre que a cada 4 bits temos um algarismo em hexadecimal).

MAC	00	0A	27	5C	88	19
-----	----	----	----	----	----	----

EUI-64	00	0A	27	FF	FE	5C	88	19
--------	----	----	----	----	----	----	----	----

Lembre-se que se recebermos um prefixo /64 podemos perfeitamente utilizar o EUI-64 para formar o Interface ID e assim termos o endereço global do computador (endereço de Internet), além do link local. Esse processo se chama autoconfiguração do IPv6. Por exemplo, um computador que tem como endereço MAC 001e.130b.1aee e recebe um prefixo 2001::/64 do seu roteador terá os seguintes endereços de Link Local e Global Unicast:

- FE80::21E:13FF:FE0B:1AEE
- 2001::21E:13FF:FE0B:1AEE -> Prefixo 2001::/64

Como chegamos nesses valores acima? Note que o MAC é 001e.130b.1aee, portanto vamos achar o sétimo bit e fazer a inversão: 00 -> 00000000 -> 00000010 -> 02. Agora vamos inserir o FF-FE no meio e formar o EUI 64: 021e:13ff:fe0b:1aee.

## 6 Recursos e Serviços do IPv6

Assim como no IPv4 tem o ICMP, o IPv6 possui o ICMPv6 para reportar mensagens de erro e realização de testes, porém o ICMPv6 teve suas capacidades aumentadas devido ao fato de não existir mais o broadcast. Consequentemente, alguns protocolos que eram baseados no broadcast também não existem mais, por exemplo, o ARP foi substituído pelo NDP (Protocolo de Descoberta de Vizinhança).

Além disso, com mecanismos como a autoconfiguração, o DHCPv6 pode funcionar de maneiras diferentes.

Outro detalhe é que algumas funcionalidades que eram externas ao cabeçalho do IPv4 foram trazidas para dentro do cabeçalho do IPv6, como a parte de segurança e criptografia.

Vamos agora estudar os principais serviços e recursos do IPv6 e suas características.

### 6.1 ICMPv6

O protocolo ICMPv6, assim como já era o ICMPv4, é responsável pelas funções de relatar erros no processamento de pacotes, realizar diagnósticos e informar características da rede. O cabeçalho do ICMPv6 vem logo após o cabeçalho principal do IPv6 ou de algum cabeçalho de extensão (quando existir) com o campo de próximo cabeçalho (Next Header) indicando o código 58. Veja o cabeçalho do ICMPv6 na figura a seguir.

Tipo (type)	Código (code)	Soma de Verificação (checksum)
Dados		

Abaixo segue uma descrição resumida dos campos do cabeçalho:

- **Tipo:** tipo da mensagem (8 bits).
- **Código:** informações adicionais para determinados tipos de mensagens (8 bits).
- **Soma de Verificação:** utilizado para detectar dados corrompidos no cabeçalho ICMPv6 e em parte do cabeçalho IPV6 (16 bits).
- **Dados:** informações de diagnóstico e erro, de acordo com o tipo de mensagem. (Tamanho varia de acordo com a mensagem).

O ICMPv6 tem mais mensagens que a versão anterior, pois além das mensagens padrões ele incorpora funções de outros protocolos como o ARP/RARP e IGMP (Internet Group Management Protocol). Tais protocolos são importantes para:

- Descoberta de Vizinhança (Neighbor Discovery Protocol - NDP)
- Gerenciamento de Grupos Multicast
- Mobilidade
- Descoberta do Path MTU

As mensagens de erro que o ICMPv6 pode notificar seguem na tabela abaixo.

<b>Tipo</b>	<b>Nome</b>	<b>Descrição</b>
1	Destination Unreachable	Indica falhas na entrega do pacote como endereço ou porta desconhecida ou problemas na comunicação.
2	Packet too big	Indica que o tamanho do pacote é maior que a MTU de um enlace.
3	Time Exceeded	Indica que o limite de roteamento ou o tempo de remontagem do pacote foi excedido.
4	Parameter Problem	Indica erro em algum campo do cabeçalho IPv6 ou que o tipo indicado no campo "próximo cabeçalho" não foi reconhecido.
100-101	-	Uso experimental.
102-126	-	Não utilizado.
127	-	Reservado para expansão das mensagens de erro ICMPv6.

Existem ainda as mensagens de informação, as quais são utilizadas pelos protocolos que estudaremos a seguir.

## 6.2 NDP (Neighbor Discovery Protocol)

O protocolo de descoberta de vizinhos ou simplesmente NDP tem várias funções dentro do IPv6, conforme listadas abaixo:

- Determinar o endereço MAC dos nós da rede (substituto do ARP).
- Encontrar roteadores vizinhos.
- Determinar prefixos e outras informações de configuração da rede.
- Detectar endereços duplicados.
- Determinar a acessibilidade dos roteadores.
- Redirecionamento de pacotes.
- Autoconfiguração de endereços.

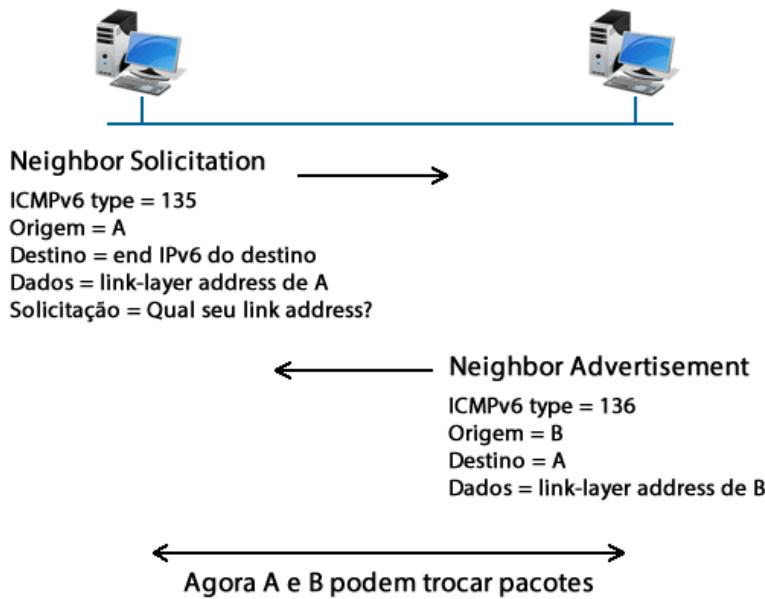
Os recursos acima são realizados com as seguintes mensagens d ICMPv6:

<b>Cód ICMP</b>	<b>Mensagem ICMP</b>	<b>Função</b>
133	Router Solicitation	Mensagens utilizadas para que hosts requisitem aos roteadores as mensagens de Router Advertisements proativamente, ou seja, sem esperar um anúncio por parte do roteador.
134	Router Advertisment	Mensagens enviadas periodicamente pelos roteadores ou em resposta a uma Router Solicitation enviada por um host. São utilizadas pelos roteadores para anunciar sua presença em uma rede local ou na Internet.
135	Neighbor Solicitation	Mensagem de multicast enviada por um nó para determinar o endereço MAC e a acessibilidade de um vizinho. Utilizada também para detectar a existência de endereços duplicados.
136	Neighbor Advertisment	Mensagem enviada como resposta a um Neighbor Solicitation. Pode também ser enviada para anunciar a mudança de algum endereço MAC dentro do enlace.
137	Redirect Message	Mensagem utilizada por roteadores para informar ao host que existe um roteador mais indicado para se alcançar um destino, ou seja, um redirecionamento.

### 6.2.1 Determinando o Endereço MAC de Hosts Vizinhos

Assim como a comunicação do IPv4, para enviar um pacote IPv6 para um vizinho, o computador precisa saber o endereço MAC de origem (dele mesmo, portanto já sabe) e o endereço MAC do destino (computador remoto), o que é função do ARP na versão 4 do protocolo IP.

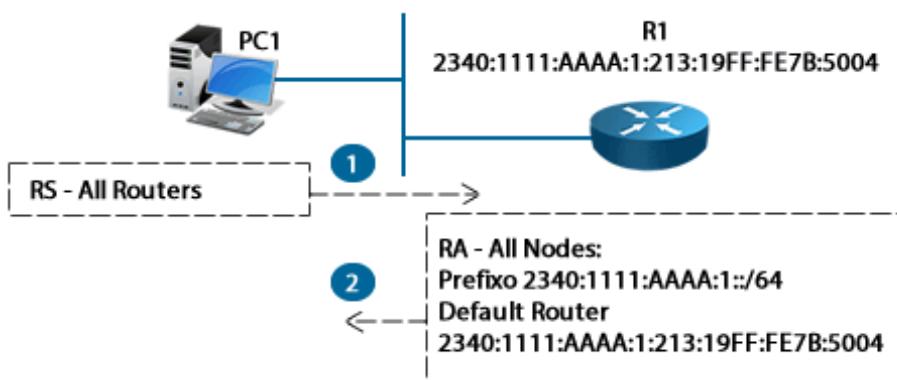
Já no IPv6 o processo é realizado através da troca de mensagens ICMP e funciona com um host enviando uma mensagem **Neighbor Solicitation** informando no campo de dados **seu endereço MAC** e também **solicitando o endereço MAC do vizinho**. Ao receber a mensagem, o vizinho a responde enviando uma mensagem **Neighbor Advertisement** informando seu endereço MAC. Após essa troca de mensagens o computador de origem tem condições de iniciar a troca de pacotes com o computador de destino. Veja a figura.



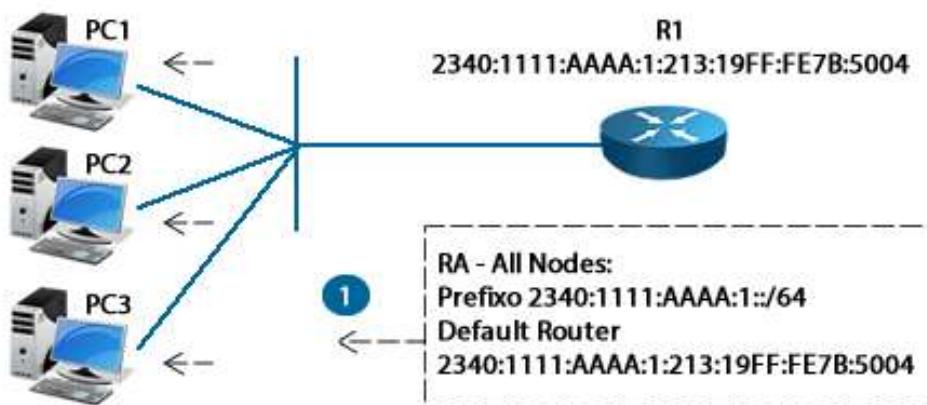
### 6.2.2 Encontrando Roteadores Vizinhos

O processo utilizado para localizar roteadores vizinhos dentro do mesmo enlace, bem como aprender prefixos e parâmetros relacionados à autoconfiguração de endereço, se inicia com o envio de um **Router Solicitation (RS)** pelo host. O roteador local responde com uma mensagem de **Router Advertisement (RA)** para o endereço multicast all-nodes com as informações configuradas nele.

Mais para frente você aprenderá mais sobre a autoconfiguração e o DHCPv6, os quais utilizam o processo de descoberta de roteadores no seu funcionamento.



Também é possível que o host receba uma mensagem de Router Advertisement sem ter enviado a solicitação (Router Solicitation), isso porque os roteadores fazem o anúncio de suas redes periodicamente, de maneira proativa.



### 6.2.3 Detectando Endereços IPv6 Duplicados

No IPv4 a detecção de IPs duplicados era feita pelo protocolo ARP utilizando ARPs gratuitos (Gratuitous ARP). No IPv6 essa detecção é realizada utilizando mensagens "Neighbor Solicitation" para o endereço "All-nodes Multicast" da seguinte maneira, o host envia seu endereço IPv6 na mensagem "Neighbor Solicitation" e aguarda uma resposta. Caso haja uma resposta ele sabe que o IP que ele utiliza está duplicado.

### 6.2.4 Determinando a Acessibilidade dos Vizinhos

O NDP é capaz de determinar a disponibilidade de um vizinho analisando protocolos da camada superior. Por exemplo, verificando os ACKs recebidos pelo protocolo TCP, ou então, proativamente realizando uma resolução de endereços (via ICMPv6) quando certos limites são excedidos, porém esse monitoramento só é realizado para comunicações **unicast** (comunicações host a host, roteador a host ou roteador a roteador).

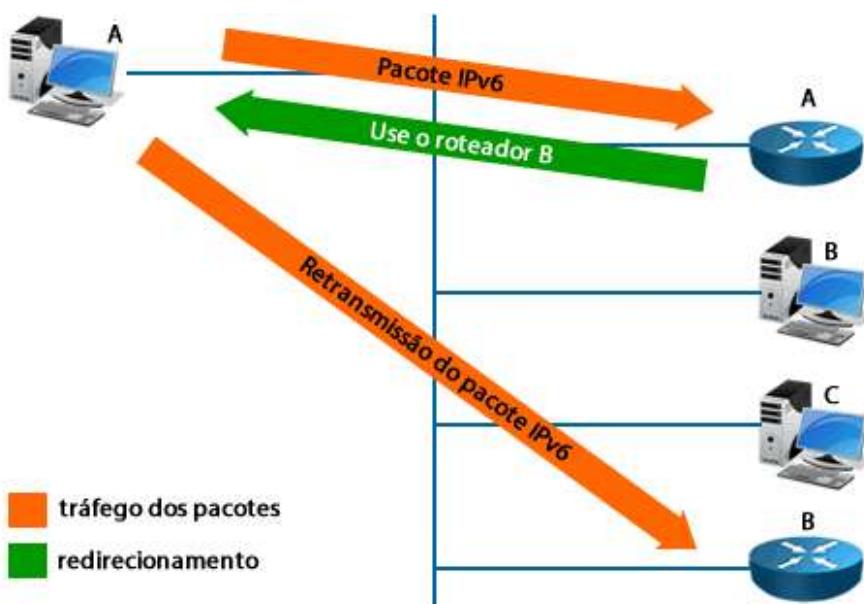
Para esse rastreamento são utilizadas duas tabelas:

- **Neighbor Cache:** Mantém uma lista de vizinhos locais para os quais foi enviado tráfego recentemente. Essas listas contém o endereço IP, o endereço MAC, um flag que identifica se esse IP é um Host ou um Router, se há pacotes na fila para serem enviados a esse destino, a sua acessibilidade e a próxima vez que um evento de detecção de vizinhos está agendado. É semelhante à tabela ARP do IPv4.

- **Destination Cache:** Mantém informações sobre destinos, locais e/ou remotos, para os quais foi enviado tráfego recentemente. As entradas dessa tabela são atualizadas com informações recebidas por mensagens "Redirect". A tabela Neighbor Cache pode ser considerada como um subconjunto dessa tabela.

#### 6.2.5 Redirecionamento de Pacotes

As mensagens de redirecionamento no IPv6 são quase idênticas as mensagens de redirecionamento no IPv4. Elas são enviadas por roteadores e tem como função redirecionar um host automaticamente para outro roteador mais apropriado ou para informar ao host que o destino encontra-se no mesmo enlace.



### 6.3 Distribuindo Endereços - Autoconfiguração e DHCPv6

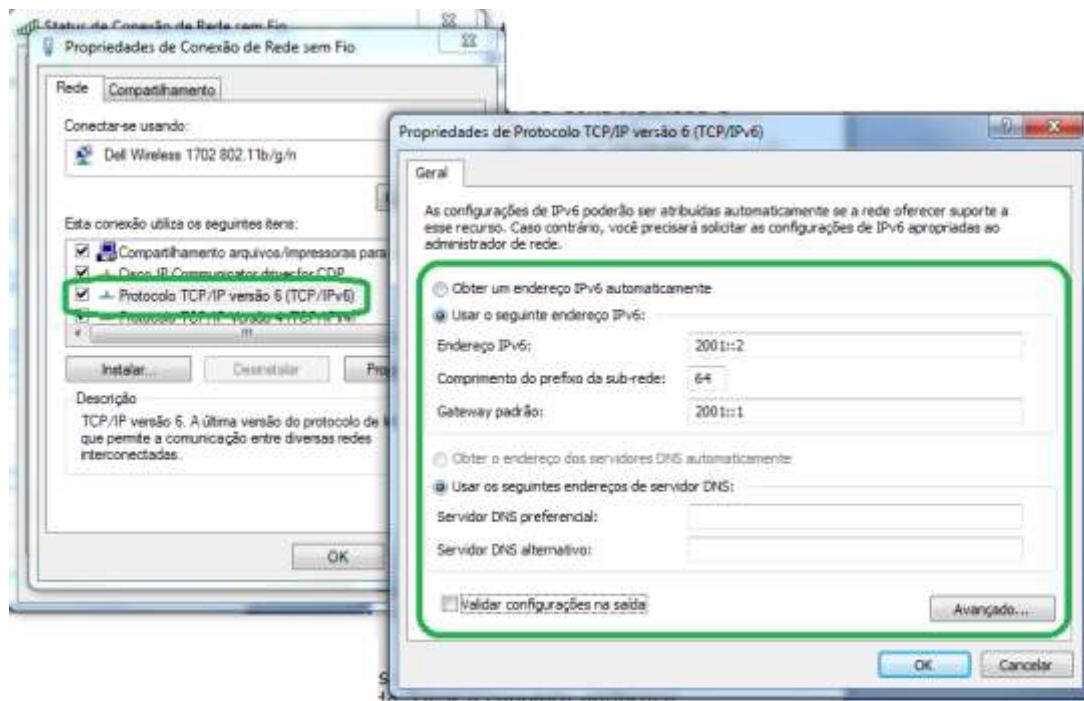
Assim como na versão 4 do protocolo IP, a primeira etapa para que um host tenha acesso à rede é a atribuição de um endereço de host à sua Interface. No IPv4 tínhamos a possibilidade de configurar um IP estaticamente (manual) ou através de um servidor DHCP.

Para o IPv6 temos quatro opções: a configuração **manual dos endereços**, a **autoconfiguração stateless**, o **DHCPv6 stateless** e o **DHCPv6 statefull**.

#### 6.3.1 Configuração Manual

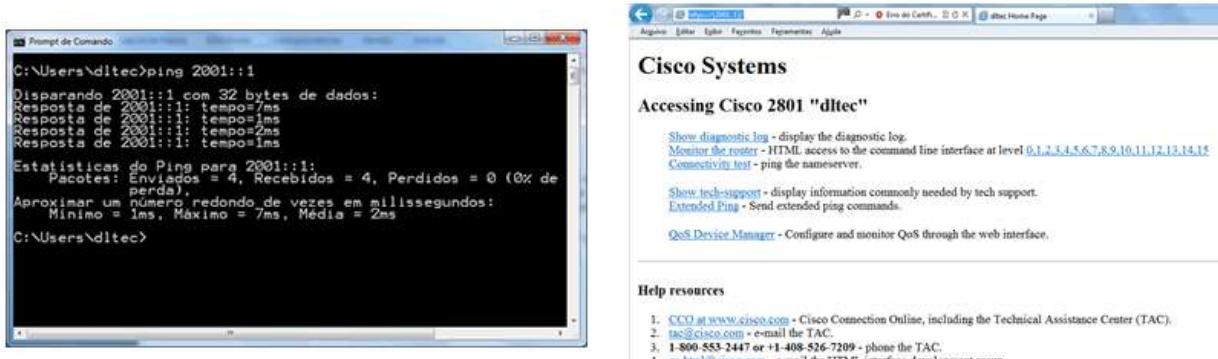
A configuração manual dispensa comentários, nela o administrador de redes deve definir manualmente o endereço IPv6 a ser utilizado, assim como os demais parâmetros.

No Windows 7, ou acima, o IPv6 já vem habilitado e o caminho para chegar às configurações é parecida, porém escolha no final o protocolo IPv6 ao invés do IPv4. Vá em “Painel de Controle > Rede e Internet > Central de Rede e Compartilhamento”, clique na interface de rede desejada, depois clique em propriedades e dois cliques no protocolo TCP/IP versão 6 (TCP/IPv6), conforme tela da figura mostrada a seguir.



Assim como para o IPv4, o IPv6 vem configurado para pegar os dados automaticamente via DHCP ou autoconfiguração no Windows 7, porém você pode clicar na opção de "Usar o seguinte endereço IPv6" e definir manualmente o endereço, prefixo, gateway padrão e servidor DNS.

Para testar a configuração podemos utilizar o ping para o IP do gateway configurado, veja a saída do comando na tela da figura a seguir (a esquerda). Na direita, você tem a tela do acesso via HTTPS ao roteador com IP 2001::1, assim testamos a conectividade das camadas 2 e 3 com o ping e até a camada 7 com o acesso HTTPS.



Para verificar as configurações você pode utilizar o comando "ipconfig /all" ou "netsh int ipv6 sh addr", conforme mostrado abaixo.

```

C:\Users\dltec>netsh int ipv6 sh addr
Interface 1: Loopback Pseudo-Interface 1
Tipo End. Estado DAD Vida Válida Vida Pref. Endereço
Outros Preferencial infinite infinite ::1
Interface 12: Conexão de Rede sem Fio Global Unicast
Tipo End. Estado DAD Vida Válida Vida Pref. Endereço
Manual Preferencial infinite infinite 2001::2
Outros Preferencial infinite infinite fe80::fe80:ae76:db9:bcdx12
Interface 24: Teredo Tunneling Pseudo-Interface
Tipo End. Estado DAD Vida Válida Vida Pref. Endereço Link Local
Outros Substituído infinite infinite fe80::e0:0:0:0%24
Interface 11: Conexão local
Tipo End. Estado DAD Vida Válida Vida Pref. Endereço
Outros Substituído infinite infinite fe80::943c:8f31:8302:6acx11
Interface 43: Isatap.(C8B88380-BAA9-4243-AA04-03297B37015C)
Tipo End. Estado DAD Vida Válida Vida Pref. Endereço

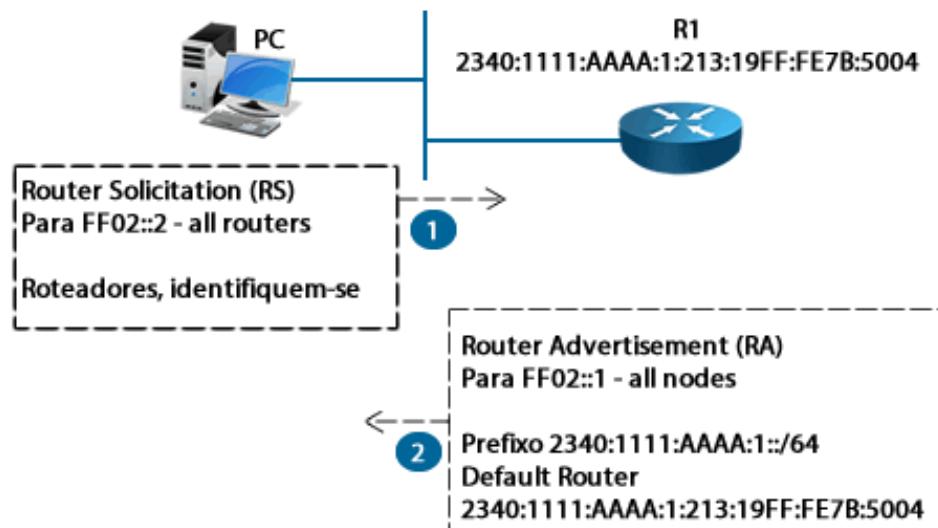
```

### 6.3.2 Autoconfiguração Stateless

O processo de **autoconfiguração stateless** consiste na **atribuição automática** do endereço sem que haja intervenção do administrador. O endereço é gerado em duas etapas:

1. Formação dos 64 Bits de Host (Interface ID) através do padrão EUI-64.
2. Formação dos 64 Bits de Prefixo através de um anúncio realizado pelo roteador.

O prefixo será descoberto por meio da comunicação entre o host com algum roteador previamente configurado. Para que essa atribuição automática ocorra o protocolo NDP (Neighbor Discovery Protocol – Protocolo de Descoberta de Vizinhos) é utilizado entre o host e o roteador.

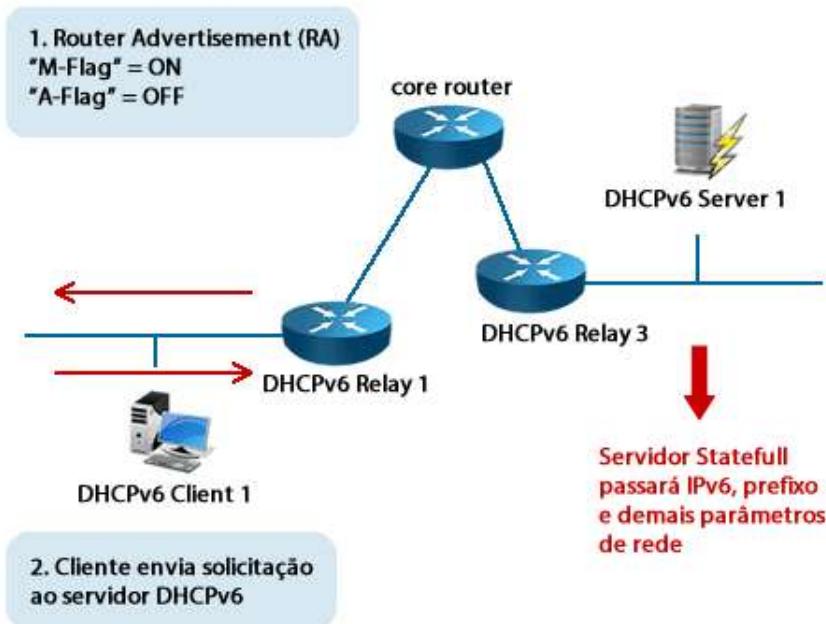


Portanto os computadores enviam uma solicitação chamada "Router Solicitation" para o endereço de multicast FF02::2, o qual significa todos os roteadores ou "all routers". Ao receber essa mensagem, o roteador que está na mesma subrede responde com o prefixo e o seu endereço, o qual será utilizado como roteador padrão, através de um "Router Advertisement" para o endereço FF02::1, que é o endereço de multicast para todos os computadores (uma espécie de emulação do broadcast utilizando multicast).

Com isso o computador já tem seu endereço de Internet e o IP do roteador padrão. Além disso, o roteador pode passar o MTU e o limite de encaminhamento do cabeçalho IPv6.

### 6.3.3 DHCPv6 – Stateless e Stateful

Com o DHCPv6 Stateful, os endereços dos hosts, servidores DNS, nome do domínio e demais opções necessárias aos clientes são automaticamente atribuídos através de um serviço DHCPv6 previamente habilitado em um servidor, o qual irá manter uma tabela atualizada de hosts ativos para fins de controle. Daí o nome **Statefull**, pois guarda o estado dos hosts configurados.



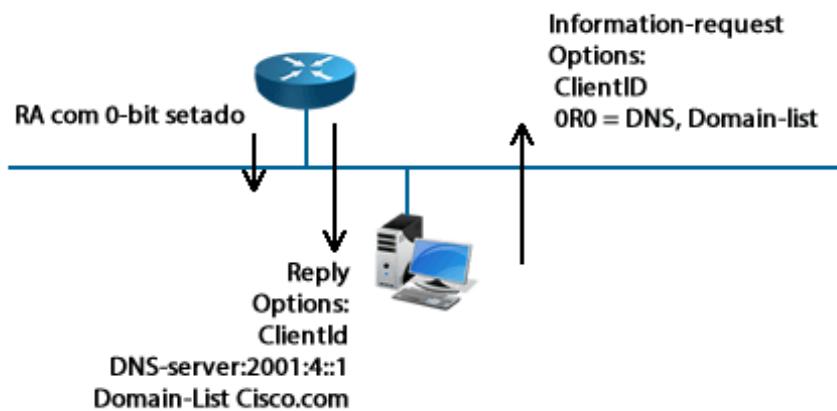
No DHCP stateful o roteador desabilita a autoconfiguração através de flags (indicadores no cabeçalho da mensagem de RA – "M-Flag ON" e "A-Flag OFF" para indicar o DHCPv6 Stateful) e repassa tanto a alocação do endereço IP quanto a configuração dos demais parâmetros de rede para o servidor DHCP. Dessa forma, o servidor consegue manter uma tabela que vincula os endereços de host IPv6 alocados para cada máquina.

Os Flags que são passados na mensagem de RA pelos roteadores aos hosts é que dizem como o host deve se configurar (autoconfig, DHCPv6 Stateful ou Stateless), veja o que eles significam:

- "M" flag ("Managed Address Configuration"): diz ao host que tem um servidor DHCPv6 disponível para alocação de IP e parâmetros de rede.
- "A" flag ("Autonomous Address Configuration"): diz ao host que a autoconfiguração está disponível (SLAAC) para alocação de IPs e parâmetros de rede.
- "O" flag ("Other Stateful Configuration"): diz ao computador que existe um servidor DHCPv6 disponível para que ele possa pegar apenas os parâmetros de rede, mas não para atribuição de endereço.

Além disso, existe uma variação desse serviço de DHCPv6 denominada **Stateless**, na qual servidor não mantém nenhum registro dos endereços atribuídos. Nesse caso a configuração do IP é feita pelo processo de autoconfiguração pelo próprio roteador (vista no tópico anterior) e depois o computador faz uma solicitação ao servidor DHCP requisitando os parâmetros adicionais, tais como nome de domínio e servidores DNS.

Veja a figura abaixo, onde o roteador envia o RA com o "A-Flag" em ON e "O-Flag" também em ON, ou seja, o flag A diz que o computador deve usar a autoconfiguração para pegar seu endereço IP e o flag O diz que ele deve ainda solicitar ao DHCP as demais configurações de rede.



A grande vantagem do DHCPv6 em relação ao DHCPv4 é que não existem mais broadcasts no IPv6 e a descoberta do servidor não inunda mais o switch com **ARP Requests**. Agora a busca é feita através de um endereço **multicast** que identifica todos os servidores DHCPv6 (FF05::1:3 ou FF02::1:2).

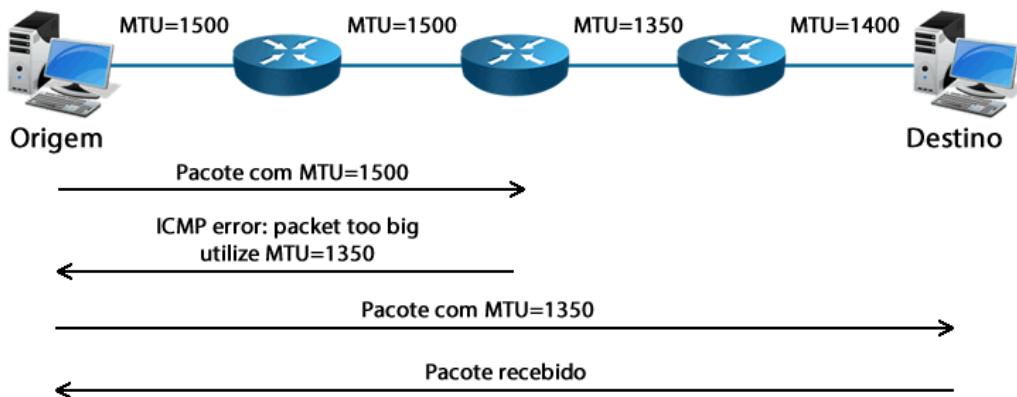
Em ambos os casos, DHCPv6 stateful ou stateless, se o servidor DHCP não estiver na mesma rede local que os clientes é utilizado um DHCP Relay para o encaminhamento das mensagens até o servidor DHCP. Nesse caso a configuração é feita nos roteadores para que eles sirvam de intermediário entre os hosts e o servidor DHCP.

#### 6.4 Fragmentação

O processo de fragmentação de um pacote de dados se inicia utilizando o protocolo **Path MTU Discovery**, o qual tem a função de descobrir de forma dinâmica qual **o tamanho máximo permitido ao pacote**, permitindo identificar previamente os **MTUs** de cada enlace no caminho até o destino.

O MTU é o Maximum Transmission Unity, o qual depende de configurações locais em cada roteador e também do tipo de interface, por exemplo, o MTU do protocolo Ethernet são 1500Bytes.

O Path MTU Discovery assume que o MTU de todo o caminho é igual ao MTU do primeiro salto. Se o tamanho de qualquer um dos pacotes enviados for maior do que o suportado por algum roteador ao longo do caminho, este irá descartá-lo e retornar uma mensagem **ICMPv6 - Packet Too Big** (pacote muito grande). Após o recebimento dessa mensagem, o nó de origem reduzirá o tamanho dos pacotes de acordo com o MTU do caminho indicado na mensagem **packet too big**. O procedimento termina quando o tamanho do pacote for igual ou inferior ao menor MTU do caminho e todos os roteadores deixarem o pacote seguir até seu destino.



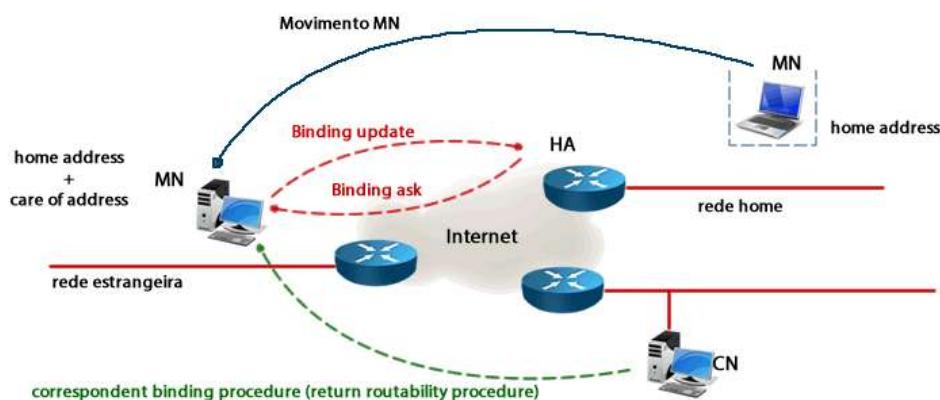
Portanto, o processo de fragmentação do IPv6 é realizado somente na origem, o que reduz a sobrecarga dos roteadores intermediários com cálculos dos cabeçalhos. Essa troca de mensagens pode ser feita várias vezes até que o menor MTU seja descoberto e o pacote alcance seu destino.

Outra diferença entre o IPv4 e o IPv6 é referente ao envio de pacotes de tamanho elevado, chamados **jumbograms**. No IPv6 existe uma opção do cabeçalho de extensão hop-by-hop (chamada jumbo payload), que permite o envio de pacotes com cargas úteis (payload) entre 65.536 e 4.294.967.295 bytes de comprimento, o que no IPv4 existia uma limitação de 64Kbytes.

## 6.5 Mobilidade

O suporte à mobilidade no IPv6 permite que um dispositivo móvel se desloque de uma rede para outra, sem necessidade de alterar seu IP de origem. Quando um dispositivo móvel se desloca da sua rede de origem, ele obtém um novo endereço IPv6 na rede remota. Este endereço remoto pode ser obtido através de mecanismos de autoconfiguração stateless ou statefull.

Para ter certeza de que os pacotes IPv6 chegam a sua rede remota, é necessária a associação entre o endereço remoto (Care-of Address) e o endereço de origem (Home Address). Essa associação é feita pelo **agente de origem**, o qual registra o endereço remoto enviado em uma mensagem **binding update** pelo dispositivo móvel e responde com uma mensagem **binding acknowledgement**.



Para que tudo isso seja possível um novo cabeçalho de extensão foi criado e chamado **Mobility**, além disso, foi adicionado um novo tipo de cabeçalho routing, o Type 2, para dar suporte ao recurso de mobilidade no IPv6. Foram criadas também quatro novas mensagens ICMPv6 para mobilidade:

- Home Agent Address Discovery Request
- Home Agent Address Discovery Reply
- Mobile Prefix Solicitation
- Mobile Prefix Advertisement

## 6.6 QoS – Qualidade de Serviços

O QoS (Qualidade do Serviço) para redes é um conjunto de **padrões e mecanismos** que asseguram o desempenho de alta qualidade para aplicativos críticos. Os administradores de rede podem utilizar mecanismos de QoS para **priorizar** e gerenciar a taxa de envio do tráfego de rede de saída, assim como o atraso do envio desses pacotes. O uso desses mecanismos assegura que os recursos sejam utilizados de forma eficiente para fornecer o nível desejado de serviço.

Foram designados dois campos do cabeçalho IPv6 para o tratamento de QoS: "classe de tráfego" (utilizando valores de DSCP) e "indicador de fluxo", ambos com o objetivo de implementar a priorização do fluxo de determinados pacotes.

No cabeçalho do IPv4, o valor de DSCP (Differentiated services ou DiffServ) é armazenado no campo TOS (Tipo de Serviço). No cabeçalho IPv6, esse valor é armazenado no campo **Classe de Tráfego**. Roteadores que oferecem suporte a DSCP verificam o valor de DSCP e posicionam o pacote a ser enviado em uma fila (priorização). Configurando as filas e valores de DSCP para roteadores em uma rede, é possível alcançar níveis diferenciados de serviço para tráfego marcado com o DSCP correto na rede.

O QoS é importante, tanto em uma rede IPv4 como em uma rede Ipv6, para que determinados tipos de fluxos possam ser devidamente identificados, através da marcação da classe do tráfego, para que eles recebam a prioridade e a largura de banda necessária para seu funcionamento.

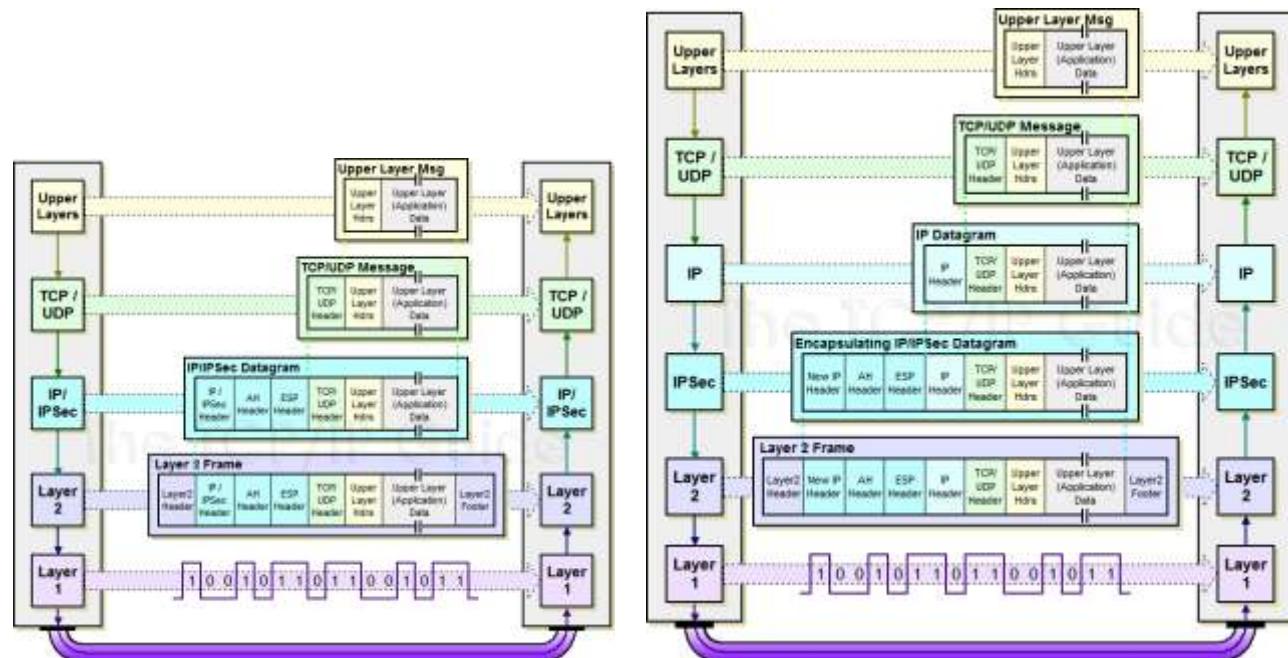
Por exemplo, tráfegos de tempo real como voz e vídeo sobre IP necessitam de um mínimo de atraso e uma quantidade de largura de banda garantida. Com a marcação correta dos fluxos de voz e vídeo, seus pacotes podem receber o tratamento correto pelos roteadores (através das configurações de QoS) e não serão afetados mesmo sendo transmitidos com protocolos mais agressivos como o HTTP, FTP ou programas P2P.

## 6.7 Conceitos de Segurança em Ambiente IPv6

O IPv6 traz a parte de segurança da comunicação já nativa como uma extensão de cabeçalho através do IPSec. Como no IPv6 não há necessidade de se fazer mais o NAT, pois todos os hosts terão IPs válidos de Internet devido ao grande número de endereços, e o IPSec poderá funcionar sem restrições, diferente do que ocorria nas redes IPv4.

O IPSec no IPv6 poderá funcionar, assim como no IPv4, no modo transporte ou túnel. No modo transporte o IPSEC protege somente o payload do pacote IP (informações da camada de transporte e aplicação). Já no modo túnel o IPSEC protege todo o conteúdo do pacote IPv6, inclusive seu cabeçalho, pois todo o pacote IPv6 antes de sair para a rede é criptografado e inserido dentro de outro pacote IPv6, por isso o nome de túnel.

Veja a figura a seguir com o IPSec em modo transporte (esquerda) e compare com o IPSec em modo túnel (figura da direita).



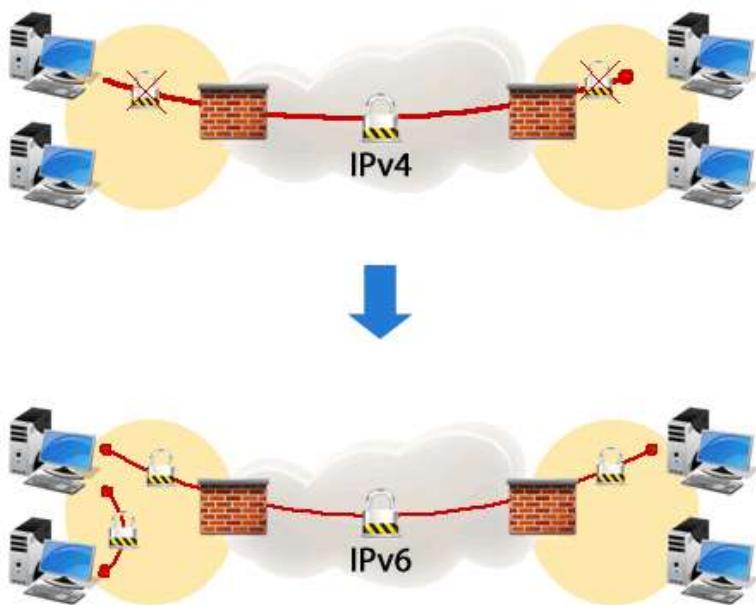
Fonte das figuras:

[http://www.tcpipguide.com/free/t\\_IPSecModesTransportandTunnel-3.htm#Figure\\_120](http://www.tcpipguide.com/free/t_IPSecModesTransportandTunnel-3.htm#Figure_120)

[http://www.tcpipguide.com/free/t\\_IPSecModesTransportandTunnel-3.htm#Figure\\_119](http://www.tcpipguide.com/free/t_IPSecModesTransportandTunnel-3.htm#Figure_119)

e

Outra diferença é que com o IPv6 o suporte ao IPSec será obrigatório em todos os endpoints, o que no IPv4 é um opcional. Portanto, em uma rede IPv6 será possível proteger tanto a comunicação interna (Intranet) como através da Internet.



Apesar disso tudo, o IPSec que vimos no capítulo anterior sobre segurança é o mesmo padrão para ambas as versões do protocolo IP (IPv4 e IPv6).

Além disso, devido ao grande número de endereços IPv6, a varredura por endereços IP (scanning) torna-se naturalmente mais complexa. Vamos fazer uma suposição que um Hacker queira varrer uma rede que tem um prefixo /64, portanto temos aqui  $2^{64}$  hosts que dão 18.446.744.073.709.551.616 de hosts. Agora, vamos também supor que o computador do Hacker possui a capacidade de varrer 1 milhão de IPs por segundo, se você dividir o número de hosts por um milhão e depois converter os segundos em anos o Hacker **levaria mais de 500 mil anos para varrer toda a subrede!**

Porém, devido às técnicas de transição (túneis e pilha dupla), a mudança do ICMPv6 com a entrada de novos recursos, autoconfiguração e demais facilidades novas inerentes ao IPv6, novas ameaças deverão surgir ao longo do uso e da disseminação do protocolo. No entanto, as medidas aplicadas de segurança às camadas superiores continuam as mesmas, pois acima da camada de Internet nada mudou, assim como abaixo na camada de acesso aos meios. Os recursos tradicionais de segurança como os Firewalls, IPSs, IDSs, anti-vírus e demais deverão ser atualizados e aos poucos serão adaptados à nova realidade com a entrada em massa do protocolo IPv6 na Internet.

## 6.8 Roteamento IPv6

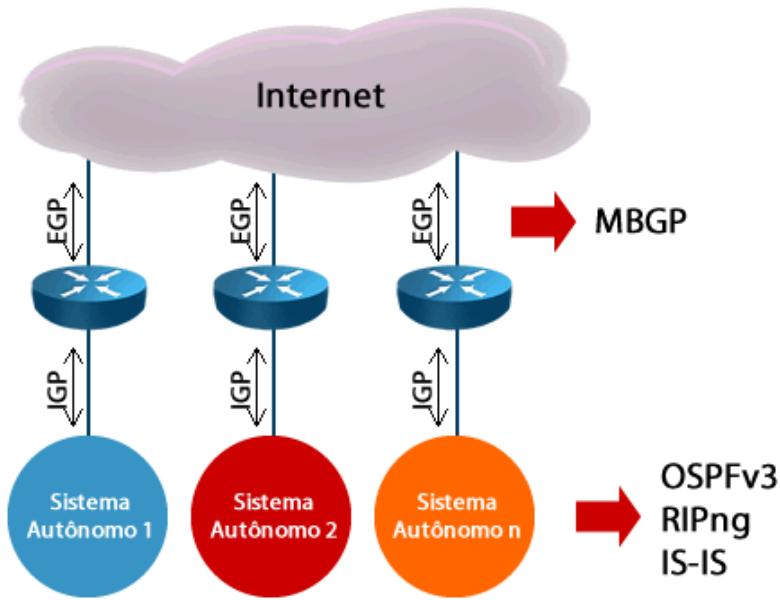
Os protocolos de roteamento para o IPv6 continuam tendo a mesma base dos utilizados para o IPv4, porém recebem novos nomes. Os principais protocolos de roteamento interno para IPv6 (IGP) são:

- **RIPng** (baseado no RIP versão 2 do IPv4)
- **OSPFv3** (baseado no OSPFv2 do IPv4)
- **IS-IS** (não teve alteração de versão, apenas inserções de campos para tratativa do endereçamento IPv6)

Além dos protocolos IGP acima, ainda existe um protocolo proprietário do fabricante Cisco chamado EIGRP que tem também sua versão para IPv6 chamado EIGRPv6.

Todos eles têm seu princípio de funcionamento, cálculo de melhor rota (métrica) e formas de trocar informações (updates) mantidas da mesma maneira que no IPv4, porém tudo agora baseado no endereçamento IPv6.

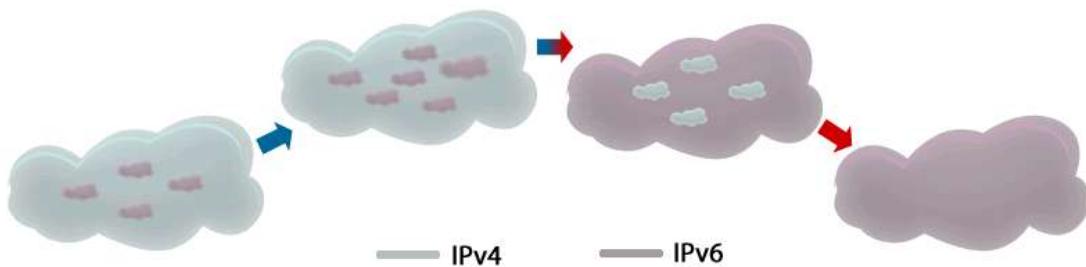
Já para o roteamento externo (EGP) o BGP continua sendo utilizado, porém com uma extensão multiprotocolo (MBGP – BGP Multiprotocolo ou Multiprotocol Border Gateway Protocol), a qual possui as mesmas funcionalidades do BGP para IPv4, porém com capacidade de tratar endereços tanto do IP versão 4 como da versão 6.



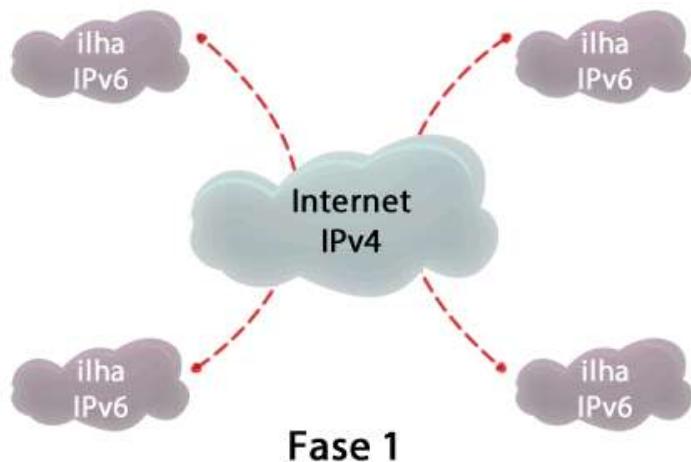
## 7 Técnicas de Convivência e Transição entre o IPv4 e IPv6

Atualmente tanto as redes corporativas como a Internet estão implementadas encima do protocolo IPv4, portanto não será possível apenas “virar a chave” e transformar tudo em IPv6 “da noite para o dia”. Daí surgem os termos **convivência** ou **coexistência** dos protocolos IPv4 e IPv6, assim como o termo “**transição**” ou “**migração**”.

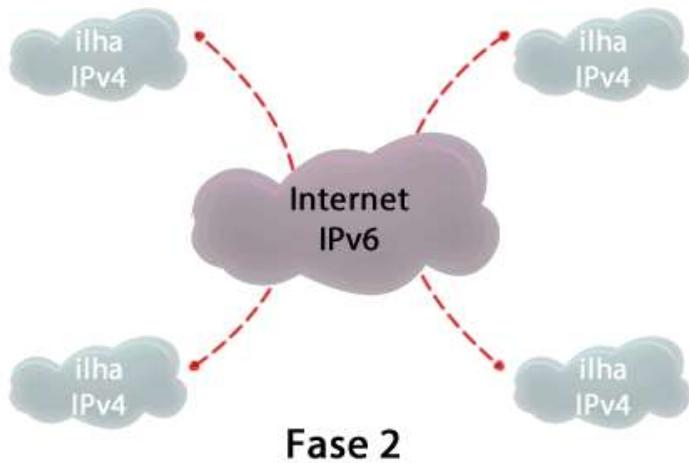
Veja a figura abaixo representando a migração gradual do IPv4 para o IPv6, note que em um primeiro momento teremos uma predominância do IPv4, que aos poucos será invertida para uma predominância do IPv6, até chegar o momento que a rede será toda Ipv6.



Portanto, a coexistência (ou convivência) é o termo utilizado para técnicas que possibilitam a configuração de ambos os protocolos na rede (seja nos hosts como nos dispositivos de rede). Já a transição é o termo utilizado para quando a rede interna for sendo migrada para IPv6 e precisar ainda se comunicar através de uma rede IPv4 com outras redes IPv6 remotas, pois ao longo do tempo teremos “ilhas IPv6” isoladas em meio a uma rede IPv4 (Internet) e precisaremos cruzar a rede IPv4 para fazer a comunicação entre essas ilhas de IPv6 ou então traduzir do IPv6 para IPv4 (e vice-versa) para permitir a comunicação entre hosts que ainda não foram migrados. Veja a figura abaixo onde em uma primeira fase teremos as ilhas IPv6 querendo se comunicar através da Internet predominantemente IPv4.



Já na figura a seguir temos uma segunda fase onde as Intranets e Internet estarão já em fase avançada de migração para o IPv6 e há uma inversão, onde teremos algumas ilhas IPv4 querendo se comunicar em uma nuvem IPv6, até chegar ao ponto que a rede vai estar toda IPv6 em uma terceira fase.



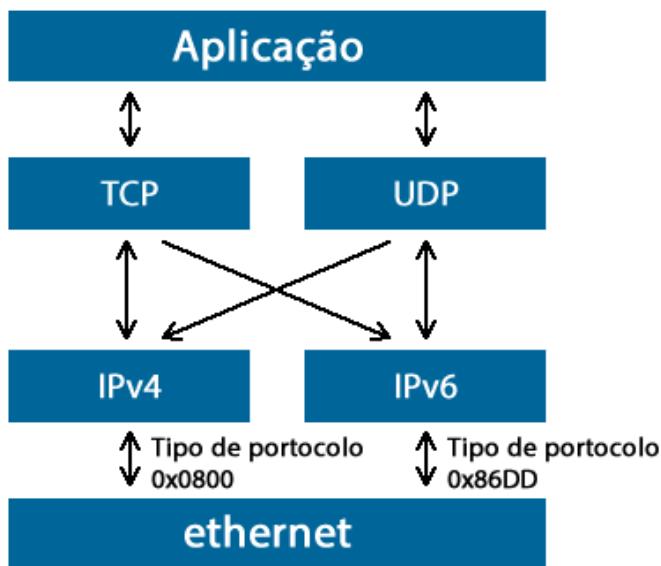
Para que isso seja possível podemos classificar os recursos de coexistência e transição em três categorias:

- **Pilha Dupla ou Dual Stack:** suportar os dois protocolos na mesma rede.
- **Tunelamento:** passar o tráfego IPv6 encapsulado em um pacote IPv4.
- **Tradução:** traduzir endereços IPv6 para IPv4 e vice-versa possibilitando que hosts em diferentes versões do protocolo IP se comuniquem e também que hosts IPv6 possam acessar recursos da rede IPv4 na fase de transição.

Vamos agora analisar cada uma das tecnologias citadas acima.

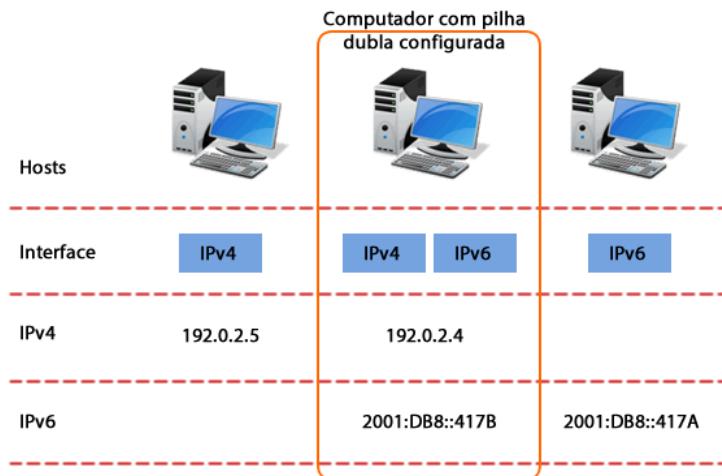
## 7.1 Pilha Dupla

A pilha dupla, como o próprio nome diz, é ter ambos os protocolos IPv4 e IPv6 configurados tanto nas interfaces dos dispositivos de rede como nos hosts, ou seja, em todos os nós e endpoints da rede.



Dessa maneira, quando o host for se comunicar com outros hosts IPv4 ele utiliza a pilha do protocolo IP versão 4, porém quando for conversar com um host ou servidor IPv6 utilizará a pilha referente ao protocolo IP versão 6. Note que nessa técnica não há nenhum tipo de tradução ou interconexão entre os protocolos, ou seja, os fluxos IPv4 e IPv6 são separados e o computador usa um ou outro. Note também que não há comunicação entre o protocolo IPv6 e IPv4, ou seja, a camada de transporte escolhe enviar seu fluxo por um ou por outro.

Portanto, em uma rede poderemos encontrar dispositivos somente Ipv4, com pilha dupla ou somente IPv6, sendo que o único que irá conseguir falar com dispositivos remotos tanto com IPv4 e IPv6 será o que possui a pilha dupla configurada. Veja a próxima figura mostrando na prática que um host com pilha dupla possui um endereço IPv4 e um IPv6 configurado na mesma interface de rede.



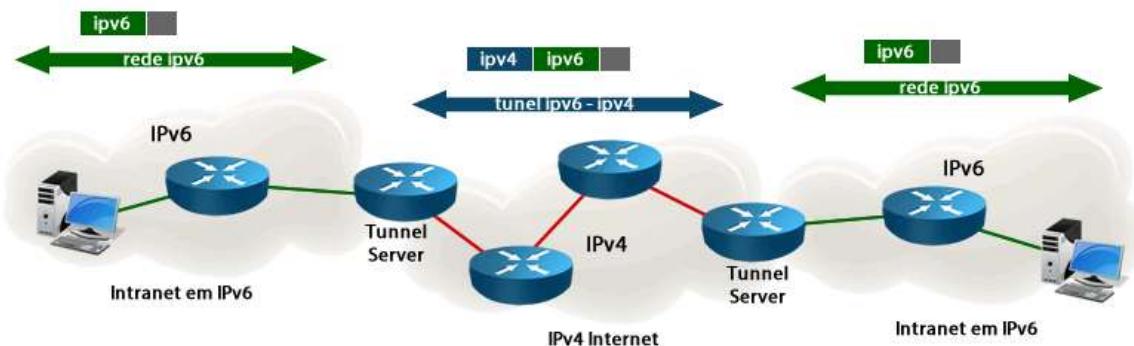
Na implementação de uma pilha dupla é importante lembrar que as configurações dos recursos de rede para o IPv4 e IPv6 serão independentes em diversos aspectos, seguem alguns pontos importantes a serem considerados abaixo:

- Informações nos servidores DNS autoritativos, pois as entradas para os servidores IPv6 no DNS possuem necessidades de configuração específica;
- Protocolos de roteamento, pois os roteadores deverão ser configurados para rotear as redes IPv6, isto não é automático;
- Firewalls, pois agora serão necessárias regras de filtragem baseadas também no fluxo IPv6, sendo que o mesmo vale para os IPSs e IDSs;
- Gerenciamento das redes, pois o uso do SNMP exige que os gerenciadores e as MIBs tenham suporte ao IPv6 e provavelmente configurações específicas serão necessárias.

## 7.2 Tunelamento

Os túneis tem aplicação para que um fluxo de informações IPv6 consiga chegar ao seu destino através de uma rede IPv4 e vice-versa. Nesse caso temos dois hosts IPv6, por exemplo, querendo se comunicar através de uma rede corporativa ou pela Internet, porém essa rede não tem suporte completo ao IPv6 e por isso não será possível enviar os pacotes diretamente entre os hosts de origem e destino.

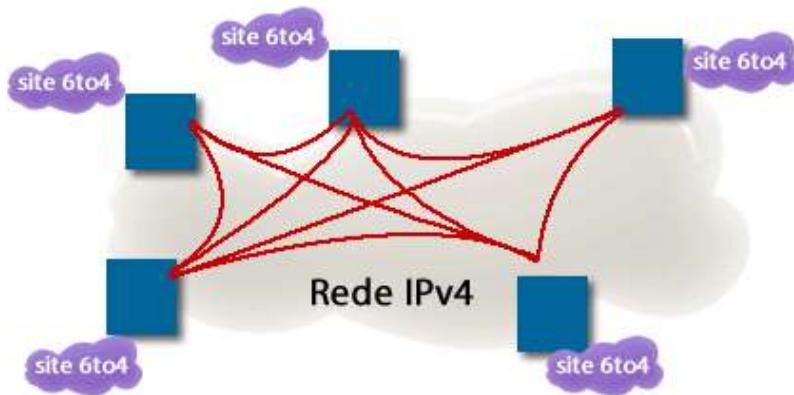
Os túneis criam caminhos, como se fossem tubos, encapsulando o pacote IPv6 dentro de um pacote IPv4. Veja a figura a seguir, onde usamos como exemplo duas redes IPv6 que desejam se comunicar utilizando a Internet IPv4. Nesse caso os pacotes enviados pela origem ao sair pelo roteador que está conectado à Internet são encapsulados, ou seja, inseridos dentro de um pacote IPv4 e ao chegar do outro lado o cabeçalho do IPv4 é retirado e o destino recebe um pacote IPv6.



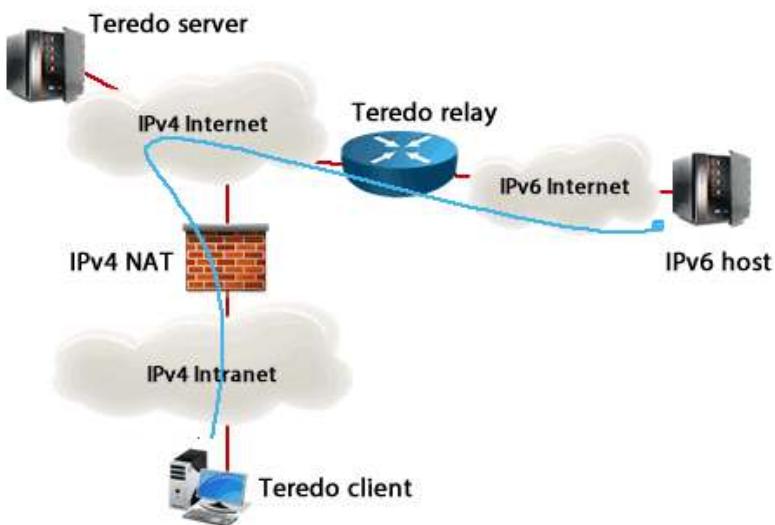
Os túneis podem ser fechados diretamente entre dois hosts, entre dois roteadores ou entre host/roteador ou roteador/host. Os túneis entre dois roteadores são normalmente chamados **"site-to-site"** e permitem a comunicação de vários dispositivos através do túnel.

Os principais tipos de túneis utilizados são:

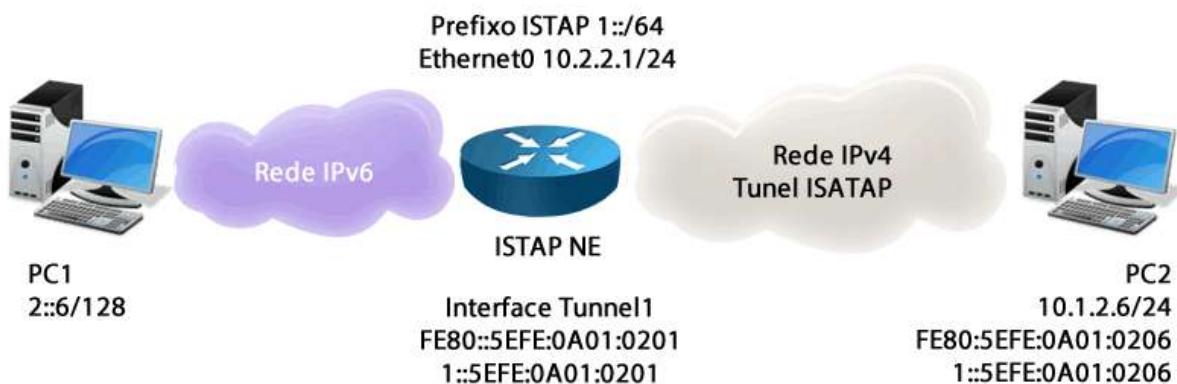
- **Tunnel Broker:** Este tipo de túnel é fornecido por provedores de serviço e permitem que dispositivos isolados ou toda uma rede IPv4 obtenham conectividade IPv6 por meio do estabelecimento de um túnel com um provedor.
- **6to4:** Este túnel, descrito na RFC 3056, permite que redes IPv6 isoladas comuniquem-se entre si através da rede IPv4 no modo ponto. Existe também o modo conhecido como multiponto, o qual é chamado de túnel automático ou 6to4. O 6to4 é uma das técnicas de transição mais antigas em uso e é a técnica que inspirou a criação do 6rd.



- **Teredo:** Trata-se de uma técnica de tunelamento automática criada pela Microsoft e definida na RFC 4380. O Teredo permite que hosts que utilizam Network Address Translations (NAT) obtenham conectividade IPv6 utilizando tunelamento em IPv4, usando o protocolo UDP. Sua utilização não é recomendada, por questões de eficiência e segurança.



- **ISATAP:** O “Intra-Site Automatic Tunnel Addressing Protocol” é um tipo de tunelamento que conecta um dispositivo ao roteador (host-roteador). Sua utilização normalmente ocorre dentro das redes corporativas (Intranets), pois não há serviço público de ISATAP. A utilização do ISATAP é quando o backbone do provedor de serviços já está em IPv6, mas sua infraestrutura interna ou parte dela ainda está em IPv4.



- **GRE:** O “Generic Routing Encapsulation” (RFC 2784) é um túnel estático para o transporte de pacotes IPv6 em redes IPv4. Este túnel foi desenvolvido pela Cisco com a finalidade de encapsular vários tipos diferentes de protocolos, permitindo uma flexibilidade maior em termos de roteamento. Basicamente são utilizados para criar túneis roteador a roteador e o mais interessante do GRE é que ele não depende da infraestrutura da Internet para funcionar.

### 7.3 Técnicas de Tradução

As técnicas de tradução permitem que equipamentos usando IPv6 comuniquem-se com outros configurados com endereço IPv4 por meio da **conversão ou tradução dos pacotes** de uma versão para outra, filosofia muito parecida com o que estudamos para o NAT (Network Address Translation) do IPv4.

Um ponto que deve ser ressaltado é que tanto túneis quanto as técnicas de tradução podem ser implementadas de maneira stateful ou stateless. Como já vimos no DHCPv6, as técnicas stateful necessitam da manutenção de **tabelas de estado** contendo informações sobre os endereços ou pacotes para processá-los. Já nas técnicas stateless não é necessário guardar informações, pois os pacotes são tratados de forma independente. Analisando os dois tipos de técnicas podemos concluir que as stateful são mais caras, pois gastam mais processamento e memória das máquinas responsáveis por manter as tabelas de estado atualizadas. Por esse motivo encontramos em diversas bibliografias sobre o IPv6 recomendações para dar preferência a técnicas stateless, pois elas são mais baratas e escaláveis que as técnicas stateful.

As principais técnicas de tradução utilizadas são:

- **Stateless IP/ICMP Translation (SIIT):** É um mecanismo de tradução stateless de cabeçalhos IP/ICMP, permitindo a comunicação entre hosts com suporte apenas ao IPv6 apenas com IPv4.
- **NAT-PT (NAT - Protocol Translation) e NAPT-PT (Network Address and Port Translation – Protocol Translation):** Faz o mapeamento entre endereços IPv6 e IPv4, tem o funcionamento semelhante ao NAT do IPv4, pois quando um pacote com IPv6 quer atravessar a rede ele faz a tradução do protocolo IPv6 para um cabeçalho do IPv4 e mantém um mapeamento entre o IPv6 interno e o endereço IPv4 utilizado na rede externa para fazer a tradução. O NAPT-PT permite utilizar também as portas TCP e UDP para a tradução dos endereços, estendendo a capacidade de tradução do NAT-PT, muito similar ao PAT do IPV4.

- **Application Gateway (ALG):** São gateways de aplicação, trabalham como um proxy HTTP, onde o cliente primeiramente inicia a conexão com o ALG, e a partir desse momento o ALG estabelece uma conexão com o host remoto ou servidor, retransmitindo as requisições de saída e os dados de entrada.
- **Transport Relay Translator (TRT):** Tem apenas a função de um tradutor de camada de transporte, ou seja, esse mecanismo possibilita a comunicação entre hosts apenas IPv6 e hosts apenas IPv4 através de tráfego TCP ou UDP.

## 8 Próximos Passos Rumo a Transição para o IPv6

Lembrem-se que na data de 6 de junho de 2012, a Internet Society promoveu o **IPv6 World Launch**, o dia em que grandes provedores de Internet (ISPs), fabricantes de equipamentos de rede e empresas da Web ao redor do mundo habilitaram permanentemente o IPv6 em seus produtos e serviços. Portanto, a partir dessa data o IPv6 vem sendo implantado oficialmente, mesmo que de maneira gradativa, na Internet e deve funcionar em conjunto com o IPv4 por um longo período.

Apesar de não termos precisão desse período de transição entre as versões de IP, o futuro do IPv4 está com os dias contados. Por isso, as grandes empresas e provedores de Internet estão se movimentando em direção ao IPv6, pois além de tudo o espaço reservado de endereços IPv4 também está com seus dias contados!

Portanto aproveite a onda do IPv6 e navegue nesse novo ambiente, pois em breve podemos todos ser convocados para migrar nossos sistemas corporativos ou até mesmo residenciais.

*No capítulo final do curso de redes de computadores da DlteC vamos fazer o projeto (dimensionamento) de um escritório, definindo desde os equipamentos de rede até a estrutura física a ser utilizada.*

*Esperamos com esse capítulo que você consiga conectar os conteúdos aprendidos com a vida prática!*

*Aproveitem e bons estudos!*

## **Capítulo 12 - Estudo de Caso - Projeto e Implementação de Rede**

### **Objetivos do Capítulo**

O objetivo desse capítulo é a prática dos conceitos aprendidos aplicando em um projeto proposto. Lembre-se que algumas especificações necessitam de análise de catálogos de equipamentos ou um conhecimento maior sobre linhas de produtos, portanto faremos algumas simplificações para que o assunto não se compleique demais.

Bons Estudos!

## Sumário do Capítulo

<b>1 Requisitos do Projeto</b>	<b>398</b>
<b>2 Planejamento das Atividades</b>	<b>400</b>
<b>3 Topologia Lógica e Definição dos Dispositivos de Rede</b>	<b>401</b>
3.1 Esboço da Topologia Lógica e Definição das VLANs	402
3.2 Definindo as redes IP	403
<b>4 Topologia Física e Dimensionamento do Cabeamento Estruturado</b>	<b>406</b>
4.1 Definição do posicionamento do AP	406
4.2 Definição do rack e seu posicionamento	407
4.3 Dimensionamento dos Cabos	410
4.3.1 Recepção	411
4.3.2 Sala de Reunião	412
4.3.3 Escritório Sala 2	412
4.3.4 Escritório Sala 1	413
4.3.5 Sala da Diretoria	413
4.3.6 Access Point	414
4.3.7 Saída dos Cabos na Sala de Telecom/Equipamentos e Totalização	414
4.4 Acessórios para o Cabeamento	415
<b>5 Documentação do Projeto</b>	<b>419</b>
<b>6 Qual Caminho Seguir Após esse Curso?</b>	<b>419</b>

## 1 Requisitos do Projeto

A empresa **Golden Gratesf S/A**, uma multinacional Americana está montando um escritório na cidade de São Paulo e contratou sua empresa para fazer o projeto lógico e físico relativo à infraestrutura de cabeamento, equipamentos de rede e demais dispositivos e acessórios afins. O objetivo do projeto físico é dar uma estimativa quantitativa de materiais.

O escritório será composto por 25 posições, uma recepção mais uma sala de reuniões, onde em cada mesa deve haver um ponto de rede que permita conexão física 10/100/1000 Mbps e também a cobertura de sinal wireless no padrão 802.11 b/g/n, incluindo um ponto na recepção e outro para a sala de reuniões. O escritório contará ainda com duas impressoras de rede, uma mais simples que será posicionada na recepção e outra de maior porte para o escritório. É importante que o projeto comporte crescimento de 15% do total de pontos instalados.

A Intranet corporativa deve ser acessível apenas via rede cabeada, enquanto a rede sem fio deve permitir somente acesso à Internet para visitantes e dispositivos móveis, como tablets e smartphones dos funcionários e visitantes.

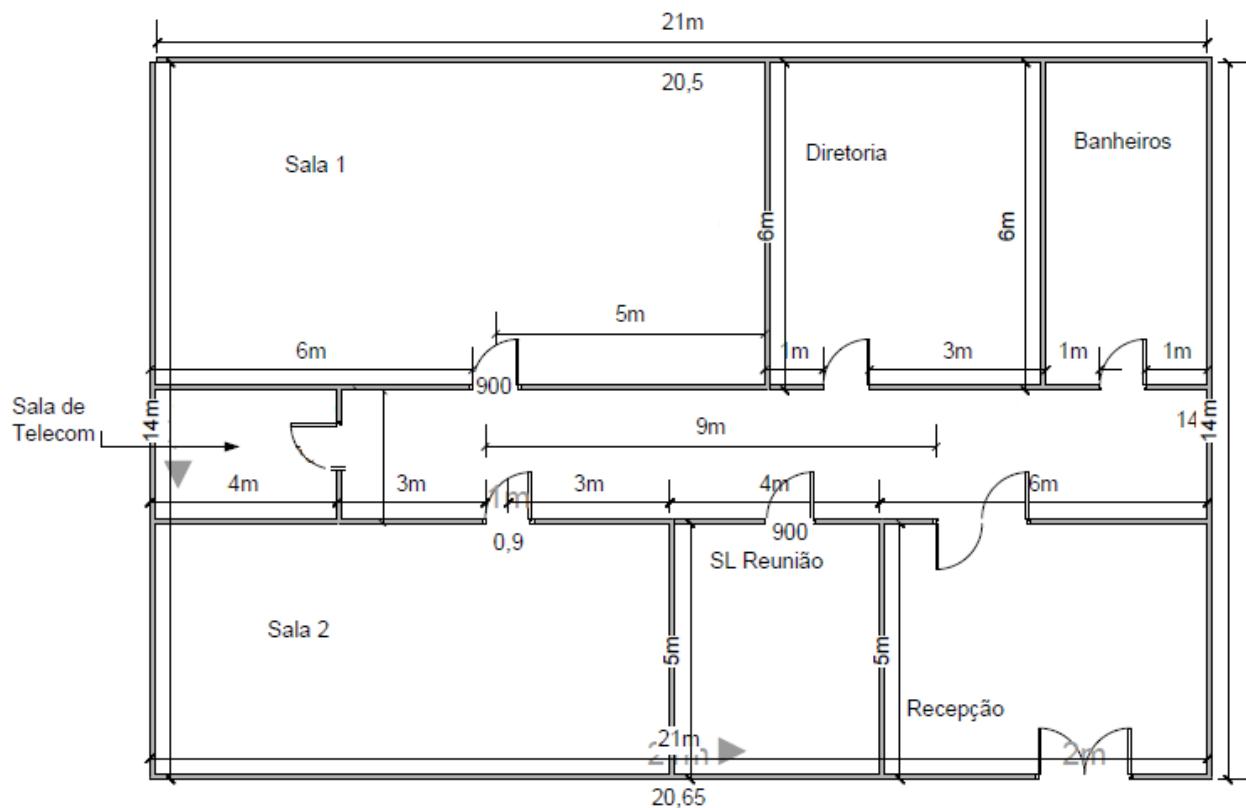
A empresa já possui dois servidores locais que ocupam duas unidades de rack (2Us) cada um, um no-break que ocupa quatro unidades de rack (4Us) e um PABX-IP que ocupa duas unidades de rack (2Us). O AP precisa ficar posicionado fora do rack e deve ser alimentado via PoE, para evitar necessidade de mais ponto de elétrica. A empresa não utilizará telefones convencionais, somente softphones instalados nos computadores. Precisa haver um ponto para linha de fax que será conectada à impressora multifuncional da recepção.

Já foi contratado um link de Internet dedicado de 10 Mbps (para acesso à VPN IPSec corporativa que irá conectar a rede do Brasil aos EUA e saída de Internet) e um circuito E1 para conexão com o PABX-IP. O link de Internet será entregue via conversor óptico pela operadora da Telecom e o E1 através de um modem E1 óptico (ambos de bandeja ocupando no máximo 2Us), todos os equipamentos alimentados com tensão de 127V.

A faixa de IPs liberada para o Brasil foi a rede 10.20.128.0 /22 e por questões de segurança deve haver separação por VLANs com a primeira agrupando os pontos de rede das mesas, a segunda VLAN para a recepção e sala de reuniões, a terceira VLAN para a rede sem fio e a quarta VLAN para os servidores. Com isso podem ser implementadas regras de acesso entre as redes, pois a rede sem fio não pode acessar a rede Interna.

Outro dado importante, toda parte da infraestrutura elétrica já está pronta.

Juntamente com os requisitos acima foi passada a planta baixa do escritório para ajudar no dimensionamento do cabeamento, conforme figura mostrada abaixo. Você pode baixar na área do aluno o arquivo em PDF (**Cap12 – Planta Baixa**), o qual utiliza a escala de 1cm=1m para facilitar o levantamento do cabeamento necessário.



Para finalizar, o contratante informou que os cabos podem ser passados pelo teto da edificação e aí baixados por dutos ou canaletas que descerão pela parede e serão distribuídas para os computadores, impressoras e demais equipamentos dos usuários. As paredes da edificação têm aproximadamente 3 metros de altura (pé direito). Não há definição de layout de mesas, por isso a estimativa deve ser feita com uma média de distância ou pelo pior caso.

## 2 Planejamento das Atividades

O próximo passo é analisar os requisitos e pensar sobre os seguintes aspectos (*sugerimos que você tenha um caderno ou uma folha à mão e anote suas respostas para atender os requisitos do projeto*):

1. Quais os dispositivos de redes necessários para a conectividade do escritório conforme requisitos? Vamos utilizar um roteador? Quantos pontos de rede serão necessários e quantos switches vamos precisar? Que tipo de switch (porta, funcionalidades, etc.)?
2. Qual a melhor posição para o AP? E o tipo de antena a ser utilizada? Vamos utilizar que padrão de criptografia? Será que a empresa tem autenticação?
3. Como vamos dividir o endereçamento IP a ser utilizado? Precisamos de quantos IPs fixos? E as faixas de IP a serem utilizadas no DHCP para cada VLAN?
4. Como vai ser a topologia lógica da rede com as conexões e endereçamento dos dispositivos de rede? Será que uma topologia em três camadas se aplica a esse projeto?
5. Sobre a topologia física, temos que pensar sobre:
  - a. Tipo de cabeamento a ser utilizado?
  - b. Quais acessórios serão necessários para infraestrutura (canaletas, piso elevado, patch panel, cabos, patch Cord, tomadas de Telecom, rack, conectores, etc.)? E como estimar as quantidades aproximadas?
  - c. Qual o tipo e a disposição dos dispositivos no rack? Será que um rack será suficiente? O rack deve ser aberto ou fechado?
  - d. Nesse momento do projeto já vamos definir o encaminhamento e nomenclatura dos cabos de rede?
6. Depois de analisar os requisitos e as questões acima será que as informações que o cliente passou são suficientes para montar o projeto?
7. Você consegue pensar em algum outro ponto importante a ser considerado que não foi citado? Anote e sinta-se à vontade para compartilhar com os demais alunos e tutores no fórum desse capítulo na área do aluno.

Portanto, o momento do planejamento do projeto é um dos mais importantes, pois esse passo acaba evitando retrabalhos futuros. Nesse ponto é onde devemos tirar todas as dúvidas com quem está requisitando o serviço para atender às expectativas explícitas e verificar se não existe nada implícito, ou seja, que não esteja claro para que o projeto saia conforme as requisições.

Nos próximos capítulos vamos abordar o projeto utilizando uma metodologia do mais macro para o micro, ou seja, vamos iniciar pela topologia lógica, definição de equipamentos de rede para depois ir para topologia física, cabeamento e seus acessórios.

### 3 Topologia Lógica e Definição dos Dispositivos de Rede

Antes de definir a topologia lógica vamos analisar os requisitos e definir os equipamentos que serão necessários para depois definir como interligá-los.

Iniciando pela necessidade de switch e AP temos os seguintes dados:

1. O escritório será composto por 25 posições, uma recepção mais uma sala de reuniões, onde em cada mesa deve haver um ponto de rede que permita conexão física 10/100/1000 Mbps e também a cobertura de sinal wireless no padrão 802.11 b/g/n, incluindo um ponto na recepção e outro para a sala de reuniões.
2. O escritório contará ainda com duas impressoras de rede, uma mais simples que será posicionada na recepção e outra de maior porte para o escritório.
3. É importante que o projeto comporte crescimento de 15% do total de pontos instalados.
4. Temos um roteador com Internet e deve sair pelo menos um ponto para LAN.
5. Um PABX IP que também precisará de um ponto de rede.

Portanto precisamos, em termos de portas de switch, um total de:

- 29 pontos (25 mesas+1 recepção+1 sala de reunião+2 impressoras)
- 3 pontos para os dispositivos de redes (1 roteador de Internet+1 AP+1 PABX-IP)
- Crescimento de 15% →  $(31 * 15\%) = 4,65 \rightarrow 5$  pontos de rede
- Total de portas de switch: 37 pontos de rede
- Nesse caso temos a opção de um switch de 48 portas ou dois de 24 portas
- Vamos optar por dois de 24 portas, pois se um "queimar" não irá parar todo o escritório
- Como teremos telefones IP com PoE não podemos de esquecer na escolha do modelo do switch um que conte com essa facilidade, além do suporte à criação de VLANs e trunks 802.1Q para conexão com o roteador
- Nesse caso não precisam ser layer 3, pois o escritório é pequeno e precisaremos do roteador
- As portas do switch devem ser 10/100/1000 Mbps

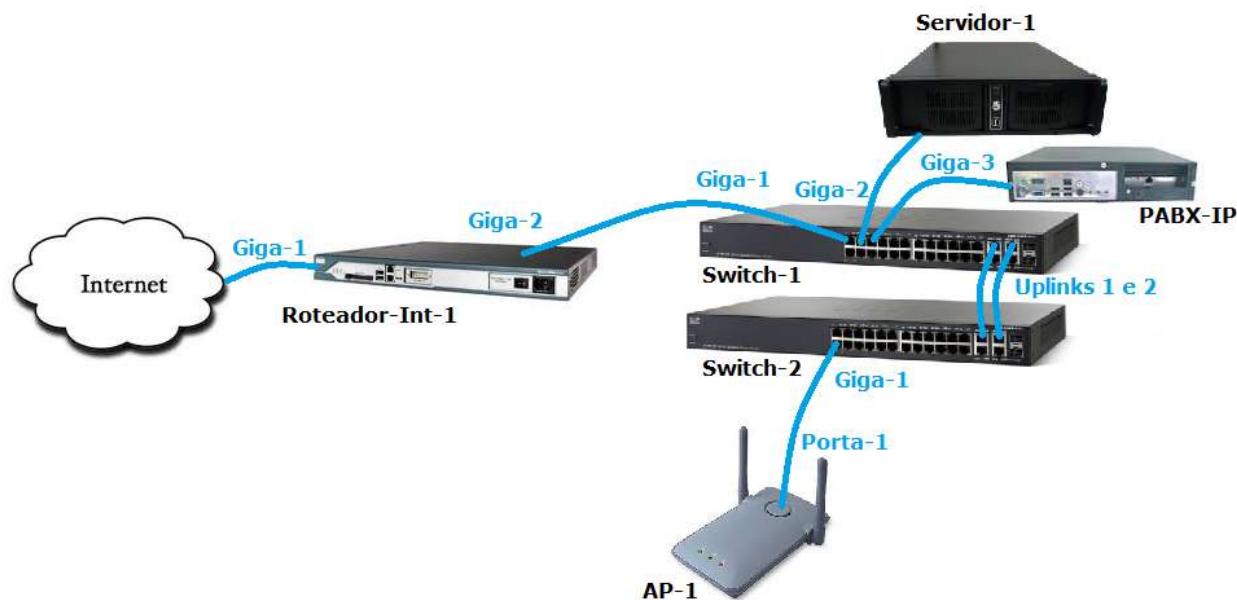
A especificação para o modelo do AP já foi dado pelo próprio cliente, deve suportar 802.11 b/g/n e é aconselhável um AP ou roteador sem fio com antena omnidirecional de potência maior que a convencional.

O roteador deve ter no mínimo duas portas para conexão via 10/100 Mbps ou 10/100/1000 Mbps. Como a Internet será limitada a 10Mbps pode ser uma porta 10/100 Mbps, porém como a LAN será a Giga o melhor é que o roteador suporte 10/100/1000 Mbps. Como temos uma conexão com a Internet e IP fixo o roteador deverá suportar a configuração de firewall ou então teremos que especificar um firewall para conectar entre a LAN e o roteador. Para esse tipo de topologia existem modelos de firewalls que podem atuar também como roteador, fazendo inclusive o roteamento entre VLANs e com suporte a trunks 802.1Q, como por exemplo, o ASA da Cisco e o Netscreen da Juniper. Além disso, os roteadores multisserviço suportam a configuração de firewall e IPS, por exemplo, tudo é uma questão de custo e como o cliente deseja sua infraestrutura. Em nosso projeto, vamos escolher um roteador que já faz a parte de firewall e VPN integradas nele.

### 3.1 Esboço da Topologia Lógica e Definição das VLANs

Para montar a topologia lógica e fazer o desenho para inserir na documentação o software mais utilizado é o **Visio** da Microsoft, porém existem versões gratuitas em software livre como o **Kivio** e o **OpenOffice Draw** que você pode utilizar para fazer os diagramas de rede.

Veja na figura a seguir o primeiro esboço do diagrama lógico da rede com os principais dispositivos e suas conexões, onde posicionamos os equipamentos e já definimos as portas dos switches e do roteador onde ficará conectado cada equipamento, podendo assim definir na sequência a alocação de portas para os hosts.



Como nos requisitos foi solicitada a separação por VLANs da parte de servidor, AP, Sala de reunião/recepção e escritório já podemos fechar a definição de portas por VLAN:

- **VLAN 10** – nome **Servidores**: Switch-1 portas 2 a 5 (temos o servidor e o PABX-IP mais três portas para expansão).
- **VLAN 20** – nome **APs**: portas 1 e 2 do Switch-2 (deixada uma porta a mais para expansão).
- **VLAN 30** – nome **Escrítório**: Portas 6 a 23 (18 portas) no Switch-1 e de 3 a 14 (12 portas) no Switch-2 (total de 30 para o escritório mais uma Impressora, portanto tem quatro portas a mais como reserva e crescimento).
- **VLAN 40** – nome **Recep-Reun**: Portas de 15 a 20 no Switch-2 (total de 6 portas ficando 3 reservas ou expansão, pois temos dois pontos na recepção – micro+impressora – e um ponto na sala de reunião).
- Ficaram ainda as portas de 21 a 24 no Switch-2 sem alocação para manobra e reserva. A porta 24 do Switch-1 também ficou vaga como reserva ou expansão.
- A porta 1 do Switch-1, assim como as portas de Uplink 1 e 2 em ambos switches devem ser configuradas como trunk e ter o protocolo 802.1Q e STP habilitados.

Apesar de parecer meio estranho, na topologia lógica estarmos definindo que portas dos switches vamos utilizar, pois parece muito mais físico que lógico, lembrem-se que para a definição das VLANs precisamos desse dado, pois as VLANs são centradas em portas e por isso já definimos nesse passo a alocação de portas por VLAN.

		Switch-1	Switch-2	Roteador-Int-1
Dispositivos de Rede	<b>Servidor-1</b>	Porta-2		
	<b>PABX-IP</b>	Porta-3		
	<b>AP-1</b>		Porta-1 - Trunk	
	<b>Internet</b>			Porta-1
	<b>Impressora Escritório</b>		Porta-3	
	<b>Impressora Recepção</b>		Porta-15	
	<b>Switch-1</b>		Uplink-1 e 2 - Trunk	Porta-2 Trunk
	<b>Switch-2</b>	Uplink-1 e 2 - Trunk		
VLANS e Portas Vagas	<b>VLAN 10</b>	Portas 2 a 5		
	<b>VLAN 20</b>		Portas 1 e 2	
	<b>VLAN 30</b>	Portas 6 a 23	Portas 3 a 14	
	<b>VLAN 40</b>		Portas 15 a 20	
	<b>Portas vagas</b>	Porta 24	Portas 21 a 24	

### 3.2 Definindo as redes IP

Como o IP de Internet será fornecido pelo prestador de serviços de Telecom, essa definição só poderá ser realizada após o serviço contratado e entregue os dados, portanto sobre o IP da porta 1 do roteador não precisaremos definir.

Nos requisitos a empresa solicitou uma VLAN para cada rede, porém não citou a VLAN de gerenciamento, a qual tem o IP de gerenciamento dos switches e do próprio AP, portanto além das quatro VLANs solicitadas temos que definir uma quinta para fins de gerenciamento.

Agora que já sabemos a quantidade de VLANs que teremos, ou seja, a quantidade de domínios de broadcast ou subredes que necessitaremos e vamos definir a alocação dos endereços IP com base no que a empresa definiu partindo da subrede 10.20.128.0 /22.

Uma subrede /22 permite um total de  $2^{10-2}$  endereços IP, ou seja, temos 1022 endereços IP se não fizermos a divisão em subredes. Voltando ao enunciado original e analisando a tabela de alocação de portas que foi feita no passo anterior essa faixa atende os requisitos e tem uma boa margem de sobra. Esta subrede tem as seguintes características:

- Subrede 10.20.128.0 máscara /22 ou 255.255.254.0
- Máscara em binário 11111111.11111111.11111100.00000000 e estas subredes variam de 4 em 4, ou seja, a próxima subrede será a 10.20.132.0 /22
- Os IPs vão de 10.20.128.1 a 10.20.131.254
- Broadcast 10.20.131.255

Como temos um total de 5 VLANs e o máximo de 30 dispositivos na maior VLAN de todas, vamos utilizar subredes /25 que comportam 126 IPs válidos, conforme abaixo:

- **VLAN 10 (servidores)**: subrede 10.20.128.0 /25, IPs válidos de 10.20.128.1 a 10.20.128.126, broadcast 10.20.128.127.
- **VLAN 20 (APs)**: subrede 10.20.128.128 /25, IPs válidos de 10.20.128.129 a 10.20.128.254, broadcast 10.20.128.255.
- **VLAN 30 (Escritório)**: subrede 10.20.129.0 /25, IPs válidos de 10.20.129.1 a 10.20.129.126, broadcast 10.20.129.127.
- **VLAN 40 (Recepção e Salas de reunião)**: subrede 10.20.129.128 /25, IPs válidos de 10.20.129.129 a 10.20.129.254, broadcast 10.20.129.255.
- **VLAN 1 (Gerenciamento)**: subrede 10.20.130.0 /25, IPs válidos de 10.20.130.1 a 10.20.130.126, broadcast 10.20.130.127.

Agora que já temos as faixas de IP precisamos definir quem terá IP fixo, qual IP, quem terá IP dinâmico e que faixa ou escopo vamos configurar no DHCP. Este passo é bem simples, pois os dispositivos de rede precisam de IP fixo e os computadores e telefones IP terão seus IPs distribuídos via DHCP. Normalmente as impressoras de rede também recebem IPs fixos, padrão que vamos considerar nesse projeto. Veja a alocação dos IPs na tabela abaixo.

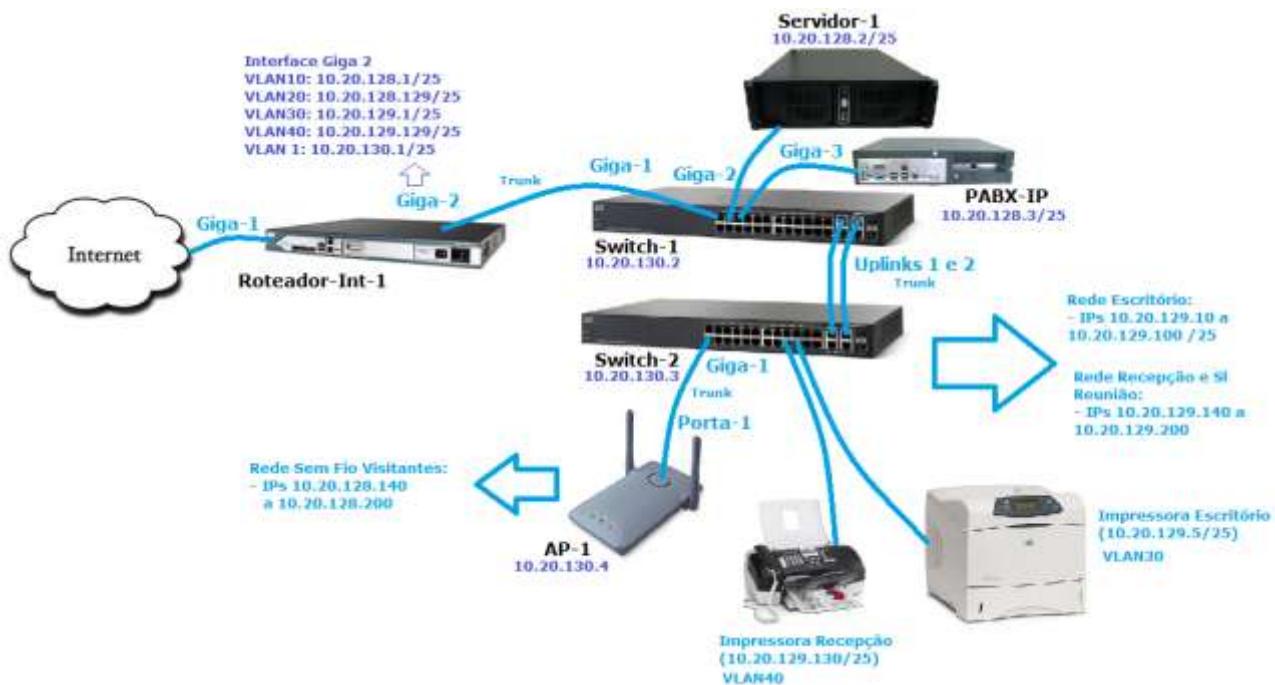
Dispositivos/Hosts	Tipo	VLAN 10 (Servidores)	VLAN 20 (Visitantes)	VLAN 30 (Escritório)	VLAN 40 (Recep e SI Reunião)	VLAN 1 (Gerenciamento)
Servidor-1	Fixo	10.20.128.2/25				
PABX-IP	Fixo	10.20.128.3/25				
Switch-1	Fixo					10.20.130.2/25
Switch-2	Fixo					10.20.130.3/25
AP	Fixo					10.20.130.4/25
Impressora Escritório	Fixo			10.20.129.5/25		
Impressora Recepção	Fixo				10.20.129.130/25	
Roteador (primeiro IP de cada VLAN)	Fixo	10.20.128.1/25	10.20.128.129/25	10.20.129.1/25	10.20.129.129/25	10.20.130.1/25
Computadores Escritório	DHCP			10.20.129.10 a 10.20.129.100		
Computadores Recep e SI Reunião	DHCP				10.20.129.140 a 10.20.129.200	
Rede Sem Fio - Visitantes	DHCP		10.20.128.140 a 10.20.128.200			

O IP do gateway padrão (roteador padrão) a ser configurado em cada um dos dispositivos é o IP do roteador, o qual é o primeiro IP de cada VLAN criada e que ele fará o roteamento. Ainda falta definir o endereço IP do servidor DNS, o qual deve ser passado pela empresa, antes do dia da implantação, para que o DHCP e demais equipamentos possam ser configurados.

Vamos supor que a empresa passou que o DNS será o IP do servidor-1, portanto o escopo dos micros do escritório seria:

- **Rede:** 10.20.129.0 máscara 255.255.255.128 (/25)
- **IP inicial:** 10.20.129.10
- **IP final:** 10.20.129.100
- **Gateway padrão:** 10.20.129.1
- **DNS:** 10.20.128.2

Agora podemos completar a topologia lógica com as informações dos endereços IP para mais tarde preparar a documentação.



Esta é uma possível resolução para o projeto lógico, pois as redes poderiam ser divididas de uma maneira diferente e levando em conta o número de dispositivos e hosts por rede, por exemplo.

Também frisamos que devido ao tamanho pequeno da rede fizemos uma figura mais didática com fotos de equipamentos e diretamente em um editor de imagens ao invés de utilizar o Visio, por exemplo. A ferramenta de desenho fica a critério de cada projetista e também depende da complexidade de rede.

#### 4 Topologia Física e Dimensionamento do Cabeamento Estruturado

O projeto envolve apenas um escritório, ou seja, não teremos distribuidores intermediários ou principais. Isso significa que toda a infraestrutura ficará centralizada em apenas uma sala de telecomunicações/equipamentos e o cabeamento fica mais simples de ser realizado.

Se pensarmos nos dois tipos de cabeamento, horizontal e vertical, também é simples deduzir que o cabeamento vertical ficará todo na mesma sala, a não ser o cabo entre o switch-2 e o AP que pode ficar em uma posição diferente dependendo do próximo passo sobre a definição do posicionamento do AP. Todos os demais equipamentos estarão instalados em um mesmo rack ou no máximo em dois racks um próximo do outro, dependendo da definição do rack e de seu posicionamento que será feito na sequência.

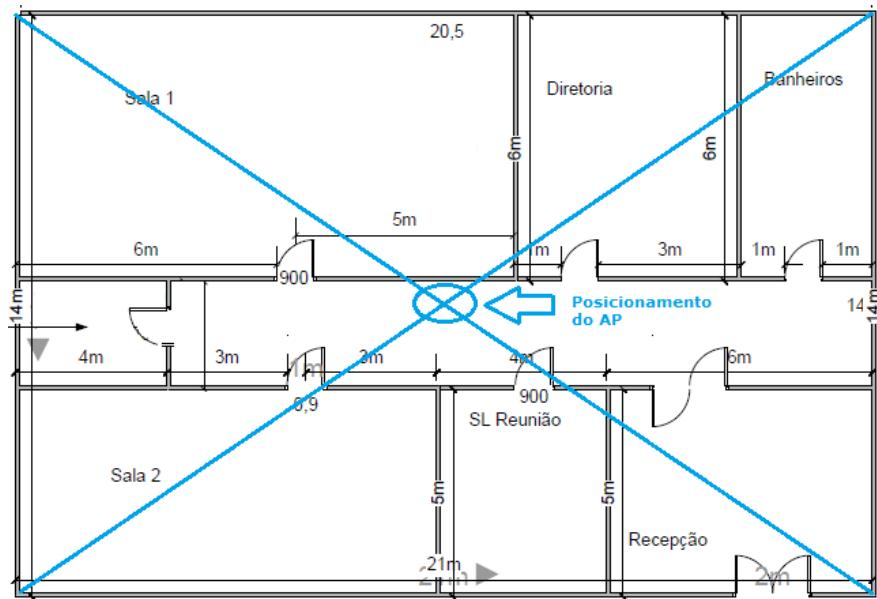
O dimensionamento dos cabos de rede pode ser realizado de duas maneiras:

1. Medição in-loco, ou seja, ir até o escritório e fazer a medida entre a ou as salas de telecomunicações e os hosts ou
2. Utilizando a planta baixa para estimar a quantidade de cabos necessários.

Nesse exercício faremos com a opção 2.

##### 4.1 Definição do posicionamento do AP

Como o cliente solicitou cobertura de 100% via rede sem fio o correto seria realizar um site survey para fazer a definição da quantidade de APs, potência das antenas e melhor posicionamento. Porém, como estamos fazendo um exercício teórico vamos posicionar o AP no centro do escritório e com uma antena de ganho maior que o padrão, por exemplo, uma antena omnidirecional de 12dBi, assim poderemos estimar a quantidade de cabo para a conexão do AP.



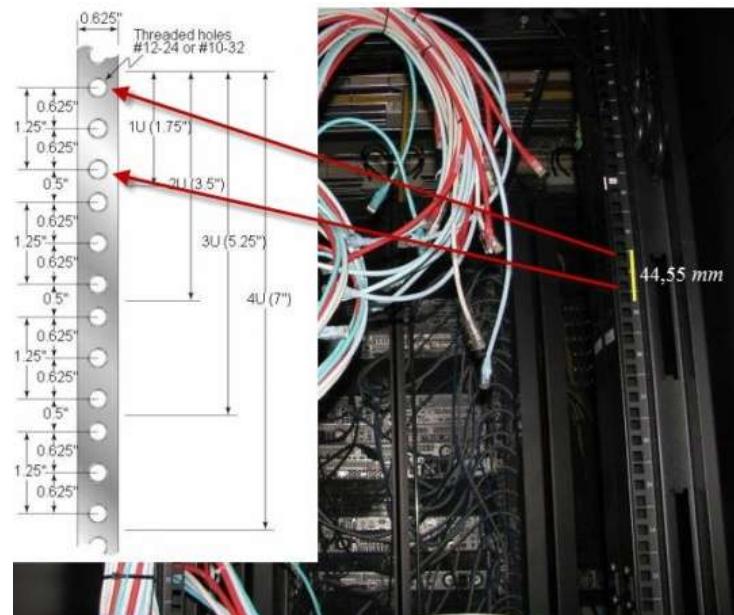
Além disso, o AP deve ser alimentado via PoE pelo switch, por isso um dos switches deve possuir portas PoE. Existem modelos de switches que possuem apenas algumas portas PoE para minimizar o custo ou então pode-se adquirir um injetor PoE, o qual fica ligado entre a porta do switch e o AP. O injetor fica normalmente no rack e precisa de um ponto de alimentação externo para ser alimentado. Veja a figura a seguir, note que ele tem duas entradas, um IN para conectar o switch e outra OUT para conectar o cabo que liga ao dispositivo que deve ser alimentado via PoE.



#### 4.2 Definição do rack e seu posicionamento

Como já temos todos os dispositivos de rede que serão utilizados e suas dimensões em Us (Unidades de Rack), podemos agora fazer o dimensionamento de quantos racks iremos precisar.

Vamos lembrar o que é uma Unidade de Rack, veja a figura, portanto a dimensão em termos de altura total do rack varia das necessidades de cada projeto, porém a altura é normalmente especificada em unidades rack ou "U", a qual corresponde a 44,55 mm.



De uma maneira geral, os Racks ou Gabinetes são feitos de alumínio ou aço, com pintura ou tratamento anti-corrosivo com 19" de largura (dezenove polegadas ou 483 mm) onde é possível ter uma melhor visualização dos equipamentos e uma melhor dissipação do calor.

Para o nosso projeto em específico já temos os equipamentos que serão acomodados no rack e a altura de cada um dada em "Us", conforme listagem abaixo:

- Servidor: 2Us
- PABX-IP: 2Us
- Equipamentos de Telecom: bandeja e 2Us

Para os equipamentos que vamos definir, como o roteador e switches, vamos estimar 1U por equipamento, portanto teremos ainda:

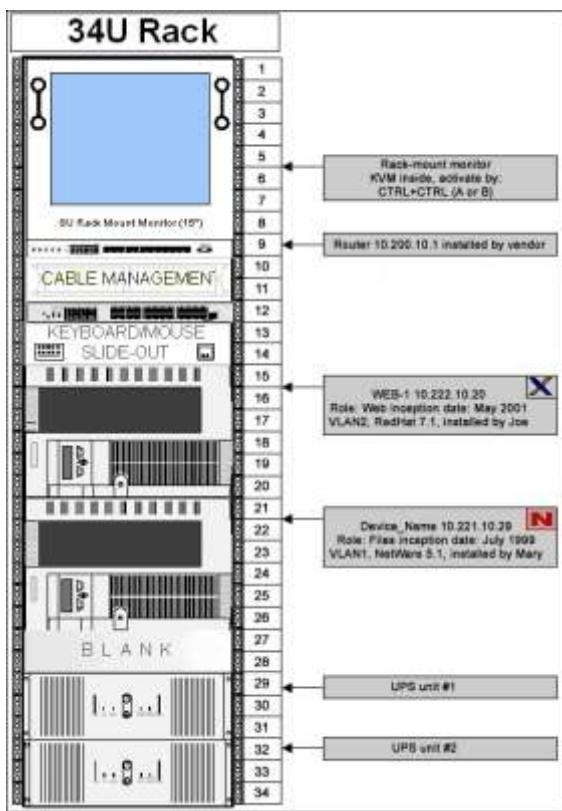
- Roteador: 1U
- Switch-1: 1U
- Switch-2: 1U
- AP: não será instalado no rack

Portanto, de equipamentos de rede temos um total de 9Us, porém sem considerar separação entre eles nem os acessórios para o cabeamento como patch panel e passadores de cabo. Sendo assim, vamos finalizar a definição com estes itens, pois temos dois switches de 48 portas, logo, precisaremos de um patch panel de 48 portas ou dois de 24 portas, mais um ou dois passadores de cabo (organizadores de cabo). Vamos utilizar dois patch panels de 24 portas com 2 passadores de cabo, cada um ocupa 1U, portanto teremos mais 4Us, totalizando 13Us.

Portanto vamos utilizar um rack fechado de piso de 24Us, por exemplo, o qual tem uma altura interna de aproximadamente 1069,2mm (aproximadamente 1m de altura), porém a altura externa será maior devido à estrutura do rack. Alguns administradores de rede preferem trabalhar com racks mais altos para poder fixar os equipamentos em uma altura mais fácil de trabalhar, porém isso depende de cada projeto e os requisitos dos solicitantes.

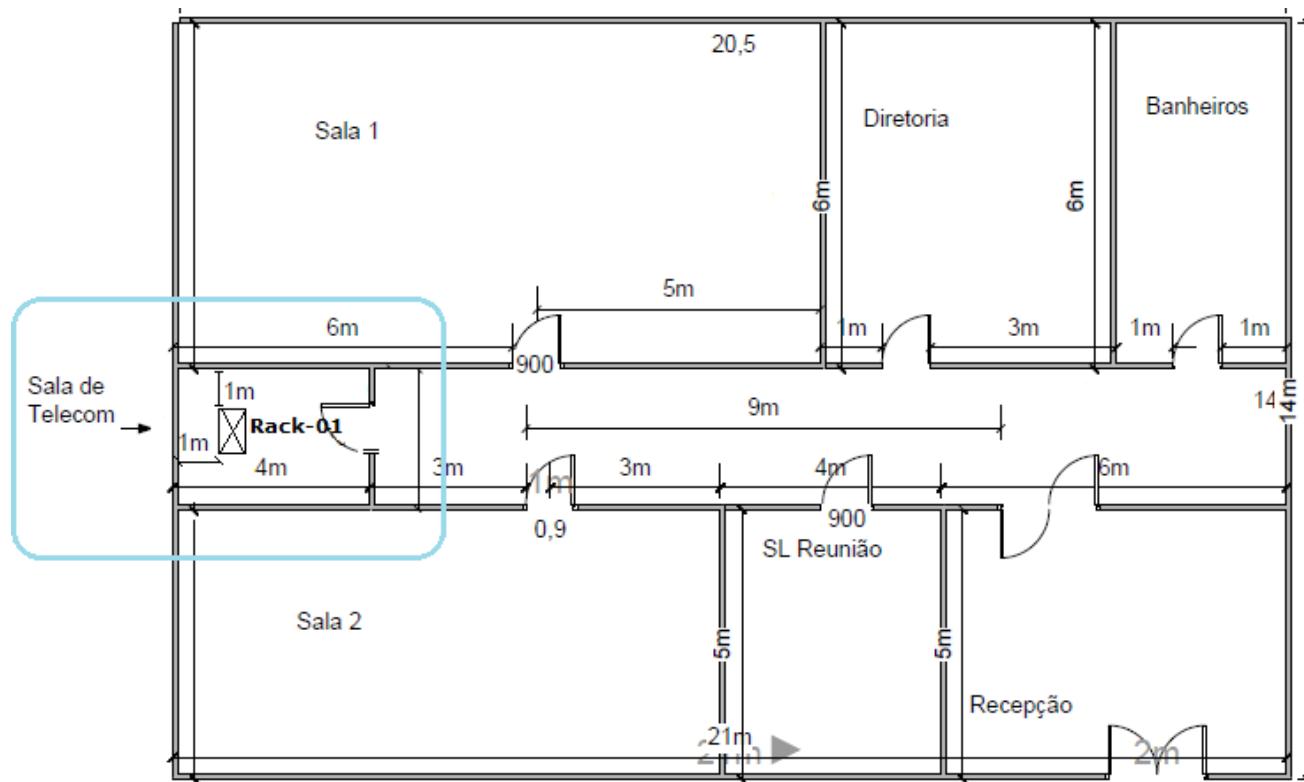


Outra maneira de apresentar o rack na documentação do projeto é desenhando o “Bay-Face” do rack, ou seja, como os equipamentos irão ficar alocados na vista frontal do rack, veja um exemplo na figura abaixo.



O Visio da Microsoft possui padrões muito interessantes chamados “**Stencils**” para facilitar o desenho. Trata-se de formas pré-definidas onde você apenas arrasta e muda o nome. O exemplo da figura acima foi feito utilizando esse recurso do Visio. Vários fabricantes até disponibilizam gratuitamente em seus Websites os Stencils do Visio com seus equipamentos, como roteadores, switches, racks, etc.

Agora que definimos o tamanho do rack precisamos definir sua posição na planta baixa. Temos apenas um local para posicioná-lo, ou seja, na sala de equipamentos e devemos nos preocupar em fixá-lo em uma posição que permita que os técnicos e administradores de rede consigam fácil acesso, tanto frontal como traseiro. Vamos posicionar nosso rack no canto direito da sala de equipamentos conforme ressaltado na planta baixa mostrada abaixo.



#### 4.3 Dimensionamento dos Cabos

Para dimensionar o cabeamento vamos utilizar as medidas passadas na planta baixa e também a quantidade de computadores por sala para determinar quantos cabos precisaremos em cada lance de cabos para cada uma das salas.

Note que na planta não temos o posicionamento exato das mesas, portanto teremos que fazer uma estimativa. Além disso, vamos considerar que utilizaremos dutos aparentes (canaletas) de parede para a passagem dos cabos da sala de equipamentos/telecomunicações até os pontos de rede que estarão disponíveis nas tomadas de telecomunicações (espelhos).

Vamos fazer uma estimativa sem considerar subidas e descidas de cabos no início, aí no final colocamos um fator de correção, pois na prática os cabos saem do patch panel do rack, o qual está a uma determinada altura, sai pelo chão até a parede, aí tem mais uma subida para ser distribuído a partir de um duto principal.

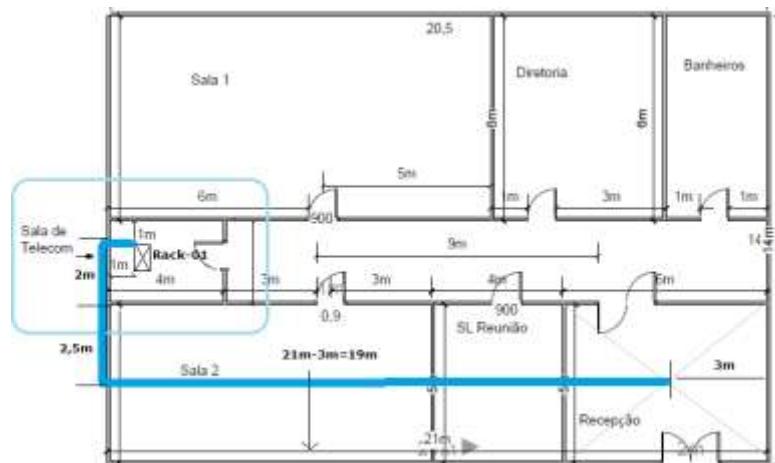
Veja uma foto de exemplo, perceba que da traseira do patch panel o cabo tem um descida onde irá ser encaminhado para a canaleta, essa distância será estimada no final do projeto, pois como todos os cabos saem do mesmo rack será apenas utilizar um valor padrão e multiplicar pelo número de cabos.



Vamos então estimar a quantidade de cabos por sala na sequência iniciando pela recepção e lembrando que passaremos os cabos pelo teto.

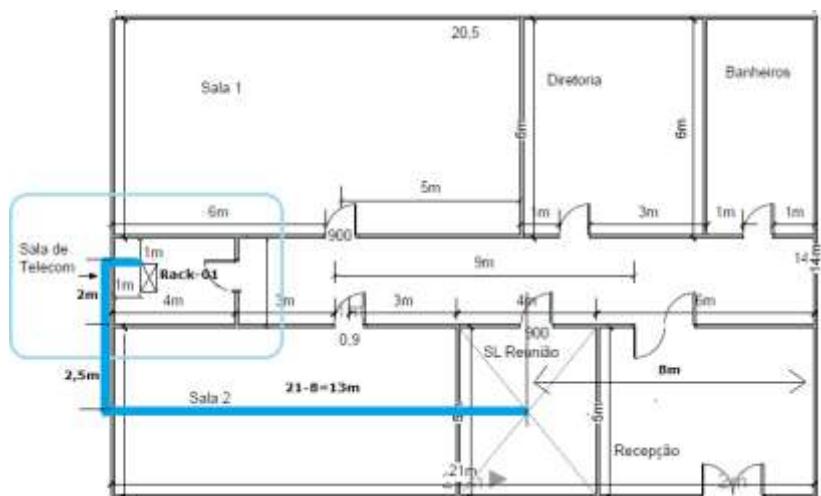
#### 4.3.1 Recepção

Para a recepção precisaremos de três pontos de rede (Computador, Impressora e linha do Fax), portanto vamos traçar o caminho do cabo até a recepção e multiplicar o valor por três, pois todos os pontos ficarão na mesa da recepcionista. Veja a figura abaixo onde temos do rack até a parede 1m, mais uma subida de 3 metros, mais 4,5m de cabo e mais 19m para chegar ao centro da recepção, para finalizar temos mais 3 metros de descida de cabo, totalizando 30,5m, porém temos 3 pontos na recepção: Computador, Impressora e Fax, portanto o valor final será de 91,50m de cabo.



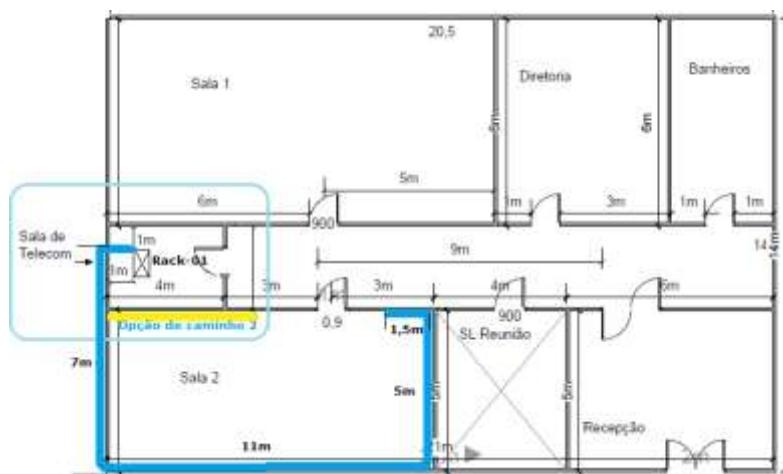
#### 4.3.2 Sala de Reunião

Na sala de reunião teremos apenas um ponto, portanto é só a distância do caminho do cabeamento e podemos utilizar o mesmo caminho feito para a recepção indo até o centro da sala. Veja a figura abaixo onde temos um metro de cabo até a parede, mais 3 metros de subida, mais 4,5m até o centro da sala dois, mais 13 metros até a sala de reunião e vem a descida de 3 metros, portanto temos um total de 24,50m de cabo para o ponto da sala de reunião.



#### 4.3.3 Escritório Sala 2

Para facilitar didaticamente vamos fazer a sala 2, pois assim utilizamos o mesmo caminho da recepção e sala de reunião. Lembre-se que temos mais 10 computadores, vamos seguir o mesmo raciocínio feito até o momento. Veja a figura abaixo, porém agora como temos mais computadores e diversas possibilidades de layout de mesas vamos utilizar o pior caso para o dimensionamento de cabos, que é chegar até a parede onde temos a porta.

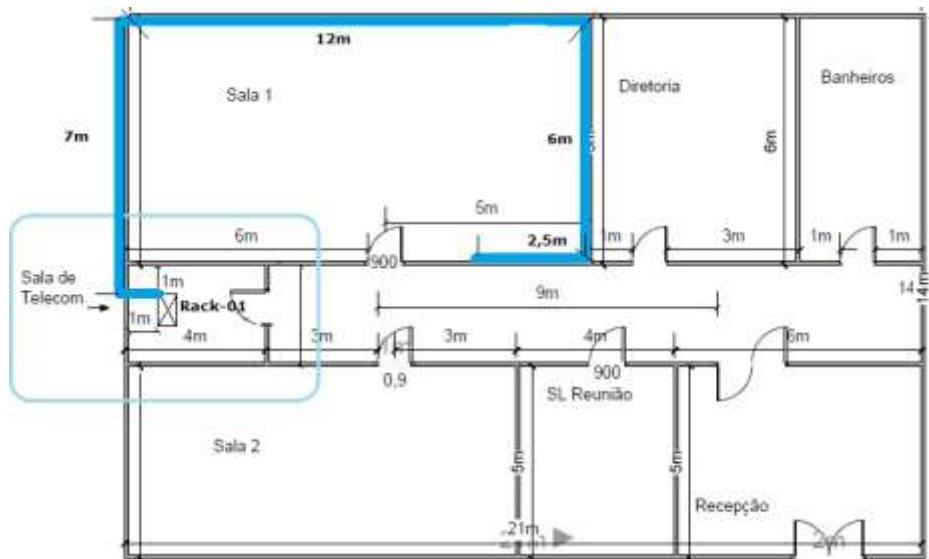


Portanto vamos ter 1 metro de cabo do rack até a parede, 7 metros até a ponta da outra parede, 11 metros, mais 5 metros e 1,5m até metade da parede onde temos a porta, mais 3 metros de subida no rack e 3 metros de descida na sala, totalizando 31,50m por cabo, porém temos um total de 10 computadores o que dará 315m de cabo para a sala 2.

Esta abordagem garante que não teremos surpresas de falta de cabo na hora da instalação.

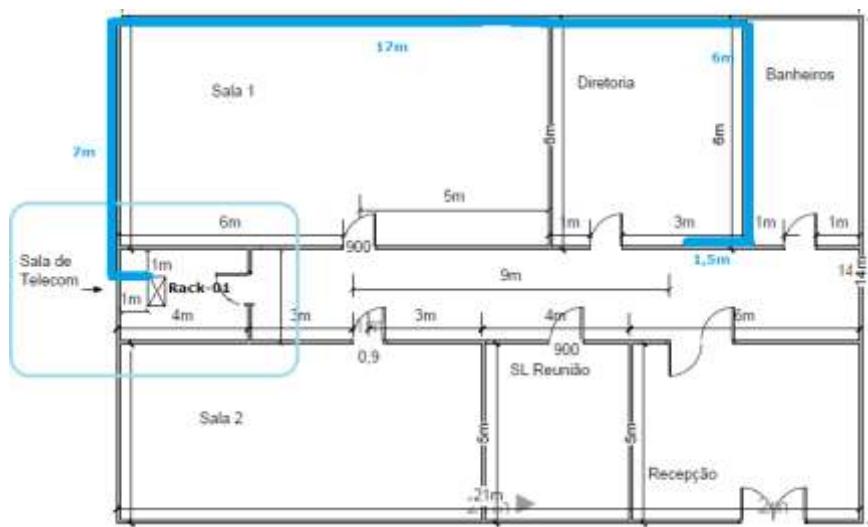
#### 4.3.4 Escritório Sala 1

Na sala 1 temos 14 computadores e a impressora compartilhada, vamos traçar um caminho até próximo de cada mesa e somar esses valores. Veja a figura abaixo onde vamos utilizar também uma abordagem de pior caso. Portanto vamos ter 1m da saída do rack até a parede, mais uma subida de 3 metros, 7 metros até o final da parede, mais 12 metros, mais 6 metros para a parede frontal, mais 2,5m até a metade da parede até a porta e 3 metros de descida de cabo, portanto teremos um total por cabo de 34,50m de cabo, porém temos que multiplicar por 15 (14 micros e uma impressora), totalizando 517,50m de cabo.



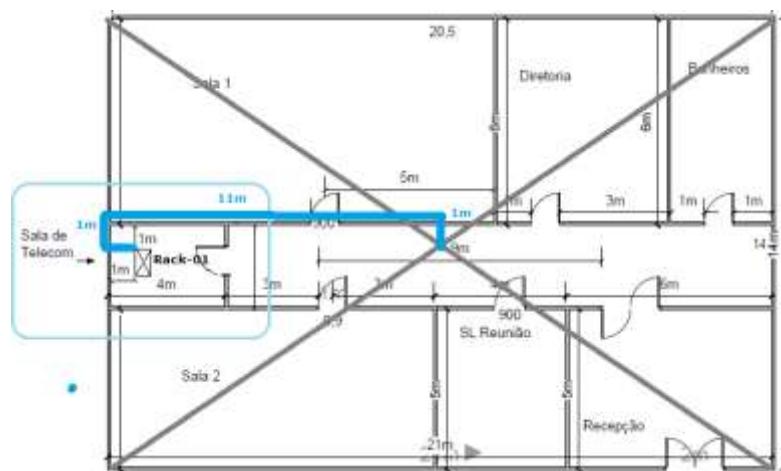
#### 4.3.5 Sala da Diretoria

Por último, na sala da diretoria temos uma secretária e o diretor, mais dois pontos de rede para traçarmos o caminho e estimarmos o comprimento desse cabo. Veja a figura abaixo e note que vamos utilizar o mesmo princípio utilizado para as salas 1 e 2. Portanto teremos 1m do rack até a parede, mais 7 metros até o final da parede, mais 17 metros até o final da parede da diretoria, mais 6 m para chegar à parede da porta e 1,5m para chegar até a metade da parede da porta. Além disso, temos 3m de subida no rack e 3m de descida na sala da diretoria. Portanto teremos 32,50m por cabo, porém como temos dois pontos de rede o total será de 65m de cabo.



#### 4.3.6 Access Point

Agora ainda está faltando o AP que ficará centralizado e fixado no teto do escritório, portanto temos mais uma subida de cabo para considerar. Veja o traçado e a distância na figura a seguir onde teremos um total de 1m até a parede, mais uma subida de 3m, mais 1 metro até a prumada da parede lateral, 11m até chegar ao centro da edificação, mais 1 metro até o AP e vamos colocar mais 1m de folga de cabo, pois o AP ficará fixado no teto, totalizando 18m de cabo.



#### 4.3.7 Saída dos Cabos na Sala de Telecom/Equipamentos e Totalização

Agora para finalizar, como o rack tem aproximadamente 1m de altura e considerando que os patch panels serão instalados a meio metro de altura (0,50m) temos que multiplicar a quantidade de cabos por 0,5 para dar o valor de descida do rack até o chão para todos os cabos, porém vamos multiplicar por 0,85 para dar folga devido a distância da entrada do cabo ao patch panel ser variável, portanto temos ainda que somar ao total que calculamos até o momento mais 30 pontos vezes 0,85 metros que dão mais 25,50 metros de cabo.

Portanto, com o que calculamos até o momento temos as seguintes quantidades de cabo:

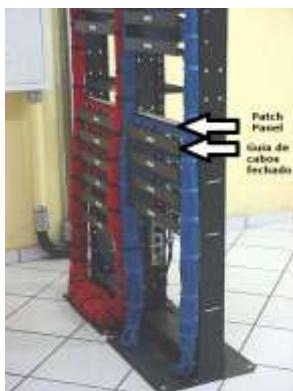
- Recepção: 91,50m
- Sala 1: 517,50m
- Sala 2: 315m
- Diretoria: 65m
- AP: 18m
- Descida do Rack ao Chão: 25,50m
- Total de cabos: 1032,50

Como cada caixa de cabos tem 305m precisaremos de 3 caixas (915m) mais 117m de cabo avulso. Alguns fabricantes vendem rolos de 50m, 100m e 150m, porém tudo depende da escolha no momento da compra dos produtos.

#### 4.4 Acessórios para o Cabeamento

Além disso, precisaremos de diversos acessórios para realizar a montagem, alguns já foram citados no início do projeto e outros não. Abaixo segue uma listagem dos principais acessórios que deverão ser utilizados na montagem, porém dependendo de cada fabricante algumas partes específicas são requeridas, por isso fizemos uma listagem o mais geral possível.

- Dois patch panels de 24 portas e dois passadores/guia de cabos para organização dos cabos no rack. O guia de cabos pode ser aberto ou fechado, no exemplo da figura temos um guia fechado, onde os cabos do patch panel ficam ocultos e são levados dos guias para a lateral do rack. Existem também passadores para a lateral do rack que auxiliam na organização e podem esconder os fios para deixar a aparência do rack mais limpa ainda.



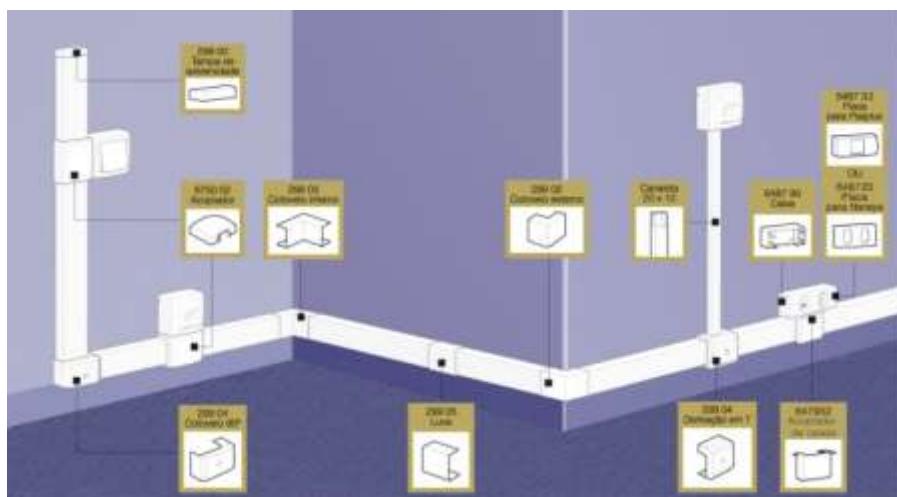
- 30 patch cords para ligar do patch panel ao switch (1,5m) e 30 patch cords para ligar das tomadas de telecomunicações (espelhos) aos computadores (3m). Veja figura abaixo. É importante lembrar que no início do projeto que escolhemos cabos categoria 6, por isso os patch cords também devem ser categoria 6, assim como os patch panels.



- 30 tomadas de telecomunicações com 30 conectores RJ-45 fêmea. As tomadas podem ser de embutir, como a mostrada no exemplo da figura, ou aparentes e existem modelos que possuem de um a oito posições para os RJ-45 fêmeas. Aqui também os RJ-45 fêmeas devem ser categoria 6.



- Canaletas (Dutos) para passagem dos cabos até as tomadas de telecomunicações, assim como luvas, curvas, cotovelos e demais acessórios para montagem conforme cada fabricante. Veja na figura abaixo um exemplo do fabricante Pial Legrand com a linha de dutos chamado "Sistema X 50x20". Nessa figura estão todos os componentes que podem compor uma instalação realizada com dutos aparentes, sendo que esse modelo específico de dutos é fixado com fita dupla-face que já faz parte dos dutos. A largura e profundidade do duto depende da quantidade de cabos a serem passados, nesse mesmo fabricante existem dutos de 20x10 até 110x20. Outro fabricante de dutos muito conhecido no mercado brasileiro é a Dutotec. A quantidade de dutos a serem passados e acessórios necessários não será tema desse projeto.



- Fitas com velcro, abraçadeiras de plástico (cintas), tubos flexíveis e demais acessórios para fixar e organizar os cabos tanto no rack como nas mesas.



Fitas com velcro



Kit organizador de cabos



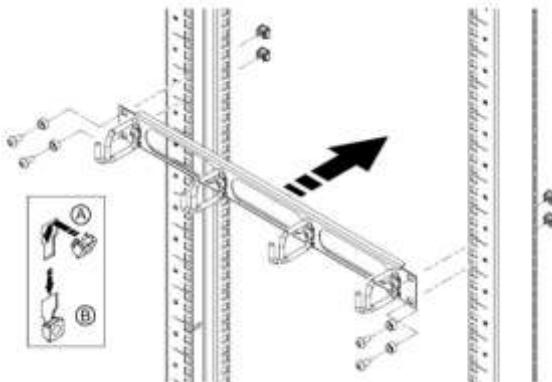
Abraçadeiras de nylon



Organizador para fios flexivel

- Parafusos e porcas para fixação do rack no chão.

- Porca-gaiola e parafusos para fixação dos equipamentos no rack (quatro por equipamento/acessório a ser fixado). Veja a figura abaixo onde tem o exemplo de um guia de cabos aberto de 1U sendo fixado em um rack 19 polegadas, note que são necessárias quatro porcas-gaiola para a fixação do guia no rack e o mesmo vale para os demais equipamentos de rede.



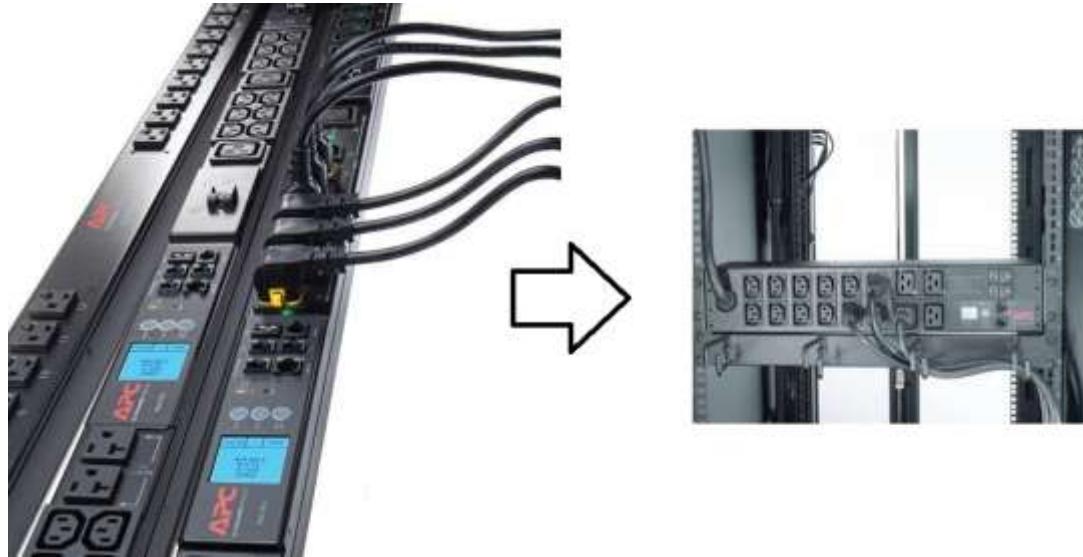
- Duas bandejas de 19 polegadas para os equipamentos de telecomunicações. Veja na figura a seguir um exemplo de bandeja deslizante. Existem bandejas de vários tipos e tamanhos, as quais podem ser fixas ou deslizantes, porém o mais importante é verificar o peso dos equipamentos que ela deve suportar e comprar a bandeja de acordo com essa especificação para que não haja riscos de quebra ou que equipamentos "caiam" no chão durante a operação.



- Etiquetadora com fita de identificação suficiente para marcação dos equipamentos, cabos, patch panel, tomadas de telecomunicações, enfim, para realizar toda identificação dos dispositivos de rede e pontos, tanto no rack como nas mesas. Lembre-se que existem normas também para a identificação de cabos, pontos de rede e dispositivos de rede, uma delas é a "EIA/TIA-606-A - Labeling Standard For Networks" (Nomenclatura Padrão para Redes).



- PDU para montagem em rack (Power Distribution Unity - réguas de alimentação com padrão 19 polegadas ou próprias para fixação em rack). Veja alguns exemplos do PDUs do fabricante APC abaixo.



- Adaptadores para o novo padrão de pinos de tomadas elétricas, pois muitos dos equipamentos de rede ainda vêm com o padrão tradicional de três pinos antigo.



- Fita dupla face para fixar os equipamentos nas bandejas.

## 5 Documentação do Projeto

A documentação do projeto, o qual poderá servir como base para solicitação de uma proposta comercial ou até mesmo ser uma proposta comercial para fornecimento dos produtos mais o serviço de instalação deve conter no mínimo:

- Histórico da empresa que prestará o serviço (definição de nomes, localização, quem prestará o serviço);
- Breve histórico da empresa contratante;
- Escopo contratado, ou seja, os requisitos do projeto combinados com o contratante;
- Dados estatísticos, pois é importante montar uma tabela referenciando cada sala/setor da empresa;
- Desenho das plantas baixas;
- Lista de material;
- Valores discriminados de produtos (todos os equipamentos e materiais a serem utilizados) e serviços de instalação e configuração da rede.

Esta é apenas uma sugestão, pois cada empresa adota um modelo de entrega de propostas ou projetos, lembrando que a intenção do exercício é que você visualize as partes integrantes da rede e possa confrontar com o que encontrar no seu dia a dia.

## 6 Qual Caminho Seguir Após esse Curso?

Essa é uma pergunta que vários alunos fazem e uma sugestão é que se você se identificou com a área de redes, procure seguir um caminho de certificação, por exemplo, indo para o nosso curso do CCNA Network e seguindo uma carreira na área de Roteamento e Switching, Voz sobre IP, Segurança ou Redes sem fio na sequência!

Esperamos que vocês tenham gostado do curso e recomendem para seus amigos!

Equipe DLteC do Brasil

## Sobre o E-book/Apostila

O conteúdo desse documento é uma adaptação da **matéria online de leitura** do curso.

O presente material traz conteúdo teórico do curso online, porém temos que deixar claro que **não é um curso e sim uma adaptação do nosso material online para e-book/apostila**. Portanto recursos como exercícios, simulados, tutoria (tira dúvidas com professores) e vídeo aulas não fazem parte desse e-book, pois são exclusivos para alunos devidamente matriculados em nosso site oficial.

Para maiores informações sobre nossos treinamento visite o site:

>>> [<<<](http://www.dltec.com.br)