

**DLtec**

do Brasil

# eBook

Atualizado e Revisado  
materia completa em português



# Cisco CCENT/ CCNA

ICND1 100-105

## 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.

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 - TCP/IP e Modelo OSI .....</i>	<b>10</b>
<i>Capítulo 03 - Redes LAN e Switches.....</i>	<b>59</b>
<i>Capítulo 04 – Redes WAN e Roteadores.....</i>	<b>110</b>
<i>Capítulo 5 - TCP-IP e Introdução ao Endereçamento IP versão 4 .....</i>	<b>170</b>
<i>Capítulo 6 - Introdução ao Roteamento, Rotas Estáticas e DHCP .....</i>	<b>248</b>
<i>Capítulo 7 - Segmentando Redes Locais com VLANs .....</i>	<b>287</b>
<i>Capítulo 8 - Projetando Redes IP com Sub-rede e VLSM.....</i>	<b>332</b>
<i>Capítulo 9 - Roteamento Dinâmico e RIPv2 .....</i>	<b>366</b>
<i>Capítulo 10 - Reforçando a Segurança nos Dispositivos e Listas de Controle de Acesso .....</i>	<b>402</b>
<i>Capítulo 11 - NAT PAT e Acesso à Internet .....</i>	<b>438</b>
<i>Capítulo 12 - Troubleshooting e Administração de Dispositivos Cisco .....</i>	<b>459</b>
<i>Capítulo 13 -Protocolo IPv6 .....</i>	<b>494</b>
<i>Capítulo 14 – Upgrades, Licenciamento e Manipulação de Arquivos .....</i>	<b>541</b>

## **Capítulo 01 - Introdução**

### **Objetivos do Capítulo**

Olá,

Esse material faz parte do curso CCNA CCENT da DLteC do Brasil. Aqui colocamos uma adaptação em texto do nosso material online de estudo (matéria online do curso CCNA CCENT 100-105).

Nesse capítulo você encontrará uma relação dos itens cobrados na prova atual em relação aos tópicos desse eBook e também do nosso curso online preparatório para o CCENT 100-105.

Esperamos que você aproveite o material e bons estudos.

## Blueprint do CCNA CCENT 100-105

Vamos começar esse material com o blueprint atual divulgado pela Cisco em seu site oficial ([www.cisco.com/go/certifications](http://www.cisco.com/go/certifications)) e relacioná-los com os capítulos do e-Book/Curso Online.

Tópico do Exame	E-Book
<b>1.0 Network Fundamentals – 20%</b>	
1.1 Compare and contrast OSI and TCP/IP models	
1.2 Compare and contrast TCP and UDP protocols	
1.3 Describe the impact of infrastructure components in an enterprise network	Cap 2
1.3.a Firewalls	
1.3.b Access points	
1.3.c Wireless controllers	
1.4 Compare and contrast collapsed core and three-tier architectures	Cap 7
1.5 Compare and contrast network topologies	
1.5.a Star	
1.5.b Mesh	Cap 2 e 7
1.5.c Hybrid	
1.6 Select the appropriate cabling type based on implementation requirements	
1.7 Apply troubleshooting methodologies to resolve problems	
1.7.a Perform fault isolation and document	
1.7.b Resolve or escalate	
1.7.c Verify and monitor resolution	
1.8 Configure, verify, and troubleshoot IPv4 addressing and subnetting	Cap 8
1.9 Compare and contrast IPv4 address types	
1.9.a Unicast	
1.9.b Broadcast	Cap 5
1.9.c Multicast	
1.10 Describe the need for private IPv4 addressing	
1.11 Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment	
1.12 Configure, verify, and troubleshoot IPv6 addressing	
1.13 Configure and verify IPv6 Stateless Address Auto Configuration	
1.14 Compare and contrast IPv6 address types	
1.14.a Global unicast	
1.14.b Unique local	Cap 13
1.14.c Link local	
1.14.d Multicast	
1.14.e Modified EUI 64	
1.14.f Autoconfiguration	
1.14.g Anycast	

<b>2.0 LAN Switching Fundamentals 26%</b>	
2.1 Describe and verify switching concepts	Caps 3 e 7
2.1.a MAC learning and aging	
2.1.b Frame switching	
2.1.c Frame flooding	
2.1.d MAC address table	
2.2 Interpret Ethernet frame format	
2.3 Troubleshoot interface and cable issues (collisions, errors, duplex, speed)	Cap 12
2.4 Configure, verify, and troubleshoot VLANs (normal range) spanning multiple switches	Cap 7
2.4.a Access ports (data and voice)	
2.4.b Default VLAN	
2.5 Configure, verify, and troubleshoot interswitch connectivity	
2.5.a Trunk ports	
2.5.b 802.1Q	
2.5.c Native VLAN	
2.6 Configure and verify Layer 2 protocols	Cap 12
2.6.a Cisco Discovery Protocol	
2.6.b LLDP	
2.7 Configure, verify, and troubleshoot port security	
2.7.a Static	
2.7.b Dynamic	
2.7.c Sticky	
2.7.d Max MAC addresses	Caps 3 e 7
2.7.e Violation actions	
2.7.f Err-disable recovery	
<b>3.0 Routing Fundamentals 25%</b>	
3.1 Describe the routing concepts	Cap 5
3.1.a Packet handling along the path through a network	
3.1.b Forwarding decision based on route lookup	
3.1.c Frame rewrite	
3.2 Interpret the components of routing table	Caps 5, 8 e 9
3.2.a Prefix	
3.2.b Network mask	
3.2.c Next hop	
3.2.d Routing protocol code	
3.2.e Administrative distance	
3.2.f Metric	
3.2.g Gateway of last resort	

3.3 Describe how a routing table is populated by different routing information sources	Caps 5, 8 e 9
3.3.a Admin distance	
3.4 Configure, verify, and troubleshoot inter-VLAN routing	Cap 7
3.4.a Router on a stick	
3.5 Compare and contrast static routing and dynamic routing	Cap 9
3.6 Configure, verify, and troubleshoot IPv4 and IPv6 static routing	
3.6.a Default route	
3.6.b Network route	
3.6.c Host route	Cap 5 e 13
3.6.d Floating static	
3.7 Configure, verify, and troubleshoot RIPv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution)	
<b>4.0 Infrastructure Services 15%</b>	
4.1 Describe DNS lookup operation	Caps 2 e 5
4.2 Troubleshoot client connectivity issues involving DNS	Cap 12
4.3 Configure and verify DHCP on a router (excluding static reservations)	Cap 6
4.3.a Server	
4.3.b Relay	
4.3.c Client	
4.3.d TFTP, DNS, and gateway options	
4.4 Troubleshoot client- and router-based DHCP connectivity issues	Cap 10
4.5 Configure and verify NTP operating in client/server mode	
4.6 Configure, verify, and troubleshoot IPv4 standard numbered and named access list for routed interfaces	
4.7 Configure, verify, and troubleshoot inside source NAT	Cap 11
4.7.a Static	
4.7.b Pool	
4.7.c PAT	
<b>5.0 Infrastructure Maintenance 14%</b>	Caps 10, 12 e 14
5.1 Configure and verify device-monitoring using syslog	
5.2 Configure and verify device management	
5.2.a Backup and restore device configuration	
5.2.b Using Cisco Discovery Protocol and LLDP for device discovery	
5.2.c Licensing	
5.2.d Logging	
5.2.e Timezone	
5.2.f Loopback	
5.3 Configure and verify initial device configuration	Cap 12

5.4 Configure, verify, and troubleshoot basic device hardening	Cap 4 e 12
5.4.a Local authentication	
5.4.b Secure password	
5.4.c Access to device	Caps 3, 4, 7 e 12
5.4.c. [i] Source address	
5.4.c. [ii] Telnet/SSH	
5.4.d Login banner	
5.5 Perform device maintenance	
5.5.a Cisco IOS upgrades and recovery (SCP, FTP, TFTP, and MD5 verify)	Cap 14
5.5.b Password recovery and configuration register	
5.5.c File system management	
5.6 Use Cisco IOS tools to troubleshoot and resolve problems	
5.6.a Ping and traceroute with extended option	Cap 12
5.6.b Terminal monitor	
5.6.c Log events	

*Nesse capítulo do curso vamos estudar o Modelo de Referência OSI e o TCP/IP, fazendo uma comparação entre suas diversas camadas.*

*Bons estudos.*

## **Capítulo 02 – TCP/IP e Modelo OSI**

### **Objetivos do Capítulo**

Ao final do estudo desse capítulo e realização das atividades você deverá ter a capacidade de:

- Conseguir diferenciar os tipos de redes LAN, MAN e WAN.
- Entender e diferenciar comutação por circuitos e por pacotes.
- Diferenciar os equipamentos em uma rede de computadores.
- Entender o Modelo OSI.
- Conseguir explicar as principais características de cada camada, seus principais protocolos e exemplos de equipamentos.
- Conseguir montar uma topologia de rede em simulador.

## Sumário do Capítulo

<b>1 Redes de Computadores</b>	<b>12</b>
<b>2 Classificações de Redes de Computadores</b>	<b>13</b>
<b>2.1 Classificações de Redes de Computadores por Área de Abrangência</b>	<b>14</b>
2.1.1 Redes LAN	14
2.1.2 Redes MAN	14
2.1.3 Redes WAN	14
<b>2.2 Classificações de Redes de Computadores por Tipo de Comutação</b>	<b>15</b>
2.2.1 Rede Comutada por Circuito	15
2.2.2 Rede Comutada por Pacotes	17
2.2.3 Comutação de Circuitos vs. Comutação de Pacotes	19
2.2.4 Linhas Dedicadas/Privativas (Circuitos Ponto a Ponto)	19
<b>2.3 Classificações de Redes de Computadores pela Topologia</b>	<b>20</b>
<b>3 Modelos de Referência OSI e TCP/IP</b>	<b>21</b>
<b>3.1 Definição do Modelo OSI</b>	<b>21</b>
<b>3.2 Camada de Aplicação</b>	<b>22</b>
<b>3.3 Camada de Apresentação</b>	<b>23</b>
<b>3.4 Camada de Sessão</b>	<b>23</b>
<b>3.5 Camada de Transporte</b>	<b>24</b>
3.5.1 Protocolos TCP e UDP	24
<b>3.6 Camada de Rede</b>	<b>25</b>
<b>3.7 Camada de Enlace</b>	<b>27</b>
3.7.1 Entendendo o Endereço MAC	28
<b>3.8 Camada de Física</b>	<b>29</b>
3.8.1 Tipos de Cabos	30
<b>3.9 Encapsulamento de Dados</b>	<b>33</b>
<b>3.10 Identificando e Resolvendo Problemas de Rede com Base no Modelo OSI</b>	<b>36</b>
<b>4 Introdução a Arquitetura TCP/IP</b>	<b>39</b>
<b>5 Características e Elementos de uma Rede de Computadores</b>	<b>40</b>
<b>5.1 Dispositivos Finais (Endpoints) – Clientes e Servidores</b>	<b>40</b>

5.1.1 Computadores	41
5.1.2 Servidores	42
5.1.3 Outros Dispositivos Finais	43
<b>5.2 Componentes da Infraestrutura de Redes</b>	<b>45</b>
<b>5.3 Dispositivos de Rede</b>	<b>49</b>
5.3.1 Repetidores	49
5.3.2 Hub	49
5.3.3 Conversor de Mídia	50
5.3.4 Bridge	50
5.3.5 Switch	51
5.3.6 Access Point (AP) e Controladoras Wireless	51
5.3.7 Roteador (Router)	53
5.3.8 Modem e CSU/DSU	54
<b>5.4 Dispositivos de Segurança de Redes</b>	<b>55</b>
5.4.1 Firewall	55
5.4.2 IDS – Sistemas de Detecção de Intrusão	55
5.4.3 IPS – Sistemas de Prevenção de Intrusão	56
5.4.4 Aplicativos para Desktops	57
<b>6 Resumo do Capítulo</b>	<b>57</b>

## 1 Redes de Computadores

Uma definição simples de Rede de Computadores pode ser dita como um conjunto de computadores ou dispositivos capazes de trocar informação e compartilhar recursos entre si através de um protocolo de rede.

Dentro de uma rede de computadores atualmente podemos encontrar os seguintes dispositivos:

- Computadores (workstations e laptops)
- Servidores
- Roteadores
- Switches
- Access Points (Wireless)
- Wireless Controllers (controladoras de redes sem fio)
- Gateways de voz
- Telefones IP
- Equipamentos de armazenamento (storage)
- Distribuidores de conteúdo (IPTV)
- Firewall
- E muitos outros dispositivos

Veja abaixo a ilustração dos principais dispositivos de rede.



Além disso, as redes de computadores podem ser públicas, como a Internet, ou privadas, chamadas de "Redes Corporativas".

A maior rede atualmente, com amplitude mundial, é a Internet. Milhões de equipamentos fazem parte dessa grande rede, dentre roteadores, switches e servidores de todo o tipo e porte. Para fornecer uma ideia da dimensão da Internet, em novembro de 2015 aproximadamente 3.366.261.156 de pessoas acessaram a Internet de acordo com o Internet World Stats, mais de 3 bilhões de pessoas, sendo que no Brasil foram 117.653.652 de pessoas acessando em comparação a uma população de pouco mais de 204 milhões de pessoas nesse período.

A grande diferença entre as redes corporativas e públicas tais como a Internet, é a questão da privacidade, segurança e porte, porém o princípio de funcionamento dos equipamentos e tecnologias utilizadas são as mesmas. Por exemplo, um roteador de Internet e de uma rede corporativa muitas vezes tem a diferença na capacidade de tráfego suportada, pois um Provedor de Serviços de Internet precisa de um equipamento muito mais robusto em termos de memória e CPU do que um roteador que conecta uma empresa de pequeno ou médio porte.

## 2 Classificações de Redes de Computadores

Vamos agora ver um pouco sobre as possíveis formas de se classificar uma rede de computador. Normalmente as redes podem ser classificadas por:

### Área de Abrangência

- **LAN - Local Area Network**: rede de abrangência local, por exemplo, um escritório.
- **MAN- Metropolitan Area Network**: rede de abrangência metropolitana, por exemplo, a rede de um provedor de serviços que fornece acesso a usuários em uma região de determinada cidade.
- **WAN- Wide Area Network**: rede de longa distância que interliga cidades, estados e até países diferentes.

### Tipo de Comutação

- **Comutada por Circuito**: um circuito ou caminho dedicado é criado a cada necessidade de comunicação. Exemplo, telefonia convencional.
- **Comutada por Pacotes**: a transmissão não necessita de caminho específico, os pacotes trafegam pelo melhor caminho disponível. Exemplo, a Internet e TCP/IP.
- **Linhas Dedicadas/Privativas (Circuitos Ponto a Ponto)**: caminhos criados exclusivamente para determinada comunicação, normalmente através de circuitos ponto a ponto.

### Topologia

- Ponto a Ponto
- Barramento
- Anel
- Malha
- Mista

### Finalidade

- **Internet**: rede de dados pública, formada por diversas empresas, provedores de serviço e entidades não governamentais chamadas de Sistemas Autônomos.
- **Intranet**: rede de dados privativa, normalmente chamada também de rede corporativa.
- **Extranet**: rede utilizada para conectar parceiros e clientes a uma rede corporativa, podemos dizer que é uma extensão da Intranet.
- **VPN**: rede virtual privativa que permite acesso à Intranet passando pela Internet de maneira segura. As VPNs utilizam técnicas de segurança tais como criptografia e autenticação para garantir que os dados que são enviados através da Internet não possam ser capturados e lidos para fins escusos, por exemplo, espionagem.

Para contextualizar melhor todos esses conceitos podemos dizer que a Internet utiliza principalmente circuitos comutados por pacotes, conexões WAN e diversos tipos de topologia.

Outro exemplo seria uma rede corporativa de uma empresa com dois escritórios em cidades diferentes, as quais teriam duas LANs (duas redes locais, uma para cada escritório) conectadas por uma rede WAN através da Internet utilizando uma VPN.

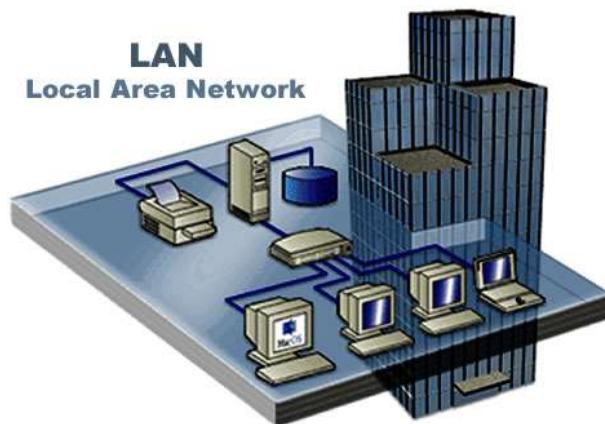
A seguir vamos estudar mais os conceitos desse tópico.

## 2.1 Classificações de Redes de Computadores por Área de Abrangência

### 2.1.1 Redes LAN

Como características de LANs podemos destacar:

- Altas taxas de transmissão (de 10Mbps até 10Gbps).
- Propriedade privada.
- Viabiliza a troca e o compartilhamento de informações e dispositivos periféricos, ou seja, dá acesso aos micros e servidores à rede.
- Geralmente composta por switches, computadores, servidores e uma rede de cabeamento estruturado.



É onde se origina o tráfego de rede. Uma rede LAN pode ser composta por computadores, servidores, switches e roteadores, geralmente todos pertencentes a mesma empresa. Utilizam cabeamento via UTP (Metálico) ou fibra (Backbone) com velocidades de 10/100/1000Mbps.

### 2.1.2 Redes MAN

Como características de MAN podemos destacar:

- Taxas de transmissão entre 10Mbps e 10Gbps.
- Utilização de cabos ópticos, rádio digital ou metro-ethernet.
- Propriedade pública ou privada.



### 2.1.3 Redes WAN

Como características de uma WAN podemos destacar:

- Conecta redes locais geograficamente distantes.
- Meios de transmissão: satélite, fibra óptica, micro-ondas e cabo submarino.
- Baixas taxas de transmissão em comparação às redes LAN e MAN.



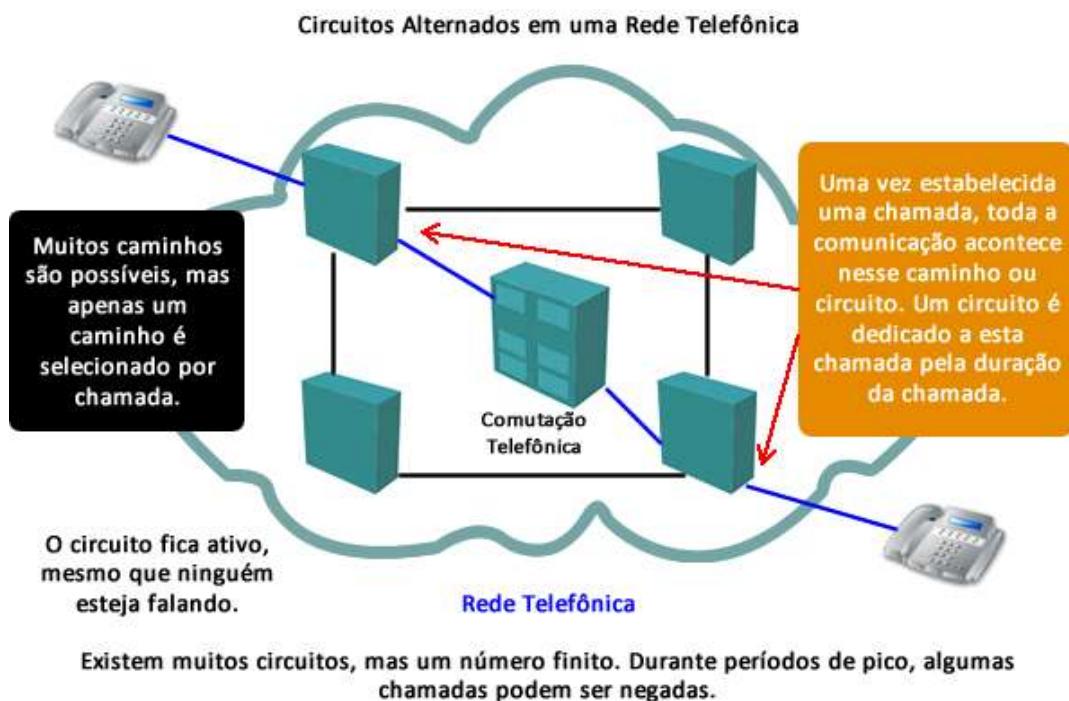
Geralmente são de propriedade de uma operadora de Telecomunicações ou ISP (Internet Service Provider – Provedor de Internet) e interliga várias LAN's, ou seja, diversas unidades em bairros, cidades ou até países diferentes.

Utiliza conexões seriais com taxas mais baixas que em uma LAN podendo ir de 64kbps a 2Mbps (E1) ou taxas mais altas ou até fibras ópticas para acesso metropolitano com velocidades tão altas como as disponibilizadas em redes locais.

## 2.2 Classificações de Redes de Computadores por Tipo de Comutação

### 2.2.1 Rede Comutada por Circuito

Comutação segundo o dicionário Michaelis significa permutação, substituição. Em computação, a Comutação de circuitos e pacotes é utilizada, por exemplo, em sistemas de comunicação onde o tráfego é constante.



Inicialmente as redes comutadas surgiram por uma necessidade da área de telecomunicações. Com o surgimento e ampliação das redes telefônicas, houve a necessidade de interligar os pontos. A princípio eram interligadas uma a uma, mas esta opção gradativamente tornou-se inviável devido à grande quantidade de fios exigida.

Iniciou-se então a comutação manual onde cada telefone era interligado a uma central com um telefonista e este era encarregado de transferir a ligação. Porém, era também inconveniente pois além de ter a demora natural do operador, ainda perdia-se a privacidade, uma vez que o operador poderia ouvir toda a conversa.

Observando a necessidade de um mecanismo mais eficiente, em 1891 foi criada a primeira central telefônica automaticamente comutada. Para seu funcionamento, foi necessária a adaptação da aparelhagem. Os telefones passaram a ter o sinal decádico, que representavam os números de 0 a 9. A interpretação dos sinais pelos comutadores gerava uma cascata interligada destes até o estabelecimento da ligação.

Entre 1970 e 1980 houve o desenvolvimento e implantação de centrais telefônicas eletrônicas, ou seja, os comutadores operados eletromecanicamente foram substituídos por sistemas digitais operados computacionalmente, tudo graças às tecnologias de digitalização da voz.

A expansão dos conceitos para transmissão de dados foi quase imediata, gerando os paradigmas de comunicação comutada existentes.

A comutação por circuitos exige que as estações comunicantes possuam um caminho dedicado exclusivo, que pode ser estabelecido de quatro maneiras:

- Circuito físico exclusivo.
- Frequency Division Multiplexing (FMD - multiplexação por canais de frequência).
- Time Division Multiplexing (TDM - multiplexação por canais de tempo), o qual é o mais comum em ambientes reais.
- Statistical Time Division Multiplexing (STDM - multiplexação estatística por canais de tempo).

Uma chamada em uma linha comutada por circuito se divide em três etapas básicas:

1. Estabelecimento do circuito
2. Conversação
3. Desconexão do circuito

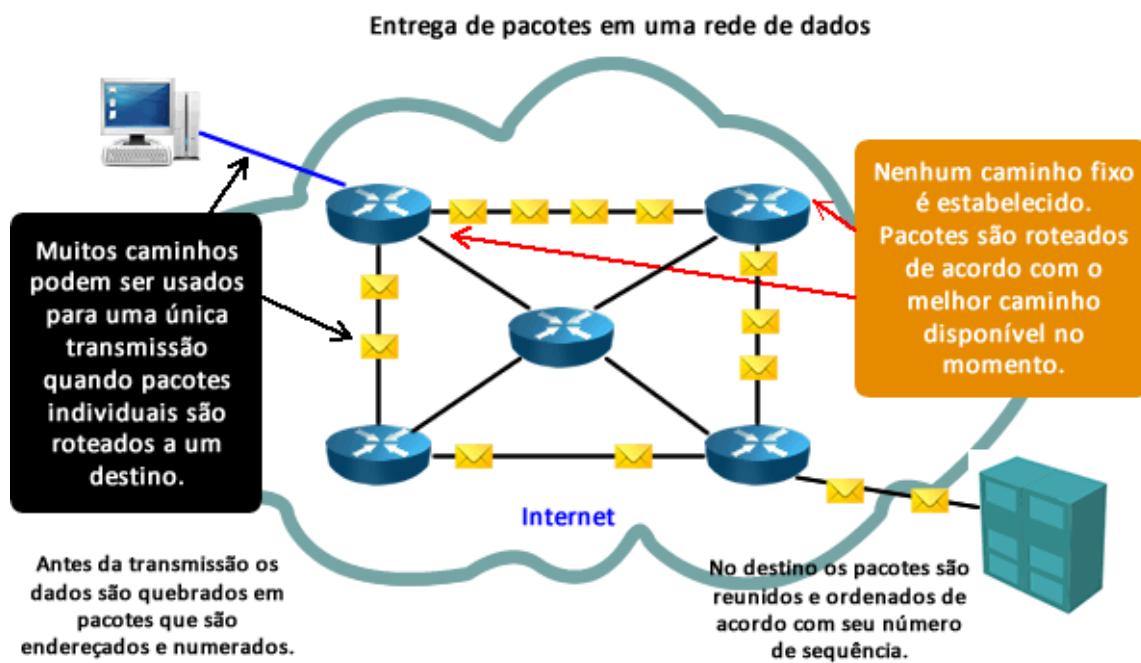
Caso uma destas etapas tenha problemas, há quebra da conexão. Um exemplo claro é uma ligação telefônica, onde há a necessidade de um canal dedicado em ambos os terminais. Outro exemplo é a Internet discada.

Apesar de ser cada vez mais raro o termo "Internet Discada", essa tecnologia de enviar dados através de uma linha telefônica ainda é utilizada nos dias de hoje para realização de acesso remoto aos dispositivos de rede, por exemplo, a linha principal está indisponível e um administrador de rede precisa entrar com comandos para fazer a manutenção (troubleshooting) a partir de um ponto remoto, nesse caso ele "disca" através de um modem analógico e acessa remotamente os dispositivos de rede.

Outro exemplo de uso de circuitos analógicos e modems analógicos são os circuitos backup, chamados de contingência discada. Os ATMs ou caixas eletrônicos que ficam em shopping centers e outras localidades remotas podem utilizar linhas discadas como forma de contingenciamento caso a linha principal caia, pode até ficar mais lento, porém o serviço aos clientes do banco em questão não é totalmente interrompido.

### 2.2.2 Rede Comutada por Pacotes

A comutação por pacotes não exige o estabelecimento de um circuito dedicado para a comunicação, o que implica menores custos com meios físicos. Este paradigma utiliza a ideia da segmentação de dados em partes discretas, compostas de cabeçalho (com bits de verificação de integridade), corpo e rodapé (onde é realizada a verificação cílica de redundância), que são denominados pacotes (ou outros nomes, como quadro, bloco, célula, segmento, dependendo do contexto).



**Durante períodos de pico, a comunicação pode ser atrasada, mas não negada.**

Neste tipo de comutação é usada a multiplexação estatística (STDM). Diferentemente do paradigma anterior (por circuitos), neste o tempo é alocado para os terminais mais ativos prioritariamente, porém sem o risco da quebra da conexão.

Há basicamente duas implementações básicas de comutação por pacotes: circuitos virtuais e datagramas.

Com Circuitos Virtuais cada roteador grava em uma tabela seus VCs (abreviação de Circuito Virtual ou Virtual Circuit) e os identificaunicamente. As tabelas são montadas por ordem hierárquica, ou seja, dos mais abrangentes para os menos.

Após a identificação e montagem das tabelas, é necessário primeiramente o comutador estabelecer um circuito para então iniciar a transferência de dados. O circuito implica que todos os pacotes seguirão o mesmo caminho durante a conexão. Há uma grande desvantagem neste método, pois ele é vulnerável a pontos cegos (buraco negro). Caso um comutador saia do ar e este faça parte do circuito virtual há uma perda da conexão.

O funcionamento assemelha-se ao sistema de uma transportadora, onde são definidas rotas para a entrega de mercadorias. O exemplo mais significativo é o Frame-relay.

Os circuitos virtuais podem ser ainda divididos em:

- **SVC Switched Virtual Circuit:** O circuito é estabelecido dinamicamente, sob demanda, e encerrado assim que finda a transmissão. Seu estabelecimento segue os mesmos passos de uma comutação por circuitos.
- **PVC Permanent Virtual Circuit:** Nesta implementação temos um circuito virtual permanente que fica dedicado à transferência de dados. Os circuitos virtuais permanentes (PVC) são bastante utilizados por fornecedores de serviços públicos ATM e Frame-relay para criar e estabelecer uma complexa infraestrutura baseada em ATM para as respectivas redes internas.

Já a implementação por datagramas permite aos pacotes serem enviados por caminhos diferentes. A cada pacote é determinada uma rota individual, com base na tabela de roteamento presente em cada comutador (roteador) e no endereço de destino. Não é garantida a chegada dos pacotes em ordem, sendo necessária a reorganização após a chegada.

O funcionamento é semelhante a uma viagem, sabendo o destino e partindo do mesmo local muitos carros podem fazer diversas rotas e chegarem, sem garantias de ordem de chegada.

As principais vantagens da comutação por pacotes são:

- Melhor uso do meio de transmissão
- Melhor eficiência de linha
- Melhora a confiabilidade da transmissão de dados
- Pode não haver tempos de estabelecimento e desconexão de circuito (datagramas)
- Baixo tempo de transmissão desde a origem ao destino
- Os erros não precisam chegar ao terminal para serem recuperados
- Possibilidade de armazenar pacotes (transmissão e recepção assíncronas)
- Alteração de encaminhamento em caso de congestionamento
- Possibilidade de aceitar pacotes em situações de tráfego intenso, com posterior envio

Já as principais desvantagens são:

- Disputa por banda nó a nó
- Congestionamento excessivo (choque de pacotes e atraso)
- Sem garantia de banda
- Tempos de atraso entre origem e destino variáveis no tempo
- Possibilidade de chegada de pacotes ao destino por ordem diferente da de emissão (datagramas)

Para resolver as desvantagens citadas acima utilizam técnicas de Qualidade de Serviços ou QoS, as quais permitem definir prioridades e formar filas com o intuito de garantir o melhor serviço para cada tipo de tráfego existente na rede.

### 2.2.3 Comutação de Circuitos vs. Comutação de Pacotes

A comutação de circuitos e a comutação de pacotes diferem em diversos aspectos. Nesta seção, faremos uma comparação entre estas duas técnicas, no que diz respeito à configuração de chamada, forma de envio de dados/pacotes, suscetibilidade a falhas, congestionamento, transparência e tarifação.

Na comutação de circuitos, é necessário estabelecer, previamente, um caminho fim a fim, para que os dados possam ser enviados. Isso garante que, após a conexão ter sido efetuada, não haverá congestionamento e os dados serão enviados de forma ordenada. Entretanto, configurar um caminho com antecedência provoca reserva e provável desperdício de largura de banda. Esse tipo de comutação não é muito tolerante a falhas, sendo que na inatividade de um switch, os circuitos que o utilizam serão encerrados. Os bits fluem continuamente pelo fio e a transmissão de dados é feita de forma transparente, ou seja, o transmissor e o receptor determinam a taxa de bits, formato ou método de enquadramento, sem interferência da concessionária de comunicações, o que proporciona, por exemplo, a coexistência de voz, dados e mensagens de fax no sistema telefônico.

Já na comutação de pacotes, não é necessário estabelecer uma comunicação previamente. Assim sendo, diferentes pacotes poderão seguir caminhos distintos, dependendo das condições da rede no momento em que forem enviados, não chegando, necessariamente, ao receptor de forma ordenada. Existe, entretanto, a possibilidade de atraso/congestionamento em todos os pacotes, uma vez que não é reservada, antecipadamente, largura de banda para a transmissão. Esta técnica é mais tolerante a defeitos e, em caso de inatividade de um switch, os pacotes são roteados de modo a contornar os inativos. É utilizada a transmissão store-and-forward, na qual os pacotes são reservados na memória de um roteador, e depois de inspecionados em busca de erros, são enviados ao roteador seguinte. Por fim, essa transmissão não se dá de forma transparente sendo que os parâmetros básicos, tais como taxa de bits, formato e método de enquadramento, são determinados pela concessionária de comunicações. No sistema como um todo, a comutação de pacotes é mais eficiente que a comutação de circuitos.

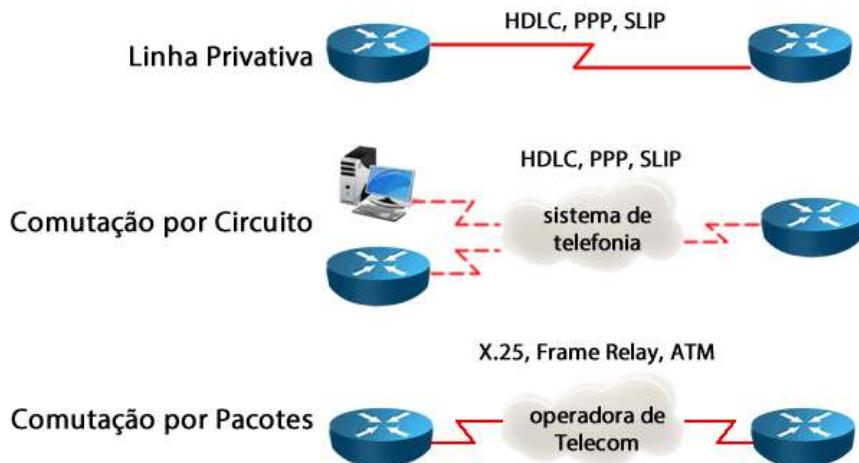
Após estas comparações, podemos chegar a seguinte conclusão: de um lado temos um serviço garantido, porém com desperdício de recursos (comutação de circuitos); de outro, temos serviço não garantido, porém com velocidade maior e sem desperdício de recursos (comutação de pacotes).

Qual o método mais utilizado quando falamos em conexões para transmissão de dados atualmente? Com certeza a comutação por pacotes, princípio básico do TCP/IP.

### 2.2.4 Linhas Dedicadas/Privativas (Circuitos Ponto a Ponto)

As linhas dedicadas, também conhecidas como circuitos ponto a ponto ou linhas privativas, exigem um canal com banda garantida e exclusiva ponto a ponto entre duas localidades. Nesse caso uma prestadora de serviços de telecomunicações teria que disponibilizar essa banda e infraestrutura exclusivamente ao seu cliente, tornando uma solução mais cara e menos flexível como desvantagem, porém com muito mais segurança e garantia total de banda como vantagens.

Veja a figura a seguir ilustrando uma linha privativa e já comprando os tipos de comutação estudados anteriormente.



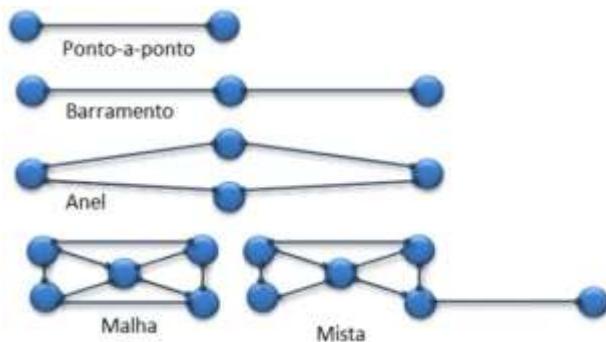
Se formos comparar as três técnicas de comutação podemos concluir que:

- Na tecnologia comutada por circuito temos as linhas discadas analógicas e digitais, as quais são mais baratas, porém com menor banda.
- Na tecnologia comutada por pacotes como as redes IP, por exemplo, temos uma maior eficiência, pois estas redes são mais flexíveis em termos de alocação de banda, topologia e equipamentos, porém elas acabam sendo bem mais complexas.
- Já nas conexões utilizando circuitos privativos ponto a ponto, temos uma qualidade maior, porém com menor flexibilidade.

### 2.3 Classificações de Redes de Computadores pela Topologia

As principais topologias utilizadas tanto em redes de computadores como em comunicações de dados em geral são:

- **Ponto-a-ponto:** São geralmente utilizadas em redes WAN e conectam apenas dois equipamentos, normalmente roteadores ligados por interfaces seriais (PPP ou HDLC).
- **Estrela e Estrela Estendida:** São utilizadas em redes LAN com Hubs e Switches (redes Ethernet, Fastethernet ou Gigabitethernet).
- **Redes em Anel:** Normalmente são utilizadas pelas operadoras de Telecom para conectar seus pontos de presença (PoP) através de redes SDH ou Sonet.
- **Full-meshed e Partial-meshed:** São topologias em malha completa (full) ou mista (partial ou híbrida - Hybrid) formando circuitos virtuais entre os diversos dispositivos da rede. Muito utilizadas em redes Frame-relay.



### 3 Modelos de Referência OSI e TCP/IP

É de conhecimento geral que nos últimos vinte anos houve um grande aumento na quantidade e no tamanho das redes de computadores.

O problema é que esse crescimento não foi implementado de maneira ordenada pelos mais diversos fabricantes e fornecedores, ou seja, cada um implementava seu hardware e software da maneira que lhe fosse mais vantajoso.

O resultado é que essas redes de computadores eram incompatíveis umas com as outras. Isso trazia um enorme problema, tanto para os desenvolvedores de soluções quanto para os clientes (donos) dessas redes, que ficavam como que “reféns” de seus fornecedores.

Foi então que a ISO (a International Organization for Standardization) lançou em 1984 o modelo de referência OSI (Open Systems Interconnection).

Como o próprio nome diz, esse modelo serve de referência para que os desenvolvedores programem redes que podem se comunicar e trabalhar independente do fabricante. O grande segredo é **padronização e interoperabilidade**.

Já o TCP/IP é uma pilha de protocolos que realmente foi implementada na prática e utilizada até os dias de hoje, porém precisamos conhecer ambos os modelos, pois os equipamentos de rede são classificados conforme o modelo de referência OSI, apesar do TCP/IP estar funcionando na prática e o OSI não! Isso porque tudo se iniciou com o modelo OSI, portanto ele acabou sendo um modelo teórico para os desenvolvedores e estudiosos.

#### 3.1 Definição do Modelo OSI

O modelo OSI divide as funções da rede em sete camadas (numeradas de 01 a 07). Veja as camadas e seus respectivos nomes na figura a seguir.



A camada mais próxima ao usuário final é a sete (7), chamada de camada de aplicação. Já a camada um (1) ou física é a mais próxima do cabeamento ou da infraestrutura de redes. Cada camada possui uma estrutura própria, chamada PDU (Protocol Data Unit).

Essa divisão em camadas traz diversas vantagens, dentre elas:

- Decompõe as comunicações de rede em partes menores e mais simples.
- Padroniza os componentes de rede.
- Possibilita a comunicação entre diferentes tipos de hardware e de software de rede.
- Evita que as modificações em uma camada afetem as outras.

Cada uma das camadas deve fornecer seus serviços exclusivamente à camada imediatamente superior, e consequentemente a função de cada camada depende dos serviços da camada imediatamente inferior.

Nos próximos tópicos veremos as principais características de cada uma das camadas do modelo OSI.

Informação extra: link para modelo osi da wikipedia

[http://pt.wikipedia.org/wiki/Modelo\\_OSI](http://pt.wikipedia.org/wiki/Modelo_OSI)

### **3.2 Camada de Aplicação**

A camada de aplicação é a que está mais próxima do usuário e sua função é fornecer serviços de rede aos aplicativos do usuário.

Uma peculiaridade dessa camada é que ela não fornece serviços a nenhuma outra camada OSI, mas apenas a aplicativos (que estão fora do modelo OSI).

A camada de aplicação estabelece a disponibilidade dos parceiros de comunicação pretendidos, sincroniza e estabelece o acordo sobre os procedimentos para a recuperação de erros e o controle da integridade dos dados.

Exemplos de aplicações e serviços dessa camada são HTTP, FTP, Telnet, SMTP, POP3, etc.

**Palavras-chave:** aplicativos, navegadores, etc...

**Aplicações Típicas:** FTP, TFTP, SMTP, SNMP, HTTP, DHCP



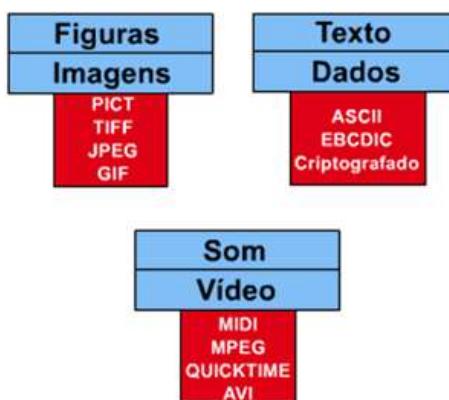
### 3.3 Camada de Apresentação

A camada de apresentação existe para garantir que toda a informação vinda da camada de aplicação de um determinado sistema seja legível para a camada de aplicação de outro sistema (a outra ponta da comunicação). Para tanto, ela deve ser capaz de fazer conversão de dados em um formato comum a ambas as partes.

São exemplos de recursos da camada de aplicação os diversos formatos de arquivos, como binário e ASCII, recursos de multimídia, tais como mp3, wav, mov, mpg e mp3, e formatos de figuras, tais como pict, tif, bmp e jpg.

Além disso, ela trata da compactação e criptografia.

**Palavras-chave:** formato de dados comum.

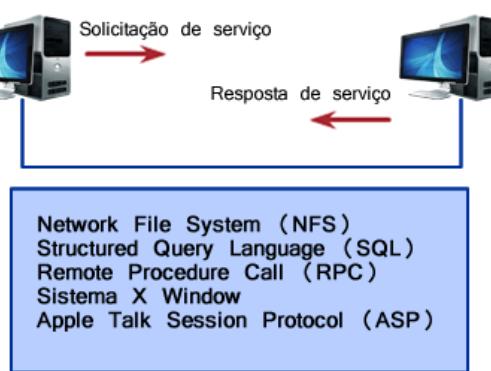


### 3.4 Camada de Sessão

Como o próprio nome diz essa camada estabelece, gerencia e termina sessões entre dois hosts que se comunicam. Ou seja, ela deve sincronizar o diálogo entre as camadas de apresentação dos dois hosts e deve gerenciar a troca de informação entre eles.

Basicamente ela deve manter os dados de diferentes aplicações separados uns dos outros. Alguns exemplos de protocolos dessa camada são: NFS (Network File System), SQL (Structured Query Language), RPC (Remote Procedure Call), etc...

**Palavras-chave:** diálogos e conversações.



### 3.5 Camada de Transporte

A camada de transporte provê mecanismos que possibilitam a troca de dados fim-a-fim, ou seja, a camada de transporte não se comunica com máquinas intermediárias na rede, como pode ocorrer com as camadas inferiores.

A função dessa camada é segmentar os dados do sistema transmissor e remontá-los no lado do destino.

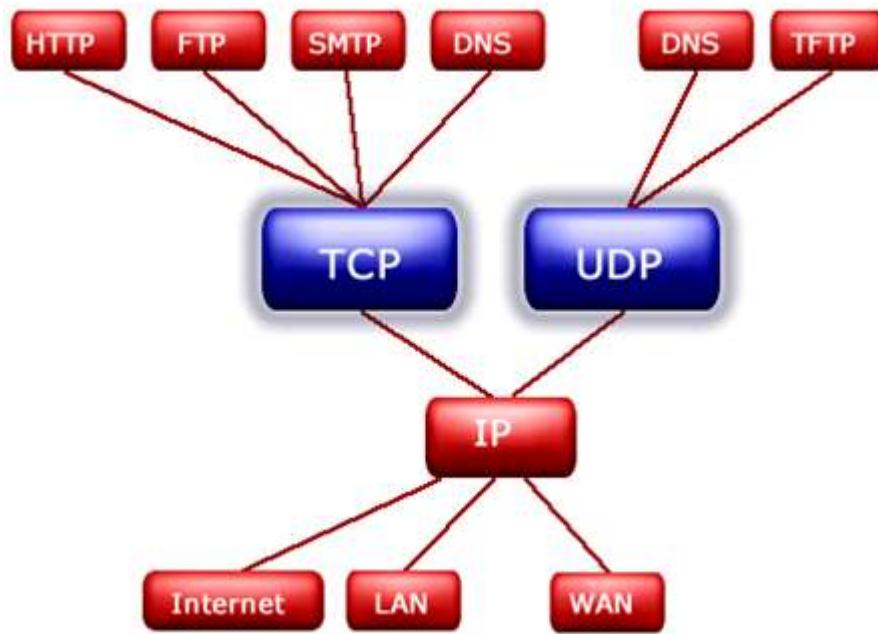
A camada de transporte deve ser capaz de estabelecer, manter e terminar circuitos virtuais bem como realizar o controle de fluxo de informações e a detecção e correção de erros de transportes.

Os protocolos mais comuns encontrados nessa camada são o TCP (Transmission Control Protocol) e UDP (User Datagram Protocol).

**Palavras-chave:** qualidade de serviço, confiabilidade.

#### 3.5.1 Protocolos TCP e UDP

As conexões TCP e UDP são diferenciadas por números de portas ou socket. Por exemplo, ao acessar uma página de Web você está utilizando a porta 80 do protocolo TCP.



Abaixo seguem mais informações sobre os protocolos TCP e UDP, os quais serão estudados com mais detalhes no capítulo específico sobre TCP/IP.

#### TCP (Transmission Control Protocol)

- Confiável
- Orientado p/ conexão
- Fornece controle de fluxo/confiabilidade
- Handshake triplo, janelamento, PAR, números de confirmação e retransmissão.
- Vantagem: entrega garantida
- Ex: HTTP, FTP, SMTP, etc.

### UDP (User Datagram Protocol)

- Não orientado a conexão (best effort)
- Não confiável
- Não faz verificação de software
- Vantagem: velocidade
- Ex: voz, vídeo

**Dica prática:** Cada programa de computador ou aplicativo que acessa a rede utiliza o TCP ou UDP para enviar suas informações, portanto você pode verificar em seu computador essas conexões abertas utilizando o comando "netstat -n" no prompt de comando do Windows ou Linux. Veja na figura ao lado o exemplo do comando "netstat -n" em um computador.

```
C:\>
C:\>netstat -n
Active Connections
 Proto  Local Address          Foreign Address        State
 TCP    127.0.0.1:1066        127.0.0.1:88         CLOSE_WAIT
 TCP    127.0.0.1:1659        127.0.0.1:3386       ESTABLISHED
 TCP    127.0.0.1:3386        127.0.0.1:1659       ESTABLISHED
C:\>
C:\>
C:\>
C:\>
```

Nessa figura temos as colunas:

- **Proto:** indica o tipo de protocolo - TCP ou UDP.
- **Local Address:** endereço local e porta utilizada (seu endereço).
- **Foreign Address:** endereço remoto e porta utilizada (nesse campo você consegue ver o endereço dos computadores que você está conectado ou que estão conectados aos seus serviços de rede).
- **State:** estado da conexão.

No endereço local e remoto, após os dois pontos ":" temos a porta TCP ou UDP que está sendo utilizada nessa conexão. Por exemplo, na linha onde temos a saída "TCP 127.0.0.1:1066" quer dizer que o IP 127.0.0.1 está utilizando a porta 1066 para fazer uma conexão TCP.

### 3.6 Camada de Rede

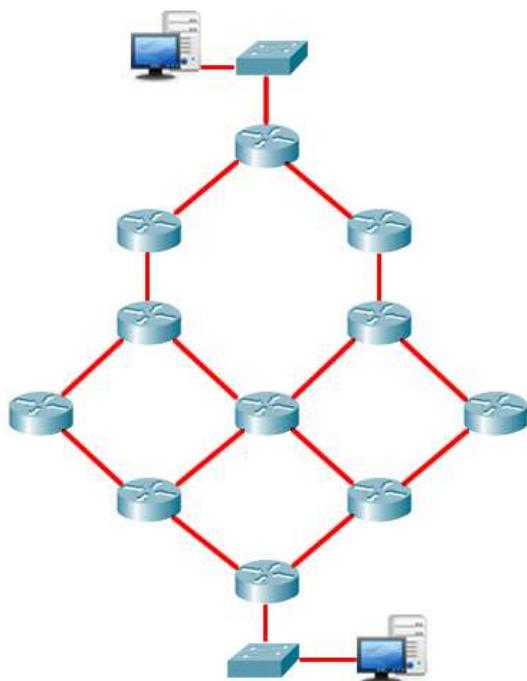
O objetivo da camada de rede é fornecer conectividade e seleção de caminhos entre dois sistemas que podem estar localizados em redes geograficamente separadas. Além disso, a camada de rede fornece o endereçamento lógico para os diversos elementos de rede.

Nessa camada estão os roteadores e o exemplo de protocolo mais conhecido dessa camada é o IP (Internet Protocol).

Note aqui para a diferença entre protocolos roteados e protocolos de roteamento:

- **Protocolos Roteados ou Roteáveis** (Camada 3) fornecem suporte a camada de rede e tratam das informações e dos dados do usuário. Podem ser roteados em uma internetworking. Exemplos: IP, IPX e AppleTalk.
- **Protocolos de Roteamento** têm função de trocar informações sobre as possíveis rotas e determinar o melhor caminho para as diversas redes. Eles trabalham com as informações e endereços fornecidos pelos protocolos roteados. Exemplos: RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First).

**Palavras-chave:** seleção de caminhos, endereçamento e roteamento.



Conforme citado acima, na camada 3 do modelo OSI temos o endereçamento lógico, onde em nossos computadores são representados pelos endereços IP (Internet Protocol). Você pode visualizar o endereço IP do seu computador com o comando "ipconfig" se ele for Windows ou "ip address show" se for uma máquina Linux. Em roteadores Cisco podemos visualizar os endereços IP configurados em suas interfaces com o comando "show ip interface brief".

Você já configurou uma placa de rede? Se sim parabéns, se não você pode realizar o laboratório sugerido disponível para download na área do aluno com o nome: "Laboratório 2.4 - Configurando Placas de Rede no Windows 7".

### 3.7 Camada de Enlace

A camada de enlace proporciona trânsito confiável de dados através de um enlace físico e está relacionada ao:

- Endereçamento físico (MAC)
- Topologia lógica de rede
- Forma de acesso aos meios
- Notificação de erros (FCS)

Endereços da camada de enlace geralmente serão alterados para endereços do próximo enlace. Endereços físicos em dispositivos da família Ethernet (802.3) são chamados de MAC, o qual é o endereço físico gravado em maioria das placas de rede dos elementos de rede.

Os protocolos da camada de enlace incluem: ETHERNET, TOKEN RING, PPP, HDLC, FR, X25, ISDN.

Os dispositivos de rede que atuam na camada 2 são bridges, switches e placas de rede (NIC), veja as figuras a seguir onde temos uma placa de rede e switches Cisco da linha Catalyst 2960.



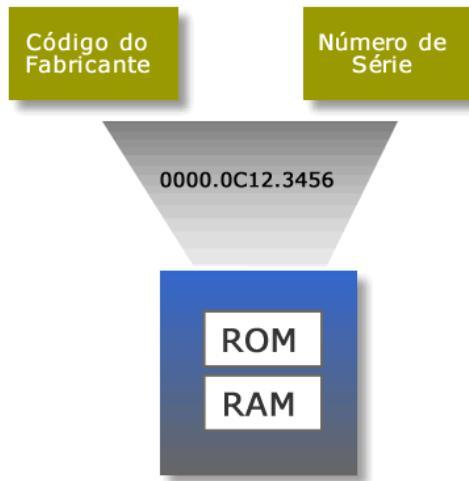
**Palavras-chave:** quadros e controle de acesso ao meio.

### 3.7.1 Entendendo o Endereço MAC

O endereço MAC (Media Access Control) é o endereço físico da estação, ou melhor, da interface de rede. É um endereço de 48 bits, representado em hexadecimal. Este endereço é o utilizado na camada 2 (Enlace) do Modelo OSI em redes Ethernet.

Os três primeiros octetos são destinados à identificação do fabricante, os 3 posteriores são números arbitrados pelo fabricante, ou seja, um serial. É um endereço único, ou seja, não existem, em todo o mundo, duas placas com o mesmo endereço físico, pelo menos na teoria, pois na prática são relatados casos de placas de rede "clonadas" (piratas) com seriais iguais, porém isso é uma história para quando começarmos a praticar em switches.

Abaixo temos como um endereço MAC é formado.



O endereço MAC pode ser escrito de outras formas dependendo do sistema operacional do endpoint, por exemplo, em máquinas Windows ele seria escrito da seguinte maneira:

- 00-00-0C-12-34-56

Em um computador com Linux o mesmo endereço seria visualizado como 00:00:0C:12:34:56, portanto o importante é que são 12 algarismos em Hexa, totalizando 48 bits, pois cada algarismo em Hexa possui 4 bits.

Abaixo segue um resumo das características de um endereço MAC:

- Endereço da camada 2
- Gravado no chip da ROM em uma placa de rede Ethernet
- Número exclusivo de 48 bits que está gravado como doze números hexadecimais. ( físico )
- Os primeiros 24 bits representam o fornecedor ou o fabricante (OUI)
- Os últimos 24 bits do fornecedor formam o número de série

Dica prática: com o comando "ipconfig /all" você consegue visualizar os endereços "IP" e "MAC" das placas de redes instaladas no seu micro. Veja na a seguir onde temos os campos "Physical Address" e "IP Address", respectivamente o endereço MAC e o endereço IP. Em máquinas Linux você pode utilizar o comando "ip address show" e em roteadores e switches Cisco "show ip address".

```
C:\>ipconfig/all
Windows IP Configuration

Host Name . . . . . : [REDACTED]
Primary Dns Suffix . . . . . : [REDACTED]
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : [REDACTED]

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Description . . . . . : Broadcom 440x 10/100 Integrated Controller
    Physical Address. . . . . : 00-15-C5-B2-F9-98

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Dell Wireless 1390 WLAN Mini-Card
    Physical Address. . . . . : 00-16-CP-80-D4-86
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 192.168.1.124
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway. . . . . : 192.168.1.1
    DNS Servers . . . . . : [REDACTED]

C:\>_
```

### 3.8 Camada de Física

A camada física define as especificações elétricas, mecânicas, funcionais e de procedimentos para ativar, manter e desativar o link físico entre sistemas finais.

Características como níveis de voltagem, distâncias máximas de transmissão, conectores físicos são definidas pelas especificações da camada física.

A camada física tem como função básica a adaptação do sinal ao meio de transmissão. Nessa camada estão situados os Hubs, repetidores, transcievers, patch pannel, cabos e conectores.

Os padrões de nível físico utilizados são, por exemplo, X.21, X.21 bis, V.24, V.28, V.35, RS-232 I.430, I.431, G.703, etc...

**Palavras-chave:** sinais e meios.

A seguir temos figuras de dispositivos típicos da camada física, sendo que o HUB é o mais citado, pois ele foi o precursor das redes LAN que temos atualmente implementadas com switches. Os HUBs atuam na camada física porque eles não conseguem ler endereços de camada 2 ou 3, ele atua como um simples repetidor de sinais, ou seja, o que entra em uma porta é simplesmente replicado para as demais portas, como se fosse um curto circuito.



### 3.8.1 Tipos de Cabos

Falando em camada física, nada melhor que já estudar os principais tipos de cabos que vamos encontrar durante o curso quando falamos de conexões locais.

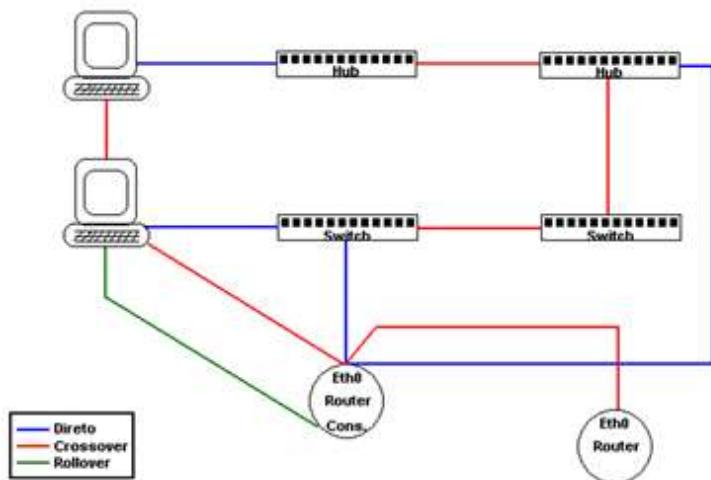
Os três principais cabos de pares trançados encontrados são o direto, cruzado e rollover.

Utilizamos um cabo direto para conectar PC-HUB, PC-Switch, Router-HUB, Router-Switch, ou seja, um endpoint a um dispositivo de rede concentrador. Note que o roteador ou router é considerado como um endpoint nesse caso, pois ele é um computador de uso especial. O PC é um computador, apenas outra nomenclatura que significa personal computer.

Já os cabos cruzados ou cross utilizamos para conectar dois dispositivos de mesma função, por exemplo, PC-PC, HUB-HUB, Switch-Switch, Switch-HUB, Router-Router ou Router-PC.

Os cabos rollover podem ser uma novidade para você, eles são utilizados para conectar a porta chamada de Console dos roteadores e switches Cisco à saída serial de um computador para fins de gerenciamento local via terminal.

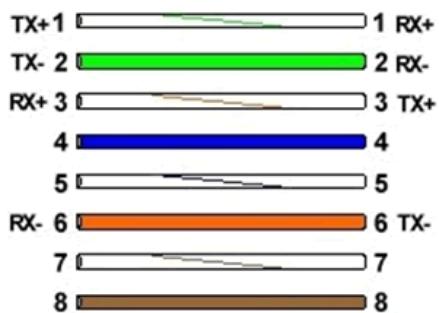
Veja a figura a seguir com o exemplo de uso dos cabos aqui citados.



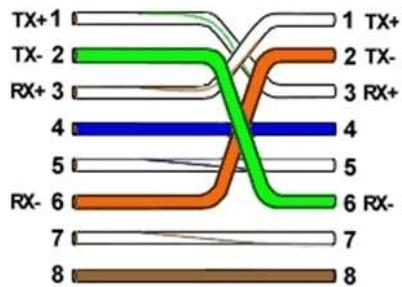
**Informação extra:** link para o site sobre par-trançado  
[http://pt.wikipedia.org/wiki/Cabo\\_de\\_par\\_tran%C3%A7ado](http://pt.wikipedia.org/wiki/Cabo_de_par_tran%C3%A7ado)

Portanto, os cabos de rede LAN podem ser diretos (straight-through) ou cruzados (cross ou crossover).

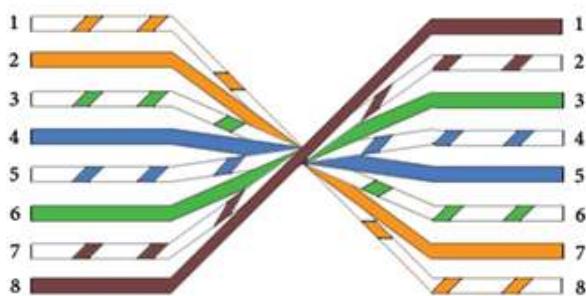
Os cabos diretos são utilizados para ligar equipamentos de usuário (como hosts, servidores, telefones IP, lap-tops) aos equipamentos de rede (HUBs e Switches). Lembre que um roteador é como se fosse um micro de aplicação especial, sendo considerado um host para o cabeamento. Veja a pinagem de um cabo direto na figura a seguir.



Já o cabo cruzado tem a função de interligar equipamentos com a mesma função na rede, por exemplo, dois micros, um servidor a um micro, um roteador a um micro, dois switches, dois HUBs, um HUB a um switch e assim por diante. Veja a pinagem de um cabo cruzado na figura a seguir.



Os cabos rollover são utilizados para ligar os computadores aos roteadores e switches Cisco para fins administrativos. Para tal é utilizada a porta de console do roteador/switch, com conector serial DB-9, que deve ser ligada a porta serial do computador (conector DB-9). Essa conexão é chamada de console. Outra função dos cabos rollover é para conexão da porta auxiliar (chamada de AUX) dos roteadores a um modem discado para realizar a administração remota dos roteadores, sendo que essa conexão é feita com um adaptador DB-25. Na figura abaixo você tem a pinagem do cabo rollover.



O cabo de console pode vir de duas maneiras:

1. Rollover com duas pontas RJ-45 e para conectar ao micro é necessário um adaptador RJ-45 para DB-9.



2. Rollover com uma ponta RJ-45 e outra DB-9.

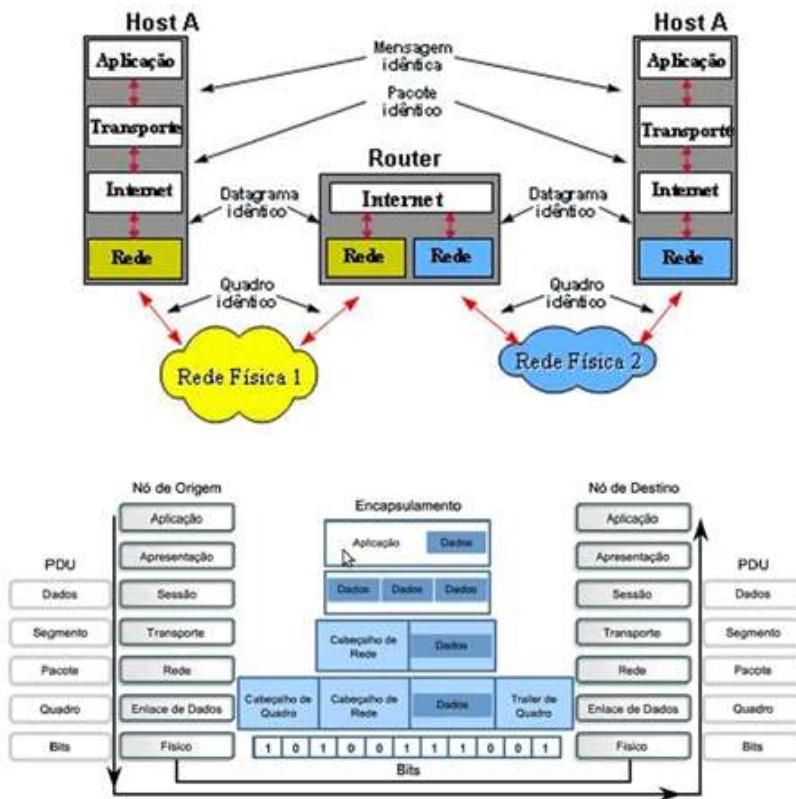


Porém, nos computadores novos é difícil encontrarmos conexão serial, sendo necessário um adaptador DB-9 para USB.

### 3.9 Encapsulamento de Dados

Cada camada possui um protocolo próprio e informações de controle específicas que ficam armazenados em seu cabeçalho. Portanto cada camada se comunica com seu par remoto através dessas informações.

O processo de encapsulamento controla essa troca de informações entre as camadas.



Portanto, conforme mencionado no slide anterior o processo de encapsulamento é realizado para podermos enviar os dados de um host a outro ou de um host a um servidor de rede. A comunicação é como se fosse camada a camada, por exemplo, como se a camada de aplicação se comunicasse diretamente com a outra camada de aplicação do host remoto, sendo que as camadas inferiores são como se fossem módulos de transporte. A figura ao lado representa cada camada e os cabeçalhos inseridos a cada passo. Ao chegar do outro lado, ou seja, no micro remoto esse cabeçalho é lido e os dados encaminhados à camada superior.

Então vamos traduzir o processo de encapsulamento do modelo OSI, o qual descreve como os dados são “preparados” para poderem ser enviados pela rede e então enviados à aplicação em outro host ou servidor:

1. O aplicativo, por exemplo, um cliente de e-mail deseja enviar seus dados para a rede.
2. A camada de aplicação recebe essa mensagem e encapsula os dados inserindo um cabeçalho com as informações de controle referentes à camada 7 (A) e envia para a camada inferior.
3. A camada de apresentação recebe a informação e agora os dados mais o cabeçalho da camada de aplicação viram os dados da camada de apresentação, a qual insere seu cabeçalho (P) com seus controles e envia para a camada de sessão.
4. A camada de sessão recebe agora essa informação e trata como seus dados de entrada, insere suas informações de controle através do cabeçalho de camada 5 (S - sessão) e envia para a camada de transporte.
5. Agora sim começa a preparação para a entrada na rede, pois a camada de transporte vai numerar essa aplicação com uma porta TCP ou UDP de origem e destino (T), se os dados forem muito grandes eles são segmentados e enviados para a camada de rede. Esse número de porta TCP ou UDP serve para identificar internamente no computador a quem pertence esse fluxo de informações, pois as portas de origem TCP ou UDP em um cliente são sempre diferentes, ou seja, únicas. O nome da informação que é trocada pela camada de transporte pode ser chamado de segmento, se pertencer ao TCP, ou datagrama se for UDP.
6. A camada de rede recebe o segmento TCP ou Datagrama UDP e irá inserir os endereços de camada 3 (normalmente o IP) de origem e destino e montar um pacote que será enviado pela rede e utilizado pelos roteadores para que esse pacote possa chegar ao seu destino (N).
7. Após montado o pacote IP ele é enviado para a camada de enlace (L), a qual tem a função de “adaptar” o pacote em um “quadro” para que essa informação possa ser enviada pelo meio físico. O quadro de camada 2 depende da tecnologia que está sendo utilizada. Agora que o quadro está montado ele é enviado à camada física para ser transportado pelo meio físico.
8. As informações do quadro de camada 2 são convertidas em bits (zeros e uns) e enviadas pelo meio físico, que pode ser par metálico, uma rede sem fio, fibra óptica, satélite e assim por diante.

A partir desse ponto essa informação vai percorrer a rede e o endereço IP de destino é lido pelos roteadores para que o pacote possa chegar ao seu destino. A cada roteador a camada de enlace é desmontada e remontada, porém da camada 3 (rede) para cima é apenas lida e encaminhada ao próximo roteador.

Quando o pacote alcança seu destino ele é enviado ao host final, o qual captura os bits recebidos pela rede e inicia o processo de desencapsulamento, ou seja, os bits são transformados em quadros, que são lidos, tem seu cabeçalho removido e enviado à camada superior, a qual faz o mesmo processo até que os dados são enviados pela camada de aplicação ao serviço de rede ou aplicação remota.

Agora que a aplicação remota recebeu e tratou a informação ela pode responder ao emissor com a solicitação enviada até que a requisição seja finalizada e nenhum dado mais tenha que ser trocado entre origem e destino.

Podemos interpretar que o protocolo de rede, como o OSI e o TCP/IP, são como um meio de transporte para as informações entre o emissor e o receptor, ou seja, como se os dados fossem a carga que precisa ser transportada por uma via e o protocolo com suas diversas camadas são os meios de transporte, como uma carga sendo enviada do produtor ao fabricante através de uma rodovia, onde o meio de transporte são os caminhões e os dados o insumo produzido pelo produtor.

Outro sistema que podemos fazer uma analogia são os correios, enviando cartas e produtos entre as pessoas através de um protocolo específico (regras de envio), pois para que uma pessoa receba a carta você deve seguir uma regra de endereçamento e envio.

Fazendo uma analogia com os correios a camada 7 é o emissor, o qual vai escrever uma carta, que são os dados. Esses dados são “encapsulados” em uma carta que precisa um endereçamento para chegar no outro lado, no receptor, sendo que o endereçamento tem a origem que é o remetente e o destino que é o destinatário. Esse endereçamento, no Brasil, precisa do nome do remetente e destinatário, endereço completo com rua, número, cidade, estado e CEP. Com esses dados o “pacote” que é a carta é enviada ao destino sendo roteada pelas diversas agências do correio até chegar ao seu destino, onde ele vai desencapsular (abrir a carta) e ler o conteúdo da mensagem.

Caso tenha a necessidade de resposta quem recebeu a carta vai escrever uma carta de resposta, utilizando agora seu endereço como origem (remetente) e o endereço de quem enviou a carta agora vira o destino (destinatário). E assim a transmissão e recepção de dados vão ser trocadas até que não haja mais necessidade de transmissão.

Acompanhe a animação abaixo que ilustra o processo de encapsulamento do modelo OSI.

Link para animação no youtube: <http://www.youtube.com/watch?v=fiMswfo45DQ#at=12>

### 3.10 Identificando e Resolvendo Problemas de Rede com Base no Modelo OSI

Identificar e resolver problemas em Redes de Computadores também é conhecido como processo de **Troubleshooting** e é um dos requisitos cobrados de um candidato à certificação CCENT ou CCNA.

Como usuário de computador e redes você já deve estar familiarizado com muitos dos problemas que são reportados e até já aconteceram com você mesmo, vamos citar alguns problemas comuns que podem ser reportados por usuários de redes:

- Estou sem acesso à rede e/ou à Internet
- Estou sem acesso a uma pasta compartilhada na rede
- Meu acesso à rede e/ou à Internet está lento
- Estou notando lentidão na rede e/ou no acesso à Internet
- Não consigo enviar ou receber e-mails
- O site da web que estou tentando acessar está bloqueado

Para resolver um problema de rede existem algumas metodologias e fluxogramas que podem auxiliar o administrador de redes na solução, porém veremos o troubleshooting de maneira mais detalhada em capítulos posteriores.

Em linhas gerais, para resolvemos um problema temos que entendê-lo primeiro, depois investigar suas causas, elaborar uma possível solução, implementar essa solução, testar a solução e se funcionou precisaremos documentá-la e encerrar o caso. Se a solução não funcionou será preciso voltar à situação inicial, ou seja, desfazer o que fizemos como provável solução e voltar à fase de investigação para que possamos elaborar e testar novas soluções até resolver o problema.

Se levarmos em conta o modelo OSI podemos atacar os problemas “**por camada**”, por exemplo, quando um usuário reclama de **falta de conectividade à rede** devemos iniciar pela camada física, pois a grande maioria dos problemas de rede está nessa camada do modelo OSI. Os problemas da camada física são cabos desconectados ou rompidos, mau contato, equipamentos desligados, ou seja, tudo que está vinculado à parte física da rede. Veja a figura abaixo.



Se o cabeamento está OK e a placa de rede do usuário, assim como o switch de acesso estão com os leds indicadores de conexão acesos (leds verdes) temos que partir para a camada superior, portanto temos que verificar a **Camada de Enlace**.

Os problemas típicos da camada de enlace são relacionados aos protocolos de camada 2, por exemplo, você tem dois roteadores conectados via interface serial em uma rede WAN e um deles tem configurado o protocolo HDLC e outro o protocolo PPP em sua interface, portanto a camada 2 não irá se comunicar, pois dos dois lados temos que ter os mesmos protocolos. Veja a figura abaixo.



Em placas de rede podemos ter problemas de velocidade e modo de transmissão, por exemplo, um switch configurado como 100 Mbps com modo de transmissão Full-Duplex e a placa de rede estava como 10 Mbps Half-Duplex. Esse tipo de problema é difícil de acontecer nos dias de hoje porque tanto as placas de rede como os switches fazem a “**autonegotiação**”, permitindo que sejam suportados diversos padrões.

Uma vez verificada a camada de enlace e o problema persiste devemos ir para a **Camada de Rede**. O troubleshooting na camada de rede pode ser bastante complexo, pois envolvem endereços lógicos, máscaras de rede, roteadores padrões, protocolos de roteamento, etc.

Normalmente quando falamos em um computador o teste que permite verificar a conectividade fim a fim é o “**ping**”. Em capítulos posteriores estudaremos que o ping faz parte de um protocolo chamado **ICMP** ou **Internet Control Message Protocol**. Com o ping podemos fazer um teste para um host remoto e ver se ele responde, caso haja resposta indica que a camada 3 do modelo OSI, ou seja, a camada de rede está OK.

Em caso de problemas você pode receber um “**Request Timeout**” (tempo de espera ou limite expirado ou perdido) ou um “**Destination Unreachable**” (destino ou rede inalcançável). Veja a figura abaixo.

A captura de tela mostra o terminal de comando (CMD) no Windows. O usuário executa o comando 'ping 10.0.0.20' e 'ping www.cisco.com'. As saídas são:

```
C:\>ping 10.0.0.20
Disparando 10.0.0.20 com 32 bytes de dados:
Esgotado o tempo limite do pedido.

Estatísticas do Ping para 10.0.0.20:
  Pacotes: Enviados = 4, Recebidos = 0, Perdidos = 4 (100% de perda),
C:\>
C:\>ping www.cisco.com
Disparando e144.dscl.akamaiedge.net [23.57.128.170] com 32 bytes de dados:
Resposta de 23.57.128.170: bytes=32 tempo=15ms TTL=54
Resposta de 23.57.128.170: bytes=32 tempo=22ms TTL=54
Resposta de 23.57.128.170: bytes=32 tempo=15ms TTL=54
Resposta de 23.57.128.170: bytes=32 tempo=15ms TTL=54

Estatísticas do Ping para 23.57.128.170:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
  Aproximar um número redondo de vezes em milissegundos:
    Minimo = 15ms, Máximo = 22ms, Média = 16ms
C:\>
```

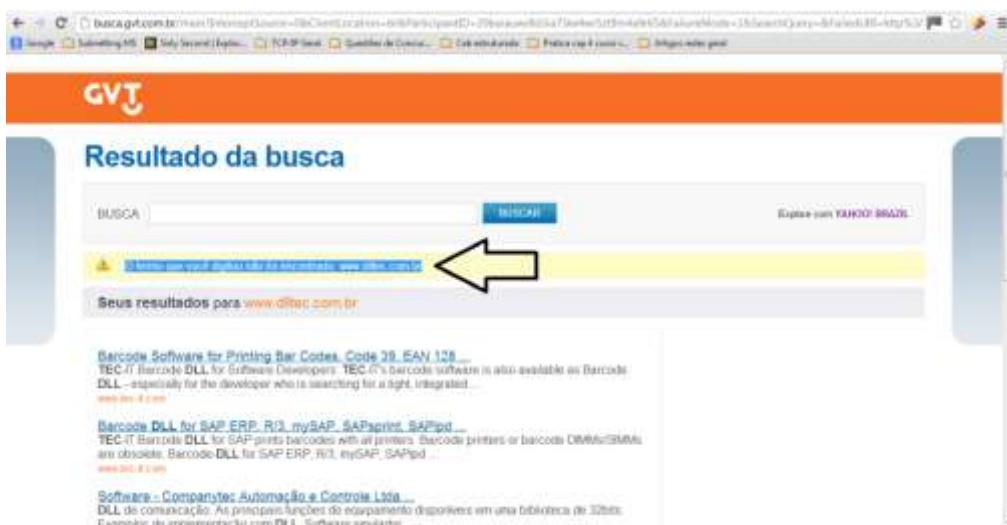
As linhas de texto entre parênteses em destaque representam resultados de ping problemáticos ('Ping com problemas') e resultados de ping OK ('Ping OK').

Os problemas nas camadas 1, 2 e 3 são os que estão diretamente envolvidos com a rede, pois a comunicação em rede se dá nessas três camadas do modelo OSI.

A partir da camada 4 ou Transporte os problemas podem envolver situações mais complexas, tais como a ação de firewalls ou filtros de conteúdo, portanto elas tem mais haver com os servidores e computadores, ou seja, os hosts.

Na camada 7 ou Aplicação podemos ter problemas de compatibilidade dos protocolos com os aplicativos dos usuários ou então com os recursos do próprio computador para processar as informações necessárias.

Além disso, para acesso à Internet é necessário um serviço chamado DNS (Domain Name System), o qual tem a função de traduzir o nome das URLs (links de internet) e caso ele esteja indisponível ou com problemas não será possível o acesso aos sites de Internet. Outro problema comum é a própria URL ser digitada de maneira errada, por exemplo, ao invés de **www.dltec.com.br** o usuário digita **www.dltec.com.br**, se o domínio **dltec.com.br** existir virá uma página que não era a desejada, porém se ele não existir o usuário terá uma resposta de **página ou domínio inexistente**. Veja a figura abaixo.



Para finalizar o assunto lembre sempre que um troubleshooting levando em conta o modelo OSI deve ser realizado da camada 1 para a 7, ou seja, da mais baixa ou física em direção à camada mais alta ou aplicação. Portanto você deve iniciar pelo cabeamento, depois verificar a placa de rede, para aí passar para as camadas superiores até chegar a camada 7, verificando problemas com o servidor DNS ou então com a própria URL digitada em seu navegador de Internet, por exemplo.

Não se preocupe nesse momento com os detalhes do acesso ou sobre os protocolos mencionados, pois ao decorrer do curso veremos estes e outros protocolos com mais detalhes. O importante nesse momento é entender a abordagem de resolução de problemas (troubleshooting) por camadas, ou seja, utilizando as camadas do modelo OSI para resolução de problemas de rede.

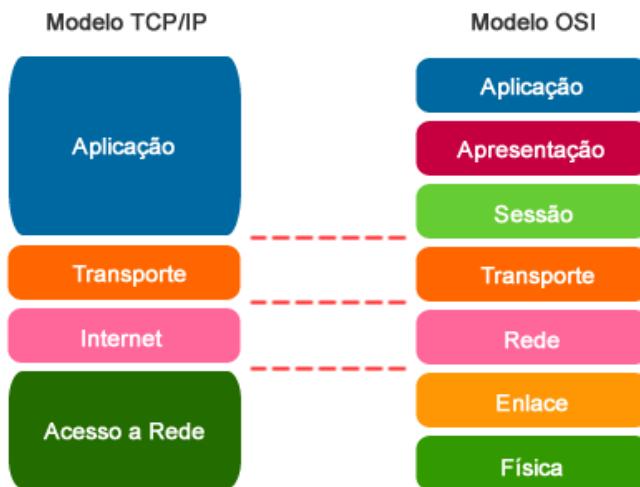
#### 4 Introdução a Arquitetura TCP/IP

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**.

Por fim, 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 a seguir.



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.

Como o TCP/IP é o protocolo que usamos na Internet ele será estudado com profundidade posteriormente, nesse momento vamos ficar por aqui, apenas com esses conceitos básicos sobre ele.

A seguir você será apresentado aos principais dispositivos de rede e conceitos que nem todos são foco do exame de certificação 100-105, porém como procuramos preparar nossos cursos não somente para o exame vamos apresentar informações úteis que você pode encontrar em seu dia a dia como futuro CCENT e CCNA!

## 5 Características e Elementos de uma Rede de Computadores

Segundo a Cisco uma rede de computadores deve ter as seguintes características abaixo:

- **Tolerância a falhas:** as redes devem prever redundância.
- **Escalabilidade:** crescer sem precisar construir uma nova rede.
- **Qualidade de Serviços:** suportar diversos tipos de tráfego priorizando cada um de acordo com suas características e necessidades.
- **Segurança:** evitar ataques, invasões, espionagem industrial, destruição de dados, quebra de privacidade, etc.

Para isso diversas tecnologias e recursos devem ser suportados pelos dispositivos ou elementos de rede. Basicamente podemos dividir os elementos de uma rede em:

- **Endpoints:** os dispositivos finais dos clientes, tais como computadores, telefones IP, laptops, tablets, etc.
- **Servidores e dispositivos de armazenamento (Storages):** elementos de rede que têm a função de fornecer serviços de rede aos clientes.
- **Dispositivos da infraestrutura de redes:** cabeamento estruturado, roteadores, switches, access points e demais elementos de rede que tem a função de encaminhar os dados entre os dispositivos finais e servidores.

A seguir vamos estudar rapidamente os principais elementos e dispositivos de rede para que você tenha maior facilidade nos conceitos que serão estudados ao longo do curso. No CCENT/CCNA Routing and Switching o foco são roteadores e switches Cisco, porém é necessário que o aluno conheça os elementos que podem ser encontrados em uma rede de computadores, pois o dia a dia vai além de "Routers and Switches"!

### 5.1 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.



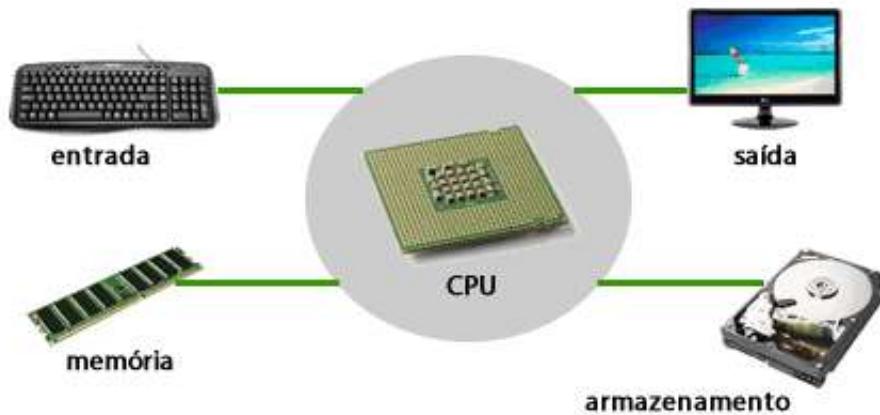
### 5.1.1 Computadores

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.

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).

### 5.1.2 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.

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.



#### 5.1.3 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.

## 5.2 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 chamadas de "cabeamento horizontal" e também a interligação entre os equipamentos de rede chamados "**cabeamento vertical**" ou "**backbone**".

Veja a seguir uma imagem que representa esse ambiente.



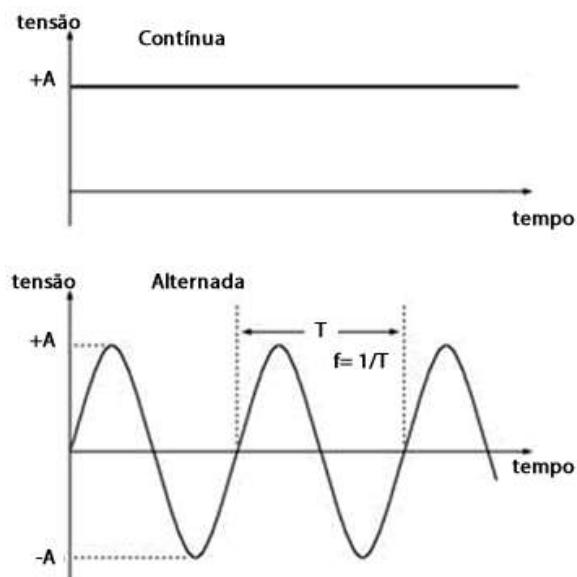
Na infraestrutura física não temos somente os cabos e seus conectores, pois para montar a rede física podemos precisar também de:

- **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 ou “energização” 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.



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 aerosol 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.

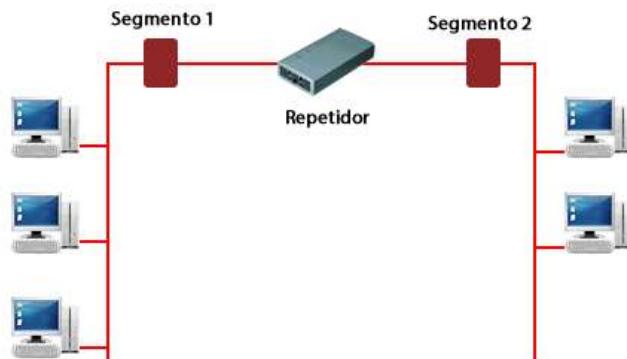
### 5.3 Dispositivos de Rede

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:

#### 5.3.1 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.



#### 5.3.2 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.

### 5.3.3 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.

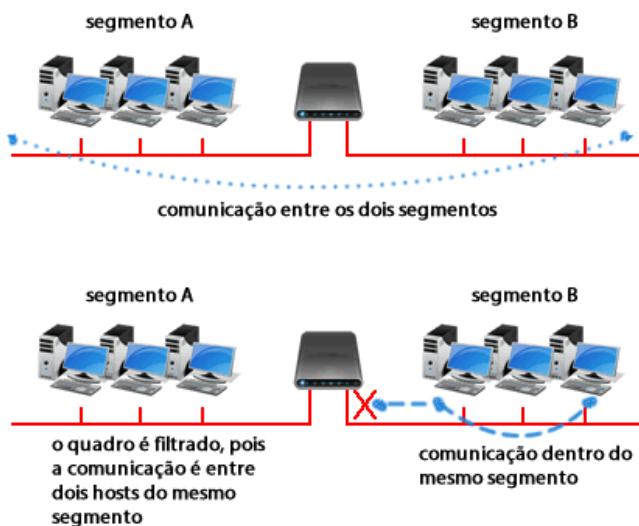


### 5.3.4 Bridge

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.

### 5.3.5 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.

### 5.3.6 Access Point (AP) e Controladoras Wireless

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.

Em redes de pequeno porte os APs são autônomos, ou seja, cada dispositivo precisa ser configurado manualmente um a um. Agora imagine em uma grande empresa que possui 100 APs, será que seria simples administrar um a um esses equipamentos? Com certeza não e para isso você pode utilizar uma rede integrada, a qual utiliza controladoras para gerenciar diversos APs.

Uma controladora de redes sem fio ou “Wireless LAN controller” tem a função de controlar e gerenciar as funções de TODOS os APs (Access Points) na rede, por exemplo, roaming, que redes sem fio e SSIDs os APs utilizarão WLANs, autenticação e muito mais.

Veja a figura a seguir onde temos um roteador sem fio e um repetidor fornecendo acesso wireless aos computadores de um pequeno escritório.



Na Cisco os Access Points podem ser configurados como **APs autônomos** e **LAPs (Lightweight Access Points)** ou APs controlados por **WLCs - Wireless LAN Controllers** na LAN ou Campus.

Os APs autônomos são configurados como os APs residenciais, ou seja, um a um de maneira individual.

Já no modo LAP os Access points são controlados pelas controladoras sem fio ou WLCs, as quais passam a controlar todos os aspectos da comunicação sem fio, inclusive todas as configurações dos LAPs.

Portanto APs em modo LAP são projetados para serem configurados pela WLC, conhecido como **“zero touch deployment”**, ou seja, não precisa fazer nada nos LAPs, eles inicializam e pegam todas as configurações da sua controladora (WLC - Wireless LAN Controller).



### 5.3.7 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.

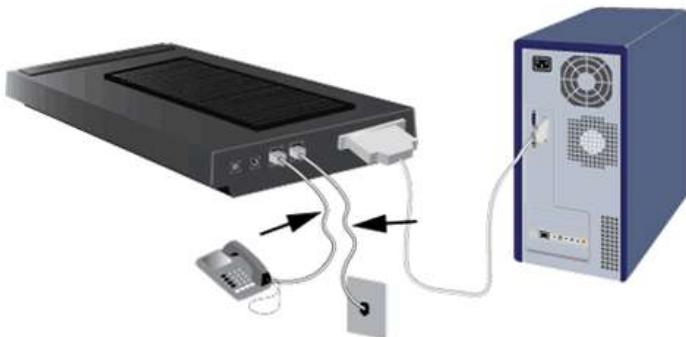
Já em ambientes corporativos os roteadores podem assumir outros papéis, atuando como gateways e servindo como ponto de conexão de diferentes tipos de interfaces e tecnologias. Por exemplo, uma empresa que utiliza telefonia IP normalmente precisa, além dos canais de voz que trafega via rede, de uma conexão 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.

#### 5.3.8 Modem e CSU/DSU

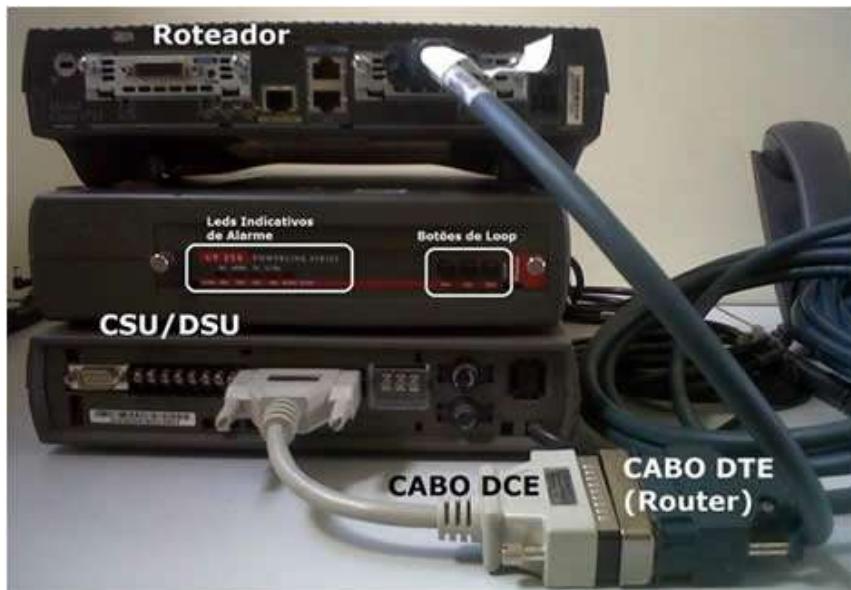
O modem é o dispositivo eletrônico utilizado para a conversão entre sinais analógicos e digitais. A palavra tem como origem as funções de **modulação** e **demodulação**. São geralmente utilizados para estabelecer a conexão entre computadores e redes de acesso através de linhas discadas, ou seja, utilizando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



Os modems analógicos atualmente são utilizados para acesso remoto aos 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 a seguir onde temos um CSU/DSU conectado a um roteador.



## 5.4 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.

### 5.4.1 Firewall

“Firewall” 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.



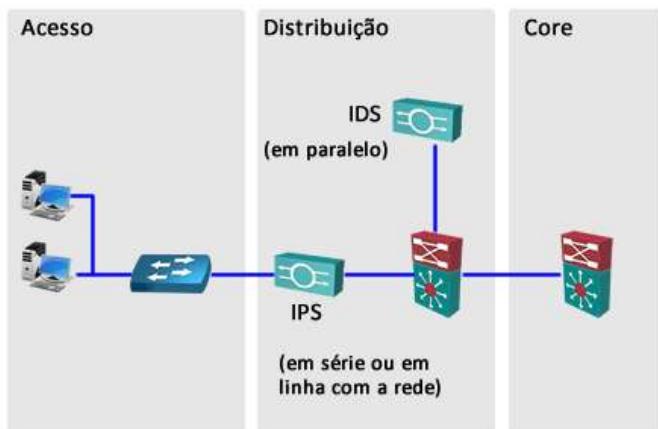
Vamos ativar um dos recursos que o firewall pode utilizar para fazer filtragem nos roteadores chamado “ACL” ou listas de controle de acesso, as quais verificam o tipo de tráfego que está entrando na rede e filtram conforme configuração realizada.

Normalmente eles são posicionados entre a rede interna da empresa e a Internet, fazendo a filtragem do tráfego que entra e sai da empresa por motivos de segurança ou até mesmo regras de acesso conforme política de segurança.

Outra aplicação é a de isolar servidores que precisam estar expostos na Internet, criando uma zona desmilitarizada ou DMZ (Demilitarized Zone), permitindo que determinados serviços e servidores sejam acessados por usuários da Internet.

### 5.4.2 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.

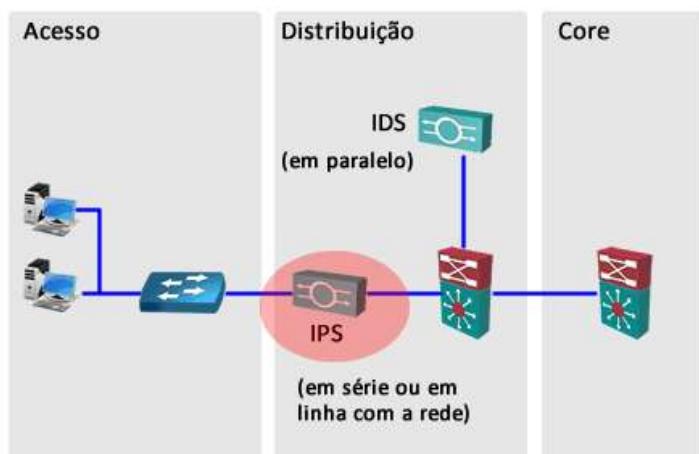


Os IDSs são ligados em paralelo com a rede, escutando todo o tráfego e emitindo alertas para os administradores de rede. Aqui vem “o segredo”, descobrir o que é realmente uma invasão ou não. Pode ocorrer uma invasão e ela não ser detectada, o que é chamado de um **falso negativo** ou então um determinado 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.

#### 5.4.3 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.

#### 5.4.4 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 (cavalos 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.



## 6 Resumo do Capítulo

Bem pessoal, chegamos ao final do capítulo. É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Conseguir diferenciar os tipos de redes LAN, MAN e WAN.
- Entender e diferenciar comutação por circuitos e comutação por pacotes.
- Listar os principais tipos de topologia física de rede.
- Diferenciar os tipos de equipamentos em uma rede de computadores.

- Entender o Modelo OSI e suas camadas.
- Conseguir explicar as principais características de cada camada, seus principais protocolos e exemplos de equipamentos.
- Saber diferenciar e utilizar os diferentes tipos de cabos (direto, cruzado e rollover).
- Conseguir montar uma topologia de rede no simulador Packet Tracer (laboratório).

Lembrem-se, o seu objetivo nesse treinamento é estar preparado para ser aprovado na Prova de Certificação CCENT da Cisco e se tornar um profissional qualificado para o mercado de trabalho. Por isso, não prossiga para o capítulo seguinte até ter esse conhecimento bem afiado.

*Nesse capítulo iremos aprofundar nosso estudo em alguns conceitos que se aplicam a redes LAN.*

*Estudaremos com mais detalhes algumas características funcionais de redes LAN, veremos as configurações básicas dos switches Cisco, aprenderemos o conceito de Virtuais LAN (VLAN) e do protocolo Spanning Tree.*

*Esperamos que você aproveite o capítulo e aprenda bastante!*

## **Capítulo 03 - Redes LAN e Switches**

### **Objetivos do Capítulo**

Ao final desse capítulo você terá estudado e deverá compreender:

- Entender o funcionamento de uma rede full-duplex e half-duplex.
- Entender o processo do CSMA/CD no controle de colisões.
- Conseguir explicar a relação entre hub/bridge/switch e domínios de colisão.
- Diferenciar os três meios de encaminhamento de quadro em um switch (Cut through, Fragment Free e Store and forward).
- Ter uma noção das configurações básicas que podemos realizar em um switch Cisco (banners, telnet, portas e vlan).
- Entender o que é uma VLAN e como elas segmentam domínios de broadcast.
- Entender a utilidade do protocolo spanning-tree na eliminação de loops e tempestades de broadcast.
- Entender o uso da segurança de portas em switches Cisco (Port Security).

## Sumário do Capítulo

<b>1 Revisão do Modelo OSI e Camada 2</b>	<b>61</b>
<b>2 Introdução a Redes Locais – LAN</b>	<b>63</b>
2.1 Comunicação Half-Duplex versus Full-Duplex	64
2.2 Ethernet Half-Duplex	65
2.3 Colisões e Domínios de Colisões	66
2.4 Controle de Colisão Ethernet	67
2.4.1 Detecção de colisão	68
2.5 Ethernet Full Duplex	69
2.6 Segmentando Domínios de Colisão	70
2.7 Entendendo o Funcionamento de uma Bridge	71
2.8 Entendendo o Funcionamento de Switches	72
2.9 Métodos de Comutação	73
<b>3 Padrões e Tecnologias Ethernet</b>	<b>74</b>
3.1 Ethernet 10BASE-T	74
3.2 Fastethernet – 100 Mbps	75
3.3 Gigabit Ethernet – 1.000 Mbps	76
3.4 Conceitos de Infraestrutura de Redes	77
<b>4 Redes Locais Virtuais - VLAN</b>	<b>79</b>
<b>5 Spanning-Tree Protocol - STP</b>	<b>83</b>
5.1 Topologia Comutada Redundante Simples	83
5.2 Usando Bridging Loops para Redundância	83
5.2.1 Tempestade de Broadcast	84
5.3 Protocolo Spanning-Tree	84
5.3.1 Exemplo - Protocolo Spanning-Tree	85
5.4 Resumo Domínio de Colisão x Domínio de Broadcast	87
<b>6 Entendendo e Configurando Switches Cisco Catalyst</b>	<b>88</b>
6.1 Arquitetura Básica de Switches	89
6.2 Introdução ao CLI – Command Line Interface	90

6.3 Formas de Acesso aos Equipamentos	90
6.4 Modos de Execução (Exec) e Privilégios de Acesso	91
6.5 Comando Help do Switch do Modo EXEC Usuário	92
6.6 Navegando pelo CLI	94
6.7 Outros Recursos de Navegação e Edição via CLI	96
6.8 Comando Show Version	97
6.9 Conteúdo Default da Memória Flash	98
6.10 Reinicialização e Voltando às Configurações de Fábrica	98
6.11 Configurações Padrões em Switches de Acesso	99
6.12 VLANs Padrões em Switches Cisco Catalyst	101
6.13 Configurações Básicas – Hostname, Senhas e IP de Gerenciamento	102
6.14 Configuração do Modo Duplex e Velocidade das Portas	103
6.15 Serviços de HTTP e HTTPS	103
6.16 Verificando a Tabela de Endereços MAC	104
6.17 Exemplo de Análise de Tabela MAC Avançado	106
6.18 Salvando e Verificando as Configurações do Switch	107
6.19 Configurações Gerais em Switches Cisco – Resumão!	108
<b>7 Resumo do Capítulo</b>	<b>109</b>

## 1 Revisão do Modelo OSI e Camada 2

Antes de iniciar o capítulo vamos rever alguns conceitos sobre o modelo OSI e TCP/IP:

- A Camada de Aplicação fornece a interface para o usuário.
- A Camada de Transporte é responsável pela divisão e gerenciamento das comunicações entre os processos que são executados nos dois sistemas finais.
- Os protocolos da Camada de Rede, como o IP, organizam os dados de comunicação de modo que eles possam viajar através da conexão de rede a partir do host de origem até o host de destino.

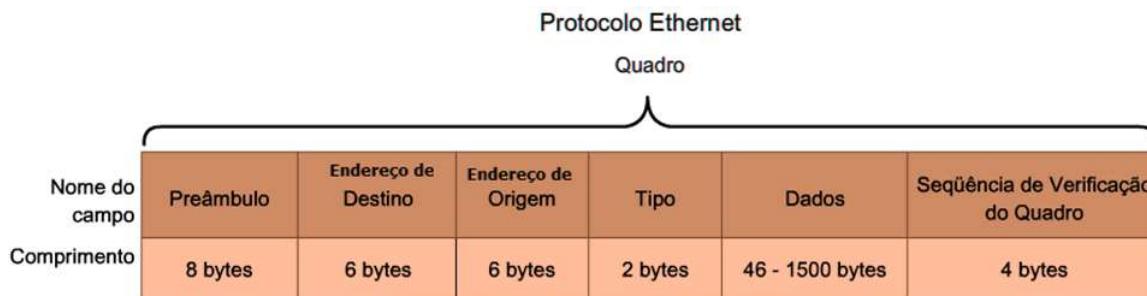
Para que os pacotes da Camada de Rede sejam transportados do host de origem ao host de destino, eles devem atravessar diferentes redes físicas, por diferentes meios físicos de transmissão, por exemplo, podem pegar uma fibra óptica, rádios digitais e até satélites. Essas redes físicas podem ser diferentes e devem ser transparentes para a Camada de Rede, ou seja, para os pacotes IP. Os pacotes da Camada de Rede não têm um caminho para acessar diretamente estes diferentes meios, portanto a Camada de Enlace quem deve desempenhar esse papel.

Portanto, o papel da Camada de Enlace do modelo OSI é preparar os pacotes da Camada de Rede para transmissão no meio físico.

Em uma rede LAN veremos protocolos da família Ethernet (Fastethernet, Gigabit Ethernet ou 10 Gigabit Ethernet), cujo endereço MAC tem papel fundamental, pois redes Ethernet são primordialmente meios compartilhados, ou seja, são utilizados por vários elementos (computadores ou servidores) que desejam se comunicar ao mesmo tempo utilizando o mesmo meio físico.

Portanto, o endereço MAC vai identificar o tipo de comunicação que a camada-3 quer realizar e com quem dentro da mesma rede, pois estamos tratando de redes Locais (LAN).

Veja na figura abaixo o formato do quadro Ethernet da camada-2 e a seguir o que significa cada campo.



- **Preâmbulo** - utilizado para sincronização. Também contém um delimitador para marcar o final da informação cronometrada.
- **Endereço de Destino** - Endereço MAC de 48 bits do nó de destino.
- **Endereço de Origem** - Endereço MAC de 48 bits do nó de origem.
- **Tipo** - valor para indicar que protocolo de camada superior receberá os dados depois que o processo Ethernet for concluído.
- **Dados** - esta é a PDU, normalmente um pacote IPv4, que deve ser transportado pelos meios.
- **Seqüência de Verificação de Quadro** (FCS) - um valor utilizado para verificar quadros danificados.

Mas porque eu preciso saber esse quadro de camada 2? Na realidade é necessário entender o quadro e saber que ele possui dois identificadores que mostram a origem e destino da comunicação, ou seja, quando um computador quer enviar informações a outro em uma LAN ele deve montar um quadro e colocar seu endereço MAC como origem e como destino deve colocar o endereço MAC do computador remoto, o qual ele deseja se comunicar.

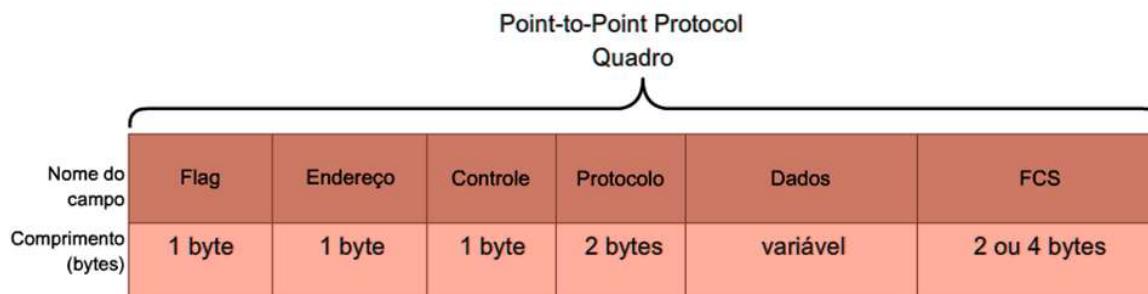
Note que antes de enviar ele também faz uma conta com os bits que serão enviados e coloca o resultado no campo FCS, chamada Check de Redundância Cíclica. Essa conta permite que o receptor saiba se houve erros na transmissão. A família Ethernet não prevê recuperação de erros, ou seja, o receptor recebe um quadro, recalcula o campo FCS, compara com o valor que foi calculado no campo FCS pelo transmissor e aceita ou rejeita o quadro. A recuperação de erros é função das camadas superiores.

Outra informação importante do quadro ethernet é que ele aceita no máximo 1500 bytes de informação, o que é chamado de MTU ou tamanho máximo para transmissão (Maximum Transmission Unit). Se vierem mais que 1500 bytes o receptor irá descartar aquele quadro e incrementar um erro em sua interface.

Para finalizar o estudo do quadro ethernet veja agora o campo Tipo ou Type, ele traz a informação do protocolo de camada superior que será transportado pelo quadro, por exemplo, o protocolo IP é representado pelo valor 0x0800 e o IPv6 é representado pelo valor 0x 86DD. O símbolo "0x" indica que os algarismos estão escritos em Hexadecimal.

Portanto, a troca de quadros é realizada dentro de uma mesma rede LAN, com finalidade de formar um link local entre dois dispositivos!

Nas redes WAN redes ponto a ponto, o endereçamento é uma sequência fixa de valores pelo simples fato de que não há um terceiro elemento, ou seja, sempre os mesmos dois equipamentos conversam entre si e não há necessidade de identificação. Na figura abaixo temos um exemplo de um quadro do protocolo PPP para ilustrar a diferença.



- **Flag** - Um único byte que indica o início ou final de um quadro. O campo flag consiste na sequência binária 01111110.
- **Endereço** - Um único byte que contém o endereço de transmissão PPP padrão. O PPP não designa endereços individuais de estações.
- **Controle** - Um único byte que contém a sequência binária 00000011, que pede pela transmissão dos dados do usuário em um quadro não sequenciado.
- **Protocolo** - Dois bytes que identificam o protocolo encapsulado no campo de dados do quadro. Os valores mais atualizados do campo protocolo estão especificados em números designados - Request For Comments (RFC).
- **Dados** - Zero ou mais bytes que contêm o datagrama do protocolo especificado no campo de protocolo.
- **Sequência de Verificação de Quadros** (FCS) - Normalmente 16 bits (2 bytes). Por acordo anterior, o consentimento com as implementações PPP pode utilizar um FCS de 32 (4 bytes) para detecção de erros melhorada.

No caso de um quadro PPP, por ser ponto a ponto e ter apenas um vizinho o campo de endereço é fixo, pois ele não tem outra opção de envio de quadros.

Quando tratarmos de redes WAN mais especificamente você verá que o Frame-relay utiliza para identificar seus circuitos um endereço de camada 2 chamado DLCI ou Data Link Circuit Identifier, o qual permite criar circuitos virtuais entre dois pontos para que haja comunicação bidirecional.

Mas para que realmente o quadro é utilizado? A resposta é simples, imagine uma sequência de bits sendo recebida por um computador: 01111110111100001110101010111000111101... É assim que dois computadores se comunicam, com esse "trem" ou sequência de bits. Como ele vai identificar se isso é realmente para ele? O quadro permite que essa informação seja decodificada, ou seja, dá sentido ao "monte de bits" recebidos.

Vamos analisar novamente a sequência de bits:

- **0111110**111100001110101010111000111101...

Note que o início identificamos o preâmbulo ou flag, portanto sabemos o que vem na sequência e podemos ler e identificar os campos! O que é feito a seguir pelo computador?

Ele analisa o MAC de destino e compara com seu próprio MAC, se for igual ele lê o quadro, pega o payload ou dados e passa para a camada superior, ou seja, passa o pacote IP para a camada de Internet! Nada mais que o processo de desencapsulamento de dados que estudamos no capítulo anterior.

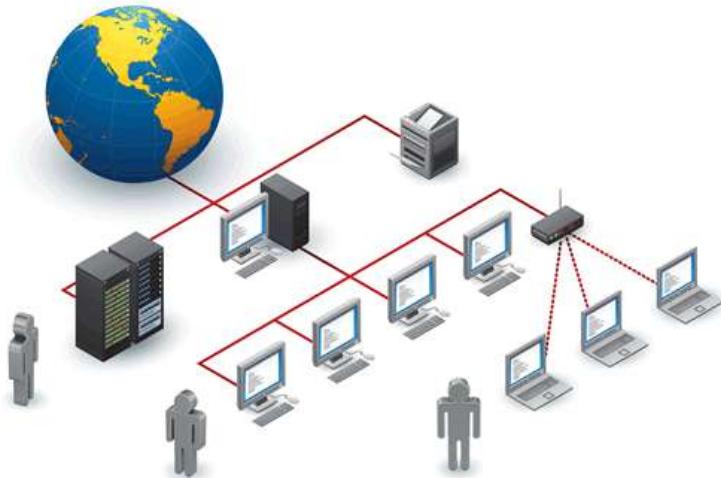
## 2 Introdução a Redes Locais – LAN

Como vimos no capítulo anterior redes LAN são redes locais. Uma Rede Local (LAN) é um conjunto de estações de trabalho em uma área geográfica restrita: para um grupo de trabalho, departamento e/ou organização.

Normalmente as Redes Locais se restringem a um prédio ou, no máximo, a uma área de prédios, muitas vezes chamada de Rede Campus.

As redes LAN normalmente operam em curtas distâncias e altas taxas de transmissão:

- Ethernet 10Mbps
- Fastethernet 100Mbps
- Gigabit Ethernet 1000Mbps ou 1Gbps
- 10 Gigabit Ethernet 10Gbps



Normalmente a rede LAN é composta por um cabeamento de Backbone ou Vertical, o qual faz a conexão entre os equipamentos de rede utilizando Fibra Óptica ou par metálico, e um cabeamento Horizontal, o qual conecta os endpoints (computadores e servidores) à rede.

Podemos ainda ter redes LAN sem fio da família 802.11, porém devido a existência de certificação específica para redes sem fio esses conceitos foram retirados com a última revisão do CCENT/CCNA Routing and Switching.

As LANs atualmente são construídas utilizando switches, porém por questões históricas e didáticas também estudaremos redes baseadas em HUBs. Abaixo seguem fotos de switches da linha Catalyst da Cisco.



## 2.1 Comunicação Half-Duplex versus Full-Duplex

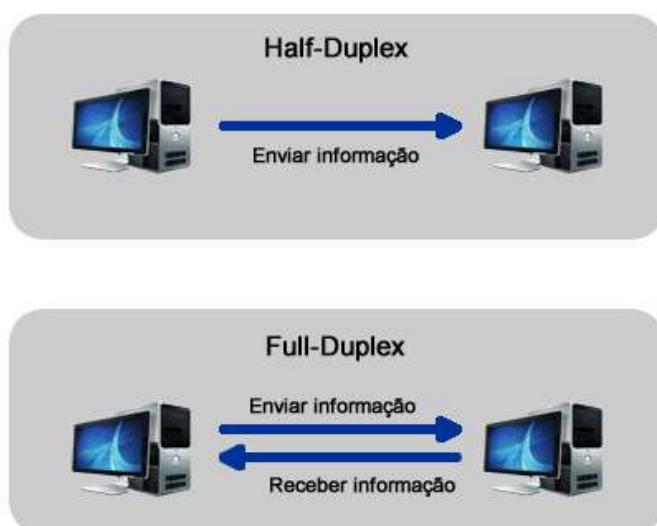
Vamos agora ver a diferença entre os dois tipos de comunicação Ethernet – Half-duplex e Full-duplex, ou seja, o funcionamento de redes com HUBs e Switches.

Quando um dispositivo opera em modo half-duplex significa que ele pode transmitir e receber dados, mas uma coisa de cada vez. É o oposto do modo full-duplex, onde existem dois canais de comunicação separados e o dispositivo pode enviar e receber simultaneamente.

A principal diferença entre os dois modos é o desempenho.

Por exemplo, considere uma rede de 100 megabits operando em modo half-duplex. Como existe um canal único de 100 megabits, usado tanto para transmitir quanto para receber nunca um dispositivo conseguirá executar as duas atividades simultaneamente. O canal é dividido e é possível (em situação ideal) no máximo enviar 50 megabits e receber 50 megabits.

Já em uma rede full-duplex, existem dois canais de 100 megabits separados e o dispositivo poderia enviar 100 megabits e receber mais 100 megabits, ao mesmo tempo. Os dois canais não podem ser somados para apenas enviar ou apenas receber. Ou seja, quando é necessário apenas enviar dados, a transmissão continua sendo feita a apenas 100 megabits. O modo full-duplex representa ganho de desempenho apenas quando é necessário fazer as duas coisas simultaneamente. Veja a figura a seguir representando ambos os modos de transmissão.



Em redes half-duplex se dois dispositivos enviam informações ao mesmo tempo ocorre uma colisão, ou seja, duas ondas eletromagnéticas colidem e uma nova forma de onda é criada com a “soma” das duas ondas originais. Nesse exemplo a informação enviada por ambos os dispositivos é deformada e perdida! Isso ocorre porque em redes half-duplex apenas um par metálico é utilizado no cabo UTP tanto para transmissão como para recepção.

Em redes full-duplex esse problema não ocorre porque são utilizados dois pares, um para transmissão e outro par separado para a recepção, portanto não há possibilidade de ocorrer colisões.

Vamos estudar a seguir que os dispositivos que utilizam tecnologias da família Ethernet utilizam um protocolo chamado CSMA/CD (Carrier Sense Multiple Access with Collision Detection) para lidar com os efeitos da colisão em redes half-duplex.

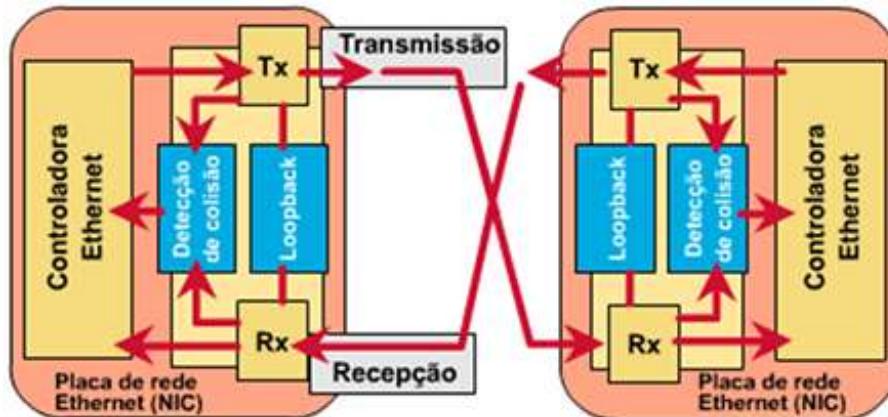
## 2.2 Ethernet Half-Duplex

O modo de comunicação half duplex permite que dois ou mais dispositivos se comuniquem entre si, mas apenas um dispositivo por vez, pois utilizam o mesmo meio físico para transmissão e recepção. Logo, se dois ou mais dispositivos tentarem se comunicar ao mesmo tempo ocorrerá uma colisão dos sinais.

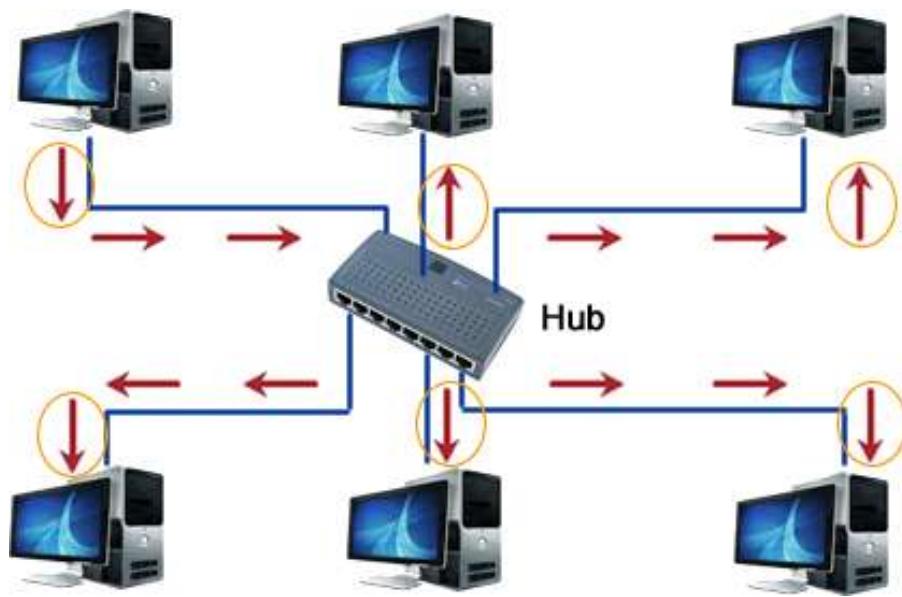
Um exemplo de redes Half-duplex são as LANs implementadas com Hub's.

Os Hub's são equipamentos situados na camada física do modelo OSI, ou seja, não analisam os quadros ou pacotes recebidos. Funcionando de maneira similar a um “Curto-circuito”, ou seja, os hub's encaminham o que recebem em uma porta para todas as demais portas. Esse é o motivo de poder haver colisões em redes Half-duplex, pois os equipamentos transmitem e recebem em apenas um par metálico.

Quando uma porta é configurada como half-duplex um circuito de detecção de colisão é ativado, acionando a escuta por sinais de colisão e o algoritmo do CSMA/CD, conforme figura a seguir.



Note na figura ao lado que o micro do canto superior esquerdo está transmitindo um sinal no meio de transmissão. Ao receber o sinal o hub irá propagá-lo para todas as portas e todos os outros micros da rede irão receber esse sinal.



**Lembrete:** A camada física define as especificações elétricas, mecânicas, funcionais e de procedimentos para ativar, manter e desativar o link físico entre sistemas finais. Características como níveis de voltagem, distâncias máximas de transmissão, conectores físicos são definidas pelas especificações da camada física.

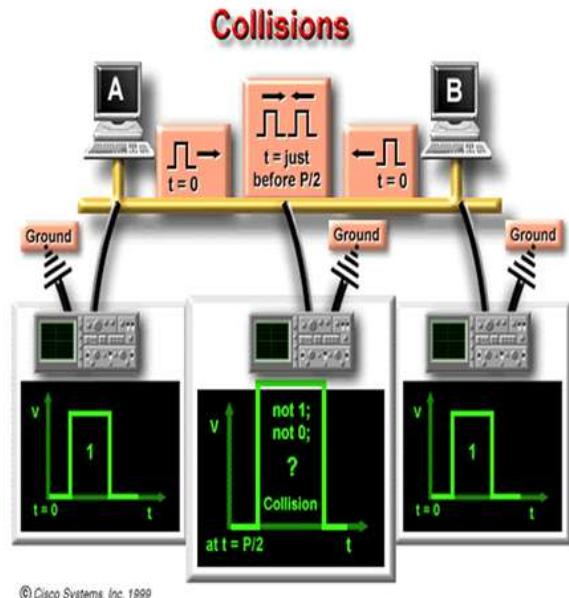
A camada física tem como função básica a adaptação do sinal ao meio de transmissão. Nessa camada estão situados os Hubs, repetidores, transcievers, patch panel, cabos e conectores.

### 2.3 Colisões e Domínios de Colisões

Uma colisão acontecerá toda vez que dois bits se propagarem ao mesmo tempo e no mesmo meio físico.

Lembrem-se de um princípio muito conhecido na física que dois corpos não podem ocupar o mesmo lugar no mesmo espaço de tempo. O mesmo vale para sinais elétricos em redes de comunicações - dois sinais não podem ocupar o mesmo meio físico ao mesmo tempo.

Perceba na figura abaixo que o dispositivo A está enviando um sinal elétrico no meio de transmissão de amplitude 1. E ao mesmo tempo o dispositivo B também envia o sinal de amplitude 1 no meio.



Logo, haverá uma colisão dos sinais no meio de transmissão e os dispositivos que estiverem "ouvindo" o meio não irão reconhecer nem o sinal 0 e nem o sinal 1. Isso é o que chamamos de colisão em meios de transmissão.

Esse comportamento descrito anteriormente traz o conceito de “**Domínio de Colisão**”. Um domínio de colisão é a área onde os pacotes originados podem sofrer colisão. Portanto, se temos um Hub de 24 portas, o domínio de colisão dos computadores conectados a esse Hub são as 24 portas do Hub.

Se estendermos essa rede conectando na porta 24 do primeiro Hub um segundo Hub de 48 portas teremos um domínio de colisão de 24 mais 48 portas, um total de 72 portas, pois o primeiro computador conectada na primeira porta do primeiro Hub pode colidir com bits enviados pelo computador conectado à porta 48 do segundo switch!

Redes compostas somente por Hubs geram domínios de colisão do tamanho da soma de todas as portas dos hubs interconectados. O que isso pode causar em uma rede com muitas portas em hubs cascataeados (ligados em série uns com os outros)? Lentidão! Haverão tantas colisões que simplesmente pode parar a rede!

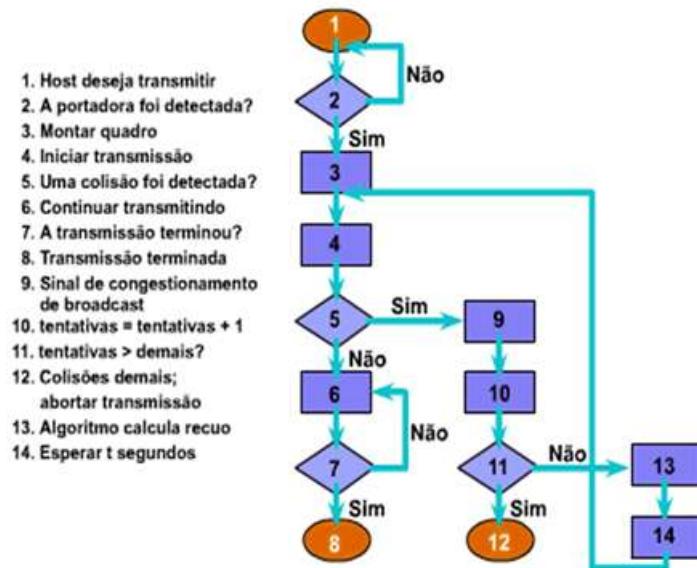
## 2.4 Controle de Colisão Ethernet

Como estudamos anteriormente, se dois dispositivos tentarem se comunicar ao mesmo tempo em redes half-duplex haverá uma colisão dos sinais. Essa colisão irá degradar o sinal, de forma que os dispositivos envolvidos não conseguirão entender o sinal e a comunicação irá falhar.

Para evitar que esse processo ocorra a ethernet lançou mão de um controle de colisão no meio, chamado de CSMA/CD (Carrier Sense Multiple Access with Collision Detection), o qual dita as seguintes regras para utilização do meio físico compartilhado:

- Todos os hosts que estiverem no sistema devem escutar o meio físico para detectar se existe uma estação transmitindo.
- A transmissão só deve ocorrer se a portadora (sinal sendo transmitido) não é detectada.
- Se mesmo assim duas estações tentam transmitir ao mesmo tempo, ocorre uma colisão.
- Detectada a colisão espera-se um tempo aleatório para retransmissão aleatória (algoritmo de backoff) para reiniciar a transmissão.

## CSMA/CD Ethernet



A sigla CSMA/CD significa, em inglês, carrier-sense multiple access with collision detection (acesso múltiplo com detecção de portadora e detecção de colisão) descreve como o protocolo de Ethernet regula a comunicação entre os nós de uma rede. A expressão pode intimidar, mas se analisarmos os conceitos de seus componentes, separadamente, vamos ver que ele descreve regras muito similares àquelas que as pessoas utilizam em conversações civilizadas. Para ajudar a ilustrar a operação da Ethernet, vamos usar uma analogia: uma conversação à mesa de jantar.

Nosso segmento Ethernet é a mesa de jantar, e os nós são as pessoas conversando educadamente. A expressão múltiplo acesso (multiple access) fala sobre o que acabamos de discutir. Quando uma estação de Ethernet transmite, todas as estações no meio ouvem a transmissão. Da mesma maneira que quando uma pessoa fala, todo mundo escuta.

Agora vamos imaginar que você esteja à mesa e tenha alguma coisa a dizer. No momento, entretanto, existe uma pessoa falando. Já que essa é uma conversação educada, em vez de imediatamente falar e interromper o outro você espera até que ele termine de falar. Na terminologia da Ethernet, esse processo se chama carrier sense (detecção de portadora). Antes de uma estação começar a transmitir, ela "ouve" o meio para saber se outra estação está transmitindo. Se o meio estiver em silêncio, a estação reconhece que esse é o momento apropriado para transmitir.

#### **2.4.1 Detecção de colisão**

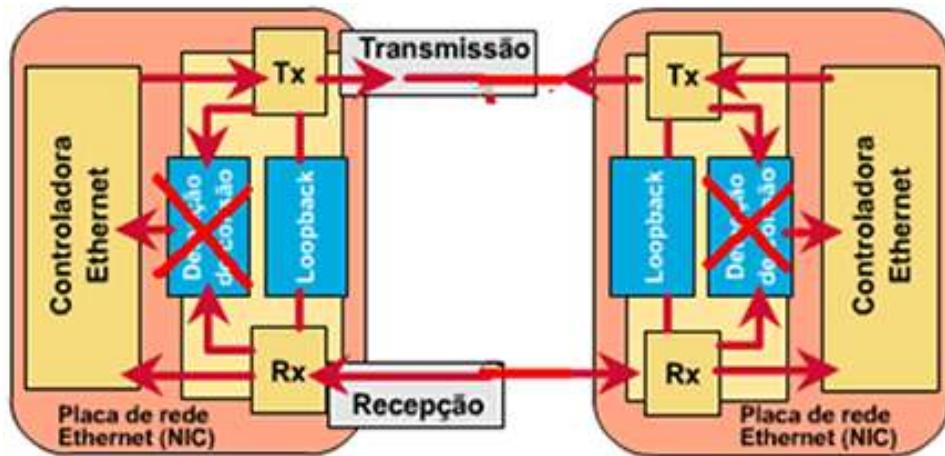
O acesso de múltiplos dispositivos de rede é uma boa maneira de começarmos a explorar as limitações da Ethernet, mas existe outro cenário que ainda temos de analisar. Vamos criar uma analogia da mesa de jantar e imaginar que existe um silêncio momentâneo na conversação. Você e eu temos coisas a falar e ambos sentimos o "peso do silêncio". Para resolver isso, começamos a falar quase ao mesmo tempo. Na terminologia da Ethernet, ocorre uma colisão quando os dois tentam falar ao mesmo tempo.

Em nosso caso, podemos resolver a situação de maneira civilizada. Após a percepção de que estávamos falando ao mesmo tempo, um de nós para de falar para escutar o outro. Os nós da Ethernet também escutam o meio enquanto transmitem, para ter certeza de que são a única estação transmissora naquele momento. Se as estações começam a ouvir sua própria transmissão de forma distorcida ou misturada com a de outra estação sabem que uma colisão aconteceu. Às vezes, um segmento de Ethernet é chamado de domínio de colisão porque duas estações no segmento não podem transmitir ao mesmo tempo sem causar uma colisão. Quando as estações detectam uma colisão, elas interrompem a transmissão, esperam durante um período aleatório e tentam transmitir novamente quando detectam silêncio no meio.

A pausa aleatória e a repetição do envio do sinal representam parte importante do protocolo. Se as duas estações colidem quando estão transmitindo, então ambas terão de transmitir novamente. Na próxima oportunidade de transmissão, as estações envolvidas na colisão anterior terão dados prontos para transmitir. Se elas transmitissem novamente na primeira oportunidade, colidiriam de novo. Por isso existe um tempo de espera aleatório. Assim, dificilmente as duas estações vão continuar colidindo por muito tempo.

## 2.5 Ethernet Full Duplex

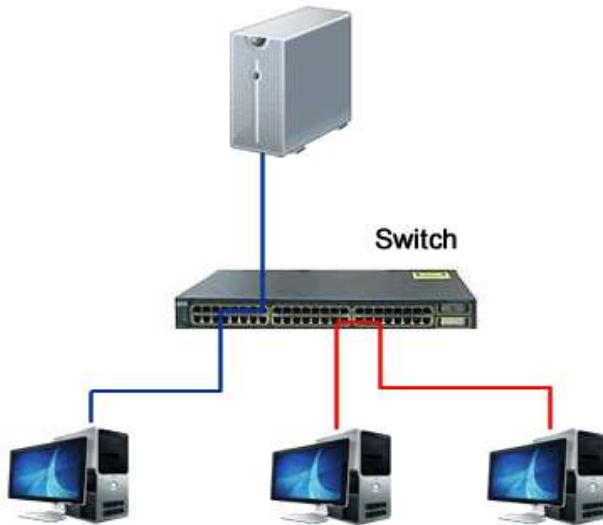
O modo de comunicação full-duplex utiliza dois pares de fio no cabo de rede UTP e permite que dois ou mais dispositivos se comuniquem entre si e ao mesmo tempo, ou seja, simultaneamente. O full-duplex duplica a quantidade de throughput no enlace e é livre de colisões. Hubs não tem essa capacidade, apenas os switches.



Em redes full-duplex as portas transmitem e recebem em dois pares, ou seja, podem transmitir e receber dados simultaneamente. As conexões são fechadas pelo switch em caminhos virtuais sem o risco de colisão, processo chamado microssegmentação.

A velocidade aumenta substancialmente e a segurança é naturalmente melhorada por não ter o risco de um usuário capturar pacotes de outros usuários.

Note na figura ao lado que o switch fecha o caminho para a comunicação entre cada par de dispositivo.



Dessa forma, cada par de dispositivo tem seu próprio "circuito" de comunicação e um não interferirá no meio do outro.

**Lembrete:**

A camada de enlace proporciona trânsito confiável de dados através de um enlace físico. A camada de enlace está relacionada:

- Endereçamento físico (MAC)
- Topologia lógica de rede
- Forma de acesso aos meios
- Notificação de erros (FCS)

Os dispositivos de rede que atuam na camada 2 são bridge, switch e placa de rede (NIC).

## 2.6 Segmentando Domínios de Colisão

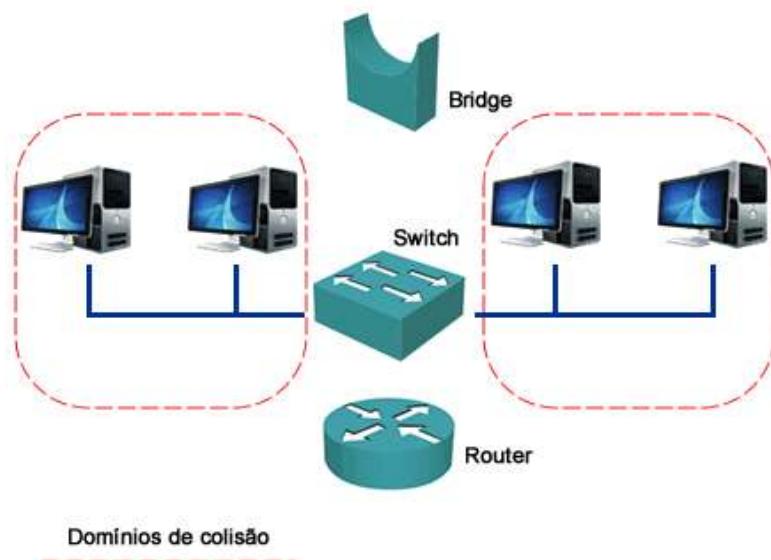
Para entendermos o conceito de segmentação de rede vamos voltar a nossa analogia da mesa. Se na mesa existem poucas pessoas, se tiver só uma pessoa falando de cada vez não chega a causar tantos problemas de comunicação. Mas o que aconteceria se fosse muita gente reunida e só um pudesse falar?

Na prática, sabemos que essa analogia gera situações como a que veremos a seguir. Em grandes grupos de pessoas, é normal que aconteçam diferentes conversas simultaneamente. Se, em uma sala lotada somente uma pessoa pudesse falar a qualquer momento, muitas pessoas ficariam frustradas esperando um momento para falar.

Para os humanos, o problema se corrigiria automaticamente: O alcance da voz humana é limitado e o ouvido consegue focar em uma conversa específica mesmo que esteja em um ambiente barulhento. Por isso, é comum que existam diversas conversas simultâneas em uma mesma sala. Isso não acontece com os cabos de rede, já que eles conseguem carregar sinais rapidamente e de forma eficiente por longas distâncias.

As redes Ethernet enfrentaram problemas de congestionamento ao ficarem maiores. Se há um grande número de estações conectadas a um mesmo segmento e cada uma gera uma quantidade considerável de tráfego, muitas estações tentarão transmitir assim que houver uma oportunidade. Nessas circunstâncias, as colisões se tornariam mais frequentes e poderiam prejudicar outras transmissões, que levariam mais tempo para ser concluídas.

Um jeito de reduzir os congestionamentos seria dividir cada segmento em múltiplos segmentos e assim criar múltiplos domínios de colisão.



Para segmentar domínio de colisão podemos utilizar bridges ou switches. Abaixo seguem algumas informações sobre domínios de colisão:

- Redes com HUBs → domínio de colisão único.
- Segmentação → diminui domínio de colisão
- Bridges e switches → segmentam domínios de colisão.
  - Filtram o tráfego baseado no endereço físico da estação
  - Tráfego pesado -> bridge se torna gargalo

Mas o que significa "segmentar" uma rede? É colocar um dispositivo que tenha a capacidade de aprender os endereços físicos dos computadores e demais dispositivos de rede conectados a ele e fazer a filtragem das informações com base nessa "tabela de endereços MAC".

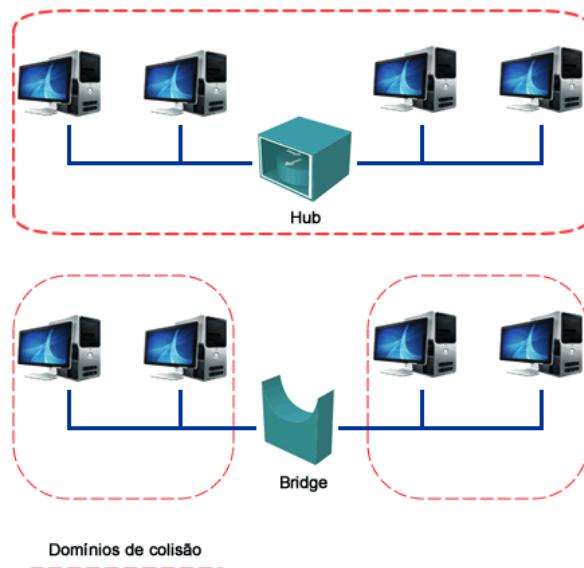
Por exemplo, temos um Hub conectado na porta 1 de um switch com os computadores A e B, já na porta 2 desse switch temos um segundo Hub com os micros C e D conectados. Nessa topologia o switch aprenderia esses endereços e quando o computador A quisesse falar com o B ele não encaminhará esse quadro para a porta 2. Isso se chama filtragem.

## 2.7 Entendendo o Funcionamento de uma Bridge

Uma Bridge ou ponte é um dispositivo que liga duas redes que usam protocolos distintos ou dois segmentos da mesma rede que usam o mesmo protocolo, por exemplo, em redes ethernet ou token ring.

Uma bridge ignora os protocolos utilizados nos dois segmentos de rede que interliga, já que opera na camada 2 do modelo OSI, enviando dados de acordo com o endereço do quadro de camada 2. Este endereço não é o endereço IP (internet protocol), e sim o endereço MAC (Media Access Control) que é único para cada placa de rede.

Os únicos dados que são permitidos atravessar uma bridge são dados destinados a endereços válidos no outro lado da ponte. Desta forma é possível utilizar uma bridge para manter um segmento da rede livre dos dados que pertencem a outro segmento.



Informações adicionais sobre bridges:

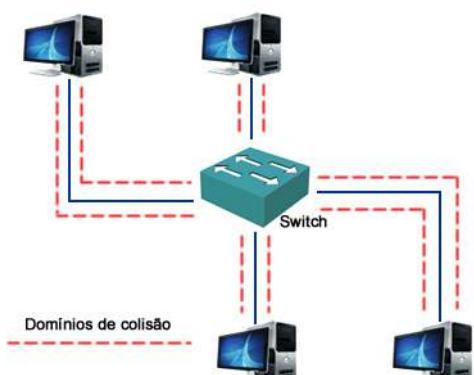
- Possuem duas portas e operam na camada 2, aprendendo endereços de origem e fazem o processo de filtragem.
- Dispositivos de comutação e segmentação de domínios de colisão.
- Adicionam latência na rede (tornam a rede mais lenta) por tomarem decisões baseadas em software.
- Utilizam a comutação de armazenamento e encaminhamento (Store and forward), ou seja, gravam os quadros inteiros em uma memória temporária, examinam o endereço de destino e o FCS para verificar se tem erro, somente após isso encaminham o quadro.
- Dobra o numero de domínios de colisão.

## 2.8 Entendendo o Funcionamento de Switches

Um switch é um dispositivo utilizado em redes para reencaminhar quadros entre os diversos nós da rede. Assim como os hubs, os switches possuem diversas portas, no entanto, ele segmenta a rede internamente, fazendo com que cada porta corresponda a um domínio de colisão diferente. Isso faz com que não exista a colisão entre os pacotes de segmentos diferentes, ao contrário dos hubs, cujas portas partilham o mesmo domínio de colisão.

O switch opera na camada 2 do modelo OSI (camada de enlace), encaminhando os quadros de acordo com o endereço MAC de destino e sua principal utilização é para a segmentação de redes locais. Podemos dizer que os switches são bridges multiporta.

Atualmente existem switches que operam em conjunto na camada 3 (camada de rede), herdando algumas propriedades dos roteadores (routers).



Algumas características dos switches são:

- Os switches encaminham quadros com base nos endereços de destino da camada 2.
- O switch toma conhecimento desses endereços ao examinar o endereço de destino da camada 2 a medida que recebe os quadros.
- Quando endereço não existe na tabela SAT "CAM", o switch faz flood dele por todas as portas.
- Quando ele tem o endereço MAC de destino do quadro em sua tabela ele faz o encaminhamento do quadro.

As principais funções de switch são:

1) Aprender os MACs dos dispositivos conectados nas portas – mapear MAC versus porta do switch:

- Ao ligar o switch ele não conhece os hosts conectados às portas.
- À medida que os quadros são encaminhados na rede os switches aprendem os MAC's e criam uma tabela relacionando os endereços de camada-2 às portas do switch.
- Quando o switch não conhece o endereço de destino o quadro é encaminhado a todas as portas – processo de flooding.
- O aprendizado dos MACs é realizado através do **endereço MAC de origem** dos quadros quando eles são enviados através das portas do switch.

**Dica:** flooding é uma inundação ou cópia do quadro em todas as portas menos para a porta de origem. Não confunda com broadcast, pois ele tem o MAC de destino ffff.ffff.ffff.

2) Encaminhar ou filtrar quadros entre portas – decisões baseadas no endereço MAC:

- Após a tabela de MACs por porta estar completa, os switches encaminham o quadro ou filtram baseado no endereço de destino.
- Quadros com endereço de destino contendo um endereço de broadcast (ffff.ffff.ffff) ou multicast (inicia com 01:00:5e para IPv4 ou 33:33:33 para o IPv6) são encaminhados para todas as portas menos a porta de origem por padrão.

**Dica:** existem três tipos de comunicação básicas em IPv4 que são Unicast (um para um), Broadcast (um para todos) e Multicast (um para um grupo). Quando dois computadores se comunicam usam Unicast e como endereços de origem e destino seus próprios endereços MAC

gravados na placa de rede. No broadcast utilizam seu MAC de origem e como destino tudo 1 no MAC ou ffff.ffff.ffff. No multicast temos uma comunicação de em grupo, onde todos os hosts usam o mesmo endereço de camada-3 e como MAC se for IPv4 inicia com 01:00:5e e se for um multicast IPv6 o MAC inicia sempre com 33:33:33.

### 3) Evitar Loops utilizando o protocolo Spanning-tree (STP):

- Caminhos redundantes são necessários, porém trazem problemas de loop de camada-2 e o spanning-tree é um protocolo que aprende os caminhos redundantes e evita loops.

As três funções descritas acima resumem a principais funções de um switch camada-2. Muitos alunos ficam se perguntando "Porque um switch filtraria um quadro?", a resposta é simples, é só colocar um HUB em uma das portas que pode haver a necessidade de filtragem se dois computadores conectados ao mesmo HUB tentarem se comunicar.

## 2.9 Métodos de Comutação

Além das características estudadas anteriormente, os switches precisam encaminhar os quadros baseados no endereço MAC de destino do quadro de camada-2.

O primeiro método foi o desenvolvido para as Bridges e suportado até os dias de hoje pelos switches chamados Store and Forward ou, em português, Armazena e Encaminha. Este método é o mais lento de todos, pois exige que o dispositivo armazene o quadro todo, leia o FCS para verificar se tem erros e aí sim encaminhar o quadro. Nas bridges esse método era implementado por software, já nos switches ele é realizado por hardware através de ASICs.

Com o passar do tempo os HUBs começaram a diminuir nas redes e métodos mais rápidos de encaminhamento foram desenvolvidos e chamados de Cut-Through. Esses métodos não leem mais todo o quadro, pois para encaminhar é necessário saber apenas o destino, depois o switch já pode fazer o envio do quadro, portanto esses métodos foram desenvolvidos com essa base.

Como as colisões estatisticamente acontecem até o byte 64 de um quadro ethernet, o primeiro método desenvolvido foi o cut-through chamado "Fragment-free" ou "Livre de Fragmentos". Para isso antes de encaminhar o switch deve ler até o byte 64 do quadro para garantir que não existam "Runts", nome dado aos fragmentos resultantes de colisões.

Com o uso cada vez mais intensivo de switches na rede foi possível o desenvolvimento de um método mais rápido ainda, pois somente com switches não temos mais colisões, chamado de cut-through somente, o qual permite que o switch leia somente até o endereço de destino e já encaminhe o quadro para a porta de destino.

Abaixo segue resumo dos três métodos de comutação são o cut-through, store-and-forward e fragment free. Pode ser configurado em cada porta individualmente.

- **Store-and-forward:** aqui o switch primeiro armazena todo o quadro no seu buffer de memória e depois executa a verificação de erro (FCS) para validar a integridade de todo quadro. Se nenhum erro for encontrado encaminha o quadro para o destino. Possui o maior delay, mas é o método mais confiável.
- **Cut-through:** o switch verifica até o byte 13 do quadro e então aprende o endereço de destino. Logo em seguida começa a encaminhar o quadro. Possui o menor delay, mas é menos confiável pois não faz verificação de erro.
- **Fragment-Free** (cut-throug modificado): nesse método o switch verifica até o byte 64 em busca de erros no quadro. Se não encontra nenhum erro encaminha o quadro para o endereço de destino. Possui um delay um pouco maior, no entanto é mais confiável que o cut-through.

### 3 Padrões e Tecnologias Ethernet

As redes Ethernet fazem parte da família de recomendações da IEEE 802.3 e estão na camada inferior da arquitetura TCP/IP, a qual 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, portanto são tecnologias responsáveis pelo controle do envio dos quadros através do meio físico.

Normalmente as diversas opções dessa família de tecnologias recebe 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.

Os principais meios físicos são os cabos UTP categorias 5e e 6, sendo que a categoria do cabo diz qual a resposta em frequência que o cabo possui e cada um possui conectores e patch panels próprios, ou seja, não se deve misturar categoria 5e com 6, pois considera-se nesse caso que um cabo categoria 6 conectado a um patch panel categoria 5e irá possuir as mesmas características de um 5e, portanto será rebaixado.

Já as fibras ópticas têm as monomodo ou multimodo. O modo é a maneira que a luz irá trafegar dentro de uma fibra óptica, sendo que na monomodo ela trafega em apenas um modo e na multimodo a luz é espalhada pela fibra, portanto as fibras monomodo utilizam lasers como fonte luminosa e permitem conexões com maiores distâncias, já as fibras multimodo podem ser utilizadas com lasers e leds e permitem links mais curtos.

Vamos ver os principais padrões utilizados até os dias de hoje nas redes LAN cabeadas. Não vamos abordar as redes coaxiais.

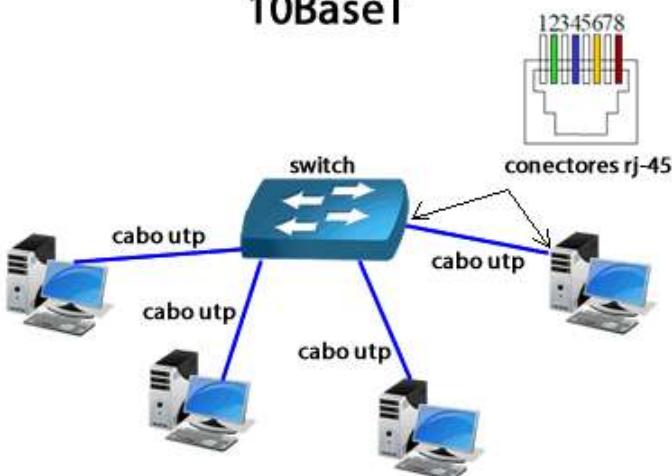
#### 3.1 Ethernet 10BASE-T

O padrão 10BASE-T foi introduzido nos anos 90 e possui as seguintes características:

- Segue o padrão IEEE 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 quando utilizando HUB na camada de acesso.
- 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, com exceção das conexões entre HUBs.
- 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 Gigabit Ethernet, podendo variar apenas o tipo de cabo (categoria).

## 10BaseT



### 3.2 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.

Os principais tipos de conexão a 100 Mbps 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 Gigabit Ethernet 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).
- Utiliza conectores do tipo ST ou SC (veja a figura 1).



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.

### **3.3 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.

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 nano segundo, porém utilizando fibra ótica 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.

#### **10 Gigabit Ethernet**

O novo padrão Ethernet de 10 gigabites 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.

### 3.4 Conceitos de Infraestrutura de Redes

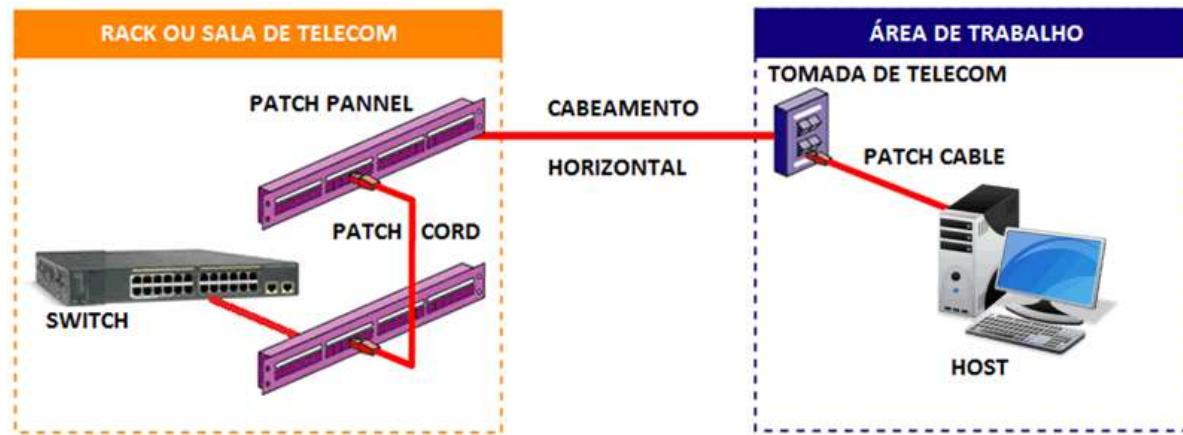
Uma rede LAN é composta basicamente pelo cabeamento horizontal e vertical, sendo que o cabeamento horizontal é o que interliga os hosts (micros, servidores, lap-tops, telefones IP e outros dispositivos de usuário) à rede, basicamente aos Switches e HUBs.

Já o cabeamento vertical é o que chamamos de backbone ou “espinha dorsal” da rede e serve para interligar os diversos elementos de rede, como switches, Access-points, roteadores e demais dispositivos de rede.

Resumidamente, o cabeamento horizontal interliga o host através de um Patch Cord (cabo de rede ou patch cable) a uma tomada de telecomunicações, dessa tomada de telecomunicações um cabo horizontal é encaminhado pela infraestrutura (através de canaletas ou por baixo do piso elevado através de guias) até os patch panels, os quais são terminações que ficam entre os micros e os switches e permitem a manobra dos cabos.

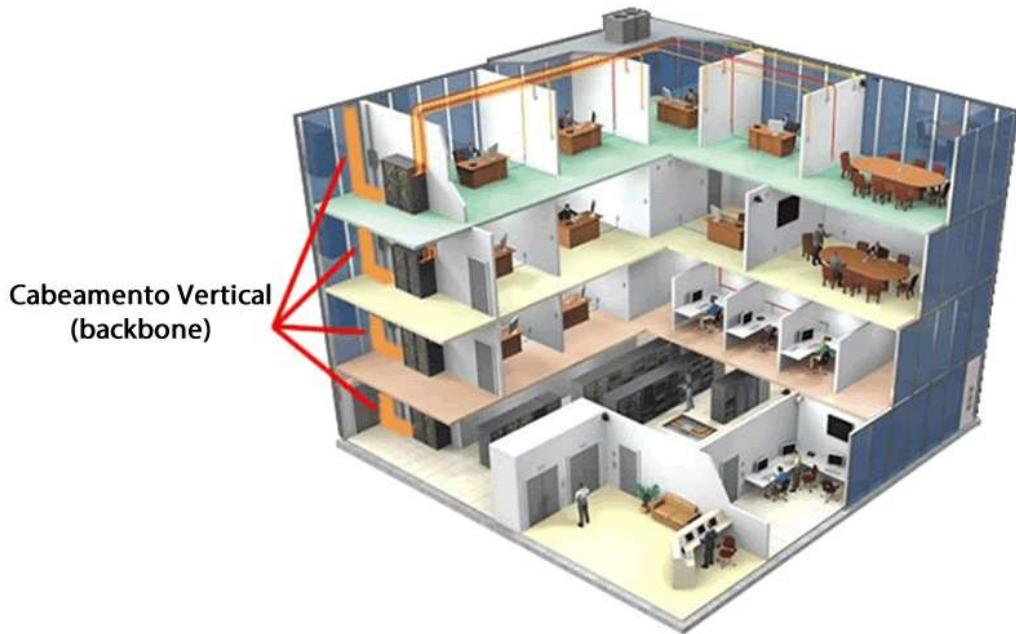
Dos patch panels fazemos a interligação com os switches e finalizamos o cabeamento horizontal. Algumas vezes podemos interligar de um patch panel para outro patch panel intermediário antes de conectar ao switch, porém não é muito recomendado.

Outro ponto importante é que esse caminho do cabeamento horizontal está limitado a 100m, distância padrão das tecnologias Ethernet, Fastethernet e Gigabit Ethernet para cabos metálicos UTP categorias 5e (CAT-5e) e Categoria 6 (CAT-6). Veja na figura a seguir temos um exemplo de cabeamento horizontal.



Já o cabeamento vertical ou backbone é utilizado para interligar os diversos switches até um Datacenter, rack de telecomunicações (wiring closet), sala de servidores ou a uma saída de Internet, normalmente um ponto central onde os hosts (dispositivos dos usuários) tem acesso às demais redes internas ou externas e acesso aos serviços de redes, como um CRM, banco de dados corporativo, dentre outros.

Veja na figura a seguir onde temos um exemplo de cabeamento vertical, os diversos cabeamentos horizontais de cada andar são interligados através de racks com seus switches instalados em racks por andar.



O cabeamento vertical normalmente é realizado por fibra óptica, porém quando está próximo é realizado com par metálico UTP. Existem vários padrões para interligar os switches via fibra e normalmente precisam ser instaladas pequenas interfaces de fibra chamadas GBIC ou "Gigabit Interface Converter".

Cada tipo de padrão tem uma especificação de velocidade e distância máxima do sinal, veja ao lado uma tabela com os principais tipos de padrão e suas respectivas distâncias padrões:

Nome	Meio de transmissão	Distância padrão
1000BASE-CX	Cabo STP	25 metros
1000BASE-SX	Fibra Multimodo	220 a 550 metros dependendo do diâmetro da fibra
1000BASE-LX	Fibra Multimodo	550 metros
1000BASE-LX	Fibra Monomodo	5 km
1000BASE-LX10	Fibra Monomodo com 1,310 nm	10 km
1000BASE-ZX	Fibra Monomodo com 1,550 nm	acima de 70 km
1000BASE-BX10	Fibra Monomodo, porém utilizando apenas uma fibra: 1,490 nm downstream 1,310 nm upstream	10 km
1000BASE-T	Par trançado UTP (Cat-5, Cat-5e, Cat-6 ou Cat-7)	100 metros
1000BASE-TX	Par trançado UTP (Cat-6, Cat-7)	100 metros

Portanto, para utilizar um switch com interface de fibra você terá que escolher uma GBIC, de acordo com um dos padrões da tabela ao lado, e cada padrão tem um conector específico. Veja a figura a seguir.



Uma rede com fibra precisa também de emendas, as quais são feitas de maneira especial para interligar a fibra a um painel de conexão ótica que terá a ponta de um conector onde você irá interligar um cabo chamado "pigtail" do switch a esse painel óptico (patch panel óptico), veja a figura abaixo.



#### 4 Redes Locais Virtuais - VLAN

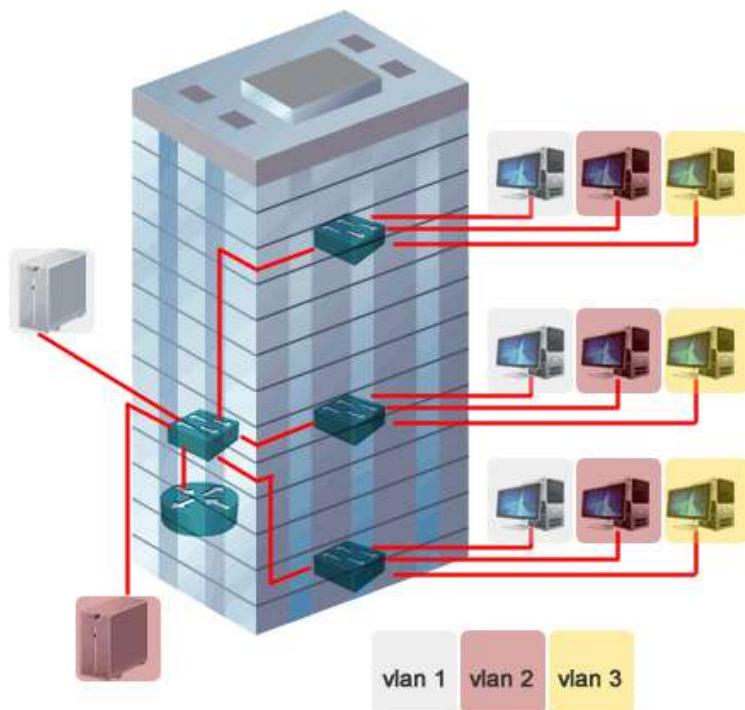
Até o momento estudamos como segmentar domínios de colisão utilizando switches ou bridges, porém esses dispositivos não conseguem segmentar domínios de broadcast.

Os broadcasts são mensagens enviadas para o endereço específico de camada 2 “ffff.ffff.ffff”, ou seja, todos os bits do endereço MAC em 1. Quando um broadcast é enviado na rede todos os dispositivos devem processar essa informação e também os switches devem encaminhar esses quadros para todas as portas.

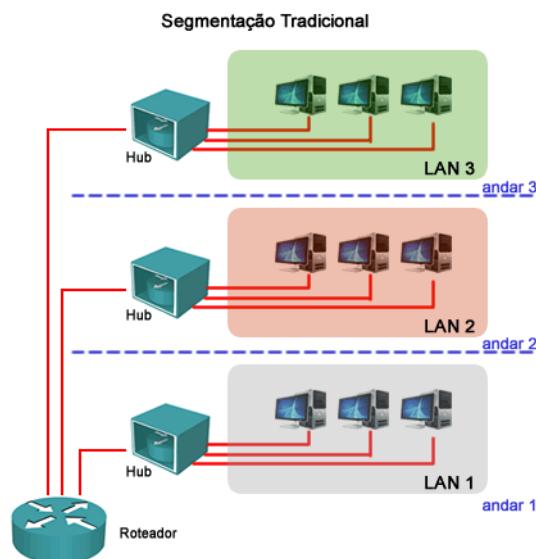
Em uma topologia de rede simples onde existem apenas switches ethernet de camada 2 possuímos apenas um domínio de broadcast. Isso significa que, todos os dispositivos conectados aos switches, receberão os pacotes de broadcast.

Isso em uma rede com poucos dispositivos, não é problema, mas quando aumentamos a quantidade de dispositivos conectados, passa a ser um problema.

Para solucionar foi criada a técnica conhecida como VLAN, utilizada para a segmentação de redes. O termo VLAN (Virtual LAN) refere-se a criação de LAN's virtuais em um mesmo equipamento ou pilha de equipamentos de rede. Com isso os pacotes de broadcast só são recebidos pelos dispositivos com portas alocadas na mesma VLAN.



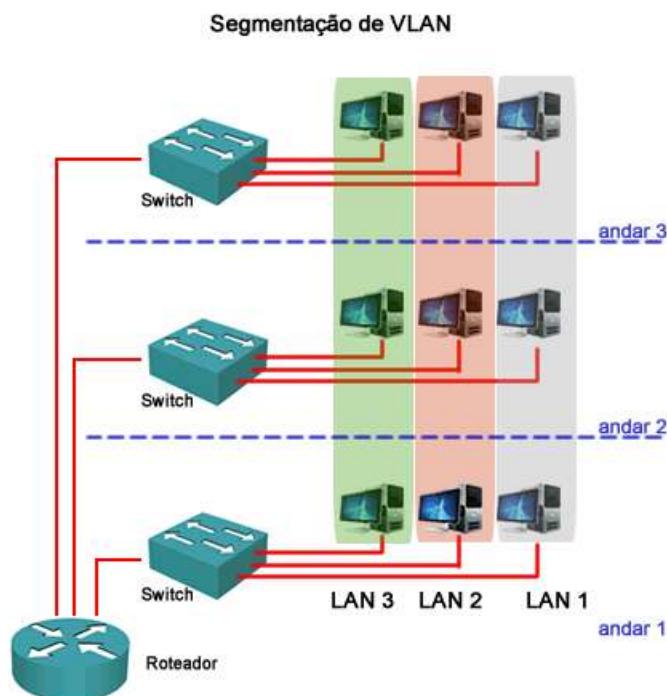
Em LAN's tradicionais os agrupamentos são por proximidade, de acordo com a infraestrutura física que ela está conectando, conforme figura a seguir.



Com VLAN's isso passa a ser independente, pois podemos agrupar dispositivos de maneira lógica.

O agrupamento de usuários fisicamente distantes tem sido cada vez mais exigido. Com a utilização de VLANs os agrupamentos lógicos de dispositivos ou usuários passam a ser realizados por função, departamento ou aplicativo, não mais importando a localização de seus segmentos físicos.

As VLANs são realizadas nos switches através de software e por não serem padronizadas, requerem o uso de software proprietário.



As implementações antigas de VLAN, possuíam recursos limitados e valiam para um dispositivo (somente um switch). Atualmente os recursos de VLAN cobrem a rede inteira, sendo distribuídos entre diversos switches e até mesmo através de WAN's.

Nos dias atuais, os agrupamentos de usuários seguem associação lógica e não mais física.

Mas como funciona uma VLAN na prática? É relativamente simples:

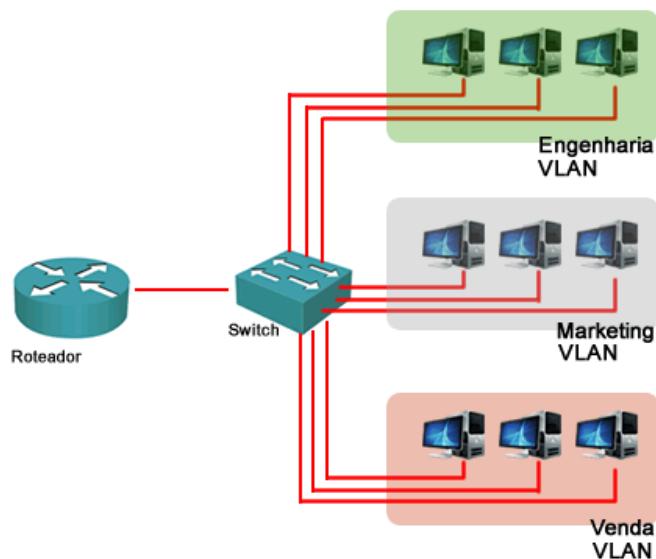
1. Criamos identificadores chamados de VLAN-ID, por exemplo, as VLANs 1, 2 e 3.
2. Depois vinculamos as portas do switch a uma dessas VLANs criadas, por exemplo, em um switch de 24 portas vinculamos das portas 1 a 10 à VLAN1, de 11 a 15 à VLAN2 e as demais à VLAN 3.
3. Pronto, agora os computadores que foram colocados na VLAN 1 não se comunicam mais com os que estão na VLAN 2.

Mas como fazemos para que as VLANs se comuniquem? Utilizando um roteador ou switch de camada 3 que encaminhe os quadros entre as VLANs, chamado de roteamento entre VLANs.

Com esse tipo de recurso temos a otimização do envio de broadcasts na rede, diminuindo a sobrecarga nos links de backbone e também no processamento dos computadores.

Quando estudarmos o protocolo IP você aprenderá que mensagens de broadcast são constantemente utilizadas em redes IP versão 4 para diversas funções, tais como descobrir endereços MAC remotos através do protocolo ARP e alocação dinâmica de IPs pelo protocolo DHCP.

Na topologia abaixo você tem uma rede típica chamada “router-on-a-stick”, utilizada em redes de pequeno porte. Nessa topologia temos switches com VLANs e uma conexão a um roteador que tem a função de fazer o roteamento entre essas diversas LANs virtuais.

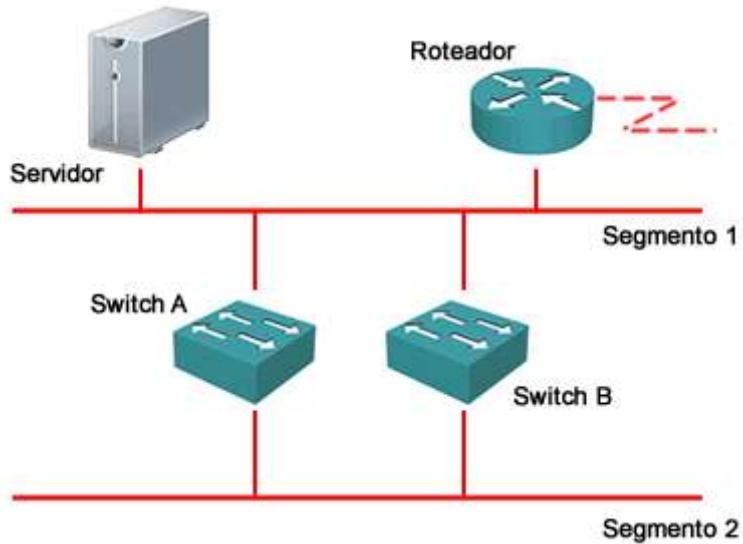


## 5 Spanning-Tree Protocol - STP

A seguir aprenderemos o básico sobre o protocolo spanning-tree e seu funcionamento.

### 5.1 Topologia Comutada Redundante Simples

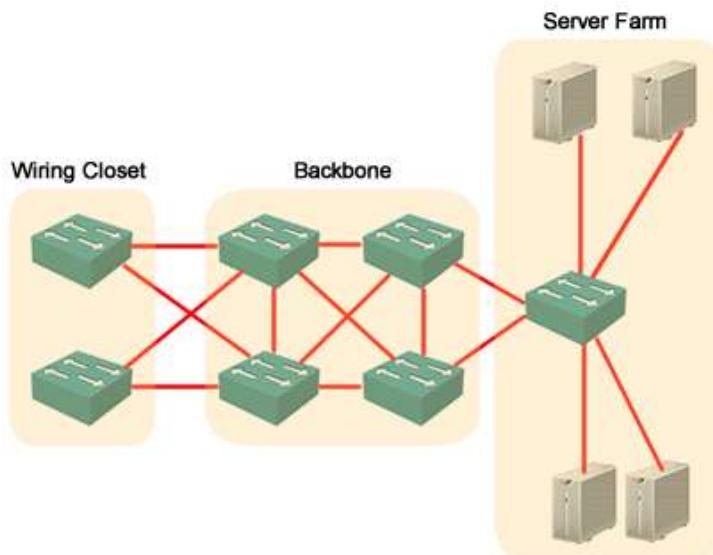
É muito comum a utilização de redes com caminhos e dispositivos redundantes, pois as redes com caminhos e dispositivos redundantes oferecem maior tempo de atividade e eliminam os pontos únicos de falha. Se um caminho ou dispositivo falhar, o caminho ou dispositivo redundante pode assumir suas tarefas.



Por exemplo, na topologia anterior se o Switch A falhar, o tráfego ainda pode fluir do Segmento 2 para o Segmento 1 e para o roteador através do Switch B.

### 5.2 Usando Bridging Loops para Redundância

Topologias de rede redundantes são concebidas para garantir que as redes continuem a funcionar eliminando a presença de pontos únicos de falha.



Por exemplo, se uma das conexões entre o wiring closet e o backbone falhar temos links redundantes. Mesmo assim, se um dos switches de backbone ficar down (falhar), temos o segundo switch para assumir todo o tráfego enquanto o problema é corrigido.

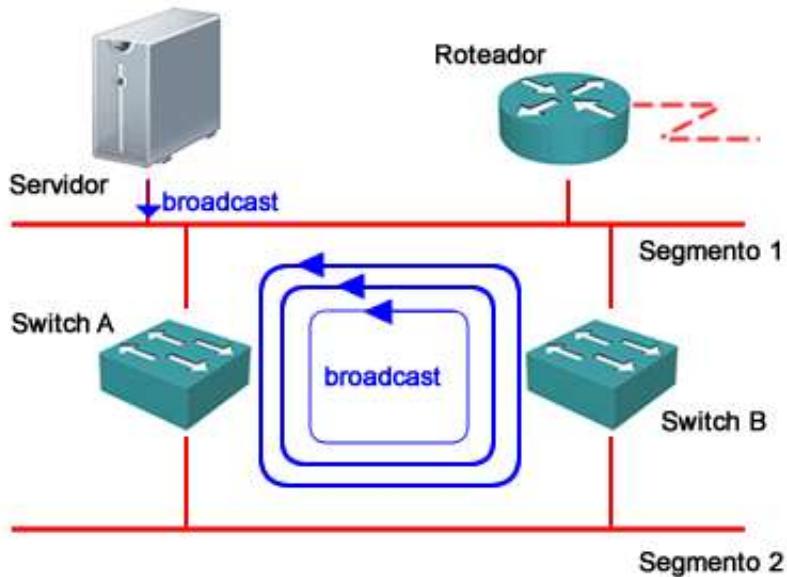
Porém, esse tipo de solução traz problemas para comunicação em camada 2, pois quadros enviados podem retornar através dos caminhos redundantes e causar problemas chamados loops. Os loops podem causar diversos problemas, tais como degradação da banda total, duplicação de dados recebidos e assim por diante.

Um dos problemas mais descritos nesse tipo de cenário é a tempestade de broadcast, a qual vamos estudar a seguir.

#### 5.2.1 Tempestade de Broadcast

O fenômeno conhecido como tempestade de broadcast pode ocorrer e degradar consideravelmente o desempenho de uma rede, pois em uma rede com loop de camada 2 tem o quadro de broadcast copiado diversas vezes até esgotar toda a banda disponível nos caminhos entre os switches.

Imagine na figura a seguir onde o servidor envia um pacote de broadcast para a rede através do segmento 1. Ambos os switches iriam propagar repetidamente esse broadcast formando um loop na rede e inundando a rede com pacotes de broadcast.



#### 5.3 Protocolo Spanning-Tree

Spanning-Tree ou STP é um protocolo de administração de link que fornece redundância de caminho, evitando os loops indesejáveis na rede. Esse protocolo é baseado na norma da IEEE 802.1d.

Para uma rede Ethernet funcionar corretamente, apenas um caminho ativo pode existir entre dois switches, pois caso existam vários caminhos ativos entre as estações podem surgir loops na rede.

Se existe um loop na topologia da rede, existe a possibilidade de duplicação de mensagens. Quando os loops ocorrem, alguns switches podem interpretar que uma determinada estação da rede aparece em ambos os lados do switch. Esta condição confunde o algoritmo de encaminhamento e permite a duplicação dos quadros encaminhados.

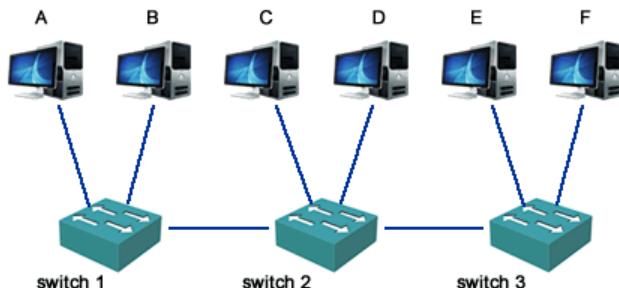
Para fornecer redundância de caminho, o protocolo Spanning-Tree define uma árvore que se estende por todos os switches em uma rede estendida. O STP força determinados caminhos de dados redundantes para o estado de espera (bloqueado). Se um segmento de rede se torna inacessível ou se o custo do STP se alterar, o algoritmo spanning-tree reconfigura a topologia dessa árvore estendida e restabelece o link, ativando o caminho de espera.

A operação do STP é baseada no envio de pequenos quadros chamados BPDUs (bridge protocol data units). Os switches de uma rede trocam BPDUs em períodos regulares (2s) para construir uma topologia sem loops.

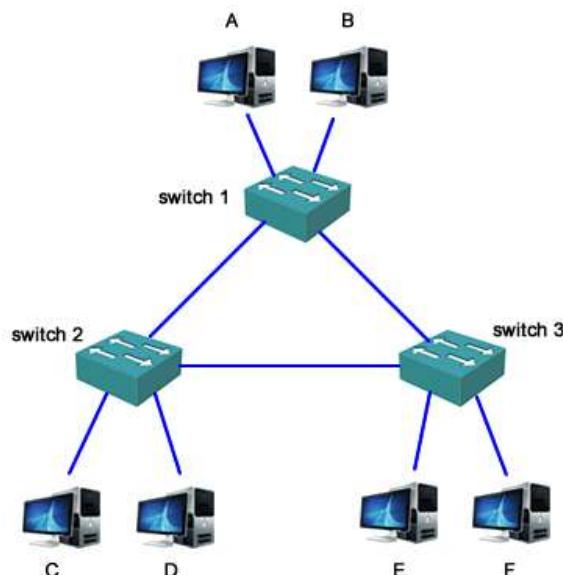
Os switches usam STP em todas portas Ethernet, Fastethernet e Gigabit Ethernet baseadas em VLAN (uma instância para cada VLAN-ID criado).

### 5.3.1 Exemplo - Protocolo Spanning-Tree

Analisando a figura abaixo podemos notar facilmente que o switch 2 é um ponto crítico dessa topologia, pois caso o switch 2 venha a falhar toda a rede poderá ser afetada.



Para resolver esse problema podemos alterar a topologia dessa rede, construindo caminhos redundantes, conforme mostrado na figura abaixo.



Nesse caso se um dos switches falhar não ocorrerá a paralisação da rede, pois a comunicação poderá ser restabelecida através do caminho redundante. Por exemplo, a comunicação entre a máquina C e a máquina F pode ser feita tanto pelo caminho entre os switches 1-3 como também pelo caminho entre os switches 1-2-3.

No entanto essa topologia causa um sério problema, conhecido como loop na rede. Imagine a seguinte situação. A máquina F está desligada e a máquina B dispara um frame que tem como destino a máquina F. Nesse caso o frame ficará em um loop infinito entre os switches, pois os switches não possuem o endereço MAC da máquina F em suas tabelas. Vamos ver passo a passo como isso acontece:

1. Ao serem inicializadas as tabelas de endereços MAC dos switches estão vazias.
2. Máquina B precisa mandar um pacote tendo como endereço destino máquina F.
3. Então B envia uma solicitação ARP em broadcast pedindo pelo MAC de F.
4. O switch 1 encaminha esse quadro para todas as suas portas, menos para a porta que conecta ao host B e originou o broadcast. Portanto os switches 2 e 3 recebem uma cópia desse quadro de broadcast.
5. O switch 2 encaminha esse broadcast para todas as suas portas, menos pela porta que conecta ao switch 1 (porta que recebeu o quadro original). Inclusive a porta que o conecta ao switch 3 recebe uma cópia do quadro de broadcast gerado pelo host B.
6. O switch 3 recebe o quadro do switch 2 e envia esse broadcast para todas as suas portas (menos para a porta do switch 2 que enviou o quadro), inclusive aquela que o conecta ao switch 1 recebe uma cópia do quadro novamente.
7. Como o switch 1 recebe uma cópia do mesmo quadro e não tem como saber que era o que ele enviou originalmente, ele reencaminha para todas suas portas, menos para a porta que conecta o switch 3.
8. O switch 2 recebe esse quadro e envia para o switch 3, que reenvia para o switch 1, que reenvia para o switch 2...

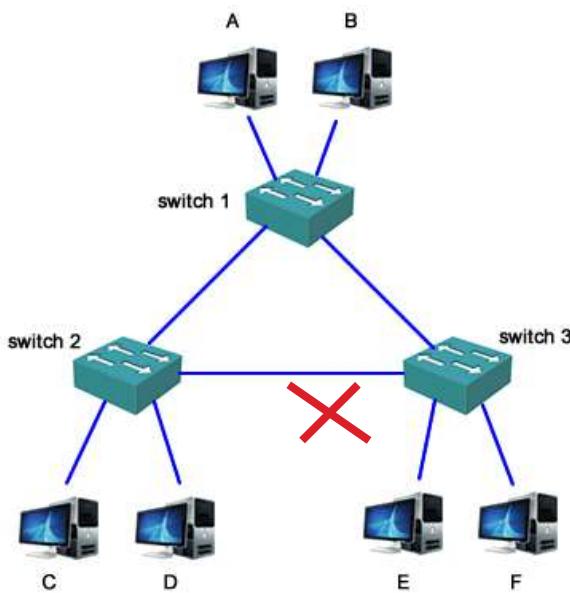
O processo se repete indefinidamente gerando loops de forma crescente para cada quadro de broadcast gerado pelos hosts, criando uma tempestade de broadcasts, já que cada switch recebe o mesmo frame pelas portas que o conectam aos demais switches. Por isso as tempestades de broadcasts podem até paralisar uma rede.

Note que analisamos o que ocorre no sentido horário (1-2-3), mas o switch 3 recebe o mesmo quadro, envia para 2 que envia para o switch 1, portanto pode acontecer também um fluxo simultâneo em sentido contrário!

Para solucionar esse tipo de problema é que existe o STP. Com o STP, somente um caminho físico estará ativo em um dado momento.

O algoritmo realiza uma eleição entre os switches, onde um deles será eleito raiz (root-bridge) e controlará toda a operação da rede. As portas passam por estados de blocking, listening, learning e forwarding.

Voltando a figura com a topologia redundante, a porta que liga o switch 2 e 3, por exemplo, poderia estar em estado de blocking e não chegaria aos demais estados. Só passaria a estar em forwarding se houvesse uma mudança de topologia ou uma falha em um dos switches, evitando loops de camada 2.



#### 5.4 Resumo Domínio de Colisão x Domínio de Broadcast

Domínio de colisão são os segmentos físicos da rede onde podem ocorrer colisões. Essas colisões fazem com que a rede se torne ineficiente, pois cada vez que ocorre uma colisão em uma rede, todas as transmissões são interrompidas por um período de tempo.

Os tipos de dispositivos que interligam os segmentos da rede definem os domínios de colisão.

- Dispositivos da Camada 1 (hub e repetidores) não dividem os domínios de colisão.
- Dispositivos da Camada 2 (bridge e switches) dividem domínios de colisão.
- Dispositivos de Camada 3 (roteadores e VLANs) dividem domínios de broadcast.

A divisão ou aumento no número de domínios de colisão pelos dispositivos das Camadas 2 e 3 é conhecida como segmentação.

Quando um nó precisa comunicar com todos os hosts na rede, envia um pacote de broadcast com um endereço MAC de destino FF-FF-FF-FF-FF-FF.

Em alguns casos, a circulação de pacotes de broadcast pode saturar a rede de tal maneira que não sobra largura de banda para a informação das aplicações. Esta situação é conhecida como tempestade de broadcast e aumenta com o crescimento da rede.

Um domínio de broadcast é um agrupamento de domínios de colisão que estão interligados por dispositivos da Camada 2. Os broadcasts são encaminhados pelos dispositivos da Camada 2 e são controlados apenas pelos dispositivos da Camada 3.

O encaminhamento da Camada 3 é baseado no endereço IP de destino e não no endereço MAC.

Resumo dos dispositivos e segmentação:

**Hub:**

- Dispositivo da camada 1 que reenvia todo o tráfego recebido.
- Não dividem domínios de colisão.
- Redes com HUBs possuem um domínio de colisão único.

**Switch:**

- Dispositivo da camada 2 utilizado para segmentar a rede (segmentar domínios de colisão).
- Cada porta corresponde a um domínio de colisão diferente.
- Encaminham os pacotes de acordo com o endereço MAC de destino.
- Os dispositivos da Camada 2 propagam todo o tráfego de broadcast e multicast.

**Router:**

- Dispositivo da camada 3, segmenta a rede em diferentes domínios de broadcast.
- Tomam a decisão de encaminhamento do pacote baseado no endereço IP e não no endereço MAC.

## 6 Entendendo e Configurando Switches Cisco Catalyst

Nesse tópico faremos uma introdução ao CLI (linha de comando) para ensinar as configurações básicas de um switch Cisco indo até a inserção do IP de gerenciamento do Switch.

Antes de iniciar esse capítulo faça download na biblioteca do programa simulador de routers e switches Cisco Packet Tracer e instale no seu computador caso ainda não o tenha feito. Lembre-se que para a parte introdutória sobre o packet tracer você deve realizar os laboratórios do capítulo 2.

O foco do CCENT são os Switches de camada-2 principalmente da linha Catalyst 2960.

Apesar de serem camada 2, estes switches possuem um endereço IP de gerenciamento, pois precisam ser acessado e gerenciado remotamente.

No dia a dia os switches dos modelos como 2950, 2960 ou 3560, ou seja, os que utilizam o sistema operacional IOS, vêm com uma configuração básica, porém sem um endereço IP pré-configurado, por isso começamos a configuração inicial via linha de comando (CLI) através de uma porta local de console que utiliza um cabo serial RS-232.

Portanto, basicamente um switch terá as portas de LAN (fastethernet ou gigabitethernet) e uma porta de console. As portas LAN podem ser via RJ-45 e cabo metálico UTP ou GBICs para conexão via fibra óptica, isso deve ser definido no projeto da rede. Aqui trabalharemos com switches padrões 2950 e 2960 com portas RJ-45.

Pense da seguinte maneira, a configuração geral de um switch define parâmetros básicos como se o switch fosse um "computador", por isso vamos dar um nome ao dispositivo, definir senhas de acesso, qual o roteador padrão e servidor DNS que ele utilizará, etc.

Basicamente estudaremos como entrar em um switch, alterar seus parâmetros, o comando help e comandos show.

Você pode agora abrir seu packet tracer e repetir os comandos que serão mostrados durante esse capítulo, basta puxar para a área de trabalho um switch modelo 2960 e divertir-se!

## 6.1 Arquitetura Básica de Switches

Vamos aqui abordar switches de camada 2 e não modulares, ou seja, switches com número de porta fixas, tais como a linha Catalyst 2960.

Muitos switches usam uma arquitetura baseada em ASIC (Application Specific Switching Circuits), ao invés dos microprocessadores tradicionais, permitindo maior velocidade na comutação e um barateamento do custo. Nos switches a comutação dos quadros é realizada em hardware, por isso são mais rápidas que a comutação realizada pelos roteadores que é realizada por software.

Os switches Cisco da linha 2960 utilizam como sistema operacional o Cisco IOS, tendo muito de suas configurações iguais a de um roteador. A diferença é que esses switches não possuem porta de acesso auxiliar, suas interfaces são de camada 2, não contendo endereço IP e sem suporte a roteamento.

O sistema operacional dos switches 2960 fica armazenado em uma memória flash, sendo que quando inicializado ele é copiado e executado na memória RAM do switch, a qual é utilizada para armazenamento de tabelas e conteúdos temporários, tais como buffers.

Quando configuramos um switch as informações que entramos via console ou VTY são armazenadas na memória RAM (running-config), a qual é volátil. Para que essa configuração seja armazenada em uma memória não volátil precisamos copiá-la para a NVRAM (startup-config) com o comando “copy running-config startup-config”, ou seja, copiar da origem na memória RAM para o destino na memória NVRAM.

O sistema operacional em roteadores e switches Cisco não precisa ser instalado como em computadores comuns, pois ele é uma imagem, ou seja, é um arquivo que fica armazenado em uma memória e é executado diretamente na memória RAM sem necessidade de instalação.

Quando ligamos um roteador ou switch de fábrica, sem configurações, ele possui um mínimo pré-configurado e normalmente mostrará um prompt chamado “modo setup”, uma espécie de wizard via CLI para ajudar o operador a configurar o equipamento. Abaixo segue um exemplo do prompt. Você pode sair desse modo de operação com um “no” ou pressionando a tecla control mais a letra C.

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no] :

Outra informação importante é que por padrão todas as interfaces dos switches estão ligadas ou UP, não precisando de comando para ativação, pois por padrão um switch deve encaminhar os quadros mesmo sem configuração, basta desembalar, energizar e conectar os cabos para que ele funcione.

Na prática essas portas já possuem uma pré-configuração vindo com os seguintes parâmetros:

- Velocidade automática
- Modo duplex via autonegotiação
- Pertencente à VLAN 1 (VLAN de gerenciamento ou nativa padrão para switches Cisco)

Com o comando “show running-config” você pode visualizar a configuração padrão do switch ou roteador antes de entrar com as configurações nos dispositivos. Essa configuração padrão pode variar de acordo com os modelos dos equipamentos e versões de sistema operacional.

Portanto, são equipamentos “plug-and-play”.

A seguir vamos estudar algumas configurações e comandos básicos em switches Catalyst.

## 6.2 Introdução ao CLI – Command Line Interface

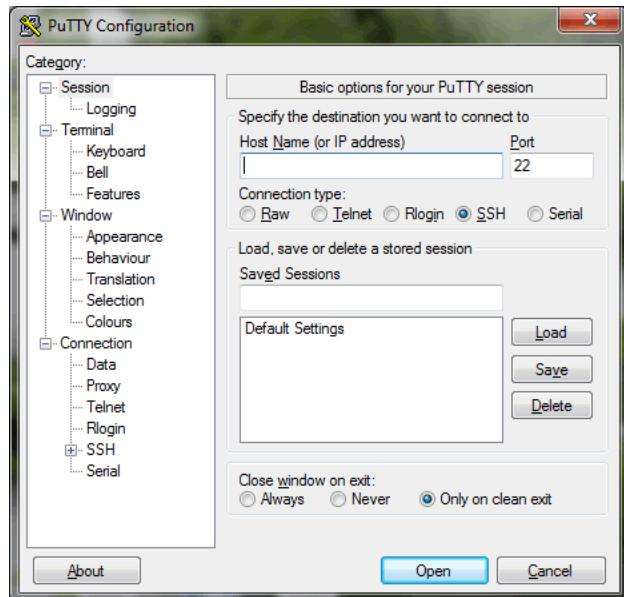
Podemos encontrar diversas maneiras para monitorar e configurar equipamentos de rede como, por exemplo, através do CLI (Command Line Interface ou Interface de Linha de Comando), utilizando o GUI (Grafic User Interface) ou utilizando ferramentas de gerenciamento como SNMP.

Nesse tópico abordaremos o CLI, a interface de usuário mais utilizada e divulgada entre profissionais que trabalham com roteadores e switches da Cisco. O CLI é baseado em linha de comando e, apesar de ser mais trabalhoso para a memorização dos comandos, torna o sistema mais leve, permitindo uma compreensão maior do que está sendo configurado pelo administrador de redes.

Diversos aplicativos emuladores de terminal podem ser encontrados no mercado para realizar o acesso local via console em dispositivos Cisco, cada um com seus recursos e aplicativos particulares. No próprio Windows existe um emulador de terminal chamado "Hyper Terminal".

Outros exemplos de aplicativos são:

- Teraterm
- SecureCRT
- Putty (tela a seguir)



## 6.3 Formas de Acesso aos Equipamentos

Para acessar um roteador ou switch da Cisco são disponibilizadas as linhas (lines) de console, auxiliar e VTY (Telnet/SSH).

As linhas de console e auxiliar são interfaces para conexão física serial assíncrona. A console é utilizada para configuração inicial através de um micro ou laptop local conectado diretamente ao equipamento. Utiliza-se um cabo rollover para conexão com a interface serial do computador à porta de console do roteador ou switch.

A porta auxiliar é utilizada para acesso remoto via modem, normalmente não disponível em switches.

As linhas VTY na realidade são portas para conexão virtual remota através de Telnet ou SSH. O número de conexões via VTY depende do modelo do roteador ou switch, por exemplo, em um 2501 você tem 5 portas VTY (de 0 a 4), ou seja, cinco conexões simultâneas. Em roteadores da linha 1800/2800/3800, 1900/2900/3900 e switches Catalyst 2960 você irá encontrar 16 portas VTY (de 0 a 15).

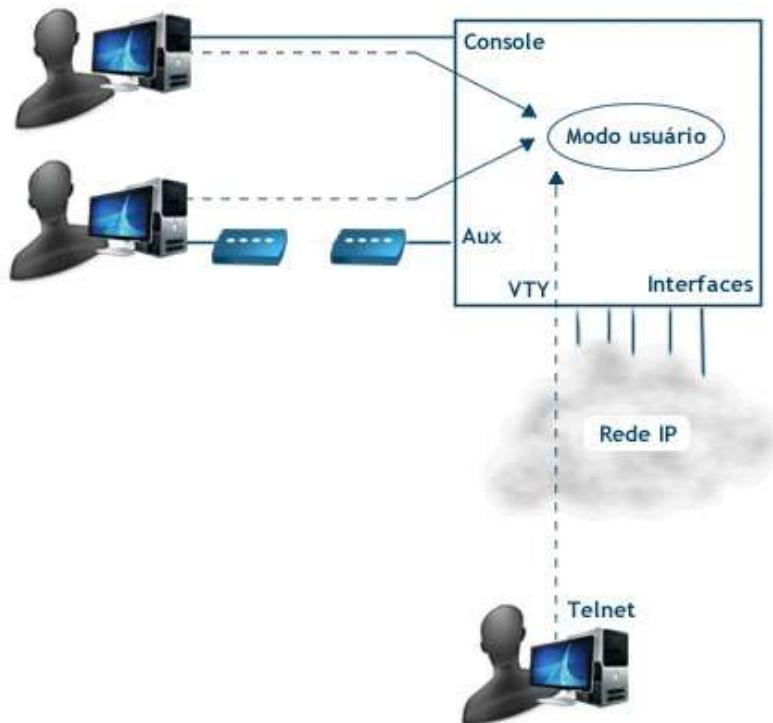
Para acessar um equipamento via telnet, basta digitar o comando "telnet x.x.x.x" onde "x.x.x.x" é o endereço IP de alguma interface do equipamento, sendo que em switches é o endereço configurado na VLAN de gerenciamento. Você pode fazer isso utilizando o próprio Prompt de comando ou programas específicos como o Putty.

[Clique na imagem para ampliar.](#)



#### 6.4 Modos de Execução (Exec) e Privilégios de Acesso

Iniciar uma sessão de execução é o ato de acessar o sistema operacional ou IOS (Internetwork Operating System) da cisco via uma das linhas de configuração (telnet/VTY, console ou porta auxiliar).



Além disso, é importante compreender que existem três níveis de execução básicos dentro do IOS:

- Modo de usuário - prompt - **Switch>**
- Modo privilegiado - prompt - **Switch#**
- Modo de configuração global - prompt – **Switch(config)#**

No modo de usuário (prompt >) você terá acesso aos comandos básicos para monitoração (show) e o “ping” para teste de conectividade.

Já no modo de usuário privilegiado (prompt #) você terá acesso a todos os comandos, inclusive ao modo de configuração (config), onde você poderá alterar os parâmetros de funcionamento do roteador ou switch. Portanto é importante definir quem terá acesso ao modo executivo privilegiado através de usuários e senhas, pois essas pessoas poderão alterar parâmetros que afetam o funcionamento da sua rede.

Ao se conectar a um roteador ou switch, normalmente a primeira senha solicitada, se configurado, permite entrada no modo de usuário. Para você entrar em modo privilegiado você deve digitar o comando “enable”. Veja o exemplo abaixo de acesso a um roteador.

```
Password: *****      (solicitação de senha para o modo de usuário)
Router>                  (prompt para o modo de usuário)
Router>enable            (comando para entrar em modo privilegiado)
Password: *****          (solicitação de senha para modo privilegiado)
Router#                 (prompt para o modo privilegiado)
Router#disable
Router>
```

Para voltar para o modo de usuário você deve digitar o comando “disable”. Com o comando “exit” você encerrará a sessão.

## 6.5 Comando Help do Switch do Modo EXEC Usuário

Um importante recurso, que com certeza você irá utilizar bastante, é o help. O comando help nos ajuda descobrir quais os comandos são suportados em cada modo de operação e muitas outras informações.

Para utilizar o help basta pressionar a tecla “?”, a qual funciona como o help do windows, porém dentro do IOS da Cisco. Por exemplo, no modo usuário a saída do comando será como mostrado abaixo.

```
Switch>?
Exec commands:
<1-99>      Session number to resume
connect       Open a terminal connection
disconnect    Disconnect an existing network connection
enable        Turn on privileged commands
exit         Exit from the EXEC
logout       Exit from the EXEC
ping         Send echo messages
resume       Resume an active network connection
show         Show running system information
telnet       Open a telnet connection
terminal     Set terminal line parameters
traceroute   Trace route to destination
Switch>
```

A lista de comandos pode variar de acordo com o roteador, switch ou versão de IOS, mas a forma de exibir o recurso de ajuda é sempre a mesma. Lembre-se que o CLI é baseado em contexto, ou seja, cada modo terá uma lista de opções diferentes.

Você pode utilizar o recurso "?" para descobrir a lista de comandos que iniciam com determinadas palavras ou letras, conforme exemplo abaixo onde queremos descobrir todos os comandos que iniciam com "t".

```

Switch>t?
telnet  terminal  traceroute
Switch>
Switch>show ?
  cdp          CDP information
  clock        Display the system clock
  dtp          DTP information
  flash:       display information about flash: file system
  history      Display the session command history
  interfaces   Interface status and configuration
  ip           IP information
  mac-address-table MAC forwarding table
  sessions    Information about Telnet connections
  tcp          Status of TCP connections
  terminal    Display terminal configuration parameters
  users        Display information about terminal lines
  version     System hardware and software status
  vlan         VTP VLAN status
  vtp          VTP information
Switch>
```

Você também pode verificar a lista de opções de um determinado comando, conforme exemplo abaixo onde queremos descobrir quais as opções do comando show.

```

Switch#show ?
  access-lists      List access lists
  arp              Arp table
  boot             show boot attributes
  cdp              CDP information
  clock            Display the system clock
  crypto           Encryption module
  dtp              DTP information
  etherchannel     EtherChannel information
  flash:           display information about flash: file system
  history          Display the session command history
  hosts             IP domain-name, lookup style, nameservers, and host
  table
  interfaces       Interface status and configuration
  ip               IP information
  logging          Show the contents of logging buffers
  mac              MAC configuration
  mac-address-table MAC forwarding table
  mls              Show MultiLayer Switching information
  port-security     Show secure port information
  privilege         Show current privilege level
  processes         Active process statistics
  running-config    Current operating configuration
  sessions          Information about Telnet connections
  snmp             snmp statistics
```

```

spanning-tree      Spanning tree topology
ssh                Status of SSH server connections
startup-config    Contents of startup configuration
storm-control     Show storm control configuration
tcp                Status of TCP connections
tech-support       Show system information for Tech-Support
terminal          Display terminal configuration parameters
users              Display information about terminal lines
version            System hardware and software status
vlan               VTP VLAN status
vtp                VTP information
Switch#

```

Por exemplo, com o comando acima descobrimos que com o comando “show arp” podemos visualizar a tabela de endereços MAC aprendidos pelo protocolo ARP.

## 6.6 Navegando pelo CLI

O CLI nos roteadores e switches Cisco é orientado por contexto, por exemplo, se quero configurar a primeira interface do switch preciso entrar em modo privilegiado, depois em modo de configuração global e aí entrar em modo de configuração da interface fastethernet 0/1, primeira interface de um switch 2960 que possui portas 10/100. Veja exemplo na saída abaixo.

```

Switch>enable
Switch#config term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fast0/1
Switch(config-if)#

```

Note que a cada passo o prompt foi alterado para indicar a mudança de contexto. Para sair e voltar, por exemplo, de modo de configuração de interface para o privilegiado você pode utilizar o comando “exit”, veja abaixo.

```

Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#

```

Com o exit saímos passo a passo, você poderia utilizar o end e sair diretamente para o modo privilegiado.

```

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/1
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#

```

Note que ao sair do modo de configuração e voltar ao privilegiado uma mensagem será mostrada, esses tipos de mensagem são geradas na saída de console para informar eventos. Por exemplo, quando uma interface cai (vai de UP para Down) uma mensagem é gerada. Abaixo segue exemplo que a interface 0/1 foi desativada com o comando shutdown e caiu, por isso uma mensagem de UPDOWN foi gerada.

```

Switch(config)#int f0/1
Switch(config-if)#shut

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down

Switch(config-if)#

```

Perceba que o comando shutdown foi aplicado com a abreviação "shut", esse tipo de abreviação é possível sempre que não exista ambiguidade, por exemplo, o comando show pode ser aplicado com sh, por não com "s", veja abaixo.

```

Switch#sh interface fast0/1
FastEthernet0/1 is administratively down, line protocol is down (disabled)
  Hardware is Lance, address is 000a.f3d9.2e01 (bia 000a.f3d9.2e01)
  BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    956 packets input, 193351 bytes, 0 no buffer
    Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    2357 packets output, 263570 bytes, 0 underruns

```

```

Switch#s interface
% Ambiguous command: "s interface"
Switch#

```

Veja que uma mensagem de comando ambíguo foi gerada.

Quando erramos um comando um acento circunflexo é mostrado indicando onde ocorreu o erro, veja exemplo abaixo.

```

Switch#show as
^
% Invalid input detected at '^' marker.

Switch#show a?
access-lists arp
Switch#show arp

Switch#

```

Note que o comando "show a" até existe, mas o "s" atrás do "a" não existe. Temos apenas o show arp e o show access-lists iniciando com "show a".

**Dica:** se um comando não entrar no packet tracer verifique a sintaxe, se ele existe pode não ter sido implementado no packet tracer, pois ele é um simulador e não um equipamento real!

## 6.7 Outros Recursos de Navegação e Edição via CLI

Por padrão o CLI guarda o histórico de até 10 comandos digitados. Essa configuração pode ser alterada com o comando "history size", conforme exemplo abaixo onde alteramos o tamanho do histórico de 10 para 20.

```
Switch#terminal history size ?
<0-256>  Size of history buffer
Switch#terminal history size 20
Switch#
```

Para visualizar o histórico podemos utilizar os comandos control mais a tecla P ou utilizando a seta para cima do teclado. Para voltar o comando podemos utilizar o control mais a tecla N ou a setinha para baixo do teclado. O comando show history mostra esse histórico de comandos.

```
Switch#show history
conf t
sh arp
sh interface brief
sh interface
s interface
showma
show as
show arp
conf t
terminal history size 20
show history
```

As linhas tem um tamanho máximo de caracteres e quando digitamos muitas coisas em uma mesma linha um dólar \$ indica que existem mais caracteres à esquerda. Assim como o monitor suporta um número máximo de linhas e quando damos um comando com muitas saídas o entra pula comando a comando ou a barra de espaço pode ser utilizada para pular por páginas.

```
Switch#show ?
access-lists      List access lists
arp               Arp table
boot              show boot attributes
cdp               CDP information
clock             Display the system clock
crypto            Encryption module
dtp               DTP information
etherchannel     EtherChannel information
flash:            display information about flash: file system
history           Display the session command history
hosts             IP domain-name, lookup style, nameservers, and host table
interfaces        Interface status and configuration
ip                IP information
logging           Show the contents of logging buffers
mac               MAC configuration
mac-address-table MAC forwarding table
mls               Show MultiLayer Switching information
port-security     Show secure port information
```

<b>privilege</b>	Show current privilege level
<b>processes</b>	Active process statistics
<b>running-config</b>	Current operating configuration
<b>sessions</b>	Information about Telnet connections
<b>--More--</b>	

Note que o More indica que a tela do terminal atingiu seu tamanho máximo e existem mais comandos na sequência.

Outro fato interessante é que no console você não consegue posicionar cursor com o mouse, precisa utilizar as setinhas de navegação para esquerda e direita para avançar e recuar o cursor em uma linha. Com o control mais a tecla A leva o cursor para o início da linha e o control mais a tecla E leva para o fim da linha.

Apesar dessas informações parecerem simples, para que você tenha fluência no CLI precisará dominar a base, pois como aprender comandos avançados sem saber o mais simples? Por isso abra o packet tracer e pratique!

## 6.8 Comando Show Version

Com o comando "show version" podemos verificar várias informações de um switch ou roteador, dentre elas a versão do IOS utilizada e o registro de configuração (Config Register). Veja um exemplo do comando abaixo.

```
Switch> show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(0.0.16)FX,
CISCO
DEVELOPMENT TEST VERSION
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Tue 17-May-05 01:43 by yenanh

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M), Version 12.2 [lqian-flo_pilsner 100]

Switch uptime is 3 days, 20 hours, 8 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-0.0.16.FX.bin"

cisco WS-C2960-24TC-L (PowerPC405) processor with 61440K/4088K bytes of memory.
Processor board ID FHH0916001J
Last reset from power-on
Target IOS Version 12.2(25)FX
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address      : 00:0B:FC:FF:E8:80
Motherboard assembly number    : 73-9832-02
Motherboard serial number      : FHH0916001J
Motherboard revision number   : 01
System serial number          : FHH0916001J
Hardware Board Revision Number : 0x01
```

Switch	Ports	Model	SW Version	SW Image
*	1	26	WS-C2960-24TC-L	12.2(0.0.16)FX C2960-LANBASE-M

**Configuration register is 0xF**

A quantidade de memória RAM e memória Flash são importantes para determinar se uma versão de IOS pode ser suportada pelo switch ou roteador. Na página da Cisco existem referências sobre o recurso de memória exigido para cada versão de IOS, portanto se uma nova versão de sistema operacional é lançada, antes de fazer o Upgrade em um switch é preciso verificar se seus requisitos de memória estão compatíveis com o sistema operacional lançado.

Com o comando show version podemos verificar algumas dessas informações. Marcado em amarelo na saída do comando temos a quantidade de memória RAM de 64M bytes (61440K+4088K). Note que na mesma linha em amarelo temos o modelo do switch WS-C2960-24TC-L.

Em azul temos destacadas as interfaces que o switch possui.

## 6.9 Conteúdo Default da Memória Flash

Por padrão, o diretório flash tem um arquivo que contém a imagem do IOS e outros arquivos do sistema. Inclusive nos switches não existe uma NVRAM exclusiva, ela é simulada dentro da memória Flash, por isso cuidado ao apagar o conteúdo dela, pois a configuração será também apagada.

```
Switch#sh flash:  
Directory of flash:/  
 2  -rw-    3058048      <no date>  c2950-i6q412-mz.121-22.EA4.bin  
 3  -rw-     269      <no date>  env_vars  
 4  -drw-   10240      <no date>  html  
64016384 bytes total (60958336 bytes free)  
Switch#
```

Depois que o switch for configurado, o diretório flash conterá um arquivo chamado config.text e um banco de dados de VLANs chamado vlan.dat contendo as configurações de VLAN e do protocolo VTP.

Além do comando "show flash" mostrado na tela anterior, você pode utilizar também o comando "dir flash:".

Note que com o comando "show flash" podemos verificar o tamanho da memória total, utilizada e livre.

## 6.10 Reinicialização e Voltando às Configurações de Fábrica

Algumas vezes é necessário "zerar" completamente a configuração de um switch. As etapas a seguir garantem que uma nova configuração sobrescreva completamente a configuração atual:

- 1) Para remover as atuais informações de VLAN, exclua o arquivo de banco de dados de VLANs, chamado vlan.dat com o comando "delete", do diretório flash.
- 2) Apague o arquivo de configuração de backup, chamado startup-config, com o comando "erase".
- 3) Reinicie o switch com o comando "reload".

Abaixo seguem os comandos para zerar um Catalyst 2950 e 2960.

```
Switch#delete flash:vlan.dat  
Delete filename [vlan.dat]  
Delete flash:vlan.dat? [confirm]  
Switch#erase startup-config
```

```
<output omitted>
Switch#reload
```

Portanto, o comando "reload" faz a reinicialização do roteador.

### 6.11 Configurações Padrões em Switches de Acesso

Um exemplo das configurações padrões de um switch segue abaixo.

```
Switch#show running-config
Building configuration...
Current configuration : 863 bytes
!
version 12.1
no service password-encryption
!
hostname Switch
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
```

```
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface Vlan1
  no ip address
  shutdown
!
line con 0
!
line vty 0 4
!
line vty 5 15
!
!
end
```

O nome padrão de um switch é “switch”, conforme marcado em verde na configuração.

Os pontos de exclamação na configuração são campos de comentário, tudo que está atrás de um ponto de exclamação é desconsiderado pelo IOS.

Outra informação importante que podemos tirar desse comando é que o switch possui 24 portas, da fast 0/1 até a porta fast 0/24. Conforme marcado em cinza na configuração.

Note que a VLAN 1 de gerenciamento não tem IP configurado e vem como shutdown, ou seja, não tem como pingar ou dar telnet para o switch. Além disso, as configurações das lines ou linhas de console para acesso local e VTY para acesso remoto não possuem senha. Conforme marcado em amarelo na configuração.

Um switch pode receber um endereço IP para fins de gerenciamento. Isso é configurado na interface virtual, VLAN 1. Por padrão, o switch não tem endereço IP configurado. Note na saída do comando show interfaces para a primeira interface do switch que só é mostrado o endereço MAC da interface, ela não possui endereço IP.

```
Switch#show interfaces fastEthernet 0/1
FastEthernet0/1 is down, line protocol is down (disabled)
  Hardware is Lance, address is 000b.be64.1d01 (bia 000b.be64.1d01)
    MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
      reliability 255/255, txload 1/255, rxload 1/255

### saídas omitidas ###

Switch#
```

## 6.12 VLANs Padrões em Switches Cisco Catalyst

Por padrão todas as portas do switch estão na VLAN 1, a qual é conhecida como VLAN de gerenciamento ou VLAN Nativa. Além disso, todas as portas do switch já vêm habilitadas, portanto é só plugar um computador que ele irá funcionar.

Isso é feito para que se o administrador de rede não quiser configurar nada e simplesmente conectar um switch a outro e conectar os computadores nas portas tudo funcione como se fosse uma rede com HUBs, ou seja, sem precisar de configuração alguma. Apesar de ser possível e até bastante utilizada esse tipo de instalação não é recomendada na prática.

O comando “show vlan” ou “show vlan brief” permite que possamos visualizar as VLANs que estão criadas, assim como quais portas pertencem a cada VLAN. Veja exemplo da saída do comando abaixo.

```
Switch# show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1 enet	100001	1500	-	-	-	-	-	0	0	
1002 fddi	101002	1500	-	-	-	-	-	0	0	
1003 tr	101003	1500	-	-	-	-	-	0	0	
1004 fdnet	101004	1500	-	-	-	ieee	-	0	0	
1005 trnet	101005	1500	-	-	-	ibm	-	0	0	

```
Remote SPAN VLANs
```

Primary	Secondary	Type	Ports

```
Switch#
```

Na coluna VLAN podemos verificar o número da VLAN e como já estudamos a VLAN 1 é a default. Além da VLAN 1 temos também por padrão as VLANs de 1002 a 1005 criadas. Essas cinco VLANs (1, 1002, 1003, 1004 e 1005) não podem ser apagadas ou alteradas.

A próxima coluna chamada “NAME” temos o nome da VLAN, note que a VLAN 1 tem o nome “default”.

Em seguida podemos verificar se a VLAN está ativa ou não na coluna “Status”. Por último, na coluna Ports, verificamos que por padrão todas as portas estão alocadas na VLAN 1.

As portas nos switches são nomeadas como Fastethernet ou Gibabitethernet 0/1 até 0/24 se for um switch de 24 portas, se tivermos um switch de 48 portas teremos da fast0/1 até fast 0/48.

Número da porta é informado no chassis do switch e um led de identificação fica verde se um dispositivo estiver conectado à porta e operacional.

### 6.13 Configurações Básicas – Hostname, Senhas e IP de Gerenciamento

Note da tela ao lado que ao entrar com o comando "hostname" o prompt muda para o hostname configurado.

```
Switch>
Switch>enable
Switch#config term
Switch(config)#hostname DlteC
DlteC(config)#enable secret dltec123
DlteC(config)#line console 0
DlteC(config-line)#password dltec
DlteC(config-line)#login
DlteC(config-line)#line vty 0 15
DlteC(config-line)#password dltec
DlteC(config-line)#login
```

Logo abaixo são configuradas as senhas de acesso privilegiado como "dltec123", para acesso local (line console 0) e acesso remoto via Telnet/SSH (line vty 0 15) como "dltec", tudo em minúsculo. Vale a pena lembrar que as senhas identificam maiúsculo, minúsculo e caracteres especiais.

Para que o acesso remoto seja possível ainda é necessário que o switch tenha um IP de gerenciamento. Por padrão, a VLAN1 é a VLAN de gerência. A VLAN de gerência é utilizada para gerenciar todos os dispositivos de uma rede. Numa rede baseada em switches, todos os dispositivos de rede devem estar na VLAN de gerência.

Todas as portas são pertencentes a VLAN 1 por default. Uma boa prática é remover todas as portas de acesso da VLAN 1 e colocá-las em outra VLAN. Isso permite a gerência dos dispositivos de rede enquanto mantém o tráfego dos hosts da rede fora da VLAN de gerência.

Veja exemplo de configuração abaixo.

```
DlteC(config)#interface VLAN1
DlteC(config-if)#ip address 192.168.1.2 255.255.255.0
DlteC(config-if)#no shutdown
DlteC(config-if)#exit
DlteC(config)#ip default-gateway 192.168.1.1
DlteC(config)#ip name-server 8.8.8.8
```

O comando "ip default-gateway" define o roteador padrão do switch e o "ip name-server" o servidor DNS que o switch utilizará para resolução de nomes.

Por padrão os switches e roteadores tentam traduzir nomes mesmo que o comando "ip name-server" não esteja configurado. Nesse caso o switch envia uma solicitação ao endereço de broadcast 255.255.255.255. Para desativar esse comportamento você pode utilizar o comando "no ip domain-lookup" em modo de configuração global.

Quando digitamos algo errado o IOS inicia um processo de tradução que pode demorar, para interromper você pode utilizar a sequência de escape apertando as teclas control, shift mais a o número 6.

## 6.14 Configuração do Modo Duplex e Velocidade das Portas

Por padrão a porta de um switch vem de fábrica configurada com a velocidade automática (auto-speed) e modo duplex automático (auto-duplex). Isso permite que as interfaces negociem essas configurações através do processo de autonegotiation ou autonegotiação.

Se necessário, os administradores de rede podem configurar manualmente a velocidade da interface e os valores duplex, conforme exemplo abaixo.

```
DlteC(config)#interface fastEthernet 0/1
DlteC(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation
DlteC(config-if)#duplex full
DlteC(config-if)#
DlteC(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration
DlteC(config-if)#speed 100
DlteC(config-if)#

```

Outro recurso que maioria dos switches mais novos possui é o Auto-MDI<sub>X</sub>, recurso que permite ao switch descobrir qual o tipo de cabo (cross ou direto) conectado e automaticamente configurar sua interface para aceitá-lo, possibilitando que duas portas de switch sejam conectadas com cabo direto, por exemplo.

## 6.15 Serviços de HTTP e HTTPS

Além da CLI existe uma interface baseada na web para fins de configuração e gerenciamento.

Uma vez configurado com um endereço IP e um gateway default, um switch pode ser acessado através de um navegador pelo seu endereço IP e a porta 80, a porta padrão do http. Veja a configuração a seguir.

```
DlteC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DlteC(config)#username dltec password dltec
DlteC(config)#ip http ?
  access-class  Restrict access by access-class
  authentication Set http authentication method
  path          Set base path HTML
  port          HTTP port
  server        Enable HTTP server
DlteC(config)#ip http server
DlteC(config)#ip authentication local
DlteC(config)#

```

Note que foi criado um usuário e senha para o switch com privilégio de root, ativado o serviço de HTTP e definida uma autenticação local para o HTTP.

Caso o gerenciador esteja instalado no switch você terá uma tela similar a mostrada a seguir, podendo variar conforme versão de IOS e modelo de switch.



## 6.16 Verificando a Tabela de Endereços MAC

Uma vez configurado e conectado à rede, para verificar os endereços MAC aprendidos pelas portas do switch utilize o comando "show mac address-table" (o comando pode variar conforme versão de IOS). Note que a tabela traz a VLAN que o MAC pertence (Vlan), o endereço MAC (Mac Address), o tipo de endereço (como ele foi aprendido - Type) e a porta que esse MAC está vinculado (Ports).

```

Switch#sh mac-address-table
      Mac Address Table
-----
Vlan   Mac Address        Type      Ports
----  -----
All    000d.6562.f240    STATIC    CPU
All    000d.0ccc.cccc    STATIC    CPU
All    000d.6562.cccd    STATIC    CPU
All    000d.6562.dddd    STATIC    CPU
1      0d0d.6561.f240    DYNAMIC   Fa0/3
2      0d0d.6561.f24f    DYNAMIC   Fa0/4

Switch#
Switch#clear mac-address-table dynamic
Switch#sh mac-address-table
      Mac Address Table
-----
Vlan   Mac Address        Type      Ports
----  -----
All    000d.6562.f240    STATIC    CPU
All    000d.0ccc.cccc    STATIC    CPU
All    000d.6562.cccd    STATIC    CPU
All    000d.6562.dddd    STATIC    CPU

```

Quando um computador conectado a uma porta de um switch envia um quadro, esse switch vincula seu MAC a uma porta e também à VLAN que aquela porta está vinculada! O MAC aprendido pode ser estático (static) ou dinâmico (dynamic), ou seja, estático é um MAC interno do switch ou então inserido manualmente por um administrador de redes. Já o dinâmico foi aprendido com o processo normal durante o recebimento dos quadros ethernet e analisando o campo do endereço MAC de origem do quadro recebido.

Portanto é nessa tabela de endereços MAC que o switch irá se basear para fazer seus encaminhamentos. Se o MAC de destino estiver listado aí o switch faz um encaminhamento direto entre os hosts, caso não esteja o quadro é copiado para todas as portas menos para porta que o enviou, conforme processo de flooding ou inundação que já estudamos. Endereços de multicast ou broadcast não são gravados nessa tabela, pois eles sempre são encaminhados via processo de flooding.

Olhe a saída do comando ao lado e note que temos as primeiras quatro entradas definidas com MACs estáticos e portas do tipo CPU, o que significa que são endereços internos do switch utilizados para processos internos. Já nas últimas duas linhas temos os MACs de dois computadores, note que o primeiro está ligado na porta fast 0/3 e pertence à VLAN 1, já o segundo está ligado na porta fast 0/4 e pertence à VLAN 2.

```
1      0d0d.6561.f240    DYNAMIC   Fa0/3
2      0d0d.6561.f24f    DYNAMIC   Fa0/4
```

Com essa tabela MAC podemos chegar a conclusão que não haverá flooding apenas se o computador com MAC 0d0d.6561.f240 tentar se comunicar com o 0d0d.6561.f24f e vice versa. Se qualquer outro MAC de host for inserido no destino o switch precisará fazer um flooding para descobrir a porta a qual o computador está conectado.

Para limpar a tabela de endereços e remover todos os endereços inválidos ou forçar ao switch reaprender os endereços MAC você pode utilizar o comando "clear mac-address table dynamic".

Também é possível atribuir estaticamente um endereço MAC para uma interface. Nesse caso o endereço MAC não será considerado obsoleto automaticamente pelo switch. Um exemplo para alocação estática é determinado servidor ou estação de trabalho de usuário precisam ser conectados à porta e o endereço MAC é conhecido., assim a segurança aumenta.

Veja exemplo de configuração abaixo.

```
Switch(config)#mac-address-table ?
  static  static keyword
Switch(config)#mac-address-table static 0000.1111.4444 ?
  vlan  VLAN keyword
Switch(config)#mac-address-table static 0000.1111.4444 vlan 1 ?
  interface  interface
Switch(config)#mac-address-table static 0000.1111.4444 vlan 1 inter
Switch(config)#mac-address-table static 0000.1111.4444 vlan 1 interface f0/8
Switch(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch#
Switch#sh mac-address-table
  Mac Address Table
-----
Vlan  Mac Address        Type      Ports
----  -----
All   000d.6562.f240    STATIC    CPU
All   000d.0ccc.cccc    STATIC    CPU
All   000d.6562.ccccd   STATIC    CPU
All   000d.6562.dddd    STATIC    CPU
1     0000.1111.4444    STATIC    Fa0/8
Switch#
```

Uma alternativa é definir port-security em uma interface do switch. A quantidade de endereços MAC por porta pode ser limitada a 1. O primeiro endereço aprendido dinamicamente pelo switch se torna o endereço seguro.

```
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport port-security ?
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
<cr>
Switch(config-if)#switchport port-security
```

O port-security é utilizado para limitar a quantidade de MACs que podem ser aprendidos por porta, evitando ataques relativos a camada 2, por exemplo, ataque de inundação de endereços MAC que visam gerar o estouro da tabela de MACs do switch fazendo com que ele faça o flooding de todos os quadros recebidos, possibilitando a escuta de pacotes em qualquer porta.

Vamos estudar mais opções de uso do port-security ao longo do curso.

### **6.17 Exemplo de Análise de Tabela MAC Avançado**

Vamos agora ao lado analisar uma saída de tabela MAC mais complexa, com diversos endereços aprendidos em diversas portas para podermos entender melhor o que pode ser cobrado na prova de certificação.

```
SW-DlteC#show mac address-table
  Mac Address Table
-----
Vlan   Mac Address        Type      Ports
----  -----
A11    0100.0ccc.cccc  STATIC    CPU
A11    0100.0ccc.cccd  STATIC    CPU
A11    0180.c200.0000  STATIC    CPU
A11    0180.c200.0001  STATIC    CPU
A11    0180.c200.0002  STATIC    CPU
A11    0180.c200.0003  STATIC    CPU
A11    0180.c200.0004  STATIC    CPU
A11    0180.c200.0005  STATIC    CPU
A11    0180.c200.0006  STATIC    CPU
A11    0180.c200.0007  STATIC    CPU
A11    0180.c200.0008  STATIC    CPU
A11    0180.c200.0009  STATIC    CPU
A11    0180.c200.000a  STATIC    CPU
A11    0180.c200.000b  STATIC    CPU
A11    0180.c200.000c  STATIC    CPU
A11    0180.c200.000d  STATIC    CPU
A11    0180.c200.000e  STATIC    CPU
A11    0180.c200.000f  STATIC    CPU
A11    0180.c200.0010  STATIC    CPU
A11    fffff.ffff.ffff  STATIC    CPU
 20     000a.f4d3.e481  DYNAMIC  Gi0/2
 10     000a.f4d3.e480  DYNAMIC  Gi0/2
 10     000a.f4d3.e481  DYNAMIC  Gi0/2
 10     000c.295e.bb64  DYNAMIC  Fa0/3
 10     0012.7b50.01f6  DYNAMIC  Fa0/1
 10     0018.e761.77a8  DYNAMIC  Fa0/1
 10     001b.0c96.c5e8  DYNAMIC  Fa0/6
 10     001d.7060.d31b  DYNAMIC  Fa0/5
```

```

10  001e.130b.1aee  DYNAMIC  Fa0/2
10  0023.339d.0792  DYNAMIC  Fa0/4
10  2893.fe6c.e163  DYNAMIC  Gi0/1
10  c018.85e5.ecbf  DYNAMIC  Fa0/1
10  c018.85e5.eedb  DYNAMIC  Fa0/1
30  000a.f4d3.e481  DYNAMIC  Gi0/2
30  2893.fe6c.e163  DYNAMIC  Gi0/1
1   000a.f4d3.e481  DYNAMIC  Gi0/2
1   2893.fe6c.e163  DYNAMIC  Gi0/1

```

Total Mac Addresses for this criterion: 37

SW-DlteC#

Vamos iniciar a análise olhando da primeira saída até a vigésima, você lembra que tipo de endereço é estático e utiliza a porta do tipo CPU? Isso mesmo, são endereços MAC utilizados pelo próprio sistema interno do switch. Note que no campo VLAN eles tem escrito "All", em português "Todas", pois como são endereços internos podem pertencer a todas as VLANs. Além disso, na vigésima linha temos uma entrada para o broadcast que tem endereço MAC ffff.ffff.ffff e pertencendo à todas as VLANs, como já estudamos.

Nas próximas linhas, temos MACs aprendidos dinamicamente, pois eles tem o tipo ou type como dynamic. Analise os MACs, as VLANs que eles pertencem e a que porta cada um está vinculado. Você notou algo que chamou sua atenção? Se você prestou atenção existem MACs que estão vinculados a uma mesma porta, veja as três primeiras linhas a partir da vigésima:

```

20  000a.f4d3.e481  DYNAMIC  Gi0/2
10  000a.f4d3.e480  DYNAMIC  Gi0/2
10  000a.f4d3.e481  DYNAMIC  Gi0/2

```

Temos os MACs 000a.f4d3.e481, 000a.f4d3.e480 e 000a.f4d3.e481 vinculados a porta gigabit de número 0/2. Você consegue dizer o porquê?

Normalmente nesses casos ou temos uma porta de entroncamento entre switches (trunk) ou um HUB conectado nessa porta. Para ter certeza outros comandos mais avançados que aprenderemos nos capítulos 9 e 11 serão necessários, mas basicamente você pode com um protocolo da Cisco chamado CDP descobrir se o vizinho conectado a porta é um equipamento Cisco ou não. Além disso, se for um HUB a porta deve estar como Half-duplex.

Agora volte à tabela e responda: Quantas portas desse switch podem ser de tronco (trunk) ou estarem conectadas a um HUB?

Para responder basta procurar as que estão repetidas na coluna Ports, pois são as que têm mais de um MAC por porta, portanto são as portas Giga 0/1, Giga 0/2 e a Fast 0/1.

## 6.18 Salvando e Verificando as Configurações do Switch

Vale a pena reforçar que os switches e roteadores Cisco **não salvam diretamente a configuração**, pois tudo o que você alterar é gravado em uma memória RAM ou DRAM que é volátil (chamada de running-config pelo IOS), ou seja, ao desligar o equipamento perde as informações. Para isso existe uma memória de backup que é utilizada para salvar a configuração chamada NVRAM (chamada de startup-config pelo IOS), portanto ao final das configurações você deverá salvar o conteúdo da RAM para a NVRAM através do comando copy, veja a sintaxe abaixo:

**Copy running-config startup-config**

Para verificar os comandos da RAM entre com o comando “show running-config” e da NVRAM com o “show startup-config”.

Para verificar opções como o sistema operacional que o switch está utilizando ou há quanto tempo ele está ligado (Uptime) utilize o comando “show version”.

### **6.19 Configurações Gerais em Switches Cisco – Resumão!**

Abaixo segue um resumo das configurações gerais ou básicas em switch são:

- 1) Conectar um cabo de console na porta serial do seu computador ou abrir uma tela do packet tracer e selecionar um switch 2950. No packet tracer você pode também utilizar um computador e um cabo de console para acessar os equipamentos via terminal.
- 2) Abrir o Hyperterminal ou a tela CLI do packet tracer.
- 3) Entrar em modo privilegiado com o comando “enable”.
- 4) Entrar em modo de configuração global digitando “configure terminal”.
- 5) Alterar o nome do host que por padrão vem como Switch com o comando hostname. É importante que cada switch tenha um hostname que normalmente segue um padrão definido pelas empresas, assim podemos identificá-los em uma topologia de rede que tenham diversos equipamentos.

**hostname Novo\_nome**

- 6) Inserir uma senha secreta para entrada no modo privilegiado (“super-user”) com o enable secret. Quando você entra em um switch ou roteador Cisco via CLI ele vem em um modo que chamamos de Usuário, identificado pelo símbolo “>”. Para fazer as configurações o operador deve estar em modo Privilegiado (#) e essa senha previne que pessoas não autorizadas acessem o modo privilegiado e alterem indevidamente as configurações.

**enable secret senha**

- 7) Configurar as senhas de acesso local via console para conexão local segura:

```
Line console 0
Password senha
Login
```

- 8) Idem para o acesso remoto via telnet, o qual é chamado de VTY no IOS da Cisco:

```
Line vty 0 15
Password senha
Login
```

- 9) Configurar o banner de entrada para que usuários que tentem acessar os equipamentos recebam um aviso de segurança e acesso restrito a pessoas autorizadas:

**Banner motd @ Aviso de segurança@**

10) Definir o IP de gerenciamento para conexão remota:

```
Interface vlan 1
Ip address 192.168.1.1 255.255.255.0
No shutdown
```

11) Definir um roteador padrão e um servidor DNS para acesso à Internet ou outras redes locais:

```
Ip default-gateway 10.0.0.1
Ip name-server 4.4.4.4
```

12) Copiar a configuração para a NVRAM (memória backup):

```
copy running-config startup-config
```

Com os passos acima você fez a configuração inicial em um switch Cisco.

Voltaremos a configurar switches no Capítulo-7, onde vamos mais a fundo nas configurações de VLANs, trunks e demais assuntos referentes ao conteúdo do CCENT.

## 7 Resumo do Capítulo

Bem pessoal, chegamos ao final do capítulo. É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Entender o funcionamento de uma rede full-duplex e half-duplex.
- Entender o processo do CSMA/CD no controle de colisões.
- Conseguir explicar a relação entre hub/bridge/switch e domínios de colisão.
- Diferenciar os três meios de encaminhamento de quadro em um switch (Cut through, Fragment Free e Store and forward).
- Ter uma noção das configurações básicas que podemos realizar em um switch Cisco (banners, telnet, portas e vlan).
- Entender o que é uma VLAN e como elas segmentam domínios de broadcast.
- Entender a utilidade do protocolo spanning-tree na eliminação de loops e tempestades de broadcast.
- Entender os princípios de funcionamento e configurações iniciais de switches camada 2 da Cisco.

Nesse capítulo iremos estudar as redes de longa distância.

Veremos seus principais fundamentos e padrões.

Além disso, estudaremos os princípios básicos de funcionamento dos Roteadores Cisco e suas configurações iniciais.

Aproveite o capítulo e bons estudos!

## Capítulo 04 – Redes WAN e Roteadores

### Objetivos do Capítulo

Ao final desse capítulo você terá estudado e deverá compreender:

- Visão geral dos protocolos de roteamento;
- Principais modelos de design de rede;
- Como planejar a implantação e resolução de problemas envolvendo protocolos de roteamento.

### Sumário do Capítulo

<b>1 Onde Está Posicionada uma WAN na Topologia de Rede? .....</b>	<b>112</b>
1.1 Exemplos de Topologias de Rede WAN 113	
1.2 Terminologia Utilizada em WAN .....	115
1.3 Conectando Roteadores via Serial em Laboratório .....	116
1.4 Links WAN e o Modelo OSI – Links Seriais HDLC .....	117
1.5 Enviando Informações Através da WAN 118	
<b>2 Serviços de WAN .....</b>	<b>120</b>
2.1 Introdução ao MPLS.....	121
2.2 Utilizando Ethernet na WAN - EoMPLS 121	
<b>3 Acesso à Internet.....</b>	<b>122</b>
3.1 Opções de Conexão à Internet .....	124
3.2 Entendendo o Acesso Banda Larga DSL 125	
3.3 Entendendo o Acesso Banda Larga via Cable Modem .....	127
<b>4 Interpretando e Montando Topologias de Rede LAN e WAN .....</b>	<b>128</b>
4.1 Interpretando e Montando Topologias – Exemplo 1 .....	128

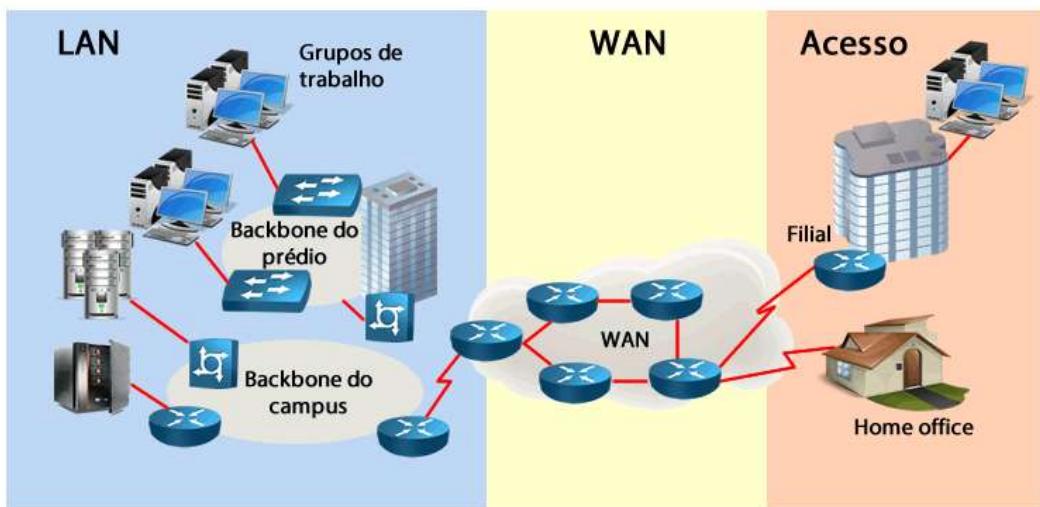
<b>4.2 Interpretando e Montando Topologias – Exemplo 2 .....</b>	<b>129</b>	<b>6.9 Atividade Prática .....</b>	<b>152</b>
<b>5 Introdução o Hardware e Inicialização de Roteadores Cisco.....</b>	<b>129</b>	<b>7 Configurações de Interface em Roteadores.....</b>	<b>153</b>
<b>5.1 Sistema Operacional - IOS (Internetwork Operating System) .....</b>	<b>130</b>	<b>7.1 Interfaces LAN - Ethernet, Fastethernet e Gigabitethernet .....</b>	<b>154</b>
<b>5.2 Memórias.....</b>	<b>131</b>	<b>7.2 Interfaces Seriais .....</b>	<b>156</b>
5.2.1 RAM/DRAM.....	131	7.3 Configurando Links Seriais HDLC .....	158
5.2.2 NVRAM.....	132	7.4 Verificação das Configurações e Troubleshooting Básico.....	160
5.2.3 Flash .....	132	7.4.1 Verificando a Configuração do Protocolo IP das Interfaces .....	164
5.2.4 ROM .....	132	7.4.2 Acrescentando um Link WAN na Topologia .....	166
<b>5.3 Interfaces de LAN e WAN.....</b>	<b>132</b>	<b>8 Resumo do Capítulo .....</b>	<b>169</b>
<b>5.4 Linhas de Configuração (Console, Auxiliar e VTY) .....</b>	<b>134</b>		
<b>5.5 Revisando o Básico da CLI e Inicialização</b>	<b>136</b>		
<b>5.6 Acessando Roteadores e Switches....</b>	<b>137</b>		
<b>5.7 Configurações Padrões em Roteadores</b>	<b>140</b>		
<b>5.8 Verificando o Hardware e Memórias dos Roteadores com o Show Version.....</b>	<b>141</b>		
<b>5.9 Troubleshooting – Show versus Debug</b>	<b>143</b>		
<b>5.10 Logging Synchronous e Exec-Timout</b>	<b>144</b>		
<b>6 Configurações Gerais em Roteadores e Switches – Revisão e Comandos Adicionais</b>	<b>145</b>		
<b>6.1 Hostname.....</b>	<b>145</b>		
<b>6.2 Senhas de Enable.....</b>	<b>146</b>		
<b>6.3 Senhas das Lines Console, VTY e Auxiliar</b>	<b>146</b>		
<b>6.4 Comandos Relacionados ao DNS (Resolução de Nomes) .....</b>	<b>149</b>		
<b>6.5 Configurando Banners .....</b>	<b>149</b>		
<b>6.6 Salvando e Manipulando Arquivos de Configurações.....</b>	<b>150</b>		
<b>6.7 Comparando com as Configurações do Capítulo-3 para Switches.....</b>	<b>151</b>		
<b>6.8 Considerações sobre Questões Simuladas no Exame .....</b>	<b>151</b>		

## 1 Onde Está Posicionada uma WAN na Topologia de Rede?

No capítulo anterior estudamos conceitos ligados às redes Locais, ou seja, utilizando switches para “dar acesso” aos computadores e servidores aos serviços de rede locais. Mas e se tivermos localidades remotas, por exemplo, a empresa onde trabalho possui uma unidade principal (Matriz ou Headquarter) em São Paulo e um escritório remoto (Filial ou Branch Office) em Curitiba, como podemos fazer a comunicação entre esses dois pontos?

A resposta é utilizando um serviço de longa distância ou WAN – Wide Area Network.

### O que é uma WAN? Wide Area Network (Rede de Longa Distância)



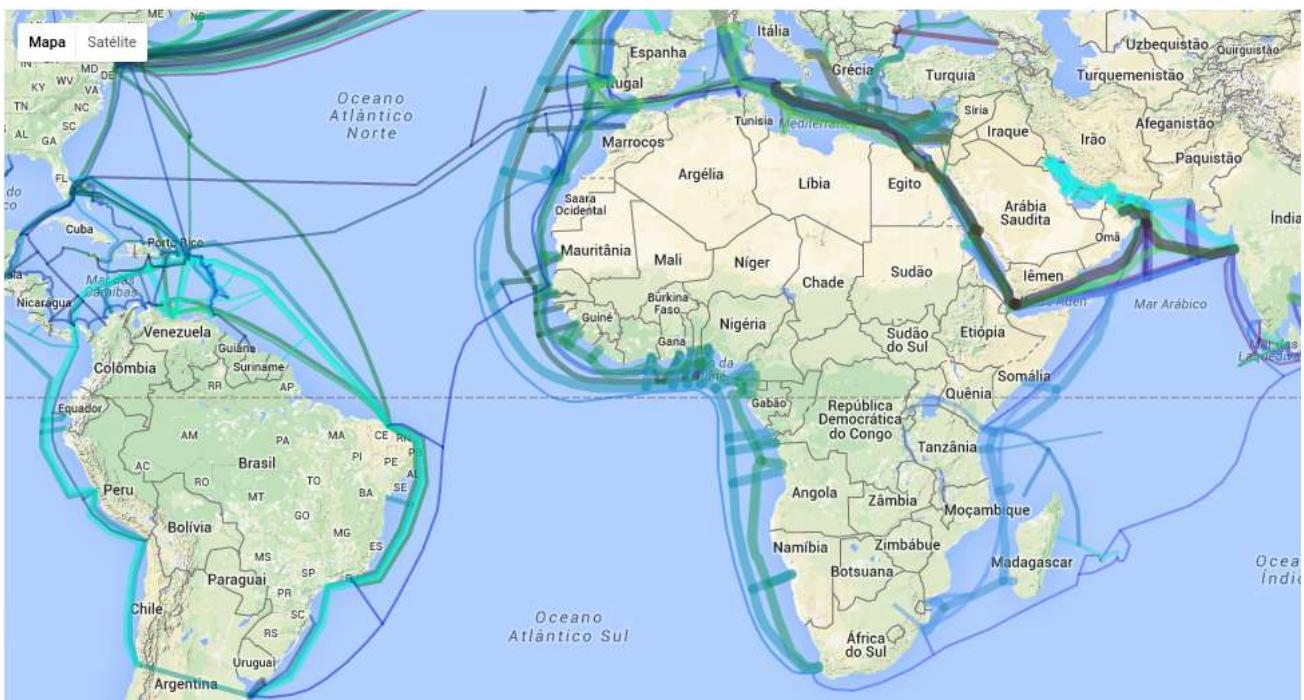
A história da WAN ou Redes de Longa Distância começa em 1965 quando Lawrence Roberts e Thomas Merrill ligaram dois computadores, um TX-2 em Massachusetts a um Q-32 na Califórnia, através de uma linha telefônica de baixa velocidade, criando a primeira rede de área alargada (WAN). Atualmente as redes WAN interligam redes situadas em localidades diversas e são providas quase que em sua totalidade por operadoras de telecomunicações.

Atualmente a maior WAN que existe é a **Internet**, contendo milhares de roteadores e switches para interconectar os diversos computadores espalhados ao redor do globo.

Falando em termos de mercado Brasileiro, a abertura do mercado das telecomunicações proporcionou uma oferta maior de serviços cada vez mais variados para conectividade WAN. Atualmente o investimento dessas empresas vem sendo focado na migração para redes MPLS, fornecimento de VoIP e Telefonia IP, qualidade de serviço ou QoS e IPTV (TV via Internet), a fim de atingir um número cada vez maior de usuários atraídos pelo custo cada vez menor devido a concorrência na prestação destes serviços.

Portanto, podemos simplificar o conceito de WAN e dizer que ela interliga diversas LANs de uma mesma empresa, formando a rede corporativa.

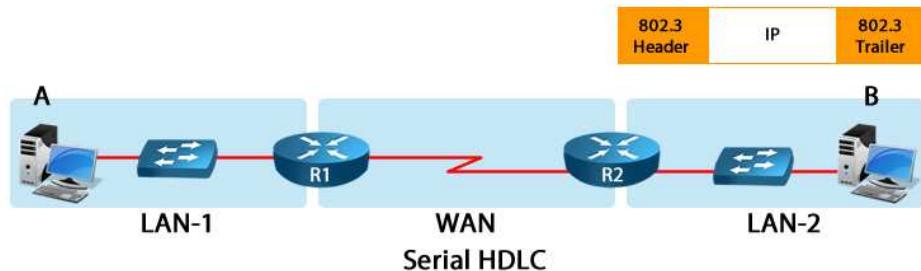
Para dar uma ideia de dimensão que uma WAN pode ter, na figura a seguir temos um mapa de maioria dos links ópticos (fibra óptica) que circulam o globo e fazem parte das conexões da Internet e demais serviços globais de conexão.



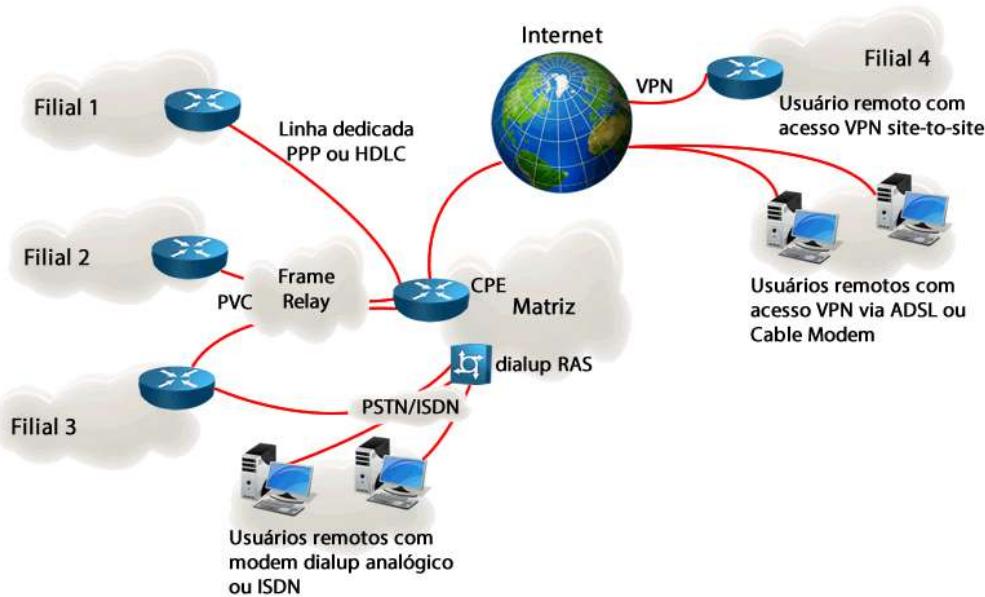
Fonte: <http://www.cablemap.info/> retirado 10-06-2016.

## **1.1 Exemplos de Topologias de Rede WAN**

Na figura a seguir temos um exemplo de uma pequena empresa utilizando uma linha dedicada para conectar apenas uma unidade remota utilizando um link serial ponto a ponto HDLC.



Agora na figura a seguir vamos analisar um exemplo de rede WAN mais complexo. Note que temos uma empresa conectada a diversas unidades remotas utilizando variados tipos de acesso WAN, tais como linhas privativas e circuitos VPN através da Internet.



Note que essa empresa possui uma Matriz (Unidade Central ou Headquarter) e quatro Unidades Remotas (Remote Office ou Branch Office), além disso, ela possui funcionários que trabalham remotamente ou atuam em campo e precisam acesso à rede corporativa para leitura de seus e-mails ou acessar bases de dados corporativas.

Note que a Filial 1 utiliza um circuito dedicado (linha privativa) ponto a ponto, a qual pode utilizar como protocolo de camada 2 o HDLC ou PPP, no caso da Cisco lembre-se que o HDLC é proprietário. Já as Filiais 2 e 3 conectam-se à Matriz através de um backbone Frame-relay. Além disso, a Filial 3 utiliza uma solução de backup discado, via uma linha telefônica digital ISDN, para o caso da linha principal fique indisponível esse circuito é utilizado como contingência. Note que a conexão é direta entre o roteador um dispositivo chamado RAS ou Servidor de Acesso Remoto.

O RAS é um dispositivo que de um lado se conecta a rede tradicional de telefonia PSTN ou ISDN e na outra ponta conecta-se à rede de dados da empresa, permitindo que usuários remotos ou então unidades remotas conectem-se à rede de dados via um circuito discado, seja ele analógico (PSTN) ou digital (ISDN ou RDSI). Nesse caso, temos um circuito de baixa velocidade utilizado no caso de backup apenas para serviços essenciais ou troubleshooting da linha principal.

Depois temos a conexão da Matriz com a Internet, sendo que nessa topologia para que os computadores das Filiais 1 a 3 acessem a Internet deverão passar pela Matriz, pois eles não têm acesso direto local.

Note que conectados à Internet temos uma Unidade Remota chamada Filial 4, a qual pode acessar a rede corporativa (Intranet) através de um circuito VPN (Rede Virtual Privativa) fechada entre o roteador local e o roteador Matriz. Algumas empresas fazem essa conexão com um **“Concentrador VPN”** na Matriz, o qual tem a função de ponto único de acesso para todas as conexões VPN da empresa, seja de Unidades Remotas com topologias site-to-site, como a Filial 4, ou então de usuários remotos que trabalham em casa em Home-Office. Esse tipo de funcionário que trabalha em sua residência possui um aplicativo VPN Client que permite a conexão do seu computador de maneira segura com a rede interna da empresa.

Nesse segundo exemplo ilustramos uma topologia real de WAN de uma empresa de médio porte, porém a rede WAN ainda depende do que as prestadoras de serviço conseguem disponibilizar para cada localidade e também de quanto a empresa deseja investir em seus links WAN.

Portanto, complexidade das topologias de rede depende do número de unidades conectadas e porte de cada empresa.

Perceba também que um projeto de rede básico depende de uma topologia da rede local ou LAN de cada unidade e do projeto da interconexão dessas LANs através de uma rede WAN. Lembre-se que na maioria dos casos as redes WAN pertencem aos provedores de serviço e existe um custo de instalação mais um valor mensal para uso dos serviços que sempre são considerados na escolha da melhor opção em um projeto real.

Além disso, os serviços disponibilizados para conexão WAN pelos provedores de serviços de Telecomunicação podem ser bastante variados. No conteúdo do CCENT 100-105 vamos analisar conceitualmente as opções mais comuns e também o protocolo HDLC, os demais protocolos e configurações de WAN serão estudados no conteúdo da prova 200-105.

## 1.2 Terminologia Utilizada em WAN

A opção de WAN mais comum e mencionada em bibliografias de redes são as linhas privativas ou circuitos dedicados.

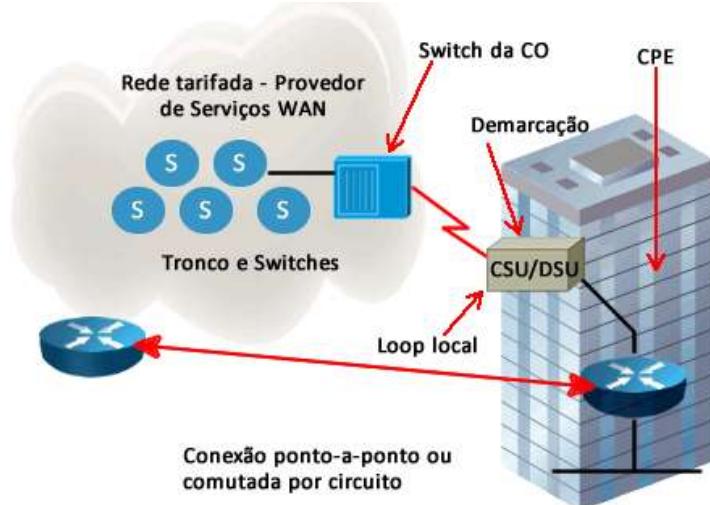
Historicamente são utilizados vários termos para descrever esse tipo de serviço:

- Linha privada ou privativa ou circuito dedicado
- Link T1 ou E1
- Link serial, serial ponto a ponto ou simplesmente link ponto a ponto
- Link WAN

Os termos privativo ou dedicado vêm do conceito que uma linha privativa não é compartilhada, por isso garante a privacidade dos dados. Já os termos E1 e T1 são tipos de circuitos utilizados para possibilitar essas conexões dedicadas através de redes convencionais de Telecomunicações.

Os termos “serial” e “ponto a ponto” é porque normalmente esse tipo de circuito tem apenas dois pontos e utiliza uma interface serial no roteador para conexão com a rede do provedor de serviços (ISP ou Service Provider).

Normalmente esse tipo de conexão utiliza a topologia ao lado.



Para entender uma rede WAN temos que apresentar os principais termos envolvidos na figura anterior:

- **CPE (Customer Premises Equipment):** Dispositivos localizados nas instalações do assinante. Inclui os dispositivos de propriedade do assinante e os dispositivos que o provedor de serviços aluga ao assinante. O roteador do cliente é um CPE.
- **Demarcação (Demarc):** O ponto onde o CPE termina e a parte do loop local do serviço começa. Geralmente ocorre no POP de um prédio.
- **Loop local ("last mile"):** Cabeamento da demarcação até o escritório central do provedor de serviços de WAN. Podem ser links metálicos (par metálico como HDLS e ADSL), fibras ópticas, rádios digitais ou links via satélite.
- **Switch da Operadora (CO - Central Office):** Recurso de comutação que fornece o serviço de WAN do provedor ao ponto de presença (POP) mais próximo. Switch é um termo genérico, porém a rede da operadora de Telecom é composta por diversos equipamentos como Multiplexadores DWDM, roteadores, switches, rádios, etc.
- **Rede tarifada:** O conjunto de switches e recursos (chamados de entroncamentos) dentro da nuvem do provedor da WAN. O tráfego do cliente pode atravessar entroncamentos de operadoras setoriais regionais e internacionais, à medida que a chamada trafega o longo caminho até seu destino.
- **CSU/DSU e Modem:** o dispositivo que a operadora faz a entrega dos serviços no caso das linhas privativas ou circuitos digitais é chamado de CSU/DSU (Unidade de Serviço de Canal/Unidade de Serviço de Dados). No caso de linhas analógicas utiliza-se o termo Modem no CCNA. No Brasil chamamos o CSU/DSU de Modem Digital, porém no CCENT e CCNA o termo Modem é para linhas analógicas. O CSU/DSU é um dispositivo DCE, enquanto o router ou CPE é DTE.

Na prática, as duas pontas de um circuito dedicado ponto a ponto tem a mesma estrutura, sendo que as informações podem cruzar diversos dispositivos dentro do provedor de serviços até alcançar o ponto remoto.

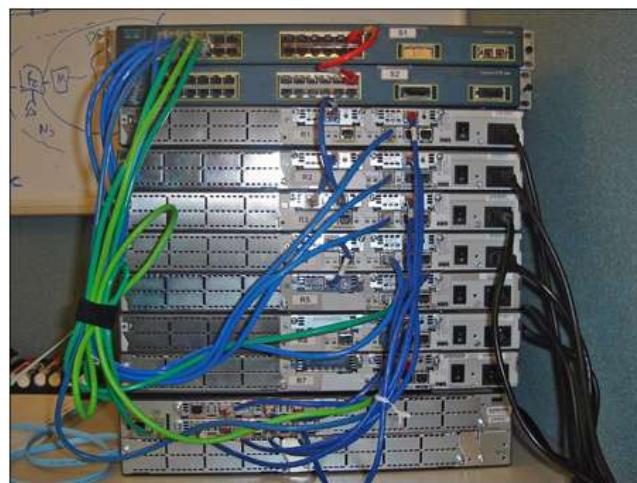
### 1.3 Conectando Roteadores via Serial em Laboratório

Você deve estar agora se perguntando o que a frase "O CSU/DSU é um dispositivo DCE, enquanto o router ou CPE é DTE" significa se nunca ouviu falar desses termos DCE e DTE.

Em Telecomunicações a velocidade de leitura dos dados é que define a taxa ou velocidade em bits por segundo. Mas quem define essa velocidade? É o roteador ou o CSU/DSU? Isso é definido pelos padrões DCE e DTE, o DCE é o padrão utilizado pelos equipamentos de comunicação e fornecem essa taxa de leitura chamada aqui de "clock rate". Já um dispositivo DTE recebe esse relógio (clock) e se sincroniza com o que o DCE está enviando.

Por esse motivo o equipamento do provedor de serviços é DCE e do cliente ou empresa é DTE, senão como o provedor iria cobrar por velocidade se os clientes pudessem alterar ou mandar nesse parâmetro?

Em topologias de laboratório não temos os CSU/DSUs disponíveis, por isso utilizamos um artifício de colocar um cabo DCE em um dos roteadores e no outro um cabo DTE, simulando uma conexão real, porém sem o uso de CSU/DSU. Essa topologia se chama **back-to-back** ou **costa a costa**. Veja figura abaixo.



Em ambientes de laboratório temos então que inserir um cabo do tipo DCE em um dos roteadores e configurar a velocidade ou “clock rate” na interface onde esse cabo foi conectado para que o link entre os roteadores funcione.

Na prática, links seriais dedicados utilizam interfaces seriais nos roteadores, chamadas de WIC (WAN Interface Card) ou HWIC (High-Speed WAN Interface Card). Por exemplo, uma interface HWIC-1T possui uma (1) interface serial (T).

O que define se a placa será DCE ou DTE é o tipo de cabo conectado. Em ambientes reais utilizamos nos roteadores cabos DTE, os quais possuem dois modelos disponibilizados pela Cisco dependendo do tipo de conector na placa serial:

- **CAB-SS-V35-MT:** cabo V.35 DTE macho com conexão smart-serial para o roteador, normalmente utilizada com WIC-2T, HWIC-1T e HWIC-2T.
- **CAB-V35-MT:** cabo V.35 DTE macho com conexão DB-60 para o roteador, normalmente utilizada com WIC-1T.

Portanto, os cabos descritos acima são os que ligam o roteador ao cabo DCE do CSU/DSU da operadora de Telecom.

#### 1.4 Links WAN e o Modelo OSI – Links Seriais HDLC

Os links WAN, tais como circuitos dedicados, fornecem conectividade física, ou seja, um meio para transmissão pura e simples dos bits entre dois pontos.

Sabemos que isso não é suficiente, precisamos de um protocolo de camada 2 que monte um quadro para que esses bits trocados possam ser interpretados, removido o cabeçalho e enviado o pacote IP para a camada superior, lembre-se do processo de encapsulamento e desencapsulamento que estudamos no capítulo 2.

Os dois protocolos mais utilizados nesse tipo de conexão são o Point-to-Point Protocol (PPP) e High Level Data Link Control (HDLC). Conforme já citado, no CCENT vamos utilizar como protocolo WAN o HDLC sem entrar em detalhes, pois as demais opções são cobradas apenas no exame 200-105.

O HDLC é um protocolo da camada de enlace de dados do modelo OSI com orientação bit a bit, por isso ele pode ser utilizado em conexões seriais síncronas. O HDLC é um protocolo ponto a ponto utilizado em linhas privadas e não possui qualquer método de autenticação.

Além disso, ele é um método de encapsulamento padrão utilizado em routers Cisco para ligações através de ligações seriais síncronas. Portanto, sem configuração alguma uma interface serial Cisco já vem com o protocolo HDLC ativo.

Ele é um protocolo proprietário e não funciona com interfaces de outros fabricantes, somente entre roteadores Cisco. Abaixo segue o quadro do HDLC e a descrição dos seus campos.

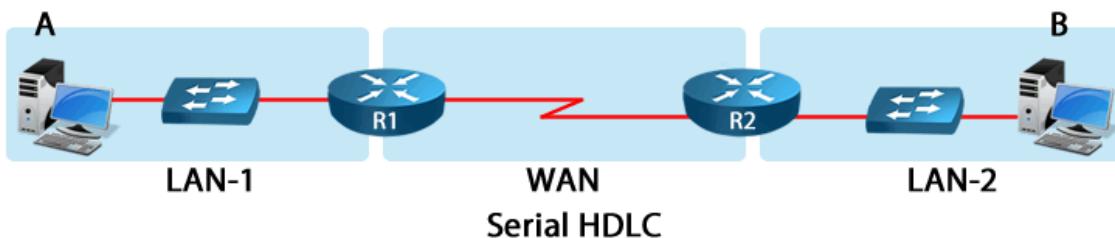
1	1	1	2	Variable	2	1
Flag 0x7E	Address	Ctrl 0x00	Protocol	Data	FCS	Flag 0x7E

- **Flag:** início e fim do quadro com o padrão 0x7E.
- **Address:** campo que identifica o tipo de quadro que está sendo enviado:
  - 0x0F – Unicast.
  - 0x80 – Broadcast.
- **Controle (Ctrl):** fixo em 0x00.
- **Protocol:** tipo de protocolo encapsulado no campo de dados, por exemplo, 0x0800 para IPv4 (utiliza o mesmo padrão do ethernet).
- **Data:** dados da camada superior, por exemplo, um pacote IP.
- **FCS:** checksum para verificação de erros, similar ao utilizado pela Ethernet.

Quando dois roteadores configurados com HDLC trocam informações elas são encapsuladas conforme o quadro mostrado acima.

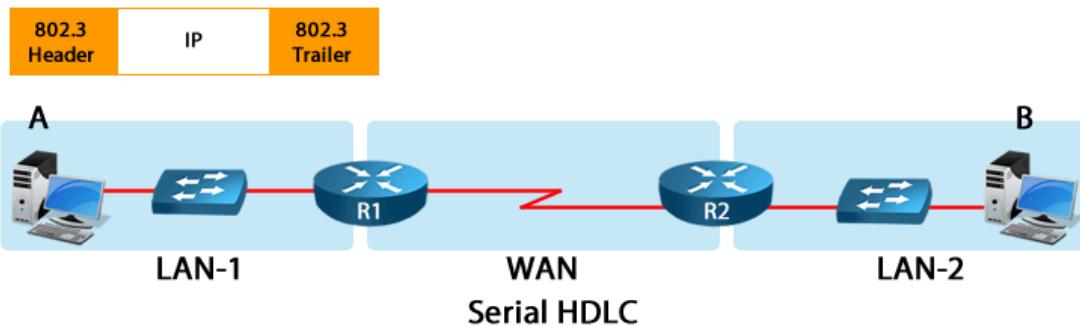
## 1.5 Enviando Informações Através da WAN

Vamos agora entender a dinâmica de envio de informações iniciadas em um LAN e que necessitam passar por uma WAN para chegar ao seu destino utilizando a topologia abaixo.



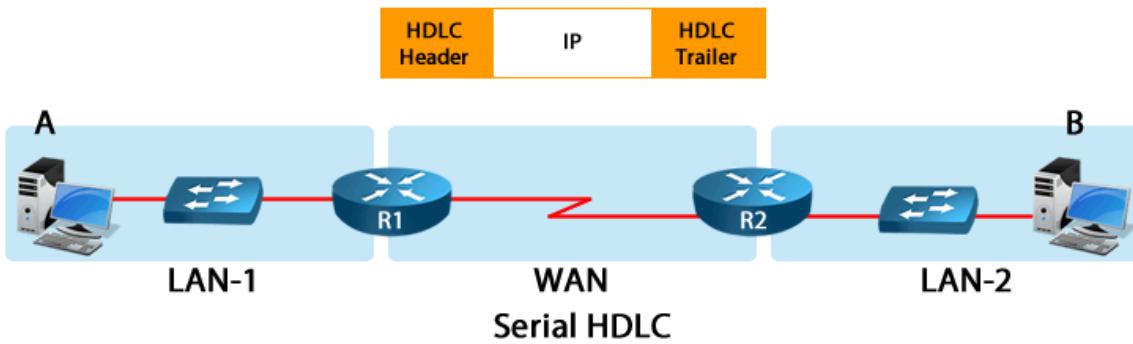
Nesse exemplo, o computador A deseja enviar informações para o computador B, porém os dois estão separados por uma rede WAN que é um link serial entre os roteadores R1 e R2.

No capítulo que estudamos as redes e endereçamento IP você vai aprender que o computador A tem um endereço da mesma rede que R1 e quando ele precisa falar para fora da sua rede o R1 será o intermediário, chamado gateway ou roteador padrão. Portanto, quando A for enviar pacotes para B ele irá direcioná-los para R1.



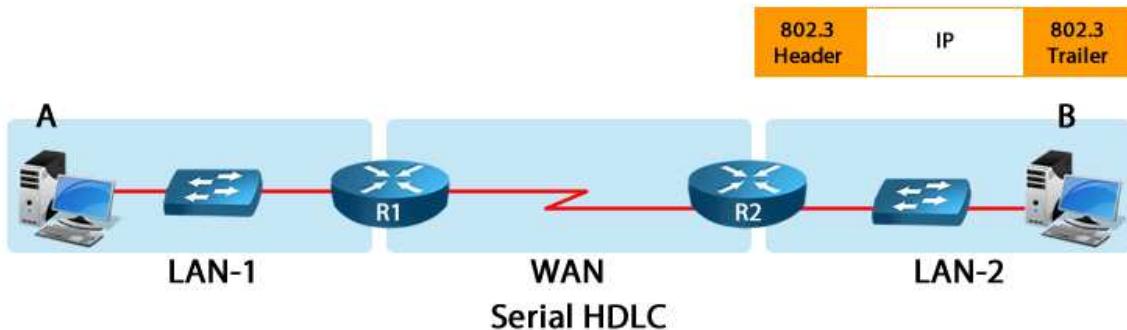
Ao chegar em R1 esses pacotes estão encapsulados em quadros ethernet, portanto R1 precisa desencapsular, analisar o endereço IP de destino do pacote (computador B) e decidir para onde encaminhar os pacotes.

Para tomar essa decisão R1 analisa sua tabela de roteamento e se tudo estiver correto descobre que precisa encaminhar esse pacote IP pela interface serial que está conectada com R2. Para isso R1 monta um quadro HDLC e coloca o pacote IP dentro do campo de dados do HDLC (payload), enviando as informações para R2.



Quando R2 recebe esse quadro ele desmonta para obter o pacote IP, analisa o endereço IP de destino do pacote e descobre que precisa enviá-lo para o computador B.

Como B está em uma LAN com padrão ethernet, R2 precisa agora montar um quadro ethernet e enviar para B, que recebe o quadro e repassa para as camadas superiores tratarem das informações e passarem para a aplicação de destino.



Claro que vários passos foram omitidos, os quais serão estudados no próximo capítulo mais específico sobre TCP/IP, porém com o exemplo mostrado aqui você já pode notar um dos segredos de sucesso do TCP/IP: "suportar diversos tipos de meio físico", o que o torna um protocolo de rede extremamente flexível, pois permite que as empresas, usuários e instituições se conectarem a rede utilizando o mais variado tipo de tecnologias possíveis.

## 2 Serviços de WAN

Conforme já estudamos, os serviços utilizados em uma WAN podem ser classificados como:

- **Leased Lines ou Circuitos Dedicados:** são links normalmente ponto a ponto e dedicados a apenas um cliente, ou seja, não há compartilhamento de banda entre outros usuários da operadora. São normalmente mais caros, porém tem sua banda garantida e são mais seguros pelo fato de não haver compartilhamento. Utilizam os protocolos HDLC e PPP na camada 2.
- **Circuitos Comutados ou Comutação por Circuitos:** são compostas pelas redes de telefonia convencional ou ISDN (rede digital de serviços integrados). São redes determinísticas, ou seja, um circuito fim a fim é criado quando uma chamada é estabelecida e o caminho é fixo do início ao fim da chamada.
- **Comutação por Pacotes:** essa é a opção mais econômica, pois permite a operadora compartilhar os recursos entre diversos clientes, como um link de Internet. O protocolo IP é o melhor exemplo de uma rede comutada por pacotes. O ATM, Frame-Relay e X.25 são exemplos de comutação por pacotes que podem ir de taxas de 56kbps a taxas acima de 34Mbps.

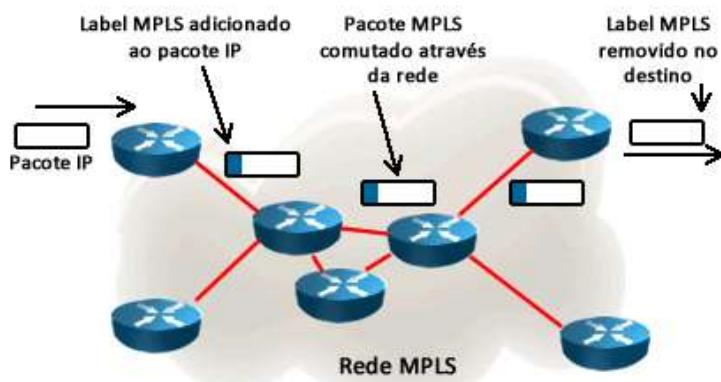
Existem algumas velocidades que as operadoras normalmente trabalham na comercialização de circuitos dedicados ou via comutação por pacotes:

- Nx64 (n vezes 64kbps): links que irão de 64kbps até 2048kbps variando de 64 em 64kbps (de 1 a 32 no Brasil e de 1 a 24 nos EUA). As mais comumente encontradas são links de 64kbps, 128kbps, 256kbps, 512kbps, 1024kbps ou 1Mbps e 2048kbps ou 2M.
- O padrão americano de velocidades é baseado em múltiplos de 64kbps, porém limitados de 1 a 24 circuitos de 64k:
  - T1: 1,5Mbps (24x 64k)
  - T2: 6Mbps (4x T1)
  - T3: 45Mbps (28x T1)
- O Brasil segue o padrão europeu baseado em normas definidas pela ITU-T e as velocidades são baseadas em links de 64kbps e agregados múltiplos de 2048kbps:
  - E1: 2048kbps ou 2Mbps (32x 64k)
  - E2: 8Mbps (4x 2M)
  - E3: 34Mbps (4x8M ou 16x E1s)
  - E4: 140Mbps (4x 34M ou 64x E1s)
- A partir de links de 140Mbps iniciamos com equipamentos síncronos (SDH ou DWDM) que transportam links a partir de 155Mbps, chamado de STM-1 com 63 x links de 2Mbps.

As velocidades acima são as tradicionalmente utilizadas em Telecomunicações, porém atualmente vem crescendo as ofertas de LAN-to-LAN, ou seja, a operadora entrega uma porta Ethernet, Fast ou Giga para os clientes interligarem suas redes utilizando a tecnologia MPLS encima de redes Ethernet, chamada de Metro Ethernet.

## 2.1 Introdução ao MPLS

O MPLS ou MultiProtocol Label Switching é uma tecnologia de encaminhamento de pacotes baseada em rótulos (labels) que funciona com base na adição de um rótulo (label) nos pacotes de tráfego na entrada do backbone (chamados de roteadores de borda) e, a partir daí, todo o encaminhamento pelo backbone passa a ser feito com base neste rótulo. Comparativamente ao encaminhamento IP, o MPLS torna-se mais eficiente uma vez que dispensa a consulta das tabelas de roteamento. O MPLS é indiferente ao tipo de dados transportado, podendo ser tráfego IP ou qualquer outro protocolo de camada 3. Veja a figura abaixo.



Este protocolo permite a criação de Redes Virtuais Privadas garantindo um isolamento completo do tráfego com a criação de tabelas de "labels" (usadas para roteamento) exclusivas de cada VPN.

Além disso, é possível realizar QoS (Quality of Service) com a priorização de aplicações críticas, dando um tratamento diferenciado para o tráfego entre os diferentes pontos da VPN. QoS cria as condições necessárias para o melhor uso dos recursos da rede, permitindo também o tráfego de voz e vídeo, sendo um dos diferenciais do MPLS.

## 2.2 Utilizando Ethernet na WAN - EoMPLS

Utilizar redes Ethernet em áreas Metropolitanas e geograficamente distribuídas através do uso conjunto da tecnologia Ethernet e do protocolo MPLS é chamado Ethernet over MPLS ou EoMPLS.

Esse conceito surgiu, pois, de acordo com alguns estudos, o tráfego de dados estaria superando o tráfego de voz convencional nas redes metropolitanas, portanto é mais interessante utilizar uma infraestrutura de transmissão de dados do que uma estrutura convencional TDM (Time Division Multiplexing) criada para a transmissão de voz, além disso, a tecnologia Ethernet é uma escolha lógica, devido ao seu baixo custo, flexibilidade e facilidade de manutenção e operação.

Utilizando esse tipo de serviço para o cliente existe a impressão que ele tem um link ethernet ponto a ponto, pois a meio de transmissão por entre os dispositivos da operadora é transparente. Veja a figura abaixo.



### 3 Acesso à 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).

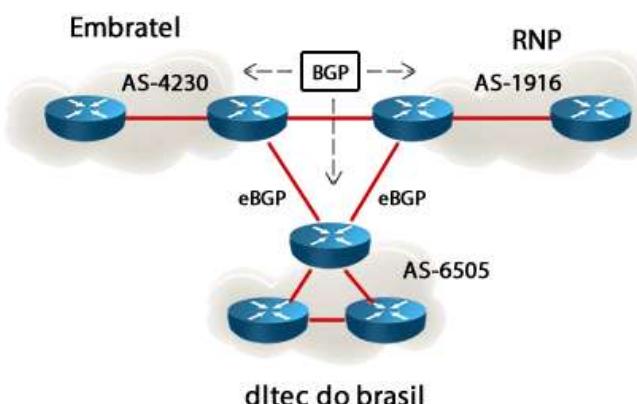
Os sistemas autônomos são identificados por números de sistema autônomo ou ASN (Autonomous System Number), seguem alguns exemplos de ASNs brasileiros:

- 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.

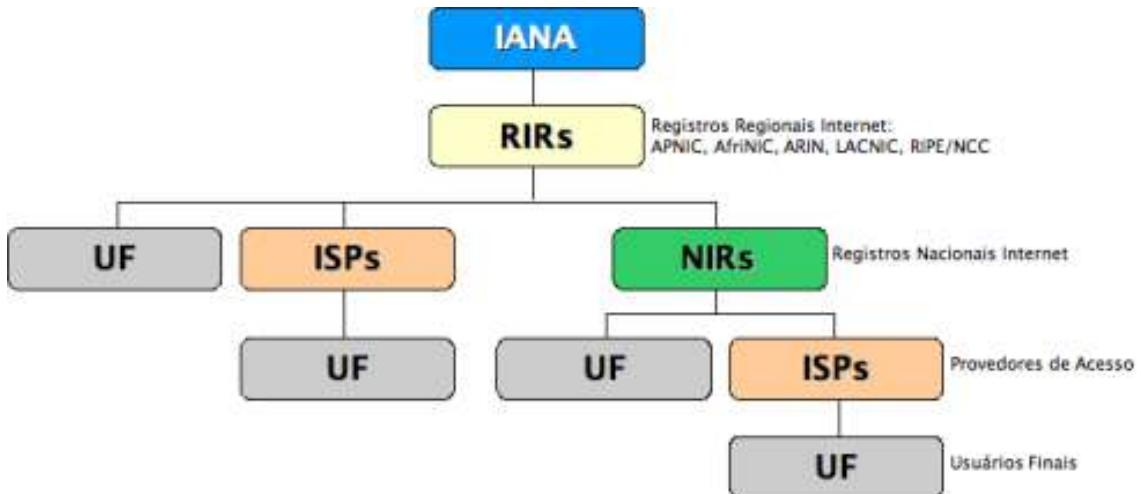


Os clientes que utilizam serviço de Internet sem ser um sistema autônomo utiliza um endereço IP da faixa alocada para o ISP a quem ele está conectado, é como se estivéssemos alugando aquele IP que utilizamos para acessar a Internet. Existem dois tipos de IPs que podemos utilizar nesse caso, o **fixo** 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.

### **3.1 Opções de Conexão à Internet**

Como atualmente todas as empresas precisam de acesso a serviços disponibilizados pela Internet e algumas até utilizam a Internet como link WAN através de VPNs vamos encontrar nas redes corporativas uma ou mais saídas para a rede mundial de computadores.

Essas saídas dependem do porte da empresa, mas podem ser classificadas em três tipos básicos:

- Acesso dedicado, tais como links seriais ponto a ponto de alta velocidade.
- Acesso banda larga:
  - Serviço DSL – Digital Subscriber Line, por exemplo, serviço ADSL.
  - Serviço via Cable modem fornecido por operadoras de TV a cabo.

Em redes de médio e grande porte os links de Internet dedicados são os preferidos, pois tem garantia de banda e são mais estáveis.

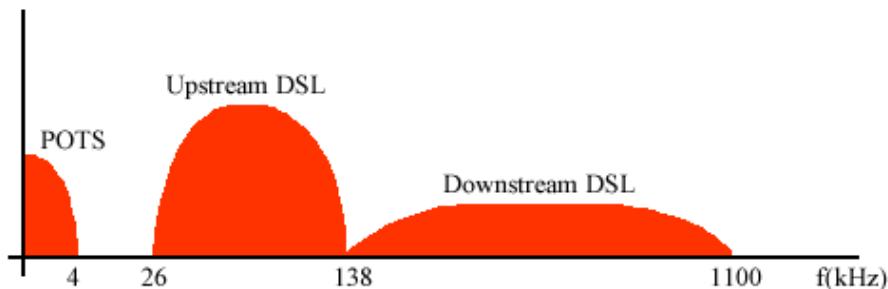
Já para conectar escritórios remotos de pequeno porte (small-office) ou usuários que trabalham em suas residências (home-office) as opções de banda larga são as mais utilizadas pela relação custo/benefício. Essa arquitetura de pequenos escritórios ou trabalhadores em home-office é chamada SOHO ou Small-Office/Home-Office. Normalmente é composta por um acesso banda larga e apenas um ou poucos computadores.

### 3.2 Entendendo o Acesso Banda Larga DSL

Os DSLs (Digital Subscriber Line ou xDSL) são tecnologias de comunicação de dados que permitem a transmissão de dados mais rápida através de linhas de telefone quando comparamos a taxa que um modem convencional pode oferecer, permitindo o compartilhamento da voz analógica tradicional com dados de alta velocidade (banda larga).

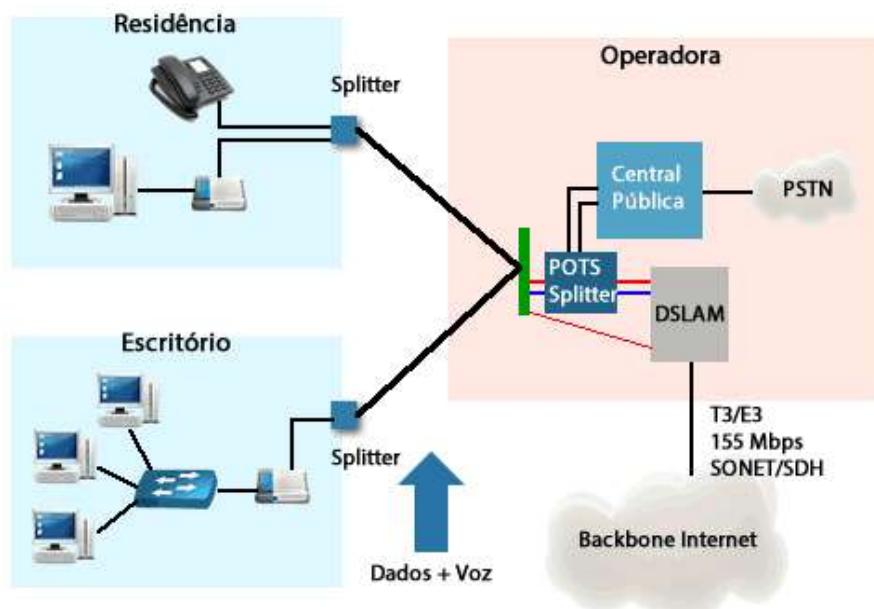
A grande vantagem das tecnologias xDSL, tais como o ADSL, é o aproveitamento da infraestrutura de pares metálicos utilizados pela rede de telefonia convencional para prover serviços de maior valor agregado à clientes residenciais e corporativos.

Uma das principais tecnologias é o ADSL, o qual foi concebido em 1989 através de modems chamados "assimétricos". O "A" da sigla ADSL se dá devido à transmissão ser assimétrica (Asymmetric), diferenciando-o de outros formatos, ou seja, teremos um canal de comunicação mais rápido para receber os dados (download ou downstream) e outro mais lento para enviar (upload ou upstream) os dados. Veja a figura abaixo.



O ADSL utiliza de técnicas de modulação (padrões da ANSI e ETSI usam os esquemas de modulação DMT) para a transmissão do sinal, ou seja, a voz ficará na faixa de frequência até 4kHz, enquanto o sinal de upload e download do ADSL em outras faixas de frequência, permitindo o uso do mesmo meio de transmissão para a voz e dados.

A topologia do ADSL integra duas redes que normalmente são distintas nas operadoras, a rede de voz convencional e a rede de dados. O ADSL terá um dispositivo que fará conexão via a tecnologia IP (normalmente utilizando ATM na camada 2) com a rede de dados e transformará esse sinal de dados em um padrão modulado, o qual será inserido junto com o sinal de voz no mesmo par metálico. No cliente ele será novamente dividido com um splitter (divisor de frequências) em dois sinais, um de voz que vai para seu telefone e outro de dados que vai para o modem ADSL. Veja o que foi explicado acima na figura a seguir.



Note que o equipamento que faz a interconexão com a Internet e gera o sinal ADSL é chamado de DSLAM ou "DSL Access Multiplexer". Ele é responsável por modular os dados em uma frequência que seja possível de passar pelo cabo metálico e chegar até as residências ou escritórios que utilizam o serviço de dados via ADSL. De outro lado temos uma central telefônica convencional ligada no mesmo par metálico e o seu sinal é misturado com o de dados antes de ser enviado na linha (POTS Splitter). Ao chegar à casa do cliente outro splitter fará a separação do sinal que irá para o telefone e para o modem ADSL, ou seja, separa a voz dos dados.

No lado do cliente podemos utilizar um modem ADSL, normalmente chamado de roteador ADSL, pois ele também acaba fazendo outros papéis dentro da rede dos clientes. Outras opções são utilizar uma placa de rede ADSL diretamente no computador ou então utilizar uma interface ADSL em um roteador comercial, por exemplo, uma WIC-1ADSL nos roteadores da Cisco.



Modem ADSL

Placa de Rede ADSL

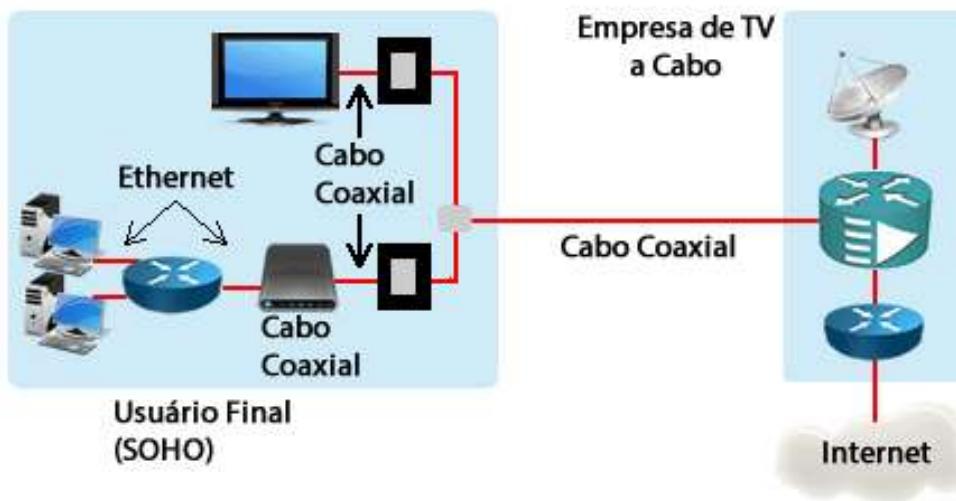


### 3.3 Entendendo o Acesso Banda Larga via Cable Modem

Assim como as tecnologias DSL tiram proveito da rede metálica existente para telefonia convencional para transmitir dados de alta velocidade, o cable modem utiliza o mesmo princípio, porém encima de uma rede de cabos coaxiais utilizadas para prover serviços de TV a cabo.

A banda larga via cable modem utiliza também faixas de frequências livres para envio de sinais de dados com intuito de conectar os assinantes de TV a cabo à Internet utilizando o mesmo meio físico, por isso as tecnologias DSL e Cable para banda larga tem muita similaridade, porém funcionam de maneira distinta uma da outra.

Na tecnologia de Cable sinal da Internet chega no mesmo cabo coaxial que o sinal de TV, um splitter é utilizado para conectar o mesmo cabo a um Cable Modem e ao Set-top-box (receptor de TV) do cliente. Veja figura abaixo.



Podemos concluir que ambas as opções de banda larga são interessantes para empresas que possuem pequenos escritórios remotos e funcionários que trabalham em suas casas, sendo que a melhor escolha depende da oferta local de serviços e preços oferecidos pelos provedores. Outro ponto importante na decisão é a largura de banda, pois muitas vezes os serviços de banda larga podem ter restrições de velocidade de acordo com a região em que o usuário final se encontra.

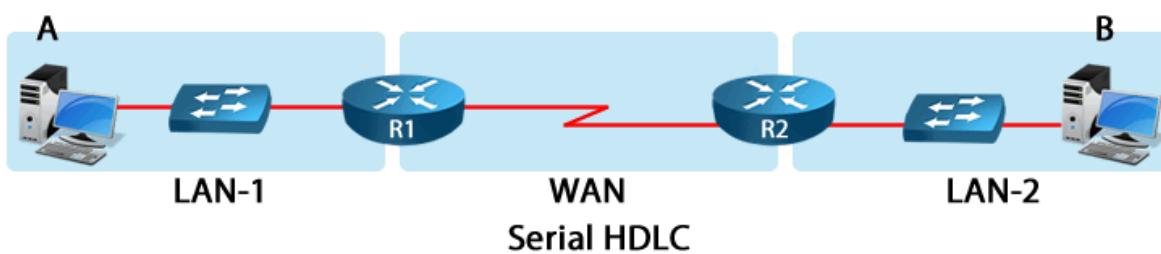
#### 4 Interpretando e Montando Topologias de Rede LAN e WAN

Nesse ponto do curso esperamos que você consiga entender uma topologia de rede, onde temos uma ou várias LANs interconectadas via uma rede WAN e também com uma ou mais saídas de Internet para que os usuários possam surfar na rede mundial de computadores.

Nesse tópico vamos estudar dois exemplos de análise e montagem de topologia seguindo requisitos de projeto.

##### 4.1 Interpretando e Montando Topologias – Exemplo 1

Voltando a topologia mais básica de rede com apenas duas unidades conectadas via um link serial vamos identificar os componentes, tipos de cabos necessários e demais características gerais. Veja a figura abaixo e tente responder às perguntas na sequência.



1. Qual o tipo de cabo o computador A utiliza para se conectar ao switch LAN-1?
2. Qual o tipo de cabo é utilizado entre o switch LAN-1 e o roteador R1?
3. Se conectarmos o computador diretamente ao roteador, qual tipo de cabo devemos utilizar?
4. Considerando que temos uma topologia de laboratório, qual o nome dado a essa topologia WAN?
5. Quais os tipos de cabo devem ser utilizados para conectar R1 a R2? Esses cabos são iguais? Porque?
6. Existe algum requisito específico necessário para essa conexão serial WAN ponto a ponto? Qual o requisito e para qual dispositivo ele se aplica?
7. Qual o tipo de cabo o computador B utiliza para se conectar ao switch LAN-2?
8. Qual o tipo de cabo é utilizado entre o switch LAN-2 e o roteador R2?
9. Se removermos os roteadores e conectarmos o switch LAN-1 ao LAN-2, qual tipo de cabo teríamos que utilizar entre eles?
10. Quantas redes IP precisamos no mínimo para endereçar essa topologia?

**Sugestão de prática:** volte aos laboratórios do capítulo 2 e analise as topologias propostas com os conceitos aprendidos nesse capítulo. Tudo deve ficar muito mais claro!

Ficou com dúvidas? Utilize os fóruns para perguntar.

## 4.2 Interpretando e Montando Topologias – Exemplo 2

Nesse segundo exemplo você deve desenhar uma topologia de rede, escolher os equipamentos e interfaces que devem ser conectadas.

A rede que você deseja montar possui dois escritórios, sendo que cada um deles deve ter seu acesso de Internet via banda larga própria e a conexão de Intranet entre eles deve ser feita utilizando um link serial dedicado ponto a ponto.

Cada unidade utilizará computadores através de cabo UTP e laptops sem fio.

Agora mãos a obra, faça um rascunho da sua topologia seguindo as recomendações acima!

Ficou com dúvidas? Utilize os fóruns para perguntar.

## 5 Introdução o Hardware e Inicialização de Roteadores Cisco

Seguindo o mesmo princípio do capítulo de redes locais onde iniciamos as configurações básicas dos switches da linha Catalyst, quando falamos de redes de longa distância o principal dispositivo de rede envolvido é o roteador (router), por isso vamos também estudar os conceitos relativos ao hardware de roteadores Cisco e configurações iniciais.

A diferença principal entre os roteadores e switches vem na diversidade e complexidade de recursos e protocolos que os roteadores suportam em relação aos switches, os quais também podem desempenhar muitas funções, porém no CCENT o foco dos switches é realmente no básico para fazer uma rede LAN funcionar, sem muitos “enfeites” e comandos adicionais.

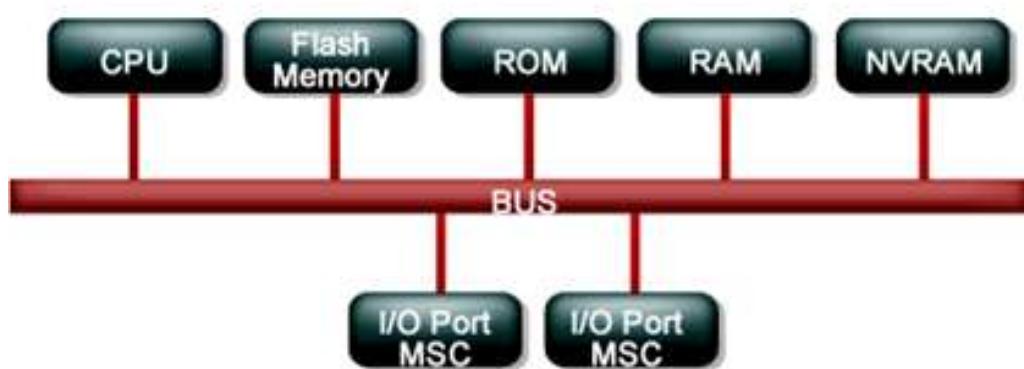
O roteador é um dispositivo situado na camada de rede do modelo OSI, o qual tem a principal função de fazer o roteamento dos pacotes dentro de uma rede de dados, que pode ser tanto na Internet como em uma Intranet.

O roteador pode também assumir outros papéis na rede, tais como de firewall, gateway H323 para voz sobre IP, servir como ponto de tradução de endereços IP via NAT ou PAT, e muitas outras funções, por isso a linha atual de roteadores Cisco é chamada de Multisserviços ou ISR G2 – Integrated Services Router Generation 2.

Os modelos que representam essas linhas de roteadores são das linhas Cisco 1900, Cisco 2900, Cisco 3900 e o Cisco 4451-X, além dos roteadores de menor porte da série 800.

Podemos dividir de maneira genérica o hardware um roteador da seguinte maneira:

- CPU (processador).
- Memórias (RAM, Flash, NVRAM e ROM).
- Interfaces (seriais, ethernet, fastethernet, ATM, etc.).
- Linhas de configuração (lines console, auxiliar e VTY).



Você vai notar que muita coisa permanece a mesma em relação aos comandos estudados no capítulo-3, pois as configurações básicas de roteadores e switches são idênticas, uma vez que ambos são baseados no sistema operacional IOS da Cisco.

O mesmo vale para as configurações dos roteadores, pois opções mais avançadas foram deixadas para o 200-105, onde realmente quem vai fazer deseja entrar na área de roteamento e switching e deve se preparar para o CCNP R&S e quem sabe até para o CCIE!

### **5.1 Sistema Operacional - IOS (Internetwork Operating System)**

O software Cisco IOS é um sistema operacional que fornece funcionalidade, escalabilidade e segurança comuns para os produtos da arquitetura Cisco.

O software Cisco IOS permite a instalação centralizada, integrada e automatizada, e o gerenciamento de internetworks, enquanto assegura o suporte a uma grande variedade de protocolos, meios, serviços e plataformas.

Assim como nos switches, o IOS do roteador é uma imagem gravada na memória flash e é carregado e executado na memória RAM quando ele é inicializado.

Atualmente os roteadores estão utilizando o IOS versão 15. A versão anterior se chamava 12.4.

## 5.2 Memórias

Vamos agora conhecer um pouco mais sobre os componentes internos de um roteador iniciando pelas memórias.



A diferença em relação a memória entre roteadores e switches é que a NVRAM em um switch é emulada dentro da memória flash, já no roteador as duas memórias são componentes distintos. Além disso, normalmente os roteadores possuem mais capacidade instalada que os switches quando tratamos das linhas básicas de equipamentos.

As memórias do roteador desempenham função essencial para o armazenamento das informações, a seguir serão descritos os tipos de memórias utilizadas e suas funções.

### 5.2.1 RAM/DRAM

Armazena tabelas de roteamento, cache ARP, cache de comutação rápida, buffers de pacotes e filas de espera de pacotes.

A memória RAM fornece também armazenamento temporário e/ou de execução para os arquivo de configuração do roteador (running-config) enquanto o roteador estiver ligado. O conteúdo da RAM é perdido quando você desliga ou reinicia o roteador, pois a RAM é uma memória volátil. Veja um exemplo de pente de memória RAM na figura a seguir.

**Memória RAM para o roteador Cisco 2821 de 256MB**



Para verificar o conteúdo da running-config utilize o comando "show running-config" em modo privilegiado, assim como fizemos para verificar as configurações dos switches.

### 5.2.2 NVRAM

A NVRAM ou Non-volatile RAM é uma RAM não volátil com função de armazenamento do arquivo de configuração de backup (startup-config) para inicialização de um roteador. O conteúdo será mantido quando você desligar ou reiniciar o roteador. Além disso, a NVRAM armazena o registro de configuração ou "config register".

Para verificar o conteúdo da startup-config utilize o comando "show startup-config" em modo privilegiado.

### 5.2.3 Flash

É uma ROM reprogramável que pode ser apagada. Ela contém a imagem e o microcódigo do sistema operacional, permite atualizar o software sem remover e substituir os chips no processador. Seu conteúdo será mantido quando você desligar ou reiniciar o roteador. Várias versões do software IOS podem ser armazenadas na memória Flash dependendo de sua capacidade. Outros tipos de arquivos podem também ser armazenados na memória flash de acordo com a necessidade da solução.



Para verificar o conteúdo da memória flash utilize o comando "show flash" em modo privilegiado.

### 5.2.4 ROM

É uma memória apenas de leitura que contém o bootstrap, diagnósticos de power-on e parte do sistema operacional. Sua atualização é feita através de substituição de chip, pois ela não é gravável.

## 5.3 Interfaces de LAN e WAN

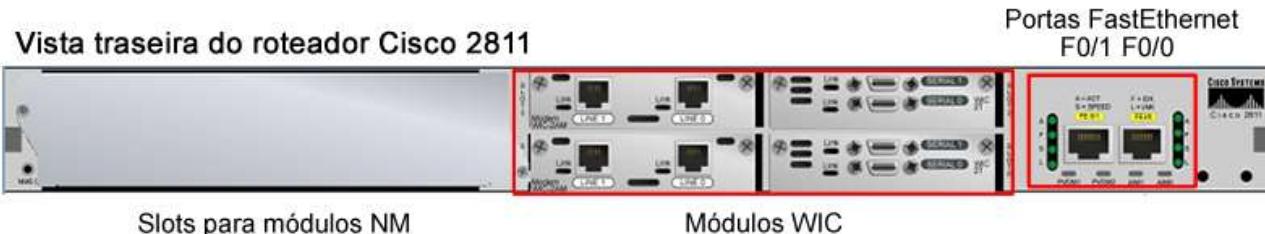
Existem diversos tipos de interfaces para os roteadores Cisco, porém o foco do curso será em interfaces do tipo serial, ethernet, fastethernet e gigabit ethernet.

Dependendo do modelo do roteador as interfaces podem ser de configuração fixa, ou seja, não há possibilidade de escolha, ou inseridas através de "slots".

Os roteadores da linha 2500 tem configuração fechada, por exemplo, o Cisco 2501 têm uma interface ethernet e duas seriais. Já equipamentos como os da linha 1700, 1800, 2600 e 2800 permitem a escolha do tipo de interface a ser utilizada.

É importante acostumar-se com o nome das interfaces, por exemplo, um roteador 2500 terá a interface "ethernet 0", "serial 0" e "serial 1". Em um 2600, o qual tem dois slots, você pode ter uma interface serial 1/0, ou seja, slot 1 interface 0.

Na figura abaixo temo um exemplo da vista traseira de um roteador Cisco 2811 onde podemos observar a localização das interfaces.



Na figura abaixo segue um exemplo de uma placa WIC-2T utilizada para conexões de linhas seriais.



Módulo WIC-2T para conexão de interfaces seriais

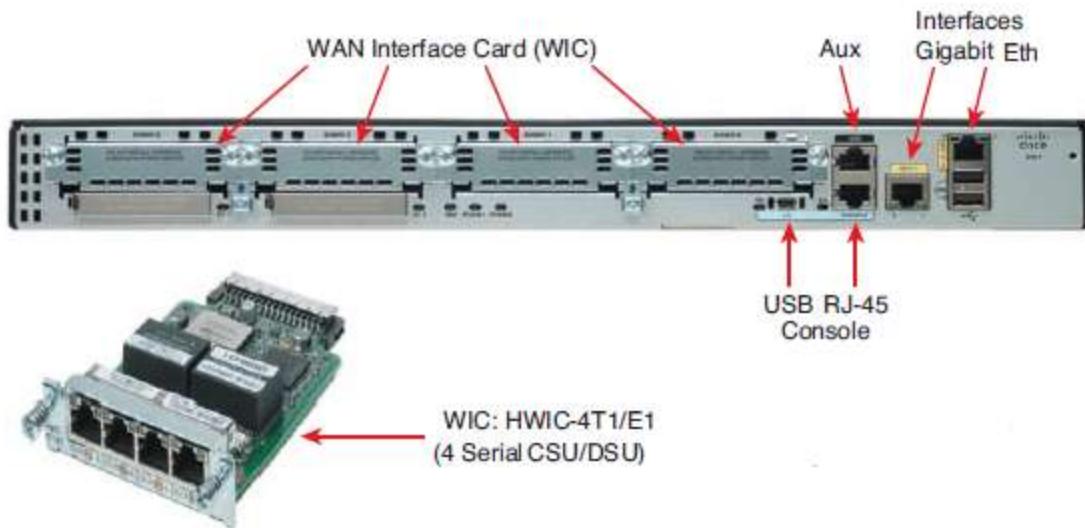
Na próxima figura temos uma placa WIC-2AM para conexões de linhas discadas.



Módulo WIC-2AM para conexão de linha discada

Já nos roteadores atuais da série ISR-G2 1900, 2900 e 3900 a numeração das interfaces é bem parecida com da série anterior ISR-G1 1800, 2800 e 3800 com dois ou três números separados por uma barra "/", por exemplo giga 0/0 e serial 0/0/0, porém nem todas as interfaces antigas são compatíveis com essa nova linha de roteadores.

Por exemplo, as interfaces de WAN WIC-1T e WIC-2T foram substituídas pelas HWICs, ou seja, agora temos a HWIC-1T e HWIC-2T. É importante sempre verificar antes de especificar uma interface ou software a compatibilidade entre versão e modelo de equipamento. Veja a foto abaixo da parte traseira de um roteador ISR-G2 modelo 2901 e uma interface WAN HWIC-4T1/E1.



É importante lembrar-se que para instalar ou remover módulos em roteadores das linhas citadas acima é necessário desligar o equipamento antes.

Veja na animação ao lado a saída do comando "show ip interface brief". Com esse comando podemos visualizar de forma rápida o estado de todas as interfaces do roteador.

#### 5.4 Linhas de Configuração (Console, Auxiliar e VTY)

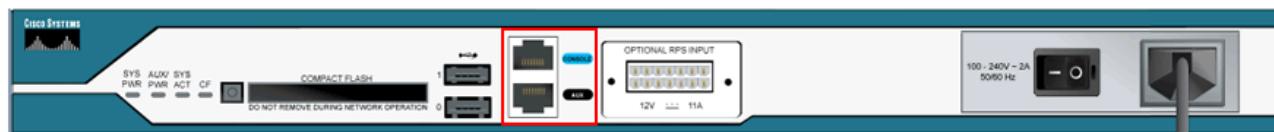
O acesso local e remoto através de Telnet/SSH de um roteador é idêntico ao que configuramos e estudamos para os switches.

A porta de console (line console 0) é utilizada quando queremos nos conectar diretamente (localmente) com o roteador ou switch.

Todo roteador ou switch Cisco possui uma porta console, onde nós podemos "plugar" um laptop para ter acesso ao equipamento. Geralmente a porta console está indicada pela cor azul no roteador. A configuração da porta console é realizada na line console.

Para um acesso remoto, via modem, utilizamos a porta auxiliar. A configuração da porta auxiliar é realizada na line auxiliar. Essa porta não está disponível nas linhas básicas de switches.

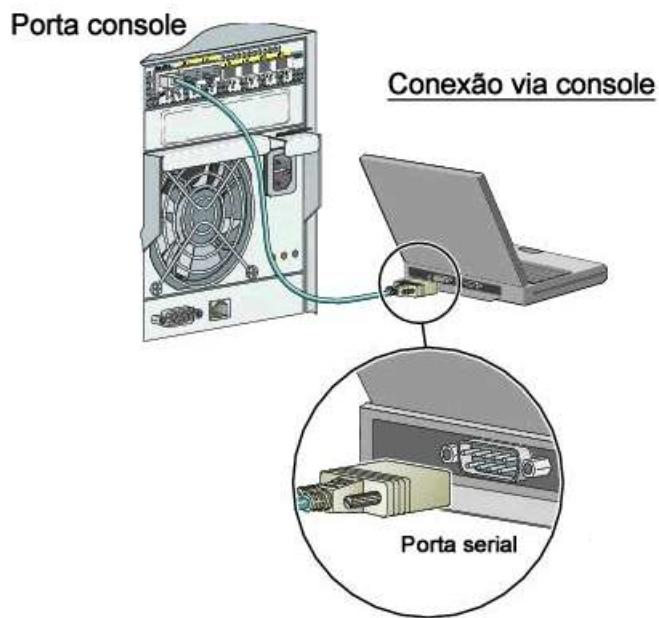
Veja a figura abaixo temos um exemplo de localização das portas console e aux em roteador Cisco2811.



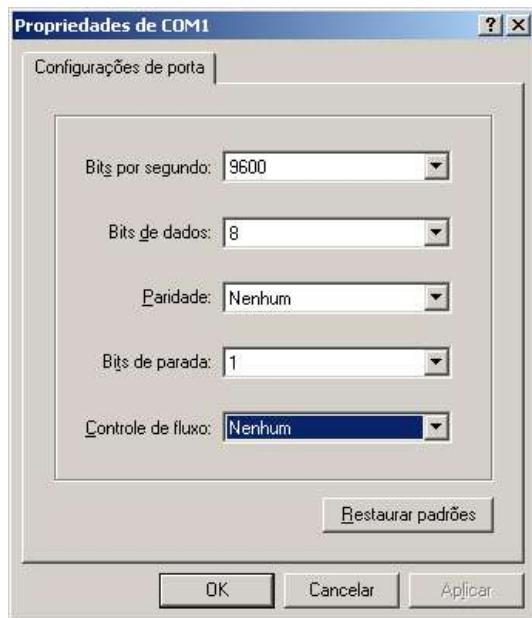
Vista frontal do roteador Cisco 2811

Porta Console e  
Porta Auxiliar

A conexão de um laptop na porta console é efetuada via um cabo de console ou cabo rollover da mesma maneira que fizemos para os switches. Veja a figura a seguir.



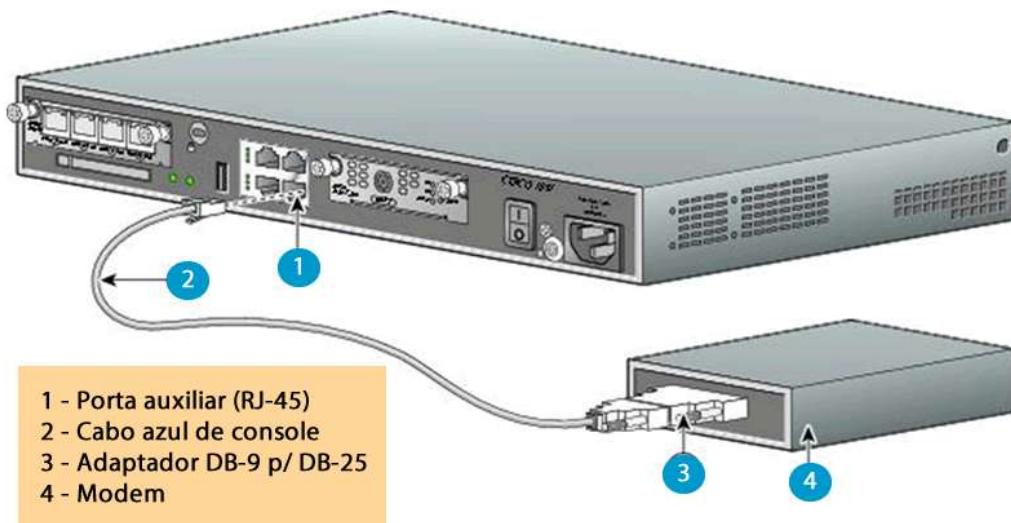
Já a configuração via console exige um programa emulador de terminal, como o teraterm ou hyper-terminal com a configuração conforme figura a seguir: velocidade de 9600bps, bits de dados 8, sem paridade, um bit de parada de sem controle de fluxo.



Já as linhas VTY são portas para conexão remota via telnet ou SSH (via rede IP). O número de conexões via telnet/SSH depende também do modelo do roteador, por exemplo, em um 2501 você tem 5 portas VTY (line vty 0 4), ou seja, cinco conexões simultâneas para acesso via telnet. Em roteadores da linha 2600 você irá encontrar 16 portas VTY (line vty 0 15).

O acesso via telnet é inseguro, por isso muitas empresas optam por ativar o SSH ou Secure Shell, o qual possibilita uma conexão segura e criptografada entre o computador de gerenciamento e o roteador ou switch. Veja a seguir uma animação com acesso telnet utilizando o Putty.

A porta auxiliar é conectada a um modem utilizando o mesmo cabo de console com um adaptador DB-9 para DB-25, pois a entrada serial dos modems é feita por um conector DB-25, ou então através de um cabo especial com uma ponta RJ-45 e outra em DB-25, porém ainda é um cabo do tipo rollover, assim como o cabo de console, porém somente com um conector diferente. Veja a figura abaixo.



O modem é conectado a uma linha telefônica comum para que possa ser realizado um acesso remoto discado (dial-up).

Outro uso da porta auxiliar é para realizar um backup discado, porém como a velocidade é muito baixa é somente para aplicações simples ou também possibilitar acesso remoto, portanto se a linha principal cair o roteador faz uma discagem para outro roteador para que seja aberta uma conexão de dados via a linha discada, assim como os antigos modems analógicos.

## 5.5 Revisando o Básico da CLI e Inicialização

Tudo que estudamos sobre como entrar na CLI, modos de operação EXEC de usuário e privilegiado, modos de configuração global, de interfaces e demais componentes para o switch valem para o roteador.

Lembre-se que se o roteador não tiver configuração você precisará se conectar via cabo de console e assim como estudamos para os switches o modo chamado Setup pode ser exibido, mais um indicativo que o roteador está “zerado”, ou seja, sem configurações.

Dependendo da versão de IOS os roteadores têm como padrão o usuário cisco e senha cisco pré-configuradas, necessitando ser alterado no primeiro acesso, normalmente informado em uma mensagem na inicialização, por isso é recomendável ao ligar um roteador que estava desligado com o cabo de console plugado e o terminal já aberto para verificar as mensagens.

Ainda sobre o modo setup, ele pode ser utilizado para configuração e mesmo você saindo no início pode chamá-lo a qualquer momento digitando "setup" em modo de usuário privilegiado, veja saída abaixo:

```
Router> enable
Password: <password>
Router# setup
    --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no] :yes
```

Ao digitar "Yes" para continuar a usar esse wizard de configuração várias perguntas serão apresentadas com o intuito de fazer uma configuração básica e ativar o acesso remoto via Telnet para que um administrador mais experiente finalize a configuração.

Uma dica importante é que quando for solicitada uma interface você precisará digitar o nome completo, veja o exemplo abaixo quando o setup pergunta a interface de gerenciamento:

```
management network from the above interface summary: gigabitethernet0/1
Configuring interface GigabitEthernet0/1:
Configure IP on this interface? [yes]: yes
IP address for this interface [10.10.10.12]:
Subnet mask for this interface [255.0.0.0] : 255.255.255.0
Class A network is 10.0.0.0, 24 subnet bits; mask is /24
```

Ao final das perguntas será exibida a configuração e a seguinte mensagem:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]: 2
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started! RETURN
```

Portanto você deve escolher se sai do setup sem salvar (0), retornar ao início do setup sem salvar (1) ou salvar e voltar ao modo de configuração (2). No exemplo acima a configuração foi salva.

## 5.6 Acessando Roteadores e Switches

Se o roteador ou switch já tiver sido configurado você pode ter no prompt a solicitação por uma senha ou usuário e senha, conforme configuração prévia realizada pelo administrador.

Se você conectou ao roteador via console e foi solicitado senha, essa é a senha de console configurada na "lina console 0". Para entrar em modo privilegiado devemos digitar "enable", se não houver senha configurada ele passa do prompt com sinal de maior (>) para sustentido (#), porém se houver uma senha de enable configurada será mostrado um prompt solicitando a senha, veja exemplo na saída abaixo:

```
Router con0 is now available
```

```
Press RETURN to get started.
```

```
User Access Verification
```

```
Password:
```

```
Router>enable
```

```
Password:
```

```
Router#
```

Para acesso remoto via telnet ou SSH é necessária a configuração da "line vty", sendo que por padrão a VTY aceita apenas conexões Telnet, o SSH necessita de configurações adicionais.

Para que o acesso Telnet seja habilitado corretamente o roteador ou switch deve ter um IP configurado e estar acessível, ter uma senha de enable configurada e também a senha na line VTY configurada. Se essas condições não forem satisfeitas a conexão remota será recusada pelo roteador.

Veja abaixo um exemplo onde o roteador tem o IP 192.168.1.1 respondendo, porém sem a line VTY configurada, por isso o telnet será rejeitado.

```
PC>ping 192.168.1.1
```

```
Pinging 192.168.1.1 with 32 bytes of data:
```

```
Reply from 192.168.1.1: bytes=32 time=7ms TTL=255
Reply from 192.168.1.1: bytes=32 time=2ms TTL=255
Reply from 192.168.1.1: bytes=32 time=2ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
```

```
Ping statistics for 192.168.1.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 1ms, Maximum = 7ms, Average = 3ms
```

```
PC>telnet 192.168.1.1
```

```
Trying 192.168.1.1 ...Open
```

```
[Connection to 192.168.1.1 closed by foreign host]
```

```
PC>
```

Agora vamos configurar a senha de VTY de modo simples como cisco e refazer o teste.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty 0 15
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#

```

Vamos ao computador fazer o telnet e tentar entrar em modo privilegiado, porém como não configuramos a senha de enable não será possível passar do modo EXEC de usuário.

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open
```

```
User Access Verification
```

```
Password:
Router>en
% No password set.
Router>
```

Agora vamos completar a configuração com a senha de enable secreta e ver o resultado.

```
Router(config-line)#exit
Router(config)#enable secret cisco
Router(config)#
```

Agora no computador vamos de novo com o comando enable tentar entrar em modo EXEC privilegiado, digitar a senha cisco e confirmar se funcionou.

```
Router>en
% No password set.
Router>enable
Password:
Router#
```

A autenticação que utilizamos para acesso local e remoto foi o mais simples possível, porém os dispositivos Cisco permitem o uso de autenticação local com usuário e senha ou através de servidor externo via padrões TACACS+ ou RADIUS utilizando o AAA. O AAA é matéria do CCNA Security, porém configurar um usuário e senha e ativar isso na VTY é bem simples, veja exemplo abaixo:

```
Router(config)#username dltec password dltec
Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#
```

Com o comando username/password criamos um usuário e senha para esse usuário, depois dentro da line VTY configuramos com o comando "login local" a autenticação com a base de dados local de usuários, com isso ao nos conectarmos via telnet será solicitado um usuário além da senha, veja exemplo a seguir:

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open
```

```
User Access Verification
```

```
Username: dltec
Password:
% Login invalid
```

```
Username: dltec
Password:
Router>
```

Note que erramos de propósito a senha na primeira tentativa e não foi permitido login via Telnet. Com essa configuração é possível até criar níveis de privilégio para diferentes usuários, porém esse assunto é do CCNA Security.

## 5.7 Configurações Padrões em Roteadores

Assim como estudamos para os switches, os roteadores Cisco também possuem uma configuração básica de fábrica que varia conforme a linha de equipamento e versão de IOS.

A diferença é que os roteadores têm todas as suas interfaces desativadas (em shutdown) por padrão e possuem suporte a camada 3, ou seja, nos roteadores as interfaces recebem endereços IP e fazem encaminhamento de pacotes (roteamento IP). Abaixo segue um exemplo de configuração padrão em um roteador modelo 7200.

```
R1#show running-config
Building configuration...

Current configuration : 1267 bytes
!
upgrade fpd auto
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex full
speed 1000
media-type gbic
negotiation auto
!
interface Serial1/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
ip forward-protocol nd
!
!
line con 0
```

```
line aux 0
line vty 0 4
line vty 5 15
!
end
```

R1#

Note que esse roteador possui quatro interfaces marcadas em amarelo na configuração, duas LANs e duas interfaces WAN seriais:

- Ethernet0/0
- GigabitEthernet0/0
- Serial1/0
- Serial1/1

Perceba nas interfaces os comandos “no ip address” e “shutdown”, removendo o endereço IP da interface e desabilitando-a respectivamente.

O hostname do roteador vem configurado como “Router” e nenhuma senha veio configurada por padrão.

Além disso, por padrão após a inicialização o roteador mostrará o modo setup, conforme estudamos para os switches no capítulo-3.

## 5.8 Verificando o Hardware e Memórias dos Roteadores com o Show Version

Antes de iniciarmos as configurações vamos estudar o comando show version executado em um roteador. A saída do comando muda um pouco em relação ao que estudamos para os switches.

O “show version” permite verificar algumas informações importantes sobre os equipamentos, tais como:

- O sistema operacional que foi carregado e está em execução no roteador;
- Quantidade de memória RAM/DRAM, Flash e NVRAM instaladas no roteador;
- Registro de configuração;
- O tempo que o roteador está ativo (em inglês Uptime) e o motivo do ultimo desligamento (reboot ou reload);
- Quantidade e tipo de interfaces/módulos instalados no roteador.

A quantidade de memória RAM e Flash que o roteador possui são muito importantes para definição do software IOS que pode ser instalado no dispositivo em caso de um Upgrade (instalação de uma versão mais nova de IOS), pois existem várias versões de IOS, cada uma com necessidades específicas, portanto dependendo da quantidade o roteador pode ser limitado a uma versão de sistema operacional mais simples. Veja na abaixo temos um exemplo do comando com os campos comentados.

```

Router>SHOW VER
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.0(5)T1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc. ( IOS IMAGE and RELEASE LEVEL )
Compiled Tue 17-Aug-99 13:57 by cmong
Image text-base: 0x80008088, data-base: 0x8072C5D4

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
      ( BOOT ROM LEVEL )

Router uptime is 3 minutes
System returned to ROM by power-on
System image file is "flash:c2600-i-mz.120-5.T1.bin" →
- Uptime
- Motivo do reload
- IOS que está sendo executado

cisco 2610 (MPC860) processor (revision 0x202) with 26624K/6144K bytes of memory
      ( TOTAL DRAM: 26624K + 6144K = 32MB )
Processor board ID JAD041108S0 (35972843)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0. →
Interfaces instaladas
1 Ethernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory. →
Quantidade de NVRAM
8192K bytes of processor board System flash (Read/Write)
      ( TOTAL FLASH 8192K = 8MB )
Configuration register is 0x2142 →
Registro de configuração

```

Vamos analisar os campos grifados de cima para baixo:

1. Versão de IOS que está rodando – 12.0(5)T1
2. Versão do bootstrap: 11.3(2)XA4
3. Tempo que o roteador está ligado (Uptime) – 3 minutos
4. Motivo da última reinicialização – por desligamento normal ou Power on
5. IOS que está rodando: o IOS está na flash e tem o nome c2600-i-mz.120-5.T1.bin
6. A quantidade de memória RAM é de 26624K mais 6144K, o que dá aproximadamente 32Mbytes de memória
7. Interfaces do roteador: apenas uma Ethernet 802.3
8. Quantidade de memória NVRAM (arquivo backup de configuração): 32Kbytes
9. Quantidade de memória flash (IOS e outros arquivos): 8192K ou 8Mbytes
10. Registro de configuração (o valor padrão deve ser 0x2102): 0x2142 (valor utilizado para recuperação de senhas)

Note que a quantidade de RAM ou DRAM vem separada em duas partes 26624K/6144K e você precisa somar esses dois valores para ter o valor total em Quilo Bytes. Lembre-se que um K byte não é 1000 e sim 1024!

## 5.9 Troubleshooting – Show versus Debug

Até o momento já mostramos alguns comandos show, os quais são utilizados para verificação do estado de determinados componentes do roteador ou switch, como se fosse uma foto até aquele momento.

Por exemplo, o comando “show ip interface brief” no roteador lista as interfaces, endereços e estado de cada uma delas, veja saída abaixo:

```
Router#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.1.1    YES manual up       up
FastEthernet0/1    unassigned     YES unset administratively down down
Vlan1              unassigned     YES unset administratively down down
Router#
```

Outro tipo de comando que pode ser utilizado para manutenção é o Debug, a diferença é que o debug vai além de dar um instantâneo da condição, ele mostra o funcionamento de determinado módulo ou recurso em tempo real, enviando mensagens à console por padrão, veja exemplo abaixo onde vamos fazer um “debug ip packet” para analisar todos os pacotes IP sendo recebidos pelo roteador.

```
Router#debug ip packet
Packet debugging is on

IP: tableid=0, s=192.168.1.2 (FastEthernet0/0), d=192.168.1.1 (FastEthernet0/0),
routed via RIB

IP: s=192.168.1.2 (FastEthernet0/0), d=192.168.1.1 (FastEthernet0/0), len 41,
rcvd 3

IP: tableid=0, s=192.168.1.1 (local), d=192.168.1.2 (FastEthernet0/0), routed via
RIB

IP: s=192.168.1.1 (local), d=192.168.1.2 (FastEthernet0/0), len 48, sending

IP: tableid=0, s=192.168.1.1 (local), d=192.168.1.2 (FastEthernet0/0), routed via
RIB
```

A partir desse momento todos os pacotes que chegam ao roteador fazem com que ele gere um log, ou seja, um registro desse evento. Imagine agora que você está em um roteador de um provedor de serviços de Internet e entra com esse comando em um horário de pico, o que você supõe que irá ocorrer? Simples, vai parar o roteador!

Isso mesmo, o debug é um comando que pode parar o roteador, pois ele pode consumir todo o recurso de processamento (CPU) e memória do roteador com o registro e envio dessas mensagens para o console. Por isso esse comando deve ser utilizado com muito cuidado.

Para desativar um debug podemos digitar “no debug all”, “undebbug all” ou “no” mais o debug específico que acionamos, nesse exemplo seria “no debug ip packet”. Os dois primeiros métodos desativam TODOS os debugs.

Note que tanto a ativação como a desativação foi realizada em modo privilegiado.

## 5.10 Logging Synchronous e Exec-Timout

Um problema que você irá notar é que o debug e outras mensagens geradas pelo roteador não respeitam a digitação, ou seja, se você está tentando digitar “udebug all” as mensagens do debug ativo vão entrar e se misturar com o que você está digitando.

Para melhorar um pouco existe o comando “logging synchronous” pode ser adicionado às configurações da VTY e console, assim a situação melhora um pouco, porém se o debug estiver gerando muitas mensagens ainda assim você terá problemas.

Veja um exemplo de configuração das lines mais completo abaixo:

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#logging synchronous
Router(config-line)#exec-timeout 5 30
Router(config-line)#line vty 0 15
Router(config-line)#login local
Router(config-line)#logging synchronous
Router(config-line)#exec-timeout 5 30
Router(config-line)#

```

Note que foi inserido um comando novo em cinza “exec-timeout 5 30”, por padrão os roteadores com usuário logado pela console ou VTY se não receberem comandos, ou seja, se o usuário ficar inativo, ele sai automaticamente em 10 minutos, como se fosse a proteção de tela nos computadores. Com o comando exec-timeout nós podemos alterar esse valor, sendo que no exemplo alteramos para 5 minutos e 30 segundos sem atividade o roteador sai do modo de operação que estiver e o usuário terá que se logar novamente para voltar às atividades com o dispositivo.

O comando “**exec-timeout 0 0**” desabilita o temporizador, porém deve ser utilizado apenas na fase de implantação dos equipamentos, porque se alguém deixar o roteador ou switch logado em modo privilegiado o próximo usuário vai entrar também assim, pois ele só vai sair do modo com um logout manual!

Para desativar essas mensagens que são enviadas ao console você pode utilizar o comando “**no logging console**” dentro da configuração global, porém se algo ocorrer com o roteador você não saberá, por exemplo, se uma interface cair, por exemplo, não será gerada a mensagem de UPDOWN informando esse evento na tela do seu terminal.

Quando estamos via Telnet ou SSH por padrão essas mensagens não são enviadas, você pode ativar o envio com o comando “**terminal monitor**” em modo privilegiado. Para desativar e voltar o padrão digite “**terminal no monitor**”.

## 6 Configurações Gerais em Roteadores e Switches – Revisão e Comandos Adicionais

Agora vamos iniciar as configurações gerais dos roteadores e switches. A maioria das configurações gerais são as mesmas, porém existem algumas diferenças que serão mostradas posteriormente.

Para ficar mais claro, dividimos as configurações dos roteadores e switches em blocos para facilitar o aprendizado. Dentro das configurações gerais estão comandos para:

- Definir senhas
- Banners
- Servidor DNS
- etc.

Uma dica importante antes de prosseguir é que vários comandos fazem parte do CCENT e você pode utilizar a facilidade de digitar parte dele, como já fizemos até o momento, porém para que você aprenda e acostume com a sintaxe é importante ou digitar o comando inteiro ou utilizar a tecla "Tab" (com as duas setinhas normalmente encima do Caps-Lock) para autocompletar o comando. Por exemplo, se digitarmos "ena sec cisco" o roteador entende como "enable secret cisco", porém você pode digitar "ena" e a tecla TAB para o roteador autocompletar para enable e assim por diante.

Portanto nos próximos tópicos e capítulos serão tratadas as configurações de interface e protocolos de roteamento separadamente. Lembre-se que, para fazer as configurações, você deve estar em modo de configuração global.

Lembrete: Para entrar no modo de configuração global você deve antes entrar no modo privilegiado ("enable"). Então em modo privilegiado utilize o comando "configure terminal" ou simplesmente "conf t".

Nesse modo o prompt do roteador deverá mostrar algo semelhante a "Router#(config)".

```
Router>enable  
Router#conf t  
Router(config)#
```

Sugestão: abra o packet tracer ou GNS3 e repita os comandos, lembrando que alguns comandos não são suportados pelo packet tracer e não vamos fazer essas especificações, pois o curso é de roteador e switch Cisco real e não do simulador!

### 6.1 Hostname

Vamos iniciar as configurações com o hostname, comando que define o nome do roteador. Isto facilitará a lembrar de qual roteador está sendo configurado.

Imagine que em uma rede de médio porte você poderá encontrar dezenas de roteadores e switches diferentes. A configuração do hostname ajuda a não confundir os equipamentos, evitando que você configure por engano o equipamento errado.

Caso não seja configurado nenhum nome de hostname os roteadores exibirão o prompt "Router" e os switches o prompt "Switch". Para alterar esse nome basta entrar com o comando "hostname nomedesejado". Assim que o comando for aceito o prompt do equipamento mudará para o nome configurado. Veja o exemplo de configuração de hostname abaixo.

```
Router>enable  
Router#conf t  
Router(config)#hostname MatrizCTBA  
MatrizCTBA(config)#
```

## 6.2 Senhas de Enable

Agora vamos definir a senha de "enable" como "cisco". Essa senha será solicitada quando alguém tentar entrar em modo privilegiado e o comando utilizado é o "enable secret cisco". O comando é o mesmo que utilizamos para o switch no capítulo-3.

Caso não seja configurada nenhuma senha de enable qualquer pessoa que acessar o equipamento poderá entrar em modo privilegiado e uma vez nesse modo toda e qualquer configuração pode ser realizada. Sendo assim, em nome da segurança de sua rede é altamente aconselhável que todo equipamento possua configurada uma senha de enable.

```
MatrizCTBA(config)#enable secret cisco
```

Lembre que esta senha é "case sensitive", ou seja, distingue entre maiúsculo e minúsculo.

Existem dois comandos que são utilizados com essa finalidade, o "enable secret" e o "enable password". A diferença é que o primeiro é armazenado criptografado e o segundo em texto claro, ou seja, se alguém visualizar a configuração do roteador e for configurada a senha com o comando "enable password", a pessoa poderá ver a senha configurada.

Já com o "enable secret" não. Por razões de segurança é recomendado sempre utilizar o "enable secret". O enable password, apesar de não ser recomendado utilizar, foi mantido nas versões mais novas de IOS por uma questão de compatibilidade com versões mais antigas, pois em algumas versões antigas do sistema operacional da Cisco o comando enable secret, assim se você copiar a configuração de um equipamento mais antigo e colar em um novo é melhor que ele venha com o enable password que fique sem nenhuma senha de controle de acesso ao modo privilegiado.

## 6.3 Senhas das Lines Console, VTY e Auxiliar

Vamos relembrar as configurações e mostrar a configuração da auxiliar, que é semelhante, porém não disponível em switches.

```
! Configuração do usuário e senha para acesso VTY e via Auxiliar
!
MatrizCTBA(config)#username dltec password dltec123
!
! Entrando na configuração das lines VTY de 0 a 4
!
MatrizCTBA(config)#line vty 0 4
!
! O comando Login local ativa a solicitação de
! Usuário e senha configurados localmente no comando username
!
MatrizCTBA(config-line)#login local
!
! O roteador sai desse modo após 5 minutos sem utilização
!
MatrizCTBA(config-line)#exec-timeout 5 0
!
! Sincronizando as mensagens com a digitação
!
MatrizCTBA(config-line)#logging synchronous
!
! comando utilizado para voltar um nível na configuração
!
```

```

MatrizCTBA(config-line)#exit
!
! Entrando na configuração da porta de console
!
MatrizCTBA(config)#line console 0
!
! Os comandos são os mesmos utilizados para VTY
! Porém com senha definida diretamente na console, sem usuário
!
MatrizCTBA(config-line)#password cisco
MatrizCTBA(config-line)#login
MatrizCTBA(config-line)#exec-timeout 5 10
MatrizCTBA(config-line)#logging synchronous
!
! Vamos configurar a aux 0
! Os comandos são os mesmos utilizados anteriormente
!
MatrizCTBA(config)#line aux 0
MatrizCTBA(config-line)#login local
MatrizCTBA(config-line)#logging synchronous
MatrizCTBA(config-line)#exec-timeout 5 10

```

Um detalhe importante é que as senhas das lines não são criptografadas como a senha de enable secreta, para que isso seja feito entre com o comando "service password-encryption" em modo de configuração global, como exemplo abaixo:

```
MatrizCTBA(config)#service password-encryption
```

Esse comando esconde as senhas na configuração (running-config e startup-config) com um hash (espécie de técnica de criptografia) proprietário da Cisco nível 7.

Veja a saída abaixo com um exemplo da aplicação desse comando onde vamos utilizar o comando show running-config com um modificador de saída (output modifier) e a opção "section" para visualização apenas da configuração das lines:

```

MatrizCTBA#show running-config | section line
line con 0
  exec-timeout 5 10
  password cisco
  logging synchronous
  login
line aux 0
  exec-timeout 5 10
  logging synchronous
  login local
line vty 0 4
  exec-timeout 5 10
  password cisco
  logging synchronous
  login
line vty 5 15
  exec-timeout 5 10
  password cisco
  logging synchronous
  login
MatrizCTBA#

```

Note que em destaque estão as senhas sendo mostradas, agora vamos inserir o comando para esconder as senhas e repetir o comando, veja abaixo:

```
MatrizCTBA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MatrizCTBA(config)#service password-encryption
MatrizCTBA(config)#do show run | section line
line con 0
  exec-timeout 5 10
  password 7 094F471A1A0A
  logging synchronous
  login
line aux 0
  exec-timeout 5 10
  logging synchronous
  login local
line vty 0 4
  exec-timeout 5 10
  password 7 045802150C2E
  logging synchronous
  login
line vty 5 15
  exec-timeout 5 10
  password 7 070C285F4D06
  logging synchronous
  login
MatrizCTBA(config) #
```

Perceba que em destaque pintado de amarelo está o comando e as senhas criptografadas com o nível 7.

Se você lembrar a senha de enable secreta tem um número “5” antes de mostrar a senha criptografada e no caso das senhas criptografadas com o “service password-encryption” o número na frente da senha é “7”.

Esses números indicam o “hash” utilizado (algoritmo utilizado para descaracterizar a senha). No caso do enable secret é utilizado um hash forte chamado MD5, já no caso do service password-encryption é utilizado um hash proprietário da Cisco e fraco, pois existem diversos sites que conseguem quebrar esse hash proprietário, basta copiar e colar o código dado como senha que uma rotina configurada no site quebra essa senha.

No link abaixo tem um site que quebra essa senha com hash nível 7 da Cisco, faça o teste e veja como é simples.

<http://www.ifm.net.nz/cookbooks/passwordcracker.html>

Outro detalhe sobre os comandos é que se você for bom observador notou falamos anteriormente que os comandos show e debug poderiam ser inseridos em modo privilegiado, mas como ele foi usado em modo de configuração global? Podemos inserir esses comandos em outros modos de configuração global com ajuda da opção “**do**”. O detalhe é que o autocompletar não funciona com esse comando!

Esse comando para esconder as senhas esconde TODAS as senhas em modo texto, inclusive o enable password e a senha definida no comando username.

Uma opção para definir um username já com senha segura é utilizar a opção “secret” ao invés de “password”, o comando “username dltec secret cisco” já cria a senha na configuração criptografada em MD5, assim como para a senha de enable segura.

#### **6.4 Comandos Relacionados ao DNS (Resolução de Nomes)**

O comando “**ip host**” permite que você adicione uma entrada estática de nomes, ou seja, é utilizado para mapear nomes e endereços IP.

Esse comando é similar a tabela de hosts utilizada antigamente. Quando você quiser fazer um telnet para uma máquina você poderá digitar somente o nome configurado com esse comando e seu roteador iniciará uma conexão com o host.

A sintaxe do comando segue abaixo, primeiro digite o nome do host e em seguida os IPs dele, caso deseje inserir mais de um endereço IP separe-os com espaço. Veja um exemplo abaixo.

```
MatrizCTBA(config)#ip host FilialPGO 167.10.56.100
```

O roteador pode utilizar o comando “ip host” ou então um servidor DNS para resolver nomes, assim como configuramos nos switches, inclusive esse comando “ip host” também é aceito pelos switches.

O servidor DNS pode ser configurado com o comando “**ip name-server**”. Neste caso para todo nome não conhecido pelo roteador será utilizado o servidor DNS do endereço configurado, no exemplo 223.8.151.10.

```
MatrizCTBA(config)#ip name-server 223.8.151.10
```

É padrão o roteador procurar por um DNS para resolver nomes, caso você deseje cancelar essa opção utilize o comando abaixo.

```
MatrizCTBA(config)#no ip domain-lookup
```

Para fazer com que o roteador volte a fazer a busca via DNS digite “ip domain-lookup”. O “no” remove uma configuração realizada. Para alterar um parâmetro basta redigitar o comando, pois maioria dos comandos não é cumulativo e sim substitutivo.

#### **6.5 Configurando Banners**

Existem maneiras de configurar mensagens de aviso aos usuários que estão se conectando aos roteadores e switches para informar sobre regras e normas da corporação ou avisos legais sobre acesso não autorizado. Para isso temos os seguintes tipos de banners mais importantes:

- **Message of the day** (MOTD – mensagem do dia): mostrado quando o usuário entra via console, aux ou VTY. Este banner é utilizado para mensagens temporárias, por exemplo, informar que entre 0h até 6h haverá manutenção naquele dispositivo.
- **Login**: mostrado após o banner MOTD e geralmente utilizado para enviar mensagens permanentes, tais como restrições de acesso ou mensagens legais: “Acesso restrito a TI”.
- **Exec**: mostrado após o usuário entrar em modo privilegiado e usado para mensagens que devem ser ocultas aos usuários sem privilégio.

Veja exemplo de configuração e como as mensagens são mostradas abaixo:

```
R1(config)#banner motd # --- Dia 06/08 haverá manutenção das 0h às 5h--- #
R1(config)#banner login @ --- Acesso restrito ao time de TI --- @
R1(config)#banner exec X --- Servidor 10.0.0.1 fora do ar acessar via 10.0.0.2 X
```

A configuração é feita em modo de configuração global e precisa de um símbolo para indicar o início e o fim da edição, os quais foram marcados em amarelo. O texto escrito entre esses índices é o texto que será mostrado.

Veja a seguir o exemplo de acesso após aplicada a configuração.

```
R1 con0 is now available
Press RETURN to get started.

*Jul 10 12:33:08.099: %SYS-5-CONFIG_I: Configured from console by console
--- Dia 06/08 haverá manutenção das 0h as 5h--- --- Acesso restrito ao time de
TI ---

User Access Verification

Password: --- Servidor 10.0.0.1 fora do ar acessar via 10.0.0.2
R1#
```

## 6.6 Salvando e Manipulando Arquivos de Configurações

Ao finalizar uma configuração é importante salvar esse arquivo na memória NVRAM (startup-config), pois tudo o que você fizer de configuração ficará na memória RAM (running-config), a qual é volátil e para não perder essa configuração ao reiniciar grave-a na NVRAM, ou seja, assim como estudamos para os switches o mesmo vale para os roteadores. Lembre-se do comando abaixo.

```
MatrizCTBA#copy running-config startup-config
```

Podemos também gravar essa configuração em um servidor externo utilizando o serviço de TFTP ou Trivial File Transfer Protocol. Na área do aluno, dentro da biblioteca disponibilizamos o 3Com Daemon, programa que ativa um servidor TFTP, FTP e de Syslog.

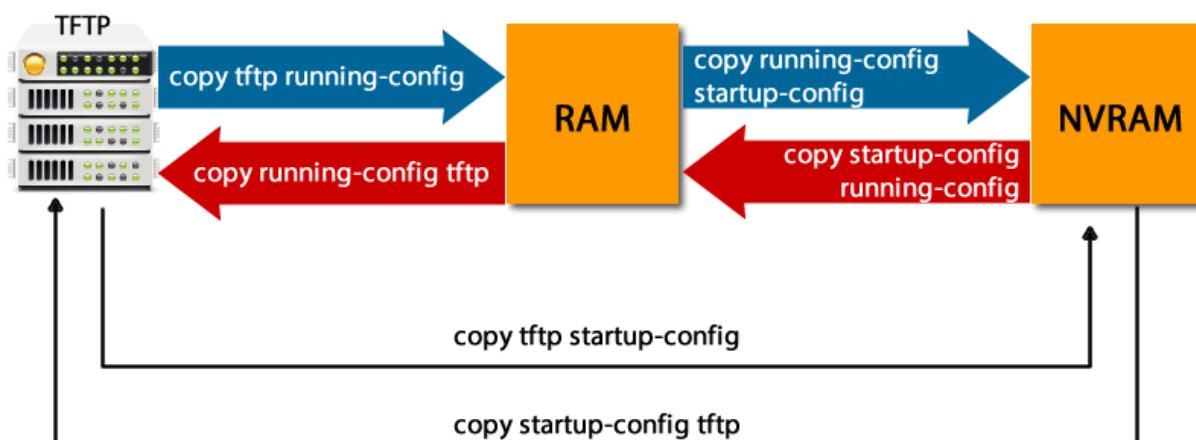
Para fazer a gravação desse arquivo no TFTP utilize o comando copy running-config tftp, veja exemplo abaixo:

```
SW-DlteC>en
Password:
SW-DlteC#copy running-config tftp
Address or name of remote host []? 192.168.1.71
Destination filename [sw-dltec-config]?
!!
13650 bytes copied in 1.594 secs (8563 bytes/sec)
SW-DlteC#
```

Os pontos de exclamação indicam sucesso, portanto agora na pasta padrão do servidor TFTP temos o arquivo chamado sw-dltec-config, o qual pode ser editado com o notepad, por exemplo.

Você poderia gravar uma cópia da configuração na memória flash também com o comando "copy running-config flash". O endereço IP do servidor TFTP nesse caso é 192.168.1.71 e ele deve estar ativo e permitir a conexão, em testes de laboratório verifique se o seu firewall não bloqueia esse serviço.

Lembre-se que o comando copy pede primeiro a origem e depois o destino do arquivo a ser gravado. Veja na figura abaixo um resumo de como você pode manipular os arquivos de configuração em roteadores e switches com o comando copy.



Os dois comandos destacados em vermelho, onde copiamos algo para a running-config não substituem o conteúdo atual da memória RAM e sim se mesclam a eles, fazendo um “merge”, ou seja, o resultado final não será exatamente o que foi copiado e sim uma mistura dos dois.

É importante mantermos backup das configurações e do sistema operacional para o caso de um equipamento ficar totalmente indisponível e a troca ser a única opção de voltar o serviço.

O mesmo pode ser feito para gravar um backup do sistema operacional, porém como o IOS está na memória flash o comando ficaria “`copy flash tftp`”.

### 6.7 Comparando com as Configurações do Capítulo-3 para Switches

Se você comparar o que estudamos para os roteadores em termos de configurações gerais com as configurações do capítulo-3 verá que apenas a linha auxiliar não está disponível nos switches, porém aqui não falamos de IP de gerenciamento, você sabe responder por quê?

O roteador tem por padrão o protocolo IP ativado (comando `ip routing`) por padrão e por isso suas interfaces têm suporta a camada 3.

Devido a esse fato os endereços IP do roteador são inseridos diretamente nas interfaces físicas, se você lembrar-se dos switches inserimos o IP em uma interface virtual chamada “VLAN 1”.

Outra diferença é em relação ao gateway padrão, nos roteadores não usamos o comando “`ip default-gateway`”, esse comando é utilizado apenas em dispositivos que não suportam roteamento IP, por isso utilizamos nos switches, pois aqui estamos estudando apenas os situados na camada 2.

### 6.8 Considerações sobre Questões Simuladas no Exame

Normalmente nesse momento muitos alunos perguntam: “Ok, mas em um laboratório simulado que pode ser cobrado na prova de certificação o que eu devo configurar?”.

A resposta é: “O que for solicitado na questão!”. Se você colocar configurações a mais não tem problemas, desde que estejam corretas, porém a menos você perde ponto.

Por exemplo, uma questão pede para configurar um roteador com o nome R1, senha de acesso privilegiado cisco, senha de console cisco1 e senha de telnet cisco2 a configuração será:

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret cisco
R1(config)#line console 0
R1(config-line)#password cisco1
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco2
R1(config-line)#login
R1(config-line)#end
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Mas e os banners, criptografia das senhas, ip host, DNS...? Se não foi pedido não precisa configurar. Outro ponto é sobre salvar as configurações, se o comando estiver disponível salve se não estiver não se preocupe.

Normalmente em questões práticas em simulador o help (?) está disponível, porém se não estiver você precisará digitar os comandos, por isso aconselhamos a utilizar no mínimo o recurso de autocompletar.

## 6.9 Atividade Prática

Agora vamos fazer o laboratório 4.1.

A partir desse laboratório começaremos a construir a configuração de uma topologia de redes completa. Essa topologia irá ser utilizada em vários laboratórios ao longo desse curso, de forma que, ao longo do curso iremos inserir novas configurações nessa topologia até que a rede esteja operacional.

Por isso fique atento e guarde a topologia final desse laboratório para que você possa utilizá-la novamente quando for solicitado.

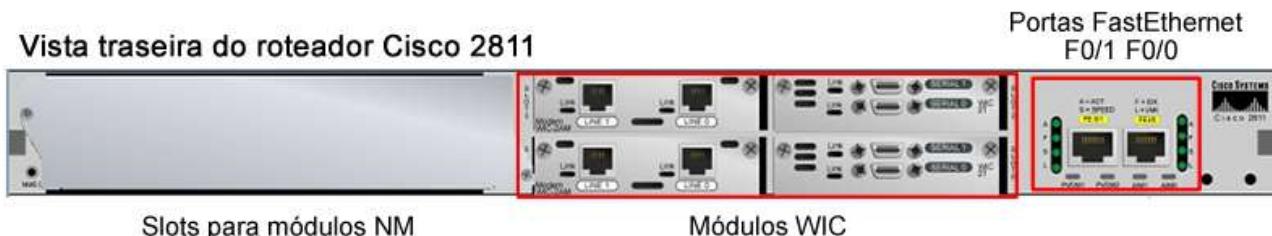
A topologia que iremos configurar é a mostrada ao lado. O arquivo da topologia está disponível para download na página do curso "**Topologia\_lab4.1.pkt**". Faça o download desse arquivo, pois nos exercícios propostos no laboratório iremos configurar os equipamentos.

No decorrer dessa atividade iremos aprender a inserir as configurações básicas dos equipamentos, como por exemplo:

- Configuração de hostname,
- Configuração de banners,
- Configuração de senhas,
- etc.

## 7 Configurações de Interface em Roteadores

Nesse capítulo trataremos das configurações referentes às camadas de enlace e redes do modelo OSI necessárias para a ativação de interfaces Seriais (PPP e HDLC), Ethernet, Fastethernet ou Gigabitethernet.



Apesar de não termos visto ainda nada sobre endereçamento IP vamos mostrar essas configurações com endereços e máscaras pré-definidas, ou seja, você precisará apenas inserir os dados fornecidos no exercício. Não se preocupe ainda com o que é um endereço IP, pois vamos estudar com detalhes no próximo capítulo.

Os dados transmitidos na rede são recebidos através de uma interface LAN (ethernet, fastethernet, gigabit-ethernet, token-ring ou FDDI), então os cabeçalhos da camada 2 são removidos e os pacotes são enviados para a RAM. Quando estas ações acontecem, a CPU analisa o endereço IP de destino, examina suas tabelas de rotas para determinar a porta de saída dos pacotes e o formato no qual os pacotes devem ser encapsulados.

Este processo é chamado de **process switching**, no qual cada pacote deve ser processado pela CPU que consulta as tabelas de rota e determina para onde enviar os pacotes. Os roteadores Cisco possuem outro processo chamado de **fast switching**. Nesta forma de processo, o roteador mantém um cache na memória com informações sobre o destino dos pacotes IP e a próxima interface, a qual pode ser outra interface LAN ou WAN (serial, ATM, POS – Packet Over Sonet, ISDN e outras). Os protocolos de roteamento serão mais bem analisados nos próximos capítulos.

Para entrar na configuração da interface, você deve estar em modo de configuração global e digitar o comando "interface", veja um exemplo na animação a seguir.

Dependendo do tipo de roteador as interfaces recebem uma nomenclatura diferente. Por exemplo, em um roteador 2501, o qual tem a configuração fixa, ou seja, sem slots para inserção de placas, a primeira interface serial é "serial 0", a segunda é a "serial 1" e a interface ethernet é a "ethernet 0". Para você saber as interfaces que um roteador possui utilize o comando **"show ip interface brief"**.

Abaixo segue um exemplo:

```
MatrizCTBA#show ip interface brief
Interface          IP-Address      OK?    Method   Status   Protocol
FastEthernet0      10.0.0.1        YES    NVRAM    up       up
Serial0            167.10.10.1     YES    NVRAM    up       up
Serial1            192.10.10.1     YES    NVRAM    up       up
MatrizCTBA#
```

Em roteadores mais novos a configuração é flexível e você encontrará slots para inserção de módulos conforme necessidade. O formato da numeração das interfaces segue o padrão número-do-slot/número-da-Interface. Por exemplo:

- Ethernet 0/0 (primeiro slot – primeira interface);
- Serial 1/2 (segundo slot – terceira interface);
- Serial 0/1 (primeiro slot – segunda interface);
- Fastethernet 1/0 (segundo slot – primeira interface);

Lembre-se que o primeiro slot é o “0” e a primeira interface também é a “0”.

Na linha ISR-G1 e ISR-G2 podemos encontrar três números para definir as interfaces separados por uma barra “/”, por exemplo, em um Cisco 1941 temos dois slots para encaixar WICs (módulos de interface WAN), se inserirmos duas HWICs 1-T (placas com uma interface) teremos as interfaces serial 0/0/0 e 0/1/0.

## 7.1 Interfaces LAN - Ethernet, Fastethernet e Gigabitethernet

Interfaces ethernet/fastethernet/gigabitethernet são utilizadas em redes LAN, sendo que atualmente é mais comum encontrarmos interfaces fastethernet ou gigabitethernet nos roteadores.

Os comandos básicos para ativar interfaces ethernet / fast / giga, seriais e ISDN são:

- **ip address**: define o IP e a máscara de rede/subrede a ser utilizada.
- **description**: insere uma descrição da interface que pode ser visualizada no comando “show interfaces”.
- **shutdown** e **no shutdown**: o comando “shutdown” desabilita a interface e o “no shutdown” habilita a interface.

Quando a interface está shutdown no comando “show interfaces” aparecerá que a interface está “**administratively down**”.

Abaixo segue um exemplo de configuração de uma interface Fastethernet utilizando o endereço IP 10.0.0.1 e a máscara de rede 255.0.0.0.

```
MatrizCTBA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MatrizCTBA(config)#int f0
MatrizCTBA(config-if)#ip address 10.0.0.1 255.0.0.0
MatrizCTBA(config-if)#description int F0 conectada a porta 01 do switch-1
MatrizCTBA(config-if)#no shutdown
```

Por padrão as interfaces vêm no estado “administratively down”, ou seja, desligadas e para tirar uma interface desse estado deve-se utilizar o comando “no shutdown” no modo de configuração dessa interface.

```
MatrizCTBA(config)#interface f0
MatrizCTBA(config-if)#no shutdown
```

Depois de realizada a configuração e o cabo da porta ter sido conectado ao Hub ou Switch o status da interface deverá passar de “Down” para “Up”, o que quer dizer que a porta está pronta para transmitir os dados. Você pode verificar o status da interface com o comando “show interfaces” ou “show ip interface brief”.

A seguir uma saída típica do comando “**show interfaces**”. Na primeira linha é mostrado o status conforme abaixo.

```
MatrizCTBA#show interfaces
FastEthernet0 is up, line protocol is up
    Hardware is PQUICC_FEC, address is 000a.f414.2b51 (bia 000a.f414.2b51)
    Description: interface F0 conectada a porta 15 do switch-1
    Internet address is 10.0.0.1/8
    MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Full-duplex, 100Mb/s, 100BaseTX/FX
    ARP type: ARPA, ARP Timeout 04:00:00
    Last input 00:02:14, output 00:00:04, output hang never
    Last clearing of "show interface" counters never
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: fifo
    Output queue: 0/40 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
        62 packets input, 10893 bytes
        Received 62 broadcasts, 0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
        0 watchdog
        0 input packets with dribble condition detected
        1313 packets output, 109465 bytes, 0 underruns
        5 output errors, 0 collisions, 2 interface resets
        0 babbles, 0 late collision, 0 deferred
        5 lost carrier, 0 no carrier
        0 output buffer failures, 0 output buffers swapped out
```

Na saída do comando mostrado acima podemos observar a frase "FastEthernet0 is up, line protocol is up". O primeiro "up" está relacionado a interface física, quer dizer que o cabo está ok. Já o segundo "up" representa a parte lógica da camada de enlace e quer dizer que os quadros podem ser transmitidos e recebidos normalmente.

Caso haja problema com o cabo, normalmente a interface ficará "FastEthernet0 is Down, line protocol is Down".

Se houver problemas na camada de enlace, ou seja, na parte lógica, a saída ficará "FastEthernet0 is up, line protocol is down".

Já a condição "FastEthernet0 is down, line protocol is up" nunca ocorrerá, pois não tem como passar informações lógicas se o meio físico estiver danificado.

Além disso você pode alterar as opções de operação half ou full-duplex e para as interfaces 10/100/1000Mbbs você pode escolher a velocidade desejada, porém o padrão é que essas configurações sejam detectadas automaticamente.

Para alterar esses parâmetros, você deve assegurar-se que os dados estejam corretos e ter em mente que em caso de troca dos switches talvez sejam necessárias alterações nessas configurações. Abaixo seguem os comandos para configurar a velocidade e o modo de transmissão half ou full duplex:

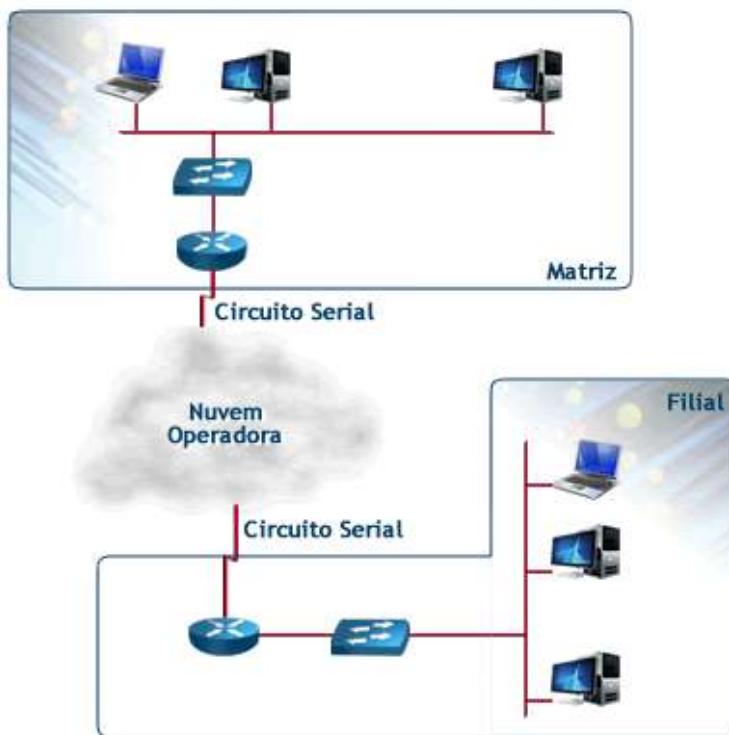
```

MatrizCTBA(config-if)#speed ?
 10   Force 10 Mbps operation
 100  Force 100 Mbps operation
 auto  Enable AUTO speed configuration
MatrizCTBA(config-if)#duplex ?
 auto  Enable auto duplex configuration
 full   Force full duplex operation
 half   Force half-duplex operation

```

## 7.2 Interfaces Seriais

Interfaces seriais são utilizadas em redes de longa distância (WAN) para conexões ponto a ponto ou ponto-multiponto.



Para interligações das redes WAN é necessário utilizar a infraestrutura de uma operadora de telecomunicações, a qual pode oferecer diversos tipos de soluções e interfaces de WAN para seus clientes. Os tipos mais comuns de tecnologia WAN são:

- Linhas dedicadas utilizando HDLC ou PPP (nx64kbps – 64k a 2048kbps)
- Links Frame-relay
- Linhas DSL (ADSL e HDSL) e Cable Modem

As interfaces seriais utilizam cabeamento específico e interfaces como:

- EIA/TIA-232
- EIA/TIA-449
- V.35 (utilizado para conectar um CSU/DSU)
- X.21 (utilizado para X.25)
- EIA-530

Os três tipos de protocolos de camada-2 mais comuns suportados pelas interfaces seriais são:

- **HDLC**: proprietário da Cisco e padrão nas interfaces seriais.
- **PPP**: o point-to-point protocol é um padrão aberto e suporta autenticação.
- **Frame-relay**: é um protocolo aberto, estatístico e que permite compartilhamento de recursos por parte da operadora.

Lembre-se que existem dois tipos de cabos para conexão WAN: DTE e DCE. O DTE é o que normalmente utilizamos nos roteadores e o cabo DCE normalmente é o cabo que vem no equipamento da prestadora de serviços de telecomunicações. Porém, por questões de laboratório teremos que utilizar uma topologia chamada costa-a-costa ou back-to-back, na qual usamos um roteador diretamente conectado ao outro.

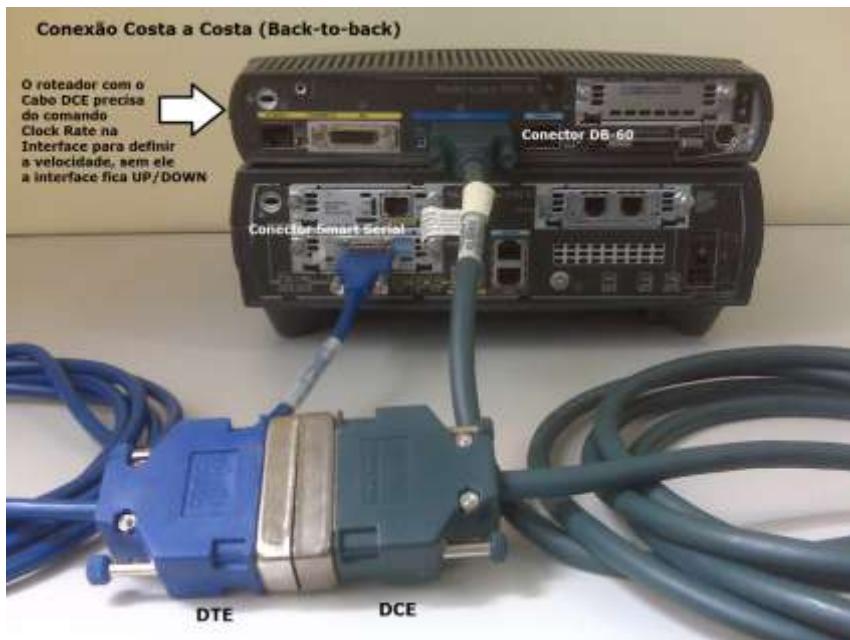
Por esse motivo um dos roteadores terá que simular a Operadora com um cabo DCE, fornecendo clock ou a temporização (velocidade do link), e o outro roteador fará o papel normal com um cabo DTE, se sincronizando com o equipamento DCE.

Você verá no próximo capítulo que um equipamento DCE precisa em sua interface um comando a mais: "**clock rate**", o qual define a taxa de bits que a interface irá funcionar.

Veja figura abaixo com a foto dos cabos DCE e DTE com os tipos de conectores DB-60 e Smart-serial ilustrados. Em ambiente de laboratório com equipamentos reais precisamos de um cabo de cada modelo desses abaixo para conectar as interfaces seriais.



Abaixo temos dois roteadores costa a costa um com cabo DCE e outro com cabo DTE, inclusive nos laboratórios práticos do exame do CCENT esse conceito das conexões costa a costa pode ser cobrado!



Na prática os roteadores são conectados aos CSU/DSUs das operadoras e, conforme já comentado, é conectado com um cabo DTE ao dispositivo da operadora que é DCE e fornece o clock para o circuito de dados.

### 7.3 Configurando Links Seriais HDLC

O protocolo HDLC em roteadores Cisco tem um formato proprietário, não podendo ser configurado para comunicação entre equipamentos Cisco e diferentes fabricantes.

Além disso, ele é o protocolo padrão das interfaces Seriais, mesmo que você não utilize o comando “**encapsulation**” para definir o protocolo de camada 2, o roteador da Cisco se autoconfigura como HDLC.

Veja um exemplo de configuração completa abaixo de uma interface serial com HDLC que possui um cabo DCE conectado.

```
MatrizCTBA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MatrizCTBA(config)#interface serial 0
MatrizCTBA(config-if)#ip address 200.171.51.1 255.255.255.252
MatrizCTBA(config-if)#bandwidth 128
MatrizCTBA(config-if)#clock rate 128000
MatrizCTBA(config-if)#description Serial 0 conectada a FilialPGO
MatrizCTBA(config-if)#encapsulation hdlc
MatrizCTBA(config-if)#no shutdown
MatrizCTBA#
```

Como as interfaces seriais utilizam o protocolo HDLC como padrão, ou seja, se você não utilizar o comando “**encapsulation**” sua interface será automaticamente configurada como HDLC.

Observe que o comando “**clock rate**” deve ser utilizado somente quando a interface serial estiver conectada a um **cabo DCE**, no caso da interface DTE não é necessário definir o “**clock rate**”, apenas o “**bandwidth**”.

Portanto, o comando **clock rate** é dado em bits por segundo e define a velocidade física que a interface irá trafegar, por exemplo, se você deseja uma velocidade de 1Mbps você deve digitar "clock rate 1000000" (um milhão de bits por segundo).

Já o comando **bandwidth** é utilizado apenas pelos protocolos de roteamento dinâmicos que tem como métrica a taxa da interface, por exemplo, o EIGRP e o OSPF. O valor do **bandwidth** é dado em kilo bits por segundo, por isso é o valor do **clock rate** divididos por mil. No exemplo da taxa de 1Mbps o **bandwidth** ficaria com o valor 1000 (bandwidth 1000).

Se você não configurar o comando **bandwidth** em interfaces seriais por padrão roteador arbitra a velocidade de um link T1 para a interface, ou seja, 1.5Mbps, o que pode trazer problemas para os cálculos dos protocolos de roteamento se as interfaces seriais tiverem velocidades variadas.

Dependendo do equipamento o valor do **clock rate** é pré-definido e você não pode digitar outros valores, caso você tenha tentado digitar um valor e recebeu uma mensagem de erro utilize para descobrir os valores permitidos o comando **Help** da seguinte maneira "**clock rate ?**".

Se você não configurar comando **bandwidth** a interface DCE ou DTE não irá parar de funcionar, porém se ela for DCE e você esquecer-se do **clock rate** a interface não funcionará e ficará com o status "UP/DOWN", ou seja, a camada física está OK, mas a camada de enlace não, pois você não definiu sua velocidade.

No packet tracer as interfaces seriais são representadas por um "raio" e a DCE é a que tem um **relógio** na figura, se você fizer a conexão utilizando esse ícone o primeiro router que você clicar será o DCE e o segundo será o DTE.

Para verificar se a interface é DCE ou DTE utilize o comando "**show controller serial [nº-da-serial]**". Veja exemplos abaixo (a saída foi suprimida e somente parte do comando foi inserido no texto).

### **Exemplo 1: Cabo desconectado**

```
show controllers serial 0
Interface Serial0
Hardware is PowerQUICC MPC860
No serial cable attached
```

### **Exemplo 2: Cabo DCE conectado**

```
show controllers serial 0
Interface Serial0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 128000
```

Para verificar as configurações podemos utilizar os comandos "show running-config", "show interfaces" e "show ip interface brief".

Você pode também ver somente o status da interface específica com o comando "show interface serial 0", conforme exemplo abaixo:

```
MatrizCTBA#show interface serial0
Serial0 is up, line protocol is up
Hardware is PowerQUICC Serial
Description: Serial 0 conectada a FilialPGO
Internet address is 200.171.51.1/30
```

```

MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:03, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 96 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
509 packets input, 36414 bytes, 0 no buffer
Received 509 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
519 packets output, 38532 bytes, 0 underruns
0 output errors, 0 collisions, 16 interface resets
0 output buffer failures, 0 output buffers swapped out
2 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
MatrizCTBA#
```

Vamos descrever algumas informações úteis sobre o comando show interfaces conforme campos grifados e na sequência:

1. **Serial0 is up, line protocol is up** → campo que indica o estado operacional da interface, queremos que esteja UP/UP.
2. **Description:** Serial 0 conectada a FilialPGO → descrição configurada com o comando description.
3. **BW 128 Kbit** → largura de banda configurada no comando bandwidth.
4. **509 packets input** → pacotes recebidos pela interface, se estiver zerado ou não sendo incrementado quer dizer que a interface não está recebendo pacotes.
5. **519 packets output** → pacotes enviados pela interface, se estiver zerado ou não sendo incrementado quer dizer que a interface não está enviando pacotes.

**Lembrete:** Os demais campos do comando serão estudados em capítulos posteriores.

#### 7.4 Verificação das Configurações e Troubleshooting Básico

Uma vez definida a topologia, as configurações gerais que faremos nos roteadores e as redes IPs que configuraremos nas interfaces disponíveis o passo seguinte é aplicar as configurações.

Portanto, mesmo resolvendo um exercício prático em uma prova é importante termos uma **sequência ou uma metodologia para sua resolução**, é importante entender o que está sendo pedido, planejar rapidamente a configuração e depois passar para a execução, ou seja, aplicar as configurações.

Para verificar se o que fizemos está realmente correto isso podemos utilizar os comandos show que aprendemos até o momento e também o próprio conceito de funcionamento dos equipamentos, por exemplo, para testar se um banner do dia foi configurado corretamente você pode sair do roteador e entrar novamente para verificar o banner exibido.

O mais aconselhável é iniciar verificando as configurações com o comando "**show running-config**", pois nele temos todas as informações que inserimos.

Já estudamos que tanto os roteadores como os switches vêm com uma configuração básica padrão, note na saída do comando na abaixoo mais uma vez a configuração padrão de um roteador Cisco 2620XM, o qual tem por padrão em seu chassi apenas uma interface Fastethernet e as lines de console e auxiliar.

```

Router#show running-config
Building configuration...

Current configuration : 329 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
ip classless
!
line con 0
line vty 0 4
login
!
end

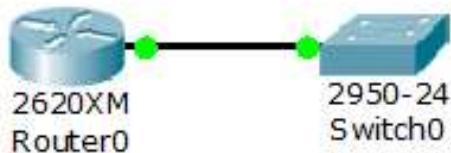
```

Router#

Portanto alguns comandos já estão inseridos de fábrica e dependem da versão de IOS que você está utilizando no equipamento, mas em termos gerais o roteador tem o hostname **Router** e os switches **Switch**.

Agora vamos fazer a configuração geral do roteador 2620XM, conectá-lo a um e verificar o show running, você pode fazer essa configuração utilizando o packet tracer. Dados a serem configurados (veja a figura a seguir):

- Nome do roteador Dltec-Teste (hostname)
- Senha de acesso privilegiado secreta dltec123 (enable secret)
- Banner do dia: Config de Teste – Capítulo 6
- Senhas de acesso a console e telnet (VTY): cisco
- Configurar a criptografia das senhas em modo texto
- Endereço IP da interface fastethernet: 192.168.1.1
- Máscara da interface fastethernet: 255.255.255.0



Veja os comandos de configuração e a saída do show running-config a seguir. Faça a comparação do show run mostrado no início com o roteador zerado e o novo pós-configuração mostrado na abaixo. É importante que você saiba encontrar os parâmetros de configuração, pois em algumas questões práticas você precisará analisar o show run e descobrir problemas ou determinados parâmetros pedidos nos exercícios.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host
Router(config)#hostname DlteC-Teste
DlteC-Teste(config)#enable secret dltec123
DlteC-Teste(config)#line cons 0
DlteC-Teste(config-line)#pass cisco
DlteC-Teste(config-line)#login
DlteC-Teste(config-line)#line vty 0 15
DlteC-Teste(config-line)#pass cisco
DlteC-Teste(config-line)#login
DlteC-Teste(config-line)#exit
DlteC-Teste(config)#service password-encryption
DlteC-Teste(config)#banner motd # Config Teste - Cap 6 #
DlteC-Teste(config)#interface fastEthernet 0/0
DlteC-Teste(config-if)#ip add 192.168.1.1 255.255.255.0
DlteC-Teste(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

DlteC-Teste(config-if)#end
DlteC-Teste#
%SYS-5-CONFIG_I: Configured from console by console

DlteC-Teste#
DlteC-Teste#show running-config
Building configuration...

Current configuration : 533 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname DlteC-Teste
!
enable secret 5 $1$mERr$QJxDeNCP2Xze0Xk2Hvlxr.
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
ip classless
!
banner motd ^C Config Teste - Cap 6
^C
!
line con 0
```

```

password 7 0822455D0A16
login
line vty 0 4
password 7 0822455D0A16
login
line vty 5 15
password 7 0822455D0A16
login
!
!
end
DlteC-Teste#

```

Para se certificar que os IPs das interfaces foram configurados corretamente e se elas estão ativas você pode utilizar o comando "show interfaces" ou "show ip interface brief", veja a saída do comando a seguir.

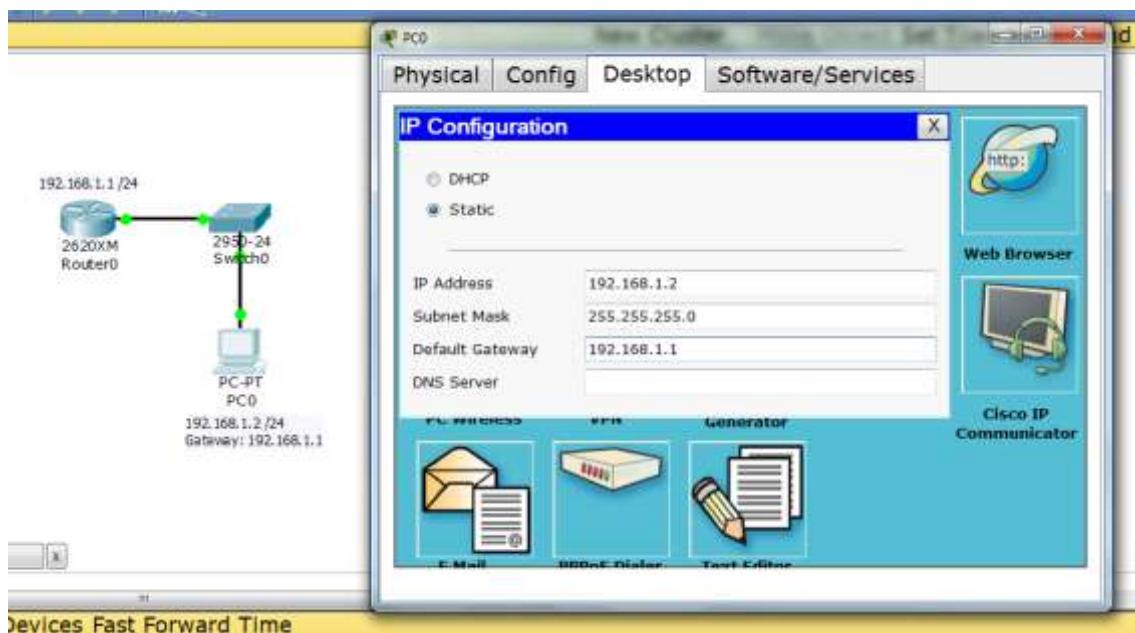
```

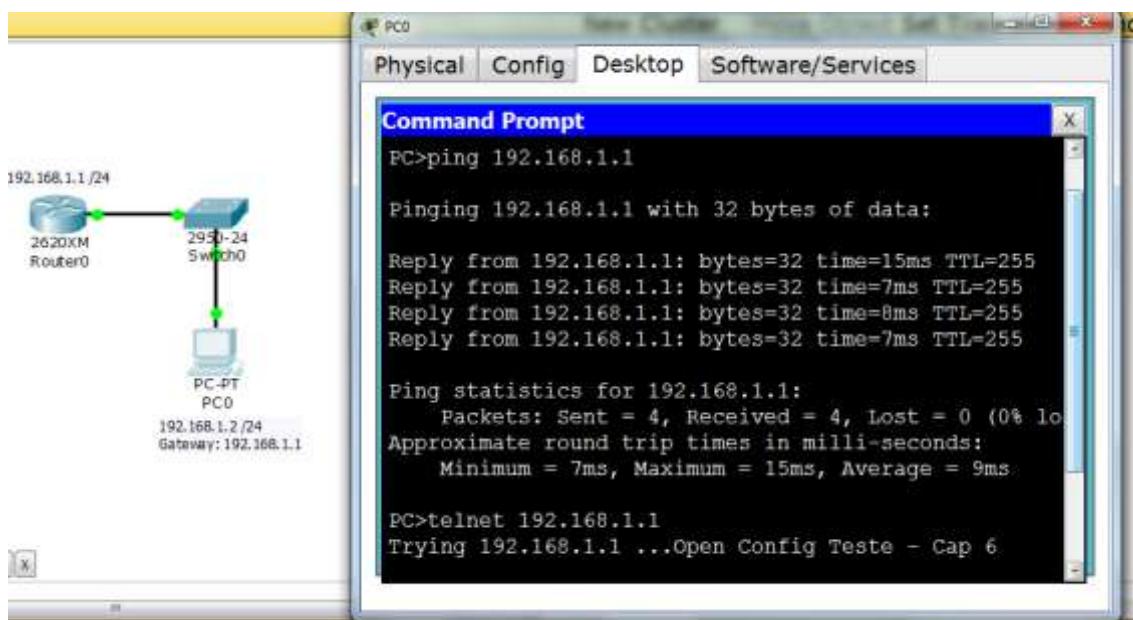
DlteC-Teste#sho ip interface brief
Interface          IP-Address      OK? Method Status   Protocol
FastEthernet0/0    192.168.1.1    YES manual up        up
DlteC-Teste#

```

Note que temos a interface, o IP que está configurado nela, se ela está OK ou não, o método de configuração (manual, dhcp, etc.), o status da camada física e o status da camada de enlace (Protocol). É importante nesse comando verificar o IP configurado e se a interface está **UP/UP**.

Outro teste interessante é inserir um computador na topologia, configurá-lo na mesma faixa de IPs do roteador e fazer testes de ping e telnet. Veja as figuras a seguir baseadas no packet tracer.





#### 7.4.1 Verificando a Configuração do Protocolo IP das Interfaces

Para verificar a configuração da interface já estudamos anteriormente o comando “**show running-config**” e “**show running-config interface serial 0/0/0**”, o qual mostra a saída apenas da interface que você deseja analisar. Esse segundo comando não é suportado no Packet Tracer. Veja exemplo abaixo.

```
DlteC-FW-GW#show running-config interface fastEthernet 0/0
Building configuration...

Current configuration : 231 bytes
!
interface FastEthernet0/0
  description $FW_INSIDE$
  ip address 192.168.10.2 255.255.255.0
  duplex auto
  speed auto
end

DlteC-FW-GW#
```

Também estudamos o comando “**show ip interface brief**” que dá o IP configurado e o estado da interface, sendo que o primeiro Up/Down é da camada física e o segundo da camada de enlace. Acompanhe no exemplo abaixo.

DlteC-FW-GW#show ip interface brief

Any interface listed with OK? value "NO" does not have a valid configuration

Interface		IP-Address	OK?	Method	Status
Protocol					
FastEthernet0/0	192.168.10.2	YES NVRAM	up		up
FastEthernet0/1	unassigned	YES NVRAM	up		up
FastEthernet0/1.10	192.168.1.1	YES NVRAM	up		up
FastEthernet0/1.20	10.0.1.1	YES NVRAM	up		up
FastEthernet0/1.30	192.168.2.1	YES NVRAM	up		up
Loopback1	10.10.10.10	YES NVRAM	up		up
DlteC-FW-GW#					

Uma outra forma é utilizar o comando “**show interfaces**” ou “**show interfaces serial 0/0/0**”, porém esses comandos mostram informações mais detalhadas das interfaces. Bem no começo da saída eles trazem a máscara de rede ou sub-rede e endereço MAC da interface, informações que não são mostradas no comando anterior. Além disso, mostram também detalhes de contadores das interfaces. Veja exemplo abaixo.

```
DlteC-FW-GW#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001e.130b.1aee (bia 001e.130b.1aee)
  Description: $FW_INSIDE$
  Internet address is 192.168.10.2/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  ### Saidas omitidas ###
```

Por último, temos a opção do comando para verificar os protocolos de camada 3 ativos, estado e endereço/máscara das interfaces: “**show protocols**” ou “**show protocolos serial 0/0/0**”. Veja exemplo abaixo.

```
DlteC-FW-GW#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.2/24
FastEthernet0/1 is up, line protocol is up
FastEthernet0/1.10 is up, line protocol is up
  Internet address is 192.168.1.1/24
FastEthernet0/1.20 is up, line protocol is up
  Internet address is 10.0.1.1/24
FastEthernet0/1.30 is up, line protocol is up
  Internet address is 192.168.2.1/24
NVI0 is up, line protocol is up
  Interface is unnumbered. Using address of FastEthernet0/0 (192.168.10.2)
Virtual-Access1 is down, line protocol is down
Virtual-Template1 is down, line protocol is down
  Interface is unnumbered. Using address of FastEthernet0/0 (192.168.10.2)
Virtual-Access2 is down, line protocol is down
Loopback1 is up, line protocol is up
```

```

Internet address is 10.10.10.10/32
DlteC-FW#show protocols fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.2/24
DlteC-FW#

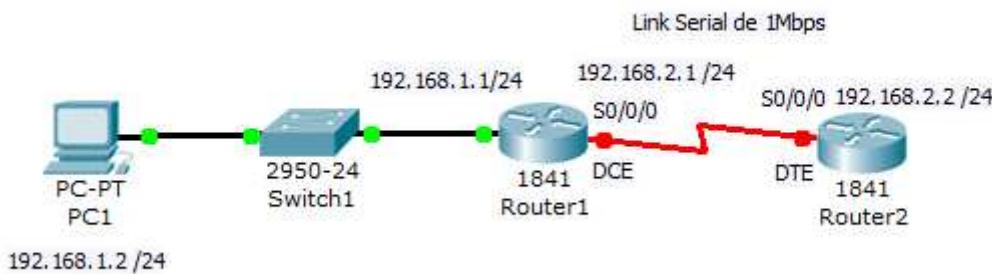
```

Note em amarelo que o comando “**show protocols**” traz a informação dos protocolos de camada 3 ativos (Internet Protocol routing is enabled), estado de todas as interfaces e endereço/máscara configurada. Repare também no detalhe em verde, onde podemos ver o estado da interface fast 0/0, portanto note que o comando traz o estado da interface e seu endereço de camada 3.

Todos esses comandos show são úteis para verificação após a configuração de roteadores Cisco ou para auxiliar na resolução de problemas (troubleshooting).

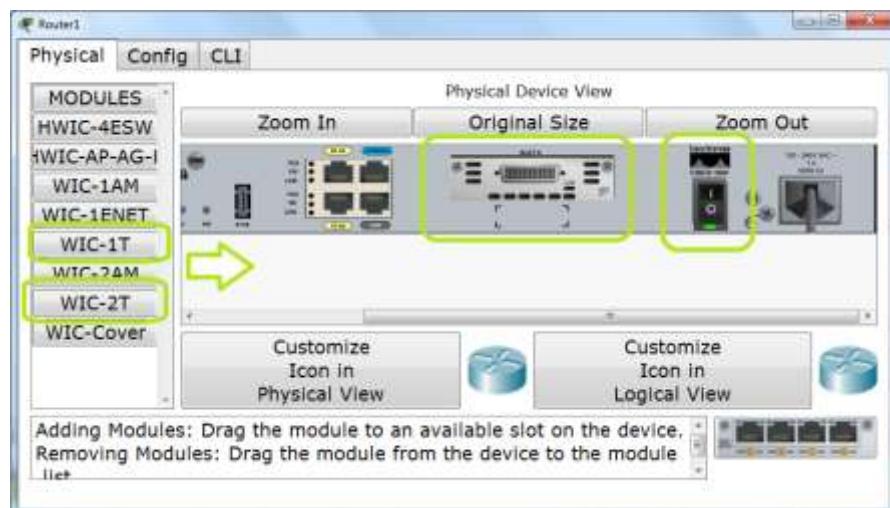
#### 7.4.2 Acrescentando um Link WAN na Topologia

Vamos aproveitar a mesma topologia e acrescentar mais um roteador e um switch e conectá-lo ao roteador já configurado via um link WAN com topologia costa a costa (back-to-back), conforme figura abaixo, porém agora vamos utilizar roteadores modelo 1841.



Para acrescentar ou remover um módulo em um roteador primeiro você precisará **desligá-lo**, como este é um fato muito importante o packet tracer tem um botão de liga e desliga na aba Physical.

Portanto desligue o roteador, arraste uma WIC-1T ou WIC-2T para o “slot 0” e ligue novamente o roteador. Veja a figura abaixo.



Depois de inserir as interfaces em ambos os equipamentos escolha o cabo serial DCE (com o relógio), clique no Router 1, selecione a interface Serial 0/0/0 e depois ligue na interface Serial 0/0/0 do Router 2, conforme já realizamos nos laboratórios do capítulo 2.

Agora vamos às configurações e testes, iniciando pelo Router 1 que tem a interface DCE, note que os IPs estão definidos na topologia.

```
DlteC-Teste#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DlteC-Teste(config)#interface serial 0/0/0
DlteC-Teste(config-if)#ip add 192.168.2.1 255.255.255.0
DlteC-Teste(config-if)#clock rate 1000000
DlteC-Teste(config-if)#bandwidth 1000
DlteC-Teste(config-if)#description Serial do router 1 conectada ao Router 2
DlteC-Teste(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
DlteC-Teste(config-if)#

```

Note que a interface ficou em Down, pois ainda não configuramos o Router 2.

Agora vamos configurar o router 2 e note na sequência o comando show ip interface brief com a interface agora em UP/UP.

```
DlteC-Teste2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DlteC-Teste2(config)#int s 0/0/0
DlteC-Teste2(config-if)#ip add 192.168.2.2 255.255.255.0
DlteC-Teste2(config-if)#bandwidth 1000
DlteC-Teste2(config-if)#description conectado ao router 1
DlteC-Teste2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

DlteC-Teste2(config-if)#end
DlteC-Teste2#
%SYS-5-CONFIG_I: Configured from console by console

DlteC-Teste2#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

```

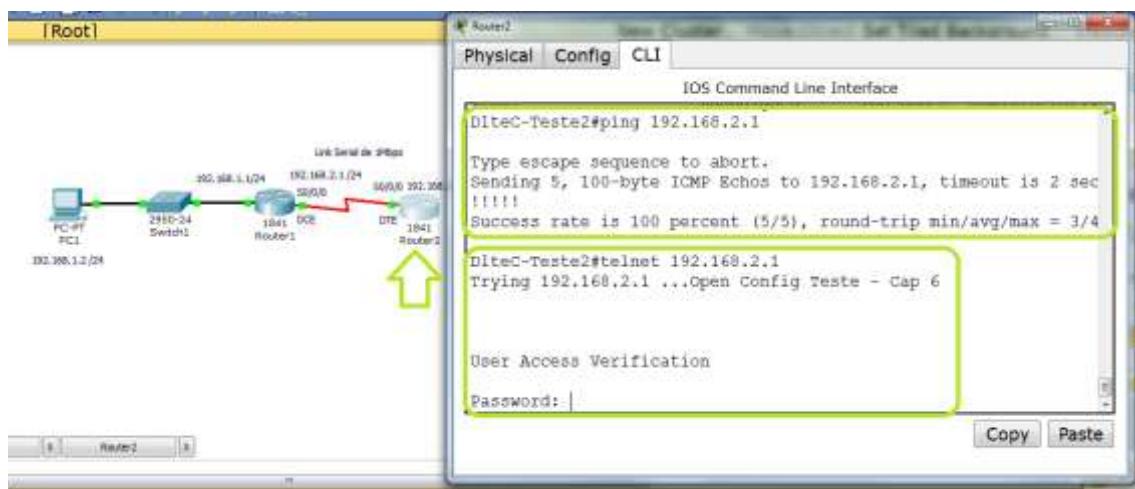
```
DlteC-Teste2#show ip inter bri
Interface          IP-Address      OK? Method Status   Protocol
FastEthernet0/0    unassigned      YES manual up       down
FastEthernet0/1    unassigned      YES unset  up       down
Serial0/0/0        192.168.2.2    YES manual up       up

DlteC-Teste2#

```

Para testar as interfaces seriais você pode a partir do Router 2 fazer ping para o Router 1 e também um teste de Telnet.

Lembre-se que para o Router 2 aceitar uma conexão de Telnet você precisará configurar a line VTY, pois sem uma senha na VTY o roteador não aceitará a conexão via telnet. Veja a figura a seguir.



Com o comando “**show ip route**” você pode verificar se uma rota para a rede configurada no roteador foi criada.

Você aprenderá em capítulos posteriores que ao configurar IP em uma interface e ela está no estado Up/Up uma rota diretamente conectada é criada na tabela de roteamento, indicando qual o melhor caminho para a rede que inserimos naquela interface.

Veja um exemplo da saída do comando na figura abaixo e note que as redes das interfaces diretamente conectadas aparecem com a letra C na frente.

```
Roteador_A#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      192.168.1.0/28 is subnetted, 2 subnets
C        192.168.1.0 is directly connected, FastEthernet0/0
C        192.168.1.16 is directly connected, Serial0/0/0
Roteador_A#
```

Nesse exemplo temos a rede 192.168.1.0 /28 configurada nas fast 0/0 e a rede 192.168.1.16/28 configurada na serial 0/0/0 do roteador chamado Roteador\_A.

Para verificar o IP que está configurado precisamos do comando “**show ip int brief**”, pois o “**show ip route**” nas versões 12.x do IOS não fornecem os IPs das interfaces na tabela de roteamento.

No IOS versão 15 uma rota local com um “L” na frente é criada indicando o IP da própria interface na tabela de roteamento.

## 8 Resumo do Capítulo

Bem pessoal, chegamos ao final do capítulo. É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Saber explicar os principais componentes de uma rede WAN.
- Entender a terminologia utilizada em redes WAN.
- Saber descrever o protocolo HDLC.
- Entender o fluxo de informações em camada 2 entre a LAN e WAN.
- Saber explicar os principais componentes de hardware em um roteador Cisco.
- Conhecer os principais tipos de interfaces em roteadores Cisco.
- Entender o conceito das linhas de Console, Auxiliar e VTY em equipamentos Cisco.
- Começar a ter domínio do CLI da Cisco.
- Entender perfeitamente como funciona os modos de execução e privilégios de acesso.
- Ter noção das facilidades de navegação no CLI da Cisco.
- Saber configurar, sem dificuldade, banners, hostname e senhas de acesso em equipamentos Cisco.
- Conseguir realizar, sem dificuldade, as configurações gerais de interfaces em um roteador Cisco.
- Entender o comando show interfaces e seus principais campos.
- Saber diferenciar equipamento DTE e DCE.
- Conseguir realizar uma configuração de interfaces seriais HDLC costa-a-costa.

*Ao longo desse capítulo iremos aprender sobre o modelo TCP/IP, suas camadas e principais protocolos. Também veremos conceitos importantes sobre endereçamento IP e cálculos de sub-rede.*

*Esperamos que você aproveite o capítulo e aprenda bastante.*

*Bons estudos!*

## **Capítulo 5 - TCP-IP e Introdução ao Endereçamento IP versão 4**

### **Objetivos do Capítulo**

Ao final desse capítulo você terá estudado e deverá compreender:

- Entender o Modelo TCP/IP e suas camadas.
- Ser capaz de comparar o modelo OSI e TCP/IP.
- Ser capaz de explicar as diferenças entre os protocolos TCP e UDP.
- Ter conhecimento sobre os principais campos do cabeçalho dos protocolos TCP e UDP.
- Entender como o TCP estabelece e encerra uma conexão.
- Entender os processos de reagrupamento, retransmissão e controle de congestionamento no TCP.
- Dominar o cálculo de transformação de números decimais e binários
- Entender a lógica do endereçamento IP e suas classes.
- Dominar o conceito do fluxo de dados em uma rede LAN.

## Sumário do Capítulo

<b>1</b>	<i>Introdução ao TCP/IP</i>	<b>172</b>
<b>2</b>	<i>Camada de Aplicação</i>	<b>173</b>
<b>3</b>	<i>Camada de Transporte</i>	<b>175</b>
3.1	Protocolos TCP e UDP	177
3.2	Identificando Conexões e Aplicações Com Portas TCP e UDP	178
3.3	TCP - Transmission Control Protocol	182
3.3.1	Processo TCP em Servidores – Arquitetura Cliente/Servidor	183
3.3.2	Conexão TCP - Estabelecimento e Encerramento	185
3.3.3	Confirmação de Recebimento de Segmentos TCP	188
3.3.4	Retransmissão de Segmentos TCP	190
3.3.5	Controle de Congestionamento TCP	192
3.3.6	Reagrupamento de Segmentos TCP	193
3.3.7	Aplicações Cliente Servidor com TCP	194
3.4	Protocolo UDP	195
3.5	Hora de Refletir sobre as Camadas de Aplicação e Transporte do TCP/IP	196
3.6	Hora de Praticar	199
<b>4</b>	<i>Camada de Internet</i>	<b>199</b>
4.1	Cabeçalho do Protocolo IPv4	200
4.2	Protocolo ICMP	201
4.3	Protocolos ARP, RARP e Proxy ARP	206
4.3.1	Entendendo o ARP	206
4.3.2	Entendendo o RARP	209
4.3.3	Entendendo do Proxy ARP	209
<b>5</b>	<i>Camada de Acesso à Rede (ou Acesso aos Meios)</i>	<b>210</b>
<b>6</b>	<i>Entendendo o Fluxo de Dados em Redes LAN e WAN</i>	<b>211</b>
6.1	Conceitos Básicos de Roteamento IP	211
6.2	Entendendo o Fluxo de Informações dentro da mesma LAN	213
6.3	Entendendo o Fluxo de Dados para Internet	214
6.4	Considerações sobre o fluxo de dados em uma rede IP e QoS	216
6.5	Hora de Praticar	218

<b>7</b>	<i>Introdução ao Endereçamento IP</i>	<b>218</b>
7.1	Sistemas de Numeração	218
7.1.1	Sistema Decimal	218
7.1.2	Sistema Binário	219
7.2	Conversão Binária	220
7.3	Hosts, Redes e Máscaras	221
7.4	Endereçamento IP e a Internet	222
7.5	Classes de Endereços IP	224
7.5.1	Endereço IP Classe A	225
7.5.2	Endereço IP Classe B	227
7.5.3	Endereço IP Classe C	228
7.5.4	Endereço IP Classe D e Classe E	229
7.6	Tipos de Comunicação Suportada pelo Protocolo IP	229
7.7	Endereçamento IPv4 na Prática	231
7.8	Resumo dos Tipos de Endereços e Máscaras	234
7.8.1	Máscara de Rede ou Netmask	234
7.8.2	Endereço de Rede	235
7.8.3	Endereço de Host	235
7.8.4	Endereço de Broadcast	235
7.8.5	Endereço de Loopback	235
7.9	Exemplo de Projeto Lógico de Rede SOHO	236
7.10	Endereçando Redes Classful	237
7.10.1	Projeto com Classe C	238
7.10.2	Projeto com Classe B	239
7.10.3	Projeto com Classe A	240
7.11	Introdução ao Conceito de Sub-Redes	240
<b>8</b>	<i>Configurando Endereços em Interfaces de Roteadores e Switches</i>	<b>242</b>
8.1	Endereços IPs Secundários	242
8.2	Erros Comuns ao Configurar Interfaces	243
8.3	Configurando Endereços IP em Switches	244
8.4	Apagando e Alterando Endereços Configurados	244
8.5	Verificando as Configurações das Interfaces	245
<b>9</b>	<i>Resumo do Capítulo</i>	<b>247</b>

## 1 Introdução ao TCP/IP

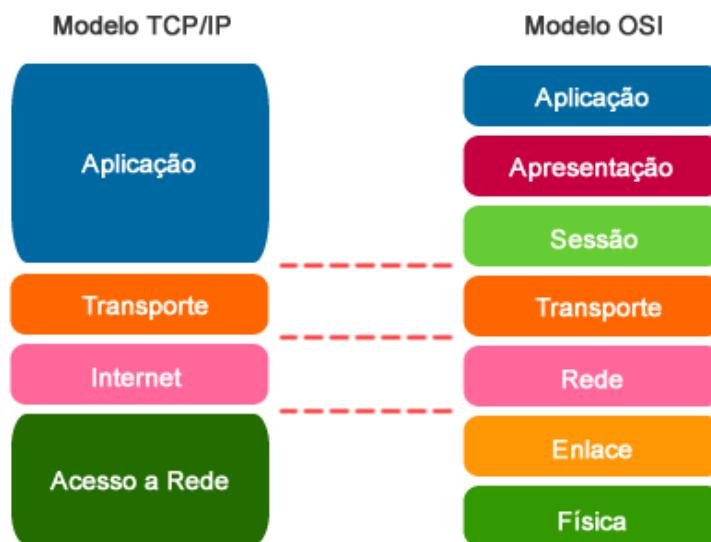
O modelo OSI é um padrão reconhecido universalmente, no entanto o modelo **TCP/IP** (Transmission Control Protocol / Internet Protocol) tem um importante papel histórico e prático, pois foi graças a ele que a Internet se desenvolveu e ele continua até hoje sendo o protocolo que a Internet utiliza. Por isso a importância de estarmos familiarizados com ambas os modelos.

O TCP/IP também pode ser chamado de “**pilha de protocolos**”, pois ele é formado por diversos protocolos de rede, dos quais o TCP e o IP fazem parte.

Para começar vamos deixar claro o seguinte: existe uma diferença fundamental entre um modelo (camadas, interfaces e especificações de protocolo) e um protocolo de fato que é usado em redes. Devemos focar nosso estudo de forma a compreender o modelo OSI, mas os protocolos TCP/IP também. Modelo TCP/IP não é a mesma coisa que protocolos TCP e IP.

Historicamente o modelo TCP/IP surgiu da necessidade do DoD (Departamento de Defesa dos Estados Unidos) em desenvolver uma forma de manter suas comunicações operantes no caso de uma guerra de grandes proporções. Ou seja, uma rede que fosse capaz de se manter operante nas condições mais adversas possíveis (uma guerra nuclear, por exemplo). Os pacotes deviam continuar trafegando não importando o meio que estivesse sendo utilizado (cabos, fibra, satélite etc...).

Assim sendo, caso um determinado ponto da rede fosse destruído pelo inimigo o tráfego deveria ser direcionado para outro link. Com esse intuito surgiu o modelo TCP/IP. Semelhante ao modelo OSI, o modelo TCP/IP também divide as funções da rede em camadas, só que utiliza apenas 04 (quatro) camadas: Aplicação, Transporte, Internet e Acesso à Rede (ou acesso aos meios).



Note que algumas camadas de ambos os modelos têm o mesmo nome e não devemos confundir as camadas dos dois modelos.

Por exemplo, a camada de aplicação tem funções diferentes em cada modelo. As camadas que tem a mesma função em ambas os modelos são a de transporte e de rede, chamada de Internet no TCP/IP.

A camada de acesso à rede é uma fusão das camadas física e enlace do modelo OSI e a camada de aplicação no TCP/IP faz a função das camadas de aplicação, apresentação e sessão do modelo OSI.

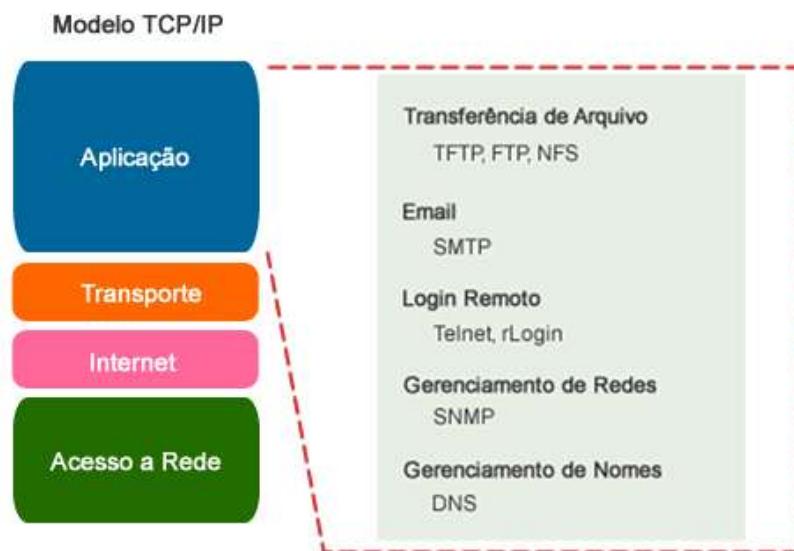
O TCP/IP é o modelo adotado na Internet, sendo o modelo OSI adotado como guia nos desenvolvimentos de redes. Um bom profissional de rede precisa conhecer ambos os modelos. Veremos ao longo desse capítulo maiores detalhes sobre cada uma das camadas do TCP/IP e os principais protocolos em cada uma delas.

## 2 Camada de Aplicação

Assim como no Modelo OSI, a camada de Aplicação é a camada superior do modelo TCP/IP.

Ela é responsável por fornecer a interface entre as aplicações que utilizamos para comunicação e a rede subjacente pela qual nossas mensagens são transmitidas.

Os protocolos da camada de aplicação são utilizados para troca de dados entre programas executados nos hosts de origem e de destino. Existem diversos protocolos da camada de Aplicação, e outros novos estão em constante desenvolvimento, veja alguns exemplos na figura a seguir.



A camada de aplicação do modelo TCP/IP trata de protocolos de alto nível, questões de representação, codificação e controle de diálogos, ou seja, o que as camadas 5, 6 e 7 do modelo OSI fazem separadamente a aplicação do TCP/IP trata como um pacote só, fazendo interface direta com a camada de transporte.

Abaixo temos mais de detalhes sobre alguns dos principais protocolos da camada de aplicação:

- **DNS (Domain Name System – Sistema de Nomes de Domínio)** – O DNS é um sistema usado na Internet para converter os nomes de domínios e seus respectivos nós de rede divulgados publicamente em endereços IP.
- **DHCP (Dynamic Host Configuration Protocol)** – Utilizado para fornecer dados de configuração das interfaces dinamicamente aos computadores e demais endpoints da rede. Os dados fornecidos são no mínimo endereço IP, máscara de rede, endereço do roteador padrão e servidor DNS. Sem ele os administradores de rede teriam um imenso trabalho braçal.
- **WWW ou HTTP (Hypertext Transfer Protocol)** – Serviço básico utilizado pelos navegadores de Internet ou browsers para acessar o conteúdo das páginas web. Sua versão segura (com criptografia) é o HTTPS.
- **FTP (File Transfer Protocol – Protocolo de Transferência de Arquivos)** – é um serviço confiável, orientado a conexões, que usa o TCP para transferir arquivos. Suporta transferências bidirecionais de arquivos binários e ASCII.
- **TFTP (Trivial File Transfer Protocol – Protocolo de Transferência de Arquivos Simples)** – serviço sem conexão que usa o UDP (User Datagram Protocol – Protocolo de Datagrama de Usuário). É usado no roteador para transferir arquivos de configuração e imagens IOS da Cisco e para transferir arquivos entre sistemas que suportam TFTP. É útil em algumas redes locais porque opera mais rápido do que o FTP em um ambiente estável.
- **SMTP (Simple Mail Transfer Protocol – Protocolo Simples de Transferência de Correio)** – Administra a transmissão de correio eletrônico através de redes de computadores. Ele não oferece suporte à transmissão de dados que não estejam em texto simples.
- **POP3 e IMAP** – São os protocolos utilizados pelos clientes para a leitura do e-mail. A diferença entre eles é que o POP3 baixa os arquivos para o micro do usuário apagando no servidor, já o IMAP é possível deixar uma cópia dos e-mails, utilizando como um espelho sem apagar as mensagens, assim o usuário pode ler seus e-mails antigos independente do micro que está utilizando.
- **Telnet (Terminal emulation – Emulação de terminal)** – Permite o acesso remoto a outro computador. Permite que um usuário efetue logon em um host da Internet e execute comandos, porém os dados são transmitidos em texto claro, podendo ser capturado e lido por um invasor no meio do caminho. Existe também uma versão segura chamada Secure Shell ou SSH, o qual possibilita a transferência de informações criptografadas pela rede.
- **NFS (Network File System – Sistema de Arquivos de Rede)** – Conjunto de protocolos de sistema de arquivos distribuído, desenvolvido pela Sun Microsystems, que permite acesso a arquivos de um dispositivo de armazenamento remoto, como um disco rígido, através da rede.
- **SNMP (Simple Network Management Protocol – Protocolo Simples de Gerenciamento de Rede)** – Oferece uma forma de monitorar e controlar dispositivos de rede e de gerenciar configurações, coleta de dados estatísticos, desempenho e segurança.

Normalmente esses protocolos são chamados também de “serviços de rede”, os quais são programas de computador instalados nos servidores para que os usuários finais possam acessar e realizar suas funções diárias.

Por exemplo, o registro de uma venda ou consulta de preços pelos funcionários de uma loja em uma página de web utilizando o protocolo HTTP no servidor que tem um programa de automação de vendas.

Quem utiliza Internet usa diariamente os serviços de DHCP e DNS sem mesmo perceber. Seu Access Point ou roteador ADSL passa as configurações de rede para seu computador via DHCP e

toda vez que você acessa a Internet uma consulta DNS é realizada para resolver o nome do web site para um endereço IP.

Vamos estudar também que cada serviço de rede pode utilizar na camada de transporte o serviço do protocolo TCP ou UDP, sendo identificado por número de portas.

Essas informações são importantes porque quando formos estudar as listas de controle de acesso ou ACL precisaremos lembrar-nos desses detalhes, por isso estude com atenção. Outro motivo para aprender esses conceitos é que se você está entrando na área de redes e deseja ser um bom administrador precisa conhecer os serviços de rede e suas características, concorda? Isso é básico na vida de um profissional de redes.

Após estudarmos o TCP e UDP falaremos com mais detalhe dos protocolos mais importantes para o dia a dia de um CCENT.

### 3 Camada de Transporte

A função da camada de Transporte é proporcionar segmentação de dados e o controle necessário para reagrupar esses segmentos em fluxos de comunicação. Veja a figura abaixo.



Para tal a camada de transporte deve ser capaz de fazer as seguintes tarefas:

- Rastreamento de Conversações Individuais
- Segmentação de Dados
- Reagrupamento de Segmentos
- Identificação das Aplicações

No TCP/IP a camada de transporte pode oferecer dois caminhos ou serviços, confiável através do protocolo TCP e não confiável através do protocolo UDP. Na teoria essa camada se refere às características gerais do protocolo TCP.

Vamos agora estudar cada uma das funções gerais da camada de transporte.

#### Rastreamento de Conversações Individuais

Qualquer host pode ter múltiplas aplicações que se comunicam através da rede. Cada uma destas aplicações irá se comunicar com uma ou mais aplicações em hosts remotos. É responsabilidade da camada de Transporte manter fluxos múltiplos de comunicação entre estas aplicações.

**Segmentação de Dados**

Como cada aplicação cria um fluxo de dados para ser enviado a uma aplicação remota, estes dados devem ser preparados para serem enviados através do meio em segmentos gerenciáveis.

Os protocolos de camada de Transporte descrevem serviços que segmentam estes dados a partir da camada de Aplicação. Isto inclui o encapsulamento necessário em cada lado do segmento. Cada segmento de dados de aplicação requer a adição de cabeçalhos da camada de Transporte para indicar a qual comunicação ele está associado.

**Reagrupamento de Segmentos**

No host de destino, cada segmento de dados pode ser direcionado para a aplicação apropriada. Em adição a isso, estes segmentos de dados individuais também precisam ser reconstruídos em um fluxo completo de dados que seja útil para a camada de Aplicação.

Os protocolos da camada de Transporte descrevem como a informação do cabeçalho da camada de Transporte é usada para reagrupar os segmentos de dados em fluxos a serem passados para a camada de Aplicação.

**Identificação das Aplicações**

Para passar os fluxos de dados para as aplicações apropriadas, a camada de Transporte deve identificar a aplicação de destino. Para realizar isso, a camada de Transporte designa à aplicação um identificador. Os protocolos TCP/IP chamam esse identificador de número de porta. A cada processo de software que precise acessar a rede é designado um número de porta único naquele host. Este número de porta é usado no cabeçalho da camada de transporte para indicar a qual aplicação aquele segmento de dado está associado.

A camada de Transporte é o link entre a camada de Aplicação e a camada inferior, que são responsáveis pela transmissão na rede. Esta camada aceita dados de diferentes conversações e os passa para as camadas inferiores como segmentos gerenciáveis que podem ser finalmente multiplexados no meio.

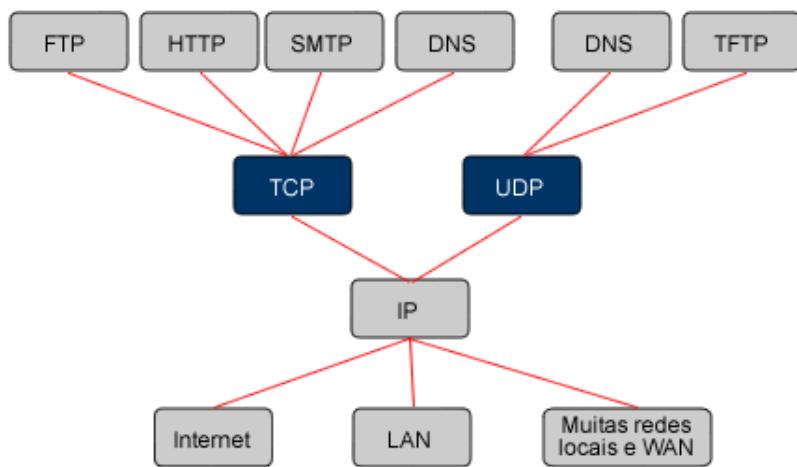
As aplicações não precisam saber dos detalhes operacionais da rede em uso. As aplicações geram dados que são enviados de uma aplicação a outra, sem considerar o tipo de host de destino, o tipo de meio sobre o qual o dado deve trafegar, o caminho tomado pelo dado, o congestionamento em um link ou o tamanho da rede.

Adicionalmente, as camadas inferiores não estão a par de que existem múltiplas aplicações enviando dados na rede. Sua responsabilidade é entregar os dados ao dispositivo apropriado. A camada de transporte então organiza esses segmentos antes de entregá-los à aplicação apropriada.

### 3.1 Protocolos TCP e UDP

Os dois protocolos da camada de Transporte mais comuns da pilha de protocolos TCP/IP são o Protocolo TCP e UDP. Ambos os protocolos gerenciam a comunicação de múltiplas aplicações que desejam acessar a rede simultaneamente. As diferenças entre os dois são as funções específicas que cada protocolo programa.

Veja a figura a seguir para entender melhor o posicionamento da camada de transporte dentro da pilha de protocolos TCP/IP. Perceba que as aplicações normalmente usam um ou outro protocolo como serviço de transporte ponto a ponto.



O TCP é um protocolo orientado à conexão, descrito na RFC 793. O TCP causa sobrecarga adicional na rede, pois possui funções adicionais - entrega ordenada, entrega confiável e controle de fluxo.

Cada segmento TCP tem 20 bytes de overhead no cabeçalho que encapsula o dado da camada de Aplicação, enquanto que o segmento UDP tem apenas 8 bytes. Algumas das aplicações que usam TCP são:

- Navegadores web (HTTP e HTTPS)
- E-mail (SMTP, POP e IMAP)
- FTP
- DNS – consulta entre servidores

O UDP é um protocolo simples e sem conexão, descrito na RFC 768. Ele tem a vantagem de fornecer uma entrega de dados com baixa sobrecarga e maior velocidade, pois ele não possui os mecanismos de controle do TCP. Sua desvantagem é que não é confiável, por isso a camada de aplicação deve tratar dessas características.

Os segmentos de comunicação em UDP são chamados datagramas. Estes datagramas são enviados como o "**melhor esforço**" por este protocolo da camada de Transporte, ou seja, o UDP envia e não espera por confirmação nem tampouco controla fluxo. As aplicações que usam UDP incluem:

- DNS – consulta de cliente a servidor
- Voz Sobre IP (RTP – Real time protocol)
- TFTP
- SNMP

São características comuns ao TCP e UDP:

- Segmentação de dados das aplicações das camadas superiores.
- Envio de segmentos de um dispositivo em uma ponta para um dispositivo em outra ponta.
- Multiplexação de informações da camada de aplicação (transporte de vários fluxos simultaneamente).
- Identificação das aplicações e conexões de cliente utilizando números de porta.

São características exclusivas do TCP:

- Estabelecimento de operações ponta a ponta (hand-shake de três vias).
- Controle de fluxo proporcionado pelas janelas móveis (janelamento).
- Confiabilidade proporcionada por números de sequência e confirmações de entrega dos segmentos.
- Retransmissão de segmentos perdidos.

Podemos fazer aqui uma comparação da aplicação sendo um veículo que tem duas estradas para escolher, uma das estradas é segura e com certeza você vai chegar ao seu destino, porém ela tem tantos pontos de checagem, pedágios e outros mecanismos de controle de tráfego que acaba sendo mais lenta, esse é o TCP.

Por outro lado temos uma pista sem controle de tráfego nenhum e por isso ela é muito mais rápida, porém para trafegar nessa pista seu carro vai precisar que você tenha um mapa preciso, GPS e muita atenção do motorista (a aplicação), pois ela não tem indicações. Esse é o UDP.

Por isso o UDP é utilizado, por exemplo, para o tráfego de Voz sobre a rede IP e implementações de VPN (redes virtuais privadas), pois a voz e o acesso VPN precisam de velocidade. Já aplicações como HTTP para leitura de páginas não precisam dessa urgência, por isso utilizam o TCP como meio de transporte.

### **3.2 Identificando Conexões e Aplicações Com Portas TCP e UDP**

Imagine que você tem vários produtos para entregar em um só prédio, porém cada um para um morador distinto. Você pega uma caixa coloca todos os produtos nessa caixa e envia para a portaria sem identificação de quem é cada produto, o que vai ocorrer? Considerando o mundo dos seres humanos e não dos bits e bytes será uma confusão!

Vamos agora trazer esse exemplo para nosso computador. Nós não fazemos uma conexão de rede por vez correto? Por exemplo, vou ler e-mail, depois que finalizou vou acessar o google, depois faço outra atividade e assim por diante. Na realidade estamos com o browser aberto acessando pelo menos dez páginas diferentes, falando pelo Skype, acessando um servidor via SSH, recebendo e enviando e-mails e assim por diante, ou seja, nosso acesso à rede pode ser múltiplo e simultâneo. Por isso mesmo que o TCP e o UDP precisam identificar de que programa ou aplicativo cada conexão pertence e o faz utilizando os números de porta.

Se não fosse assim como o TCP ou o UDP iriam saber para que aplicação encaminhar os dados recebidos dos computadores e servidores remotos que eles estão conectados?

Portanto, para diferenciar os segmentos e datagramas para cada aplicação tanto o TCP como o UDP possuem campos de cabeçalho que permitem identificar unicamente essas aplicações. Estes identificadores únicos são os números de porta.

Quando dizemos único é porque não se pode utilizar a mesma porta para identificar mais de uma conexão, senão o TCP ou UDP não saberia quem é o verdadeiro dono daquela informação!

No cabeçalho de cada segmento ou datagrama, há uma porta de **origem** e **destino**. O número da porta de origem é o número para essa comunicação associado ao programa ou aplicativo que originou a comunicação no host local.

A porta de destino representa a aplicação remota que o computador local deseja acessar, por exemplo, um serviço HTTP para ler uma página de Web via protocolo TCP na porta 80.

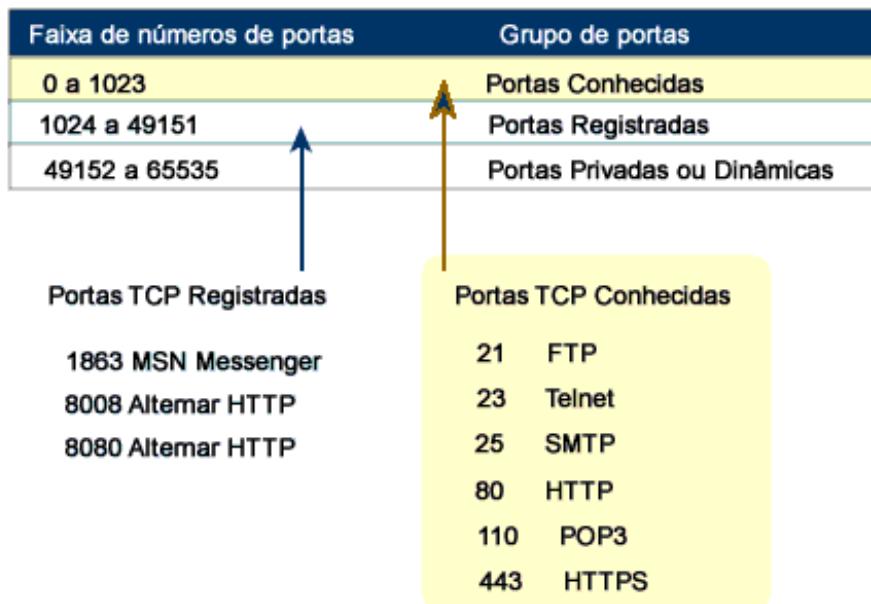
A IANA (Internet Assigned Numbers Authority) é o órgão não governamental responsável pela designação de vários padrões de endereçamento internacionalmente, dentre eles os números de portas. Veja na figura a seguir uma classificação geral dos números de porta alocados pela IANA.

Faixa de números de portas	Grupo de portas
0 a 1023	Portas conhecidas
1024 a 49151	Portas Registradas
49152 a 65535	Portas Privadas ou Dinâmicas

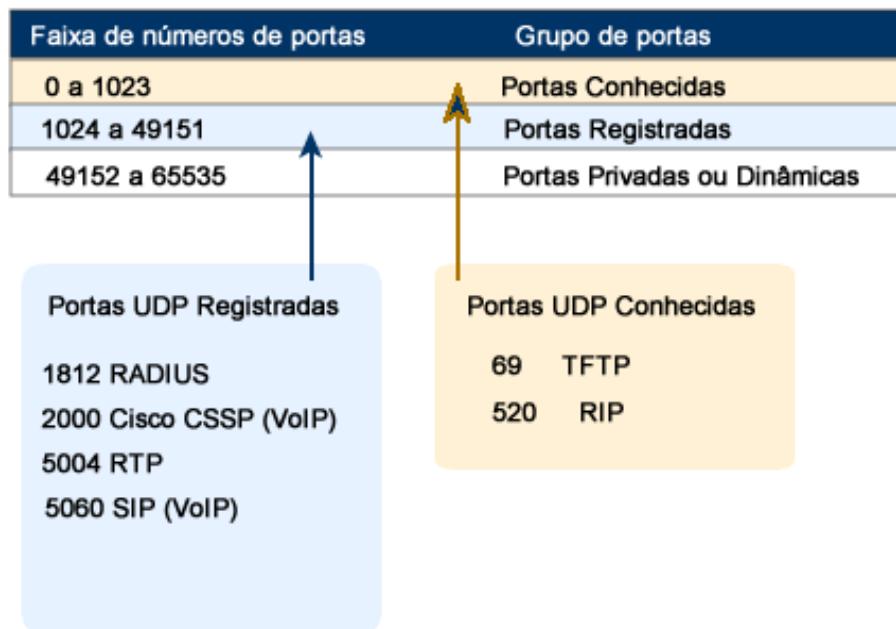
Portanto existem três diferentes tipos de números de portas:

- **Portas Conhecidas (Números 0 a 1023)** - Esses números de portas estão reservados para serviços e aplicações. Eles são comumente usados para aplicações como o HTTP (servidor web) POP3/SMTP (servidor de e-mail) e Telnet. Através da definição destas portas conhecidas para aplicações de servidor, aplicações de clientes podem ser programadas para solicitar uma conexão com essa porta específica e seu serviço associado. São também chamadas como **Well Known Ports**.
- **Portas Registradas (Números 1024 a 49151)** - Estes números de portas são designados para processos ou aplicações de usuário. Estes processos são principalmente aplicações individuais que um usuário escolheu para instalar em vez de aplicações comuns que receberiam uma Porta Conhecida. Quando não usadas para um recurso de servidor, estas portas também podem ser dinamicamente selecionadas por um cliente como sua porta de origem.
- **Portas Dinâmicas ou Privadas (Números 49152 a 65535)** - Elas são geralmente designadas dinamicamente a aplicações de cliente quando se inicia uma conexão. Não é muito comum um cliente se conectar a um serviço usando uma Porta Dinâmica ou Privada, embora alguns programas de compartilhamento de arquivos peer-to-peer o façam.

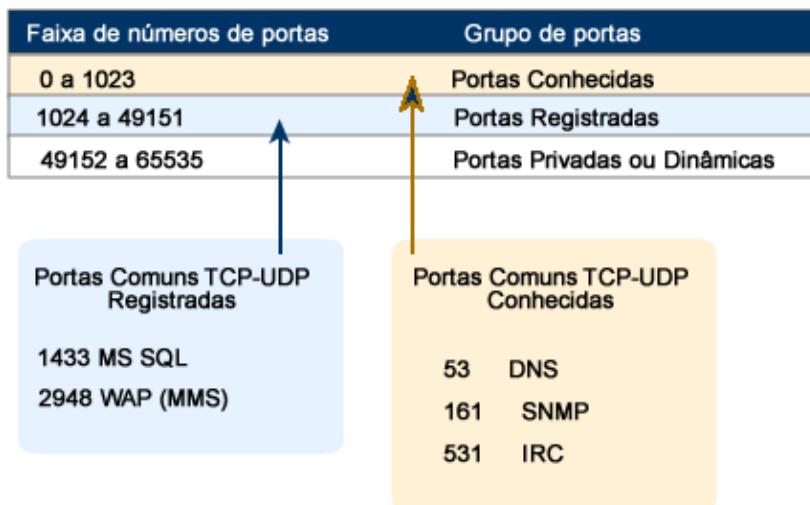
Exemplo de números portas TCP:



Exemplos de portas UDP:



Portas comuns ao UDP e TCP:



Portanto, quando um computador acessa um serviço remoto, por exemplo, quer acessar uma página de Web através do HTTP ele utiliza o protocolo TCP com porta de origem dinâmica com número entre 49152 a 65535, por exemplo, a porta 51000, já a porta de destino será a 80, pois o HTTP utiliza uma porta bem conhecida com o número 80.

Quando o servidor receber esse segmento na porta 80 ele sabe que precisa encaminhar os dados ao programa instalado com o serviço HTTP, por exemplo, um servidor Apache. Esse servidor irá tratar a informação e devolver uma resposta.

Nessa resposta a porta de origem será 80, pois quem está gerando é o servidor HTTP, e de destino será a porta 51000 conforme alocada no host de origem.

Quando o computador que originou a conversa recebe a informação na porta 51000 ele sabe para que programa encaminhar essa informação e assim fechar o ciclo de conversa até finalizar o envio e recebimento de informações e completar a página de Web na tela do computador do usuário.

### 3.3 TCP - Transmission Control Protocol

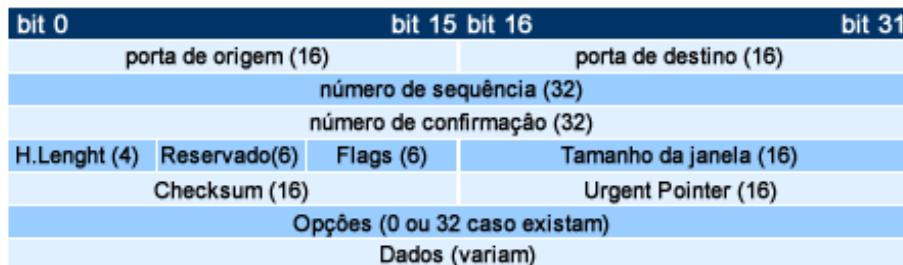
O TCP é um dos principais protocolos da camada transporte do modelo TCP/IP.

Sua versatilidade e robustez o torna adequado a redes globais, uma vez que este protocolo verifica se os dados são enviados de forma correta, na sequência apropriada e sem erros pela rede.

As características fundamentais do TCP são:

- **Orientado à conexão** - A aplicação envia um pedido de conexão para o destino e usa a "conexão" para transferir dados.
- **Ponto a ponto** - uma conexão TCP é estabelecida entre dois pontos.
- **Confiabilidade** - O TCP usa várias técnicas para proporcionar uma entrega confiável dos pacotes de dados, que é a grande vantagem que tem em relação ao UDP, e motivo do seu uso extensivo nas redes de computadores. O TCP permite a recuperação de pacotes perdidos, a eliminação de pacotes duplicados, recuperação de dados corrompidos e pode recuperar a ligação em caso de problemas no sistema e na rede.
- **Full duplex** - É possível a transferência simultânea em ambas as direções (cliente-servidor) durante toda a sessão.
- **Handshake** - Possui mecanismo de estabelecimento e finalização de conexão a três e quatro tempos, respectivamente, o que permite a autenticação e encerramento de uma sessão completa. O TCP garante que, no final da conexão, todos os pacotes foram bem recebidos.
- **Entrega ordenada** - A aplicação faz a entrega ao TCP de blocos de dados com um tamanho arbitrário num fluxo (ou stream) de dados, tipicamente em octetos. O TCP parte estes dados em segmentos de tamanho especificado pelo valor MTU. Porém, a circulação dos pacotes ao longo da rede (utilizando um protocolo de encaminhamento, na camada inferior, como o IP) pode fazer com que os pacotes não cheguem ordenados. O TCP garante a reconstrução do stream no destinatário mediante os números de sequência.
- **Controle de fluxo** - O TCP usa o campo janela ou window para controlar o fluxo. O receptor, à medida que recebe os dados, envia mensagens ACK (=Acknowledgement), confirmindo a recepção de um segmento. Como funcionalidade extra, estas mensagens podem especificar o tamanho máximo do buffer no campo (janela) do segmento TCP, determinando a quantidade máxima de bytes aceita pelo receptor. O transmissor pode transmitir segmentos com um número de bytes que deverá estar confinado ao tamanho da janela permitido: o menor valor entre sua capacidade de envio e a capacidade informada pelo receptor.

Veja na figura a seguir os campos do cabeçalho do segmento TCP e logo abaixo a explicação de cada campo.



- **Porta de origem**: Número da porta chamadora.
- **Porta de destino**: Número da porta chamada.

- **Número de sequência:** Número utilizado para garantir a sequência correta dos dados que estão chegando. Especifica o número do último octeto (byte) em um segmento.
- **Número de confirmação:** Próximo octeto TCP esperado. Especifica o octeto seguinte esperado pelo receptor.
- **H.Length:** Comprimento do cabeçalho do segmento em bytes.
- **Reservado:** Definido como zero.
- **Flags:** Funções de controle, como a configuração e término de uma sessão. Utilizado no gerenciamento de sessões e no tratamento de segmentos.
- **Janela:** Número de octetos que o remetente está disposto a aceitar. É o valor da janela dinâmica, quantos octetos podem ser enviados antes da espera do reconhecimento.
- **Checksum:** Cálculo de verificação feito a partir de campos do cabeçalho e dos dados. Utilizado para verificação de erros no cabeçalho e dados.
- **Urgent Pointer:** Indica o final de dados urgentes. Utilizado somente com um sinalizador URG flag.
- **Opção:** Informações opcionais. Uma opção atualmente definida é o tamanho máximo do segmento TCP.
- **Dados:** Dados de protocolo da camada superior, chamado também de Payload.

### 3.3.1 Processo TCP em Servidores – Arquitetura Cliente/Servidor

Vamos agora ver como funciona o processo do TCP em um servidor ao executar diversas aplicações.

Cada processo de aplicação sendo executado no servidor é configurado para usar um número de porta, seja no modo padrão ou manualmente através de um administrador do sistema. Conforme já comentamos em um mesmo servidor não podem existir dois serviços designados ao mesmo número de porta dentro dos mesmos serviços da camada de Transporte.

Por exemplo, um host executando uma aplicação de servidor web e uma aplicação de transferência de arquivo não pode ter ambos configurados para usar a mesma porta.

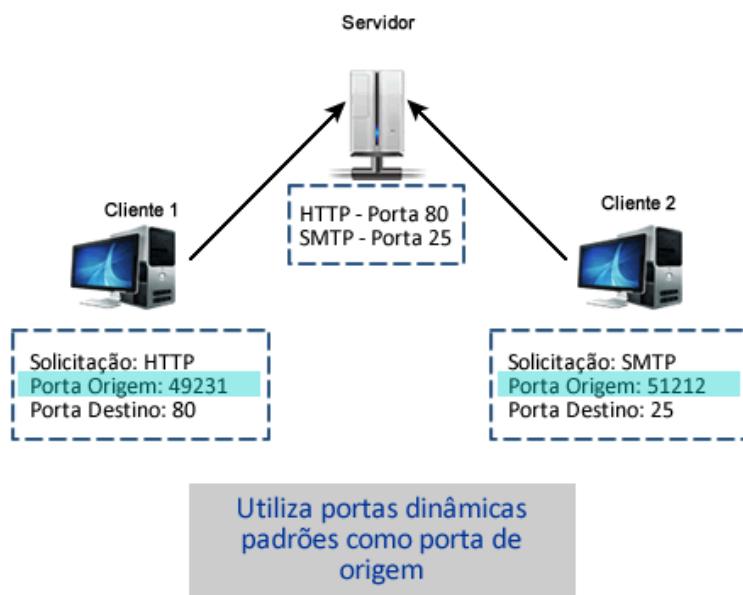
Quando uma aplicação de servidor ativa é designada a uma porta específica, essa porta é considerada como estando "aberta" (listening) no servidor. Isto significa que a camada de Transporte aceita e processa segmentos endereçados àquela porta.

Qualquer solicitação de cliente que chega endereçada a essa porta é aceita e os dados são transmitidos à aplicação do servidor. Pode haver muitas portas simultâneas abertas em um servidor, uma para cada aplicação de servidor ativa, pois é comum para um servidor fornecer mais de um serviço, como serviço web e servidor FTP ao mesmo tempo no mesmo servidor.

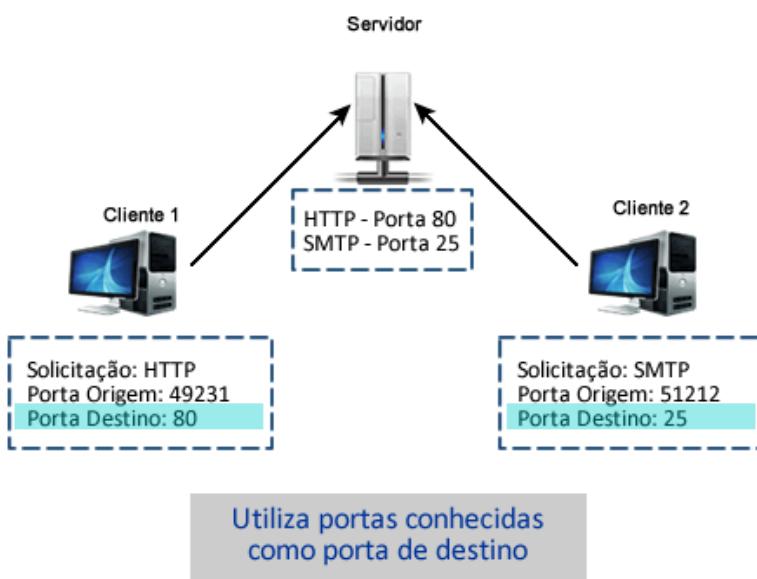
Uma maneira de melhorar a segurança em um servidor é restringir o acesso de servidor a apenas essas portas associadas com os serviços e as aplicações que devem ser acessíveis para solicitantes autorizados.

Esse modelo de acesso a serviços de rede é chamado arquitetura cliente/servidor, pois temos os computadores clientes que precisam acessar informações que são disponibilizadas pelos servidores de rede. A arquitetura cliente servidor é muito utilizada em redes até os dias de hoje. Existem outros modelos, tal como o peer-to-peer, onde dois clientes se comunicam diretamente sem o uso de um servidor.

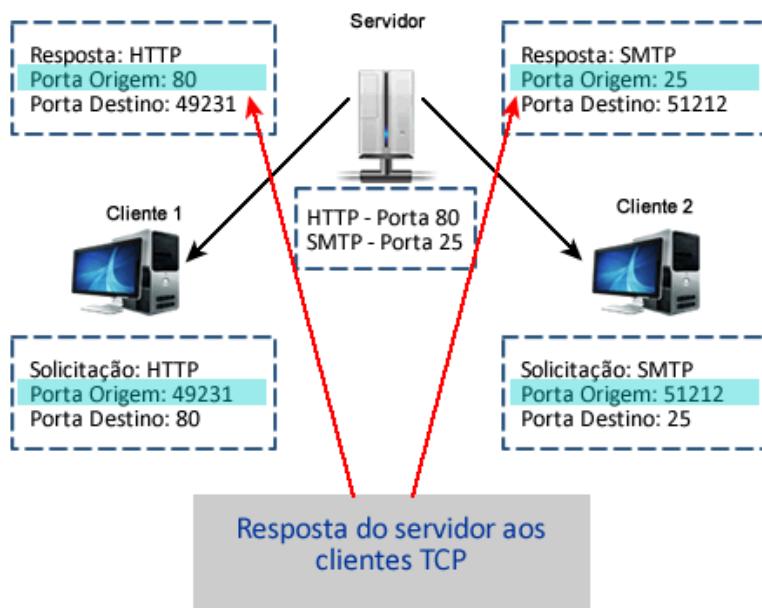
Veja nas figuras a seguir um exemplo de comunicação cliente/servidor através do TCP. Nesse exemplo o computador chamado cliente 1 deseja acessar uma página de Web e o cliente 2 enviar um e-mail. Na primeira figura temos os clientes enviando a solicitação ao servidor utilizando como porta de origem os números 49231 e 51212 respectivamente.



A porta de destino do cliente 1 é a 80, pois ele deseja acessar o serviço de HTTP, já do cliente 2 é 25, pois ele deseja enviar um email através do SMTP. Veja a figura a seguir com as portas destacadas.



O servidor recebe as solicitações, verifica se existe serviço ativo nessas portas e passa as informações recebidas para a camada de aplicação, a qual passa para os aplicativos que cuidam de cada um dos recursos solicitados. Após os aplicativos tratarem as solicitações o servidor responde aos clientes utilizando a porta do serviço solicitado como origem e destino a porta que o cliente enviou como origem na sua solicitação.



Essa troca de informações será feita até que a requisição esteja completa ou um problema de rede ocorra e interrompa o tráfego.

### 3.3.2 Conexão TCP - Estabelecimento e Encerramento

O TCP é classificado como um protocolo orientado a conexão. Vamos agora ver como funciona o estabelecimento e encerramento de uma sessão TCP entre dois hosts.

Para que dois hosts se comuniquem utilizando o TCP é necessário que seja estabelecida uma conexão antes que os dados possam ser trocados. Depois da comunicação ter sido completada, as sessões devem ser fechadas e a conexão é encerrada. É esse mecanismo de conexão e sessão que fornecem a característica de confiabilidade ao TCP.

Dentro do cabeçalho de segmento TCP, existem seis campos de 1 bit que contêm a informação de controle usada para gerenciar os processos TCP. Esses campos são:

- URG - Indicador urgente de campo significativo
- ACK - Campo significativo de confirmação
- PSH - função Push
- RST - Restabelecer a conexão
- SYN - Sincronizar números de sequência
- FIN - Não há mais dados do remetente

Estes campos são referidos como flags (flags), porque o valor de um desses campos é apenas 1 bit e, portanto, tem apenas dois valores: 1 ou 0. Quando um valor de bit é definido como 1, ele indica que a informação de controle está contida no segmento.

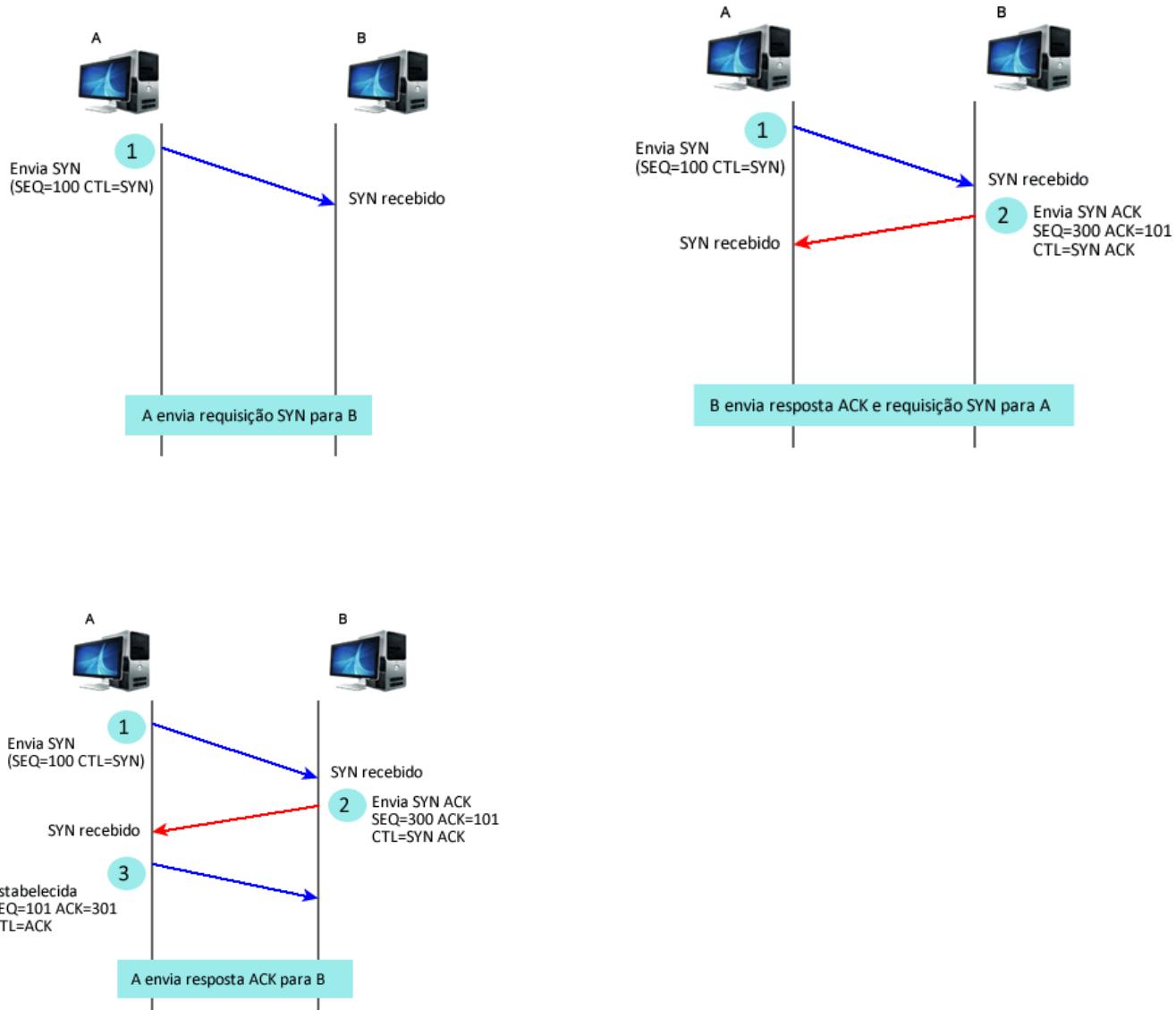
Cada conexão representa dois fluxos de comunicação, ou sessões. Para estabelecer uma conexão, os hosts realizam um handshake triplo. Bits de controle no cabeçalho TCP indicam o progresso e o status da conexão. Abaixo as funções do handshake triplo:

- Confirma que o dispositivo de destino esteja presente na rede.
- Verifica se o dispositivo de destino tem um serviço ativo e está aceitando solicitações no número de porta de destino que o cliente pretende usar para a sessão.
- Informa o dispositivo de destino que o cliente de origem pretende estabelecer uma sessão de comunicação nesse número de porta.

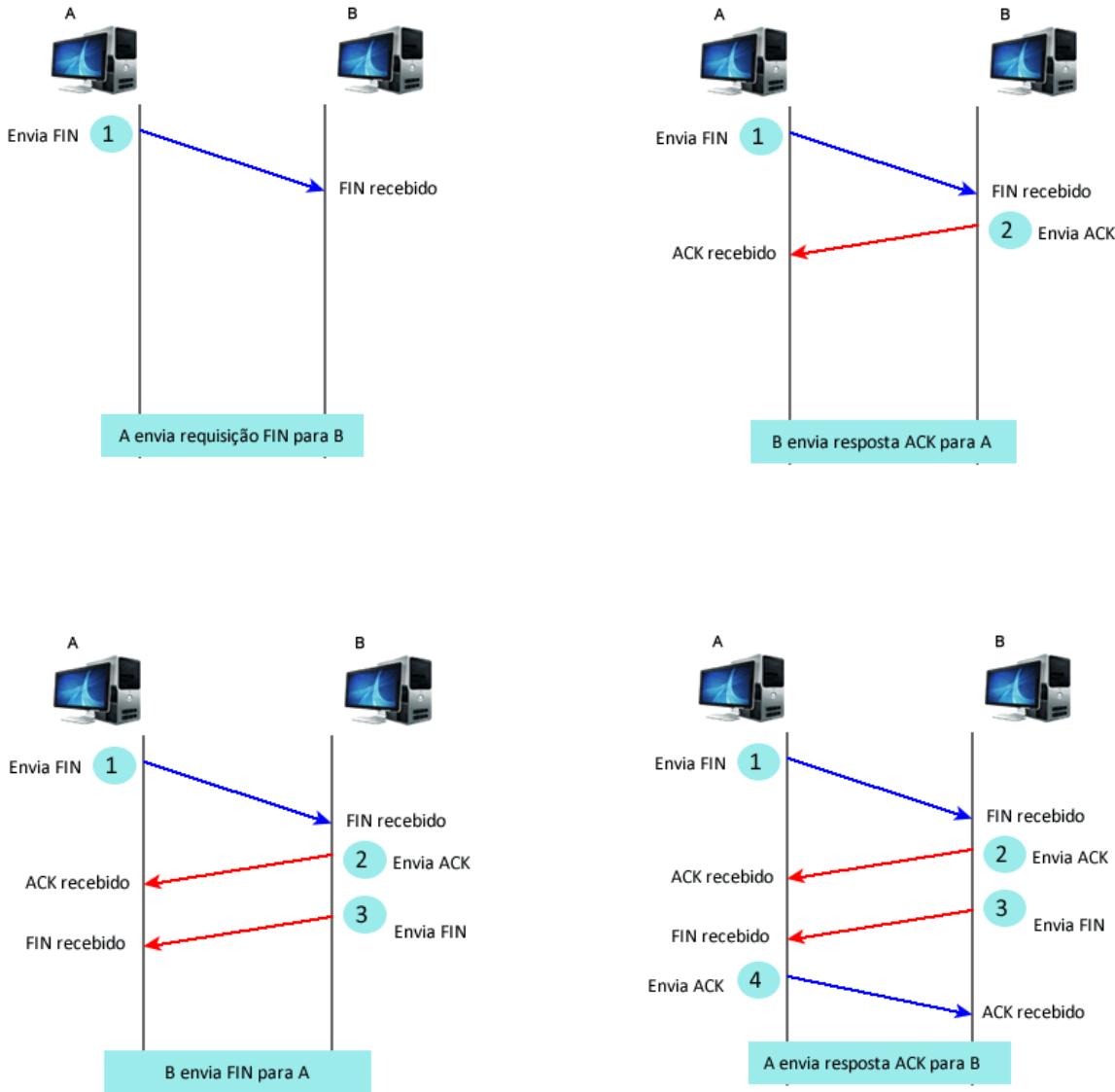
Em todas as conexões TCP, o host que serve como um cliente é quem inicia a sessão para o servidor. Os três passos no estabelecimento de uma conexão TCP são:

1. O cliente envia um segmento contendo um valor sequencial inicial (ISN – Initial Sequence Number) com o flag SYN ativo. Esse segmento serve como uma solicitação ao servidor para começar uma sessão.
2. O servidor responde com um segmento contendo um valor de confirmação igual ao valor sequencial recebido mais 1, mais seu próprio valor sequencial de sincronização (flag SYN e ACK ativos). O valor é maior do que o número sequencial porque o ACK é sempre o próximo Byte ou Octeto esperado.
3. O cliente responde com um valor de confirmação igual ao valor sequencial que ele recebeu mais um. Isso completa o processo de estabelecimento da conexão.

Veja as figuras abaixo com a ilustração da abertura da conexão com handshake de três vias.



Com o uso de um processo de quatro etapas acontece também uma troca de mensagens para encerrar uma conexão TCP e liberar os recursos alocados para a conexão. Veja a ilustração abaixo.



Abaixo segue a explicação da troca de informações para finalização da conexão TCP:

1. Quando o cliente não tem mais dados para enviar no fluxo, ele envia um segmento com uma flag FIN ativo.
2. O servidor envia uma ACK para confirmar o recebimento do FIN para encerrar a sessão do cliente para o servidor.
3. O servidor envia um FIN para o cliente, para encerrar a sessão do servidor para o cliente.
4. O cliente responde com um ACK para confirmar o FIN do servidor.

### 3.3.3 Confirmação de Recebimento de Segmentos TCP

Outro campo importante no cabeçalho TCP é o "**número de confirmação**".

O número de sequência definido durante a abertura da conexão TCP e o número de confirmação são utilizados para confirmar o recebimento dos bytes de dados contidos nos segmentos.

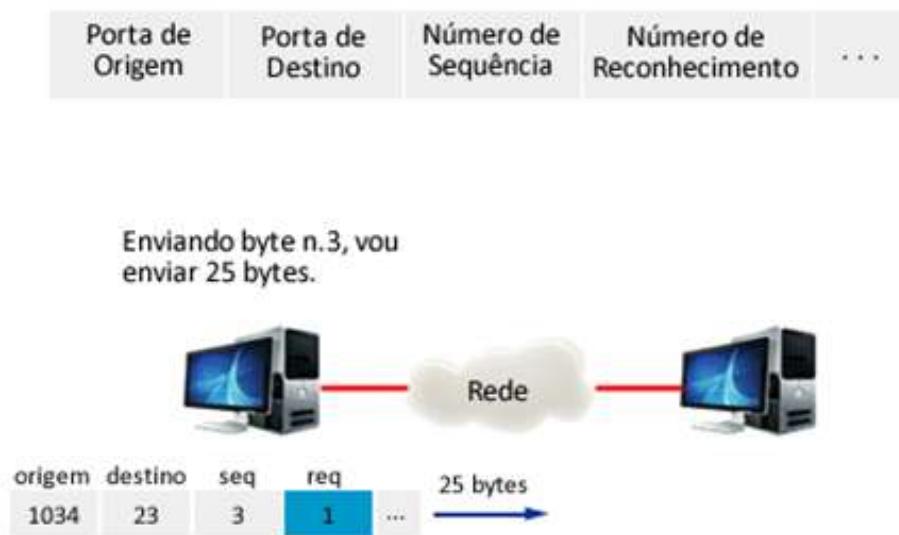
O número de sequência é o número relativo de bytes que foram transmitidos na sessão com iniciado pelo ISN definido no início da conexão, já o número de confirmação é o valor recebido mais 1.

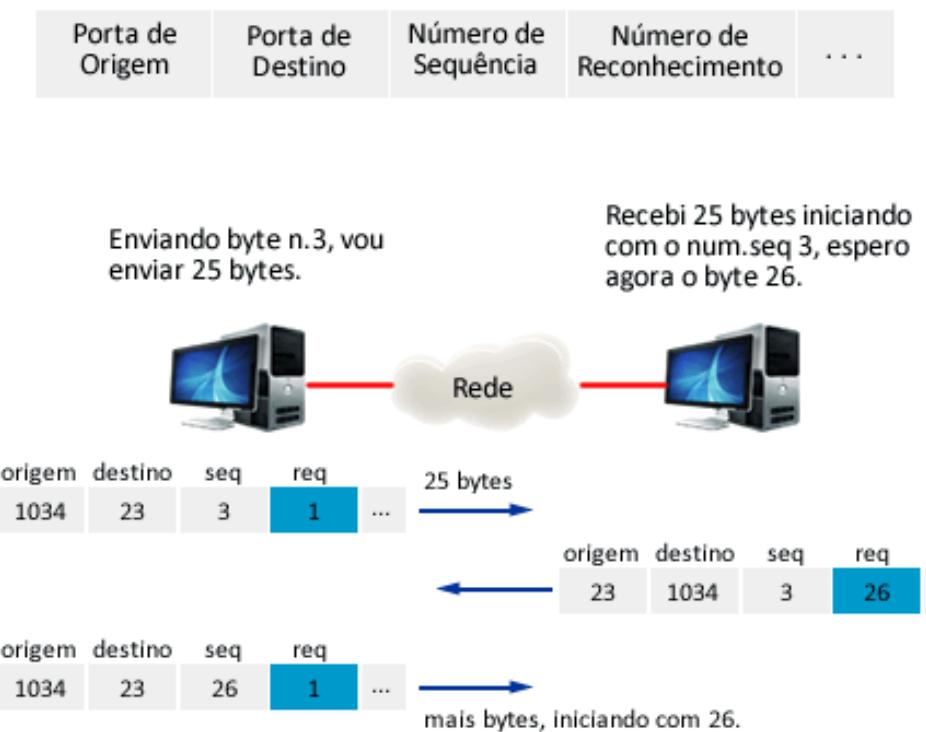
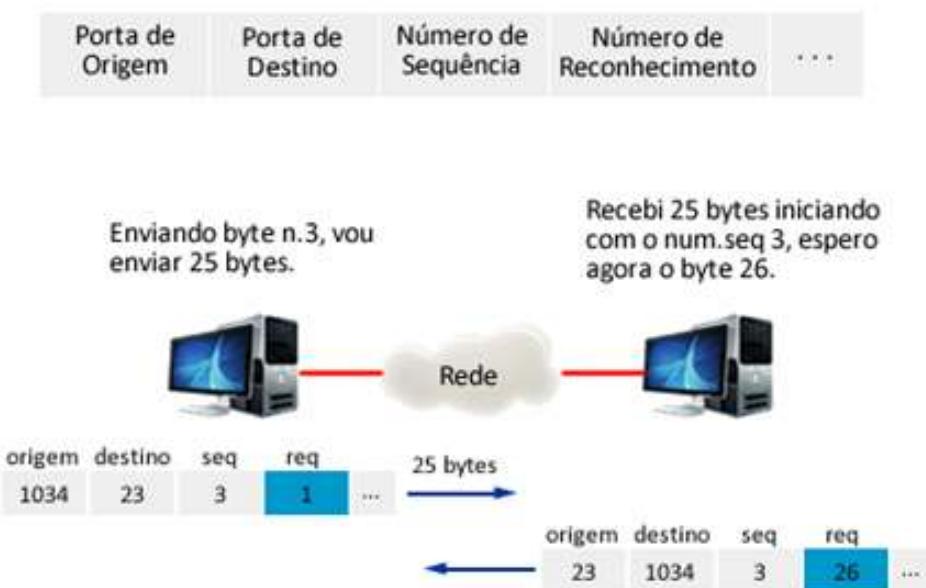
O TCP usa o número de confirmação em segmentos enviados de volta à origem para indicar o próximo byte que o receptor espera receber nessa sessão. Isto é chamado de confirmação esperada. Dessa forma o TCP assegura que cada segmento atinja o seu destino.

A origem é informada de que o destino recebeu todos os bytes neste fluxo de dados até, mas não incluindo, o byte indicado pelo número de confirmação. Espera-se que o emissor envie um segmento que utilize um número de sequência que é igual ao número de confirmação.

Lembre-se, cada conexão é na verdade composta por duas sessões unidirecionais. Os números de sequência e de confirmação estão sendo trocados em ambas as direções.

Vamos exemplificar com as figuras a seguir, sendo que a explicação está contida nas próprias imagens.





Vamos supor que o host da esquerda está enviando dados para o host da direita. Ele envia um segmento contendo 25 bytes de dados para essa sessão e um número de sequência igual a 3 no cabeçalho.

O host receptor da direita recebe o segmento na Camada 4 (Camada de Transporte) e determina que o número de sequência é 3 e que ele tem 25 bytes de dados. O host então envia um segmento de volta ao host da esquerda para confirmar o recebimento deste dado. Neste segmento, o host define o número de confirmação em 26 para indicar que o próximo byte de dados que ele espera receber nessa sessão é o byte número 26.

Quando o host emissor da esquerda recebe essa confirmação, ele pode agora enviar o próximo segmento contendo dados para essa sessão iniciando com o byte número 26.

Examinando esse exemplo, se o host de envio tiver que esperar pela confirmação de recebimento de cada 25 bytes, a rede teria muito overhead. Para reduzir o overhead dessas confirmações, múltiplos segmentos de dados podem ser enviados e confirmados com uma única mensagem TCP na direção oposta. Este confirmação contém um número de confirmação baseado no número total de bytes recebidos na sessão.

Por exemplo, começando com um número de sequência de 1000, se 10 segmentos de 1000 bytes cada fossem recebidos, o número de confirmação 11001 seria retornado à origem.

```
#####SIN=1000
10 segmentos de 1000 bytes = 10 x 1000 = 10000
ACK=1000 + 10000 + 1 = 11001
#####
```

A quantidade de dados que a origem pode transmitir antes que uma confirmação seja recebida é chamada de tamanho da janela. O Tamanho de Janela é um dos campos no cabeçalho TCP que habilita o gerenciamento de dados perdidos e o controle de fluxo.

### 3.3.4 Retransmissão de Segmentos TCP

Por melhor que seja o projeto de uma rede ocasionalmente ocorrerão perdas de alguns dados. Para contornar essa perda de dados, o TCP possui um mecanismo que retransmite segmentos com dados não confirmados.

Um serviço de host de destino usando TCP geralmente reconhece os dados apenas para bytes sequenciais contíguos. Se algum segmento não for recebido apenas os dados nos segmentos que completam o fluxo serão confirmados. Por exemplo, se os segmentos com números de sequência de 1000 a 3000 e de 4000 a 5000 fossem recebidos, o número de confirmação seria 3001. Isto porque existem segmentos com os números de sequência de 3001 a 3999 que não foram recebidos.

Quando o TCP no host de origem percebe que não recebeu uma confirmação depois de um período pré-determinado de tempo, ele voltará ao último número de confirmação que recebeu e retransmitirá os dados a partir daquele ponto para frente.

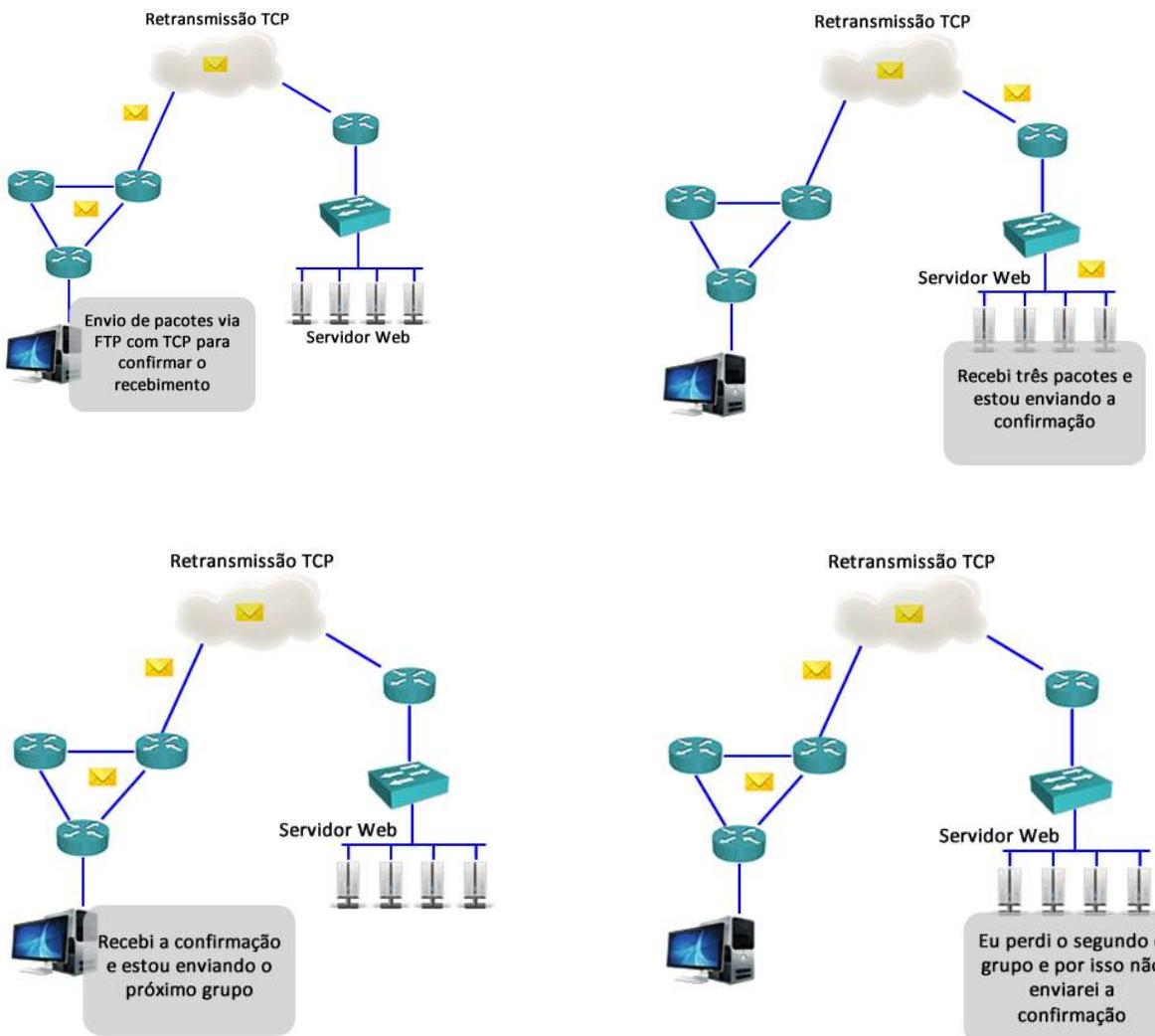
Para uma implementação de TCP típica, um host pode transmitir um segmento, colocar uma cópia do segmento numa fila de retransmissão e iniciar uma contagem. Quando a confirmação do dado é recebida, o segmento é deletado da fila. Se a confirmação não for recebida antes da contagem expirar, o segmento é retransmitido.

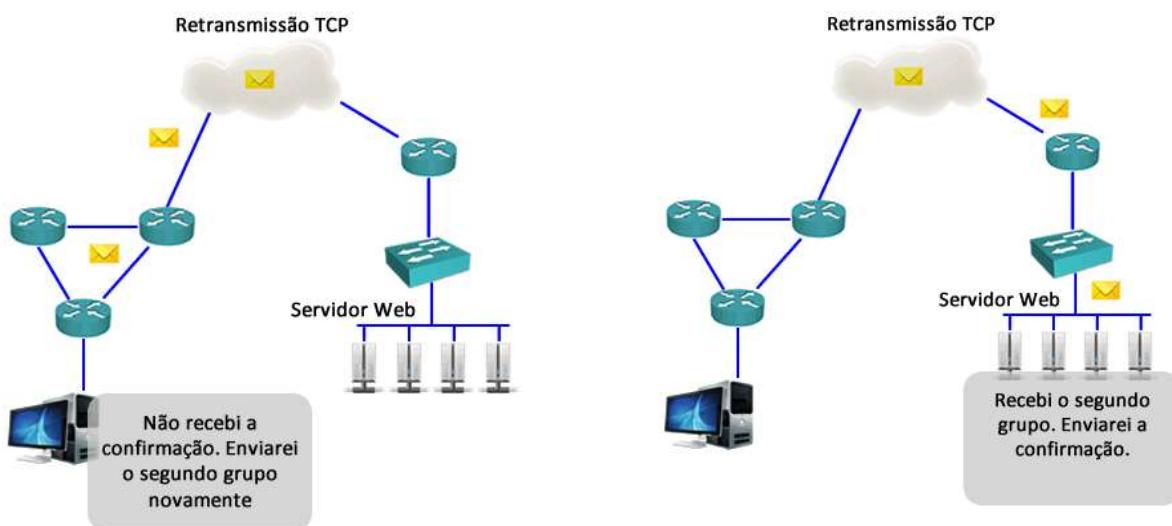
Existe também um método chamado de Confirmação Seletiva. Quando ambos os hosts suportam Confirmações Seletivas, é possível para o destino confirmar bytes em segmentos não contíguos e o host precisará apenas retransmitir os dados perdidos.

Veja na figura ao lado uma ilustração da retransmissão TCP.

Na prática, se você desconfiar que a sua rede está congestionada verifique o número de retransmissões solicitadas pelos equipamentos, pois se está existindo muita necessidade de retransmissão é sinal que os pacotes não estão chegando ao seu destino e a mais provável causa é uma sobrecarga na rede ou um congestionamento. Isso pode ser verificado colocando um "Analizador de Protocolo" para fazer uma varredura dos pacotes que estão sendo trocados na rede.

Veja as figuras a seguir com um exemplo de retransmissão.

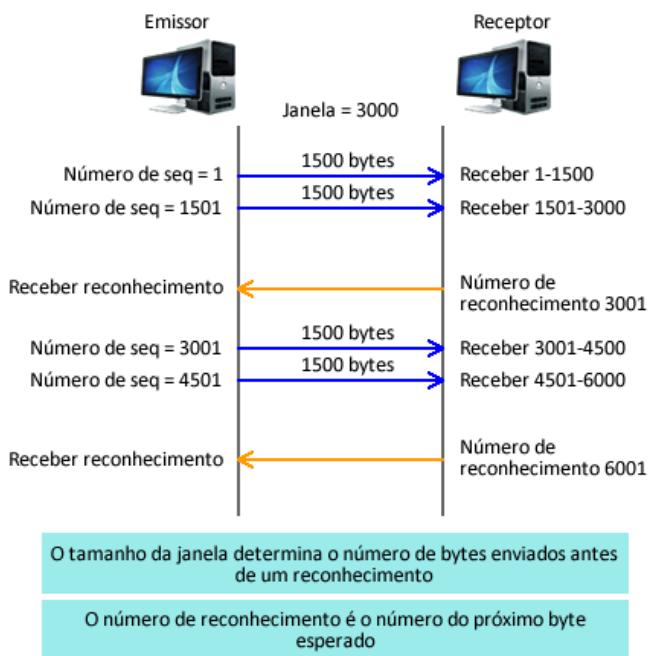




### 3.3.5 Controle de Congestionamento TCP

O controle de congestionamento no TCP é realizado através do tamanho da janela de transmissão, ou seja, através de quantos bytes foram confirmados através do número de reconhecimento.

Por exemplo, o computador que iniciou a comunicação tentou mandar uma quantidade de 1500 bytes por janela, se o receptor não conseguir tratar essa quantidade de informações ou a rede estiver lenta, a confirmação não será 1501, como deveria, e sim um número menor até ajustar o tamanho da janela, por isso esse processo é chamado de janelamento ou janela móvel.



Outra forma de controle de congestionamento é chamada “**Slow Start**”, ou seja, o TCP inicia o envio de informações com poucos bytes e vai aumentando o tamanho da janela gradativamente

até que seja encontrado o valor ideal. Esse processo é dinâmico e se adapta às condições da rede.

### 3.3.6 Reagrupamento de Segmentos TCP

Mais uma vez (para gravar bem) vamos reforçar que o TCP é um protocolo orientado a conexão. No entanto, quando algum serviço utiliza o protocolo TCP para enviar dados, os segmentos de dados podem chegar fora de ordem. Mas por quê?

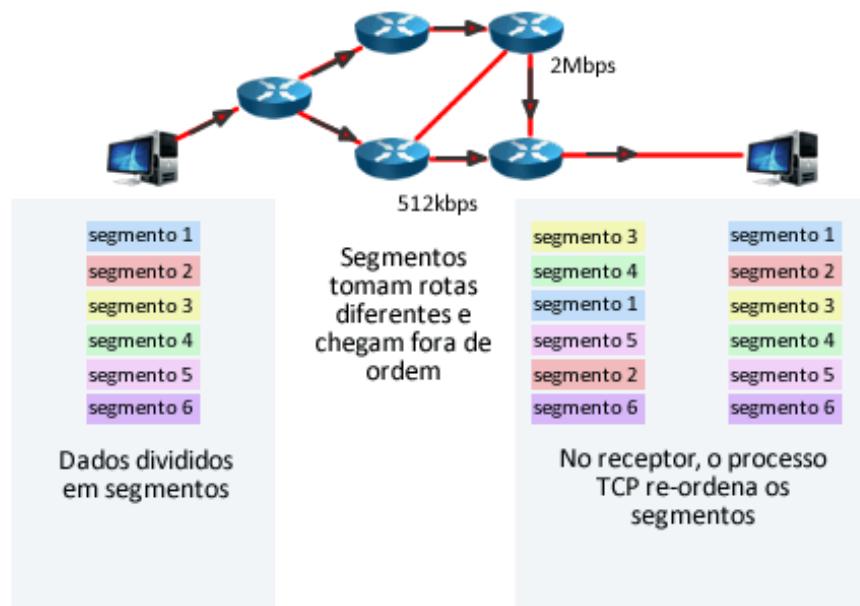
Porque os diversos segmentos podem percorrer caminhos diferentes para chegar no destino. Um segmento pode ser roteado dentro da rede e percorrer um caminho que tenha uma velocidade mais rápida ou um delay menor.

No entanto, para que a mensagem original seja entendida pelo receptor, os dados desses segmentos precisam ser reagrupados em sua ordem original. Para isso existe no cabeçalho TCP o campo "número de sequência".

Durante a instalação de uma sessão, um número de sequência inicial (ISN) é definido. Este número de sequência inicial representa o valor de partida para os bytes para esta sessão. À medida que os dados são transmitidos durante a sessão, o número de sequência é incrementado pelo número de bytes que foram transmitidos. Dessa forma cada segmento pode ser identificado e reconhecido, pois cada um terá um número de sequência único que seguirá uma ordem definida.

O processo TCP do receptor coloca os dados de um segmento em um buffer. Os segmentos são então colocados na ordem do número de sequência apropriada e passados para a camada de Aplicação quando reagrupados. Quaisquer segmentos que cheguem com números de sequência não contíguos são retidos para processamento posterior. Então, quando os segmentos com os bytes perdidos chegam, esses segmentos são processados.

Esse processo de sequenciamento é que fornece a confiabilidade do TCP, pois garante que os segmentos serão entregues na ordem corretas e sem faltar nenhum pedaço.



### 3.3.7 Aplicações Cliente Servidor com TCP

Em aplicações que utilizam o TCP como protocolo de transporte existe uma diferenciação entre os clientes e servidores.

Os clientes são os micros que solicitam serviços, por exemplo, você utilizando a Internet para assistir o curso precisou acessar uma página da Web em HTML, a qual utiliza o protocolo TCP na porta 80 do servidor. No seu computador você utiliza uma porta de cliente acima de 1024.

Uma característica importante é que o servidor tem seu programa sempre esperando uma conexão de um cliente, ficando com suas portas de servidor em um estado de escuta ou listening. Com o comando netstat -a você pode verificar se o seu computador tem portas em listening e programas instalados como servidores.

Active Connections			
Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	MICROALUNO-T4:0	LISTENING
TCP	0.0.0.0:445	MICROALUNO-T4:0	LISTENING
TCP	10.0.0.107:139	MICROALUNO-T4:0	LISTENING
TCP	10.0.0.107:55822	sn1msg3010716:msnp	ESTABLISHED
TCP	10.0.0.107:55826	204.56.87.25:https	ESTABLISHED
TCP	10.0.0.107:55867	mail:https	ESTABLISHED
TCP	10.0.0.107:55868	mail:https	ESTABLISHED
TCP	10.0.0.107:55870	mail:https	ESTABLISHED
TCP	10.0.0.107:56479	yw-in-f121:http	CLOSE_WAIT
TCP	10.0.0.107:56480	bs-in-f104:http	CLOSE_WAIT
TCP	10.0.0.107:56481	187:http	CLOSE_WAIT
TCP	10.0.0.107:57346	smtp:http	TIME_WAIT
TCP	10.0.0.107:57363	10.194.8.229:https	SYN_SENT
TCP	127.0.0.1:5550	MICROALUNO-T4:0	LISTENING
TCP	127.0.0.1:5679	MICROALUNO-T4:0	LISTENING
TCP	[::]:135	MICROALUNO-T4:0	LISTENING
TCP	[::]:445	MICROALUNO-T4:0	LISTENING
TCP	[::]:990	MICROALUNO-T4:0	LISTENING
TCP	[::]:3389	MICROALUNO-T4:0	LISTENING
TCP	[::]:5357	MICROALUNO-T4:0	LISTENING
TCP	[::]:8081	MICROALUNO-T4:0	LISTENING
TCP	[::]:49152	MICROALUNO-T4:0	LISTENING
TCP	[::]:49153	MICROALUNO-T4:0	LISTENING
TCP	[::]:49154	MICROALUNO-T4:0	LISTENING
TCP	[::]:49157	MICROALUNO-T4:0	LISTENING
TCP	[::]:49158	MICROALUNO-T4:0	LISTENING
TCP	[::]:49159	MICROALUNO-T4:0	LISTENING
TCP	[::1]:5679	MICROALUNO-T4:0	LISTENING
UDP	0.0.0.0:123	*:*	
UDP	0.0.0.0:427	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:3544	*:*	
UDP	0.0.0.0:3702	*:*	
UDP	0.0.0.0:3702	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	0.0.0.0:5355	*:*	
UDP	0.0.0.0:60305	*:*	
UDP	0.0.0.0:64833	*:*	
UDP	10.0.0.107:9	*:*	

```

UDP  10.0.0.107:137      *:*
UDP  10.0.0.107:138      *:*
UDP  10.0.0.107:427      *:*
UDP  10.0.0.107:1900     *:*
UDP  192.168.1.111:9      *:*
UDP  [::]:123            *:*
UDP  [::]:500             *:*
UDP  [::]:3702            *:*
UDP  [::]:3702            *:*
UDP  [::]:4500            *:*
UDP  [::]:5355            *:*
UDP  [::]:64834           *:*
UDP  [::1]:1900           *:*

```

C:\>

Perceba que as portas TCP possuem vários status, os mais importantes são:

- **Estabelecido ou Established:** significa que a conexão foi estabelecida e estão sendo transmitidas informações entre o seu computador e o servidor remoto.
- **Escutando ou Listening:** significa que existe um programa ou serviço instalado em modo servidor em seu computador. O Windows tem vários serviços desse tipo e aplicativos P2P, como Kazaa e Emule também costumam instalar portas em modo de escuta em seu computador. Se você preferir faça uma pesquisa na Internet sobre a porta que está aberta e verifique se não foi invadido.
- **SYN enviado ou SYN sent:** significa que o processo de negociação para abertura de uma comunicação TCP foi iniciada. Lembre que o SYN é enviado no início da comunicação. Nesse momento o SYN está setado para 1 e o Established em 0, pois não há conexão. Ao final da negociação do handshake triplo o Ack ou reconhecimento passa para 1. No capítulo de Listas de controle de acesso essa informação será importante, pois é através dela que você define uma conexão a um programa servidor, pois se seu micro é somente cliente ele deveria rejeitar todas as conexões com o ACK igual a 0, ou seja, rejeitar iniciar uma conexão, pois você quem deveria iniciar.

Portanto, resumindo, um servidor terá uma porta no estado de listening sempre esperando conexão, ele aceitará tantas conexões quanto for sua capacidade de processamento e memória. Caso hajam solicitações em excesso o servidor pode ser afetado e "cair", isso é chamado ataque de negação de serviço ou DoS (Denial of service), utilizado pelos hackers para derrubar um determinado servidor ou sobrecarregá-lo para propiciar uma invasão.

Importante: não deixe de ler o documento "O Comando netstat" que se encontra na "Área do Aluno" na guia de programação do capítulo 05.

### 3.4 Protocolo UDP

Ao contrário do TCP o protocolo UDP não é orientado a conexão, portanto não possui mecanismos sofisticados de controle de congestionamento e erros como o TCP.

O UDP transmite os datagramas de forma "best-effort" ou seja "melhor esforço", ficando a cargo das aplicações tratarem dos erros e controle da transmissão. O único campo de controle do UDP é o Checksum para verificar a integridade do datagrama recebido. Veja na figura ao lado o datagrama do UDP.

Sobre a comunicação através de portas o funcionamento do UDP é similar ao TCP, tendo portas específicas para determinados serviços. A grande diferença é que não existe conexão, elas sempre estão preparadas para receber dados de um host remoto que deseja se comunicar.

Pelo fato do UDP ser mais simples, ele acaba se tornando mais rápido e preferido para aplicações onde a velocidade é fundamental, como a voz sobre o protocolo IP ou VoIP. O protocolo RTP (Real Time Protocol) utiliza o serviço UDP para transmitir a voz entre aparelhos IP. Outro exemplo de aplicação são as VPN's ou redes virtuais privadas, elas também normalmente utilizam serviço UDP para transmissão dos seus dados criptografados, pois os pacotes acabam sendo enviados mais rápidos e com menos cabeçalho, pois o UDP tem bem menos bits de controle que o TCP.

As portas do UDP não tem estado, pois elas estão sempre prontas para receber dados.

bit 0	bit 15	bit 16	bit 31
porta de origem (16)		porta de destino (16)	
comprimento (16)		checksum (16)	
Dados (caso existam)			

- **Porta de origem:** Número da porta chamadora.
- **Porta de destino:** Número da porta chamada.
- **Comprimento:** Número de bytes que inclui cabeçalho e dados.
- **Checksum:** Cálculo de verificação (checksum) feito através de campos do cabeçalho e dados.
- **Dados:** Dados de protocolo de camada superior.

### 3.5 Hora de Refletir sobre as Camadas de Aplicação e Transporte do TCP/IP

Antes de você executar o laboratório 5.1 e passar para o próximo tópico vamos dar uma parada para refletir e resumir o que foi estudado até o momento.

Se você não conseguiu notar, até o momento ainda estamos dentro do computador e nossa informação ainda não está pronta para ser enviada através da rede na camada de Transporte, vamos resumir o que aconteceu até o momento quando, por exemplo, o usuário abriu um navegador da Web e digitou [www.exemplo.com.br](http://www.exemplo.com.br):

1. A camada de aplicação recebeu do navegador de Internet uma solicitação para acessar o conteúdo da página [www.exemplo.com.br](http://www.exemplo.com.br).
2. A camada de aplicação do TCP/IP irá verificar se o computador tem recursos para processar as informações e como ela faz a parte das camadas de aplicação, apresentação e sessão do modelo OSI, ela irá formatar os dados e inserir os controles de sessão, inserindo seu cabeçalho de aplicação e repassará as informações para a camada de transporte solicitando uma conexão do tipo TCP, pois como já estudamos o protocolo HTTP utiliza o transporte TCP para envio de suas informações.
3. Quando a camada de transporte recebe essa requisição ela deve abrir uma porta de origem, a qual em clientes deve ser uma porta Dinâmica ou Privada com um valor entre 49152 e 65535, vamos utilizar a porta 51000 nesse caso, por exemplo. Esta porta de origem indica que todo o tráfego que vier como resposta para o computador de origem destinado à porta 51000 pertence ao navegador de Web e será encaminhado para esse programa em específico. Se não houvesse esse recurso o acesso à rede seria "monotask", ou seja, teríamos que acessar um conteúdo por vez. Portanto as portas TCP

e UDP tem a função de identificar a que programa cada fluxo pertence e também possibilitar o uso compartilhado da rede (chamado de multiplexação).

4. Como o cliente quer se comunicar com um servidor HTTP a camada de transporte vai utilizar a porta de destino com o número 80, pois assim quando essa informação chegar ao servidor ele irá encaminhar essa solicitação HTTP ao programa que estiver utilizando a porta 80 no estado de escuta (listening).
5. Após a camada de transporte inserir todas as informações de controle (cabeçalho) ela passa seus segmentos à camada inferior (de rede) para que esses segmentos sejam endereçados e aí sim encaminhados pela rede.

O encaminhamento pela rede será visto nos tópicos seguintes, portanto vamos supor que tudo correu bem e as informações chegaram ao destino e mais especificamente foram entregues à camada de transporte do servidor de destino. Com as informações em mãos e servidor de destino irá analisar a porta de destino que está no cabeçalho do TCP e checar se existe um programa esperando informações nessa porta. Em caso positivo ele retira seu cabeçalho e repassa as informações ao serviço HTTP para que o servidor processe as informações. O servidor nesse caso irá receber um comando HTTP parecido com o descrito abaixo:

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

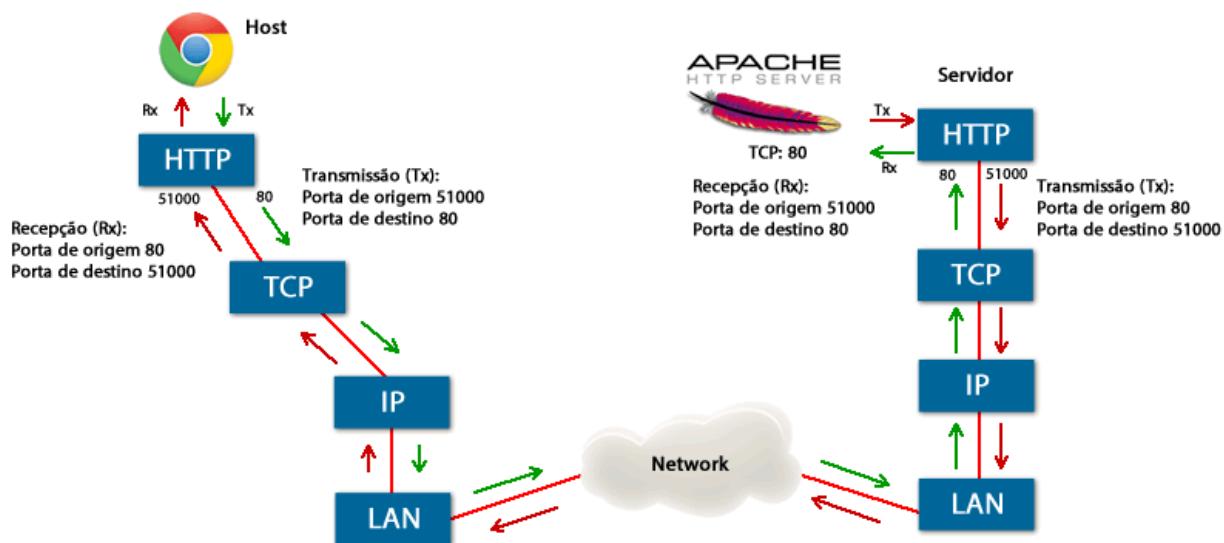
Com isso ele irá responder passando a página de Web com o conteúdo do site solicitado. Com o conteúdo da resposta definido o servidor irá seguir os passos parecidos com o que o cliente realizou para enviar a resposta, porém agora o que era endereço de origem fica como destino e vice versa. Portanto a porta TCP de origem fica como 80 (a do servidor) e de destino como 51000 (porta que o programa no computador do cliente está utilizando). A mensagem que o servidor enviará no HTTP será como a abaixo:

```
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>
```

Quando o cliente receber a resposta, a camada de transporte passará as informações recebidas para a porta 51000 e no navegador de internet do cliente aparecerá a seguinte página solicitada conforme a figura abaixo.



Veja na abaixo uma representação da comunicação entre o cliente HTTP e o servidor.



Portanto, para que não haja problemas de identificação das comunicações no computador de origem, as portas TCP e UDP utilizadas devem ser únicas, por isso em um servidor pode existir apenas um programa utilizando a porta 80, se você instalar dois programas servidores HTTP um deles terá que utilizar outra porta.

No final desse capítulo você verá que esse acesso a um conteúdo na rede pode ser um pouco mais complexo e envolver outros protocolos auxiliares, tais como ARP e DNS para resolução de nomes em nível local e de Internet. Além disso, nesse exemplo omitimos o processo de abertura de conexão realizado pelo handshake de três vias realizado pelo TCP.

Entender o fluxo dos pacotes, quadros e segmentos na rede é muito importante tanto para realizar o exame CCENT como na vida prática, pois somente entendendo bem o fluxo de informações em uma rede seremos capazes de realizar projetos e resolver problemas mais complexos em redes de computadores! Além disso, você precisará desses conceitos para fazer regras de firewall no capítulo de ACL (Listas de Controle de Acesso).

### 3.6 Hora de Praticar

Agora chegou a hora de um pouco de ação...

Entre na área do aluno, no capítulo 5 e faça o download do Laboratório 5.1 sobre Aplicações TCP/IP e execute em seu computador.

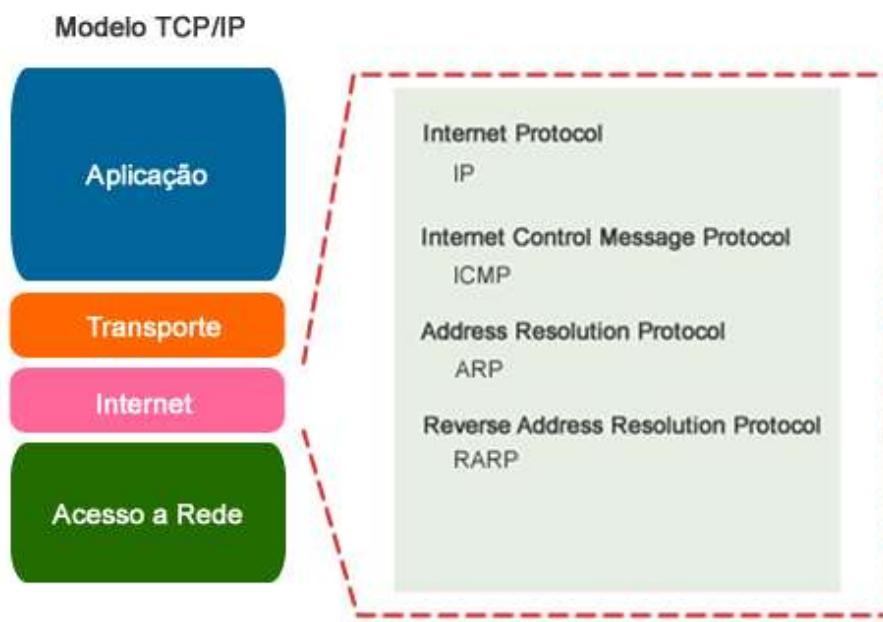
Algumas tarefas desse laboratório pedem a instalação de programas no computador do aluno, essas etapas são opcionais e de inteira responsabilidade do aluno, caso não seja do seu interesse apenas leia com atenção o que foi apresentado no documento.

## 4 Camada de Internet

A finalidade da Camada de Internet é a mesma que a camada de rede do modelo OSI, ou seja, fornecer esquema de endereçamento e escolher o melhor caminho para os pacotes viajarem através da rede.

A determinação do melhor caminho e a comutação de pacotes também ocorre nesta camada.

Veja os principais protocolos da camada de Internet na figura a seguir.



Abaixo seguem as principais funções de cada um dos protocolos:

- O **IP** oferece roteamento de pacotes sem conexão, e uma entrega de melhor esforço. Ele não se preocupa com o conteúdo dos pacotes, apenas procura um caminho até o destino.
- O **ICMP** (Internet Control Message Protocol – Protocolo de Mensagens de Controle da Internet) oferece recursos de controle e de mensagens, tais como ping.
- O **ARP** (Address Resolution Protocol – Protocolo de Resolução de Endereços) determina o endereço da camada de enlace (endereço MAC) para os endereços IP conhecidos.
- O **RARP** (Reverse Address Resolution Protocol – Protocolo de Resolução Reversa de Endereços) determina os endereços IP quando o endereço MAC é conhecido.
- **Protocolos de roteamento** são responsáveis por ler o endereçamento IP configurado e trocar informações de rota para definir o melhor caminho entre as diversas redes da Internetwork.

O protocolo IP atualmente possui duas versões: IPv4 e IPv6, ou seja, a versão 4 e versão 6. Ambos diferem em diversas características e são redes que funcionam em paralelo.

Atualmente a maioria das redes utiliza o IPv4, porém a implementação do IPv6 vem crescendo a partir do lançamento global realizado em 2012.

Ambas as versões do protocolo IP são “**best effort**”, ou seja, enviam suas informações na rede como o UDP estudado anteriormente, sem pedir confirmações.

Nesse momento vamos estudar o IPv4 e mais no final do curso vamos também abordar o IPv6.

#### 4.1 Cabeçalho do Protocolo IPv4

Abaixo segue o cabeçalho do protocolo IP versão 4 e logo abaixo a descrição dos campos.

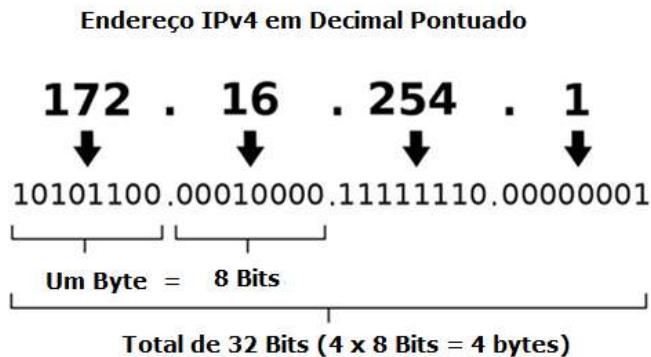
+	0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Versão	Tamanho do cabeçalho	Tipo de Serviço (ToS) (agora DiffServ e ECN)	Comprimento (pacote)	
32		Identificador		Flags	Offset
64	Tempo de Vida (TTL)		Protocolo	Checksum	
96		Endereço origem			
128		Endereço destino			
160		Opções			
192		Dados			

- **Versão:** Definido como 4.
- **IHL:** Comprimento do Cabeçalho da Internet com o número de palavras de 32 bits no cabeçalho IPv4.
- **Tipo de serviço:** Definido na RFC 791 e define o tipo de serviço (ToS – Type of Service), agora DiffServ e ECN utilizados para definir marcação de QoS.
- **Tamanho total:** Define todo o tamanho do datagrama incluindo cabeçalho e dados. O tamanho mínimo do datagrama ou pacote IP é de vinte bytes e o máximo é 64 Kbytes, porém o MTU mínimo que os hosts precisam suportar é de 576 bytes. Se os pacotes ultrapassarem o MTU precisam ser "fragmentados", ou seja, quebrados em pedaços menores para caberem dentro do tamanho máximo do protocolo do caminho. No IPv4 a fragmentação pode ser feita pelos computadores ou diretamente nos roteadores.
- **Identificador:** Usado principalmente para identificar fragmentos do pacote IP original.
- **Flags:** Usado para controlar ou identificar fragmentos.
- **Offset do fragmento:** permite que um receptor determine o local de um fragmento em particular no datagrama IP original.
- **Tempo de vida:** Chamado de TTL (time to live) ajuda a prevenir que os pacotes IP entrem em loop na rede. Utilizado para o teste de traceroute.
- **Protocolo:** Define o protocolo que será transportado no pacote, sendo que os protocolos comuns e os seus valores decimais incluem o ICMP (1) e o TCP (6).
- **Checksum:** Campo de verificação de erros para o cabeçalho do datagrama IPv4. Cobre apenas verificação do cabeçalho, não dos dados.

- **Endereço de origem/destino:** Campos que trazem os endereços de origem (transmissor) e de destino (receptor) de 32 bits cada um. Os endereços IP tem seus campos divididos em 4 conjuntos de 8 bits, ou seja, 4 bytes escritos em decimal pontuado, por exemplo, 192.168.1.1.
- **Opções:** Normalmente não utilizados.
- **Dados:** Informações das camadas superiores, por exemplo, segmentos TCP ou datagramas UDP.

Sem dúvida alguma os campos de endereçamento de origem e destino são os mais importantes do cabeçalho IP, pois eles que fornecem o endereçamento lógico utilizado para transporte do pacote através da rede. Lembre-se que o quadro de camada-2 é trocado durante a viagem do IP pela rede conforme o protocolo utilizado pelo link local, já o pacote IP é aberto somente pelo destino da transmissão.

Abaixo segue como um endereço IP é escrito em decimal pontuado e depois em bits.



Com 32 bits temos um total de  $2^{32}$  bits ou 4.294.967.296 de possíveis endereços IP. Portanto, o primeiro endereço IP versão 4 possível tem todos os bits em zero e o último todos os bits em 1:

- 1º endereço IP: 00000000.00000000.00000000.00000000 -> 0.0.0.0
- Último endereço IP: 11111111.11111111.11111111.11111111 -> 255.255.255.255

A faixa de variação dos endereços entre o primeiro 0.0.0.0 e o último 255.255.255.255 corresponde a todo espaço de endereçamento IPv4 disponível. Mais para frente você vai aprender que essa faixa foi dividida no início em classes (A, B, C, D e E) para possibilitar a divisão dos endereços entre instituições e empresas para possibilitar o endereçamento dos computadores na Internet.

Para aprender o endereçamento IP, divisão em redes, sub-redes e super-redes você precisará conhecer um pouco de matemática binária, por isso temos um tópico nesse capítulo e um documento extra tratando dos sistemas numéricos. Além do binário é importante entender também números Hexadecimais.

#### 4.2 Protocolo ICMP

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.

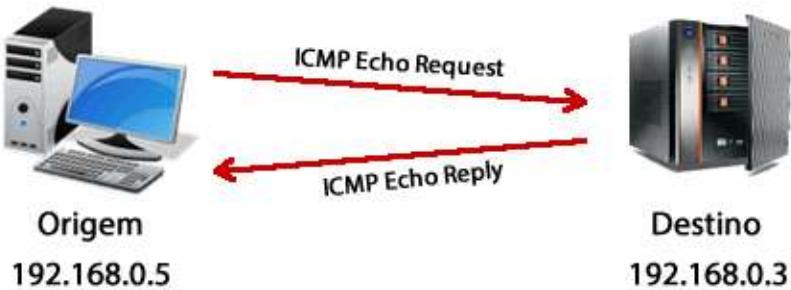
Qualquer computador que utilize IP precisa aceitar as mensagens ICMP e alterar o seu comportamento de acordo com o erro relatado. Os gateways (roteadores) devem estar programados para enviar mensagens ICMP quando receberem pacotes que provoquem algum tipo de erro.

O ICMP é transportado no campo de dados do pacote IP e identificado como tipo de protocolo 1 pelo cabeçalho do IP. As mensagens de erro ou de teste do 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 tempo de vida expirado ou “**time exceeded**”.
- O roteador não consegue retransmitir os pacotes na frequência adequada, ou seja, o roteador está congestionado (mensagem “**source quench**”).
- O roteador indica uma rota melhor para o host que está enviando pacotes (mensagem de redirecionamento de rota ou “**redirect**”).
- Quando um host de destino ou rota não está alcançável (mensagem “**destination unreachable**” ou destino inalcançável).
- Quando o host ou o roteador descobrem um erro de sintaxe no cabeçalho do IP (mensagem “**parameter problem**”).

Existem diversas outras mensagens que o ICMP pode fornecer e cada uma é representada por um tipo ou código, conforme será mostrado no quadro do ICMP no final desse tópico. Você pode baixar na área do aluno o documento em PDF com todas as mensagens ICMP com a descrição de outras mensagens de erro ou informações que o ICMP pode fornecer. Nesse tópico iremos focar nos recursos de **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 figura abaixo.



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

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

Disparando 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),

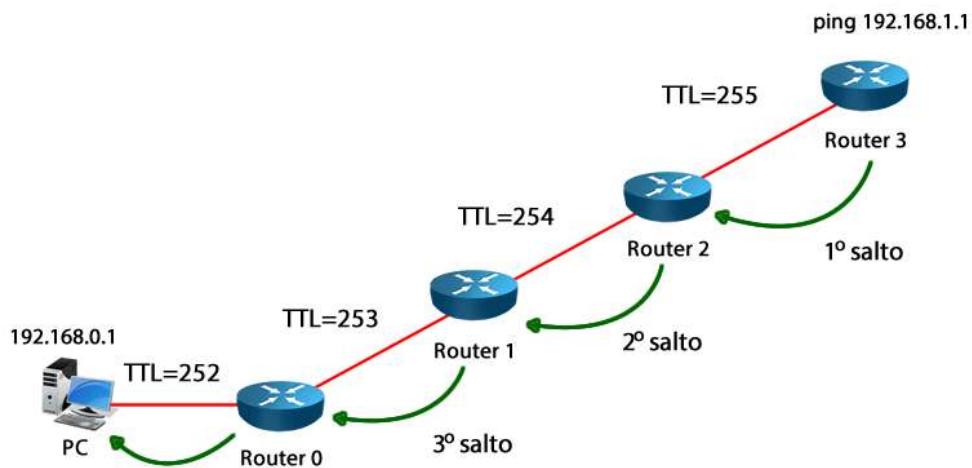
C:\Users\dltec>
```

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 (Intrusion Prevention System), 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 (Time to Live ou Tempo de Vida). O tempo de vida de um pacote é um contador que é decrementado a cada salto ou nó que o pacote IP passa. Cada sistema operacional define um TTL para seus pacotes, em roteadores Cisco o TTL é definido com o valor de 255. Abaixo seguem os valores padrões de TTL para os sistemas operacionais mais comuns:

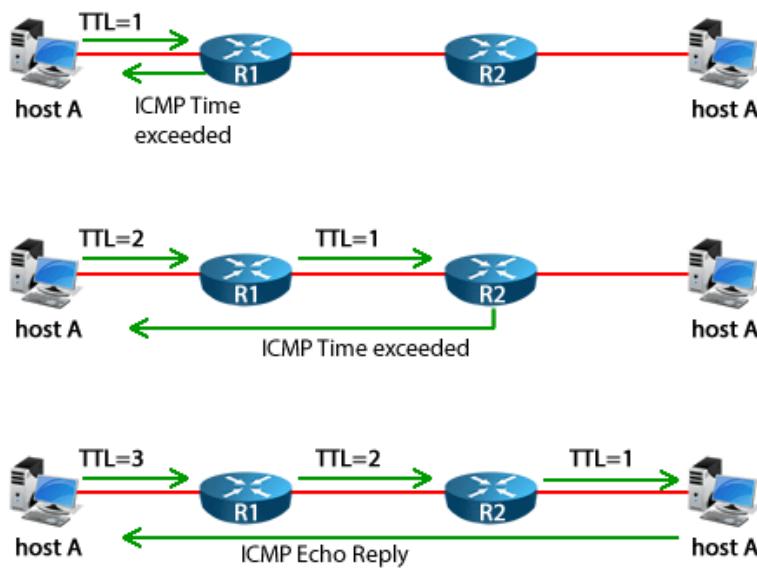
- **UNIX:** 255
- **Linux:** 64
- **Linux + Iptables** = 255
- **Windows:** 128
- **Cisco:** 255

Portanto, quando um roteador Cisco origina um pacote ele coloca o tempo de vida como 255 e a cada roteador que esse pacote passar será decrementado em 1, por exemplo, se o caminho entre o originador do pacote e o destino existirem 3 roteadores quando o pacote chegar ao destino ele terá o valor de TTL 252. Veja o exemplo citado anteriormente na figura abaixo.



Analisando a figura acima se um pacote IP trafegar por um número de saltos muito grande ele tem seu tempo de vida expirado o roteador que recebeu o pacote com TTL igual a zero deve enviar uma mensagem à origem do pacote com uma mensagem ICMP indicando esse problema. Nessa mensagem vem o IP do roteador e com isso o computador consegue saber por onde o problema ocorreu.

Podemos utilizar também essa característica para determinar o caminho que o pacote está passando entre a origem e o destino, para isso o host onde foi originado o traceroute manda um pacote com TTL igual a 1, no primeiro salto o pacote expira e o roteador responde com seu IP. 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 abaixo, onde o host de destino está a 3 saltos da origem.



Na tela da figura abaixo temos um exemplo do “**tracert**” que é o comando do Windows para o “**traceroute**” (Cisco, Unix 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.

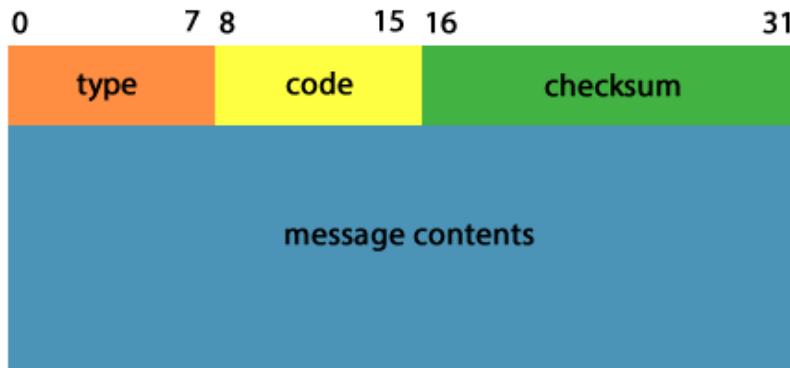
```
C:\Windows\system32\cmd.exe
C:\Users\dltec>tracert www.dltec.com.br

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-0-0-4-rt02.spo.gvt.net.br [187.115.214.194]
 9 171 ms  179 ms  184 ms  Xe0-1-1-0-grtsaos12.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 [213.140.51.19
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.
```

Na figura a seguir temos o formato do pacote ICMP e logo depois a explicação dos campos.



- **TYPE (8 bits)**: identifica o tipo mensagem, por exemplo, se o valor for 8 é uma requisição (echo request). Se o conteúdo for 0 é uma resposta (echo reply).
- **CODE (8 bits)**: utilizado em conjunto com o campo TYPE para identificar o tipo de mensagem ICMP que está sendo enviada.
- **CHECKSUM (16 bits)**: verifica a integridade do pacote ICMP.
- **MESSAGE CONTENTS (Tamanho Variável)**: contém o conteúdo da mensagem ICMP.

#### 4.3 Protocolos ARP, RARP e Proxy ARP

Existe uma polêmica normalmente sobre onde o ARP e RARP estão posicionados no modelo OSI, porém como eles não utilizam endereços de camada 3 para tomarem decisões e são encaminhados utilizando endereços MAC são considerados da camada 2 do modelo OSI.

Em algumas bibliografias da Cisco você pode até ouvir falar que ele está na “**camada 2.5**”, ou seja, **entre as camadas 2 e 3** do modelo OSI.

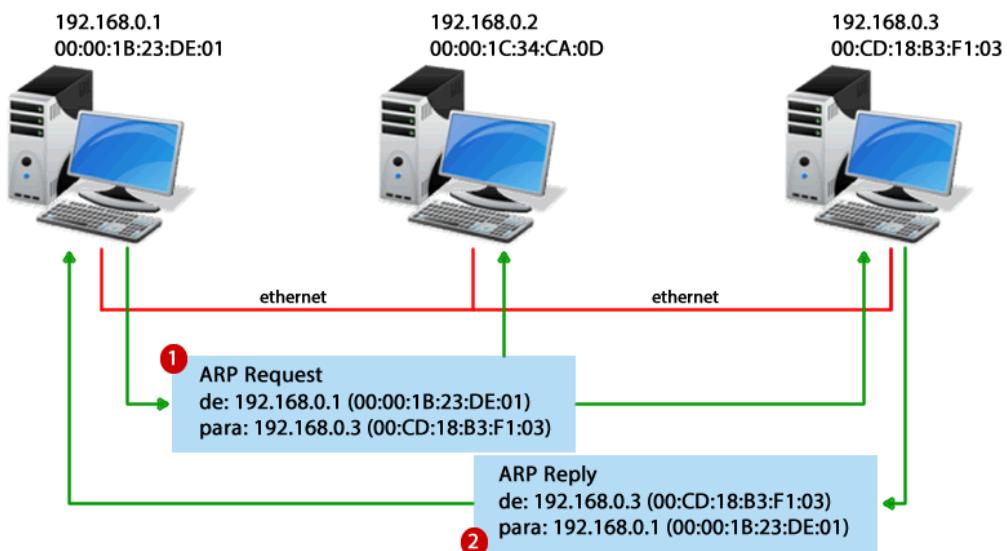
##### 4.3.1 Entendendo o ARP

Para que um pacote IP possa ser encaminhado em uma rede broadcast multiacesso, como são as redes do padrão 802.3 (Ethernet) e 802.11 (WLAN), é necessário que o computador que está originando o tráfego conheça os endereços físico e lógico do computador remoto. Normalmente quando vamos fazer um teste de ping, por exemplo, o nosso computador conhece seu próprio MAC e IP, ou seja, os endereços de origem e nós iremos digitar o endereço IP de destino, portanto falta um detalhe: “**Qual o endereço MAC do computador de destino?**”.

Esta resposta é o objetivo do protocolo ARP (definido na RFC826), descobrir um MAC de destino dado um IP. Portanto o protocolo ARP é sempre utilizado antes que um pacote IP seja enviado, a não ser que o computador já conheça o endereço MAC do computador de destino.

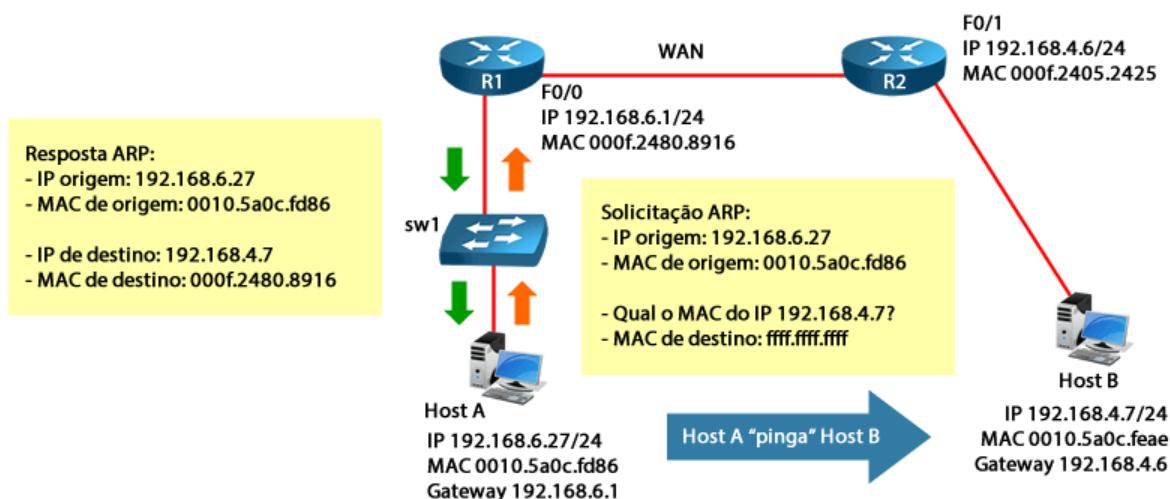
Existem três cenários principais em que o ARP é utilizado:

1. Quando dois computadores pertencem à mesma LAN o computador de origem solicita em broadcast o endereço MAC do computador de destino em broadcast. Veja a figura abaixo, onde o computador com IP 192.168.0.1 faz uma requisição ARP (ARP Request) em broadcast para descobrir o MAC do computador com IP 192.168.0.3, o qual responde a solicitação ARP com um “ARP Reply” ou resposta ARP diretamente para o solicitante.



2. Quando dois computadores não pertencem à mesma LAN ou estão separados por uma WAN, por exemplo, é um servidor da Internet, o computador de origem solicita em

broadcast o endereço MAC do seu roteador padrão (gateway padrão) que está configurado em suas opções de rede. Veja a figura abaixo onde o Host A deseja fazer um ping para o Host B, porém como eles estão em redes diferentes o Host A solicita o MAC do seu gateway para que ele possa servir de intermediário entre as duas redes, encaminhando os pacotes para que eles cheguem ao seu destino.



- Envio de **ARP Gratuito (Gratuitous ARP)**, o qual é uma requisição ARP gerada pelo próprio Host para obter o seu próprio endereço IP. O ARP Gratuito é utilizado para **detectar duplicação de endereços** ou para que outros computadores atualizem seu cachê de ARP (tabela onde os endereços MACs aprendidos são armazenados). O Gratuitous ARP também pode ser utilizado por atacantes para redirecionar pacotes e realizar ataques como o Man-in-the-Middle.

Na figura abaixo você pode verificar o formato do quadro que o ARP utiliza e logo a seguir as explicações de cada campo.

0	8	16	24	31			
HARDWARE TYPE		PROTOCOL TYPE					
HLEN	PLEN	OPERATION					
SENDER HA(OCTETS 0-3)							
SENDER HA(OCTETS 4-5)		SENDER IP(OCTETS 0-1)					
SENDER IP (OCTETS 2-3)		TARGET HA(OCTETS 0-1)					
TARGET HA(OCTETS 2-5)							
TARGET IP(OCTETS 0-3)							

- **Hardware Type (tipo do hardware)**: composto de dois octetos e especifica o tipo de hardware utilizado na rede física. Se for 1, é rede Ethernet.
- **Protocol Type (tipo do protocolo)**: composto de dois octetos e especifica o endereço do protocolo utilizado no nível superior do emissor.
- **Operation (operação)**: especifica se o datagrama é um pedido ARP (request 1) ou uma resposta ARP (reply 2), ou ainda um RARP (request 3, reply 4).
- **HLEN e PLEN**: habilitam o ARP para ser usado com redes arbitrárias porque eles especificam o comprimento dos endereços do hardware e dos protocolos do nível superior. O HLEN (Hardware Length) é utilizado para identificar o tamanho dos campos SENDER HA e TARGET HA. PLEN (Protocol Length) especifica o tamanho dos campos SENDER IP e TARGET IP.
- **SENDER HA (Endereço MAC de origem)**: endereço físico (Ethernet) de quem envia o pacote.
- **SENDER IP (Endereço IP de Origem)**: endereço lógico (IP) de quem envia o pacote.
- **TARGET HA (Endereço MAC de Destino)**: Endereço físico desejado. Na operação de request vai em branco, e, quem responder preenche este campo.
- **TARGET IP (Endereço IP de Destino)**: Endereço lógico da máquina desejada.

Uma vez que o computador utilizou o ARP para aprender endereço MAC ele armazena os resultados em uma tabela de endereços MAC chamada **cachê ARP** ou **ARP Cache**. Esta tabela de endereços MAC é utilizada para reduzir os broadcasts na rede. Depois de algum tempo o endereço MAC no ARP Cache é removido, independentemente de estar sendo usado ou não. Isto é chamado de **Aging Time** (tempo de envelhecimento ou de obsolescência).

Outra forma de um computador aprender endereços MAC é de maneira estática, ou seja, endereços que são inseridos manualmente pelo administrador de redes ou então pelo próprio sistema operacional. Para esses tipos de entradas o computador nunca precisará utilizar um ARP Request, porém como o MAC de um host está vinculado à sua placa de rede, toda vez que a placa de rede for trocada o administrador precisará alterar a entrada estática do endereço MAC configurada manualmente em um ou mais hosts.

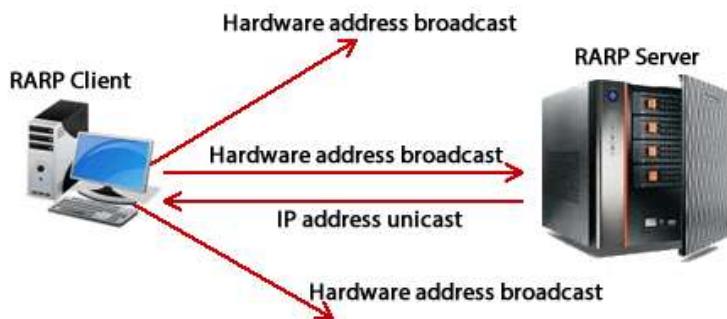
Para verificar o conteúdo da tabela ARP no Windows você pode abrir o prompt de comando e digitar o comando “**arp -a**”. Já em um roteador ou switch Cisco você deve digitar em modo de usuário privilegiado o comando “**show arp**” (Router#show arp).

No **laboratório 5.2** você poderá fazer vários testes relacionados ao ICMP e ARP importantes para a compreensão do que estudamos até o momento e fundamentais para resolução de exercícios que podem ser pedidos no CCENT, não deixe de realizar os testes e estudar muito bem o assunto, pois o ARP é um protocolo transparente no uso das redes no dia a dia, porém utilizado constantemente por nossos computadores.

#### 4.3.2 Entendendo o RARP

**Reverse Address Resolution Protocol (RARP)** ou **Protocolo de Resolução Reversa de Endereços** associa um endereço MAC conhecido a um endereço IP que se deseja conhecer. Permite que os dispositivos de rede encapsulem os dados nos pacotes 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. Veja a figura abaixo.



Atualmente o RARP foi substituído pelo serviço de alocação dinâmica de IPs realizado pelo protocolo **DHCP**.

#### 4.3.3 Entendendo do Proxy ARP

O **Proxy ARP** é um método onde um determinado roteador responde um **ARP Request** em nome de outro dispositivo. Este protocolo está definido na RFC-1027 foi desenvolvido no final dos anos 80 pelo Departamento de Ciências da Computação da Universidade do Texas em Austin devido à necessidade de segmentação de redes que utilizavam apenas uma classe de endereços IP sem divisão em sub-redes (veremos mais para frente nesse capítulo).

Naquela época, nem todos os dispositivos de rede podiam ter seus endereços de redes segmentados em sub-redes, ou seja, um endereço classe A não poderia ser dividido em duas, quatro, oito, ou outras quantidades de redes diferentes, pois os hosts somente reconheciam a classe de seu IP.

Com o método de Proxy ARP, foi possível que com um endereço de classe A configurado em diversos hosts com máscara padrão para esta classe fossem segmentados por roteadores ou firewalls que tivessem o método de Proxy ARP implementado.

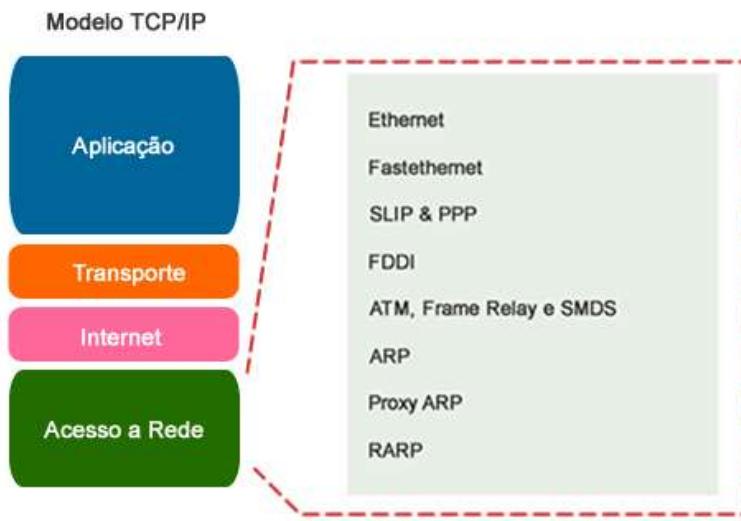
O Proxy ARP habilitado (comando “ip proxy-arp) em sua interface de LAB Fast 0/0. Este recurso é habilitado por padrão em roteadores Cisco e é recomendado que fosse desabilitado caso seu uso não seja necessário (comando no ip proxy-arp).

Atualmente não é possível fazer a configuração de uma mesma rede IP em interfaces diferentes, por isso se você habilitar o Proxy ARP o roteador com esse comando habilitado iria fornecer seu próprio MAC para uma requisição ARP que viesse para um IP de uma rede que esse roteador conhecesse, mesmo que não fosse a melhor opção de roteamento.

## 5 Camada de Acesso à Rede (ou Acesso aos Meios)

O objetivo da camada de acesso à rede (algumas fontes bibliográficas também chamam de acesso aos meios) é que o pacote IP estabeleça efetivamente um link físico com os meios físicos disponíveis da rede de maneira transparente, ou seja, não importando o meio de transmissão que esteja sendo utilizado.

Inclui detalhes de tecnologia de redes locais e de WANs e todos os detalhes contidos na camada física e de enlace de dados do modelo OSI e suas funções incluem o mapeamento de endereços IP para endereços físicos de hardware e o encapsulamento de pacotes IP em quadros. Veja a figura abaixo.



É importante lembrar que durante a transmissão de dados em uma rede IP os cabeçalhos da camada de acesso à rede ou camada de enlace do modelo OSI variam de acordo com a tecnologia adotada, porém o cabeçalho do IP nunca irá variar do início ao fim da comunicação.

Os quadros são montados e remontados a cada salto de rede diferente que o IP navega, mas o IP nunca é alterado.

Assista novamente ao vídeo guerreiros da net e veja o processo de encapsulamento, que é o montar e remontar dos quadros de camada-2 até que o pacote IP seja entregue. Note que o IP é desmontado somente quando chega ao seu destino.

Agora, vá até a Área do Aluno e assista o vídeo "Guerreiros da Internet".

## 6 Entendendo o Fluxo de Dados em Redes LAN e WAN

Antes de passarmos para o estudo dos endereços IP versão 4 vamos analisar como as aplicações se comunicam utilizando a pilha de protocolo IP em duas situações:

1. Computadores se comunicando dentro de uma rede LAN, estando na mesma rede IP e conectados ao mesmo switch ou HUB.
2. Computadores se comunicando em redes LAN distintas conectadas através da WAN.

Vamos responder uma pergunta que sempre vem na cabeça de todo estudante que está entrando na área de redes: **“Como a informação flui dentro da rede até chegar a seu destino?”**.

Essa é uma questão importante para o dia a dia de um profissional de redes, pois muitos dos problemas serão resolvidos fazendo a análise desse caminho e isolando os trechos para encontrar o ponto de falha.

A análise será simplificada utilizando como modelo uma rede tradicional. Outros protocolos além dos mostrados nos exemplos a seguir podem estar envolvidos na troca de informação e a utilização deles depende da topologia e tecnologia empregada na rede.

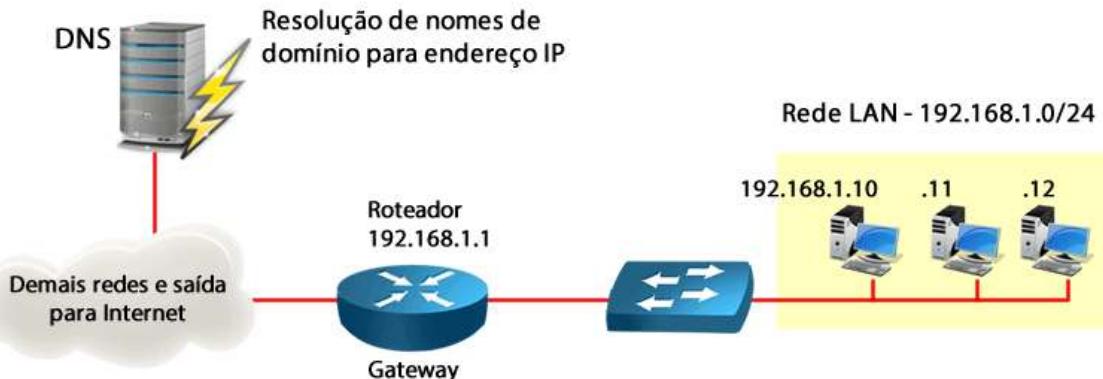
### 6.1 Conceitos Básicos de Roteamento IP

Antes de tratarmos de como cada protocolo atua quando dois computadores trocam informações precisamos entender alguns conceitos básicos sobre roteamento IP e as configurações das placas de rede dos computadores.

Se você lembra-se do que estudamos sobre o endereço IP a alguns tópicos atrás temos um total de mais de 4 bilhões de endereços, os quais são divididos em conjuntos menores chamados “redes” ou “sub-redes”. Cada computador ou conjunto de computadores está conectado a uma dessas redes e normalmente conhece apenas a sua própria rede por motivos óbvios: “Como um computador iria armazenar como chegar aos 4 bilhões de possíveis destinos?”. Imagine o quanto de memória e processamento seria gasto para isso.

Para resolver esse problema entram em cena os roteadores, os quais guardam não os endereços individuais de cada computador na Internet ou na Internet, mas sim as redes que eles pertencem. Essa informação está contida nas tabelas de roteamento dos roteadores e também nos próprios endereços IP de origem e destino dos computadores.

Portanto, na tabela de roteamento de um computador ele possui a rede dele mesmo, mais um endereço para o seu roteador de saída para a Internet, chamado gateway ou roteador padrão. Veja a topologia abaixo com o que estudamos até o momento.



Vamos considerar o computador com endereço 192.168.1.10, na placa de rede dele existe uma rota ou caminho indicando que a saída para a Internet ou demais redes que ele não conhece deve ser através do roteador 192.168.1.1. Isso normalmente é passado pelo servidor DHCP.

Quando ele deseja enviar pacotes para um computador que está na mesma rede ele faz diretamente para o destinatário, ou seja, a comunicação não precisa do gateway como intermediário.

Outro ponto importante é que não existe campo no protocolo IP para um endereço de web sites ou URLs, portanto quando digitamos em um navegador de Internet www.dltec.com.br isso não pode ser inserido no campo de destino do protocolo IP, pois ele não suporta esse tipo de informação como destino.

Na realidade, todo web site ou servidor registrado na Internet possui um endereço IP e quem traduz o nome para esse endereço é o serviço chamado DNS (Domain Name System - Sistema de Nomes de Domínios). A consulta DNS de um cliente para o servidor DNS é feita em UDP utilizando a porta 53.

Por esse motivo anteriormente foi citado que um computador para acessar a Internet precisa no mínimo das seguintes configurações de rede:

- Endereço IP e máscara de rede
- Endereço do Gateway
- Endereço do servidor DNS

Essas configurações podem ser feitas de maneira estática pelo administrador de redes (manualmente) ou passadas dinamicamente por um servidor DHCP. Você pode as configurações de rede no computador utilizando o prompt de comando ou terminal com o comando:

- Windows: ipconfig /all
- Linux: ip address show ou ifconfig
- MAC OS-X: ifconfig

Veja exemplo abaixo para um computador com Windows 7 conectado através da interface sem fio:

The screenshot shows a Windows Command Prompt window titled "Prompt de Comando". The title bar also includes the text "Adaptador de Rede sem Fio Conexão de Rede sem Fio:". The window displays the following network configuration details:

```
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::c8ce:4c54:efe3:2186%19(Preferencial)
Endereço IPv4. . . . . : 192.168.1.76(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : quinta-feira, 11 de julho de 2013 10:39:54
Concessão Expira. . . . . : sexta-feira, 12 de julho de 2013 10:39:53
Gateway Padrão. . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
Servidores DNS. . . . . : 192.168.10.1
NetBIOS em Tcpip. . . . . : Habilitado
```

Os computadores também possuem uma tabela de roteamento através do prompt de comando ou terminal com o comando:

- Windows: route print
- Linux e MAC OS-X: netstat -nr

Veja abaixo um exemplo da tabela de roteamento em um computador com Linux Ubuntu:

```

File Edit View Terminal Go Help
dltec@dltec-VirtualBox:~$ netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask        Flags   MSS Window irtt Iface
0.0.0.0         192.168.1.1   0.0.0.0       UG        0 0          0 eth0
169.254.0.0     0.0.0.0       255.255.0.0   U         0 0          0 eth0
192.168.1.0     0.0.0.0       255.255.255.0 U         0 0          0 eth0
dltec@dltec-VirtualBox:~$ 

```

Note que a primeira rota aponta para uma rede 0.0.0.0, esse é o endereço que representa a Internet e qualquer IP diferente da rede 169.254.0.0 ou 192.168.1.0 será direcionado para o IP 192.168.1.1, o qual é o gateway passado pelo serviço de DHCP.

A rede 168.254.0.0 é uma rede utilizada para autoconfiguração pelos sistemas operacionais quando não é encontrado um servidor DHCP disponível, já a rede 192.168.1.0 é a própria rede IP do computador, a qual foi aprendida via DHCP.

Sempre que um computador ou roteador precisa enviar ou encaminhar um pacote recebido ele busca pela rede na tabela de roteamento se ele conhece a rede do endereço contido no campo IP de destino do cabeçalho IP e faz o seguinte:

1. A rede de destino está presente na tabela de roteamento?
2. Se sim, encaminha para a interface de destino configurada, no exemplo anterior está definido no campo **Iface**, bem no final da tabela.
3. Se não está presente na tabela ele verifica se tem um gateway configurado (rota para a rede 0.0.0.0)
  - a. Tem gateway? Sim, então encaminha para ele.
  - b. Não tem gateway configurado? Não, então descarta o pacote.

Em capítulos posteriores vamos estudar com detalhes o roteamento, inclusive configurando rotas e protocolos de descoberta de rotas dinâmicos!

Agora vamos analisar o fluxo completo inserindo mais protocolos e aprender como realmente os pacotes são montados e encaminhados através da rede.

## 6.2 Entendendo o Fluxo de Informações dentro da mesma LAN

Dentro da LAN o próprio computador pode resolver o problema do envio dos pacotes por si só, utilizando apenas o protocolo **ARP**, o qual já estudamos e sabemos que tem a função importante de descobrir qual o **endereço MAC** do computador remoto que já sabemos o seu endereço IP.

Não há conversação se o computador que está originando o fluxo não souber o endereço MAC e o endereço IP do vizinho para montar o quadro de camada-2 e o pacote de camada-3 (IP).

Vamos supor que o micro A (endereço IP 192.168.1.76) quer fazer um teste de ping para o vizinho com IP 192.168.1.67 com o nome de micro B. O usuário vai entrar no prompt de comando e digitar "ping 192.168.1.67". Veja figura a seguir.



O computador A primeiro deve analisar se o IP do micro B está dentro da sua rede ou fora dela, utilizando o endereço do computador B e sua tabela de roteamento. Ao fazer essa análise o micro A verifica que eles estão na mesma faixa pertencente à rede 192.168.1.0, ou seja, o micro B está na mesma rede que está configurada na placa de rede do micro A, sendo assim ele tratará o fluxo como local.

Agora o micro precisa descobrir o **endereço MAC** de B utilizando o protocolo **ARP** mandando uma mensagem **ARP** para todos os computadores da rede local (destino é um broadcast). O computador B recebe e responde ao ARP com seu endereço MAC.

Agora sim o micro A pode montar o pacote com o comando ping, que será recebido pelo vizinho e respondido com sucesso.

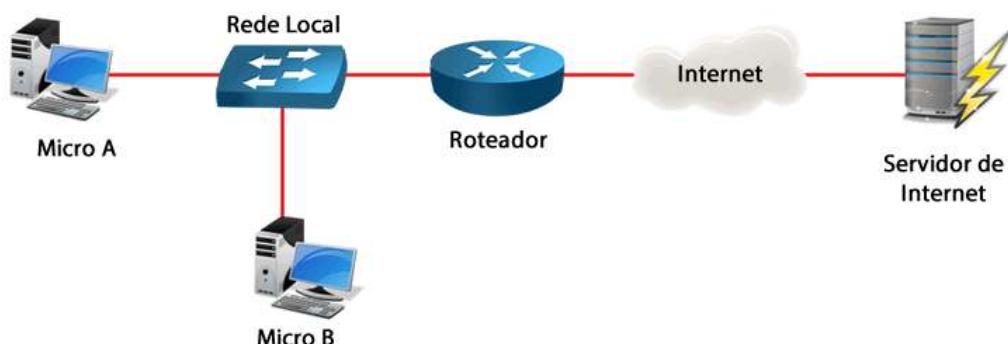
Resumindo uma conversação na rede local:

1. Originador precisa falar com Destino que está na mesma LAN.
2. Originador conhece o IP e precisa descobrir o MAC.
3. Envia um comando de ARP na rede solicitando o MAC do micro remoto.
4. Micro remoto responde o ARP com seu MAC.
5. Micro originador monta o pacote IP e o de camada-2 e envia a informação para o vizinho com uma mensagem do ICMP contendo um "Echo Request".
6. Vizinho recebe os dados, processa e responde com um "Echo Reply".
7. O processo se repete de envio e recebimento de dados até finalizar a conversação conforme padrão do ping.

### 6.3 Entendendo o Fluxo de Dados para Internet

Qual a diferença para o envio de dados de dentro para fora da LAN? Dentro da LAN o computador sabe como encaminhar, precisando apenas do ARP para descobrir o MAC remoto, porém fora da LAN o computador precisará da ajuda de um equipamento que conheça os outros destinos, sejam eles da Intranet ou da Internet, pois a visão do computador é apenas local.

O equipamento que faz esse papel de encaminhar os pacotes dos micros para redes que estão conectadas remotamente é o Roteador, o qual tem seu endereço IP configurado na placa de rede como "**roteador padrão**" ou "**gateway padrão**".



Além disso, quando estamos falando de Internet, normalmente não utilizamos o endereço IP remoto e sim a URL ou endereço de Web, como por exemplo <http://www.dltec.com.br/>. Porém, para enviar informações o protocolo IP precisa do endereço de camada-3 e para resolver esse problema existe o serviço de DNS, o qual tem a função de traduzir os nomes de página da Web ou nomes de domínio para seu real endereço IP do servidor onde o serviço está sendo disponibilizado.

Agora vamos simular que o micro A do exercício anterior que acessar uma página da Internet digitando em seu browser <http://www.dltec.com.br/>.

Nesse momento o computador vai analisar a informação e buscar qual o IP corresponde ao site desejado pelo usuário utilizando o serviço de DNS, o qual foi passado pelo DHCP ou inserido manualmente. Verificando esse endereço de DNS existem duas possibilidades: o DNS está na mesma rede ou em outra LAN.

Nesse caso vamos supor que ele está na mesma LAN que o computador A, então antes de enviar a consulta DNS para resolver o nome desejado o computador A vai fazer uma solicitação ARP para descobrir o MAC do servidor DNS.

Após descobrir o MAC do DNS o computador A faz a solicitação via UDP porta 53 ao servidor e recebe a resposta que o IP da página solicitada é o **200.98.197.60**.

Agora a análise é a mesma que o micro A realizou no exemplo anterior, portanto ele verifica que o endereço remoto com certeza não está na mesma LAN, pois o web site está na rede 200.98.197.0 e na Internet.

Como o computador agora não sabe encaminhar para essa rede por si só, por isso ele precisa de outro dispositivo que conheça o destino, o qual é o endereço do roteador que vem configurado na placa de rede como roteador padrão ou default gateway.

Agora, mais uma vez, o micro A verifica que precisa encaminhar para o roteador, faz um ARP para descobrir o MAC do roteador, com a resposta do ARP monta o pacote IP e o de camada-2, encaminhando a requisição da página da Internet.

Aqui vem um detalhe importante, o endereço IP de origem e destino são o do computador A e do site **200.98.197.60**. Na camada 2 o quadro ethernet terá como MAC de origem o da placa de rede do computador A, porém o MAC de destino não será do computador remoto e sim do roteador padrão, pois é o roteador padrão que servirá de intermediário nessa comunicação!

Esse mesmo fluxo de envio para roteadores padrões vai se seguir pela Internet até que o roteador onde o servidor Web está conectado seja encontrado. Nesse momento o pacote será encaminhado ao servidor, que irá processar a requisição da página e responderá ao computador, seguindo o caminho inverso do fluxo e utilizando ARP em redes com padrão Ethernet.

Dessa maneira a troca de informações prosseguirá até que toda a página seja carregada e a conexão finalizada.

Resumindo uma conversação fora da rede local:

1. Usuário digita URL em seu navegador de Internet.
2. Originador conhece a URL e precisa descobrir o endereço IP do servidor de Web para montar o pacote IP.
3. Computador envia uma requisição de tradução do nome para o servidor DNS configurado em sua placa de rede através do UDP porta 53.
4. DNS responde com o IP do Website.

5. Originador descobre que o endereço de rede do web site não pertence a sua sub-rede e precisa utilizar o gateway para envio das informações ao destino.
6. Originador precisa encaminhar o pacote para o roteador e envia uma solicitação ARP na rede procurando pelo o MAC do roteador.
7. Roteador responde o ARP com seu MAC.
8. Micro originador monta o pacote IP e o de camada-2 e envia a informação para o roteador.
9. O roteador envia o pacote para sua saída de Internet.
10. O pacote é roteado na Internet até encontrar a rede onde está conectado o servidor Web.
11. Servidor Web recebe os dados, processa e responde com o conteúdo do web site.
12. O processo se repete de envio e recebimento de dados até finalizar a conversação.

Lembre-se que entre os passos 2 e 3 ainda pode haver a necessidade do uso do ARP para resolver o MAC do servidor DNS se ele estiver na mesma rede. Se ele não estiver na mesma rede o ARP é feito pedindo pelo gateway e ele fará o intermédio no envio e recebimento da consulta DNS.

#### **6.4 Considerações sobre o fluxo de dados em uma rede IP e QoS**

Levando em conta os exemplos anteriores, notamos que diversos tipos diferentes de fluxos podem ser gerados pelos equipamentos de rede, por exemplo:

- Acesso à Internet – páginas de Web
- Acesso a arquivos – como FTP ou pastas compartilhadas na rede
- Envio e recebimento de e-mails
- Downloads de arquivos e músicas utilizando softwares P2P (peer-to-peer)
- Tráfego de voz sobre IP
- Tráfego de vídeo sobre IP
- Tráfego referente a realização de backups de dados agendados através da rede, etc.

Cada aplicação de rede tem sua característica específica, por exemplo, para Voz os pacotes são pequenos e com um fluxo que deve ser constante, pois se houver atraso ou perda de pacotes a comunicação pode ser prejudicada.

As redes IP são conhecidas como redes **Best Effort**, ou seja, serviço de entrega pelo melhor esforço. Quando o roteador opera por este tipo de serviço faz sempre o melhor possível para encaminhar os pacotes de acordo com os recursos que ele tem disponível naquele instante de tempo, mas sem quaisquer garantias de entrega.

Por padrão redes com serviço Best Effort oferecem o mesmo tratamento a todos os pacotes entrantes e saíntes, sem nenhuma distinção entre eles. Este serviço é implementado normalmente pelo mecanismo de gerência de filas **FIFO** (First In, First Out), ou seja, o primeiro pacote que entra é o primeiro pacote que sai do roteador, essa é a principal razão que serviço Best Effort não atende aos requisitos de qualidade de serviço da maior parte das aplicações. Portanto para o dimensionamento de uma rede IP deve ser levado em conta não somente a **banda**, mas também o tipo de tráfego que você irá passar, ou seja, a aplicação.

Um exemplo simples de problema é você imaginar um fluxo de voz sobre IP passando junto com o backup da rede em um mesmo roteador.

O pacote de voz é pequeno e precisa de tempo real (com o mínimo de atraso e variações desse atraso), já o backup são pacotes grandes, portanto quando um pacote do backup ocupar uma interface do roteador ele vai praticamente parar a interface, e os pacotes voz, que são menores, terão que esperar até que o pacote de backup inteiro seja enviado!

Vamos supor que o pacote do backup tenha 1M bytes e o de voz 200 bytes, portanto para cada pacote de backup enviado aproximadamente **5000 pacotes de voz serão enfileirados**. Com certeza a comunicação entre os usuários de telefonia IP será prejudicada com atraso e interrupções na conversação devido a essa espera.

Se extrapolarmos a análise do exemplo acima e imaginarmos que 10 pacotes de 1 Mbyte do backup entraram na fila antes dos pacotes de voz, o que você diria dessa rede de telefonia IP? Com certeza seria um usuário insatisfeito!

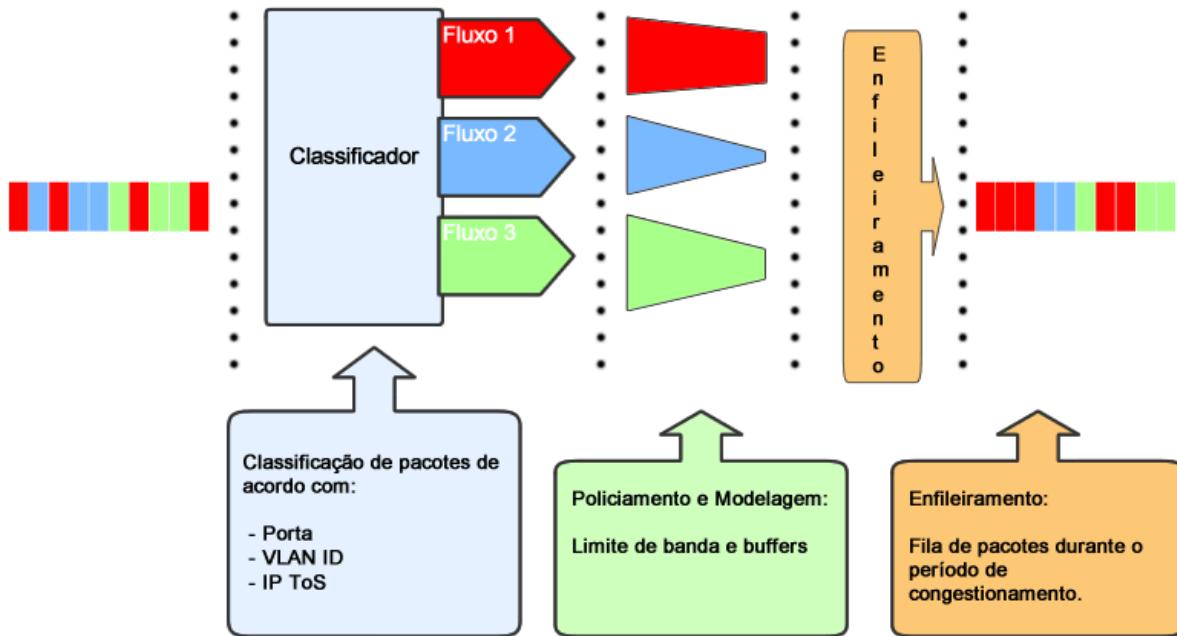
Mesmo que você aumente a banda, muitas aplicações simplesmente tendem a tentar usar a banda inteira, por isso definir parâmetros diferentes que atendam as diferentes necessidades de tráfego é tão importante nas redes atualmente, pois cada vez mais serviços são incorporados pelas redes e novos dispositivos também necessitam de acesso.

O mecanismo que evita esse tipo de problema é chamado de **QoS ou Qualidade de Serviço**. O QoS é na realidade um conjunto de recursos utilizados desde os endpoints para fazer com que os tráfegos mais importantes tenha o tratamento correto nos pontos que podem representar "gargalos de rede", por exemplo, ao enviar em links WAN de baixa velocidade.

Sua função é classificar e marcar os diversos tipos de pacote, depois colocá-los em filas corretas e priorizar essas comunicações, fazendo com que os pacotes mais prioritários saiam primeiro e otimizando o uso das interfaces.

No mundo IP um link com alta velocidade não significa que a rede terá alto desempenho devido às características das aplicações que já estudamos anteriormente.

Veja abaixo uma figura que ilustra de maneira geral a configuração do QoS em dispositivos de rede.



O QoS não faz parte do CCENT, porém é importante que saibamos sua função e necessidade de implantação, além disso, também temos a noção que banda não é tudo, muitas vezes o problema de uma rede é a falta da configuração de QoS!

Agora vamos continuar o estudo analisando mais o protocolo IP e seu esquema de endereçamento.

## 6.5 Hora de Praticar

Agora chegou a hora de um pouco mais de ação...

Entre na área do aluno, no capítulo 5 e faça os laboratórios 5.2 e 5.3.

No laboratório 5.3 você poderá verificar os pacotes trocados entre o cliente e o servidor via HTTP e poderá analisar os PDUs do HTTP e TCP utilizando recursos avançados do Packet Tracer.

Após realizar esses laboratórios leia também o documento em PDF com o nome "**Material Extra - Protocolo ICMP - Mensagens e Recursos Extras**", onde você no final do documento encontrará um teste para verificar manualmente o MTU de um caminho.

Não deixe de realizar esses laboratórios!

## 7 Introdução ao Endereçamento IP

Começaremos a estudar agora um importante tópico do currículo do CCENT - **O endereçamento IP**.

É muito importante que você aprenda os conceitos que serão apresentados, pois eles o acompanharão em toda a sua vida no mundo das redes de computadores e administração de redes!

Sendo assim, leia, estude, pesquise, releia o material, faça os exercícios e insista até que tenha assimilado **toda a matéria**, pois várias questões nos exames 100-105 e 200-201 dependem desses conceitos.

Como os endereços IP, apesar de escritos em números decimais, são na realidade números binários nada melhor que começar revisando o sistema de numeração binário. Caso a explicação mostrada a seguir não seja suficiente temos ainda uma apostila de sistemas de numeração para ajudá-lo a aprender melhor o assunto.

### 7.1 Sistemas de Numeração

Vamos iniciar com o tópico "Matemática para Redes de Computadores", onde iremos rapidamente abordar os seguintes assuntos:

- Sistema de Numeração Decimal.
- Sistema de Numeração Binário.

#### 7.1.1 Sistema Decimal

Os sistemas numéricos consistem em símbolos e regras para a utilização destes símbolos. O sistema numérico mais frequentemente utilizado é o sistema numérico Base 10 ou decimal. Um sistema dito de base 10 significa que são utilizados dez símbolos para sua representação (0, 1, 2, 3, 4, 5, 6, 7, 8 e 9). Estes símbolos podem ser combinados para representar todos os valores numéricos possíveis.

O sistema numérico decimal é baseado em potências de 10. Cada posição colunar de um valor, da direita para a esquerda, é multiplicada pelo número 10, que é o número base, elevado a uma potência, que é o expoente.

A potência à qual é elevado o valor 10 depende da sua posição à esquerda do ponto decimal. Quando um número decimal é lido da direita para a esquerda, a primeira posição, ou a mais à direita representa 10 elevado por 0 (1), a segunda posição representa 10 elevado por 1 ( $10 \times 1 = 10$ ). A terceira posição representa 10 elevado por 2 ( $10 \times 10 = 100$ ). A sétima posição à esquerda representa 10 elevado por 6 ( $10 \times 10 \times 10 \times 10 \times 10 \times 10 = 1,000,000$ ). Esta é a verdade independentemente de quantas colunas sejam ocupadas pelo número.

### Sistema de Numeração Base 10

Símbolos: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

$$\begin{array}{r}
 1 \quad 3 \quad 4 \quad 5 \\
 10^3 \quad 10^2 \quad 10^1 \quad 10^0 \\
 1 \times 10^3 = 1000 \\
 3 \times 10^2 = +300 \\
 4 \times 10^1 = +\ 40 \\
 5 \times 10^0 = +\ 5 \\
 \hline
 1345
 \end{array}$$

### 7.1.2 Sistema Binário

Os computadores reconhecem e processam dados, utilizando-se o sistema binário ou Base 2. O sistema binário utiliza dois símbolos, 0 e 1, em vez dos dez símbolos utilizados no sistema numérico decimal.

A posição, ou casa, de cada algarismo da direita para a esquerda em um número binário representa 2, o número base, elevado a uma potência ou expoente, começando com 0.

Exemplo: 1011 base 2 =  $(1 \times 2 \text{ elevado por } 3 = 8) + (0 \times 2 \text{ elevado por } 2 = 0) + (1 \times 2 \text{ elevado por } 1 = 2) + (1 \times 2 \text{ elevado por } 0 = 1) = 11$  ( $8 + 0 + 2 + 1$ ).

### Sistema de Numeração Base 2

Símbolos: 0, 1

$$\begin{array}{r}
 1 \quad 0 \quad 1 \quad 1 \\
 2^3 \quad 2^2 \quad 2^1 \quad 2^0 \\
 1 \times 2^3 = 8 \\
 0 \times 2^2 = 0+ \\
 1 \times 2^1 = 2+ \\
 1 \times 2^0 = 1+ \\
 \hline
 11
 \end{array}$$

**Observação:** Os computadores foram concebidos para utilizarem grupos de oito bits. Este grupo de oito bits é denominado byte. Em um computador, um byte representa um único local de armazenamento endereçável. Estes locais de armazenamento representam um valor ou um único caractere de dados, por exemplo, um código ASCII.

O número total de combinações de oito chaves ou bits ligadas ou desligadas é de 256. Já a faixa de valores de um byte é de 0 a 255. Veja abaixo como é o crescimento em binário da sequência entre 0 e 255:

- 00000000 -> 0
- 00000001 -> 1
- 00000010 -> 2
- 00000011 -> 3
- 00000100 -> 4
- 00000101 -> 5
- 00000110 -> 6

- 00000111 -> 7
- 00001000 -> 8
- 00001001 -> 9
- 00001010 -> 10
- 00001011 -> 11
- 00001100 -> 12
- 00001101 -> 13
- 00001110 -> 14
- 00001111 -> 15
- 00010000 -> 16
- ...
- 11111100 -> 252
- 11111101 -> 253
- 11111110 -> 254
- 11111111 -> 255

Os valores em binário dentro de um byte crescem da esquerda para direita somando-se um a cada passo. Por esse motivo cada campo do endereço IP pode ir apenas de 0 a 255, não existe IP 1.1.1.256, por exemplo, pois o valor do quarto byte não é possível com apenas 8 bits!

Outra dica interessante é que os números pares tem o último bit sempre em zero e os ímpares em 1, note na sequência mostrada anteriormente esse fato.

É importante entender o conceito do byte ao trabalhar com computadores e redes.

## 7.2 Conversão Binária

Vamos ver agora um pouco de como realizar conversão de sistemas numéricos começando pela conversão decimal-binário e na sequência veremos a conversão binário-decimal.

### Conversão Decimal-Binário

Existem várias maneiras de realizar a conversão de decimal para binário, vamos mostrar nesse tópico um método simples de comparar o número decimal que queremos converter em binário com os valores de cada bit. A dica é verificar se o número decimal é maior ou menor que cada bit e ir subtraindo antes de passar ao próximo caso ele seja maior. Veja abaixo os valores em decimal de cada bit em um octeto (byte):

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

Sempre comece comparando o decimal a ser convertido com o valor do bit mais significativo (**128**). Veja o exemplo prático a seguir para converter o número decimal 168 em número binário de oito bits utilizando esse método:

- 128 cabe dentro de 168? Sim. Portanto, o bit mais à esquerda do número binário é um.
- Agora fazemos a diferença  $168 - 128 = 40$ .
- 64 cabe dentro de 40? Não cabe. Portanto, o segundo bit da esquerda é zero.
- 32 cabe dentro de 40? Sim. Portanto, o terceiro bit da esquerda é um.
- Agora subtraímos  $40 - 32 = 8$ .
- 16 cabe dentro de 8? Não cabe. Portanto, o segundo bit da esquerda é zero.
- 8 cabe dentro de 8? Sim. Portanto, o quinto bit da esquerda é um.
- Agora subtraímos  $8 - 8 = 0$ . Como o resto foi zero todos os bits à direita serão zero, mesmo assim vamos continuar a análise até o final.
- 4 cabe dentro de 0? Não cabe. Portanto o sexto bit é zero.
- 2 cabe dentro de 0? Não cabe. Portanto o sétimo bit é zero.
- 1 cabe dentro de 0? Não cabe. Portanto o oitavo bit mais à esquerda também é zero.

- Resultado:  $10101000 = 168$  decimal

**Conversão Binário-Decimal:**

Os números binários podem ser convertidos em números decimais, multiplicando os dígitos binários pelo número base do sistema, o qual é Base 2, e elevando-os ao expoente da sua posição.

Exemplo: Para converter o número binário 01110000 em um número decimal fazemos o seguinte:

$0 \times 2^0 = 0$   
 $0 \times 2^1 = 0$   
 $0 \times 2^2 = 0$   
 $0 \times 2^3 = 0$   
 $1 \times 2^4 = 16$   
 $1 \times 2^5 = 32$   
 $1 \times 2^6 = 64$   
 $0 \times 2^7 = 0$

Agora é só somar o valor dos bits e temos o resultado:  $0+0+0+0+16+32+64+0 = 112$

Lembre-se que as provas da Cisco não permitem uso de calculadora, por isso é importante que você entenda bem as conversões em binário e também interpretar números Hexadecimais.

Importante: Caso você ainda tenha dúvidas sobre o sistema de numeração decimal, binário e hexadecimal baixe na "Área do Aluno" o arquivo "**Apostila de Sistemas de Numeração - Decimal Binario e Hexa**".

**7.3 Hosts, Redes e Máscaras**

Como já estudamos, um endereço IP é representado por um número binário de 32 bits, divididos em quatro conjuntos de oito bits, chamados de octetos ou bytes.

Todo endereço IP é dividido em duas partes, sendo que a inicial identifica a rede e a final é o endereço do host de rede, chamado também de Host-ID (Host Identification ou identificação do host).

A melhor analogia para entender o endereçamento IP é o endereçamento postal, onde para encontrar um destino você necessita do nome da rua e do número da casa, ou seja, o endereço de rede seria o nome da rua e o endereço de host o número da casa. Portanto a principal função do endereçamento IP é **identificar um dispositivo** (micro, roteador, servidor, etc.) **dentro de uma rede**, a qual é um conjunto de computadores.

Quem delimita a porção de rede e de host em um endereço IP é a **máscara de rede** também chamada de **máscara de sub-rede**. Na realidade **não existe endereço IP sem uma máscara de rede**.

A máscara de rede também é representada por 32 bits, sendo que os bits "0" representam a porção de host e os bits "1" a de rede. A máscara sempre inicia com uma sequência de bits 1 e depois têm uma sequência de zeros, nunca veremos bits um e zero intercalados, isso porque o que é rede é rede, não existe uma rede-host para o endereçamento IP.

Por exemplo, uma máscara 1111111.00000000.00000000.00000000 = 255.0.0.0 é válida, já a máscara 11111110.00000000.00000000.11111111 = 254.0.0.255 não é válida.

Usando a mesma máscara acima, se tivermos o endereço IP 1.2.3.4 com a máscara 255.0.0.0 podemos tirar que a porção de rede desse endereço é "**1**" e o host-ID "**.2.3.4**".

A rede que um endereço IP pertence pode ser definida com uma conta binária chamada AND lógico entre o endereço e sua máscara. No AND lógico qualquer número AND zero é zero e um AND um é igual a um, portanto se fizermos o cálculo teremos:

- 1.2.3.4 AND 255.0.0.0
- 00000001.00000010.00000011.00000100 AND  
11111111.00000000.00000000.00000000
- 00000001.00000000.00000000.00000000 = 1.0.0.0

Portanto a rede que o IP 1.2.3.4 pertence é 1.0.0.0 com a máscara 255.0.0.0.

Podemos também representar o IP e máscara através da notação de prefixo de rede com a máscara não em decimal, mas representada por uma barra (/) mais o número de bits um nela contidos. Por exemplo, a rede calculada acima pode ser escrita 1.0.0.0/8, porque na máscara 255.0.0.0 temos oito bits um.

**Observação:** Lembre-se que um endereço IP identifica não uma máquina, mas **uma conexão à rede**. Máquinas com mais de uma interface de rede (roteadores, por exemplo) possuem um endereço IP para cada interface. Até mesmo um computador pode possuir vários endereços IP.

#### 7.4 Endereçamento IP e a Internet

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 chamadas: **classes A, B e C**.

Essas classes foram baseadas na premissa que teríamos na Internet poucas redes de grande porte (126 redes com mais de 16 milhões de hosts cada uma), as quais estão na classe A, uma quantidade maior de redes de médio porte (aproximadamente 16 mil redes com mais de 65 mil hosts cada uma) que ficariam dentro da classe B e uma quantidade muito maior de redes de pequeno porte que ficariam dentro da classe C (aproximadamente 2 milhões de redes com apenas 254 hosts cada uma).

Para termos uma ideia de como a alocação de IPs foi realizada nos primórdios da Internet 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!**

Outras duas classes foram definidas além das citadas anteriormente, a classe D dedicada a serviços de Multicast e a classe E reservada para estudos e pesquisas.

O roteamento com base em classes é chamado de **Classful**.

Com o crescimento da Internet esse tipo de classificação e distribuição de IPs 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 muito tempo temos que saber sobre as duas versões.

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.
- Em 2012 a ISC (Internet System Consortium) estimou que existissem até o mês de julho de 2012 aproximadamente **908.585.739** hosts na Internet.

Em novembro de 1991 é formado o grupo de trabalho ROAD (Routing and Addressing) para atuar sobre o problema da escassez de endereços IP versão 4, o qual 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 na Internet.

Outras duas técnicas 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), as quais estudaremos em capítulos posteriores.

Mas como esses computadores irão acessar a Internet se esses endereços não são roteáveis na rede pública? Através de uma tradução do endereço privado para um endereço público de Internet, o qual é realizado pelo NAT (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.

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. O NAT será estudado mais profundamente em capítulos posteriores.

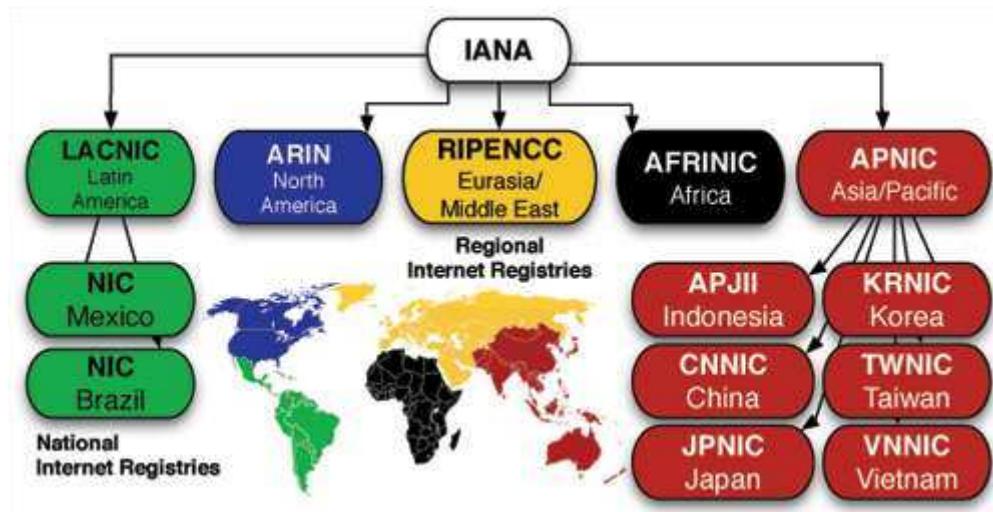
Se você utiliza um serviço ADSL ou Cable Modem em sua casa e tem acesso às configurações dos equipamentos de acesso à Internet pode verificar na que Interface WAN, a que está conectada à Internet, normalmente terá um IP válido de Internet. Já no seu computador ou computadores, você terá um endereço de alguma das faixas da RFC 1918, normalmente uma rede pertencente à faixa do 192.168.1.0 /24.

Utilize o comando **ipconfig** para verificar o IP do seu computador e o depois clique em um dos links 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).

Mundialmente quem administra os IPs é a entidade chamada **IANA** (Internet Assigned Numbers Authority), a qual repassa as responsabilidades de alocação em cada região do mundo para outras cinco entidades, sendo que para a América Latina a **LACNIC** é a responsável.

No Brasil a LACNIC delegou a administração dos endereços IP para o **Registro BR** (<http://registro.br>), nesse link você pode registrar domínios, solicitar endereços IPs e também verificar a disponibilidade de domínios. Veja na figura abaixo um organograma das entidades que administram a alocação de IPs ao redor do mundo.



## 7.5 Classes de Endereços IP

Ao todo foram definidas cinco classes de endereços IP, ou seja, classes A, B, C, D e E. Veja a figura abaixo com as classes e como identificá-las.

	octeto 1	octeto 2	octeto 3	octeto 4
classe A	0 rede		host	
classe B	10 rede		host	
classe C	110 rede		host	
classe D	1110 endereço de multicast			
classe E	11110 reservado para uso futuro			

Valores de cada bit

128	64	32	16	8	4	2	1
-----	----	----	----	---	---	---	---

O que caracteriza cada classe é o primeiro octeto do endereço IP, sendo que para a Classe A ele sempre inicia em zero, para a Classe B inicia em 10, para a Classe C em 110, na Classe D em 1110 e finalmente para a Classe E em 1111.

Aqui temos o primeiro uso da conversão de decimal para binário, se você enfrentar uma pergunta querendo saber a classe de um endereço IP é só converter o primeiro octeto em binário e seguir a regra estudada anteriormente!

Na figura também podemos tirar uma importante informação sobre quantas redes e endereços de host que as classes A, B e C podem fornecer. Note que para a classe A temos o primeiro octeto para rede e os demais para host, na B temos dois octetos para rede e dois para host e

na classe C são três para rede e um para host, o que nos fornece a máscara de rede padrão de cada uma das classes:

- **Classe A** -> Rede.Host.Host.Host = 255.0.0.0
- **Classe B** -> Rede.Rede.Host.Host = 255.255.0.0
- **Classe C** -> Rede.Rede.Rede.Host = 255.255.255.0

As classes D e E não utilizam o conceito de rede e host, elas utilizam somente endereçamento de host, por isso não possuem máscara de rede.

Portanto, a faixa de endereços de Internet não vai de 0.0.0.0 a 255.255.255.255, ela está limitada aos endereços das classes A, B e C.

Além disso, temos diversas faixas de endereços reservados. A mais conhecida é a RFC 1918 que define endereços para uso privativo, ou seja, para criação de Intranets, evitando o uso de endereços válidos para Internet em ambientes corporativos. Abaixo seguem as faixas de endereços privados:

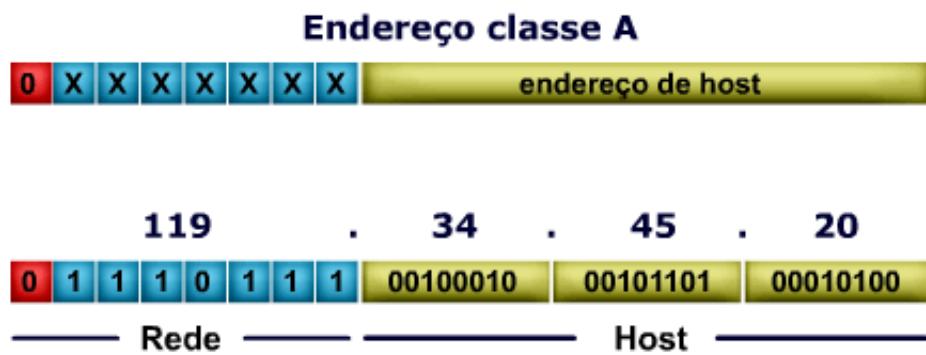
- Classe A: de 10.0.0.0 até 10.255.255.255
- Classe B: de 172.16.0.0 até 172.31.255.255
- Classe C: de 192.168.0.0 até 192.168.255.255

Os endereços começados em zero também não são utilizados para endereçar computadores, pois a rede 0.0.0.0 com a máscara 0.0.0.0 representa a Internet. Outra faixa reservada é a 127.0.0.0 a 127.255.255.255, a qual representa a faixa de loopback utilizada pelos computadores para endereçar a própria interface de rede. Se você pingar o endereço 127.0.0.1 no Windows, Linux ou MAC OS-X deve receber 100% de retorno, pois você está pingando sua própria placa de rede, portanto se ela não responder você está com sérios problemas.

Outra faixa de endereço reservada e não utilizada na Internet é a iniciada em 169.254.0.0 com a máscara 255.255.0.0, esses endereços são reservados para o Zeroconf, uma autoconfiguração da placa de rede quando o computador não encontra um servidor DHCP na rede. Se você entrar com um ipconfig no Windows ou ifconfig no Linux e verificar um endereço na faixa de 169.254.0.1 a 169.254.255.254 é sinal que sua placa de rede encontrou um servidor DHCP para fornecer os dados necessários para seu correto funcionamento.

### 7.5.1 Endereço IP Classe A

Os endereços da classe A sempre terão o primeiro bit do primeiro octeto igual a 0 (0xxxxxxxx), veja figura abaixo ilustrando o endereço.



Ao lado segue a variação completa do primeiro octeto que representa as redes da classe A.

Note que o primeiro bit nunca será diferente de "0". Uma dica interessante para descobrir em que classe o endereço IP está situado é converter o primeiro octeto em binário e verificar os primeiros bits.

0	0	0	0	0	0	0	→ 0
0	0	0	0	0	0	1	→ 1
0	0	0	0	0	1	0	→ 2

:

0	1	1	1	1	1	1	0	→ 126
0	1	1	1	1	1	1	1	→ 127

Os endereços de classe A pertencem das redes **1.0.0.0** até a **126.0.0.0**. As redes 0.0.0.0 (Internet) e 127.0.0.0 (127.0.0.0) são de uso especial e não podem ser utilizadas para endereçar redes, conforme já estudamos anteriormente.

A máscara de rede padrão de uma classe A é **255.0.0.0**. Outra forma de representar uma máscara de rede é utilizando a notação decimal, onde a máscara será representada pela quantidade de bits "1" nela contidos, para a classe A o prefixo é "/8". Para determinar a quantidade de hosts que uma classe possui, ou seja, o número de computadores que ela pode endereçar utiliza-se a fórmula abaixo:

$$* \text{ Número de hosts} = 2^n - 2$$

(onde n representa o número de bits 0 da máscara de rede)

#### Máscara da classe A

255	.	0	.	0	.	0
11111111	.	00000000	.	00000000	.	00000000

24 bits "0"

$$\text{Número de hosts} = 2^{24} - 2 = 16.777.216 - 2$$

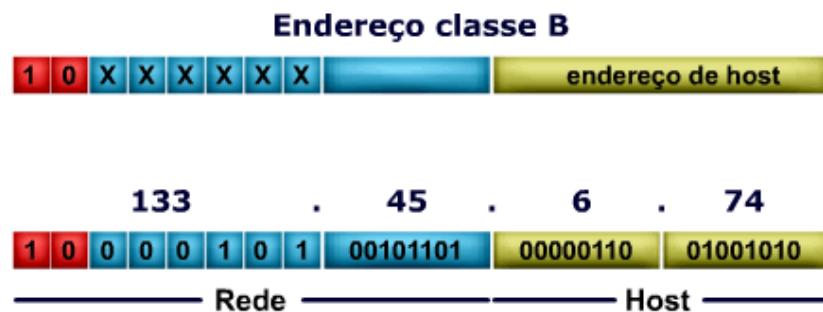
$$\text{Número de hosts} = 16.777.214$$

Note que na fórmula diminuímos dois endereços IPs do total, isso porque o primeiro representa a própria rede e o último representa o endereço de broadcast, e ambos não podem ser utilizados para endereçar computadores.

As **126** redes da classe A possuem endereços suficientes para endereçar até **16.777.214** hosts (computadores) cada uma.

### 7.5.2 Endereço IP Classe B

Os endereços da classe B sempre terão os dois primeiros bits do primeiro octeto igual a 10 (10xxxxxx), veja ilustração abaixo.



Abaixo segue a variação completa dos dois primeiros octetos que representam as redes da classe B.

1 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 → 128.0	1 0 1 0 1 0 1 0 . 0 0 0 0 0 0 0 0 → 170.0
1 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 1 → 128.1	1 0 1 0 1 0 1 0 . 0 0 0 0 0 0 0 1 → 170.1
1 0 0 0 0 0 0 0 . 0 0 0 0 0 0 1 0 → 128.2	1 0 1 0 1 0 1 0 . 0 0 0 0 0 0 1 0 → 170.2
:	:
1 0 0 0 0 0 0 0 . 1 1 1 1 1 1 1 0 → 128.254	1 0 1 1 1 1 1 0 . 1 1 1 1 1 0 1 1 → 190.251
1 0 0 0 0 0 0 . 1 1 1 1 1 1 1 → 128.255	1 0 1 1 1 1 1 0 . 1 1 1 1 1 1 0 0 → 190.252
1 0 0 0 0 0 1 . 0 0 0 0 0 0 0 0 → 129.0	1 0 1 1 1 1 1 0 . 1 1 1 1 1 1 0 1 → 190.253
1 0 0 0 0 0 1 . 0 0 0 0 0 0 0 1 → 129.1	1 0 1 1 1 1 1 0 . 1 1 1 1 1 1 1 0 → 190.254
1 0 0 0 0 0 1 . 0 0 0 0 0 0 1 0 → 129.2	1 0 1 1 1 1 1 0 . 1 1 1 1 1 1 1 1 → 190.255
:	:
1 0 0 0 0 0 1 . 1 1 1 1 1 1 1 0 → 129.254	1 0 1 1 1 1 1 1 . 1 1 1 1 1 1 0 1 → 191.253
1 0 0 0 0 0 1 . 1 1 1 1 1 1 1 1 → 129.255	1 0 1 1 1 1 1 1 . 1 1 1 1 1 1 1 0 → 191.254
1 0 0 0 0 1 0 . 0 0 0 0 0 0 0 0 → 130.0	1 0 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 → 191.255

Conforme mostrado acima, as redes classe B variam de 128.0.0.0 até 191.255.0.0, sendo que a máscara de rede padrão de uma classe B é 255.255.0.0 ou /16.

O número de redes classe B é o número de bits 1 que podem variar na máscara elevado a dois, ou seja, como temos 16 bits de rede e dois deles são fixos (**10xxxxxx.xxxxxxxx**) temos  $2^{14}$  endereços de classe B o que dão **16.384 redes**.

Para determinar a quantidade de hosts que uma classe possui, ou seja, o número de computadores que ela pode endereçar utiliza-se a fórmula abaixo (mesma conta utilizada para a classe A):

\* Número de hosts =  $2^n - 2$   
(onde n representa o número de bits 0 da máscara de rede)

Máscara da classe B

255 . 255 . 0 . 0
<b>11111111 . 11111111 . <u>00000000 . 00000000</u></b>
16 bits "0"

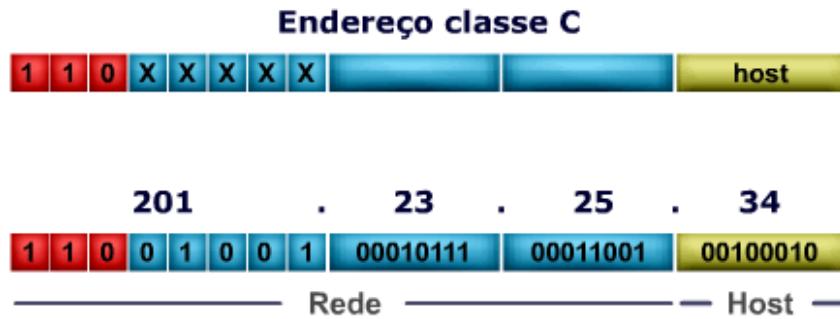
$$\text{Número de hosts} = 2^{16} - 2 = 65.536 - 2$$

$$\text{Número de hosts} = 65.534$$

Portanto a classe B possui endereços suficientes para endereçar **16.384 redes** diferentes com até **65.534 hosts** (estações) cada uma.

### 7.5.3 Endereço IP Classe C

Os endereços da classe C sempre terão os três primeiros bits do primeiro octeto igual a 110 (110xxxxx), conforme figura abaixo.



As redes classe C variam de 192.0.0.0 (**11000000.00000000.00000000.00000000**) até a 223.255.255.0 (**11011111.11111111.11111111.00000000**), sendo que a máscara de rede padrão de uma classe C é 255.255.255.0 ou /24.

O número de redes classe C segue o mesmo princípio que utilizamos para a classe B, ou seja, temos 24 bits de host com os três primeiros do primeiro octeto fixos em "110", portanto podemos ter  $2^{21}$  (24-3) redes classe C, ou seja, um total de **2.097.152 redes**.

Para determinar a quantidade de hosts que uma classe possui, ou seja, o número de computadores que ela pode endereçar utiliza-se a mesma fórmula das classes A e B (**o cálculo de host nunca varia!**):

\* Número de hosts =  $2^n - 2$   
(onde n representa o número de bits 0 da máscara de rede)

Máscara da classe C

255 .	255 .	255 .	0
<b>11111111</b>	<b>11111111</b>	<b>11111111</b>	<b>. 00000000</b>
_____			
08 bits "0"			

Número de hosts =  $2^8 - 2 = 256 - 2$

Número de hosts = 254

Portanto a classe C possui endereços suficientes para endereçar **2.097.152** redes diferentes com até **254** hosts cada uma.

#### 7.5.4 Endereço IP Classe D e Classe E

Os endereços da classe D são utilizados para **multicasting** e variam dos Ips 224.0.0.0 até 239.255.255.255. Os demais IPs pertencem à classe E, a qual é reservada para testes e estudos.

classe D	1 110	endereço de multicast
classe E	1 1110	reservado para uso futuro

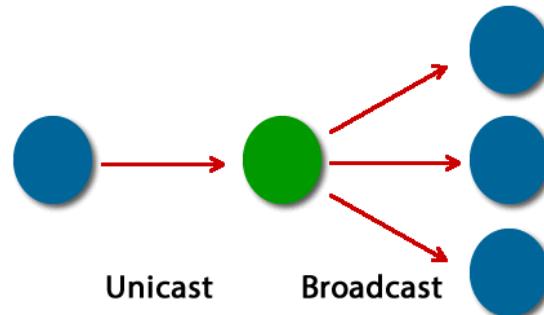
#### 7.6 Tipos de Comunicação Suportada pelo Protocolo IP

Conforme vimos anteriormente os endereços IP foram divididos em classes, sendo que nas **Classes A, B e C** temos os endereços utilizados pelos computadores para que eles possam se comunicar em rede, chamados de **Unicast**.

Além disso, nessas três classes de IP temos também os endereços de **Broadcast**, utilizados para comunicação com **todos os hosts** de uma rede.

Portanto, a comunicação **Unicast** é realizada de **um para um**, ou seja, **host a host**, já a comunicação em **broadcast** é de **um para todos**, ou seja, quando um pacote é endereçado no destino para um endereço de broadcast **todos os hosts** daquela rede **irão receber e processar** aquele pacote IP.

Veja a figura ao lado.



Em uma rede IP o primeiro endereço representa a própria rede para o roteamento e **não pode ser utilizado para endereçar hosts**. Este endereço recebe o nome de “**endereço de rede**” ou “**endereço de subrede**” e é utilizado para criar “**rotas**” para as redes IP.

Os endereços de Unicast vão do segundo ao penúltimo IP de cada rede ou sub-rede, por exemplo, na rede classe C 192.168.1.0 os endereços de Unicast vão de 192.168.1.1 até 192.168.1.254, pois o endereço 192.168.1.0 é o endereço de rede e o último IP 192.168.1.255 é o endereço de broadcast dessa rede.

Os endereços de Unicast são chamados de **endereços de Host (hosts válidos ou IPs válidos)** e podem ser **utilizados para endereçar os hosts ou interfaces de rede**, já os **endereços de rede e broadcast NÃO podem ser utilizados para endereçar os hosts ou interfaces dos roteadores**.

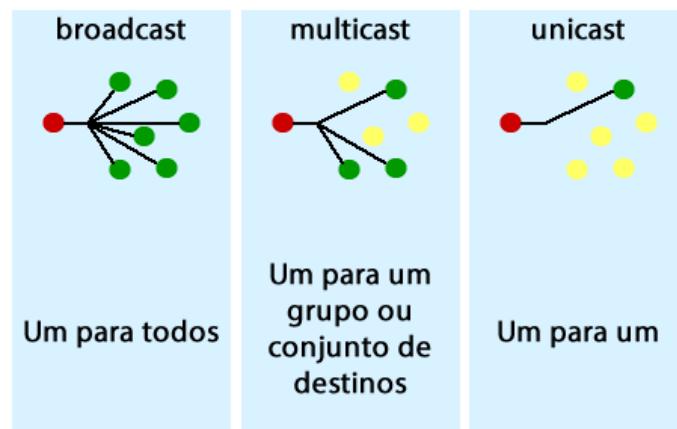
O endereço de broadcast que representa **todos os IPs** (de qualquer classe) é o endereço IP **255.255.255.255**, porém cada rede ou sub-rede IP tem também um endereço de broadcast que representa todos os IPs daquela rede ou sub-rede específica, o qual é o **último IP de cada rede ou subrede**. Por exemplo, na rede classe C 192.168.1.0 o IP 192.168.1.255 é o broadcast direcionado dessa rede, o que significa se você fizer um “ping 192.168.1.255” todos os IPs dessa rede irão responder, ou seja, os computadores configurados com IPs de 192.168.1.1 até 192.168.1.254.

Normalmente esse teste proposto acima não deve funcionar, pois ele permite um tipo de ataque chamado de Smurf e por isso normalmente o ping para endereços de broadcast não são respondidos por muitos sistemas operacionais.

Os **broadcasts direcionados** a uma sub-rede específica, ou seja, para o **último IP** de uma rede ou sub-rede, por padrão não são encaminhados entre interfaces de um roteador, porém esse comportamento pode ser alterado com o comando “**ip directed-broadcast**” que pode ser inserido nas interfaces dos roteadores e permitir o envio do broadcast direcionado por aquela interface. Esse comando vem por padrão desabilitado.

Já uma mensagem de broadcast para o endereço **255.255.255.255** nunca será encaminhado pelas interfaces, mesmo com o comando citado acima.

Já os endereços de **Classe D** são utilizados para a comunicação Multicast, a qual é uma comunicação de **um para um grupo**, ou seja, utilizada para **comunicação em um grupo** de elementos que possuem o **mesmo endereço de Multicast**. Veja a figura abaixo com a diferença entre os três tipos de comunicação.



Por exemplo, quando um roteador é configurado com o EIGRP como protocolo de roteamento, as informações de roteamento trocadas entre os roteadores são feitas utilizando o **multicasting**.

Os roteadores que estão rodando o EIGRP recebem o endereço IP classe D 224.0.0.10 e se um roteador em uma rede LAN enviar uma mensagem de roteamento e houver mais roteadores OSPF todos receberão essa mensagem, porém diferente do broadcast somente os roteadores com o IP 224.0.0.10 irão processar essa informação.

Note que todos os roteadores EIGRP enviam e recebem informações de roteamento pelo mesmo endereço classe D 224.0.0.10, por isso o termo "**grupo de multicast**".

No Unicast precisamos ter um IP de origem e outro de destino **únicos** na rede, já no broadcast temos um endereço de origem do host que está enviando o pacote e o destino será 255.255.255.255 ou um dos endereços de broadcast direcionados de uma rede, por exemplo, 192.168.1.255.

## 7.7 Endereçamento IPv4 na Prática

Na prática um endereço IP versão 4 possui 32 bits e é dividido em quatro "**octetos**", ou seja, quatro conjuntos de oito bits 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 a 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 na máscara indica que o número que está no endereço IP representa uma rede, convertendo a máscara em binário 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, laptop, impressora, switch ou interface de um roteador vão do primeiro IP após o endereço de rede até o penúltimo número da sequência (um antes do broadcast).

Lembrem-se endereços de host são também chamados de endereços de **Unicast**, para utilização de comunicação entre dois terminais apenas, já o último valor 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 (192.168.10.**00000000** - 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 (192.168.1.**00000001** - o próximo após a rede) até 192.168.10.254 (192.168.10.**11111110** - um a menos que o 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).

Lembre-se que 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 a quantidade de redes e hosts por rede e como isso tudo pode ser calculado. Se você conhecer bem o binário conseguirá responder essa pergunta sozinho, senão vamos aprender ou revisar 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 - rede) para redes (24 menos 3 que são fixos) e 8 bits (h - hosts) para fazer os hosts.
- 110**rrrrrr.rrrrrrrr.rrrrrrrr.aaaaaaaa**

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,  $2^{21}$  (dois elevado a vinte e um) 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 são dois elevados 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 o prefixo /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 (**10rrrrrr.rrrrrrrr.hhhhhh.hhhhhh**).
- 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 dois últimos octetos variando como host, pois ela é uma classe A (**10rrrrrr.hhhhhh.hhhhhh.hhhhhh**).
- 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.

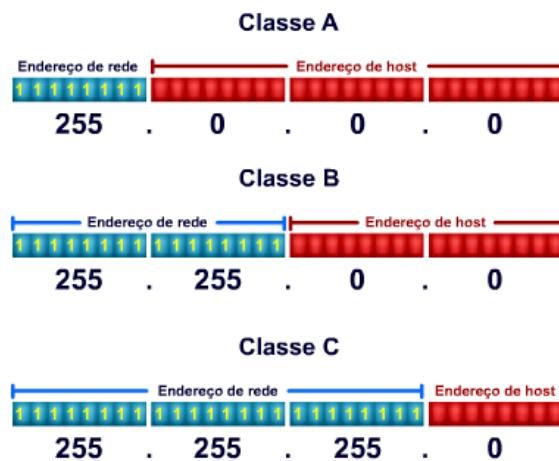
Na prática cada rede LAN, VLAN ou WAN precisa de uma rede IP **própria e única**, portanto endereçar é atribuir uma rede a uma interface de um roteador ou a uma VLAN e distribuir os endereços de host para essas interfaces e demais terminais.

O que estudamos aqui são as **redes IP baseadas em classes** ou **classfull**. Mais para frente no curso vai dividir essas redes em **sub-redes** e também analisar o cálculo de **redes classless** ou **CIDR**, ou seja, como a Internet funciona atualmente, desconsiderando as classes de IP e utilizando **prefixos** ao invés de máscaras de sub-rede.

## 7.8 Resumo dos Tipos de Endereços e Máscaras

### 7.8.1 Máscara de Rede ou Netmask

Tem a função de delimitar o que é rede e host dentro de um endereço IP, os "uns" representam a porção da rede do endereço e os "zeros" representam a porção host. Abaixo seguem as máscaras das classes A, B e C:



As máscaras de sub-rede podem ser representadas pelo termo "prefixo" o qual é a contagem de bits 1 da máscara com uma barra na frente. Por exemplo, a máscara da classe A é uma /8 (11111111.00000000.00000000.00000000 - 255.0.0.0).

O roteador consegue distinguir a porção de rede de um endereço IP através do AND lógico, o qual é uma conta feita bit a bit entre o endereço IP e a máscara de subrede, sendo que o resultado dessa operação é o endereço de Rede. A regra do AND é simples, qualquer bit com 0 dará 0 e 1 com 1 dará 1 como resposta. Veja exemplo na figura abaixo.

<b>Classe A</b>	11111111 . 00000000 . 00000000 . 00000000
	255 . 0 . 0 . 0
	89 . 23 . 201 . 16
	<b>Endereço de rede = 89.0.0.0</b>
	<b>Endereço de host = .23.201.16</b>
<b>Classe B</b>	11111111 . 11111111 . 00000000 . 00000000
	255 . 255 . 0 . 0
	135 . 101 . 56 . 59
	<b>Endereço de rede = 135.101.0.0</b>
	<b>Endereço de host = .56.59</b>
<b>Classe C</b>	11111111 . 11111111 . 11111111 . 00000000
	255 . 255 . 255 . 0
	201 . 230 . 201 . 16
	<b>Endereço de rede = 201.230.201.0</b>
	<b>Endereço de host = .16</b>

### 7.8.2 Endereço de Rede

Identifica a própria rede e não uma interface de rede específica. Representado por todos os bits de host com o valor zero. É o primeiro IP de uma faixa de endereçamento IP e não pode endereçar hosts, sendo utilizado para criar rotas ou caminhos até determinados destinos.

### 7.8.3 Endereço de Host

Identifica uma interface de rede específica ou um host. É o valor numérico onde na máscara de rede está representado com valor zero.

Por exemplo, se você tiver o IP 10.150.20.1 com máscara de rede padrão 255.0.0.0, a rede será 10 e o host é representado pelo valor 150.20.1.

Os endereços de host vão do primeiro IP após o endereço de rede (segundo endereço de uma faixa de IPs) até o penúltimo IP da faixa (um endereço antes do broadcast), por exemplo, na rede 192.168.10.0 com máscara 255.255.255.0 o primeiro IP será o 192.168.10.1 (192.168.10.00000001) e o último o 192.168.10.254 (192.168.10.11111110).

São os endereços Unicast utilizados para endereçar as interfaces de rede e computadores. Utilizam na camada-2 em redes LAN o endereço MAC da própria placa de rede para identificação na rede local.

### 7.8.4 Endereço de Broadcast

Identifica todas as máquinas na rede, representado por todos os bits de host com o valor UM (255.255.255.255), pode ser chamado broadcast local, ou seja, para todos os usuários de uma LAN. Existe também o broadcast direcionado para apenas uma rede ou sub-rede (ex: 200.192.121.255).

Ambos os broadcasts local ou direcionado utilizam o endereço MAC com todos os bits em 1 (ffff.ffff.ffff). Em situações normais não são utilizamos como **origem** de uma comunicação e sim como **destino**, pois sempre um host origina um broadcast, não tem como um broadcast se "auto-originar".

### 7.8.5 Endereço de Loopback

Identifica a própria máquina e serve para enviar uma mensagem para a própria ou fazer a comunicação de processos internos ao sistema operacional, ficando a mensagem restrita ao próprio host, sem ser enviada à rede.

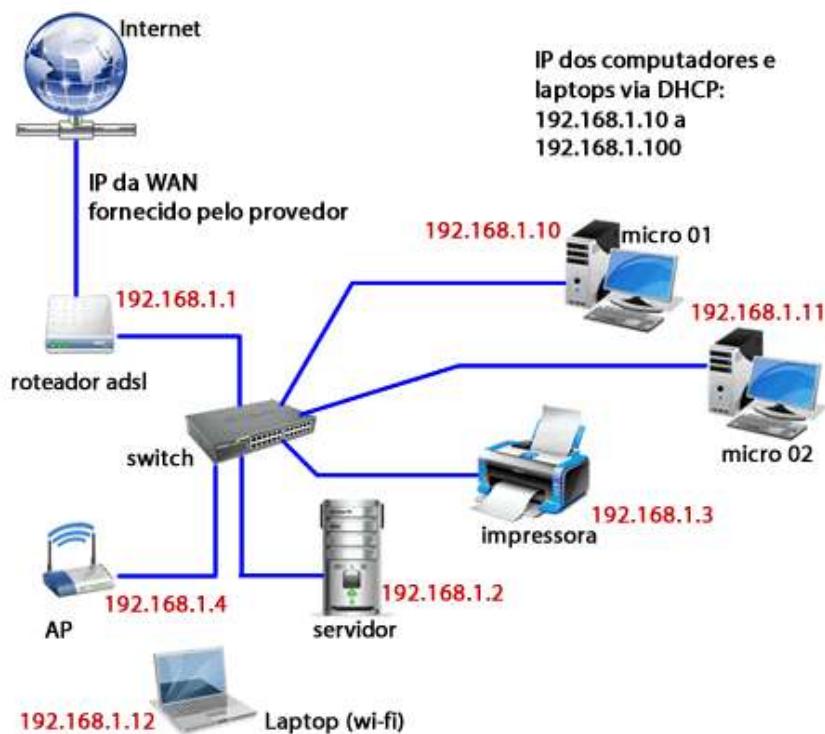
Este endereço é 127.0.0.1 em maioria dos sistemas operacionais, porém em roteadores e switches Cisco ele não vem configurado e normalmente utilizamos uma faixa dos IPs de rede como Loopback e não a rede 127.0.0.0.

As loopbacks em roteadores são utilizadas para garantir estabilidade em processos vinculados a Interfaces, pois ela é uma interface lógica e mesmo que desliguem um cabo essa interface não cai, não interrompendo assim o funcionamento do processo.

## 7.9 Exemplo de Projeto Lógico de Rede SOHO

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 192.168.1.0/24. Para atribuir os IPs aos computadores utilizaremos o serviço de DHCP, liberando dos IPs 192.168.1.10 a 192.168.1.100 para os computadores que pegam IP dinâmico. Dos IPs 192.168.1.1 até 192.168.1.9 vamos reservar para configurar os IPs fixos, conforme abaixo:

- O IP 192.168.1.1 configuramos na interface LAN do roteador;
- O IP 192.168.1.2 para o servidor local;
- O IP 192.168.1.3 para uma impressora de rede;
- O IP 192.168.1.4 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 192.168.1.4, 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.

## 7.10 Endereçando Redes Classful

Agora vamos utilizar um exemplo de topologia simples utilizado em capítulos anteriores e fazer o endereçamento dos de redes LAN e WAN utilizando IPs classes A, B e C para analisar as consequências. Veja a topologia abaixo.



Vamos iniciar pensando em quantos hosts cada LAN precisa supondo que a rede LAN-1 vai utilizar 100 endereços para dividir entre computadores, servidores e dispositivos de rede em uma mesma LAN. Já para a LAN 2 termos a necessidade de duas sub-redes para criação de duas VLANs no switch cada uma para suportar até 80 endereços.

Para a rede WAN não precisamos pensar muito, pois uma rede ponto a ponto só tem dois pontos, portanto precisamos dois IPs para endereçar cada uma das séries dos roteadores R1 e R2.

Vamos utilizar somente redes privativas, conforme RFC 1918.

### 7.10.1 Projeto com Classe C

As redes classe C privativas iniciam em 192.168.0.0, portanto precisamos de 4 redes:

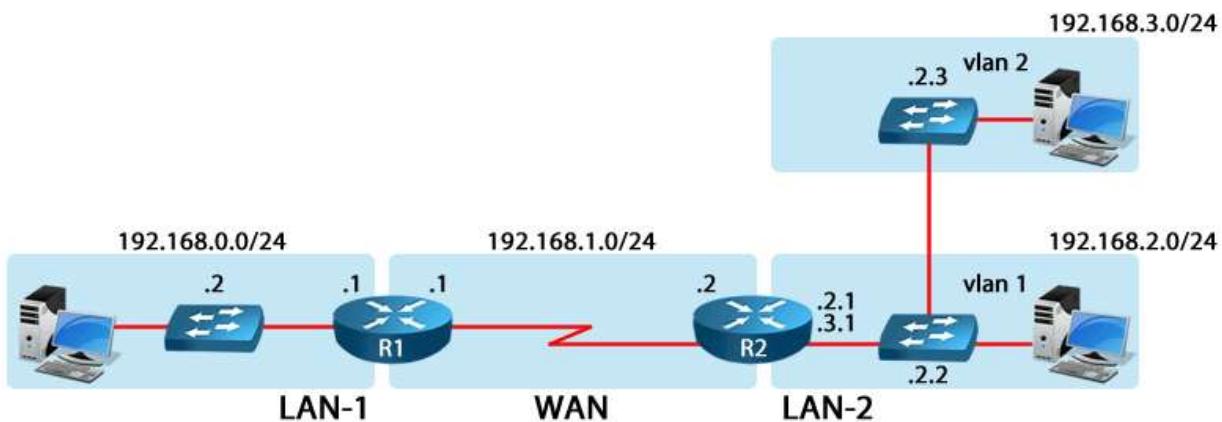
1. LAN-1: 192.168.0.0 255.255.255.0 – 100 endereços.
2. WAN: 192.168.1.0 255.255.255.0 – 2 endereços.
3. LAN-2 VLAN 1: 192.168.2.0 255.255.255.0 – 80 endereços.
4. LAN-2 VLAN 2: 192.168.3.0 255.255.255.0 – 80 endereços.

Agora vamos dividir os endereços IP para os hosts em cada rede:

1. LAN-1 tem os IPs de 192.168.0.1 a 192.168.0.254 -> IPs de 192.168.0.1 a 192.168.0.10 reservados para endereçar roteadores, switches e impressoras e IPs de 192.168.0.100 a 192.168.0.210 para endereçar os hosts via DHCP.
2. WAN tem os IPs de 192.168.1.1 a 192.168.1.254 -> IP 192.168.1.1 para a serial de R1 e 192.168.1.2 para a serial do R2, assim os dois estão na mesma rede IP e podem se comunicar.
3. LAN-2 VLAN 1 tem os IPs de 192.168.2.1 a 192.168.2.254 -> mesmo princípio usado em LAN-1, dos IPs com final .1 a .10 para dispositivos de rede e de .100 a .200 para o DHCP.
4. LAN-2 VLAN 2 tem os IPs de 192.168.3.1 a 192.168.3.254 -> idem ao anterior.

Com a definição acima já poderíamos configurar os roteadores, switches e servidores de rede.

Uma parte importante do projeto é ter um diagrama da rede ou vários diagramas com os diversos segmentos de rede dependendo do tamanho da empresa. Veja na figura a seguir o diagrama de rede com o endereçamento especificado.



Note no diagrama acima que indicamos a rede geral e depois as interfaces indicamos apenas como ".1", ".2", etc. Essa notação é bem comum, por exemplo, na WAN sabemos que a rede é 192.168.1.0 e a serial de R1 (.1) é 192.168.1.1.

No roteador R1 a configuração das interfaces (supondo que ele tem uma serial DTE de banda 1Mbps e uma fastethernet na LAN):

```

R1>enable
R1#config term
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#bandwidth 1000
R1(config-if)#description WAN conectada ao R2
R1(config-if)#no shut
R1(config-if)#interface fast 0/0

```

```
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#description LAN-1
R1(config-if)#no shut
R1(config-if)#end
R1#copy run start
```

Veja novamente o diagrama final da rede e responda por que os switches estão com IPs da rede 192.168.2.0?

**Resp:** "Porque a rede 192.168.2.0 é a rede da VLAN 1, a qual é por padrão a VLAN de gerenciamento."

Analizando ainda esse exemplo o que você diria da alocação de IPs, houve desperdício de endereços? Onde esse desperdício foi maior?

**Resp:** "Sim, pois uma rede classe C tem 254 IPs e a maior LAN precisava de apenas 100 endereços. O maior desperdício foi na rede WAN que precisava de dois IPs e alocamos uma rede com 254 endereços, um desperdício de 252 endereços."

### 7.10.2 Projeto com Classe B

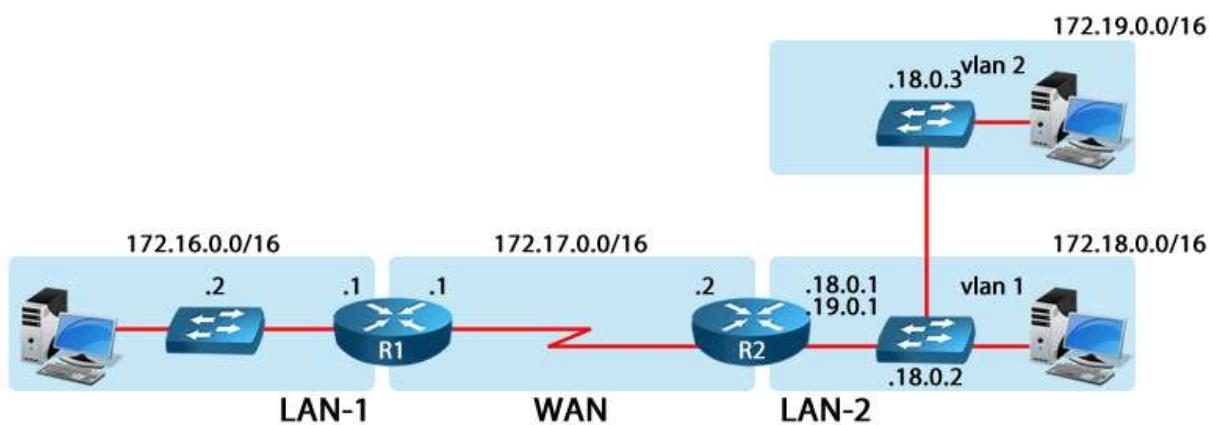
As redes classe C privativas iniciam em 172.16.0.0 e precisamos de 4 redes:

1. LAN-1: 172.16.0.0 255.255.0.0 – 100 endereços.
2. WAN: 172.17.0.0 255.255.0.0 – 2 endereços.
3. LAN-2 VLAN 1: 172.18.0.0 255.255.0.0 – 80 endereços.
4. LAN-2 VLAN 2: 172.19.0.0 255.255.0.0 – 80 endereços.

Agora vamos dividir os endereços IP para os hosts em cada rede:

1. LAN-1 tem os IPs de 172.16.0.1 a 172.16.0.254 -> IPs de 172.16.0.1 a 172.16.0.10 reservados para endereçar roteadores, switches e impressoras e IPs de 172.16.0.100 a 172.16.0.210 para endereçar os hosts via DHCP.
2. WAN tem os IPs de 172.17.0.1 a 172.17.0.254 -> IP 172.17.0.1 para a serial de R1 e 172.17.0.2 para a serial do R2.
3. LAN-2 VLAN 1 tem os IPs de 172.18.0.1 a 172.18.0.254 -> IPs de 172.18.0.1 a 172.18.0.10 reservados para endereçar roteadores, switches e impressoras e IPs de 172.18.0.100 a 172.18.0.210 para endereçar os hosts via DHCP.
4. LAN-2 VLAN 2 tem os IPs de 172.19.0.1 a 172.19.0.254 -> lógica idem ao exemplo anterior.

Agora vamos ao diagrama de rede.



No roteador R1 a configuração das interfaces (supondo que ele tem uma serial DTE de banda 1Mbps e uma fastethernet na LAN):

```
R1>enable
R1#config term
R1(config)#interface fast 0/0
R1(config-if)#ip address 172.16.0.1 255.255.255.0
R1(config-if)#description LAN-1
R1(config-if)#no shut
R1(config-if)#interface serial 0/0/0
R1(config-if)#ip address 172.17.0.1 255.255.255.0
R1(config-if)#bandwidth 1000
R1(config-if)#description WAN conectada ao R2
R1(config-if)#no shut
R1(config-if)#end
R1#copy run start
```

Analisando ainda o exemplo do projeto com classe B o que você diria da alocação de IPs, houve desperdício de endereços? Onde esse desperdício foi maior?

**Resp:** "Sim, pois uma rede classe B tem mais de 65 mil IPs e a maior LAN precisava de apenas 100 endereços. O maior desperdício foi na rede WAN, porém a comparação entre o número de hosts pedidos e a quantidade disponível na classe B a diferença se torna irrelevante."

### 7.10.3 Projeto com Classe A

O projeto da rede com classe A agora é por sua conta!

Considere a mesma topologia e requisitos para elaborar seu projeto.

Pense bem e clique no link ao lado para ver a resposta:

**Resp:** "Esse projeto não é possível com rede classe A cheia da RFC 1918 porque temos apenas uma rede, a 10.0.0.0, e precisamos de 4 redes, por isso com não é possível fazer o projeto com esses requisitos!"

## 7.11 Introdução ao Conceito de Sub-Redes

O conceito de sub-redes nasceu da necessidade de melhor se aproveitar o endereçamento IP, flexibilizando a tradicional divisão em classes (onde a divisão entre rede e host ocorre somente a cada 8 bits, como visto anteriormente).

Com esse novo conceito a identificação de rede e host no endereçamento IP é feita de forma variável, podendo utilizar qualquer quantidade de bits (e não mais múltiplos de 8 bits). Para tal foi criado um identificador adicional chamado "**Máscara de sub-rede**", onde podemos emprestar bits de host para criar novas redes, chamadas de sub-redes.

Com esse novo conceito podemos criar níveis hierárquicos que possibilitarão uma melhor utilização do endereçamento IP, permitindo dividir faixas de endereço por setores da empresa, departamentos ou tecnologias.

A "máscara" identifica em um endereço IP que porção de bits é utilizada para identificar a rede e que porção de bits identifica o host. Ela é formada por 4 bytes com uma sequência contínua de bits um, seguida de uma sequência de bits zero de host. A porção de bits em 1 identifica quais bits são utilizados para identificar a rede no endereço e a porção de bits em 0, identifica que bits do endereço identificam a estação.

Outra notação também muito utilizada é identificar a "máscara" como um número inteiro que diz a quantidade de bits 1 (um) utilizados. Por exemplo, uma máscara com valor 255.255.255.192 pode também ser representada como /26. Ou seja, essa máscara utiliza 26 bits para identificar a rede e os 06 bits restantes para identificar os hosts.

Por exemplo, vamos admitir que no endereço 220.150.38.X iremos utilizar uma máscara de sub-rede /26. Dessa forma a parte de rede terá 26 bits para identificar a rede e os 6 bits restantes serão utilizados para identificar os hosts. Ou seja, para o endereço 220.150.38.0 da antiga classe C foram emprestados 2 bits de host para que sejam criadas as novas sub-redes. Logo, esse endereço poderá ser dividido em quatro redes com as identificações abaixo. Note que os 4 endereços de rede são independentes entre si. Elas podem ser empregadas em redes completamente separadas, e até mesmo serem utilizadas em instituições distintas.

220.150.38.[00XXXXXX]  
220.150.38.[01XXXXXX]  
220.150.38.[10XXXXXX]  
220.150.38.[11XXXXXX]

Em termos de identificação da rede, utilizam-se os mesmos critérios anteriores, ou seja, todos os bits de identificação da estação são 0. Quando os bits da estação são todos 1, isto identifica um broadcast naquela rede específica. Desta forma temos as seguintes identificações para endereço de rede:

220.150.38.0  
220.150.38.64  
220.150.38.128  
220.150.38.192

Os endereços de broadcast nas redes são:

220.150.38.63  
220.150.38.127  
220.150.38.191 e  
220.150.38.255

Os possíveis endereços de estação em cada rede são:

220.150.38.[1-62]  
220.150.38.[65-126]  
220.150.38.[129-190] e  
220.150.38.[193-254]

Repare no exemplo da sub-rede /26 que o último bit emprestado tinha valor 64 (2 elevado a 6, igual a 64). Veja como as sub-redes variaram na mesma proporção (0, 64, 128, 192).

220.150.38.0  
220.150.38.64  
220.150.38.128  
220.150.38.192

Portanto, a divisão em sub-redes poderia resolver o problema dos exemplos anteriores, poderíamos, por exemplo, utilizar uma máscara /30 na WAN (255.255.255.252). Essa máscara possibilita a divisão de uma rede em sub-redes de 4 endereços IP, sendo que dois deles são válidos, bem o que precisamos para uma rede WAN.

Se utilizarmos diversas máscaras de sub-rede com comprimentos diferentes, por exemplo, /24, /25 para LAN e /30 para WAN, temos o conceito de VLSM ou Máscaras de Sub-Rede de Comprimento Variável.

Não se preocupe agora em aprender o cálculo de sub-redes, pois esse é apenas um tópico introdutório, em um capítulo posterior vamos tratar somente de aprender a calcular sub-redes, VLSM, CIDR e sumarização de redes!

## 8 Configurando Endereços em Interfaces de Roteadores e Switches

No capítulo 4 estudamos a configuração básica de uma interface IP, inserindo um endereço estático (manual) utilizando o comando “**ip address**” dentro do modo de configuração global. Veja exemplo abaixo:

```
R1(config-if)#interface fast 0/0
R1(config-if)#ip address 172.17.0.1 255.255.255.0
R1(config-if)#description LAN-1
R1(config-if)#no shut
```

Existem outras opções para configurar o IP em uma interface de roteadores e switches Cisco, através do DHCP ou então inserindo endereços IP secundários, o que possibilita que uma interface responda para duas ou mais redes diferentes. Veja a saída do comando **ip address** com o help para ver as opções possíveis em um roteador abaixo:

```
R1(config-if)#ip address ?
  A.B.C.D  IP address
  dhcp      IP Address negotiated via DHCP
  pool      IP Address autoconfigured from a local DHCP pool
R1(config-if)#ip address dhcp
```

Portanto com o comando “**ip address dhcp**” o roteador enviará uma solicitação ao serviço de DHCP local para fazer a atribuição dinâmica de IP na interface, porém não é muito utilizada porque os dispositivos de redes normalmente precisam ter um endereço bem conhecido.

Por exemplo, imagine que o roteador R1 é seu gateway e devido a algum problema no DHCP ele muda de endereço. O que vai ocorrer é que todos os hosts que tinham o IP antigo do roteador não conseguiram mais sair para a Internet através desse gateway.

### 8.1 Endereços IPs Secundários

Cada interface IP possui um endereço principal e para inserir mais endereços na mesma interface você precisa utilizar o comando “secondary” no final da declaração da configuração de IP, veja exemplo abaixo:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip address 172.16.0.1 255.255.255.0
R1(config-if)#ip address 172.17.0.1 255.255.255.0 secondary
R1(config-if)#ip address 172.18.0.1 255.255.255.0 secondary
R1(config-if)#do show run interface f0/0
Building configuration...

Current configuration : 187 bytes
!
interface FastEthernet0/0
  ip address 172.17.0.1 255.255.255.0 secondary
  ip address 172.18.0.1 255.255.255.0 secondary
```

```
ip address 172.16.0.1 255.255.255.0
shutdown
duplex half
end

R1(config-if) #
```

No exemplo acima configuramos o endereço 172.16.0.1 como principal e 172.17.0.1 e 172.18.0.1 como secundários, podemos ter diversos IPs secundários configurados, porém não é muito usual atualmente.

Existe uma desvantagem do uso desse tipo de solução com todos os hosts em uma mesma VLAN e separados por sub-redes diferentes, pois assim você não segregá os broadcasts enviados na rede e também insere mais saltos para que dois hosts em uma mesma rede física se comuniquem, pois eles estão compartilhando o mesmo meio, poderiam estar na mesma sub-rede e simplesmente trocar informações entre si sem precisar enviar para o roteador padrão fazer o encaminhamento entre as sub-redes.

Com switches suportando VLANs é mais comum termos cada rede ou sub-rede IP segregada nos switches em diferentes VLANs, assim realmente segregamos o domínio de broadcast.

Na prática redes secundárias podem servir como medida paliativa para quando uma rede cresce demais e é preciso mudar a máscara de sub-rede. Para evitar transtornos aos usuários, pode-se fazer uma configuração da rede secundária para que os novos computadores tenham acesso à rede até que o projeto de integração completa da rede possa ser configurado nos roteadores.

## 8.2 Erros Comuns ao Configurar Interfaces

Devemos lembrar-nos de algumas regras descritas sobre configuração de endereços IP que servem para todos os dispositivos de rede:

1. Endereços de rede e de broadcast não podem ser utilizados para endereçar Hosts.
2. Endereços IP devem ser únicos na Intranet e/ou na Internet.
3. Cada interface do roteador deve pertencer a uma rede ou sub-rede distinta, não podemos repetir rede ou sub-rede em interfaces diferentes.

Caso você não obedeça a essas regras básicas mensagens de erro serão geradas, veja alguns exemplos abaixo onde.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip add
R1(config-if)#ip address 10.0.0.0 255.0.0.0
Bad mask /8 for address 10.0.0.0
R1(config-if)#ip address 192.168.1.255 255.255.255.0
Bad mask /24 for address 192.168.1.255
```

Note em amarelo que ao tentar inserir o IP 10.0.0.0/8 o roteador emitiu uma mensagem de "Bad mask", ou seja, com essa máscara esse IP não pode ser configurado nessa interface, pois como já estudamos trata-se de um endereço de rede e não de host.

O mesmo acontece para o exemplo abaixo destacado em verde, ao tentarmos configurar um broadcast na interface recebemos um "Bad mask".

No próximo exemplo vamos tentar inserir um IP de uma rede já configurada em uma das interfaces do roteador.

```
R1(config-if)#int f0/0
R1(config-if)#ip add 10.0.0.1 255.255.255.0
R1(config-if)#int f0/1
R1(config-if)#ip add 10.0.0.10 255.255.255.0
% 10.0.0.0 overlaps with FastEthernet0/0
R1(config-if)#

```

Perceba que nesse segundo exemplo o roteador mostra uma mensagem de erro diferente, na qual ele informa um “**overlap**” indicando que esse IP está na faixa da interface fast0/0.

É importante sempre “ficar ligado” nas mensagens que os roteadores e switches enviam para identificar possíveis erros e não perder tempo!

### 8.3 Configurando Endereços IP em Switches

Conforme estudamos no capítulo 3, os switches camada 2 não suportam endereço IP em suas interfaces físicas (fast ou giga), por isso precisamos configurar o IP em uma “interface vlan”, sendo que por padrão essa configuração é feita na “interface vlan 1”. Veja exemplo abaixo:

```
SW-DlteC>en
Password:
SW-DlteC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-DlteC(config)#interface vlan 1
SW-DlteC(config-if)#ip address ?
  A.B.C.D  IP address
    dhcp      IP Address negotiated via DHCP
    pool      IP Address autoconfigured from a local DHCP pool

```

Perceba acima que a configuração é a mesma do roteador. Inclusive permite a configuração de IPs secundários, conforme saída abaixo:

```
SW-DlteC(config-if)#ip address 192.168.1.5 255.255.255.0 ?
  secondary  Make this IP address a secondary address
<cr>
SW-DlteC(config-if)#ip address 192.168.1.5 255.255.255.0 secondary
```

### 8.4 Apagando e Alterando Endereços Configurados

O comando “ip address” é do tipo substitutivo, ou seja, como cada interface só pode ter um endereço principal, para trocar o endereço é só sobrescrever o comando, veja exemplo abaixo:

```
R1(config)#int f0/0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#do sho run int f0/0
Building configuration...

Current configuration : 81 bytes
!
interface FastEthernet0/0
  ip address 10.0.0.1 255.255.255.0
  duplex half
end

R1(config-if)#ip add 10.0.0.2 255.255.255.0
R1(config-if)#do sho run int f0/0
Building configuration...
```

```

Current configuration : 81 bytes
!
interface FastEthernet0/0
 ip address 10.0.0.2 255.255.255.0
 duplex half
end

```

Para remover o IP da interface basta entrar com o comando “**no ip address**”. Essa opção apaga o endereço IP principal e os secundários ao mesmo tempo.

Para apagar somente um ip secundário é preciso especificar o IP a ser apagado. Veja exemplo abaixo onde temos três IPs secundários configurados e precisamos apagar apenas o referente à rede 12.0.0.0/8:

```

R1(config-if)#ip address 11.0.0.1 255.0.0.0 secondary
R1(config-if)#ip address 12.0.0.1 255.0.0.0 secondary
R1(config-if)#ip address 13.0.0.1 255.0.0.0 secondary
R1(config-if)#do show run int f0/0
Building configuration...

```

```

Current configuration : 204 bytes
!
interface FastEthernet0/0
 ip address 11.0.0.1 255.0.0.0 secondary
 ip address 12.0.0.1 255.0.0.0 secondary
 ip address 13.0.0.1 255.0.0.0 secondary
 ip address 10.0.0.2 255.255.255.0
 duplex half
end

R1(config-if)#no ip add 12.0.0.1 255.0.0.0 secondary
R1(config-if)#do show run int f0/0
Building configuration...

```

```

Current configuration : 163 bytes
!
interface FastEthernet0/0
 ip address 11.0.0.1 255.0.0.0 secondary
 ip address 13.0.0.1 255.0.0.0 secondary
 ip address 10.0.0.2 255.255.255.0
 duplex half
end

R1(config-if)#

```

Portanto, para apagar um endereço secundário precisamos inserir a opção “no” mais o comando completo.

## 8.5 Verificando as Configurações das Interfaces

Para verificar as configurações das interfaces você pode utilizar o comando “show running-config” ou especificar apenas a interface que deseja ver as configurações com o “show running-config interface **tipo-interface num-interface**”, por exemplo, para ver apenas a configuração da interface fast 0/0 utilizamos o “show running-config interface fast 0/0”, conforme utilizamos nos exemplos anteriores para verificar as configurações.

Se você não estiver em modo privilegiado utilize a opção “**do**” para não precisar sair do modo de configuração e executar o comando show.

Também podemos utilizar o “show interfaces” e o “show ip interface brief”, veja exemplo abaixo.

```
R1#sho ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    10.0.0.2        YES manual up       up
FastEthernet1/0    unassigned      YES unset administratively down down
FastEthernet1/1    unassigned      YES unset administratively down down
R1#
```

Com esse comando podemos verificar a interface, o endereço IP no campo (IP-Address), depois no OK se a interface está com problema, no campo Method temos a maneira que a configuração foi realizada, por exemplo, a interface fast 0/0 tem a configuração manual (IP estático) e por último temos os campos Status indicando se a camada física está up ou down e no campo Protocol temos o estado do protocolo de camada 2 se está up ou down.

Nesse comando não temos o detalhe da máscara de rede, para saber essa informação temos que utilizar o show interface ou show running-config.

Lembre-se que o status da Interface deve estar UP/UP, significando que tanto as camadas físicas como a de enlace estão funcionando perfeitamente. Os outros estados possíveis são:

- **UP/DOWN**: a camada física está OK mas a de enlace está com problemas, por exemplo protocolo de camada 2 de um dos lados está configurado errado ou falta do comando clock rate em interfaces DCE.
- **DOWN/DOWN**: a camada física está com problemas, por exemplo, cabo rompido ou modelo errado.
- **Administratively Down**: falta o comando “no shutdown” na interface, ou seja, a interface está desabilitada.

Por último, sempre que configuramos e ativamos uma interface uma rota para a rede da interface configurada é inserida na tabela de roteamento, assim como uma rota local com máscara de host /32 para indicar o endereço configurado na própria Interface. Veja exemplo abaixo.

```
R1(config)#int f2/0
R1(config-if)#ip add 15.0.0.1 255.0.0.0
R1(config-if)#no shut
R1(config-if)#end
R1#sho
*Jul 11 22:49:37.215: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      + - replicated route, % - next hop override

Gateway of last resort is not set

      15.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        15.0.0.0/8 is directly connected, FastEthernet2/0
L        15.0.0.1/32 is directly connected, FastEthernet2/0
R1#
```

A informação na tabela de roteamento destacada em amarelo e com o termo “**directly connected**” é uma rota diretamente conectada, ou seja, pertence ao próprio roteador local. Note que as rotas diretamente conectadas são marcadas com um “C” na frente.

A rota local destacada em verde e marcada com o símbolo “L” no início foi inserida em IOSs versão 15, se você estiver realizando testes em IOSs mais antigos essa informação não é mostrada na saída desse comando. Ela indica o endereço IP configurado na interface, por isso a máscara inserida na tabela de roteamento é /32 ou 255.255.255.255.

Uma máscara 255.255.255.255 tem todos os IPs de rede, ou seja, indica um IP único, sem faixa de IPs válidos ou broadcast.

## 9 Resumo do Capítulo

Bem pessoal, chegamos ao final do capítulo. É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Entender o Modelo TCP/IP e suas camadas.
- Ser capaz de comparar o modelo OSI e TCP/IP.
- Ser capaz de explicar as diferenças entre os protocolos TCP e UDP.
- Ter conhecimento sobre os principais campos do cabeçalho dos protocolos TCP e UDP.
- Entender como o TCP estabelece e encerra uma conexão.
- Entender os processos de reagrupamento, retransmissão e controle de congestionamento no TCP.
- Dominar o cálculo de transformação de números decimais e binários.
- Entender a lógica do endereçamento IP e suas classes.
- Entender o conceito de subredes.
- Dominar o conceito do fluxo de dados em uma rede LAN e através da WAN.
- Saber configurar endereços IP primários, secundários e via DHCP em roteadores e switches Cisco.
- Saber os principais comandos para verificar as configurações de interfaces em roteadores e switches.

Iremos estudar nesse capítulo conceitos importantes sobre roteamento e protocolos de roteamento. No decorrer desse capítulo você aprenderá os princípios de roteamento, roteamento estático e o serviço de DHCP em clientes e servidores.

Esse é um tópico muito importante tanto para o dia a dia de um profissional da área de redes e também para o exame de certificação.

Esperamos que você aproveite o capítulo e aprenda bastante.

Bons estudos!

## **Capítulo 6 - Introdução ao Roteamento, Rotas Estáticas e DHCP**

### **Objetivos do Capítulo**

Ao final desse capítulo você terá estudado e deverá compreender:

- Entender o conceito de interfaces diretamente conectadas e como elas aparecem na tabela de roteamento.
- Dominar o conceito e configuração de rotas estáticas.
- Entender como funciona e a configuração de uma rota padrão.
- Entender os conceitos de métrica e distância administrativa.
- Saber resolver problemas básicos de roteamento em roteadores e clientes.
- Entender o processo de roteamento em roteadores e clientes.
- Entender e configurar o serviço de DHCP no Cisco IOS.
- Ser capaz de manter o serviço de DHCP com comandos show e debug no Cisco IOS.

## Sumário do Capítulo

<b>1 Visão Geral do Roteamento em Roteadores Cisco</b>	<b>250</b>
<b>2 Interfaces Diretamente Conectadas e Processo de Encaminhamento</b>	<b>251</b>
2.1 Interfaces Diretamente Conectadas	252
2.2 Exemplo de Configuração e Alcance com Interfaces Conectadas	253
2.3 Analisando a Tabela de Roteamento	255
2.4 Process Switching, Fast Switching e CEF	
258	
2.5 Escolha da Melhor Rota – Regra do “Longest Match”	260
2.6 Questões sobre Processo de Roteamento e Desempenho	261
<b>3 Configurando e Verificando Rotas Estáticas</b>	<b>263</b>
3.1 Opções do Comando IP-Route	265
3.2 Exemplo de Configuração - Rota Estática	
265	
3.3 O que é Melhor Interface ou IP na Rota Estática?	271
3.4 Configurando uma Rota Padrão (Default-Gateway)	272
3.4.1 Uso do Comando ip default-gateway	272
3.5 Rota Estática Flutuante	273
<b>4 Roteamento em Clientes de Rede</b>	<b>275</b>
4.1 Problemas Comuns de Alcançabilidade em Clientes	276
<b>5 Configurando o Serviço de DHCP em Roteadores Cisco</b>	<b>277</b>
5.1 Visão Geral do DHCP	277
5.2 Funcionamento do DHCP	278
5.3 Configurando o DHCP Servidor no Cisco IOS	279
5.4 Exemplo Prático de Configuração do DHCP	
280	
5.5 Configurando o DHCP Relay	283

<b>5.6 Monitorando e Mantendo o DHCP</b>	<b>284</b>
<b>6 Resumo do Capítulo</b>	<b>286</b>

## 1 Visão Geral do Roteamento em Roteadores Cisco

Nesse capítulo vamos estudar os princípios básicos de roteamento, como criar rotas estáticas e conceitos teóricos dos protocolos de roteamento dinâmico.

A principal função de um roteador é **encaminhar pacotes** através da rede e ele cumpre essa missão utilizando os **protocolos de roteamento**, os quais foram projetados para alimentar a principal tabela que um roteador mantém a “**tabela de roteamento**” ou “**routing table**”.

A tabela de roteamento guarda as informações das redes que um roteador pode alcançar, caso determinada rede não seja conhecida pelo roteador, ou seja, a **rota** para aquela rede não está na tabela de roteamento, ele descartará a rota e enviará uma mensagem de “unreachable” (fora de alcance) através do protocolo ICMP para o computador que estava tentando se comunicar com a rede em questão.

Portanto, sempre que entra um pacote IP em um roteador ele lê o **endereço de destino** contido no pacote e verifica se a rede a que esse pacote IP pertence está presente em sua tabela de roteamento. Caso não esteja, ou ele descarta o pacote ou então envia para uma rede **padrão (default gateway)**, a qual pode ser uma rota para a internet, por exemplo.

A visualização das rotas nos roteadores é um pouco diferente do que ilustramos anteriormente em um computador Windows, porém o princípio é o mesmo, uma rota é composta por:

- **Endereço ou rede de destino:** rede remota que o roteador sabe como encaminhar.
- **Máscara de rede**
- **Gateway e/ou Interface de saída:** por onde os pacotes para a rede de destino serão encaminhados.
- **Métrica:** valor numérico para definir qual a melhor rota quando vários caminhos são aprendidos para um mesmo destino.
- **Distância administrativa:** valor numérico que define qual origem de roteamento é mais confiável, por exemplo, o RIP tem distância administrativa 120 e o OSPF 110, se o router aprender rota para o mesmo destino através dos dois protocolos ele irá escolher sair pela rota aprendida pelo OSPF, pois ele tem distância menor que a do RIP, por isso é mais confiável.

O conceito de métrica e distância administrativa em alguns sistemas operacionais dos computadores é unificado na métrica. Esses conceitos serão mais bem estudados ao longo desse capítulo.

Basicamente nos roteadores as rotas ou caminhos para redes remotas podem ser aprendidas de quatro maneiras:

1) **Via Rota Diretamente Conectada:**

```
R1(config)#interface fast 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
```

2) **Via Rota Estática:**

```
R1(config)#ip route rede mask gateway/interface
```

3) **Via Roteamento Dinâmico:**

```
R1(config)#router rip/ospf/eigrp/is-is/bgp
```

**4) Via Gateway Padrão:**

```
R1(config)#ip route 0.0.0.0 0.0.0.0 gateway/interface
```

Quando configuramos o IP em uma interface e ela fica Up/Up uma rota é inserida na tabela de roteamento automaticamente indicando que a rede configurada naquela interface está diretamente conectada a ela.

Esta rota é identificada com a letra "C" na frente da rota. Dizemos que esse tipo de rota é uma "Rota Diretamente Conectada".

Ao mesmo tempo uma rota local indicada com a letra "L" também é criada apontando para o próprio endereço IP da interface com uma máscara /32 (máscara de host – 255.255.255.255).

Você pode criar uma rota de host (host route) com a máscara /32 apontando para um computador específico, por exemplo, tem um computador com IP isolado na sua rede LAN 192.168.1.10, você pode criar uma rota de host para ele com o comando:

```
R1(config)#ip route 192.168.1.10 255.255.255.255 fast0/0
```

Podemos dizer que o processo de roteamento se inicia com a configuração das interfaces diretamente conectadas, pois sem interfaces configuradas e ativas como os pacotes serão encaminhados?

Já as rotas estáticas são inseridas e alteradas **manualmente** por um administrador de rede. Elas consomem pouca memória e processamento do roteador, porém em casos de alteração da topologia da rede é necessário um grande esforço de configuração por parte do administrador para alterar as configurações em todos os equipamentos, pois tudo é feito manualmente.

Rotas estáticas são recomendadas em redes "**stub**", ou seja, com apenas uma saída possível. Elas são identificadas com uma letra "**S**" na frente da rota.

Normalmente uma rota padrão é configurada através de uma rota estática e um **asterisco** identifica que aquela rota é a rota candidata a padrão ou "Gateway of Last Resort", por exemplo, uma rota padrão configurada com rota estática é identificada com um "**S\***".

As rotas dinâmicas dependem da configuração de um **protocolo de roteamento dinâmico**, por exemplo, o RIP, OSPF ou EIGRP. Os protocolos de roteamento dinâmico basicamente aprendem as rotas locais do roteador (diretamente conectadas) e trocam essas informações entre si para montar um mapa da rede e inserir as melhores rotas em suas tabelas de roteamento.

## **2 Interfaces Diretamente Conectadas e Processo de Encaminhamento**

As Redes **Diretamente Conectadas** ou "**Directly Connected**" (indicadas com um "**C**" na tabela de roteamento) pertencem às Interfaces do roteador, ou seja, são as redes IP que foram configuradas nas interfaces de LAN e WAN presentes no roteador em questão.

Essas rotas são essenciais, pois sem interfaces configuradas e rotas diretamente conectadas o roteador não consegue receber ou encaminhar os pacotes IP.

Portanto, com as interfaces configuradas e ativas se inicia o processo de roteamento em um roteador, o qual a princípio é capaz de encaminhar pacotes somente entre essas interfaces.

Ao longo desse tópico vamos aprender como as interfaces diretamente conectadas interferem no roteamento e como o processo de roteamento é realizado pelo roteador, você vai ver que rotear um pacote é um processo muito interessante.

## 2.1 Interfaces Diretamente Conectadas

Se uma rede **directly connected** foi mostrada em sua tabela de roteamento quer dizer que a interface que ela está referenciada foi configurada com um endereço pertencente àquela rede e a interface está **UP/UP**.

Elas são inseridas automaticamente pelo roteador à sua tabela de roteamento assim que uma interface tem um endereço IP configurado e seu status alterado para "UP/UP" (comando no shutdown).

Elas são a base para o funcionamento do roteamento estático e dinâmico, pois sem redes IP diretamente conectadas a outros roteadores não existe roteamento ou encaminhamento de pacotes.

Veja abaixo o que ocorre com uma interface fast 0/0 no momento em que é configurada e sua rota é adicionada à tabela de roteamento. Para isso inserimos o comando "debug ip routing", o qual mostra alterações na tabela de roteamento, portanto quando configurarmos a interface e inserirmos o comando "no shut" o debug deve mostrar uma rota sendo inserida na tabela de roteamento, veja a saída dos comandos a seguir.

```
Router#debug ip routing
IP routing debugging is on
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fast 0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up
RT: interface FastEthernet0/0 added to routing table
RT: SET_LAST_RDB for 192.168.1.0/24
    NEW rdb: is directly connected

RT: add 192.168.1.0/24 via 0.0.0.0, connected metric [0/0]
RT: NET-RED 192.168.1.0/24
Router(config-if)#

```

Como o comando "debug ip routing" monitora a entrada e saída de rotas na tabela de roteamento, após o comando "no shut" ser inserido uma mensagem de que a interface foi para UP (mensagem: %LINEPROTO-5-UPDOWN: Line protocol ...) foi gerada e a rede IP configurada na interface é adicionada à tabela de roteamento (Mensagem: RT: interface FastEthernet0/0 added to routing table).

Agora através dessa rede pacotes IP podem ser encaminhados e ela já pode fazer parte do processo de roteamento estático ou dinâmico para conexão com redes remotas.

Com o comando "**show ip route**" você conseguirá verificar que a rede adicionada foi para a tabela de roteamento e a letra **C** no início da linha indica que a rota é pertencente a uma rede diretamente conectada. Veja a saída do comando abaixo.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

ia - IS-IS inter area, \* - candidate default, U - per-user static route  
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP  
 + - replicated route, % - next hop override

Gateway of last resort is not set

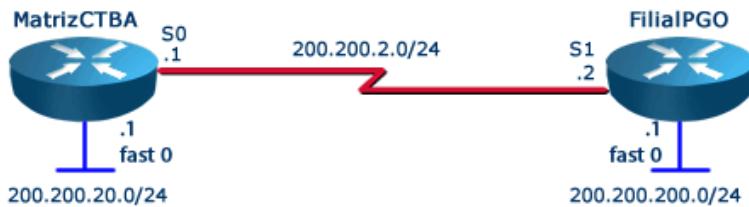
```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, FastEthernet0/0
L      192.168.1.1/32 is directly connected, FastEthernet0/0
R1#
```

Logo abaixo da rota para a rede classe C 192.168.1.0 com máscara padrão /24 (255.255.255.0) temos a entrada apontando para a própria interface 192.168.1.1 com máscara de host /32 (255.255.255.255). Essa entrada não será verificada em versões 12.x do Cisco IOS.

Com o comando “**show ip interface brief**” você pode verificar o status da interface caso a rota não tenha subido na tabela de roteamento. Lembre-se que para a interface subir a camada física e de enlace devem estar corretamente configuradas e conectadas.

## 2.2 Exemplo de Configuração e Alcance com Interfaces Conectadas

Agora veja a topologia onde temos dois roteadores conectados por um link serial ponto a ponto (linha dedicada) e cada um deles tem uma interface de LAN com endereçamento classe C e máscara padrão /24 (255.255.255.0) conforme a topologia abaixo.



Vamos supor que a conexão de WAN entre os roteadores está OK e fornecido por uma operadora, portanto ambas as interfaces são DTE, assim como a conexão de cada uma das LANs. Ao configurarmos as interfaces e executarmos o comando “no shut” elas devem subir perfeitamente. Veja abaixo as configurações:

### MatrizCTBA

```
Int Serial 0
Ip add 200.200.2.1 255.255.255.0
No shut
!
Int fast 0
Ip add 200.200.20.1 255.255.255.0
No shut
```

### FilialPGO

```
Int Serial 0
Ip add 200.200.2.2 255.255.255.0
No shut
!
Int fast 0
Ip add 200.200.200.1 255.255.255.0
No shut
```

Quais redes serão mostradas quando executarmos o comando show ip route após as configurações inseridas anteriormente? Tente responder sozinho e depois verifique a resposta analisando as tabelas de roteamento a seguir.

**MatrizCTBA#sho ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
\* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route

Gateway of last resort is not set

```
C      200.200.20.0 /24 is directly connected, Fastethernet0
C      200.200.2.0 /24 is directly connected, Serial0
```

**FilialPGO#sho ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
\* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route

Gateway of last resort is not set

```
C      200.200.200.0 /24 is directly connected, Fastethernet0
C      200.200.2.0 /24 is directly connected, Serial1
```

Com as saídas das tabelas de roteamento acima responda as seguintes perguntas:

1. Qual o alcance que um host conectado ao switch de LAN do roteador MatrizCTBA teria?
2. Que IPs do roteador MatrizCTBA e FilialPGO esse host conseguiria pingar se ele tivesse configurado como seu gateway default o IP 200.200.20.1 (IP da fast 0 do roteador MatrizCTBA)?

Para responder as perguntas temos que analisar a tabela do roteador onde o host está conectado e será seu gateway padrão, ou seja, o roteador MatrizCTBA.

Portanto esse computador conseguiria pingar a interface LAN do roteador MatrizCTBA e seu IP da WAN com certeza, pois o computador está em uma rede conhecida pelo roteador local.

O que vai acontecer quando esse computador pingar o IP da WAN do roteador FilialPGO? Esse ping terá sucesso ou não?

A resposta é NÃO, pois o roteador FilialPGO não tem rota de saída para a rede que o computador está configurado.

O que acontece é que ao receber o ping o roteador Matriz encaminhará para o FilialPGO, pois ele tem rota para o IP da WAN do roteador remoto, porém na hora do roteador Filial responder o ping ele perceberá que não tem rota para devolver essa resposta, pois ele conhece somente as redes 200.200.2.0 e 200.200.200.0, como o IP do computador pertence à rede 200.200.20.0 o roteador Filial irá descartar o pacote.

E se o mesmo computador que está na LAN do Matriz pingar a LAN do roteador FilialPGO, o que acontecerá nesse caso? Tente analisar e responder: haverá sucesso nesse ping? Onde o problema ocorrerá: no roteador Matriz ou Filial?

Nesse caso o computador enviará para o roteador Matriz um pacote com IP de destino pertencente à rede 200.200.200.0, aí vem a pergunta: "**O roteador Matriz tem rota para esse destino?**", a resposta é **NÃO**, portanto o roteador Matriz encaminhará para o host uma mensagem de destino inalcançável e descartará os pacotes recebidos, veja a saída do teste na saída abaixo coletada no computador conectado à LAN do roteador Matriz.

```
Host1>ping 200.200.200.1
```

```
Pinging 200.200.200.1 with 32 bytes of data:
```

```
Reply from 200.200.20.1: Destination host unreachable.  
Reply from 200.200.20.1: Destination host unreachable.  
Reply from 200.200.20.1: Destination host unreachable.  
Reply from 200.200.20.1: Destination host unreachable.
```

```
Ping statistics for 200.200.200.1:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
Host1>
```

Como o roteador Matriz não tem entrada na tabela de roteamento para a rede 200.200.200.0/24, ele mesmo envia via ICMP uma resposta ao computador que originou o ping contendo a mensagem "Destination host unreachable", ou seja, o computador de destino está inalcançável.

Portanto, quando montamos uma topologia ou uma rede e apenas configuramos as interfaces, por padrão elas terão alcance somente às suas redes **diretamente conectadas**. Para que possamos alcançar as redes remotas precisaremos configurar um protocolo de roteamento dinâmico ou utilizar rotas estáticas para que o roteador aprenda como chegar a cada rede de destino.

Vamos estudar nesse capítulo como configurar o roteamento através de rotas estáticas.

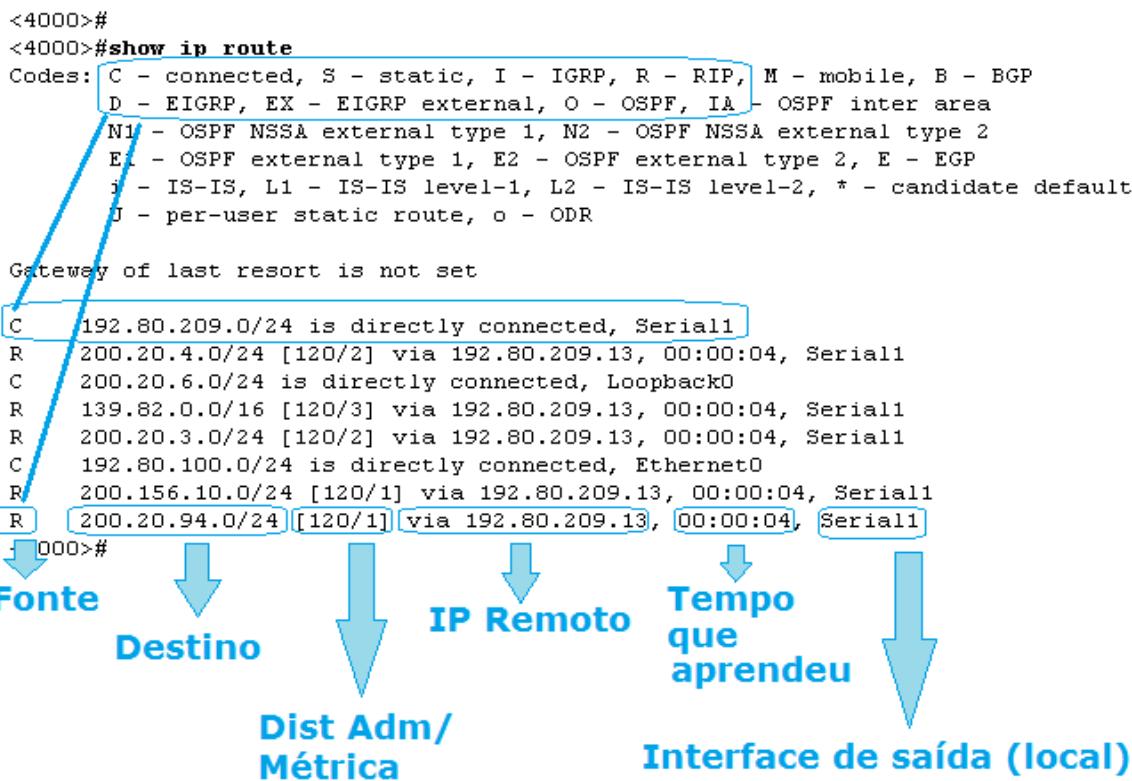
Agora vamos a seguir estudar mais sobre a tabela de roteamento e como os roteadores processam os pacotes IP para encaminhá-los através da rede.

### 2.3 Analisando a Tabela de Roteamento

Como estudamos anteriormente, o processo de roteamento, seja ele estático ou dinâmico, tem a finalidade de instalar uma "rota" para um determinado "destino" na "tabela de roteamento IP" do roteador.

Antes de continuarmos a estudar como inserir rotas vamos fazer um estudo do que a tabela de roteamento nos fornece de informações, pois saber interpretar essa tabela é fundamental para sua vida prática e para o exame.

Veja a figura abaixo com a saída do comando "**show ip route**".



Note que logo após o comando temos uma legenda com o tipo a fonte de aprendizado daquela rota, veja os principais abaixo:

- **C**: diretamente conectada (uma rede IP configurada em uma interface que está UP/UP).
- **S**: rota inserida manualmente ou estática.
- **R**: rota aprendida pelo RIP.
- **D**: rota aprendida pelo EIGRP.
- **O**: rota aprendida pelo OSPF.

Logo abaixo temos a frase "**Gateway of last resort is not set**", a qual significa que não existe **rota padrão** (gateway) configurada. Nesse caso se chegar um pacote com um destino que **não esteja especificado** na tabela, esse **pacote será descartado** ou "dropado". Quando temos uma rota padrão especificada nesse campo é especificado o IP do gateway.

Logo abaixo do gateway padrão temos as rotas, sendo que na primeira linha temos uma rota para uma rede diretamente conectada, nesse caso o roteador avisa com a frase "**is directly connected**" e depois da vírgula indica qual interface ela está conectada.

Quando vemos esse tipo de rota quer dizer que aquela interface, nesse exemplo a serial1, tem um IP da rede 192.80.209.0 configurado nela e a interface está UP/UP. Para ver o IP que está configurado nela podemos utilizar o "**show ip interface brief**". Nas versões 15 do IOS da Cisco ele apresenta também uma rota chamada local (indicada por um L) com o IP da interface com máscara /32 para facilitar o troubleshooting.

Agora vamos para a última linha do comando que está em destaque, onde o roteador mostra uma rota aprendida pelo RIP.

Note que quando a saída da tabela de roteamento é referente a um protocolo de roteamento dinâmico muitas outras informações são mostradas. Temos os seguintes parâmetros:

- **200.20.94.0 /24**: rede de destino.
- **[120/1]**: 120 é a distância administrativa e 1 é a métrica (veremos mais tarde o que significam esses parâmetros).
- **Via 192.80.209.13**: é o IP do próximo salto, ou seja, o IP do vizinho por onde o roteador enviará os pacotes destinados à rede 200.20.94.0/24.
- **00:00:04**: tempo em que essa rota foi aprendida, nesse exemplo a quatro segundos.
- **Serial 1**: a interface local que será utilizada para encaminhar os pacotes à rede 200.20.94.0/24. Com esse parâmetro e o "via 192.80.209.13 sabemos que a interface serial 1 do roteador local, o qual você executou o show ip route, está conectado com um roteador com IP 192.80.209.13.

Além disso, em algumas situações quando temos sub-rede você pode ter rotas **primárias** e **secundárias**.

As rotas primárias indicam somente que uma rede class A, B ou C foi "subnetada" (subnetted ou quebrada em sub-redes), não sendo utilizada para encaminhar rotas.

Somente as rotas com uma letra na frente são utilizadas para encaminhamento. Veja o exemplo na figura abaixo e perceba que acima da rota com o **R** indicando que ela foi aprendida pelo RIP temos a frase "**192.168.1.0/30 is subnetted, 3 subnets**", a qual é somente uma indicação que esta rede foi dividida em sub-redes e temos 3 sub-redes, a 192.168.1.0, 192.168.1.4 e 192.168.1.8.

```

RouterC#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

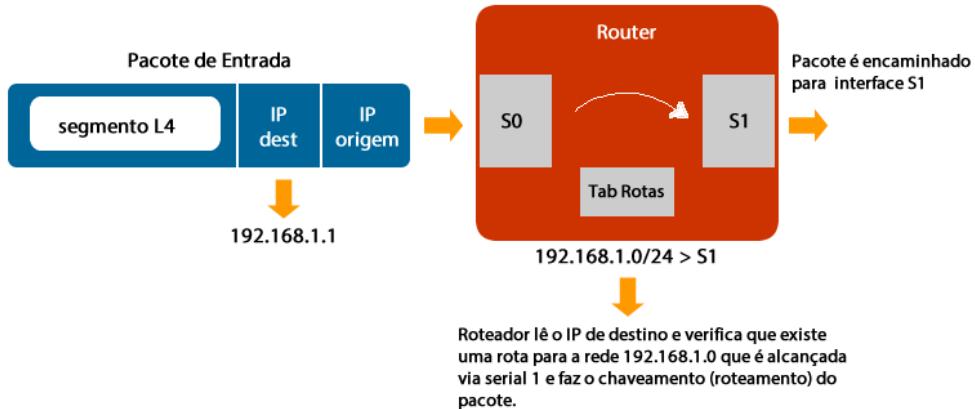
192.168.1.0/30 is subnetted, 3 subnets
R    192.168.1.0 [120/1] via 192.168.1.6, 00:00:06, Serial0/0
      [120/1] via 192.168.1.9, 00:00:04, Serial0/1
C    192.168.1.4 is directly connected, Serial0/0
C    192.168.1.8 is directly connected, Serial0/1
RouterC#

```

A seguir vamos estudar como o roteador usa as informações da tabela de roteamento para encaminhar os pacotes. O processo clássico é chamado de Process Switching, porém existem processos mais rápidos como o Fast Switching e o CEF.

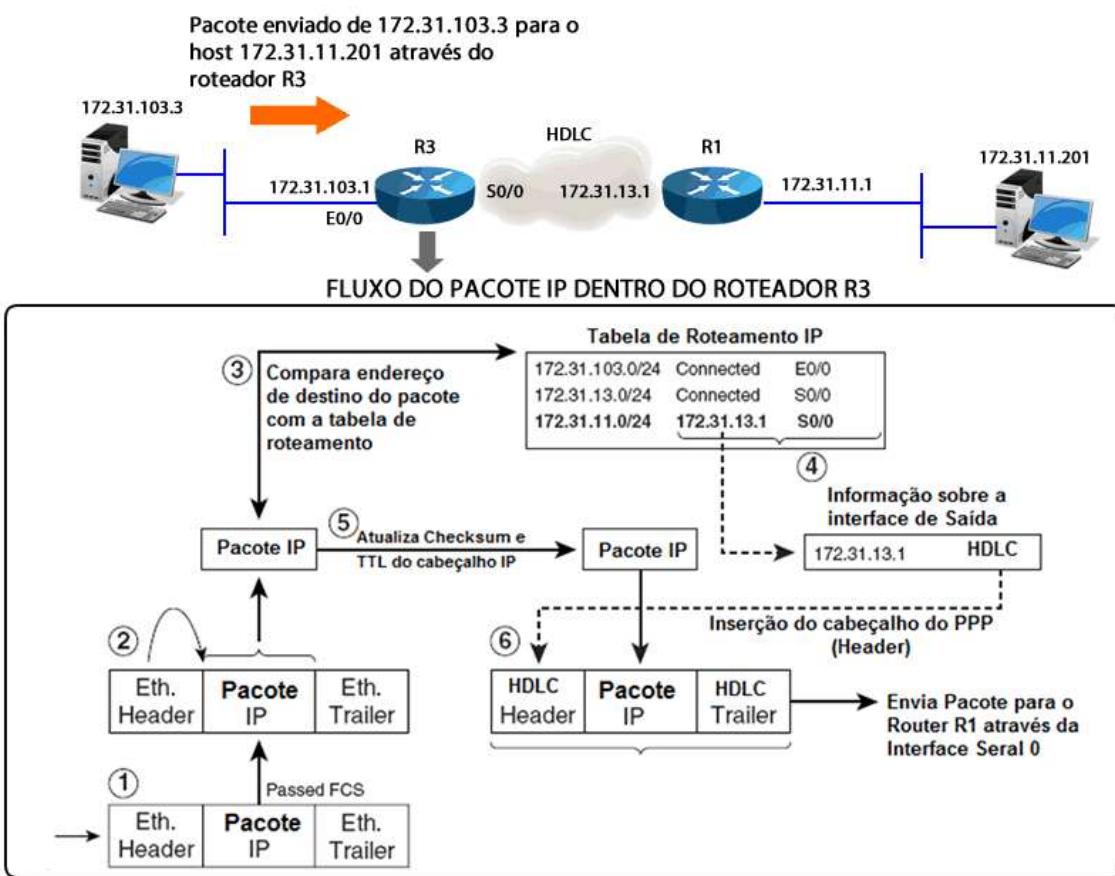
## 2.4 Process Switching, Fast Switching e CEF

O processo de roteamento clássico é a ação do roteador receber um pacote, analisar seu endereço IP de destino, verificar em sua tabela de roteamento se existe uma rota, remontar o quadro de camada 2 e encaminhar esse pacote pela interface de saída definida nessa rota. Veja a figura abaixo com um diagrama resumido do processo de roteamento.



Se não houver uma rota explícita definida na tabela de roteamento, o roteador verifica se existe uma rota padrão (Gateway of last resort) e encaminha para a saída definida nessa rota ou então, se não houver a rota padrão configurada, ele simplesmente descarta o pacote e envia uma informação de destino inalcançável (destination unreachable) através do ICMP para o host de origem.

Este é o processo mais simples de roteamento chamado **Process Switching**, onde a CPU é envolvida a todo o momento para ler e decidir para que interface encaminhar o pacote IP. Veja o fluxo detalhado do encaminhamento de um pacote utilizando o Process Switching na figura abaixo. Nesse exemplo um computador conectado à LAN do R3 envia um pacote para o host conectado à LAN do R1.



Os passos que o roteador segue para fazer o roteamento por padrão seguem a sequência conforme mostrado na figura. Veja abaixo a explicação de cada passo:

- O quadro de camada 2 é recebido pela Interface Eth 0/0 do roteador e se o FCS (checksum de camada 2) estiver correto ele é processado, caso contrário ele é descartado. Vamos supor que o quadro está com o FCS correto e passa para a próxima etapa.
- Agora o quadro de camada 2 (Ethernet) é removido e o pacote IP é enviado para a camada de rede do roteador R3.
- O roteador R3 verifica o **IP de destino** do pacote IP e **procura pelo prefixo mais específico** na tabela de roteamento para poder encaminhar o pacote para uma interface de saída, ou seja, verifica a melhor rota para encaminhar o pacote sempre pela máscara de sub-rede ou prefixo **mais longo** (longest match - quanto mais bits "1" na máscara melhor o caminho). O pacote então é encaminhado para a interface de saída. Como o IP de destino é o 172.31.11.201 o roteador verifica que há uma rota de saída através da sua serial 0 que está diretamente conectada ao IP 172.31.13.1 do seu roteador vizinho.
- Como foi encontrada uma saída viável para o pacote IP um novo quadro de camada 2 precisa ser remontado conforme o tipo de interface de saída (nesse caso utilizando o encapsulamento conforme protocolo HDLC). Nessa etapa o roteador verifica e prepara as informações de camada 2 para a etapa final de encapsulamento e envio pela camada física.
- O pacote IP é atualizado com o incremento do campo de TTL e tem seu checksum recalculado, pois o TTL foi alterado.
- O pacote IP é encapsulado dentro do novo quadro de camada 2 (nesse caso um quadro HDLC) e encaminhado para a camada física através da interface serial 0.

O item 6 é conhecido também como "frame rewrite", ou seja, quando o roteador reescreve o quadro de camada-2 com as novas informações conforme o link de próximo salto do pacote IP.

Uma vez recebida à informação pelo roteador R1 ele seguirá o mesmo processo para encaminhar o pacote recebido na interface serial para sua LAN, para que assim o host de destino seja alcançado.

Além do processo mostrado anteriormente, existem outros dois processos mais rápidos e econômicos em termos de utilização da CPU que podem ser utilizados pelos roteadores Cisco:

- **Fast Switching**
- **CEF (Cisco Express Forwarding)**

O **Fast Switching** foi criado para agilizar o processo de verificação do melhor caminho e encaminhamento para a interface de saída quando temos fluxos repetidos de pacotes, pois quando temos pacotes de uma mesma origem e mesmo destino a consulta feita é igual e repetida. Portanto, o primeiro pacote aciona a criação de uma entrada no **Fast-switching cache** (router cache) que agiliza o processo de encaminhamento, porém continua utilizando a CPU para essas verificações.

Já quando utilizamos o **CEF (Cisco Express Forwarding)** o roteador cria o **Forwarding Information Base (FIB)**, a qual é uma base de dados que contém TODAS as rotas conhecidas. Esta tabela ou banco de dados contém tudo o que o roteador precisa saber para encaminhar um pacote e agiliza muito o processo de roteamento.

Se formos fazer uma comparação bem simplificada é como se o roteador utilizando o **Process Switching** tivesse que calcular manualmente tudo o que ele precisa para fazer o encaminhamento dos pacotes, isso tudo para cada pacote recebido, ou seja, um a um. Já com o **Fast Switching** ele utiliza uma memória de cálculo, onde ele faz a conta uma vez quando recebe o primeiro pacote e depois lembra as respostas para os próximos pacotes que vêm na sequência (cache). Por último, quando o roteador utiliza o **CEF** para encaminhar os pacotes é como se ele tivesse uma planilha do Excel e quando os números são inseridos nas células essa planilha já dá o resultado calculado, acelerando o processo como um todo.

Portanto tanto o CEF quanto o Fast Switching visam economizar tempo e processamento nas etapas 3 e 4 do processo de roteamento, ou seja, na pesquisa da melhor rota na tabela de roteamento e também no levantamento dos dados para montagem do quadro de camada 2.

**Lembrete importante:** Seja qual for o processo utilizado sempre a escolha da melhor rota é feita através do **prefixo mais longo** ou **longest match**.

## 2.5 Escolha da Melhor Rota – Regra do “Longest Match”

Nós vimos no tópico anterior que a escolha da melhor rota é feita através do **prefixo mais longo** ou **longest match**.

Mas antes de analisarmos você deve lembrar que uma "rota" em uma rede IP versão 4 nada mais é que o endereço de rede com uma máscara de sub-rede. Lembre-se que no capítulo 5 estudamos que uma rede IP é dividida em:

- **Endereço de Rede ou Subrede** → primeiro IP de uma rede ou sub-rede IP (todos os bits de host estão em zero).
- **IPs Válidos** (endereço de host ou hosts válidos) → do segundo ao penúltimo IP de uma rede ou sub-rede IP.
- **Endereço de Broadcast** → último IP de uma rede ou sub-rede IP (todos os bits de host estão em um).

Portanto, quando você tem em uma rede LAN configurados computadores com IPs classe C 192.168.1.1, 192.168.1.2, 192.168.1.3 e 192.168.1.10 com máscara 255.255.255.0 (/24) você deve ter nos roteadores uma rota para a rede 192.168.1.0 /24 que no final apontem para a Interface de LAN que esses hosts estão conectados.

Porém, se em um dos roteadores tivermos as seguintes rotas abaixo, para qual das interfaces o roteador irá encaminhar os pacotes se ele receber um pacote com IP de destino 192.168.1.10?

- 192.168.1.0 255.255.255.0 (/24): serial 0
- 192.168.1.0. 255.255.255.240 (/28): serial 1

É nesse tipo de situação que usamos a regra do prefixo mais longo, nesse caso apesar do IP 192.168.1.10 estar contido nas duas redes apresentadas o roteador irá encaminhar para a **serial 1**, pois ela tem o **prefixo mais longo**.

É como se comparássemos assim, você precisa encontrar uma pessoa e tem 3 informações:

- 1) O Fulano da Silva está no Brasil.
- 2) O Fulano da Silva está no Paraná.
- 3) O Fulano da Silva está na Av. Sete de Setembro, 3728, conjunto 500, em Curitiba Paraná.

Qual das três você escolheria para encontrar o Fulano? Com certeza a terceira.

A mesma análise é para a escolha através do prefixo mais longo, pois na rota 192.168.1.0 /24 temos os IPs de 192.168.1.1 até 192.168.1.254, totalizando 254 hosts, porém com a rota 192.168.1.0 /28 temos apenas os IPs de 192.168.1.1 até 192.168.1.14, totalizando apenas 14 hosts, por isso essa informação é mais confiável, pois há **maior probabilidade de encontrarmos** o host nessa rede de menor tamanho.

## 2.6 Questões sobre Processo de Roteamento e Desempenho

Nesse ponto você já deve ter notado que o processo de roteamento não é tão simples, não é só encaminhar um pacote pura e simplesmente.

Note que o roteador precisa fazer alguns processos que consomem memória RAM, por exemplo, armazenar os pacotes recebidos para serem processados, e também processador (CPU), por exemplo, ler o endereço de destino de cada pacote para saber qual interface de saída deve encaminhá-lo se estiver utilizando Process Switching.

Ao receber um quadro de camada 2 o roteador deve ler o endereço MAC e decidir se deve processar e encaminhar aquele pacote, para isso ele deve verificar se seu endereço MAC está contido no campo de endereço de destino do quadro. Se estiver, antes de processar o conteúdo dos dados que geralmente é um pacote IP, o roteador deve ler o campo FCS e verificar se o quadro está íntegro, pois se houver erros esse quadro deve ser descartado.

Um detalhe, se o MAC de destino for um broadcast o roteador também será obrigado a processar o pacote IP.

Após essa fase, supondo que o quadro tinha o MAC de destino igual ao do roteador e estava íntegro o roteador deve descartar o cabeçalho de camada 2 e gravar esse pacote em um espaço de memória RAM chamado buffer ou fila de entrada para ser processado.

Ao processar o pacote IP o roteador deve verificar o checksum, que é similar ao FCS e verificar se o pacote está íntegro. Caso contenha erros o pacote será descartado, senão será processado. O processamento se dá com a leitura do endereço de destino do pacote IP.

Se o IP de destino for igual ao configurado em uma das interfaces do roteador ele enviará para as camadas superiores para que a informação seja tratada. Agora, se o endereço for diferente o roteador terá que analisar a tabela de roteamento, usando a regra do “**longest match**” e escolher uma interface de saída para fazer o encaminhamento.

Uma vez definida a interface de saída o roteador precisará inserir o pacote IP em um novo quadro de camada 2, conforme protocolo configurado na interface de saída, por exemplo, um quadro HDLC se for uma interface serial.

Caso a interface de saída seja padrão ethernet, por exemplo, uma interface Gigabit via fibra óptica, antes de montar e enviar o quadro o roteador precisará fazer uma solicitação ARP pelo MAC do roteador remoto, chamado se “next hop” ou “próximo salto”, para aí sim montar o quadro de camada 2 e encaminhar o pacote.

Se formos resumir todo esse trabalho em passos temos:

- Passo 1: roteador recebe quadro de camada 2 através de uma de suas interfaces.
- Passo 2: toma decisão sobre processar ou não o quadro de entrada recebido por uma das interfaces.
- Passo 3: desencapsula o pacote IP (remover o cabeçalho de camada 2).
- Passo 4: escolhe para onde encaminhar o pacote (interface de saída).
- Passo 5: faz o frame rewrite, encapsulando o pacote conforme quadro de camada 2 da interface de saída.
- Passo 6: transmite o quadro no meio físico (envio dos bits).

Todo esse processamento consome tempo de uso do processador dos roteadores (ciclos de CPU) e podem congestionar o dispositivo elevando o uso da CPU de tal maneira que o roteador pode ficar lento ou até mesmo parar de funcionar.

Por esse motivo se você procurar especificações de capacidade de roteadores normalmente ela virá expressa em **pacotes por segundo (PPS – Packet per Second)** e não em bits por segundo (bps).

Devido a esses problemas potenciais os roteadores Cisco podem ser configurados com diferentes metodologias de encaminhamento, conforme estudamos anteriormente, tais como o CEF e Fast Switching, pois essas tecnologias visam minimizar o impacto do roteamento sobre a CPU dos roteadores.

Se colocarmos em ordem de desempenho o CEF vem em primeiro lugar, depois o Fast Switching e por último o process switching, porém a escolha de qual usar depende de vários fatores que não serão tratados nesse curso devido a sua complexidade.

O comando “**show processes**” ou “**show processes cpu**” você pode verificar quando de CPU está sendo utilizado pelo roteador em porcentagem. O normal é esse índice de utilização estar entre 20% e 25% ou abaixo. Veja exemplo abaixo.

```
R1#show processes
CPU utilization for five seconds: 1%/100%; one minute: 0%; five minutes: 0%
 PID QTy      PC Runtime (ms)    Invoked   uSecs   Stacks  TTY Process
   1 Cwe 6381F45C          12        42     285 3968/6000    0 Chunk Manager
   2 Csp 60610EFC         404      1584     255 2432/3000    0 Load Meter
### Saídas Omitidas ###
```

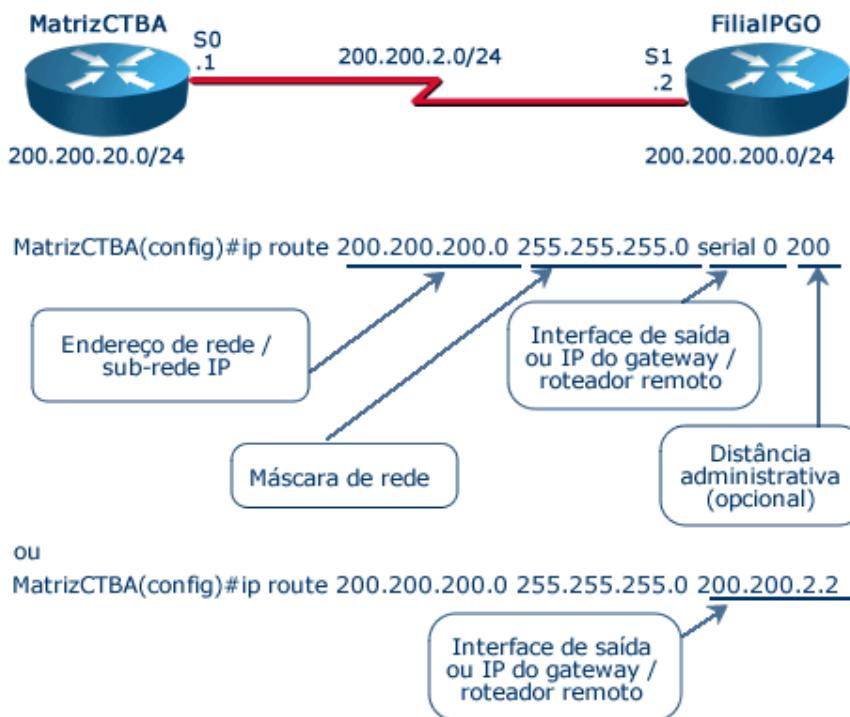
Além da sobrecarga de recebimento de pacotes e forma de processamento outros motivos podem fazer o uso da CPU aumentar, como o já citado comando “debug”.

### 3 Configurando e Verificando Rotas Estáticas

O método mais simples e econômico de fazer a configuração de roteamento nos roteadores Cisco é utilizando Rotas Estáticas, pois não há nenhuma necessidade de cálculo ou processamento por parte do roteador, uma vez que o administrador já definiu os melhores caminhos e simplesmente instruiu ao roteador via o comando “**ip route**” como os destinos remotos podem ser alcançados.

As rotas estáticas então nada são que entradas manuais feitas por um administrador de redes e utilizadas principalmente em redes stub (redes de apenas uma saída), para configuração de um gateway default ou em DDNs (dial-on-demand routing).

A figura abaixo mostra a sintaxe para configuração de uma rota estática.



Nesse exemplo o roteador "MatrizCTBA" aprendeu estaticamente uma rota para a rede LAN do roteador "FilialPGO" (rede de destino 200.200.200.0/24), a qual pode ser encontrada via a "serial 0", esse parâmetro poderia ser ainda o endereço IP da serial do roteador vizinho.

A distância administrativa é opcional e se não for configurada nas rotas estáticas o valor padrão 1 é automaticamente utilizado quando a rota é configurada com o próximo salto sendo um endereço IP.

Para verificar a configuração utilize o comando "show ip route" conforme exemplo abaixo:

```
MatrizCTBA(config)#ip route 200.200.200.0 255.255.255.0 serial 0 200
MatrizCTBA(config)#^Z
MatrizCTBA#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
    IS-IS inter area
    * - candidate default, U - per-user static route, o - ODR
    P - periodic downloaded static route
Gateway of last resort is not set
S 200.200.200.0 [200/0] via Serial 0
C 200.200.2.0 is directly connected, Serial 0
C 200.200.20.0 is directly connected, FastEthernet 0
MatrizCTBA#
```

Veja a primeira linha em destaque na tabela de roteamento iniciando com S significando que é uma entrada estática, a seguir entre colchetes temos distância administrativa (200) e a métrica (0) respectivamente, logo após o roteador informa por qual interface ou gateway você alcança a rota em questão (via Serial 0).

A distância administrativa de uma rota diretamente conectada é zero e da rota estática depende da configuração do next-hop ser um gateway remoto (endereço IP) ou uma interface local. No caso da referência ser um endereço de próximo salto a distância padrão será configurada com o valor um, já quando apontamos uma rota para uma interface local de saída ela terá o valor igual ao de uma interface conectada, ou seja, valor padrão igual à zero.

Ainda com referência a saída do comando "show ip route" acima, note que o roteador informa que o "**Gateway of last resort is not set**", ou seja, não existe rota padrão anunciada. Essa informação é muito importante e significa que se um pacote com rede de destino diferente das redes 200.200.200.0, 200.200.2.0 ou 200.200.20.0 for enviado ao roteador, ele irá ignorar o pacote e o descartará.

Para a configuração de um gateway default você pode utilizar o comando:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 interface/gateway
```

A rede 0.0.0.0 com a máscara 0.0.0.0 representa a Internet. O gateway default também é chamado de "**Gateway of last resort**", como vimos acima, pois se não há entrada para a rede de destino ele é a **última opção de envio do pacote**.

Lembre-se que se não houver um gateway padrão configurado e nenhuma entrada na tabela de roteamento para a rede de destino o pacote será **descartado**. Exemplo de configuração:

```
R1720A(config)#ip route 0.0.0.0 0.0.0.0 10.0.1.20
```

Outra configuração interessante é a criação de uma rota para **um host específico**, por exemplo, você deseja alcançar um host de IP 200.150.160.1/24 que está conectado a sua interface fastethernet mas a rede dele não está presente em sua tabela de roteamento, o seguinte comando pode ser utilizado:

```
R1720A(config)#ip route 200.150.160.1 255.255.255.255 fastEthernet 0
```

Note que a máscara de rede utilizada foi uma /32 e não a /24, pois a /32 é a qual especifica um host único, conforme já estudamos.

### 3.1 Opções do Comando IP-Route

Vamos analisar as opções do comando IP Route abaixo.

```
Dltec-FW-GW(config)#ip route 10.0.0.0 255.255.255.0 192.168.1.1 ?
<1-255>      Distance metric for this route
name          Specify name of the next hop
permanent     permanent route
tag           Set tag for this route
track         Install route depending on tracked item
<cr>
```

O primeiro **<1-255>** já estudamos, que é a distância administrativa, vamos ver exemplo do uso no item sobre rotas flutuantes.

O “**name**” é apenas uma referência, assim como o **description** das interfaces.

Já a opção “**permanent**” cria uma rota permanente, ou seja, se você referenciar a rota a uma interface, por exemplo, e essa interface cair a rota continuará na tabela, porém você vai ter problemas com esse destino, pois esse comando não é “mágico”, ou seja, se a rota está fora os pacotes serão dropados (descartados).

A opção “**tag**” coloca uma marcação na rota, normalmente utilizada pelos CCNPs na configuração de “route-maps”.

E por último temos a opção “**track**” que pode ser utilizada em conjunto com o IP SLA para ativar a rota quando uma determinada condição ocorrer, porém o IP SLA será estudado no ICND-2.

A seguir vamos estudar um exemplo ilustrativo de configuração do roteamento de uma pequena rede com apenas dois roteadores via rotas estáticas.

### 3.2 Exemplo de Configuração - Rota Estática

O exercício que faremos agora será simular a configuração de um laboratório com dois roteadores e dois roteadores partindo do “zero”, ou seja, como se abrissemos a caixa dos roteadores novos para configurá-los com o mínimo possível de comandos gerais.

Para iniciar temos que pensar primeiro nas redes IP que utilizaremos para configurar as interfaces. Teremos uma rede LAN via Fastethernet em cada roteador e uma rede WAN interligando os roteadores via interface Serial, totalizando 3 redes IP.

Vamos escolher redes Classe C privadas para o laboratório, podendo ser a 192.168.1.0 e 192.168.2.0 para as redes LAN, e para a rede WAN vamos utilizar a rede 192.168.10.0. Veja na figura a seguir a escolha dos endereços IP por interface.



Vamos considerar que o laboratório já foi montado e corretamente conectado com os devidos cabos, sendo que na conexão serial do roteador R1 foi colocado um cabo DCE e o DTE foi conectado ao roteador R2. Além disso, utilizaremos o protocolo HDLC nas interfaces seriais.

Para as interfaces de LAN, as Fastethernets foram conectadas com cabos diretos entre as portas Fast 0/0 dos roteadores e as Fasts 0/1 dos switches.

Estamos prontos para ligar os roteadores, clique aqui para ver a saída do comando "show ip route" no roteador R1 sem configuração abaixo. Note que não existe rota na tabela de roteamento.

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route
```

Gateway of last resort is not set

Agora vamos configurar as interfaces seriais e Fastethernet do roteador R1, conforme configurações abaixo.

```
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
*Mar 1 00:12:28.363: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:12:29.363: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to up
R1(config-if)#int s0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#clock rate 128000
R1(config-if)#no shut
R1(config-if)#
*Mar 1 00:13:13.907: %LINK-3-UPDOWN: Interface Serial0, changed state to up
*Mar 1 00:13:14.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to up
*Mar 1 00:13:36.323: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to down
```

```
R1(config-if)#end
R1#
*Mar 1 00:14:02.079: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip route
R1#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

C      192.168.1.0/24 is directly connected, FastEthernet0/0
```

R1#

Note que a interface Fast 0/0 ficou "up", enquanto a serial ficou "Down", isto se deve ao fato de não termos configurado o roteador da outra ponta, o R2. Por esse motivo, apenas a rota para a rede LAN aparece na tabela de roteamento como diretamente conectada.

O próximo passo será configurar as interfaces do roteador R2, veja as configurações e show ip route abaixo.

```
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R2
R2(config)#int f0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#
00:06:02: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
00:06:03: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
R2(config-if)#int s0
R2(config-if)#ip address 192.168.10.2 255.255.255.0
R2(config-if)#clock rate 128000
R2(config-if)#no shut
R2(config-if)#
00:06:35: %LINK-3-UPDOWN: Interface Serial0, changed state to up
00:06:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state
to up
R2(config-if)#end
R2#
00:07:48: %SYS-5-CONFIG_I: Configured from console by console
R2#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route
```

Gateway of last resort is not set

```
C      192.168.10.0/24 is directly connected, Serial0
C      192.168.2.0/24 is directly connected, FastEthernet0/0
R2#
```

Com a interface serial do roteador R2 configurada, ambas as interfaces subiram e na tabela de roteamento de R2 apareceram as duas rotas diretamente conectadas, a rede da serial e a rede da Fast.

Vamos ver a saída do comando para R1 e verificar se o mesmo ocorreu. Clique aqui e veja a saída do comando para o roteador R1.

```
R1#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route
```

Gateway of last resort is not set

```
C      192.168.10.0/24 is directly connected, Serial0
C      192.168.1.0/24 is directly connected, FastEthernet0/0
R1#
```

Comparando as tabelas de roteamento vemos que os roteadores R1 e R2 conhecem a rota 192.168.10.0, a qual é a rede WAN comum aos dois roteadores. Porém, um não conhece a rede LAN do outro.

No cenário atual se um micro conectado ao switch da rede LAN do roteador 1 tentar trocar arquivos ou mensagens com um micro do switch 2 ele não terá sucesso, pois os roteadores não sabem como encontrar a rede LAN um do outro.

Vamos agora configurar uma rota estática em cada roteador ensinando o caminho para as redes LAN um do outro. Note que eles conseguem alcançar as redes LAN um do outro através de suas interfaces seriais e essa facilidade que utilizaremos abaixo para fazer a configuração toda a partir de R1 via Telnet.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
! entrando com a rota para a LAN de R2
R1(config)#ip route 192.168.2.0 255.255.255.0 serial 0
R1(config)#end
R1#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route
```

Gateway of last resort is not set

```
C      192.168.10.0/24 is directly connected, Serial0
C      192.168.1.0/24 is directly connected, FastEthernet0/0
S      192.168.2.0/24 is directly connected, Serial0
```



```
R1#
R1#telnet 192.168.10.2
Trying 192.168.10.2 ... Open

User Access Verification
Password:
R2>enable
Password:
R2#
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
! Entrando com a rota para a LAN de R1
R2(config)#ip route 192.168.1.0 255.255.255.0 serial 0
R2(config)#end
R2#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, Serial0
S    192.168.1.0/24 is directly connected, Serial0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

R2#

Note que após entrarmos com as redes LAN de maneira estática nos routers, ela aparece no comando "show ip route" diferenciada com um "S" na frente, o que representa "static" ou estático em português.

Agora vamos testar com o comando ping se os roteadores conseguem alcançar a LAN remota, conforme saídas abaixo.

```
R2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/20/28 ms
R2#
R1#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms
R1#
```

Podemos perceber que com as rotas estáticas o ping funcionou 100% em ambos os roteadores. O ponto de exclamação no ping significa que o Echo Req enviado teve uma resposta bem sucedida. Se desse problema poderia aparecer um ponto (.) se o tempo de espera pela resposta expirar ou a letra U se o destino for inalcançável ou algum filtro no destino está aplicado impedindo uma resposta do host.

### 3.3 O que é Melhor Interface ou IP na Rota Estática?

Nessa altura desse tópico de rotas estáticas você pode ter ficado com a pergunta: "**O que é melhor configurar como saída então? Um IP do próximo salto ou uma interface local?**".

Em questões práticas no exame de certificação CCENT e/ou CCNA você deve configurar com o que for solicitado, se não for especificado nada valem os dois formatos.

Na prática, quando utilizamos a interface local de saída o roteamento tem menos passos de processamento, pois o roteador não precisa resolver ou verificar quem é a interface de saída daquele IP.

Por exemplo, se configurarmos "**ip route 192.168.1.0 255.255.255.0 192.168.10.10**" toda vez que chegar um pacote cujo destino é a rede 192.168.1.0 ele deve ser encaminhado ao IP 192.168.10.10, porém o roteador não encaminha a um IP e sim para uma Interface, portanto antes de encaminhar o roteador terá que descobrir para qual interface possui a rede que o IP 192.168.10.10 pertence.

Ao passo que se configurarmos "**ip route 192.168.1.0 255.255.255.0 serial 0**" o roteador não precisará fazer a análise anterior, pois ele já sabe que precisará encaminhar para a interface serial 0, economizando um passo para encaminhar o pacote.

Existem também restrições para apontar para uma serial local quando temos uma rede Broadcast, por exemplo, uma rede Ethernet, Fast ou Giga.

Em uma rede fast temos um switch e diversos hosts na mesma LAN, se criarmos a rota "ip route 102.10.1.0 255.255.255.240 fast 0/0" o roteador encaminhar pacotes para a rede 102.10.1.0 /28 para a porta fast que chega a um switch e temos diversos hosts nessa rede, portanto quem será responsável por receber e encaminhar esses pacotes? Por isso que no caso de rotas estáticas que tem saída em uma **rede LAN** o correto é utilizar o **IP do próximo salto** como destino, assim teremos certeza que o vizinho correto irá receber os pacotes e encaminhá-los até a rede de destino.

Lembre-se que o IP do próximo salto **SEMPRE** será um IP de um roteador vizinho pertencente a uma rede diretamente conectada, não utiliza IPs de redes remotas.

Outro ponto interessante é que ao configurarmos rotas estáticas apontando para interfaces o Cisco IOS remove e insere a rota automaticamente conforme a interface de saída fica UP ou Down. Você pode fazer com que a rota nunca saia da tabela de roteamento com a opção "permanent" no final do comando, veja exemplo a seguir.

```
R1(config)#ip route 10.0.0.0 255.0.0.0 fast 0/0 ?
<1-255>      Distance metric for this route
A.B.C.D      Forwarding router's address
DHCP         Default Gateway obtained from DHCP
multicast    multicast route
name        Specify name of the next hop
permanent   permanent route
tag          Set tag for this route
track       Install route depending on tracked item
<cr>
```

```
R1(config)#ip route 10.0.0.0 255.0.0.0 fast 0/0 permanent
```

### 3.4 Configurando uma Rota Padrão (Default-Gateway)

A rota padrão ou Gateway of last resort nos roteadores tem a função de ser o IP para qual o equipamento vai enviar os pacotes quando não houver uma entrada na tabela de roteamento.

Quando um roteador recebe um pacote para encaminhar ele analisa a rede de destino e busca em sua tabela de roteamento uma rota correspondente. Sem uma rota padrão o roteador irá buscar a rota para determinado endereço em sua tabela de roteamento e caso não seja encontrada, o pacote será descartado.

Por esse motivo a rota padrão é intitulada muitas vezes como a “**saída para internet**” ou **saída padrão**, pois quando não há rota específica para a rede de destino o pacote é encaminhado para ela.

Nos roteadores ela deve ser configurada com uma rota estática para a rede 0.0.0.0 com máscara 0.0.0.0, ou seja, todos os IP's menos os que ele conhece na tabela de roteamento.

Para a configuração de um gateway default você pode utilizar o comando visto nos tópicos anteriores “ip route 0.0.0.0 0.0.0.0 interface/gateway”. Abaixo segue mais um exemplo prático onde o gateway default é o IP 10.0.1.20:

```
R1720A(config)#ip route 0.0.0.0 0.0.0.0 10.0.1.20
```

Na tabela de roteamento você reconhecerá a rota padrão com um asterisco (\*) ao lado dela, além de aparecer o IP no campo “Gateway of last resort is...”, conforme figura ao lado.

```
R1720A(config)#ip route 0.0.0.0 0.0.0.0 10.0.1.20  
R1720A(config)#end
```

```
R1720A#show ip route  
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
      * - candidate default, U - per-user static route, o - ODR  
      P - periodic downloaded static route  
Gateway of last resort is 10.0.1.20 to network 0.0.0.0  
    10.0.0.0/24 is subnetted, 2 subnets  
C        10.0.1.0 is directly connected, FastEthernet0/0  
S*   0.0.0.0/0 [1/0] via 10.0.1.20  
R1720A#
```

O maior cuidado que se deve ter com a configuração das rotas padrões é a de não causar **loops de roteamento** entre dois roteadores. Por exemplo, se em um roteador você criar uma rota padrão apontando para a interface do vizinho e no vizinho criar uma rota apontando para o primeiro router, quando um dos dois enviar um pacote não conhecido nas tabelas de roteamento dos dois, um ficará enviando para o outro o mesmo pacote até que o TTL padrão configurado pelo protocolo IP seja esgotado.

Apesar de ser um problema simples acontece muito na prática.

#### 3.4.1 Uso do Comando ip default-gateway

O comando “**ip default-gateway**” difere dos outros dois comandos apresentados, pois ele deve ser usado apenas quando o roteamento IP estiver desativado no roteador Cisco, ou seja, o comando “no ip routing” foi executado em modo de configuração global.

O exemplo a seguir mostra a configuração do endereço IP 172.16.15.4 como a rota padrão:

```
Switch(config)#ip default-gateway 172.16.15.4
```

Lembre-se que esse comando é utilizado nos switches de camada-2 para definir o gateway padrão.

### 3.5 Rota Estática Flutuante

As rotas estáticas flutuantes são utilizadas para servirem como backup de uma rota principal, a qual pode ser uma outra rota estática ou uma rota aprendida através de um protocolo de roteamento dinâmico.

O segredo da configuração de rotas estáticas flutuantes ou “floating static” é o uso correto do parâmetro “administrative distance” (AD ou distância administrativa) que existe na configuração das rotas estáticas no comando “ip route”.

Para que a rota seja flutuante ou backup sua distância administrativa deve ser maior que o AD da rota principal, pois quanto menor a distância administrativa melhor será a rota para o roteador (será estudado mais a fundo no capítulo 9 – Roteamento Dinâmico e RIPv2).

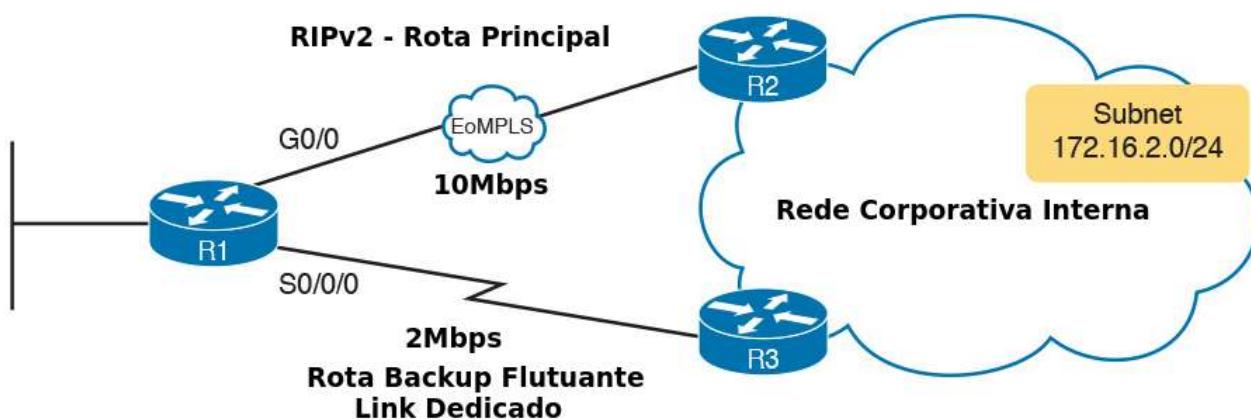
Por exemplo, por padrão o AD de uma rota estática que aponta para um IP do próximo salto é 1, se temos que criar uma rota flutuante para o mesmo destino basta colocar o AD dessa segunda rota maior que 1. Veja abaixo.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0
R1(config)#ip route 0.0.0.0 0.0.0.0 serial0/1 100
```

Nesse exemplo teremos a rota principal para a Internet apontando para serial0/0 e a rota apontando para serial0/1 ficará como stand-by, pois seu AD é 100 e maior que da rota principal que é 1.

Caso a rota principal via interface serial0/0 caia, imediatamente o roteador subirá a saída para a Internet via serial0/1, a qual estava configurada, mas não ativa na tabela de roteamento, por isso o nome “flutuante”.

Esse mesmo tipo de configuração pode ser utilizada em conjunto com protocolos de roteamento dinâmico como RIP (AD 120), EIGRP (AD 90) e OSPF (AD 110). Veja exemplo na figura abaixo.



Como o RIP tem distância administrativa 120, para criar uma rota backup flutuante via serial 0/0/0 podemos utilizar um AD 130, por exemplo. Veja a configuração abaixo:

```
R1(config)#ip route 172.16.2.0 255.255.255.0 s0/0/0 130
```

Se a rota do RIP cair vamos ter as seguintes saídas na tabela de roteamento.

```
R1# show ip route static
! Saída omitida...

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
S         172.16.2.0/24 is directly connected, Serial0/0/0

R1# show ip route 172.16.2.0
Routing entry for 172.16.2.0/24
    Known via "static", distance 130, metric 0 (connected)
    Routing Descriptor Blocks:
        * directly connected, via Serial0/0/0
            Route metric is 0, traffic share count is 1
```

Para verificar a distância administrativa da rota utilizamos o comando "show ip route" seguido da rota em questão 172.16.2.0.

#### 4 Roteamento em Clientes de Rede

O processo de roteamento dos roteadores normalmente é bem mais complexo que o realizado em computadores clientes, pois alguns servidores também podem fazer o papel de roteador.

Até mesmo seu computador possui uma tabela de roteamento. Para você visualizá-la basta abrir o prompt de comando e digitar o comando “**route print**” no Windows. Veja a figura abaixo e note que várias rotas estão presentes em um computador.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 15 c5 cf 54 e6 ..... Broadcom 440x 10/100 Integrated Controller - Packet Scheduler Miniport
0x10004 ...00 18 de b3 bf f8 ..... Intel(R) PRO/Wireless 3945ABG Network Connection - Packet Scheduler Miniport
=====
Active Routes:
Network Destination      Netmask          Gateway        Interface Metric
          0.0.0.0          0.0.0.0    192.168.1.1  192.168.1.2    25
         127.0.0.0        255.0.0.0   127.0.0.1    127.0.0.1     1
        169.254.0.0      255.255.0.0  192.168.1.2  192.168.1.2    30
       192.168.1.0      255.255.255.0 192.168.1.2  192.168.1.2    25
      192.168.1.2      255.255.255.255 127.0.0.1    127.0.0.1    25
     192.168.1.255     255.255.255.255 192.168.1.2  192.168.1.2    25
     224.0.0.0          240.0.0.0   192.168.1.2  192.168.1.2    25
    255.255.255.255    255.255.255.255 192.168.1.2        2        1
    255.255.255.255    255.255.255.255 192.168.1.2  192.168.1.2    1
Default Gateway:           192.168.1.1
=====
Persistent Routes:
  None
C:\Documents and Settings\Administrator>
```

Por exemplo, a rota para a rede (Network Destination) “**0.0.0.0**” com máscara (Netmask) “**0.0.0.0**” representa a saída para Internet, ou seja, está indicando para onde os pacotes de redes desconhecidas devem ser encaminhados. Se a rede de destino não estiver contida em nenhuma das rotas contida na tabela ele enviará o pacote para esse **gateway** com IP 192.168.1.1.

Note que na segunda linha temos uma rota para a rede de Loopback 127.0.0.1, logo abaixo uma rota para a rede Zeroconf 169.254.0.0 e a seguir para a rede em que o computador está alocado que é a 192.168.1.0 com máscara 255.255.255.0.

Logo abaixo da entrada para a rede 192.168.1.0 temos o IP do próprio comutador configurado com uma máscara que chamados de “máscara de host”, porque ela tem todos os bits configurados em um (255.255.255.255). Note que os campos gateway e interface apontam para o IP de loopback 127.0.0.1, o que representa que essa é uma interface local.

No Linux e MAC OS-X o comando a ser utilizado é o “netstat -rs”, porém as saídas e redes padrões são bem semelhantes ao que observamos para um computador padrão Windows.

É importante ter em mente que maioria das redes os clientes não irão conhecer rotas ou encaminhar pacotes entre diferentes redes, eles apenas recebem um endereço de gateway através do serviço de DHCP e quando não conhecem uma rede de destino encaminham os pacotes para esse gateway, o qual fará o papel de intermediário entre os dispositivos de uma LAN e o mundo externo, seja ele outras redes da Intranet ou até mesmo a Internet.

#### 4.1 Problemas Comuns de Alcançabilidade em Clientes

Os problemas mais comuns em clientes quando estamos estudando roteamento são relacionados à parte física, ou seja, cabos rompidos ou com problemas intermitentes, de conectividade com o servidor DHCP ou com o servidor DNS.

Quando temos um cabo rompido ou com intermitência, haverá um aviso de conectividade que maioria dos sistemas operacionais fornece em sua interface gráfica para indicar um cabo desconectado.

Se o cabo estiver conectado e mesmo assim o computador apresenta problemas alguns testes devem ser realizados para identificar onde o problema de acesso a serviços da Intranet ou Internet está acontecendo. Uma metodologia interessante de ser utilizada é seguir os passos abaixo:

1. Fazer ping para o endereço de Loopback para detectar problemas com a própria interface de rede do computador. Se o teste for bem sucedido passe para o próximo teste.
2. Utilizar o comando ipconfig/ifconfig e verificar se o computador conseguiu pegar endereço via DHCP.
3. Se aparecer na configuração um endereço da rede 169.254.0.0 é sinal que o computador não conseguiu adquirir endereço via DHCP e se autoconfigurou.
4. Utilize os comandos em máquinas Windows **ipconfig /release** e **ipconfig /renew** liberar e tentar renovar o endereço IP com o servidor DHCP. Se mesmo assim o computador não pegar um IP esperado via DHCP o problema ainda pode ser físico ou o cabo do switch foi conectado a uma porta errada, por exemplo.
5. Caso a aplicação dos comandos do item 4 resultou em um IP que você sabe que é da rede daquele computador é sinal que a renovação de IP solucionou o problema inicial.  
Agora vamos utilizar o ping para testar a conectividade da seguinte maneira:
  - a. Primeiro pingar o próprio IP, basicamente é o mesmo teste do passo 1;
  - b. Em segundo lugar pingar o gateway;
  - c. Por último pingar o endereço ou os endereços do DNS, pois normalmente pode haver um DNS primário (principal) e um secundário.

Se o próprio IP da máquina não pingar é aconselhável verificar o driver da placa de rede. Se o gateway não responder pode ter algum filtro (firewall) ou problema em algum dos sentidos da comunicação. Se ambos pingarem você pode testar pingar para outros endereços da sua Intranet.

Se o DNS não pingar está descoberto o problema de acesso do computador, nesse caso o administrador de redes deve verificar se é um problema isolado, ou seja, somente do computador em questão, ou generalizado em todos ou um grupo de usuários para poder identificar quais os próximos passos a serem tomados.

Caso os três testes funcionem significa que pode estar havendo uma filtragem do tráfego que o usuário está tentando realizar ou então simplesmente o serviço que ele está acessando está indisponível. Você pode utilizar o computador de outro usuário na mesma sub-rede e realizar o teste de acesso que o usuário com problemas está tentando realizar e verificar se é um problema com o micro dele ou em outras máquinas acontece o mesmo.

Além disso, é interessante verificar se o acesso que ele está dizendo que não funciona está permitido pela política da empresa, às vezes é um bloqueio padrão.

A seguir vamos estudar mais sobre o serviço de alocação dinâmica de IPs DHCP nos roteadores Cisco.

## 5 Configurando o Serviço de DHCP em Roteadores Cisco

O DHCP permite a alocação dinâmica de endereços IP e facilita a configuração local dos computadores, pois elimina a necessidade da configuração manual dos hosts da rede um a um.

O Cisco IOS suporta o serviço de DHCP tanto como servidor e também a ativação do cliente em suas interfaces de LAN.

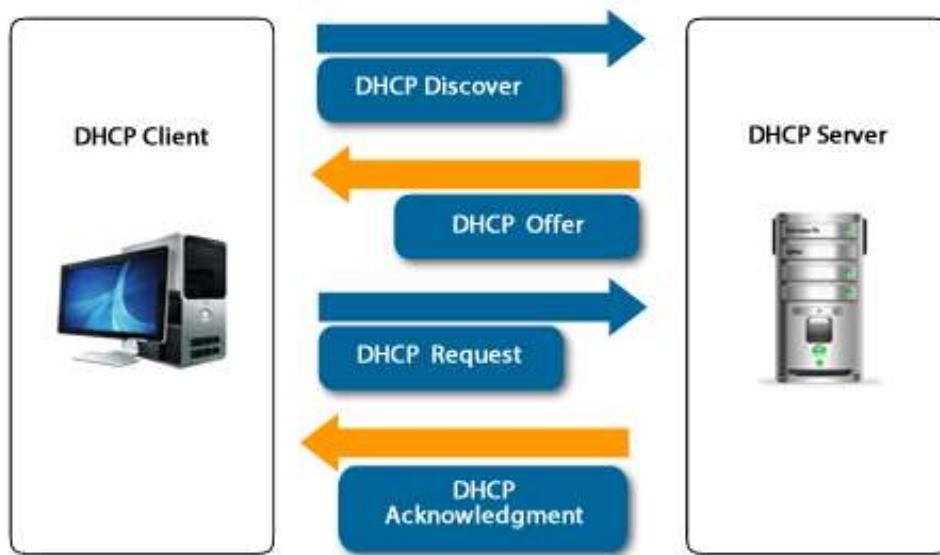
### 5.1 Visão Geral do DHCP

O **Dynamic Host Configuration Protocol** é um protocolo cliente-servidor derivado do BOOTP - RFCs 951 e 1084 - e tem a função de fornecer endereços de IP dinamicamente. O DHCP provê todos os dados de configuração requeridos pelo TCP/IP além de dados adicionais requeridos para servidores específicos.

O DHCP facilita a vida do administrador de rede, pois ele pode configurar toda sua rede TCP/IP de forma centralizada a partir de um servidor. Sempre que um novo host entra no segmento da rede, ele é configurado dinamicamente pelo servidor DHCP. A máquina pede um IP e esse pedido é interceptado pelo servidor de DHCP que fornece um endereço de IP disponível em sua lista.

O DHCP funciona da seguinte maneira:

- O cliente de DHCP pede um endereço IP (DHCP Discover).
- Um endereço IP é oferecido ao cliente (DHCP Offer).
- O cliente aceita a oferta e pedidos do endereço (DHCP Request).
- O endereço é nomeado oficialmente (DHCP Acknowledge).



Para que os endereços possam ser reutilizados caso um computador seja desligado ou retirado da rede, os administradores de rede definem um tempo limite (**lease time**) para o endereço alugado, assim se um computador for removido ou trocado o endereço IP alocado para ele será apagado após o tempo de aluguel definido pelo administrador.

Existem três tipos de componentes no DHCP, o servidor, o cliente e o agente relay.

O servidor DHCP é o componente que fornece os IPs dinamicamente aos clientes. Os parâmetros de configuração TCP/IP do servidor de DHCP podem incluir:

- Endereço de rede e máscara que será distribuída aos clientes.
- Endereço do Default gateway (roteador).

- Endereços de servidores DNS
- Lease time.

Parâmetros de configuração adicionais que são enviados aos clientes de DHCP: endereços de IP para servidores de DNS, WINS e outros mais. Por exemplo, em redes de telefonia IP Cisco é necessário um servidor TFTP para os telefones buscarem suas configurações e firmware, o qual é aprendido pelos telefones via DHCP através de uma opção com o número 150.

Diversas plataformas agem como clientes DHCP, o próprio roteador pode utilizar o DHCP cliente em suas interfaces LAN para configuração do endereço IP. As regras estão definidas na RFC 2132.

Os protocolos BOOTP e DHCP usam **broadcast** para trocar informações entre os clientes e os servidores. Os roteadores da Cisco não repassam broadcast de uma interface para outra, portanto um componente terá que capturar a requisição do cliente e encaminhar para um servidor situado em outro segmento de rede, esse componente é o **Agente Relay**. Utilizando um agente relay DHCP elimina-se a necessidade de um servidor de DHCP em cada segmento de rede.

O Cisco IOS suporta as três funções: servidor, cliente e agente relay. A seguir vamos estudar o funcionamento do protocolo DHCP.

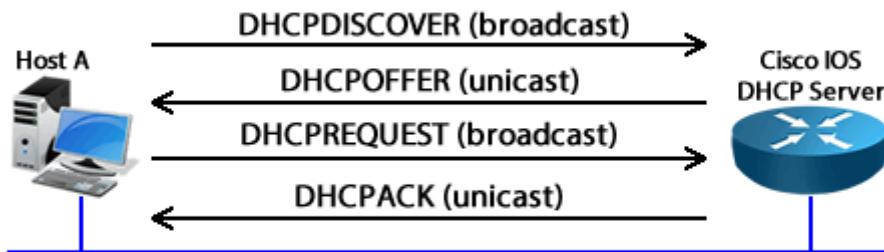
## 5.2 Funcionamento do DHCP

O DHCP é um serviço cliente/servidor onde o servidor DHCP pode ser configurado de três maneiras:

- **Alocação automática**, onde o DHCP fornece um endereço IP permanente ao cliente.
- **Alocação dinâmica**, onde o DHCP fornece um endereço IP a um cliente por um período limitado de tempo (ou até que o cliente libere esse IP). Essa é a alocação convencional utilizada pelos servidores DHCP para aluguel de IPs aos clientes.
- **Alocação Manual via servidor**, onde um administrador de rede determina um IP a um cliente e o DHCP é utilizado simplesmente para repassar esse endereço atribuído.

Os endereços IP estáticos configurados diretamente nos hosts devem ser removidos da faixa ou escopo de endereços do servidor DHCP pelo administrador para que não haja conflito de IPs (dois computadores utilizando o mesmo endereço).

Um detalhe que pode ser cobrado do aluno em prova é como cada uma das mensagens trocadas entre o cliente e o servidor é enviada, veja a figura abaixo.



Note que o DHCP Discover e Request são enviados em **Broadcast** (255.255.255.255), já as mensagens de DHCP Offer e ACK são enviadas em Unicast.

Antes de um servidor alugar um IP ao host ele faz por padrão dois testes de ping para o endereço do pool que ele escolheu para fornecer ao cliente para evitar conflito de endereços IP na rede, ou seja, evitar que seja fornecido um IP duplicado na rede.

Já os clientes utilizam ARPs gratuitos (Gratuitous ARP) para detectar conflitos de IP. Os ARPs gratuitos são requisições ARP enviadas perguntando se existe MAC com aquele IP que o cliente recebeu do servidor DHCP, caso alguém responda quer dizer que há ou pode haver um conflito de IPs.

Mesmo com os testes acima se um conflito for detectado o servidor DHCP retira aquele endereço da faixa de IPs “alocáveis” e não o utiliza até que o conflito seja resolvido pelo administrador de redes.

Uma curiosidade, enquanto o cliente não tem IP configurado ele utiliza o endereço 0.0.0.0 nas mensagens DHCP.

A seguir vamos começar a estudar as configurações do serviço de DHCP.

### **5.3 Configurando o DHCP Servidor no Cisco IOS**

Para configurar o DHCP devemos seguir alguns passos básicos:

1. Definir os endereços IPs que serão excluídos do pool (faixa de IPs alocáveis com o comando “ip dhcp excluded-address”).
2. Configurar um escopo DHCP chamado de pool no Cisco IOS com o comando “ip dhcp pool”.
3. Dentro do pool configurar os parâmetros mínimos:
  - a. Rede a ser atribuída e máscara (network);
  - b. Roteador padrão (default-router);
  - c. Servidor DNS (dns-server);
  - d. Definir o tempo de aluguel dos IPs do pool (lease);
  - e. Opções necessárias do DHCP, por exemplo, servidor TFTP para telefones IP (“option 150 ip” ou next-server).

Se o roteador for fornecer IP localmente uma de suas interfaces deve estar na mesma rede que a definida no passo 3, pois no DHCP não há necessidade de vínculo com a interface LAN através de comando comando, esse vínculo é automático quando configuramos uma interface com o IP de uma das faixas do DHCP pool.

Veja um exemplo com uma sequência de configuração conforme itens citados anteriormente.

```
R1(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10 ! exclui IPs de 1 a 10
R1(config)#ip dhcp excluded-address 172.16.2.100 172.16.2.254 ! exclui IPs de 100 a 254
R1(config)#ip dhcp pool dltec-ccent
R1(dhcp-config)#network 172.16.1.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.1.254
R1(dhcp-config)#dns-server 172.16.1.10 172.16.20.10 ! endereço do DNS primário e reserva
R1(dhcp-config)#lease 7 ! uma semana – 7dias
R1(dhcp-config)#domain-name dltec-ccent.com
R1(dhcp-config)#next-server 172.16.2.5 ! ou “option 150 ip 172.16.2.5”
```

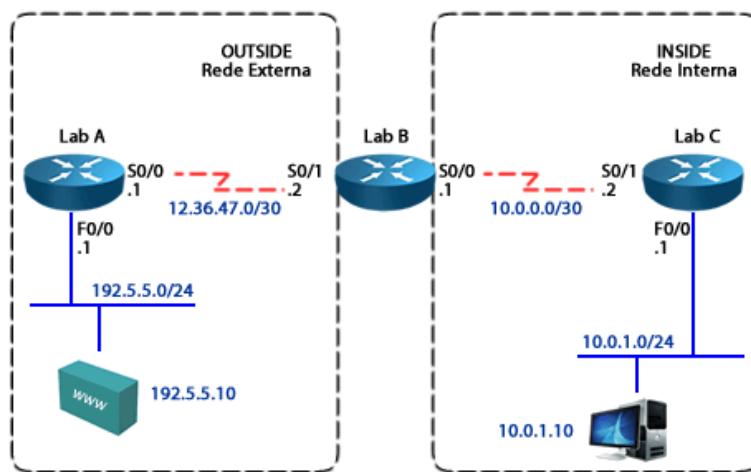
Não é preciso vincular o pool a uma interface, pois o serviço de DHCP é automaticamente ativado na interface LAN com IP configurado dentro da faixa definida pelo comando “network”.

Se você tiver VLANs em roteadores com ROAS (Router on a Stick – estudaremos no cap 7) também não é necessário comando para vincular com as sub-interfaces, assim que o Cisco IOS DHCP detecta que a rede foi configurada ele passa a fornecer IP na VLAN.

Veja na sequência um exemplo de configuração com as explicações de como ativar o DHCP básico nos roteadores Cisco.

#### 5.4 Exemplo Prático de Configuração do DHCP

A explicação da configuração do DHCP será realizada com um exemplo prático abaixo onde o Lab\_C da figura ao lado será configurado como servidor DHCP para sua rede LAN.



A seguir seguem as configurações e explicações sobre os comandos.

```
LAB_C#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Para configurar o DHCP Server em um roteador Cisco entre com o comando:
LAB_C(config)#ip dhcp ?
Conflict          DHCP address conflict parameters
Database         Configure DHCP database agents
excluded-address Prevent DHCP from assigning certain addresses
limited-broadcast-address Use all 1's broadcast address
ping              Specify ping parameters used by DHCP
pool              Configure DHCP address pools
relay             DHCP relay agent parameters
smart-relay       Enable Smart Relay feature
```

Primeiro defina a faixa de endereços IP fixos que serão utilizados para configurar dispositivos de rede e servidores e exclua-os da faixa de endereços dinâmicos do servidor DHCP:

```
LAB_C(config)#ip dhcp excluded-address 10.0.1.58
LAB_C(config)#ip dhcp excluded-address 10.0.1.10 10.0.0.20
```

Você pode excluir um IP isolado ou um range de IPs. No exemplo acima o IP 10.0.1.58 foi excluído e também o range de IPs de 10 a 20. Geralmente os IPs excluídos são utilizados para servidores e hosts que necessitam de endereços fixos.

Crie um pool para o DHCP e dê um nome a ele. Ao digitar o comando para criar o escopo ou pool do serviço de DHCP você cairá em um prompt de configuração do DHCP "dhcp-config".

Veja a configuração a seguir onde o pool será criado com o nome Lanlabc.

```

LAB_C(config)#ip dhcp pool Lanlabc
LAB_C(dhcp-config)#
LAB_C(dhcp-config)#
DHCP pool configuration commands:
  accounting          Send Accounting Start/Stop messages
  bootfile            Boot file name
  class               Specify a DHCP class
  client-identifier   Client identifier
  client-name         Client name
  default-router      Default routers
  dns-server          DNS servers
  domain-name         Domain name
  exit                Exit from DHCP pool configuration mode
  hardware-address    Client hardware address
  host                Client IP address and mask
  import              Programatically importing DHCP option parameters
  lease               Address lease time
  netbios-name-server NetBIOS (WINS) name servers
  netbios-node-type   NetBIOS node type
  network             Network number and mask
  next-server         Next server in boot process
  no                 Negate a command or set its defaults
  option              Raw DHCP options
  origin              Configure the origin of the pool
  relay               Function as a DHCP relay
  remember            Remember released bindings
  renew               Configure renewal policy
  server              Configure the server ID option value
  subnet              Subnet allocation commands
  update              Dynamic updates
  utilization         Configure various utilization parameters
  vrf                Associate this pool with a VRF

```

**LAB\_C(dhcp-config) #**

Configure a rede e máscara que serão fornecidas aos clientes pelo servidor DHCP e demais opções conforme abaixo:

```

LAB_C(dhcp-config)#network 10.0.1.0 ?
/nn or A.B.C.D  Network mask or prefix length
<cr>
LAB_C(dhcp-config)#network 10.0.1.0 /24
Configure o nome do domínio:
LAB_C(dhcp-config)#domain-name lab_c.com
Configure o IP do servidor DNS da sua rede:
LAB_C(dhcp-config)#dns-server 192.5.5.10
Entre com o IP do gateway padrão para a rede:
LAB_C(dhcp-config)#default-router 10.0.1.1
Entre com o IP do servidor de WINS e o tipo:
LAB_C(dhcp-config)#netbios-name-server 10.0.1.58
LAB_C(dhcp-config)#netbios-node-type ?
<0-FF>  Hexadecimal number
b-node   Broadcast node
h-node   Hybrid node
m-node   Mixed node
p-node   Peer-to-peer node
LAB_C(dhcp-config)#netbios-node-type h-node

```

Note que além da rede e máscara foi passado o domínio "lab\_c.com", servidor DNS 192.5.5.10, roteador padrão 10.0.1.1 e um endereço de servidor WINS. O tipo de WINS h-node era utilizado em redes Windows mais antigas, atualmente não se utiliza mais esse parâmetro.

Entre agora com o tempo de empréstimo (lease time – dias horas minutos) do IP para os clientes:

```
LAB_C(dhcp-config)#lease ?
<0-365> Days
infinite Infinite lease
LAB_C(dhcp-config)#lease 30 ?
<0-23> Hours
<cr>
LAB_C(dhcp-config)#lease 30 2 ?
<0-59> Minutes
<cr>
LAB_C(dhcp-config)#lease 30 2 30 ?
<cr>
LAB_C(dhcp-config)#lease 30 2 30
```

O empréstimo durará trinta dias, duas horas e trinta minutos. Após esse período o cliente terá que renovar o IP. Agora saia do modo de configuração global e salve a configuração na NVRAM:

```
LAB_C(dhcp-config)#+^Z
Lab_C#copy run start
```

Veja abaixo a saída do comando "show run" onde é mostrada somente a configuração do DHCP Server.

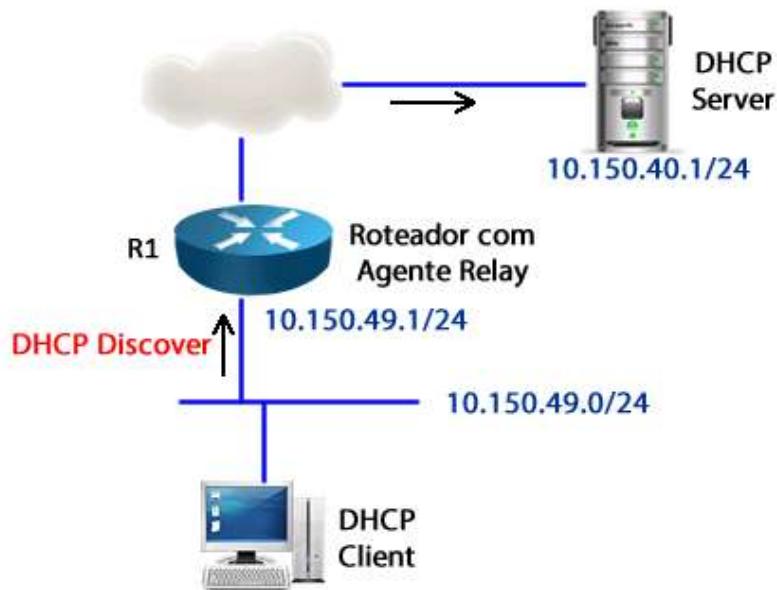
```
Lab_C#sho run
! ### algumas saídas foram suprimidas ###
hostname LAB_C
!
no ip dhcp conflict logging
!
ip dhcp excluded-address 10.0.1.58
ip dhcp excluded-address 10.0.1.10 10.0.0.20
!
ip dhcp pool Lanlabc
  network 10.0.1.0 255.255.255.0
  domain-name lab_c.com
  dns-server 192.5.5.10
  default-router 10.0.1.1
  netbios-name-server 10.0.1.58
  netbios-node-type h-node
  lease 30 2 30
```

## 5.5 Configurando o DHCP Relay

Algumas empresas ao invés de adotarem uma solução de DHCP distribuída, como a que configuramos no exemplo anterior, onde cada router remoto administraria sua própria faixa de IPs, preferem uma arquitetura centralizada por questões de administração e segurança.

Nesse tipo de arquitetura o servidor DHCP segue pode não estar situado na mesma sub-rede dos hosts locais, portanto quando um cliente enviar um **DHCP Request** em **broadcast** solicitando o aluguel de um IP o roteador irá bloquear essa mensagem, pois os roteadores não encaminham broadcasts (255.255.255.255).

Para solucionar esse problema os roteadores podem ser configurados como **agente relay**, ou seja, um agente que irá **encaminhar requisições DHCP** pela rede, porém não em broadcast, mas em unicast diretamente para o endereço IP do servidor DHCP remoto com o comando “**ip helper-address**”.



Veja abaixo a configuração necessária para o roteador R1 na topologia da figura acima.

```
R1(config)#interface FastEthernet0
R1(config-if)#ip address 10.150.49.1 255.255.255.0
R1(config-if)#ip helper-address 10.150.40.1
R1(config-if)#^Z
R1#
```

Com essa configuração, quando o roteador R1 receber o DHCPDISCOVER de um cliente DHCP que esteja conectado à sua rede LAN ele enviará a mensagem para o servidor 10.150.40.1 e ficará como intermediário na troca de informações entre o cliente e o servidor até que a negociação seja finalizada.

Portanto, sem o comando “ip helper-address”, quando um roteador recebe uma mensagem de DHCP Discover em broadcast ele “dropa” ou deleta essa mensagem, pois ele não pode encaminhar mensagens de broadcast de camada 3 (255.255.255.255).

Se você estiver utilizando a topologia ROAS, no roteador esse comando deve ir nas sub-interfaces criadas para a VLAN que necessitar do helper-address, não configure na interface física. Você vai aprender sobre essa topologia no próximo capítulo.

## 5.6 Monitorando e Mantendo o DHCP

Para manter e monitorar o DHCP utilize o comando “**show dhcp binding**”. Esse comando mostra os micros que receberam IP passado pelo servidor DHCP. Veja exemplo abaixo.

IP address	Client-ID/ Hardware address	Lease expiration	Type
10.0.1.2	0063.6973.636f.2d30. 3030.632e.3330.3431. 2e66.6334.302d.566c. 31	Mar 02 1993 11:37 AM	Automatic
10.0.1.3	0063.6973.636f.2d30. 3030.632e.3330.3431. 2e65.6263.302d.566c. 31	Mar 02 1993 11:38 AM	Automatic

No exemplo acima o roteador forneceu os IPs 10.0.1.2 e 10.0.1.3 para dois clientes.

Abaixo segue outro exemplo do comando “**show ip dhcp binding**” com uma variação que pode ser encontrada em outras versões de Cisco IOS.

```

Dltec-FW#show ip dhcp ?
binding    DHCP address bindings
conflict   DHCP address conflicts
database   DHCP database agents
import     Show Imported Parameters
pool       DHCP pools information
relay      Miscellaneous DHCP relay information
server    Miscellaneous DHCP server information

Dltec-FW#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/          Lease expiration        Type
                           Hardware address/
                           User name
192.168.1.20         0100.18e7.6177.a8    Dec 04 2012 10:57 AM  Automatic
192.168.1.21         01c0.1885.e8ee.db    Dec 04 2012 09:19 AM  Automatic
192.168.1.22         01c0.1885.e5ec.bf    Dec 04 2012 09:27 AM  Automatic
192.168.2.20         0100.1d70.60d3.1b    Dec 04 2012 01:25 PM  Automatic
192.168.2.22         0100.2333.9d07.92    Dec 04 2012 01:25 PM  Automatic
192.168.2.24         0100.1b0c.96c5.e8    Dec 04 2012 01:25 PM  Automatic
Dltec-FW#

```

Com o comando “**show ip dhcp pool**” podemos ver estatísticas gerais de um pool específico, veja exemplo abaixo do comando para o pool Lanlabc.

Pool Lanlabc :		
Utilization mark (high/low)	:	100 / 0
Subnet size (first/next)	:	0 / 0
Total addresses	:	254
Leased addresses	:	0
Pending event	:	none
1 subnet is currently in the pool :		
Current index	IP address range	Leased addresses
10.0.1.1	10.0.1.1 - 10.0.1.254	0

Lab\_C#

Note nos campos destacados que temos o nome do pool e a quantidade de endereços que foram alocados por ele, nesse exemplo ainda nenhum endereço foi alocado.

Outro comando que pode ser utilizado para mostrar estatísticas gerais do serviço DHCP é o “**show ip dhcp server statistics**”.

O comando “**show ip dhcp conflict**” pode ser utilizado para verificar os conflitos de IP detectados pelo servidor DHCP para que possam ser tratados pelo administrador de redes.

Veja um exemplo abaixo onde foram detectados conflitos para os endereços 172.16.1.32 e 172.16.1.64, porém para o final 32 o conflito foi detectado pelo ping, já para o final 64 através dos ARPs gratuitos.

```
Router> show ip dhcp conflict
IP address Detection Method Detection time
172.16.1.32 Ping Feb 16 1998 12:28 PM
172.16.1.64 Gratuitous ARP Feb 23 1998 08:12 AM
```

Também podemos utilizar o “clear” para limpar informações aprendidas pelo DHCP, seguem os comandos abaixo:

- Router# clear ip dhcp binding **endereço\_IP** | \*: Você pode utilizar um IP específico para apagar a entrada dinâmica feita pelo servidor ou com o asterisco para apagar todas as entradas dinâmicas feitas pelo servidor.
- Router# clear ip dhcp conflict **endereço\_IP** | \*: Com esse comando você pode apagar as informações de conflitos detectados pelo servidor digitando um endereço específico ou com o asterisco para apagar todas as entradas.
- Router# clear ip dhcp server statistics: Reinicializa os contadores das estatísticas do DHCP.

Além dos comandos show você pode utilizar o “**debug ip dhcp server packet**” para verificar a troca de mensagens entre o servidor DHCP e os clientes. Abaixo segue um exemplo de um host solicitando IP ao Lab\_C.

```
LAB_C#debug ip dhcp server ?
events Report address assignments, lease expirations, etc.
linkage Show database linkage
packet Decode message receptions and transmissions
LAB_C#debug ip dhcp server packet
11:46:31: DHCPD: DHCPDISCOVER received from client 0100.0854.10c1.67 on interface FastEthernet0/0.
11:46:33: DHCPD: Sending DHCPOFFER to client 0100.0854.10c1.67 (10.0.1.4).
11:46:33: DHCPD: creating ARP entry (10.0.1.4, 0008.5410.c167).
11:46:33: DHCPD: unicasting BOOTREPLY to client 0008.5410.c167 (10.0.1.4).
11:46:33: DHCPD: DHCPREQUEST received from client 0100.0854.10c1.67.
11:46:33: DHCPD: Sending DHCPACK to client 0100.0854.10c1.67 (10.0.1.4).
11:46:33: DHCPD: creating ARP entry (10.0.1.4, 0008.5410.c167).
11:46:33: DHCPD: unicasting BOOTREPLY to client 0008.5410.c167 (10.0.1.4).
LAB_C#
```

As quatro mensagens mais importantes estão marcadas em amarelo.

## 6 Resumo do Capítulo

Bem pessoal, chegamos ao final de mais um capítulo!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Entender o conceito de interfaces diretamente conectadas e como elas aparecem na tabela de roteamento.
- Entender o processo de roteamento em roteadores Cisco.
- Diferenciar os três processos básicos de roteamento.
- Dominar o conceito e configuração de rotas estáticas.
- Entender como funciona e a configuração de uma rota padrão.
- Dominar os conceitos básicos de métrica e distância administrativa.
- Entender o processo de roteamento de configuração de redes em clientes.
- Entender os conceitos e aplicações do DHCP.
- Saber configurar, sem dificuldade, um roteador Cisco como servidor DHCP em sua rede.
- Ser capaz de realizar troubleshooting no DHCP em roteadores Cisco.
- Entender o conceito e dominar a configuração de um roteador Cisco atuando como agente relay.

*Nesse capítulo vamos dar o toque final a topologia de rede inserindo VLANs e Trunks às redes locais.*

*A segmentação das redes com VLANs traz maior segurança e flexibilidade às LANs.*

*Também estudaremos o protocolo VTP, vamos nos aprofundar nas configurações do Port Security e fazer o roteamento entre VLANs utilizando roteadores e switches camada-3.*

*Esperamos que você aproveite o capítulo e aprenda bastante.*

*Bons estudos!*

## **Capítulo 7 - Segmentando Redes Locais com VLANs**

### **Objetivos do Capítulo**

Ao final desse capítulo você terá estudado e deverá compreender:

- As opções de topologia de rede de acordo com o porte das empresas.
- Entender definitivamente os cabos e necessidades de conexão em dispositivos da rede corporativa.
- Funcionamento e configurações de VLANs, Trunks e protocolo VTP.
- Configuração e funcionamento do Port Security.
- Configuração do roteamento entre VLANs utilizando roteadores e switches camada 3.
- Aplicação dos conhecimentos para entender e configurar topologias de redes de pequeno e médio porte.

## Sumário do Capítulo

<b>1 Apresentação</b>	<b>289</b>
<b>2 Revisão sobre Topologias e Componentes de Redes</b>	<b>289</b>

<b>2.1 Topologias e Dispositivos de Rede</b>	<b>289</b>
2.1.1 Projeto de Redes Hierárquicas em Três Camadas	291

<b>2.2 Questões sobre Cabeamento em LANs</b>	
294	

<b>3 Revisão sobre o Funcionamento dos Switches de Camada 2</b>	<b>295</b>
---	------------

<b>3.1 Leds Indicativos em Switches e Roteadores</b>	<b>297</b>
--	------------

<b>3.2 Revisão das Configurações Gerais em Switches</b>	<b>299</b>
---	------------

<b>4 Configurando VLANs e Trunks</b>	<b>301</b>
--------------------------------------	------------

<b>4.1 Criando VLANs</b>	<b>303</b>
--------------------------	------------

<b>4.2 Atribuindo Portas às VLANs</b>	<b>304</b>
4.2.1 Exemplo Prático de VLAN Membership	306

<b>4.3 Interligando Switches e Roteadores – Configurando Links Trunk</b>	<b>307</b>
--	------------

4.3.1 Administrando o Encaminhamento de VLANs nos Trunks	308
4.3.2 VLAN Nativa	309

<b>4.4 Entendendo o Protocolo DTP</b>	<b>310</b>
---------------------------------------	------------

<b>4.5 Protocolo VTP</b>	<b>313</b>
4.5.1 Numeração Estendida de VLANs e VTP	314

<b>4.6 Roteamento entre VLANs</b>	<b>316</b>
-----------------------------------	------------

4.6.1 Roteamento entre VLANs com Roteadores	317
4.6.2 Roteamento entre VLANs com Switches Camada 3	319

<b>4.7 Exemplo Prático de VTP, VLAN e Roteamento entre VLAN</b>	<b>321</b>
---	------------

<b>5 Aumentando a Segurança dos Switches</b>	
<b>324</b>	

<b>5.1 Configurando o Port Security</b>	<b>325</b>
---	------------

<b>5.2 Verificando o Port Security</b>	<b>327</b>
--	------------

<b>5.3 Protegendo Interfaces não Utilizadas</b>	<b>328</b>
---	------------

<b>5.4 Configurando o Acesso Seguro via SSH</b>	
<b>329</b>	

<b>6 Scripts de Configuração</b>	<b>330</b>
----------------------------------	------------

<b>7 Resumo do Capítulo</b>	<b>331</b>
-----------------------------	------------

## 1 Apresentação

Até o capítulo 6 estudamos redes onde os dispositivos na LAN estão todos em uma só rede, ou seja, não utilizamos ainda o conceito de VLANs para segregar domínios de broadcast em nossas redes locais utilizadas até o momento.

O uso de VLANs traz benefícios para a administração da rede, pois facilita a alocação de portas em um switch de maneira lógica e também permite alocar dispositivos semelhantes em um mesmo domínio de broadcast.

Por exemplo, em uma rede onde temos todos os dispositivos da rede local em uma única rede, ou seja, em um único domínio de broadcast, a sobrecarga dos dispositivos recebendo e processando pacotes com endereço de destino ffff.ffff.ffff torna-se cada vez maior a medida que novos equipamentos são conectadas à rede.

Além disso, não é possível implementar uma forma de controle de tráfego entre dispositivos através da rede, pois se todos estão no mesmo segmento como criar regras de encaminhamento entre dispositivos? A única opção nesses casos é implementar regras de filtragem nos próprios endpoints, por exemplo, utilizando iptables (filtro de pacotes) em servidores Linux ou firewall em servidores Microsoft para limitar acesso a determinados serviços. Apesar de ser viável essa opção ela não é escalável, pois a medida que o número de servidores cresce a complexidade de administração individual também cresce.

Por esses motivos de administração e maior controle de segurança em ambientes de LAN vamos nesse capítulo aprender a configurar e manter redes de switches Cisco com VLANs.

Aproveite o material e bons estudos!

## 2 Revisão sobre Topologias e Componentes de Redes

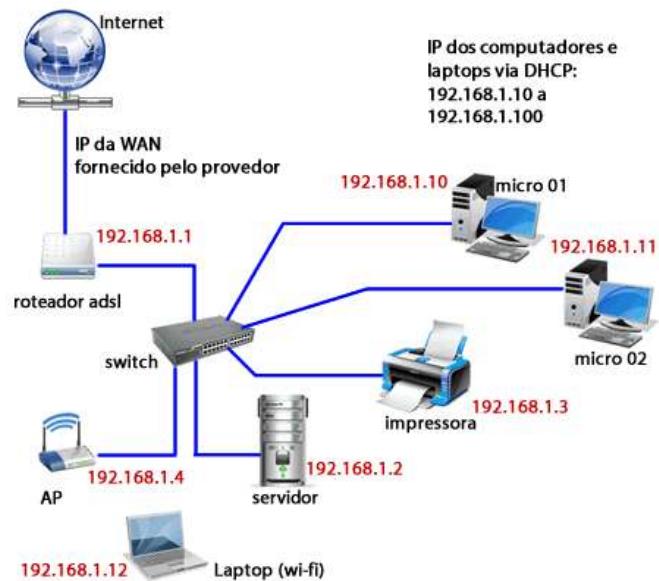
Antes de iniciar o novo assunto sobre a implementação de VLANs vamos analisar um pouco melhor as opções de topologia que estudamos até o momento e também aprender mais um pouco sobre o que podemos encontrar na prática quando estivermos trabalhando com administração de redes.

### 2.1 Topologias e Dispositivos de Rede

Para simplificar o assunto dividimos as redes nesse curso em cinco categorias:

- **SOHO**: Pequeno escritório ou escritório residencial.
- **Redes de pequeno porte**: compostas por dois ou mais pontos, por exemplo, uma rede de farmácias com uma matriz e duas filiais.
- **Redes de médio porte**: composta por diversos pontos e com complexidade média, por exemplo, uma rede de lojas espalhadas por dez cidades com o datacenter situado em sua Matriz.
- **Redes Campus**: redes compostas por prédios próximos uns dos outros.
- **Redes de grande porte**: composta por diversos tipos de redes de diferentes níveis de complexidade e requisitos de segurança, por exemplo, a rede de uma grande instituição bancária.

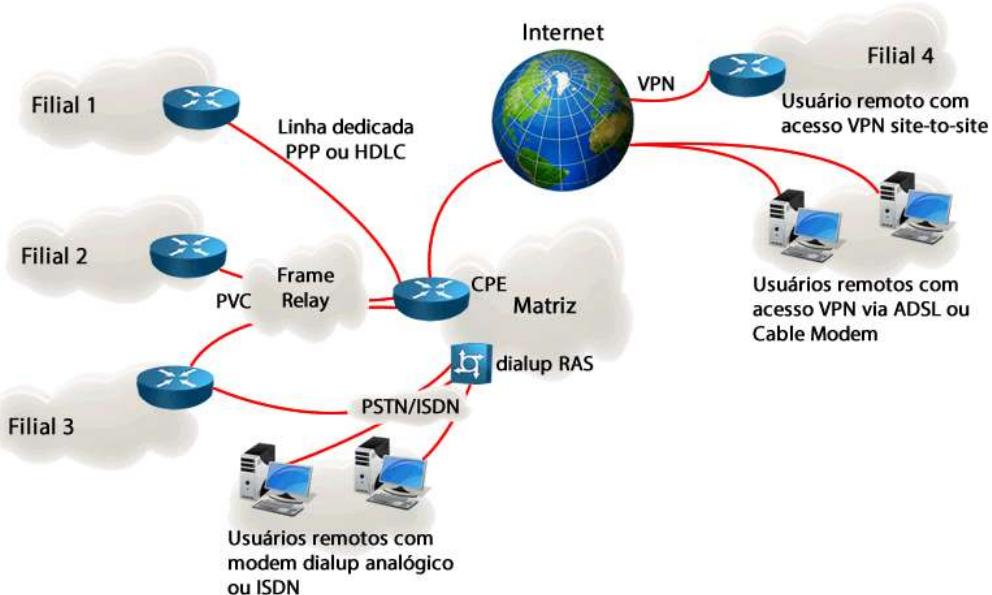
Em uma topologia SOHO ou "Small-Office/Home Office" temos a topologia mais simples, normalmente composta por apenas um acesso Internet banda larga, onde o dispositivo de acesso muitas vezes pode ter integrado as funções de roteador, ponto de acesso sem fio, switch e VPN, possibilitando conectar um pequeno escritório ou usuário remoto com segurança.



Para esse tipo de solução existe a linha de roteadores da série 800.

A mesma topologia anterior pode ser utilizada em redes de pequeno porte, porém com a diferença que pode haver diversas LANs do tipo mostrada acima com necessidade de comunicação, formando uma Intranet. Também o uso de roteadores e switches em dispositivos separados será mais comum nesse tipo de topologia, por exemplo, roteadores da linha 1900 ou 2900 e switches da linha Catalyst 2960.

As redes de médio porte têm maior complexidade e muitas vezes necessidades de conexão e segurança que normalmente não são uma preocupação nos dois exemplos de redes anteriores.



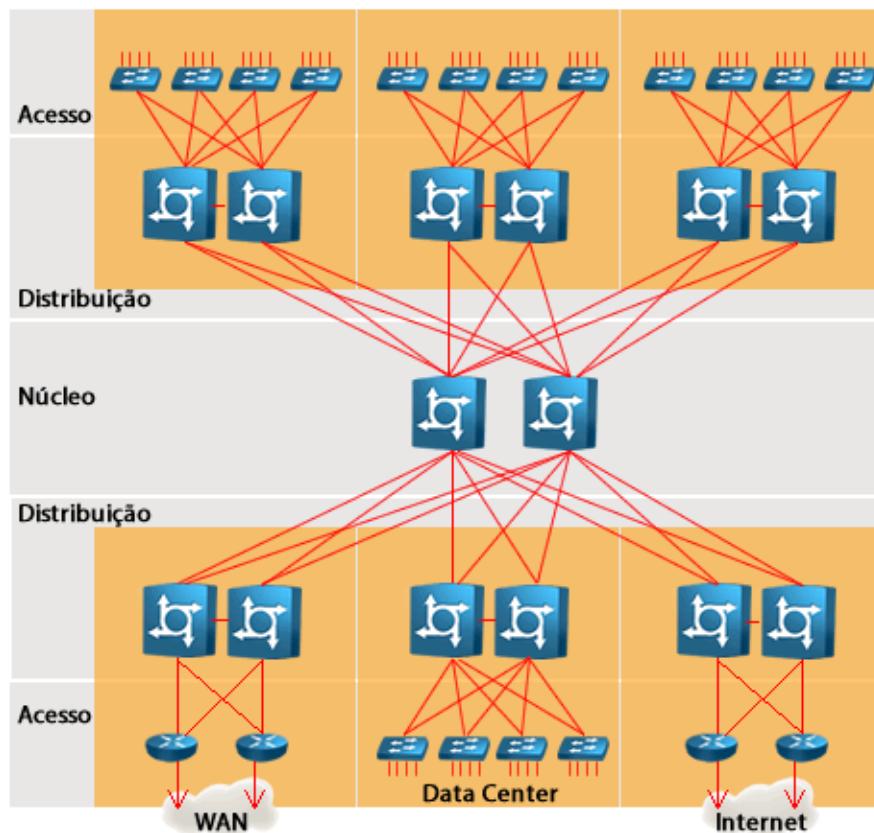
Nesse tipo de topologia podem ser utilizados roteadores das séries 800, 1900, 2900 e 3900, devido à variedade de ambientes e requisitos de cada unidade. Além disso, podem ser utilizados switches com recursos de camada-3 como a série Catalyst 3560.

Em redes campus e de grande porte normalmente os projetos de LAN utilizam um modelo de projeto orientado pela Cisco em três camadas: Acesso, Distribuição e Core.

Nessas topologias estamos tratando de LANs com mais de 1.000 computadores, espalhados em grandes edificações ou até mesmo composta por diversos prédios próximos conectados entre si por links redundantes de fibra óptica, visando alto desempenho e alta disponibilidade.

### 2.1.1 Projeto de Redes Hierárquicas em Três Camadas

O modelo de projeto hierárquico em três camadas da Cisco permite a agregação (junção) de tráfego em três níveis diferentes: Acesso (Access), Distribuição (Distribution) e Núcleo (Core), sendo um modelo mais escalável para grandes redes corporativas. Veja a figura abaixo.



Na figura acima, cada quadrado conectado ao Core (Núcleo) representa um prédio ou edificação, o qual possui switches redundantes e também links redundantes para garantir a alta disponibilidade desse modelo.

Note que nas pontas temos switches de acesso também conectados com links redundantes e a dois switches distintos na distribuição, portanto, para que um cliente fique indisponível é preciso acontecer muitos acidentes simultâneos quando utilizamos esse tipo de topologia, é o que chamados de “cúmulo do administrador de redes azarado!” se houver indisponibilidade.

Cada camada tem um papel específico e permite que outros equipamentos e serviços sejam adicionados de maneira simples e escalonável ou escalável, o que quer dizer que você pode fazer sua rede crescer sem precisar de um novo projeto.

As três camadas são:

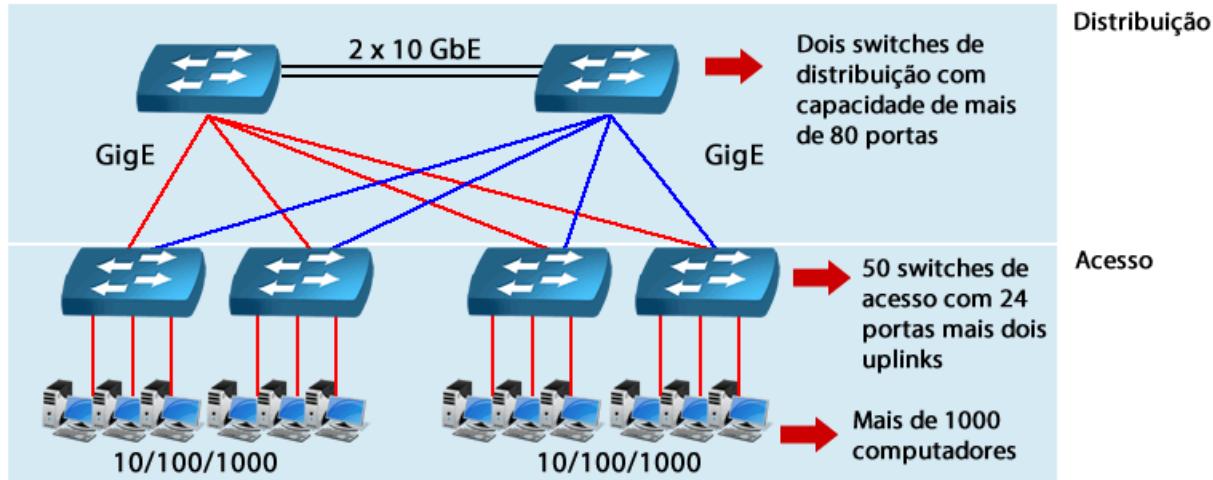
- **Camada de Núcleo ou Core:** provê transporte rápido entre sites. Normalmente são switches de grande porte.
- **Camada de Distribuição ou Distribution:** conecta as diversas edificações ao core e implementa políticas de segurança, roteamento e agregação de tráfego. Normalmente são switches camada 3.
- **Camada de Acesso ou Access:** provê acesso aos equipamentos finais, como micros, servidores e telefones IP. Normalmente são switches camada 2.

A camada core é o backbone de alta velocidade da rede, a qual deve ser projetada para minimizar o atraso através de dispositivos de alta vazão, sacrificando outros recursos. Deve possuir componentes redundantes devido a sua criticidade para a interconexão, seu diâmetro deve ser pequeno (para ter baixo atraso).

A camada de distribuição pode ter muitos papéis no modelo hierárquico, tais como roteamento entre VLANs, implementação de regras de encaminhamento através de filtros de pacotes, summarização de rotas, etc.

A camada de acesso é o final da rede, aquela que provê acesso à rede para usuários nos segmentos locais. Frequentemente usa apenas switches, porém pode utilizar roteadores para dar acesso a pequenos escritórios remotos e usuários em home Office. Normalmente é a camada onde as VLANs são configuradas.

Outro modelo que pode ser utilizado em redes de menor porte (1000 usuários) é o colapsado (collapsed core).

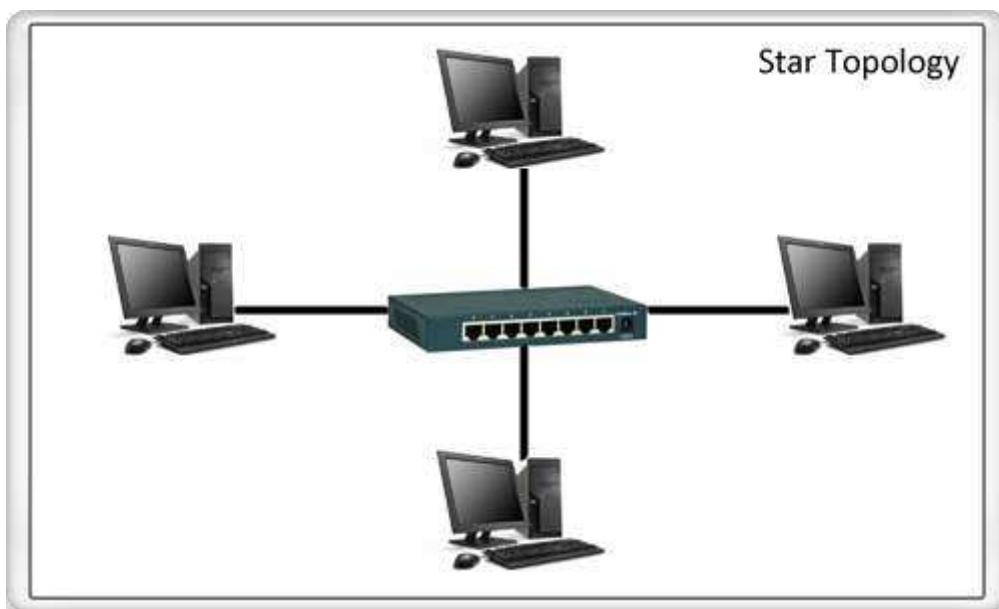


Nessa topologia podemos conectar o acesso aos switches de distribuição sem a necessidade do Core, uma vez que estamos falando de um ambiente único de LAN.

A forma de conexão entre os switches de acesso e distribuição pode ser aproveitada aproveitada nesse modelo colapsado, porém com a mesma disponibilidade aos serviços de rede para os usuários.

Os cabos que conectam os switches de distribuição aos switches de acesso são chamados de **Uplinks** e normalmente são conectados de forma parcial (partial mesh) na topologia.

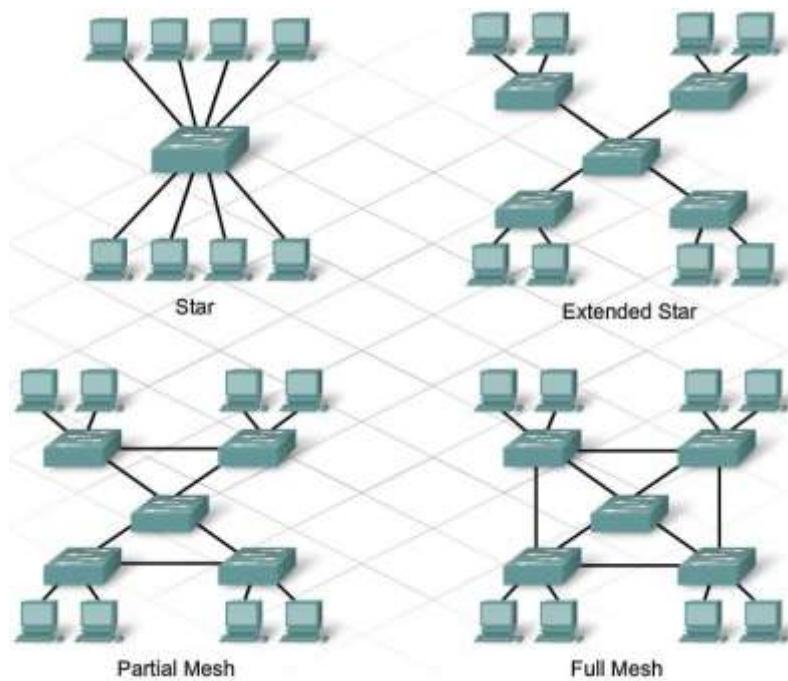
Já os switches de acesso formam uma topologia em estrela com seus hosts (star), veja ilustração a seguir.



Portanto, você pode ouvir em algumas literaturas ou até mesmo no exame do CCENT que a topologia em três camadas, seja ela completa ou com core colapsado, forma uma topologia híbrida, pois utiliza partial meshed entre o acesso e a distribuição e estrela entre o acesso e seus hosts.

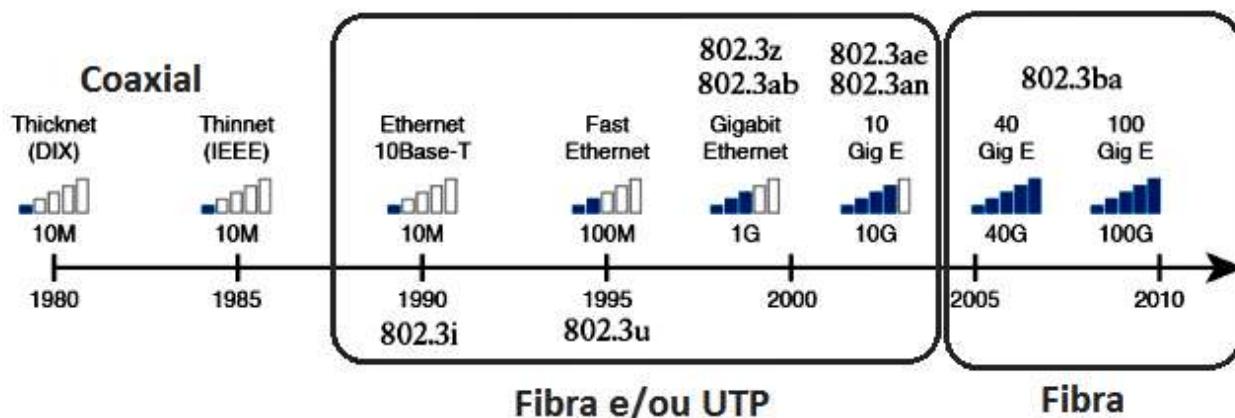
Dificilmente você encontrará uma topologia em três camadas full meshed (malha completa), pois o custo de conectar todos os dispositivos entre si seria impeditivo, além disso, a quantidade de cabos necessárias poderia ultrapassar o número de portas que switches modulares suportam.

Veja na imagem abaixo uma comparação entre as topologias (estudadas no capítulo 2).



## 2.2 Questões sobre Cabeamento em LANs

É importante ao projetar uma LAN conhecer as distâncias permitidas para cada tipo de opção de camada física e padrão disponível no mercado. Veja abaixo a linha do tempo com os padrões desenvolvidos.



Os cabos UTP com os padrões 10/100/1.000/10.000 Mbps (Eth, Fast, Giga e 10Giga) tem uma limitação de 100m na distância entre dois pontos a serem conectados, portanto acima dessa distância temos que procurar outras soluções de cabeamento, por exemplo, fibras ópticas ou links de rádio.

Em redes LAN Campus, onde esse tipo de barreira de distância é mais comum de aparecer, é comum a interligação do backbone da rede ser realizado com fibra óptica, tanto por questões de distância como pelo desempenho e velocidade.

Sabemos que os links de fibra são imunes a interferências eletromagnéticas e raios, por isso em ambientes externos ou chão de fábrica, essa é uma opção bastante interessante.

Os switches Cisco por padrão têm saídas em par metálico, porém vários modelos de switches suportam a instalação de interfaces chamadas GBIC (Gigabit Interface Converter) e SFP (Small Form-Factor Pluggable), as quais fornecem vários modelos para transmissão e recepção via fibra óptica.

Para os cabos UTP (pares metálicos trançados) temos o padrão Ethernet, Fastethernet e Gigabitethernet que utilizam conectores RJ-45 machos para conectar nos computadores e nos patch panels utilizam o RJ-45 fêmea. Os cabos de rede UTP podem ser cruzados ou diretos, dependendo dos dispositivos das pontas a serem conectados, conforme já estudado no capítulo 2.

Os principais padrões de cabos e tecnologias LAN mais utilizados e suas distâncias seguem abaixo:

Nome	Meio de transmissão	Distância padrão
10BASE-T	UTP categoria 3 ou melhor	100 metros
100BASE-T	UTP categoria 5 ou melhor	100 metros
1000BASE-T	UTP Categoria 5e ou melhor	100 metros
1000BASE-SX	Fibra Multimodo	550 metros com diâmetro da fibra de 50 micrôn
1000BASE-LX	Fibra Multimodo	550 metros com diâmetro da fibra de 50 e 62,5 micrôn
1000BASE-LX	Fibra Monomodo	5 km

Para as conexões a 10Gbps via UTP ou 10GBASET normalmente são utilizados cabos categoria 6A (Cat6A) podendo chegar a 100m, porém em redes mais antigas com CAT6 essa distância é reduzida para uma faixa entre 38 e 55 metros no máximo.

### 3 Revisão sobre o Funcionamento dos Switches de Camada 2

Os switches são equipamentos que estão classificados por padrão na camada-2 do modelo OSI, ou seja, conseguem ler o endereço MAC e tomar decisão de encaminhamento com base na porta onde esse endereço está registrado.

As funções básicas de um switch camada 2 (layer-2) são:

- **Aprender endereços MAC** de origem dos dispositivos (micros, telefones IP, etc) conectados às suas portas.
- **Encaminhar ou filtrar quadros** com base no endereço MAC de destino dos quadros, lembrando que a filtragem ocorre geralmente quando temos HUBs conectados às portas dos switches.
- **Evitar Loops** de camada de enlace com o protocolo **Spanning-tree**, possibilitando redes com caminhos redundantes.

Ao iniciar um switch ele não tem conhecimento dos endereços MAC dos computadores conectados às suas portas. Nessa condição o switch faz um procedimento chamado **flooding** ou **inundação** de quadros quando recebe um MAC de destino desconhecido para encaminhar, pois como ele não sabe para que porta encaminhar o quadro ele envia para todas as portas uma cópia do quadro recebido (menos para a porta que originou o quadro), assim com certeza se o destino estiver conectado naquele segmento ele vai responder.

Não confunda esse processo com o envio de um broadcast, pois o processo de flooding não altera o MAC de destino, apenas envia uma **cópia** para as portas.

À medida que os computadores se comunicam o switch vai inserindo os MACs de origem em sua tabela de conteúdo (SAT/CAM – Content Adressable Memory), com isso o flooding é drasticamente reduzido e os quadros são encaminhados para as portas diretamente através de um link virtual ponto a ponto livre de colisões, o qual é chamado de microssegmento.

O encaminhamento dos quadros é realizado pela análise do endereço MAC de destino do quadro. Já o aprendizado dos MACs é feito com base no MAC de origem do quadro ethernet.

Quando um switch aprende um MAC de origem em uma de suas portas ele inicia um temporizador de inatividade, o qual se chegar ao máximo definido apaga o MAC aprendido, assim garante que se o computador foi movido ou retirado da rede não terá seu MAC preso naquela porta. Quando o mesmo MAC é recebido pela porta, ou seja, ele já é conhecido pelo switch, seu contador de inatividade é zerado e começa a contar novamente.

O nome desse temporizador é “aging timer” (temporizador de envelhecimento do endereço MAC). Maioria dos Cisco IOS definem 300s como padrão (5 minutos), porém esse parâmetro pode ser alterado. Veja saída do comando abaixo.

```
SW-DlteC#show mac address-table aging-time
Global Aging Time: 300
Vlan      Aging Time
-----
SW-DlteC#
```

A tabela de endereços MAC pode ser visualizada com o comando “**show mac address-table**”. As opções “**dynamic**” e “**static**” podem ser utilizadas com o comando “**show mac address-table**” para visualizar apenas entradas dinâmicas ou estáticas. Veja as saídas dos comandos abaixo, onde na coluna TYPE é possível identificar se o MAC foi aprendido de maneira estática ou dinâmica.

```
SW-DlteC#show mac address-table dynamic
```

Mac Address Table

Vlan	Mac Address	Type	Ports
10	001d.7060.d31b	DYNAMIC	Fa0/4
10	001e.130b.1aef	DYNAMIC	Gi0/1
30	001d.7060.d31b	DYNAMIC	Fa0/4
30	001e.130b.1aef	DYNAMIC	Gi0/1
1	001e.130b.1aef	DYNAMIC	Gi0/1

Total Mac Addresses for this criterion: 5

```
SW-DlteC#show mac address-table static
```

Mac Address Table

Vlan	Mac Address	Type	Ports
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU

Total Mac Addresses for this criterion: 4

SW-DlteC#

Conforme já mencionado, o broadcast é tratado pelo switch da mesma maneira que em uma rede com hubs, ou seja, é encaminhado (flooded) para todas as portas, pois o switch não tem a capacidade de segmentar os domínios de broadcast por não ler os endereços de camada-3.

O endereço de broadcast, seja local ou sobrecarregado, tem o endereço MAC **FFFF.FFFF.FFFF**.

Os endereços de multicast também tem seu encaminhamento igual ao de um broadcast, porém o MAC de um endereço de multicast está na faixa de **01-00-5E-00-00-00** até **01-00-5E-7F-FF-FF**. Note que os endereços de multicast em IPv4 sempre iniciam com **01-00-5E**.

Portanto o processo de flooding (copiar os quadros em todas as portas menos na porta de origem) é realizado quando o switch não conhece a porta para encaminhar o MAC de destino, quando recebe um quadro com MAC de destino contendo um endereço de broadcast ou de multicast.

Com isso podemos concluir que uma rede com switches elimina as colisões e segmenta perfeitamente os domínios de colisão, pois cada porta do switch é um domínio de colisão e como apenas um dispositivo está conectado a cada porta não acontece mais esse problema!

Mas no caso dos broadcasts o switch com a configuração padrão não tem a capacidade de segmentação, pois quando um switch recebe um broadcast ele precisa encaminhar a todas as portas, portanto todos os computadores receberão essas mensagens. Por isso é importante segmentar as redes utilizando VLANs.

Em redes de pequeno e até médio porte isso pode não ser um problema, mas agora imagine uma rede com mais 1.000 computadores (veja a foto abaixo). Com os sistemas operacionais atuais e serviços de rede IPv4 que utilizam os broadcasts em larga escala com certeza teremos problemas.



Quando segmentamos as LANs utilizando VLANs, cada LAN Virtual criada é um domínio de broadcast separado, portanto **melhora tanto a segregação do envio de broadcasts como do flooding**, pois se um quadro de destino não é conhecido em um switch com VLANs o **flooding é feito somente para as portas que estão na mesma VLAN** e não mais para todas as portas do switch.

Por exemplo, considere a tabela MAC mostrada com endereços dinâmicos anteriormente, suponha que a porta Fast 0/4 recebe um quadro com o destino 001b.5020.b310, para que porta o switch vai encaminhar esse quadro? Se você prestar atenção a porta fast 0/5 tem esse MAC mapeado, portanto o switch envia o quadro para essa porta. E se a mesma porta recebe na sequência um quadro para o destino a001.2220.bcb0, o que irá acontecer? Tente analisar antes de ler o próximo parágrafo.

Primeiro passo para resolver o problema anterior é **verificar se MAC está listado na tabela de endereços**, que nesse caso não está. Portanto o switch fará o Flooding, enviando para todas as portas que estão na mesma VLAN da fast 0/4, a qual é a VLAN 10, menos para a própria interface fast 0/4 que originou o quadro. Portanto as portas fast 0/5, Giga 0/1 e fast 0/6 receberão o quadro.

Entender esse funcionamento e saber analisar a tabela de endereços MAC é fundamental para a prova do CCENT!

### 3.1 Leds Indicativos em Switches e Roteadores

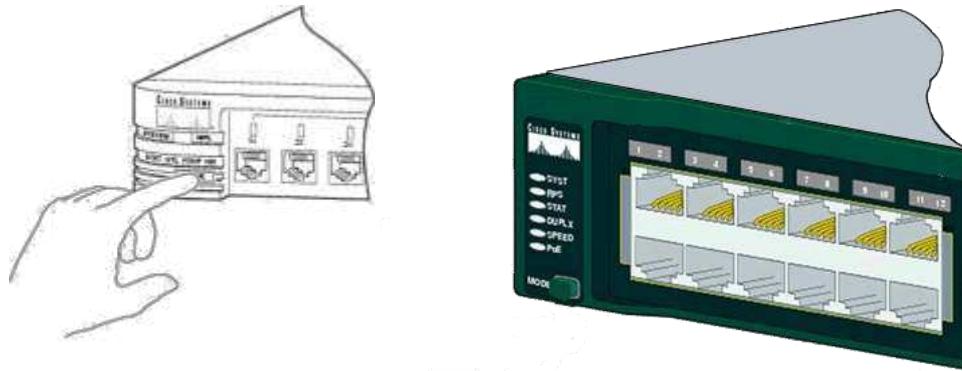
Existe uma variedade de tipos de Switches Cisco com diferentes capacidades de portas, eles podem variar de 8, 16, 24 ou 48 portas em modelos com portas fixas não modulares, isto é, sem opção de instalação de módulos de tributário (mais portas LAN), ou switches modulares onde o administrador de rede pode alojar portas conforme necessidade e capacidade máxima do switch. Abaixo temos a foto de switches da família Catalyst 2960.



Outras classificações de switches são baseadas na camada do modelo OSI que ele atua, por exemplo, switches Catalyst modelo 2950 e 2960 atuam na camada 2 do modelo OSI, já switches modelo Catalyst 3550 e 3560 podem atuar nas camadas 2 e 3 do modelo OSI, dependendo da sua configuração e versão de IOS, chamados **switches Layer-3** ou de **Camada-3**.

Nas empresas é comum também encontrarmos os switches chamados “**empilháveis**” ou “**stackable**”. Esses modelos de switch permitem a conexão local através de um cabo especial que permite o empilhamento deles, ou seja, a conexão realizada diretamente entre as placas mães dos switches chamadas de backplane. Isso ajuda a economizar portas dos switches, pois não precisaremos fazer entroncamento entre eles. Além disso, os switches empilhados são gerenciados como se fosse um único dispositivo, facilitando a configuração e manutenção.

Nos switches camada-2 não modulares da Cisco você encontrará na parte frontal esquerda um conjunto de LEDs e um botão chamado “Mode”, além disso, encima de cada porta existe um Led de status por porta Fast/Giga. A figura abaixo mostra o Sistema de leds dos Switches Cisco Catalyst 2950 e na figura 2 de um Catalyst 2960.



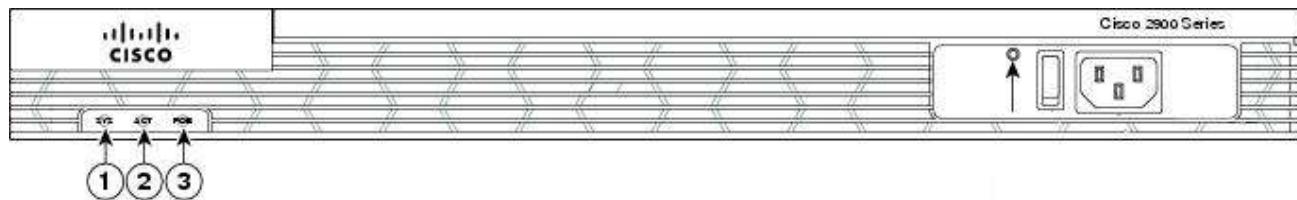
Você tem quatro opções de visualização para os switches da linha Catalyst 2950: Stat, Util, FDUP e 100 - as quais você seleciona apertando o botão MODE. Para a série Catalyst 2960 existem seis opções de visualização: SYST, RPS, Stat, Duplex, Speed e PoE - as quais você seleciona apertando o botão MODE.

A tabela a seguir mostra como interpretar as possibilidades de cores dos principais Leds por modo de visualização para o switch Catalyst 2950 e 2960.

Modo de Operação	Cor do Led (portas Fast)	Significado
STAT (Estado da porta)  Idem para os modelos 2950 e 2960	Desligado	Sem conexão física.
	Verde	Link lógico e físico detectado.
	Piscando Verde	Significa que a porta está trafegando dados.
	Alternando laranja e verde	Link com problema, por exemplo, erros CRC detectado, colisões em excesso, etc.
	Laranja	A porta não está trafegando dados, o STP está calculando Loops.
UTL (utilização)	Verde	Os LEDs mostram a utilização do Painel Traseiroplane em uma escala logarítmica.
FDUP (full ou half duplex)	Laranja	Porta está em half duplex.
	Verde	Porta está em full duplex.
100 (taxa de bits)	Laranja	Porta está em 10 Mbps.
	Verde	Porta está em 100 Mbps.

Em ambos os switches o Led de sistema **System** ou **Syst** deve estar verde, indicando funcionamento normal, caso esteja em laranja ou âmbar significa que o sistema está comprometido, normalmente sendo um problema grave e necessitando a troca do equipamento. Se o Led de sistema estiver apagado significa que o equipamento está desligado.

Nos roteadores os leds indicativos são normalmente três: de sistema (SYS - 1), de atividade (ACT - 2) e PoE (3), sendo que o terceiro pode não ter em alguns modelos. Veja figura abaixo com o painel frontal de um Cisco 2901.



O led SYS deve estar verde, se estiver apagado pode ser falta de energia e piscando problemas na inicialização, por exemplo, falta de IOS na memória Flash. O led de atividade indica recebimento de pacotes através de suas interfaces.

Além disso, as interfaces de LAN e/ou WAN também possuem leds indicativos de atividade.

Estes leds indicativos podem ajudar a resolver problemas no momento da instalação inicial dos equipamentos ou até mesmo durante a operação normal do sistema.

### 3.2 Revisão das Configurações Gerais em Switches

As **configurações gerais** de um switch variam em poucos detalhes da configuração de um roteador, por exemplo, o fato do switch não ter IP nas interfaces e também não ter porta auxiliar, porém a maioria das configurações é idêntica.

Para configurar o **IP de gerenciamento** do Switch temos que entrar na **VLAN** (Virtual LAN) de gerenciamento e adicionar o endereço. Todo switch da Cisco vem com as portas na VLAN1, chamada de VLAN default, de gerenciamento ou Nativa. Não existe switch sem VLAN, porém para facilitar a VLAN nativa se comporta diferente das outras e não marca seus quadros mesmo estando em um link entre switches ou trunk.

Vamos a um exemplo prático para relembrar o que vimos no capítulo 3, configurando um switch com os seguintes parâmetros gerais:

- Nome do host SW\_Vendas (**hostname**).
- Senha secreta para acesso ao modo privilegiado (**enable secret**) "dltec".
- Senhas de acesso a console "cisco1".
- Acesso telnet com usuário "dltec" e senha "cisco2" através de autenticação local.
- Limitar o tempo de inatividade quando o usuário estiver logado para 5 minutos (exec-timeout) em todas as lines disponíveis.
- Sincronizar o envio de mensagens para o terminal com a digitação (logging synchronous) em todas as lines disponíveis.
- Criptografar as senhas em modo texto (**service password-encryption**).
- IP de gerenciamento 10.0.0.2 /24 (**interface VLAN 1**).
- Configurar o IP do servidor DNS para 10.0.0.1 (**ip name-server**).
- O gateway padrão como 10.0.0.10 (**ip default-gateway**).
- Banner do dia como "ACESSO RESTRITO" (**banner motd**).

**Sugestão:** abra o Packet Tracer ou utilizando um switch modelo 2960 faça as configurações solicitadas acima sem olhar o resultado que está na sequência, depois compare com as configurações que realizamos a seguir e as explicações.

```

Switch#config term
! Configuração do hostname
Switch(config)#hostname SW_Vendas
SW_Vendas(config)#enable secret dltec
! Configuração do usuário e senha para autenticação local do acesso telnet
SW_Vendas(config)#username dltec password cisco2
! Configuração da line console
SW_Vendas(config)#line cons 0
SW_Vendas(config-line)#password cisco1
SW_Vendas(config-line)#login
SW_Vendas(config-line)#logging synchronous
SW_Vendas(config-line)#exec-timeout 5 0
! Configuração das lines vty
SW_Vendas(config-line)#line vty 0 15
SW_Vendas(config-line)#login local
SW_Vendas(config-line)#logging synchronous
SW_Vendas(config-line)#exec-timeout 5 0
SW_Vendas(config-line)#exit
SW_Vendas(config)#service password-encryption
SW_Vendas(config)#ip name-server 10.0.0.1
SW_Vendas(config)#ip default-gateway 10.0.0.10
! Configuração do banner
SW_Vendas(config)#banner motd @ ACESSO RESTRITO@
! Configuração da vlan1
SW_Vendas(config)#int vlan1
SW_Vendas(config-int)#ip address 10.0.0.2 255.255.255.0
SW_Vendas(config-int)#no shut
SW_Vendas(config-int)#end

```

**! Salvando a configuração para a startup-config**

SW\_Vendas#copy run start

SW\_Vendas#

Após essa breve revisão e estudo de topologias vamos iniciar a configuração de VLANs e outros recursos para melhorar o desempenho da nossa LAN.

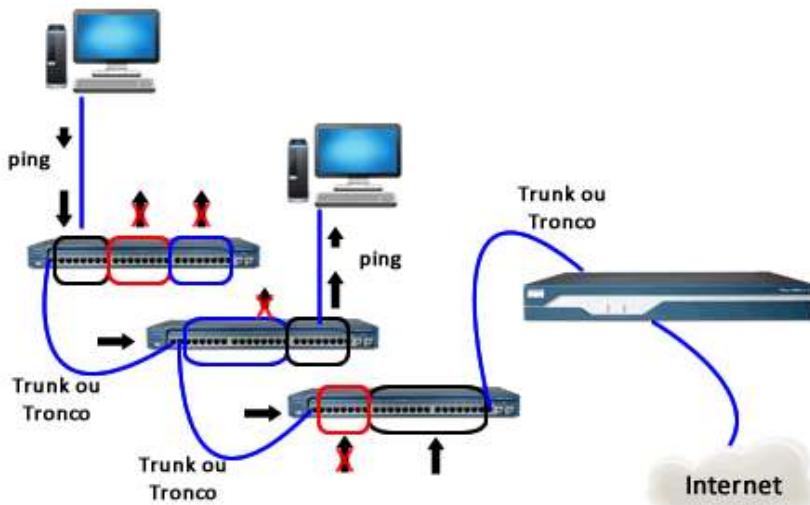
#### 4 Configurando VLANs e Trunks

Os Switches trabalham normalmente na camada-2 e **segmentam os domínios de colisão** através do encaminhamento ou filtragem baseado no MAC Address, porém **não segmentam domínios de broadcasts**. Ao receber um broadcast o switch automaticamente envia esse quadro para todas as portas, sendo que o quadro será parado apenas quando encontrar um roteador ou outro equipamento de camada-3.

Para melhorar a segmentação da rede e aumentar o nível de segurança podemos utilizar as **VLANs (LANs Virtuais)** para criar mais domínios de broadcast, separando a comunicação por função, área, setor ou quaisquer outras características necessárias que podem ser agrupadas logicamente.

Portanto, as **VLANs** são utilizadas nos switches para **separar domínios de broadcast**, por isso cada VLAN necessita de uma rede IP ou sub-rede própria. Em seus projetos de rede é importante lembrar que cada rede LAN ou WAN precisa de uma rede própria e quando sua LAN for dividida em VLANs, cada uma delas também precisará de uma sub-rede própria.

Além disso, não é possível uma VLAN acessar outra sem um equipamento de camada-3, o qual pode ser um roteador ou um switch layer-3, por exemplo, para um computador alocado na VLAN 10 pingar um micro que está na VLAN 20, mesmo que eles estejam conectados à portas do mesmo switch, eles necessitarão de um roteador para fazer essa comunicação.



Note na figura anterior que existem dois tipos de portas ou links em um switch:

- **Portas de acesso:** onde são conectados os dispositivos finais, como computadores, telefones IP, servidores, etc.
- **Portas de tronco ou trunk:** as quais são utilizadas para fazer a comunicação entre os switches.

As **portas de acesso** são portas que você conecta o usuário final e não devem ser conectadas a outros switches para estender a rede, pois se subentende que nessa porta você terá apenas **um** elemento configurado.

Para conectar outros switches são utilizadas as **portas tronco (trunk)**, as quais tem uma função especial de transmitir o tráfego das VLANs configuradas no switch.

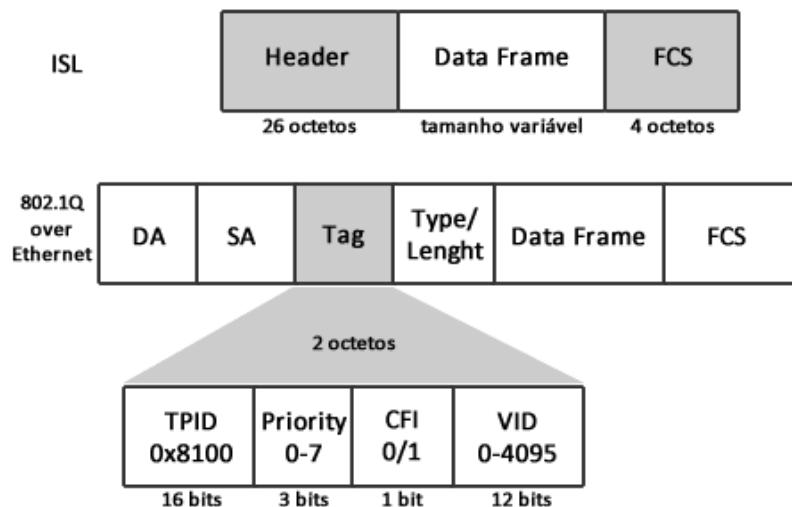
Para fazer esse tipo de função é preciso uma técnica de identificação dos pacotes pertencentes a cada VLAN, pois senão como o switch remoto vai identificar para que portas encaminhar os pacotes? Lembre que a regra das VLANs é que somente portas que pertencem ao mesmo grupo podem se comunicar.

Para que um trunk transporte a informação de todas as VLANs e consiga separar de quem é cada quadro é utilizada uma técnica chamada “**marcação de quadros**” ou “**frame tagging**”.

Existem dois padrões suportados pelos equipamentos da Cisco para marcação de quadro:

- **802.1Q** – padrão aberto para comunicação entre Switches.
- **ISL (Inter Swicth Link)** – padrão proprietário da Cisco.

O 802.1 Q e o ISL utilizam uma estrutura de quadro de camada 2 ligeiramente diferente do quadro original do Ethernet, incluindo **um campo para identificar a que VLAN** aquele quadro pertence. Portanto, quando um switch recebe um quadro por um link trunk ele consegue saber para que porta ou portas o quadro deve ser encaminhado. Veja na figura abaixo o quadro do 802.1Q. Perceba que existe um campo chamado Tag onde existe o **VID** ou **VLAN ID**, que indica o número da VLAN que aquele quadro pertence.



As VLANs que vamos trabalhar durante o curso são **centradas em portas**, ou seja, vamos definir quais portas dos switches pertencem a uma determinada VLAN (alocação manual).

Existem VLANs que podem utilizar o protocolo de camada-3 como base ou ainda serem alocadas automaticamente através de um controle central, porém não são abordadas no CCENT/CCNA.

Resumindo, utilizar VLAN é criar um **grupo de portas** que vai ser definido por um **número identificador (VLAN ID)** e **definir que portas do switch pertencem a esse grupo**. Esse grupo deve pertencer a uma mesma rede ou sub-rede IP e não poderão se comunicar com outros grupos diferentes (outras VLANs) sem um dispositivo de camada 3 que faça o roteamento desses pacotes, pois as VLANs segregam domínios de broadcast.

Traduzindo o que falamos acima em configuração você deverá seguir os seguintes passos para criar uma VLAN e alocar as portas:

- Configurar o VTP (Vlan trunk protocol) como transparente ou servidor (config padrão), que será visto posteriormente;
- Configurar os links trunks;
- Criar as VLANs;
- Fazer o **VLAN membership**, ou seja, vincular as portas dos switches às VLANs.

#### 4.1 Criando VLANs

Nos switches da linha 2950/2960/3560 e demais com Cisco IOS pode-se criar uma VLAN de duas formas. A primeira em modo de configuração global e a segunda através do VLAN DATABASE. Abaixo segue exemplo de configuração em modo de configuração global com o comando "vlan".

```
Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#vlan 5
Switch1(config-vlan)#name informatica
Switch1(config-vlan)#vlan 6
Switch1(config-vlan)#name engenharia
Switch1(config-vlan)#end
Switch1#
```

Portanto o comando "**vlan**" vem seguido do número da VLAN (VLAN-ID). O segundo comando opcional "**name**" define um nome para a VLAN. Para apagar uma VLAN criada basta digitar "no **vlan**" seguido do VLAN-ID a ser apagado, por exemplo, "**no vlan 6**" apaga o VLAN-ID 6 do banco de dados de VLAN.

Segundo método utilizando o banco de dados de VLANs ou "**Vlan Database**" em modo privilegiado. O switch mostrará um aviso indicando que esse método não é aconselhável e deve-se preferencialmente utilizar os comandos em modo de configuração global, além disso, é necessário dar um comando "apply" para validar a configuração no switch no final da configuração, veja exemplo abaixo.

```
Switch1#vlan database
Switch1(vlan)#?
Switch1(vlan)#vlan 5 name informatica
VLAN 5 modified:
  Name: informatica
Switch1(vlan)#vlan 10 name marketing
VLAN 10 added:
  Name: marketing
Switch1(vlan)#vlan 11 name administracao
VLAN 11 modified:
  Name: administracao
Switch1(vlan)#apply
APPLY completed.
Switch1(vlan)#^Z
Switch1#
```

Após criadas as VLANs podemos utilizar os comandos "show vlan" ou "show vlan brief" para verificar se as VLANs foram criadas corretamente. Acompanhe o exemplo abaixo.

Switch2#show vlan brief		
VLAN Name	Status	Ports

```

1    default           active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                      active   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                      active   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                      active   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                      active   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                      active   Fa0/21, Fa0/22, Fa0/23, Fa0/24

10   ADM              active
20   OP               active
30   DIR              active

1002 fddi-default    active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default   active

Switch2#

```

O comando "show vlan brief" é um resumo do "show vlan".

É importante verificar que existem VLANs pré-configuradas nos switches, as quais não podem ser apagadas ou modificadas. No total são cinco VLANs: a VLAN 1 e de 1002 a 1005.

A faixa total de VLANs permitidas vai de 1 a 4094, sendo que o valor padrão vai de 1 a 1005 e os valores acima de 1005 fazem parte de uma faixa estendida de valores que não são suportadas por todos os modelos de switches.

Além disso, a faixa de valor estendida de VLANs não é suportada pelo protocolo VTP, ou seja, se você criar uma VLAN com ID 1010, por exemplo, ele não será anunciado pelos servidores VTP.

As VLANs criadas podem ser desabilitadas com o comando "shutdown" dentro do modo de configuração de VLANs.

Todas as portas dos switches já vem alocadas na VLAN 1, a qual é chamada VLAN Nativa ou de gerenciamento.

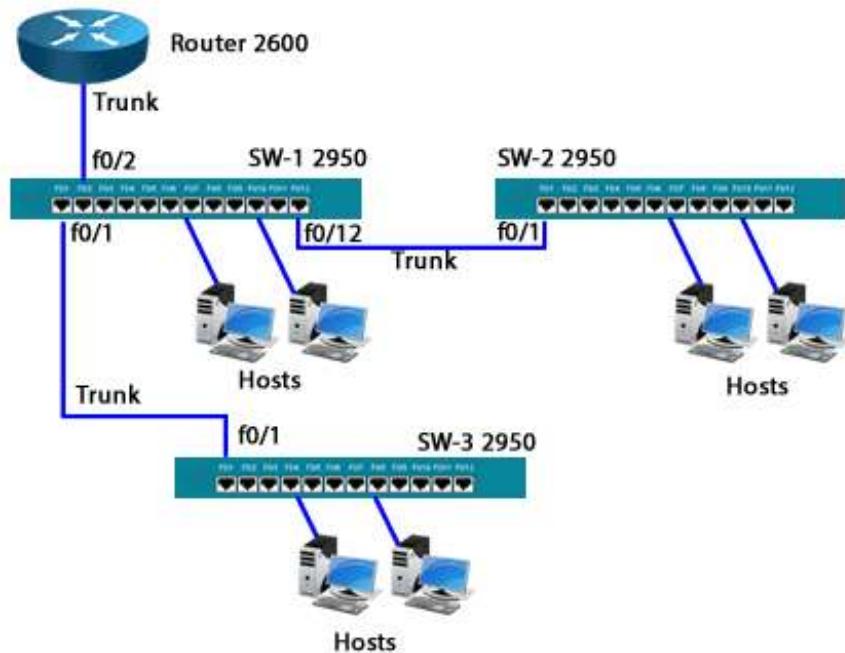
#### 4.2 Atribuindo Portas às VLANs

Agora que as VLANs estão criadas podemos associar as portas dos switches às VLANs recém-criadas, processo que chamados de "**VLAN Membership**".

Uma porta só pode pertencer a uma VLAN de dados e por default todas as portas estão associadas à VLAN 1. Existe mais um tipo de VLAN chamada "Voice VLAN" utilizada para os telefones IP. Em portas onde temos simultaneamente computadores e telefones IP podemos alocá-la a uma VLAN de dados para os computadores e uma VLAN de voz para o telefone IP.

**Sugestão de atividade prática:** Abra o Packet Tracer ou o terminal do seu switch de laboratório, pode ser um 2950 ou 2960, entre em modo privilegiado e digite o comando "**show vlan brief**", confirme que todas as portas estão no padrão alocadas na **VLAN 1**. Mantenha o simulador ou seu switch conectado para repetir os comandos que vamos estudar a seguir.

As portas de um switch podem ser do tipo acesso "**access**" (para conexão de hosts – sem marcação de quadro ou Tag) ou "**trunk**" (para entroncamento entre switches – com marcação de quadro ou Tag). Antes de alocar uma porta em uma VLAN é recomendado que ela seja configurada como **acesso**.



Para fazer o VLAN Membership entre em modo de configuração de interface com o comando **“switchport mode access”** para configurar a porta como acesso. Em seguida defina a VLAN que a porta pertence com o comando **“switchport access vlan”** seguido do **VLAN-ID**. Veja exemplo a seguir.

```

Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#interface f0/5
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 5
Switch1(config-if)#inter f0/10
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)^Z
Switch1#
  
```

No exemplo acima colocamos a porta fast0/5 na VLAN 5 e a fast0/10 na VLAN10.

Você pode também configurar várias portas simultaneamente através da opção **Range**. Veja exemplo abaixo onde as portas fast 0/2 até a 0/24 serão alocadas na VLAN 10 com apenas três linhas de configuração.

```

Switch1(config-if)#interface range fast0/2 - 24
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
  
```

Utilizando o comando **“show vlan brief”** podemos verificar a configuração realizada, conforme exemplo abaixo.

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/6, Fa0/7, Fa0/8, Fa0/9

```

Fa0/11, Fa0/12, Fa0/13, Fa0/14
Fa0/15, Fa0/16, Fa0/17, Fa0/18
Fa0/19, Fa0/20, Fa0/21, Fa0/22
Fa0/23, Fa0/24

5   Operacao          active  Fa0/5
10  Comercial         active  Fa0/10
1002 fddi-default    active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default   active
SwitchA1#

```

Você pode ainda optar por ver a configuração de uma VLAN individualmente, usando o comando "show vlan id [#]", por exemplo, o comando "Switch1#show vlan id 10" mostra os parâmetros somente da VLAN 10. Veja exemplo abaixo.

```

dltecswicth#conf t
dltecswicth(config)#interface range fast 0/1 - 9
dltecswicth(config-if)#switchport mode access
dltecswicth(config-if)#switchport access vlan 10
dltecswicth(config-if)#interface fast 0/24
dltecswicth(config-if)#switchport mode access
dltecswicth(config-if)#switchport access vlan 10
dltecswicth(config-if)#end
dltecswicth#
dltecswicth#show vlan id 10
VLAN Name                  Status     Ports
-----                    -----
10  VLAN0010                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                         Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                         Fa0/9, Fa0/24
-----                    -----
VLAN Type      SAID      MTU      Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----                    -----
10  enet        100010    1500      -       0       0       -      -      -
-----                    -----
Remote SPAN VLAN
-----
Disabled
Primary Secondary Type      Ports
-----                    -----
dltecswicth#

```

Você pode ter uma VLAN configurada estaticamente ou dinamicamente. Nos exemplos anteriores estão sendo configuradas **VLANs estáticas**, ou seja, entradas manuais via administrador de rede. Para configurar VLANs dinamicamente você necessita ter um servidor VMPS instalado em sua rede, porém esse assunto não é abordado no CCENT/CCNA.

#### 4.2.1 Exemplo Prático de VLAN Membership

Vamos a mais um exemplo para finalizar o capítulo. Vamos configurar um switch 2960 com 24 portas que possui duas interfaces Giga para entroncamento com as seguintes características:

- VLAN Nativ: 1
- VLAN COMERCIAL: 10
- VLAN ADMINISTRATIVA: 20
- VLAN SUPORTE: 30

As portas de 1 a 10 devem pertencer à VLAN comercial, de 11 a 15 à VLAN administrativa, de 16 a 20 à VLAN do suporte e as portas de 21 a 24 devem ser desabilitadas. As portas Gigabit serão links trunks. A configuração será realizada nas seguintes etapas:

- Criação e nomenclatura das VLAN's
- Alocação de portas
- Configuração dos trunks com o comando "**switchport mode trunk**".

Vamos supor que as demais configurações gerais já foram realizadas. Veja abaixo a aplicação dos comandos.

```
Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#vlan 10
Switch1(config-vlan)#name COMERCIAL
Switch1(config-vlan)#vlan 20
Switch1(config-vlan)#name ADMINISTRATIVA
Switch1(config-vlan)#vlan 30
Switch1(config-vlan)#name SUPORTE
Switch1(config-vlan)#interface range f0/1 - 10
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#interface range f0/11 - 15
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 20
Switch1(config-if)#interface range f0/16 - 20
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 30
Switch1(config-if)#interface range f0/21 - 24
Switch1(config-if)#shutdown
Switch1(config-vlan)#interface range Giga0/1 - 2
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#end
Switch1#copy run start
Switch1#
```

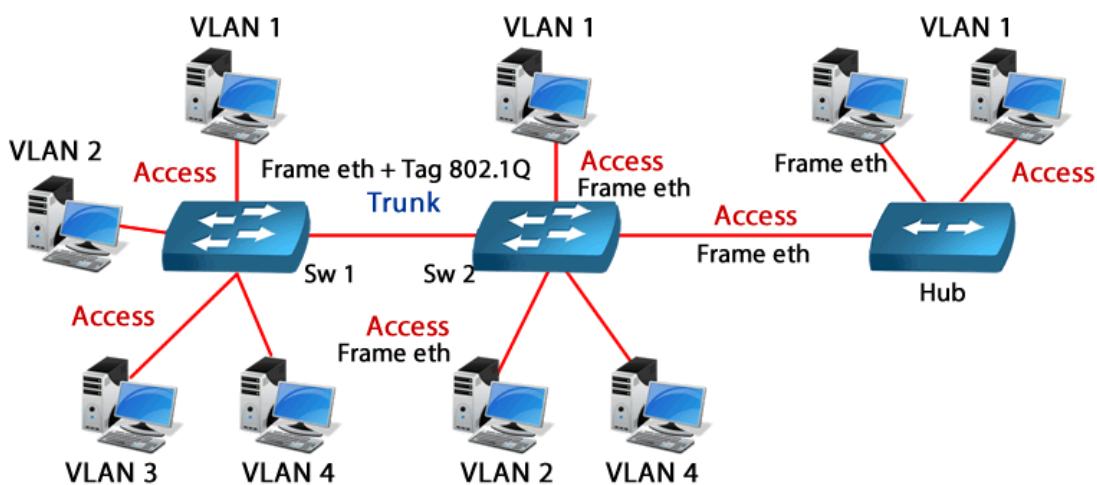
**Dica prática:** Quando os trunks forem conectados e devidamente configurados em ambos os lados as portas deles não serão mais visualizadas em nenhuma VLAN no comando "**show vlan brief**", pois nesse comando aparecerão somente portas de acesso.

#### 4.3 Interligando Switches e Roteadores – Configurando Links Trunk

Como já comentado anteriormente, os "**trunks**" são links utilizados para transportar as informações de VLANs por entre uma rede de switches. Eles são utilizados em conexões entre switches ou entre roteadores e switches para fazer o roteamento entre VLAN.

Nos switches da Cisco os dois tipos de protocolos que executam trunking são o ISL (proprietário da Cisco) e o 802.1Q (protocolo aberto da IEEE).

Ambos utilizam o mesmo princípio de marcar com uma etiqueta ou tag os quadros quando eles são enviados através dos trunks. Quando eles são recebidos no switch remoto essa tag é avaliada e os quadros são encaminhados conforme VLAN-ID contido na etiqueta. Quando o quadro é enviado para o computador através do link de acesso é realizado via um quadro ethernet normal, sem marcação. Veja figura abaixo.



Em switches camada-2 como os da linha 2950 e 2960 a configuração de trunking pode ser realizada apenas utilizando o protocolo **802.1Q**. Veja exemplo de configuração abaixo.

```
2950#config t
Enter configuration commands, one per line. End with CNTL/Z.
2950(config)#int fastethernet 0/12
2950(config-if)#switchport mode trunk
2950(config-if)#^Z
2950#
```

Normalmente em switches camada-3 as interfaces suportam mais de um protocolo, por exemplo, o 802.1Q e ISL, portanto antes de configurar o trunk é necessário **definir o protocolo** ser utilizado. Veja exemplo abaixo onde um trunk 802.1Q será habilitado com o comando “switchport trunk encapsulation dot1q”. A opção dot1q representa o protocolo 801.Q.

```
Switch(config)#int fastethernet 0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
```

Para verificar as portas que estão em trunking utilize o comando “**show interfaces trunk**”.

Para desabilitar o trunking em uma porta entre com o comando “**switchport mode access**” na interface. Para verificar a configuração digite o comando “**show running-config**”.

#### 4.3.1 Administrando o Encaminhamento de VLANs nos Trunks

As portas trunk nos switches por padrão encaminham informações de **todas as VLANs**, portanto todos os VLAN-IDs possíveis de 1 a 4094 estarão associados a um link de trunking a menos que sejam excluídos manualmente daquele link.

Uma maneira de administrar as VLANs que serão encaminhadas em um “trunk” é com o comando “**switchport trunk allowed vlan [vlan-ID1, vlan-ID2,...]**”. No exemplo abaixo mostramos a configuração para permitir que somente as vlans 5, 6 e 7 acessem o “trunk” da porta fast 0/1 do switch.

```
2960(config)#int fastethernet 0/1
2960(config-if)# switchport trunk allowed vlan 5,6,7
```

Existem outras opções no comando que possibilitam administrar as mudanças (**Moves, Adds and Changes**) que precisam ser realizadas no dia a dia da operação de uma rede de switches,

por exemplo, adicionar ou remover uma VLAN em um trunk. Veja na saída abaixo as opções possíveis para administração dos trunks.

```
2960(config-if)#switchport trunk allowed vlan ?
WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
add     add VLANs to the current list
all     all VLANs
except  all VLANs except the following
none    no VLANs
remove   remove VLANs from the current list
2960(config-if)#switchport trunk allowed vlan
2960(config-if)#^Z
2960#
```

Vamos agora estudar com exemplos o uso dessas demais opções.

Por exemplo, você deseja permitir todas as VLANs menos às de ID 100 a 200 de serem encaminhadas por um trunk, nesse caso podemos utilizar a opção “**except**”, que permite todas exceto as definidas no comando, veja a configuração abaixo.

```
2960(config)#int fastethernet 0/1
2960(config-if)# switchport trunk allowed vlan except 100-200
```

O traço entre o 100 e 200 significa “até”. Você pode fazer expressões utilizando o traço (até) e a vírgula (e), por exemplo, a opção “**1,3,5-10**” seleciona as VLANs 1, 3 e de 5 até 10 no mesmo comando.

As opções “**add**” e “**remove**” adicionam e removem VLANs sem alterar toda a lista de permissão já configurada. Por exemplo, você quer tirar da lista das VLANs permitidas apenas a VLAN 10 poderia utilizar o comando “**switchport trunk allowed vlan remove 10**”.

Em switches de outros fabricantes geralmente as VLAN's são bloqueadas nos trunks e o administrador deve configurar as VLANs que podem trafegar no backbone. Filosofia onde todas as VLANs são bloqueadas a não ser as permitidas.

#### 4.3.2 VLAN Nativa

Já estudamos durante o curso que a VLAN 1 é a padrão utilizada em todas as portas dos switches Cisco e também chamada de Nativa.

Mas o que tem de especial em uma VLAN Nativa? Simplesmente que ela não usa marcação de quadro em links de trunk e também que um switch camada-2 responde para o IP de gerenciamento configurado nela.

Você saberia dizer porque a VLAN Nativa não pode marcar seus quadros com um protocolo de trunking como o 802.1Q ou ISL? **Pense um pouco antes de ver a resposta abaixo.**

**Resposta:** Para que o switch remoto possa identificar que VLAN-ID está sendo utilizado como VLAN Nativa e possibilitar entroncamento com dispositivos que não suportam protocolos de trunking.

Para que o gerenciamento via IP funcione corretamente em todos os switches a VLAN Nativa deve ser a mesma em toda a rede, por isso que o padrão é sempre o VLAN-ID 1 nos switches Cisco, sejam eles camada 2 ou 3.

Como a informação da VLAN nativa padrão é de conhecimento público, a Cisco recomenda que você utilize um VLAN-ID não utilizado para esse fim. Para isso basta criar uma nova VLAN diferente de “1” e configurar nos links trunks qual a nova VLAN nativa ou untagged.

Veja exemplo abaixo onde vamos configurar a VLAN 100 como nativa em um switch que usa apenas a porta fast 0/1 como trunk:

```
Cat2950(config)#vIan 100
Cat2950(config-vlan)#name Nova-Nativa
Cat2950(config-vlan)#interface fast 0/1
Cat2950(config-if)#switchport trunk native vIan 100
```

Depois você precisará também desativar a VLAN 1 e trocar o IP de gerenciamento para a Interface VLAN 100.

```
Cat2950(config-if)#interface vIan 1
Cat2950(config-if)#shut
Cat2950(config-if)#interface vIan 100
Cat2950(config-if)#ip address 192.168.1.10 255.255.255.0
Cat2950(config-if)#no shutdown
```

Lembre-se que ao mudar a VLAN nativa ou de gerenciamento do VLAN-ID 1 para outro valor essa configuração deve ser aplicada em todos os links de trunk, senão haverá um problema de "mismatch" entre os switches, ou seja, não haverá comunicação via VLAN nativa e o switch não poderá ser gerenciado via acesso remoto.

#### 4.4 Entendendo o Protocolo DTP

As portas dos switches Cisco vêm por padrão com um protocolo chamado **DTP** (Dynamic Trunk Protocol – protocolo de trunk dinâmico) ativado, o qual é proprietário da Cisco.

Esse protocolo tem a função de determinar qual o estado que uma porta deve subir em determinadas condições através de uma **negociação**. Normalmente as portas estão configuradas por padrão com o **DTP em modo automático**.

A recomendação da Cisco é **não utilizar o DTP** e definir nas portas o modo de operação de acesso (**switchport mode access**) para as portas de clientes e trunk (**switchport mode trunk**) para as portas de backbone que conectam switches e roteadores.

Existem também os modos dinâmicos: automático (auto – padrão das portas) ou desejável (desirable), veja a saída abaixo:

```
Switch(config-if)#switchport mode ?
  access  Set trunking mode to ACCESS unconditionally
  dynamic Set trunking mode to dynamically negotiate access or trunk mode
  trunk   Set trunking mode to TRUNK unconditionally
Switch(config-if)#switchport mode dynamic ?
  auto    Set trunking mode dynamic negotiation parameter to AUTO
  desirable Set trunking mode dynamic negotiation parameter to DESIRABLE
```

Resumidamente temos então três tipos de condições de entroncamento:

- **Ativado com o comando “switchport mode trunk”**: os anúncios DTP são enviados periodicamente para porta remota anunciando que ela está mudando dinamicamente para um estado de entroncamento, ou seja, que é um trunk. A porta local nesse caso está sempre ativada, independente do estado da porta remota. Para que uma porta trunk ativa com esse comando não faça nunca a negociação do DTP basta adicionar na interface o comando **“switchport nonegotiate”**.
- **Dinâmico automático com o comando “switchport mode dynamic auto” (Padrão)**: anúncios DTP são enviados periodicamente para porta remota, sendo que a porta local anuncia para porta remota que é capaz de entroncar, mas não solicita a

passagem para o estado de tronco, pois a porta local só muda para o estado de tronco caso a porta remota fosse configurada como ativo ou desejável (desirable). Se ambas as portas nos switches forem definidas como auto, elas negociam para ficar no estado do modo de acesso.

- **Dinâmico desejável com o comando “switchport mode dynamic desirable”:** os anúncios DTP também são enviados periodicamente para porta remota, porém a porta local anuncia para porta remota que é capaz de entroncar e solicita a passagem para o estado de entroncamento. A porta local muda para o estado de tronco caso a porta remota estiver sido configurada como ativa, desejável (desirable) ou automático. Se a porta remota estiver no modo de não negociação (Access ou acesso), a porta do switch permanecerá como uma porta de acesso.

A recomendação da Cisco é **não utilizar o DTP** e definir o estado das portas, ou seja, se a porta é de acesso insira o comando **“switchport mode Access”** e se ela é um trunk deve ser inserido o comando **“switchport mode trunk”** e o comando **“switchport nonegotiate”** para evitar que portas trunks negoçiem via DTP, dessa maneira a porta trunk sobe somente se uma outra porta trunk for conectada do outro lado.

Na tabela abaixo temos os estados que as portas entre dois switches podem assumir dependendo da configuração do seu modo administrativo (Administrative Mode).



Administrative Mode	access	dynamic auto	trunk	dynamic desirable
access	Access	Access	Access	Access
dynamic auto	Access	Access	Trunk	Trunk
trunk	Access	Trunk	Trunk	Trunk
dynamic desirable	Access	Trunk	Trunk	Trunk



O estado que a porta assume é chamado “modo de operação” (Operational Mode), você vai ver na sequência onde encontrar esses dados em comandos show. Note na tabela o porquê se pegarmos dois switches com configuração padrão e interconectá-los com um cabo cruzado (cross) a porta sobre como Acesso (Access), pois como as duas estão configuradas como **“Dynamic Auto”** elas sobem como uma porta de acesso.

A configuração em uma ponta do link entre dois switches como **trunk** e na interface remota como **access** não é recomendada, pois podem gerar problemas e a porta não subir.

Para verificar o estado do DTP utilize o comando **“show interfaces fast 0/1 switchport”**. Nesse exemplo o trunk está configurado na porta fast 0/1. Você pode também utilizar simplesmente o comando **“show interfaces switchport”**, porém assim serão mostradas todas as portas e a visualização pode ficar mais complicada.

Veja a saída do comando abaixo para a interface Fast 0/1 com o comando “**switchport mode trunk**” habilitado.

```
Switch0#show interfaces fast 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
Switch0#
```

Para verificar quais interfaces estão ativadas como trunk utilize o comando “**show interface trunk**”, veja a saída do comando a seguir.

```
Switch0#show interfaces trunk
Port      Mode       Encapsulation  Status      Native vlan
Fa0/1     on        802.1q        trunking   1
Fa0/2     auto      n-802.1q      trunking   1
Fa0/3     auto      n-802.1q      trunking   1
Fa0/4     on        802.1q        trunking   1

Port      Vlans allowed on trunk
Fa0/1    1-1005
Fa0/2    1-1005
Fa0/3    1-1005
Fa0/4    1-1005

Port      Vlans allowed and active in management domain
Fa0/1    1,10,20
Fa0/2    1,10,20
Fa0/3    1,10,20
Fa0/4    1,10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,10,20
Fa0/2    1,10,20
Fa0/3    1,10
Fa0/4    1,10,20
```

No campo **mode** você poderá ver se a interface está ativa (on – switchport mode trunk), automática (auto – switchport mode dynamic auto) ou desejável (desirable - switchport mode dynamic desirable). No campo “**Vlans allowed on trunk**” temos as VLANs que esses trunks

podem encaminhar, como já vimos o padrão dos switches da Cisco é encaminhar todas as VLANs, ou seja, do VLAN-ID 1 até 1005, faixa padrão de numeração de VLANs.

Logo abaixo temos o campo “**Vlans allowed and active in management domain**” mostrando as VLANs que estão ativas no momento, apesar do trunk permitir todas as VLANs ele só envia as que estão configuradas, pois senão seria gerado tráfego extra sem utilidade para a rede.

No último campo marcado em amarelo “**Vlans in spanning tree forwarding state and not pruned**” podemos verificar que as VLANs criadas são já tem automaticamente uma instância de Spanning-tree criada para proteger a topologia contra loops de camada-2.

#### 4.5 Protocolo VTP

O protocolo VTP é utilizado para propagar informações sobre VLANs entre os switches de uma mesma rede local, sendo um protocolo da camada 2 utilizado para manter a configuração de VLANs consistentes em uma rede de switches Cisco, pois ele é um protocolo proprietário.

Com o protocolo VTP o administrador de redes pode criar VLANs em apenas um ponto (**switch VTP servidor**) e esses VLANs ID criados são passados através de anúncios de VTP através de links trunks para os demais switches **Clientes** na rede. O VTP define um domínio formado por um switch configurado como servidor e outros como cliente.

Para criar VLANs em switches Cisco ele deve estar configurado como Servidor VTP (**vtp mode server**), transparente (**vtp mode transparent**) ou com o VTP desabilitado (**vtp mode off**).

Os switches que estiverem como clientes (**vtp mode client**) **não terão permissão** para inclusão ou alteração de VLANs, eles recebem anúncios do servidor VTP com as VLANs criadas nos servidores e o administrador de rede pode apenas alocar as portas dos clientes nessas VLANs.

**Por padrão** todos os switches vêm configurados como **Server**, por isso que normalmente não percebemos a presença do VTP nos switches, porém se o protocolo não for utilizado é importante desabilitar ou configurar os switches como transparente, pois o VTP pode trazer consequências negativas na rede se seu uso não for devidamente planejado e configurado corretamente nos switches da rede.

**Importante:** somente a criação dos VLANs ID é feita de forma centralizada com o VTP, porém a alocação de portas nas VLANs continua sendo feitas localmente em cada switch.

O VTP será estudado mais a fundo no ICND-2, nos laboratórios do CCENT utilize os comandos “vtp mode transparent” ou “vtp mode off”, sendo que esse último é suportado em switches mais atuais.

Nessa versão do CCENT as configurações tentam ao máximo ignorar a existência do VTP e administrar as VLANs de maneira individual em cada switch da rede. Em seus laboratórios procure utilizar os switches como transparente, mas se o VTP for utilizado lembre-se que:

- Switches com Cisco IOS mais antigos suportam versões 1 e 2, os mais novos suportam das versões 1 a 3 do VTP.
- As informações do VTP são passadas apenas via links de Trunk, sem trunks configurados as mensagens não são trocadas entre os switches.
- Os servidores podem configurar VLANs apenas da faixa padrão de 1 a 1005 nas versões de VTP 1 e 2. A versão 3 suporta a faixa estendida de VLANs (1006 a 4094).
- Os clientes não podem nem criar, apagar ou modificar VLANs.
- No comando show running-config as configurações de VLAN não são mostradas.

Com o comando “show vtp status” você pode verificar as configurações do VTP, veja exemplo abaixo onde temos um switch que suporta VTP versões 1 a 3.

```
SW-DlteC-Rack-01#show vtp status
VTP Version capable          : 1 to 3
VTP version running          : 2
VTP Domain Name              : dltec
VTP Pruning Mode             : Enabled
VTP Traps Generation         : Disabled
Device ID                    : 0024.5161.6a00
Configuration last modified by 192.168.1.5 at 5-5-16 15:53:52
Local updater ID is 192.168.1.5 on interface V110 (lowest numbered VLAN interface
found)

Feature VLAN:
-----
VTP Operating Mode           : Server
Maximum VLANs supported locally : 255
Number of existing VLANs      : 13
Configuration Revision        : 14
MD5 digest                   : 0x8F 0xB1 0x3D 0x5F 0x48 0x6C 0x3C 0x5D
                                0x3D 0x37 0x35 0x5F 0x4B 0xA8 0xCE 0x96
SW-DlteC-Rack-01#
```

Você também pode encontrar essa saída se seu switch não suportar VTP versão 3.

```
SW-DlteC-Sala-01#show vtp status
VTP Version                  : 2
Configuration Revision        : 14
Maximum VLANs supported locally : 250
Number of existing VLANs      : 13
VTP Operating Mode           : Client
VTP Domain Name              : dltec
VTP Pruning Mode             : Enabled
VTP V2 Mode                  : Enabled
VTP Traps Generation         : Disabled
MD5 digest                   : 0x8F 0xB1 0x3D 0x5F 0x48 0x6C 0x3C 0x5D
Configuration last modified by 192.168.1.5 at 5-5-16 15:53:52
SW-DlteC-Sala-01#
```

#### 4.5.1 Numeração Estendida de VLANs e VTP

Até esse momento estudamos com a saída do comando “show vlan” que temos por padrão a VLAN 1 já configurada, assim como das VLANs 1002 a 1005 inseridas automaticamente pelo switch. Essas VLANs não podem ser alteradas ou apagadas.

Portanto, o VLAN-ID padrão vai de 1 a 1005, sendo que temos úteis para criar novas VLANs dos IDs 2 a 1001. Essa é a faixa padrão da numeração de VLANs e suportada pelo protocolo VTP, ou seja, VLANs de 1 a 1005 podem ser propagadas entre os switches via anúncios VTP. Veja a saída do comando “**show vlan brief**” a seguir.

```
SwitchA1#sho vlan brief
VLAN Name                               Status    Ports
----- ----- -----
1   default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                         Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                         Fa0/10, Fa0/11, Fa0/12, Fa0/13,
                                         Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                         Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                         Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Como já estudamos, existe também uma faixa de VLANs estendida (extended VLAN-ID) que vai de **1006 a 4094**, porém ela não pode ser utilizada se os switches estiverem utilizando o protocolo VTP, portanto, para que um switch utilize a faixa estendida de VLANs ele precisa ser configurado como transparente (**vtp mode transparent**).

Veja exemplo abaixo, onde ao tentar configurar a VLAN 1010 em um switch VTP server recebemos uma mensagem de erro.

```
SW-DlteC(config)#vtp mode server
Setting device to VTP Server mode for VLANS.
SW-DlteC(config)#vlan 1010
SW-DlteC(config-vlan)#exit
% Failed to create VLANs 1010
Extended VLAN(s) not allowed in current VTP mode.
%Failed to commit extended VLAN(s) changes.
```

Agora vamos repetir o mesmo teste configurando o switch como transparente abaixo.

```
SW-DlteC(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
SW-DlteC(config)#vlan 1010
SW-DlteC(config-vlan)#exit
SW-DlteC(config)#int f0/19
SW-DlteC(config-if)#switchport access vlan 1010
SW-DlteC(config-if)#do sho vlan brief
```

VLAN Name	Status	Ports
1 default	active	
10 corp	active	Fa0/1, Fa0/2, Fa0/3, Fa0/5, Fa0/6, Fa0/7, Fa0/9, Fa0/10, Fa0/11, Fa0/13, Fa0/14, Fa0/17, Fa0/18, Fa0/20 Fa0/21, Fa0/22
20 sala-aula	active	Fa0/21, Fa0/22
30 vlan-voz	active	Fa0/4, Fa0/5, Fa0/6 Fa0/8, Fa0/11, Fa0/12 Fa0/14, Fa0/15
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	
1010 VLAN1010	active	Fa0/19

Agora se tentarmos voltar o switch como servidor receberemos uma mensagem de erro confirme exemplo a seguir.

```
SW-DlteC(config)#vtp mode server
Device mode cannot be VTP Server for VLANs because extended VLAN(s) exist
SW-DlteC(config)#End
```

Na mensagem o IOS informa que não poderemos configurar o switch como VTP Server por existir VLAN na faixa estendida configurada nele. Portanto, para utilizarmos a faixa estendida de VLANs primeiro teremos que reconfigurar o switch para o modo transparente.

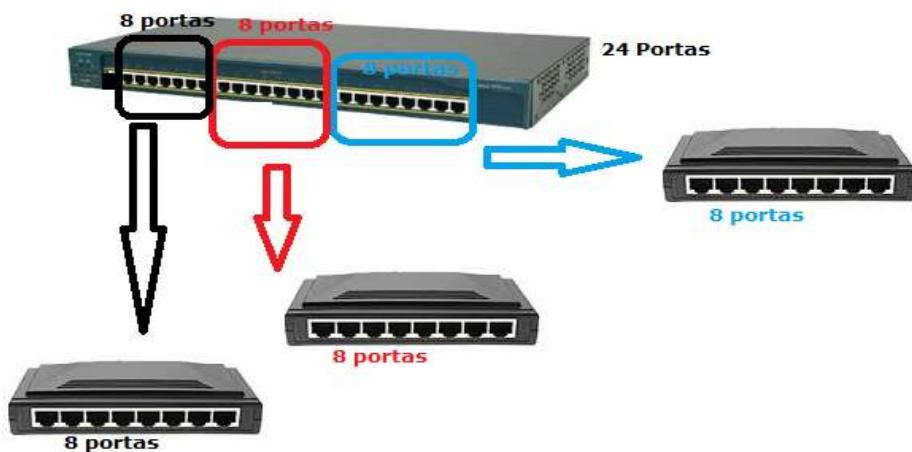
Para apagar todas as VLANs se estamos utilizando a faixa de numeração padrão podemos entrar com o comando “no vlan 2-1002” o traço entre os números 2 e 1002 significa “até”.

Se a faixa estendida estiver sendo utilizada podemos apagar as VLANs com o comando “no vlan 2-1002,1006-4094”. A vírgula no comando significa “e” e o traço “até”, portanto o comando é igual a “apague as vlans de 2 até 1002 e de 1006 até 4094”.

Outra forma de fazer essa operação é apagando o arquivo `vlan.dat`, o qual é gravado na memória flash do switch quando criamos VLANs, e reinicializando o switch (reload). Com esse procedimento também podemos zerar o número de revisão do VTP do switch.

#### 4.6 Roteamento entre VLANs

Lembre-se que ao criar uma VLAN, as portas alocadas nela formam um domínio de broadcast único. É como se cada VLAN que criada criássemos um switch novo com as portas que alocamos nessa VLAN, veja figura abaixo onde criamos três VLANs em um switch de 24 portas, formando três domínios de broadcasts novos.



Para fazer essas VLANs se comunicarem podemos conectar uma porta alocada em cada VLAN a um roteador, o que seria impraticável pelo número de portas em roteadores necessárias, portanto o que é feito na prática é configurar uma ou mais portas com o protocolo 802.1Q e conectar o switch a um dispositivo de camada-3 (roteador ou switch camada 3) para que ele faça o roteamento entre as diferentes VLANs.

O uso dos roteadores fazendo o roteamento entre VLANs é mais comum em redes com poucos hosts (até 300 computadores), formando uma topologia chamada “router-on-a-stick”. Acima de 300 hosts já se recomenda o uso de switches camada-3.

#### 4.6.1 Roteamento entre VLANs com Roteadores

Por padrão somente hosts de uma mesma VLAN podem se comunicar.

Para que computadores de VLANs diferentes se comuniquem é necessário que um equipamento de camada-3 seja inserido na rede e devidamente configurado para efetuar o encaminhamento do tráfego entre as VLANs.

Lembrem que cada VLAN está configurada em um domínio de broadcast diferente, ou seja, cada uma possui sua própria rede ou sub-rede IP, por isso para haver comunicação um roteador precisará realizar o roteamento entre as redes, ou seja, encaminhar os pacotes de uma rede para outra.

Para suportar roteamento entre VLANs, seja em redes entroncadas via ISL ou 802.1Q, a interface LAN do roteador deve ser **subdividida** e essas novas **interfaces lógicas** são chamadas **subinterfaces**.

O roteamento entre VLANs em roteadores é realizado criando subinterfaces lógicas em uma Fastethernet ou Gigabitethernet. A interface LAN física deve estar sem endereço IP configurado, pois ele será configurado nas subinterfaces lógicas.

Podemos fazer uma analogia que vamos “**fatiar a interface física**” para passar várias VLAN’s, que são **interfaces lógicas**. Caso não fosse possível essa configuração o roteador necessitaria uma interface LAN por VLAN configurada no switch.

Você pode escolher qualquer número de subinterface em um range de 0 até 4294967295, conforme mostrado abaixo.

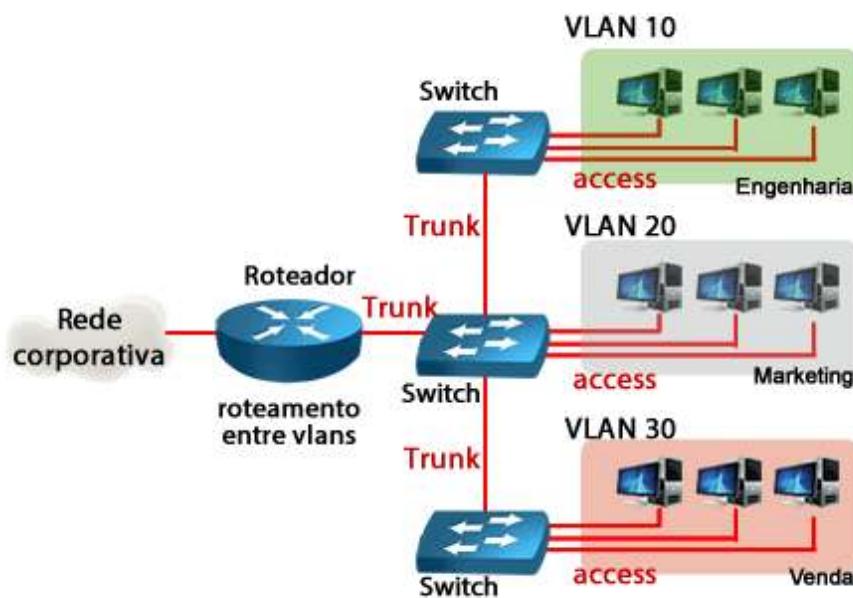
```
Router0(config)#int f0/0.?
<0-4294967295>  FastEthernet interface number
Router0(config)#int f0/0.10
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state
to up
Router0(config-subif) #
```

Assim que você cria a subinterface, se a interface principal estiver ativada, ela sobe para UP e a rede IP configurada nela é inserida na tabela de roteamento.

Uma forma interessante de configuração que facilita a manutenção é colocar o número da subinterface igual ao da VLAN a ser configurada nela, por exemplo, você vai configurar a VLAN 10 no roteador, entre com o comando “interface fast 0/0.10”, assim você poderá analisar os problemas de roteamento entre VLANs mais facilmente.

As informações de VLAN também serão criadas nas subinterfaces com o comando **“encapsulation dot1q 10”**, onde o parâmetro **“dot1q”** representa o protocolo **802.1Q** e o valor **“10”** representa a **VLAN 10**.

A seguir estudaremos outro exemplo de configuração de roteamento entre VLAN executado por um roteador 2811, onde ele irá rotear as VLANs 10 e 20 com protocolo 802.1Q e a VLAN 30 com protocolo ISL, conforme topologia abaixo.



```

2811#config t
2811(config)#int fast 0/0      ! Configurando a interface física
2811(config-if)#no ip address
2811(config-if)#no shut
2811(config)#interface fastethernet 0/0.1    ! criando a subinterface 0/0.1
2811(config-subif)#encapsulation dot1q 10    ! VLAN 1 via 802.1Q
2811(config-subif)#ip address 192.168.1.1 255.255.255.0
2811(config-subif)#exit
2811(config)#interface fastethernet 0/0.2    ! criando a subinterface 0/0.2
2811(config-subif)#encapsulation dot1q 20    ! VLAN 2 via 802.1Q
2811(config-subif)#ip address 192.168.2.1 255.255.255.0
2811(config-subif)#exit
2811(config)#int f0/0.3    ! criando a subinterface 0/0.3
2811(config-subif)#encapsulation isl 30    ! VLAN 10 via ISL
2811(config-subif)#ip address 192.168.3.1 255.255.255.0
2811(config-subif)#exit
2811(config)#

```

Reforçando, o comando “**encapsulation**” define o protocolo de camada-2 a ser utilizado na subinterface, o “**dot1q**” representa o **802.1Q** e o **isl** é o **ISL** proprietário da Cisco, utilizado nos switches de versão mais antiga, por exemplo a linha Catalyst 1900. O número colocado após o parâmetro “dot1q” ou “isl” é o número da VLAN que o roteador irá encaminhar.

Além dessa configuração é necessário configurar os endereços IPs das subinterfaces, pois cada VLAN necessita de uma rede ou sub-rede IP própria, com o comando “**ip address**” conforme já ensinado anteriormente.

É importante notar que a interface principal fica sem endereço IP, eles são configurados em cada subinterface, conforme exemplo apresentado.

Essa topologia com switches na rede LAN e um roteador fazendo o roteamento entre VLANs é conhecida como “**router-on-a-stick**” ou **ROAS**.

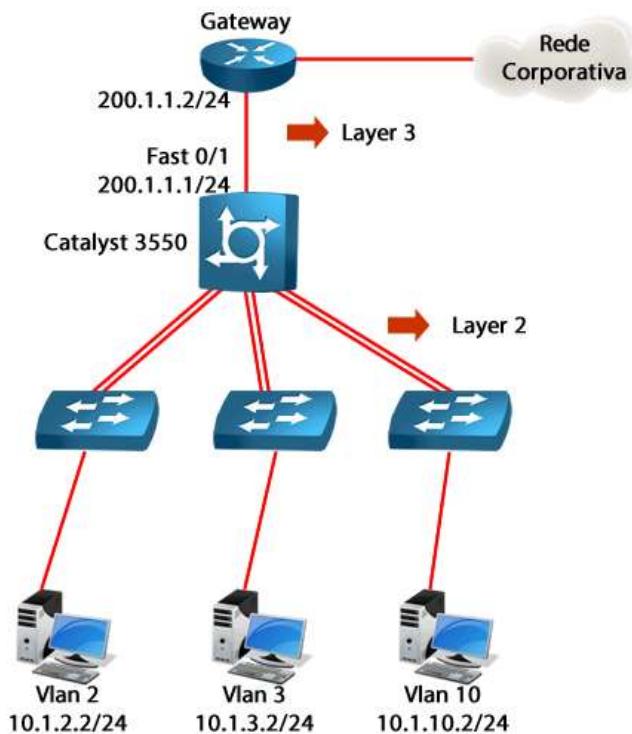
#### **4.6.2 Roteamento entre VLANs com Switches Camada 3**

Normalmente em redes com arquitetura em três camadas utilizamos switches Layer 3 nas camadas de distribuição e núcleo, sendo que o roteamento entre VLANs é recomendado ser configurado nos switches de distribuição.

A diferença de um switch camada 3 para um roteador é que ele pode realizar roteamento de pacotes de maneira semelhante ao encaminhamento dos quadros, ou seja, através de hardware ao invés de software como nos roteadores, isso torna os switches camada 3 até mais rápido que os roteadores para o encaminhamento dos pacotes.

Os switches Layer 3 da Cisco que rodam IOS são na realidade switches layer 2 por padrão e para terem a facilidade de roteamento IP (Layer 3) você deve utilizar um IOS mais avançado, que suporte o protocolo IP, e também habilitar o protocolo IP com o comando “**ip routing**” em modo de configuração global, o mesmo comando que já vem habilitado por padrão nos roteadores.

Vamos mostrar um exemplo de configuração de roteamento entre VLANs em um switch layer 3 modelo Catalyst 3550 e também como configurar uma interface para layer 3 e conexão com um roteador, veja a topologia na figura abaixo.



Vamos partir do pressuposto que as configurações básicas do switch 3550 foram realizadas e os switches de acesso também, portanto vamos apenas nos preocupar com ativar o roteamento IP no 3550, configurar o roteamento entre VLANs e ativar o recurso de layer 3 na interface Fast 0/1 para configurar um endereço IP nela.

Também teremos que configurar o roteamento no switch 3550, para que ele possa encaminhar pacotes de redes não conhecidas em direção à rede corporativa, faremos isso com uma rota estática padrão apontando para o roteador, o qual é seu gateway padrão. Veja as configurações abaixo.

## Passo 1 - Configurando o roteamento entre VLANs

Lembr-se que temos as VLANs 2, 3 e 10 e vamos alocar o primeiro IP de cada VLAN para o 3550. Vamos iniciar ativando o protocolo IP e depois configurando o roteamento entre VLANs.

```

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip routing
Switch(config)#interface Vlan2
Switch(config-if)#ip address 10.1.2.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config)#interface Vlan3
Switch(config-if)#ip address 10.1.3.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config)#interface Vlan10
Switch(config-if)#ip address 10.1.10.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#

```

Note que o roteamento entre VLANs nada mais é que criar uma interface VLAN para cada sub-rede e ativá-la. Quando o switch é Layer-2 apenas uma interface VLAN é permitida, a de gerenciamento, quando tentamos ativar mais uma ele coloca a anterior em shutdown.

Essas interfaces são chamadas SVIs ou Switched Virtual Interfaces.

## Passo 2 – Ativando o Layer 3 na Interface do Switch e Criando Rota Padrão

Agora vamos transformar a interface fast 0/1 em uma interface layer-3 com o comando “**no switchport**”, configurar o IP na interface e criar a rota padrão apontando para o gateway.

```

Switch(config)#interface FastEthernet 0/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 200.1.1.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)# ip route 0.0.0.0 0.0.0.0 200.1.1.2
Switch(config)#end
Switch#

```

Essas interfaces são chamadas portas roteadas ou "routed ports", pois elas passam a funcionar como as interfaces dos roteadores.

Agora com o comando **show ip route** podemos verificar a tabela de roteamento no switch 3550, veja abaixo.

```

Switch#show ip route
### Saídas omitidas ####
Gateway of last resort is 200.1.1.2 to network 0.0.0.0

    200.1.1.0/30 is subnetted, 1 subnets
C        200.1.1.0 is directly connected, FastEthernet0/48
        10.0.0.0/24 is subnetted, 3 subnets
C            10.1.10.0 is directly connected, Vlan10
C            10.1.3.0 is directly connected, Vlan3
C            10.1.2.0 is directly connected, Vlan2
S*   0.0.0.0/0 [1/0] via 200.1.1.2

```

Note que para cada interface VLAN criada foi inserida uma rota diretamente conectada na tabela de roteamento do switch, tendo o mesmo efeito da configuração das subinterfaces no roteador quando utilizamos a topologia “**router-on-a-stick**”, ou seja, switches conectados diretamente ao roteador através de um link layer-2.

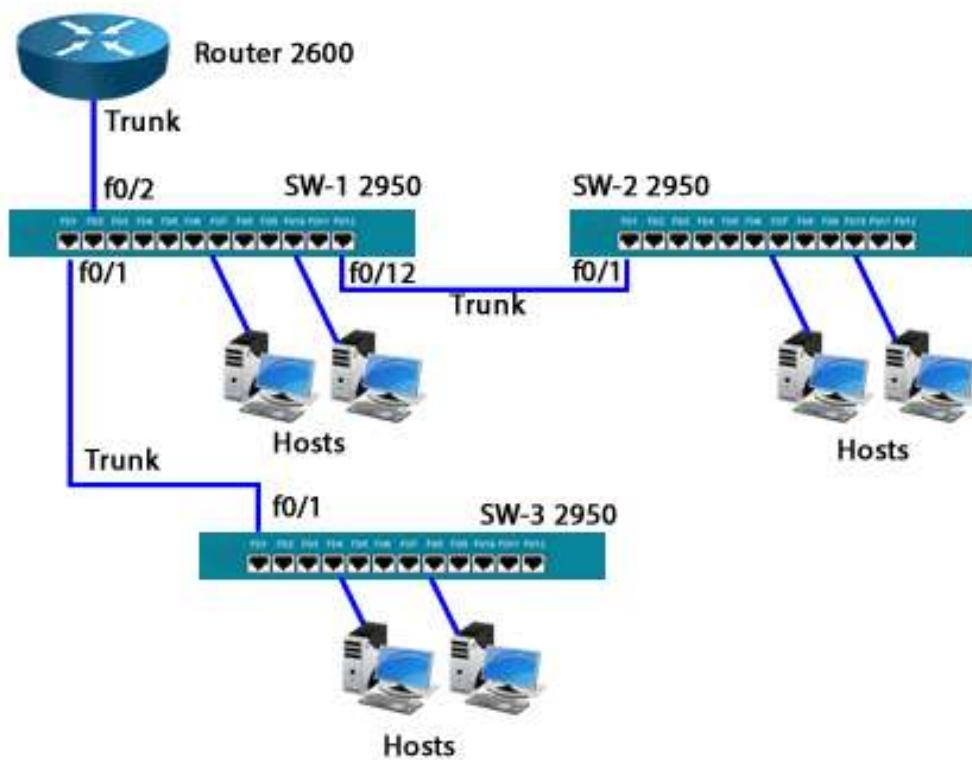
Com essa configuração o switch camada-3 fará o encaminhamento de pacotes entre as redes locais dos switches de acesso conectados a ele.

Quando um host de uma dessas redes quiser sair para a Internet o próprio switch de camada-3 encaminhará esse pacote ao roteador através da interface fast 0/1.

Esse tipo de topologia é recomendado para redes que possuam acima de 300 hosts.

#### 4.7 Exemplo Prático de VTP, VLAN e Roteamento entre VLAN

Agora vamos a um exemplo completo envolvendo desde a criação da VLAN até o uso do VTP com base na topologia “router-on-a-stick” abaixo.



Essa rede utiliza um roteador 2600 para Internet e roteamento entre VLANs e switches 2950 com 12 portas para a rede LAN.

Nesse exemplo temos uma rede corporativa com três setores (vendas, administrativo e operacional) utilizando VLANs para separar o tráfego de broadcast entre eles e ter mais controle sobre a rede.

Os switches e suas VLANs devem ser configurados conforme especificação abaixo (não é necessária a configuração geral):

- SW1 será o VTP Server (domínio Cisco) e os demais serão clientes.

- Porta 2 dos switches 2 e 3 estarão na VLAN 10 (vendas).
- Portas 3 e 4 dos switches 1, 2 e 3 estarão na VLAN 10 (vendas).
- Portas de 5 a 8 dos switches 1, 2 e 3 estarão na VLAN 20 (administrativo).
- Portas de 9 a 11 dos switches 1, 2 e 3 estarão na VLAN 30 (operação).
- Porta 12 do switch 2 e 3 também devem ser alocadas na VLAN 30 (operação).
- A VLAN 1 será utilizada para gerenciamento dos switches.
- Trunks entre SW1/SW2, SW1/SW3 e SW1/2600 via protocolo 802.1Q.

Configure também o roteamento entre VLANs no roteador 2600 utilizando como IP das subinterfaces o primeiro IP válido da sub-rede, sendo que a VLAN 10 utilizará a sub-rede 10.0.0.0/24, a VLAN 20 a sub-rede 10.0.1.0/24 e a VLAN 30 a sub-rede 10.0.2.0/24.

A VLAN 1 será utilizada para gerenciamento e utilizará a sub-rede 10.0.51.0/24. O entroncamento entre a porta f0/0 do roteador 2600 e o Switch-1 é feito via f0/2.

Resposta do exercício: Como não foi especificado nada, colocaremos o segundo, terceiro e quarto IP nas interfaces VLAN 1 de cada switch como IPs de gerenciamento.

### **Configuração do SW1:**

```
SW1#Config term  
(configuração do ip de gerenciamento)  
SW1(config)#Interface vlan 1  
SW1(config-if)#Ip address 10.0.51.2 255.255.255.0  
SW1(config-if)#no shutdown  
SW1(config-if)#exit  
(configuração do VTP)  
SW1(config)#vtp mode server  
SW1(config)#vtp domain Cisco  
(criação das VLANs)  
SW1(config)#vlan 10  
SW1(config-vlan)#name vendas  
SW1(config-vlan)#vlan 20  
SW1(config-vlan)#name administrativo  
SW1(config-vlan)#vlan 30  
SW1(config-vlan)#name operacional  
SW1(config-vlan)#exit  
(alocação de portas nas VLAN)  
SW1(config)#interface fastethernet 0/3  
SW1(config-if)#switchport access vlan 10  
(repita a mesma configuração para todas as portas access)  
ou  
SW1(config)#interface range fastethernet 0/3 - 4  
SW1(config-if)#switchport mode access  
SW1(config-if)#switchport access vlan 10  
SW1(config-if)#interface range fastethernet 0/5 - 8  
SW1(config-if)#switchport mode access  
SW1(config-if)#switchport access vlan 20  
SW1(config-if)#interface range fastethernet 0/9 - 11  
SW1(config-if)#switchport mode access  
SW1(config-if)#switchport access vlan 30
```

```
(configuração dos trunks)
SW1(config-if)#interface fastethernet 0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#interface fastethernet 0/2
SW1(config-if)#switchport mode trunk
SW1(config-if)#interface fastethernet 0/12
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
SW1(config)#exit
SW1#copy run start
```

**Configuração do SW2:**

```
SW2(config)#Config term
(configuração do ip de gerenciamento)
SW2(config)#Interface vlan 1
SW2(config-if)#Ip address 10.0.51.3 255.255.255.0
SW2(config-if)#no shutdown
SW2(config-if)#exit
(configuração do VTP)
SW2(config)#vtp mode client
SW2(config)#vtp domain Cisco
(alocação de portas nas VLAN)
SW2(config)#interface range fastethernet 0/2 - 4
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 10
SW2(config-if)#interface range fastethernet 0/5 - 8
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 20
SW2(config-if)#interface range fastethernet 0/9 - 12
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 30
(configuração dos trunks)
SW2(config-if)#interface fastethernet 0/1
SW2(config-if)#switchport mode trunk
SW2(config-if)#^Z
SW2#copy run start
```

**Configuração do SW3:**

```
SW3(config)#Config term
(configuração do ip de gerenciamento)
SW3(config)#Interface vlan 1
SW3(config-if)#Ip address 10.0.51.4 255.255.255.0
SW3(config-if)#no shutdown
SW3(config-if)#exit
(configuração do VTP)
SW3(config)#vtp mode client
SW3(config)#vtp domain Cisco
(alocação de portas nas VLAN)
SW3(config)#interface range fastethernet 0/2 - 4
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 10
SW3(config-if)#interface range fastethernet 0/5 - 8
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 20
SW3(config-if)#interface range fastethernet 0/9 - 12
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 30
```

```
(configuração dos trunks)
SW3(config-if)#interface fastethernet 0/1
SW3(config-if)#switchport mode trunk
SW3(config-if)#^Z
SW3#copy run start
```

**Questão Extra** - Para pensar: porque não foram criadas VLANs nos switches 2 e 3 e apenas no switch 1?

Resposta: Devido ao SW1 ser o VTP Server e os demais estarem configurados como Clientes. As VLANs podem ser criadas apenas nos switches configurados como VTP server ou transparente.

#### **Configuração do roteamento entre VLAN no roteador 2600:**

```
2600#Config term
2600(config)#Interface fastethernet 0/0
2600(config-if)#No ip address
2600(config-if)#No shutdown
2600(config-if)#exit
2600(config)#Interface 0/0.10
2600(config-subif)#encapsulation dot1q 10
2600(config-subif)#Ip address 10.0.0.1 255.255.255.0
2600(config-subif)#Interface 0/0.20
2600(config-subif)#encapsulation dot1q 20
2600(config-subif)#Ip address 10.0.1.1 255.255.255.0
2600(config-subif)#Interface 0/0.30
2600(config-subif)#encapsulation dot1q 30
2600(config-subif)#Ip address 10.0.2.1 255.255.255.0
2600(config-subif)#Interface 0/0.1
2600(config-subif)#encapsulation dot1q 1
2600(config-subif)#Ip address 10.0.51.1 255.255.255.0
2600(config-subif)#^Z
2600#Copy run start
```

Abra o packet tracer e refaça o exemplo utilizando a configuração ilustrada. Depois de realizada a configuração conecte computadores aos switches e teste com ping o roteamento entre as VLANs.

Depois apague tudo e repita o exercício (configurando tudo sozinho desta vez), assim você terá fixado os conceitos e os comandos. Você não precisa utilizar os mesmos roteadores, pode escolher outros modelos.

#### **5 Aumentando a Segurança dos Switches**

Para aumentar a segurança na LAN podemos realizar algumas configurações recomendadas pela Cisco utilizando o recurso de Port Security, alterando a VLAN de gerenciamento e desativando portas e protocolos ou serviços não utilizados.

Outra maneira de aumentar a segurança em roteadores e switches é ativar o protocolo SSH para acesso remoto seguro ao invés do Telnet, o qual envia informações através da rede em modo texto, sem nenhum tipo de criptografia.

Outra recomendação de segurança básica é manter o sistema operacional Cisco IOS sempre atualizado para evitar riscos de segurança que são corrigidos regularmente através de correções. Esse processo de atualização se chama "Upgrade".

## 5.1 Configurando o Port Security

O objetivo do **port security** é **impedir** que **hosts não autorizados** acessem a rede, restringindo o número máximo de endereços MAC por porta do switch. Caso haja uma violação da regra uma ação é tomada conforme configuração realizada.

A principal função do Port Security é proteger contra ataques de inundação de MAC (MAC Flooding). Esse ataque, a grosso modo, visa transformar o switch em um HUB.

O atacante inunda a tabela de endereços MAC até estourar o máximo que ela suporta, normalmente 8.000 endereços, assim o switch dará o flooding de todos os quadros permitindo que o atacante "sniffe" ou espione tudo que passar pela VLAN onde o computador dele está conectado.

Esse ataque é muito simples de ser realizado (desde que você conheça Linux) com um aplicativo chamado DSNIF e o comando macof, por isso o Port Security é tão importante.

Existem três tipos de configurações básicas do Port Security:

1. **Endereços MAC seguros estáticos (Static)** - Configurados manualmente dentro da configuração de interface. Esse endereço é armazenado na tabela de endereços e se outro computador for conectado a essa porta ela pode ser bloqueada, conforme configuração.
2. **Endereços MAC seguros dinâmicos (Dynamic)** - Estes são configurados dinamicamente, armazenados apenas na tabela de endereços na memória RAM e removidos na reinicialização do switch. Esse é o padrão ativado pelos switches.
3. **Endereços MAC seguro fixos (Sticky)** - Podem ser aprendidos dinamicamente ou configurados manualmente, são armazenados na tabela de endereços. Se os endereços estão salvos na NVRAM, quando o switch é reinicializado, a interface não tem necessidade de ser reconfigurada dinamicamente, mas para isso você deve especificar o MAC.

Abaixo seguem os passos para configuração da segurança de portas:

1. Colocar a porta em modo de acesso (switchport mode access);
2. Habilitar port security (switchport port security);
3. Definir o limite de endereços MAC na porta (padrão 1);
4. Especificar os endereços MACs permitidos (padrão dinâmico);
5. Definir ações de violação (padrão shutdown).

Com o comando "**port security**" o padrão de segurança é implementado com as seguintes características:

- Limite de MACs aprendidos por porta **1**.
- Modo de aprendizagem dos MACs **dinâmico** sem gravar o MAC aprendido na NVRAM, ou seja, com um reload o switch apaga o MAC da tabela e terá que aprender novamente.
- Ação em caso de violação **shutdown**, ou seja, derruba a porta e coloca em estado e "**error disable**" ou desabilitada por erro, pois assim indica que a porta está em shutdown por um motivo diferente de um "no shut".

```

Switch(config)#int fast 0/1
Switch(config-if)#switchport mode access
Switch(config-if)# switchport port-security ?
  aging          Port-security aging commands
  mac-address   Secure mac-address
  maximum        Max secure addrs
  violation      Security Violation Mode
<cr>
Switch(config-if)#switchport port-security
Switch(config-if)#

```

Em modo de Interface no switch teremos as seguintes opções para configurar o Port Security, acompanhe abaixo.

```
Switch(config-if)#switchport port-security ?
aging                  Port-security aging commands
mac-address            Secure mac-address
maximum                Max secure addrs
violation               Security Violation Mode
<cr>
```

Portanto, podemos alterar a maneira que os switches aprendem endereços MAC (**opção mac-address**), qual o limite de endereços que a porta pode aprender (**opção maximum**) e também qual ação o switch deve tomar se uma violação for detectada (**opção violation**), ou seja, se o máximo de MACs seguros permitidos for ultrapassado.

A opção aging define o tempo que um MAC seguro ficará mantido na tabela quando há aprendizado dinâmico, caso ele não seja detectado é apagado da tabela de MACs seguros, por padrão ele é infinito.

Para alterar o padrão de aprendizado de dinâmico para sticky ou manual utilizamos o comando **"switchport port-security mac-address"** definindo a seguir o padrão a ser configurado.

A primeira opção de configuração que vamos estudar é através do parâmetro **"sticky"** (em português "pegajoso"), o comando fica **"switchport port-security mac-address sticky"**. Esse parâmetro faz com que o switch **escreva na NVRAM** o endereço que ele aprendeu, com isso mesmo que você reinicialize o switch ele manterá em sua configuração o MAC que ele aprendeu quando você ativou o Port Security.

Com a opção "sticky" podemos definir um MAC estático, por exemplo, com o comando **"switchport port-security mac-address sticky aaaa.bbbb.cccc"**. Essa opção permite definir um MAC específico para porta e mesmo assim ter um máximo de MACs seguros maior que um.

Você pode também definir manualmente o MAC digitando o endereço no formato H.H.H, por exemplo, **"switchport port-security mac-address aaaa.aaaa.aaaa"**. Com esse comando o switch considera que o host com o MAC **aaaa.aaaa.aaaa** está conectado na porta e o máximo de MACS seguros para essa porta é definido para um automaticamente.

Por exemplo, com os comandos **"switchport port-security"** e **"switchport port-security mac-address aaaa.bbbb.cccc"** em uma das portas do switch, se um computador com MAC diferente de **aaaa.bbbb.cccc** se conectar à porta ela será colocada em "error disable" e será desabilitada, gerando uma mensagem de erro para a console e para um servidor SNMP, caso tenha sido configurado.

A configuração da violação tem três padrões de ação no port security, veja a saída do comando abaixo.

```
SW-DlteC(config-if)#switchport port-security violation ?
protect    Security violation protect mode
restrict   Security violation restrict mode
shutdown   Security violation shutdown mode
```

O padrão é o **shutdown**, o qual desabilita a porta e coloca ela em um estado chamado "error disable" e gera um alarme para o gerenciamento via snmp trap e mensagem de syslog.

Se a violação estiver configurada como **"protect"** ou protegido, caso haja uma violação o switch bloqueia os quadros dos hosts com os MACs que ultrapassaram o máximo permitido no

comando “**switchport port-security maximum**” e o switch continua operando normalmente para os MACs permitidos, sem gerar avisos.

Na opção “**restrict**” ou restringido o switch faz a mesma operação do protect, porém envia uma mensagem para o gerenciamento do switch avisando que o máximo de portas configurado foi excedido via snmp trap e mensagem de syslog.

Conforme já citado, o máximo de MACs seguros padrão do port security é 1, porém pode ser alterado com o comando “switchport port-security maximum”, por exemplo, se a porta precisa ter até 3 MACs seguros podemos utilizar o comando “switchport port-security maximum 3”.

## 5.2 Verificando o Port Security

No exemplo a seguir vamos analisar a configuração do port security para fazer com que no máximo 2 MACs sejam aprendidos dinamicamente e em caso de violação a porta seja colocada em shutdown.

```

Switch(config-if)#interface fast0/1
Switch(config-if)# switchport port-security
!
! comando habilita o port-security
!
Switch(config-if)# switchport port-security mac-address sticky
!
! comando para fazer o switch aprender dinamicamente o MAC do micro conectado
! na porta fast 0/1
!
Switch(config-if)# switchport port-security maximum 2
!
! define o número máximo de endereços permitidos em 2
! o valor 1 é o default
!
Switch(config-if)# switchport port-security violation shutdown
!
! A ação de violação foi definida para colocar a interface em shutdown,
! ou seja, caso um terceiro dispositivo tente se conectar nesta interface
! a porta será colocada em shutdown.
!
end

```

Para mostra informações sobre o Port Security podemos utilizar o comando “show port-security”, conforme abaixo.

```

Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)        (Count)        (Count)
-----
Fa0/1          2             0             0           Shutdown
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024

```

No comando “**show port-security**” é possível as principais informações para realizar o troubleshooting em switches com essa função habilitada, veja o que significa cada campo:

- **Secure Port**: número da porta com o port security habilitado.
- **MaxSecureAddr**: máximo de MACs que podem ser aprendidos pela porta (nesse exemplo são 2).

- **CurrentAddr:** quantos endereços a porta aprendeu (nesse exemplo a porta ainda não aprendeu nenhum endereço).
- **SecurityViolation:** quantas violações de segurança aconteceram na porta (nesse exemplo nenhuma violação de segurança aconteceu).
- **Security Action:** qual a ação de segurança configurada na porta (nesse caso é shutdown).

Caso uma violação seja detectada com o modo de operação “shutdown” a porta entra em “error disable”. Para voltar a porta em operação é preciso tirar o computador que causou a violação e em modo de interface dar “shut” e depois “no shut” respectivamente.

O comando “**show port-security interface fast 0/x**” mostra informações mais detalhadas do port security, veja um exemplo abaixo onde estão mostradas informações referentes à porta 19 do switch (fast 0/19). Com esse comando temos todas as informações do comando anterior, porém com o detalhamento específico da porta 0/19.

```
SW-DlteC#show port-security interface fast0/19
Port Security           : Enabled -> Indica se o port security está habilitado
Port Status              : Secure-up -> Indica se a porta está protegida
Violation Mode          : Shutdown -> Tipo de ação de violação configurada
Aging Time               : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled -> Indica se existe MAC estático seguro
Maximum MAC Addresses    : 1 -> Número máximo de MACs aprendidos
Total MAC Addresses       : 1 -> Número de MACs aprendidos
Configured MAC Addresses : 0 -> Número de MACs estáticos configurados
Sticky MAC Addresses     : 0 -> Número de MACs gravados na NVRAM
Last Source Address:Vlan : 001d.7060.d31b:30 -> Último MAC aprendido
Security Violation Count : 0 -> Quantidade de violações ocorridas
```

SW-DlteC#

Perceba acima que no campo “**Last Source Address:Vlan**” é mostrado o último MAC aprendido com a VLAN a qual ele pertence, nesse exemplo é o **001d.7060.d31b** que está na VLAN 30.

Outro detalhe interessante é que se estivermos utilizando os modos de violação shutdown ou restrict o campo de contagem de violações (**Security Violation Count**) será incrementado, mas no caso do protect esse campo não é incrementado.

### 5.3 Protegendo Interfaces não Utilizadas

Interfaces não utilizadas podem ser protegidas de uma maneira bem simples com o comando “**shutdown**” para desativá-la.

Caso desabilitar a interface não seja uma opção devido à política da empresa as seguintes medidas podem ser utilizadas para proteção contra ataques diretos às portas dos switches:

- Inserir o comando “**switchport mode access**” para evitar que trunks indesejados sejam formados.
- Inserir a porta em uma VLAN não utilizada, isolando os computadores que se conectem nessas portas.
- Não utilizar a VLAN 1 como nativa, configurando uma VLAN não utilizada pelos computadores como nativa, assim não há possibilidade de computadores invasores tentarem se conectar via acesso remoto diretamente aos switches.

No curso 200-105 e também no CCNA Security são estudadas mais opções de segurança para as portas dos switches.

## 5.4 Configurando o Acesso Seguro via SSH

Já aprendemos como configurar a **line vty** que é o acesso remoto via **Telnet** para o roteador ou switch Cisco. Uma das características do Telnet é que ele passa em **modo texto seu usuário e senha** pela rede, assim como toda a comunicação entre o roteador e o computador de gerenciamento remoto.

A configuração básica do Telnet é realizada na line vty definindo uma senha e o login:

```
Line vty 0 4
Password cisco
Login
```

Já o **Secure Shell** ou **SSH** é um serviço de rede que permite a conexão com outro computador na rede assim como o Telnet, porém com a vantagem da conexão entre o cliente e o servidor ser **criptografada** e, portanto, mais segura que o Telnet.

O SSH utiliza o protocolo TCP na porta 22 e o Telnet a porta 23. Acompanhe abaixo os comandos necessários para ativar o SSH.

**Passo 1.** Configure o hostname e um usuário e senha para login na base de dados local do roteador:

```
Hostname DlteC
username dltc password cisco
```

**Passo 2.** Configure o domínio do DNS:

```
ip domain-name dltc.com.br
```

**Passo 3.** Crie a chave para acesso seguro via SSH a ser utilizada. A chave de criptografia recomendada é maior que 1024 bits definida após a opção modulus abaixo. Você pode entrar com o comando “**crypto key generate rsa**” e definir o tamanho da chave que será solicitada logo após durante a configuração.

```
crypto key generate rsa modulus 1024
```

Opcionalmente você pode utilizar os comandos abaixo para definir o tempo de espera máximo da conexão e também o número de tentativas:

```
ip ssh time-out 60
ip ssh authentication-retries 2
```

**Passo 4.** Habilite o SSH nas lines VTY com o comando “transport input”.

```
line vty 0 15
transport input ssh
login local
```

**Passo 5.** Opcionalmente configure a versão do SSH.

Configurando SSH v1:  

```
Router(config)#ip ssh version 1
```

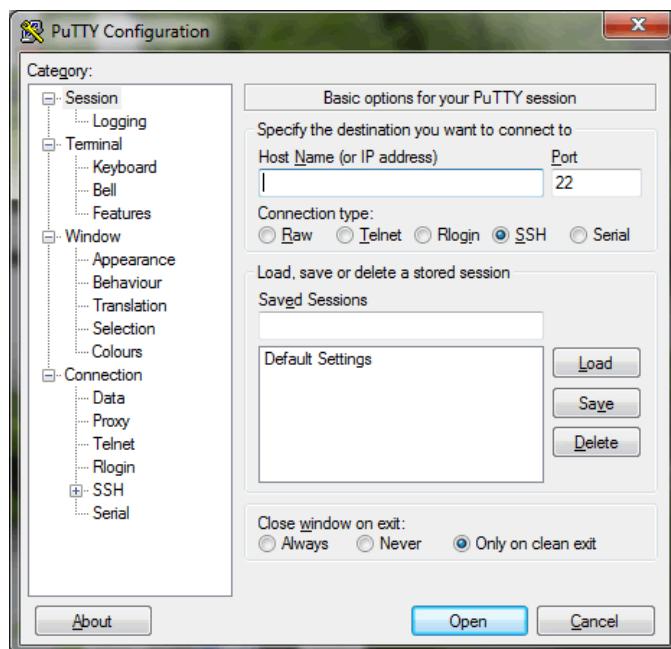
Configurando SSH v2:  

```
Router(config)#ip ssh version 2
```

Configurando SSH v1 e v2:

```
Router(config)#no ip ssh version
```

Para acessar um roteador ou switch via SSH você deverá utilizar um programa SSH Client, por exemplo, o Putty.



## 6 Scripts de Configuração

A configuração em um roteador ou switch não precisa necessariamente ser configurada diretamente via console ou terminal virtual, podemos também elaborar scripts de configuração e aplicá-los posteriormente nos equipamentos.

Por exemplo, você pode abrir um arquivo no bloco de notas e digitar:

```
Configure terminal
Interface fast 0/0
Ip address 192.168.1.10 255.255.255.0
No shut
```

Logo após podemos nos logar em um roteador localmente ou via telnet/SSH, copiar e colar essas configurações estando em modo privilegiado.

Alguns programas de “shell script” permitem até mesmo o login remoto e configuração ou coleta de informações que podem ser utilizadas na automação de tarefas de operação e manutenção que devem ser realizadas no dia a dia dos administradores de rede.

Sobre a ação de “copiar e colar” configurações na console ou através de um terminal remoto nos roteadores e switches deve-se tomar cuidado com comandos com linhas muito grandes, pois eles podem acabar sendo “truncados”. Para que isso não ocorra deve-se configurar a velocidade de escrita dos programas que estão fazendo a emulação de terminal.

Outra opção para aplicar configurações completas no Cisco IOS é de copiar a configuração via TFTP para a NVRAM e reinicializar o roteador, pois esse método evita eventuais problemas de comandos truncados.

## 7 Resumo do Capítulo

Bem pessoal, chegamos ao final de mais um capítulo!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Entender os requisitos de cabeamento em redes corporativas.
- Funcionamento dos leds indicativos em roteadores e switches.
- Conceito e configuração de VLANs, trunks, VTP e Port Security.
- Aplicação dos conceitos aprendidos em redes reais.
- Compreender e configurar o roteamento entre VLANs em roteadores e switches camada 3.
- Entender como aumentar a segurança nas portas dos switches.

*Até o capítulo-7 fizemos  
maioria das  
implementações  
considerando o conceito de  
redes Classful, ou seja, redes  
puramente Classe A, B ou C.*

*Para maioria das redes de  
pequeno porte ou SOHO as  
redes classful são suficientes  
para endereçamento de  
seus segmentos de rede,  
dispositivos e LANs, porém  
em ambientes reais de  
maior porte normalmente  
não é o que encontramos.*

*Por isso, nesse capítulo  
vamos estudar como  
projetar redes utilizando os  
conceitos de divisão em sub-  
redes e máscaras com  
comprimento variável  
(VLSM).*

*Aproveite o capítulo e bons  
estudos!*

## **Capítulo 8 - Projetando Redes IP com Sub-rede e VLSM**

### **Objetivos do Capítulo**

Ao final desse capítulo você terá estudado e deverá compreender:

- Ser capaz de compreender o uso de sub-redes.
- Interpretar endereços dada uma máscara de sub-rede.
- Fazer projetos utilizando como requisito a quantidade de hosts ou a quantidade de redes IP necessárias em uma rede corporativa.
- Entender o conceito de VLSM e projetar redes com máscaras de sub-rede de comprimento variável.
- Entender o conceito de summarização de redes e ser capaz de calcular a melhor máscara de rede summarizada dada um conjunto de sub-redes.
- Entender o conceito de roteamento Classless (CIDR).
- Saber quais protocolos suportam os recursos de sub-rede, VLSM e CIDR.
- Entender os requisitos e necessidades de endereçamento em redes corporativas.

## Sumário do Capítulo

<b>1 Revisão das Classes de Endereços IP</b>	<b>334</b>
1.1 Componentes do Endereçamento IP	335
<b>2 Entendendo o Conceito de Sub-rede, VLSM e CIDR</b>	<b>336</b>
<b>3 Dividindo Redes em Sub-redes</b>	<b>337</b>
3.1 Método Tradicional de Análise de Endereços IP	338
3.2 Exemplo Prático I – Dividindo Redes Classe A, B e C em duas Sub-redes	340
3.3 Exemplo Prático II - Projeto de Sub- redes por Redes	341
3.4 Entendendo a Subnet-Zero e Broadcast- Subnet	343
3.5 Exemplo Prático III - Projeto de Sub- redes por Hosts	343
3.6 Análise de Endereços IP com a Metodologia DlteC	344
3.7 Máximo de Bits de Host Emprestados	345
3.8 Resumo das Máscaras de Sub-rede por Classe	346
3.9 Dicas Finais sobre Exercícios de Sub- rede para o CCENT/CCNA	349
<b>4 VLSM (Variable Length Subnet Masks)</b>	<b>351</b>
4.1 Como Resolver Exercícios com VLSM	353
4.2 Outra Visão sobre VLSM	355
4.3 Considerações finais sobre VLSM	356
<b>5 Roteamento Classless – CIDR</b>	<b>357</b>
5.1 Exemplo de Cálculo de IPs com CIDR	358
5.2 Comprimentos de Prefixos CIDR	359
<b>6 Sumarização de Rotas</b>	<b>359</b>
6.1 Sumarização de Rotas - Exemplo	360
6.2 Exemplo de Sumarização na Prática	361
<b>7 Projetando Redes e Endereçando Dispositivos</b>	<b>364</b>

## 1 Revisão das Classes de Endereços IP

Como já estudamos no capítulo 5, a Internet foi criada com o conceito chamado Classful, ou seja, toda a faixa de endereços IP versão 4 foram divididos em cinco classes: A, B, C, D e E, as quais somente os endereços das classes A, B e C são realmente utilizados para a comunicação entre dois hosts em Unicast.

A classe D foi reservada para serviços de Multicasting, para comunicação em grupos, e a classe E reservada para uso experimental.

Abaixo temos uma figura que descreve como reconhecer cada classe, seus bits de rede e de host.

	Bits de Rede	Bits de Host	Bits da Classe	
Classe	1º Byte	2º Byte	3º Byte	4º Byte
Classe A	00000000	00000000	00000000	00000000
Classe B	10000000	00000000	00000000	00000000
Classe C	11000000	00000000	00000000	00000000
Classe D	11100000	00000000	00000000	00000000
Classe E	11110000	00000000	00000000	00000000

Com essa divisão em classes não flexibilidade, pois temos apenas 126 classes A com mais de 16 milhões de hosts por rede, para a classe B a relação entre rede e host é de 16.384 redes com mais de 65 mil hosts possíveis por rede e para a classe C a relação é de mais de 2 milhões de redes com apenas 254 hosts possíveis por rede.

Mas e se minha rede precisa de 1000 hosts? Com o conceito classful ou você utilizar uma classe A ou uma classe B e convive com o excesso de endereços!

Outra opção para o exemplo acima seria quebrar a LAN em várias VLANs utilizando classe C com 254 hosts por sub-rede e com 5 VLANs você conseguiria endereçar os 1000 hosts e ter uma folga.

O maior problema que o roteamento Classful trouxe (por isso foi logo abandonado na prática) é a extinção de endereços válidos de Internet, pois com a explosão do uso da Internet e número de usuários esse modelo de classes acabaria resultando em uma depleção muito rápida dos endereços.

Portanto, atualmente na Internet e redes corporativas utilizam-se diferentes máscaras de sub-rede além dos padrões /8 (Classe A - 255.0.0.0), /16 (Classe B - 255.255.0.0) e /24 (Classe C - 255.255.255.0).

Nesse capítulo vamos estudar quais são esses recursos de divisão em sub-rede, tais como VLSM e CIDR, já com um enfoque de projeto de redes IP Hierárquicas, as quais permitem além de aproveitar melhor toda faixa de endereçamento IP também permitem realizar a summarização de redes, possibilitando economia no anúncio de redes realizado pelos roteadores.

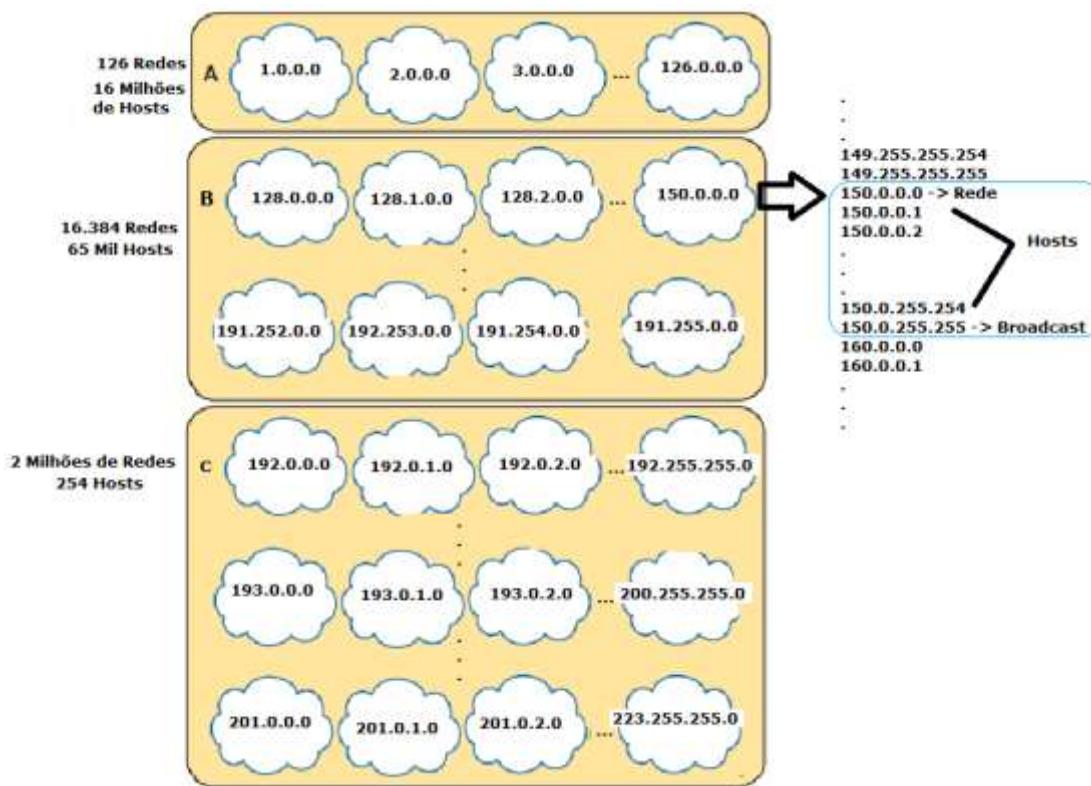
## 1.1 Componentes do Endereçamento IP

Os endereços IP utilizados para o endereçamento dos computadores, servidores e demais dispositivos de rede, seja em uma rede classful ou classless, estão dentro da faixa de endereçamento das Classes A, B e C.

Os endereços são compostos pelo IP e uma máscara de rede ou sub-rede. O IP traz a informação do endereço de rede e host, o qual é delimitado pela máscara, portanto em uma rede IP temos:

- **Endereços de Rede:** Identificam a própria rede e não uma interface de rede específica. Representado por todos os bits de host com o valor zero e é o primeiro IP de uma rede ou Sub-rede. Descobrimos o endereço de rede calculando o AND lógico entre um IP e sua máscara.
- **Endereços de Host:** Identificam uma interface de rede específica ou um host. É o valor numérico onde na máscara de rede está representado com valor zero. Por exemplo, se você tiver o IP 10.150.20.1 com máscara de rede padrão 255.0.0.0, a rede será 10 e o host é representado pelo valor 150.20.1. Os endereços de host vão do primeiro IP após a rede ao penúltimo IP, anterior ao endereço de broadcast.
- **Endereços de Broadcast:** Identificam todas as máquinas na rede específica, representado por todos os bits de host com o valor UM. Ainda um endereço de broadcast pode ser chamado broadcast local (255.255.255.255 – último IP da faixa total de endereços IP), ou seja, para todos os usuários de uma LAN, ou broadcast direcionado para apenas uma rede ou sub-rede (ex: 200.192.121.255 – é o último IP de uma rede ou sub-rede).

Na figura abaixo temos uma representação das três classes de IP e em destaque uma rede IP específica classe B 150.0.0 com máscara padrão /16 mostrando o endereço de rede, faixa de IPs que pode ser utilizada para endereçar hosts e seu broadcast.



Em resumo os endereços de rede representam um conjunto de endereços, mais que endereços estão nesse conjunto? Quem diz isso é a máscara. Então para termos quantidades diferentes de endereços por rede basta utilizarmos máscaras diferentes? É isso mesmo!

Basicamente fazer sub-redes é trabalhar com os bits de host (bits zero) das máscaras padrões das classes para cria sub-redes, ou seja, vamos quebrar as máscaras padrões em máscaras menores possibilitando acomodar diferentes tamanhos de rede, o que chamamos de sub-redes.

## 2 Entendendo o Conceito de Sub-rede, VLSM e CIDR

O conceito de sub-redes nasceu da necessidade de se melhor aproveitar o endereçamento IP, flexibilizando a tradicional divisão em classes onde a divisão entre rede e host ocorre somente a cada oito bits. Com as sub-redes a identificação de rede e host no endereçamento IP é feita de forma variável, podendo utilizar outras quantidades de bits além de múltiplos de oito.

Porém, normalmente o conceito de sub-redes divide uma rede classe A, B ou C inteira em tamanhos iguais, por exemplo, se pegarmos a rede privativa classe A 10.0.0.0 e aplicarmos a máscara 255.255.255.0 vamos dividir essa rede como classes C iniciando em 10.0.0.0/24, 10.0.1.0/24, 10.0.2.0/24 até 10.255.255.0/24. Dessa maneira temos mais de 65 mil sub-redes cada uma com 254 hosts, pois "emprestamos" 16 bits da máscara original para fazer sub-rede e sobraram oito bits para os hosts.

Mesmo assim esse conceito é limitado, por isso as redes normalmente não utilizam apenas uma rede classe A, C ou C dividida com um tamanho de máscara único, utiliza-se o /24 para redes de até 254 hosts, mas e se a rede precisar de sub-redes com apenas 10 endereços? Nesse caso cria-se uma máscara para esse tamanho de rede também! Daí vem o conceito de **VLSM** ou **Variable Length Subnet Mask**, o uso de vários comprimentos de máscaras para melhor adaptar os requisitos de endereçamento de cada segmento de rede.

Até o momento respeitamos o tamanho das classes, ou seja, se tenho uma classe C e faço uma sub-rede ou VLSMs com ela utilize máscaras maiores que /24 (/25 ou maior), porém existem uma outra maneira de encarar os endereços IP simplesmente esquecendo das classes, ou seja, uma rede IP é uma rede e uma máscara. Por exemplo, a faixa de endereços classe C privativos iniciam em 192.168.0.0 e vai até 192.168.255.0, com o conceito acima posso representar todos esses endereços com uma rede 192.168.0.0/16, pois essa rede pega os IPs de 192.168.0.1 até 192.168.255.255.

O que descrevemos acima é o conceito de roteamento sem classes ou CIDR (Classless Intra Domain Routing), atualmente utilizado em toda a Internet para possibilitar que os endereços IPs sejam tratados em blocos e possam ser summarizados ou agregados em um único ou poucos anúncios.

Imagine um roteador de Internet que possui em seu domínio todos os IPs de 192.0.0.0 até 192.255.255.255. Dividindo em classes C ele teria que anunciar simplesmente mais de 65 mil redes, com o CIDR o roteador pode criar uma rota sumário 192.0.0.0/8 e anunciar todos os IPs com uma única entrada de roteamento, salvando recursos de memória e CPU em toda a Internet!

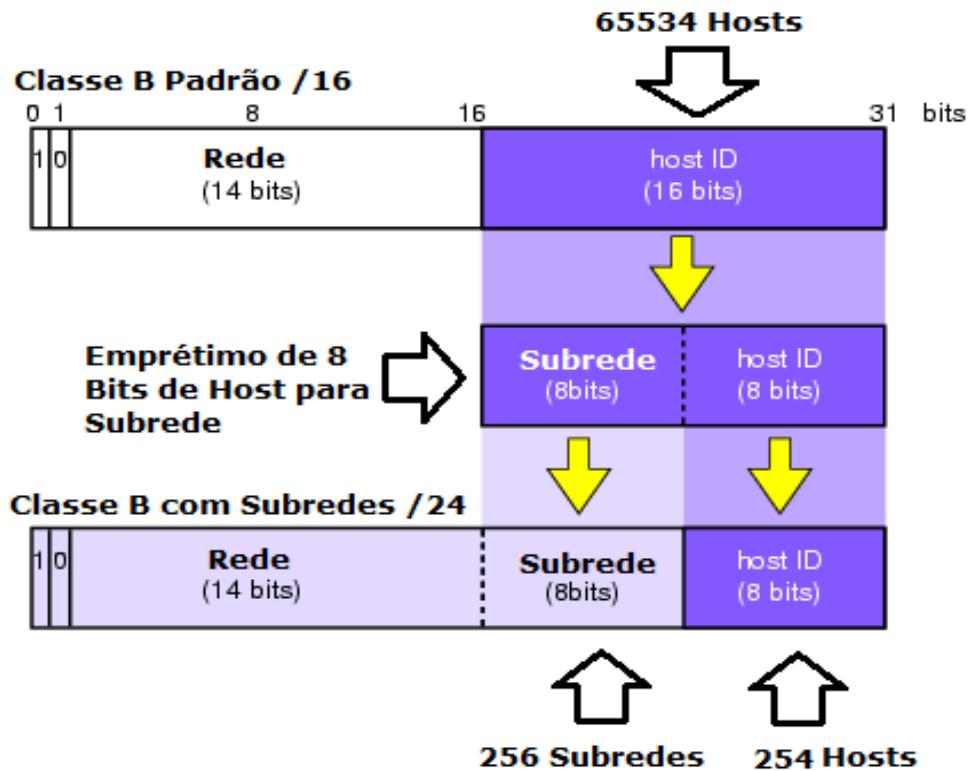
Portanto aqui nesse breve resumo temos seu objetivo desse capítulo:

- Aprender a calcular sub-rede.
- Aprender a dividir essas sub-redes em máscaras menores criando VLSMs.
- Aprender a criar rotas que summarizem várias sub-redes e VLSMs em um único ou poucos anúncios.
- Por fim, aprender o conceito e calcular redes CIDR.

Para isso é muito importante entender binário e a conversão de decimal para binário, se você ainda não entendeu esses assuntos vale a pena voltar ao capítulo 5 e revisar!

### 3 Dividindo Redes em Sub-redes

Dividir redes classful em sub-redes é “**emprestar**” ou “**roubar**” bits da máscara padrão para criar sub-redes, dividindo as máscaras padrões em um tamanho menor, veja a figura abaixo.



Nessa figura temos uma máscara classe B padrão **255.255.0.0**, em binário **11111111.11111111.00000000.00000000**, portanto onde temos bits 1 na máscara são endereços fixos e não podemos alterar, agora podemos sim “emprestar” bits de host (zero) da máscara para criar redes menores ou sub-redes. Nesse exemplo emprestamos oito bits da máscara de rede para criar 256 sub-redes ( $2^8$  bits emprestados) cada uma com 254 hosts ( $2^8$  bits zero que sobraram na máscara de sub-rede). Com isso a máscara de rede padrão 255.255.0.0 vira a máscara de sub-rede 255.255.**255**.0, pois emprestamos 8 bits dela para criar sub-redes.

Se estivermos utilizando a rede 128.0.0.0, no total ela tem dos IPs 128.0.0.1 até 128.0.255.255, agora vamos subdividir esses IPs em sub-redes menores iniciando em 128.0.0.0 até 128.0.0.255, depois 128.0.1.0 até 128.0.1.255, 128.0.2.0 até 128.0.2.255 e assim segue até a última sub-rede 128.0.255.0 até 128.0.255.255.

Esse é o princípio básico de divisão em sub-redes e é importante que você saiba o **porquê de calcular sub-redes** para continuar os estudos e realmente aprender esse assunto, para assim poder resolver os exercícios das provas 100-105, 200-105 ou CCNA Composite!

Vamos elaborar melhor essa necessidade entendendo o problema e suas soluções:

- **Problema 1:** as classes dividem as redes e hosts em valores fixos e não flexíveis, por exemplo, se eu precisar de uma máscara que suporte pelo menos 1000 hosts por sub-rede não é possível com classe A, B e C pura sem exceder ou ter a necessidade de dividir esses hosts em redes menores.
- **Problema 2:** Minha rede corporativa é composta por 50 segmentos, assim como no exemplo anterior não temos uma máscara que suporte o mais próximo possível de 50 redes sem termos desperdício de endereços.
- **Problema 3:** Uma rede precisa de 128 sub-redes cada uma com até 1000 hosts. Idem aos dois exemplos anteriores.
- **Solução:** para os três problemas é escolher uma classe que melhor se encaixe nas quantidades mínimas de endereçamento e utilizar a divisão em sub-rede para encontrar uma máscara mais precisa.

Os problemas citados acima são de projeto, onde é passado um requisito de quantidade de hosts ou de sub-redes para que o aluno calcule a melhor máscara.

Outro modelo de questão de sub-rede é a análise do endereçamento dado um endereço e máscara. Por exemplo, a questão fornece o endereço 192.168.1.10 com a máscara 255.255.255.240 e realiza perguntas como:

- Qual o endereço de sub-rede desse host?
- Qual o endereço de broadcast dessa sub-rede?
- Quais endereços em uma lista pertencem à mesma sub-rede que aquele host?
- Dada uma lista de endereços reconheça IPs válidos (que podem ser endereçados em hosts)?

Além desse conceito poder ser cobrado em conjunto com questões práticas, por exemplo, configure uma interface LAN do roteador, sendo que seu endereço IP é o primeiro IP válido pertencente à quinta sub-rede de 192.168.0.0/29. Nesse caso o aluno terá que calcular a sub-rede que o IP pertence e aí sim poder realizar a configuração da interface LAN.

Para realizar esses cálculos existem vários métodos, porém desenvolvemos uma metodologia simples e principalmente veloz de resolução de problemas de sub-rede, a qual estudaremos ao longo do capítulo.

Nesse capítulo vamos ensinar os cálculos utilizando sempre exemplos práticos, além de mais produtivo é muito mais simples de ensinar e aprender!

### 3.1 Método Tradicional de Análise de Endereços IP

A maneira tradicional de analisar um endereço IP é utilizando a definição, ou seja, fazendo o AND lógico entre o endereço e sua máscara d sub-rede. Com esse método conseguiremos descobrir seu endereço de rede, faixa de valores válidos para endereçamento em hosts e também o broadcast direcionado da sub-rede em questão.

Vamos a um exemplo prático, onde temos o endereço 192.168.10.170 com a máscara 255.255.255.240 ou /28.

1. Primeiro passo da análise é descobrir a classe, a qual é C, pois se convertermos o primeiro octeto em binário temos 192=11000000.
2. Em seguida vamos fazer o AND lógico. Essa conta é realizada em binário, porém como qualquer bit com zero é zero e somente bit um com bit um dá um não precisamos converter todos os octetos, pois somente quando a máscara é diferente de zero (tudo zero) ou 255 (tudo um) que precisaremos converter, veja a seguir.

192.168.10 .170  
 AND 255.255.255.240  
 192.168.10 .???

Como qualquer coisa com 1 dá ela mesma, 192 AND 255=192, 168 AND 255=168 e 10 AND 255=10, porém com o 240 teremos que transformar o octeto do endereço e da máscara em binário, veja abaixo:

170 = 10101010  
 240 = 11110000  
 $10100000 = 128+0+32+0+0+0+0 = 160$

Portanto, o endereço pertence à sub-rede **192.168.10.160**.

3. Agora vamos encontrar o endereço de broadcast dessa sub-rede. Por definição o broadcast tem todos os bits de host setados em "1", portanto teremos:  
 $192.168.10.1010\textcolor{yellow}{1111} = \textbf{192.168.10.175}$ .
4. Os hosts válidos estão entre o endereço de rede e o broadcast, ou seja, iniciando em 192.168.1.161 e vão até 192.168.1.174, totalizando 14 hosts válidos por sub-rede. Veja a sequência de IPs válidos dessa sub-rede:
  - 1) 192.168.10.1010**0001** → 161 → **1º endereço válido**
  - 2) 192.168.10.1010**0010** → 162
  - 3) 192.168.10.1010**0011** → 163
  - 4) 192.168.10.1010**0100** → 164
  - 5) 192.168.10.1010**0101** → 165
  - 6) 192.168.10.1010**0110** → 166
  - 7) 192.168.10.1010**0111** → 167
  - 8) 192.168.10.1010**1000** → 168
  - 9) 192.168.10.1010**1001** → 169
  - 10) 192.168.10.1010**1010** → 170
  - 11) 192.168.10.1010**1011** → 171
  - 12) 192.168.10.1010**1100** → 172
  - 13) 192.168.10.1010**1101** → 173
  - 14) 192.168.10.1010**1110** → 174 → **último endereço válido (broadcast -1)**

Na prática a cada bit emprestado de uma máscara você divide essa rede em dois elevados a n, onde esse n são os bits emprestados. Note no exemplo acima que temos um endereço classe C com uma máscara /28, como a padrão é /24 emprestamos 4 bits para sub-rede, portanto estamos dividindo essa rede em  $2^4$  sub-redes, o que nos dá um total de 16 sub-redes.

Como uma classe C tem um total de 256 endereços (primeiro a rede, do segundo ao penúltimo os hosts válidos e o último o broadcast), se dividirmos 256 por 16 teremos que cada sub-rede tem um total de 16 endereços, como cada sub-rede terá seu próprio endereço de sub-rede e um broadcast direcionado, sobre 14 hosts para cada uma delas.

Se você notou acima, em termos quantitativos as contas continuam basicamente as mesmas, o número de sub-redes são dois elevados à quantidade de bits emprestados e os hosts são dois elevados à quantidade de bits zero que sobraram na máscara de sub-redes.

Existem na Internet os famosos “**subnet calculators**” ou calculadoras de sub-rede, você pode utilizar esses recursos apenas para conferir seus cálculos, porque tanto no CCENT como no CCNA não é permitida calculadora nem qualquer dispositivo de ajuda, as contas são feitas pelo próprio aluno!

### 3.2 Exemplo Prático I – Dividindo Redes Classe A, B e C em duas Sub-redes

Conforme o que já estudamos de sub-rede, para dividir uma rede Classe A, B ou C em duas sub-redes precisamos emprestar apenas um bit de host e transformá-lo em bit de sub-rede (1).

Vamos iniciar utilizando um endereço classe C padrão 192.168.1.0 com máscara 255.255.255.0 (/24). Seus IPs válidos ou de hosts vão de 192.168.1.1 a 192.168.1.254 e o endereço de broadcast é 192.168.1.255.

Agora vamos emprestarmos 1 bit e dividir a rede em duas sub-redes, assim teremos:

- Primeira sub-rede: 192.168.1.0 com máscara 255.255.255.128
  - Hosts válidos 192.168.1.1 a 192.168.1.126
  - Broadcast 192.168.1.127
- Segunda sub-rede: 192.168.1.128 com máscara 255.255.255.128
  - Hosts válidos 192.168.1.129 a 192.168.1.254
  - Broadcast 192.168.1.255

Note que a máscara padrão era 255.255.255.0, se emprestamos um bit ela fica 255.255.255.10000000 ou 255.255.255.128. Com um bit apenas emprestado temos duas opções de sub-rede, quando ele for zero e depois quando for 1, por isso temos a primeira sub-rede 192.168.1.0 e a segunda 192.168.1.128.

Outra forma de analisar é que temos um total de 256 endereços contando todos, incluindo a rede e o broadcast, por isso dividindo em dois conjuntos temos que um tem os endereços de 0 a 127 e o segundo de 128 a 255. Sendo que o primeiro endereço é a sub-rede e o último é o broadcast.

Para as classes A e B a análise de emprestar um bit é parecida, porém em octetos diferentes.

Na classe B os hosts iniciam no terceiro octeto, portanto teremos a máscara 255.255.100000000.00000000 = 255.255.128.0. Se utilizarmos a rede 172.16.0.0 como exemplo teremos as sub-redes 172.16.0.0/17 e 172.16.128.0/17, dividimos na realidade 65.536 endereços (incluindo rede e broadcast) em dois conjuntos de 32.768 endereços. Vamos analisar as sub-redes abaixo:

- Primeira sub-rede: 172.16.0.0 com máscara 255.255.128.0
  - Hosts válidos 172.16.0.1 até 172.16.127.254
  - Broadcast 172.16.127.255
- Segunda sub-rede: 172.16.128.0 com máscara 255.255.128.0
  - Hosts válidos 172.16.128.1 até 172.16.255.254
  - Broadcast 172.16.255.255

Para dividir uma classe A em duas sub-redes temos a máscara /9 ou 255.128.0.0, onde estamos dividindo  $2^{24}$  endereços (16.777.216) em dois conjuntos de 8.388.608 endereços, incluindo o endereço de sub-rede e broadcast. Com isso teremos as seguintes sub-redes para a rede privativa 10.0.0.0/8:

- Primeira sub-rede: 10.0.0.0 com máscara 255.128.0.0
  - Hosts válidos 10.0.0.1 até 10.127.255.254
  - Broadcast 10.127.255.255
- Segunda sub-rede: 10.128.0.0 com máscara 255.128.0.0
  - Hosts válidos 10.128.0.1 até 10.255.255.254
  - Broadcast 10.255.255.255

Portanto, em última análise, fazer sub-rede é adicionar bits “1” nas máscaras padrões das classes A, B e C para permitir a divisão dessas redes em sub-redes.

Seguindo o padrão do binário emprestamos um bit dividimos a rede em duas sub-redes ( $2^1=2$ ), se emprestarmos dois bits dividimos a rede em quatro sub-redes ( $2^2=4$ ), se emprestarmos três bits dividimos a rede em oito sub-redes ( $2^3=8$ ) e assim por diante.

Note que quando falamos em sub-rede a classe continua sendo importante, porque o empréstimo de bits se dá na faixa de hosts, o que é dado pela classe do endereço IP. Na classe A o empréstimo inicia no segundo octeto, já na classe B no terceiro octeto e na classe C no quarto octeto. O mesmo vale para o VLSM.

### 3.3 Exemplo Prático II - Projeto de Sub-redes por Redes

Vamos acompanhar a solução de um problema prático muito comum na vida de um administrador de rede. Suponha que você é o administrador de rede da empresa **Mantra LTDA** e necessita de pelo menos **10 sub-redes** para prover endereçamento para seus grupos de usuários da rede interna. Ele deverá utilizar a rede classe C **192.168.0.0/24** (**255.255.255.0**) para efetuar o endereçamento.

Antes da implementação o gerente da área faz as seguintes indagações sobre esse projeto e o administrador deve respondê-las:

- 1) Quantos bits serão necessários emprestar da parte de host da máscara de rede original para fazer a divisão e obter no mínimo 10 sub-redes?
- 2) Qual a nova máscara de sub-rede?
- 3) Quantos números endereços válidos (hosts) estarão disponíveis em cada sub-rede para endereçar os computadores?
- 4) Qual a faixa de endereços de cada sub-rede (sub-rede, endereços válidos e broadcast).

Lembre-se que criar uma sub-rede nada mais é que “**emprestar bits de host**” (bits zero) para criar novas redes, chamadas sub-redes. Com uma rede Classe C, a qual tem a máscara padrão 255.255.255.0 ou /24, quantos bits precisamos emprestar do **último octeto** para termos 10 sub-redes?

Para responder essa pergunta vamos aos valores de cada binário de um octeto:

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

Para caber 10 sub-redes teremos que emprestar 4 bits da máscara, que dão 16 sub-redes, aí teremos as dez que precisamos mais seis de reserva. Nesse tipo de exercício sempre pegamos a que mais se aproxima do valor pedido.

Agora já podemos responder o item 1, são 4 bits emprestados, assim como o item 2, pois a nova máscara será 255.255.255.**11110000** = 255.255.255.240 (128+64+32+16+0+0+0+0).

Se analisarmos então teremos um total de 16 sub-redes com 14 hosts cada uma, pois temos quatro bits zero sobrando na máscara e o número de hosts é igual a dois elevados ao número de bits zero da máscara menos dois, pois temos que descontar o endereço de rede e de broadcast, por isso temos “ **$2^4-2 = 16 - 2 = 14$** ” hosts por sub-rede.

A faixa de IPs inicia com a primeira sub-rede chamada “**subnet zero**” ou sub-rede zero e nesse exemplo crescem em múltiplos de 16, veja sequência abaixo iniciando na subnet zero:

0. **192.168.0.0**, sendo que o primeiro IP válido é 192.168.0.1 e o último é 192.168.0.14, já o broadcast é 192.168.0.15. A partir de agora elas variam de 16 em 16.
1. **192.168.0.16** (0+16), sendo que o primeiro IP válido é 192.168.0.17 e o último é 192.168.0.30, já o broadcast é 192.168.0.31.
2. **192.168.0.32** (16+16), sendo que o primeiro IP válido é 192.168.0.33 e o último é 192.168.0.46, já o broadcast é 192.168.0.47.

3. **192.168.0.48** (32+16), sendo que o primeiro IP válido é 192.168.0.49 e o último é 192.168.0.62, já o broadcast é 192.168.1.63.
4. **192.168.0.64** (48+16), sendo que o primeiro IP válido é 192.168.0.65 e o último é 192.168.0.78, já o broadcast é 192.168.1.79.

E assim continua até a última sub-rede (subnet 15) que tem o valor do último octeto igual ao valor da máscara: **192.168.0.240**, endereços válidos de 192.168.0.241 até 192.168.0.254, com broadcast 192.168.0.255. A última sub-rede é chamada de "broadcast subnet", porque todos os bits de sub-rede tem o valor 1: 192.168.0.**1111**0000.

A seguir veremos mais detalhes sobre a subnet zero e a de broadcast.

Note que em binário as sub-redes são a variação dos bits uns da máscara de sub-rede calculada, veja exemplo abaixo:

0. 192.168.0.**0000**0000 → 192.168.0.0
1. 192.168.0.**0001**0000 → 192.168.0.16
2. 192.168.0.**0010**0000 → 192.168.0.32
3. 192.168.0.**0011**0000 → 192.168.0.48
4. 192.168.0.**0100**0000 → 192.168.0.64
5. 192.168.0.**0101**0000 → 192.168.0.80
6. 192.168.0.**0110**0000 → 192.168.0.96
7. 192.168.0.**0111**0000 → 192.168.0.112
8. 192.168.0.**1000**0000 → 192.168.0.128
9. 192.168.0.**1001**0000 → 192.168.0.144
10. 192.168.0.**1010**0000 → 192.168.0.160
11. 192.168.0.**1011**0000 → 192.168.0.176
12. 192.168.0.**1100**0000 → 192.168.0.192
13. 192.168.0.**1101**0000 → 192.168.0.208
14. 192.168.0.**1110**0000 → 192.168.0.224
15. 192.168.0.**1111**0000 → 192.168.0.240

Note uma característica interessante, o que dá o valor de quanto em quanto uma sub-rede varia é o último bit da máscara de sub-rede, por exemplo, na máscara 255.255.255.240 o último octeto é 240, em binário **11110000** e seu último bit vale 16. Isso não é uma coincidência e pode ser utilizado nos cálculos de sub-rede, você verá mais para frente como esse conceito é útil para resolver problemas de sub-rede.

Outro fato importante que podemos tirar dos cálculos realizados até o momento é que o broadcast de uma sub-rede é um valor a menos que a sub-rede seguinte, por exemplo, o broadcast da sub-rede 13 (192.168.0.208/28) é 192.168.0.223, ou seja, o valor da sub-rede 14 192.168.0.224 menos 1. Com isso a faixa de IPs válidos dica fácil de ser encontrada, pois vai de um após a sub-rede "**192.168.0.208 + 1 = 192.168.0.209**" até um a menos que o broadcast "**192.168.0.223 - 1 = 192.168.0.222**".

Esse é outro princípio para facilitar e acelerar os cálculos, achando as sub-redes temos automaticamente os broadcast, portanto o que está entre o endereço de sub-rede e o broadcast são os endereços válidos.

Resumindo, se você tem a máscara, com o último bit 1 dela tem também de quanto em quanto as sub-redes variam. Escrevendo as sub-redes uma embaixo da outra, olhando um valor a menos que a próxima você tem o broadcast, por último, tudo que está entre o endereço de sub-rede e o broadcast são os IPs válidos!

Com esse conceito **99,9%** dos exercícios de sub-rede, VLSM e CIDR são resolvidos, por isso entenda esse conceito que vamos praticar ao longo desse capítulo!

### 3.4 Entendendo a Subnet-Zero e Broadcast-Subnet

Nos primórdios do endereçamento IP costumava-se não utilizar nem a subnet zero nem a de broadcast, isso devido a implementação nos roteadores, porém atualmente esse tipo de cálculo é uma exceção, pois todos os equipamentos da Cisco utilizam o comando em modo de configuração global “**ip subnet-zero**”, o qual ativa no roteador a utilização da subnet zero. A subnet de broadcast já era suportada, porém não utilizada apenas por uma convenção entre os administradores de rede.

Portanto, se inserirmos o comando no roteador “**no ip subnet-zero**” ele não aceitará a configuração de IPs da primeira sub-rede disponível, veja exemplo abaixo:

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip subnet-zero
R1(config)#int f0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.240
Bad mask /28 for address 192.168.0.1
```

Portanto, com o comando “no ip subnet-zero”, ao tentarmos configurar a interface fast 0/0 com o primeiro IP da subnet zero recebemos uma mensagem de Bad Mask e o comando não foi aceito. Agora note abaixo quando tentamos configurar na sequência um IP da última sub-rede, a de broadcast, note que o roteador irá aceitar sem problemas:

```
R1(config-if)#ip address 192.168.0.254 255.255.255.240
R1(config-if)#do sho ip route
### Saídas omitidas ###

      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.0.240/28 is directly connected, FastEthernet0/0
L         192.168.0.254/32 is directly connected, FastEthernet0/0
R1(config-if) #
```

É preciso tomar cuidado com esse detalhe da subnet zero ser válida ou não em exercícios de sub-rede, pois podem ser cobradas ambas as filosofias de endereçamento, ou seja, a atual que todas as sub-redes são aceitas ou a antiga onde devíamos desconsiderar a primeira (subnet zero) e a última (broadcast subnet) das nossas contas.

### 3.5 Exemplo Prático III - Projeto de Sub-redes por Hosts

Nesse segundo exemplo prático o administrador de redes recebeu o endereço de classe B 172.16.0.0/16 (255.255.0.0) e precisa descobrir a máscara de sub-rede que suporte no mínimo **1000 endereços válidos para hosts**. Mais uma vez o gerente da área faz as seguintes indagações sobre esse projeto:

1. Quantos bits serão necessários emprestar para fazer a divisão e obter pelo menos 1000 hosts?
2. Qual a nova máscara de sub-rede?
3. Quantas sub-redes estarão disponíveis para esse número de hosts?
4. Listar a faixa de endereços para as cinco primeiras sub-redes iniciando pela sub-rede zero.

No exemplo prático 2, onde fizemos um projeto pela quantidade de sub-redes tivemos que pensar em quantos bits uns teríamos que emprestar para suportar 10 sub-redes. Agora nesse exemplo precisamos projetar nossa máscara utilizando a informação quantitativa de hosts.

Nesse tipo de exercício temos que procurar o número de bits zero temos que deixar na máscara para suportar a quantidade de hosts necessários! Alguns valores em binário são importantes

saber, tais como os valores dos oito bits de um octeto e também valores como  $2^8$ ,  $2^9$  e  $2^{10}$ . É simples, já sabemos que  $2^7$  é 128, portanto elevado a 8 será 256 ( $128 \times 2$ ),  $2^9$  será 512 ( $256 \times 2$ ) e  $2^{10}$  será 1024 ( $512 \times 2$ ). Portanto, para termos 1000 hosts precisamos deixar 10 bits na máscara de sub-rede.

A máscara de classe B tem 16 bits uns e 16 bits zero, portanto temos 255.255.0.0 ou 11111111.11111111.00000000.00000000, se temos que deixar 10 bits zero basta deixar da esquerda para a direita e depois completar com bits uns! Teremos então 11111111.11111111.11111111.00.00000000 que dá a máscara /22, ou seja, emprestamos 6 bits e deixamos 10 dos dezesseis para os hosts.

As questões 1 e 2 já podem ser respondidas, teremos que emprestar 6 bits uns e teremos a máscara 255.255.252.0 (11111100 =  $128+64+32+16+8=252$ ).

A questão 3 sobre quantas sub-redes teremos se resolve elevando dois ao número de bits emprestados, ou seja,  $2^6=64$  sub-redes com até  $2^{10-2}=1024-2=1022$  hosts por sub-rede.

A questão 4 confunde muita gente, pois ficamos muito acostumados a calcular sub-redes para classes C, ou seja, de /25 para cima. Para máscaras /23 ou menores temos que tomar cuidado, vamos à resolução. Primeiro vamos descobrir a variação, que é o valor do último bit 1 da máscara: 255.255.11111111.00000000 = 4, portanto as sub-redes variam de 4 em 4 a partir do terceiro octeto! Veja abaixo como fica:

0. **172.16.0.0** → broadcast 172.16.3.255 e IPs válidos de 172.16.0.1 até 172.16.3.254
1. **172.16.4.0** → broadcast 172.16.7.255 e IPs válidos de 172.16.4.1 até 172.16.7.254
2. **172.16.8.0** → broadcast 172.16.11.255 e IPs válidos de 172.16.8.1 até 172.16.11.254
3. **172.16.12.0** → broadcast 172.16.15.255 e IPs válidos de 172.16.12.1 até 172.16.15.254
4. **172.16.16.0** → broadcast 172.16.19.255 e IPs válidos de 172.16.16.1 até 172.16.19.254
5. **172.16.20.0** (inserida somente para poder encontrar o broadcast)

A sequência de resolução é: escrever as sub-redes, encontrar o broadcast e depois a faixa de IPs válidos.

### 3.6 Análise de Endereços IP com a Metodologia Dltc

Podemos também utilizar a metodologia de análise realizada nos exercícios de projeto para resolver problemas onde envolvem a análise de endereços IP e máscara.

Vamos fazer o mesmo exemplo da análise realizada com o método tradicional com o endereço 192.168.10.170 e máscara 255.255.255.240 ou /28. Vamos descobrir as seguintes informações:

- 1) Qual a sub-rede que o IP pertence?
- 2) Qual o endereço de broadcast da sub-rede?
- 3) Qual a faixa de endereços válidos?

Vamos à resolução!

Passo 1 - Pelo nosso método tudo começa verificando a variação das sub-redes com a máscara /28, que é o valor do último bit "1" da máscara em decimal. A máscara /28 em binário é 11111111.11111111.11111111.11111000, portanto o bit vale 16 em decimal, o que nos leva que as sub-redes variam de 16 em 16.

Passo 2 – Agora escreva as sub-redes uma embaixo da outra até que o endereço a ser analisado (**192.168.10.170**) esteja entre duas das sub-redes escritas (é só somar 16 no último octeto):

- 0. 192.168.10.0
  - 1. 192.168.10.16
  - 2. 192.168.10.32
  - 3. 192.168.10.48
  - 4. 192.168.10.64
  - 5. 192.168.10.80
  - 6. 192.168.10.96
  - 7. 192.168.10.112
  - 8. 192.168.10.128
  - 9. 192.168.10.144
- 10.192.168.10.160**  
**11.192.168.10.176**

Achamos, o IP 192.168.10.170 pertence à sub-rede 192.168.10.160, agora fica fácil, porque o broadcast é um valor antes da próxima sub-rede (192.168.10.176) e é 192.168.10.175, por isso os IPs válidos estão entre a sub-rede e o broadcast, por isso vão de 192.168.10.161 até 192.168.10.174.

Se o exercício pedisse para reconhecer broadcasts entre redes que iniciam nas redes 192.168.10.0 com a máscara /28 fica simples, porque são os IPs ímpares antes das sub-redes escritas.

Se a pergunta fosse reconhecer endereços de sub-rede seria mais fácil ainda, assim como reconhecer IPs válidos, pois é só escrever as sub-redes como fizemos nesse exercício, anotar também os broadcasts e tudo que não for sub-rede ou broadcast é IP válido!

Nas vídeo-aulas do capítulo vamos explorar esses conceitos e ensinar a utilizar essa metodologia que agiliza as contas, pois para exames de certificação a velocidade e automação na resolução de exercícios são muito importantes, pois um dos fatores que mais reprovam é a administração do tempo de prova.

### **3.7 Máximo de Bits de Host Emprestados**

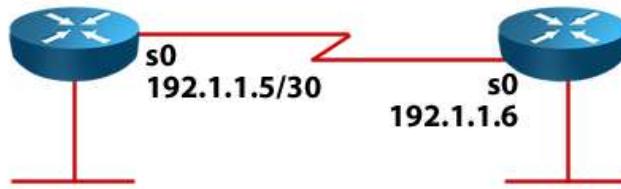
Nesse tópico vamos procurar responder até quantos bits podemos emprestar para criar sub-redes. Para isso lembre-se que uma rede IP tem:

- 1) Endereço de rede
- 2) Hosts válidos
- 3) Endereço de broadcast

Por isso, teoricamente precisamos no mínimo de 3 endereços em uma sub-rede para que ela tenha hosts válidos. Não existe máscara com 3 endereços, lembre-se que as máscaras sempre são valores pares, por isso a última máscara válida para sub-redes é a /30 ou 255.255.255.252, pois com ela temos 4 endereços totais, sendo que o primeiro será a sub-rede, dois endereços de hosts e um broadcast.

Essa máscara é utilizada em redes WAN ponto a ponto, onde precisamos de apenas dois endereços, um para cada ponta do link. Veja figura a seguir, onde temos um link ponto a ponto configurado com IPs da rede 192.168.1.4/30.

### WAN Ponto a Ponto



Essa recomendação vale para todas as Classes, apesar de atualmente existir a RFC 3021 (Using 31-Bit Prefixes on IPv4 Point-to-Point Links), normalmente no CCENT/CCNA essas máscaras não são utilizadas, sendo o máximo permitido até a /30.

### 3.8 Resumo das Máscaras de Sub-rede por Classe

As máscaras de sub-rede possíveis por classe tem um número limitado, por exemplo, como a classe A tem por padrão um comprimento de oito bits (/8), suas sub-redes iniciam com nove bits (/9) e vão até /32 (/9, /10, /11, ..., /30, /31 e /32).

Para a classe B, fazendo a mesma análise, temos de /17 até /32, pois o padrão é /16. Já para a classe C, como o padrão é /24 temos de /25 até /32. Lembrando que a /31 depende do suporte à RFC 3021 e a /32 representa um host único, chamada de máscara de host.

Veja na tabela abaixo todas as máscaras possíveis para a classe A.

Classe A (1-126) - Padrão 255.0.0.0 com prefixo /8				
Bits emprestados	Máscara	Prefixo	Sub-redes ( $2^n$ )	Hosts ( $2^n - 2$ )
1	255.128.0.0	/9	2	8388606
2	225.192.0.0	/10	4	4194302
3	225.224.0.0	/11	8	2097150
4	225.240.0.0	/12	16	1048574
5	225.248.0.0	/13	32	524286
6	225.252.0.0	/14	64	262142
7	225.254.0.0	/15	128	131070
8	255.255.0.0	/16	256	65534
9	255.255.128.0	/17	512	32766
10	255.255.192.0	/18	1024	16382
11	255.255.224.0	/19	2048	8190
12	255.255.240.0	/20	4096	4094
13	255.255.248.0	/21	8192	2046
14	255.255.252.0	/22	16384	1022
15	255.255.254.0	/23	32768	510
16	255.255.255.0	/24	65536	254
17	255.255.255.128	/25	131072	126
18	255.255.255.192	/26	262144	62
19	255.255.255.224	/27	524288	30
20	255.255.255.240	/28	1048576	14
21	255.255.255.248	/29	2097152	6
22	255.255.255.252	/30	4194304	2
			n= bits 1 emprestados	n= bits 0

Portanto, podemos iniciar com a máscara /9 temos um bit emprestado para sub-rede, dividindo a rede classe A em duas sub-redes com 8.388.606 hosts cada uma, e emprestar até 22 bits para formar uma máscara /30 com 4.194.304 sub-redes de apenas dois hosts cada uma, utilizados para endereçar redes WAN ponto a ponto.

Para a classe B o empréstimo de bits inicia no terceiro octeto, pois o primeiro e segundo bytes são fixos para rede. Veja a tabela com todas as sub-redes possíveis para endereços classe B abaixo.

<b>Classe B (128-191) - Padrão 255.255.0.0 com prefixo /16</b>				
<b>Bits emprestados</b>	<b>Máscara</b>	<b>Prefixo</b>	<b>Sub-redes (<math>2^n</math>)</b>	<b>Hosts (<math>2^n - 2</math>)</b>
1	255.255.128.0	/17	2	32766
2	255.255.192.0	/18	4	16382
3	255.255.224.0	/19	8	8190
4	255.255.240.0	/20	16	4094
5	255.255.248.0	/21	32	2046
6	255.255.252.0	/22	64	1022
7	255.255.254.0	/23	128	510
8	255.255.255.0	/24	256	254
9	255.255.255.128	/25	512	126
10	255.255.255.192	/26	1024	62
11	255.255.255.224	/27	2048	30
12	255.255.255.240	/28	4096	14
13	255.255.255.248	/29	8192	6
14	255.255.255.252	/30	16384	2

Fazendo a mesma análise que realizamos anteriormente para a classe A, para a classe B podemos iniciar com a máscara /17 (um bit emprestado para sub-rede), dividindo a rede em questão em duas sub-redes com 32.766 hosts cada uma, e emprestar até 14 bits para formar uma máscara /30 com 16.384 sub-redes de apenas dois hosts cada uma, utilizadas também para endereçar redes WAN ponto a ponto.

Para a classe C temos um escopo menor de empréstimo, pois ela tem três octetos de rede e apenas um byte de host, por isso temos apenas oito bits para criar sub-redes. Veja a tabela da classe C abaixo.

<b>Classe C (192-223) - Padrão 255.255.255.0 com prefixo /24</b>				
<b>Bits emprestados</b>	<b>Máscara</b>	<b>Prefixo</b>	<b>Sub-redes (<math>2^n</math>)</b>	<b>Hosts (<math>2^n - 2</math>)</b>
1	255.255.255.128	/25	2	126
2	255.255.255.192	/26	4	62
3	255.255.255.224	/27	8	30
4	255.255.255.240	/28	16	14
5	255.255.255.248	/29	32	6
6	255.255.255.252	/30	64	2

Para a classe C podemos iniciar com a máscara /25 (um bit emprestado para sub-rede), dividindo a rede em questão em duas sub-redes com 126 hosts cada uma, e emprestar até 6 bits para formar uma máscara /30 com 64 sub-redes de apenas dois hosts cada uma, utilizadas também para endereçar redes ponto a ponto.

Se você prestar bastante atenção perceberá que os octetos das máscaras, não importando a classe podem ser apenas:

- o 0 → 00000000
- o 128 → 10000000
- o 192 → 11000000
- o 224 → 11110000
- o 240 → 11111000
- o 248 → 11111100
- o 252 → 11111110
- o 254 → 11111111
- o 255 → 11111111

A variação das sub-redes é bem conhecida e apenas nos valores conforme abaixo do último octeto da máscara (último bit 1 marcado na lista de valores de octeto anterior):

- o 255 → 1 em 1 ( $2^0$ )
- o 254 → 2 em 2 ( $2^1$ )
- o 252 → 4 em 4 ( $2^2$ )
- o 248 → 8 em 8 ( $2^3$ )
- o 240 → 16 em 16 ( $2^4$ )
- o 224 → 32 em 32 ( $2^5$ )
- o 192 → 64 em 64 ( $2^6$ )
- o 128 → 128 em 128 ( $2^7$ )

Portanto, se você anotar esses valores antes de iniciar a prova na folha de rascunho também ajudará bastante para agilizar as conversões decimal/binário para encontrar a variação dos bits e resolver questões de sub-rede, VLSM e CIDR.

Maioria dos roteadores Cisco com IOS acima da versão 12 aceitam a máscara /31 para endereçar interfaces WAN ponto a ponto, gerando mais economia de endereços que uma rede /30, assim como a configuração de endereços /32 utilizados para configurar interfaces de loopback nos roteadores, pois as loopbacks não formam redes e sim são endereços lógicos locais dos dispositivos. Veja os exemplos abaixo, onde as saídas referentes a rede /31 estão destacadas em amarelo e da /32 em verde.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip add 192.118.1.1 255.255.255.254
R1(config-if)#int loop 0
R1(config-if)#ip add 192.168.1.1 255.255.255.255
R1(config-if)#
*Jul 16 12:21:30.775: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
R1(config-if)#do sho ip rou
### Saídas omitidas ###

      192.118.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.118.1.0/31 is directly connected, FastEthernet0/0
L       192.118.1.1/32 is directly connected, FastEthernet0/0
          192.168.1.0/32 is subnetted, 1 subnets
C       192.168.1.1 is directly connected, Loopback0
R1(config-if)#

```

As redes /31 no CCENT/CCNA não são exploradas no material oficial por terem alguns problemas em certos tipos de interfaces, por isso nas respostas de questão de prova normalmente redes ponto a ponto utilizam máscaras /30.

### **3.9 Dicas Finais sobre Exercícios de Sub-rede para o CCENT/CCNA**

No CCENT/CCNA ou qualquer outra prova que cobre a divisão de uma rede em sub-redes, você poderá encontrar alguns modelos de questões. Vamos a alguns exemplos comuns.

Dado um IP e máscara perguntar:

- o Qual a sua sub-rede
- o Qual a porção de rede ou de host
- o Qual a faixa de IPs válidos dessa sub-rede
- o Qual o broadcast da sub-rede em questão
- o Etc.

Nesse caso os conceitos estudados anteriormente resolvem o problema. Por exemplo, dado o IP 172.16.33.45 com a máscara 255.255.255.248 vamos obter todas as informações possíveis sobre essa sub-rede.

A primeira coisa a fazer é descobrir a sub-rede com um AND lógico:

$$\begin{array}{r} 172.16.33.45 \\ \text{AND } \underline{255.255.255.248} \\ 172.16.33.? \end{array}$$

obs: lembra-se que no AND qualquer bit com 0 dá 0 e 1 com 1 dá 1.

$$\begin{array}{r} 45 = 00101101 \\ \text{AND } 248 = \underline{11111000} \\ 00101000 = 40 \end{array}$$

Portanto sub-rede 172.16.33.40

Para achar a faixa de IPs é só descobrir a próxima sub-rede, analisando a máscara sabemos que a variação será de 8 em 8, portanto a próxima sub-rede será a 172.16.33.48. Com essa informação sabemos que:

- o A faixa total de IPs será de 172.16.33.40 a 172.16.33.47.
- o Os IPs válidos serão de 172.16.33.41 a 172.16.33.46.
- o O broadcast será o 172.16.33.47.

Um "macete" muito útil para quando você tem uma rede de qualquer classe com uma máscara maior que /24 (255.255.255.xxx) e precisa identificar em uma lista de IPs quem é endereço de rede, IPs válidos ou broadcast é o seguinte:

1. Primeiro com a máscara de sub-rede encontre a variação (valor em decimal do último bit 1 da máscara de sub-rede).
2. Com esse valor divida o último octeto do IP dado no exercício pela variação, os que resultarem em zero na divisão, ou seja, forem múltiplos da variação são endereços de sub-rede.
3. Se você somar 1 e dividir pela variação e resultar em zero, ou seja, der múltiplo da variação é um broadcast.
4. Os demais são endereços válidos.

Outro modelo de questão são os de projeto, onde dado um número de hosts ou de sub-redes você terá que achar qual a máscara que melhor se adapta ao projeto. Nesse caso existem dois tipos de análise para resolução:

1. Quando o projeto é pelo **número de sub-redes** você deve pensar em **quantos bits "emprestar"**, ou seja, quantos bits zero da máscara original você terá que transformar em bits 1 para fazer a sub-rede. Aqui tome cuidado com que fórmula utilizar, pois como já estudamos temos duas abordagens, com ou sem a subnet zero.
2. Quando o projeto é pelo **número de hosts** ou computadores que você terá na rede pense em **quantos bits zero você terá que deixar na máscara** de sub-rede. Aqui a fórmula não muda, sempre será  $2^n-2$ , onde o n são os bits zero que você terá na máscara para representar os hosts.

Para resolver esse problema basta utilizar a tabela de potências de 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

Por exemplo, o exercício fornece um IP de classe A e quer que você o divida em 30 sub-redes. Basta você procurar na tabela o que se encaixa com o 30 e a potência de 2 desse número será o número de bits que você terá que emprestar. Nesse exemplo o melhor é o  $2^5$  que dá 32, portanto vamos emprestar 5 bits. A máscara de sub-rede será 255.248.0.0, lembre que a máscara padrão da classe A é 255.0.0.0.

Cuidado nos exercícios que envolvem sub-redes para certificar **se você deve ou não desconsiderar a sub-rede zero e a broadcast**. Se não falar nada valem todas as sub-redes.

Agora vamos relembrar o projeto a partir dos hosts. Por exemplo, você tem um IP de classe C, máscara padrão 255.255.255.0, e precisa ter 12 hosts por sub-rede. Agora a fórmula é  $2^n-2$ , onde o n são os bits zero.

Quanto bit zero precisará deixar na máscara? Analisando a tabelinha são 4, pois  $2^4-2=14$ , cabem os 12 micros e temos uma sobra de 2. Portanto a máscara será 255.255.255.240 (11111111.11111111.11111111.11110000).

Estude bem esses conceitos, tire dúvidas antes de prosseguir se necessário e no final não se esqueça de fazer as listas de exercícios extras de sub-rede que estão disponíveis na área do aluno. Os gabaritos estão comentados para que vocês possam entender melhor os modelos de questão possíveis e como resolvê-los.

Veja também na área do aluno a “**Folha de rascunho para cálculo de Sub-redes**”, documento em PDF com um “**resumão**” para facilitar na hora das contas relacionadas ao IP. Uma boa dica é decorar o que está sugerido nessa folha de rascunho para anotar no quadro de anotações dado pelas entidades certificadoras da Pearson VUE antes de iniciar a prova do CCENT/CCNA, isso irá acelerar e facilitar os cálculos de IP e sub-rede.

Nas vídeo-aulas ensinaremos a utilizar a folha de rascunho!

Esse capítulo é muito importante para o CCENT/CCNA e será cobrado isoladamente e em conjunto com outras questões, por exemplo, você terá que calcular uma sub-rede para determinar que IP configurar em uma interface de um roteador, por isso pratique bastante!

#### 4 VLSM (Variable Length Subnet Masks)

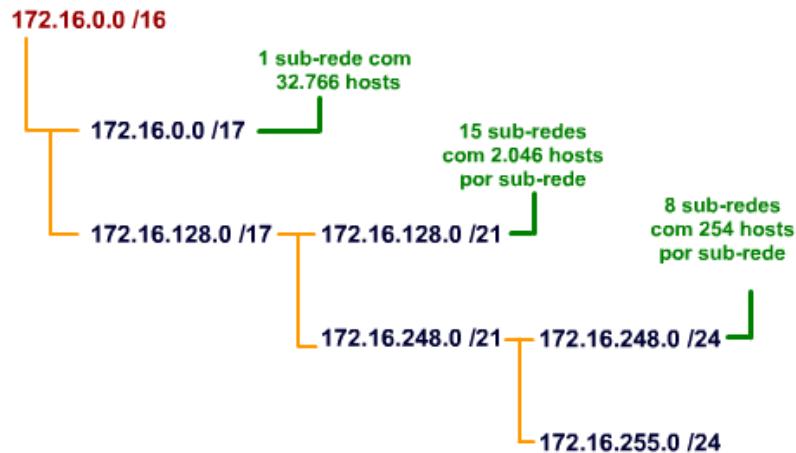
As sub-redes de tamanhos diferentes (**VLSM - Variable Length Subnet Masks**) podem existir em uma rede IP baseada em classe para melhorar ainda mais a alocação dos endereços IP.

Esta forma de subdivisão é bastante aplicável no mundo real, onde o ambiente de rede das organizações contêm diferentes números de hosts por rede, pois cada departamento tem uma necessidade específica de elementos de rede. Logo, sub-redes com tamanhos diferentes são necessárias para minimizar o desperdício de endereços IPs.

Podemos chamar essa técnica de sub-rede da sub-rede, pois o VLSM quebra sub-redes em tamanhos menores. Nesse modelo vamos dividir os endereços IP em rede, sub-rede, sub-rede da sub-rede e assim por diante, dependendo do número de níveis hierárquicos que desejarmos.

Originalmente o uso de sub-redes era destinado à subdivisão de uma rede baseada em classes em uma série de sub-redes de **mesmo tamanho**, onde a mesma máscara de sub-rede era compartilhada por todos os segmentos. Por exemplo, a subdivisão de 4-bits de hosts de uma rede classe B produzirá 16 sub-redes do mesmo tamanho, cada uma com 4094 endereços IP. Mas se um departamento necessitar de apenas 30 endereços IP? Será que esse desperdício de endereçamento pode ser suportado pela organização?

Assim, com o VLSM um administrador pode criar sub-redes de tamanho variável e que supram as necessidades de cada departamento de sua organização. Um exemplo de subdivisão com máscara de tamanho variável da rede 172.16.0.0/16 e exibida na animação (ver matéria online na área do aluno).



Vamos entender a divisão realizada. Tudo começou pegando a rede classe B privativa (RFC 1918) 172.16.0.0/16, depois o administrador quebrou ela em duas sub-redes com uma máscara /17 (emprestando um bit), com isso temos uma sub-rede disponibilizada para endereçar mais de 32 mil hosts e outra que será novamente quebrada em sub-redes.

A segunda sub-rede /17 foi quebrada com a máscara /21, resultando em 16 sub-redes, pois  $21-17=3$  e temos 3 bits de sub-rede. Desses 16 sub-redes, 15 foram reservadas para segmentos com 2.046 hosts e a última será novamente subdividida.

Para a última sub-rede 172.16.248.0/21 o administrador quebrou utilizando máscaras /24, portanto temos também 3 bits de sub-rede ( $24-21=3$ ), gerando 8 sub-redes /24 com 254 hosts por sub-rede.

Essa subdivisão poderia continuar, por exemplo, poderíamos pegar a sub-rede 172.16.255.0 e quebrá-la em sub-redes /30, criando 64 sub-redes para endereçamento de links ponto a ponto.

Uma dica importante é que na prática costuma-se fazer a divisão das redes com maior número de endereços para a menor, assim você consegue aproveitar melhor a faixa de endereços disponíveis com a rede escolhida para VLSM.

Vamos reforçar o uso da máscara de sub-rede /30 (255.255.255.252) utilizada principalmente para endereçamento de interfaces serias ponto a ponto, pois elas fornecem apenas 2 endereços IP válidos, o suficiente para uma interface serial ponto a ponto, veja figura a seguir.

**Com a máscara /30 apenas dois endereços de host são disponíveis.**

**A sub-rede será 201.100.20.4/30 e os endereços de host disponíveis serão .5 e .6.**



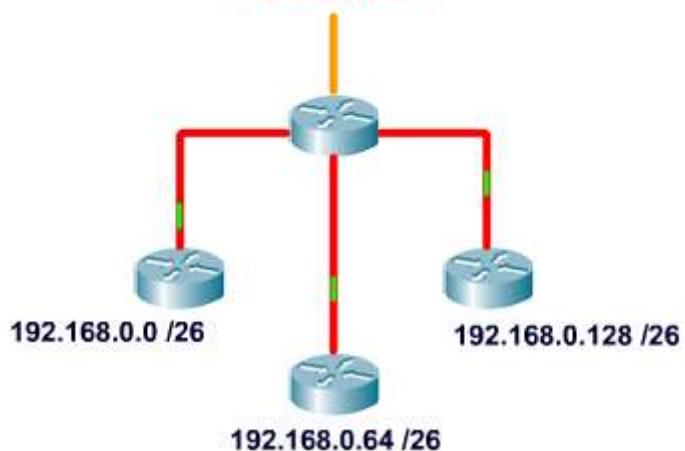
Outra vantagem que um projeto com VLSM proporciona é a possibilidade de **hierarquização** da rede e **agregação de rotas** (route summarization ou route aggregation). Por exemplo, suponha que abaixo de um roteador você tenha as sub-redes 192.168.0.0/26, 192.168.0.64/26 e 192.168.0.128/26. Você terá que anunciar três rotas para o roteador vizinho, porém você pode agrregar essas rotas e representá-las como 192.168.0.0/24, veja figura abaixo.

**Eu conheço as rotas para as redes:**

192.168.0.0 /26  
192.168.0.64 /26  
192.168.0.128 /26

**E posso anunciar-las somente como:**

192.168.0.0 /24



Dentro da rede 192.168.0.0/24 não estão contidos todos os endereços IP das três redes apresentadas? Faça essa conta e confirme.

A única restrição do uso do VLSM é com relação aos **protocolos de roteamento**, pois alguns protocolos como RIP versão 1 e IGRP não suportam esse tipo de endereçamento, porém o RIP versão 2, EIGRP, OSPFv2, IS-IS e BGP suportam tanto o VLSM como o CIDR.

Para que os protocolos de roteamento para suportem o VLSM e CIDR precisam enviar a **máscara de sub-rede** dentro de seus anúncios (updates), sendo que o RIP-v1 e o IGRP não enviam essas informações quando trocam tabelas de roteamento, eles enviam apenas o prefixo ou rede, sem anunciar a máscara ou tamanho do prefixo.

Já o RIP-v2, EIGRP, OSPFv2, IS-IS e BGP enviam tanto o prefixo de rede (endereço de rede ou sub-rede) como o comprimento do prefixo (máscara) em seus anúncios de roteamento, por isso conseguem trocar informações em topologias de rede baseadas em classe, com sub-rede, VLSM ou CIDR, pois o roteador vizinho vai receber a informação precisa sobre a rede e máscara no anúncio de roteamento.

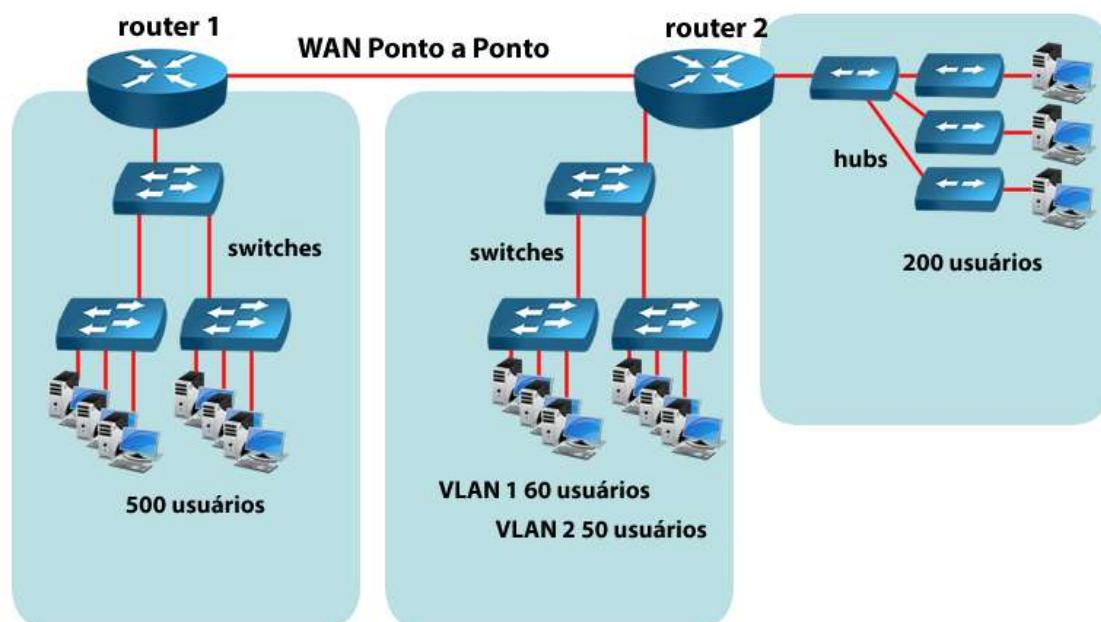
#### 4.1 Como Resolver Exercícios com VLSM

Os exercícios de VLSM nada mais são que vários exercícios de sub-rede em apenas uma questão, pois vamos precisar quebrar as sub-redes em outras menores quantas vezes for necessária, conforme necessidade de cada cenário de rede das questões de prova.

Podemos encontrar questões de projeto ou análise de endereçamento, assim como estudamos para as questões de sub-rede puras.

O cuidado maior que temos que ter com os exercícios de VLSM é com o **“overlapping”** ou **sobreposição** de redes, pois essa é uma das “pegadinhas” cobradas em provas não somente da Cisco como de outros fabricantes que trabalham com o assunto.

Vamos entender o overlapping na prática utilizando a topologia abaixo, onde faremos um projeto utilizando VLSM a partir da rede classe A privativa 10.0.0.0/8 utilizando o mínimo de faixas de endereçamento possível.



Analisando a figura chegamos a conclusão que necessitaremos de cinco sub-redes, sendo:

- 500 usuários para LAN do router-1
- 2 endereços para WAN entre router-1 e router-2
- Na rede do router-2:
  - VLAN 1 com 60 usuários
  - VLAN 2 com 50 usuários
  - 200 usuários para a rede legada com Hubs (rede antiga)

Vamos começar descobrindo a máscara para a rede com maior número de hosts: 500. Para isso podemos deixar nove bits zero na máscara, pois  $2^9-2=510$ , o que nos leva a uma máscara /23 (32 bits 1 – 9 bits zero = 23 bits 1 na máscara) ou 255.255.254.0.

Essa máscara em uma classe A nos dá um total de 23 bits menos 8 da padrão, ou seja, emprestamos 15 bits para sub-rede, portanto teremos  $2^{15}$  ou 32.768 sub-redes. Vamos reservar a primeira para a LAN do router-1: 10.0.0.0/23 (broadcast 10.0.1.255 e faixa de IPs válidos de 10.0.0.1 até 10.0.1.254). A próxima sub-rede será a 10.0.2.0/23, pois sub-redes com máscara /23 variam de 2 em 2 (11111111.11111111.11111111.00000000), indo até 10.0.3.255, pois na sequência teremos a 10.0.4.0/23.

Então vamos utilizar a sub-rede 10.0.2.0/23 para quebrá-la no tamanho dos demais segmentos que precisamos iniciando pela de 200 hosts do router-2 (maior para a menor). Para 200 hosts o mais próximo que temos é utilizando oito bits ( $2^8-2=254$ ), portanto deixando oito bits temos uma /24 ou 255.255.255.0:

- LAN de 200 hosts do router-2: 10.0.2.0/24 (broadcast 10.0.2.255 e IPs válidos de 10.0.2.1 até 10.0.2.254)

Para a VLAN 1 com 60 hosts podemos deixar seis bits zero na máscara, pois  $2^6-2=62$  hosts, vamos alocar a próxima sub-rede depois da anterior: 10.0.3.0/26 (32-6 = /26 ou 255.255.255.192 ou 11111111.11111111.11111111.11000000). Essa rede varia de 64 em 64, portanto a próxima sub-rede será a 10.0.3.64, por isso ela tem broadcast 10.0.3.63 e faixa de IPs válidos de 10.0.3.1 a 10.0.3.62.

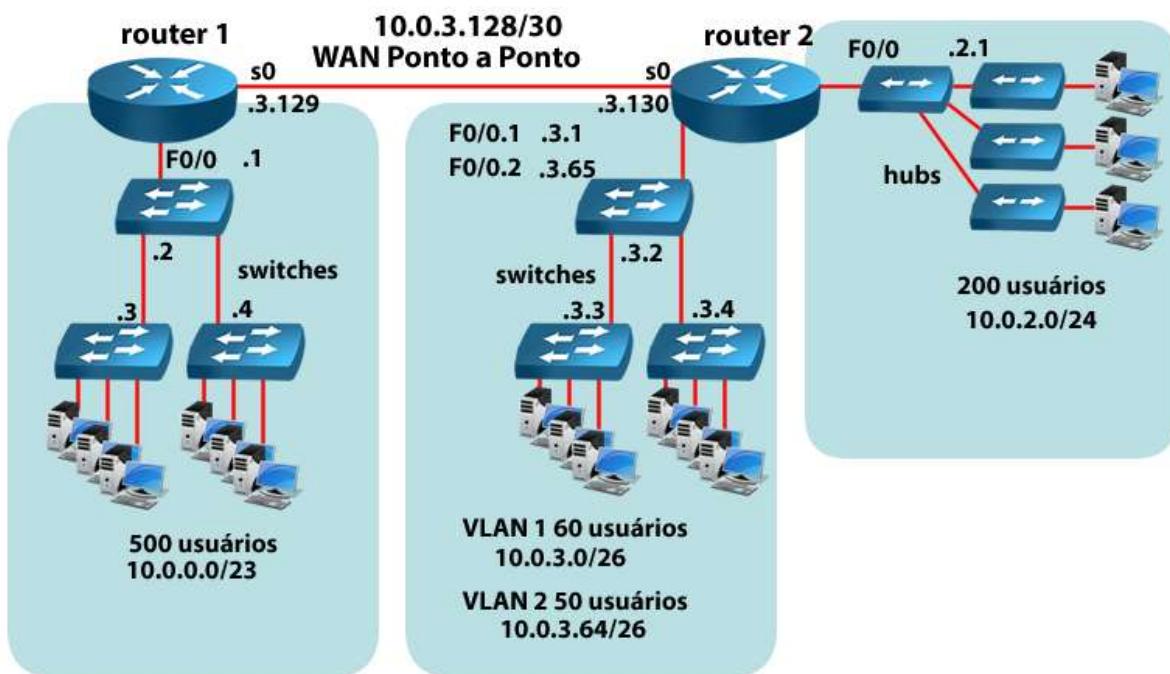
Para a VLAN 2 precisamos de 50 IPs, porém abaixo de seis bits zero, ou seja, com cinco bits conseguimos apenas 30 hosts, por isso precisaremos utilizar mais uma vez uma /26, idem ao cálculo anterior, portanto utilizaremos a sub-rede 10.0.3.64/26, a qual tem o IP 10.0.3.127 como broadcast e a faixa de endereços válidos entre 10.0.3.65 e 10.0.3.126.

Por último vamos alocar a rede WAN entre os roteadores utilizando a próxima sub-rede disponível que é a 10.0.3.128/26, porém como precisamos apenas de 2 hosts válidos vamos utilizar a /30 como esse prefixo 10.0.3.128/30, sendo os IPs válidos o final 129 e 130, com broadcast o 10.0.3.131.

Com isso finalizamos nosso projeto de VLSM sem sobreposição, ou seja, uma rede única em cada segmento. Se utilizássemos, por exemplo, a rede 10.0.3.128/25 em outra sub-rede teríamos uma sobreposição, pois essa sub-rede tem dos IPs 10.0.3.129 até 10.0.3.254, porém os IPs de final 129 e 130 já pertencem à WAN entre router-1 e router-2!

VLSM é como fatiar uma pizza que já está fatiada, por exemplo, temos uma pizza com 4 fatias, você pode fatiá-la novamente e criar uma de 8 fatias, mas se tentar das 4 fatias fazer 3 não dá, pois ela já está cortada, o conceito é o mesmo, você não pode fornecer uma fatia do VLSM que já está sendo utilizado em um segmento de redes para outro, ou então teremos IPs duplicados na rede e isso não é permitido, pois os endereços IP devem ser únicos dentro de um domínio de roteamento!

Veja a seguir a topologia já com os endereços de cada sub-rede e os IPs das interfaces dos roteadores e de gerenciamento dos switches definidos.



Nesse exemplo podemos aprender a questão do overlapping de endereços, como projetar VLSMs e como endereçar os hosts utilizando VLSM, todas são questões que podem ser cobradas no exame CCENT/CCNA em questões unificadas ou separadamente.

Conforme já citamos, a base de tudo é o nosso modelo de cálculo de sub-redes, com ele vocês conseguirem resolver quase a totalidade das questões, pois variações podem aparecer e serem resolvidas com a mesma base, porém em cenários e aplicações práticas diferentes. Na área do aluno disponibilizamos duas listas de exercícios, sendo a primeira com a resolução comentada, é importante que antes da prova de capítulo essas listas sejam realizadas e bem compreendidas!

#### 4.2 Outra Visão sobre VLSM

Outra maneira de visualizar as VLSMs é através dos vários níveis que são divididos os endereços de sub-rede, pois se lembre de que temos nesse tipo de cenário nada mais que a sub-rede de uma sub-rede, ou seja, vamos emprestar bits para formar máscaras e depois fazer um segundo ou até terceiro empréstimo para criar subníveis de endereços.

Veja o exemplo abaixo para uma VLSM gerada com classe B, onde temos a máscara padrão /16:

- **/16** – **11111111.11111111.00000000.00000000** → máscara padrão com 1 rede e 65534 hosts.
- **/20** – **11111111.11111111.11110000.00000000** → emprestando 4 bits temos 16 subredes com 4094 hosts cada uma. Sobram ainda 12 bits zero na máscara para criarmos outras sub-redes via VLSM.
- **/27** – **11111111.11111111.11111111.11100000** → utilizando a /27 emprestamos 7 bits da primeira máscara de VLSM e temos mais 128 sub-redes criadas a partir das sub-redes anteriores com 30 hosts.

Podemos emprestar mais bits de uma das /27 e criar sub-redes menores, por exemplo, emprestando 3 bits para criar 8 sub-redes /30 e endereçar oito circuitos ponto a ponto, conforme mostrado abaixo e destacado em cinza.

- /30 – 11111111.11111111.11111111.11111100

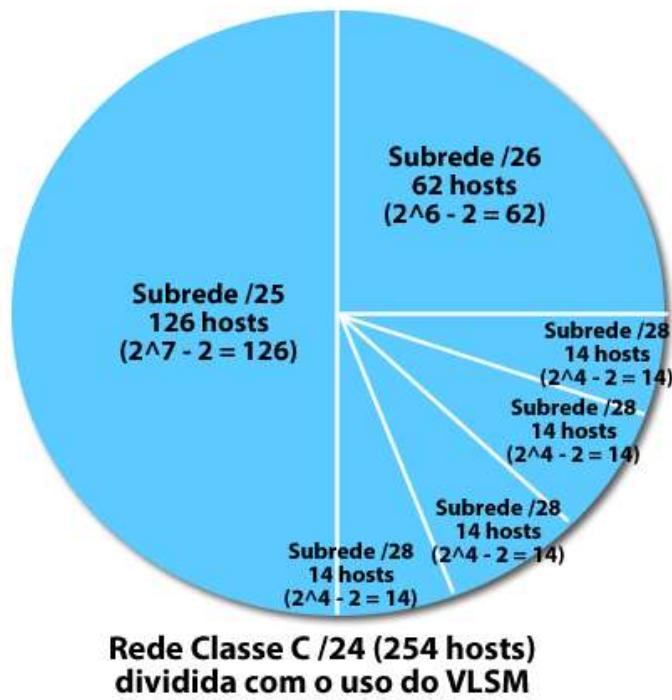
Essa segmentação em pedaços cada vez menores auxilia a criar hierarquias ou tamanhos diferentes de sub-redes e melhora a alocação de IPs em uma rede.

#### 4.3 Considerações finais sobre VLSM

Em uma prova, seja do CCENT, CCNA ou qualquer outro exame, o VLSM pode ser cobrado em forma de projeto, sendo que você terá que escolher uma máscara adequada ou uma rede IP, ou ainda para que você escolha IPs que devem ser configurados nas Interfaces.

Deve-se tomar cuidado com a sobreposição de IPs (overlapping), pois como você deve ter notado nos exemplos práticos é muito fácil nos enganarmos e escolhermos uma faixa de IPs que já está sendo usada por outra sub-rede.

Por exemplo, se você divide uma rede com uma máscara /25 (255.255.255.128) a primeira sub-rede pega os IPs de x.x.x.0 até x.x.x.127 e a segunda vai de x.x.x.128 até x.x.x.255. Se você utilizou a rede x.x.x.0 /25 e utilizar a x.x.x.64 /28 para endereçar outro roteador você estará cometendo o erro de sobreposição, que nada mais é que a duplicação de IPs, pois a rede x.x.x.64 /28 vai dos IPs x.x.x.64 até x.x.x.79, os quais já estão contidos na faixa do x.x.x.0 /25, por isso a faixa disponível após a x.x.x.0 /25 é a x.x.x.128 /25. Veja a figura ao lado com uma representação gráfica em forma de pizza da divisão em sub-redes utilizando VLSM para uma classe C.



Note que a cada sub-rede que criamos com o VLSM perdemos dois IPs válidos, pois um deles será utilizado como endereço de rede e o último como broadcast direcionado daquela sub-rede. Ou seja, início com a classe C tínhamos 256 IPs com 254 válidos, com a divisão dessa classe C em uma /25, mais uma /26 e quatro /28 temos um total de 244 IPs válidos, ou seja, uma perda de 10 IPs que eram válidos e passaram a ser sub-rede e broadcast.

Essas perdas de IPs serão maiores quanto mais máscaras de sub-rede forem utilizadas, porém mesmo assim essa divisão acaba sendo utilizada na prática.

## 5 Roteamento Classless – CIDR

Aproveitando o conceito de máscara de sub-rede com comprimento variável, vamos estudar também **Classless Interdomain Routing**.

O CIDR (**Classless Inter-Domain Routing**) foi introduzido em 1993 como um refinamento para a forma como o tráfego era conduzido pelas redes IP. Permitindo flexibilidade acrescida quando dividindo margens de endereços IP em redes separadas, promoveu assim um uso mais eficiente para os endereços IP cada vez mais escassos. O CIDR está definido no **RFC 1519**.

O CIDR usa máscaras de comprimento variável, o VLSM (de Variable Length Subnet Masks), para alocar endereços IP em sub-redes de acordo com as necessidades individuais e não nas regras de uso generalizado em toda a rede a partir de classes pré-definidas. Assim a divisão de rede/host pode ocorrer em qualquer fronteira de bits no endereço. Porque as distinções de classes normais são ignoradas, o novo sistema foi chamado de **roteamento sem classes** ou **classless**. Isto levou a que o sistema original passasse a ser chamado de roteamento de classes ou classful.

Basicamente com o CIDR **deixamos de utilizar as classes** e passamos a utilizar um prefixo para identificar as redes e um comprimento de prefixo para definir a faixa de IPs contidas nessas redes, sem levar em consideração as classes.

Por exemplo, um provedor que tem as redes IP classe C 200.200.0.0 até 200.200.255.0 poderá representar com o CIDR apenas o bloco ou prefixo **200.200.0.0** com o comprimento **/16** (16 bits de rede ou 255.255.0.0). Isso possibilita o anúncio de apenas uma rede que representa um bloco de 256 redes classe C, princípio básico de uso da sumarização!

Vamos analisar a faixa de IPs do bloco CIDR do exemplo acima 200.200.0.0/16. Uma máscara /16 é 255.255.0.0, portanto os hosts estão no terceiro e quarto bytes do endereço IP, temos a seguinte faixa de endereços:

- Rede 200.200.0.0 /16
- Broadcast 200.200.255.255
- IPs válidos: 200.200.0.1 até 200.200.255.254

Note que a análise de IPs ou cálculos referentes a redes classless podem ser realizados com o que aprendemos para sub-redes e VLSM, por isso que frisamos ao longo do capítulo que aprendendo sub-redes com nosso método você já aprende “de quebra” VLSM e CIDR!

Devido à possibilidade de termos comprimentos de prefixo menores que a máscara padrão das classes essa tecnologia se chama CIDR, ou Domínio de Roteamento sem Classes de IP.

A principal vantagem do uso do CIDR na Internet é reduzir o tamanho das tabelas de roteamento trocadas entre roteadores, promovendo uma agregação das rotas. Além disso, essa tecnologia permitiu que endereços IP sem uso tanto classe A como classe B utilizados por grandes corporações no início da Internet fossem reutilizados, prolongando mais a vida útil do IPv4. Se não fossem recursos como VLSM, CIDR, endereçamento privativo e traduções (NAT, PAT e Proxy) os endereços IPv4 de Internet já teriam se esgotado a muito mais tempo.

## 5.1 Exemplo de Cálculo de IPs com CIDR

Nesse exemplo vamos considerar a rede 192.168.0.0 /24, a qual tem em si os 256 endereços IPv4 de 192.168.0.0 até 192.168.0.255 inclusive, com 192.168.0.255 sendo o endereço de broadcast para a rede. Esta é a maneira classful de enxergar uma rede classe C.

Agora vamos pegar o bloco CIDR com prefixo 192.168.0.0/22. Ele representa 1024 endereços IPv4 de 192.168.0.0 até 192.168.3.255 inclusive, com 192.168.3.255 sendo o endereço de broadcast para esse bloco de endereços.

Vamos analisar outro exemplo de CIDR onde você deve calcular qual faixa de IPs que pode ser utilizado como hosts válidos dado o bloco 114.64.4.0/22.

Para iniciar o cálculo vamos descobrir que máscara é a /22 e o ultimo bit da máscara para verificar a variação das sub-redes:

- /22 em binário: 11111111.11111111.11111100.00000000 ou 255.255.252.0
- A variação será de 4 em 4 no terceiro octeto
- O primeiro IP válido do range é um depois da rede: 114.64.4.1

Basta agora descobrir qual sub-rede que após a 114.64.4.0, pois um IP antes da sub-rede subsequente será o broadcast da rede e um antes do broadcast será o último IP válido. Com a variação acima as sub-redes serão: 114.64.0.0, **114.64.4.0**, **114.64.8.0**, 114.64.12.0, etc. Portanto o range de IPs será:

- 114.64.4.0 – rede
- 114.64.4.1 – primeiro IP válido
- 114.64.7.254 – último IP válido
- 114.64.7.255 – endereço de broadcast

O exemplo anterior é bastante interessante, pois possui uma variação atípica e considerada difícil, pois varia no terceiro octeto, vamos analisar agora como ocorre a sequência da rede 114.64.4.0 até a 114.64.8.0.

- Os IP's irão variar de 144.64.4.1, 144.64.4.2 ... até 144.64.4.254, 144.64.4.255, quando o quarto octeto chega em 255 somamos 1 no terceiro octeto e voltamos a contagem do quarto para zero, resultando em 144.64.5.0.
- Continuando 144.64.5.1, 144.64.5.2, 144.64.5.3 ... até 144.64.5.254, 144.64.5.255
- Agora somamos mais um no terceiro octeto indo para 144.64.6.0.
- Continuando 144.64.6.1, 144.64.6.2, 144.64.6.3 ... até 144.64.6.255, 144.64.7.0, 144.64.7.1, 144.64.7.2 ... até 144.64.7.254 e finalmente 144.64.7.255.
- Agora ao somar 1 no terceiro octeto passamos para a próxima sub-rede 144.64.8.0.

Mais um fato interessante é que nesse caso IPs com final zero e 255 são IPs válidos por causa da máscara de sub-rede, por exemplo: 144.64.7.0, 144.64.6.255, 144.64.6.0, 144.64.5.255, 144.64.5.0 e 144.64.4.255, podem ser configurados em Hosts.

Cuidado, pois essa pode ser uma “**pegadinha**” na prova, pois são as máscaras desse tipo que diferenciam os que dominam a “**arte do IP**”.

## 5.2 Comprimentos de Prefixos CIDR

Diferente do que estudamos para sub-redes e VLSM, no roteamento classless a primeira máscara possível para qualquer octeto é a "/1" ou 128.0.0.0, isso mesmo, podemos ter uma rede com máscara /1 com CIDR.

Aqui valem /1, /2, /3 até a máscara /32 que representa apenas um host. A rede 0.0.0.0/0 continua sendo a Internet, conforme já estudamos anteriormente. Veja exemplo prático abaixo.

```
B#conf t
Enter configuration commands, one per line. End with CNTL/Z.
B(config)#int f0/0
B(config-if)#ip add 10.0.0.1 128.0.0.0
B(config-if)#no shut
B(config-if)#do sho ip rou
### Saídas omitidas ###

      170.1.0.0/22 is subnetted, 1 subnets
S          170.1.4.0 [1/0] via 172.16.1.1
      172.16.0.0/30 is subnetted, 1 subnets
C          172.16.1.0 is directly connected, Serial0/0
C          0.0.0.0/1 is directly connected, FastEthernet0/0
```

Note que a rede criada com o IP 10.0.0.1/1 aparece na tabela de roteamento como 0.0.0.0/1.

## 6 Sumarização de Rotas

Outro benefício do CIDR e VLSM, vistos anteriormente, é a possibilidade de agregação de prefixos de roteamento ou simplesmente "**agregação de rotas**".

Por exemplo, 16 redes /24 contíguas podem agora ser agregadas, e mostradas como sendo uma única rota de máscara de sub-rede ou prefixo /20 (caso os primeiros 20 bits dos endereços de rede coincidam). Duas /20 contíguas podem ser agregadas em um prefixo /19, e assim por diante.

Isto permite uma redução significativa do número de rotas anunciadas pelas operadoras e provedores de Internet, prevenindo que haja a "**explosão da tabela de roteamento**". Com tabelas de roteamento muito grandes a necessidade de CPU e memória dos roteadores de Internet é bastante alta, consequentemente encarecendo os equipamentos. Atualmente a tabela de roteamento completa da Internet, chamada full-routing, gira em torno de 450 mil rotas já com a agregação sendo realizada (dados de julho de 2013).

Portanto a **agregação** de rotas ou **sumarização** de rotas é descobrir uma máscara de sub-rede que contenha um conjunto de rotas dentro dela para reduzir a quantidade de anúncios entre os roteadores.

Outra definição para agregação ou sumarização de rotas é a de combinar rotas para múltiplas redes em uma supernet ou super-rede (rede com prefixo de valor menor que o padrão da classe, por exemplo, uma classe C com prefixo /20).

Como calcular uma rota sumarizada (rota agregada)? Um dos métodos é comprar as rotas em binário, seguindo os seguintes passos:

1. Anote as redes uma embaixo da outra em ordem crescente;
2. Verifique os octetos iguais nas rotas;
3. Converta os octetos que diferem um do outro para binário;
4. Procure sequência de bits iguais e deixe com bit "1" na nova máscara de sub-rede, onde varia ficará como bit "0";

5. Cuidado com a porção de host da máscara de sub-redes, ela sempre será 0, ou seja, onde tem 0 na máscara original deve ser 0 na nova máscara summarizada.

Na sequência vamos ver esse método sendo calculado passo a passo em um exemplo prático.

### 6.1 Sumarização de Rotas - Exemplo

Veja o exemplo da figura ao lado. Suponha que o roteador 1 está trabalhando com roteamento dinâmico e o administrador de rede quer fazer uma **rota summarizada ou agregada** para anunciar uma única rede para o roteador 2. Vamos seguir o passo a passo da summarização:

**170.1.4.0 /25**  
**170.1.4.128 /25**  
**170.1.5.0 /24**  
**170.1.6.0 /24**  
**170.1.7.0 /24**

Note que os dois primeiros octetos são iguais em todas as redes, e o quarto octeto em algumas irão variar de 0 a 255, pois temos 3 redes /24. Portanto a summarização vai estar no terceiro octeto:

- Rede → 172.1.x.0
- Máscara → 255.255.x.0

#### Vamos converter em binário:

- 170.1.4.0 → 170.1.**000001**00.00000000
- 170.1.4.128 → 170.1.**000001**00.10000000
- 170.1.5.0 → 170.1.**000001**01.00000000
- 170.1.6.0 → 170.1.**000001**10.00000000
- 170.1.7.0 → 170.1.**000001**11.00000000

Note que temos fixo até o 22º bit, portanto a rede summarizada será 170.1.4.0/22 ou 255.255.252.0. Se você for verificar nessa rota summarizada os IPs permitidos, como se fosse uma sub-rede, notará que todos os IPs contidos nessas sub-redes estão representados:

#### Rede

**170.16.4.0**

#### Primeiro IP

**170.16.4.1**

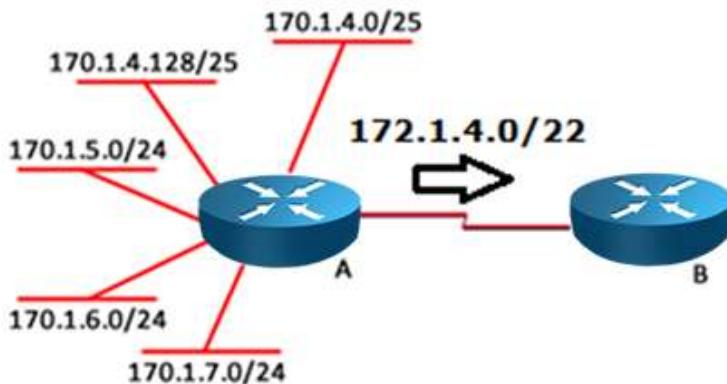
#### Último IP (um a menos que o broadcast)

**170.16.00000111.11111110 ou 170.16.7.254**

#### Broadcast (todos os IP's de host em 1)

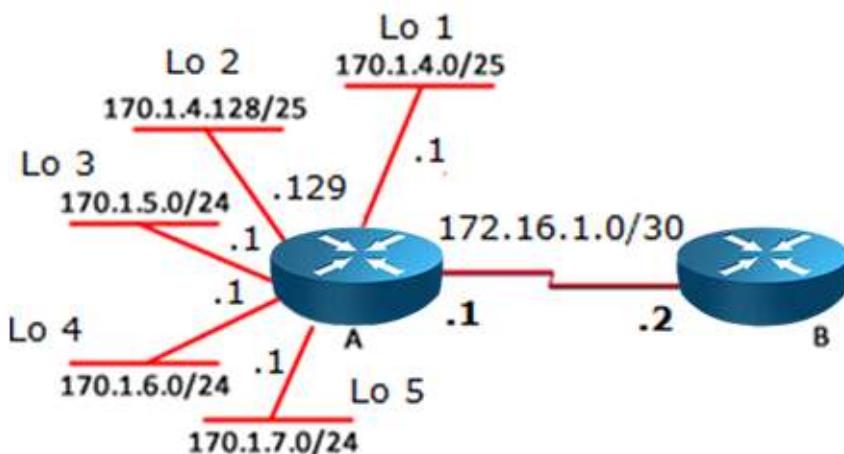
**170.16.00000111.11111111 ou 170.16.7.255**

Veja a topologia abaixo representando o roteador A anunciando apenas uma rota summarizada para o roteador B. Na tabela de B ao invés de termos as 5 rotas teremos apenas uma entrada para a rede 170.1.4.0/22, a qual representa todos os IPs das redes que estão abaixo do roteador A.



## 6.2 Exemplo de Sumarização na Prática

Vamos implementar na prática utilizando simulador ou equipamentos reais, conforme sua disponibilidade. Inicie conectando os dois roteadores A e B via cabo serial e utilize a rede 172.16.1.0/30, com o IP ".1" no roteador A e ".2" no roteador B, conforme topologia abaixo.



Após a configuração realize teste de ping entre as séries de A e B. Não esqueça que uma das pontas do link serial dever ser configurada como DCE e ter o comando “**clock rate**” definindo a taxa de bit em sua configuração.

Na sequência vamos configurar cinco interfaces loopback no roteador A com endereçamento conforme a topologia:

- Loopback 1 → 170.1.4.1 /25
- Loopback 2 → 170.1.4.129 /25
- Loopback 3 → 170.1.5.1 /24
- Loopback 4 → 170.1.6.1 /24
- Loopback 5 → 170.1.7.1 /24

Para configurar uma interface loopback basta entrar em modo de configuração global e digitar "loopback" e o número da interface, a configuração do IP é o mesmo padrão já estudado para as interfaces físicas. A diferença é que a loopback não necessita do comando "no shut", pois ela já fica UP/UP quando criamos a interface.

Depois de criar as interfaces utilize o "show ip route" para verificar a tabela de roteamento.

Nesse ponto somente os IPs da WAN entre os roteadores A e B estão acessível via ping entre eles, tente a partir de B pingar as interfaces loopback de A.

Agora vamos configurar a rota summarizada através de roteamento estático em B para que ele tenha acesso a todas as sub-redes de A. Entre com o comando em B:

- B(config)#ip route 170.1.4.0 255.255.252.0 172.16.1.1

Realize mais uma vez os testes de ping e verifique que com a rota estática summarizada há comunicação, provando que a summarização realmente funciona e não precisamos ter rota para cada sub-rede específica para haver comunicação entre dois pontos.

Abaixo seguem os passos de configuração e testes sugeridos nessa implementação, caso você não tenha tido sucesso nos seus testes pode verificar o problema e corrigir com base nas saídas a seguir. Conectamos o cabo DCE no roteador A, sendo que as seriais estão com a numeração s0/0 em ambas as pontas.

#### **Configurando a interface serial de B:**

```
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#hostname B
B(config)#int s0/0
B(config-if)#ip add 172.16.1.2 255.255.255.252
B(config-if)#no shut
```

#### **Configurando a interface serial de A e realizando teste de ping:**

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#hostname A
A(config)#int s0/0
A(config-if)#ip add 172.16.1.1 255.255.255.252
A(config-if)#clock rate 64000
A(config-if)#no shut
A(config-if)#
*Mar 1 00:01:34.927: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
A(config-if)#
*Mar 1 00:01:35.931: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up
A(config-if)#do ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/11/20 ms
A(config-if)#

```

#### **Configurando as loopbacks de A:**

```
A(config)#interface Loopback 1
A(config-if)#ip add 170.1.4.1 255.255.255.128
A(config-if)#interface Loopback 2
```

```
A(config-if)# ip add 170.1.4.129 255.255.255.128
A(config-if)#interface Loopback 3
A(config-if)# ip add 170.1.5.1 255.255.255.0
A(config-if)#interface Loopback 4
A(config-if)# ip add 170.1.6.1 255.255.255.0
A(config-if)#interface Loopback 5
A(config-if)# ip add 170.1.7.1 255.255.255.0
A(config-if)#
*Mar 1 00:05:38.339: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
*Mar 1 00:05:38.563: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2,
changed state to up
*Mar 1 00:05:38.743: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback3,
changed state to up
*Mar 1 00:05:38.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4,
changed state to up
*Mar 1 00:05:38.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5,
changed state to up
A(config-if)#do sho ip rou
### Saída omitida ###

170.1.0.0/16 is variably subnetted, 5 subnets, 2 masks
C     170.1.4.128/25 is directly connected, Loopback2
C     170.1.7.0/24 is directly connected, Loopback5
C     170.1.6.0/24 is directly connected, Loopback4
C     170.1.5.0/24 is directly connected, Loopback3
C     170.1.4.0/25 is directly connected, Loopback1
    172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/0
A(config-if)#

```

**Configurando e testando a rota estática summarizada em B:**

```
B#ping 170.1.4.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 170.1.4.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
B#ping 170.1.4.129

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 170.1.4.129, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
B#ping 170.1.5.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 170.1.5.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
B#ping 170.1.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 170.1.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
B#ping 170.1.7.1

Type escape sequence to abort.
```

```

Sending 5, 100-byte ICMP Echos to 170.1.7.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
B#conf t
B(config)#Ip route 170.1.4.0 255.255.252.0 172.16.1.1
B(config)#do ping 170.1.4.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 170.1.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/40 ms
B(config)#do ping 170.1.7.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 170.1.7.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/52 ms
B(config)#

```

Na tabela de roteamento de B temos agora uma rota que representa as cinco rotas contidas nas redes do roteador A:

```

B#sho ip route
### Saída Omitida ###

      170.1.0.0/22 is subnetted, 1 subnets
S         170.1.4.0 [1/0] via 172.16.1.1
      172.16.0.0/30 is subnetted, 1 subnets
C         172.16.1.0 is directly connected, Serial0/0
B#

```

## 7 Projetando Redes e Endereçando Dispositivos

Ao longo dos capítulos 5 e nesse capítulo estudamos diversos exemplos de endereçamento IP utilizando vários tipos de endereçamentos (Classful, Sub-redes, VLSM e CIDR). Na prática projetar o endereçamento IP de uma rede é atribuir redes aos diversos segmentos que compõe a topologia.

Os principais tipos de topologia que você pode encontrar na prática são:

- **Broadcast**: redes LAN compartilhadas, tais como da família Ethernet, onde temos um ou mais domínios de broadcast com diversos hosts compartilhando o meio físico. Nessas redes temos as LANs, representadas por uma interface física e lógica, ou as LANs Virtuais em redes com switches que necessitam de uma sub-rede para cada VLAN criada.
- **NBMA**: redes não-broadcast multiacesso utilizam endereçamento similar a uma rede broadcast, ou seja, uma única sub-rede endereça várias interfaces, porém essas redes são utilizadas em WANs com tecnologias como Frame-relay.
- **Ponto a ponto**: redes tipicamente utilizadas em WANs utilizando links seriais através dos protocolos PPP e HDLC, precisam apenas de dois endereços válidos, um para cada uma das pontas do link serial.

Nesse ponto do curso não vamos estudar as redes NBMA, somente LANs, VLANs e redes WAN ponto a ponto. O projeto de redes é definir as redes e máscaras que serão utilizadas para cada segmento e também definir o endereçamento das interfaces dos roteadores, IPs de gerenciamento de switches e escopo de DHCP para os computadores e servidores.

Para saber quais máscaras utilizaremos na rede precisamos basicamente saber quantos hosts por LAN ou VLAN serão utilizados. Depois para as topologias WAN precisaremos saber quantas conexões teremos para definir as redes /30 que serão necessárias.

Já para definir o endereçamento a ser utilizado nos endpoints e dispositivos de infraestrutura normalmente existem políticas corporativas que regem ou padronizam essa atividade. Veja exemplo de política de endereçamento abaixo:

- **Endereços de interfaces de redes LAN ou subinterfaces de VLANs:** primeiro IP da sub-rede.
- **Endereços de gerenciamento de switches camada-2:** do segundo ao décimo endereço IP.
- **Endereços de Access Points:** décimo primeiro ao décimo quinto IPs.
- **Endereços de Impressoras de rede:** décimo sexto ao vigésimo.
- **Endereços de host:** acima do vigésimo primeiro indo até a faixa necessária por tamanho de sub-rede.

Acima temos uma parte da política de endereçamento para redes LAN e seus dispositivos, podemos ainda ter políticas para o Data Center, saída de Internet, portarias, recepções e assim por diante, tudo conforme o porte da empresa e os tipos de endpoints existentes.

## 8 Resumo do Capítulo

Bem pessoal, chegamos ao final de mais um capítulo!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Aprender a calcular sub-redes.
- Aprender a dividir essas sub-redes em máscaras menores criando VLSMs.
- Aprender a criar rotas que sumarizem várias sub-redes e VLSMs em um único ou poucos anúncios.
- Aprender o conceito e calcular redes baseadas em CIDR.
- Entender os requisitos de projeto lógico de uma rede IP (endereços necessários por tipo de rede e endereçamento de endpoints).

*Nesse capítulo estudaremos os princípios do roteamento dinâmico e seus protocolos, implementando na prática o RIPv2.*

*Aproveite o capítulo e bons estudos!*

## **Capítulo 9 - Roteamento Dinâmico e RIPv2**

### **Objetivos do Capítulo**

Ao final desse capítulo você terá estudado e deverá compreender:

- Visão geral dos protocolos de roteamento dinâmicos.
- Diferenciar protocolos IGP e EGP.
- Saber diferenciar métrica e distância administrativa.
- Entender os conceitos de protocolos vetor de distância e de estado de enlace.
- Conhecer o princípio de funcionamento do protocolo RIP versão 2.
- Saber implementar e manter o RIPv2.
- Realizar testes com ping, telnet e traceroute de maneira estendida.

## Sumário do Capítulo

<b>1 Revisão de Rotas Conectadas e Estáticas</b>	
<b>368</b>	
<b>2 Conceitos de Roteamento Dinâmico</b>	<b>369</b>
<b>2.1 Protocolo de Roteamento versus</b>	
<b>Protocolo Roteado</b>	<b>369</b>
<b>2.2 Funções de um Protocolo de</b>	
<b>Roteamento</b>	<b>369</b>
<b>2.3 IGP versus EGP</b>	<b>371</b>
<b>2.4 Métrica versus Distância Administrativa</b>	
<b>372</b>	
<b>2.5 Algoritmos dos Protocolos IGP</b>	<b>374</b>
<b>2.6 Outras Características dos IGPs</b>	<b>375</b>
<b>3 Funcionamento e Configuração do RIP</b>	
<b>376</b>	
<b>3.1 Comandos para Ativação do RIP</b>	<b>377</b>
<b>3.2 Processo de Convergência do RIP</b>	<b>378</b>
<b>3.3 Atualizações do RIP em Detalhe</b>	<b>380</b>
<b>3.4 Timers do RIP</b>	<b>385</b>
<b>3.5 Balanceamento de Cargas</b>	<b>387</b>
<b>3.6 Anunciando a Rota Padrão pelo RIP</b>	<b>388</b>
<b>3.7 Evitando Loops no RIP – Split Horizon, Route Poisoning e Contagem ao Infinito</b>	<b>390</b>
<b>3.8 Entendendo os Problemas da Sumarização Classful Automática do RIP</b>	<b>391</b>
<b>3.9 Dicas de Troubleshooting do RIP</b>	<b>393</b>
<b>4 Testando a Conectividade com Ping, Traceroute e Telnet</b>	<b>394</b>
<b>4.1 Utilizando o Ping</b>	<b>394</b>
<b>4.1.1 Exemplo Prático de Uso do Ping e Revisão do ARP</b>	<b>394</b>
<b>4.1.2 Opções Avançadas – Alterando o IP de Origem no Ping Estendido</b>	<b>396</b>
<b>4.2 Utilizando o Traceroute</b>	<b>397</b>
<b>4.3 Utilizando o Telnet e SSH</b>	<b>398</b>
<b>4.3.1 Testando Servidores e Serviços com Telnet</b>	<b>400</b>
<b>5 Resumo do Capítulo</b>	<b>401</b>

## 1 Revisão de Rotas Conectadas e Estáticas

Basicamente os roteadores podem aprender caminhos em uma rede IP de quatro maneiras no CCENT/CCNA:

### Interfaces diretamente conectadas:

```
R1(config)#interface fast 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
```

### Rotas Estáticas:

```
R1(config)#ip route rede mask gateway/interface
```

### Roteamento Dinâmico:

```
R1(config)#router rip | eigrp 100 | ospf 1 | is-is 1 | bgp 6500
```

### Gateway padrão:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 gateway/interface
```

As rotas conectadas são criadas automaticamente quando inserimos IP e máscara em uma interface que esteja ativa. A entrada de roteamento será inserida na tabela de roteamento com uma letra "C" na frente. Se nenhuma configuração a mais for realizada o roteador conseguirá rotear apenas através das suas interfaces locais.

Uma opção de roteamento realizada através de rota estática é a configuração de um gateway padrão, pois dessa maneira o roteador fará o encaminhamento dos pacotes das redes conectadas e as demais redes não conhecidas serão encaminhadas para o gateway padrão. Essa configuração é recomendada em redes stub, as quais são redes com apenas uma saída para a Internet ou demais redes da topologia.

Se o roteador possuir várias saídas para a rede corporativa as rotas padrões não são mais recomendadas, aí teremos que utilizar ou o roteamento estático, ensinando ao roteador como sair manualmente para cada rede distante, ou roteamento dinâmico, onde os roteadores trocam informações sobre suas entradas de roteamento para montar dinamicamente a tabela de roteamento para as demais redes da topologia.

Independente da fonte das entradas da tabela de roteamento (dinâmicas ou estáticas) o processo de roteamento será sempre o mesmo, ou seja, se houver entrada explícita na tabela de roteamento o pacote é encaminhado para essa interface, caso não haja e existir gateway padrão configurado, será realizado o encaminhamento do pacote para esse gateway, senão o pacote será descartado.

## 2 Conceitos de Roteamento Dinâmico

Nos capítulos anteriores estudamos o roteamento local (rotas diretamente conectadas) e como rotear entre dois pontos utilizando rotas estáticas. Também aprendemos que as rotas estáticas são bastante **leves** para o roteador, pois quem faz o trabalho de “pensar” e “calcular” as melhores rotas é o administrador de redes, por isso ele são econômicas em termos de uso da memória RAM e CPU.

Mas e se a topologia contiver **50 roteadores** cada um com **10 rotas**, totalizando **500 rotas**, será que o roteamento estático é uma boa opção? Com certeza não, pois o **trabalho manual** para criar novas rotas ou apagar rotas não utilizadas seria tão grande que não compensaria a economia de memória e CPU.

Quando a rede cresce e mais pontos são adicionados é recomendado utilizar um **protocolo de roteamento dinâmico**. Com o roteamento dinâmico o administrador de redes faz uma **configuração inicial**, ensinando apenas as redes que devem participar do processo de roteamento e o resto **o próprio protocolo de roteamento trata** de maneira dinâmica.

Rotas inseridas ou apagadas das configurações com o protocolo de roteamento configurado são automaticamente inseridas ou excluídas nas tabelas de roteamento dos roteadores que estão participando daquele domínio de roteamento sem a intervenção do administrador.

### 2.1 Protocolo de Roteamento versus Protocolo Roteado

Já estudamos no capítulo 5 que os protocolos IP versão 4 ou versão 6 são protocolos roteados ou roteáveis, pois eles por si só não descobrem rotas ou caminhos na rede.

Os protocolos de roteamento tem a função de ler esses protocolos roteados, ou seja, os endereços e redes IP configuradas e descobrir dinamicamente as melhores rotas.

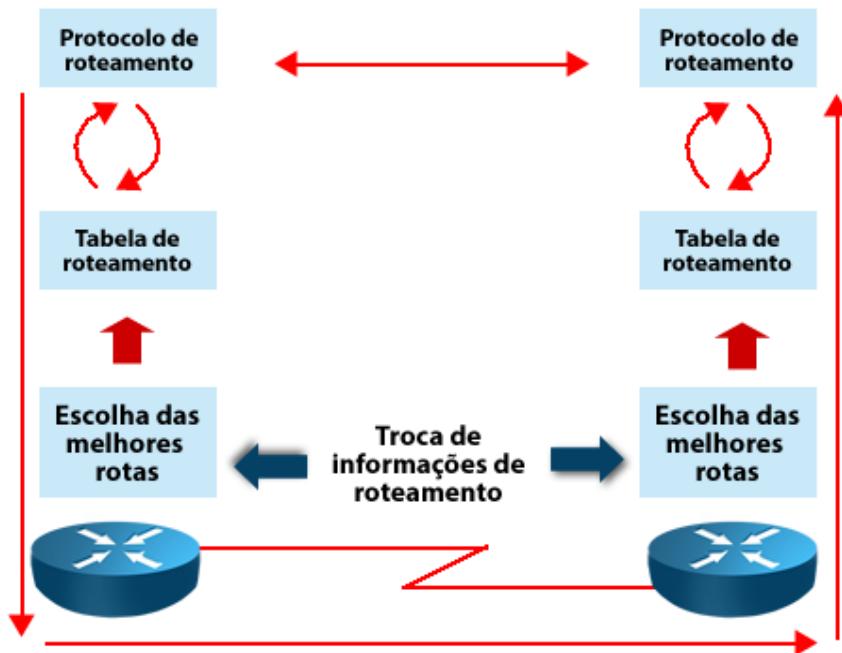
### 2.2 Funções de um Protocolo de Roteamento

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, repassando essas informações aos demais roteadores da rede em momentos oportunos.

Com essas informações trocadas, 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**. Podemos resumir as funções básicas dos protocolos de roteamento em:

- Aprender as informações de roteamento (sub-redes) dos seus vizinhos de rede;
- Ensinar a outros vizinhos sobre suas sub-redes e as demais aprendidas;
- Se mais de um caminho for descoberto utilizar a métrica como critério de desempate e incluir a rota na tabela de roteamento;
- Utilizar mecanismos que para os casos de mudanças na rede essas alterações sejam percebidas em sua própria tabela de roteamento e também sejam repassadas aos vizinhos.

Veja a figura a seguir com uma ilustração das funções básicas de um protocolo de roteamento dinâmico.



Os protocolos de roteamento devem também atuar sobre **alterações na rede** por motivos de:

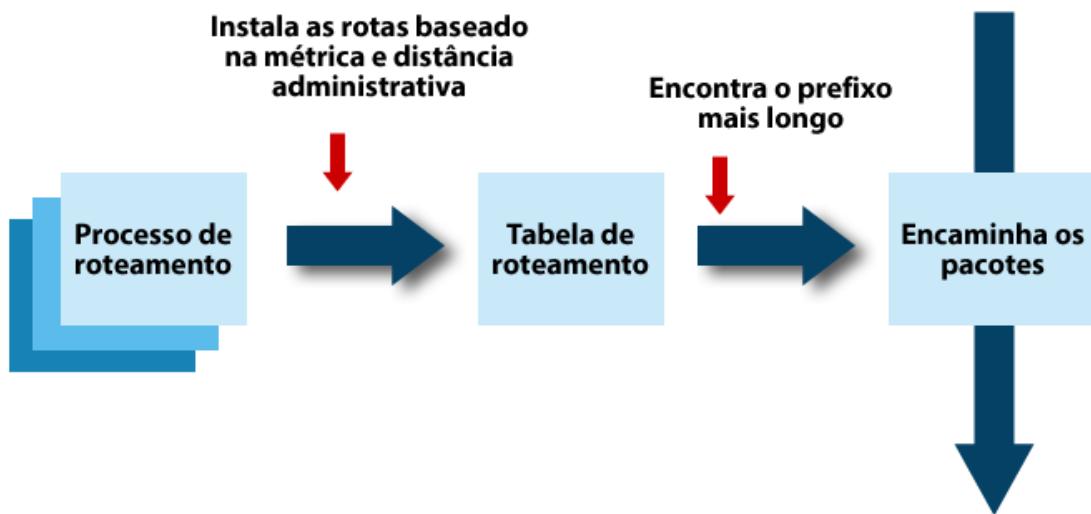
- Problemas, tais como a queda de um link de uma operadora ou um dispositivo que saiu do ar por falta de energia elétrica. Nesses casos a indisponibilidade daquelas redes deve ser refletida para todos os dispositivos.
- Adição de novas redes pelo administrador de redes, pois as redes são dinâmicas e novos pontos podem ser adicionados à topologia atual.
- Exclusão de redes pelo administrador de redes, pois assim como novas filiais podem ser criadas outras podem ser fechadas.

Atualmente na Internet o protocolo de roteamento utilizado é o BGP-4 (Border Gateway Protocol – versão 4).

Já nas Intranets utilizamos o RIP (versões 1 e 2), OSPF ou IS-IS que são protocolos abertos, ou seja, funcionam entre fabricantes diferentes, e existe também o protocolo proprietário da Cisco que é muito famoso chamado EIGRP. Apesar de no início o EIGRP ser um protocolo proprietário, em 2013 a Cisco divulgou seu código, tornando o EIGRP de conhecimento público.

Portanto, temos protocolos para serem utilizados dentro dos sistemas autônomos, chamados de IGP, e também para fazer a comunicação entre os sistemas autônomos, chamados de EGP.

O CCENT aborda roteamento estático e o RIP versão 2, enquanto o ICND-2 e CCNA terão foco no EIGRP, OSPF e ativação básica do BGP. O IS-IS não é mais estudado nas certificações de roteamento e switching Cisco. Para resumir o funcionamento geral dos protocolos de roteamento veja a figura a seguir.



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 com a menor métrica é instalada na tabela de roteamento. Quando temos mais de um protocolo habilitado que vai para a tabela de roteamento é o que possui a menor **Distância Administrativa**, valor padrão utilizado para desempate entre protocolos diferentes (menor é melhor).

Uma vez decidida qual rota a ser utilizada ela é instalada na tabela de roteamento e a decisão sobre para que interface rotear é baseado no prefixo mais longo.

### 2.3 IGP versus EGP

Uma das classificações dos protocolos de roteamento é sobre onde ele é utilizado:

- **IGP – Interior Gateway Protocol:** protocolos utilizados dentro de um domínio de roteamento ou sistema autônomo.
- **EGP – Exterior Gateway Protocol:** protocolos utilizados para comunicação entre diferentes domínios de roteamento ou sistema autônomo.

Essa terminologia vem da Internet, a qual 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).

Portanto, protocolos IGP são usados no interior dos sistemas autônomos e os EGP para conectar essas diversas entidades através da Internet.

O protocolo EGP atualmente utilizado é o BGP-4, todos os demais são IGPs (RIP, EIGRP, IS-IS e OSPFv2).

## 2.4 Métrica versus Distância Administrativa

Os roteadores Cisco suportam diversos protocolos de roteamento simultaneamente, mas como ele decide que informação utilizar?

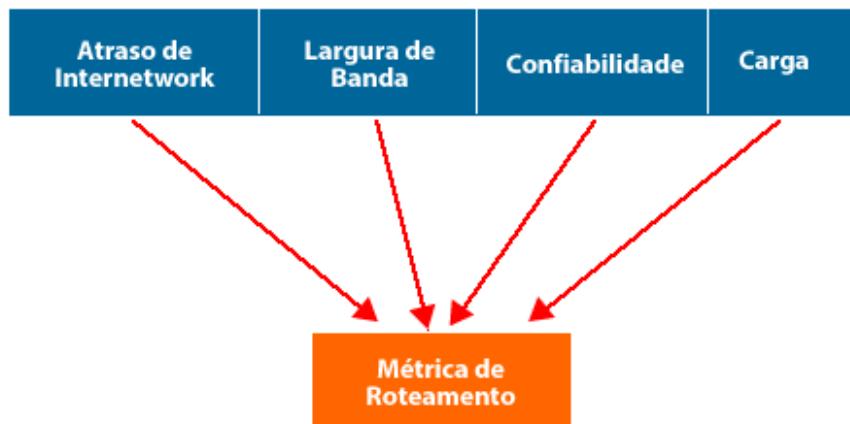
Quando um roteador aprende a informação sobre o caminho até uma rede (rota) através de mais de uma fonte, ou seja, aprendeu rota para uma mesma rede de destino através de mais de um protocolo de roteamento, a **distância administrativa (AD)** ou Administrative Distance é utilizada como fator de escolha da rota que deve ser utilizada para encaminhamento dos pacotes pelo roteador. Nesse caso, o roteador escolhe a rota aprendida pelo protocolo de roteamento com **menor distância administrativa**.

Cada protocolo ou entrada de roteamento possui uma distância administrativa padrão, porém ela pode ser configurada manualmente. Veja a tabela abaixo com as ADs padrões.

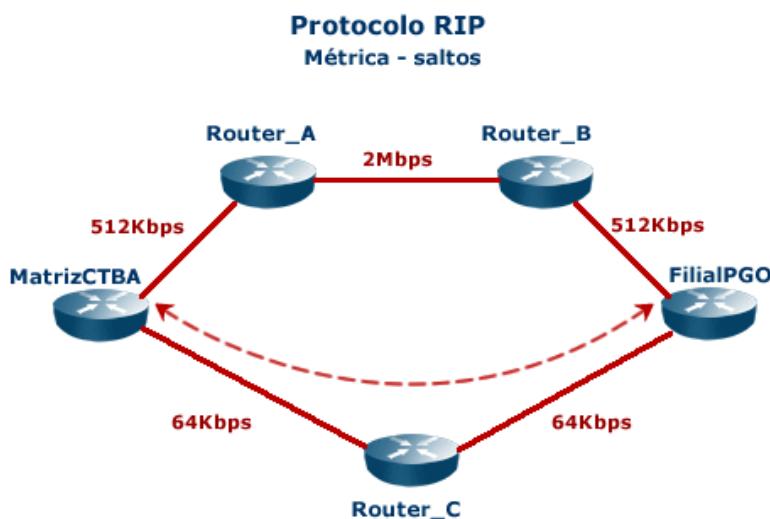
Origem das Rotas	Distância Administrativa
Interface diretamente conectada	0
Rota estática com IP como referência	1
Rota estática com Interface como referência	0
EIGRP – rota sumário	5
External Border Gateway Protocol (BGP)	20
EIGRP interno	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
EIGRP – rota externa	170
BGP interno	200
Desconhecido	255

Para construir a tabela de roteamento, além da distância administrativa temos também o conceito da métrica das rotas que é utilizada quando um mesmo protocolo de roteamento aprende mais de uma entrada para o mesmo caminho. Assim como a AD, a **menor métrica** é a que irá ser inserida na tabela de roteamento.

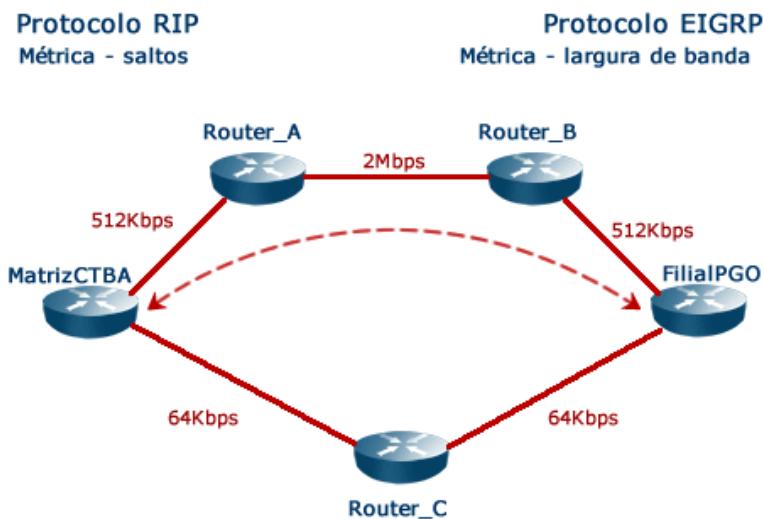
Cada protocolo de roteamento possui um tipo de métrica, por exemplo, no RIP a métrica utilizada é o número de saltos, já protocolos mais avançados como EIGRP e OSPF consideram a velocidade do link em suas métricas. Veja a figura abaixo com exemplos de parâmetros utilizados no seu cálculo.



Vamos a um exemplo de como a métrica pode influenciar na escolha dos caminhos. Considere a rede da figura abaixo, para o roteador "MatrizCTBA" enviar um pacote para o "FilialPGO" ele utilizará o caminho do "Router\_C", pois o protocolo RIP utiliza como métrica o número de saltos (hops).



Agora imagine que você também configurou o protocolo EIGRP nessa mesma rede, conforme mostrado agora na a seguir. Nesse novo cenário o roteador deverá primeiramente escolher qual dos dois protocolos ele utilizará para determinar o melhor caminho, o RIP ou o EIGRP. Nesse caso a escolha será pelo protocolo EIGRP, pois a distância administrativa do EIGRP é **90** enquanto que a do RIP é **120**. O roteador sempre irá escolher o protocolo que possui a menor distância administrativa.



Depois de decidido o protocolo ele deverá escolher o melhor caminho através da métrica. No caso do EIGRP será através do "Router\_A" e "Router\_B". Isso porque o EIGRP leva em consideração a informação de **largura de banda** para o cálculo da melhor métrica e não o número de saltos. O link pelo "Router\_A" e "Router\_B" possui largura de banda de 512Kbps e 2Mbps respectivamente, sendo muito melhor do que um caminho com menos saltos mas onde a largura de banda é de apenas 64Kbps.

Para os protocolos de roteamento que levam em conta a largura de banda do link é importante configurar na interface o parâmetro "**bandwidth**" corretamente, pois em uma interface serial quando o comando não é configurado o roteador assume a banda de **1,5Mbps (T1)** para a interface. Se todas as interfaces possuírem o mesmo "**clock rate**" não há problemas, porém quando a rede não é simétrica haverá métricas que não corresponderão à realidade.

## 2.5 Algoritmos dos Protocolos IGP

Cada protocolo de roteamento funciona segundo um algoritmo que dita como ele deve enviar suas informações, o que está contido nessas informações, quando enviá-las e assim por diante.

Basicamente podemos dividir os IGPs em três categorias:

- **Vetor de distância** (Distance Vector – RIP v1/v2 e IGRP)
- **Estado de enlace** (Link State ou SPF – OSPFv2 e IS-IS)
- **Vetor de Distância Avançado** (Protocolo Híbrido - EIGRP)

Ser um protocolo vetor de distância ou Distance Vector significa que as rotas são anunciadas como vetores com uma distância e direção. A distância é definida em termos de uma métrica, como contagem de saltos para o RIP, e a direção é simplesmente a interface de saída para esses pacotes. Também é conhecido como algoritmo de Bellman-Ford.

Os protocolos de roteamento do vetor de distância pedem que o roteador anuncie periodicamente a tabela de roteamento inteira para cada um de seus vizinhos. As atualizações periódicas são enviadas em intervalos regulares (30 segundos para o RIP e 90 segundos para o IGRP). Mesmo que a topologia não tenha sido alterada, as atualizações periódicas continuarão sendo enviadas a todos os vizinhos indefinidamente.

Os roteadores que usam roteamento do vetor de distância não conhecem a topologia da rede onde estão inseridos, pois eles têm apenas a visão da rede através de seus vizinhos diretamente conectados, as demais redes são vistas por eles através de uma interface de saída

e uma métrica, porém sem conhecimento do caminho que o pacote fará até chegar ao seu destino.

Os protocolos de roteamento link-state também são conhecidos como protocolos de roteamento pelo caminho mais curto e são criados a partir do algoritmo SPF criado por Edsger Dijkstra, por isso pode ser chamado também de algoritmo de Dijkstra.

Os protocolos de roteamento link-state IP mais famosos são o Protocolo OSPF versão 2 (Open Shortest Path First ) e o IS-IS (Intermediate-System-to-Intermediate-System). Os protocolos de estado de enlace não trocam tabela de roteamento e sim mensagens sobre seus enlaces chamadas LSAs (Link State Advertisements).

Os protocolos híbridos ou vetores de distância avançados utilizam características dos vetores de distância e também dos protocolos link-state, por isso o nome híbrido. Como foi construído com mais características de vetores de distância que link-state recebe a designação de vetor de distância avançado. O protocolo que representa essa classe é o EIGRP, o qual é foco do exame ICND-2.

## 2.6 Outras Características dos IGPs

Existem algumas características que foram citadas sobre os protocolos de roteamento e a tabela abaixo resume o mais importante que pode ser cobrado em prova.

Protocolo	Tipo	Classful/ Classless	Métrica	Dist. Admi.	Escalabilidade	Tempo de convergência	Consumo de recurso
RIP v1	Distance Vector	Classful	Saltos	120	15 saltos	Lento	Mem- baixo CPU - baixo BW - alto
RIP v2	Distance Vector	Classless	Saltos	120	15 saltos	Lento	Mem- baixo CPU – baixo BW – alto
IGRP	Distance Vector	Classful	Banda passante, atraso, confiabilidade, carga	100	255 saltos	Rápido	Mem- baixo CPU – baixo BW – alto
EIGRP	Advanced Distance Vector ou Híbrido	Classless	Banda passante, atraso, confiabilidade, carga	90	Milhares de roteadores	Rápido	Mem- médio CPU – baixo BW – baixo
OSPF	Link State	Classless	Custo (depende fabricante)	110	Aprox. 50 roteadores por área	Rápido	Mem- alto CPU – alto BW - baixo

O IS-IS tem as mesmas características do OSPF.

Além disso, o RIP-v1 não suporta summarização e os demais protocolos suportam. Também sobre a forma de envio de updates para os vizinhos, o RIPv1 e IGRP utilizam broadcast, já o EIGRP e OSPF utilizam multicast.

Lembrem que quando na tabela o protocolo é classificado como classful quer dizer que ele não envia a máscara na tabela de roteamento e por isso não suporta VLSM nem CIDR. Os protocolos classless suportam VLSM e CIDR porque enviam a máscara em seus anúncios de roteamento.

Agora vamos estudar o funcionamento e configuração do RIP versão 2.

### 3 Funcionamento e Configuração do RIP

O RIP ou Routing Information Protocol apareceu no mundo dos protocolos de roteamento no BSD versão 4.2 em 1982, sendo formalizado pelo IETF na RFC 1058 publicada em junho de 1988, chamada de RIP versão 1 ou RIPv1.

Ele é um protocolo vetor de distância suportado em maioria dos fabricantes, muito simples e eficaz, por isso é encontrado em campo até os dias de hoje na sua versão 2 (RIP versão 2 ou RIPv2). Sua métrica é a contagem de salto ou "hop count", ou seja, quanto menos saltos até uma rede de destino melhor é a rota para o RIP, simples assim.

Portanto, para o RIP decidir que rota utilizar para uma rede remota não importa banda, atraso, se o link é ruim ou seja o parâmetro que for, para ele só importa salto, tem menos salto é o caminho que ele escolhe para enviar seus pacotes, como já estudamos anteriormente.

Outra coisa importante é que o RIP não conhece a topologia completa da rede, ele somente sabe quem são os vizinhos e acredita nas informações que eles passam, por isso você vai estudar durante esse capítulo várias técnicas para evitar loops de roteamento devido a informações falsas ou atrasos no envio das informações.

Abaixo seguem várias características do RIP e outras que são exclusivas de cada versão, preste bastante atenção que isso pode cair na sua prova de certificação!

Podemos dizer que o RIP versão 1 e 2 possuem alguns pontos em comum, por exemplo:

- Ambos são protocolos de vetor de distância.
- Métrica por saltos e máxima contagem de saltos 15 (16 saltos considerado infinito).
- Enviam uma cópia da tabela de roteamento a cada 30 segundos para seus vizinhos, sendo que a convergência é incremental e mais lenta, ou seja, o roteador ensina o que conhece através dos vizinhos.
- Utilizam Split Horizon, Route-poisoning, Hold down timers e contagem ao infinito para evitar loops.
- Utilizam atualizações disparadas (triggered updates) para melhorar o tempo de convergência (atualizações fora do timer de 30s em caso de problemas).
- Protocolos abertos e compatíveis com roteadores de outros fabricantes.
- Não tem conhecimento da topologia da rede, apenas dos seus vizinhos diretamente conectados.
- Tem distância administrativa 120.
- Suportam balanceamento de carga entre rotas de mesma métrica (Equal cost path load balancing).

Características exclusivas do RIP versão 1:

- Suporta roteamento classfull, ou seja, classes A, B ou C cheias, não suporta VLSM somente máscaras de subrede com mesmo comprimento (subrede pura)
- Troca mensagens ou updates através de endereço de broadcast (255.255.255.255)
- Não suporta autenticação
- Não envia a informação de subrede (prefixo) nos anúncios
- Não suporta summarização de rotas (somente automática e classe cheia)

Características exclusivas do RIP versão 2:

- Suporta roteamento Classless (CIDR e VLSM), ou seja, não importa a classe, uma vez que a máscara de subrede é enviada no anúncio
- Troca mensagens ou updates através de endereço de multicast (224.0.0.9)
- Suporta autenticação para troca de mensagens
- Suporta summarização de rotas

### 3.1 Comandos para Ativação do RIP

Para ativar o processo do RIP basta entrar em modo de configuração global e digitar o comando “router rip”.

A seguir vamos listar os comandos necessários para completar as configurações do RIP versão 2:

- **(config)#router rip** – ativa o RIP em modo de configuração global.
- **(config-router)#version 2** - por padrão o RIP vem na versão 1, com o comando “version 2” você passa para a versão 2 do protocolo.
- **(config-router)#no auto-summary** - desativa a summarização automática, normalmente já é padrão em versões mais atuais do Cisco IOS (versão 15).
- **(config-router)#network rede-classe-cheia** - com o comando “network” seguido da rede classe cheia (classe A, B ou C) configurada nas interfaces diretamente conectadas defina as interfaces que farão parte do processo de roteamento.
- **(config-router)#passive-interface fast0/0** - com o comando “passive-interface” desativa as mensagens de update nas interfaces que não tem vizinhos RIP diretamente conectados
- **(config-router)# default-information originate** - defina a saída padrão no roteador conectado à Internet e com uma rota padrão instalada. Dessa maneira a rota padrão é espalhada entre os roteadores RIP da rede automaticamente, sem necessidade de configuração manual router a router.

O comando passive-interface pode ser utilizado também com a opção “passive-interface default”, a qual desativa o RIP em todas as interfaces. Nesse caso você precisa utilizar o comando “no passive-interface” para cada interface que deve participar do processo e formar vizinhança, o contrário do realizado anteriormente.

Veja exemplo abaixo onde as interfaces seriais de um roteador devem ficar ativas e as demais interfaces inativas ou passivas.

```
R1(config-router) #passive-interface default  
R1(config-router) #no passive-interface s0/0/0  
R1(config-router) #no passive-interface s0/0/1
```

Veja abaixo um exemplo de configuração onde o roteador tem os IPs 10.0.0.1/24 configurado em sua serial0/0 e 192.168.1.1/25 em sua fast0/0. Não existem outros roteadores RIP conectados na LAN do roteador, por isso essa interface será colocada como passiva.

```
R1(config)#router rip  
R1(config-router)#version 2  
R1(config-router)#network 10.0.0.0  
R1(config-router)#network 192.168.1.0  
R1(config-router)#passive-interface fastEthernet 0/0  
R1(config-router) #no auto-summary
```

Para desativar o RIP basta utilizar o comando “R1(config)#no router rip”

Dica: O comando network é acumulativo, para alterar de 10.0.0.0 para 11.0.0.0, por exemplo, você precisa apagar o da rede 10 e depois inserir o da rede 11, veja exemplo abaixo:

```
R1(config-router) #no network 10.0.0.0  
R1(config-router) #network 11.0.0.0
```

O real funcionamento do comando network é que ele faz com que a rede das interfaces com endereços IP dentro daquela faixa ou classe passem a ser anunciadas no processo de roteamento, assim como elas passam a enviar e receber updates do RIP.

Por esse motivo que precisamos utilizar o passive-interface nas interfaces que não tem vizinhos RIP conectados, pois senão um "hacker" ou por erro humano seu roteador pode começar a trocar rotas falsas com quem não deveria.

A seguir vamos aplicar cada um dos comandos e explicar mais o funcionamento/configurações do RIP versão 2.

### **3.2 Processo de Convergência do RIP**

No capítulo anterior estudamos que o RIP versões 1 e 2 utilizam o mesmo processo para determinar as melhores rotas e fazer com que as informações de roteamento de toda rede esteja consistente, processo chamado de "convergência", onde todos os roteadores conhecem as mesmas informações sobre todas as redes.

Portanto, o RIP por padrão de 30 em 30 segundos envia sua tabela de roteamento para seus vizinhos diretamente conectados.

Quando ele recebe uma tabela de roteamento de um dos seus vizinhos ele analisa as redes recebidas, compara com sua própria tabela de roteamento e verifica se as rotas recebidas através de seu vizinho estão ou não presentes em sua tabela.

Caso a rota não esteja presente, o roteador insere a rota em sua tabela de roteamento, vinculando um "vetor", ou seja, a interface que ele alcança essa rede inserida na tabela de roteamento.

Se a rota já existe em sua tabela de roteamento existem três possibilidades:

1. A rede recebida tem a métrica maior que a rota que está em sua tabela de roteamento? Nesse caso o roteador descarta a informação e mantém a sua própria rota, pois a métrica é pior do que a já inserida em sua tabela.
2. A rede recebida tem métrica menor que a inserida em sua tabela de roteamento? Nesse caso ela é melhor que a rota anterior e o roteador descarta a informação atual, inserindo essa nova rota em sua tabela de roteamento.
3. A rota tem métrica igual à rota que está atualmente inserida na tabela de roteamento? Nesse caso o roteador fará por padrão o balanceamento de carga e deixará ambas as entradas na tabela de roteamento. Por padrão os roteadores RIP fazem balanceamento de carga com até quatro rotas de métricas iguais.

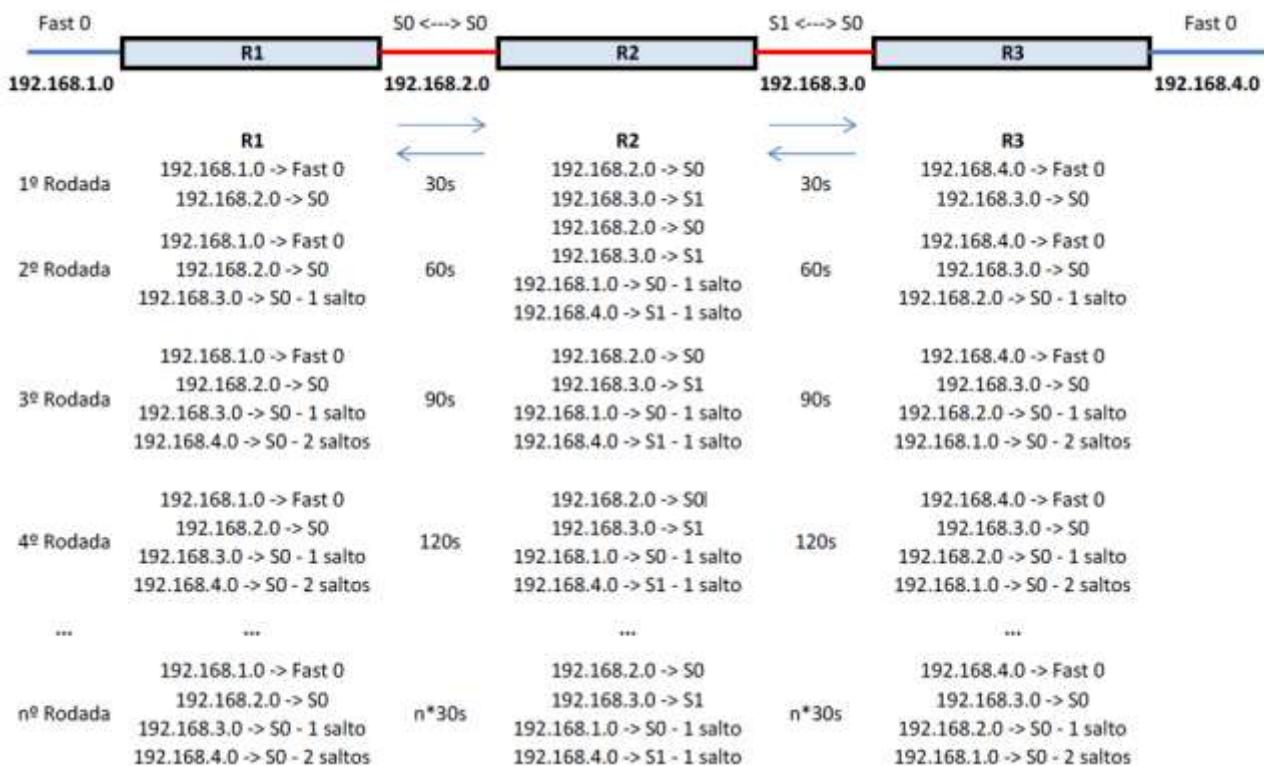
Portanto, o processo de convergência do RIP é incremental e a cada rodada de envio e recebimento de tabelas entre os vizinhos os roteadores vão conhecendo mais informações até o momento que eles conhecem informações de todas as redes.

É importante lembrar que no início os roteadores conhecem apenas as redes diretamente conectadas.

Quando ativamos o RIP os roteadores mandam na primeira rodada as redes diretamente conectadas aos seus vizinhos.

Na segunda rodada eles já conhecem suas redes conectadas e também as redes de seus vizinhos.

Na terceira rodada eles irão conhecer as redes de três saltos, ou seja, até os vizinhos de seus vizinhos, e assim vai até conhecerem todas as redes com um limite de 15 saltos de profundidade. Veja a figura a seguir que ilustra esse processo.



Vamos analisar a convergência no roteador R1, na primeira atualização ele envia as redes dele mesmo e recebe as redes diretamente conectadas do R2.

Na segunda rodada, o roteador R1 recebe as rotas diretamente conectadas de R2 ele verifica que a rede 192.168.3.0 não existe em sua tabela de roteamento, por isso insere essa nova informação com métrica 1.

Já para a rede 192.168.2.0, como ele já possui essa entrada em sua tabela de roteamento como diretamente conectada (com métrica zero) e a recebida do R2 está com 1 salto, o router R1 mantém rota original e descartará a informação recebida sobre essa rota através do R2.

Na terceira rodada o roteador R1 envia toda sua tabela de roteamento novamente. Em seu anúncio teremos as rotas 192.168.1.0 e 192.168.2.0 com métrica 1 e a rota 192.168.1.3 com métrica 2 sendo anunciada ao roteador R2.

Já o R2 envia para R1 as redes 192.168.2.0 e 192.168.3.0 com métrica 1, pois estão diretamente conectadas, e as rotas 192.168.1.0 e 192.168.4.0 com métrica 2.

Quando R1 recebe essas informações descarta as informações sobre as rotas conhecidas (192.168.1.0, 192.168.2.0 e 192.168.3.0) e a nova rota 192.168.4.0 que ainda não é conhecida é inserida em sua tabela de roteamento com métrica 2.

Nesse ponto R1 já aprendeu as informações sobre todas as rotas utilizadas na topologia, portanto dizemos que o protocolo convergiu.

Você pode visualizar essa comunicação em tempo real ativando o comando "debug ip rip" nos roteadores RIP.

As atualizações enviadas são identificadas com o termo “Sending Update” e as atualizações recebidas com “Received Update”, além disso, é informa a versão do RIP enviada e recebida na atualização. Além disso, quando há uma atualização disparada o RIP informa a construção de uma “flash update” e envia uma requisição na sequência.

Veja um exemplo abaixo onde uma flash update está sendo gerada devido a um problema na rede 10.0.1.0/24 e está “envenenando” (poisoning) a rota com o Route Poisoning, ou seja, enviando novamente para seu vizinho um update com métrica infinita (16) indicando que a rota está down e evitando que anúncios errados sejam propagados pela rede.

```
00:34:32: RIP: build flash update entries
00:34:32: 10.10.1.0/24 via 0.0.0.6, metric 16, tag 0
00:34:32: RIP: sending v2 flash update to 224.0.0.9 via Loopback
(10.10.1.1)
```

Lembre-se que os Updates do RIP versão 1 são enviados em broadcast (255.255.255.255) e da versão 2 em multicast (224.0.0.9).

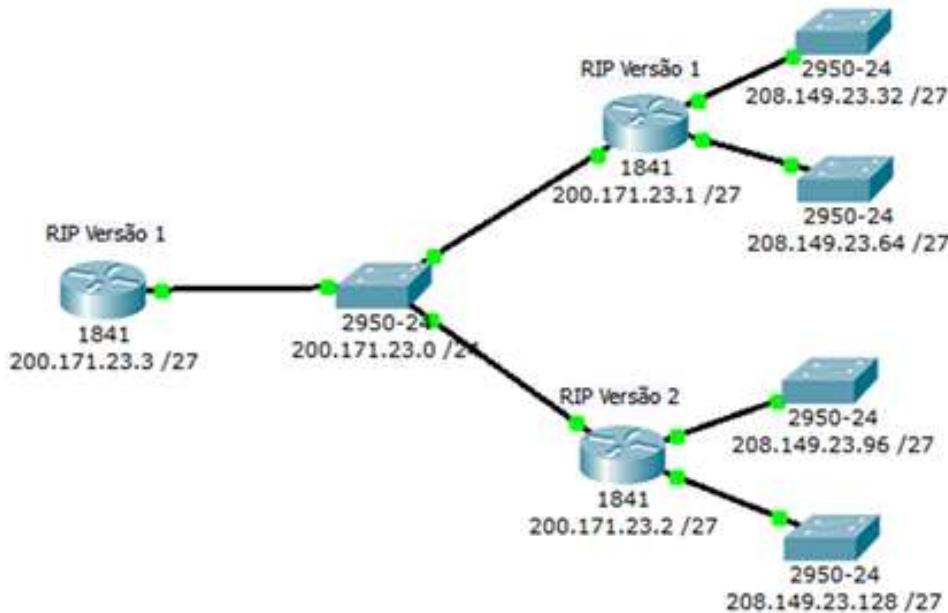
Este algoritmo utilizado pelo RIP é conhecido como “Bellman-Ford”.

### 3.3 Atualizações do RIP em Detalhe

O RIP envia suas atualizações ou “updates de roteamento” a cada 30 segundos indefinidamente, não importa se a rede convergiu ou não.

Na configuração padrão o RIP envia anúncios da versão 1 mas pode receber de ambas as versões. Já configurado com o comando “version 2” o RIP irá ignorar anúncios recebidos da versão 1.

A topologia da figura a seguir será utilizada como base para os exemplos desse tópico.



Veja abaixo as configurações do roteador 1841- 200.171.23.3, o qual tem o RIP v.1 padrão configurado nele.

```
router rip
network 200.171.23.0
```

Você pode verificar como o RIP se comporta para envio e recebimento dos anúncios com o comando "show ip protocols", conforme saída desse comando para o roteador 1841 – 200.171.23.3 abaixo.

```
Router#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 12 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface          Send   Recv   Triggered   RIP   Key-chain
      FastEthernet0/0     1       2       1
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    200.171.23.0
  Passive Interface(s):
  Routing Information Sources:
    Gateway          Distance      Last Update
    200.171.23.1        120          00:00:16
    200.171.23.2        120          00:00:15
  Distance: (default is 120)
Router#
```

Note na parte destacada que ele está com o controle de versão padrão: "Default version control: send version 1, receive any version", ou seja, enviando (send) a versão 1 e recebendo (receive) quaisquer versões, assim rotas aprendidas por anúncios de RIP versão 1 e 2 serão adicionadas à tabela de roteamento.

Logo abaixo no comando temos por que interface o roteador está se comunicando com o vizinho e que versões de RIP ela recebe e envia:

```
Interface          Send   Recv   Triggered   RIP   Key-chain
  FastEthernet0/0     1       2       1
```

Outra maneira de analisar os envios e recebimentos de anúncios é através do comando "debug ip rip", no qual o roteador mostrará cada anúncio recebido (received) ou enviado (sent) na interface CLI.

```
Router#RIP: received v2 update from 200.171.23.2 on FastEthernet0/0
  208.149.23.96/27 via 0.0.0.0 in 1 hops
  208.149.23.128/27 via 0.0.0.0 in 1 hops
RIP: received v1 update from 200.171.23.1 on FastEthernet0/0
  208.149.23.0 in 1 hops
```

Note na saída do comando que podemos verificar que o roteador está recebendo informações de um vizinho com IP 200.171.23.2 e um segundo vizinho com IP 200.171.23.1. Além disso, podemos verificar que:

1. O vizinho 200.171.23.2 está enviando anúncios de RIP com versão 2 e suas rotas anunciadas vem com a informação de subrede no anúncio
2. O segundo vizinho de IP 200.171.23.1 está enviando anúncios de RIP versão 1 e sua rota vem sem a informação da máscara de subrede

A seguir temos mais um exemplo do comando debug quando um dos roteadores está configurado como "version 2" e o outro está configurado com versão 1. Esta é a saída do roteador 1841 - 200.171.23.2.

Router#RIP: **sending v2 update** to 224.0.0.9 via FastEthernet0/1 (208.149.23.97)

RIP: build update entries

200.171.23.0/27 via 0.0.0.0, metric 1, tag 0  
208.149.23.128/27 via 0.0.0.0, metric 1, tag 0

RIP: **ignored v1 packet** from 200.171.23.1 (illegal version)

Note que ele envia a versão 2 e quando recebe o pacote versão 1 do vizinho 200.171.23.1, é informado que aquela versão de pacote recebido foi ignorado: RIP: ignored v1 packet from 200.171.23.1 (illegal version).

Vamos aproveitar a topologia e verificar o comportamento classfull do RIP versão 1.

Veja que o roteador com o IP 200.171.23.1 apesar de ter 2 subredes para a rede 208.148.23.0, apenas uma rota é anunciada a 208.148.23.0 para seu vizinho. Essa é a característica do RIP v1, não anuncia a informação de subrede para o vizinho.

Já o router que tem RIP v2 configurado anunciou suas subredes. Veja abaixo a saída do comando "show ip route" do roteador 1841 - 200.171.23.3.

```
Router#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
      - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route
Gateway of last resort is not set
      200.171.23.0/27 is subnetted, 1 subnets
C          200.171.23.0 is directly connected, FastEthernet0/0
      208.149.23.0/24 is variably subnetted, 3 subnets, 2 masks
R          208.149.23.0/24 [120/1] via 200.171.23.1, 00:00:23,
FastEthernet0/0
```

```
R      208.149.23.96/27 [120/1] via 200.171.23.2, 00:00:00,
FastEthernet0/0
R      208.149.23.128/27 [120/1] via 200.171.23.2, 00:00:00,
FastEthernet0/0
Router#
```

Note que as redes do roteador configurado com RIP versão 2 são exibidas na tabela de roteamento.

Já as rotas do roteador 200.171.23.1, que está com RIP v.1 são colocadas como apenas uma entrada para a rede 208.149.23.0 /24, pois o RIP v.1 não anuncia o prefixo e apenas uma rede classe cheia, veja o “debug ip rip” do roteador 200.171.23.3.

```
RIP: received v1 update from 200.171.23.1 on FastEthernet0/0
208.149.23.0 in 1 hops
RIP: received v2 update from 200.171.23.2 on FastEthernet0/0
208.149.23.96/27 via 0.0.0.0 in 1 hops
208.149.23.128/27 via 0.0.0.0 in 1 hops
```

Para que o roteamento nesse caso seja completado e bem sucedido basta converter o RIP v.1 para v.2 nos roteadores 200.171.23.1 e 200.171.23.3 conforme configurações abaixo. Lembre-se que o comando network já foi configurado.

```
Router#config term
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
```

O comando “no auto-summary” foi inserido para que não haja summarização automática para rotas classfull e todos os roteadores enunciem as rotas completas, veja o “show ip route” do roteador 200.171.23.3 abaixo.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
- BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area
          * - candidate default, U - per-user static route, o - ODR
          P - periodic downloaded static route
Gateway of last resort is not set
          200.171.23.0/27 is subnetted, 1 subnets
C        200.171.23.0 is directly connected, FastEthernet0/0
          208.149.23.0/27 is subnetted, 4 subnets
R        208.149.23.32 [120/1] via 200.171.23.1, 00:00:11,
FastEthernet0/0
R        208.149.23.64 [120/1] via 200.171.23.1, 00:00:11,
FastEthernet0/0
```

```
R      208.149.23.96 [120/1] via 200.171.23.2, 00:00:18,  
FastEthernet0/0  
R      208.149.23.128 [120/1] via 200.171.23.2, 00:00:18,  
FastEthernet0/0  
Router#
```

Agora todas as rotas estão presentes, pois todos os roteadores estão utilizando a versão 2 e enviando as redes com suas respectivas máscaras em seus anúncios.

### 3.4 Timers do RIP

Ambas versões do RIP trabalham com os mesmos temporizadores de Update e Hold down.

Os Updates (atualizações de roteamento) são trocados a cada 30 segundos, podendo ser alterado com o comando "timers basic" dentro do modo de configuração do roteador RIP.

Além disso, o mesmo comando altera os timers de Invalid, Hold down e Flushed.

O exemplo ao lado mostra a configuração padrão dos timers. Você pode alterar, por exemplo, somente o update para 40 segundos com o comando "timers basic 40".

Agora para alterar somente o flush para 250 você teria que entrar com o comando "timers basic 30 180 180 250".

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config-router)#timers basic ?
<0-4294967295> Interval between updates
Router(config-router)#timers basic 30 ?
<1-4294967295> Invalid
Router(config-router)#timers basic 30 180 ?
<0-4294967295> Holddown
Router(config-router)#timers basic 30 180 180 ?
<1-4294967295> Flush
Router(config-router)#timers basic 30 180 180 240 ?
<cr>
Router(config-router)#timers basic 30 180 180 240
```

O valor configurado no roteador pode ser visto no comando "show ip protocols", conforme estudamos anteriormente.

```
Router#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 12 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  ... Saída omitida
```

Como podemos observar, os roteadores RIP possuem 4 temporizadores:

- Atualizações ou updates
- Hold down
- Inválido ou invalid e
- Flush

Por padrão, o temporizador de atualização é de 30 segundos, o temporizador inválido é 6 vezes a atualização (180 segundos), o HOLD DOWN também é 180 segundos e o flush é de 240 segundos.

O temporizador de inválido (invalid) se refere como o temporizador de validade ou limite, é ele que determina quando uma rota será marcada como inacessível (possibly down), após um período de tempo sem ser atualizada (neste caso 180 segundos).

Após a rota ser marcada como inacessível entra em cena o temporizador de HOLDDOWN e quando nesse estado o roteador não vai considerar nenhum anúncio de rota com métrica melhor para essa rota. A rota fica nesse estado até que o tempo de HOLDDOWN expire.

Por padrão, nos roteadores da Cisco o holddown vem setado como 180 segundo. Após expirar o tempo de holddown o roteador passa a aceitar novas atualizações sobre a rota.

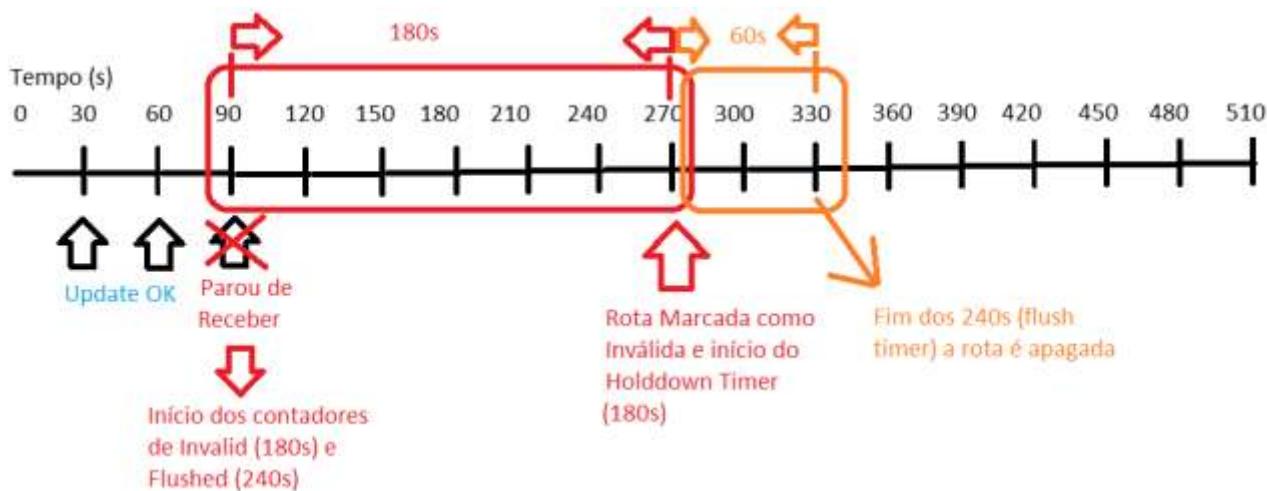
O temporizador de flush é o que vai retirar a rota da tabela de roteamento, portanto quando o tempo de flush expirar a rota é deletada.

Por padrão, o flush vem configurado como 240, ou seja, com a configuração padrão o RIP leva 4 minutos ou 240 segundos para apagar uma rota da sua tabela de roteamento se ele não receber atualização dela por seus vizinhos.

Perceba que por padrão o timer holddown é configurado para 180s, e o flush é para 240s, portanto a rota ficará em holddown por apenas 60 segundos.

Isso porque o holddown começou a contar 180s após o último update (após a finalização do timer invalid) e o flush será 240s após o último update, logo a rota ficará em holddown apenas 60s, após esse prazo a rota será apagada.

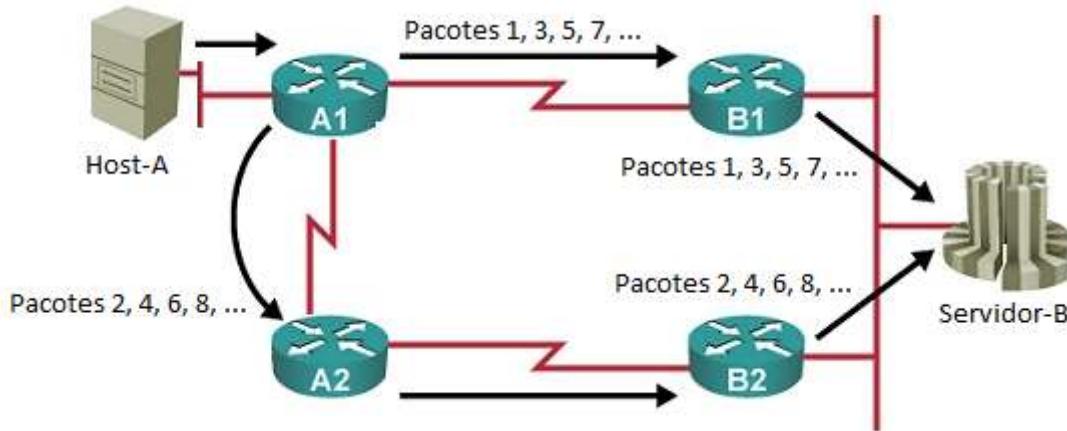
Veja a sequência de ativação dos contadores na figura abaixo, note que o início dos contadores de invalid e flush são logo após o RIP parar de receber o primeiro update (atualização) do seu vizinho sobre determinada rota. Após a rota ser marcada como inválida ela ficará apenas mais 60s em hold-down e depois será apagada.



Você tem mais informações sobre o funcionamento dos timers nesse artigo do nosso blog:  
<http://www.dltec.com.br/blog/cisco/rip-timers-em-roteadores-cisco/>

### 3.5 Balanceamento de Cargas

O balanceamento de carga é uma propriedade do RIP, OSPF e EIGRP utilizar um segundo link backup para compartilhar o envio de dados. Veja a abaixo com um exemplo de balanceamento de carga de custos iguais por pacotes.



Quando o protocolo de roteamento ativa o balanceamento de carga em dois ou mais links se um host envia pacotes para uma rede de destino o roteador divide os pacotes (per packet) ou fluxos (per destination – por destino) entre as interfaces balanceando (dividindo) o envio dos pacotes (carga) entre esses caminhos.

No balanceamento de carga por pacotes os roteadores enviam um pacote para cada interface que participa do processo.

No balanceamento por fluxo (ou destino) o balanceamento de carga é realizado por conexão TCP ou UDP aberta, ou seja, se um usuário solicitou uma página de internet aquele fluxo vai seguir até o final por um link, quando um segundo usuário abrir outra sessão na sequência o fluxo dele será encaminhado ao segundo link.

Por padrão os roteadores Cisco fazem o entre rotas de métricas de mesmo custo chamado “equal cost path load sharing”, em inglês.

Além disso, por padrão a carga é balanceada em até 4 links de custos iguais automaticamente.

Esse número de links pode ser configurado no máximo de 6 links em versões mais antigas do Cisco IOS ou até mais de 16 em versões mais atualizadas.

A configuração de quantos links devem participar do balanceamento de carga está dentro do modo de configuração de roteamento com o comando “maximum-paths” (padrão “maximum-paths 4”).

Nos tópicos anteriores estudamos que podemos verificar esse parâmetro no comando “show ip protocols”.

Na tabela de roteamento você consegue verificar o balanceamento de carga através de entradas repetidas para a mesma rede com custos (métricas) iguais.

Essa propriedade melhora o uso dos links, pois diminui a sobrecarga de termos uma topologia redundante com link principal e backup em espera (stand-by) entrando em atividade somente em caso de problemas, assim como o balanceamento de carga evita que o link backup fique ocioso.

Veja exemplo da saída de uma tabela de roteamento com rotas em balanceamento ativo.

```
router# show ip route
...
    172.30.0.0/16 is variably subnetted, 1 subnets, 1 masks
R      172.30.32.0/20 [120/2] via 10.1.1.2
          172.30.32.0/20 [120/2] via 10.1.1.1
S*    0.0.0.0/0 [1/0] via 10.1.1.3
```

Note que a rede 172.30.32.0 tem duas saídas possíveis indicadas na tabela de roteamento, através de 10.1.1.2 e 10.1.1.1. Note também que ambas as rotas tem a mesma métrica "2", por isso o平衡amento foi ativado entre elas.

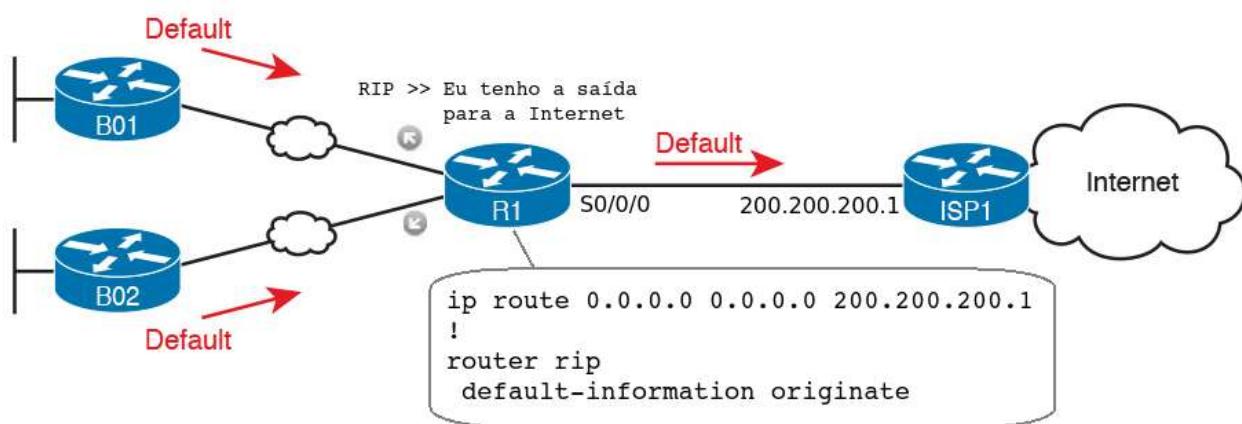
Para desabilitar o平衡amento de carga basta utilizar o comando "maximum-paths 1" (padrão é 4 e o máximo depende da versão do Cisco IOS).

O RIP e OSPF tem o mesmo funcionamento para o平衡amento de cargas, já o EIGRP também suporta平衡amento entre rotas com métricas diferentes.

### 3.6 Anunciando a Rota Padrão pelo RIP

Para facilitar a divulgação da rota padrão os protocolos RIP e OSPF possuem um comando em modo de configuração de roteador que pode ser inserido no roteador que possui o link de saída para Internet para que essa saída padrão seja anunciada automaticamente para todos os demais roteadores, o comando é o "**default-information originate**".

Portanto, no roteador com a saída para Internet basta configurar uma rota estática padrão e digitar o comando "default-information originate" dentro da configuração do RIP ou OSPF que o próprio protocolo de roteamento dinâmico fará o anúncio dessa rede para os demais routers, veja um exemplo abaixo.



```
hostname R1
!
ip route 0.0.0.0 0.0.0.0 200.200.200.1
!
Router rip
  Version 2
  No auto-summary
  network 10.0.0.0
```

```
network 192.168.1.0
network 192.168.4.0
default-information originate
passive-interface default
no passive-interface s0/0/0
no passive-interface s0/0/1
```

No roteador local (R1) a rota padrão vai apontar para 200.200.200.1 e será marcada com "S\*", ou seja, estática (S) e candidata a default (\*).

Com base nessa informação o RIP vai repassar para os vizinhos a informação possibilitando que o melhor caminho até essa rota padrão ou a Internet seja calculado automaticamente.

No roteador vizinho a rota padrão distribuída pelo comando "default-information originate" aparece como uma rota do RIP com "R\*" na frente, veja no exemplo a seguir.

```
B01#show ip route
Saídas omitidas...
```

```
Gateway of last resort is 192.168.1.9 to network 0.0.0.0
```

```
C      10.0.2.0 is directly connected, FastEthernet0/0
C      10.0.3.0 is directly connected, FastEthernet0/1
R      192.168.10.0 [120/2] via 192.168.1.6, 00:00:11, Serial0/0/0
C      192.168.1.0 is directly connected, Serial0/0/0
C      192.168.4.0 is directly connected, Serial0/0/1
R*     0.0.0.0/0 [120/2] via 192.168.1.9, 00:00:11, Serial0/0/1
Router-B#
```

Outra maneira do roteador local aprender a rota padrão é através do DHCP, inserindo o comando "ip address dhcp" em sua interface. Se o seu roteador conectado com a Internet por acaso tiver aprendido seu IP via DHCP, ele também aprenderá a rota padrão.

Portanto, nesse caso em específico, basta inserir o comando "default-information originate" que essa rota aprendida via DHCP cliente será disseminada via RIP. Veja exemplo a seguir.

```
R1# configure terminal
R1(config)# interface fast0/0
R1(config-if)# ip address dhcp
R1(config-if)# router rip
R1(config-router)#default-information originate
R1(config-router)#end
R1#
R1# show ip route static
! saídas omitidas ...
Gateway of last resort is 192.1.20.10 to network 0.0.0.0
S* 0.0.0.0/0 [254/0] via 192.1.20.10
```

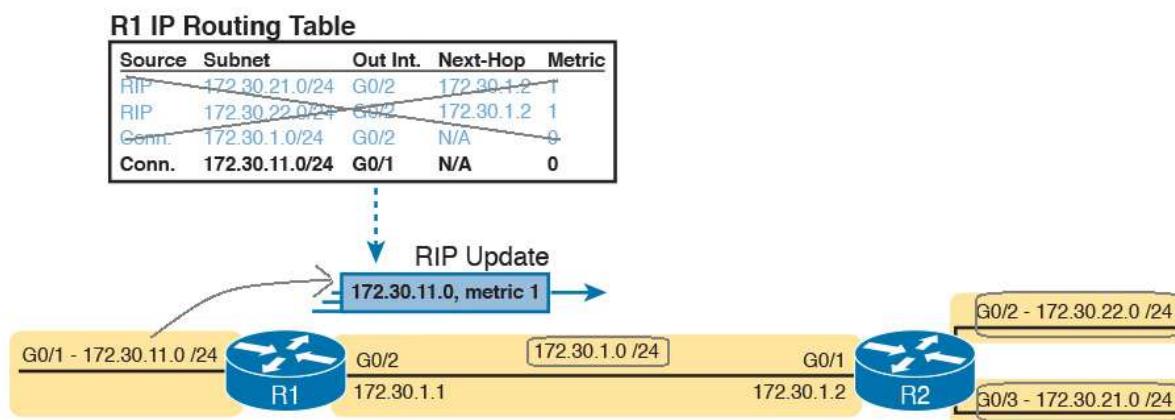
### 3.7 Evitando Loops no RIP – Split Horizon, Route Poisoning e Contagem ao Infinito

Uma maneira de se eliminar os loops de roteamento a aumentar a velocidade de convergência é utilizando o recurso chamado estreitamento de horizontes ou split horizon, em inglês, o qual já vem ativo por padrão nas interfaces com RIP ativado.

O split horizon diz que não é útil mandar informações sobre uma rota de volta na mesma direção por onde a informação original chegou, ou seja, evita que um roteador RIP propague rotas para a mesma interface que ele aprendeu, evitando loop entre estes nós.

É como se você ouvisse uma piada de um amigo e na mesma hora falasse para ele: "Cara, aprendi uma piada sensacional..." e sai contando a mesma piada de volta para ele. Isso tem sentido? Também não tem sentido um roteador receber uma atualização por uma interface dizendo que uma rota caiu e ele diz "não, não caiu não".

Veja a imagem abaixo para entender melhor o assunto do split horizon.



Note que R1 envia somente informações sobre a rota 172.30.11.0/24 para R2, pois as demais rotas foram ensinadas pelo próprio R2 através da Giga0/2 de R1, por isso ele não faz anúncios em direção a R2 sobre as rotas 172.30.1.0/24, 172.30.22.0/24 e 172.30.21.0/24, pois o split horizon evita esse tipo de anúncio devolvendo informações pela mesma interface que as R1 recebeu anteriormente.

O envenenamento de rotas (Route Poisoning) é uma ligeira modificação daquela utilizada no split horizon, sendo que seu objetivo também é a prevenção de loops de roteamento causados por atualizações inconsistentes.

O envenenamento de rotas é uma solução para loops longos, por exemplo, a rede 172.30.11.0/24 fica indisponível no roteador R1 (diretamente conectado a ele) e ele envenena este enlace.

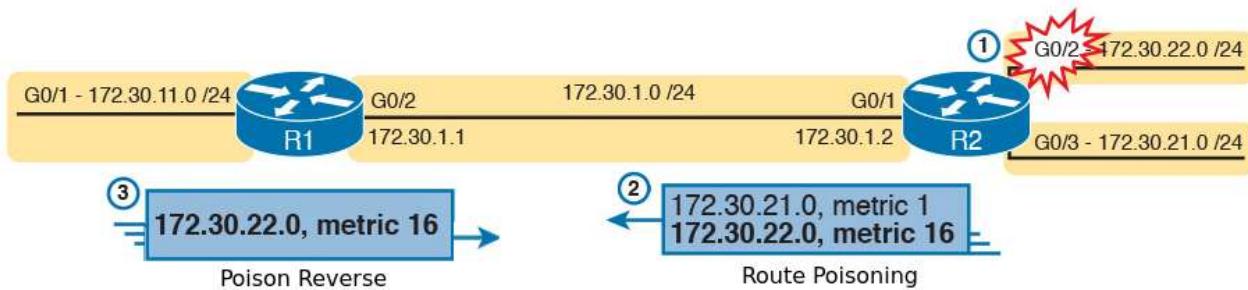
Isso significa que na tabela de roteamento de R1 ele coloca esta rede como inalcançável ou de métrica infinita (número de saltos igual a 16). Tendo envenenado a rota para este enlace, o roteador C não fica sujeito a atualizações incorretas a respeito deste enlace, vindas de roteadores vizinhos que acreditam ter rotas backup para ele.

Outro tipo de envenenamento de rotas é o Envenenamento Reverso (Poison Reverse). O split horizon em conjunto com o envenenamento reverso faz com que a rede consiga convergir em menos tempo.

Quando o roteador R2 recebe uma atualização mostrando que a métrica para se atingir a rede 172.30.11.0/24 foi alterada para infinito, ele manda uma atualização chamada de envenenamento reverso em direção ao roteador R1 avisando que a rede está inalcançável.

Além disso, ele ainda coloca este enlace como possivelmente inalcançável (possibly down) em sua tabela de roteamento. Essa é uma situação específica que se sobrepõe ao split horizon.

Veja a imagem a seguir com exemplo do route poisoning e poison reverse em ação. Vamos supor que a interface G0/2 do roteador R2 caiu (1).



Na sequência R2 envenena a rota em direção a R1 (2), o qual recebe a informação e faz um poison reverse em direção a R2 (3), garantindo que não vai haver loop de roteamento.

Agora imagine que tudo foi desativado e R1 informa para R2 que a rota que caiu é conhecida e tem métrica 2, ele vai instalar a rota com métrica 3 e passar para R2 que vai instalar com métrica 4 e assim vai.

Para evitar esse problema o RIP limita a 15 saltos, se uma rota anunciada passar de 15 saltos ela é descartada, pois 16 saltos já é considerada uma métrica infinita de saltos, por isso esse recurso de proteção contra loops é chamado contagem ao infinito.

Os pacotes IP tem um recurso bem parecido que é o TTL ou time to live (tempo de vida) do pacote. Caso o tempo de vida chegue a zero que o recebeu descarta o pacote e informa para trás com a mensagem TTL expired, assim como estudamos no funcionamento do traceroute, porém aqui o motivo não é teste e sim que a rede é muito longa ou o pacote perdeu-se na rede.

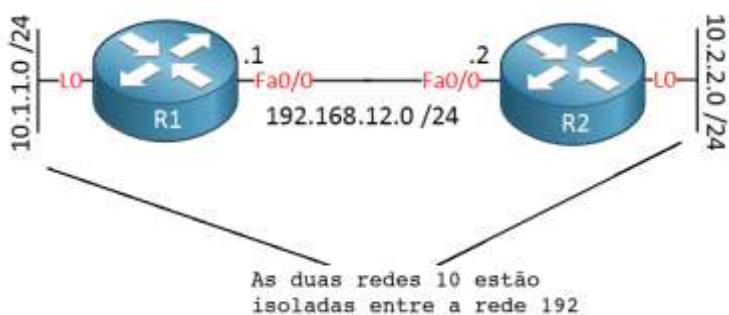
### 3.8 Entendendo os Problemas da Sumarização Classful Automática do RIP

Dependendo da versão de Cisco IOS do roteador o RIP por padrão tem um recurso chamado summarização classful automática ativado ou “auto-summary”.

Com esse recurso ativado no RIP versão 2 o roteador ao invés de anunciar cada uma das sub-redes nele configurado, ele anuncia somente a rede classful (classe cheia A, B ou C) que sumariza essas sub-redes.

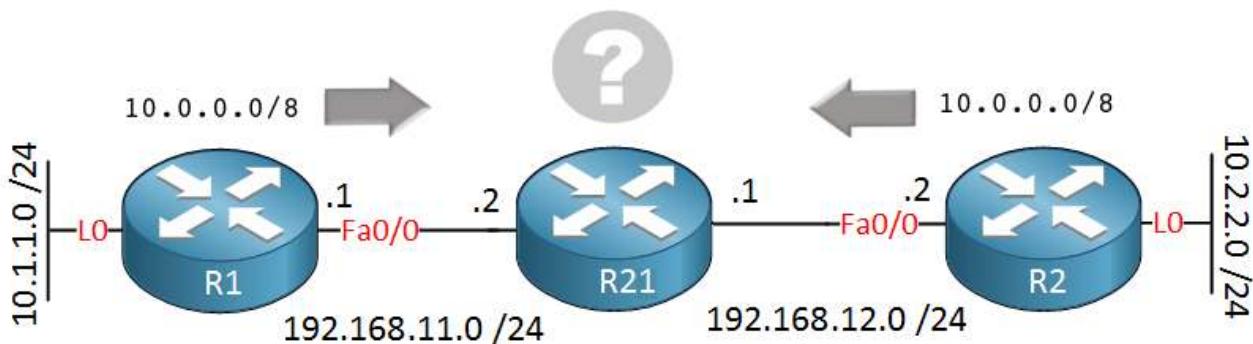
Por exemplo, se você usa as redes de 10.0.0.0/24 a 10.0.100.0/24 nas interfaces do roteador, ele vai anunciar nos seus updates apenas uma rota summarizada com a rede 10.0.0.0/8, ou seja, a rede 10 classe A cheia.

Existem duas desvantagens nesse tipo de summarização, a primeira é que ela é muito abrangente e a segunda é o risco de causar problemas de roteamento em redes descontínuas ou descontínuas. Uma rede descontínua tem uma descontinuidade em relação a alocação de IPs, veja a figura abaixo para entender melhor.



Nesse caso da figura acima não teremos grandes problemas, pois R1 vai ter a rede 10.1.1.0 como local e uma rota para 10.0.0.0/8 apontando para R2, portanto quando um pacote for criado para um destino pertencente a rede 10 que não seja para a rede local ele será encaminhado para 192.168.12.2 (R2). A mesma análise serve para R2.

Agora vamos a um exemplo que pode gerar problema, vamos colocar outro roteador entre R1 e R2, chamado R21.



Veja que no roteador R21 não existem redes 10 configuradas e ao receber anúncios summarizados de R1 e R2 com a rota 10.0.0.0/8 como ele vai conseguir definir para onde mandar quaisquer pacotes para esses destinos?

Foi criada uma inconsistência na tabela de roteamento devido a descontinuidade causada pela summarização automática.

Por isso devemos utilizar o comando “no auto-summary” com o RIPV2 e fazer a summarização manual, porém esse tipo de configuração não faz parte do conteúdo da prova atual.

Uma dica prática é sempre configure o “no auto-summary” antes de utilizar o comando “network”, pois assim os roteadores não criarião a rota summarizada. Se você não fizer isso a rota summarizada será criada e levará aproximadamente 240 segundos para ser removida da tabela de roteamento, o tempo do temporizador de flush.

A seguir você vai estudar dicas de troubleshooting e comandos show do RIP para seu exame de certificação.

### 3.9 Dicas de Troubleshooting do RIP

Os principais problemas que podemos encontrar em questões do CCENT envolvendo o RIP são:

1. **Problemas básicos de camadas 1, 2 e 3:** Muitas vezes o RIP não se comunica porque temos cabos rompidos ou tipos de cabos errados nas conexões (por exemplo, deveria ser uma cabo cross e foi utilizado um direto), na camada de enlace em interfaces serias DCE falta o comando clock rate ou o tipo de protocolo em uma das pontas está errado (encapsulation) e na camada de rede o IP/máscara das interfaces pode estar errado. Tudo isso pode fazer com que o RIP não consiga trocar mensagens de atualização e não suba corretamente, mesmo que as configurações de roteamento estejam corretas.
2. **Configurações erradas:** Redes anunciadas erradas no comando Network e erro na versão do RIP em uma das pontas (comando version).
3. **Falta de configurações:** Redes não anunciadas ou faltantes no comando network e falta do comando "no auto-summary" para evitar a sumarização automática de rotas.
4. **Comando passive-interface em interfaces que tem vizinhos:** lembre-se que o passive interface faz com que o roteador ignore o vizinho, por isso se o roteador não está trocando rotas verifique se ele não foi utilizado erroneamente.
5. **Interfaces diretamente conectadas em redes diferentes:** para que o RIP troque atualizações as interfaces diretamente conectadas devem estar na mesma rede ou sub-rede IP.

Se o exercício dá condições de acessar o roteador com problemas utilize o comando "show running-config" e analise a configuração das interfaces e do RIP, lembrando que tanto a versão 1 como a versão 2 tem a mesma configuração, diferenciando apenas no comando "version 2" para a versão 2.

Por padrão o RIP vem configurado como versão 1.

No comando "network" é importante lembrar que configuramos sempre as redes classe cheia (classfull) e não as subredes, além disso, somente as redes diretamente conectadas.

Outra maneira de cobrar conceitos de troubleshooting sobre o RIP é com os comandos "show" e "debug" relacionados a ele.

Os principais comandos para o RIP já estudamos ao longo do capítulo, porém vamos relembrar os pontos mais importantes.

- **Show running-config:** podemos analisar a configuração do RIP.
- **Show ip route:** analisar a tabela de roteamento completa.
- **Show ip route rip:** analisar apenas as entradas do RIP.
- **Show ip rip database:** analisar as entradas de roteamento aprendidas pelo RIP, vai além da tabela de roteamento, pois algumas entradas podem estar contidas no banco de dados e por não ser a melhor métrica não são inseridas na tabela de roteamento e ficam armazenadas apenas nesse banco de dados do RIP.
- **Show ip protocols:** mostra as configurações gerais dos protocolos de roteamento IP habilitados, inclusive do RIP.
- **Debug ip rip:** analisar a troca de mensagens em tempo real. Lembrar que uma mensagem de "RIP: ignored v2 packet from 172.12.23.2 (illegal version)" significa que de um lado você tem configurado RIP V1 e recebeu uma mensagem do RIP V2, a qual foi ignorada. Se a mensagem fosse "RIP: ignored v1 packet ... (illegal version)" seria ao contrário, você está com RIP V2 configurado e recebeu do vizinho uma atualização do RIP V1.

## 4 Testando a Conectividade com Ping, Traceroute e Telnet

Os comandos ping, traceroute e telnet podem ser utilizados para realizar vários testes na rede, sendo que os dois primeiros testam as camadas 1, 2 e 3 do modelo OSI, já o telnet vai até a camada de aplicação.

A diferença básica entre os três comandos é que o ping é um recurso do ICMP chamado "Echo", já o traceroute também utiliza o ICMP, porém é implementado através da mensagem de "TTL expirado", já o telnet é uma aplicação de rede, sendo que o destino do teste deve ter o servidor telnet habilitado para que o teste funcione.

Os testes de ping e trace só precisam que as mensagens ICMP de "Echo" e "TTL expirado" estejam liberadas nos firewalls de rede para funcionar, pois são suportadas por todos os dispositivos que trabalham com o protocolo IP. Algumas redes corporativas bloqueiam essas mensagens por questões de segurança.

Lembre-se que os detalhes do ping e traceroute foram estudados no capítulo 5, em caso de dúvidas volte e faça uma revisão, pois vamos focar aqui nos comandos.

Nesse capítulo vamos ver como ir além dos testes convencionais já realizados durante os capítulos anteriores e estudar opções avançadas de uso desses recursos disponíveis no Cisco IOS.

### 4.1 Utilizando o Ping

O comando ping responde uma pergunta simples: "**Existe conectividade em camada 3 entre dois pontos?**". Caso haja o teste será bem sucedido e você receberá um ponto de exclamação como resposta, senão aparecerão erros representados por símbolos tais como um ponto final (expirou o tempo limite) ou a letra U (Unreachable - destino inalcançável).

Lembre-se que ao executar um ping em seu computador ou roteador, uma mensagem de "**echo request**" (requisição de echo) é enviada através do protocolo ICMP diretamente em um pacote IP e quando o destinatário recebe essa mensagem ele deve responder com um "**echo reply**" (resposta ao echo) em até dois segundos por padrão.

O ICMP não utiliza o TCP ou UDP para envio das mensagens, pois ele é um protocolo auxiliar do protocolo IP e é inserido diretamente no pacote IP sem a necessidade de utilizar os protocolos das camadas superiores.

O comando ping permite vários opcionais, tanto nos computadores como nos roteadores, tais como alterar o tamanho do pacote de teste, alterar o endereço de origem do pacote, definir o número de mensagens de echo request a serem enviadas, etc.

Por exemplo, se você digitar no prompt de comando do Windows "**ping -l 1500 -t www.cisco.com**" você enviará pacotes com 1500 bytes, definido no parâmetro "-l", e o "-t" manda enviar o echo request indefinidamente até que seja cancelado pelo administrador no prompt. Vamos estudar nesse tópico o uso do ping e também algumas opções avançadas que são úteis para realizar diagnósticos de problemas em redes.

#### 4.1.1 Exemplo Prático de Uso do Ping e Revisão do ARP

Você acaba de inserir uma nova LAN em sua rede com diversos computadores conectados a uma VLAN. O roteamento entre as VLANs é realizado por um roteador.

Após os testes e os usuários já trabalhando nessa nova área chega um chamado ao centro de suporte da empresa, normalmente chamado de Service Desk ou Customer Service Representative (CSR), informando que ele está sem acesso ao servidor onde são armazenados os backups dos seus arquivos de trabalho.

Nesse caso existem várias opções de diagnóstico, por exemplo, ele pode acessar via Telnet ou SSH o roteador que está configurado como gateway desses hosts de rede e com o ping testar a conectividade entre o roteador padrão e o servidor de arquivos, para verificar se é um problema isolado do usuário ou se algo foi esquecido na configuração desse novo roteador. Veja exemplo abaixo da simulação do teste realizado.

```
R1# ping 192.168.2.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.101, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
R1# ping 192.168.2.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

O ping em roteadores Cisco por padrão enviam cinco mensagens de echo request. Note no primeiro teste de ping que o primeiro echo enviado não foi respondido, quando isso acontece e depois temos respostas é devido a resolução do endereço MAC sendo realizada pelo ARP, no IPv6 vocês verão que o NDP (substituto do ARP) demora bem mais para resolver o MAC de um endereço IP.

O teste acima mostrou que a rede encaminhando pacotes ao servidor, portanto podemos tentar um acesso remoto ao computador do usuário para verificar se não é um problema local, por exemplo.

Voltando a tabela ARP vamos relembrar que podemos analisar seu conteúdo nos roteadores com o comando “show arp” e se o IP de destino não estiver listado, antes de enviar o pacote com o ping, a resolução ARP deverá ser realizada, por isso a perda de um pacote.

```
DlteC-FW-GW#show arp
Protocol Address          Age (min)  Hardware Addr   Type      Interface
Internet 10.0.1.1          -          001e.130b.1aef ARPA     FastEthernet0/1.20
Internet 192.168.1.1        -          001e.130b.1aef ARPA     FastEthernet0/1.10
Internet 192.168.1.5         9          0024.5161.6a41 ARPA     FastEthernet0/1.10
Internet 192.168.1.11       14         e0cb.4ecc.9b9b ARPA     FastEthernet0/1.10
Internet 192.168.1.18       72         1cc1.def9.3f53 ARPA     FastEthernet0/1.10
Internet 192.168.1.22       0          c018.85e5.eedb ARPA     FastEthernet0/1.10
Internet 192.168.1.23       0          c018.85e5.ecbf ARPA     FastEthernet0/1.10
Internet 192.168.1.254      1          0012.7b50.01f6 ARPA     FastEthernet0/1.10
Internet 192.168.2.1          -          001e.130b.1aef ARPA     FastEthernet0/1.30
Internet 192.168.2.20       10         001d.7060.d31b ARPA     FastEthernet0/1.30
Internet 192.168.10.1        5          0022.3f3d.d916 ARPA     FastEthernet0/0
Internet 192.168.10.2        -          001e.130b.1aee ARPA     FastEthernet0/0
DlteC-FW-GW#
```

Com o comando “clear arp” e o IP do destino apaga uma entrada ARP específica e pode ser utilizado para forçar uma resolução ARP em ambientes de teste, por exemplo, “clear arp 192.168.1.11”. Em ambientes reais é difícil simular esse comportamento devido a comunicação gerada pelos sistemas operacionais, mas no packet tracer é bem simples de simular.

Quando o pacote é para uma rede externa o MAC de destino do pacote será o do gateway configurado na placa de rede.

Nos computadores Windows podemos utilizar o comando "arp -a".

#### 4.1.2 Opções Avançadas – Alterando o IP de Origem no Ping Estendido

Como já comentado anteriormente, podemos controlar com opções avançadas o comportamento do ping, por exemplo, podemos definir a origem do pacote IP ao gerar as mensagens de echo request com o ping estendido, digitando apenas "ping" no terminal do roteador, veja exemplo abaixo:

```
DlteC-FW-GW#ping
Protocol [ip]:
Target IP address: 192.168.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
DlteC-FW-GW#
```

Analisando as opções acima em destaque foram as únicas alteradas, no restante apenas foi dado um entra com o valor sugerido entre colchetes. Portanto na terceira linha definimos o IP de destino a ser testado, na sétima linha habilitamos os comandos extras, na oitava linha definimos o endereço de origem a ser utilizado, nas demais linhas só confirmamos com um entra as opções padrões. Com isso o pacote IP gerado para o ping tem agora o endereço de origem 192.168.1.1 e tivemos a perda do primeiro pacote de echo, provavelmente devido a resolução ARP em um dos dispositivos.

Mas para que precisaríamos alterar o IP de origem escolhido pelo roteador? Porque por padrão o roteador monta o cabeçalho IP do ping utilizando o **endereço da interface de saída do pacote**, a qual nem sempre pertence à rede de origem que estamos querendo testar.

Por exemplo, no teste do tópico anterior ao invés do roteador utilizar o IP da LAN onde o computador estava situado, foi utilizado o IP da interface que conecta o roteador às demais redes internas, por isso o teste não foi 100% preciso, precisaria ser refeito utilizando o IP de origem sendo o da LAN do roteador ou a própria interface ou subinterface dele.

Para utilizar uma interface como origem é preciso escrever o nome inteiro dela, por exemplo, fastethernet0/0.

Você pode executar as operações também diretamente via terminal, veja exemplo a seguir.

```
DlteC-FW-GW#ping 192.168.1.1 ?
      data      specify data pattern
```

```

df-bit    enable do not fragment bit in IP header
repeat   specify repeat count
size      specify datagram size
source    specify source address or name
timeout   specify timeout interval
validate  validate reply data
<cr>
DlteC-FW-GW#ping 192.168.10.1 repeat 10 source fastethernet0/0
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.2
!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/4 ms
DlteC-FW-GW#

```

Portanto, com o comando acima definimos uma repetição de 10 vezes e alteramos a origem do pacote para 192.168.1.1. Tudo isso pode ser feito das duas maneiras, pela linha de comando ou com o ping estendido digitando apenas o comando "ping".

#### 4.2 Utilizando o Traceroute

Com os testes de ping podemos chegar a conclusão que ele pode ajudar um analista de suporte a isolar determinado problema, porém se o ping entre o roteador onde o computador do usuário estivesse acessível e os testes de ping através dele e do roteador padrão da rede onde o computador pertence não funcionassem?

Poderíamos fazer pings sucessivos levando em conta a topologia de rede para ver onde o pacote está parando, ou então utilizar o traceroute, o qual testa a comunicação ponto a ponto (a cada salto), ao invés de fim a fim como o ping.

Com o traceroute podemos testar o caminho que o pacote percorre até chegar ao destino, portanto poderíamos nesse exemplo saber até que roteador o pacote está indo e continuar o troubleshooting a partir desse ponto.

Lembre-se do capítulo 5 que o traceroute funciona com o envio de pacotes com valores de TTLs incrementados a cada salto, fazendo com que os pacotes tenham seu tempo de vida expirado nos roteadores e assim com o envio da mensagem de tempo de vida excedido o roteador local pode mostrar os IPs de cada salto até o destino.

O comando traceroute é utilizado pelo Cisco IOS, Linux e MAC OS-X, no Windows temos os comando tracert e pathping.

Veja exemplo de traceroute a seguir.

```

R1# traceroute 192.168.2.10
Type escape sequence to abort.
Tracing the route to 172.16.2.101
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.4.2 0 msec 0 msec 0 msec
2 192.168.2.10 0 msec 0 msec *

```

No primeiro exemplo o traceroute mostrou que para o computador 192.168.2.10 está a dois saltos, veja que os índices 1 e 2 na frente representam os saltos dados.

Podemos também utilizar a opção estendida como utilizamos para o ping, veja exemplo a seguir.

```
R1# traceroute
Protocol [ip]:
Target IP address: 192.168.2.10
Source address: 192.168.1.1
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 172.16.2.101
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.4.2 0 msec 0 msec 0 msec
2 192.168.2.10 0 msec 0 msec *
```

No exemplo acima alteramos o endereço de origem padrão definindo o IP 192.168.1.1 como origem dos pacotes IP gerados para o teste de traceroute. A mesma recomendação sobre a origem que o roteador utiliza para o ping vale também para o traceroute.

Um detalhe importante sobre o traceroute gerado pelo Cisco IOS é que ele utiliza **pacotes IP com um cabeçalho UDP** para realização dos testes, por isso se o firewall bloquear tráfego UDP o traceroute não terá sucesso, mesmo que a mensagem de TTL expirado esteja liberada.

Maioria dos demais sistemas operacionais utilizam pacotes IP puros com mensagens de solicitação de Echo para realizar o teste de traceroute ao invés de datagramas UDP.

Quando o tracerout não para de exibir asteriscos ou caracteres de erro, com a sequência de teclas "Control+Shift+6" permite que você suspenda o comando. A mesma sequência pode ser utilizada para interromper o ping e resoluções de nome.

#### 4.3 Utilizando o Telnet e SSH

O telnet pode ser utilizado pelos administradores de rede e analistas de suporte para configurar e realizar testes de diagnósticos remotos em dispositivos de rede.

Em termos de testes, se um dispositivo de rede permitir conexão telnet com o endereço de uma de suas subredes é sinal que todas as camadas do modelo OSI estão funcionando perfeitamente, pois o telnet é uma aplicação de rede e para que ele responda todas as camadas devem estar operacionais.

Um recurso não muito explorado do telnet no Cisco IOS é a suspensão de sessões ou "suspend feature". Esse recurso permite que de apenas um dispositivo possamos gerenciar vários roteadores e switches via telnet ou ssh sem a necessidade de abrir uma tela para cada um deles.

Podemos suspender uma sessão e voltar ao roteador que originou as conexões teclando "**Control+Shift+6**" simultaneamente e depois apertando a tecla **X** (soltando as teclas anteriores e depois teclando o x). Com essa sequência de teclas voltamos ao roteador que originou a conexão e fazer telnet para outro dispositivo, podendo sair de um equipamento para outro com apenas uma tecla, veja exemplo a seguir.

```
DlteC-FW-GW>en
Password:
DlteC-FW-GW#ssh 192.168.1.5
```

Password:

```
SW-DlteC> → aqui foi pressionado a sequência para suspender a sessão
DlteC-FW-GW#sho sessions
Conn Host Address Byte Idle Conn Name
* 1 192.168.1.5 192.168.1.5 0 0 192.168.1.5
```

```
DlteC-FW-GW# → pressionando entra voltamos à sessão
[Resuming connection 1 to 192.168.1.5 ... ]
```

```
SW-DlteC>show users
Line User Host(s) Idle Location
* 1 vty 0 dltec idle 00:00:00 192.168.1.1

Interface User Mode Idle Peer Address
SW-DlteC>who
Line User Host(s) Idle Location
* 1 vty 0 dltec idle 00:00:00 192.168.1.1

Interface User Mode Idle Peer Address
```

```
SW-DlteC> → sessão suspensa mais uma vez
DlteC-FW-GW#where
```

```
Conn Host Address Byte Idle Conn Name
* 1 192.168.1.5 192.168.1.5 0 0 192.168.1.5
```

```
DlteC-FW-GW#sho sessions
Conn Host Address Byte Idle Conn Name
* 1 192.168.1.5 192.168.1.5 0 0 192.168.1.5
```

```
DlteC-FW-GW#disconnect 1
Closing connection to 192.168.1.5 [confirm]
DlteC-FW-GW#
```

Começando com as linhas destacadas em amarelo, do switch com hostname SW-DlteC fizemos uma conexão via SSH com o roteador de IP 192.168.1.1 e hostname DlteC-FW. Na sequência suspendemos a sessão com a sequência de teclas “**Ctrl+Shft+6 seguido do X**”, voltando ao switch e realizamos o comando “**show sessions**”.

Esse comando mostrou que nosso switch tem uma conexão identificada com o número “1” com o roteador. Digitando entra podemos voltar (**resume**) à sessão SSH, no caso de estarem abertas várias sessões é possível com o comando “**resume**” e o número da sessão escolher para que dispositivos vamos retornar a sessão.

Em verde temos o comando “**show users**” e “**who**”, os quais mostram os usuários que estão conectados remotamente ou localmente aos nossos dispositivos. Note que o usuário dltec está conectado à vty 1.

Em cinza voltamos mais uma vez a suspender a sessão para voltar ao switch e verificar as conexões realizadas com um comando igual ao **show sessions** chamado **where**, os dois mostram as mesmas informações.

No final, em azul desconectamos a sessão inicial ao roteador com o comando “**disconnect 1**”.

#### 4.3.1 Testando Servidores e Serviços com Telnet

Um uso interessante do Telnet que não é foco do CCNA ou CCENT, porém é bem útil para testes práticos e simulações onde queremos ver pacotes sendo trocados através de sniffer é simular conexões à portas de servidores via o comando telnet, isso mesmo, você pode fazer um telnet para a porta 80 para testar a conexão HTTP ou para a porta 25 para testar a conexão com um servidor SNMP.

Veja exemplo abaixo onde vamos utilizar no switch (endereço 192.168.1.5) o comando “**telnet 192.168.1.1 www**” para abrir uma conexão HTTP com o roteador e no roteador vamos utilizar o comando “**show tcp brief**” para verificar as conexões TCP abertas, similar ao netstat que utilizamos nos computadores.

```
SW-DlteC#telnet 192.168.1.1 www
Trying 192.168.1.1, 80 ... Open
```

```
DlteC-FW-GW#sho tcp brief
TCB      Local Address          Foreign Address        (state)
696EE480 192.168.2.1.2000      192.168.1.23.49411 ESTAB
697A0068 192.168.1.1.80        192.168.1.5.53921 ESTAB
679504C4 192.168.2.1.2000      192.168.2.20.44232 ESTAB
6975474C 192.168.1.1.22        192.168.1.22.65474 ESTAB
DlteC-FW-GW#
```

No final com um “Control+C” digitado no switch podemos sair e finalizar o teste. Veja na sequência o segundo teste para a porta 443 referente ao HTTPS realizada a partir do switch em direção ao roteador.

```
SW-DlteC#telnet 192.168.1.1 443
Trying 192.168.1.1, 443 ... Open
```

```
DlteC-FW-GW#sho tcp brief
TCB      Local Address          Foreign Address        (state)
696EE480 192.168.2.1.2000      192.168.1.23.49411 ESTAB
679504C4 192.168.2.1.2000      192.168.2.20.44232 ESTAB
6975474C 192.168.1.1.22        192.168.1.22.65474 ESTAB
697B3814 192.168.1.1.443       192.168.1.5.24360 ESTAB
DlteC-FW-GW#
```

Ambos os serviços foram ativados no roteador com os comandos abaixo:

```
SW-DlteC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-DlteC(config)#ip http server
SW-DlteC(config)#ip http secure-server
SW-DlteC(config)#ip http authentication local
SW-DlteC(config)#
```

Os serviços de HTTP e HTTPS nos roteadores e switches na prática geralmente são desabilitados, porém você pode utilizar para realizar testes de camada 7, principalmente quando estudarmos as listas de controle de acesso no próximo capítulo.

Para desabilitar os serviços basta colocar “no” no começo dos dois primeiros comandos, veja abaixo.

```
SW-DlteC(config)#no ip http server
SW-DlteC(config)#no ip http secure-server
```

## 5 Resumo do Capítulo

Bem pessoal, chegamos ao final de mais um capítulo!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Entender o funcionamento básico de um protocolo de roteamento dinâmico.
- Entender as diferenças entre os tipos de algoritmos de protocolos de roteamento.
- Entender as características gerais dos IGP e EGP.
- Diferenciar a métrica da distância administrativa.
- Entender o funcionamento de um protocolo vetor de distância.
- Entender o funcionamento do RIP.
- Ser capaz de configurar topologias com RIP versão 2.
- Ser capaz de realizar troubleshooting básico em uma rede com RIP versão 2.
- Ser capaz de testar uma topologia de rede utilizando ping, trace e telnet.

*Nesse capítulo estudaremos maneiras de reforçar a segurança de roteadores e switches, muitas delas já até estudadas e implementadas.*

*Também estudaremos como planejar, elaborar e implementar listas de controles de acesso em roteadores Cisco.*

*No CCENT o principal foco das ACLs é como filtro de pacotes, ou seja, para criar filtros básicos para limitar acesso a redes, hosts ou serviços.*

*Aproveite o capítulo e bons estudos!*

## **Capítulo 10 - Reforçando a Segurança nos Dispositivos e Listas de Controle de Acesso**

### **Objetivos do Capítulo**

Ao final desse capítulo você terá estudado e deverá compreender:

- Implementar comandos e recursos para reforçar a segurança de roteadores e switches Cisco.
- Entender a função e princípio de operação das listas de controle de acesso.
- Planejar e configurar listas de controle de acessos padrões e estendidas.
- Fazer adições, alterações e remoção de comandos em ACLs numeradas e nomeadas.
- Implementar ACLs para limitar acesso telnet e SSH em roteadores e switches Cisco.

## Sumário do Capítulo

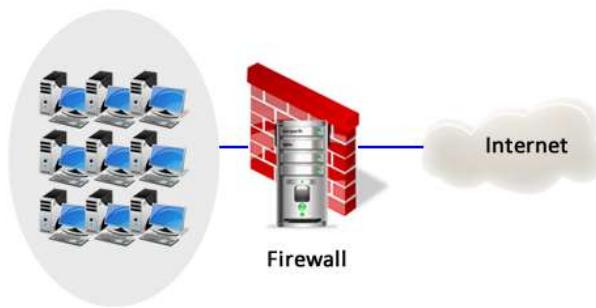
<b>1 Introdução aos Firewalls e Filtragem de Pacotes</b>	<b>404</b>	
1.1 DMZ – Zona Desmilitarizada	407	
<b>2 Recomendações antes de Iniciar o Estudo de ACLs</b>	<b>408</b>	
<b>3 Listas de Controle de Acesso - ACL</b>	<b>409</b>	
3.1 Entendendo e Criando as Regras de Filtragem de Pacotes	411	
3.2 ACL IP Padrão Numerada	414	
3.2.1 Máscara curinga para selecionar redes classful	415	
3.2.2 Selecionando apenas um Host	415	
3.2.3 Selecionando Todas as Redes	415	
3.2.4 Selecionando Sub-redes	415	
3.2.5 Selecionando Faixas de IPs Aleatórios	416	
3.3 ACL IP Estendida Numerada	418	
3.4 Exemplo de ACL Estendida	419	
3.5 Verificando ACL com Comandos Show	420	
3.6 Listas de Acesso Nomeadas	422	
3.7 Aplicando ACLs às Interfaces	424	
3.8 Limitando Acesso às Lines VTY (Telnet e SSH)	425	
3.9 Agora Vamos a Alguns Exemplos	426	
3.9.1 Exemplo 1 – ACL Padrão	426	
3.9.2 Exemplo 2 – ACL Estendida	426	
3.9.3 Exemplo 3 – ACL Nomeada Estendida	427	
3.10 Editando ACLs Numeradas	428	
3.11 Editando ACLs Nomeadas	429	
3.12 Recomendações Gerais sobre Configuração de ACLs	430	
<b>4 Reforçando a Segurança em Roteadores e Switches Cisco</b>	<b>431</b>	
4.1 Senhas de Acesso	431	
4.2 Desabilitando Serviços e Portas não Utilizadas	431	
<b>4.3 Limitando Acesso Telnet e SSH via ACL</b>	<b>433</b>	
<b>4.4 Ativando o Protocolo NTP – Network Time Protocol</b>	<b>433</b>	
4.4.1 Configurando o Roteador como Cliente NTP	434	
4.4.2 Configurando o Roteador como Mestre NTP (Servidor)	436	
<b>5 Resumo do Capítulo</b>	<b>437</b>	

## 1 Introdução aos Firewalls e Filtragem de Pacotes

Antes de iniciarmos o próximo assunto, o qual trata da lista de controle de acesso ou ACL, vamos analisar o que é um Firewall. Apesar do assunto não ser parte do CCENT é importante para um profissional de redes entenderem o papel de um firewall na rede e a relação de uma ACL com um firewall completo. A configuração de firewall completa é vista no CCNA e CCNP Security.

Os Firewalls podem ter variadas conotações para diferentes pessoas e organizações, mas todos os firewalls compartilham algumas propriedades comuns (veja figura abaixo):

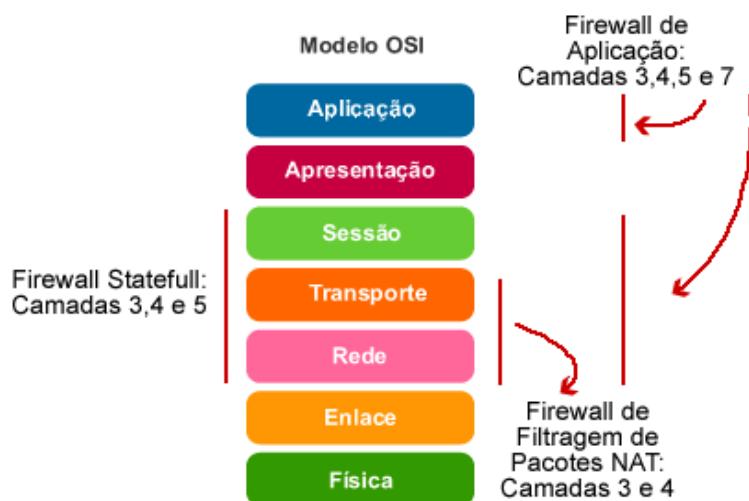
- Devem ser resistente a ataques
- Todos os fluxos de tráfego da Internet ou redes consideradas inseguras passam através do firewall (ponto único de acesso)
- Reforça a política de controle de acesso à rede (seja de dentro para fora como de fora para dentro)



As principais vantagens no uso do firewall em uma rede são a de prevenir a exposição de hosts/aplicações sensíveis para usuários/redes não confiáveis e manter o fluxo dos protocolos “higienizado”, impedindo a exploração das falhas mais conhecidas dos protocolos, normalmente exploradas no início dos ataques.

Porém, os firewalls também têm algumas limitações, sendo que a principal é que se mal configurado ele pode trazer consequências graves e se tornar um ponto único de falha – SPOF – Single Point Of Failure, ou seja, pode parar toda a rede em caso de problemas. Outro ponto importante é que sozinho o firewall não consegue garantir que todos os tipos de ataque sejam bloqueados, por isso recomenda-se o uso do firewall com outros recursos de segurança como IPS e IDS.

Existem diversas classificações e nomenclaturas para os diferentes tipos de firewalls, veja na figura a seguir os tipos de firewall em relação ao modelo de referência OSI sobre sua capacidade de filtragem por camada. Veja a figura abaixo.



De maneira geral os firewalls são classificados nos seguintes tipos:

- **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. Este é o foco das ACLs no CCENT, ou seja, a filtragem de pacotes.
- **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 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 – Estabelecido/Established – ACK)

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.

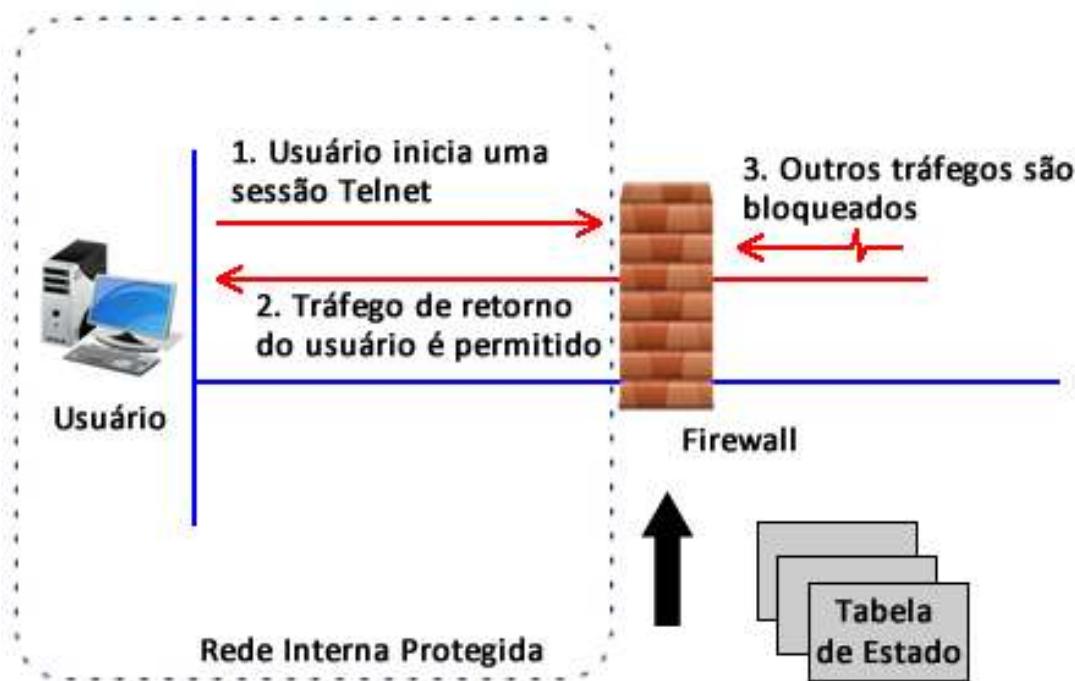
No quadro abaixo temos um exemplo de regra de firewall com filtragem de pacotes:

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

Vamos analisar, por exemplo, 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.

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". Veja a figura abaixo.



### 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. Veja a figura abaixo.



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 essa ameaça fica restrita à DMZ e não passa para a rede interna da empresa.

## 2 Recomendações antes de Iniciar o Estudo de ACLs

As listas de acesso são filtros de pacotes que se baseiam no fluxo de pacotes IP e aplicações TCP ou UDP, portanto se você tem dúvidas sobre como o fluxo de informações, formação de quadros e envio de pacotes na rede é realizado, recomendamos voltar até o capítulo 5 para dar uma revisada.

É importante também saber as portas TCP e UDP dos principais serviços de rede, tais como:

- Acesso web: HTTP e HTTPS.
- Acesso a arquivos: FTP e TFTP.
- Serviço de nomes de Domínio: DNS.
- Serviço de e-mail: SMTP, POP3 e IMAP.
- Monitoração de rede: SNMP e Syslog.
- Acesso remoto: Telnet e SSH.
- Alocação dinâmica de IPs: DHCP.
- Voz e vídeo sobre IP: protocolo RTP (Real Time Protocol – portas de 16,384 a 32,767)

Podem ser cobrados outros serviços? Sim, porém os citados acima são os mais comuns.

Além disso, é importante lembrar que as portas utilizadas pelos clientes utilizam a faixa dinâmica de portas TCP e UDP de 49152 a 65535.

Veja tabela a seguir com os principais números de portas citados anteriormente.

Número da Porta	Protocolo	Serviço de Rede	Mnemônico
20	TCP	FTP dados	ftp-data
21	TCP	FTP controle	ftp
22	TCP	SSH	—
23	TCP	Telnet	telnet
25	TCP	SMTP	smtp
53	UDP, TCP	DNS	domain
67, 68	UDP	DHCP	nameserver
69	UDP	TFTP	tftp
80	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	snmp
443	TCP	SSL	—
16,384 – 32,767	UDP	RTP (VoIP– video)	—

### 3 Listas de Controle de Acesso - ACL

Uma Lista de Controle de Acesso ou “**Access Control List**” (**ACL**) é um conjunto de instruções que diz ao roteador para aceitar (permit ou permitir) ou rejeitar (deny ou negar) determinados pacotes vindos de redes IP especificadas.

Esse filtro pode atuar até na camada-4, onde é possível especificar portas TCP ou UDP que você deseja filtrar, selecionando assim quais aplicações podem ser acessadas na rede interna e quais podem acessar a rede externa.

Uma ACL pode ser utilizada como um “Firewall”, fornecendo recursos de filtragem básicos, podendo ser aplicada como uma barreira de proteção com a finalidade de controlar o tráfego de dados entre sua rede interna e a Internet.

Essas listas devem ser criadas em **modo de configuração global**, como uma sequência de regras ou statements e, em seguida, aplicadas em uma interface LAN, WAN ou em dentro da line VTY, para limitar acesso ao Telnet e SSH, conforme estudado no capítulo anterior.

Existem duas maneiras de criar uma ACL:

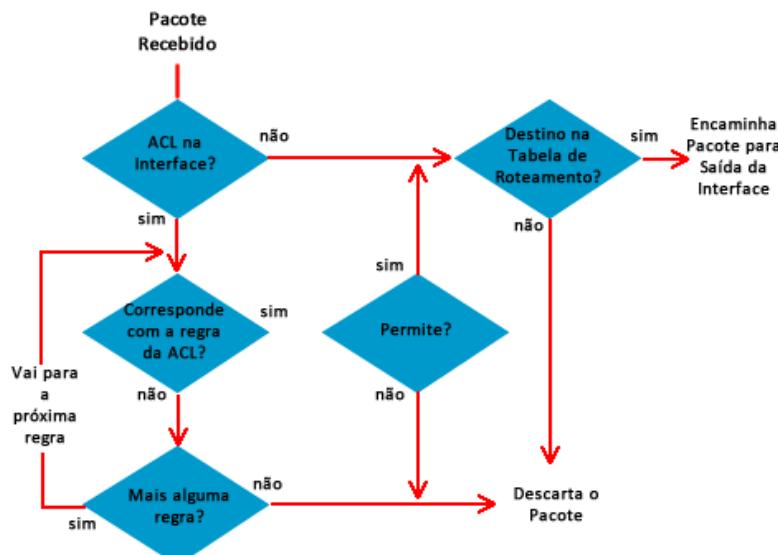
1. **ACL Numerada**: as quais podem ser **padrão** ou **estendida**.
2. **ACL Nomeada**: também podem ser padrão (**standard**) ou estendidas (**extended**).

Uma **ACL IP padrão** pode filtrar o tráfego apenas baseado em pacotes IP através do endereço ou rede de origem, tanto na forma nomeada quanto na numerada.

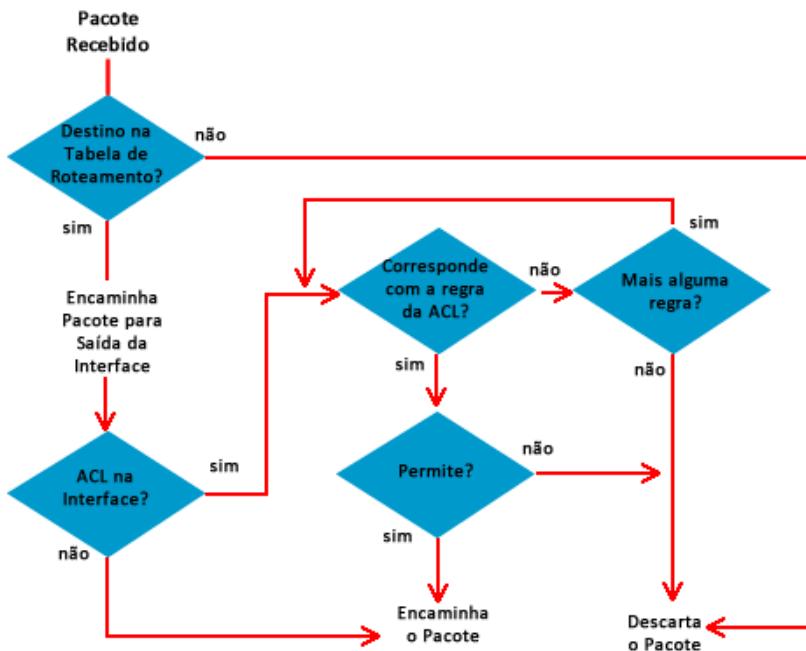
Para a **ACL IP estendida** o administrador de redes tem uma gama maior de opções de filtragem, como pacotes IP através do endereço de origem e destino, protocolos TCP e UDP, protocolo ICMP, outros protocolos como RIP, OSPF, EIGRP, GRE, pelo estado das conexões das portas TCP, etc.

Nas figuras 1 e 2 você pode verificar como um pacote é processado quando o roteador tem uma lista de acesso aplicada. As listas são aplicadas nas interfaces em duas possíveis direções:

1. In: tráfego entrante



## 2. Out: tráfego de saída do roteador.



Note que para a ACL colocada na direção de entrada da Interface ou Inbound (In), a ACL é processada antes do pacote ser roteado, ou seja, somente se ele for permitido pela ACL que o roteador fará o processo de roteamento.

Já para a direção de saída ou outbound (Out), o pacote já passou pelo processo de roteamento e após isso será processado pela ACL.

Além disso, você pode notar em ambos os diagramas que sempre no final, se você não criar uma regra com permissão o pacote será descartado, pois existe uma **negação implícita no final de toda lista de acesso**, ou seja, um “**deny any**” negando todos os pacotes. Portanto para as regras funcionarem deve existir no mínimo uma permissão ou então nenhum pacote será encaminhado.

### Resumindo:

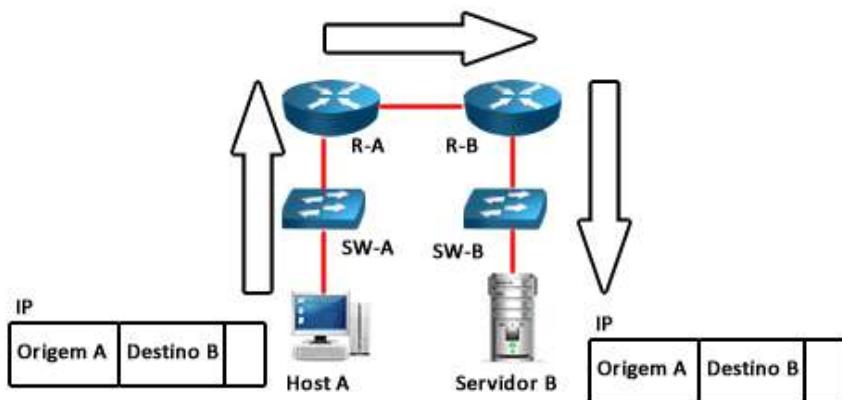
1. ACL é um conjunto de regras de teste que se satisfeitos deixarão o pacote ser encaminhado ou filtrarão o pacote;
2. Pode ser uma lista padrão, analisando apenas a rede IP de origem do pacote e decidindo se aquele pacote vai ou não ser encaminhado;
3. Caso haja necessidade de maior granularidade, ou seja, filtrar utilizando outros parâmetros como: rede de destino, tipo de protocolo, porta TCP ou UDP, estado da conexão, uma lista de acesso estendida deve ser utilizada;
4. As listas podem ser numeradas (1 a 99 – ACL IP Padrão / 100 a 199 – ACL IP estendida) ou nomeadas, as quais não tem limitação de listas por utilizarem nomes;
5. As ACLs podem ser aplicadas nas Interfaces de LAN e WAN ou na linha de Telnet (VTY) dos roteadores e switches em duas direções: Entrada (In) e Saída (Out);
6. Devem ser criadas em modo de config global e aplicadas nas Interfaces ou Lines;
7. Os pacotes serão processados um a um, regra a regra, caso atenda a uma regra ele será permitido ou negado, caso não atenda passará para o próximo teste até o final das regras.

### 3.1 Entendendo e Criando as Regras de Filtragem de Pacotes

Para entender e criar uma lista de acesso você deve entender como um pacote é formado e enviado na rede, uma sugestão caso haja dúvidas é revisar o capítulo 5 sobre os protocolos IP, UDP e TCP.

Basicamente em uma rede IP quando um micro deseja conversar com outro fora da sua rede, esse pacote atravessa a rede e o endereço ou rede IP de origem será a do micro que originou a comunicação. Já a rede IP de destino será a rede onde o IP do computador remoto está.

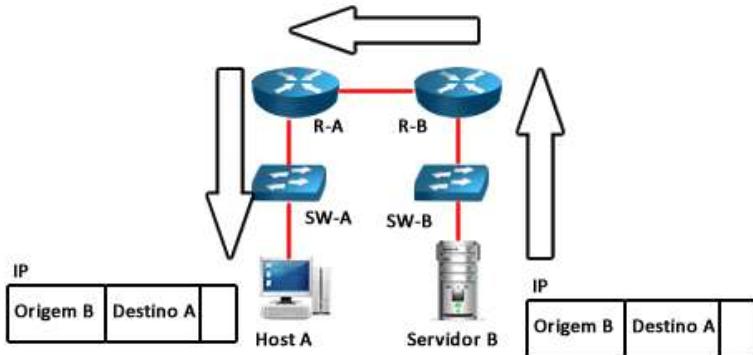
Na figura o **micro da rede A** deseja **acessar** uma página de Web do **servidor** que está **na rede B**. Portanto a rede de origem é a rede do micro A e a de destino a rede do Servidor B.



Agora vamos analisar o caminho de volta, quando o **servidor B responde a requisição do micro A**, agora ele será a origem da comunicação e o micro A será o destino.

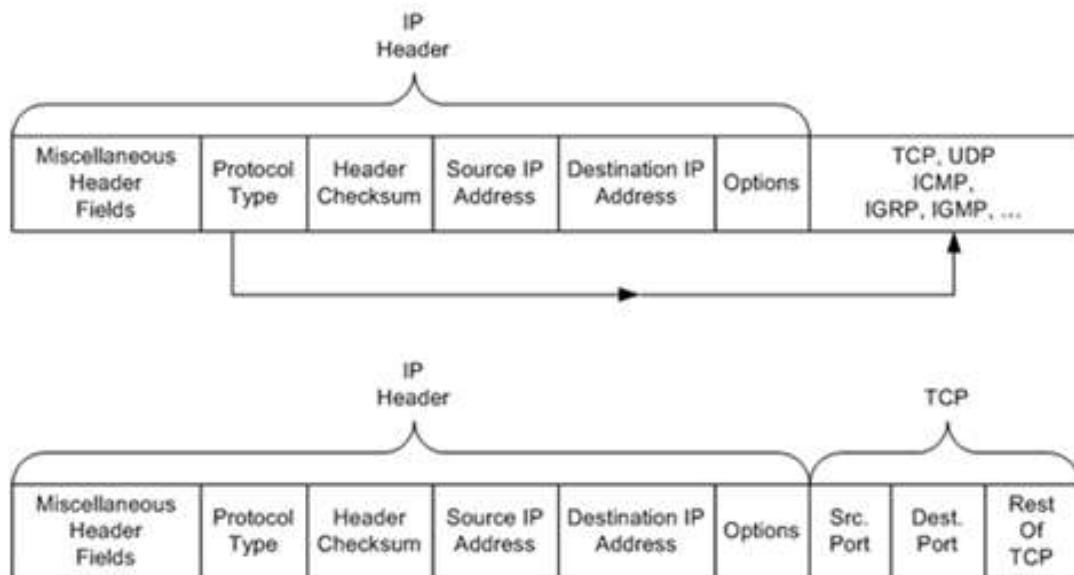
Para ACL padrão somente esse dado importa, quem é a rede IP de origem.

Utilizando a figura ao lado, você poderia criar uma regra para bloquear pacotes IP para o servidor que venham de uma determinada rede de origem, porém não pode especificar para que serviço ele esteja sendo bloqueado, porque a ACL padrão não tem essa granularidade. Ou a rede inteira ou parte dela passa ou é bloqueada.



Para a ACL estendida a regra do jogo muda bastante, pois ela pode ir além do endereço de origem, portanto você pode ir mais fundo na sua filtragem. A ACL estendida chega até a camada 4 do modelo OSI, ou seja, a camada de transporte, podendo filtrar portas TCP e UDP, consequentemente filtrando as aplicações que passam por aquela interface.

Agora veja a figura ao lado para termos um entendimento melhor do que a ACL estendida é capaz.



Você agora pode **filtrar pelas redes IP de origem e destino**, mais os **protocolos de camada 3 e 4** suportados pelos roteadores, como ICMP, IGMP, TCP, UDP e outros.

Lembrem que as **portas** TCP e UDP representam os diversos serviços de redes que os aplicativos das camadas superiores ou aplicações podem utilizar. Aqui temos uma arquitetura cliente/servidor, onde o servidor normalmente tem uma porta bem conhecida e o cliente utiliza uma porta aleatória que inicia acima de um valor padrão, conforme estudado no capítulo 5. Na continuação do curso veremos como criar as regras utilizando cada tipo de lista de acesso.

No exemplo mostrado anteriormente, o micro A formaria um pacote com o IP do Servidor B e a porta TCP com destino 80, pois é a porta padrão do protocolo Web HTTP. A porta de origem do micro depende do sistema operacional que ele está usando, mas normalmente é uma porta acima de 1024.

Quando o servidor responder ele colocará sua porta de origem 80 e a porta de destino com o número da porta que ele recebeu originalmente do computador A.

Vale também lembrar que o TCP é orientado a conexão e faz um processo de handshake triplo para inicializar a conexão. Nesse processo ele inicia enviando o SYN setado em 1 e o Ack (reconhecimento) em "0". Nas ACLs existe um operando ou opção que identifica conexões estabelecidas, ao contrário do que aconteceu anteriormente com o ACK igual a 1 (established).

Para o protocolo UDP não existe esta opção, pois ele não tem conexão, ele sempre está pronto para receber e enviar, conforme as aplicações necessitarem.

Se um exercício pedir para você filtrar a comunicação do Telnet com a rede LAN do servidor, conforme ilustrado na figura anterior, você teria que determinar:

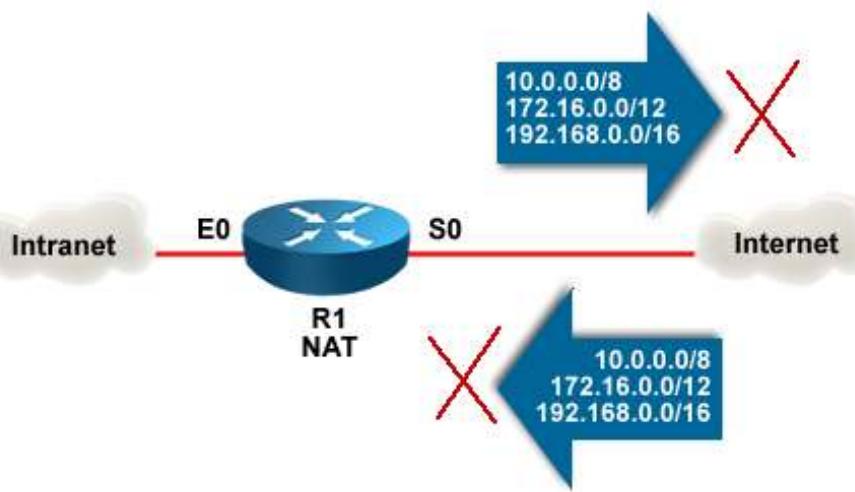
- Rede de origem e sua máscara
- Rede de destino e sua máscara (a rede da sua LAN)

- Pelo protocolo: qual a porta utilizada e se ela é TCP ou UDP
- Nesse caso a porta de destino é a 23 do protocolo TCP
- Como são clientes se conectando as portas de origem são variáveis

Tenha em mente que, quando vamos criar uma ACL estamos criando “regras de firewall” e precisamos pensar nos seguintes pontos:

- Quais protocolos queremos permitir que entrem na rede local?
- Quais protocolos podem sair da rede local em direção à Internet ou outras redes remotas?
- Quais redes, sub-redes ou endereços IP queremos limitar acesso além do que definimos como regra geral?
- Quais redes, sub-redes ou endereços IP queremos dar acesso extra além do que definimos como regra geral?

Por exemplo, sabemos que as redes privativas conforme RFC 1918 não devem nem acessar a Internet, assim como não deveriam vir a partir da Internet em direção à nossa Intranet requisições com esses IPs, pois eles são proibidos de trafegar na rede pública. Veja a figura abaixo.



Portanto uma regra a ser aplicada no roteador R1 seria bloquear tanto a saída de pacotes da rede de origem conforme RFC 1918 na entrada de sua serial 0, a qual está conectada à Internet, assim como bloquear a saída de pacotes com IPs conforme RFC 1918 de sua rede Interna em direção à Internet, garantindo que se algum pacote passou sem a tradução do NAT não seja encaminhado para a Internet, pois isso poderia ser um tipo de ataque sendo realizado por usuários da Intranet em direção à Internet.

Na sequência aprenderemos a **traduzir** essa regra em **comandos de ACL**.

### 3.2 ACL IP Padrão Numerada

O início da configuração de uma ACL numerada padrão e estendida é o mesmo, ou seja, você entra em modo de configuração global, digita o comando “**access-list**”, escolhe o número da ACL e inclui o parâmetro “**permit**” (permitir) ou “**deny**” (negar), conforme mostrado abaixo.

```
Router(config)#access-list 1 ?
  deny   Specify packets to reject
  permit  Specify packets to forward
```

A numeração de uma ACL IP Padrão vai de 1-99 e de 1300-1999 (faixa adicional). O “deny” especifica pacotes a serem rejeitados e o “permit” os que serão encaminhados.

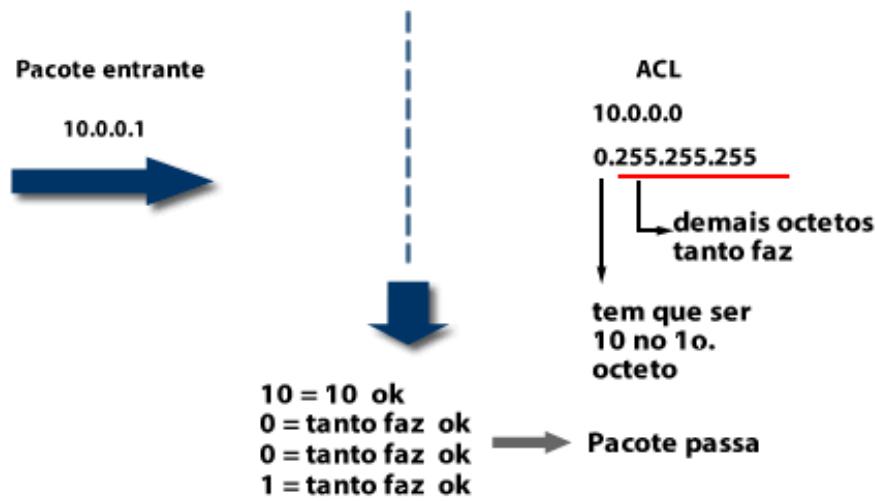
Na configuração de uma ACL IP padrão, depois de definido se você vai permitir ou negar um pacote você deverá entrar com o IP ou rede de origem e a máscara curinga. Veja a seguir um exemplo onde o tráfego originado da rede 10.0.0.0/8 é permitido.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255
```

Note que a **máscara curinga** é formada, assim como a máscara de rede, por quatro octetos de oito bits, sendo que bit 0 na máscara curinga significa que deve haver correspondência e o bit 1 significa que você pode ignorar a correspondência entre o pacote a ser testado e a rede configurada na ACL.

Um octeto com oito bits zeros significa que o octeto correspondente no endereço deve ser exatamente igual ao informado na ACL.

Já um octeto com oito bits 1 (.255) significa que quaisquer valores são aceitos para aquela entrada.



Portanto a dupla - **rede e máscara curinga** - definem o range de IPs que serão testados na ACL. A seguir seguem alguns macetes para calcular a máscara curinga.

### 3.2.1 Máscara curinga para selecionar redes classful

Redes classful são simples de serem selecionadas com a máscara curinga, basta inverter a máscara de sub-rede, veja abaixo a seleção da rede 10.0.0.0/8.

- **Classe A – “10.0.0.0 0.255.255.255”**

Em uma rede classe A o primeiro octeto é utilizado para a rede e os demais para o host, sendo assim somente o primeiro octeto tem que ser testado para garantir que a rede selecionada seja classe A, os demais octetos podem ser ignorados. Esse mesmo princípio pode ser utilizado para as classes B e C, veja abaixo.

- **Classe B – “130.0.0.0 0.0.255.255”**

- **Classe C – “200.200.100.0 0.0.0.255”**

### 3.2.2 Selecionando apenas um Host

Máscara curinga para apenas um endereço é “**192.168.1.1 0.0.0.0**” ou o mnemônico “**host**” seguido do endereço, por exemplo, “**host 192.168.1.1**”.

Lembre que um octeto inteiro “0” significa que você deve testar todos os bits, por isso todos os octetos mandam testar todos os bits. Isso faz muito sentido porque para criar uma rota para um host específico utilizamos a máscara /32, em máscara curinga ela vira /0, onde tem um passamos a utilizar zero!

Exemplo para permitir o micro 10.1.2.21:

```
Router(config)#access-list 1 permit 10.1.2.21 0.0.0.0
```

ou

```
Router(config)#access-list 1 permit host 10.1.2.21
```

### 3.2.3 Selecionando Todas as Redes

Máscara curinga para permitir ou bloquear quaisquer redes (todas as redes) é “**0.0.0.0 255.255.255.255**” ou o mnemônico “**any**”. Exemplo:

```
Router(config)#access-list 1 permit any
```

ou

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
```

Fazendo a mesma análise anterior, para criar uma rota para a Internet utilizamos a rede 0.0.0.0/0, portanto em máscara curinga é 0.0.0.0 255.255.255.255, pois onde temos zero na máscara de rede vira um na máscara curinga.

### 3.2.4 Selecionando Sub-redes

Para selecionar sub-redes diminua a **255.255.255.255** (/32) da máscara de sub-rede que você está trabalhando. Por exemplo, selecione somente a subnet zero da rede 10.0.0.0/28 para ser permitida na ACL padrão 1:

– 255.255.255.255

255.255.255.240

0 . 0 . 0 . 15

Portanto a rede e a máscara curinga são: "10.0.0.0 0.0.0.15"

```
Router(config)#Access-list 1 permit 10.0.0.0 0.0.0.15
```

Note que os três primeiros octetos devem ser iguais e o último octeto é 15 em decimal, ou seja, 00001111 em binário. Se você fizer a variação de 15 em binário você terá:

- 00000000 – 0
- 00000001 – 1
- 00000010 – 2
- ...
- 00001110 – 14
- 00001111 – 15

Portanto você terá dos IPs 10.0.0.0, 0+1, 0+2,..., 0+14 até 0+15.

Agora vamos ao calcular para permitir a terceira sub-rede válida considerando a rede 10.0.0.0 com uma máscara /27 (255.255.255.224):

\_ 255.255.255.255  
255.255.255.224  
0. 0 . 0 . 31

O cálculo para obter a máscara curinga continua a mesma, porém a rede agora será: "10.0.0.96 0.0.0.31", pois o range inicia em 10.0.0.96 (terceira sub-rede válida).

```
Router(config)#Access-list 1 permit 10.0.0.96 0.0.0.31
```

Note que os três primeiros octetos devem ser iguais e o último octeto é 31 em decimal, ou seja, 00011111 em binário. Se você fizer a variação de 31 em binário você terá:

- 00000000 – 0
- 00000001 – 1
- 00000010 – 2
- 00000011 – 3
- 00000100 – 4
- ...
- 00011110 – 30
- 00011111 – 31

Portanto você terá dos IPs 10.0.0.96, 96+1, 96+2,..., 96+30 até 96+31. Ou seja, dos IPs 10.0.0.96 até 10.0.0.127. A próxima sub-rede começa em 10.0.0.128/27.

Para exemplos de seleção de sub-redes inteiras podemos fazer uma análise reversa bem simples das sub-redes selecionadas em uma ACL somando os octetos que são diferentes de zero ou um na máscara, por exemplo, no cálculo anterior temos "Access-list 1 permit 10.0.0.96 0.0.0.31", quais IPs estão permitidos? Vão de 10.0.0.96 até 10.0.0.(96+31) = 10.0.0. 127, ou seja, a faixa de IPs dessa sub-rede.

### 3.2.5 Selecionando Faixas de IPs Aleatórios

Para selecionar um range de IPs ou redes, não importando a sub-rede que ele esteja, você deverá lembrar que a seleção pode ser feita mais facilmente por **blocos de IP**.

Os blocos podem ter tamanho de 4, 8, 16, 32, 64 ou 128 endereços selecionando 2 bits, 3 bits, 4 bits, 5 bits, 6 bits ou 7 bits da máscara curinga respectivamente. Para blocos com 4 IPs você poderá ter os IPs ou redes de 0 a 3, 4 a 7, 8 a 11 e assim por diante.

Outro exemplo, para blocos com 32 IPs você terá ranges de IP ou rede variando de 0 a 31, 32 a 63, 64 a 95 e assim por diante.

Nem sempre é possível selecionar exatamente os endereços em uma faixa que queremos, por exemplo, se tentarmos selecionar de 10.0.0.20 a 10.0.0.30 não será possível em apenas uma linha de comando, porque essa faixa não fica dentro de uma variação sequencial em binário, veja abaixo.

```
10.0.0.00010100
10.0.0.00010101
10.0.0.00010110
10.0.0.00010111
10.0.0.00011000
10.0.0.00011001
10.0.0.00011010
10.0.0.00011011
10.0.0.00011100
10.0.0.00011101
10.0.0.00011110
```

Poderíamos nesse exemplo fazer uma linha de 20 a 23 "10.0.0.20 0.0.0.3", depois de 24 a 27 "10.0.0.24 0.0.0.3", uma para o 28 e 29 "10.0.0.28 0.0.0.1" e mais uma linha separada para o 30 "host 10.0.0.30".

Estas análises mais complexas não são foco do CCENT, porém não retiramos do nosso material para que os alunos que realmente desejam entender o assunto tenham como ir além do trivial cobrado no exame.

Vamos a outro exemplo para calcular a máscara curinga para permitir que as redes de 200.200.1.0 a 200.200.7.0 sejam negadas em uma ACL. As redes de 1 a 7 estão no bloco 8 IPs (de 0 a 7), escolhendo blocos de 4 bits a ACL será a:

```
Router(config)#Access-list 51 deny 200.200.0.0 0.0.7.255
```

Ora maneira de calcular faixas de IP é fazendo o seguinte, por exemplo, o exercício pede para você calcular uma máscara curinga que selecione as redes **172.16.32.0** a **172.16.63.0** com a máscara de sub-rede /24. Os octetos 172 e 16 nunca irão variar, portanto você colocará "**0.0.**" para esses dois octetos. O octeto 0 na máscara de sub-rede pode variar de 0 a 255, pois são os endereços de host possíveis dessa rede com máscara /24, portanto no último octeto temos ".255". Agora basta calcular o range de 32 a 63, conforme esquema abaixo:

```
172.16.32.0
172.16.63.0
0 . 0 . ? .255
```

Onde o range está indeterminado siga os seguintes passos:

- converta o 32 em binário
- converta o 63 em binário
- compare os números em binário, onde for igual fica 0 e diferente fica 1:  
32 -> 00100000  
63 -> 00111111  
31 -> 00011111

É o mesmo que diminuir 32 de 63, agora você deverá escolher o método que melhor se adapte a sua forma de estudo e guardar o conteúdo.

A máscara curinga é 0.0.31.255. Como rede utilize o IP de número menor (32). Portanto a ACL ficará:

```
Router(config)#Access-list 10 permit 172.16.32.0 0.0.31.255
```

Utilizando os exemplos acima, podemos escrever uma ACL que bloqueie o tráfego das redes 200.200.0.0 a 200.200.7.0 e permita a passagem dos pacotes das redes 172.16.32.0 a 172.16.63.0:

```
Router(config)#Access-list 10 deny 200.200.0.0 0.0.7.255
Router(config)#Access-list 10 permit 172.16.32.0 0.0.31.255
```

Ou aproveitando o deny implícito que o IOS coloca no final da lista poderíamos apenas permitir o tráfego referente à rede 172.16 que automaticamente todas as demais redes estariam bloqueadas:

```
Router(config)#Access-list 10 permit 172.16.32.0 0.0.31.255
Router(config)#Access-list 10 deny any (implícito)
```

Outro exemplo interessante é quando há solicitação de bloqueio de apenas algumas redes, pois você deverá lembrar-se de permitir alguma rede no final ou sua ACL bloqueará todo o tráfego que passar pela interface em que ela for aplicada. Por exemplo:

```
Router(config)#Access-list 10 deny 200.200.0.0 0.0.7.255
```

A ACL acima bloqueia as redes de 200.200.0.0 até 200.200.7.0, porém bloqueará todo o tráfego restante devido ao deny implícito colocado pelo IOS. Para solucionar o problema insira o comando:

```
Router(config)#Access-list 10 permit any
```

Assim as demais redes serão permitidas. Lembre-se que sempre que sua ACL iniciar com um "deny" você deve ter no mínimo um "permit".

### 3.3 ACL IP Estendida Numerada

As **Listas de Acesso estendidas** são utilizadas quando você deseja permitir, por exemplo, tráfego http (web) e negar o FTP (File Transfer Protocol) ou telnet de redes que não sejam da empresa, ou seja, **vão além do endereço IP de origem** e testam também outras condições **dentro das camadas 3 e 4**, por exemplo, endereços IP de origem e destino dos pacotes, protocolos específicos, números de portas (TCP e UDP) e outros parâmetros.

As ACLs estendidas numeradas estão no intervalo de 100-199 e de 2000-2699 (faixa estendida). Veja sintaxe básica abaixo.

```
Access-list <100-199> [permit | deny] [Protocolo] [Rede-de-origem] [Máscara-curinga] [Opções-origem] [Rede-de-destino] [Máscara-curinga] [Opções-destino] [Opções-extras]
```

Os **protocolos** podem ser definidos pelo número de 0 a 255 (referente ao protocolo IP) ou através dos mnemônicos: ahp, eigrp, esp, gre, **icmp**, igmp, igrp, **ip**, ipinip, nos, ospf, pcp, pimm, **tcp** e **udp**. Os mais utilizados são:

- **Ip:** representa todos os protocolos.
- **Icmp:** para selecionar o echo, por exemplo.
- **Tcp:** permite filtrar por opções da camada 4 (tráfego TCP), tais como HTTP e FTP.
- **Udp:** permite filtrar por opções da camada 4 (tráfego UDP), tais como TFTP e DNS.

A **rede de origem** é analisada no campo “IP de origem” do cabeçalho do pacote IP, já o **destino** é analisada no campo “IP de destino” do cabeçalho do pacote IP. Diferente das ACLs padrões, as estendidas permitem filtrar tanto com base em endereços de origem como destino.

**Importante:** Quando você estiver analisando um pacote que entra em sua rede, o IP de origem será um IP pertencente à rede remota e o de destino pertencente a sua própria rede. Agora, no caso de um pacote que está sendo enviado da rede interna para um roteador externo (exemplo: acesso a Internet) o IP de origem será da sua própria rede e o de destino será da rede externa. Essa análise deve ser bem entendida para resolver os problemas relativos a ACL.

As **opções para origem e destino** são: **eq** (equal – igual a), **gt** (greater than – maior que), **lt** (less than – menor que), **ne** (not equal – diferente de) e **range** (faixa). O mais utilizado é o “**eq**”, que significa equal ou igual, serve para selecionar uma porta TCP ou UDP específica por exemplo.

As opções extras podem ser ack, dscp, established, fin, log, log-input, precedence, psh, rst, syn, time-range, tos e urg. As mais utilizadas são:

- “**log**”: envia uma informação quando a instrução for casada, ou seja, houve correspondência para aquela instrução da ACL, para um servidor de “syslog” e também na console.
- “**established**”: testa se a conexão TCP já está aberta (bit ACK do protocolo TCP diferente de zero).

O cálculo da máscara curinga é o mesmo realizado para ACL padrão.

### 3.4 Exemplo de ACL Estendida

Para melhor ilustrar o uso de uma ACL estendida vamos a um exemplo, onde vamos criar uma ACL que permita a entrada de tráfego de quaisquer redes externas para acesso a Web (http), FTP. Para o Telnet permitir acesso apenas aos endereços da rede 10.0.0.0/24. Para os demais serviços vamos negar acesso.

```
Router(config)#access-list 100 permit tcp any any eq 80
Router(config)#access-list 100 permit tcp any any eq ftp
Router(config)#access-list 100 permit tcp any any eq ftp-data
Router(config)#access-list 100 permit tcp 10.0.0.0 0.0.0.255 any eq 23
```

O **primeiro statement** ou instrução indica que você permitiu acesso ao protocolo TCP (“access-list 100 permit tcp”), para quaisquer redes de origem e destino (“any any”) para porta 80 (“eq 80”), a qual é a porta referente ao serviço http.

Na **segunda e terceira instruções** foi permitido acesso ao FTP, o qual possui dois canais TCP, um para dados (ftp) e outro para controle (ftp-data). Note que ao invés do número da porta foram utilizados **mnemônicos**, porém somente algumas portas o possuem. Abaixo segue a lista dos mnemônicos, sendo que os mais importantes estão destacados:

```
R1(config)#access-list 100 permit tcp any any eq ?
<0-65535>      Port number
bgp               Border Gateway Protocol (179)
chargen          Character generator (19)
cmd               Remote commands (rcmd, 514)
daytime          Daytime (13)
discard          Discard (9)
domain           Domain Name Service (53)
drip              Dynamic Routing Information Protocol (3949)
echo              Echo (7)
```

exec	Exec (rsh, 512)
finger	Finger (79)
ftp	File Transfer Protocol (21)
ftp-data	FTP data connections (20)
gopher	Gopher (70)
hostname	NIC hostname server (101)
ident	Ident Protocol (113)
irc	Internet Relay Chat (194)
klogin	Kerberos login (543)
kshell	Kerberos shell (544)
login	Login (rlogin, 513)
lpd	Printer service (515)
nntp	Network News Transport Protocol (119)
pim-auto-rp	PIM Auto-RP (496)
pop2	Post Office Protocol v2 (109)
pop3	Post Office Protocol v3 (110)
smtp	Simple Mail Transport Protocol (25)
sunrpc	Sun Remote Procedure Call (111)
tacacs	TAC Access Control System (49)
talk	Talk (517)
telnet	Telnet (23)
time	Time (37)
uucp	Unix-to-Unix Copy Program (540)
whois	Nickname (43)
www	World Wide Web (HTTP, 80)

Na **última linha de instruções** foi inserido o comando para permitir acesso ao protocolo TCP ("access-list 100 permit tcp"), para a rede de origem 10.0.0.0/24 ("10.0.0.0 0.0.0.255"), para quaisquer redes de destino (any) quando o tráfego for direcionado ao telnet (eq 23 ou eq telnet).

O comando para bloquear o restante do tráfego não precisa ser inserido, pois o IOS colocará para você a linha "**access-list 100 deny ip any any**" no final da sua configuração, porém ela **não aparecerá** no comando "show running-config" por ser um **comando implícito**. O parâmetro "ip" inserido no campo do protocolo seleciona todos os protocolos possíveis.

Alguns administradores de rede costumam inserir o comando citado anteriormente com a opção "log" no final para monitorar a tentativa de acesso indevido na rede (**access-list 100 deny ip any any log**). Com a opção log, cada tentativa de acesso indevido será gravada no servidor de Syslog e também no registro interno dos roteadores, podendo ser visualizado com o comando "show log".

### 3.5 Verificando ACL com Comandos Show

Para verificar as ACLs padrão e estendida você pode utilizar os comandos:

- "**show run**" – mostra as ACLs configuradas e onde elas foram aplicadas (em que interfaces).
- "**show access-lists**" – Mostra todas as ACLs.
- "**show ip access-lists**" – Mostra apenas as ACLs IP.

Os comandos "show access-list" e "show ip access-list" podem ser utilizados com o número da ACL para visualização de uma única ACL criada, por exemplo, "show ip access-list 1", mostra a ACL IP padrão criada com o número 1. Veja exemplos dos comandos abaixo.

```

Router#sho ip access-lists
Standard IP access list 1
    permit 10.1.2.21
    permit 10.0.0.0, wildcard bits 0.255.255.255
    permit any
Extended IP access list 100
    permit ip 10.0.0.0 0.0.0.255 11.0.0.0 0.0.0.255
    permit tcp any any eq www
    permit tcp any any eq ftp
    permit tcp any any eq ftp-data
    permit tcp 10.0.0.0 0.0.0.255 any eq telnet

Router#show access-lists
Standard IP access list 1
    permit 10.1.2.21
    permit 10.0.0.0, wildcard bits 0.255.255.255
    permit any
Extended IP access list 100
    permit ip 10.0.0.0 0.0.0.255 11.0.0.0 0.0.0.255
    permit tcp any any eq www
    permit tcp any any eq ftp
    permit tcp any any eq ftp-data
    permit tcp 10.0.0.0 0.0.0.255 any eq telnet

```

Para verificar onde uma ACL foi aplicada (em que interface) e se ela é de entrada ou saída entre com o comando “**show ip interface**”, somente esse comando mostra o posicionamento de uma ACL, além do show run. Veja um exemplo abaixo.

```

TK2#sho ip interface
FastEthernet0/1 is up, line protocol is up (connected)
  Internet address is 200.200.200.1/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
Outgoing access list is Bloqweb → ACL de saída BloqWeb
Inbound access list is not set → Sem ACL de entrada aplicada
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled

```

WCCP Redirect exclude is disabled  
BGP Policy Mapping is disabled

### 3.6 Listas de Acesso Nomeadas

As listas de acesso estudadas acima foram padrões e estendidas numeradas.

Você pode configurar ACL padrão e estendida através de ACLs nomeadas também. A vantagem de uma ACL nomeada é que você pode utilizar um nome sugestivo para guardar a ACL e lembrar para que fim essa ACL foi criada. Além disso, ela estende o range de ACLs que podem ser criadas, pois não há limitações para criações dos nomes teoricamente.

A diferença é que não utilizamos mais o comando “access-list” e sim o comando “ip access-list”, seguido das opções “standard” para ACL padrão ou extended para ACL estendida. Veja exemplo abaixo.

```
DlteC-FW-GW(config)#ip access-list ?
  extended  Extended Access List
  log-update Control access list log updates
  logging    Control access list logging
  resequence Resequence Access List
  standard   Standard Access List
```

Depois de definido o tipo de ACL damos um nome para ela, o qual será utilizado para vincular a lista de acesso às interfaces, pois no caso das numeradas esse vínculo é feito pelo número da ACL. Veja exemplo abaixo.

```
DlteC-FW-GW(config)#ip access-list standard teste
DlteC-FW-GW(config-std-nacl) #
```

Note que ao criar a ACL padrão nomeada “teste” entramos em um modo de configuração com um prompt “(config-std-nacl) #”. Para uma ACL estendida o prompt será “(config-ext-nacl) #”, veja exemplo abaixo onde criamos a lista chamada teste1:

```
DlteC-FW-GW(config)#ip access-list extended teste1
DlteC-FW-GW(config-ext-nacl) #
```

Com as ACLs nomeadas não precisamos ficar repetindo o comando “access-list...” a cada linha, podemos utilizar direto os comandos a partir do “permit” e “deny”. Veja o exemplo a seguir da criação da ACL padrão com o nome de “bloqueiarede”, a qual bloqueia o acesso à rede 172.16.20.0/24 e permite quaisquer outras redes.

```
DlteC-FW-GW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DlteC-FW-GW(config)#ip access-list standard bloqueiarede
DlteC-FW-GW(config-std-nacl) #?
Standard Access List configuration commands:
<1-2147483647> Sequence Number
default      Set a command to its defaults
deny        Specify packets to reject
exit         Exit from access-list configuration mode
no           Negate a command or set its defaults
permit       Specify packets to forward
remark      Access list entry comment
```

```
DlteC-FW-GW(config-std-nacl)#deny 172.16.20.0 0.0.0.255
DlteC-FW-GW(config-std-nacl)#permit any
DlteC-FW-GW(config-std-nacl)#end
DlteC-FW-GW#
```

Note que marcamos em verde uma opção chamada “remark”, a qual pode ser utilizada para inserir um texto explicativo que não será removido da configuração.

Por exemplo, vamos criar uma ACL para bloquear portas TCP e UDP dinâmicas e utilizar apenas algumas vezes, podemos com um remark anotar para que serve essa ACL:

```
DlteC-FW-GW(config)#ip access-list extended portasaltas
DlteC-FW-GW(config-ext-nacl)#deny tcp any any range 49152 65535
DlteC-FW-GW(config-ext-nacl)#deny udp any any range 49152 65535
DlteC-FW-GW(config-ext-nacl)#permit ip any any
DlteC-FW-GW(config-ext-nacl)#remark ACL temporaria para bloquar portas altas
DlteC-FW-GW(config-ext-nacl)#do sho ip access-list portasaltas
Extended IP access list portasaltas
 10 deny tcp any any range 49152 65535
 20 deny udp any any range 49152 65535
 30 permit ip any any
DlteC-FW-GW(config-ext-nacl)#do show running | section portasaltas
ip access-list extended portasaltas
  deny  tcp any any range 49152 65535
  deny  udp any any range 49152 65535
  permit ip any any
  remark ACL temporaria para bloquar portas altas
DlteC-FW-GW(config-ext-nacl)#

```

Note que a anotação é visualizada no comando “show running-config” e não no “show ip access-list” ou “show access-list”. A opção remark pode ser utilizada também em ACLs numeradas.

Vemos estudar posteriormente que podemos alterar as linhas, trocar de lugar ou apagar comandos específicos para as ACLs nomeadas em qualquer versão de IOS. Já para as numeradas, apenas versões mais novas permitem esse tipo de alteração, para IOSs mais antigos a alteração em ACLs numeradas exige que ela seja apagada e criada de novo.

Para apagar uma ACL numerada padrão ou estendida inteira basta digitar “no access-list” e o número dela, por exemplo, “no access-list 4” apaga a lista padrão com número 4.

Para apagar uma ACL nomeada basta digitar “no” na frente do comando que a criou, por exemplo, vamos apagar a ACL criada anteriormente: “no ip access-list extended portasaltas”.

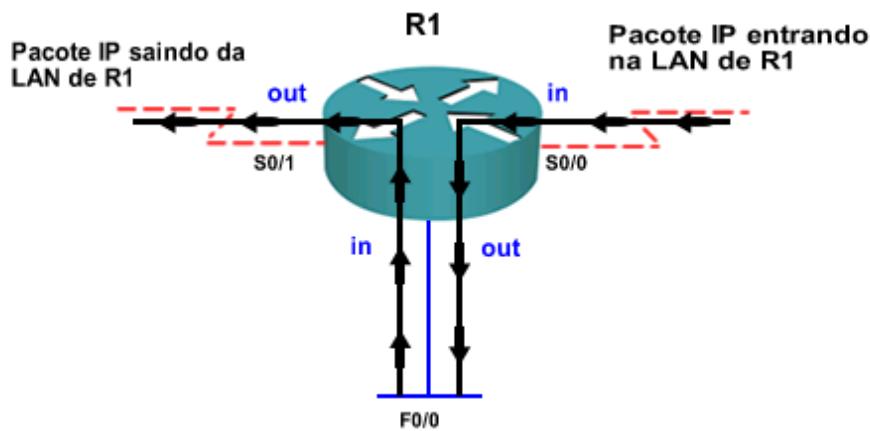
Para visualizar as ACLs nomeadas podemos utilizar os mesmo comandos show estudados anteriormente.

### 3.7 Aplicando ACLs às Interfaces

Após criar a ACL em modo de configuração global devemos aplicá-la a uma interface para que a filtragem possa efetivamente ser realizada, pois uma ACL criada e não aplicada a nenhuma interface não está fazendo nada no roteador, a não ser consumir memória.

Existem duas direções de aplicação para filtragem de tráfego (IN ou OUT) e podemos aplicar apenas uma lista, por direção por protocolo roteador, por exemplo, podemos ter uma ACL de entrada para o IPv4 e uma para o IPv6, nunca duas diferentes para o IPv4.

As ACLs de quaisquer tipos criadas anteriormente podem ser aplicadas na entrada (inbound – in) ou na saída (outbound – out) de uma ou mais interfaces do roteador. Veja a figura a seguir mostrando o sentido do tráfego em relação aos sentidos de aplicação das ACLs nas interfaces.



No sentido de entrada (in) os pacotes são processados pela lista de acesso antes de serem encaminhados pela interface de saída. Já no sentido de saída (out) os pacotes são primeiro encaminhados para a saída para depois serem processados pela lista de acesso.

Note que para bloquear um pacote IP que vem pela interface s0/0 em direção a LAN de R1 (f0/0), você pode utilizar uma ACL de entrada na s0/0 ou uma de saída na f0/0. Agora para bloquear um pacote que sai da LAN de R1 em direção a s0/1 pode ser filtrado por uma ACL de entrada na interface f0/0 ou de saída na s0/1.

O comando para aplicar a ACL em uma interface é o “**ip access-group**” em modo de configuração de interface, veja o exemplo ao lado, onde a lista 101 é aplicada no sentido de saída da interface serial 0 do roteador.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s0
Router(config-if)#ip access-group 101 out
Router(config-if)#^Z
Router#
```

Se aplicarmos uma ACL que não foi criada em uma das interfaces nada acontece, simplesmente o roteador ignora a informação e continua a encaminhar o tráfego normalmente através dela.

Vamos pegar o exemplo feito no tópico anterior aplicar na saída (out) da interface de LAN para analisar o que irá ocorrer:

```
R1(config)#ip access-list extended portasaltas
R1(config-ext-nacl)#deny tcp any any range 49152 65535
R1(config-ext-nacl)#deny udp any any range 49152 65535
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#int f0/0
R1(config-if)#ip access-group portasaltas out
R1(config-if)#end
R1#
```

Nesse exemplo, todo tráfego vindo de quaisquer redes externas para os computadores ou servidores conectados à interface fast 0/0 de R1 que tentarem se conectar com portas dinâmicas serão bloqueados tanto em TCP como em UDP, portanto nessa rede não poderá existir computadores tentando acessar serviços, pois no retorno o tráfego será bloqueado. Assim como conexões aos hosts tentando ser abertas nas portas altas também serão bloqueadas.

Esse exemplo mostra claramente o cuidado ao aplicar ACLs em roteadores, pois tentando bloquear determinado tráfego podemos parar a comunicação de um segmento de rede ou determinados serviços.

É recomendado sempre antes de aplicar listas de acesso verificar se os serviços estão todos funcionando e testá-los novamente após a aplicação, para ver se uma ação específica não acabou prejudicando outros serviços como efeito colateral.

Para desvincular a ACL da interface é só entrar novamente na configuração de interface e digitar “no” enfrente ao comando, por exemplo, o comando “no ip access-group portasaltas out” remove a ACL da interface.

### 3.8 Limitando Acesso às Lines VTY (Telnet e SSH)

Você também pode limitar o acesso remoto ao telnet e SSH diretamente nas lines VTY utilizando o comando “**access-class**” diretamente na configuração das “**lines vty**”, conforme mostrado abaixo.

```
Router(config)#access-list 10 permit 10.0.0.0 0.0.0.255
Router(config)#line vty 0 15
Router(config-line)#access-class 10 in
Router(config-line)#^Z
Router#
```

No exemplo a lista de acesso 10 que é aplicada na line vty do roteador (comando “access-class”) limita a entrada via telnet apenas para os computadores de endereços de 10.0.0.1 até 10.0.0.254. Os demais endereços não terão acesso ao telnet ou SSH do roteador via VTY devido ao deny implícito.

A configuração mostrada é a mesma para roteadores ou switches Cisco. O mesmo comando pode limitar acesso via Telnet ou SSH quando micros remotos tentarem se conectar aos roteadores e/ou switches.

### 3.9 Agora Vamos a Alguns Exemplos

O assunto ACL pode parecer difícil, mas na realidade requer bastante prática para que o aluno acostume com os comandos e lógica para elaborar filtros de pacotes, por isso repita os exemplos mostrados anteriormente e os que estudaremos a seguir, faça os laboratórios e invente cenários próprios, sempre testando se sua configuração funcionou inserindo hosts na topologia.

#### 3.9.1 Exemplo 1 – ACL Padrão

A empresa ABC Inc tem a política interna de liberar o acesso remoto aos equipamentos de rede somente para os micros de gerenciamento inseridos na rede 192.168.1.0/28. Sua tarefa é criar uma **ACL** que **limite acesso remoto** apenas aos micros pertencentes a essa rede.

Para resolver a solicitação acima temos primeiro que criar a lista padrão escolhendo a rede 192.168.1.0/28 (255.255.255.240). Mas qual a máscara curinga devemos utilizar? Lembre-se de subtrair o broadcast da máscara em questão:

- $255.255.255.255 - 255.255.255.240 = 0.0.0.15$

Criando a lista:

```
Router#conf t  
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.15
```

Como existe um deny (negação) implícito no final de uma ACL somente o comando acima é o suficiente para criar a lista, pois ele deixará passar apenas os IP's da rede 192.168.1.0/28 e os demais serão bloqueados.

Agora vamos aplicar a regra na entrada line vty:

```
Router(config)#line vty 0 15  
Router(config-line)#access-class 10 in  
Router(config-line)#end  
Router#copy run start
```

Com essa configuração os equipamentos estarão protegidos de acesso não autorizado pelos micros fora da rede de gerenciamento.

#### 3.9.2 Exemplo 2 – ACL Estendida

Um roteador, que tem a sub-rede 192.168.1.0/26 em sua LAN (Fast 0/0) que está entroncada com um Switch de acesso e possui várias sub-redes na mesma interface. Foi solicitada pelo gerente de segurança a configuração para que a rede 192.168.1.128/26 seja bloqueada quando tentar acessar os serviços de FTP e TFTP em quaisquer micros e servidores dentro dessa sub-rede específica. Todas as demais sub-redes devem ser permitidas para todos os serviços.

O primeiro passo é verificar as portas e protocolos dos serviços a serem bloqueados:

1. FTP: portas 20 e 21 do TCP
2. TFTP: porta 69 do UDP

Note que os pacotes **serão originados na sub-rede 192.168.1.128** e chegarão à rede de destino 192.168.1.0, ou seja, os micros da sub-rede 192.168.1.128 estão em um roteador remoto.

Após isso vamos selecionar a sub-rede de origem a ser bloqueada (ponta remota): 192.168.1.128 /26 ou 255.255.255.192 -> Máscara curinga = 255.255.255.255 – 255.255.255.192 = 0.0.0.63.

A sub-rede do roteador de destino (rede do roteador): 192.168.1.0 /26 ou 255.255.255.192 -> Máscara curinga = 255.255.255.255 – 255.255.255.192 = 0.0.0.63.

Agora vamos criar a lista considerando:

1. Bloquear acesso ao FTP da sub-rede 192.168.1.128 à sub-rede 192.168.1.0:

```
Access-list 100 deny tcp 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.63 eq 20
Access-list 100 deny tcp 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.63 eq 21
```

2. Bloquear acesso ao TFTP considerando as mesmas redes do item 1:

```
Access-list 100 deny udp 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.63 eq 69
```

3. Permitir as demais redes:

```
Access-list 100 permit ip any any
```

Ou podemos utilizar os comandos abaixo substituindo o número das portas pelos seus mnemônicos:

```
Access-list 100 deny tcp 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.63 eq ftp
Access-list 100 deny tcp 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.63 eq ftp-data
Access-list 100 deny udp 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.63 eq tftp
Access-list 100 permit ip any any
```

Criada a lista 100 agora teremos que ativar na interface LAN do roteador:

```
Interface fast 0/0
Ip access-group 100 out
```

A lista foi aplicada na saída da interface LAN, ou seja, quando os pacotes de FTP e TFTP vindos da rede 192.168.1.128/26 tentarem sair pela interface serão bloqueados. As demais sub-redes serão permitidas.

Podemos verificar a ACL com o comando “**show ip interfaces**” e “**show ip access-list 100**”.

### 3.9.3 Exemplo 3 – ACL Nomeada Estendida

Agora vamos repetir o exercício anterior utilizando ACL nomeada estendida, lembrando que a ACL estendida é criada com o comando “ip access-list [extended | standard] nome”. As regras serão criadas dentro do modo de configuração de ACL.

```
Lab_A(config)#ip access-list extended Exemplo3
Lab_A(config-ext-nacl)#deny tcp 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.63 eq ftp
Lab_A(config-ext-nacl)#deny tcp 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.63 eq ftp-data
Lab_A(config-ext-nacl)#deny udp 192.168.1.128 0.0.0.63 192.168.1.0 0.0.0.63 eq tftp
Lab_A(config-ext-nacl)#permit ip any any
Lab_A(config-ext-nacl)#exit
Lab_A(config)#Interface fast 0/0
    Lab_A(config-subif)#Ip access-group Exemplo3 out
    Lab_A(config-subif)#end
    Lab_A#copy run start
```

### 3.10 Editando ACLs Numeradas

As ACLs numeradas, tanto para padrão como estendida, em versões mais antigas do Cisco IOS não podiam ser editadas ou ter sua sequência de regras alteradas (repositionamento das regras). Novas regras são sempre inseridas no final da lista, por isso para alterar a sequência das regras é necessário **apagar toda a ACL e recriá-la na ordem correta**.

Por exemplo, você criou a ACL abaixo e percebeu que a terceira linha não deveria estar declarada e deseja apagá-la, conforme exemplo abaixo.

```
Access-list 100 permit tcp host 198.18.1.3 any eq www
Access-list 100 deny ip host 198.18.1.3 any
Access-list 100 deny ip any any
Access-list 100 deny tcp any any eq www
Access-list 100 permit ip any any
```

Não tem como você digitar “no Access-list 100 deny ip any any”, isso não irá funcionar. Será necessário digitar “no Access-list 100” para apagar toda a lista e recriá-la sem o comando indesejado.

```
No Access-list 100
Access-list 100 permit tcp host 198.18.1.3 any eq www
Access-list 100 deny ip host 198.18.1.3 any
Access-list 100 deny tcp any any eq www
Access-list 100 permit ip any any
```

Nos IOSs mais novos as ACLs padrões são criadas com índices e podem ser alteradas como vamos ver a seguir para as ACLs nomeadas. Apesar disso, na configuração global os índices não são exibidos, apenas com o comando “show ip access-lists”.

```
DlteC-FW-GW#sho ip access-list 1
Standard IP access list 1
    10 permit 10.0.1.0, wildcard bits 0.0.0.255
    20 permit 192.168.1.0, wildcard bits 0.0.0.255 (106877 matches)
    30 permit 192.168.2.0, wildcard bits 0.0.0.255
DlteC-FW-GW#show run | section access-list 1
access-list 1 permit 10.0.1.0 0.0.0.255
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Note que cada comando está vinculado a um índice, porém a configuração não mostra esses índices. Para fazer a alteração devemos entrar na ACL padrão como se estivéssemos entrando em uma ACL nomeada, veja abaixo.

```
DlteC-FW-GW(config)#ip access-list standard 1
DlteC-FW-GW(config-std-nacl) #
```

Para apagar e inserir comandos é só seguir os passos que vamos estudar a seguir para as ACLs nomeadas.

### 3.11 Editando ACLs Nomeadas

Para as ACLs nomeadas podemos apagar entradas únicas, ou seja, apagar linhas específicas, assim como inserir regras na posição que desejarmos. Isso porque as ACLs nomeadas têm cada regra ou statement referenciado com um **número de sequência**, o que nos permite apagar e inserir regras utilizando esse parâmetro. Veja o exemplo abaixo.

```
dltec#conf t
Enter configuration commands, one per line. End with CNTL/Z.
dltec(config)#ip access-list extended Bloqweb
dltec(config-ext-nacl)# permit tcp host 198.18.1.3 any eq www
dltec(config-ext-nacl)# deny ip host 198.18.1.3 any
dltec(config-ext-nacl)# deny tcp any any eq www
dltec(config-ext-nacl)# permit ip any any
dltec(config-ext-nacl)#do show ip access-list Bloqweb
Extended IP access list Bloqweb
 10 permit tcp host 198.18.1.3 any eq www
 20 deny ip host 198.18.1.3 any
 30 deny tcp any any eq www
 40 permit ip any any
dltec(config-ext-nacl)#

```

Note que quando criamos a ACL nomeada estendida chamada **Bloqweb** o roteador vincula automaticamente um índice ou número de sequência a cada entrada variando de 10 em 10. Se quisermos agora apagar a segunda linha basta digitar “**no 20**” dentro do modo de configuração da ACL Bloqweb.

```
dltec(config-ext-nacl)#no 20
dltec(config-ext-nacl)#do show ip access-list Bloqweb
Extended IP access list Bloqweb
 10 permit tcp host 198.18.1.3 any eq www
 30 deny tcp any any eq www
 40 permit ip any any
dltec(config-ext-nacl)#

```

Note que a linha com o número de sequência 20 foi apagada, agora podemos criar uma nova regra com o número 20 para substituir a anterior.

```
dltec(config-ext-nacl)#20 permit tcp any any eq 555
dltec(config-ext-nacl)#do show ip access-list Bloqweb
Extended IP access list Bloqweb
 10 permit tcp host 198.18.1.3 any eq www
 20 permit tcp any any eq 555
 30 deny tcp any any eq www
 40 permit ip any any
dltec(config-ext-nacl)#

```

### 3.12 Recomendações Gerais sobre Configuração de ACLs

A Cisco faz algumas recomendações sobre a criação de ACLs em cursos nos quais o CCENT e CCNA tem como base:

- Criar as ACLs utilizando um editor de texto para facilitar copiar e colar comandos no roteador, mesmo que você tenha muita prática em digitar os comandos para as ACLs esta recomendação facilita na hora de alterar a ordem de comandos, pois basta dar um “**no access-list 100**” para apagar a lista 100 inteira e trocar as opções no bloco de notas de lugar, copiar e colar novamente no roteador, ao invés de digitar tudo novamente na ordem que você estipulou.
- Posicionar ACLs padrões (standard) **mais próximo da rede de destino**, pois como elas apenas filtram por endereços IPs de origem elas não conseguem realizar a filtragem no mesmo roteador onde os pacotes estão sendo criados.
- Posicionar ACLs estendidas **mais próximo da origem dos pacotes** a serem filtrados ou descartados, pois na ACL estendida podemos fazer a filtragem onde os pacotes estão sendo originados e evitar que eles trafeguem pela rede consumindo banda até serem descartados em seu destino.
- Posicionar regras mais específicas no início das listas, pois as regras que mais são utilizadas (que mais dão match) estando no início da lista aceleram o processo de encaminhamento do roteador. Por exemplo, se o acesso HTTP é proibido na sua rede e ele é o que mais é requisitado, se você colocá-lo no final da ACL toda vez que um pacote para o HTTP entrar no roteador ele terá que passar por todas as regras anteriores até ser lido e descartado, se você colocasse no início o processamento do roteador irá melhorar.
- Desabilitar as ACLs nas interfaces quando for fazer alguma alteração em determinada regra, pois isso evita indisponibilidade na rede em caso de erros.

Além disso, se você aplicar uma ACL que não foi criada em modo de configuração global o tráfego nessa interface será permitido, pois não há regra criada com aquele número ou nome aplicado na Interface.

## 4 Reforçando a Segurança em Roteadores e Switches Cisco

Existem vários recursos de segurança que podem ser utilizados nos roteadores e switches para proteger a rede, assim como dispositivos como Firewalls, porém o foco desse tópico é a proteção do próprio roteador e switch.

### 4.1 Senhas de Acesso

Imagine que você configurou uma senha fraca para Telnet ("cisco") e um usuário mal intencionado começa a executar acessos remotos ao endereço do seu gateway, que normalmente é um roteador ou switch camada-3. Em dispositivos Cisco a primeira senha a ser tentada é "cisco" e se pedir usuário e senha é "cisco/cisco" por motivos óbvios. Com acesso ao roteador o usuário poderia executar um "erase startup-config" e "reload", apagando a configuração do roteador e fazendo-o inicializar com o padrão de fábrica!

Portanto, são muito importantes algumas configurações básicas relacionadas às senhas de acesso aos dispositivos:

- Configurar senhas de acesso fortes (mínimo de oito caracteres com letras maiúsculas, minúsculas, números e caracteres especiais).
- De preferência utilizar usuários e senhas com autenticação local ou através de servidor de autenticação (TACACS+ ou RADIUS) para Telnet, SSH ou acesso discado via porta auxiliar.
- Criptografar as senhas em modo texto com o comando "**service password-encryption**".
- **Não utilizar** o comando "**enable password**" para senha de acesso privilegiado e sim o "**enable secret**". O mesmo vale para criação dos usuários, de preferência criar com o comando username seguido da opção "secret" para definir uma senha criptografada em MD5, assim como é feito para o "enable secret", exemplo: "**username dltec secret dLt3c@admin1n**".

As senhas em modo texto são produzidas nos comandos que definem a senha com a palavra chave "password", como o enable password, username/password e o próprio comando password utilizado nas lines VTY, cosole e auxiliar.

### 4.2 Desabilitando Serviços e Portas não Utilizadas

Os roteadores e switches Cisco permitem conexão remota via Telnet, SSH, HTTP e HTTPS, sendo que nenhum deles vem ativado por padrão.

A recomendação geral é para não ativar os serviços de HTTP e HTTPS, assim como não acessar os dispositivos via Telnet a partir de redes externas, pois os pacotes trocados podem ser capturados e tanto o Telnet como o HTTP as informações são passadas em texto aberto, possibilitando que usuários e senhas sejam lidos.

Se for necessário acesso externo ative somente o SSH e HTTPS, pois assim os dados e envio de usuários e senhas estarão protegidas.

O HTTP e HTTPS são utilizados para acessar informações básicas ou então para permitir acesso via Web às configurações dos roteadores através de um programa chamado **Cisco Configuration Professional (CCP)**. Nos switches o gerenciador HTTP/HTTPS deve estar presente na memória flash e normalmente vem de fábrica instalado, permitindo a monitoração e configuração das portas via Web.

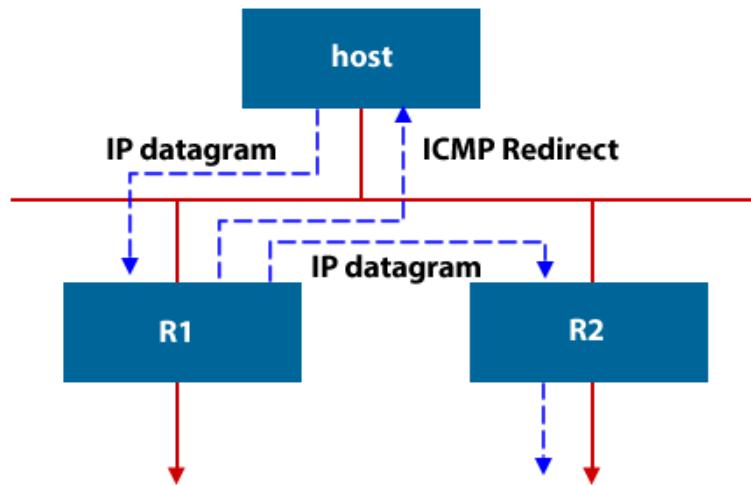
Para desativar o HTTP e HTTPS nos roteadores e switches entre com os comandos abaixo:

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip http server
R1(config)#no ip http secure-server
R1(config)#+
```

Existe também um protocolo para coleta de informações de vizinhos chamada **CDP** (Cisco Discovery Protocol), o qual estudaremos no último capítulo, que em algumas redes corporativas é desativado, porém deve ser analisado o impacto na rede, pois os telefones IP Cisco utilizam o CDP para descobrir algumas configurações e se desabilitado pode gerar problemas para o registro e funcionamento dos aparelhos.

Para desativar o CDP de todo roteador ou switch utilize o comando “**no cdp run**” em modo de configuração global ou “**no cdp enable**” para desabilitar o protocolo por interface (dentro da configuração de cada interface).

Existem também vários serviços do ICMP,TCP e UDP que podem ser desabilitados para melhorar a segurança nos dispositivos e evitar ataques simples de serem executados, por exemplo, o redirecionamento de endereço ou “ICMP Redirect” permite que ao receber um pacote o roteador avise ao host de origem que envie o tráfego para outro gateway, veja a figura abaixo.



Com o comando “**no ip redirect**” desabilitamos o envio desse tipo de mensagem pelos roteadores, sendo configurado por interface.

Outro exemplo de serviço que normalmente é desabilitado é o chamado TCP e UDP small server. Eles agem como um ping através de mensagens ICMP Echo Request e Echo Reply, mas utilizando ao invés de um pacote simples ICMP eles utilizam TCP ou UDP para serem enviados. É como um ping para testar serviços de camada 4, para descobrir serviços ativos na rede. Existem versões do Cisco IOS que desabilitam esse recurso por padrão, mas outras não, e para desabilitar basta utilizar os comandos abaixo.

```
R1(config)# no service tcp-small-servers
R1(config)# no service udp-small-servers
```

Por último, conforme estudamos no capítulo 7, as portas não utilizadas devem ser desabilitadas ou então protegidas para evitar que dispositivos e computadores invadam a rede sem

autorização. Nos roteadores por padrão as portas já são desativadas (no shut), mas nos switches o padrão é estarem todas ativadas.

#### 4.3 Limitando Acesso Telnet e SSH via ACL

Anteriormente já estudamos como realizar esse tipo de configuração. Ela é importante em um ambiente corporativo para que somente computadores permitidos tenham acesso remoto aos equipamentos de infraestrutura de redes.

Lembre-se que basta criar uma ACL liberando as redes de gerenciamento e aplicá-la diretamente na line VTY com o comando **access-class**.

#### 4.4 Ativando o Protocolo NTP – Network Time Protocol

Por último, mas não menos importante, devemos **assegurar** que todos os dispositivos Cisco (telefones, roteadores e switches) estejam com as informações de data/hora sincronizadas. Para tal, utilizamos o protocolo **NTP** (Network Time Protocol).

Manter seus dispositivos sincronizados traz uma série de vantagens, dentre elas:

- Permite exibir a informação correta de data/hora em todos os dispositivos.
- Atribui corretamente a data/hora nas mensagens de log.
- Sincroniza as mensagens de log nos roteadores e switches.

Note que as mensagens enviadas e armazenadas nos logs de registro do sistema são referenciadas a data e hora configurada nos roteadores e switches.

Logo, sem configuração nenhuma fica mais difícil de correlacionar eventos quando problemas ou até mesmo incidentes de segurança ocorrerem na rede envolvendo esses dispositivos, por isso é tão importante o uso do protocolo NTP para manter os dispositivos sincronizados. Veja exemplo abaixo.

```
DlteC-FW-GW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DlteC-FW-GW(config)#end
DlteC-FW-GW#
000080: Jul 18 2013 15:54:37.709 BR: %SYS-5-CONFIG_I: Configured from console by
dltec on vty0 (192.168.1.22)
DlteC-FW-GW#
```

Veja que ao sair do modo de configuração global o roteador informa o último usuário que esteve nesse modo de operação, assim em caso de problemas causados por alterações no sistema o administrador de redes tem como rastrear a pessoa que entrou no dispositivo e o horário que a alteração foi realizada!

**Curiosidade:** quando você reseta um roteador ou switch Cisco a maioria deles irá exibir a configuração default de data (**01 de Março de 1993**).

Para configurar a data/hora em roteador/switch você tem duas opções:

- Manualmente, com o comando `clock set` em modo EXEC privilegiado.
- Automaticamente, com o protocolo NTP.

O comando clock set é bem simples, veja exemplo abaixo:

```
DlteC-FW-GW#clock set ?
hh:mm:ss Current Time

DlteC-FW-GW#clock set 15:41:12 ?
<1-31> Day of the month
MONTH Month of the year

DlteC-FW-GW#clock set 15:41:12 18 ?
MONTH Month of the year

DlteC-FW-GW#clock set 15:41:12 18 july ?
<1993-2035> Year

DlteC-FW-GW#clock set 15:41:12 18 july 2016 ?
<cr>

DlteC-FW-GW#clock set 15:41:12 18 july 2016
DlteC-FW-GW#
```

Para visualizar a hora configurada utilize o comando "show clock".

```
DlteC-FW-GW#show clock
.15:41:34.942 BR Thu Jul 18 2016
DlteC-FW-GW#
```

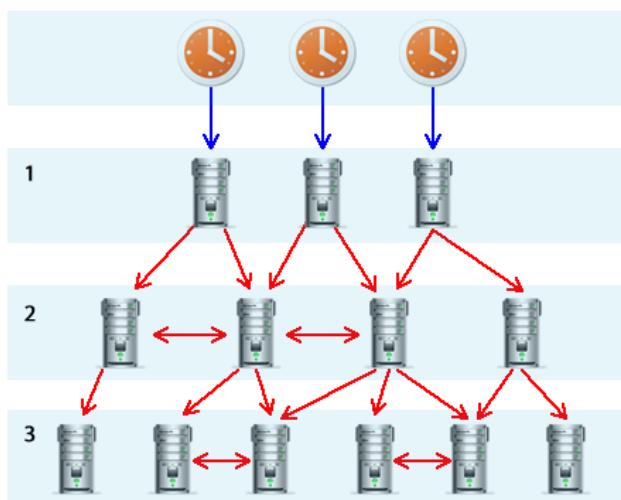
#### 4.4.1 Configurando o Roteador como Cliente NTP

Utilizando o **protocolo NTP** você terá uma informação de data/hora mais precisa e também irá garantir que todos os dispositivos fiquem sincronizados, ou seja, com a mesma informação de data/hora.

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 clicando aqui: [servidores NTP \(<http://support.ntp.org/bin/view/Servers/WebHome>\)](http://support.ntp.org/bin/view/Servers/WebHome)

Veja a seguir uma figura representando a hierarquia dos servidores NTP.



Para habilitar o NTP cliente em um roteador Cisco utilize como referência o exemplo abaixo.

```
dltec#configure terminal
dltec (config)#ntp server a.st1.ntp.br
dltec (config)#clock timezone BR -3
```

**Obs:** caso você não configure o timezone, o seu dispositivo irá exibir a hora tendo como referência o fuso-horário universal (UTC).

O **primeiro comando** “ntp server a.st1.ntp.br” informa o hostname ou endereço IP do servidor NTP utilizado. Em nosso exemplo utilizamos um servidor NTP stratum 1 localizado aqui no Brasil. Também poderíamos utilizar o comando na forma “**ntp server 200.160.7.186**”, onde 200.160.7.186 é o endereço IP para o host a.st1.ntp.br.

O **segundo comando** ajusta o fuso-horário do dispositivo, em nosso exemplo utilizamos o fuso-horário padrão do Brasil, com -3 horas em relação ao UTC (Universal Time Coordinated).

Para verificar o funcionamento do NTP utilize os comandos show a seguir.

```
dltec#sh ntp associations
address ref clock st when poll reach delay offset disp
*~200.160.7.186 .ONBR. 1 11 64 37 14.240 -1.468 439.05
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
```

O asterisco (\*) indica que o roteador está sincronizado com o servidor NTP. Você pode configurar vários servidores NTP de redundância, no entanto os roteadores irão sincronizar apenas por uma fonte de cada vez.

```
dltec#sh ntp status
Clock is synchronized, stratum 2, reference is 200.160.7.186
nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**24
reference time is D2B6C6D7.27B172D4 (11:16:55.155 BR Tue Jan 10 2012)
clock offset is -1.4685 msec, root delay is 14.24 msec
root dispersion is 946.75 msec, peer dispersion is 5.79 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000227 s/s
system poll interval is 64, last update was 412 sec ago.
dltec#sh clock
11:23:19.000 BR Tue Jan 10 2012
```

**Dica:** no comando "show ntp associations" a coluna "st" indica o stratum do servidor NTP utilizado, no nosso exemplo mostra st 1, pois o servidor que utilizamos é stratum 1. Já no comando "show ntp status" temos a informação stratum 2, pois esse é o stratum do nosso sistema. Como estamos nos referenciando com um servidor stratum 1, nós seremos stratum 2.

#### 4.4.2 Configurando o Roteador como Mestre NTP (Servidor)

A configuração mestre/escravo (**Master Mode**) é quando utilizamos um roteador da própria rede para sincronizar com um servidor NTP externo e esse roteador da rede servir como servidor NTP internamente. Isso é muito comum em telefonia IP quando utilizamos o CUCME (Callmanager Express), pois o roteador CME será utilizado como referência NTP para os telefones IP.

A configuração do cliente/escravo é a estática feita com o comando "**ntp master**" e definimos o número do estrato NTP. Se for utilizar o clock interno do roteador Master como referência de sincronismo pode utilizar o valor "1", porém se houver um sincronismo com servidor NTP externo utilize preferencialmente o valor "5" (*recomendação de best practice*).

Veja exemplo de configuração abaixo, onde R1 será o Master e R2 o escravo (Slave), além disso, note que R1 está sincronizando seu relógio com um servidor NTP externo (a.st1.ntp.br).

```
R1-ntp_server#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-ntp_server(config)#ntp server a.st1.ntp.br
R1-ntp_server(config)#ntp master 5

R2-ntp_client#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2-ntp_client(config)#ntp server 192.168.1.92
```

Você deve criar rotas estáticas nos vizinhos para que eles encontrem sua loopback ou inserir a rede para essas interfaces dentro do processo de roteamento do protocolo dinâmico que você estiver utilizando. Por exemplo, no RIP bastaria inserir "network 172.16.0.0".

Por questões de estabilidade você pode referenciar o NTP a uma interface loopback, pois ela é uma interface lógica não cai nunca, a não ser que você desligue o roteador ou a própria interface manualmente.

```
R1-ntp_server#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-ntp_server(config)#interface looppack 0
R1-ntp_server(config-if)#ip add 10.0.0.1 255.255.255.255
R1-ntp_server(config-if)#exit
R1-ntp_server(config)#ntp server a.st1.ntp.br
R1-ntp_server(config)#ntp master 5
R1-ntp_server(config)#ntp source loopback 0
```

No cliente você deve utilizar o comando "ntp Server 10.0.0.1", por isso é importante que o roteamento esteja bem configurado para que os clientes encontrem o endereço da interface loopback do roteador configurado servidor NTP.

## 5 Resumo do Capítulo

Bem pessoal, chegamos ao final de mais um capítulo!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Dominar o conceito de listas de controle de acesso (ACL).
- Saber explicar e diferenciar uma ACL padrão e estendida.
- Dominar o conceito e cálculo de máscaras curinga.
- Dominar a configuração de uma ACL padrão e estendida.
- Saber aplicar, sem dificuldade, uma ACL em uma interface.
- Saber limitar via configuração de ACL o acesso via telnet e SSH com o comando access-class em roteadores.
- Saber reforçar a segurança em roteadores Cisco.
- Saber ativar o protocolo NTP e configurar a hora local em roteadores e switches.

*Até o momento o foco do que estudamos estava mais voltado a comunicação interna, ou seja, dentro da rede corporativa da empresa.*

*Nesse capítulo vamos aprender como configurar a tradução de endereços IP para que possamos acessar à Internet e revisar as opções aprendidas até o momento para configuração da saída do tráfego Interno em direção à Internet.*

*Aproveite o capítulo e bons estudos!*

## **Capítulo 11 – NAT, PAT e Acesso à Internet**

### **Objetivos do Capítulo**

Ao final desse capítulo você terá estudado e deverá compreender:

- Entender os conceitos e aplicações do NAT e PAT.
- Saber configurar, sem dificuldade, o NAT estático e dinâmico em roteadores Cisco.
- Saber configurar, sem dificuldade, o PAT em roteadores Cisco.
- Ser capaz de realizar troubleshooting no NAT e PAT em roteadores Cisco.
- Saber configurar o acesso de uma Intranet com endereços privativos à Internet utilizando NAT e PAT.

## Sumário do Capítulo

<b>1</b>	<i>Abertura</i>	<b>440</b>
<b>2</b>	<i>Visão Geral do NAT e PAT</i>	<b>441</b>
<b>3</b>	<i>Configurando e Resolvendo Problemas com NAT e PAT</i>	<b>445</b>
3.1	Configurando NAT Estático	445
3.2	Configurando NAT Dinâmico	447
3.3	Configurando PAT	449
3.4	Configurando o PAT com Pool	450
3.5	Mantendo e Monitorando o NAT e PAT	
		451
<b>4</b>	<i>Configurando uma Topologia Completa com Saída para a Internet</i>	<b>453</b>
4.1	Exemplo Prático 1 – Configuração de um Branch Office	453
4.2	Exemplo Prático 2 – PAT com Pool e DHCP Básico	457
<b>5</b>	<i>Resumo do Capítulo</i>	<b>458</b>

## 1 Abertura

Nesse ponto do curso já estamos com nossa rede completa e já aprendemos a:

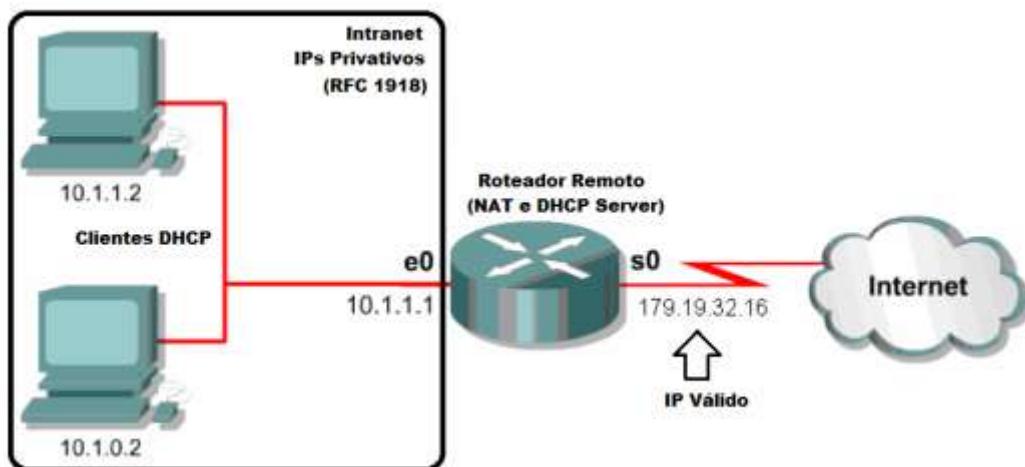
- Posicionar cada dispositivo de infraestrutura de redes (roteadores e switches) para montar uma rede corporativa.
- Projetar redes IP classful ou com VLSM e CIDR.
- Configurar opções básicas para gerenciamento local e remoto roteadores e switches.
- Configurar redes LAN com switches.
- Segmentar LANs com switches e VLANs.
- Aumentar a segurança de portas com Port Security.
- Configurar roteadores e switches camada-3 para fazer o roteamento entre VLANs.
- Configurar o roteamento IP entre as diversas redes e sub-redes utilizando rotas estáticas ou através do protocolo dinâmico OSPFv2.
- Alocar endereços dinamicamente aos clientes através do DHCP.
- Filtrar tráfego entre duas redes que estão conectadas através de roteadores Cisco com listas de controle de acesso.
- Reforçar a configuração de roteadores e switches.

Olhando tudo que estudamos até o momento já conseguimos montar uma rede corporativa de alto desempenho e com recursos bastante avançados, porém ainda está faltando como conectar essa nossa rede à Internet utilizando os próprios roteadores, pois até aprendemos a configurar rotas padrões, porém ainda falta a tradução dos endereços privativos para endereços válidos de Internet para que nossa topologia fique completa.

Portanto, nesse capítulo vamos aprender como fazer o acesso à Internet através do NAT e PAT, suas diferenças e aí sim implementar o acesso completo, ou seja, Intranet e acesso à Internet!

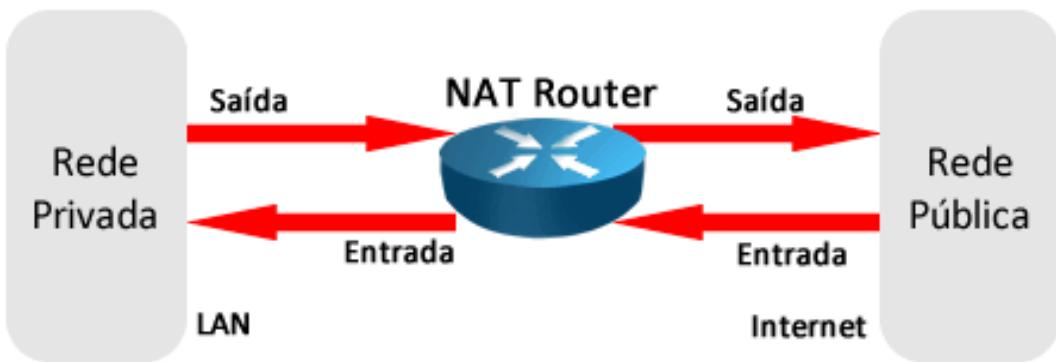
O NAT, PAT e acesso à Internet foram agrupados em um mesmo capítulo porque são recursos que permitem que um roteador tenha tudo o que uma unidade remota de pequeno ou médio porte necessita para permitir acesso à Internet sem a necessidade da instalação de servidores locais, fazendo com que os serviços sejam agregados em um mesmo dispositivo e reduzindo o custo da implantação.

O NAT e o PAT são utilizados para o compartilhamento da Internet entre diversos computadores que na Intranet utilizam endereçamento IP privativo (RFC 1918). Além disso, o NAT e PAT foram desenvolvidos para minimizar o efeito da escassez de endereços IP versão 4, assim como o CIDR e summarização de rotas que já estudamos nos capítulos 5 e 9.



## 2 Visão Geral do NAT e PAT

**NAT (Network Address Translator)** e o **PAT (Port Address Translation)** são técnicas de **tradução de endereços** de camada-3 (rede) que visam minimizar os efeitos da escassez de endereços IP versão 4 e também aumentar a segurança da rede interna das empresas. Veja figura abaixo.



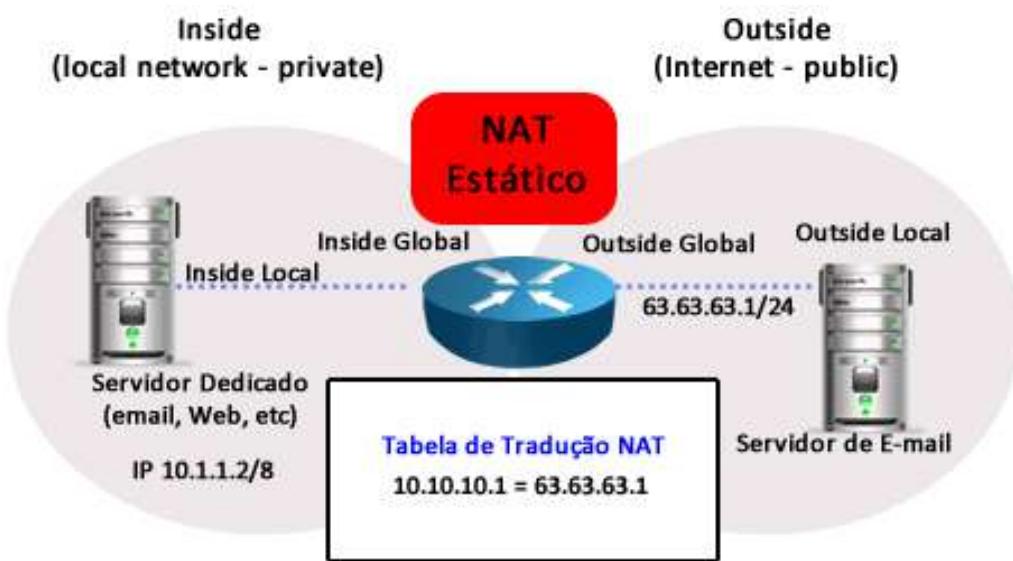
Com a RFC 1918 foram criadas regras que permitem a utilização de endereços privativos, não utilizáveis na Internet, apenas em redes locais privadas. Tais endereços são chamados **endereços privados**.

Portanto, é possível que várias empresas utilizem esses endereços privados em suas redes internas, sem a preocupação com o número de IPs que suas redes demandam, porém, como esses endereços não são propagados pela Internet é necessário um mecanismo para efetuar essa conexão. O NAT e o PAT são mecanismos para conectar redes privadas à Internet, pois eles servem como pontos de tradução de IPs privados (não roteáveis na Internet) para IPs públicos (roteáveis na Internet).

O NAT e o PAT podem ser implementados de três maneiras:

- **Estático:** É estabelecida uma relação entre endereços locais e endereços da Internet de maneira fixa, isto é, sempre um IP interno será traduzido para o mesmo IP externo pré-definido.
- **Dinâmico:** Ocorre um mapeamento de endereços locais e endereços da Internet conforme a necessidade de uso. Existe uma faixa de endereços que podem ser utilizados dinamicamente.
- **Reverso:** Utilizado para mapear um host ou servidor em uma rede IP privativa a partir de um endereço e porta específicos válidos de Internet.

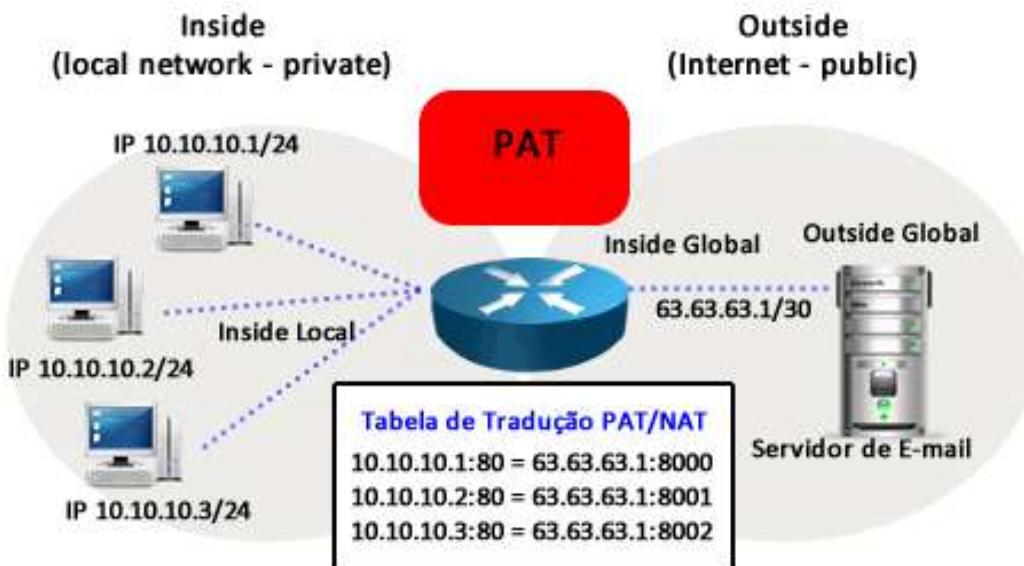
As traduções estáticas são recomendadas para oferecer serviços na rede interna, por exemplo, quando um servidor está localizado na rede interna. Sendo assim, quando houver um pedido de conexão ao roteador a um IP definido via **NAT estático**, o NAT consulta a tabela de endereços e transcreve para o IP interno correspondente, permitindo assim, que seja possível fazer uma conexão no sentido da Internet para a rede interna. Veja figura abaixo.



O **NAT dinâmico** foi projetado para mapear um endereço IP privado para um endereço público. Qualquer endereço IP de um pool de endereços IP públicos pode ser atribuído a um host da rede. Aqui não existe relação fixa entre os IPs internos e externos, não sendo possível abrir uma conexão a partir da Internet, aumentando a segurança da rede interna.

Já o **PAT**, além de traduzir o endereço IP de origem, também utiliza números de porta TCP e UDP de origem para distinguir cada uma das traduções, daí vem o nome **Port Address Translation**, ou seja, tradução de porta e endereço.

O número da porta TCP ou UDP é codificado utilizando 16 bits, o que nos leva ao número total de  $2^{16}$  endereços internos que podem ser traduzidos para um único endereço externo, ou seja, o valor de 65.536 possíveis traduções por endereço IP válido. Na prática, a quantidade de portas que podem receber um único endereço IP é aproximadamente 4.000.



Outra característica do PAT é que ele tenta preservar a porta TCP ou UDP de origem do segmento entrante. Se a porta de origem já estiver sendo utilizada em outra tradução, o PAT atribui o primeiro número de porta disponível para essa conexão. Quando não há mais portas disponíveis e há mais de um endereço IP externo configurado, o PAT passa para o próximo.

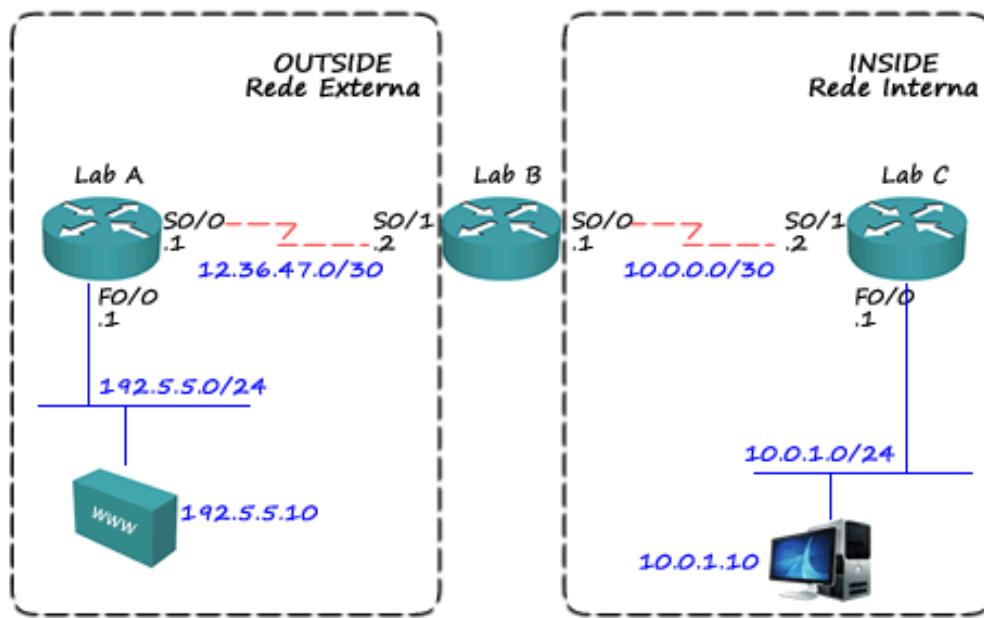
endereço IP, para tentar alocar novamente a porta de origem. Esse processo continua até que não haja mais portas disponíveis nem endereços IP externos.

No IOS da Cisco alguns termos são definidos para configuração e melhor compreensão do NAT e do PAT:

- **Endereço local interno (Inside local address):** endereço privado pertencente a rede interna. Endereço a ser traduzido.
- **Endereço global interno (Inside global address):** endereço válido na Internet pertencente ao roteador que está com o NAT configurado.
- **Endereço local externo (Outside local address):** é o endereço interno do host que será acessado na rede externa, ou seja, é a forma como um endereço IP público é visto na rede interna.
- **Endereço global externo (Outside global address):** Endereço do host remoto pertencente à Internet.

Normalmente os endereços local e global outside são iguais, porém a casos onde o mesmo IP existe na rede interna (inside) e externa (outside) e o endereço outside local pode ser outro para permitir que faixas repetidas de IPs possam ser utilizadas em ambos os lados, portanto o outside local fica diferente do outside global para permitir essa comunicação. Por exemplo, quando duas empresas são fundidas e possuem uma faixa sobreposta de IPs.

Nesse tipo de configuração o roteador além de traduzir os endereços, terá também que alterar a resposta do DNS quando um computador procurar por um recurso que tem o mesmo nome interno, por esses fatores e complicações essa é uma técnica que deve ser utilizada somente em casos de real necessidade.



Na figura ao lado o roteador B é o responsável pelo NAT. O roteador C faz parte rede Interna e utiliza o endereço privado 10.0.1.0/24. O roteador A representa a Internet. Suponhamos que o host 10.0.1.10, o qual está na rede do Lab\_C, tem um mapeamento estático em B utilizando o IP 12.36.47.2. Quando ele acessar a Internet buscando pelo servidor de web 192.5.5.10, o roteador B receberá o pacote pela interface serial 0/0 e trocará o endereço de origem de 10.0.1.10 para 12.36.47.2 e enviará pela interface serial 0/1.

O servidor receberá a requisição e passará as informações solicitadas para o IP 12.36.47.2. O roteador B receberá esse pacote, verificará sua tabela de traduções do NAT e repassará as informações para o host 10.0.1.10.

Pelas definições da Cisco temos que:

Inside global address	Inside local address	Outside local address	Outside global address
12.36.47.2	10.0.1.10	192.5.5.1	192.5.5.1

Portanto o roteador B é um roteador de borda que faz a ponte entre a rede interna e a internet. Ainda podemos dizer que a interface s0/0 é uma interface interna (inside) e a s0/1 é uma interface externa (outside).

Agora se no roteador B fosse configurado o NAT dinâmico, ao invés de termos um IP interno mapeado a um externo, teríamos uma faixa de IPs internos mapeados a uma faixa de IPs externos, possibilitando que mais de um host da rede interna acesse a Internet. Porém o NAT dinâmico é muito dispendioso, pois ele necessita de vários IPs válidos para que o processo funcione de acordo com o esperado.

Agora vamos supor que o roteador B foi configurado com PAT e apenas um IP válido na Internet foi disponibilizado para efetuar a tradução. Em um determinado momento o host 10.0.1.10 e o host 10.0.1.20 enviaram pacotes para conexão com o servidor de web 192.5.5.10 simultaneamente. Abaixo seguem os pacotes que chegarão à interface s0/0 do Lab\_B:

IP de Origem	Porta de Origem	IP de Destino	Porta de Destino
10.0.1.10	1235	192.5.5.10	80
10.0.1.20	1236	192.5.5.10	80

O Lab\_B receberá as solicitações e fará a tradução utilizando as portas TCP de origem preferencialmente iguais à dos pacotes originais, porém se as portas estiverem em uso ele utilizará outras. Abaixo seguem os pacotes traduzidos e enviados via s0/1 para o servidor 192.5.5.10:

IP de Origem	Porta de Origem	IP de Destino	Porta de Destino
12.36.47.2	1235	192.5.5.10	80
12.36.47.2	1236	192.5.5.10	80

O roteador montará uma tabela relacionando os IPs e portas internas com as traduções:

IPs da Rede Interna		Tradução	
IP de Origem Inside Local	Porta de Origem	Inside Global Address	Porta de Destino
10.0.1.10	1235	12.36.47.2	1235
10.0.1.20	1236	12.36.47.2	1236

Quando o servidor responder a requisição para o IP 12.36.47.2, o roteador fará separação para quem ele deve enviar o pacote analisando a tabela do PAT mostrada acima. Ou seja, quando o servidor responder para o 12.36.47.2 na porta 1235 ele passará para o host 10.0.1.10, e pela porta 1236 ele encaminhará para o host 10.0.1.20.

### 3 Configurando e Resolvendo Problemas com NAT e PAT

As configurações do NAT e do PAT são bem parecidas e realizadas em modo de configuração global e também nas interfaces.

A seguir você aprenderá os quatro tipos de configurações mais comuns que são utilizadas com NAT e PAT:

- NAT Estático
- NAT Dinâmico
- NAT com Overload ou PAT em Interfaces
- NAT com Overload Dinâmico ou PAT Dinâmico

Vamos começar pelo mais simples, o NAT estático!

#### 3.1 Configurando NAT Estático

Para configurar o **NAT Estático** basta definir o IP a ser traduzido e as interfaces inside e outside global. Abaixo seguem os passos para configuração.

**1)** Defina uma tradução estática entre um “inside local address” e um “inside global address” com o comando “ip nat inside”:

```
Router(config)#ip nat inside source static local-ip global-ip
```

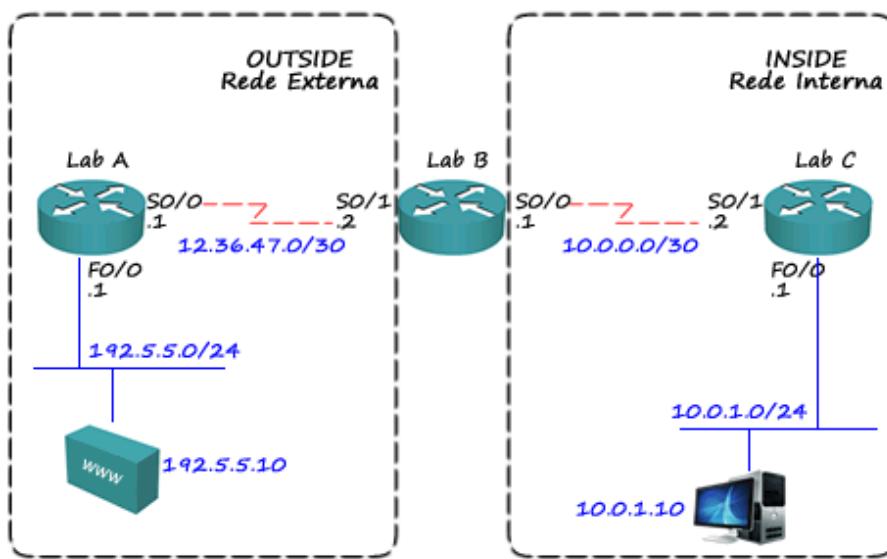
O parâmetro “**source static**” define que você utilizará o NAT estático. O parâmetro “**local-ip**” é o IP privado interno a ser traduzido e o “**global-ip**” é o IP externo que servirá de interface com a Internet.

**2)** Defina a interface interna por onde o IP a ser traduzido acessa a rede externa (inside):

```
Router(config-if)#ip nat inside
```

**3)** Defina a interface que se conecta a externa (outside):

```
Router(config-if)#ip nat outside
```



Note que na topologia de ensino o Lab\_B é o roteador que está configurado com o NAT, ou seja, ele está na fronteira entre a rede interna (Lab\_C) e a Internet (Lab\_A). A rede interna ou “**inside global**” está configurada com a rede privada de classe A 10.0.0.0. Para que os computadores acessem a Internet é preciso que seja feita a tradução desses endereços para um endereço IP válido.

Para tal a interface s0/0 do roteador B foi configurada como “**ip nat inside**”, ou seja, define que toda a rede para trás da interface s0/0 de B seja a rede interna (inside global). Já a rede externa (saída ou “outside global”) está conectada na interface s0/1 do roteador B, definido através do comando “**ip nat outside**”. Portanto quando um pacote IP entrar via s0/0 do Lab\_B em direção a Internet, ele será traduzido com um IP válido e enviado via s0/1.

Essa tradução é mantida em uma tabela para que o roteador saiba para quem encaminhar na rede interna quando o host ou servidor externo responder.

Algumas configurações foram omitidas e apenas as mais relevantes foram mantidas. Note que foram mantidas as configurações de roteamento, pois muitas vezes os problemas relativos à configuração e implementação do NAT e PAT são devidos a configurações de roteamento.

#### Configuração do roteador Lab\_A:

```

hostname LAB_A
!
interface GigabitEthernet0/0
ip address 192.5.5.1 255.255.255.0
!
interface Serial0/0
ip address 12.36.47.1 255.255.255.252

```

#### Configuração do roteador com função de NAT Lab\_B:

```

Hostname Lab_B
!
interface Serial0/0
ip address 10.0.0.1 255.255.255.252
ip nat inside
!
interface Serial0/1
ip address 12.36.47.2 255.255.255.252
ip nat outside
!
ip nat inside source static 10.0.1.10 12.36.47.2

```

```
!
ip route 0.0.0.0 0.0.0.0 Serial0/1
ip route 10.0.1.0 255.255.255.0 serial0/0
```

Com essa configuração apenas o computador 10.0.1.10 poderá acessar a Internet utilizando o IP 12.36.47.2. Os demais hosts não poderão acessar a Internet.

```
Configuração do roteador Lab_C:
Hostname Lab_C
!
interface GigabitEthernet0/0
ip address 10.0.1.1 255.255.255.0
!
interface Serial0/1
ip address 10.0.0.2 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
```

Outro detalhe importante do NAT estático é que automaticamente ele ativa o NAT Reverso, ou seja, o computador com endereço 10.0.1.10 poderá ser acessado pela Internet quando vier uma conexão com destino ao IP 12.36.47.2.

### 3.2 Configurando NAT Dinâmico

Para configurar o NAT dinâmico você terá que definir uma faixa de endereços externos (outside global) que você utilizará para tradução e também quais endereços internos (inside global) poderão ser traduzidos.

Essa **faixa de endereços externos** recebe o nome de “**pool**” de endereços. Já a **faixa de endereços internos** é definida utilizando uma **ACL**.

**1)** Crie um pool de endereços globais que serão alocados dinamicamente conforme a necessidade com o comando “**ip nat pool**”:

```
Router(config)#ip nat pool name ip-inicial ip-final netmask máscara
```

O parâmetro **name** é o nome do pool que será utilizado mais tarde no comando “**ip nat inside**”. Após o nome do pool você deverá configurar o range de IPs desse pool colocando o IP inicial e o IP final. Depois de definido o range do pool entre com a máscara de subrede a ser utilizada. Por exemplo, o seu pool terá o nome teste, utiliza os IPs 12.0.0.1, 12.0.0.2 e 12.0.0.3 com a máscara /24, então o comando será:

```
Router(config)#ip nat pool teste 12.0.0.1 12.0.0.3 netmask 255.255.255.0
```

No exemplo acima os IPs da rede interna serão traduzidos com os IPs 12.0.0.1 a 3, ou seja, apenas três computadores da rede interna poderiam acessar o Internet simultaneamente.

**2)** Configure uma access list IP padrão permitindo os “**inside local addresses**” (endereços internos) que poderão ser traduzidos:

```
Router(config)#access-list <1-99> permit rede_de_origem máscara_curinga
```

**3)** Estabeleça traduções dinâmicas da origem, especificando a ACL definida no passo anterior para seleção dos IPs que poderão ser traduzidos:

```
Router(config)#ip nat inside source list número_da_ACL pool nome_do_pool
```

No parâmetro “**source list**” coloque o **número da ACL** criada no **passo 2**. Para o parâmetro **pool** configure o **nome do pool** criado no **passo 1**.

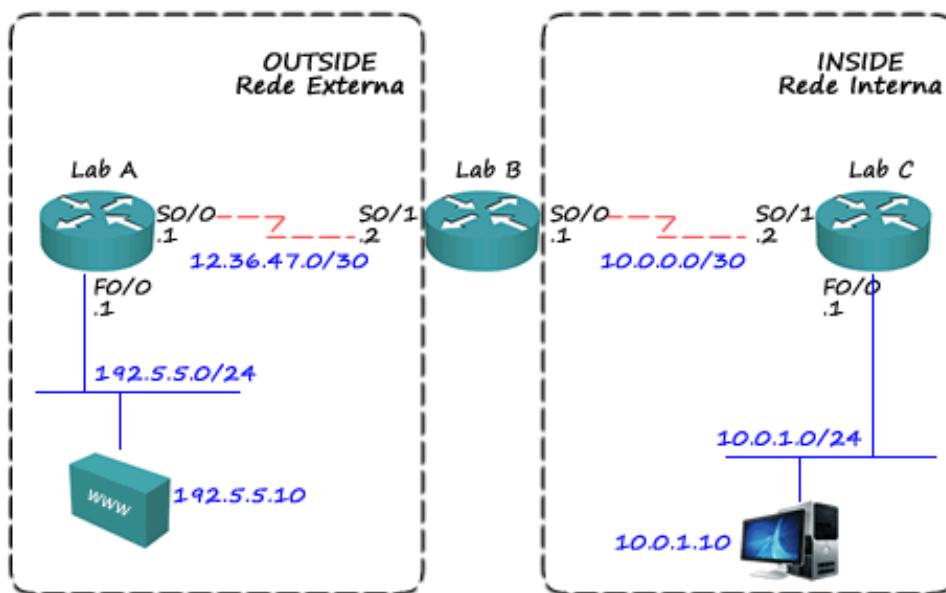
**4)** Defina a interface interna por onde o IP a ser traduzido acessa a rede externa (**inside**):

```
Router(config-if)#ip nat inside
```

**5)** Defina a interface que se conecta a externa (**outside**):

```
Router(config-if)#ip nat outside
```

Ao seguir teremos um exemplo de configuração do NAT dinâmico utilizando a topologia mostrada anteriormente. Para esse exemplo a rede entre as seriais do Lab\_A e B foi alterada para uma máscara /28, assim teremos mais IPs para configuração do pool de IPs que serão utilizados pelo NAT.



Configuração do roteador Lab\_A:

```
hostname LAB_A
!
interface GigabitEthernet0/0
ip address 192.5.5.1 255.255.255.0
!
interface Serial0/0
ip address 12.36.47.1 255.255.255.240
```

Configuração do roteador com função de NAT Lab\_B:

```
Hostname Lab_B
!
interface Serial0/0
ip address 10.0.0.1 255.255.255.252
ip nat inside
!
interface Serial0/1
ip address 12.36.47.2 255.255.255.240
ip nat outside
!
ip nat pool testedinamico 12.36.47.3 12.36.47.10 netmask 255.255.255.240
ip nat inside source list 1 pool testedinamico
!
```

```
ip route 0.0.0.0 0.0.0.0 Serial0/1
ip route 10.0.1.0 255.255.255.0 Serial0/0
!
access-list 1 permit 10.0.0.0 0.0.255.255
```

A configuração do Lab\_C não sofreu alterações.

No comando “**ip nat pool**” foi criado um pool com o nome testedinamico, que tem configurado a faixa de IPs de 12.36.47.3 a 10, ou seja, oito IPs serão utilizados na tradução para acesso a Internet. A máscara de subrede é uma /28.

No comando “**ip nat inside**” foi configurada a lista de acesso 1 para definir que endereços internos podem ser traduzidos. O pool “testedinamico” define os IPs externos que servirão para a tradução.

Por exemplo, quando o computador 10.0.1.10, pertencente à rede do Lab\_C tentar acessar a Internet ele irá alcançar a interface serial 0/0 do Lab\_B (a qual é a interface interna – inside global), o Lab\_B verificará na ACL 1 se o IP pode acessar o NAT, então o IP será trocado por um IP do pool “testedinamico” (por exemplo o IP 12.36.47.3) e enviará pela interface s0/1 em direção a Internet. Quando o computador remoto responder a requisição para o IP 12.36.47.3, o Lab\_B consultará a tabela de traduções e verificará para quem o IP foi emprestado e encaminhará a resposta ao computador que originou a solicitação.

### 3.3 Configurando PAT

O **port address translation** além de traduzir o endereço IP também utiliza os números de porta TCP na tradução. Isso pode trazer uma economia no número de IPs necessários no lado externo para tradução, pois com apenas um IP externo você pode executar até 65 mil traduções, pois é aproximadamente o número de portas TCP que existem.

O que ativa o uso das portas TCP e UDP nas traduções é a opção **overload** que deve ser colocada no final da definição do NAT em modo de configuração global.

**1)** Defina uma “access list” IP padrão selecionando os “inside local addresses” que serão traduzidos:

```
Router(config)#access-list <1-99> permit rede_de_origem máscara_curinga
```

**2)** Estabeleça uma tradução dinâmica dos endereços com o comando “**ip nat inside**”, especificando os IPs internos que poderão acessar a rede externa via o PAT utilizando a ACL definida no passo anterior:

```
Router(config)#ip nat inside source list número_ACL interface interface overload
```

No parâmetro “source list” você deve colocar o número da lista criada no passo 1 que define os IPs que irão acessar o PAT. No parâmetro “interface” você deve indicar a interface de saída (outside global interface) que está ligada à rede externa. O parâmetro “overload” ativa o PAT, ou seja, a tradução por IP e porta TCP ou UDP.

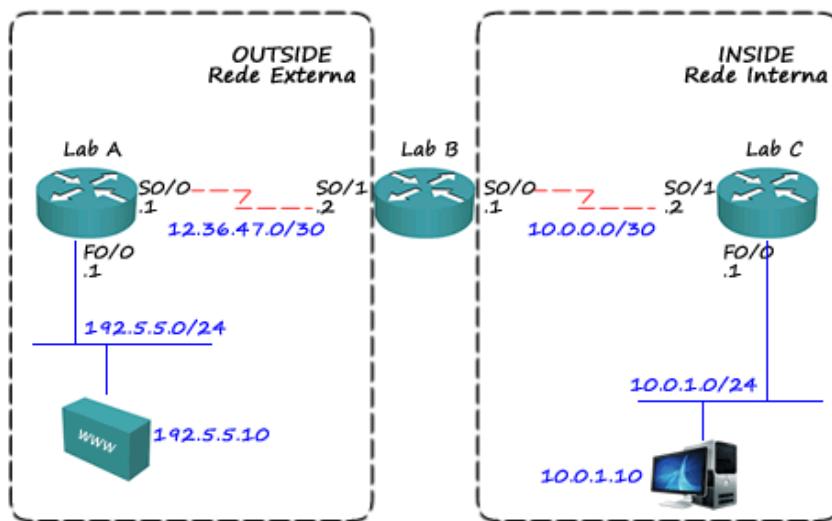
**3)** Defina a interface interna por onde o IP a ser traduzido acessa a rede externa (inside):

```
Router(config-if)#ip nat inside
```

4) Defina a interface que se conecta a externa (outside):

```
Router(config-if)#ip nat outside
```

Ao exemplo s seguir de **configuração do PAT** utilizando a mesma topologia mostrada nos exemplos do NAT.



Na configuração mostrada a lista de acesso 1 define que os IPs de 10.0.0.0 até 10.0.255.255 podem ser traduzidos através do PAT. Além disso, a serial 0/1 será utilizada como interface externa com overloading, ou seja, com transbordo de endereço, pois apenas o IP da serial 0/1 será utilizado para traduzir quaisquer IPs que queiram acessar a Internet.

Configuração do roteador com função de PAT Lab\_B:

```
Hostname LAB_B
!
interface Serial0/0
ip address 10.0.0.1 255.255.255.252
ip nat inside
!
interface Serial0/1
ip address 12.36.47.2 255.255.255.252
ip nat outside
!
ip nat inside source list 1 interface Serial0/1 overload
!
ip route 0.0.0.0 0.0.0.0 Serial0/1
ip route 10.0.1.0 255.255.255.0 Serial0/0
!
access-list 1 permit 10.0.0.0 0.0.255.255
```

### 3.4 Configurando o PAT com Pool

Outra configuração possível com o PAT é utilizar o recurso que fizemos com o NAT Dinâmico e definir mais de um IP Global Outside (IPs válidos) para serem utilizados no acesso à Internet fazendo o PAT Dinâmico ou com Pool.

Basta para isso configurar um Pool assim como fizemos para o NAT dinâmico, por exemplo, você recebeu os IPs válidos do seu ISP na faixa 200.200.200.0 /29 e deseja configurar todos esses IPs para o PAT basta configurar um pool conforme abaixo:

```
ip nat pool PATdinamico 200.200.200.1 200.200.200.6 netmask 255.255.255.248
```

Aí para criar a tradução e aplicar nas interfaces continua a mesma coisa, porém não podemos esquecer a opção **overload** no final da definição do NAT em modo global. Veja como fica a configuração completa do exemplo anterior com o PAT dinâmico.

```
Hostname Lab_B
!
access-list 1 permit 10.0.0.0 0.0.255.255
!
interface Serial0/0
 ip nat inside
!
interface Serial0/1
 ip nat outside
!
ip nat pool PATdinamico 200.200.200.1 200.200.200.6 netmask 255.255.255.248
ip nat inside source list 1 pool PATdinamico Overload
```

Note que ao invés de referenciar a uma interface apenas configuramos a referência do lado outside com o Pool PAT dinâmico e no final inserimos a opção overload para que o roteador faça a tradução de endereço e portas TCP/UDP.

### 3.5 Mantendo e Monitorando o NAT e PAT

Para a manutenção e monitoração do NAT e PAT utilize os comandos:

- “**Show ip nat translations**” – Mostra as traduções feitas pelo NAT/PAT.
- “**Show ip nat statistics**” – Mostra as estatísticas do NAT/PAT.

Veja a seguir as saídas dos comandos a seguir.

```
LAB_B#sho ip nat ?
statistics      Translation statistics
translations   Translation entries
LAB_B#sho ip nat translations
Pro           Inside global        Inside local          Outside local        Outside
global
icmp 12.36.47.2:8752  10.0.1.1:8752    192.5.5.1:8752    192.5.5.1:8752
icmp 12.36.47.2:8753  10.0.1.1:8753    192.5.5.1:8753    192.5.5.1:8753
icmp 12.36.47.2:8754  10.0.1.1:8754    192.5.5.1:8754    192.5.5.1:8754
icmp 12.36.47.2:8755  10.0.1.1:8755    192.5.5.1:8755    192.5.5.1:8755
icmp 12.36.47.2:8756  10.0.1.1:8756    192.5.5.1:8756    192.5.5.1:8756

LAB_B#sho ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
Serial0/1
Inside interfaces:
Serial0/0
Hits: 75 Misses: 75
Expired translations: 75
Dynamic mappings:
Inside Source
[Id: 1] access-list 1 interface Serial0/1 refcount 0
```

No comando acima podemos ver na primeira linha o número de traduções, depois as interfaces configuradas com outside, na sequência as insides e depois o total de Hits/Misses, ou seja, quantos computadores tentaram tradução (Hits) e quantos não foram traduzidos (Misses). Aqui temos 100% de eficácia. Se o número de misses aumentar muito é sinal que algo está errado com seu NAT, pode ser processamento ou esgotamento dos endereços alocados.

Para limpar as traduções feitas pelo NAT e PAT utilize o comando “**clear ip nat translations**”, conforme mostrado ao lado.

Note que no exemplo ao lado foram excluídas de maneira forçada todas as traduções feitas pelo NAT e ao entrar com o comando “**show ip nat translations**” nenhuma entrada foi visualizada.

```
LAB_B#clear ip nat translation ?
Delete all dynamic translations
forced Delete all dynamic translations (forcefully)
inside Inside addresses (and ports)
outside Outside addresses (and ports)
tcp Transmission Control Protocol
udp User Datagram Protocol
LAB_B#clear ip nat translation forced
LAB_B#sho ip nat translations
LabB#
```

Para visualização online do NAT e PAT utilize os comandos de debug relacionados, conforme exemplo abaixo. O mais utilizado é o “debug ip nat”, que mostra em tempo real as traduções sendo realizadas.

```
R1#debug ip nat ?
<1-99>      Access list
detailed      NAT detailed events
fragment      NAT fragment events
generic       NAT generic ALG handler events
h323          NAT H.323 events
ipsec         NAT IPSec events
nvi           NVI events
piggyback    NAT Piggyback support events
port          NAT PORT events
pptp          NAT PPTP events
route         NAT Static route events
sbc           NAT SIP Session Border Controller events
sip            NAT SIP events
skinny        NAT skinny events
vrf            NAT VRF events
wlan-nat     WLAN NAT events
<cr>

R1#debug ip nat
IP NAT debugging is on
006415: Jul 18 2013 17:17:07.603 BR: NAT*: s=198.57.234.87, d=192.168.10.2-
>192.168.1.22 [29274]
006416: Jul 18 2013 17:17:07.607 BR: NAT*: s=192.168.1.22->192.168.10.2,
d=198.57.234.87 [12276]
006417: Jul 18 2013 17:17:07.619 BR: NAT*: s=198.57.234.87, d=192.168.10.2-
>192.168.1.22 [12067]
006418: Jul 18 2013 17:17:07.619 BR: NAT*: s=198.57.234.87, d=192.168.10.2-
>192.168.1.23 [0]
006419: Jul 18 2013 17:17:07.619 BR: NAT*: s=192.168.1.22->192.168.10.2,
d=198.57.234.87 [12277]
```

```
006420: Jul 18 2013 17:17:07.619 BR: NAT*: s=192.168.1.23->192.168.10.2,
d=198.57.234.87 [25888]
006421: Jul 18 2013 17:17:07.623 BR: NAT*: s=192.168.1.23->192.168.10.2,
d=64.210.72.64 [25889]
```

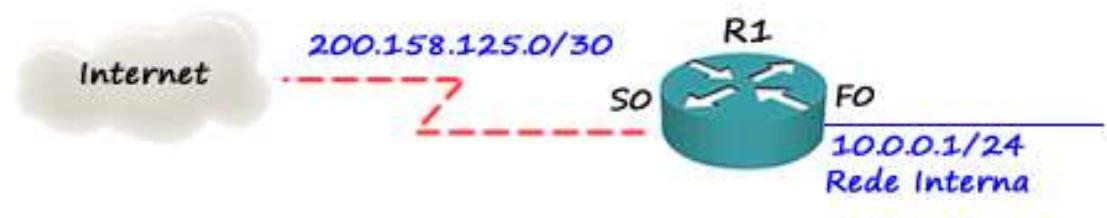
Na linha em destaque podemos ver que o endereço interno 192.168.1.23 está usando o endereço inside global 192.168.10.2 e está se comunicando com o destino 64.210.72.64.

#### 4 Configurando uma Topologia Completa com Saída para a Internet

Nesse tópico vamos estudar alguns exemplos práticos de configuração completa de roteadores, incluindo a saída para a Internet e NAT/PAT.

##### 4.1 Exemplo Prático 1 – Configuração de um Branch Office

Para esse exemplo vamos considerar a topologia mostrada na figura abaixo.



Nesse exemplo você foi designado para configurar o roteador de um pequena empresa chamada **XYZ.com Comunicações** que está migrando o acesso de Internet via banda larga por um link dedicado de 2Mbps. Foi adquirido um roteador ISR-G2 modelo Cisco 1941 com uma interface serial HWIC-2T, a qual foi instalada no **slot 0** do roteador.

Além disso, esse roteador possui duas interfaces de LAN em Giga (Giga0/0 e Giga0/1)

Você terá que configurar o roteador, passando a rede interna para ele e a saída de Internet com um PAT dinâmico com overload, ou seja, apenas um IP será utilizado para traduzir os micros da rede Interna quando houver acesso à Internet. Além disso, o fornecimento automático de IP's via DHCP deverá ser migrado para o roteador.

Atualmente é reservada a faixa de IP's de 1 a 20 para uso dos equipamentos de rede e impressoras e os demais IP's são fornecidos aos computadores. A rede Interna a ser utilizada é a 10.0.0.0/24, sendo que o IP da interface LAN do roteador é o 10.0.0.1/24.

Os IP's da Internet são 200.158.125.1 para a ponta da operadora e o 200.158.125.2 para o roteador da empresa.

Passos de configuração a serem seguidos:

- Configuração geral do roteador: hostname, senhas, banner do dia, criptografia das senhas em modo texto, acesso remoto via SSH para melhorar a segurança, etc.
- Configuração das Interfaces LAN e WAN
- Configuração da rota para Internet
- Testes de conectividade do roteador com a Internet
- Configuração e testes do DHCP
- Configuração do PAT com Overload e testes de conectividade dos micros com a Internet
- Salvar a configuração na NVRAM
- Fazer backup da configuração em um servidor TFTP

- Configuração do switch local (modelo 2960 com 24 portas 10/100/1000 mais 2 portas giga para conexão de Uplink) com hostname SWlocal1, mesmas configurações globais do roteador e endereço de gerenciamento 10.0.0.2/24.
- Implementar a segurança de portas no switch permitindo no máximo 3 MACs seguros e em caso de violação a porta deve ser desativada e enviar mensagem ao gerenciamento.
- A porta que conectará o switch ao roteador será a Giga 0/1 e não deve utilizar trunk, pois não utilizaremos VLAN nessa configuração.

Os testes listados acima são recomendados na prática, porém serão omitidos para dar foco aos comandos de configuração nesse exemplo. A Operadora forneceu que o DNS a ser utilizado é o IP 200.200.200.1. As senhas e nome do router são de definição da empresa. O nome do domínio da empresa é xyz.com.br.

```

Router#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Roteador_Internet
Roteador_Internet(config)#enable secret admin@1
Roteador_Internet(config)#username Admin secret admin@2
Roteador_Internet(config)#ip domain-name xyz.com.br
Roteador_Internet(config)#ip name-server 200.200.200.1
Roteador_Internet(config)#crypto key generate rsa modulos 1024
Roteador_Internet(config)#line console 0
Roteador_Internet(config-line)#password admin@2
Roteador_Internet(config-line)#login
Roteador_Internet(config-line)#logging synchronous
Roteador_Internet(config-line)#exec-timeout 5 30
Roteador_Internet(config-line)#line vty 0 15
Roteador_Internet(config-line)#transport input ssh telnet
Roteador_Internet(config-line)#login local
Roteador_Internet(config-line)#logging synchronous
Roteador_Internet(config-line)#exec-timeout 5 30
Roteador_Internet(config-line)#exit
Roteador_Internet(config)#banner motd @
Enter TEXT message. End with the character '@'.
#####
Acesso Restrito
#####
@
Roteador_Internet(config)#service password-encryption
Roteador_Internet(config)#

```

O roteador da operadora também é do fabricante Cisco, por isso utilizaremos o HDLC como encapsulamento da Interface Serial.

```

Roteador_Internet(config)#interface giga 0/0
Roteador_Internet(config-if)#ip address 10.0.0.1 255.255.255.0
Roteador_Internet(config-if)#description LAN da empresa XYZ.com
Roteador_Internet(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Roteador_Internet(config-if)#interface serial 0/0/0
Roteador_Internet(config-if)#ip address 200.158.125.2 255.255.255.0
Roteador_Internet(config-if)#description Circuito conectado a internet
Roteador_Internet(config-if)#bandwidth 2000
Roteador_Internet(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

```

```
Roteador_Internet(config-if)#end  
Roteador_Internet#
```

Como a rede é do tipo Stub, ou seja, com apenas uma saída para a Internet vamos configurar o rotamento com rota estática padrão.

```
Roteador_Internet#config term  
Roteador_Internet(config)#ip route 0.0.0.0 0.0.0.0 200.158.125.1  
Roteador_Internet(config)#
```

Com o comando mostrado, definimos que a saída para a Internet é o roteador da Operadora, poderíamos ainda ter escolhido a Interface local serial 0/0/0 como referência de saída, conforme podemos confirmar com a saída do "show ip route" analisando a tabela de roteamento.

```
Roteador_Internet#sho ip route  
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
- candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route
```

```
Gateway of last resort is 200.158.125.1 to network 0.0.0.0
```

```
10.0.0.0/24 is subnetted, 1 subnets  
C      10.0.0.0 is directly connected, GigabitEthernet0/0  
200.158.125.0/30 is subnetted, 1 subnets  
C      200.158.125.0 is directly connected, Serial0/0/0  
S*    0.0.0.0/0 [1/0] via 200.158.125.1  
Roteador_Internet#
```

Os testes de conectividade podem ser realizados com o uso do ping e telnet para o roteador da Operadora. Mesmo que você não tenha a senha, se aparecer o prompt solicitando é sinal que há comunicação até a camada-7 entre as duas pontas.

Para configurar o DHCP devemos deixar reservados dos IP's 1 a 20 para uso interno e distribuir o restante entre os micros da empresa, conforme dados iniciais passados. Vamos aos demais dados importantes:

- A rede e máscara são 10.0.0.0 255.255.255.0 ou /24
- Gateway padrão para os micros será o roteador – IP 10.0.0.1
- DNS: o domínio dado anteriormente é o xyz.com.br e o IP do DNS fornecido pela Operadora é o 200.200.200.1

Vamos colocar o tempo de expiração do IP para 30 dias (lease time), caso o usuário fique mais de 30 dias sem entrar na rede ele perde o IP e no próximo acesso terá um novo IP alocado. O IP anterior será liberado para uso.

Ao lado, além da configuração, segue o comando "show ip dhcpc binding" que mostra as alocações de IP realizadas pelo DHCP.

```
Roteador_Internet#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Roteador_Internet(config)#no ip dhcp conflict logging  
Roteador_Internet(config)#ip dhcp excluded-address 10.0.0.1 10.0.0.20  
Roteador_Internet(config)#ip dhcp pool LanXYZ
```

```
Roteador_Internet(dhcp-config)#network 10.0.0.0 255.255.255.0
Roteador_Internet(dhcp-config)#default-router 10.0.0.1
Roteador_Internet(dhcp-config)#domain-name xyz.com.br
Roteador_Internet(dhcp-config)#dns-server 200.200.200.1
Roteador_Internet(dhcp-config)#lease 30
Roteador_Internet(dhcp-config)#exit
Roteador_Internet(config)#end
Roteador_Internet#show ip dhcp binding
IP address Client-ID/ Lease expiration Type
Hardware address
10.0.0.21 0001.63A6.0847 --
10.0.0.22 000B.BE57.4699 --
10.0.0.23 0001.9761.41E2 --
Roteador_Internet#
```

Para configurar a tradução dinâmica com overload teremos que:

- Criar a lista de acesso para selecionar os micros da LAN que poderão acessar a Internet.
- Criar o Poll do nat para utilizar como saída para Internet a serial 0/0/0 com overload, ou seja, todos os IP's internos serão traduzidos para o IP da serial e terão suas conexões identificadas com o uso de diferentes portas TCP e UDP.
- Definir as interfaces inside e outside do roteador.

```
Roteador_Internet#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Roteador_Internet(config)#access-list 1 permit 10.0.0.0 0.0.0.255
Roteador_Internet(config)#ip nat inside source list 1 interface serial 0/0/0
overload
Roteador_Internet(config)#
Roteador_Internet(config)#int g0/0
Roteador_Internet(config-if)#ip nat inside
Roteador_Internet(config-if)#
Roteador_Internet(config-if)#int s0/0/0
Roteador_Internet(config-if)#ip nat outside
Roteador_Internet(config-if)#end
Roteador_Internet#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 200.158.125.2:1024 10.0.0.21:1 200.200.10.20:1 200.200.10.20:1024
icmp 200.158.125.2:1025 10.0.0.21:2 200.200.10.20:2 200.200.10.20:1025
icmp 200.158.125.2:1026 10.0.0.21:3 200.200.10.20:3 200.200.10.20:1026
icmp 200.158.125.2:1027 10.0.0.21:4 200.200.10.20:4 200.200.10.20:1027
icmp 200.158.125.2:2 10.0.0.22:2 200.200.10.20:2 200.200.10.20:2
icmp 200.158.125.2:3 10.0.0.22:3 200.200.10.20:3 200.200.10.20:3
icmp 200.158.125.2:4 10.0.0.22:4 200.200.10.20:4 200.200.10.20:4
udp 200.158.125.2:1025 10.0.0.22:1025 200.200.200.1:53 200.200.200.1:53
Roteador_Internet#copy running-config startup-config
```

Configuração geral do switch local:

```
Switch#config term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWlocal1
SWlocal1(config)#enable secret admin@1
SWlocal1(config)#username Admin secret admin@2
SWlocal1(config)#ip domain-name xyz.com.br
SWlocal1(config)#ip name-server 200.200.200.1
SWlocal1(config)#crypto key generate rsa modulus 1024
SWlocal1(config)#line console 0
```

```

SWlocal1(config-line)#password admin@2
SWlocal1(config-line)#login
SWlocal1(config-line)#logging synchronous
SWlocal1(config-line)#exec-timeout 5 30
SWlocal1(config-line)#line vty 0 15
SWlocal1(config-line)#transport input ssh telnet
SWlocal1(config-line)#login local
SWlocal1(config-line)#logging synchronous
SWlocal1(config-line)#exec-timeout 5 30
SWlocal1(config-line)#exit
SWlocal1(config)#banner motd @
Enter TEXT message. End with the character '@'.
#####
Acesso Restrito
#####
@

SWlocal1(config)#service password-encryption

```

Vamos configurar na sequência o IP de gerenciamento do Switch (10.0.0.2) e o gateway apontando para o roteador local (10.0.0.1).

```

SWlocal1(config)#interface vlan 1
SWlocal1(config-if)#ip address 10.0.0.2 255.255.255.0
SWlocal1(config-if)#description Switch de LAN da empresa XYZ.com
SWlocal1(config-if)#no shutdown
%LINK-5-CHANGED: Interface VLAN1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN1, changed state to up
SWlocal1(config-if)#exit
SWlocal1(config)#ip default-gateway 10.0.0.1

```

Agora vamos configurar o Port Security nas portas dos computadores de fast 0/1 até fast 0/24, não vamos alterar as configurações das duas portas Giga.

```

SWlocal1(config)#interface range fast 0/1 - 24
SWlocal1(config-if)#switchport mode access
SWlocal1(config-if)#switchport port-security
SWlocal1(config-if)#switchport port-security maximum 3
SWlocal1(config-if)#switchport port-security violation shutdown
SWlocal1(config-if)#end
SWlocal1#copy running-config startup-config

```

Com esse exemplo você tem uma base de configuração para utilizar em seu dia a dia para pequenas empresas ou escritórios remotos.

#### **4.2 Exemplo Prático 2 – PAT com Pool e DHCP Básico**

Seu roteador possui duas interfaces, a Serial 0/0 que tem a saída para a Internet, e a fast 0/0 que possui a rede Interna conectada. Você recebeu da operadora os IP's válidos de Internet de 200.200.200.1 a 200.200.200.7 /29, sendo que sua interface serial terá o IP 200.200.200.1.

Sua rede Interna está configurada com a rede 172.16.0.16/28 (IP's de 172.16.0.17 a 172.16.0.30). Você deve configurar um NAT dinâmico que permita 14 conexões simultâneas utilizando todos os IP's disponibilizados pela operadora, permitindo acesso à Internet dos micros da rede LAN.

```

ip nat pool exe13 200.200.200.1 200.200.200.7 netmask 255.255.255.248
ip nat inside source list 1 pool exe13 overload
access-list 1 permit 172.16.0.16 0.0.0.15

```

```
end  
copy run start
```

Considerando o mesmo exercício, entre nas interfaces e faça a configuração do “**ip nat inside**” e “**ip nat outside**” corretamente.

```
Interface fast 0/0  
Ip nat inside  
Interface serial 0/0  
Ip nat outside
```

Agora, considerando que o primeiro IP da LAN é o da porta fast do roteador, configure um DHCP básico que forneça IP, máscara e rota default, excluindo o primeiro e segundo IP’s que são do roteador e switch respectivamente.

```
ip dhcp excluded-address 172.16.0.17 172.16.0.18  
ip dhcp pool Exe15  
network 172.16.0.16 255.255.255.240  
default-router 172.16.0.17
```

## 5 Resumo do Capítulo

Bem pessoal, chegamos ao final de mais um capítulo!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Entender os conceitos e aplicações do NAT e PAT.
- Saber configurar, sem dificuldade, o NAT estático e dinâmico em roteadores Cisco.
- Saber configurar, sem dificuldade, o PAT em roteadores Cisco.
- Ser capaz de realizar troubleshooting no NAT e PAT em roteadores Cisco.
- Saber configurar o acesso de uma Intranet com endereços privativos à Internet utilizando NAT e PAT.
- Entender a configuração completa em um brach office (pequeno escritório).

*Agora que já sabemos configurar uma rede completa com roteadores e switches Cisco vamos nos dedicar a aprender como resolver problemas básicos que fazem parte do escopo do CCENT e também os requisitos e ferramentas básicas para administrar redes com roteadores e switches Cisco.*

*Aproveite o capítulo e bons estudos!*

## **Capítulo 12 - Troubleshooting e Administração de Dispositivos Cisco**

### **Objetivos do Capítulo**

Ao final desse capítulo você terá estudado e deverá compreender:

- Entender e utilizar ferramentas de troubleshooting através de comandos show e debug.
- Entender os principais problemas e recursos de troubleshooting em interfaces LAN e WAN.
- Entender e saber utilizar o protocolo CDP para resolver problemas e descobrir informações sobre vizinhos de rede.
- Entender o encaminhamento de quadros em redes com switches.
- Entender e aplicar comandos para resolver problemas com interfaces de switches, VLANs e trunks.
- Entender os princípios de administração em redes com switches e roteadores Cisco.

## Sumário do Capítulo

<b>1</b>	<i>Introdução</i>	<b>461</b>		
<b>2</b>	<i>Como Iniciar um Processo de Troubleshooting?</i>	<b>461</b>		
<b>3</b>	<i>Analizando Problemas com as Configurações Gerais</i>	<b>462</b>		
<b>4</b>	<i>Cisco Discovery Protocol</i>	<b>464</b>		
4.1	CDP Aplicado em Situações Práticas	465		
<b>5</b>	<i>Link Layer Discovery Protocol (LLDP)</i>	<b>469</b>		
<b>6</b>	<i>Examinando e Resolvendo Problemas em Interfaces</i>	<b>470</b>		
6.1	Um pouco mais sobre Comando Show Interfaces	471		
6.2	Problemas Comuns e Testes em Interfaces LAN e WAN	475		
6.3	Problemas com Half/Full-Duplex	476		
6.4	Testando as Interfaces com Ping e Traceroute	478		
6.5	Verificando a Tabela ARP	479		
<b>7</b>	<i>Analizando o Encaminhamento de Quadros em Switches</i>	<b>480</b>		
7.1.1	Analizando o Encaminhamento de Quadros – Exemplo Prático	481		
7.1.2	Quadro sendo Filtrado na Porta?	484		
<b>8</b>	<i>Analizando Problemas com VLANs e Trunks</i>	<b>486</b>		
8.1	Portas de Acesso Alocadas à VLANs Erradas	486		
8.2	VLANs não Existem ou estão Desabilitadas	486		
8.3	VLANs Bloqueadas na Lista dos Trunks	487		
8.4	Interfaces Configuradas como Trunk não Sobem	488		
<b>9</b>	<i>Utilizando o Comando Debug</i>	<b>489</b>		
<b>10</b>	<i>Dicas Sobre Administração de Roteadores e Switches Cisco</i>	<b>491</b>		
10.1	Verificando a Memória e CPU dos Dispositivos	492		
<b>11</b>	<i>Resumo do Capítulo</i>	<b>493</b>		

## 1 Introdução

O troubleshooting ou resolução de problemas com a atualização do CCNA ganhou um destaque especial, porém ela foi espalhada de maneira desigual entre as duas provas que compõe o CCNA Routing & Switching, pois no CCENT (exame 100-105) o foco é a resolução de problemas em redes LAN, principalmente em redes com switches e VLANs, sendo os assuntos mais pertinentes os quatro tópicos abaixo:

- **Cisco Discovery Protocol (CDP):** Usado para confirmar a documentação, e aprender sobre a topologia da rede, para prever o funcionamento normal da rede.
- **Link Layer Discovery Protocol (LLDP):** é a versão aberta (não proprietária) do protocolo CDP.
- **Examinando o estado das interfaces:** As interfaces devem estar operacionais antes de um switch encaminhar quadros através delas (UP/UP). Por isso devemos saber determinar se uma interface está funcionando e também as causas potenciais (root cause ou causa raiz) de problemas em portas de switches que podem fazer com que ela pare de encaminhar quadros.
- **Analizando como os pacotes são encaminhados:** Devemos saber como analisar tabela de endereços MAC de um switch e prever como ele irá encaminhar um quadro em particular através de suas interfaces.
- **Analizando VLANs e VLAN trunking:** Mantendo o foco na camada 2, nessa última seção analisaremos o que pode dar errado com VLANs e trunks.

Para manter também o foco tanto na prova como na vida prática dos nossos alunos, inserimos um capítulo sobre como administrar redes com roteadores e switches Cisco, passando um pouco do que já sofremos em situações práticas para ajudá-lo a manter sua rede organizada e simplificar o processo de resolução de problemas.

## 2 Como Iniciar um Processo de Troubleshooting?

Ao longo dos capítulos já fomos mostrando o processo de troubleshooting em redes com roteadores e switches Cisco, agora vamos mostrar mais opções e formas para você poder organizar mentalmente o processo e poder se preparar para a prova, pois mesmo antes da prova é necessário que você inicie a sua preparação para resolver problemas que com certeza irão ser cobrados sobre situações de problema e a resolução com base em comandos (show e debug) e também no comportamento normal do funcionamento dos dispositivos.

Existem vários processos e metodologias para resolver problemas, mas para o CCENT vamos recomendar o mesmo processo recomendado na bibliografia oficial, seguindo os passos abaixo:

1. **Analizar ou prever o funcionamento normal:** prever os detalhes do que deve acontecer se a rede está funcionando corretamente, com base em documentação, configuração e comandos show e debug.
2. **Isolar o Problema e documentar:** determinar até onde no caminho esperado do quadro/pacote a comunicação está fluindo normalmente, novamente com base em documentação, configuração, comandos ping, traceroute, show e debug. Após encontrar o problema ele deve ser devidamente documentado no sistema de gerenciamento de incidentes/problemas que normalmente as empresas possuem.
3. **Analisar a causa raiz:** Identificar as causas dos problemas identificados na etapa anterior e determinar uma ação específica para resolver o problema.
4. **Resolver o problema ou escalar?:** em alguns casos o problema não poderá ser identificado no seu nível de atuação ou a resolução será complexa, envolvendo áreas e privilégios que você não possui e aí? O que fazer nesses casos? Normalmente as empresas possuem um processo de "escalation" que é passar o problema para um nível

superior. Esse processo pode ser passar o problema para um nível técnico superior ao seu ou então até mesmo para a gerência definir os próximos passos para a resolução.

5. **Verificar e monitorar a solução:** após todos os passos anteriores realizados você precisa certificar-se que realmente o problema foi resolvido. Em alguns casos alguns comandos show já garantem isso, porém vão existir casos mais complexos que será necessário acompanhar o ambiente ou dispositivo afetado por um tempo. Esse acompanhamento mais longo ou monitoração deve ser realizada quando a causa raiz do problema não foi identificada para garantir que o problema não volte a acontecer.

Resumindo, sabendo como é o funcionamento normal da rede podemos identificar onde o problema está acontecendo, descobrindo onde o problema está podemos analisar a situação e encontrar uma solução específica para resolvê-lo.

Levando em conta o modelo OSI podemos fazer também uma análise por camadas, começando da camada física e indo em direção à aplicação, porém em prova os problemas mais simples de serem cobrados são os envolvendo as camadas de enlace e de rede.

Portanto, para usar essa metodologia é importante lembrarmos a teoria do funcionamento da rede, dispositivos e como os quadros e pacotes são enviados através da topologia.

Também como interpretar os comandos show e debug para verificar se os dispositivos estão realmente funcionando como esperado, por exemplo, com o “**show running-config**” podemos verificar se um dispositivo recém-implementado foi corretamente configurado.

Além disso, temos que saber como utilizar os comandos ping e traceroute para isolar problemas de camada 3 ou então via Telnet testar se o caminho está funcionando até a camada 7, ou seja, permitindo que as aplicações troquem mensagens de alto nível entre si.

Por isso que ao longo do curso fomos mostrando comandos show e metodologias para descobrir se a configuração foi aplicada corretamente, ou seja, mostrando como é o funcionamento normal da rede.

Mais uma vez vamos frisar a importância de entender como se dá o fluxo de quadros na camada 2 quando utilizamos Hubs ou switches, como os pacotes são enviados em uma rede LAN ou através da WAN, os protocolos envolvidos (ARP, DNS, etc.) e assim por diante.

Por exemplo, em uma topologia simples, onde temos dois computadores conectados a um mesmo switch e pertencentes à mesma VLAN será muito mais simples de resolver que em uma topologia mais complexa envolvendo roteadores se comunicando através da WAN, pois no segundo cenário podem estar envolvidos problemas de roteamento e situações mais complexas.

Vamos a seguir analisar problemas e mostrar o uso de ferramentas de troubleshooting para identificação e resolução deles.

### 3 Analisando Problemas com as Configurações Gerais

Apesar de simples, as configurações gerais podem ser cobradas em exercícios de laboratórios (simulados) e é importante que o aluno costume-se desde já a inserir os dados conforme solicitados nos exercícios, por exemplo, se o enunciado pede para que o Hostname de um dispositivo seja Cisco1, se você colocar Cisco vai perder a pontuação referente ao comando, por isso preste bem atenção no enunciado. É importante ler o enunciado e anotar o que deve ser configurado, essa é a fase de planejamento.

É comum nos laboratórios de configuração geral serem fornecidas senhas diferentes para cada tipo de acesso, por exemplo, cisco1 para enable, cisco2 para console e cisco3 para VTY, tenha

cuidado para digitar as senhas corretas e lembre que elas são “case-sensitive”, ou seja, há diferenciação entre letras maiúsculas e minúsculas.

Após inserir os comandos execute um “show run” (show running-config) para certificar-se que tudo está correto.

Nas lines VTY, as quais têm os acessos via telnet e SSH, o seu funcionamento depende da definição de uma senha, se não houver uma senha ou processo de autenticação definido para a line VTY ela não conecta, veja a mensagem de erro na figura 1 ao lado onde o roteador responde ao ping, ou seja, há conectividade em camada 3 entre os dispositivos, porém o telnet não é aceito pela senha não estar configurada.

```
DlteC-Teste#ping 192.168.1.3
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/5 ms
```

```
DlteC-Teste#telnet 192.168.1.3  
Trying 192.168.1.3 ...Open  
  
[Connection to 192.168.1.3 closed by foreign host]  
DlteC-Teste#
```

Agora entramos no dispositivo remoto e fizemos a configuração da senha das lines VTY conforme abaixo, porém não configuramos uma senha de enable, veja o que ocorre quando tentamos acessar o modo privilegiado do roteador.

```
DlteC-Teste#telnet 192.168.1.3  
Trying 192.168.1.3 ...Open
```

```
User Access Verification
```

```
Password:  
Router>enable  
% No password set.  
Router>
```

Portanto, sem uma senha de enable mesmo com a line configurada corretamente via telnet não conseguiremos acessar o modo privilegiado, para corrigir esse problema temos que entrar no roteador remoto e configurar um “enable secret”, conforme abaixo.

```
Router(config)#line vty 0 15  
Router(config-line)#pass cisco  
Router(config-line)#login  
Router(config-line)#exit  
Router(config)#enable secret cisco  
Router(config)#
```

Agora veja a nova tentativa de acesso com a senha da VTY e de enable configuradas.

```
DlteC-Teste#telnet 192.168.1.3  
Trying 192.168.1.3 ...Open
```

```
User Access Verification
```

```
Password: → Senha da VTY
```

```
Router>enable
Password: → Senha de enable
```

#### 4 Cisco Discovery Protocol

O **CDP** é um **protocolo proprietário da Cisco** com função de **descobrir** informações sobre **vizinhos** de rede. Ele irá descobrir informações apenas das **interfaces diretamente conectadas** e não de redes remotas.

O CDP trabalha na **camada-2** do modelo OSI, sendo que seu enquadramento é feito com quadros SNAP. É importante lembrar que o CDP vem habilitado em todas as interfaces dos roteadores e switches.

Você poderá verificar as seguintes informações via CDP:

- Informações similares ao **show version**
- Um endereço por protocolo roteado
- Portas de entrada e saída
- Plataforma de hardware e versão do Cisco IOS
- Nome do vizinho (hostname)

Para desabilitar o CDP você pode fazer em modo de configuração global, desabilitando em todas as interfaces simultaneamente, ou dentro de cada interface. Veja um exemplo abaixo.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
!desabilita o CDP para todo o roteador
Router(config)#no cdp run
!habilita o CDP para todo o roteador
Router(config)#cdp run
Router(config)#interface s0/0
!habilita o CDP para uma interface específica
Router(config-if)#cdp enable
!desabilita o CDP para uma interface específica
Router(config-if)#no cdp enable
Router(config-if)#end
Router#
```

Para visualizar as informações obtidas pelo CDP utilize os comandos:

```
SW-DlteC#show cdp ?
entry      Information for specific neighbor entry
interface  CDP interface status and configuration
neighbors   CDP neighbor entries
tlv         CDP optional TLVs
traffic    CDP statistics
|
<cr>
```

Para verificar as informações sobre os vizinhos utilize o “**show cdp neighbors**”, com o comando “**show cdp neighbors detail**” você terá informações mais detalhadas. Veja o exemplo abaixo.

```
LAB_A#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID    LocalIntrfce Holdtme Capability  Platform          Port ID
Switch Fas   0/1           155      S I       WS-C2950-2        Fas 0/2
Switch Fas   0/0           155      S I       WS-C2950-2        Fas 0/1
Lab_B Ser    0/0.1         133      R         2620XM            Ser 0/0.1
```

LAB_C Ser	0/0.200	164	R	2620XM	Ser 0/0.1
Lab_D Ser	0/0.300	164	R	1721	Ser 0.1

Para verificar informações sobre um vizinho específico, entre com o comando “**show cdp entry hostname\_do\_vizinho**”. O comando “**show cdp entry \***” tem a mesma função do comando “**show cdp neighbors detail**”.

```
LAB_A#show cdp entry Lab_B

Device ID: Lab_B
Entry address(es):
IP address: 192.168.0.2
Platform: cisco 2620XM, Capabilities: Router
Interface: Serial0/0.1, Port ID (outgoing port): Serial0/0.1
Holdtime : 127 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JSX-M), Version 12.2(121),
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Thu 21-Apr-05 02:54 by kellmill
advertisement version: 2
```

Para verificar as informações sobre os timers do CDP, utilize o comando “**show cdp interfaces**” e, sobre o tráfego trocado e estatísticas do CDP, utilize o comando “**show cdp traffic**”.

```
LAB_A#show cdp traffic
CDP counters :
  Total packets output: 8443,   Input: 8435
  Hdr syntax: 0,   Chksum error: 0,   Encaps failed: 12
  No memory: 0,   Invalid packet: 0,   Fragmented: 0
  CDP version 1 advertisements output: 0,   Input: 0
  CDP version 2 advertisements output: 8443,   Input: 8435
LAB_A#show cdp interface serial 0/0.1
Serial0/0.1 is up, line protocol is up
  Encapsulation FRAME-RELAY
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

O CDP troca informações de 60 em 60 segundos. Em caso de perda de comunicação com o vizinho ele guarda a informações por 180s antes de retirá-la de sua base de dados (holdtime). Para alterar esses valores utilize os comandos mostrados a seguir.

```
!altera o valor do timer do CDP
LAB_A(config)#cdp timer ?
  <5-254> Rate at which CDP packets are sent (in sec)
!altera o valor do holdtime do CDP
LAB_A(config)#cdp holdtime ?
  <10-255> Length of time (in sec) that receiver must keep this packet
```

#### 4.1 CDP Aplicado em Situações Práticas

Conforme analisamos anteriormente, o CDP roda na camada 2 do modelo OSI, ou seja, na camada de enlace, portanto ele pode ser utilizado para verificar se há conectividade de camada 2 em casos de problemas de camada 3.

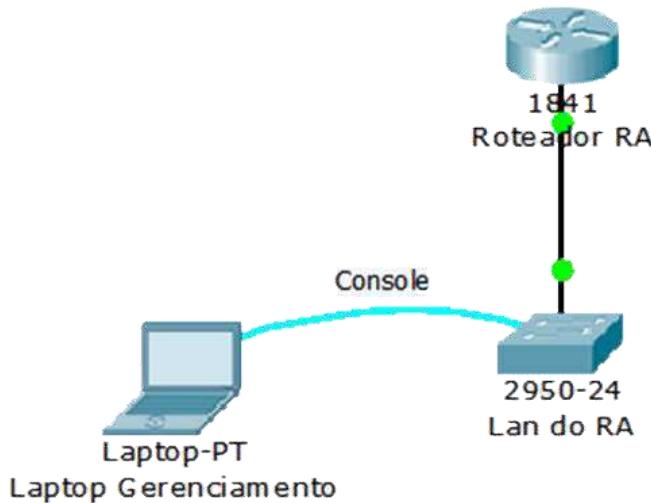
Vamos supor que há uma queda na comunicação IP entre dois roteadores, com o comando "**show cdp neighbor**" você pode verificar se há conectividade de camada 2. Caso o roteador vizinho não apareça listado no comando significa que há problemas nas duas camadas do modelo OSI.

Outra aplicação útil é a de **descobrir o endereço IP** dos vizinhos diretamente conectados para fazer acesso remoto via Telnet ou SSH.

Por exemplo, você é administrador de redes de uma empresa onde existe um roteador conectado a um switch, o qual você não tem em mãos o IP do roteador, porém está conectado via console no Switch de acesso da rede LAN do roteador. Basta você entrar no switch e dar um dos comandos abaixo conforme para descobrir o IP do roteador:

- **Show cdp neighbor detail**
- **Show cdp entry \***
- Ou o comando "**show cdp neighbor**", descubra o hostname do switch (device ID) e entre com o comando "**show cdp entry device-ID**"

Veja o exemplo citado acima em uma situação prática conforme topologia abaixo.



Primeiro vamos a partir da console do switch entrar com o comando "**show cdp neighbor detail**".

```
SwitchA>show cdp neighbors detail
Device ID: RA
Entry address(es):
  IP address : 192.168.1.1
Platform: cisco C1841, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/0
Holdtime: 110
Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
advertisement version: 2
Duplex: full
```

Acompanhe agora a saída do comando "**show cdp entry \***".

```
SwitchA>sho cdp entry *
Device ID: RA
Entry address(es):
    IP address : 192.168.1.1
Platform: cisco C1841, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/0
Holdtime: 101
Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
advertisement version: 2
Duplex: full
```

Outra maneira de usar o CDP para esse exemplo é utilizando o comando "**show cdp neighbor**" para descobrir o hostname do roteador (device ID) e depois entrar com o comando "**show cdp entry device-ID**" para descobrir o endereço IP, podendo assim entrar via telnet no roteador.

```
SwitchA>show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce     Holdtme   Capability   Platform  Port ID
RA            Fas 0/1          126        R           C1841     Fas 0/0
SwitchA>
SwitchA>show cdp entry RA
Device ID: RA
Entry address(es):
    IP address : 192.168.1.1
Platform: cisco C1841, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/0
Holdtime: 153
Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
advertisement version: 2
Duplex: full
-----
SwitchA>
```

Vamos agora analisar mais de perto a saída dos comandos "**show cdp neighbor**" e "**show cdp neighbor detail**".

No "**show cdp neighbor**" o roteador trouxe as seguintes informações:

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
RA	Fas 0/1	126	R	C1841	Fas 0/0

O **Device ID** é o **hostname** configurado no roteador, a **Local Intrfce** é a **interface local** do switch e o **Port ID** é a **interface remota** - a interface do vizinho - nesse caso do roteador RA.

Temos também a Capability, que é a capacidade do equipamento, ou seja, o tipo do equipamento remoto onde o R representa um roteador.

No “**show cdp neighbor detail**”, “**show cdp entry \***” e “**show cdp entry RA**” temos os mesmos tipos de informações mais detalhadas.

```

Device ID: RA - Hostname do equipamento vizinho
Entry address(es):
  IP address : 192.168.1.1 - endereço IP, aparecerá apenas 1 dos IP's
  configurados
Platform: cisco C1841, Capabilities: Router - modelo do roteador e suas
  capacidades
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/0
  -> Interface é a interface local e o "Port ID (outgoing port)" é a interface do
  equipamento remoto, com as informações acima sabemos que o Swicth está conectado
  pela sua porta Fast 0/1 na porta Fast 0/0 do roteador RA
Holdtime: 101
Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE -> Características do IOS, versão e release
  
```

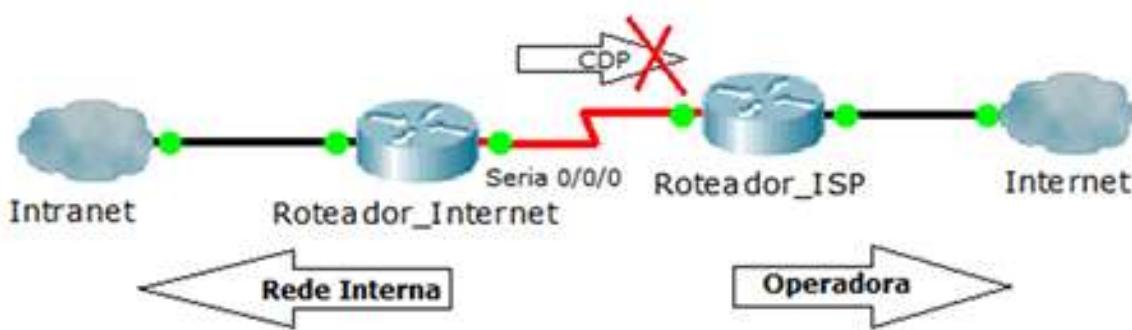
Para finalizar, existem empresas que **consideram o CDP** um **risco** para sua **segurança** e tem como padrão desabilitar o protocolo em seus equipamentos. Para desabilitar o envio e recebimento do CDP em todas as interfaces utilize o comando em modo de configuração global:

```
router(config)#no cdp run
```

Outra necessidade é, por exemplo, na saída de internet de uma empresa sendo realizada através de uma conexão serial (conforme figura ao lado) conectada a um roteador de um provedor de serviços (ISP ou Operadora de Telecom). Nesse caso não há necessidade de trocar CDP com o roteador da operadora, portanto aconselha-se a desabilitar o CDP naquela interface. Para isso, o comando “**no cdp enable**” deve ser aplicado na interface em questão. Veja os comandos para o exemplo da topologia mostrada a seguir.

```

Router_Internet#config term
Router_Internet(config)#interface serial 0/0/0
Router_Internet(config-if)#no cdp enable
Router_Internet(config-if)#end
Router_Internet#
  
```



## 5 Link Layer Discovery Protocol (LLDP)

O protocolo LLDP (IEEE 802.1AB) permite que dispositivos de rede como Servidores, Switches e Roteadores descubram uns aos outros indo além do CDP por ser um protocolo aberto e não limitado aos dispositivos Cisco, ou seja, ele permite que dispositivos de outros fabricantes sejam descobertos também.

Ele opera na camada de enlace do modelo OSI (camada 2) permitindo que informações básicas como hostname, versão do Sistema Operacional , endereço da interface, entre outros, sejam aprendidas dinamicamente por equipamentos diretamente conectados.

A extensão do LLDP chamada de Media Endpoint Discovery extension (LLDP-MED) é muito utilizada para Telefonia IP e provê informações como VLAN de voz a ser utilizada, prioridades na marcação de pacotes e quadros para fins de QoS, identificação do local do dispositivo, funções para PoE, etc.

Por padrão o LLDP vem desabilitado nos roteadores e switches Cisco e para verificar o status do protocolo você pode utilizar o comando "show lldp".

Para ativar e desativar o LLDP utilizamos o comando "lldp run" em modo de configuração global e "no lldp run" respectivamente. Veja exemplo abaixo.

```
SW-DlteC-Rack-01(config)#do show lldp
% LLDP is not enabled
SW-DlteC-Rack-01(config)#lldp run
SW-DlteC-Rack-01(config)#do show lldp
```

### Global LLDP Information:

```
Status: ACTIVE
LLDP advertisements are sent every 30 seconds
LLDP hold time advertised is 120 seconds
LLDP interface reinitialisation delay is 2 seconds
SW-DlteC-Rack-01(config) #
```

Para ativar ou desativar o LLDP em uma interface específica utilize o comando abaixo em modo de configuração de interface:

```
R1(config-if)#[ no ] lldp { receive | transmit }
```

O comando "show lldp neighbors [ type member/module/number ] [ detail ]" permite verificar as mesmas informações que estudamos anteriormente via CDP. Veja exemplo a seguir.

```
SW-DlteC-Rack-01#show lldp neighbors
```

### Capability codes:

```
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

Device ID	Local Intf	Hold-time	Capability	Port ID
SEP0023339D0792	Fa0/8		180	B,T
0023339D0792:P1				
SEP001D7060D31B	Fa0/4		180	B,T
001D7060D31B:P1				
SEP001B0C96C5E8	Fa0/5		180	B,T
001B0C96C5E8:P1				

Total entries displayed: 3

SW-DLteC-Rack-01#

Lembre-se que o uso do LLDP faz-se necessário quando utilizamos dispositivos de outros fabricantes e assim como a recomendação para o CDP também devemos utilizá-lo somente nas portas necessárias, desativando o protocolo onde ele não se faz necessário pelo risco de segurança que ele representa por divulgar informações sobre vizinhos e até mesmo o próprio dispositivo local.

Assim como o CDP o LLDP consegue descobrir vizinhos DIRETAMENTE CONECTADOS, tenha sempre essa informação em mente pois pode ser cobrado no exame.

## 6 Examinando e Resolvendo Problemas em Interfaces

Os problemas mais comuns envolvendo interfaces LAN e WAN são:

1. **Falta do clock rate em interfaces seriais DCE:** nesse caso a interface serial fica em Up / Down.
2. **Encapsulamento errado nas interfaces seriais** (definição do protocolo de camada 2): idem ao sintoma anterior, a interface serial fica em Up / Down.
3. **Falta do comando "no shut" para ativar a interface:** a interface fica em Administratively Down.
4. **Interfaces de switches desabilitadas pelo port security:** o port security desabilita interfaces que excedem o número de MACs seguros configurados.
5. **IP configurado, Máscara de rede/subrede ou ambos configurados errados:** os testes de ping não irão funcionar até a correção do problema, nem sempre há aviso nesses casos, somente se você tentar configurar um IP inválido na Interface (um endereço de rede, broadcast ou de uma faixa já configurada no roteador).

Vale a pena relembrar abaixo o status que o show interfaces pode nos fornecer (*grave muito bem cada uma das condições, seu significado, problemas e como resolvê-los quando aplicável*):

- **up, line protocol is up:** Camadas 1 e 2 funcionando perfeitamente.
- **down, line protocol is down:** Essa saída indica problema na camada física. Pode ser, por exemplo, cabo desconectado nessa interface ou na interface remota. Na prática estes são os problemas mais comuns, ou seja, cabos com problemas ou mal conectados, portanto a resolução passa por verificar o cabeamento ou se a interface remota não está ativada (em shutdown).
- **up, line protocol is down:** Nesse caso a camada física está ok, mas a camada de enlace não. Possíveis razões para isso podem ser problema na configuração do encapsulamento errado em uma das pontas ou clock rate faltando na interface DCE em interfaces seriais. Portanto a resolução do problema se existe alguma interface com um cabo DCE conectado nela (comando show controllers) e inserir o comando **clock rate** se estiver faltando, caso esteja tudo OK verifique se nas duas pontas o protocolo de camada 2 está configurado corretamente no comando **"encapsulation"** dentro da interface (verifique com o show run ou show interfaces). Em interfaces LAN de switches essa é uma condição que dificilmente será encontrada.
- **is administratively down, line protocol is down:** Essa saída indica que a sua interface foi localmente colocada no estado de shutdown. Entre na configuração da interface e dê um "no shutdown".
- **down, line protocol is down (err-disabled):** O **port security** desabilitou a interface devido a uma violação (excede o número de MACs seguros). Verifique os MACs conectados à porta com o "show mac address-table", retire o MAC causador da violação e aplique "shut/no shut" na interface para ela voltar ao normal.

Com isso resolvemos os problemas de 1 a 4.

Para o quinto item a resolução se inicia com um "**show run**" ou "**show interfaces**" ou "**show ip interface brief**" para verificar se o IP e máscara estão configurados corretamente, além

disso, pode ser necessário um cálculo de sub-redes para verificar se escolhemos o IP e a máscara correta.

Lembre-se que IPs como o de broadcast ou de rede não podem ser configurados nas interfaces, veja o erro que será mostrado ao se tentar configurá-los nas interfaces na figura 4 ao lado.

```
DlteC-Teste#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DlteC-Teste(config)#int f0/1
DlteC-Teste(config-if)#ip add 192.168.0.0 255.255.255.0
Bad mask /24 for address 192.168.0.0
DlteC-Teste(config-if)#ip add 192.168.0.255 255.255.255.0
Bad mask /24 for address 192.168.0.255
```

A mensagem de **Bad mask** (máscara errada) indica que para essa máscara esses IPs que tentamos configurar não são válidos, pois são a rede e o broadcast da faixa 192.168.0.0 /24.

Outro erro é o “**overlap**” ou sobreposição de IPs. Isso ocorre quando tentamos configurar um IP de uma rede ou subrede já configurada em outra interface, veja o exemplo abaixo, onde a mensagem de erro diz que a rede 192.168.1.0 já está configurada na interface fast 0/0, por isso não pode ser utilizada para outra interface.

```
DlteC-Teste(config-if)#ip add 192.168.1.4 255.255.255.0
% 192.168.1.0 overlaps with FastEthernet0/0
DlteC-Teste(config-if)#

```

Lembre-se que cada Interface do roteador é um Domínio de Broadcast, por isso cada interface deve estar em uma rede IP única.

## 6.1 Um pouco mais sobre Comando Show Interfaces

Apesar de o comando **show interfaces** ser bem conhecido, a maioria das vezes ele é utilizado apenas para ver se a interface está up ou down. No entanto, muitas outras informações úteis podem ser retiradas da saída desse comando.

O comando pode ser utilizado para exibir informações de todas as interfaces (show interfaces) ou para uma interface específica (show interfaces serial 0/1 – ou simplesmente sh int s0/1). Veja o exemplo da saída do comando abaixo para uma interface serial.

```
Router#show interfaces serial 0/1
Serial0/1 is up, line protocol is up
Hardware is PowerQUICC Serial
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:02, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 8000 bits/sec, 1 packets/sec
5 minute output rate 8000 bits/sec, 1 packets/sec
31468 packets input, 2394818 bytes, 0 no buffer
```

```
Received 31263 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
31475 packets output, 2398672 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
109 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
Router#
```

Vamos agora ver as informações mais importantes ainda não estudadas até o momento, porém dividiremos as explicações em dois blocos.

- **Internet address is 192.168.1.1/24** - esse campo nos diz o endereço IP configurado na interface.
- **MTU** - O MTU (Maximum Transmission Unit ou Unidade Máxima de Transmissão) é 1500 bytes. O MTU refere-se ao tamanho máximo do datagrama que uma camada de um protocolo de comunicação pode transmitir.
- **BW 1544 Kbit/sec** - essa parte nos mostra a largura de banda configurada na interface (comando bandwidth). Caso esse parâmetro não seja configurado em interfaces seriais será adotado o valor padrão de 1544 Kbit/sec. Lembre-se que o parâmetro bandwidth é utilizado por alguns protocolos de roteamento (EIGRP, por exemplo) para calcular a métrica de uma rota. Para as interfaces LAN (Eth, Fast e Giga) não é preciso configurar o bandwidth.
- **DLY** - representa o Delay ou atraso padrão de uma interface. Esse valor é padrão e cada tipo de Interface tem um atraso pré-definido medido em micro segundos, por exemplo, o atraso dessa interface serial é de 20.000 micro segundos, ou seja, 0.02 segundos.
- **Reliability** - é a confiabilidade da interface medida em um máximo de 255, portanto o 255/255 representa que essa interface está 100% confiável. Caso a confiabilidade caia o primeiro valor ficará menor que 255 e quando chegar à zero quer dizer que a interface está inoperante.
- **Tx Load e Rx Load** - é a carga da Interface, ou seja, quantos por cento da largura de banda está sendo utilizada pela Interface. A medida é parecida com o da confiabilidade, ou seja, 1/255 representa que a interface está praticamente sem tráfego, já 255/255 representa que está 100% da sua capacidade de banda em uso.
- **Encapsulation HDLC** - mostra o tipo de encapsulamento utilizado. Como estamos com uma interface serial e deixamos no padrão da interface, está mostrando HDLC. Poderia ser também Frame-Relay ou PPP (no escopo do CCNA).
- **Last input, output** - número de horas, minutos e segundos desde que o último pacote foi recebido ou transmitido com sucesso. Essa informação é útil nos casos de falha da interface para verificar a quanto tempo ela está com problemas.
- **Input queue** - exibe informação sobre o número de pacotes na fila de entrada. Size/max/drops = número atual de quadros na fila / número de máximo permitido de quadros na fila antes de começar a descartar quadros / número atual de quadros descartados devido a ter excedido o máximo permitido.
- **Total output drops** - número de pacotes descartados devido à fila estar cheia. Por exemplo, imagine que uma grande quantidade de tráfego está chegando ao seu roteador através de interfaces com largura de banda de 2Mbps e que todo esse tráfego está saindo por uma outra interface com um link de 64Kbps. Esse excesso de tráfego na interface de 64Kbps pode fazer com que o parâmetro total output drops aumente, pois ela pode não conseguir processar todas as informações e enviá-las a tempo.
- **Output queue** - após os pacotes serem processados, eles são enviados para fila de saída da interface de saída. Essa linha nos mostra o tamanho da fila de saída, o número máximo permitido e os descartados.
- **Minute input/output rate** - exibe a média da taxa de entrada e saída na interface nos últimos 5 minutos. Aqui podemos ver se nossa interface está sobrecarregada ou não.

O segundo bloco da saída do comando exibe informações dos contadores de erros. São esses campos que o comando **clear counters** irá zerar, quando executado. Vamos ver os tipos de erros abaixo.

```
5 minute output rate 8000 bits/sec, 1 packets/sec
31468 packets input, 2394818 bytes, 0 no buffer
Received 31263 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
31475 packets output, 2398672 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
109 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

- **Packets input/output** – número de total de pacotes recebidos/transmitidos pela interface. Monitorar o incremento desse contador é útil para verificarmos se o tráfego está fluindo corretamente pela interface.
- **Broadcasts** - número total de pacotes de broadcast ou multicast recebidos.
- **Runt**s - número de quadros recebidos que são menores do que o tamanho de quadro mínimo do IEEE 802.3 (64 bytes para Ethernet) e com inconsistência no CRC. Possível causa podem ser incompatibilidade no modo duplex ou problemas físicos, como cabeamento, porta ou placa de rede no dispositivo conectado.
- **Giants** - número de quadros recebidos que superam o tamanho máximo permitido pelo IEEE 802.3. Na maioria dos casos esse erro é causado por problema na placa de rede de algum dispositivo (NIC). Procure pelo dispositivo com problema e retire-o da rede.
- **Throttles** - número de vezes que a recepção na porta foi desabilitada, possivelmente devido a uma sobrecarga no buffer do processador. Se exibir um asterisco (\*) logo após o valor, significa que a interface está apresentando o problema no exato momento que o comando foi rodado. Exemplos de pacotes que podem sobrecarregar o buffer do processador são pacotes IP com opções, TTL expirado, encapsulamento non-ARPA, fragmentação, tunelamento, pacotes ICMP e outros.
- **Input Errors** - somatório de todos os erros, incluindo runts, giants, no buffer, CRC, frame, overrun e ignored counts. Outros tipos de erros também podem incrementar esse contador e alguns quadros podem apresentar mais de um tipo de erro.
- **CRC** - esse contador incrementa quando o CRC gerado pelo dispositivo remoto não coincide com o checksum calculado no receptor. Geralmente é um indicativo de ruído ou problema na transmissão. Um elevado número de erros de CRC geralmente é um resultado de um elevado número de colisões, mas também pode ser um indicativo de problemas físicos (cabeamento, NIC) ou disparidade no modo duplex configurado.
- **Frame** - número de pacotes recebidos incorretamente com erros de CRC e um número não inteiro de octetos (erro de alinhamento). Geralmente são causados por colisões, problemas físicos (cabeamento, NIC) ou disparidade no modo duplex configurado.
- **Overrun** - número de vezes que o hardware do receptor não foi capaz de suportar os dados recebidos no hardware do buffer. Ou seja, o tráfego de entrada excedeu a capacidade do receptor.
- **Ignored** - número de pacotes recebidos e ignorados pela interface devido a uma baixa na performance do hardware dos buffers internos da interface. Pode ser causado por tempestades de broadcast e tráfego com rajadas de ruídos.
- **Bytes** - número total de bytes transmitido pelo sistema, incluindo dados e encapsulamento MAC.
- **Underruns** - número de vez que o transmissor do dispositivo remoto operou mais rápido do que o receptor do lado local pode suportar. Isso pode ocorrer, por exemplo, em situações onde uma interface esteja recebendo uma grande quantidade de tráfego em rajadas vindo de outras interfaces. Durante uma situação de overrun a interface pode reiniciar.

- **Output Errors** – somatório dos erros que impediram a transmissão final dos datagramas para fora da interface. Geralmente é causado por um tamanho reduzido da fila de saída.
- **Collisions** - número de vezes que ocorreu uma colisão antes que a interface pudesse transmitir o quadro para o meio com sucesso. Colisões são comuns quando a interface está configurada com half-duplex e não deve ocorrer em interfaces full-duplex. Se o número de colisões aumentarem pode ser indicativo de alta utilização do link ou erro na configuração do modo duplex (um lado full e outro half – o correto é ambos serem full ou half).
- **Interface Resets** – número de vezes que a interface foi completamente resetada.
- **Unknown protocol drops** – esse contador exibe o número de pacotes descartados com protocolo desconhecidos ou não configurados na interface. Caso você não consiga identificar o erro você pode utilizar um sniffer para identificar o protocolo desconhecido.
- **Output buffers swapped out** – esse número indica o número de pacotes que foram armazenados na DRAM quando a fila de saída lotou. Quando a fila de saída da interface de saída está lotada o pacote é copiado para a DRAM, depois é copiado de volta para a fila quando essa estiver livre, como forma de evitar o seu descarte. Normalmente esse número incrementa quando estamos em situação de rajadas de tráfego.
- **Carrier Transitions** – número de vezes que houve a interrupção no sinal da portadora. Pode ser causado por reset na interface ou desconexão do cabo, por exemplo.

Quando realizamos testes na prática muitas vezes é necessário zerar os contadores de erros para que possamos verificar com mais clareza se a interface está ou não incrementando erros.

Para isso existe o comando em modo EXEC privilegiado “**clear counters**”, você pode utilizar, por exemplo, o “**clear counters serial 0/0**” para zerar os contadores somente dessa interface. Para zerar tudo utilize o comando Clear Counters, ele apaga os contadores de todas as interfaces. Veja um exemplo abaixo.

```
dltec#clear counters
Clear "show interface" counters on all interfaces [confirm]
dltec#clear counters fast 0/0
Clear "show interface" counters on this interface [confirm]
dltec#
```

O comando show interfaces que vimos aqui é bem semelhante para as portas LAN de roteadores e switches, o que varia é o tipo de protocolo (**encapsulamento**) e a parte de baixo dos contadores, veja abaixo do comando show interface fast 0/0 abaixo.

```
Switch#show interfaces f0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 000a.f4d3.e481 (bia 000a.f4d3.e481)
    MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
      reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 100BaseTX
  input flow-control is unsupported output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:29:03
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
    5 minute input rate 30000 bits/sec, 7 packets/sec
    5 minute output rate 28000 bits/sec, 5 packets/sec
      11165 packets input, 6022222 bytes, 0 no buffer
```

```
Received 4598 broadcasts (2333 multicast)
  0 runts, 0 giants, 0 throttles
  2 input errors, 2 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 2333 multicast, 0 pause input
  0 input packets with dribble condition detected
  9213 packets output, 5730801 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 PAUSE output
  0 output buffer failures, 0 output buffers swapped out
Switch#
```

No comando acima as partes grifadas onde temos o endereço MAC da Interface, que no caso de um switch é o MAC do switch como um todo, o seu encapsulamento é o ARPA, logo abaixo temos grifado o modo de operação e velocidade da interface (Full-duplex a 100 Mbps) e o timeout do ARP em 4 horas. Em interfaces de roteadores teremos também um endereço IP.

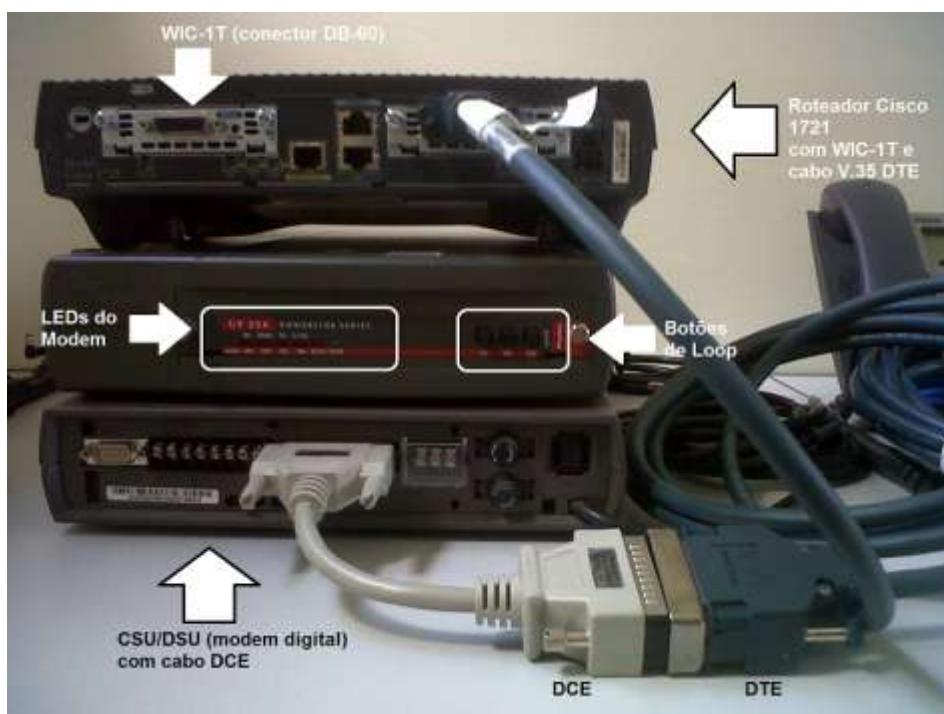
Note que para a interface de LAN temos além do contador de colisões há também um contador chamado “**Late Collisions**” ou colisões atrasadas que ocorrem normalmente fora do esperado do padrão que é até o 64º byte do quadro Ethernet. A possível causa de uma late collision são inconsistência do modo de operação **full-duplex/half-duplex** (os dois lados devem ter a mesma configuração), exceder os limites do tamanho do cabo Ethernet (100m), excesso de hubs na rede ou defeito na placa de rede.

## 6.2 Problemas Comuns e Testes em Interfaces LAN e WAN

O recomendado para testar problemas de conectividade em interfaces LAN e WAN é iniciar da camada física e depois testar a camada de enlace. O problema de camada de rede que pode afetar uma interface LAN ou WAN está relacionado a endereçamento IP, conforme já estudamos anteriormente.

Normalmente em interfaces seriais os problemas são detectados pelo incremento dos Input Errors (erros de entrada) e CRC simultaneamente. O CRC é um check de redundância cíclica que calcula um valor através de um algoritmo (normalmente paridade) e faz uma comparação com um valor previamente calculado na origem. Geralmente Input Errors acompanhados de erros de CRC significam problemas com a linha de transmissão, com o CSU/DSU da operadora de Telecom ou com um dos cabos que conectam a placa serial ao CSU/DSU.

Já o output errors em uma interface serial pode significar que a própria placa está com problemas. Além disso, os sinais indicativos de conexão com o modem ou CSU DSU devem estar todos em UP (DCD=up DSR=up DTR=up RTS=up CTS=up) para que a interface esteja operacional. Estes sinais indicadores de conexão normalmente são representados por LEDs nos CSU/DSUs e nos modems. Veja a figura abaixo.



A maneira mais simples de testar problemas com conexões seriais é através da troca da placa defeituosa por uma que sabemos que está 100% operacional ou a realização de teste de Loop com o CSU/DSU, o qual será mais bem estudado no curso preparatório para o 200-105.

Sobre o primeiro método ele é muito utilizado em campo pelas empresas prestadoras de serviço, onde eles possuem um equipamento **sobressalente (spare part)** operacional e testado, fazendo a substituição do equipamento defeituoso. Se o circuito voltar a ficar operacional o problema é do equipamento atualmente instalado, seja a placa ou o chassis, porém se o problema persistir deve-se examinar outras possibilidades de defeito.

Em interfaces LAN ethernet, fastethernet ou gigabit ethernet os problemas mais comuns são cabos com padrão errado para conexão dos dispositivos (cross ou direto) e configuração errada da velocidade e/ou modo de operação Duplex/Half-Duplex.

Quando ligamos um cabo errado a interface não irá subir, ou seja, ficará Down/Down. Existem switches, como os da linha 2960, que possuem o recurso de **Auto-MDIX**, o qual permite que você conecte qualquer tipo de cabo, cruzado ou direto, com o switch que ele irá internamente converter o padrão e fazer a interface funcionar.

No CCENT ou CCNA normalmente são temos o recurso de auto-mdix nos equipamentos e temos que lembrar que entre dois switches, switch/HUB, Roteador/Computador, Computador/Computador e HUB/HUB utilizam-se cabos cruzados, já entre Roteador/Switch ou HUB, Computador/Switch ou HUB utiliza-se cabos diretos.

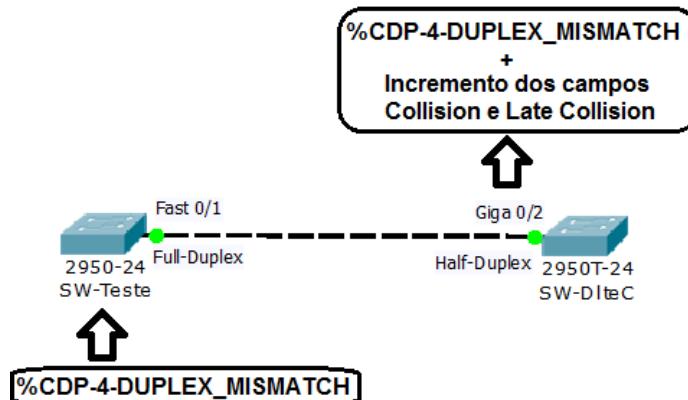
### 6.3 Problemas com Half/Full-Duplex

Quando o problema entre duas interfaces LAN é o modo de operação, no roteador ou switch será gerada uma mensagem de erro do tipo "**Mismatch**" (tipo errado ou descasamento de configurações entre as duas pontas).

As mensagens de mismatch são geradas quando em uma das pontas não temos o protocolo ou processo correto configurado, abaixo segue a mensagem que o equipamento dá quando uma das pontas é Half e deveria ser Full-Duplex:

14:46:13: %CDP-4-DUPLEX\_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not half duplex), with SW-DlteC.dltec.com.br GigabitEthernet0/2 (half duplex).

Traduzindo a mensagem o switch local detectou que sua interface fast 0/1 está conectada ao switch remoto SW-DlteC.dltec.com.br via Interface Giga 0/2, a qual é Half-Duplex, porém ela está como Full-Duplex, por isso o erro está acontecendo. Veja a figura abaixo.



Como a interface que está configurada como Full-duplex desativa o circuito de detecção de colisões (não detecta mais colisões), os campos de **Collisions** e **Late Collisions** tendem a ser **incrementados** somente na interface que está **configurada como Half-Duplex** nos casos de descasamento do modo de operação.

Para visualizar o status das interfaces em **switches**, se elas são half ou full e a velocidade utilize o comando "**show interface status**", veja exemplo abaixo.

SW-DlteC#sho interfaces status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	portas sem telefon	connected	10	a-full	a-100	10/100BaseTX
Fa0/2	portas sem telefon	notconnect	10	auto	auto	10/100BaseTX
Fa0/3	portas sem telefon	connected	10	a-full	a-100	10/100BaseTX
Fa0/4	com vlan de voz	connected	10	a-full	a-100	10/100BaseTX
Fa0/5	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/6	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/7	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/8	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/9	portas sem telefon	notconnect	10	auto	auto	10/100BaseTX
Fa0/10	portas sem telefon	notconnect	10	auto	auto	10/100BaseTX
Fa0/11	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/12	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/13	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/14	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/15	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/16	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/17	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/18	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/19	com vlan de voz	notconnect	10	auto	auto	10/100BaseTX
Fa0/20		notconnect	10	auto	auto	10/100BaseTX
Fa0/21		notconnect	1	auto	auto	10/100BaseTX
Fa0/22		notconnect	20	auto	auto	10/100BaseTX
Fa0/23	Portas da sala de	notconnect	20	auto	auto	10/100BaseTX
Fa0/24		notconnect	1	auto	auto	10/100BaseTX
Gi0/1		connected	trunk	a-full	a-100	10/100/1000BaseTX
Gi0/2		notconnect	trunk	auto	1000	10/100/1000BaseTX

SW-DlteC#

Note que o comando traz várias informações úteis para o dia a dia da administração de redes com switches Cisco, tais como porta, VLAN, o estado se a porta está conectada ou não, etc. O prefixo “a-” enfrente do estado de **Duplex** e **Speed** (velocidade) significa que esse parâmetro foi autonegociado.

#### 6.4 Testando as Interfaces com Ping e Traceroute

Assim como estudamos até o capítulo 9 para os hosts os comandos de teste da camada 3 ping e traceroute também estão disponíveis nos roteadores e switches Cisco.

Lembre-se que o ping testa a conectividade fim a fim, ou seja, entre um host e outro, não especificando por onde esse pacote está passando. Se você precisa especificar o caminho deve utilizar o comando traceroute (normalmente digitamos apenas trace, mas o comando é traceroute), portanto dizemos que o teste realizado pelo traceroute é ponto a ponto.

Para executar um teste simples de ping e traceroute basta digitar o comando e o IP ou nome do domínio a ser testado, porém para testes com nomes de domínio (ping www.cisco.com) o roteador precisa do comando “ip domain-lookup” e um servidor DNS configurado no “ip name-server”. Veja o exemplo de dois testes abaixo.

```
dltec#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
dltec#traceroute 192.168.10.1

Type escape sequence to abort.
Tracing the route to www.routerlogin.net (192.168.10.1)

 1 192.168.1.1 0 msec 4 msec 4 msec
 2 www.routerlogin.net (192.168.10.1) 12 msec 4 msec 4 msec
dltec#
```

Além disso, o ping no roteador pede ser executado de maneira estendida, inserindo apenas a palavra ping, sem o IP de destino. Veja um exemplo abaixo.

```
dltec#ping
Protocol [ip]:
Target IP address: 192.168.1.1
Repeat count [5]: 20
Datagram size [100]: 1000
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]: aaaaaaaa
Invalid pattern, try again.
Data pattern [0xABCD]: 0xaaaa
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 20, 1000-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with the DF bit set
```

```
Packet has data pattern 0xAAAA
!!!!!!!
Success rate is 100 percent (20/20), round-trip min/avg/max = 1/2/4 ms
dltec#
```

As mensagens que o ping e o traceroute podem fornecer nos roteadores da Cisco podemos encontrar estão na tabela abaixo.

!	Indica o recebimento do echo reply com sucesso.
.	Indica que o echo reply não foi recebido e o tempo de espera se esgotou.
U	Indica o recebimento de um destination unreachable.
Q	Indica o recebimento de uma mensagem de Source quench (destino muito ocupado).
M	Indica que precisa de fragmentação mas o bit DF está setado.
?	Tipo de pacote desconhecido.
&	Tempo de vida do pacote excedido.

Se você deseja testar até a camada 7 utilize o telnet para fazer o teste.

## 6.5 Verificando a Tabela ARP

Tanto os roteadores como os switches guardam também uma tabela ARP, assim como estudamos no capítulo 5 para os hosts. A visualização da tabela ARP é feita com o comando “**show ip arp**”, veja um exemplo abaixo.

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	10.0.1.1	-	2893.fe6c.e163	ARPA	FastEthernet0/1.20
Internet	10.0.1.2	161	0026.5a9e.9f25	ARPA	FastEthernet0/1.20
Internet	192.168.1.1	-	2893.fe6c.e163	ARPA	FastEthernet0/1.10
Internet	192.168.1.5	249	0024.5161.6a41	ARPA	FastEthernet0/1.10
Internet	192.168.1.6	65	001e.130b.1aee	ARPA	FastEthernet0/1.10
Internet	192.168.1.11	4	e0cb.4ecc.9b9b	ARPA	FastEthernet0/1.10
Internet	192.168.1.18	0	Incomplete	ARPA	FastEthernet0/1.10
Internet	192.168.1.201	2	000c.295e.bb64	ARPA	FastEthernet0/1.10
Internet	192.168.1.254	3	0012.7b50.01f6	ARPA	FastEthernet0/1.10
Internet	192.168.2.1	-	2893.fe6c.e163	ARPA	FastEthernet0/1.30
Internet	192.168.2.20	32	001d.7060.d31b	ARPA	FastEthernet0/1.30
Internet	192.168.2.22	32	0023.339d.0792	ARPA	FastEthernet0/1.30
Internet	192.168.2.24	32	001b.0c96.c5e8	ARPA	FastEthernet0/1.30
Internet	192.168.10.1	0	0022.3f3d.d916	ARPA	FastEthernet0/0
Internet	192.168.10.2	-	2893.fe6c.e162	ARPA	FastEthernet0/0

Note que alguns endereços aparecem com um traço (-) no campo “Age (min)”, pois são endereços internos do próprio roteador, por isso eles não possuem o contador de tempo para que a entrada não seja nunca apagada (aging time) como as outras entradas aprendidas dinamicamente. As entradas com o valor zero são MACs aprendidos a muito pouco tempo, normalmente a menos de um minuto e ainda não receberam o contador (aging time).

As entradas com um contador definido são aquelas que foram aprendidas pelo processo de ARP e serão apagadas quando seu contador de envelhecimento ou obsolescência chegar à zero. O valor padrão do aging time do ARP são de 4 horas (240 minutos), porém pode variar dependendo da versão do IOS.

## 7 Analisando o Encaminhamento de Quadros em Switches

Esse assunto já foi estudado no capítulo 3 e sabemos que para verificar como um switch encaminhará um quadro precisamos analisar a tabela de endereços MAC (SAT/CAM) com o comando “**show mac address-table**”. Em alguns switches podemos utilizar também o “**show mac-address-table**”, quando utilizando versões mais antigas do Cisco IOS.

Se quisermos analisar apenas os MACs aprendidos dinamicamente podemos utilizar o comando “**show mac address-table dynamic**”.

Lembre-se que temos basicamente três tipos de endereços MAC utilizados em comunicações via IPv4:

- **MAC de endereços de Unicast**: é o MAC da placa de rede do computador.
- **MAC de broadcast**: todos os 48 bits setados em 1 “ff:ff:ff:ff:ff:ff”.
- **MAC de multicast**: faixa de 01:00:5e:00:00:00 até 01:00:5e:7f:ff:ff, sempre iniciando em “01:00:5e”.

Os MACs de **broadcast** e **multicast** enviados pelos dispositivos conectados ao switch **não são armazenados pela tabela de endereços MAC**, por isso quando o switch recebe como endereço de destino um desses tipos de endereço MAC é feito o **flooding** dos quadros para todas as portas menos para a porta que originou o quadro.

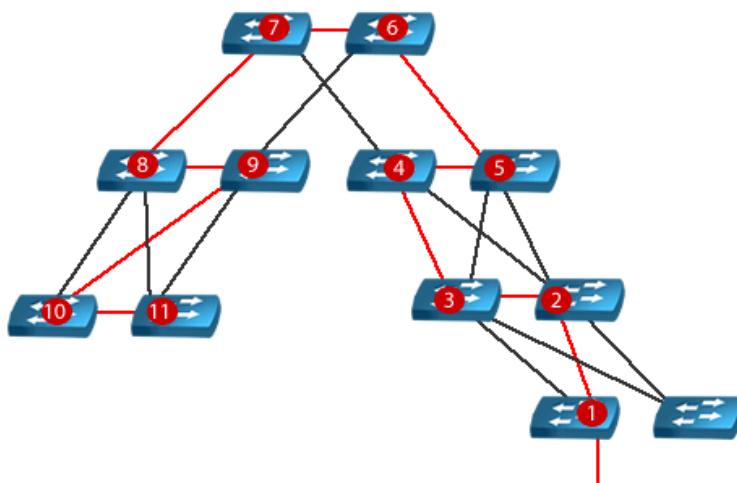
Os switches encaminham quadros em suas portas de acesso (**access**) com base no endereço **MAC de destino** seguindo as regras básicas de abaixo:

1. **O quadro recebido tem MAC de destino de Unicast está na tabela de endereços MAC** → encaminha para a porta de destino conforme tabela.
2. **O quadro recebido tem MAC de destino de Unicast e não está na tabela de endereços MAC** → fazer o flooding do quadro para todas as portas menos a de origem.
3. **O quadro recebido tem como MAC de destino um endereço multicast ou broadcast** → fazer o flooding do quadro para todas as portas menos a de origem.
4. **O MAC de destino é de Unicast e está listado na mesma porta que o MAC de origem** → o quadro deve ser filtrado, pois ou há um hub conectado à porta ou ela está configurada como trunk.

Com as regras acima podemos prever o comportamento normal do switch para o encaminhamento de um quadro para determinado destino específico através de portas de acesso. Agora vamos analisar o que acontece com os quadros em portas trunk.

Em portas configuradas como **trunk**, sejam **802.1Q** ou **ISL**, quando um quadro é recebido ele **vem marcado** com a Tag da VLAN que ele pertence (VLAN-ID). O switch que recebeu o quadro precisa **retirar a Tag** para encaminhar esse quadro recebido para a porta de acesso ou trunk que pertencem à mesma VLAN e tem o MAC de destino cadastrado.

Se o switch de destino também não conhece o MAC ele fará um flooding do quadro para todas as portas, menos para o trunk que o enviou. Note que esse processo de retransmissão do flooding pelos trunks vai sendo repetido até o último switch que estiver em cascata, por isso não se recomenda ter redes com um diâmetro muito grande, ou seja, muitos switches em cascata. Veja a figura a seguir.



A topologia em três camadas evita esse tipo de problema, pois o roteamento entre VLAN é feito na distribuição e nunca teremos mais que três switches de diâmetro.

No caso de um quadro sendo **enviado através de um trunk**, o switch que está enviando o quadro precisa **determinar a VLAN** da porta que está transmitindo o quadro para etiquetá-lo com a Tag (VLAN-ID) correta e encaminhá-lo através do trunk devidamente identificado.

Outra informação importante é que quando dois computadores pertencentes a uma mesma VLAN, porém em switches diferentes conectados via trunk se comunicam, os MACs remotos que se comunicaram ficam **vinculados ao trunk**, por isso ao verificar portas com mais de um MAC listado nela podemos ter duas situações:

1. A porta é um trunk.
2. Existe um HUB conectado a essa porta.

A maneira mais simples de se certificar que tipo de porta é essa é com o comando “**show vlan brief**” e se ela não aparecer no comando é um trunk, além desse comando podemos utilizar o “**show interface trunk**” para fazer a verificação. Lembre-se que um HUB terá que se conectar a uma porta de acesso, pois eles não suportam 802.1Q por estarem na camada física.

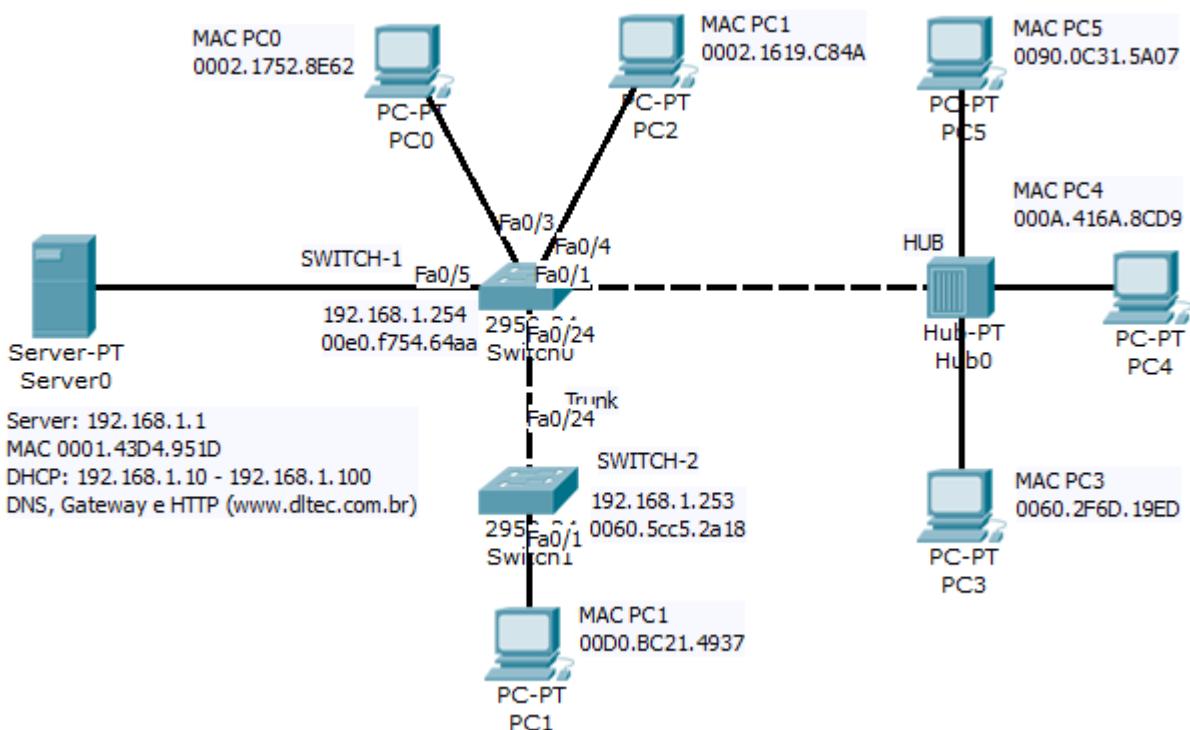
Outro comando que pode ajudar a certificar o tipo de equipamento conectado à porta em questão é o **show cdp neighbor**, pois se tivermos um roteador ou switch conectado via trunk ele deve aparecer na saída do comando.

Portanto, existe um número limitado de possibilidades e o processo de encaminhamento de quadros em switches de camada-2 é bem previsível e simples de ser mapeado, portanto é entender as regras de processamento acima para ir bem nas questões referentes ao assunto na prova.

A seguir veremos um exemplo prático utilizando comandos para analisar o comportamento de encaminhamento de quadro pelos switches.

#### 7.1.1 Analisando o Encaminhamento de Quadros – Exemplo Prático

Vamos utilizar a topologia abaixo para realizar testes e demonstrar o encaminhamento dos quadros na prática. Essa topologia está disponível para baixar na área do aluno em um arquivo do Packet Tracer.



Os computadores estão configurados para obter IP via DHCP, já o servidor tem o IP fixo mostrado na topologia e possui os serviços de DHCP, DNS e HTTP configurados nele. Os switches também têm seus IPs de gerenciamento fixos conforme a topologia. Na topologia são mostrados todos os endereços MAC dos equipamentos conectados nessa rede.

Seguindo a linha de prever o comportamento do switch e o conteúdo de sua tabela MAC, se um computador emite um ping para o endereço 192.168.1.255 e todos respondem ao ping, como ficaria a tabela MAC dos switches? Qual o MAC considerando apenas os computadores e o servidor está vinculado a cada porta do switch 1 e do switch 2?

Para fazer essa análise, primeiro temos que pensar sobre os quadros sendo enviados, vamos supor que o PC1 é que está gerando os quadros. A princípio, como ele é um computador, sua porta deve ser de acesso, vamos confirmar com o comando **"show interfaces switchport"**:

```
SWITCH-2#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
### Saída Omitida ###
```

Uma vez confirmado (veja os campos destacados) sabemos que ao receber o quadro o switch fará o encaminhamento baseado no MAC de destino, como estamos pingando o endereço 192.168.1.255 seu MAC é de broadcast ff:ff:ff:ff:ff:ff, por isso ele será copiado em todas as portas do switch (flooding), inclusive para o trunk.

Como todos os computadores, switches e servidor estão na mesma VLAN, receberão o ping e responderão à mensagem, por isso o switch após esse teste terá todos os MACs registrados nas portas. Analisando as portas teremos:

- **SWITCH-1:**

- Fast 0/1: MACs de PC3, PC4 e PC5 (temos um hub na ponta)
- Fast 0/3: MAC do PC0
- Fast 0/4: MAC do PC2
- Fast 0/5: MAC do Servidor
- Fast 0/24: é uma porta trunk e deve ter pelo menos o MAC do PC1 e do SWITCH-2

- **SWITCH-2:**

- Fast 0/1: MAC do PC1
- Fast 0/24: também é uma porta trunk e terá os MACs de PC0, PC2, PC3, PC4, PC5, Servidor e SWITCH-1

Vamos executar o comando em PC1 e executar o comando “**show mac address-table dynamic**” em ambos os switches, veja abaixo:

```
SWITCH-1#show mac address-table dynamic
      Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	0001.43d4.951d	DYNAMIC	Fa0/5
1	0002.1619.c84a	DYNAMIC	Fa0/4
1	0002.1752.8e62	DYNAMIC	Fa0/3
1	000a.416a.8cd9	DYNAMIC	Fa0/1
1	0060.2f6d.19ed	DYNAMIC	Fa0/1
1	0060.5cc5.2a18	DYNAMIC	Fa0/24
1	0090.0c31.5a07	DYNAMIC	Fa0/1
1	00d0.bc21.4937	DYNAMIC	Fa0/24

Conferindo a tabela de endereços MAC confirmamos a previsão de aprendizados das portas no primeiro switch. Grifamos os MACs registrados no trunk, os quais são do PC1 e switch-2.

```
SWITCH-2#show mac address-table dynamic
      Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	0001.43d4.951d	DYNAMIC	Fa0/24
1	0002.1619.c84a	DYNAMIC	Fa0/24
1	0002.1752.8e62	DYNAMIC	Fa0/24
1	000a.416a.8cd9	DYNAMIC	Fa0/24
1	000c.cfc4.b118	DYNAMIC	Fa0/24
1	0060.2f6d.19ed	DYNAMIC	Fa0/24
1	0090.0c31.5a07	DYNAMIC	Fa0/24
1	00d0.bc21.4937	DYNAMIC	Fa0/1
1	00e0.f754.64aa	DYNAMIC	Fa0/24

Idem para o switch-2, temos apenas o MAC do PC1 alocado na por fast 0/1 e os MACs dos dispositivos conectados no switch-1 estão todos vinculados à porta de trunk fast 0/24.

### 7.1.2 Quadro sendo Filtrado na Porta?

Um quadro que não está chegando ao seu destino e está sendo enviado somente através de switches pode estar sendo filtrado (bloqueado).

Existem vários mecanismos de proteção e segurança que podem filtrar quadros em switches de camada 2, mesmo a porta estando ativa (UP/UP), por exemplo, ACLs baseadas em endereçamento MAC (não faz parte do escopo desse material) ou violações ao máximo de MACs protegidos em portas configuradas com **Port Security**.

Vamos lembrar um pouco do Port Security, pois ele pode ter três ações quando detecta uma violação ao número máximo de MACs permitidos:

1. **Shutdown**: porta desativada e em error disable.
2. **Restrict**: porta é mantida ativada, mas não encaminha quadros aos computadores causadores da violação. Avisa ao gerenciamento remoto (Syslog e trap SNMP).
3. **Protect**: porta é mantida ativada, mas não encaminha quadros aos computadores causadores da violação. Não avisa ao gerenciamento remoto.

Portanto, os modos de proteção 2 e 3 acima mantém a porta ativa, somente filtrando quadros aos computadores que causaram a violação do Port Security. Lembra como podemos verificar se houve violação?

Com os comandos "show port-security" ou "**show port-security interface fast0/x**".

Vamos agora causar uma violação na porta onde o HUB está conectado na topologia anterior inserindo a seguinte configuração:

```
SWITCH-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH-1(config)#int f0/1
SWITCH-1(config-if)#switchport port-security
SWITCH-1(config-if)#switchport port-security mac-address sticky
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
i
SWITCH-1(config-if)#

```

Note que a porta vai cair na hora, pois temos três MACs e com a configuração padrão apenas um é permitido, além disso, temos o shutdown como padrão de violação. Vamos ao comando show:

```
SWITCH-1(config-if)#do show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)      (Count)      (Count)
-----
Fa0/1      1          0          1      Shutdown
-----
SWITCH-1(config-if)#

```

Agora vamos mudar a violação para **restrict** (primeiro vamos desabilitar a porta, reconfigurar e depois habilitar).

```
SWITCH-1(config-if)#shut
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
```

```

SWITCH-1 (config-if)#switchport port-security violation restrict
SWITCH-1 (config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up

SWITCH-1#sho port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)
-----
Fa0/1      1          1          2          Restrict
-----
```

Note que com o restrict temos a violação de segurança, pois temos três computadores conectados e apenas um MAC seguro e por isso a contagem de violação de segurança está mostrando dois MACs bloqueados, mas a porta continua UP, pois o MAC seguro pode ainda enviar e receber quadros.

Quadros enviados em direção aos computadores bloqueados não serão encaminhados porque o Port Security irá filtrá-los!

Uma coisa interessante é que o Port Security registra o MAC protegido na tabela de endereços MAC como estático (somente para as configurações **protect** e **restrict**) e não mostra o MAC dos computadores que causaram violação, veja abaixo:

```

Switch#show mac address-table
    Mac Address Table
-----
Vlan   Mac Address        Type      Ports
----  -----
1      0001.43d4.951d    DYNAMIC   Fa0/5
1      0002.1619.c84a    DYNAMIC   Fa0/4
1      0002.1752.8e62    DYNAMIC   Fa0/3
1      0004.9a1b.d755    DYNAMIC   Fa0/24
1      000a.416a.8cd9    STATIC    Fa0/1
1      0060.5cc5.2a18    DYNAMIC   Fa0/24
1      00d0.bc21.4937    DYNAMIC   Fa0/24
Switch#
```

Podemos verificar o MAC do último computador que causou a violação com o comando abaixo:

```

Switch#show port-security interface fastEthernet 0/1
Port Security           : Enabled
Port Status              : Secure-up
Violation Mode          : Restrict
Aging Time               : 0 mins
Aging Type               : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses    : 1
Total MAC Addresses       : 1
Configured MAC Addresses : 0
Sticky MAC Addresses      : 1
Last Source Address:Vlan : 0060.2F6D.19ED:1
Security Violation Count : 2
```

Voltando à topologia você vai ver que é o MAC do computador PC3 e o MAC que está permitido, mostrado na tabela MAC como estático, é do PC4.

Agora que já revisamos os conceitos de encaminhamento de quadros em switches e o funcionamento da tabela de endereços MAC, vamos estudar problemas típicos que podem ser encontrados relacionados à VLANs e Trunks.

## 8 Analisando Problemas com VLANs e Trunks

Os problemas típicos relacionados à VLANs e trunking que podem ser cobrados no CCENT são:

1. Portas alocadas à VLANs erradas (tinha que ser porta 0/1 na VLAN 1 e está configurada como VLAN2).
2. VLANs não existem (não criadas localmente ou no VTP Server) ou estão inativas (shutdown) nos switches.
3. VLANs bloqueadas nos trunks onde na realidade deviam estar liberadas (comando “**switchport trunk allowed**”).
4. Trunks não sobem por não terem as configurações corretas em ambas as pontas do link (switches configurados com DTP ou estados de portas errados em um dos lados do link).

Agora vamos estudar um pouco mais sobre cada problema.

### 8.1 Portas de Acesso Alocadas à VLANs Erradas

Os problemas relacionados à alocação de portas nas VLANs podem ser resolvidos verificando o projeto ou requisito original com o comando “**show vlan brief**” e aplicando a configuração correta de VLAN nas portas alocadas erroneamente.

**Switch#show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23
1002	fdci-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Switch#

Além disso, se temos uma porta que deve estar em uma determinada VLAN supõe-se que ela deva estar configurada como acesso, por isso com os comandos “**show interface switchport**” ou “**show running-config**” conseguiremos verificar essa informação. Se esses comandos não estiverem disponíveis, podemos utilizar o “**show mac address-table**” para verificar através de uma entrada a porta e a VLAN de acesso que ela está alocada se houver entrada.

### 8.2 VLANs não Existem ou estão Desabilitadas

Os switches não encaminham informações de VLANs que não estão criadas neles ou então que estão criadas, mas desabilitadas (shutdown), por isso um quadro encaminhado a um switch remoto pode ser filtrado por falta de consistência na configuração de VLANs nos switches da rede.

Em redes que o protocolo VTP está configurado, em operação normal, todos os switches VTP clientes devem ter a mesma base de dados de VLANs e não ter problemas, porém se houverem switches configurados como transparentes ou com o VTP desabilitado podemos sim ter problemas de consistência na configuração, pois as VLANs nesses switches devem ser inseridas manualmente.

Com o comando “**show vtp status**” podemos verificar nos switches da rede o estado do VTP e verificar com o comando “**show vlan brief**” os VLANs ID conhecidos, para certificar que todas as VLANs estão presentes nos switches que compõe o caminho entre origem e destino do quadro.

Além disso, com o comando “**show vlan brief**” podemos ver se existem VLANs em shutdown. Veja abaixo.

SW-DlteC#sho vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/21, Fa0/24, Gi0/2
10	corp	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20
20	sala-aula	active	Fa0/22, Fa0/23
30	vlan-voz	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20
51	BoaIdeia	act/lshut	
100	VLAN0100	act/lshut	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdnet-default	act/unsup	
1005	trnet-default	act/unsup	
	SW-DlteC#		

Note que as VLANs 1, 10, 20 e 30 estão no estado ativo (active), já as VLANs 51 e 100 estão desativadas (act/lshut). Lembre-se abaixo dos comandos para ativar e desativar uma VLAN:

```
SW(config)#no shutdown vlan 10
SW(config)#shutdown vlan 20
SW(config)#vlan 30
SW(config-vlan)#no shutdown
SW(config-vlan)#vlan 40
SW(config-vlan)#shutdown
SW(config-vlan)#

```

### 8.3 VLANs Bloqueadas na Lista dos Trunks

Lembre-se que para minimizar o tráfego desnecessário nos trunks recomenda-se o uso do VTP pruning (se o VTP estiver sendo utilizado) ou utilizar o comando “**switchport trunk allowed vlan**” para liberar ou filtrar o tráfego de VLANs entre dois switches através dos links trunks.

Portanto, se um switch deve trafegar das VLANs de 1 a 110 e o comando foi inserido errado, as VLANs faltantes na lista terá seu tráfego bloqueado. Para verificar a lista de VLANs permitidas podemos utilizar o comando “**show interface trunk**”, veja exemplo a seguir.

```

Switch#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/24    on       802.1q        trunking    1

Port      Vlans allowed on trunk
Fa0/24    1-100

Port      Vlans allowed and active in management domain
Fa0/24    1,10,20,100

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24    1,10,20,100
Switch#

```

Destacado em amarelo temos a lista total de VLANs liberadas e em verde temos das liberadas as que estão ativas. Analisando a saída do comando e levando em conta que as VLANs que deveriam estar liberadas eram de 1 a 110 estão faltando as VLANs de 101 a 110, podemos usar o comando abaixo para adicionar as VLANs faltantes:

```

Switch(config-if)#switchport trunk allowed vlan add 101-110
Switch(config-if)#do sho interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/24    on       802.1q        trunking    1

Port      Vlans allowed on trunk
Fa0/24    1-110

Port      Vlans allowed and active in management domain
Fa0/24    1,10,20,100

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24    1,10,20,100
Switch(config-if)#

```

O comando show interface trunk mostra que agora estamos com a configuração correta.

#### 8.4 Interfaces Configuradas como Trunk não Sobem

As portas dos switches por padrão possuem o protocolo DTP ativado para negociação dinâmica de trunks, possibilitando que o estado da porta como acesso ou trunk seja negociado conforme configuração nas portas sendo conectadas.

Por exemplo, se ambos os switches tiverem a porta que deve ser trunk configurada com o comando “**switchport mode dynamic auto**” simplesmente as portas subirão como “access”, pois nesse estado a porta espera em modo passivo que o outro lado seja um trunk para que ela também assuma o mesmo estado, portanto duas portas com essa configuração nunca serão trunk.

Com o comando “show interface fast0/x trunk” podemos verificar a configuração e estado que a porta subiu, veja exemplo abaixo.

```

Switch#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access

```

```
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
### saida Omitida ###
```

No comando acima podemos ver que a porta está configurada como Dynamic Auto, mas subiu como acesso, além disso, abaixo que a negociação para subir como trunk está ativada.

Lembre-se que em ambientes reais a recomendação de configuração é bem simples, portas de acesso devem ser configuradas com o comando “**switchport mode access**” e portas trunk como “**switchport mode trunk**” com o DTP desabilitado através do comando “**switchport nonegotiate**”.

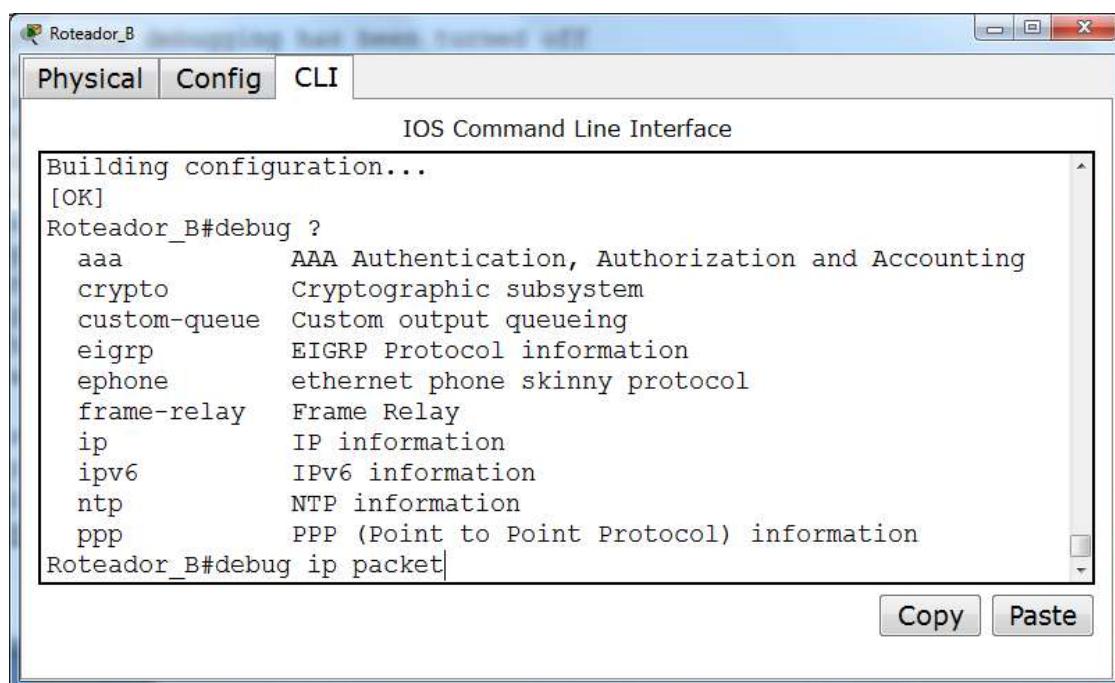
Assim várias situações de negociações do protocolo DTP são evitadas, assim como os problemas decorrentes de falhas na configuração de portas trunk.

## 9 Utilizando o Comando Debug

Outro tipo de monitoração que pode ser realizado nos roteadores e switches Cisco é através do comando **debug**. Este comando permite a monitoração em tempo real de um determinado tipo de tráfego, processo ou protocolo dos dispositivos.

A parte negativa do uso do debug é que ele pode ser “**disruptivo**”, ou seja, dependendo do que você vai monitorar com o debug o roteador pode fazer com que o roteador chegue a 100% da sua utilização de memória e/ou CPU e simplesmente “travar”, sendo necessário um desligamento e religamento manual (chamado de cold restart) para que o dispositivo solte a funcionar normalmente.

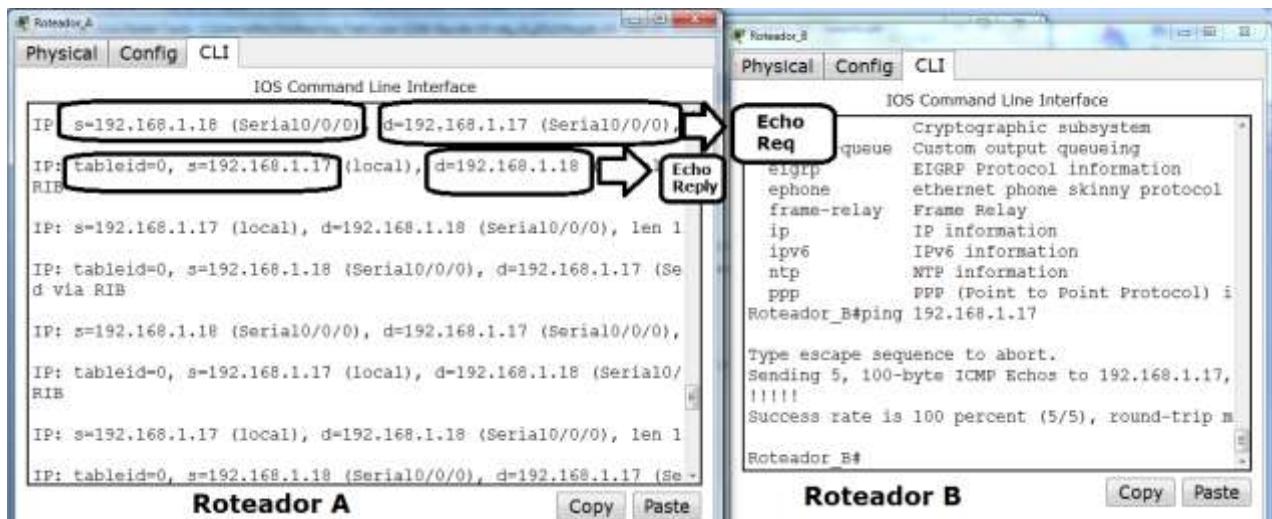
Existem diversas opções de debug, as quais devem ser ativadas via modo de usuário privilegiado, na tela da figura 1 ao lado os comandos debug disponíveis no packet tracer (em um roteador real existem muito mais opções).



Vamos iniciar estudando dois comandos debug básicos:

- **Debug ip packet**: permite visualizar o tráfego de pacotes IP em geral.
- **Debug ip icmp**: permite visualizar informações específicas do ICMP, por exemplo, verificar pacotes do comando ping em tempo real.

Vamos ativar no Roteador\_A o comando “debug ip packet”, entrar no roteador B e fazer o ping para o IP da serial do roteador A em 192.168.1.17. Veja a figura a seguir.



Note na figura acima que o debug ip packet não especifica o protocolo, diz o endereço de origem ( $s=x.x.x.x$ ) e o endereço de destino ( $d=x.x.x.x$ ). Este comando pode ser utilizado para identificar o tráfego que está vindo para uma interface, porém dependendo da quantidade de pacotes processadas ele pode travar o roteador rapidamente.

Para desativar o comando você pode digitar “**no debug ip packet**” ou “**undebbug all**” ou “**no debug all**”.

O debug ip icmp é mais simples de analisar, pois ele traz o tipo de pacote ICMP que está sendo enviado ou recebido. Veja o mesmo teste anterior com apenas o debug ip icmp ativo na figura 3 ao lado, note que foram mostrados os echo replys formados para resposta dos echo requests recebidos do roteador com IP 192.168.1.18. Note que a origem é mostrada como srs (source) e o IP de destino como DST (destination), o tipo da mensagem é mostrado no início da mensagem “ICMP: echo reply sent”, ou seja, foi enviado um echo reply.

```

Destination filename [startup-config]?
Building configuration...
[OK]
Roteador_A#und all
All possible debugging has been turned off
Roteador_A#deb ip icmp
ICMP packet debugging is on
Roteador_A#
ICMP: echo reply sent, src 192.168.1.17, dst 192.168.1.18

```

O comando “**debug all**” ativa todos os debugs possíveis no roteador e pode para o roteador em pouco tempo em condições de carga moderada ou excessiva.

## 10 Dicas Sobre Administração de Roteadores e Switches Cisco

Algumas atitudes básicas devem ser tomadas para administrar redes com roteadores e switches Cisco:

- Manter a topologia da rede atualizada através de um diagrama de rede com os principais dispositivos, suas conexões e endereços IP.
- Manter backup das configurações e Cisco IOS dos dispositivos em um servidor de arquivos.
- Manter cabos de console dos dispositivos para que em situações de emergência o atendimento possa ser realizado com agilidade.
- Deixar no laptop utilizado para realização de atendimento local os sistemas operacionais (Cisco IOS) e cópia das configurações dos dispositivos.
- Manter data e hora dos roteadores e switches sincronizados e um servidor de Syslog para coletar as mensagens de erro e problemas, pois elas são perdidas quando os dispositivos são reinicializados ou desligados.

Maioria das atividades de dia a dia são realizadas remotamente via SSH ou Telnet, porém algumas situações de emergência podem gerar a necessidade de acesso local, por exemplo, quando um roteador tem seu IOS corrompido ou apagado por problemas operacionais.

Além disso, quando há um problema grave que exige a troca do dispositivo com problemas, será necessário copiar IOS e a configuração para o equipamento sobressalente, por isso é muito importante manter os backups em servidores e também no laptop utilizado para manutenção local.

O serviço de Syslog para coleta de mensagens será estudado posteriormente, já o SNMP para gerenciamento remoto dos dispositivos será tratado na prova 200-105, o ICND-2.

Algumas situações podem gerar a necessidade de verificar as condições de memória e CPU dos roteadores, assim como voltar às configurações de fábrica, assuntos que serão estudados a seguir.

### 10.1 Verificando a Memória e CPU dos Dispositivos

No dia a dia de um profissional CCENT ou CCNA muitas vezes será necessário verificar como está a utilização da memória ou da CPU do roteador ou switch.

A verificação da utilização da CPU do roteador pode ser realizado com o comando "show processes" ou "show processes cpu" (este segundo comando não funciona no packet tracer), veja a saída do comando abaixo, note que o que nos interessa é apenas o início do comando que nos dá a porcentagem de utilização da CPU.

```
DlteC-FW#sho processes
CPU utilization for five seconds: 3%/0%; one minute: 3%; five minutes: 2%
 PID QTy      PC Runtime (ms)    Invoked   uSecs     Stacks TTY Process
  1 Cwe 625FCDDC        164       259      633 5224/6000    0 Chunk Manager
  2 Csp 607ADA48        1548     108653      14 2432/3000    0 Load Meter
  3 Mwe 60396C60         4          1      400023048/24000  0 LICENSE AGENT
```

Portanto na primeira linha da saída do comando temos a utilização da CPU nos últimos 5 segundos e também nos últimos 5 minutos. Se a utilização estiver muito alta estará acima dos 85%.

O comando "show memory" nos dá o status da utilização da memória com os processos e também com I/O (dispositivos de entrada e saída do roteador), veja a saída do comando ao lado no exemplo 2, não vamos explicar os campos porque pode ser complexo e passa do que é exigido de um CCNA, porém é importante saber que existe o comando pois ele pode ser pedido caso você utilize o Technical Assistance Center (TAC) da Cisco.

```
DlteC-FW#show memory
      Head   Total(b)    Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor  657B6820  153393120  108049044  45344076  38141356  35100168
      I/O    EEA00000    23068672   4443600   18625072  18608272  18600284

      Processor memory

      Address   Bytes   Prev   Next Ref   PrevF   NextF Alloc PC what
657B6820 0000000044 00000000 657B687C 001 ----- ----- 62D3AEF4 IPS prm
create
657B687C 0000000044 657B6820 657B68D8 001 ----- ----- 62D3AEF4 IPS prm c
"zeramos" os equipamentos.
```

## 11 Resumo do Capítulo

Bem pessoal, chegamos ao final de mais um capítulo!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Entender e utilizar ferramentas de troubleshooting através de comandos show e debug.
- Entender os principais problemas e recursos de troubleshooting em interfaces LAN e WAN.
- Entender e saber utilizar o protocolo CDP e LLDP para resolver problemas e descobrir informações sobre vizinhos de rede.
- Entender o encaminhamento de quadros em redes com switches.
- Entender e aplicar comandos para resolver problemas com interfaces de switches, VLANs e trunks.
- Entender os princípios de administração em redes com switches e roteadores Cisco.

*Nesse capítulo do curso vamos estudar em 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.*

*Você vai aprender como dividir redes IPv6 em sub-redes, como alocar esses endereços na rede e configurar o roteamento estático para fazer a comunicação entre unidades que utilizem IPv6.*

*Bons estudos.*

## **Capítulo 13 - Protocolo IPv6**

### **Objetivos do Capítulo**

Ao final desse capítulo você deverá ter estudado e compreendido os seguintes assuntos:

- Entender e saber explicar as diferenças entre o IPv6 e IPv4
- Principais características do IPv6
- Entender e saber interpretar um endereço IPv6
- Entender o protocolo ICMPv6 e seus recursos adicionais de Multicast e o protocolos NDP
- Entender como os vizinhos IPv6 descobrem o endereço MAC e prefixos de Rede
- Entender e listar os métodos de alocação de endereços no IPv6
- Entender as principais diferenças entre o DHCP e o DHCPv6
- Saber dividir redes IPv6 em sub-redes e entender a alocação dos endereços na prática
- Entender o roteamento IPv6
- Saber configurar rotas estáticas no IPv6

## Sumário do Capítulo

<b>1 Qual a Maior Diferença entre o IPv4 e o IPv6?</b>	<b>496</b>
<b>2 Campos do Pacote IPv6</b>	<b>497</b>
<b>3 Tipos de Comunicação e Endereços em IPv6</b>	<b>498</b>
<b>4 Escrevendo e Interpretando Endereços IPv6</b>	<b>500</b>
<b>5 Faixas de Endereçamento e Endereços Especiais</b>	<b>502</b>
5.1 IEEE EUI-64	504
<b>6 Recursos e Serviços do IPv6</b>	<b>505</b>
6.1 ICMPv6	505
6.2 NDP (Neighbor Discovery Protocol)	506
6.2.1 Determinando o Endereço MAC de Hosts Vizinhos	507
6.2.2 Encontrando Roteadores Vizinhos	507
6.2.3 Detectando Endereços IPv6 Duplicados - DAD	508
6.2.4 Determinando a Acessibilidade dos Vizinhos	508
6.2.5 Redirecionamento de Pacotes	509
6.3 Distribuindo Endereços - Autoconfiguração e DHCPv6	509
6.3.1 Configuração Manual	510
6.3.2 Autoconfiguração Stateless	511
6.3.3 DHCPv6 – Stateless e Stateful	512
6.4 Roteamento IPv6	513
<b>7 Planejando a Rede - Sub-redes com IPv6</b>	<b>514</b>
7.1 Endereços Globais de Unicast e Divisão em Sub-redes	514
<b>8 Alterações no Serviço de Resolução de Nomes</b>	<b>517</b>
<b>9 Pilha Dupla</b>	<b>518</b>
<b>10 Introdução à Configuração do IPv6 em Roteadores e Switches Cisco</b>	<b>519</b>
<b>11 Configurações Básicas do IPv6 – Ativação, Interfaces, Testes e Vizinhança</b>	<b>520</b>

<b>11.1 Configurando Interfaces IPv6 no Cisco IOS</b>	<b>521</b>
11.1.1 Grupos de Multicast Padrões das Interfaces Cisco	523
<b>11.2 Redes Locais e Diretamente Conectadas no IPv6</b>	<b>524</b>
<b>11.3 Testando a Conectividade das Interfaces IPv6</b>	<b>525</b>
<b>11.4 Verificando Vizinhos IPv6 – Protocolo NDP</b>	<b>527</b>
<b>12 Atribuindo IPs via Autoconfiguração e Conceitos do DHCPv6</b>	<b>528</b>
12.1 Autoconfiguração Stateless ou SLAAC	528
12.2 Endereços via DHCPv6 Statefull e Agente Relay	530
12.3 Atribuindo Endereços com SLAAC e DHCPv6 Stateless	533
<b>13 Configurando o Roteamento em Redes IPv6</b>	<b>535</b>
13.1 Roteamento Estático e Rota Padrão	535
13.2 Criando Rotas Padrões	536
13.3 Rota Padrão via SLAAC e Autoconfiguração	537
13.4 Rotas Estáticas Flutuantes no IPv6	539
13.5 Rota de Host no IPv6	540
<b>14 Resumo do Capítulo</b>	<b>540</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.

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
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.

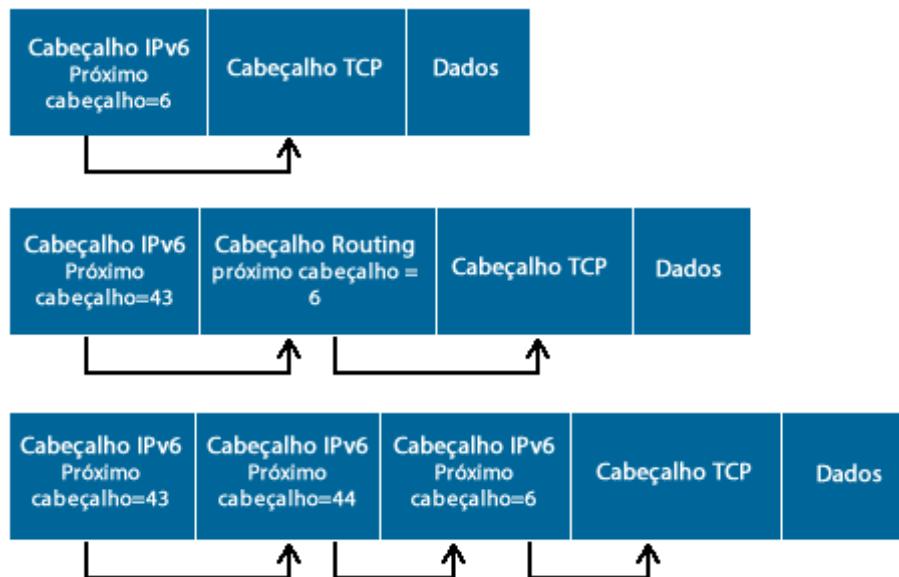


A descrição de cada campo segue abaixo:

- **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.

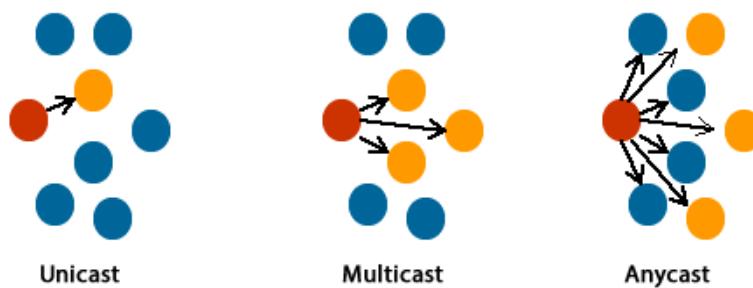
Portanto, o cabeçalho do IPv6 além de ser mais simples que o do IPv4, também trata de questões como QoS e segurança de maneira nativa, ou seja, dentro do próprio cabeçalho sem a necessidade de implementações e recursos adicionais como era necessário para o IPv4.

### 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:

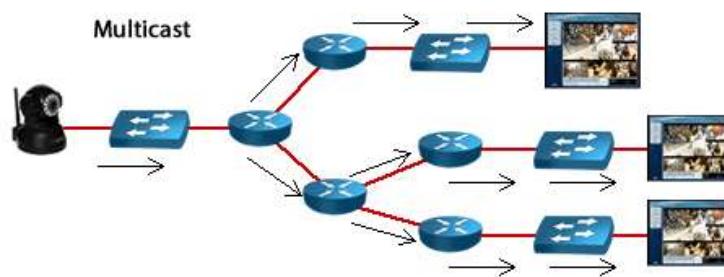
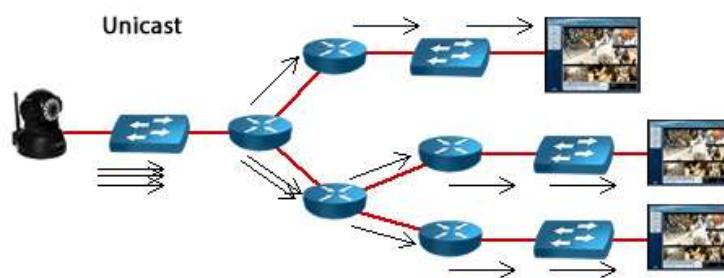
- **Unicast** → Comunicação um para um.
- **Multicast** → Comunicação um para muitos (grupo de dispositivos configurados com o mesmo endereço).
- **Anycast** → Endereço configurado em múltiplas interfaces.

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:**0:2234::**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 sub-redes 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



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    02 | 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).

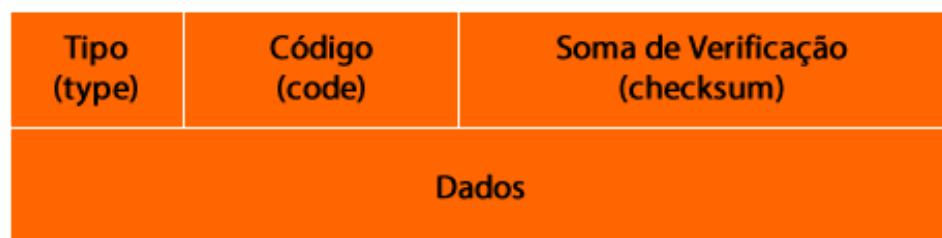
Além disso, com mecanismos como a autoconfiguração, o DHCPv6 pode funcionar de maneiras diferentes.

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.



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.
100-105	-	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:

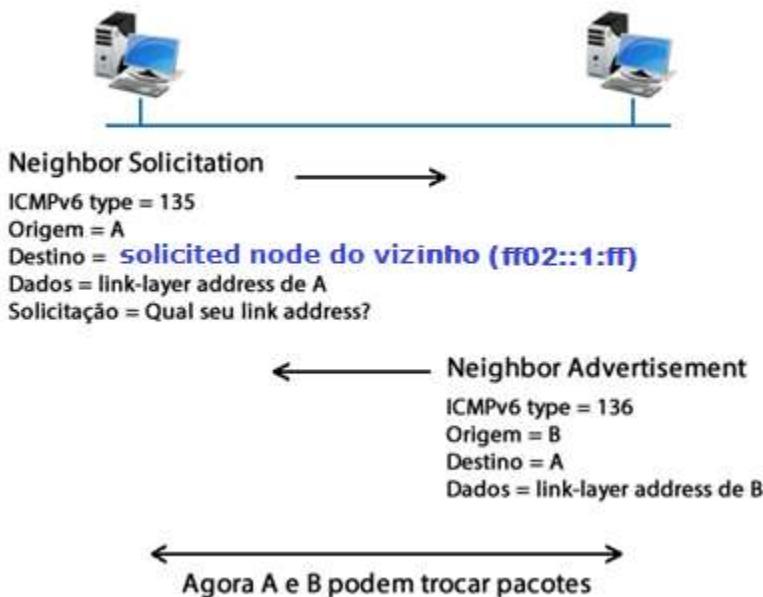
<b>Cód ICMP</b>	<b>Mensagem ICMP</b>	<b>Função</b>
133	Router Solicitation	Mensagens utilizadas para que hosts requisitem aos roteadores as mensagens de Router Advertisements proativamente, ou seja, sem esperar um anúncio por parte do roteador.
134	Router Advertisement	Mensagens enviadas periodicamente 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 Advertisement	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.

No IPv6 não podemos utilizar mais o ARP porque ele está baseado no envio das mensagens de solicitação em broadcast para a rede local, porém como não temos mais broadcasts em IPv6 foi preciso remodelar esse serviço, passando para responsabilidade do IPCMv6 descobrir o MAC dos vizinhos com o protocolo NDP.

O processo é realizado através da troca de mensagens ICMPv6 e funciona com um host enviando uma mensagem **Neighbor Solicitation** (NS) informando no campo de dados **seu endereço MAC** e também **solicitando o endereço MAC do vizinho em Multicast**. Ao receber a mensagem, o vizinho a responde enviando uma mensagem **Neighbor Advertisement** (NA) informando seu endereço MAC em **Unicast**. 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.

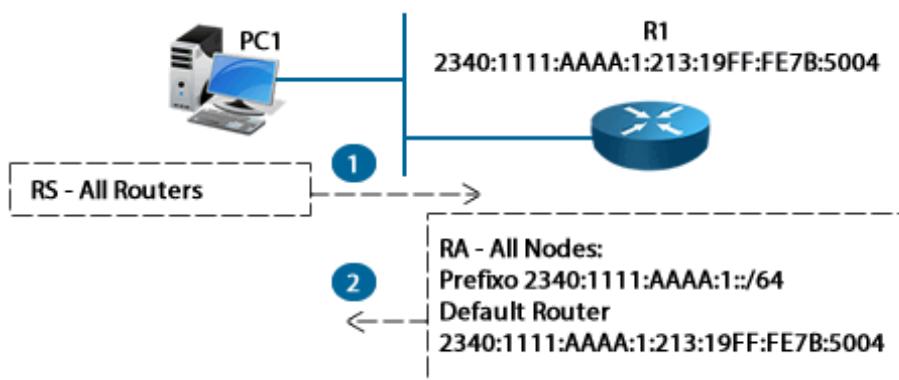


A diferença é que o NDP não utiliza o endereço IPv6 do destino e sim seu “Solicited-node” como endereço de destino na solicitação. O Solicited-node é um endereço de multicast formado pelo prefixo “**ff02::1:ff**” mais os 24 últimos bits (seis últimos algarismos em Hexadecimal) do endereço de link local ou global que está se procurando descobrir o endereço MAC.

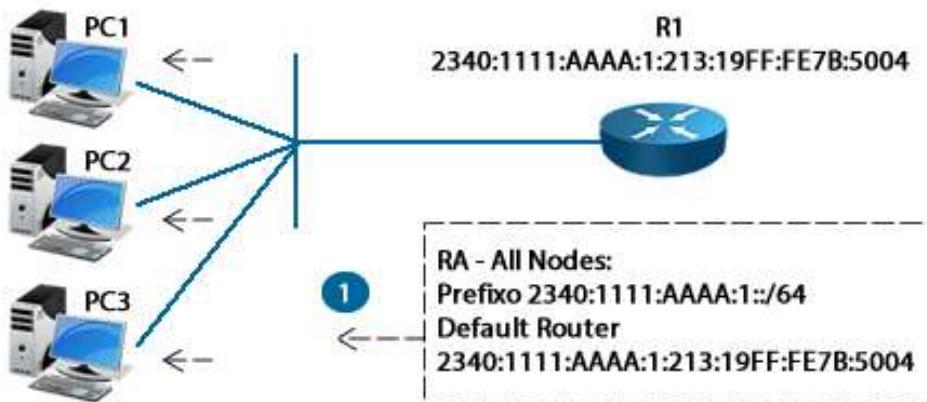
### 6.2.2 Encontrando Roteadores Vizinhos

O processo utilizado para localizar roteadores vizinhos dentro do mesmo enlace, bem como aprender prefixes e parâmetros relacionas 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 - DAD

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.

O envio do DAD (Duplicate Address Detection) também é realizado utilizando como destino o solicited-node em multicast do próprio host que está verificando se seu IP é único na rede.

### 6.2.4 Determinando a Acessibilidade dos Vizinhos

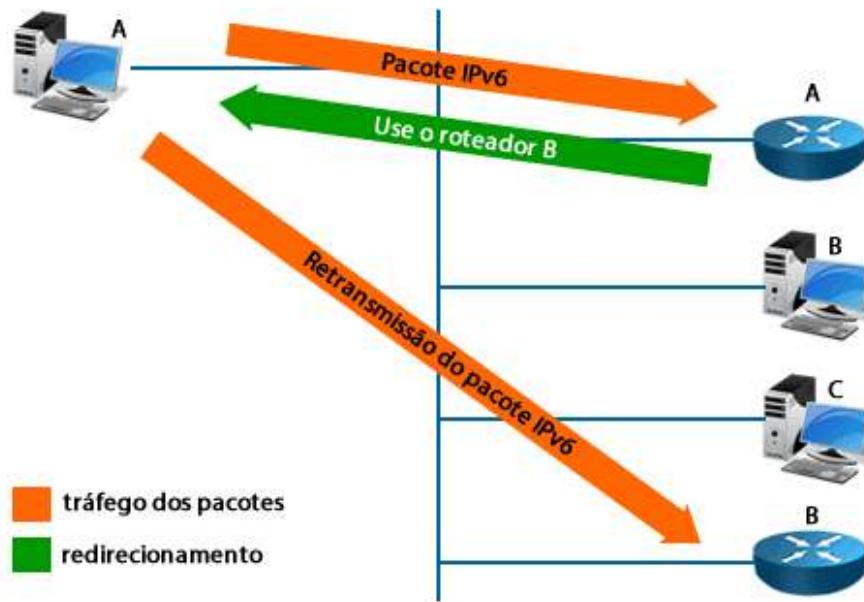
O NDP é capaz de determinar a disponibilidade de um vizinho analisando protocolos da camada superior. Por exemplo, verificando os ACKs recebidos pelo protocolo TCP, ou então, proativamente realizando uma resolução de endereços (via ICMPv6) quando certos limites são excedidos, porém esse monitoramento 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

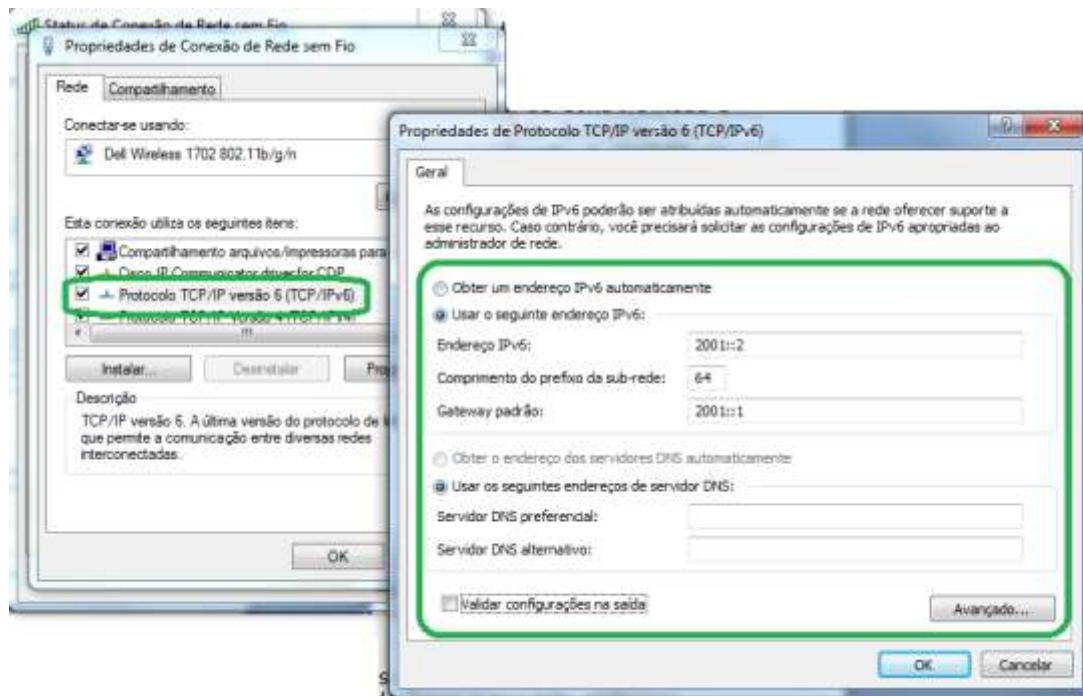
Assim como na versão 4 do protocolo IP, a primeira etapa para que um host tenha acesso à rede é a atribuição de um endereço de host à sua Interface. No IPv4 tínhamos a possibilidade de configurar um IP estaticamente (manual) ou através de um servidor DHCP.

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

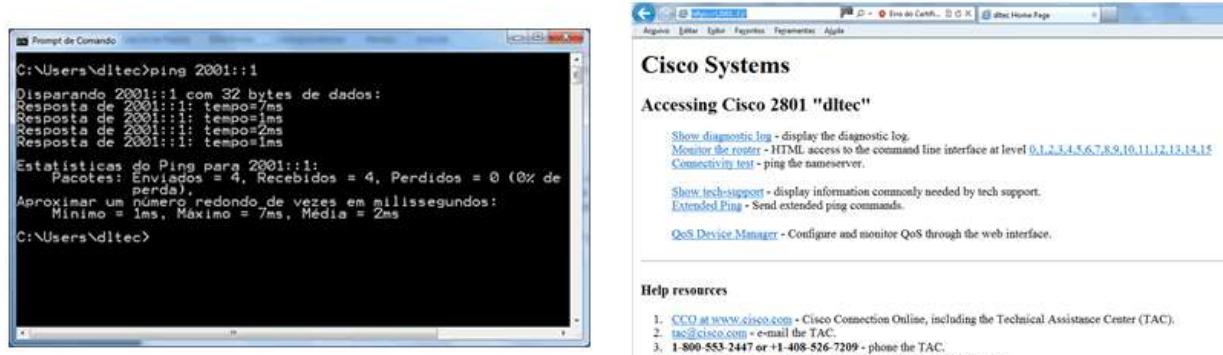
A configuração manual dispensa comentários, nela o administrador de redes deve definir manualmente o endereço IPv6 a ser utilizado, assim como os demais parâmetros.

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::9db: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::e0:0:0:0x24
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.(C8B88380-8AA9-4243-AA04-03297B37015C)
  Tipo End. Estado DAD Vida Válida Vida Pref. Endereço

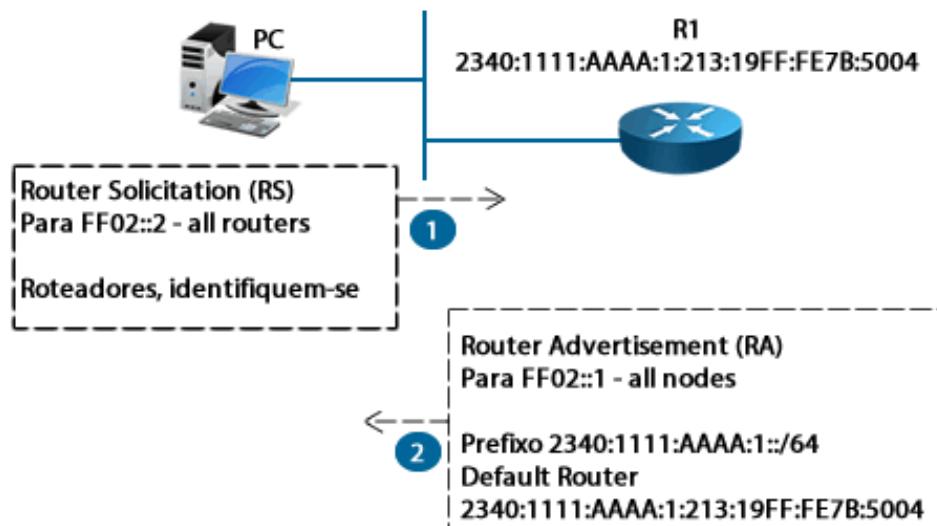
```

### 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.

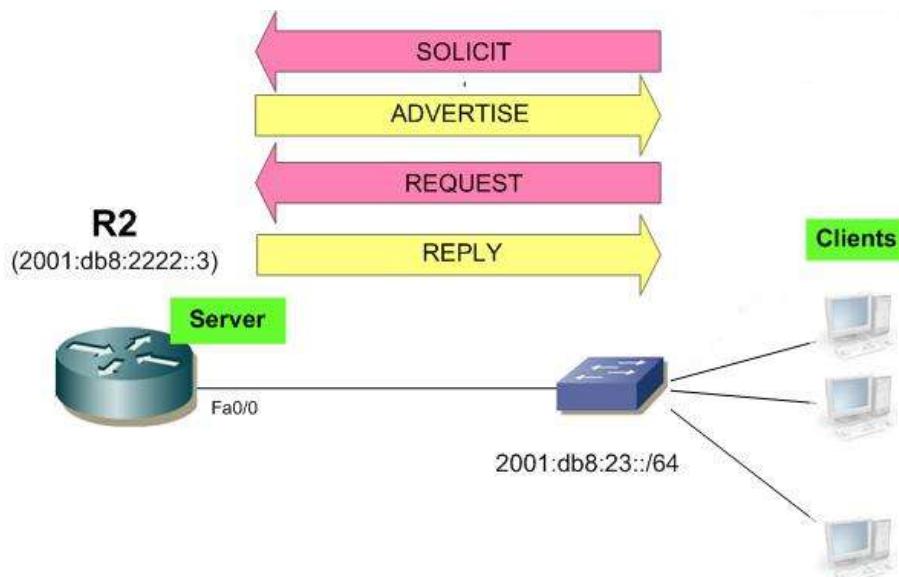
### 6.3.3 DHCPv6 – Stateless e Stateful

O DHCPv6 tem a mesma função que o DHCP estudado para o IPv4, porém ele funciona de forma distinta, pois não temos mais broadcasts no IPv6.

Existem duas formas de DHCPv6: Stateful e Stateless.

O Stateful é semelhante ao DHCP que estudamos para o IPv4, pois ele fornece IPs versão 6 conforme seu próprio pool de endereços, porém a mensagem inicial do cliente é enviada para o endereço de multicast FF02::1:2, o qual é monitorado por servidores DHCPv6 e roteadores atuando como DHCPv6 Relay.

As mensagens do DHCPv6 trocadas entre cliente e servidor seguem abaixo.



Para ativar o DHCPv6 relay em um roteador Cisco basta entrar na interface onde os clientes estão conectados e utilizar o comando “`ipv6 dhcp relay destination`” mais o IPv6 do servidor DHCPv6 remoto.

Nesse caso, assim como no Relay do IPv4 o roteador IPv6 agente relay vai servir de ponte entre os clientes e o servidor remoto que está em uma sub-rede diferente dos clientes.

O DHCPv6 Stateless não faz esse processo completo, pois ele tem a função de atuar em conjunto com o SLAAC (autoconfiguração) fornecendo o endereço do servidor DNS, o qual não é passado via auto-configuração.

Lembre-se que no processo de auto-configuração o cliente recebe apenas o prefixo da rede e utiliza o IP do roteador que respondeu sua solicitação como gateway.

As configurações relativas ao DHCPv6 Stateless e Stateful são estudadas no CCNP Routing & Switching.

#### 6.4 Roteamento IPv6

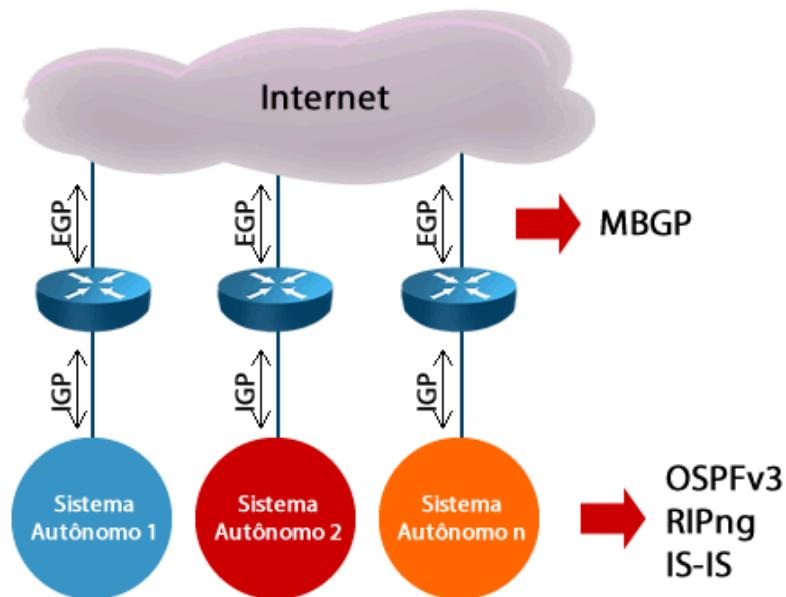
Os protocolos de roteamento para o IPv6 continuam tendo a mesma base dos utilizados para o IPv4, porém recebem novos nomes. Os principais protocolos de roteamento interno para IPv6 (IGP) são:

- **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 Multiprotocol 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.

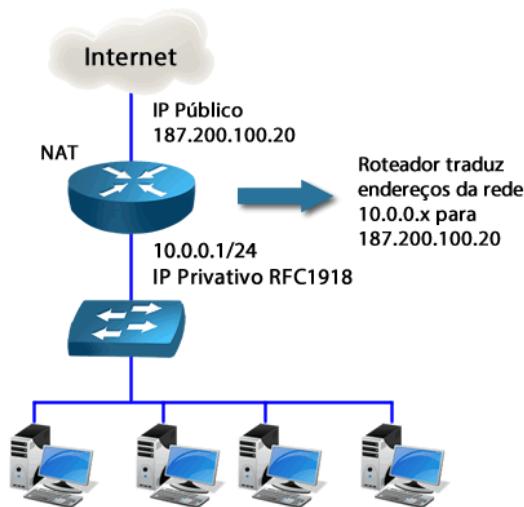


O foco do CCENT é o roteamento estático, os protocolos de roteamento dinâmicos serão estudados no ICND-2.

## 7 Planejando a Rede - Sub-redes com IPv6

Assim como para o IPv4, a implantação de uma rede IPv6 precisa da alocação de endereços para os dispositivos de redes, hosts e servidores de rede. Normalmente no IPv4 tínhamos endereços IP privativos, conforme RFC1918, na parte interna da rede ou Intranet e um ou mais endereços IPs públicos fornecidos por um ISP (provedor de Internet) configurados em uma ou mais interfaces de saída para a Internet.

Normalmente nessa saída de Internet utilizamos no IPv4 um processo de tradução com o NAT (Network Address Translation) ou um servidor Proxy, pois o IP da Intranet é privativo e não roteado na Internet pública. Veja a figura a seguir.



Essa é uma grande diferença do IPv6, pois com a quantidade de endereços disponíveis não precisaremos mais utilizar redes privativas, portanto todos os endereços de host das empresas serão endereços de Internet válidos, possibilitando comunicação fim a fim entre dispositivos na Internet IPv6.

Você verá que essa é uma vantagem do IPv6 que precisa de um cuidado maior com a segurança das redes, hosts e dispositivos de redes, pois todos os dispositivos estarão **expostos** na rede pública, o que com os IP's privativos não acontecia, pois eles escondem os hosts da rede interna dificultando um ataque direto aos hosts da rede. Isso traz uma preocupação maior com a implantação das redes IPv6 no que tange aos firewalls, IPS's e demais dispositivos de segurança. Mais para frente estudaremos os conceitos de segurança com o IPv6.

Um passo anterior à configuração é verificar se os dispositivos de rede suportam IPv6, assim como os hosts, servidores e demais clientes de rede onde o IP versão 6 será utilizado como protocolo de rede.

### 7.1 Endereços Globais de Unicast e Divisão em Sub-redes

Assim como no IPv4 o IPv6 foi dividido em diversas faixas pela IANA para divisão entre as regiões que administram os endereços de Internet, seus ISPs e empresas. Essa divisão gerou o que é chamado de "Global Address Space" e na Internet a faixa reservada para Unicast é a 2000::/3, o que resulta na faixa iniciando em 2000:0:0:0:0:0:0:0 até

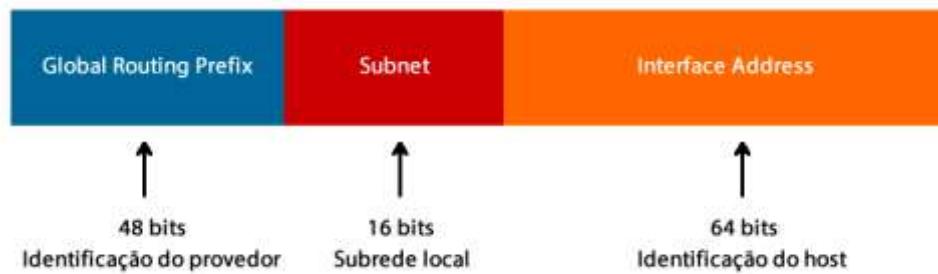
3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF para endereçamento.

Portanto a IANA dividiu essa faixa de endereços entre cada uma das regiões (RIR) e o bloco 2800::/12 corresponde ao espaço reservado para o LACNIC alocar na América Latina. O NIC.br (responsável pelas alocações do IPv6 no Brasil) por sua vez, trabalhará com um /16 que faz parte deste /12.

Essa divisão de endereços é top-down, ou seja, a IANA definiu um bloco de IPv6 para cada região ou RIR, os quais passarão para seus ISPs, que por sua vez distribuirão suas faixas de IPv6 em regiões para seus clientes e usuários finais, possibilitando uma agregação de rotas mais eficiente do que a atual para o IPv4. No projeto do IPv6 para sair de uma região para outra apenas uma rota IPv6 será necessária, por exemplo, para que um roteador de borda da Europa alcance determinada rede nos Estados Unidos apenas uma rota será necessária, assim como para um cliente alcançar as rotas do seu ISP também apenas uma rota será necessária, reduzindo a tabela de roteamento e aumentando a eficiência do IPv6 em relação ao roteamento no IPv4.

Os endereços globais de Unicast ou “Global Routing Prefix” são divididos em porção de rede e porção de host, porém a porção de rede terá algumas “fatias” que representam a região. Por exemplo, 2800::/12 representa que é um IP da LACNIC (América Latina), depois terá mais um pedaço que representará o Brasil (/16) e mais um pedaço do seu service provider ou ISP, normalmente um /32. Quando o ISP passar o bloco de endereço para o cliente será passado um /48 aí ele terá mais 16 bits para fazer subrede, uma vez que normalmente os hosts utilizam 64 bits para sua identificação.

Veja a figura abaixo com um resumo do que será um endereço de Internet em IPv6. Temos três campos básicos, o de identificação do ISP (/48) que tem dentro dele também a identificação do RIR e da entidade local que administra os IPv6 (por exemplo, NIC.BR), depois mais 16 bits de subrede e 64 bits para host.

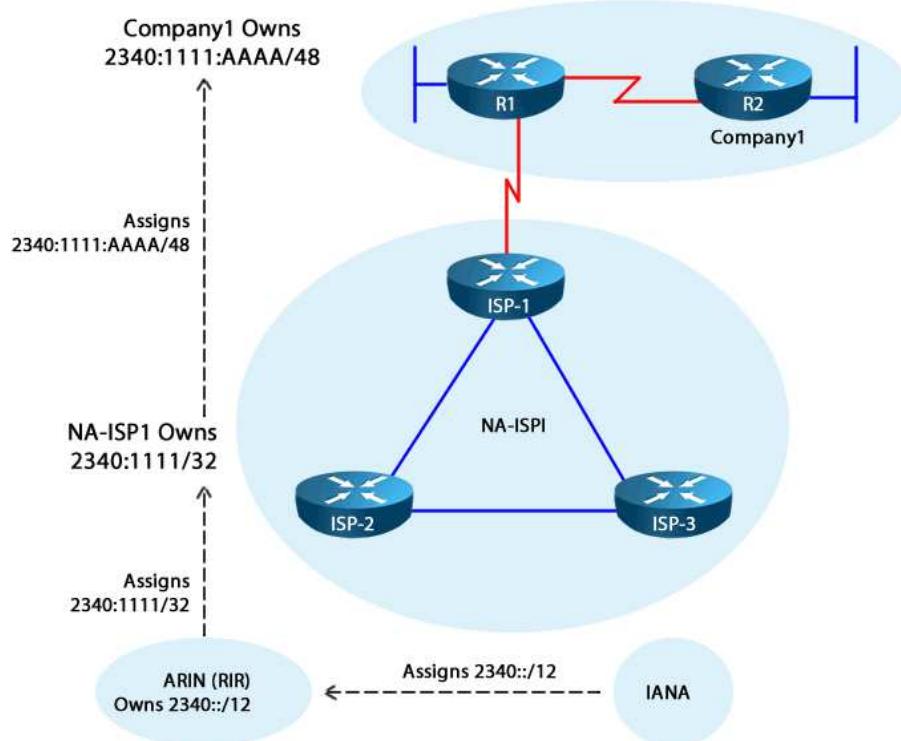


Note que a máscara de subrede utiliza a notação Classless Interdomain Routing (CIDR) com a barra “/” e a quantidade de bits de rede da máscara, conforme já citada anteriormente.

E o prefixo ou rede IPv6 é representada como um endereço IPv6 normal, porém com a porção de hosts toda em zero (assim como já era no IPv4). Portanto a notação e simplificação de um prefixo IPv6 é como para um endereço comum do IPv6 e sempre precisamos ter os dois pontos no final seguidos da barra (/) e o número de bits de subrede, por exemplo:

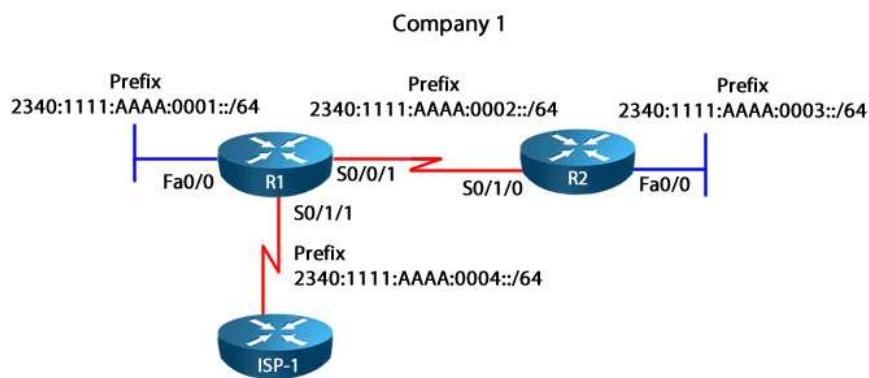
- 2800::/12 que é a faixa de IPs da América Latina é o mesmo que 2800:0000:0000:0000:0000:0000, porém as sequências de zero foram substituídas pelo “::”.
- Seria errado escrever 28::/12, porque somente o zero a esquerda pode ser suprimido.
- Seria errado escrever 2800/12, porque 2800 não é um IPv6

Veja o exemplo na figura abaixo onde a IANA fornece o bloco 2340::/12 para a ARIN (RIR que representa a região de Américas), a qual fornece para o ISP1 a faixa 2340:1111::/32, o qual alocou o bloco 2340:1111:AAAA::/48 para seu cliente chamado Company1.



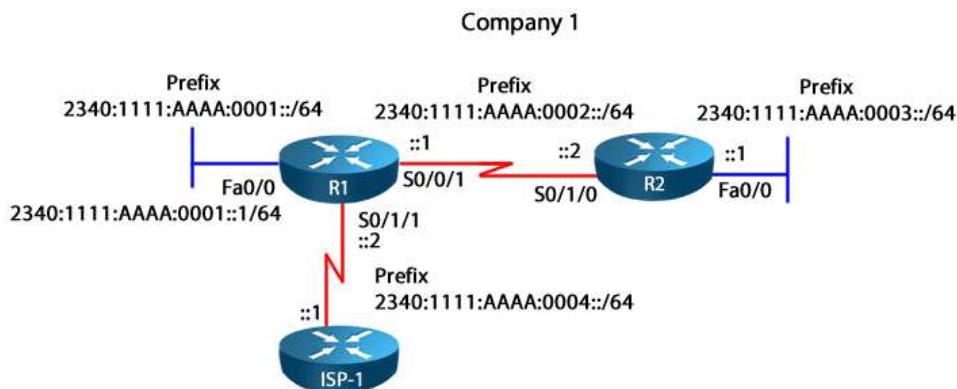
Dentro da rede de Company1 ele pode agora subdividir esse /48 em diversas sub-redes conforme suas necessidades internas. Por exemplo, na figura abaixo temos quatro sub-redes alocadas:

- 2340:1111:AAAA:0001::/64 para a LAN de R1;
- 2340:1111:AAAA:0002::/64 para a WAN entre R1 e R2;
- 2340:1111:AAAA:0003::/64 para a LAN de R3
- 2340:1111:AAAA:0004::/64 para a WAN entre R1 e o roteador do ISP.



Com 16 bits o cliente tem  $2^{16}$  sub-redes ou 65.536 sub-redes com 64 bits de host ou  $18.7 \times 10^{18}$  endereços de hosts. Devido a esse número elevado de hosts é possível quebrar mais ainda as sub-redes para um melhor aproveitamento no endereçamento de redes WAN ou dispositivos que utilizam IPs fixos. Por exemplo, pegar a sub-rede 2340:1111:AAAA:0002::/64 e dividi-la em sub-redes /112, ou seja, 48 bits para sub-rede (mais que o espaço do IPv4 de 32 bits) e 16 bits para host, dando mais 281 trilhões de sub-redes com 65536 IPs versão 6 cada sub-rede.

Esta é a lógica para você planejar e endereçar seus laboratórios e cenários de estudo relativos ao IPv6 ou até mesmo a implantação de IPv6 na empresa onde você trabalha, por exemplo, veja a mesma figura anterior já com os alguns hosts e endereços de interfaces abaixo:



Para verificar a alocação de prefixos atuais pela IANA consulte o link:  
<http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml>

Outra opção de endereçamento interno é com a utilização de endereços locais de unicast ou ULA (FD00::/8) divididos em sub-redes, porém não está previsto o NAT de IPv6 para IPv6 como no IPv4, portanto acredita-se que essa solução com o tempo será simplesmente abandonada, porém você pode ver esse tipo de endereçamento em exemplos práticos.

## 8 Alterações no Serviço de Resolução de Nomes

Até este ponto do curso você já deve ter notado que o IPv6 é um novo protocolo de infraestrutura para redes corporativas e também na Internet. Em muitos aspectos ele é bem parecido com o bom e velho protocolo IPv4, pois não foram feitas alterações nas pilhas superiores ou inferiores ao IP para o suporte a essa nova versão. Por isso mesmo continuamos utilizando DHCP, DNS, HTTP, SIP, LDAP, ou seja, quase todos os protocolos que estamos acostumados no IPv4.

Assim como para o IPv4 o serviço de resolução de nomes ou DNS em redes IPv6 será parte fundamental para o funcionamento das Intranets e da Internet, pois agora com o tamanho e escrita dos endereços vai ficar cada vez mais difícil de decorar IPs até mesmo na Intranet!

No IPv4 os hosts utilizam um padrão de registro chamado "A Record" referenciando um endereço de 32 bits. Já no IPv6 temos 128 bits por isso o registro foi chamado de "AAAA Record" ou "Quad-A Record" (registro quádruplo A), pois o IPv6 é quatro vezes maior que o endereço IPv4. Veja um exemplo abaixo.

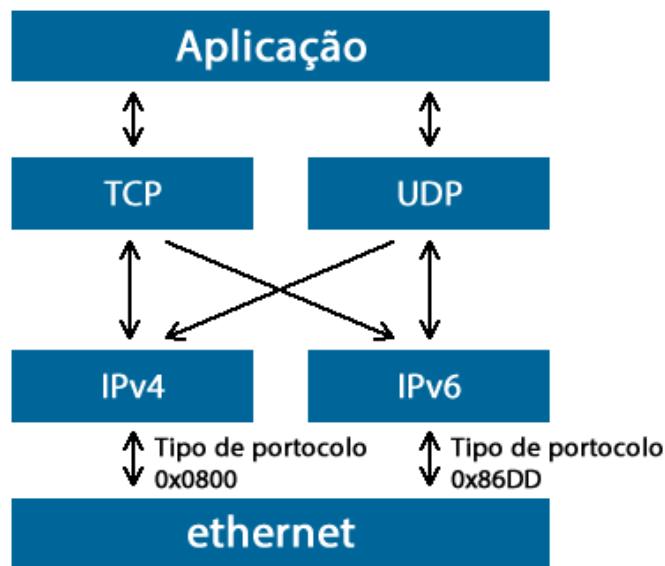
V6-host	IN	AAAA	2620:0:1cf0:face:b00c::3
---------	----	------	--------------------------

Além disso, o seu servidor DNS precisa "escutar" a porta 53 através do protocolo IPv6, pois senão os hosts farão a consulta via IPv6 mas sem porta UDP pronta para receber essa requisição simplesmente não acontecerá nada.

Outra mudança é na resolução reversa ou reverse-lookup, pois com a mudança do endereço esse parâmetro também foi revisado e deve ser considerado na configuração dos DNSs com IPv6.

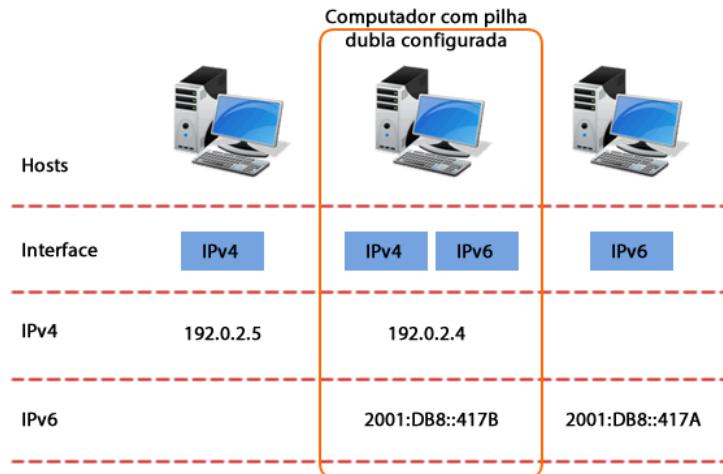
## 9 Pilha Dupla

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.

A seguir vamos aprender como configurar o IPv6 em roteadores e switches Cisco.

## 10 Introdução à Configuração do IPv6 em Roteadores e Switches Cisco

Você deve estar se perguntando: "Mas o que muda em relação ao que estudamos até o capítulo 12 para o IPv4 quando implementamos redes IPv6? Vamos jogar tudo fora e será uma nova filosofia de configuração?".

Se você estudou bem e entendeu os tópicos anteriores desse capítulo já deve ter essa resposta, pois não estamos mudando TODA a rede, apenas a camada-3.

Claro que isso acaba afetando alguns serviços de rede, mas em termos de configuração tudo continua muito parecido, pois ainda teremos que configurar:

1. Parâmetros gerais como hostname, senhas, banners, etc.
2. Acesso Telnet, SSH, HTTP e HTTPS dos roteadores continuam valendo, só que agora através de endereços IPv6 configurados em suas interfaces.
3. Configuração das interfaces para termos as redes IPv6 locais e diretamente conectadas.
4. Rotas estáticas ou protocolos de roteamento dinâmicos IPv6 para que os roteadores saibam como chegar às redes IPv6 de destino.
5. Alocação dinâmica de IPs via autoconfiguração ou DHCPv6.
6. Parâmetros de segurança, tais como ACLs para IPv6.
7. Demais recursos de rede, tais como QoS, telefonia IP, etc.

No CCENT o foco do IPv6 está na configuração de interfaces e rotas estáticas IPv6.

Vamos também estudar conceitos de alocação dinâmica de endereços IPv6, o qual tem uma mudança grande em relação ao IPv4 pela multiplicidade de métodos.

No CCENT vamos estudar como configurar o roteador como cliente e relay, não é foco do exame a configuração do servidor DHCPv6 devido a complexidades na solução, mas com certeza você não vai parar aqui e vai aprender muito mais no CCNP!

## 11 Configurações Básicas do IPv6 – Ativação, Interfaces, Testes e Vizinhança

Para configurar o IPv6 devemos começar habilitando o protocolo com o comando em modo de configuração global “**ipv6 unicast-routing**”.

```
R4#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
R4(config)#ipv6 unicast-routing  
R4(config)#
```

Você até consegue ativar um IPv6 em uma interface sem o comando acima, porém não haverá roteamento IPv6, o dispositivos camada-3 Cisco será um cliente de rede, parecido com o que ocorre com o IPv4 e os endereços de gerenciamento em switches. Veja exemplo abaixo.

```
DlteC-FW-GW#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
DlteC-FW-GW(config)#no ipv6 unicast-routing  
DlteC-FW-GW(config)#int f0/0  
DlteC-FW-GW(config-if)#ipv6 enable  
DlteC-FW-GW(config-if)#do show ipv6 interface brief  
FastEthernet0/0 [up/up]  
 FE80::21E:13FF:FE0B:1AEE  
FastEthernet0/1 [up/up]  
 unassigned  
DlteC-FW-GW(config-if)#
```

Na configuração mostrada no exemplo anterior utilizamos o comando “**ipv6 enable**” dentro da interface fast 0/0, o que faz com que o roteador crie um endereço IPv6 de Link Local mesmo que o comando “**no ipv6 unicast-routing**” esteja presente na configuração, pois o roteador não fará o roteamento com esse comando, mas nada impede que uma das suas interfaces responda através de IPv6, por exemplo, a um teste de ping.

Note outro detalhe interessante que para verificar o IPv6 configurado utilizamos o comando “**show ipv6 interface brief**”, apenas trocamos o **ip** por **ipv6** e muitos dos comandos será assim, fica aqui essa dica!

Diferente do IPv4, até as versões atuais de 2013 do Cisco IOS, o **roteamento IPv6 não vem habilitado por padrão**, por isso o comando acima ativa o roteamento IPv6 nos dispositivos camada-3.

Na maioria dos sistemas operacionais de clientes e servidores de rede essa realidade é bem diferente, sendo que o suporte nativo ao IPv6 é ativado em vários deles, tais como Windows (Vista, 7, 8, 2003 Server, 2008 Server e 2012 Server), Linux Ubuntu, Free-BSD, Unix, MAC OS-X e outros.

Para verificar se o sistema operacional suporta IPv6 nativo basta dar um ping para a loopback “**::1**”, se houver resposta o sistema operacional suporta IPv6. No Linux e MAC OS-X o comando é o “**ping6**” e no Windows e Cisco IOS continua com o “bom e velho **ping**”.

### 11.1 Configurando Interfaces IPv6 no Cisco IOS

O próximo passo é configurar os endereços **Globais de Unicast**, pois os endereços **de link-local** são automaticamente configurados via EUI-64.

Para os endereços globais temos duas opções básicas de configuração:

1. Utilizar endereços de Internet da faixa **2000::/3**, porém para navegar com esses endereços é preciso que ele seja registrado, seja locado através de um provedor de serviços ou processo de Sistema Autônomo.
2. Utilizar a faixa dos endereços ULA (Unique Local Address) para criar uma rede privativa com endereços da faixa fc00::/7, sendo que para uso em redes corporativas normalmente utilizamos a faixa **fd00::/8** com sub-redes **/48**.

Para ambiente de laboratório mostramos um exemplo de projeto e alocação de endereços IP na parte I do capítulo de IPv6, basicamente o projeto é parecido com IPv4, onde temos que definir as redes, sub-redes, endereços de Interfaces e hosts da rede. A diferença é que os endereços de host utilizam identificadores (host-ID) de 64 bits.

Nos roteadores e switches Cisco podemos configurar os endereços globais das seguintes maneiras:

1. **Configuração estática**: "ipv6 address *end-ipv6/tamanho-do-prefixo*"
2. **Configuração estática com EUI-64**: "ipv6 address *prefixo-de-rede/64 eui-64*"
3. **Autoconfiguração stateless**: "ipv6 address autoconfig [default]"
4. **DHCP statefull**: "ipv6 dhcp client"

Nas opções 1 e 2 o servidor DNS e roteador padrão deverão ser configurados manualmente. Na autoconfiguração é preciso um DHCP stateless ou configuração estática do DNS, pois o roteador padrão é passado via protocolo NDP (mensagens de RS e RA). Na opção DHCP statefull TODAS as opções são passadas pelo servidor DHCPv6, menos o roteador padrão, o qual é adquirido via NDP com a mensagem de RA (Router Advertisement).

Veja abaixo exemplos de configuração na sequência.

No primeiro exemplo vamos analisar a configuração a interface fast 0/0 com o IPv6 estático **2000:100::1/112**, já a interface fast 0/1 será configurada via **EUI-64** com o prefixo **2001:100::/64** e a interface fast 2/0 será configurada via **autoconfiguração**.

```
R1(config)#int f0/0
R1(config-if)#ipv6 address 2000:100::1/112 ?
  anycast Configure as an anycast
  eui-64 Use eui-64 interface identifier
<cr>
R1(config-if)#ipv6 address 2000:100::1/112
R1(config-if)#int f0/1
R1(config-if)#ipv6 address 2001:100::/64 eui-64
R1(config-if)#int f2/0
R1(config-if)#ipv6 address autoconfig
R1(config-if)#end
R1#
```

Com o comando "**show ipv6 interface brief**" temos um resumo das interfaces IPv6 e os endereços configurados, veja abaixo a saída para o R1 configurado anteriormente.

```
R1#sho ipv6 interface brief
FastEthernet0/0          [up/up]
  FE80::[C001:33FF:FE7C:0
    2000:100::1
FastEthernet0/1          [up/up]
  FE80::[C001:33FF:FE7C:1
    2001:100::C001:33FF:FE7C:1
FastEthernet2/0          [up/up]
  FE80::[C001:33FF:FE7C:20
    2002:100::C001:33FF:FE7C:20

-> endereço de link-local via EUI-64
-> endereço global unicast estático

-> link local e global usam EUI-64 e tem
-> mesmo interface ID "C001:33FF:FE7C:1"

-> na autoconfig também é utilizado o
-> EUI-64 para definir a interface ID
```

Com o comando “**show ipv6 interface fast 0/0**”, por exemplo, você pode ver as opções completas referentes ao IPv6, veja exemplo abaixo da saída para as interfaces f0/0 e f2/0.

```
R1#sho ipv6 int f0/0  -> Interface usando configuração estática
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C001:33FF:FE7C:0 -> link local via
EUI-64 utilizando o MAC da interface
  No Virtual link-local address(es):
  Global unicast address(es):
    2000:100::1, subnet is 2000:100::/112 -> end global e subrede
  Joined group address(es): -> endereços de multicast
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF7C:0
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1 -> detecção de endereços
duplicados está habilitada e rodou uma vez (attempts)
  ND reachable time is 30000 milliseconds -> tempo de vida do protocolo de
descoberta de hosts vizinhos
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.

R1#
R1#sho ipv6 int fast 2/0 -> interface usando autoconfiguration
FastEthernet2/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C001:33FF:FE7C:20
  No Virtual link-local address(es):
  Global unicast address(es):
    2002:100::C001:33FF:FE7C:20, subnet is 2002:100::/64 [EUI/CAL/PRE]
      valid lifetime 2591872 preferred lifetime 604672
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF7C:20
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
```

ND advertised retransmit interval is 0 milliseconds  
ND router advertisements are sent every 200 seconds  
ND router advertisements live for 1800 seconds  
ND advertised default router preference is Medium  
Hosts use stateless autoconfig for addresses.

Quando utilizamos a autoconfiguração note na saída do comando "show ipv6 int f2/0" que embaixo do IPv6 global aparece uma linha destacada com um "lifetime" e "preferred lifetime" que são os timers do tempo de vida do prefixo recebido via NDP pelo roteador vizinho.

Como o IPv6 suporta a reconfiguração da rede (network renumbering), quando é preciso trocar um prefixo antigo por um novo é possível anunciar a rede antiga com um lifetime mais curto e a rede ou prefixo mais novo com um lifetime mais longo, para que haja a troca do antigo pelo novo. Outra opção é expirar um determinado prefixo em determinada data e hora. Isto é útil para a reconfiguração de prefixes em redes de grande porta com diversos hosts na mesma sub-rede.

O DAD (descoberta de IPs duplicados) é utilizado para verificar se não existe outro IP igual na rede. Note que na saída do comando show de ambas as interfaces têm a linha "*ND DAD is enabled, number of DAD attempts: 1*", ou seja, o DAD está ativo e foi rodado 1 vez (number of DAD attempts: 1), ou seja, o IP configurado não deu nenhum conflito e foi ativado na interface. Se esse contador estiver diferente de 1 é sinal que houve conflito de endereços.

#### 11.1.1 Grupos de Multicast Padrões das Interfaces Cisco

Na saída do comando "show ipv6 interfaces" para ambas as interfaces mostradas anteriormente temos as informações sobre os grupos de multicast que elas por padrão pertencem. É importante saber essas informações porque agora não temos mais broadcast e muitas operações dependem do Multicast para funcionar.

Veja o detalhe apenas dos grupos de multicast retirados da interface fast 0/0.

```
Joined group address(es): -> endereços de multicast
  FF02::1
  FF02::2
  FF02::1:FF00:1
  FF02::1:FF7C:0
```

Os dois primeiros grupos você deve saber, pois podem ser cobrados na prova, portanto que representam os endereços **FF02::1** e **FF02::2**?

**A resposta é FF02::1 é o endereço de multicast de todos os Hosts da Rede e o FF02::2 representa todos os roteadores da rede.**

O endereço **FF02::1:FF00:1** é o solicited-node do endereço global 2000:100:**:1** e o que vem logo abaixo **FF02::1:FF7C:0** é o endereço de solicited-node do endereço de link-local da interface FE80::C001:33FF:FE**7C:0**. Lembre-se que ele é formado pelo prefixo de multicast **FF02::1:FF** mais os últimos 24 bits do endereço local ou global configurado. Para cada endereço teremos um solicited-node.

## 11.2 Redes Locais e Diretamente Conectadas no IPv6

Quando configuramos interfaces no IPv6 e elas ficam UP/UP também são criadas rotas locais, apontando para a própria interface com uma máscara /128, e para a rede IPv6 que a interface pertence, conforme prefixo configurado.

Para verificar essas informações podemos utilizar o comando “**show ipv6 route**”, lembrando que para o IPv4 é “**show ip route**”. Veja exemplo da tabela de roteamento IPv6 abaixo.

```
R1#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
C  2340:1111:AAAA:1::/64 [0/0]
  via ::, FastEthernet0/0
L  2340:1111:AAAA:1::1/128 [0/0]
  via ::, FastEthernet0/0
C  2340:1111:AAAA:2::/64 [0/0]
  via ::, Serial0/0
L  2340:1111:AAAA:2::1/128 [0/0]
  via ::, Serial0/0
L  FF00::/8 [0/0]
  via ::, Null0
```

Note na primeira linha em destaque temos a rede diretamente conectada à fast 0/0 2340:1111:AAAA:1::/64 (identificada com “C”) e logo abaixo temos uma rota local para o endereço IP configurado nessa interface 2340:1111:AAAA:1::1/128 indicada com um “L” de Local na frente.

Após a rota, entre colchetes, temos as informações de distância administrativa e métrica, basicamente as mesmas informações que utilizamos no IPv4 para classificar as rotas entre diferentes protocolos de roteamento (distância administrativa) ou entre um mesmo protocolo (métrica). Para as rotas diretamente conectadas ambos os valores são zero e as regras são as mesmas que estudamos no IPv4. Por exemplo, rotas estáticas com uma interface como referência tem distância zero e apontando para um IPv6 de destino tem distância “1”.

Quanto menor a distância administrativa e a métrica melhor é a rota, mesma regra de desempate que estudamos para o IPv4.

Você pode utilizar os comandos “**show ipv6 route connected**” e “**show ipv6 route local**” para verificar somente as rotas conectadas e locais respectivamente, veja exemplo abaixo.

```
R1#show ipv6 route connected
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
C  2340:1111:AAAA:1::/64 [0/0]
  via ::, FastEthernet0/0
C  2340:1111:AAAA:2::/64 [0/0]
  via ::, Serial0/0
```

```
R1#show ipv6 route local
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
L  2340:1111:AAAA:1::1/128 [0/0]
  via ::, FastEthernet0/0
L  2340:1111:AAAA:2::1/128 [0/0]
  via ::, Serial0/0
L  FF00::/8 [0/0]
  via ::, Null0
R1#
```

### 11.3 Testando a Conectividade das Interfaces IPv6

Como já citado, o ICMP do IPv4 foi trocado pelo protocolo ICMPv6 no IPv6, porém recursos como ping e trace continuam presentes para realizar os testes de conectividade entre hosts e interfaces IPv6. A diferença é que em determinadas versões de IOS será solicitada a interface de saída escrita de maneira completa e com o número da interface sem espaço, veja dois exemplos abaixo.

```
dltec#ping fe80::1
Output Interface: fastethernet0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::1, timeout is 2 seconds:
Packet sent with a source address of FE80::1%FastEthernet0/0
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
```

A justificativa do exemplo acima é simples, pois todas as interfaces têm endereços de link-local e eles iniciam com **FE80::/10**, portanto como saber para que interface encaminhar nesse caso? Somente identificando a interface de saída do ping ou traceroute.

Assim como para o IPv4 existem opções que você pode utilizar com o comando ping, veja um exemplo abaixo do ping com uma repetição de 100 vezes.

```
dltec#ping 2000:100::1 ?
  data      specify data pattern
  repeat    specify repeat count
  size      specify datagram size
  source    specify source address or name
  timeout   specify timeout interval
  verbose   verbose output
<cr>

dltec#ping fe80::1 repeat 100
Output Interface: fastethernet0/0
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to FE80::1, timeout is 2 seconds:
Packet sent with a source address of FE80::1%FastEthernet0/0
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 0/0/4 ms
```

Podemos também utilizar o ping estendido digitando apenas "ping", dando um "enter" e no momento de escolher o protocolo digite "ipv6", veja exemplo abaixo.

```
dltec#ping
Protocol [ip]: ipv6
Target IPv6 address: fe80::1
Repeat count [5]: 100
Datagram size [100]: 1000
Timeout in seconds [2]:
Extended commands? [no]: y
Source address or interface: fastethernet0/0
UDP protocol? [no]:
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]: y
Include destination option? [no]:
Sweep range of sizes? [no]:
Output Interface: fastethernet0/0
Type escape sequence to abort.
Sending 100, 1000-byte ICMP Echos to FE80::1, timeout is 2 seconds:
Packet sent with a source address of FE80::1%FastEthernet0/0
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 0/0/4 ms
```

Veja abaixo exemplo de traceroute no Cisco IOS. Os asteriscos representam que a partir do segundo salto não houve resposta, pois a mesma simbologia de problemas que estudamos para o ping e trace no IPv4 continua a mesma no IPv6. Para cancelar os testes ainda podemos utilizar a sequência de saída “**ctrl+shift+6**”.

```
R1#traceroute 2340:1111:AAAA:3:C006:22FF:FEEC:0

Type escape sequence to abort.
Tracing the route to 2340:1111:AAAA:3:C006:22FF:FEEC:0

 1 2340:1111:AAAA:2::2 4 msec 8 msec 12 msec
 2 * * *
 3 * * *
R1#
```

Você pode também forçar que o ping e o traceroute seja através do IPv6 quando fizer um teste para um nome de domínio, por exemplo, “**ping ipv6 www.ietf.org**”.

Antes de iniciar a configuração de protocolo de roteamento ou recursos mais avançados em seus laboratórios lembre sempre de primeiro verificar a conectividade das interfaces através do ping. Teste tanto com os IPs globais como locais, iniciando sempre pelo de link-local, assim se houver um problema de camada 2 ou 3 simples você resolverá antes da ativação do roteamento e pode evitar tempo perdido tentando resolver um problema que não existe!

## 11.4 Verificando Vizinhos IPv6 – Protocolo NDP

Uma vez configuradas as interfaces você pode iniciar os testes de ping, traceroute, telnet para verificar a conectividade em camada 3 até a 7, porém lembre-se que para os vizinhos em uma LAN se comunicarem um protocolo novo entrou no lugar do ARP chamado NDP.

O NDP funciona automaticamente, sem necessidade de configurações, e a tabela de vizinhanças pode ser visualizada com o comando “**show ipv6 neighbors**”. Veja exemplo abaixo.

```
R2#ping ff02::1
Output Interface: fastethernet0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FF02::1, timeout is 2 seconds:
Packet sent with a source address of FE80::C005:22FF:FE00:0

Reply to request 0 received from FE80::C006:22FF:FE00:0, 32 ms
Reply to request 1 received from FE80::C006:22FF:FE00:0, 24 ms
Reply to request 2 received from FE80::C006:22FF:FE00:0, 16 ms
Reply to request 3 received from FE80::C006:22FF:FE00:0, 20 ms
Reply to request 4 received from FE80::C006:22FF:FE00:0, 20 ms
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/22/32 ms
5 multicast replies and 0 errors.

R2#show ipv6 neighbors
IPv6 Address                               Age Link-layer Addr State Interface
FE80::C006:22FF:FE00:0                      0 c206.22ec.0000 REACH Fa0/0
2340:1111:AAAA:3:C006:22FF:FE00:0           9 c206.22ec.0000 STALE Fa0/0
```

R2#

Note que iniciamos o teste pingando o endereço de multicast de todos os nós da rede, assim os clientes de rede que não tem bloqueio de segurança contra esse tipo de teste irão responder e teremos entradas na tabela de vizinhança do IPv6.

Os endereços descobertos tem o mesmo final C006:22FF:FE00:0, por isso podemos concluir que é um endereço Global Unicast (faixa do 2000::/3) e seu link-local, ambos criados a partir do EUI-64. Note que ambos os endereços têm o mesmo endereço MAC.

Essa tabela é dinâmica e apagada de tempos em tempos, assim como uma entrada ARP que tem seu “aging-time” e é apagada após certo tempo sem atividade daquele endereço.

Podemos apagar a tabela de vizinhos com o comando “**clear ipv6 neighbors**”, veja exemplo abaixo:

```
R2#clear ipv6 neighbors
R2#show ipv6 neighbors
R2#
```

Portanto, após o clear a tabela de vizinhos IPv6 está vazia e não mostra nenhuma entrada com o comando “show ipv6 neighbors”.

## 12 Atribuindo IPs via Autoconfiguração e Conceitos do DHCPv6

A alocação dinâmica de IPs no IPv6 é um assunto ainda controverso e em fase de estudo e desenvolvimento, pois no IPv4 tínhamos apenas o DHCP como opção de alocação dinâmica. No IPv6 a autoconfiguração foi a princípio elaborada para suprir a necessidade de um servidor DHCP, porém em sua implementação inicial não foi inserida a opção do servidor DNS nos anúncios dos roteadores.

Por esse motivo foram desenvolvidos os serviços de DHCP para o IP versão 6, chamado DHCPv6, o qual pode ser similar ao DHCP e guardar o estado das atribuições, por isso classificado como statefull, ou então mais simples para atuar juntamente com o SLAAC e fornecer apenas informações adicionais ao prefixo e gateway padrão.

Outra opção desenvolvida é o uso do SLAAC com "Recursive DNS Server Option" ou RDNSS. A função do RDNSS é transmitir um ou mais endereços IPv6 de servidores DNS. Ele é enviado nas mensagens Router Advertisement e deve ser ignorado em outras mensagens, porém nem todos os sistemas operacionais suportam essa facilidade. Um exemplo de sistema operacional que suporta o RDNSS é o Linux.

Portanto as opções de configuração dinâmica no IPv6 são:

- **SLAAC:** Não serve como uma solução completa, pois não passa a informação do DNS e precisaria da configuração manual ou em massa via script do endereço dos servidores DNS nos clientes.
- **SLAAC com DHCPv6 Stateless:** Suportado por praticamente todos os clientes IPv6 e necessita que o bit O na mensagem de anúncio do roteador (RA ou Router Advertisement) seja ativada pelo roteador que está anunciando o prefixo.
- **SLAAC com RDNSS:** O RDNSS ou Recursive DNS Server Option está definido na RFC 6106 e permite que a mensagem de anúncio do roteador passe endereços de DNS, porém não é suportada por alguns sistemas operacionais.
- **DHCPv6 Statefull:** Passa todas as informações como no DHCP do IPv4 com exceção do gateway padrão, o qual é aprendido pelo cliente através da mensagem de RA enviada pelo roteador local. Para que os hosts entendam que precisam utilizar o DHCPv6 é necessário que o bit M da mensagem de RA enviada pelo roteador esteja setado.

### 12.1 Autoconfiguração Stateless ou SLAAC

Nos roteadores Cisco as interfaces dos roteadores já estão preparadas para passar via mensagens de RA seu prefixo e endereço de link local para que os clientes da rede se autoconfigurem. Portanto, se você configurar o endereço IPv6 2340:1111:AAAA:3::/64 e o link local FE80::C005:22FF:FEEC:0 seu roteador irá passar em sua mensagem de RA (anúncio de roteador) ou responder a solicitações (RS – Router Solicitation) com os seguintes parâmetros:

- Prefixo/comprimento: 2340:1111:AAAA:3::/64
- Tempo de vida (lifetime): válido 2591998 e preferido 604798
- Gateway: FE80::C005:22FF:FEEC:0

Veja a saída do comando em uma interface de um roteador cliente.

```
R3#sho ipv6 int f0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C006:22FF:FEEC:0
    No Virtual link-local address(es):
      Global unicast address(es):
        2340:1111:AAAA:3:C006:22FF:FEEC:0,      subnet      is      2340:1111:AAAA:3::/64
[EUI/CAL/PRE]
          valid lifetime 2591886 preferred lifetime 604686
```

O comando de configuração na interface do cliente foi “**ipv6 address autoconfig default**”, para que ele inserisse a rota padrão em sua tabela de roteamento, veja a saída abaixo:

```
R3#sho ipv6 rou
IPv6 Routing Table - 4 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external

S  ::/0 [1/0]
    via FE80::C016:BFF:FECC:0, FastEthernet0/0
C  2340:1111:AAAA:3::/64 [0/0]
    via ::, FastEthernet0/0
L  2340:1111:AAAA:3:C006:22FF:FECC:0/128 [0/0]
    via ::, FastEthernet0/0
L  FF00::/8 [0/0]
    via ::, Null0
R3#
```

Note que o gateway (rota para ::/0) é o endereço de link local do roteador que está enviando RAs na rede. Se inserirmos um cliente Windows, Linux ou MAC OS-X acontecerá o mesmo, porém outros sistemas operacionais normalmente utilizam endereços IP randômicos para gerar endereços globais seguros, veja a saída em um computador com Windows 8 abaixo conectado à mesma rede.

Os sistemas operacionais como Windows não utilizam o EUI-64 para gerar os endereços globais, isso para evitar problemas de privacidade na rede, pois o endereço MAC do computador é utilizado nesse tipo de autoconfiguração.

Nesse exemplo acima o Windows utiliza uma extensão de privacidade definida na RFC 4941, a qual utiliza um Hash MD5 para esconder o endereço MAC do computador na criação do identificador do Host. Além disso, o Windows utiliza endereços de host randômicos, ou seja,

eles são trocados de tempos em tempos, note na configuração que aparece um endereço preferencial (preferred) e outro temporário (temporary).

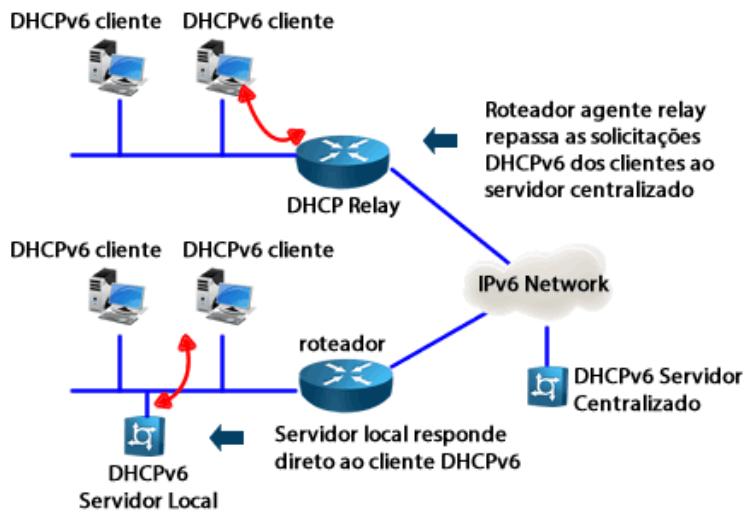
Em nosso curso de IPv6 ensinamos a trabalhar com esses tipos de endereços e também desabilitá-los no Windows e outros sistemas operacionais, aqui no CCENT o foco é a configuração em roteadores e switches Cisco, os quais utilizam o EUI-64 para geração de host-ID ou endereços fixos.

O GNS3 tem um sniffer instalado (se você instalar a versão completa) chamado Wireshark, com ele você pode selecionar uma interface para capturar pacotes e verificar as mensagens do IPv6 trocadas.

## 12.2 Endereços via DHCPv6 Statefull e Agente Relay

Assim como no mundo IPv4 o serviço de DHCP para IPv6 pode ser ativado diretamente em roteadores ou switches Layer-3. A outra opção é a ativação em servidores de rede.

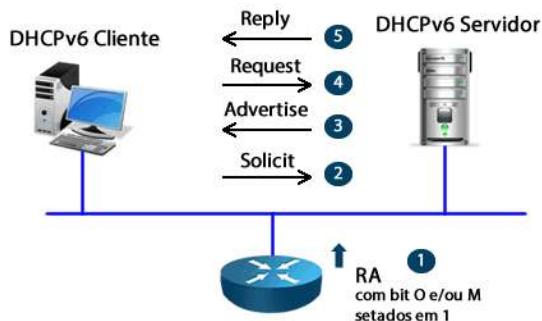
O DHCPv6 pode também trabalhar de forma distribuída ou centralizada. Na forma centralizada precisará dos agentes Relay que repassam as solicitações de IPv6 locais através da rede até chegar no servidor centralizado, o qual tem os escopos (faixas de IPv6 a serem atribuídas dinamicamente) configurados. Veja a figura a seguir.



O DHCPv6 está definido na RFC3315, sendo que os clientes utilizam a porta UDP 546 e os servidores e relays escutam as mensagens DHCP na porta UDP 547. Como o IPv6 não possui mais broadcast o multicast é utilizado para troca de informações com os seguintes endereços:

- **ff02::1:2** - todos os agentes DHCPv6 relay e servidores.
- **ff05::1:3** - todos os servidores DHCPv6.

Veja a figura abaixo com as mensagens utilizadas pelo DHCPv6.



Veja abaixo um exemplo das mensagens trocadas entre um servidor DHCPv6 e um cliente, onde o endereço **2001:db8:1111::27** foi repassado a esse cliente.

```

38:52 Srv Notice Received SOLICIT on Conexao de Rede sem Fio/20, trans-id=0x3e0f, 6 opts: 8 1 3 39 16 6 (non-relayed)
38:52 Srv Info Client 00:01:00:01:16:fb:ed:2f:24:b6:fd:06:dc:17 got 2001:db8:1111::27 (IAID=213915781, pref=86400,valid=172800).

38:52 Srv Notice Sending ADVERTISE on Conexao de Rede sem Fio/20,transID=0x3e0f, opts: 3 2 1 7 23 24, 0 relay(s).

39:53 Srv Notice Received REQUEST on Conexao de Rede sem Fio/20, trans-id=0x3e0f, 7 opts: 8 1 2 3 39 16 6 (non-relayed)
39:53 Srv Info Cache: Cached address 2001:db8:1111::27 found. Welcome back.

39:53 Srv Info Client 00:01:00:01:16:fb:ed:2f:24:b6:fd:06:dc:17 got 2001:db8:1111::27 (IAID=213915781, pref=86400,valid=172800).

39:53 Srv Notice Sending REPLY on Conexao de Rede sem Fio/20,transID=0x3e0f, opts: 3 2 1 7 23 24, 0 relay(s).

```

Portanto, as mensagens do DHCP para IPv4 Discover, Offer, Request e Acknowledgment (DORA) foram trocadas no DHCPv6 por Solicit, Advertise, Request e Reply. Além disso, o DHCPv6 está baseado em Multicast e não mais em broadcast como no DHCPv4.

Nos roteadores para que a interface IPv6 seja configurada como DHCPv6 cliente utilize o comando abaixo:

```
R4(config)#ipv6 unicast-routing
R4(config)#int f1/0
R4(config-if)#ipv6 address dhcp
R4(config-if)#no shut
```

O comando "**ipv6 address dhcp**" está disponível apenas em versões de IOS superiores a 12.24T.

Em ambientes centralizados, onde o servidor DHCPv6 está localizado em outra sub-rede e não na mesma rede local dos clientes, podemos utilizar o recurso do agente relay. Para configurar um roteador Cisco como agente DHCPv6 relay com o servidor DHCPv6 2001:DB8:1::10 localizado em um ambiente centralizado utilize o comando conforme abaixo:

```
R4(config)#int f1/0
R4(config-if)# ipv6 dhcp relay destination 2001:DB8:1::10
```

No exemplo acima, quando o roteador receber uma mensagem **Solicit** de um cliente ele repassará essa informação ao servidor DHCPv6 configurado no comando mostrado anteriormente, servindo de intermediário na alocação do IPv6, assim como para os agentes relay do IPv4.

O CCNA e CCENT não apresentam a configuração do servidor DHCPv6 por ser necessário alterar os flags M e O, além de configurações especiais para que os clientes não tenham múltiplos endereços. Vamos mostrar abaixo um script simples que você pode configurar em seus laboratórios reais ou com GNS3 (não funciona com packet tracer) para poder executar testes com clientes de rede. Nessa configuração o cliente deve pegar IPv6 apenas via DHCPv6, vamos bloquear o SLAAC na interface LAN desse roteador, por isso garanta que apenas um roteador esteja na rede para realizar os testes.

```
! DHCPv6 Statefull
! configurar pool com opções do DHCP a serem passadas pelo Roteador
ipv6 dhcp pool IPV6_DHCPPOOL
  address prefix 2001:470:E2CC:1::/64 lifetime 1800 600
  link-address 2001:470:E2CC:1::1/64
  dns-server 2001:470:20::2
  domain-name ipv6-1-dltec.com
!
! setar bit M, desabilitar o envio de prefixo via SLAAC e vincular pool DHCPv6
interface FastEthernet0/0
  ipv6 nd managed-config-flag
  ipv6 nd prefix default no-advertise
  ipv6 dhcp server IPV6_DHCPPOOL
```

A configuração inicia com a criação de um pool de endereços e opções do DHCPv6 e depois você vincula o pool na interface (para o DHCPv4 não precisa essa vínculo). No exemplo em questão estamos utilizando a rede 2001:470:E2CC:1::/64 no servidor DHCPv6, a interface fast 0/0 está sendo utilizada para fornecer o pool do DHCPv6 com endereço 2001:470:E2CC:1::/64, o endereço do DNS é 2001:470:20::2 e nome de domínio ipv6-1-dltec.com. Você pode alterar os parâmetros conforme seu laboratório.

Com os comandos “**show ipv6 dhcp binding**” você pode ver a alocação de endereços dinâmicos e com o comando “**debug ipv6 dhcp**” você pode verificar a troca de mensagens entre o servidor e clientes.

Se você for configurar um roteador Cisco como cliente no GNS3 insira o comando “**ipv6 nd prefix default no-advertise**” para que ele não anuncie seu prefixo nas mensagens de RA. Você pode também utilizar o comando “**ipv6 nd suppress-ra**” na mesma interface para que ela não envie suas mensagens de RA. Veja exemplo de configuração de roteador Cisco como cliente DHCPv6 abaixo:

```
R1-DHCPV6-Cliente#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-DHCPV6-Cliente(config)#int f0/0
R1-DHCPV6-Cliente(config-if)#ipv6 enable
R1-DHCPV6-Cliente(config-if)#ipv6 address dhcp
R1-DHCPV6-Cliente(config-if)#ipv6 nd prefix default no-advertise
R1-DHCPV6-Cliente(config-if)#ipv6 nd suppress-ra
R1-DHCPV6-Cliente(config-if)#end
```

Se você não utilizar os comandos acima o roteador que deveria agir como cliente vai passar seu prefixo via mensagens de RA e os clientes terão mais de um endereço configurado, ou seja, um via DHCPv6 e um ou mais via SLAAC, dependendo do sistema operacional.

Por padrão o Windows Vista, 7 e 8 vem configurados para pegar endereços IPv6 via SLAAC e DHCPv6, já no Linux e MAC OS-X somente via SLAAC, para pegar via DHCPv6 você precisa entrar nas configurações das placas de rede e alterar. Veja tela de configuração padrão do MAC OS-X onde em “Configure IPv6” está definido como “**Automatically**”, ou seja, SLAAC. Para que o computador utilize o DHCPv6 esta opção deve ser alterada.



## **12.3 Atribuindo Endereços com SLAAC e DHCPv6 Stateless**

Por padrão a autoconfiguração stateless ou SLAAC (StateLess Address Auto Configuration) prevista no início do desenvolvimento do IPv6 não suporta o envio de endereços de servidores DNS, sendo possível apenas receber um prefixo, seu comprimento e utilizar o endereço do roteador que enviou o anúncio como rota padrão. Portanto, com o SLAAC puro os computadores não conseguiram traduzir nomes em endereços IPv6 e não poderiam acessar conteúdo da Intranet ou Internet a não ser que soubessem o endereço dos servidores, porém seria “meio complicado”.

Uma opção para resolver esse problema é utilizar um servidor DHCPv6 sem estado ou stateless para que os clientes possam obter os demais parâmetros faltantes, tais como servidores DNS, nomes de domínio, etc.

Há uma diferença nas mensagens trocadas entre os clientes e servidor DHCPv6 stateless em relação ao statefull, pois são trocadas apenas duas mensagens: o servidor recebe um INF-REQUEST e responde com um REPLY, pois ele apenas tem que repassar os dados configurados e não mais alocar endereços IPv6.

Veja abaixo a saída do ipconfig /all parcial de um cliente Windows 7 autoconfigurado com SLAAC e DHCPv6 stateless.

Adaptador de Rede sem Fio Conexão de Rede sem Fio:

```

DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv6 . . . . . : 2001:db8:1111:0:a084:ed7e:50d8:
2b36(Preferencial)
Endereço IPv6 Temporário. . . . . : 2001:db8:1111:0:fc1b:d903:8e31:
7fbc(Preferencial)
Endereço IPv6 de link local . . . . . : fe80::a084:ed7e:50d8:2b36%12(Pr
eferencial)
Endereço IPv4. . . . . : 192.168.1.38(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : sexta-feira, 7 de junho de 2013
09:25:20
Concessão Expira. . . . . : sábado, 8 de junho de 2013 09:2
5:26
Gateway Padrão. . . . . : fe80::1%12
192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID de DHCPv6. . . . . : 230692997
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-16-FB-E6-B5-24-B6-F
D-06-BE-40
Servidores DNS. . . . . : 2001:db8:1000::1
192.168.10.1
NetBIOS em Tcpip. . . . . : Habilitado
Lista de pesquisa de sufixos DNS específicos da conexão:
cisco.com

```

A vantagem desse método é sua simplicidade, porém como não há guarda do estado não conseguimos saber quantos clientes temos nem quais endereços ou faixa de endereços esses clientes pegaram, pois eles utilizarão o EUI-64 ou as extensões de privacidade que são utilizadas por padrão para gerar os endereços nos hosts dependendo dos sistemas operacionais utilizados na rede.

Assim como mostramos para o DHCP Statefull, abaixo segue um script de configuração para o SLAAC com DHCPv6 stateless, veja abaixo:

```

ipv6 dhcp pool IPV6_DHCPOOL
dns-server 2001:DB8:1000::1
domain-name cisco.com
!
interface Ethernet0/0
    ipv6 address 2001:DB8:1000::1/64
    ipv6 enable
    ipv6 nd other-config-flag
    ipv6 dhcp server IPV6_DHCPOOL

```

Configurações nos clientes:

```

ipv6 unicast-routing
int f1/0
ipv6 enable
ipv6 address autoconfig default

```

O mesmo comando debug citado anteriormente pode ser utilizado para verificar a troca de mensagens do DHCPv6, porém a configuração stateless não armazenará os IPs dos clientes.

## 13 Configurando o Roteamento em Redes IPv6

Na parte de roteamento IPv6, basicamente os protocolos de roteamento IGP continuam com a mesma estrutura, ou seja, o RIP, EIGRP e OSPF utilizados no IPv4 foram adaptados para transportar e rotear prefixos de rede IPv6. O nome dos protocolos mudou um pouco:

- RIP passa a se chamar RIPng e tem a mesma base do RIP versão 2.
- EIGRP passa a ser chamado de EIGRPv6.
- OSPFv2 ou OSPF agora passa a ser OSPFv3 para o IPv6.

O IS-IS e BGP não mudaram, porém para eles serem capazes de rotear IPv6 são necessárias extensões ao protocolo.

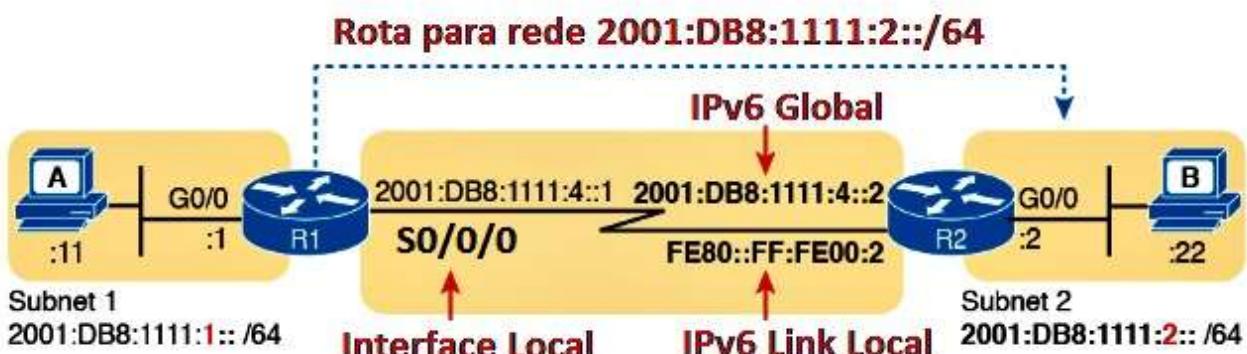
Agora vamos estudar as configurações de roteamento estático para IPv6, o qual é o foco do CCENT.

### 13.1 Roteamento Estático e Rota Padrão

As rotas estáticas e/ou padrões para o IPv6 são configuradas com o comando “**ipv6 route**”. A sintaxe do comando segue abaixo e tem algumas opções a mais:

```
Router(config)# ipv6 route ipv6-prefix/prefix-length {ipv6-address | interface-type interface-number [ipv6-address]} [administrative-distance] [administrative-multicast-distance unicast multicast] [tag tag]
```

Assim como para o IPv4 podemos configurar uma rota estática no IPv6 apontando para o IP de próximo salto (diretamente conectado) ou para a interface local de saída. Veja a representação na imagem abaixo.



Por exemplo, para criar uma rota no roteador R1 para a rede remota 2001:DB8:1111:2::/64 você pode utilizar como referência a interface serial local S0/0/0 ou um dos IPs versões 6 remotos, tanto o de link local, que inicia como FE80, como o Unique Global 2001:DB8:1111:4::2.

O comando poderia ser quaisquer uma das alternativas abaixo:

- Ipv6 route 2001:DB8:1111:2::/64 S0/0/0
- Ipv6 route 2001:DB8:1111:2::/64 S0/0/0 FE80::FF:FE00:2
- Ipv6 route 2001:DB8:1111:2::/64 2001:DB8:1111:4::2

Note que quando utilizamos o endereço de link local precisamos especificar antes qual a interface de saída dele, pois ele não é como o endereço global que deve ser único na rede IPv6 toda, ele precisa ser único apenas na sua rede local, por isso é preciso informar a interface de saída também.

Veja um exemplo abaixo onde será criada a rota para a rede 2000::/64 através da serial 0/0/0:

```
dltec(config)#ipv6 route 2000::/64 serial 0/0/0
```

Quando utilizamos como destino um IPv6 de próximo salto um link-local precisaremos também definir a interface de saída dessa rota, pois a rede FE80::/10 pertence à todas as interfaces.

```
R1(config)#ipv6 route 2000::/64 fe80::1  
% Interface has to be specified for a link-local nexthop  
R1(config)#ipv6 route 2000::/64 fast 0/0 fe80::1  
R1(config) #
```

Note acima que ao tentar criar uma rota apontando para o endereço FE80::1 recebemos uma mensagem que para o link local precisamos definir a interface de saída.

Veja que a mesma configuração apontando para o IP global pode ou não ter a interface de saída definida, os dois métodos são aceitos:

```
R1(config)#ipv6 route 2000::/64 fast 0/0 2000::1  
R1(config)#ipv6 route 2000::/64 2000::1
```

Com o comando "show ipv6 route" podemos visualizar a tabela de roteamento IPv6.

```
dltec#sho ipv6 route  
IPv6 Routing Table - default - 4 entries  
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route  
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP  
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary  
D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery  
S 2000::/64 [1/0], tag 2  
    via FastEthernet0/0, directly connected  
S 2001:DB8:1::/64 [1/0]  
    via 2001:DB8:1::1, FastEthernet0/0  
S 2001:DB8:42:1::/64 [1/0]  
    via Null0, directly connected  
L FF00::/8 [0/0]  
    via Null0, receive  
dltec#
```

Note que a rota para 2001:DB8:1::/64 através da fast 0/1 não estará presente, pois ela tem distância administrativa maior.

As regras de distância administrativa no IPv6 são iguais as que estudamos para o IPv4, ou seja, rotas estáticas que apontam para uma interface de saída tem AD zero (como se fosse diretamente conectada) e rotas que apontam para o próximo salto tem AD 1 por padrão.

### 13.2 Criando Rotas Padrões

Para criar uma rota padrão para o roteador IPv6 é só criar uma rota estática conforme criamos anteriormente apontando para a rede **::/0**. Veja exemplo abaixo.

```
R1(config)#ipv6 route ::/0 fast 0/0 2000::1
```

A configuração acima é bem interessante e vale também para uma rota estática normal, não somente para a padrão, pois em uma interface LAN temos diversos endereços e ao definirmos além da interface fast também o IPv6 remoto resolvemos o problema de alcance e vinculamos a interface da rota.

Veja saída do show ip route com os comandos aplicados anteriormente e note que o roteador padrão no IPv6 não aparece com a mensagem de "Gateway of last resort" como tínhamos na tabela do IPv4.

```
R1#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S  ::/0 [1/0]
    via 2000::1, FastEthernet0/0
S  2000::/64 [1/0]
    via ::, Serial0/0
    via FE80::1, FastEthernet0/0
C  2340:1111:AAAA:1::/64 [0/0]
    via ::, FastEthernet0/0
L  2340:1111:AAAA:1::1/128 [0/0]
    via ::, FastEthernet0/0
C  2340:1111:AAAA:2::/64 [0/0]
    via ::, Serial0/0
L  2340:1111:AAAA:2::1/128 [0/0]
    via ::, Serial0/0
S  2340:1111:AAAA:3::/64 [1/0]
    via ::, Serial0/0
L  FF00::/8 [0/0]
    via ::, Null0
R1#
```

Você pode também criar rotas padrões com os exemplos dados no tópico anterior, apontando diretamente para uma interface serial, para um IPv6 global de próximo salto ou para um endereço de Link Local e sua interface de saída. Veja exemplos abaixo:

- Ipv6 route ::/0 S0/0/0
- Ipv6 route ::/0 S0/0/0 FE80::FF:FE00:2
- Ipv6 route ::/0 2001:DB8:1111:4::2

### 13.3 Rota Padrão via SLAAC e Autoconfiguração

Outra forma que um roteador pode adquirir uma rota padrão é automaticamente através do SLAAC, ou seja, na autoconfiguração. Lembre-se que via NDP na autoconfiguração o roteador aprenderá os seguintes itens:

- **Endereço da interface:** utilizando o processo do SLAAC autoconfigura sua interface conforme prefixo passado na mensagem de RA.
- **Rota Local /128:** o roteador adiciona uma rota local (/128) para o endereço autoconfigurado, assim como é feito com quaisquer endereços locais das interfaces.
- **Prefixo da Rota Conectada:** adiciona o prefixo da rota diretamente conectada (/64) aprendida pela mensagem de RA via NDP.
- **Default route:** R1 adiciona a rota padrão com prefixo ::/0 apontando para o próximo salto que é o roteador que enviou a mensagem de resposta do processo de SLAAC.

Veja exemplo a seguir, onde os roteadores R1 e R2 estão diretamente conectados via Interface Giga 1/0. R1 será o roteador local e R2 será configurado com autoconfiguração.

Vamos começar por R1, o qual será o roteador que passará o prefixo da rede na LAN via SLAAC.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#int g1/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2000::1/64
R1(config-if)#no shut
R1(config-if)#end
R1#
```

Agora segue a configuração de R2, onde ele terá sua interface configurada via autoconfig e também com a opção para pegar a rota padrão (default).

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#int g1/0
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address ?
WORD          General prefix name
X:X:X:X::X    IPv6 link-local address
X:X:X:X::X<0-128> IPv6 prefix
autoconfig     Obtain address using autoconfiguration
dhcp          Obtain a ipv6 address using dhcp

R2(config-if)#ipv6 address autoconfig ?
default      Insert default route
<cr>

R2(config-if)#ipv6 address autoconfig default
R2(config-if)#end
R2#
```

Veja a saída da tabela de roteamento de R2 com as informações pegas via autoconfiguração passadas pela NDP através de R1.

```
R2#sho ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, NM - NEMO, ND - Neighbor Discovery
       l - LISPs
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S  ::/0 [2/0]
  via FE80::C800:5FF:FE54:1C, GigabitEthernet1/0
C  2000::/64 [0/0]
  via GigabitEthernet1/0, directly connected
L  2000::C801:20FF:FEA8:1C/128 [0/0]
  via GigabitEthernet1/0, receive
L  FF00::/8 [0/0]
  via Null0, receive
```

Note que a rota padrão tem distância administrativa 2, pois esse é o valor da rota aprendida via NDP. Essa é uma das poucas diferenças do IPv6, as demais distâncias administrativas são as mesmas estudadas para o IPv4.

Logo após vem a informação do prefixo 2000::/64 aprendido via NDP e na sequência o endereço IPv6 autoconfigurado na Interface via EUI-64 (2000::C801:20FF:FEA8:1C/128), inserido como uma rota local (L).

Em versões de Cisco IOS mais atuais você pode encontrar as duas primeiras informações anteriores com um índice diferente, pois a rota padrão pode ser marcada como "ND" ao invés de estática, assim como o prefixo local pode ser aprendido como "NDp" ao invés de diretamente conectado (C). Veja exemplo abaixo.

```
R2#sho ipv6 route
### Saídas Omitidas ####
ND  ::/0 [2/0]
    via FE80::C800:5FF:FE54:1C, GigabitEthernet1/0
NDp  2000::/64 [2/0]
    via GigabitEthernet1/0, directly connected
L   2000::C801:20FF:FEA8:1C/128 [0/0]
    via GigabitEthernet1/0, receive
L   FF00::/8 [0/0]
    via Null0, receive
```

Note que nesse caso a distância administrativa do prefixo local também é passado de zero para 2, o qual é a AD do NDP.

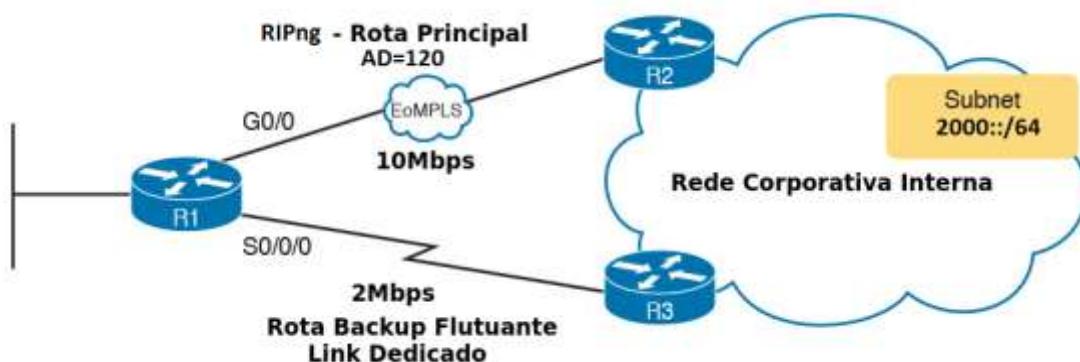
### 13.4 Rotas Estáticas Flutuantes no IPv6

O mesmo princípio que utilizamos para criar rotas backup flutuantes para o IPv4 funciona aqui no IPv6.

Portanto se quisermos ter uma rota reserva em standby para outros protocolos de roteamento ou até mesmo para uma rota estática principal basta alterar a distância administrativa da rota estática reserva para que ela seja maior que a principal.

Por exemplo, se a rota reserva for para o protocolo RIPng (versão do IPv6 do RIPv2) basta colocarmos a AD como 130, pois a AD do RIPng é 120, assim como do RIPv2. O mesmo serve para o EIGRPv6 que tem AD 90, portanto uma rota estática com AD 91 já serviria como reserva, ou então para o OSPFv3 que tem AD 110, nesse caso uma rota com AD 111 já serviria como reserva.

Veja exemplo abaixo com a mesma topologia que utilizamos para o IPv4, mas agora aplicada ao IPv6. A seguir apresentaremos a configuração da rota flutuante de R1.



```
R1(config)#ipv6 route 2000::/64 S0/0/0 130
```

Com os comandos `show ipv6 route` e `show ipv6 route 2000::/64` você pode verificar a tabela de roteamento completa e a informação específica da rota para `2000::/64`. Se você derrubar a interface principal G0/0 vai ter as saídas abaixo.

```
R1# show ipv6 route static
### Saídas Omitidas ####
S 2000::/64 [130/0]
  via 2000::2

R1# show ipv6 route 2000::/64
Routing entry for 2000::/64
  Known via "static", distance 130, metric 0
  Route count is 1/1, share count 0
  Routing paths:
    2000::2
      Last updated 00:01:35 ago
```

### 13.5 Rota de Host no IPv6

Assim como estudamos para o IPv4, o IPv6 também permite a criação de rotas estáticas para hosts específicos, basta utilizar a máscara /128, pois é a quantidade de bits que um host utiliza.

Se você lembrar para o IPv4 utilizávamos a máscara /32, que é o tamanho completo da máscara do IPv4.

As regras de criação desse tipo de rota podem ser quaisquer uma das estudadas anteriormente, por exemplo, veja abaixo uma rota para o host `2001::100/64` criada utilizando o endereço global local `2000::10`.

```
R1(config)#ipv6 route 2001::100/64 2001::10/64
```

Veja outro exemplo apontando para o endereço de link local.

```
R1(config)#ipv6 route 2001::100/64 giga0/0 FE80::10
```

## 14 Resumo do Capítulo

Bem pessoal, chegamos ao final de mais um capítulo!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Entender e saber explicar as diferenças entre o IPv6 e IPv4
- Principais características do IPv6
- Entender e saber interpretar um endereço IPv6
- Entender o protocolo ICMPv6 e seus recursos adicionais de Multicast e o protocolos NDP
- Entender como os vizinhos IPv6 descobrem o endereço MAC e prefixos de Rede
- Entender e listar os métodos de alocação de endereços no IPv6
- Entender as principais diferenças entre o DHCP e o DHCPv6
- Saber configurar interfaces de LAN e WAN com endereços IPv6.
- Saber ativar a autoconfiguração nos roteadores Cisco.
- Saber ativar o DHCPv6 cliente e relay em interfaces dos roteadores.
- Entender as diferenças das configurações como cliente através de autoconfiguração e DHCPv6.
- Entender o processo de roteamento IPv6.
- Configurar roteamento estático no IPv6.

*Para finalizar o curso, reservamos esse capítulo para estudar mais a fundo detalhes sobre a inicialização dos roteadores e switches Cisco, como fazer Upgrades de versão do Cisco IOS, como fazer a quebra de senha e recuperação do Cisco IOS em caso de problemas que levem ao roteador não inicializar corretamente.*

*Para quem pretende entrar de cabeça no mundo Cisco e seguir uma carreira esse é um capítulo fundamental, pois na prática saber esses conceitos pode fazer a diferença.*

*Aproveite o material e bons estudos.*

## **Capítulo 14 – Upgrades, Licenciamento e Manipulação de Arquivos**

### **Objetivos do Capítulo**

Ao final desse capítulo você terá estudado e deverá compreender:

- Tipos de Memórias em Roteadores e Switches Cisco
- Verificar o Hardware e Memórias dos Roteadores com o Show Version
- Processo de Inicialização dos Roteadores Cisco
- Salvar e Manipular Arquivos de Configurações
- Copiar e Manipular Arquivos de IOS
- Recuperação de IOS – Disaster Recovery
- Recuperação de Senha
- Voltar Roteadores e Switches à Configuração de Fábrica
- Gerenciamento de Redes
- Ativar e configurar o Syslog
- Gerenciar o Licenciamento do Cisco IOS
- Entender as diferenças dos Packs antigos e novos do Cisco IOS
- Ativar Licenças Manualmente
- Ativar Licenças Temporárias
- Entender o funcionamento do Cisco License Manager

## Sumário do Capítulo

<b>1</b>	<i>Introdução</i>	<b>544</b>
<b>2</b>	<i>Gerenciando Arquivos no Cisco IOS</i>	<b>544</b>
2.1	Tipos de Memórias em Roteadores e Switches Cisco	545
2.1.1	Memória RAM/DRAM	545
2.1.2	Memória NVRAM	546
2.1.3	Memória Flash	546
2.1.4	Memória ROM	547
2.1.5	Opção de memória USB Externa (USB Flash Drives)	547
2.2	Introdução ao Sistema Operacional Cisco IOS	549
2.3	Verificando o Hardware e Memórias dos Roteadores com o Show Version	549
2.4	Outros Comandos para Verificar Informações básicas de Roteadores e Switches	552
2.5	Processo de Inicialização dos Roteadores Cisco	555
2.5.1	Problemas no POST	556
2.5.2	Detalhes da Carga do Bootstrap e Cisco IOS	556
2.5.3	Roteador em ROM Monitor – Qual o problema?	557
2.5.4	Problemas com o arquivo de configuração inicial (Startup Config)	558
2.6	Salvando e Manipulando Arquivos de Configurações	559
2.7	Copiando e Manipulando Arquivos de IOS	560
2.8	Utilizando FTP e SCP para Copiar Arquivos	563
2.8.1	Serviço de SCP	564
2.9	Recuperação de IOS – Disaster Recovery	565
2.10	Recuperação de Senha	566
2.11	Voltando Roteadores e Switches à Configuração de Fábrica	567
3	<i>Gerenciamento de Redes</i>	<b>570</b>
3.1	Ativando o Syslog	571
3.1.1	Verificando as mensagens de log	573

<b>4</b>	<b><i>Gerenciando o Licenciamento do Cisco</i></b>	
<b>IOS Versão 15</b>		<b>574</b>
<b>4.1</b>	<b>Cisco IOS por Modelo, Série e</b>	
	<b>Versão/Release de Software</b>	<b>574</b>
<b>4.2</b>	<b>Novo modelo de Cisco IOS Packing –</b>	
	<b>Imagen Universal</b>	<b>576</b>
<b>4.3</b>	<b>Introdução a Ativação de Software com</b>	
	<b>Imagen Universal</b>	<b>577</b>
<b>4.3.1</b>	Ativando Licenças Manualmente	<b>578</b>
<b>4.3.2</b>	Ativando Licenças Temporárias	<b>580</b>
<b>4.3.3</b>	Cisco License Manager	<b>580</b>
<b>5</b>	<b><i>Resumo do Capítulo</i></b>	<b>581</b>
<b>6</b>	<b><i>Conclusão</i></b>	<b>581</b>

## 1 Introdução

Nesse capítulo vamos estudar como gerenciar um dispositivo Cisco, ou seja, utilizar comandos e recursos dos próprios roteadores e switches Cisco para tratar os principais arquivos e recursos dos equipamentos que podem afetar a operação normal deles.

Basicamente vamos aprender como tirar informações gerais, movimentar arquivos, realizar backup das configurações e sistema operacional Cisco IOS, etc.

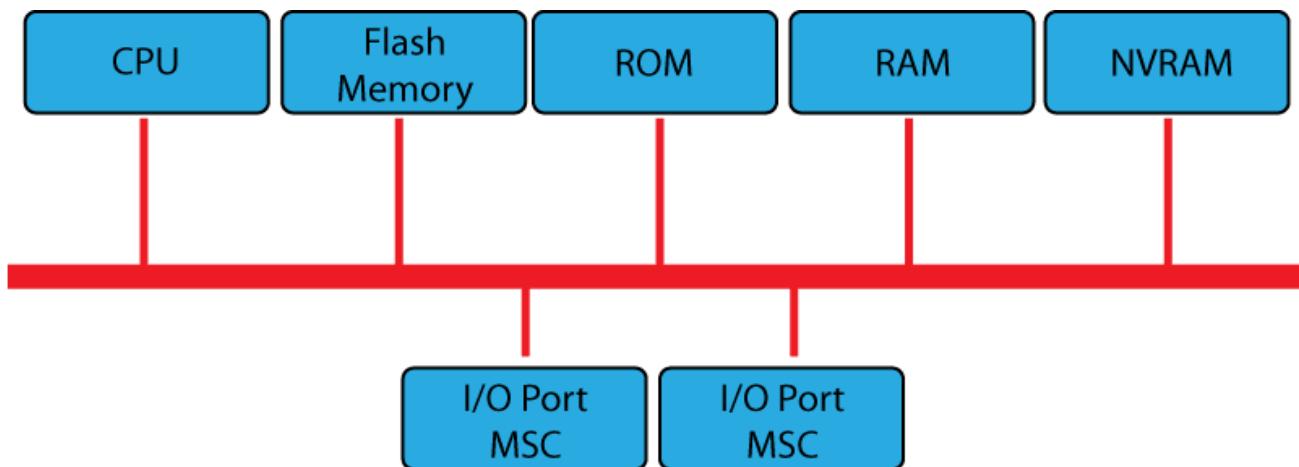
Vamos também aprender as funções e configurações do recurso de Syslog.

Por último você aprenderá conceitos sobre o IOS versão 15 e seu licenciamento.

## 2 Gerenciando Arquivos no Cisco IOS

Lembre-se que de maneira genérica o hardware um roteador pode ser dividido da seguinte maneira:

- **Chassis:** foco do CCNA R&S (ICND-1 e ICND-2) são as linhas de roteadores **ISR-G2** 800/1900/2900/3900 e switches de acesso como a linha **Catalyst** 2960, 3560 e 3750, os quais utilizam o Cisco IOS como sistema operacional.
- **Fonte de alimentação:** a maioria dos equipamentos suportam tensão **AC** (110V a 240V) ou **DC** (-48V), além disso, alguns modelos suportam fontes redundantes.
- **Placa mãe** com o **barramento** (BUS) interligando os demais componentes internos.
- **CPU** (processador).
- **Memórias:** RAM/DRAM, Flash, USB Flash, NVRAM e ROM.
- **Interfaces de LAN e WAN:** Serials, Ethernet, FastEthernet, GigabitEthernet, interfaces T1 (1,544Mbps) e/ou E1 (2,048Mbps) para voz e dados, ISDN BRI, ISDN PRI (T1-1,544Mbps ou E1-2,048Mbps), Dial-up (WIC-1 ou 2AM – Analog Module ou módulo analógico), POS, ATM, etc.
- **Linhas de configuração ou Lines** (lines console, auxiliar e VTY).

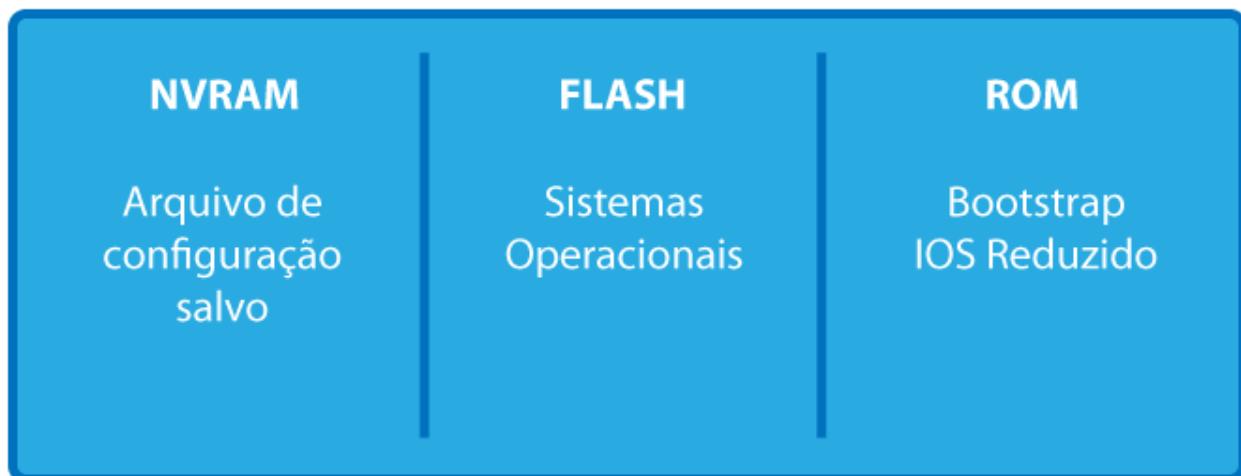


Normalmente os roteadores possuem em seu chassis uma ou duas interfaces de LAN, atualmente **Gigabitethernet**, e dependendo do modelo alguns **slots** para inserção de módulos extras, tanto de LAN como WAN ou outros módulos como placas de Voz, interfaces WLAN e módulos de serviço.

Nesse tópico vamos estudar os principais arquivos que são utilizados pelo Cisco IOS e seus comandos relacionados, assim como fazer a recuperação de senha e reset em roteadores e switches.

## 2.1 Tipos de Memórias em Roteadores e Switches Cisco

A seguir vamos relembrar os tipos de memória dos roteadores e switches, suas respectivas funções e arquivos que são armazenados nelas.



### 2.1.1 Memória RAM/DRAM

Armazenam tabelas de roteamento, cachê ARP, cachê de comutação rápida, buffers de pacotes e filas de espera de pacotes.

A memória RAM fornece também armazenamento temporário e/ou de execução para o **arquivo de configuração do roteador (running-config)** enquanto o roteador estiver ligado. O conteúdo da RAM é perdido quando você desliga ou reinicia o roteador, pois a **RAM é uma memória volátil**. Veja um exemplo de pente de memória RAM na figura a seguir.

Memória RAM para o roteador Cisco 2821 de 256MB



Para verificar arquivo de configuração em uso na memória RAM utilizamos o "**show running-config**" em modo privilegiado, mesmo comando utilizado para verificar as configurações dos switches.

### 2.1.2 Memória NVRAM

A **NVRAM** ou **Non-volatile RAM** é uma **RAM não volátil** com função de armazenamento do arquivo de configuração de backup (**startup-config**) para inicialização de um roteador. O conteúdo será mantido quando você desligar ou reiniciar o roteador.

Além disso, a NVRAM armazena o registro de configuração ou “**configuration register**”, valor de 16 bits que define como os roteadores devem buscar seu sistema operacional e arquivo de configuração inicial.

Esse registro é utilizado na inicialização dos roteadores e vamos aprender a interpretá-lo de maneira geral para influenciar como o roteador carrega seu sistema operacional e arquivo de configuração.

Para verificar o conteúdo armazenado na NVRAM utilize o comando “**show startup-config**” em modo privilegiado tanto nos roteadores como nos switches.

Lembre-se que ao ligar um roteador ou switch e entrar com comandos de configuração eles são armazenados na memória RAM, para que esses comandos não sejam perdidos ao desligar ou reiniciar o equipamento é necessário salvar esse conteúdo na memória NVRAM com o comando “**copy running-config startup-config**”. Lembre-se que a sintaxe do comando copy é bem simples:

- Copy ou copie → do arquivo de origem → para o arquivo de destino

Por isso o comando “**copy running-config startup-config**” copia o que está na memória RAM (origem: running-config) para a memória NVRAM (destino: startup-config).

A diferença em relação à memória entre roteadores e switches é que a **NVRAM em um switch é emulada dentro da memória flash**, já **no roteador as duas memórias são componentes distintos**. Além disso, normalmente os roteadores possuem mais capacidade instalada que os switches quando tratamos das linhas básicas de equipamentos.

### 2.1.3 Memória Flash

É uma **ROM reprogramável não volátil que pode ser apagada**, de maneira generalizada podemos dizer que é o **HD** de muitos roteadores e switches. A escolha desse tipo de memória é por uma questão de confiabilidade, como ela não possui partes móveis, como um HD normal, há menos chance de danos.

Ela contém a imagem do Cisco IOS e em alguns casos um microcódigo do sistema operacional, permite atualizar o Cisco IOS sem remover e substituir os chips na placa mãe. Seu conteúdo será mantido quando você desligar ou reiniciar o roteador, pois ela é uma memória não volátil.

Várias versões do Cisco IOS podem ser armazenadas na memória Flash dependendo de sua capacidade. Outros tipos de arquivos podem também ser armazenados na memória flash de acordo com a necessidade da solução.



Para verificar o conteúdo da memória flash utilize o comando "**show flash:**" em modo privilegiado.

As memórias flash e NVRAM permitem serem apagadas por completo com o comando "**erase**", por exemplo, "**erase starup-config**" apaga o arquivo de configuração inicial e ao reiniciar o roteador ele volta sem configuração. Já o **erase flash:** é mais radical, pois apaga o sistema operacional, fazendo com que o roteador ou switch não iniciem no próximo reload ou quando forem desligados e ligados.

Para apagar um arquivo específico da memória flash podemos utilizar o comando "delete", veja exemplo abaixo. Nesse exemplo vamos apagar o arquivo nomeado de "**config\_bkp\_23072013**" que está na memória flash com o comando delete e depois vamos verificar se realmente ele foi apagado.

```
DlteC-FW-GW#show flash: | include config
183      15021 Jul 23 2013 22:13:02 config_bkp_23072013
185      14648 Mar 28 2013 19:52:18 config_bkp_28032013
190      15553 Jul 25 2013 18:51:20 config_com_sip_25072013
DlteC-FW-GW#delete flash:config_bkp_23072013
Delete filename [config_bkp_23072013]?
Delete flash:/config_bkp_23072013? [confirm]
DlteC-FW-GW#show flash: | include config
185      14648 Mar 28 2013 19:52:18 config_bkp_28032013
190      15553 Jul 25 2013 18:51:20 config_com_sip_25072013
DlteC-FW-GW#
```

Além dos comandos acima podemos formatar a memória flash, comando que apaga também todo conteúdo da memória, incluindo o Cisco IOS e todos os demais arquivos assim como fizemos com o comando "erase".

```
DlteC-FW-GW#format ?
flash:  Filesystem to be formatted
```

Se você apagar ou formatar a memória flash e reiniciar o dispositivo ele não inicializará! O roteador entrará em um modo chamado Rommonitor e o switch mostrará também informações de que teve problemas de inicialização, ficando com o led SYS piscando regularmente.

#### 2.1.4 Memória ROM

É uma memória **apenas de leitura** (Read-only Memory) que contém o bootstrap, diagnósticos de power-on, parte do sistema operacional (IOS reduzido) em versões mais antigas de roteadores e o ROM Monitor nos equipamentos mais novos.

Sua atualização, se necessário, é feita através de substituição de chip, pois ela não é gravável.

#### 2.1.5 Opção de memória USB Externa (USB Flash Drives)

As linhas de roteadores ISR-G1 e ISR-G2 disponibilizam também a opção de conectar um pen-drive USB (memória externa) como opção de armazenamento, possibilitando a transferência de arquivos de maneira mais simples em casos de emergências ou até mesmo necessidades de trocas de versão de Cisco IOS nos roteadores.

A memória USB recebe normalmente o nome de **USBFlash0:** ou **USBflash1:**, dependendo do modelo do roteador. Ela precisa ser formatada em FAT32 preferencialmente para ser reconhecida pelos roteadores e switches. Em modelos antigos pode haver problemas com memórias maiores que 256M de capacidade.

Você pode utilizar o comando “**show file systems**” para verificar o nome que o Cisco IOS deu ao seu pen-drive e com um **dir** verificar o conteúdo interno da memória. Veja exemplo abaixo e note que nesse comando podemos verificar também a quantidade de memória total (campo Size) das memórias Flash e NVRAM e quanto temos livre (campo Free) em cada uma delas.

```
DlteC-FW-GW#show file systems
File Systems:
```

Size(b)	Free(b)	Type	Flags	Prefixes
-	-	opaque	rw	archive:
-	-	opaque	rw	system:
-	-	opaque	rw	tmpsys:
-	-	opaque	rw	null:
-	-	network	rw	tftp:
196600	168984	nvram	rw	nvram:
* 125804544	31911936	disk	rw	flash:#
-	-	opaque	wo	syslog:
-	-	opaque	rw	xmodem:
-	-	opaque	rw	ymodem:
-	-	network	rw	rcp:
-	-	network	rw	pram:
-	-	network	rw	http:
-	-	network	rw	ftp:
-	-	network	rw	scp:
-	-	opaque	ro	tar:
-	-	network	rw	https:
-	-	opaque	ro	cns:
3999203328	3808968704	usbflash	rw	usbflash0:

```
DlteC-FW-GW#dir usbflash0:
```

```
Directory of usbflash0:/
```

```
1 drw- 0 Apr 4 2013 17:25:54 -03:00 Megadeth - 2011
23 -rw- 50825880 Sep 23 2013 15:11:44 -03:00 c2801-adventureprisek9-
mz.124-24.T8.bin

3999203328 bytes total (3808968704 bytes free)
```

Note que no pen-drive nomeado de usbflash0: temos uma pasta chamada “**Megadeth - 2011**” e um arquivo do Cisco IOS nomeado **c2801-adventureprisek9-mz.124-24.T8.bin**.

O comando **dir** pode ser utilizado para verificar os arquivos da memória flash também (similar ao show flash), veja exemplo abaixo onde a flash contém uma grande quantidade de arquivos, pois foi tirada de um roteador que atua como roteador, gateway de voz, firewall e IPS.

```
DlteC-FW-GW#dir flash:
Directory of flash:/
```

```
1 -rw- 50825880 Mar 26 2013 14:40:42 -03:00 c2801-adventureprisek9-
mz.124-24.T8.bin
2 -rw- 2593969 Mar 26 2013 14:44:56 -03:00 APPS-1.2.1.SBN
3 -rw- 2925555 Mar 26 2013 14:45:10 -03:00 apps11.8-4-1-23.sbn
### Informações omitidas propositalmente ###

188 -rw- 4093 Aug 2 2013 16:50:28 -03:00 softkeyDefault_kpml.xml
189 -rw- 4127 Aug 2 2013 16:50:30 -03:00 softkeyDefault.xml
190 -rw- 15553 Jul 25 2013 15:51:20 -03:00 config_com_sip_25072013

125804544 bytes total (31911936 bytes free)
```

## 2.2 Introdução ao Sistema Operacional Cisco IOS

O software **Cisco IOS (Internetwork Operating System)** é um sistema operacional que fornece funcionalidade, escalabilidade e segurança comuns para os produtos da arquitetura Cisco.

Conforme já citado no tópico anterior ele pode ficar armazenado na memória Flash dos roteadores e switches, porém pode também ser armazenados em servidores TFTP (Trivial File Transfer Protocol – UDP porta 69).

O Cisco IOS não precisa ser “**instalado**” como em computadores, pois ele é uma imagem que é carregada e executada diretamente na memória RAM/DRAM dos dispositivos, portanto se for necessário trocar o sistema operacional de um roteador ou switch de acesso basta apagar o antigo (opcional), copiar o novo para a memória flash e reinicializar (reload) o equipamento.

Em versões antigas de roteadores o Cisco IOS pode ser inicializado diretamente na memória flash também. Atualmente os roteadores estão utilizando o IOS versão 15. A versão anterior se chamava 12.4.

O arquivo de IOS tem uma extensão “**.bin**” para os roteadores Cisco e pode também ser disponibilizado compactado em uma extensão “**.tar**”, porém esse tipo de arquivo vai precisar ser descompactado antes da sua utilização para que o IOS “.bin” seja encontrado e inicializado.

Por exemplo, a seguir temos o nome arquivo do Cisco IOS “**c3640-i-mz.122-7b.bin**” de um roteador modelo Cisco 3640 (**c3640**) versão 12.2 (**122**) release **7b**. Vamos estudar que para as versões mais novas do Cisco IOS temos apenas uma versão de imagem Universal, por exemplo, “**c1900-universalk9-mz.SPA.152-1.T1.bin**” é o nome de um IOS para o roteador modelo **Cisco 1941**, da família **ISR-G2**.

Antes de iniciar a operação normal em redes com dispositivos Cisco é importante fazer um backup do Cisco IOS utilizando um serviço de TFTP para casos de emergências e necessidade de troca de equipamentos, pois muitas vezes os problemas não permitem que você recupere o IOS do roteador ou switch anterior diretamente de sua memória flash. O mesmo é recomendado para a configuração inicial que fica gravada na NVRAM (startup-config).

## 2.3 Verificando o Hardware e Memórias dos Roteadores com o Show Version

Vamos agora revisar o comando **show version** executado em um roteador com Cisco IOS versão 12.x e versão 15x. A saída do comando muda um pouco para os switches, mas o foco na prova é mais voltado para os roteadores.

O “**show version**” permite verificar algumas informações importantes sobre os equipamentos, tais como:

1. Versão do IOS.
2. O uptime (há quanto tempo ocorreu o último reload – reinicialização – ou o tempo que o roteador está ligado desde a última reinicialização).
3. A razão da última reinicialização do sistema operacional IOS (comando reload, botão de power off/on ou energia desligada/ligada novamente, problemas de software, ect.).
4. O tempo que o IOS foi carregado pela última vez (se o relógio foi configurado manualmente ou via NTP).
5. A origem que o roteador utilizou para carregar o IOS que está atualmente rodando, por exemplo, através da memória flash ou servidor TFTP e qual IOS está em uso, pois podemos ter mais de um na mesma memória flash.
6. Quantidade de memória RAM.
7. Quantidade e tipo de interfaces instaladas.
8. Quantidade total de memória NVRAM disponível.

9. Quantidade total de memória flash disponível.
10. O registro de configuração (configuration register) atual e seu estado futuro se houve alguma configuração que influenciará o próximo reload.

A quantidade de memória RAM e Flash que o roteador possui são muito importantes para definição do software IOS que pode ser instalado no dispositivo em caso de um Upgrade (instalação de uma versão mais nova de IOS), pois existem várias versões de IOS, cada uma com **necessidades específicas de memória RAM/DRAM e Flash**. Portanto, dependendo da quantidade de memória disponível, o roteador pode ser limitado a uma versão de sistema operacional mais simples.

Veja a seguir um exemplo do comando com os campos comentados para um roteador modelo Cisco 2600 utilizando Cisco IOS versão 12.x.

```

Router>SHOW VER
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.0(5)T1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc. ( IOS IMAGE and RELEASE LEVEL )
Compiled Tue 17-Aug-99 13:57 by cmong
Image text-base: 0x80008088, data-base: 0x8072C5D4

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
      ( BOOT ROM LEVEL )
Router uptime is 3 minutes
System returned to ROM by power-on
System image file is "flash:c2600-i-mz.120-5.T1.bin" → - Uptime
                                                               - Motivo do reload
                                                               - IOS que está sendo executado

cisco 2610 (MPC860) processor (revision 0x202) with 26624K/6144K bytes of memory
      ( TOTAL DRAM: 26624K + 6144K = 32MB )
Processor board ID JAD041108S0 (35972843)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s) → Interfaces instaladas
32K bytes of non-volatile configuration memory. → Quantidade de NVRAM
8192K bytes of processor board System flash (Read/Write)
      ( TOTAL FLASH 8192K = 8MB )
Configuration register is 0x2142 → Registro de configuração

```

Vamos analisar os campos grifados de cima para baixo:

11. Versão de IOS que está rodando é a **12.0(5)T**.
12. Tempo que o roteador está ligado (**Uptime**) é de **3 minutos**.
13. Motivo da última reinicialização foi por desligamento normal ou **Power on**.
14. IOS que está rodando: o IOS está na memória **flash** e tem o nome **c2600-i-mz.120-5.T1.bin**.
15. A quantidade de memória RAM é de **26624K** mais **6144K**, o que dá aproximadamente 32Mbytes de memória.
16. Temos apenas **uma interface Ethernet padrão IEEE 802.3** instalada no roteador.
17. Quantidade de memória **NVRAM** (arquivo backup de configuração) é de **32Kbytes**.
18. Quantidade de memória **flash** é de **8192K** ou **8Mbytes**.
19. Registro de configuração atual e futuro são iguais a **0x2142** em hexadecimal. O valor padrão deve ser 0x2102, o valor atual de 0x2142 é utilizado para recuperação de senhas que vamos aprender em tópico posterior.

Note que a quantidade de **RAM/DRAM** vem separada em duas partes **26624K/6144K** e você precisa somar esses dois valores para ter o valor total em Quilo Bytes. Lembre-se que um K byte não são 1000 bytes e sim 1024 bytes!

Para o IOS versão 15 a diferença é que são mostradas opções de licenciamento do Cisco IOS antes do registro de configuração e alguns detalhes do número de série do equipamento. Veja saída abaixo para um roteador modelo Cisco 1941, sendo que as diferenças estão marcadas em cinza.

```
Router#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.0(1)M4,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Thu 28-Oct-10 16:26 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)

Router uptime is 10 minutes
System returned to ROM by reload at 22:14:44 UTC Mon Sep 23 2013
System image file is "flash0:c1900-universalk9-mz.SPA.150-1.M4.bin"
Last reload type: Normal Reload
Last reload reason: Reload Command
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:  
<http://www.cisco.com/wlc/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

```
Cisco CISCO1941/K9 (revision 1.0) with 487424K/36864K bytes of memory.
Processor board ID FTX150800UX
2 Gigabit Ethernet interfaces
1 Serial(sync/async) interface
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
254464K bytes of ATA System CompactFlash 0 (Read/Write)
```

#### License Info:

#### License UDI:

Device#	PID	SN
*0	CISCO1941/K9	FTX150800UX

Technology Package License Information for Module:'c1900'

Technology	Technology-package Current	Type	Technology-package Next reboot
ipbase	ipbasek9	Permanent	ipbasek9
security	securityk9	Evaluation	securityk9
data	datak9	Evaluation	datak9

Configuration register is 0x2102

Router#

## 2.4 Outros Comandos para Verificar Informações básicas de Roteadores e Switches

Nesse tópico vamos estudar alguns comandos úteis em campo para verificar se temos módulos com defeito ou mal encaixados, assim como verificar informações gerais dos dispositivos e seu funcionamento básico. Vamos iniciar pelos comandos “**show diag**” e “**show inventory**”.

Os comandos **show diag** e **show inventory** podem ser utilizados para verificar os **módulos instalados** no roteador e também **números de série** do equipamento e dos módulos.

Nem todos os roteadores fornecem o número de série via comando, aí você terá que verificar na **etiqueta** do equipamento identificada com o número de série ou **serial number (SN)**, veja na figura a seguir.



Veja a seguir a saída dos comandos **show diag** e **show inventory** respectivamente.

```
dltec#show diag
Slot 0:
      C2801 2FE 4SLOT Mainboard Port adapter, 15 ports
      Port adapter is analyzed
      Port adapter insertion time 5d05h ago
      EEPROM contents at hardware discovery:
      Chassis MAC Address      : 001e.130b.1aee
      MAC Address block size   : 34
      PCB Serial Number        : FOC11456KRJ
      Hardware Revision         : 7.0
      Part Number               : 73-8190-07
      Board Revision            : C0
```

```

Top Assy. Part Number      : 800-23435-05
Deviation Number          : 0
Fab Version                : 04
CLEI Code                  : IPM7V00CRA
RMA Test History           : 00
RMA Number                 : 0-0-0-0
RMA History                : 00
Product (FRU) Number       : CISCO2801
Version Identifier          : V04
Processor type              : 86
Chassis Serial Number      : FHK1147F1JV
EEPROM format version 4
EEPROM contents (hex):
  0x00: 04 FF C3 06 00 1E 13 0B 1A EE 43 00 22 C1 8B 46
  0x10: 4F 43 31 31 34 35 36 4B 52 4A 40 04 1C 41 07 00
### saídas omitidas...
  0x1E0: FF FF
  0x1F0: FF FF

```

**PVDM Slot 0:**

```

8-channel (G.711) Voice/Fax PVDMII DSP SIMM PVDM daughter card
Hardware Revision          : 4.0
Part Number                 : 73-8848-05
Board Revision               : B0
Deviation Number             : 0
Fab Version                  : 04
PCB Serial Number           : FOC11410QXX
RMA Test History             : 00
RMA Number                   : 0-0-0-0
RMA History                  : 00
Processor type                : 00
Product (FRU) Number         : PVDM2-8
Version Identifier            : V01
EEPROM format version 4
EEPROM contents (hex):

```

### Saída omitida propositalmente ###

**VIC Slot 0:**

```

2nd generation - E&M Voice daughter card (2 port)
Hardware Revision          : 4.1
Top Assy. Part Number        : 800-21342-01
Board Revision               : E0
Deviation Number             : 0-0
Fab Version                  : 03
PCB Serial Number           : FOC0902159J
RMA Test History             : 00
RMA Number                   : 0-0-0-0
RMA History                  : 00
Version Identifier            : V
Product (FRU) Number         : VIC2-2E/M=
EEPROM format version 4
EEPROM contents (hex):

```

### Saída omitida propositalmente ###

**WIC/VIC/HWIC Slot 3:**

```

2nd generation - FXO Voice daughter card (2 port)
Hardware Revision          : 5.0
Top Assy. Part Number        : 800-21597-02

```

```

Board Revision      : A0
Deviation Number   : 0-0
Fab Version        : 04
PCB Serial Number  : FOC10380BRE
RMA Test History   : 00
RMA Number          : 0-0-0-0
RMA History         : 00
Product (FRU) Number: VIC2-2FXO
Version Identifier  : V01
CLEI Code           : CNUIARTAAA
EEPROM format version 4
EEPROM contents (hex):

```

### Saída omitida propositalmente ###

dltec#show inventory

```

NAME: "chassis", DESCR: "2801 chassis"
PID: CISCO2801      , VID: V04 , SN: FHK1147F1JV

```

```

NAME: "motherboard", DESCR: "C2801 Motherboard with 2 Fast Ethernet"
PID: CISCO2801      , VID: V04 , SN: FOC11456KRJ

```

```

NAME: "VIC 0", DESCR: "2nd generation two port EM voice interface daughtercard"
PID: VIC2-2E/M=      , VID: V , SN: FOC0902159J

```

```

NAME: "WIC/VIC/HWIC 1", DESCR: "WAN Interface Card - Serial 2T"
PID: WIC-2T          , VID: V01, SN: 35725133

```

```

NAME: "WIC/VIC 2", DESCR: "Four port FXS DID voice interface daughtercard"
PID: VIC-4FXS/DID=    , VID: 3.1, SN: FOC12193U3S

```

```

NAME: "WIC/VIC/HWIC 3", DESCR: "2nd generation two port FXO voice interface
daughtercard"
PID: VIC2-2FXO       , VID: V01 , SN: FOC10380BRE

```

```

NAME: "PVDM 0", DESCR: "PVDMII DSP SIMM with one DSP with half channel capacity"
PID: PVDM2-8          , VID: V01 , SN: FOC11410QXX

```

Esses dois comandos podem ser utilizados também para verificar se o módulo está operacional, pois normalmente um módulo com defeito não aparece na saída desses comandos.

**Dica:** Na prática um roteador ou switch é dividido em chassi e módulos ou placas. O número de série do equipamento como um todo é o do seu chassi, note nos comandos que aprendemos que existe um número de série da motherboard do equipamento, este número é utilizado somente para algumas verificações, porém o cadastro do equipamento deve ser vinculado ao número de série do seu chassi. Muitas vezes os parceiros da Cisco chama o chassi de "caixa".

Esses dois comandos não funcionam na versão atual do packet tracer.

Outro comando útil é o **show environment** (em alguns equipamentos entra apenas com "show env"). Ele fornece o status das FANs (ventoinhas) dos roteadores e em alguns modelos pode fornecer também a temperatura do dispositivo. Veja na saída do comando a seguir um exemplo para o roteador modelo Cisco 2801, o qual tem duas ventoinhas.

```

dltec#show environment
Fan 1 OK
Fan 2 OK
ILP Power Supply - Absent
Fan Speed Setting: Normal

```

A seguir temos a saída do mesmo comando em um switch modelo 2950 (o 2960 tem saída semelhante e usa o mesmo comando), porém ele é realizado de uma maneira um pouco diferente: "**show env all**".

```
Switch>en
```

```
Password:
```

```
Switch#show env ?  
all      Show all environment status  
fan      Show fan status  
power    Show power supply status  
rps      Show RPS status
```

```
Switch#show env all  
FAN is OK  
Internal POWER supply is OK  
RPS is NOT present
```

## 2.5 Processo de Inicialização dos Roteadores Cisco

Quando ligamos um roteador ou switch Cisco ele passa por um processo de inicialização padrão que visa basicamente realizar três tarefas principais:

1. Verificar o hardware com uma rotina chamada "**POST**" ou "**Power-on Self Test**". Nesse passo o roteador descobre e testa os componentes de hardware, processo parecido com o POST que a BIOS dos computadores realizam.
2. Buscar um arquivo de IOS válido e inicializá-lo em sua memória RAM → por padrão o roteador busca o IOS na Flash, depois em um servidor TFTP e se não encontrar entra em **Rom Monitor** (Rommon1>). Na realidade esse processo é feito por um programa de baixo nível chamado "**Bootstrap**" que está gravado na **memória ROM** do roteador. Portanto, o roteador carrega esse programa em sua memória RAM, o executa e aí parte para procurar o IOS, carregá-lo e executá-lo RAM. Se o processo finaliza com sucesso o bootstrap sai de cena e dá lugar ao Cisco IOS no controle do hardware. A sequência exata do passo 2 é:
  - a. Carregar o bootstrap e executá-lo na memória RAM.
  - b. Bootstrap executa operações para localizar e carregar um IOS válido na memória RAM.
  - c. Se o IOS não é encontrado ou está corrompido o roteador pode entrar em dois modos: **Rom Monitor** (dispositivos mais novos) ou **RX Boot** (dispositivos antigos).
3. Buscar um arquivo de configuração inicial (primeiro na NVRAM e opcionalmente em um TFTP) para finalizar o processo de inicialização e entrar em operação normal.
  - a. Se um arquivo válido não é encontrado o roteador entra em **modo setup**.

Resumindo a inicialização:

- **POST (ROM)** → **Bootstrap** (copiado da ROM para a RAM e executado) → **Encontrar e carregar IOS** (copiado da flash ou servidor TFTP para a RAM e executado) → **Encontrar e carregar arquivo de configuração** (copiado da NVRAM ou servidor TFTP para a RAM e executado linha a linha).

Agora vamos estudar cada um dos passos e os principais problemas que podem acontecer.

### 2.5.1 Problemas no POST

Apesar de não ser foco do exame atual tanto para o CCENT como para o CCNA os principais problemas que podem ocorrer na inicialização e “travar” a inicialização de roteadores estão relacionados a memórias (RAM ou Flash corrompidas) ou interfaces não suportadas pelos roteadores ou com problemas.

Normalmente uma mensagem de erro aparecerá e o roteador entra em um “loop” não inicializando nunca. Você pode tentar ligar e desligar o roteador algumas vezes, mas se a situação não mudar terá que procurar ajuda da Cisco ou do representante que vendeu o equipamento à empresa que você trabalha.

### 2.5.2 Detalhes da Carga do Bootstrap e Cisco IOS

Vamos agora mostrar mais alguns detalhes desse passo e ensinar como influenciar na decisão sobre qual IOS o roteador ou switch deve utilizar.

A inicialização padrão de um roteador Cisco se dá com a carga do bootstrap na memória RAM, depois ele executa algumas rotinas básicas que precisamos entender:

1. Verifica o registro de configuração (bits finais do config-register – campo de boot).
2. De acordo com o valor o roteador segue a seguinte lógica de sequência de inicialização:
  - a. Se o roteador está com o valor padrão 0x2102 (campo de boot **2**):
    - i. Verifica comandos de **boot system** na configuração inicial da NVRAM (Startup Config).
    - ii. Faz a carga de IOS padrão (Flash → TFTP → ROM) se não houver comandos de boot system ou
    - iii. Faz a carga do IOS indicado nos comandos de boot system tentando cada comando e se nenhum funcionar carrega primeiro IOS encontrado.
  - b. Valor do registro de configuração diferente do padrão? Contando que estamos com roteadores modernos (acima da linha **ISR-G1**).
    - i. Campo de boot zero (0x0): roteador inicializa em ROM Monitor.
    - ii. Campo de boot um (0x1): roteador inicializa com o primeiro IOS encontrado na flash.
    - iii. Campo de boot de 2 a F (0x2...F):
      1. O roteador tenta cada comando de boot system encontrado na startup-config até que um deles funcione.
      2. Se nenhum funcionar ele carrega o primeiro IOS encontrado na memória flash.

Os comandos de boot system são entrados em modo de configuração global para alterar como o roteador carrega o IOS, veja exemplos de comandos abaixo:

1. **boot system flash** → carrega o primeiro arquivo de IOS disponível na flash.
2. **boot system flash nome-do-IOS.bin** → se definirmos um nome o roteador vai procurar por aquele IOS específico na memória flash. Esse comando é útil quando temos vários IOSs na flash e queremos utilizar um específico.
3. **boot system tftp nome-do-IOS.bin 10.0.0.1** → com esse comando fazemos o roteador carregar seu Cisco IOS a partir do servidor TFTP com endereço 10.0.0.1.

Para que as opções 2 e 3 funcionem corretamente o arquivo deve estar disponível com o mesmo nome definido no comando, além disso, para o TFTP o servidor deve estar acessível via rede IP.

Porque isso é importante? Por exemplo, você está utilizando o padrão dos roteadores, que é o registro 0x2102 sem nenhum comando de boot system e deseja fazer o Upgrade do arquivo de IOS. Se você simplesmente copiar o novo arquivo e não apagar o anterior, mesmo que

reinicialize o roteador ele vai continuar carregando o antigo, pois por padrão com o final 2 no campo de boot do registro de configuração o roteador carrega o primeiro IOS, que é o antigo.

Como resolver esse problema? Temos duas opções.

A primeira é apagar o IOS antigo, porém é arriscado, pois se o novo não subir o roteador ficará em ROM Monitor.

A segunda opção é inserir um comando de boot system indicando o IOS mais novo como prioridade na carga, por exemplo, "**boot system flash:c2900-universalk9-mz.SPA.152-4.M1.bin**", na sequência salvamos na NVRAM e utilizamos o comando reload para reiniciar o sistema. Se o novo IOS estiver sem problemas o roteador deve subir e você pode comprovar com o comando "**show version**" se ele está sendo utilizado.

### 2.5.3 Roteador em ROM Monitor – Qual o problema?

Conforme já citado, o registro de configuração é armazenado na NVRAM e formado por 16 bits (4 dígitos em hexadecimal) que armazenam várias informações sobre a configuração inicial dos roteadores. Por exemplo, a velocidade padrão de 9600bps da console é definida dentro do configuration register. Se os bits específicos nesse registro forem alterados, no próximo reload a velocidade da console ou outros parâmetros serão modificados.

Se configurarmos qualquer valor nesse registro com o final zero (0x---0) o roteador de modelo mais novo (ISR-G1 ou G2) entrará automaticamente em Rom Monitor e não inicializa. Podemos alterar em Rom Monitor esse valor para o padrão com o comando "**config-register 0x2102**" e com a opção "i" ou "reset" reiniciar o roteador para ver se ele volta ao normal.

Veja abaixo um exemplo onde o registro estava configurado como 0x1 (valor 1 em Hexa) e foi reconfigurado para o padrão 0x2102. No final o show version informa que ele será 0x2102 somente após o próximo reload (**will be 0x2102 at next reload**).

```
Router#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.0(1)M4,
RELEASE SOFTWARE (fc1)

### saídas omitidas###

Configuration register is 0x1

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#config-register 0x2102
Router(config)#end
Router#sho version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.0(1)M4,
RELEASE SOFTWARE (fc1)

### Saídas omitidas ###

Configuration register is 0x1 (will be 0x2102 at next reload)

Router#
```

Comandos de boot system errados podem também levar ao roteador inicializar em ROM Monitor, por exemplo, se o comando "**boot system rom**" for digitado, ele manda o roteador inicializar pela ROM e nos roteadores novos só tem o ROM Monitor nessa memória além do boot strap.

Se o problema não for no registro ou nos comandos de boot system você precisará utilizar um recurso chamado “**tftpdnl**” para copiar o IOS via TFTP para a memória flash ou utilizar o **X-MODEM** e copiar um IOS pela porta de console. Ambos os procedimentos não são foco do CCNA atual, porém mais para frente vamos ensiná-los porque é importante para sua vida prática como futuro CCNA R&S!

Muito cuidado ao alterar esses parâmetros na prática, pois eles podem parar os equipamentos!

#### 2.5.4 Problemas com o arquivo de configuração inicial (Startup Config)

Passada a etapa de carregamento do IOS o roteador precisa agora de uma configuração.

Lembre-se que se o roteador não tiver configuração, ou for novo, você precisará se conectar via cabo de console e o modo chamado **Setup** será exibido para os roteadores, pois não existe arquivo de configuração inicial válido na NVRAM.

Dependendo da versão de IOS os roteadores têm como padrão o usuário cisco e senha cisco pré-configuradas, necessitando ser alterado no primeiro acesso. Normalmente isso é informado em uma mensagem na inicialização, por isso é recomendável ao ligar um roteador que estava desligado com o cabo de console plugado e o terminal já aberto para verificar as mensagens.

Ainda sobre o modo setup, ele pode ser utilizado para configuração e mesmo você saindo no início pode chamá-lo a qualquer momento digitando “setup” em modo de usuário privilegiado, veja saída abaixo:

```
Router> enable
Password: <password>
Router# setup
    --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: yes
```

Ao digitar “Yes” para continuar a usar esse wizard de configuração várias perguntas serão apresentadas com o intuito de fazer uma configuração básica e ativar o acesso remoto via Telnet para que um administrador mais experiente finalize a configuração.

Uma dica importante é que quando for solicitada uma interface você precisará digitar o nome completo, veja o exemplo abaixo quando o setup pergunta a interface de gerenciamento:

```
management network from the above interface summary: gigabitethernet0/1
Configuring interface GigabitEthernet0/1:
Configure IP on this interface? [yes]: yes
IP address for this interface [10.10.10.12]:
Subnet mask for this interface [255.0.0.0] : 255.255.255.0
Class A network is 10.0.0.0, 24 subnet bits; mask is /24
```

Ao final das perguntas será exibida a configuração e a seguinte mensagem:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]: 2
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started! RETURN
```

Nesse ponto você deve escolher se sai do setup sem salvar (0), retornar ao início do setup sem salvar (1) ou salvar e voltar ao modo de configuração (2). No exemplo acima a configuração foi salva.

## 2.6 Salvando e Manipulando Arquivos de Configurações

Ao finalizar uma configuração é importante salvar esse arquivo na memória NVRAM (startup-config), pois tudo o que você fizer de configuração ficará na memória RAM (running-config) e precisa ser salvo em uma memória não volátil para não ser perdida após um reset. Veja comando abaixo.

```
R1#copy running-config startup-config
```

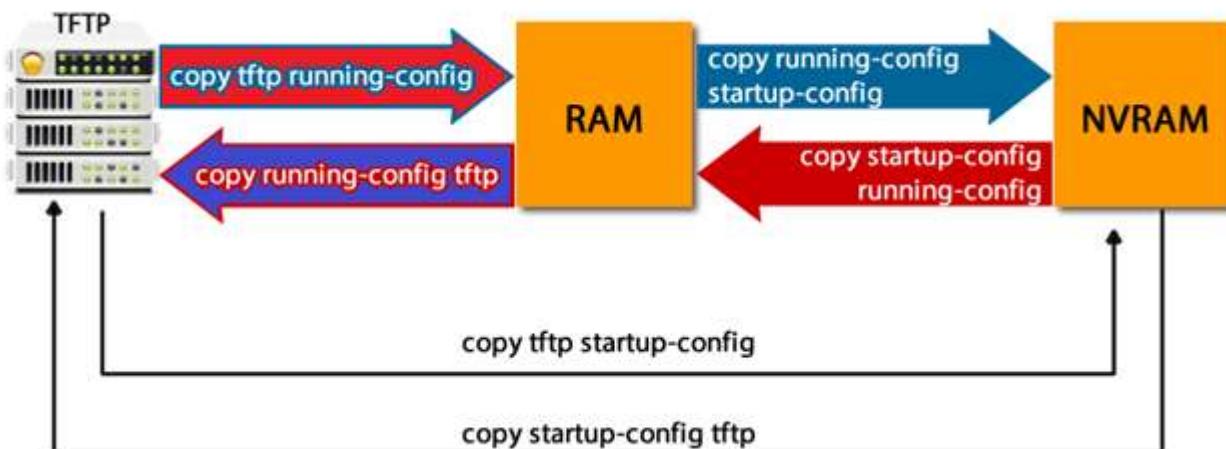
Outra opção é gravar essa configuração em um servidor externo utilizando o serviço de TFTP ou Trivial File Transfer Protocol. Para fazer a gravação desse arquivo no TFTP utilize o comando copy running-config tftp, veja exemplo abaixo:

```
SW-DlteC>en
Password:
SW-DlteC#copy running-config tftp
Address or name of remote host []? 192.168.1.71
Destination filename [sw-dltec-cfg]?
!!
13650 bytes copied in 1.594 secs (8563 bytes/sec)
SW-DlteC#
```

Os pontos de exclamação indicam sucesso, portanto agora na pasta padrão do servidor TFTP temos o arquivo chamado **sw-dltec-cfg** salvo com sucesso, o qual pode ser editado com o notepad, por exemplo. O endereço IP do servidor TFTP nesse caso é **192.168.1.71** e ele deve estar ativo e permitir a conexão, em testes de laboratório verifique se o seu firewall não bloqueia esse serviço. Na prática é interessante antes de salvar arquivos em servidores TFTP fazer teste de ping entre o roteador e o servidor.

Você poderia gravar uma cópia da configuração na memória flash com o comando “**copy running-config flash**”.

Lembre-se que o comando **copy** pede primeiro a **origem** e depois o **destino** do arquivo a ser gravado. A figura abaixo mostra um resumo de como você pode manipular os arquivos de configuração em roteadores e switches com o comando copy.



Os dois comandos destacados em vermelho, onde copiamos algo para a running-config, não substituem o conteúdo atual da memória RAM e sim **se mesclam a eles**, fazendo um “**merge**”, ou seja, o resultado final não será exatamente o que foi copiado e sim uma mistura dos dois.

É importante mantermos backup das configurações e do sistema operacional para o caso de um equipamento ficar totalmente indisponível e a troca ser a única opção de voltar o serviço. A seguir estudaremos como manipular arquivos de IOS.

## 2.7 Copiando e Manipulando Arquivos de IOS

Veremos agora um tópico muito importante no dia a dia de qualquer profissional de redes - a **atualização e backup de IOS**. Esta é uma tarefa simples, mas que pode se tornar complicada caso você não esteja totalmente familiarizado com os comandos utilizados. Sendo assim, estude bem os comandos mostrados nesse tópico e depois pratique nas atividades propostas com o Packet Tracer.

Os comandos TFTP utilizados para realizar cópia de segurança e atualização de IOS são:

- **copy tftp flash:** Transfere um IOS contido no servidor TFTP para o roteador. É necessário verificar se existe espaço na memória flash para o novo arquivo. Esse comando é utilizado para atualizar a versão do IOS (fazer Upgrade).
- **copy flash tftp:** Realiza o backup do IOS contido na memória flash para o servidor TFTP.

É importante utilizar o comando “**show flash**” para verificar se o arquivo cabe na memória flash do roteador. Além disso, antes de copiar um arquivo de um servidor TFTP é importante testar a conectividade com o comando “ping” antes de iniciar o processo de backup. Abaixo segue a saída do comando “**show flash**”:

```
MatrizCTBA#sh flash
System flash directory:
File  Length      Name/status
 1    5909248    c1700-y-mz.123-15.bin
[5909312 bytes used, 10605756 available, 16515068 total]
16384K bytes of processor board System flash (Read/Write)
MatrizCTBA#
```

No exemplo mostrado acima podemos observar que na memória flash do roteador "MatrizCTBA" existe apenas um IOS - c1700-y-mz.123-15.bin . Também é mostrado que esse IOS possui o tamanho de aproximadamente 5,9Mb.

Outra informação muito importante é o tamanho da memória flash e quantidade disponível (livre) de memória. Observe a penúltima linha da saída do comando.

```
[5909312 bytes used, 10605756 available, 16515068 total]
```

Ela nos mostra que temos:

- Quantidade de memória utilizada: 5909312 bytes (aprox. 5,9M)
- Quantidade de memória livre: 10605756 bytes (aprox. 10,6M)
- Quantidade total de memória: 16515068 bytes (aprox. 16,5M)

Caso **não exista espaço livre** suficiente para o novo IOS podemos **apagar** arquivos da memória flash com o comando "**delete flash**" ou "**erase flash**". A diferença entre os dois é que o comando "**erase flash**" irá **apagar todo o conteúdo da memória**. Já com o comando "**delete flash: xxxx**" podemos escolher o arquivo que desejamos apagar. Veja abaixo um exemplo da saída de cada um dos comandos.

Exemplo do comando "delete flash:xxxx".

Deve-se tomar cuidado com essa operação, pois se a flash estiver sem um IOS e o roteador for reinicializado, ele voltará em Rom Monitor. Ainda nesse capítulo veremos como resolver esse problema, caso ele venha a acontecer em um roteador, com o comando TFTPDOWNLD.

A seguir temos um exemplo de um download de IOS para a flash do roteador utilizando o comando “**copy tftp flash**”. Nesse exemplo iremos atualizar o IOS de um roteador Cisco1700. O IOS atual é o c1700-y-mz.123-15.bin e devemos atualiza-lo para a versão c1700-sy7-mz.124-17.bin.

Para a execução dessa atividade devemos realizar os seguintes passos:

- Verificação do conteúdo atual da flash para verificar se existe espaço livre suficiente para o novo IOS (comando show flash);
  - Teste de conexão com o servidor TFTP, que no nosso caso está no endereço IP 10.0.0.254;
  - Liberação de espaço livre na flash com o comando "del flash:xxxxx";
  - Cópia do novo IOS para flash (comando copy tftp flash).

```
MatrizCTBA#show flash
System flash directory:
File Length Name/status
 1 5909248 c1700-y-mz.123-15.bin
[5909312 bytes used, 10605756 available, 16515068 total]
16384K bytes of processor board System flash (Read/Write)
MatrizCTBA#ping 10.0.0.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
MatrizCTBA#del flash:c1700-y-mz.123-15.bin
Delete filename [c1700-y-mz.123-15.bin]?
Delete flash:c1700-y-mz.123-15.bin? [confirm]
MatrizCTBA#show flash
System flash directory:
File Length Name/status
 1 5909248 c1700-y-mz.123-15.bin [deleted]
[5909312 bytes used, 10605756 available, 16515068 total]
16384K bytes of processor board System flash (Read/Write)
```

```

MatrizCTBA#squeeze flash
Squeeze operation may take a while. Continue? [confirm]
squeeze in progress... eeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
Squeeze of flash complete
MatrizCTBA#show flash
System flash directory:
No files in System flash
[0 bytes used, 16515068 available, 16515068 total]
16384K bytes of processor board System flash (Read/Write)
MatrizCTBA#copy tftp flash
Address or name of remote host []? 10.0.0.254
Source filename []? c1700-sy7-mz.124-17.bin
Destination filename [c1700-sy7-mz.124-17.bin]?
Accessing tftp://10.0.0.254/c1700-sy7-mz.124-17.bin...
Erase flash: before copying? [confirm]n
Loading c1700-sy7-mz.124-17.bin from 10.0.0.254 (via FastEthernet0):!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
#### Saídas Omitidas
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 13135564 bytes]
Verifying checksum... OK (0xF907)
13135564 bytes copied in 502.948 secs (26117 bytes/sec)
MatrizCTBA#show flash
System flash directory:
File Length Name/status
1 13135564 c1700-sy7-mz.124-17.bin
[13135628 bytes used, 3379440 available, 16515068 total]
16384K bytes of processor board System flash (Read/Write)
MatrizCTBA#

```

É uma prática recomendável sempre **verificar a integridade** da cópia realizada antes de reiniciar o equipamento. Isso pode ser feito com o comando "**verify /md5 flash:nomedooios.bin**".

A saída desse comando exibirá o código com a chave MD5 do IOS em questão. O código para cada IOS pode ser encontrado na página da Cisco específica para o download do IOS. No caso do IOS utilizado no nosso exemplo (c1700-sy7-mz.124-17.bin) a chave MD5 é: e898c1f063a31fee6814afc387bb2ea3.

Abaixo segue um resumo dos passos para fazer o upgrade de IOS:

1. Ativar o serviço de TFTP em um servidor ou computador de rede.
2. Copiar a imagem do IOS para a pasta padrão do servidor TFTP.
3. Certificar que as permissões e o nome do IOS estão corretos (com a extensão ".bin").
4. Fazer um teste de conectividade entre o servidor e o roteador com ping ou Telnet/SSH.
5. Verificar se existe espaço na memória flash para comportar o IOS novo e o antigo ao mesmo tempo, senão apagar o IOS antigo.
6. Utilizar o comando "copy tftp: flash:" para realizar a cópia (como mostrado ao lado em modo texto a animação do slide anterior).
7. Inserir comando de boot system para fazer com que o novo IOS seja a primeira opção de inicialização.
8. Executar um reload para o roteador carregar a nova versão de IOS.

Apesar de parecer um processo simples, o Upgrade de IOS gera na prática muitos problemas se o administrador de redes responsável pela atividade não tiver domínio do processo. Os problemas mais comuns são:

- Problemas com o firewall, antivírus ou anti-spyware instalado no servidor ou computador que está com o serviço de TFTP rodando, pois muitas vezes o serviço é bloqueado por um desses softwares.
- Problemas de permissão com a pasta onde está gravada a imagem de IOS. Normalmente recomenda-se rodar o programa com serviço de TFTP como administrador se você estiver utilizando um computador com sistema operacional Windows.
- "Problemas com o nome do IOS, pois dependendo da configuração o Windows não mostra a extensão ".bin" mas ela está lá, com isso um administrador desavisado pode inserir um outro ".bin" ao nome transformando o IOS em "cxxx-xxxx-xxxx.bin.bin" e não será encontrado no servidor, pois o nome que você digita no comando deve ser idêntico ao gravado no servidor.

Quando houver erros em ambiente prático em sua empresa ou cliente, procure verificar as mensagens do roteador e também no programa do serviço TFTP, normalmente analisando os dois lados (servidor e roteador) fica mais fácil de resolver os problemas.

## 2.8 Utilizando FTP e SCP para Copiar Arquivos

O FTP é uma opção mais segura para copiar e enviar arquivos armazenados agora em um servidor que possui autenticação e acesso mais simples a partir de um computador.

Veja os passos de configuração abaixo.

```
DlteC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DlteC(config)#ip ftp username cisco
DlteC(config)#ip ftp password cisco123
DlteC(config)#no ip ftp passive
DlteC(config)#ip ftp source-interface FastEthernet0/1.10
```

O usuário e a senha são os de acesso ao servidor FTP, já o comando "no ip ftp passive" é o padrão que aceita os dois tipos de servidores FTP. Com o comando "ip ftp source-interface" você pode definir o IP da interface que será coloca como origem nos pacotes IP.

Para realizar a cópia de um arquivo do servidor para o router utilize o comando "copy ftp://IP-servidor/pasta flash:". Já para salvar um arquivo no servidor FTP utilize "copy flash: ftp://IP-servidor/pasta". Veja exemplo abaixo onde vamos fazer um backup do Cisco IOS no servidor FTP com IP 192.168.1.8.

```
DlteC#copy flash:c2801-adventerprisek9-mz.124-24.T8.bin ftp://192.168.1.12
Address or name of remote host [192.168.1.12]?
Destination filename [c2801-adventerprisek9-mz.124-24.T8.bin]?
Writing c2801-adventerprisek9-mz.124-24.T8.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
50825880 bytes copied in 83.104 secs (611594 bytes/sec)
DlteC#
```

### 2.8.1 Serviço de SCP

O SCP ou Secure Copy permite a cópia segura de arquivos através do Secure Shell, ou seja, assim como o SSH é uma versão segura do Telnet, nesse caso o SCP é uma versão segura tanto para o FTP como para o TFTP, pois os dados são criptografados antes de transmitidos pela rede.

Para ativar o serviço de SCP como servidor em um roteador Cisco precisamos seguir seis passos básicos e ativar o AAA. Abaixo seguem os comandos gerais de ativação.

1. enable
2. configure terminal
3. aaa new-model
4. aaa authentication login {default | list-name} method1[method2...]
5. aaa authorization {network | exec | commands level | reverse-access | configuration} {default | list-name} [method1 [method2...]]
6. username name [privilege level]{password encryption-type encrypted-password}
7. ip scp server enable

Veja um exemplo de configuração abaixo onde a configuração do AAA tanto para autenticação como para autorização foi realizada via banco de dados local.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
R1(config)#aaa authorization exec default local
R1(config)#username dltec privilege 15 secret dltec123
R1(config)#! Certifique-se antes que o SSH está ativado e funcionando
R1(config)#ip scp server enable
R1(config) #
```

Com a configuração acima você transformou seu roteador em um servidor SCP e pode utilizá-lo como fonte segura de cópias do Cisco IOS, por exemplo.

Para fazer a cópia segura via SCP como cliente a partir de um roteador ou switch Cisco utilize o comando "copy" com a opção "scp://" na origem ou destino, conforme a necessidade de troca de arquivos entre os roteadores, veja exemplo abaixo.

```
DlteC#copy flash:syncinfo.xml scp://192.168.1.86
Address or name of remote host [192.168.1.86]?
Destination username [dltec]?
Destination filename [syncinfo.xml]?
Writing syncinfo.xml
Password:
!
69 bytes copied in 3.916 secs (18 bytes/sec)
DlteC#
```

Vamos analisar agora a flash do roteador que está atuando como SCP server.

```
R1#show disk0:
-#- --length-- -----date/time----- path
1          24439 May 13 2015 15:13:28 dltec-config
2            69 May 13 2015 15:16:14 syncinfo.xml

133890048 bytes available (28672 bytes used)
```

Você pode utilizar o comando "copy [flash:CiscoIOS.bin ou running-config] scp://ip-scp-server" para transmitir arquivos de forma segura mesmo que se roteador não tenha um servidor SCP ativo, pois ele já atua por padrão como cliente SCP.

## 2.9 Recuperação de IOS – Disaster Recovery

A **recuperação do IOS**, chamado de "**Disaster Recovery**" na documentação da Cisco, deve ser utilizada caso o roteador ao reiniciar entre em modo Rom Monitor e ele não tenha IOS na flash. Segue abaixo o prompt de um roteador em Romon:

```
rommon 1 >  
rommon 2 >  
rommon 3 >
```

Note que um equipamento em Rommon não significa que você deve aplicar o procedimento mostrado aqui, tente reiniciar ligando e desligando a energia algumas vezes, após isso verifique o valor do registro de configuração (confreg) e certifique-se que a flash está mesmo sem IOS.

Você pode recuperar o IOS de várias maneiras, uma delas é carregando o IOS diretamente do seu laptop. Essa metodologia tem se mostrado mais eficiente na prática e vamos demonstrar abaixo os passos para executá-la.

1. Prepare o servidor TFTP no seu micro ou lap-top;
2. Configure um IP conhecido em seu computador, por exemplo, 10.0.0.254 com a máscara 255.0.0.0;
3. Conecte seu computador no switch que o roteador está conectado ou então diretamente à interface LAN do roteador com um cabo Cross-over;
4. No seu programa emulador de terminal preferido (Teraterm, Hyperterminal) entre com o comando "set", em Romon, e configure os parâmetros para o roteador buscar o IOS no servidor TFTP configurado no seu micro;
5. Após configurar os parâmetros execute o comando "tftpdnld -r";
6. Agora o roteador deve estar funcionando e você deve copiar um IOS válido para a flash com o comando "copy tftp flash".

Note que ao executar o comando "tftpdnld -r" o roteador irá inicializar o IOS através do seu laptop, ou seja, esse IOS ainda não estará na memória flash do roteador. No caso de um reset o roteador irá entrar em rommon novamente. Por isso devemos copiar o IOS para a flash com o comando "copy tftp flash".

Abaixo segue um exemplo prático e a explicação dos parâmetros a serem configurados. Faça sempre a configuração na sequência abaixo e caso erre refaça toda a configuração até acertar.

Parâmetros do comando set necessários para executar o tftpdnld:

- IP\_ADDRESS= end. do router (aqui pode ser o IP 10.0.0.1)
- IP\_SUBNET\_MASK= máscara (pode ser a máscara 255.0.0.0)
- DEFAULT\_GATEWAY= end. do laptop (pode ser 10.0.0.254)
- TFTP\_SERVER= end. do laptop
- TFTP\_FILE= nome do IOS

Exemplo prático:

```
rommon 1 >  
rommon 1 > set
```

```

rommon 2 > IP_ADDRESS=10.0.0.1
rommon 3 > IP_SUBNET_MASK=255.0.0.0
rommon 4 > DEFAULT_GATEWAY=10.0.0.254
rommon 5 > TFTP_SERVER=10.0.0.254
rommon 6 > TFTP_FILE=c1700-sy7-mz.124-17.bin
rommon 7 > tftpdnld -r
    IP_ADDRESS: 10.0.0.1
    IP_SUBNET_MASK: 255.0.0.0
    DEFAULT_GATEWAY: 10.0.0.254
    TFTP_SERVER: 10.0.0.254
    TFTP_FILE: c1700-sy7-mz.124-17.bin
Receiving c1700-sy7-mz.124-17.bin from 10.0.0.254 !!!!!!!!
!!!!!!!
File reception completed.
program load complete, entry point: 0x80008000, size: 0x54e52c
Self decompressing the image : #####
#####
##### [OK]

```

Agora basta copiar um IOS, que pode ser o mesmo utilizado acima, para a flash e verificar se ele foi mesmo gravado com o comando "show flash".

## 2.10 Recuperação de Senha

Algumas vezes pode ser necessário **quebrar a senha** de um roteador para a realização da configuração de um equipamento no qual você desconheça a senha configurada. No exemplo a seguir mostramos os passos para se quebrar a senha de um roteador Cisco 1700, porém o mesmo processo pode ser seguido para os roteadores da linha ISR-G1 e ISR-G2 mais recentes.

**Primeiro Passo:** Reinicie o roteador e interrompa o processo de carga do IOS o colocando no modo ROMMON. Para tal pressione as teclas "**CTRL + BREAK**" (se estiver utilizando o HyperTerminal) ou "**ALT + B**" (para o caso do Teraterm) durante os primeiros segundos do processo.

Assim que estiver em rommon entre com o comando "**confreg 0x2142**" e em seguida com o comando "**reset**".

```

Self decompressing the image : #####
Monitor: command "boot" aborted due to user interrupt
rommon 1 > confreg 0x2142_
You must reset or power cycle for new config to take effect
rommon 2 > reset

```

**Segundo Passo:** Após o processo de reset responda "**no**" a pergunta. Pronto, você está com acesso a linha de comando do roteador.

```

--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Router>

```

**Terceiro Passo:** Entre em modo privilegiado (enable) e copie a configuração contida na NVRAM para a memória RAM.

```

Router> enable
Router# copy startup-config running-config

```

**Quarto Passo:** Entre no modo de configuração e configure novas senhas de acesso a console, vty e enable.

```
Router# conf t
Router(config)# enable secret cisco
Router(config)# line console 0
Router(config)# login
Router(config)# password cisco
Router(config)# line vty 0 15
Router(config)# login
Router(config)# password cisco
```

**Quinto Passo:** Salve as alterações no "startup config".

```
Router(config)# exit
Router# copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

**Sexto Passo:** Volte o registro de configuração para o padrão 0x2102 e reinicie o roteador.

```
Router# conf t
Router(config)# config-register 0x2102
Router(config)# exit
Router# reload
System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

Pronto, o roteador reiniciará com a nova configuração. Entre com o usuário e as senhas que você configurou.

Como você pode notar para quebrar a senha de um roteador Cisco nós interrompemos o processo de inicialização e mudamos o registro de configuração para 0x2142, fazendo com o que roteador suba o IOS sem ler a configuração da NVRAM. Esse processo exige dois pontos principais de atenção:

1. Você deve lembrar-se de voltar o registro de configuração para 0x2102 ou seu roteador virá sem configuração toda vez que for reinicializado, seja por reload ou por falta de energia. Esse é um erro comum dos administradores iniciantes com roteadores Cisco. Nesse caso o roteador sempre virá em modo setup ao reiniciar.
2. Antes de alterar as senhas você deve dar o comando "**copy start running**" para trazer a configuração original, que já estava configurada na NVRAM, ou senão você perderá a configuração original do roteador e se não tiver um backup precisará refazer toda ela novamente.

Se você não fizer recomendação 2 acima o roteador voltará sem configuração, ou seja, reseta a senha e também volta com a condição de fábrica.

## 2.11 Voltando Roteadores e Switches à Configuração de Fábrica

Para apagar a configuração de um roteador ou switch Cisco devemos simplesmente apagar o conteúdo da NVRAM e reiniciar o roteador.

Para apagar o conteúdo da memória NVRAM utilizamos o comando "erase startup-config" em modo EXEC privilegiado, veja a saída do comando a seguir.

```
Roteador_A#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Roteador_A#
```

Ao executar o comando note que o roteador faz uma pergunta de confirmação, se você realmente quer fazer isso, caso deseje apagar a NVRAM tecle o Enter (Entra), caso queira desistir da operação digite as teclas "control+Z" ou "n" (no).

Quando pressionamos o enter, conforme exemplo anterior, o roteador envia para a console uma mensagem **%SYS-7-NV\_BLOCK\_INIT** informando que a NVRAM foi formatada.

Em um roteador se você aplicar o comando "reload" para reinicializá-lo ele voltará em modo Setup, pois não existe mais arquivo de backup na NVRAM para ele subir. Às vezes quando digitamos o comando reload ele nos oferece uma pergunta se queremos salvar a configuração alterada, se você escolher sim o roteador salvará de novo a configuração na NVRAM, portanto para zerar o roteador escolha a resposta "n" de "no" e depois tecle o enter. Veja no exemplo a seguir o que ocorre após o reload, note que não foi perguntado se queríamos salvar a configuração, por isso teclamos o enter direto após o reload.

```
Roteador_A#reload
Proceed with reload? [confirm]
%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :
#####
[OK]
Restricted Rights Legend
```

Saída omitida...

```
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
Image text-base: 0x60080608, data-base: 0x6270CD50
```

Saída omitida...

```
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
1 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
```

**--- System Configuration Dialog ---****Continue with configuration dialog? [yes/no] :**

Nos switches Cisco, além da configuração que está na NVRAM, também temos que apagar os arquivos que guardam as configurações de VLAN, chamado **vlan.dat** (de VLAN Database ou banco de dados de VLANs), pois os switches armazenam as VLANs criadas em um arquivo fora da NVRAM. Portanto para zerar um switch temos que apagar a NVRAM, apagar a base de dados de VLANs para depois reinicializá-lo, veja no exemplo a seguir.

```
SwitchA#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
SwitchA#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

SwitchA#reload
Proceed with reload? [confirm]
```

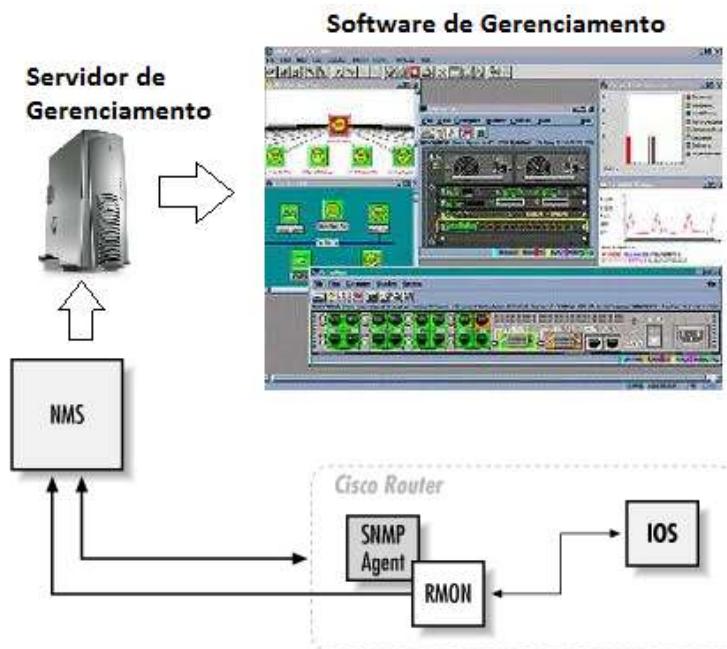
Note que o comando para apagar um arquivo específico na memória flash: é o “**delete**” e a sintaxe é “**delete flash:vlan.dat**”. Caso apareça uma mensagem que o arquivo não existe você pode ter digitado errado o nome do arquivo ou então não ter criado nenhuma VLAN, pois o arquivo é criado somente quando criamos VLANs no switch.

Com esses procedimentos voltamos os equipamentos à configuração de fábrica, ou seja, “zeramos” os equipamentos e finalizamos o gerenciamento e manipulação de arquivos locais nos roteadores e switches Cisco, a seguir vamos começar a estudar recursos para gerenciamento remoto dos equipamentos.

### 3 Gerenciamento de Redes

O tema sobre gerenciamento de redes é bastante abrangente e normalmente envolvem ferramentas, tais como **softwares de gerenciamento (NMS ou Network Management System)**, que são capazes de realizar inúmeras tarefas e monitorar o ambiente de rede de maneira abrangente.

Em uma rede de médio ou grande porte parâmetros como a utilização de memória, carga da CPU (processamento), temperatura dos dispositivos, status de dispositivos de rede, status de links WAN de roteadores, utilização de links WAN ou interfaces trunk e muitos outros parâmetros podem ser monitorados via um software de gerenciamento de redes e uma equipe de suporte pode agir **proativamente** ou de maneira **reativa** frente a problemas que esse sistema de monitoração informa em suas mensagens de alarmes ou avisos.



O CCNA como um todo cobra o conceito do gerenciamento de um dispositivo e da rede utilizando o **Syslog**, **SNMP** e o **Netflow**, porém aqui no CCENT vamos focar no Syslog.

### 3.1 Ativando o Syslog

O **Syslog** é um padrão criado pela IETF para a **transmissão de mensagens de log** em redes IP. O termo é geralmente usado para identificar tanto o protocolo de rede quanto para a aplicação ou biblioteca de envio de mensagens no protocolo syslog, o qual fica armazenado em um servidor de Syslog que pode ser instalado em qualquer computador.



O protocolo syslog é muito simples: 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.

O protocolo syslog é tipicamente usado no gerenciamento de equipamentos em rede para **auditoria de segurança** de sistemas ou análises de problemas. Por ser suportado por uma grande variedade de dispositivos em diversas plataformas, o protocolo pode ser usado para integrar diferentes sistemas em um só repositório de dados.

Nos roteadores e switches Cisco para habilitar o Syslog basta utilizar o comando em modo de configuração global: "**Router(config)#logging ip\_do\_servidor**", abaixo segue um exemplo no qual o servidor de syslog tem o IP 10.0.0.10:

```
Router#config term
Router(config)#logging 10.0.0.10
```

Os **logs do roteador** são as mensagens que ele fornece em caso de problemas, como quedas de interface, ou quando um acesso é realizado ou um evento ocorre, normalmente são as mensagens que recebemos via **console** e que atrapalham quando estamos configurando o roteador. Quando utilizamos um comando **debug**, por exemplo, essas mensagens serão também enviadas para o syslog se configurado. Esse arquivo pode ser posteriormente analisado se não está havendo acessos não autorizados ou problemas recorrentes.

Os logs possuem diversos níveis de amplitude de mensagens (de 0 a 7) que são geradas para o servidor de syslog, conforme abaixo:

- 0 - Emergency → provavelmente o sistema está fora.
- 1 - Alert → uma ação imediata é necessária.
- 2 - Critical → um evento crítico ocorreu.
- 3 - Error → o roteador teve um erro.
- 4 - Warning → essa condição requer atenção, é um aviso.
- 5 - Notification → uma situação normal, porém relevante ocorreu.
- 6 - Informational → significa que um evento normal aconteceu
- **7 - Debugging** (nível padrão nos roteadores e switches Cisco) → a saída é uma mensagem de um debugging.

Resumindo, dos níveis de 0 até 4 temos eventos que realmente podem impactar a operação do equipamento em questão, já dos níveis 5 a 7 são eventos com menor relevância. Temos que decidir no dia a dia onde monitorar para não “entupir” o servidor de mensagens que não poderão ser interpretadas ou simplesmente são inúteis.

Quanto maior a amplitude ou o nível de depuração do log, mais mensagens serão enviadas ao servidor de syslog, portanto a análise de nível do log deve ser feita com cuidado para não gerar sobrecarga no equipamento. Para configurar a amplitude do log entre com o comando em modo de configuração global:

```
router(config)#logging trap nível
```

O nível pode ser o número ou o nome contido na lista acima. O nível 7 ou debug é o mais alto e o emergency o mais baixo, ou seja, menos rico em detalhes. Abaixo segue um exemplo alterando o nível do log para informacional:

```
Router(config)#logging trap informational  
Router(config)# ! ou  
Router(config)#logging trap 6
```

Com o comando acima o roteador enviará ao syslog mensagens de nível 6 até zero, se configurássemos como nível 4 o roteador enviaria mensagens de 4 a zero.

Lembre-se que essas mensagens são armazenadas nos roteadores e switches mesmo que não configuremos um servidor, pois o syslog é utilizado internamente também para:

- O **logging buffer** → armazenamento interno em memória RAM das mensagens nos roteadores e switches, portanto é apagado se reinicializarmos os equipamentos.
- Enviada mensagem para console (**logging console**) → ativada por padrão, são as mensagens que aparecem na console enquanto estamos monitorando localmente os dispositivos.
- Na VTY podemos monitorar essas mensagens com o “**terminal monitor**” → por padrão as mensagens de syslog não são enviadas quando estamos conectados através de SSH ou Telnet, temos que ativar o recebimento das mensagens.
- Através de um servidor de syslog como estudamos anteriormente com o comando **“logging ip-do-servidor”**.

Para desabilitar o padrão de envio das mensagens de log para o console ou para o buffer na memória RAM podemos utilizar os comandos “**no logging console**” e “**no logging buffered**” respectivamente. Se ativamos a monitoração das mensagens em uma sessão de SSH ou Telnet e queremos desabilitá-la podemos utilizar o comando **“terminal no monitor”**.

Na biblioteca do curso, na área do aluno você pode baixar o programa **3Com Daemon**, o qual tem um servidor TFTP, FTP e Syslog integrado. Utilize em seu dia-a-dia de CCNA R&S, pois é uma ferramenta útil.

### 3.1.1 Verificando as mensagens de log

Para verificar as mensagens geradas pelos dispositivos e armazenadas no buffer de registros podemos utilizar o comando "**show logging**". Veja saída do comando em um roteador com a configuração padrão.

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 10 messages logged, xml disabled, filtering
disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering
disabled
Buffer logging: level debugging, 10 messages logged, xml disabled, filtering
disabled
Logging Exception size (8192 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
No active filter modules.
ESM: 0 messages dropped
Trap logging: level informational, 13 message lines logged
```

As mensagens são mostradas por padrão conforme abaixo:

```
DlteC-FW-GW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DlteC-FW-GW(config)#exit
DlteC-FW-GW#
070101: Sep 24 2013 03:04:25.389 BR: %SYS-5-CONFIG_I: Configured from console by
dltec on vty0 (187.112.176.128)
DlteC-FW-GW#
```

- Um timestamp (marcação de data e hora que o registro ocorreu): Sep 24 2013 03:04:25.389 BR
- O recurso no roteador que gerou o registro (facility): %SYS
- Nível de severidade (severity level): 5
- Um mnemônico da mensagem: CONFIG\_I
- Descrição breve da mensagem (description): Configured from console by dltec on vty0 (187.112.176.128)

Podemos mudar o formato de exibição do log de data e hora para um número de sequência com os comandos abaixo:

```
DlteC-FW-GW(config)#no service timestamps
DlteC-FW-GW(config)#service sequence-numbers
DlteC-FW-GW(config)#exit
DlteC-FW-GW#
070102: %SYS-5-CONFIG_I: Configured from console by dltec on vty0
(187.112.176.128)
DlteC-FW-GW#
```

Veja a diferença da mensagem com a nova configuração através de números de sequência.

- Número de sequência (sequence number): 070102
- Facility (recurso): %SYS
- Severity level (nível de severidade): 5
- Mnemônico: Config\_I
- Descrição: Configured from console by console

Existem outras opções que você pode configurar no comando “**Service timestamp**”, por exemplo, utilizando “**Service timestamp log datetime msec**” você define que as mensagens de data e hora sejam mostradas com os milisegundos na mensagem (03:04:25.**389**).

#### 4 Gerenciando o Licenciamento do Cisco IOS Versão 15

Já estudamos os conceitos básicos do Cisco IOS tanto no CCNA ICND-1 como no início desse capítulo, porém agora vamos nos aprofundar um pouco mais no assunto e entender como esse sistema operacional era distribuído no passado e atualmente com o novo modelo de licenciamento.

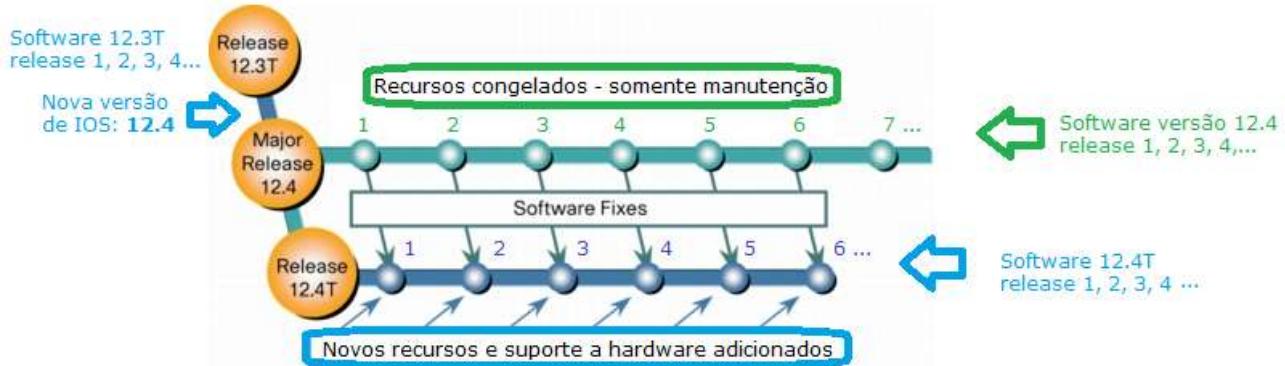
##### 4.1 Cisco IOS por Modelo, Série e Versão/Release de Software

No início desde 1980 até meados de 2012 as imagens do Cisco IOS eram distribuídas por modelo, série e por versão/release de Software. Isso acontecia desde as versões 10.x, 11.x até a 12.x, a qual finalizou com a versão 12.4 para a linha ISR-G1. Vamos entender o que isso significa.

Por exemplo, existiam vários modelos de equipamentos para uma mesma série de roteadores, tais como na linha 1700 tínhamos os modelos 1701, 1721, 1751, 1751-V e assim por diante. Por isso era preciso uma versão diferente devido aos modelos nem sempre suportarem a mesma quantidade e/ou tipo de interfaces ou utilizarem processadores diferentes, portanto a Cisco precisava compilar diferentes versões de imagens de IOS para os diferentes tipos de processadores.

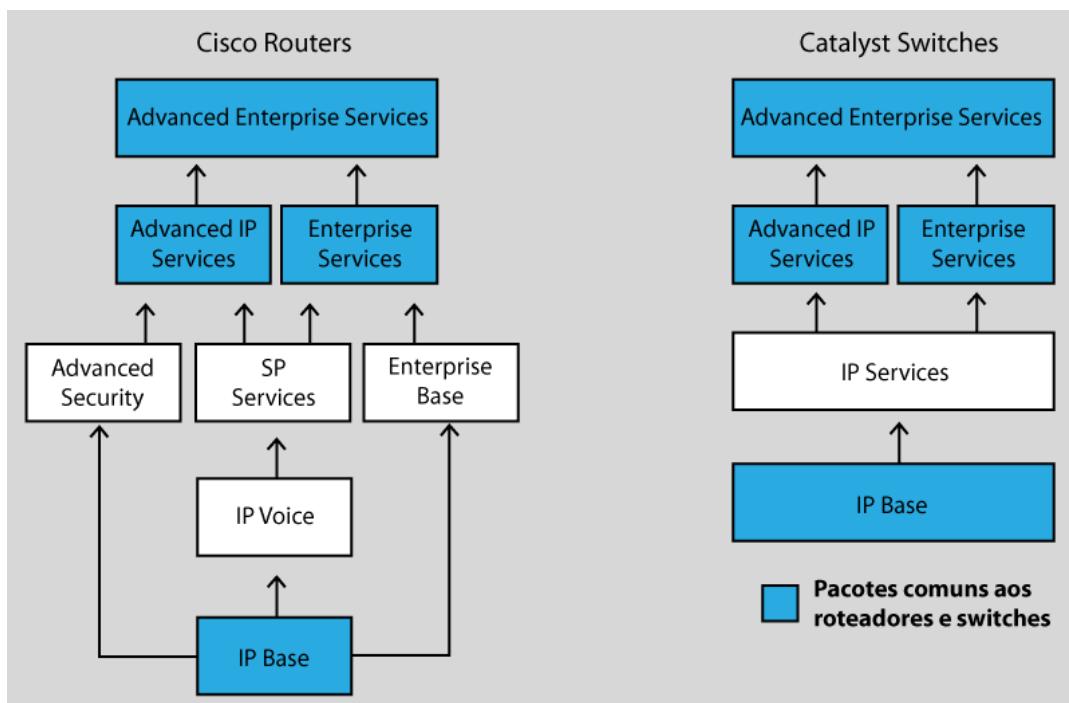
Além disso, a Cisco precisava de imagens de IOS diferentes para cada nova versão ou release de software. Uma revisão significativa (major revisions) no software Cisco IOS utilizava o termo versão (version), enquanto mudanças menores recebiam a denominação de release.

Por exemplo, ao invés da Cisco lançar um bug fix ou novo recurso como um patch, essas correções eram lançadas em arquivos de IOS separados, ou seja, em uma nova release da mesma versão de IOS ou até uma nova versão, portanto, para implantar aquela correção de problemas ou recurso adicional de software era necessário trocar o software inteiro e inserir um novo Cisco IOS no roteador. Veja figura abaixo.



Isso era feito por equipamento, modelo e lista de recursos (feature set).

Cada versão de IOS possuía listas de recursos chamadas feature set, por exemplo, os roteadores saíam com uma feature set básica chamada IP Base, com suporte a determinados recursos de software. Se a empresa precisava ativar recursos de segurança precisaria comprar outra versão de IOS com a feature set de segurança, por exemplo, para suportar a implantação de um firewall CBAC. Veja a seguir uma ilustração com as opções de feature set suportadas nas versões 12.3 e 12.4 do Cisco IOS.



Para cada item no fluxograma temos recursos específicos que vão se somando até chegar a uma versão completa chamada "Advanced Enterprise Services", o qual tem também um custo mais alto. Portanto para a Cisco lançar uma versão nova de IOS era preciso lançar pelo menos oito imagens de IOS nesse modelo, uma para cada lista de recursos desejada.

Cada pacote tem um nome específico com uma lista de recursos (features) disponíveis, segue uma descrição resumida de cada pacote abaixo (nomes válidos a partir da versão 12.3):

- **IP Base:** Imagem de IOS padrão dos roteadores com recursos básicos do protocolo IP.
- **IP Voice:** IOS para recursos de Voz e Dados (VoIP, VoFR e Telefonia IP).
- **Advanced Security:** IOS com recursos de segurança e VPN, incluindo Cisco IOS Firewall, IDS/IPS, IPSec, 3DES e VPN.
- **SP Services:** Adiciona recursos para Service Providers como SSH/SSL, ATM, VoATM, e MPLS.
- **Enterprise Base:** Protocolos básicos para empresas, porém com mais recursos que o IP Base.
- **Advanced IP Services:** IOS com todos os recursos (features) do Cisco IOS Software.
- **Enterprise Services:** Possuem os recursos do Enterprise Base, suporte IBM completa e serviços para provedores.
- **SP Services:** Recursos para empresas de Telecom como MPLS, ATM e VoATM.

No início do IOS versão 15 para os roteadores ISR-G1 (800, 1800, 2800 e 2900) foi seguido o modelo de pacotes utilizado nas versões anteriores, porém essa filosofia de pacotes mudou para um modelo de **licenciamento** com a entrada dos roteadores ISR-G2 (800, 1900, 2900 e 3900).

O nome desse processo de agrupamento de recursos em pacotes se chama IOS Packing.

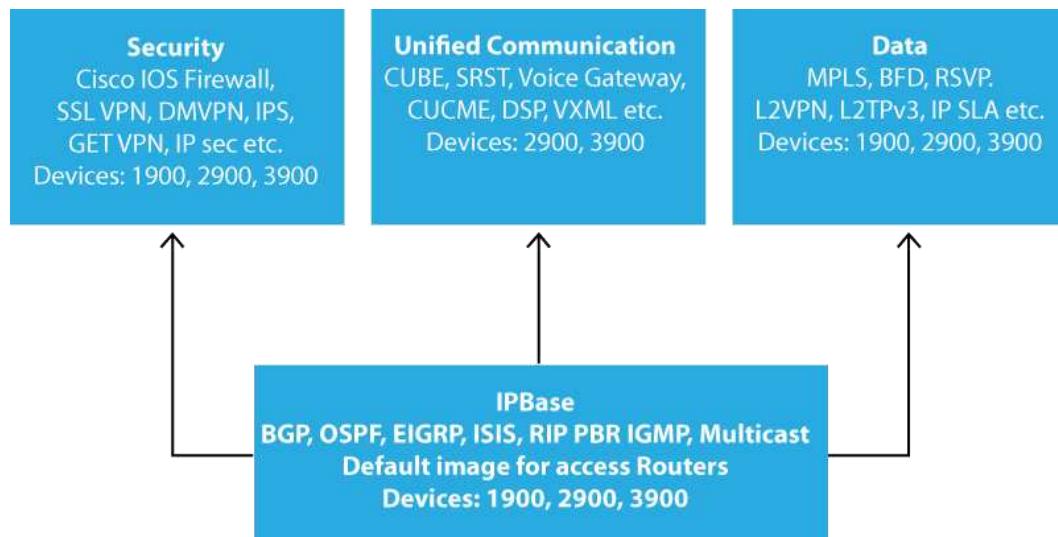
#### 4.2 Novo modelo de Cisco IOS Packing – Imagem Universal

A grande diferença com a entrada da família ISR-G2 é que ao invés da Cisco desenvolver várias imagens de IOS para diferentes feature sets, todas as feature sets estão integradas em uma mesma imagem chamada de Universal, sendo que a liberação dos recursos se dá através de um processo de licenciamento.

Portanto na versão 15 do Cisco IOS existe uma imagem única chamada de **Universal Image**, a qual possui os recursos (features) similares ao **IP Base**, ou seja, apenas recursos básicos do protocolo IP estão liberados para uso.

A diferença da versão 15 para as versões anteriores é que agora foi introduzido o conceito de licenças para liberar features avançadas (recursos de software mais avançados).

Existem licenças para recursos de Segurança (**Security**), Comunicações Unificadas (**Unified Communications** ou **Voice** – VoIP e telefonia IP) e Dados (**Data**), conforme mostrado na figura a seguir.



No Cisco IOS esses recursos ou packings são chamados de:

- **ipbasek9** (IP Base ou licença básica): funcionalidades básicas do Cisco IOS.
- **datak9** (Data ou dados): suporta recursos como MPLS, ATM, multiprotocolos e suporte a IBM.
- **uck9** (Unified Communications ou Voz): suporta recursos de VoIP e Telfonia IP.
- **securityk9** (Security ou segurança): suporta recursos de segurança tais como IOS firewall, IPS, 3DES e VPN.

Portanto, para ter recursos de voz não será necessário instalar uma nova versão de IOS como a IP Voice da versão 12.4, por exemplo. Ao invés disso, será preciso apenas liberar uma licença para ativar os recursos de voz (Unified Communications) no roteador em questão.

Então quantas versões de imagens de IOS a Cisco precisaria lançar no modelo anterior para um mesmo equipamento? Várias, uma para cada combinação de recursos (feature set) necessária. Já para a nova versão de IOS Packing é lançada apenas uma versão que contempla todos os recursos para cada modelo de equipamento e release de software, precisando de licenciamento para liberação dos recursos mais avançados.

Com o comando `show version` nos roteadores ISR-G2 podemos verificar o estado geral do licenciamento, veja exemplo abaixo.

```
Router#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.0(1)M4,
### Saídas omitidas propositalmente ##

Technology Package License Information for Module:'c1900'

-----
Technology      Technology-package      Technology-package
                Current          Type           Next reboot
-----
ipbase         ipbasek9            Permanent       ipbasek9
security       securityk9          Evaluation     securityk9
data           datak9              Evaluation     datak9

### Saídas omitidas propositalmente ##
```

Note que o roteador em questão é um Cisco 1941, o qual não tem suporte a recursos de Voz, por isso são listadas as tecnologias ipbasek9, securityk9 e datak9, sendo que a primeira é uma possui uma licença permanente e as duas últimas são apenas de avaliação, precisando de uma chave válida para ser registrada permanentemente.

#### 4.3 Introdução a Ativação de Software com Imagem Universal

A ideia por trás do licenciamento de IOS introduzido para a linha de roteadores ISR-G2 (1900/2900/3900) é simples, pois para utilizar “**feature sets**” ou recursos de software que já estão presentes na imagem universal é preciso destravar (unlock) a feature set utilizando um **processo de ativação de software** definido pela Cisco.

Esse processo de ativação de software tem dois objetivos principais:

1. **Habilitar recursos** (Enable): habilitar ou ativar as features no roteador, pois sem essa ativação de software somente os recursos básicos irão funcionar, ou seja, features avançadas e seus comandos não serão reconhecidos pela CLI.
2. **Verificar direitos legais**: com esse processo a Cisco valida se o cliente final realmente pagou pelo direito de utilizar aquela feature set no roteador onde ela está sendo ativada.

Vamos lembrar que no Cisco IOS esses recursos (feature sets ou packings) podem ser:

- **ipbasek9** (IP Base): funcionalidades básicas do Cisco IOS e base para ativação das demais feature sets ou tecnologias.
- **datak9** (Data): suporta recursos como MPLS, ATM, multiprotocolos e suporte a IBM.
- **uck9** (Unified Communications): suporta recursos de VoIP e Telefonia IP.
- **securityk9** (Security): suporta recursos de segurança tais como IOS firewall, IPS, IPsec, 3DES e VPN.

Podemos ativar as licenças manualmente ou utilizando o Cisco License Manager (CLM). Uma alternativa diferente para o licenciamento é quando compramos um roteador e as licenças são instaladas na própria fábrica, não sendo necessário nenhum trabalho por parte do administrador de redes para sua ativação.

#### 4.3.1 Ativando Licenças Manualmente

O processo de ativação manual necessita que você utilize um navegador de internet, conecte-se com o site “Cisco Product License Registration Portal” (parte do sítio de Internet Cisco.com) e também utilize alguns comandos via CLI no roteador ater licenças ativadas.

Vamos abaixo ver o processo passo a passo para juntar todas as peças e fazer o licenciamento para liberação de recursos de software no Cisco IOS em equipamentos da linha ISR-G2.

**Passo 1:** No site do Cisco Product License Registration Portal ([www.cisco.com/go/license](http://www.cisco.com/go/license)) você deve entrar com o **UDI** (unique device identifier) do roteador se necessário. A informação é obtida com o comando **show license udi**, veja exemplo abaixo.

```
Router#show license udi
Device#   PID          SN           UDI
-----
*0        CISCO1941/K9    FTX150800UX  CISCO1941/K9:FTX150800UX
```

**Passo 2:** Na mesma página digite o **PAK** para a licença comprada, serial que deve ter sido fornecido pela Cisco ou pela revenda que forneceu o roteador.

O **Product Authorization Key** ou **PAK** é uma espécie de recibo que contém um número único gerado pela Cisco com a finalidade de confirmar em um banco de dados que aquela licença de feature set realmente foi comprada. Com o UDI e o PAK será gerado pelo site de licenciamento citado no passo 1 uma chave única de ativação que você deverá utilizar para liberação da ou das feature sets adquiridas.

Pode ser que o processo de ativação na prática não peça primeiro o UDI e sim o PAK.

**Passo 3:** Preencha os campos necessários solicitados após entrar com o valor do PAK e no final copie a chave da licença (license key por download ou email) quando indicado pelo Portal de Product License Registration.

**Passo 4:** Disponibilize o arquivo via USB ou através de um servidor de rede, por exemplo, um servidor TFTP.

**Passo 5:** Pela CLI do roteador digite o comando “**license install caminho-da-licença**” para instalar a licença no roteador. Veja exemplo de instalação de licença baixada para um pen-drive.

```
R1# dir usbflash0:
Directory of usbflash1:/
1 -rw- 4096 Feb 15 2013 10:10:00 FTX1628838P_201302111432454180.lic
7783804928 bytes total (7782912000 bytes free)

R1# license install usbflash0:FTX1628838P_201302111432454180.lic

Installing...Feature:datak9...Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install

R1#
Feb 11 20:05:20.786: %LICENSE-6-INSTALL: Feature datak9 1.0 was installed in this
device. UDI=CISCO1941/K9:FTX13425643P; StoreIndex=1:Primary License Storage
```

**Passo 6:** Reinicialize o roteador (comando reload).

Para verificar as licenças em um roteador podemos utilizar os comandos:

- **show license:** permite ver detalhes sobre cada feature-set disponível para ativação.
- **show license feature:** mostra um resumo do comando anterior por feature-set
- **show version:** já analisado anteriormente.

```
Router#show license
Index 1 Feature: ipbasek9
    Period left: Life time
    License Type: Permanent
    License State: Active, In Use
    License Count: Non-Counted
    License Priority: Medium
Index 2 Feature: securityk9
    Period left: 609 weeks 6 days
    Period Used: 15 weeks 0 day
    License Type: Right to use
    License State: Active, In Use
    License Count: Non-Counted
    License Priority: Low
Index 3 Feature: datak9
    Period left: 609 weeks 6 days
    Period Used: 15 weeks 0 day
    License Type: Right to use
    License State: Active, In Use
    License Count: Non-Counted
    License Priority: Low
Index 4 Feature: SSL_VPN
    Period left: Not Activated
    Period Used: 0 minute 0 second
    License Type: Evaluation
    License State: Not in Use, EULA not accepted
    License Count: 5000/0/0 (Active/In-use/Violation)
    License Priority: None
Index 5 Feature: ios-ips-update
    Period Used: 0 minute 0 second
    License Type: Evaluation
    Start Date: N/A, End Date: Dec 31 2025
    License State: Not in Use, EULA not accepted
    License Count: Non-Counted
    License Priority: None
```

```
Router#show license feature
Feature name          Enforcement  Evaluation  Subscription  Enabled
ipbasek9              no          no          no            yes
securityk9             yes         yes         no            yes
datak9                yes         yes         no            yes
SSL_VPN               yes         yes         no            no
ios-ips-update         yes         yes         yes           no
```

#### 4.3.2 Ativando Licenças Temporárias

A Cisco permite utilizar as features atualmente sem a compra de um PAK utilizando uma licença de uso ou **right-to-use license**.

Para habilitar uma right-to-use license devemos utilizar o comando “**license boot module**”, por exemplo, para ativar temporariamente os recursos de Security no roteador R1 como right-to-use license ou licença de avaliação (evaluation) utilizamos o comando:

```
Router(config)#license boot module c1900 technology-package securityk9
```

Após um reload a licença aparecerá como de avaliação e ativa, porém normalmente uma right-to-use license aparece com a mensagem “60 days left (8 weeks, 4 days)”, ou seja, ela tem 60 dias de período de avaliação. A saída continua ao longo do tempo a contar os dias de maneira decrescente até chegar a 0 dias para expirar, sendo que com as regras atuais em setembro de 2013 ele converte para um período de tempo ilimitado.

#### 4.3.3 Cisco License Manager

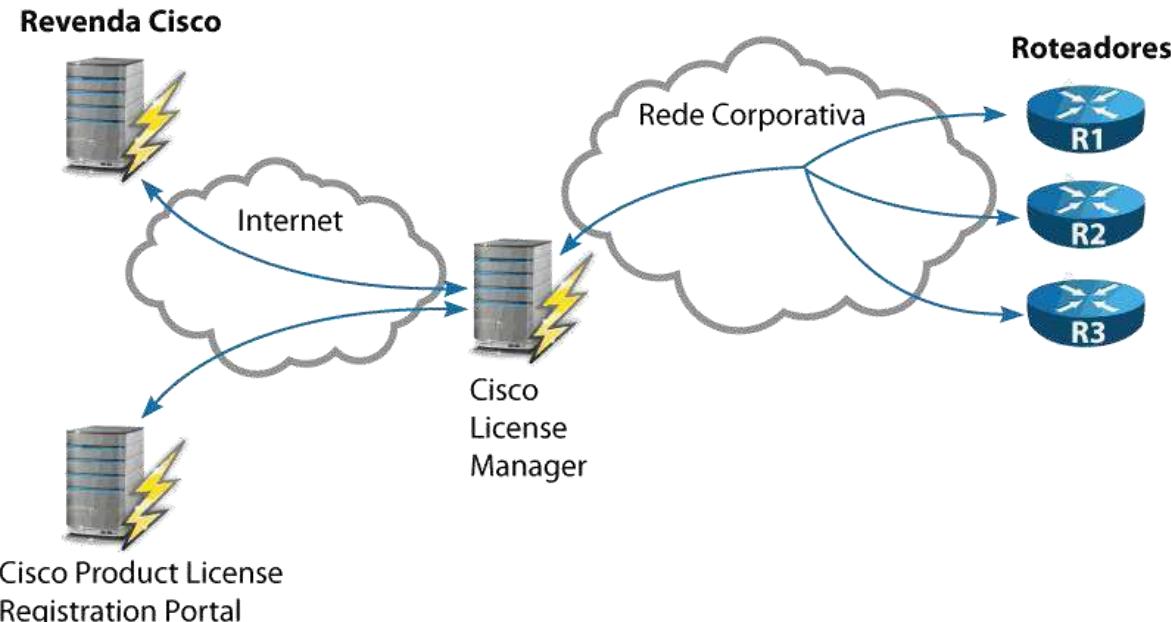
Em empresas de grande porte o gerenciamento de licenças manual pode ser um trabalho complexo e a Cisco lançou uma alternativa chamada **Cisco License Manager (CLM)** para gerenciamento do licenciamento dos seus produtos.

O CLM é um software gratuito e pode ser instalado em clientes ou servidores Windows, Sun Solaris e Linux Red Hat.

O CLM agrupa as seguintes tarefas ao seu workflow:

- Comunicação com o portal de Product License Registration via Internet.
- Como entrada utiliza informações de licenciamento obtidas a partir da revenda Cisco que forneceu os equipamentos.
- Comunica-se com os roteadores e switches da empresa Communicates e instala as licenças (license keys) ativando os recursos corretos em cada equipamento.

Portanto o CML faz tudo que fizemos manualmente nos tópicos anteriores, escondendo do administrador de redes todos aqueles passos e comandos necessários para ativação das licenças. Veja na figura abaixo uma representação da operação do CLM.



## 5 Resumo do Capítulo

Bem pessoal, chegamos ao final de mais um capítulo!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Tipos de Memórias em Roteadores e Switches Cisco
- Verificar o Hardware e Memórias dos Roteadores com o Show Version
- Processo de Inicialização dos Roteadores Cisco
- Salvar e Manipular Arquivos de Configurações
- Copiar e Manipular Arquivos de IOS
- Recuperação de IOS – Disaster Recovery
- Recuperação de Senha
- Voltar Roteadores e Switches à Configuração de Fábrica
- Ativar e configurar o Syslog
- Gerenciar o Licenciamento do Cisco IOS
- Entender as diferenças dos Packs antigos e novos do Cisco IOS
- Ativar Licenças Manualmente
- Ativar Licenças Temporárias
- Entender o funcionamento do Cisco License Manager

## 6 Conclusão

Parabéns, se você chegou até aqui é porque concluiu seus estudos!

Tenha certeza de que compreendeu todos os conceitos aqui mostrados. Dê uma repassada na matéria e tome notas dos pontos que não entendeu muito bem.

Agradecemos pela sua confiança e para quem vai fazer o exame de certificação desejamos boa sorte!

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)