DlteC do Brasil®
www.dltec.com.br
info@dltec.com.br|413045.7810

DLTEC DO BRASIL

SERVIÇOS DE REDES
(TÓPICO 4.0 DO CCNA 200-301)

Serviços de Redes

O conteúdo dessa apostila é uma adaptação da matéria online do Curso Serviços de Redes.

Para mais informação visite www.dltec.com.br

Seja muito bem-vindo(a) ao curso Curso Serviços de Redes, o qual faz parte da trilha da certificação Cisco CCNA 200-301, da Dltec!

Aqui, você terá todo o background necessário para aprender sobre Serviços de Redes em com dispositivos Cisco e também ser aprovado(a) no exame 200-301 da Cisco ao final da trilha. O exame citado anteriormente é conhecido também como exame CCNA ou Cisco Certified Network Associate.

Os assuntos encontram-se distribuídos conforme o Blueprint do exame – sendo assim, esteja bastante atento(a) a todo o conteúdo que aqui será apresentado. Não perca de vista o peso de cada tópico – isso é importante para você ter uma noção de quanto investirá o seu tempo em cada um.

Busque praticar o máximo de exercícios possíveis e, além disso, busque compreender cada assunto de maneira objetiva. Não esqueça o propósito principal: ser aprovado(a).

A DlteC estará com você em todos os momentos dessa jornada!

Bons estudos!

Introdução

Olá!

Como parte integrante da Trilha para a Certificação **CCNA 200-301** da Dltec do Brasil, esta apostila representa uma adaptação textual do material disponibilizado online do **Curso Serviços de Redes**.

O conteúdo desse curso cobre o tópico 4.0 (IP Services) da certificação Cisco CCNA 200-301.

Por isso, recomendamos que você a utilize como um importante recurso offline. Combinando-a com o conteúdo online, você estará muito mais bem preparado(a) para realizar o exame **200-301** (**CCNA**: **Cisco Certified Network Associate**).

É de suma importância que você, além de participar dos fóruns, realize o máximo possível de exercícios e simulados (todos encontrados na trilha do 200-301 Online).

Lembre-se que o curso Fundamentos de Redes Cisco é Pré-requisito para esse curso.

Esperamos que você aproveite ao máximo este material, que foi idealizado com o intuito verdadeiro de fazê-lo(a) obter êxito no exame. Estamos torcendo pelo seu sucesso!

Bons estudos!

Serviços de Redes

Peso: 10%

Objetivos

Ao final desse curso você deverá ter conhecimentos sobre:

- Configurar e verificar o NAT de maneira estática ou através de pools
- Configurar e verificar o NTP operando em modo cliente e servidor
- Explicar a função dos serviços de DHCP e DNS em uma Rede IP
- Explicar a função do protocolo SNMP na operação de uma rede IP
- Descrever o uso do syslog incluindo suas facilidades e níveis
- Configurar e verificar o DHCP cliente e relay
- Explicar o encaminhamento por salto ou "Per-hop Behavior" (PHB) para o QoS, tais como classificação, marcação, enfileiramento, congestionamento, policing e shaping
- Ativar o SSH em dispositivos Cisco
- Descrever o funcionamento e uso dos serviços de TFTP e FTP na Rede

Sumário

1 Introdução

1.1 Introdução

Bem-vindo ao **Curso Serviços de Redes**, o qual também faz parte do conteúdo preparatório para a prova de certificação **CCNA 200-301**.

O curso **Serviços de Redes** possui como objetivo fornecer ao aluno uma visão abrangente sobre os principais serviços que um CCNA precisa na administração de uma Rede IP, assim como para administrar os próprios dispositivos Cisco (routers e switches).

Ao final do curso, você deverá ser capaz de:

- Configurar e verificar o NAT de maneira estática ou através de pools
- Configurar e verificar o NTP operando em modo cliente e servidor
- Explicar a função dos serviços de DHCP e DNS em uma Rede IP
- Explicar a função do protocolo SNMP na operação de uma rede IP
- Descrever o uso do syslog incluindo suas facilidades e níveis
- Configurar e verificar o DHCP cliente e relay
- Explicar o encaminhamento por salto ou "Per-hop Behavior" (PHB) para o QoS, tais como classificação, marcação, enfileiramento, congestionamento, policing e shaping
- Ativar o SSH em dispositivos Cisco
- Descrever o funcionamento e uso dos serviços de TFTP e FTP na Rede

Mesmo que você não esteja trilhando os estudos para a certificação CCNA 200-301 você pode sim fazer esse curso para aumentar seus conhecimentos no mundo de Redes e mais especificamente sobre os serviços de redes citados na lista acima.

Mas se você está na trilha da certificação, saiba que esse curso aborda o **Tópico 4.0 ou "IP Services"**, o qual corresponde a **10% das questões do exame CCNA 200-301**.

Como a nova prova terá aproximadamente entre 100 e 120 questões, podemos dizer que **devem cair de 10 a 12 questões** relacionadas ao conteúdo desse curso, dependendo da quantidade total de questões que forem sorteadas para seu exame específico.

Não esqueça que ao final do curso você poderá emitir o seu certificado!

1.2 Sobre a Cisco e o CCNA - Cisco Certified Network Associate

A Cisco é uma empresa líder mundial em TI e redes, tendo seus produtos e tecnologias utilizadas por diversas empresas dos mais variados segmentos de mercado no mundo todo.

Fundada em 1984 por Len Bosack e Sandy Lerner atua até os dias de hoje com tecnologia de ponta e inovações que auxiliam no crescimento do mercado de TI.

A Cisco atua na área de Redes (com os famosos Roteadores e Switches), Software, Internet das Coisas, Mobilidade e Comunicação sem fio, Segurança, Colaboração (Voz e Vídeo sobre IP), Data Center, Cloud, Pequenos e Médios Negócios e Provedores de Serviço.

Para garantir que os profissionais que atuam com seus produtos e tecnologias realmente tem os conhecimentos técnicos necessários para desempenhar um bom trabalho, a Cisco desenvolveu um programa de **Certificação** com **Três Níveis** no início:

- **Associate ou CCNA (Cisco Certified Network Associate)**
- Professional ou CCNP (Cisco Certified Network Professional)
- Expert ou CCIE (Cisco Certified Internetwork Expert)

Mais especificamente falando da certificação **CCNA ou Cisco Certified Network Associate** é uma das primeiras certificações lançadas pela Indústria de Redes e com certeza a mais famosa até os dias de hoje.

A primeira versão de CCNA data de 1998 chamada de 640-407, o qual foi atualizado sete vezes até a última mudança feita em 2016 com a versão 200-125 (CCNA Routing and Switching em uma prova) e as versões do 100-105 e 200-105 (Modelo em duas provas: CCENT/ICND-1 + ICND-2).

Em **julho de 2019** foi anunciada uma grande mudança em maioria das certificações Cisco e o CCNA volta ao que era no início, sendo uma certificação unificada para diversas áreas e englobando não somente assuntos de Roteamento e Switching, mas também segurança, redes sem fio e automação de Redes.

Esse curso que você está prestes a iniciar faz parte da nossa trilha para a certificação **CCNA 200-301**.

O que se espera de um CCNA no mercado de trabalho?

Um profissional certificado CCNA deve conhecer uma larga gama de tecnologias e configurações de diversos equipamentos Cisco, tais como Roteadores, Switches, Access Points e Wireless LAN Controllers.

Além disso, deve estar preparado para a nova geração da Infraestrutura de TI, a qual a automação e programabilidade será cada vez mais utilizada.

Não confunda programabilidade com a necessidade de ser um programador, pois um profissional CCNA no mercado faz a operação e manutenção da Rede, não necessariamente precisará ser um programador e sim entender como utilizar algumas ferramentas e interagir com APIs.

É o primeiro passo de uma carreira promissora e que tem muitas possibilidades de crescimento nas mais diversas áreas de tecnologia de rede.

A seguir vamos falar sobre como a preparação para o **CCNA** está dividida no **Portal da DlteC** e como você deverá utilizar nosso material para conquistar sua certificação.

1.3 Plano de Estudos para o CCNA

Nesse novo modelo de prova existe apenas um caminho para obtenção da certificação CCNA que é através do exame 200-301, ou seja, não existe mais opção em duas provas como na versão anterior.

O **plano de estudos** para você ter sucesso na **CCNA** é o seguinte:

1. Ativar a trilha do curso **CCNA 200-301** no Menu Cursos (somente se você ainda não ativou)
2. Estudar o conteúdo de cada Capítulo dentro da trilha (sequência de capítulos/cursos express a seguir)
3. Repetir os comandos e demonstrações práticas realizadas pelo Prof. Marcelo durante as vídeo aulas como laboratório
4. Fazer os simulados que estão dentro do curso "**CCNA 200-301**"
5. A qualquer momento tirar as dúvidas do conteúdo utilizando os fóruns correspondentes de cada capítulo (*)
6. Passar para o próximo capítulo
7. Realizar a prova Final para treinar e obter o certificado do curso CCNA 200-301 (média da aprovação igual ou acima a 70 pontos em um total de 100)
8. Fazer o preparatório Final com laboratórios e questionários (em inglês) específicos para a certificação
9. Agendar a prova e realizá-la

O exame CCNA 200-301 é composto por uma prova em computador que pode ter de 100 a 120 questões (depende do sorteio que é feito por candidato).

Essas questões devem ser resolvidas em 120 minutos no dia do exame.

Cada um dos capítulos do curso um **Peso** associado na prova e quanto maior o peso, maior será a quantidade de questões desse assunto no exame, sendo que seguimos as recomendações da Cisco na divisão de questões para que você treine em um ambiente o mais real possível.

Para ser aprovado(a), você deverá conseguir obter entre 800 e 850 pontos de um máximo 1000 pontos no exame.

Se você ativou esse curso com o objetivo de tirar a certificação então a partir de agora, foco total no objetivo: **OBTER A CERTIFICAÇÃO.**

Você será aprovado(a) – já coloque isso "na cabeça".

Para isso, pratique os comandos, leia os tópicos com cautela e, de preferência, marque logo o dia do seu exame (para você já ter uma data limite).

Faça o seu cronograma, estipule as horas de estudo e, sinceramente, não tem erro.

Repita essa frase todos os dias: **Eu serei aprovado(a).**

Se você assumir esse compromisso com sinceridade e vontade de vencer, tudo **dará certo**.

Estamos ao seu lado! Bons estudos!

(*) Os fóruns do curso são exclusivos para TIRAR AS DÚVIDAS DO CURSO, caso você tenha dúvidas do dia a dia ou que não tenham correlação com o curso utilize os grupos do Facebook ou Telegram para troca de ideias.

1.4 Como Estudar com o Material da DlteC

Nesse curso você terá **vídeo aulas**, **material de leitura** e **laboratórios em simuladores** para o aprendizado do conteúdo.

Posso somente ler ou assistir aos vídeos? NÃO RECOMENDAMOS!

O ideal é você assistir aos vídeos e na sequência ler os conteúdos ou...

... se preferir leia os conteúdos e depois assistia aos vídeos, tanto faz.

POR QUE LER E ASSISTIR?

Simples, porque **um conteúdo complementa o outro**. Principalmente se você está se preparando para a prova de certificação é crucial que você tanto veja os vídeos como a matéria de leitura!

Os questionários ou simulados com questões de prova estão dentro da estrutura da trilha do CCNA 200-301.

Siga a sequência sugerida no plano de estudos e **faça os questionários apenas depois** de ter lido, assistido aos vídeos e feito os laboratórios em simulador. Assim você terá um aproveitamento muito melhor do curso.

2 Tópicos do Curso vs Blueprint do CCNA 200-310 – Peso 10%

2.1 Introdução

Na tabela abaixo seguem os itens do blueprint ou conteúdo do exame Cisco CCNA 200-301 relacionados ao conteúdo do curso. Os capítulos que não aparecem explicitamente aqui fazem parte da matéria e complementam o aprendizado. Estude TODO o conteúdo do curso.

IP Services	
Serviços de Rede	**Capítulos do Curso**
4.1 Configure and verify inside source NAT using static and pools	Configurando e Verificando o NAT
4.2 Configure and verify NTP operating in a client and server mode	Configurando e Verificando o NTP
4.3 Explain the role of DHCP and DNS within the network	"Visão Geral do DNS em Redes IP" + "Configurando e Verificando o DHCP"
4.4 Explain the function of SNMP in network operations	Uso do SNMP e Syslog em Redes IP
4.5 Describe the use of syslog features including facilities and levels	Uso do SNMP e Syslog em Redes IP
4.6 Configure and verify DHCP client and relay	Configurando e Verificando o DHCP
4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping	Conceitos de QoS e Per-hop Behavior (PHB)
4.8 Configure network devices for remote access using SSH	Configurando o Acesso Remoto via SSH
4.9 Describe the capabilities and function of TFTP/FTP in the network	Uso do TFTP e FTP em Redes IP

3 Configurando e Verificando o NAT

3.1 Introdução

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 aumentar a segurança da rede interna das empresas.

Veja figura abaixo.

Com a RFC 1918 (estudada no curso Fundamentos de Redes Cisco) 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 ou privativos**.

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.

3.2 Visão Geral do NAT e PAT

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).

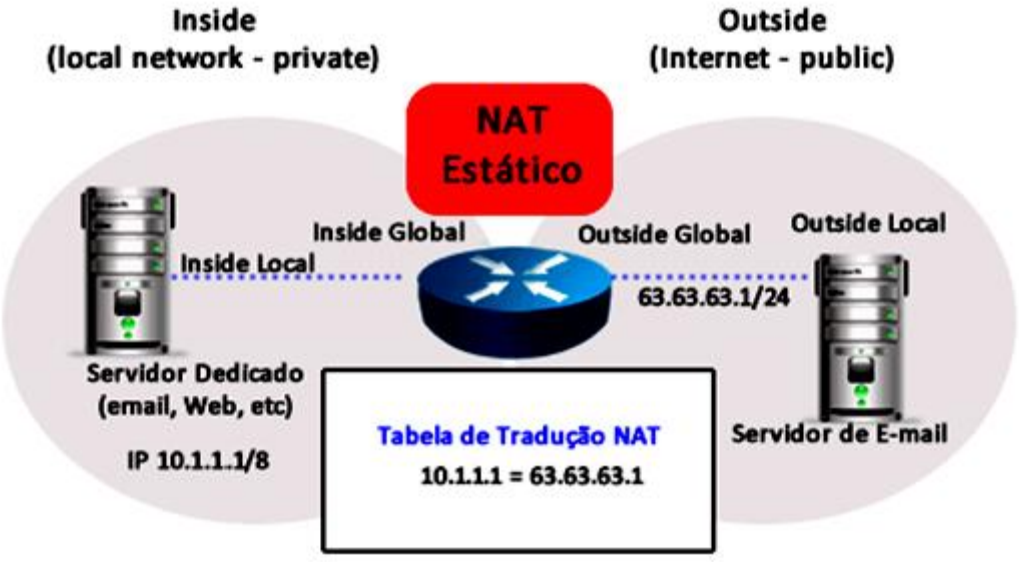
O NAT e o PAT podem ser implementados de três maneiras:

- **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.
- **Overloading**: Nessa opção o roteador NAT utiliza tanto o endereço IP como as portas TCP ou UDP para realizar a tradução do pacote.

As traduções estáticas são recomendadas para oferecer serviços na rede interna, por exemplo, quando um servidor ou dispositivo de rede 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 a seguir.



O **NAT dinâmico** foi projetado para mapear um endereço IP privado para um endereço público.

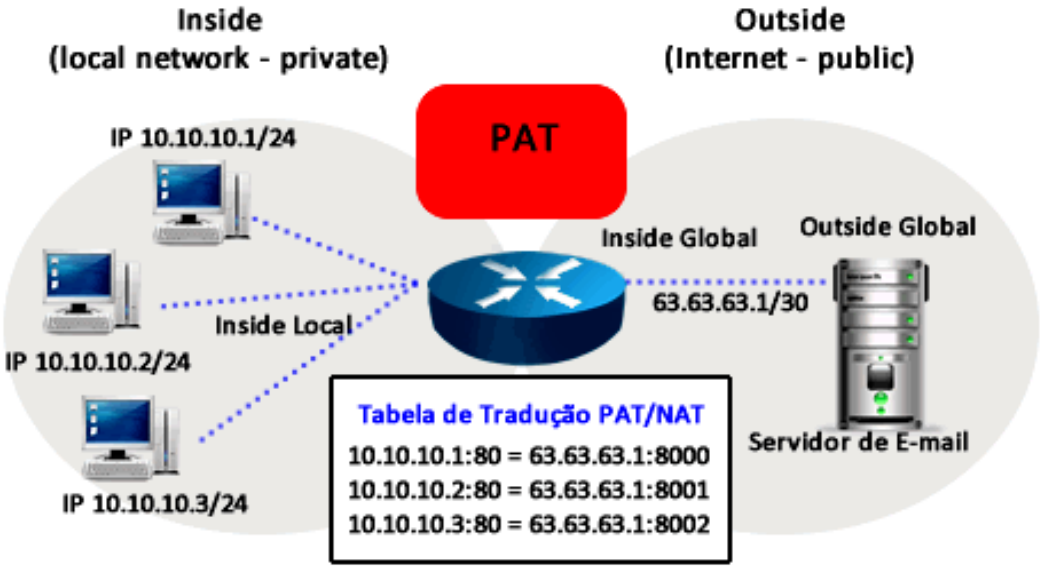
Qualquer endereço IP de um pool de endereços IP públicos pode ser atribuído a um host da rede.

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.

3.3 Terminologia do NAT no Cisco IOS

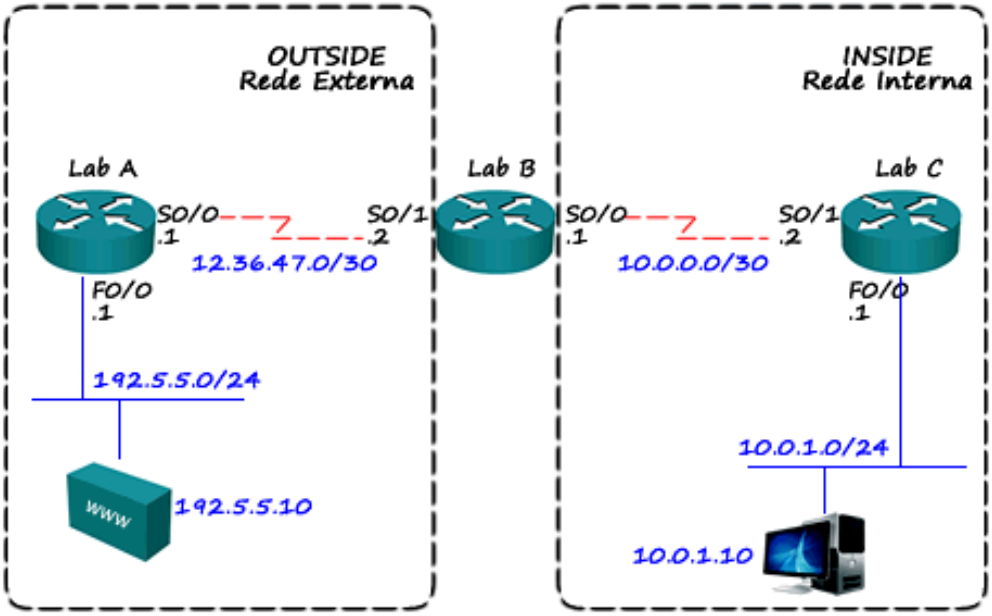
No IOS da Cisco alguns termos são definidos para configuração e melhor compreensão do NAT e do PAT:

- **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 anterior 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	192.5.5.10	192.5.5.10

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.

3.4 Configurando o NAT

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!

3.4.1 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
```

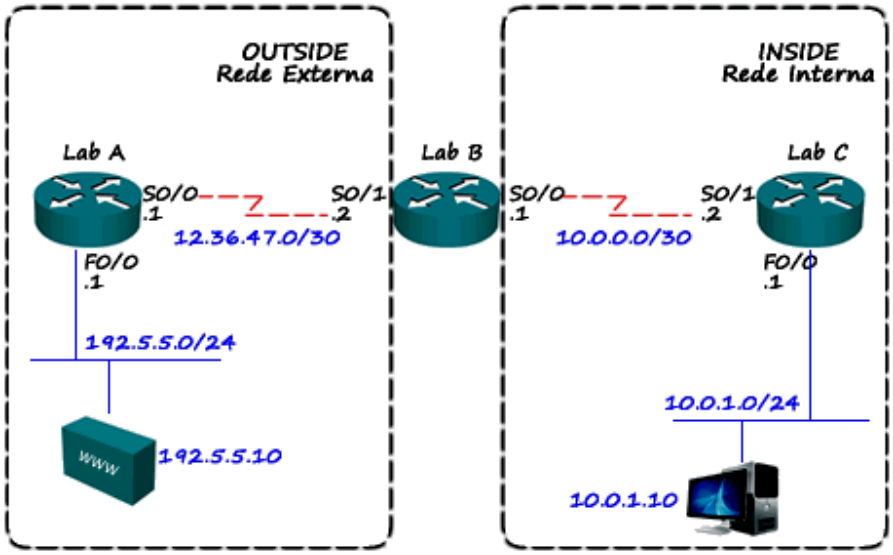
O parâmetro "**source static**" define que você utilizará o NAT estático. O parâmetro "**local-ip**" é o IP privado interno a ser traduzido e o "**global-ip**" é o IP externo que servirá de interface com a Internet.

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.

3.4.2 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 sub-rede 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 computadors da rede interna poderiam acessar a 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**.

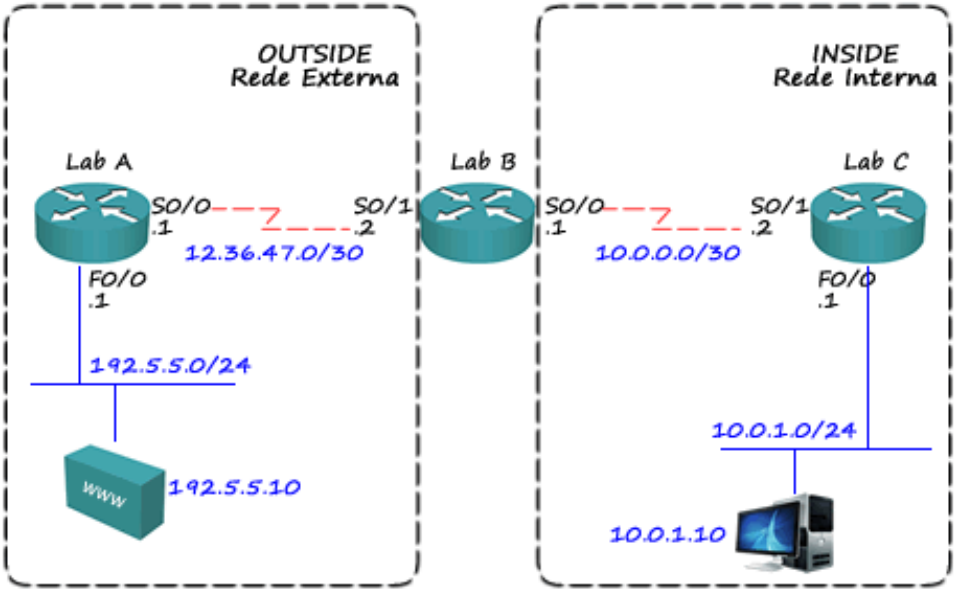
4) Defina a interface interna por onde o IP a ser traduzido acessa a rede externa (**inside**):

```
Router(config-if)#ip nat inside
```

5) Defina a interface que se conecta a externa (**outside**):

```
Router(config-if)#ip nat outside
```

A 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.

3.4.3 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.

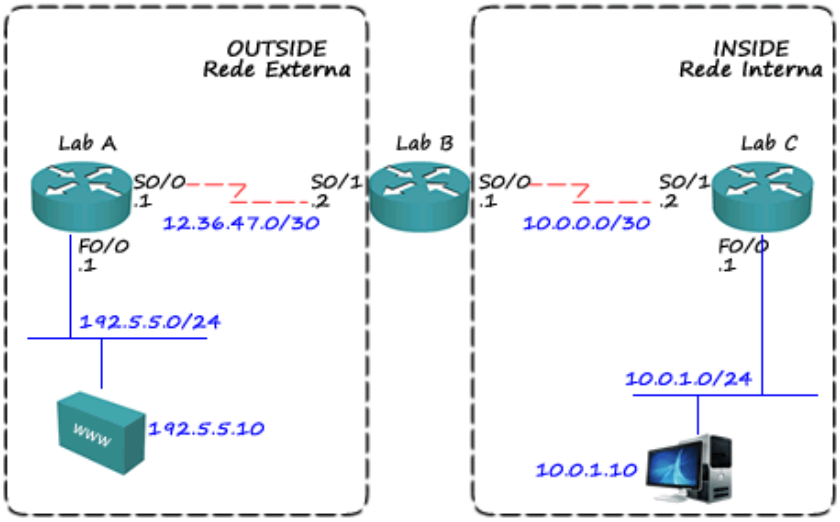
3) Defina a interface interna por onde o IP a ser traduzido acessa a rede externa (inside):

```
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
```

3.4.4 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 Poll 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.

```
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 de 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 e Verificando o NTP

4.1 Introdução

Devemos **assegurar** que todos os dispositivos Cisco (telefones, roteadores e switches) estejam com as informações de data/hora sincronizadas.

Para essa função 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 2020 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 dos 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**).

Utilizando o **protocolo NTP** você terá uma informação de data/hora mais precisa e irá garantir que todos os dispositivos fiquem sincronizados, ou seja, com a mesma informação de data/hora.

O NTP é trafegado em UDP na porta 123.

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.

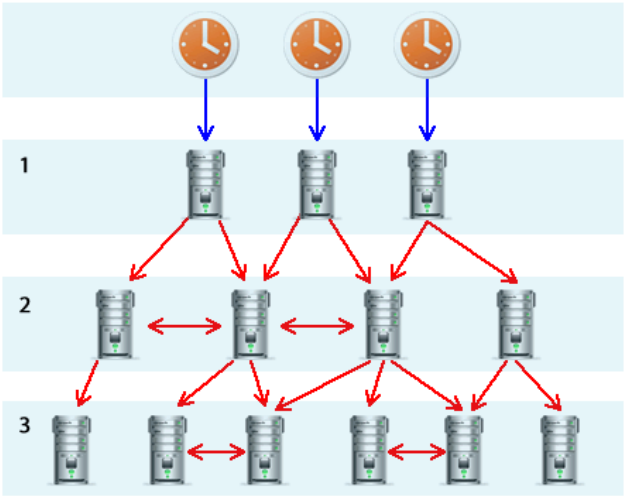
O NTP é então, simultaneamente, servidor (fornece o tempo) e cliente (consulta o tempo), formando uma topologia em árvore.

Na Internet você pode encontrar diversos servidores públicos estratos 2 ou 3 (e até mesmo alguns estrato 1) para utilizar.

Podemos dizer que o estrato ou "stratum" é a distância entre o dispositivo e a fonte de tempo confiável, isso vai ficar claro na figura a seguir.

Uma lista dos servidores NTP disponíveis na Internet pode ser encontrada clicando aqui: servidores NTP (http://support.ntp.org/bin/view/Servers/WebHome)

Veja a seguir uma figura representando a hierarquia dos servidores NTP.



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.

Vamos a seguir estudar as opções de configuração, tanto manuais como via NTP.

4.2 Configurando o Timezone: Fuso Horário

Dois parâmetros importantes na configuração relacionado a Data e Hora são o **Timezone** (**fuso horário**) e Clock Summer Time (horário de verão), porém vamos iniciar pelo fuso horário.

Caso o timezone não seja configurado o roteador irá exibir a hora tendo como referência o timezone UTC 0, por isso mesmo essa deve ser a configuração inicial quando falamos de relógio do sistema.

Você pode verificar o fuso com o comando show clock:

```
R1#sho clock
.14:51:08.653 UTC Thu Aug 13 2020
```

Note que o roteador R1 da saída anterior está utilizando o UTC ou "UTC 0" como padrão, pois ele não teve sua configuração alterada em relação ao padrão.

Aqui no Brasil, estamos no timezone UTC -3, ou seja, com 3 horas a menos que o UTC 0, pois esse é o nosso fuso horário conforme horário de Brasília. Dependendo da região do país esse valor pode variar, pois temos no total quatro fusos horários:

1. Fernando de Noronha Standard Time (GMT-2)
2. Brasilia Standard Time (GMT-3)
3. Amazon Standard Time (GMT-4)
4. Acre Standard Time (GMT-5)

Configurar o timezone em um roteador Cisco é bem simples, veja o comando abaixo.

```
dltec#configure terminal
dltec (config)#clock timezone BRA -3 0
```

A sintaxe do comando é "clock timezone *nome-da-timezone offset*", onde nome-da-timezone pode ser qualquer nome e o offset é offset do seu timezone em relação ao UTC 0.

No nosso exemplo, criamos o timezone com o nome BRA e com 3 horas de diferença ao UTC.

DICA: Se você configurar o relógio do roteador antes de definir o fuso horário, ao inserir esse comando ele ficará com 3 horas a menos em relação à configuração que você realizar, por isso o primeiro passo deve ser a configuração do fuso!

4.3 Configurando o Horário de Verão (Summer-time)

Para configurar o horário de verão (summer time) precisamos utilizar o comando "clock summer-time". Veja exemplo a seguir.

```
dltec#configure terminal
dltec (config)#clock summer-time BRV recurring 3 Sun Oct 0:00 3 Sun Feb 0:00
```

Nesse exemplo criamos um **summer-time** com o nome **BRV**, recorrente (**recurring**), que inicia no terceiro (3) Domingo (Sun) de Outubro (Oct) as 00:00h (0:00) e termina no terceiro (3) domingo (Sun) de Fevereiro (Fev) as 00:00h (0:00).

Agora quando você mandar exibir o comando show clock teremos a saída abaixo:

```
dltec#show clock
12:56:49.867 BRV Tue Jan 10 202020
```

Onde pode verificar a data/hora corretamente e também que estamos utilizando o timezone BRV que criamos.

Quando vencer o período configurado no timezone BRV, por exemplo, em 20/02/2020 passaremos a utilizar o timezone BR com o offset -3.

4.4 Definindo o Relógio Interno Manualmente

O comando clock set define a data e hora manualmente e é bem simples de ser configurado, 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 2020 ?
  <cr>

DlteC-FW-GW#clock set 15:41:12 18 july 2020
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 2020
DlteC-FW-GW#
```

Você pode utilizar também a opção "detail" no comando anterior para verificar qual a fonte de sincronismo de relógio utilizada pelo dispositivo. Veja exemplo a seguir.

```
SW6#show clock detail
*11:36:01.373 BRA Thu Aug 13 2020
No time source
SW6#
```

Note que não há fonte de sincronismo configurada nesse switch utilizado no exemplo.

4.5 Configurando o Roteador como Cliente 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 e 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).

Se você for configurar mais de um servidor NTP pode também utilizar a opção "prefer" para definir o servidor principal para sincronização do relógio.

```
dltec#configure terminal
dltec (config)#ntp server a.st1.ntp.br prefer
dltec (config)#ntp server b.st1.ntp.br
```

Com a configuração acima temos dois servidores NTP configurados, porém a preferência do sincronismo será com o servidor "a.st1.ntp.br". Caso ele fique indisponível a sincronização será feita com o servidor "b.st1.ntp.br".

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.

4.6 Configurando o Roteador como Servidor NTP

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 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.

Se você não configurar a origem dos pacotes do NTP (source) ela vai ser o endereço do próximo salto do cliente conectado ao servidor.

Por exemplo, se o servidor está conectado ao cliente via fast0/0, o IP dessa interface vai ser a origem dos pacotes do NTP que o cliente vai receber, ou seja, sempre a interface mais próxima do cliente.

4.7 Configurando Clientes NTP com Autenticação

Você pode também conectar um cliente a um servidor NTP em modo seguro utilizando uma chave ou Key para realizar a autenticação com um servidor confiável (Trusted NTP Server).

Para isso é preciso definir o endereço IP do servidor NTP que suporta o modo seguro e uma chave.

Caso a chave não tenha sido criada será necessário cria-la antes de configurar os passos citados anteriormente.

Para criar a chave entre com o comando:

```
R1(config)#ntp authentication-key 1 md5 chave-segura
```

Após a configuração, se você verificar no show running-config o nome da chave aparecerá criptografado com um Hash MD5 e será algo conforme abaixo:

```
ntp authentication-key 1 md5 113B3301213D15204E160B00626818722E133E4658 7
```

Logo após defina a autenticação e a chave que será utilizada para autenticar com o servidor NTP com os comandos abaixo:

```
ntp authenticate
ntp trusted-key 1
ntp server ntp1.server.example.com key 1
```

Com a configuração acima a chave definida na chave de autenticação 1 será utilizada para fazer a autenticação com o servidor NTP "ntp1.server.example.com".

Para verificar o estado da conexão com o servidor NTP utilize os comandos show ntp status e show ntp associations, conforme já estudado nos capítulos anteriores.

5 Visão Geral do DNS em Redes IP

5.1 Introdução

O **DNS** ou **Domain Name System** (Sistema de Nomes de Domínio) é um sistema usado na Internet para converter os nomes de domínios e seus respectivos nós de rede divulgados publicamente em endereços IP.

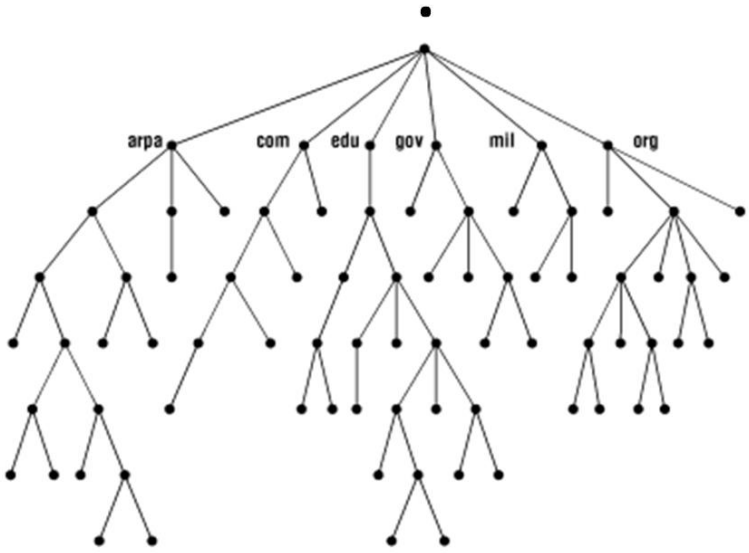
Ele é um sistema constituído por uma robusta, hierárquica e distribuída base de dados, cujo propósito é criar mapeamentos entre nomes de hosts com endereços IP (e vice versa).

Esta base utilizada pelo sistema é indexada a partir de nomes de domínios, representados por caminhos lógicos baseados em uma árvore invertida, conhecida como **Domain Name Space**.

No topo desta árvore encontramos uma única raiz (denominada **root domain**), gerenciada pela **ICANN** (Internet Corporation for Assigned Names and Numbers) e representada pelo ponto (**.**).

Com isto, os nomes de domínios são sempre lidos a partir desta raiz.

Observe na figura a seguir uma representação parcial do Domain Name Space:



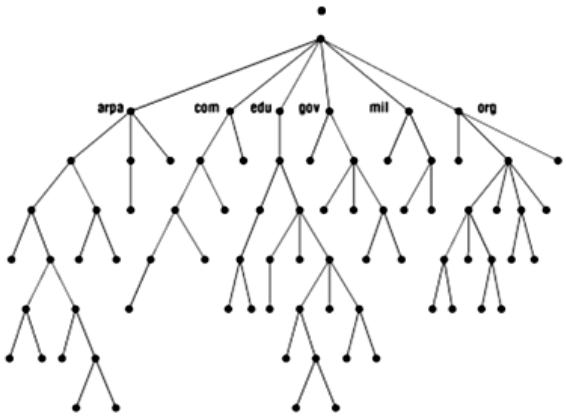
No **root domain** são encontrados diversos **root servers**, localizados em diferentes localizações do globo e classificados em 13 grandes autoridades, além disso, essa divisão é feita por questões de segurança e redundância.

Várias entradas são gravadas nos diversos servidores de DNS distribuídos pelo planeta, são milhões, bilhões de registros gravados em bases de dados distribuídas entre os diversos servidores, os quais são consultados de forma exaustiva diariamente.

A seguir você vai entender um pouco mais da hierarquia do DNS.

5.2 Domínios, TLDs e FLDs

É importante associar a ideia de "domínio" a um nome (facilmente assimilado por humanos) que possui como objetivo básico ser utilizado para disponibilizar algum recurso pela grande rede. Estes também podem ser categorizados, variando de acordo com o seu nível.



Como já vimos, tudo começa pelos servidores Raiz ou root servers representados pelo "." (ponto) no topo da árvore do DNS.

Os **Top-Level Domains** são categorizados de formas diferentes pela **IANA** (Internet Assigned Numbers Authority - entidade responsável pelo sistema de nomes globalmente).

Por exemplo, alguns daqueles considerados genéricos (gTLD - Generic Top-Level Domains) são descritos a seguir:

- **com**: utilizado principalmente por organizações comerciais.
- **edu**: utilizado por instituições de ensino superior.
- **org**: originalmente era utilizado por organizações não comerciais, mas, ainda durante a década de 1990, essa restrição foi removida.
- **net**: originalmente era utilizado por organizações relacionadas a infraestrutura de redes, mas, ainda durante a década de 1990, também se encontra disponível para ser utilizado por organizações comerciais.
- **mil**: utilizado por organizações militares.
- **gov**: Uso governamental.

A **IANA** também classifica os TLDs segundo os códigos utilizados por países – esses são conhecidos como **Country-Code TLD** (ou ccTLD).

Os caracteres utilizados para identificar os países são baseados no padrão ISO 3166. Daí entram em cena o **br** (Brasil), **fr** (França), **de** (Alemanha), **uk** (Reino Unido), **us** (Estados Unidos) dentre outros.

A gestão do **br**, por exemplo, é realizada pela associação **NIC.br** (Núcleo de Informação e Coordenação do PontoBR), criada por membros do **CGI.br** (Comitê Gestor da Internet no Brasil).

Os subdomínios diretos dos TLDs são conhecidos como **First Level Domains** (FLDs), destinados a organizações, indivíduos etc. Por exemplo, o TLD "com" possui subdomínios como "google.**com**", "globo.**com**", "redhat.**com**", "linuxmint.**com**" dentre outros.

Através do processo conhecido como **delegação de autoridade**, a gestão do FLDs poderá ser realizada pelos seus próprios mantenedores. Dito isto, a responsabilidade pela gestão do domínio "standford.edu" é delegada à própria Standford University, por exemplo.

Dentro de um FLD, o seu mantenedor poderá definir hosts a serem localizados de forma própria. Por exemplo, geralmente os servidores web são acessíveis através da definição do "host" www – ou utilizar, por exemplo, um "host" ftp para disponibilizar este serviço no domínio (como ftp.exemplo.com) etc.

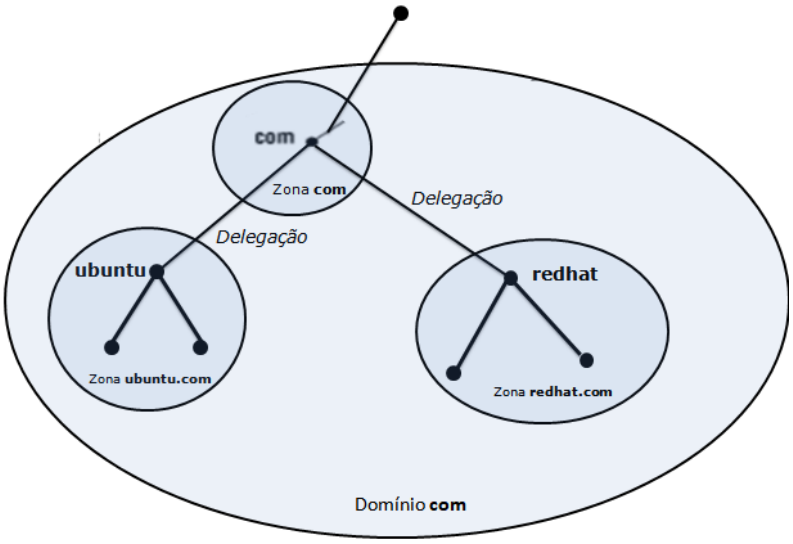
Esses serviços e servidores são definidos por diversos tipos de "entradas" no arquivo do DNS que fica gravado nos servidores. Veja alguns tipos abaixo:

- **A**: também conhecido por hostname, é o registro central de um DNS, ele vincula um domínio ou subdomínio a um endereço IPv4 direto.
- **AAAA**: registros AAAA (quad-A) executam a mesma função de A, porém, para um endereço IPv6.
- **NS**: conhecido como Name Server (Servidor de Domínio), especifica servidores DNS para o domínio ou subdomínio.
- **CNAME**: significa Canonical NAME e especifica um apelido (alias) para o hostname (A). É uma espécie de redirecionamento.
- **MX**: significa Mail eXchanger e aponta o servidor de e-mails.

Portanto, quando um cliente consulta um servidor pelo nome "www.dltec.com.br" ele está fazendo uma consulta por um registro "A" (para o endereço IPv4 do site) ou "AAAA" (para o endereço IPv6 do site).

5.3 Zonas, Nameservers e Consultas

O sistema de **DNS** pode ser subdividido em zonas diferentes. Essas zonas são partes do Domain Name Space que são gerenciadas por organizações específicas. Além disso, cada zona poderá possuir muitos domínios – da mesma forma que, no mesmo servidor de **DNS**, várias zonas poderão coexistir.



Os servidores de nomes (**nameservers**) atuantes em uma zona, conhecem todas as informações a respeito desta, já que esses detalhes são obtidos a partir de arquivos locais ou vindos a partir de outro **nameserver**. Nesse contexto, dizemos que se tratam de **nameservers autoritativos** (Authoritatives).

Veja na figura anterior que o domínio **com** possui, em seu topo, a zona de mesmo nome. Dessa forma, a gestão do subdomínio "redhat.com", por exemplo, não é de responsabilidade do **com**, mas sim da própria equipe do RedHat.

Porém, os **nameservers** atuantes no domínio **com** sabem como obter informações do "redhat.com", já que se trata de um dos seus subdomínios.

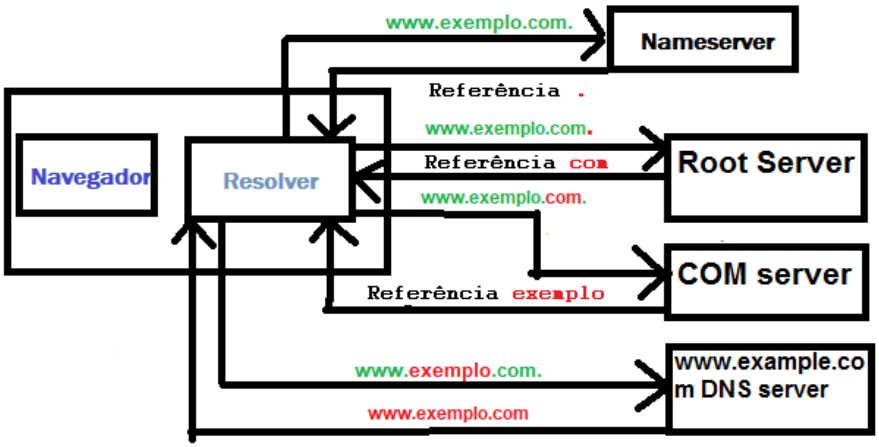
Os **nameservers autoritativos** também poderão assumir comportamentos diferentes em uma zona.

Aquele que é utilizado para armazenar os arquivos originais a respeito da zona, é identificado como **Master** (ou Primary). No processo de definição da zona neste **nameserver**, a zona também é especificada como "master". Devido a possuir os registros "master" da zona, este deverá sempre estar presente.

Já quando um **nameserver** obtém as informações sobre uma zona a partir do **Master**, dizemos que trata-se de um **nameserver Slave**. Dessa forma, esse mantém uma cópia idêntica dos dados contidos no primeiro. O processo de transferência dessas informações é conhecido Transferência entre Zonas.

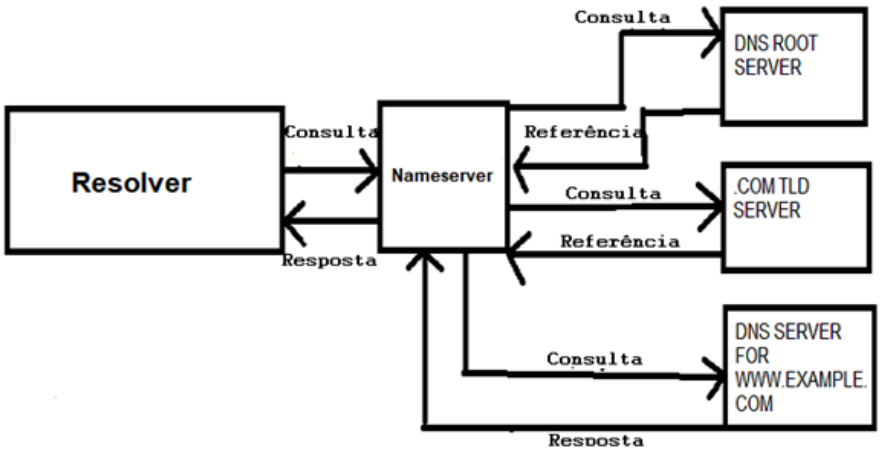
Existem variações que podem ser assumidas por um **nameserver**. Aliás, esses também se diferenciam pela forma em que manipulam as requisições de consultas que lhes são enviadas pelos resolvedores (**resolvers**) do sistema operacional.

Ao ser configurado para manipular **consultas iterativas** (ou não-recursivas) o **nameserver** não se responsabiliza por oferecer uma resposta completa à consulta do cliente – ele devolve uma referência de outros servidores de **DNS** que poderão ser usados na busca aplicada pelo **resolver** (caso o **nameserver** não possua a resposta para a pergunta, obviamente).



Um **resolver** é um programa ou rotina responsável por formular uma consulta de **DNS** (também conhecido como cliente de **DNS**).

Quando configurado para atender **consultas recursivas** o processo é inverso: o **nameserver** irá realizar todos os procedimentos até conseguir atender à requisição que lhe fora passada. Neste cenário, ele poderá até mesmo consultar os outros servidores:



Além disso, os servidores podem guardar um "cash" das consultas realizadas e responder a consultas semelhantes sem a necessidade da busca recursiva. Esse tipo de configuração acelera muito o processo de resolução de nomes.

As consultas DNS são realizadas pelos clientes através do UDP na porta 53.

5.4 Comandos Nslookup, Host e Dig

Alguns comandos oferecidos pelo Linux e Windows são bastante úteis ao trabalharmos com **DNS**. O Nslookup funciona tanto no Windows como no Linux, porém os demais mostrados aqui funcionam apenas no Linux.

O primeiro a ser destacado é o **nslookup**. Apesar de ser considerado obsoleto, ainda costuma ser utilizado para efetuar consultas aos **name servers**.

Por exemplo, se desejamos obter detalhes a respeito do domínio "centos.org", lançamos o **nslookup** da seguinte forma:

```
[root@curso8 ~]#nslookup centos.org

Server:           192.168.0.1
Address:          192.168.0.1#53

Non-authoritativeanswer:
Name:             centos.org
Address:          81.171.33.201
Name:             centos.org
Address:          81.171.33.202
Name:             centos.org
Address:          2001:4de0:aaae::201
Name:             centos.org
Address:          2001:4de0:aaae::202
```

Note que o campo Server indica o IP do servidor que foi utilizado para manipular o procedimento de consulta.

Note também que os resultados exibidos são antecedidos pela string Non-authoritativeanswer. Isto significa que o **name server** local não possui qualquer autoridade sobre o nome de domínio que lhe fora passado – as informações exibidas foram obtidas a partir de **name servers** externos.

Desta forma, podemos por exemplo informar agora ao comando **nslookup** para que use um servidor de **DNS** específico (ao contrário daquele disponível em **/etc/resolv.conf**):

```
[root@curso8 ~]#nslookup centos.org 8.8.4.4

Server:         8.8.4.4
Address:        8.8.4.4#53

Non-authoritativeanswer:
Name:   centos.org
Address: 81.171.33.201
Name:   centos.org
Address: 81.171.33.202
Name:   centos.org
Address: 2001:4de0:aaae::201
Name:   centos.org
Address: 2001:4de0:aaae::202
```

Outro comando simples porém bastante objetivo é o **host**:

```
[root@curso8 ~]#  host centos.org

centos.org hasaddress 81.171.33.201
centos.org hasaddress 81.171.33.202
centos.org has IPv6 address 2001:4de0:aaae::202
centos.org has IPv6 address 2001:4de0:aaae::201
centos.org mail ishandledby 10 mail.centos.org.
```

Note que, ao contrário do **nslookup**, por padrão o comando também exibe informações a respeito do servidor responsável por manipular e-mails no domínio especificado. Da mesma forma que o anterior, também podemos especificar um determinado servidor de **DNS** a ser consultado:

```
[root@curso8 ~]#  host centos.org 8.8.8.8

Usingdomain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

centos.org hasaddress 81.171.33.201
centos.org hasaddress 81.171.33.202
centos.org has IPv6 address 2001:4de0:aaae::201
centos.org has IPv6 address 2001:4de0:aaae::202
centos.org mail ishandledby 10 mail.centos.org.
```

Já o comando **dig** (Domain InformationGroper) é aquele que apresenta as mais diversas possibilidades de uso. Bastante flexível e robusto, o comando é um dos mais utilizados em procedimentos de troubleshooting relacionados a **DNS**:

```
[root@curso8 ~]#dig centos.org @8.4.4.4

; <<>>DiG 9.11.4-P2-RedHat-9.11.4-9.P2.el7 <<>> centos.org @8.8.4.4
;; global options: +cmd
;;Gotanswer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30874
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;udp: 512
;; QUESTION SECTION:
;centos.org.                    IN      A

;; ANSWER SECTION:
centos.org.             576     IN      A       81.171.33.202
centos.org.             576     IN      A       81.171.33.201

;; Query time: 32 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Fri Jan 17 18:50:43 -03 2020
;; MSG SIZE  rcvd: 71
```

Note que o comando exibe no campo Query time o tempo total que a consulta demorou para ser concluída, além de também informar o servidor que foi utilizado no processo.

Veja também que, através da seção Authority Section, o comando informa os nomes dos servidores que foram utilizados para oferecer respostas autoritativas a respeito do domínio que foi informado. Na seção seguinte, são exibidos os seus endereços IP.

5.5 DNS com IP versão 6

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          2620:0:1cfe: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.

5.5.1 Aspectos Práticos do DNS com IPv6

A maioria das aplicações utilizadas para prover o serviço de DNS já estão preparadas para receber consultas DNS e resolver nomes IPv6, porém não por padrão, ou seja, será necessário configuração extra para fazer o DNS escutar a porta 53 no IPv6, adicionar hosts IPv6 e se necessário configurar a consulta reversa. Para mais detalhes sobre o suporte do DNS ao IPv6 você pode consultar a RFC 3596.

Atualmente os servidores DNS já respondem com endereços IPv6 (registros AAAA) quando eles estão disponíveis para um determinado nome de domínio, pois esse é o comportamento padrão do servidor DNS, mesmo operando apenas com IPv4.

Quando o cliente recebe na resposta da consulta ambos os endereços IPv6 e IPv4 para o domínio procurado, o sistema operacional decide que protocolo usar.

Normalmente os sistemas operacionais dão preferência pelo protocolo IPv6 fazendo o fallback para o IPv4 em caso de falhas.

5.6 Roteadores e Switches Cisco como Clientes DNS

Nos roteadores e switches Cisco podemos configurar alguns parâmetros para resolução de nomes, porém sempre com os dispositivos atuando como clientes.

Por exemplo, por padrão se você entrar com um ping para um nome de domínio da Internet em um roteador ou switch Cisco verá que ele envia a solicitação de resolução de nomes em broadcast, esperando que haja um servidor DNS disponível na rede. Veja exemplo abaixo.

```
SW6#ping www.cisco.com
Translating "www.cisco.com"...domain server (255.255.255.255)
% Unrecognized host or address, or protocol not running.
```

Esse comportamento é devido ao comando padrão "ip domain-lookup". Para que os dispositivos com Cisco IOS não façam mais buscas via DNS digite o comando "no ip domain-lookup".

```
SW6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW6(config)#no ip domain-lookup
SW6(config)#end
SW6#ping www.cisco.com
Translating "www.cisco.com"
% Unrecognized host or address, or protocol not running.
```

Note que o roteador nem tenta mais traduzir o endereço IP, pois a consulta ao DNS foi desativada com o comando "no ip domain-lookup".

Porém, muitas vezes é mais fácil realizar testes utilizando um nome de domínio e para configurar um servidor DNS dentro do Cisco IOS utilize o comando "ip name-server servidor-1 serivdor-2 ...". Você pode configurar diversos endereços para ter um servidor principal e outros reservas.

Veja exemplo de configuração e teste a seguir.

```
R1(config)#ip domain-lookup
R1(config)#ip name-server 8.8.4.4 8.8.8.8
R1(config)#do ping www.cisco.com
Translating "www.cisco.com"...domain server (8.8.4.4) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 104.104.253.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms
R1(config)#
```

Note que foram configurados dois servidores DNS: 8.8.4.4 e 8.8.8.8, porém o roteador utilizou o 8.8.4.4 para a tradução de nome. Sempre o primeiro nome na lista será utilizado e caso não funcione passa para o segundo.

Por último, você pode criar entradas estáticas locais (como se configurasse o arquivo de "hosts" de um PC) no Cisco IOS utilizando o comando "ip host nome-do-host end-IP1 end-IP2...".

Veja exemplo abaixo onde vamos configurar o endereço do switch para acesso via nome. Vamos configurar o nome como "switch" e o endereço IP 192.168.1.5.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip host switch 192.168.1.5 ?
  A.B.C.D     Host IP address
  X:X:X:X::X  Host IPv6 Address
  <cr>

R1(config)#ip host switch 192.168.1.5
R1(config)#do ping switch
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1(config)#
```

Ao digitar "ping switch" o roteador utilizou o endereço IP configurado no comando para fazer a tradução local.

Lembre-se que esse comando "ip host" é local, o roteador não irá fazer traduções para outros dispositivos, essas entradas são utilizadas por ele mesmo.

6 Configurando e Verificando o DHCP

6.1 Introdução

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.

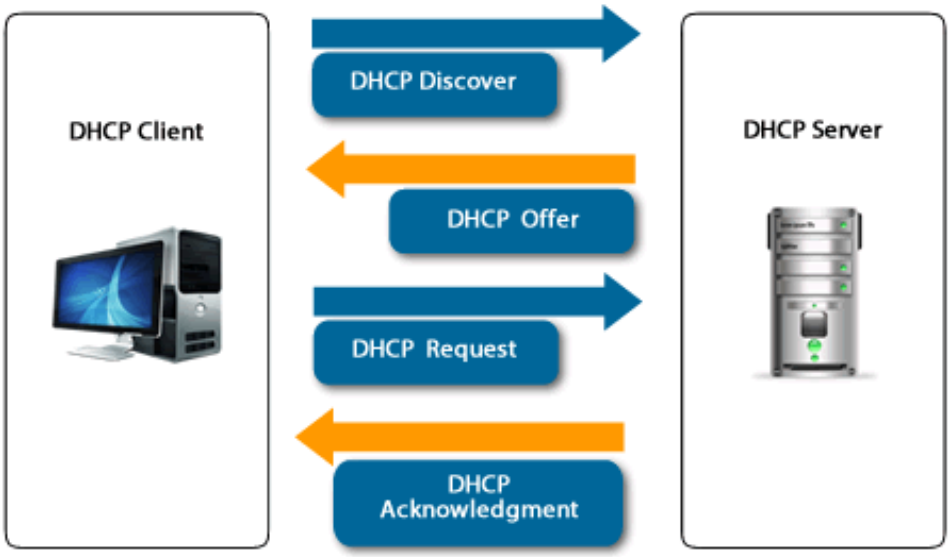
O DHCP facilita a vida do administrador de rede, pois ele pode configurar toda sua rede TCP/IP de forma centralizada a partir de um servidor.

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 reaproveitados 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 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, possibilitando que a rede tenha um servidor DHCP centralizado.

O Cisco IOS suporta as três funções:

- Servidor ou server
- Cliente ou client e
- Agente relay

A seguir vamos estudar o funcionamento do protocolo DHCP.

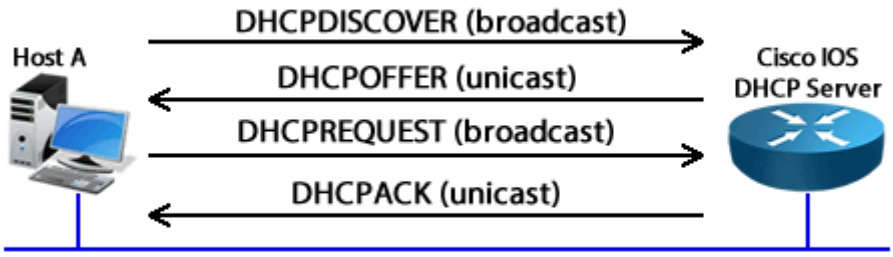
6.2 Funcionamento do DHCP

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 (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.

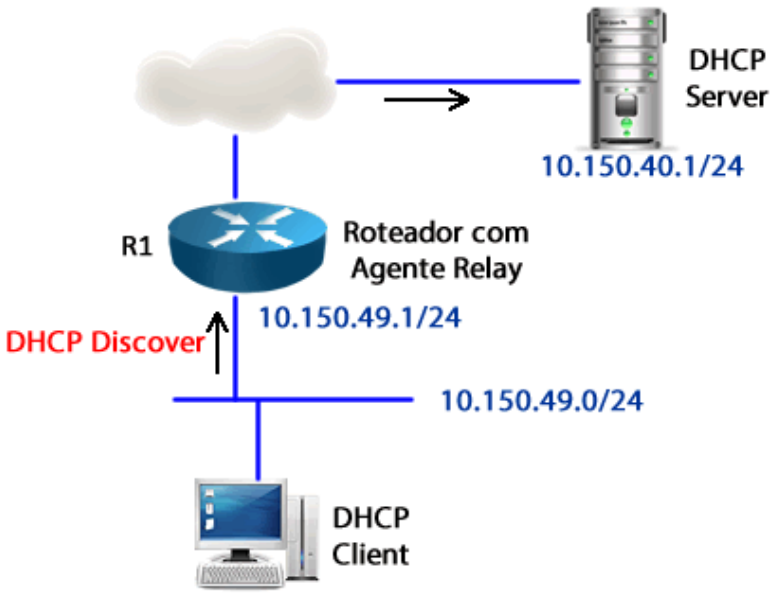
Mesmo com os testes acima se um conflito for detectado o servidor DHCP retira aquele endereço da faixa de IPs "alocáveis" e não o utiliza até que o conflito seja resolvido pelo administrador de redes.

Uma curiosidade, enquanto o cliente não tem IP configurado ele utiliza o endereço 0.0.0.0 nas mensagens DHCP.

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, conforme mostrado na imagem a seguir.



A seguir vamos começar a estudar as configurações do serviço de DHCP.

6.3 Roteadores e Switches como Clientes DHCP

Com o comando **ip address**, estudado no curso Fundamentos de Redes Cisco, traz várias opções de configuração de um IPv4 em interfaces de dispositivos Cisco.

```
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
```

Com a opção "dhcp" temos o comando "**ip address dhcp**" aplicado a uma interface L3, o roteador ou switch 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 conseguiriam mais sair para a Internet através desse roteador.
Outro ponto interessante sobre a ativação de um roteador ou switch L3 como cliente DHCP é que uma rota padrão é criada na tabela de roteamento com distância administrativa 254.

Veja exemplo de configuração a seguir.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int e0/0
Router(config-if)#ip address dhcp
Router(config-if)#no shut
*Aug 10 18:27:26.001: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Aug 10 18:27:27.001: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0,
changed state to up
Router(config-if)#end
Router#
*Aug 10 18:27:38.968: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP
address 10.0.1.2, mask 255.255.255.0, hostname Router
```

Note que o roteador informa com a mensagem "%DHCP-6-ADDRESS_ASSIGN" que a interface recebeu um IP via DHCP. Abaixo segue a confirmação do endereço com o comando show ip interface brief. Note que ele informa na opção Method que o IP está configurado via DHCP!

```
Router#sho ip int bri
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                10.0.1.2        YES DHCP   up                    up
Ethernet0/1                unassigned      YES unset  administratively down down
Ethernet0/2                unassigned      YES unset  administratively down down
Ethernet0/3                unassigned      YES unset  administratively down down
```

Com o comando show ip route podemos verificar que o roteador inseriu uma rota padrão apontando para o "Gateway" aprendido na mensagem do servidor DHCP. Note que a AD dessa rota é 254.

```
Router#show ip route
*** saídas omitidas ***
Gateway of last resort is 10.0.1.1 to network 0.0.0.0

S*    0.0.0.0/0 [254/0] via 10.0.1.1
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.1.0/24 is directly connected, Ethernet0/0
L        10.0.1.2/32 is directly connected, Ethernet0/0
Router#
```

6.4 Bônus: Configurando o DHCP Servidor no Cisco IOS

A configuração do roteador ou switch L3 como servidor não é mais obrigatória no conteúdo atual do CCNA, porém vamos fornecer como um bônus, pois você precisará dela para facilitar seus labs futuros.

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, 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
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.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".

Para monitorar a alocação de IPs pelo DHCP server em um roteador utilize o comando "**show dhcp binding**". Esse comando mostra os micros que receberam IP passado pelo servidor DHCP. Veja exemplo abaixo.

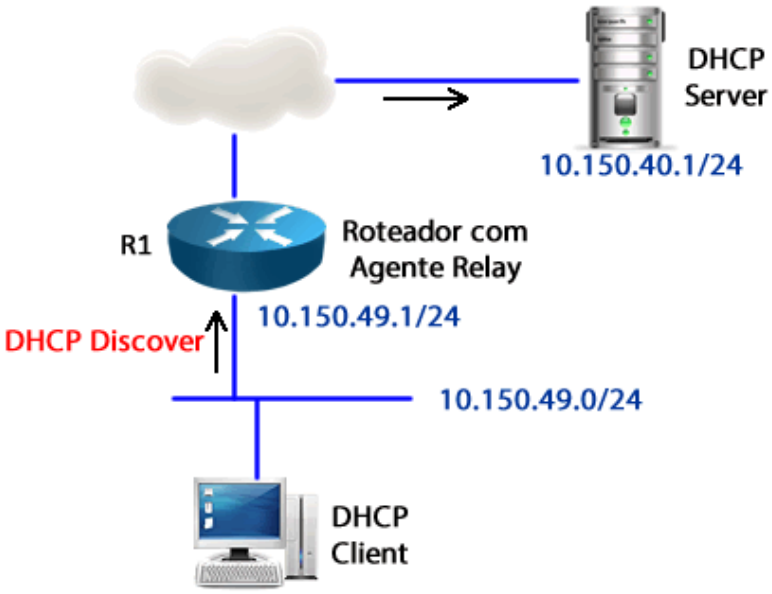
```
LAB_C#sho ip dhcp binding
IP address       Client-ID/                    Lease expiration        Type
                 Hardware address
10.0.1.2         0063.6973.636f.2d30.          Mar 02 1993 11:37 AM    Automatic
                   3030.632e.3330.3431.
                   2e66.6334.302d.566c.
                   31
10.0.1.3         0063.6973.636f.2d30.          Mar 02 1993 11:38 AM    Automatic
                  3030.632e.3330.3431.
                  2e65.6263.302d.566c.
                  31
```

No exemplo acima o roteador forneceu os IPs 10.0.1.2 e 10.0.1.3 para dois clientes.

6.5 Ativando o DHCP Relay

Nesse tópico vamos estudar a configuração do DHCP Relay para uma arquitetura DHCP Centralizada.

O relay é realizado pelos roteadores e/ou switches L3 que servem como gateway para os endpoints da Rede Local. Sua função é capturar o DHCP Request em broadcast dos clientes e criar um pacote de Unicast que será enviado pela Rede até o servidor remoto.



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 broacdast de camada 3 (255.255.255.255).

Se você estiver utilizando a topologia ROAS, no roteador esse comando deve ser inserido 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.

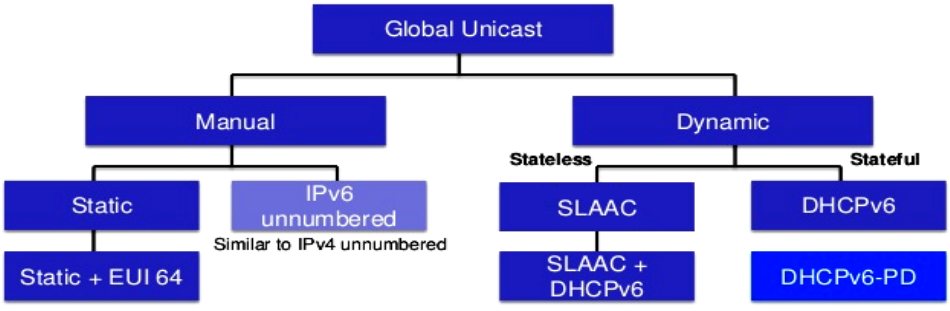
6.6 Bônus: Alocação de Endereços IPv6

Note que no blueprint ou conteúdo atual e oficial do CCNA não temos menção sobre o DHCPv6, porém não podemos deixar de falar um pouco do assunto aqui ou pelo menos relembrar de algumas coisas que já estudamos no curso Fundamentos de Redes Cisco.

Temos três tipos de endereços que são mais comuns de serem utilizados que são o de Link Local, ULA (Unique Local Address) e GUA (Global Unicast Address), sendo que o endereço de Link Local é obrigatório para as interfaces IPv6.

Normalmente não nos preocupamos com a alocação de um endereço de Link local, pois a interface se autoconfigura utilizando o EUI-64 e seu próprio endereço MAC. Apesar disso, o Link Local suporta a configuração manual ou static (estática).

Veja a figura a seguir com os tipos de alocação de endereços IPv6 mais utilizadas na prática. Nela são mostrados os endereços Globais, porém o mesmo vale para os ULAs.

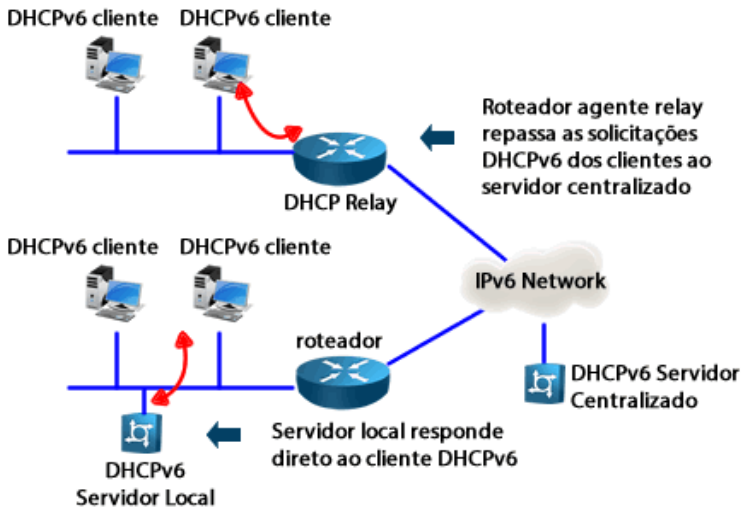


Resumindo as opções de configuração de IPv6:

- **Estático (static)**: configuração manual onde o próprio adm de redes define o IPv6.
- **SLAAC**: autoconfiguração stateless utilizando o EUI-64 ou extensão de privacidade, conforme característica de cada sistema operacional. Com essa opção o usuário recebe apenas um prefixo e seu gateway, bastante útil nos laboratórios.
- **SLAAC + DHCPv6 Stateless**: o SLAAC não passa para o usuário informações como DNS e outras opções, para isso a combinação com um servidor DHCPv6 sem estado ajuda a fornecer essas informações.
- **DHCPv6 Statefull**: a opção Statefull é similar ao DHCP do IPv4, onde o servidor passa todas as informações e registra em sua base de dados os clientes. Nas opções anteriores não há registro dos clientes da rede, pois eles mesmos se autoconfiguram. Nessa arquitetura você tem também o DHCPv6 Server, DHCPv6 Relay Agents e Clients.
- **DHCPv6-PD (prefix delegation)**: mais utilizada em ambiente de Provedores de Serviço, pois fornece um prefixo para o cliente que pode utilizar para autoconfigurar seus próprios redes IPv6.

O DHCPv6 Statefull 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.

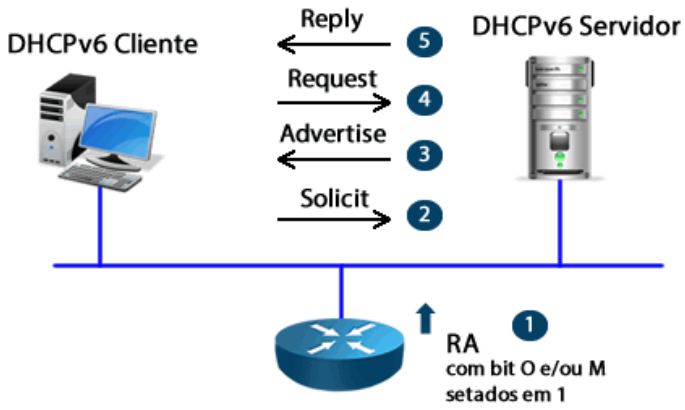


O DHCPv6 está definido na RFC3315, sendo que os clientes utilizam a porta UDP 546 e os servidores e relays escutam as mensagens DHCP na porta UDP 547.

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.



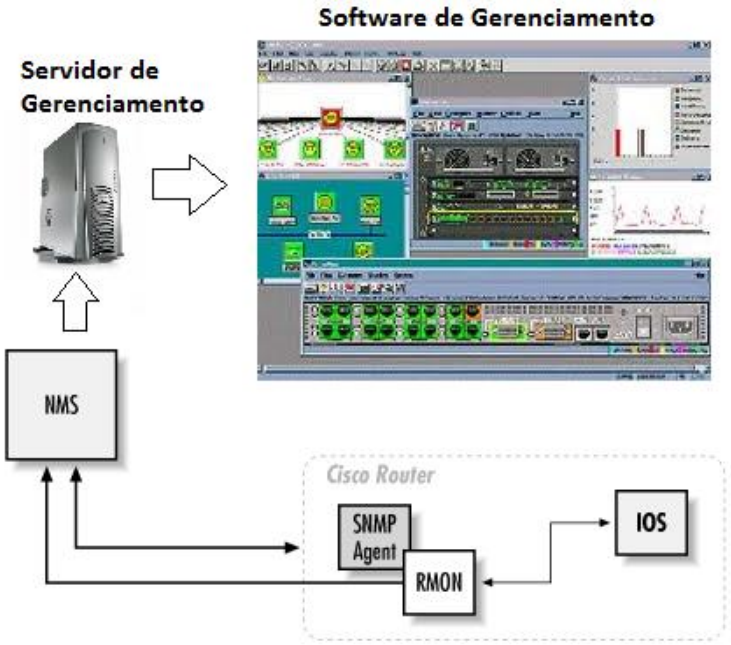
7 Uso do SNMP e Syslog em Redes IP

7.1 Introdução

Ambos os protocolos Syslog e SNMP são utilizados para monitoração e gerenciamento de Redes IP.

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.

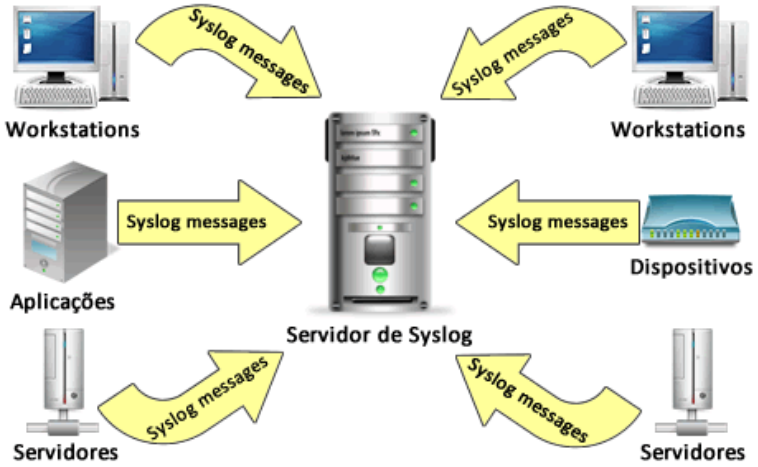


O CCNA como um todo cobra o conceito do gerenciamento de um dispositivo e da rede utilizando o **Syslog** e **SNMP**. Vamos iniciar estudando o Syslog.

7.2 Syslog

O **Syslog** é um padrão criado pela IETF para a **transmissão de mensagens de log** em redes IP, foi definido nas RFCs 5424 e 3164. Pode utilizar TCP ou UDP, porém a porta padrão é via UDP número 514.

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.

7.2.1 Ativando o Syslog

Nos roteadores e switches Cisco para habilitar o Sysylog basta utilizar o comando em modo de configuração globlal: "**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 até 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.

Outra opção de configuração é a opção "facility" que segue o padrão do Unix BSD. O padrão de configuração é o valor local7, o qual significa mensagens definidas localmente.

```
R4(config)#logging facility ?
  auth    Authorization system
  cron    Cron/at facility
  daemon  System daemons
  kern    Kernel
  local0  Local use
  local1  Local use
  local2  Local use
  local3  Local use
  local4  Local use
  local5  Local use
  local6  Local use
  local7  Local use
  lpr     Line printer system
  mail    Mail system
```

```
news     USENET news
sys10    System use
sys11    System use
sys12    System use
sys13    System use
sys14    System use
sys9     System use
syslog   Syslog itself
user     User process
uucp     Unix-to-Unix copy system
```

Vamos estudar onde esses valores são mostrados quando analisarmos o formato das mensagens de log posteriormente.

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 buffered** → 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, pois é uma ferramenta útil.

7.2.2 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

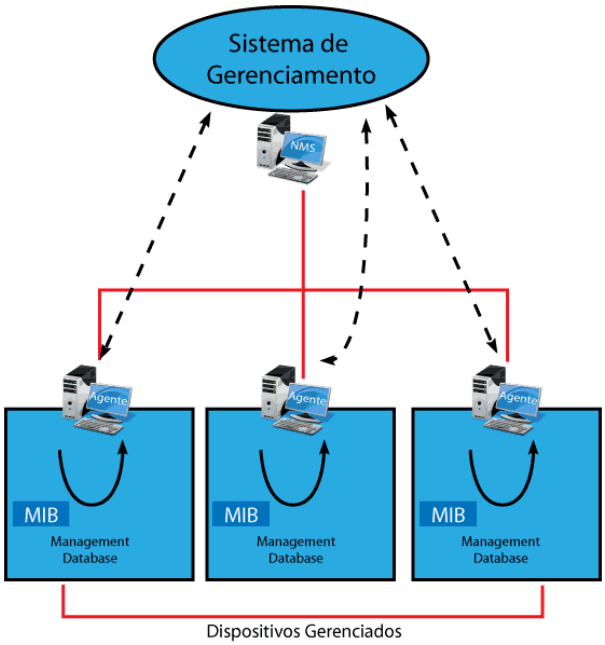
Existem outras opções que você pode configurar no comando "**Service timestamp**", por exemplo, utilizando "**Service timestamp log datetime msec**" você define que as mensagens de data e hora sejam mostradas com os milissegundos na mensagem (03:04:25.**389**).

7.3 Entendendo o Protocolo SNMP

O **protocolo SNMP** ou **Simple Network Management Protocol** é utilizado para gerenciar redes TCP/IP complexas.

Com o SNMP, os administradores podem **gerenciar e configurar** elementos de rede de um servidor localizado centralmente em vez de ter que executar o software de gerenciamento de rede.

Também é possível usar o SNMP para monitorar o desempenho da rede, detectar problemas de rede e acompanhar quem usa a rede e como ela é usada. O SNMP trabalha por padrão com o protocolo UDP na porta 161.



Uma rede gerida pelo protocolo SNMP é formada por três componentes chaves:

1. **Agentes SNMP** (**SNMP Agent**): os próprios roteadores e switches.
2. **MIB** (**Management Information Base**): base de dados padronizada que é lida por um gerente SNMP.
3. **Gerentes SNMP** ou **SNMP Manager**: Sistemas de Gestão de Redes ou NMS (Network Management Systems), por exemplo, o pacote de software da Cisco chamado **Cisco Prime**.

Um **Dispositivo Gerenciado** é um nó de rede que possui um **agente SNMP** instalado e se encontra numa rede gerenciada.

Estes dispositivos coletam e armazenam informações de gestão e mantêm estas informações disponíveis para sistemas NMS através do protocolo SNMP.

Dispositivos geridos, também às vezes denominados de **dispositivos de rede**, podem ser roteadores, servidores de acesso, impressoras, computadores, servidores de rede, switches, dispositivos de armazenamento, dentre outros.

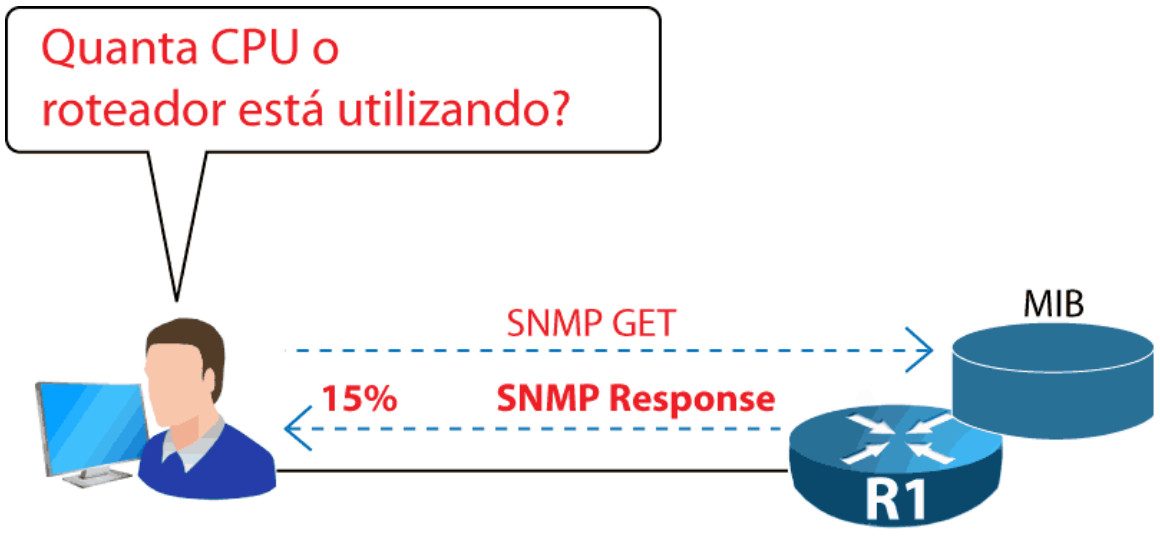
Um **Agente** é um módulo de software de gestão de rede que fica armazenado num Dispositivo Gerenciado. Um agente tem o conhecimento das informações de gestão locais e traduz estas informações para um formato compatível com o protocolo SNMP e padronizados em bancos de dados chamados **MIB** (**Management Information Base**).

Um **sistema NMS** é um **gerente SNMP** responsável pelas aplicações que monitoram e controlam os **Agentes SNMP**. Normalmente é instalado em um (ou mais que um) servidor de rede dedicado a estas operações de gestão, que recebe informações (pacotes SNMP) de todos os dispositivos geridos daquela rede, por exemplo, o Whatsup Gold, Cisco Prime e o HP Openview.

Trazendo para a realidade dos roteadores e switches, eles são os dispositivos gerenciados, os quais possuem uma MIB, que é um banco de dados que armazena de forma padronizada informações de hardware, software e parâmetros operacionais.

7.3.1 Mensagens do SNMP: Get, Set e Traps

Através de um sistema de gerenciamento (gerente SNMP) podemos ler essas informações e apresentá-las de forma mais intuitiva para que um analista de suporte, por exemplo, tenha informação de quanta CPU está sendo utilizada pelo roteador naquele momento através de um comando SNMP Get.

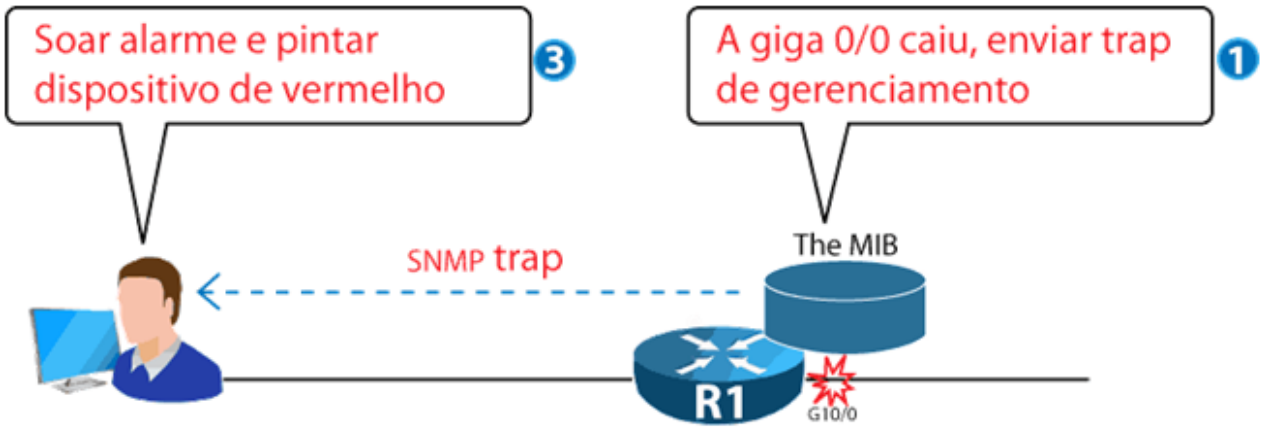


Esse tipo de operação pode ser automatizado em sistemas de gerência para geração de avisos, por exemplo, o gerenciador pode de 5 em 5 minutos checar o uso de CPU pelo roteador e se chegar a 50% gerar um aviso na tela de gerenciamento que a CPU passou desse limite configurado (threshold ou limiar).

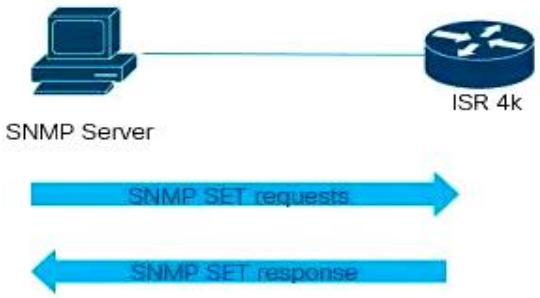
Outro tipo de mensagem que o SNMP pode gerar é um **TRAP**.

Esse tipo de mensagem é gerado espontaneamente pelo dispositivo para informar que um problema inesperado ocorreu.

Os traps são mensagens SNMP que descrevem uma variável da MIB, porém geradas pelo próprio dispositivo, sem a solicitação do NMS, o qual pode tomar uma ação diferente nesse caso, por exemplo, enviando uma mensagem para um destinatário de e-mail e soar um alarme para a equipe de monitoração.



Já o comando SET tem a função de alterar valores da MIB, ou seja, enviar configurações para os dispositivos gerenciados.



O SNMP possui três versões principais: 1, 2c e 3. A versão 1 é extremamente antiga e raramente encontrada atualmente, as versões mais utilizadas são a 2c e 3.

A diferença entre as duas últimas é que a versão 2 não possui muitos recursos de segurança, o que foi contemplado para a felicidade de muitos administradores de rede na versão 3 do SNMP.

A versão 3 possui recursos como autenticação, garantia da integridade das mensagens e criptografia.

7.3.2 MIB ou Management Information Base

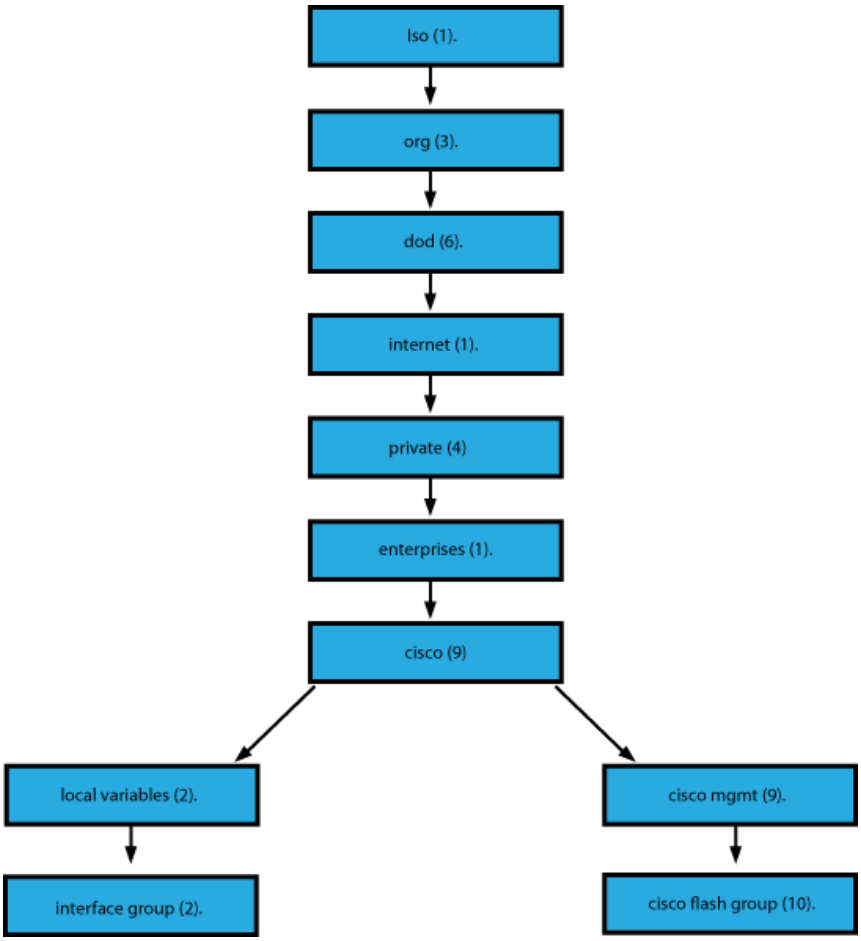
Um **Management Information Base** ou simplesmente **MIB** define variáveis de um dispositivo de rede que podem ser monitoradas e/ou controladas por um software de gerenciamento.

O termo correto para as variáveis armazenadas na MIB são objetos identificados por números chamados de **object ID** ou **OID**.

A MIB tem esses OIDs organizados em uma árvore com base em padrões definidos por RFCs formando uma hierarquia de OIDs.

Essa árvore formada pela MIB contém algumas informações (OIDs) padronizadas por RFCs e comuns a qualquer elemento de rede e características próprias dos equipamentos definidas pelo fabricante, por exemplo, informações específicas sobre a memória flash de um roteador.

Veja exemplo da árvore abaixo.



Por exemplo, se fosse necessário consultar o valor armazenado como "cisco flash group" o gerenciador teria que procurar pelo OID "1.3.6.1.4.1.9.9.10".

No dia a dia esse tipo de consulta pode se tornar inviável, porém os gerenciadores como o Cisco Prime têm essas consultas pré-configuradas e você pode escolher o que monitorar sem saber especificamente cada OID e seu caminho na árvore da MIB.

7.3.3 Versões do Protocolo SNMP e Segurança

O SNMP tem três versões de protocolo: v1, v2c e v3.

Tanto na versão 1 como na v2c do SNMP são utilizadas comunidades (**community strings**) para definir o acesso às MIBs e qual o nível podemos ter a essas informações através de dois tipos de comunidades.

- **Read-only (RO)**: permite acesso de leitura às variáveis da MIB e opção mais utilizada com a Version 2c devido à falta de recursos de segurança adicionais dessa versão de SNMP.
- **Read-write (RW)**: permite acesso de leitura e escrita a quaisquer objetos da MIB sem nenhuma verificação extra.

Portanto, com um nome ou string definimos o acesso e que tipo de acesso podemos fazer à MIB dos dispositivos com SNMPv2c ativado.

Portanto, se você descobrir qual a comunidade que um administrador de redes utiliza em sua rede você pode simplesmente ter informações via SNMP dos dispositivos de rede, simples assim.

Existe a possibilidade de limitar acesso a essas informações definindo servidores SNMP específicos e fornecer acesso via ACL apenas a esses IPs bem definidos.

No SNMP versão 3 temos realmente recursos de segurança implementados, são eles:

- **Integridade das mensagens**: através de um algoritmo de hash pode ser verificado se o conteúdo da mensagem não foi alterado em trânsito, seja por problemas na rede ou ataque.
- **Autenticação**: ajuda a validar se a origem que está enviando informações realmente tem a permissão para tal.
- **Criptografia**: protege os dados eventualmente capturados em trânsito dificultando a leitura das informações.

Com isso, a configuração do SNMPv3 tem três opções a mais que estudamos para a versão anterior:

- **noAuthNoPriv** → opção no comando **noauth** e utiliza um usuário e senha para autenticação, porém sem criptografia.
- **authNoPriv** → usa a opção **auth** no comando e implementa Message Digest 5 (MD5) ou Secure Hash Algorithm (SHA) para autenticação, porém ainda sem criptografia.
- **authPriv** → opção **priv** no comando, implementa autenticação e integridade com Message Digest 5 (MD5) ou Secure Hash Algorithm (SHA) e criptografia através do DES ou DES-56.

Isso possibilita uma maior segurança no acesso às informações.

8 Conceitos de QoS e Per-hop Behavior (PHB)

8.1 Introdução

Agora que aprendemos a configurar os roteadores e switches **será que realmente estamos prontos** para transportar os pacotes IP pela rede de forma efetiva? Será que a **infraestrutura** de redes, ou seja, nossas redes LAN e WAN **irão suportar os diferentes tipos de tráfego** simultaneamente através da rede?

Por exemplo, transportar voz sobre o protocolo IP juntamente com outras aplicações não é uma tarefa tão simples, pois cada aplicação tem uma característica (tamanho do quadro, quantidade de informação enviada, maneira que envia essa informação, ect), as quais podem prejudicar e muito o fluxo dos pacotes de voz pela rede IP, por isso é preciso uma **maneira especial para tratar esses pacotes gerados pela Telefonia IP** chamada **Qualidade de Serviços (QoS)**.

Para que uma rede VoIP (Voz sobre IP ou Voice over IP) possa operar com qualidade **a voz deve receber um tratamento especial**, ou seja, os pacotes de voz precisar ser priorizados quando cruzam a rede de dados até chegar ao seu destino. Por isso, implantar a tecnologia de voz sobre IP exige uma rede que suporte o QoS fim a fim, desde o dispositivo que gerou os pacotes de voz até o que vai receber esses pacotes. Veja abaixo a definição da Cisco sobre QoS.

> "**Qualidade de serviços** é a habilidade da rede fornecer o melhor serviço (de uma maneira especial) para determinados usuários ou aplicações em detrimento de outros usuários e aplicações."

O **serviço de voz** é um serviço de **tempo real**, ou seja, precisa de um fluxo constante e sem atrasos (delay), por isso precisa ser tratado como um serviço especial.

Se você está acessando a internet ou utilizando um programa FTP para baixar arquivos, quando a sua rede tem um problema a página ou arquivo irão demorar um pouco mais para carregar, irá aumentar o tempo total do download, mas você no final irá receber o arquivo ou a página de internet no seu browser.

Porém, em uma chamada de voz via IP se a rede começa a ter atrasos ou delay a conversação pode ficar truncada ou sobreposta, pois devido ao atraso as pessoas começam a falar ao mesmo tempo, a conversação começa a ficar picotada (ter quebras) e pode até cair em casos extremos.

Para evitar esse tipo de problema você terá que, além de **garantir uma banda para o VoIP**, **certificar-se que essa banda será alocada** em primeiro lugar para a voz sobre IP.

Isto significa que se houver um gargalo de rede onde o roteador precisa enfileirar o tráfego antes de enviá-lo através da rede, o roteador terá que mover o tráfego de voz para frente do tráfego de dados na fila de saída para garantir que a voz seja enviada no primeiro intervalo disponível.

Na realidade o **QoS** não é "uma ferramenta" e sim um **conjunto de ferramentas** utilizadas para **controlar o tráfego** através da rede.

Muitas vezes você consegue garantir o QoS com apenas uma técnica ou ferramenta, porém quando os requisitos da aplicação, tais como largura de banda e delay, forem muito complexos será necessário utilizar várias técnica simultaneamente para, por exemplo, controlar o delay, reservar largura de banda (bandwidth) e comprimir o cabeçalho dos dados quando eles estão atravessando as redes WAN para melhorar o desempenho da rede e do VoIP como um todo.

Por exemplo, a largura de banda insuficiente e o atraso (delay) são sérios "inimigos" do tráfego de voz sobre IP, porém vamos analisar com um pouco mais de detalhe cada um deles e complementar essa lista. Acompanhe abaixo.

Os problemas citados a seguir são as principais dificuldades em se utilizar um ambiente de rede de dados, porém quando **adicionamos serviços de voz (VoIP)** eles se **agravam**, pois além do tráfego de dados existentes a rede terá que suportar o novo tráfego de voz com requisitos mais complexos de qualidade.

Além disso, administradores que trabalham com um ambiente de voz tradicional com PABX estão acostumados com um sistema que está isolado e com banda garantida para o tráfego de voz. A tolerância a quebras, eco ou chamadas pedidas em redes de voz tradicionais é bastante baixa, pois o sistema dificilmente tem paradas ou interrupções.

Portanto o **objetivo do QoS** para voz sobre IP é **fornecer** uma **largura de banda** consistente para o tráfego de voz de uma maneira que haja um **pequeno**, mas constante e previsível, **delay** de uma ponta a outra da rede.

Para isso precisamos implementar o QoS de uma forma a **evitar congenstionamento** em cada ponto da rede que ele possa existir, implementando um processo fim a fim, o qual tenha a capacidade de analisar a rede e determinar os tipos de tráfego que existem e que níveis de serviços esses tráfegos precisam para serem transmitidos com qualidade e com a devida prioridade.

- **Falta de largura de banda:** vários fluxos de voz e dados competindo por uma largura de banda limitada para envio das informações podem causar falta na largura de banda.
- **Delay ou atraso:** é o tempo que um pacote leva para ser transmitido do ponto de partida até o seu destino. Ele pode ser dividido em três tipos:

    - **Fixo:** esse valor você não pode alterar, pois são intrínsecos de cada tecnologia, por exemplo, um pacote levará um tempo fixo para trafegar em longas distâncias através de um backbone IP e esse valor é fixo, portanto, o QoS não pode tratar com esse tipo de atraso.
    - **Variável:** valores de delay que você pode alterar. Por exemplo, o atraso por enfileiramente (queuing delay – quanto tempo um pacote espera em uma fila de uma determinada interface do roteador) é variável, pois depende de quantos pacotes estão atualmente na fila da interface esperando para serem enviados. Você pode alterar esse delay da fila (queuing delay – queue é fila em inglês e se pronuncia Kiu) escolhendo os pacotes que serão enviados primeiro, por exemplo, passando os pacotes de voz na frente dos pacotes de dados.
    - **Jitter (variação no delay):** são pacotes que chegam com atrasos diferentes no destino, por exemplo, o primeiro pacote chega com 90 ms (mili segundos ou 1 segundo divididos por mil – 0,001s), enquanto o segundo pacote chega com 110 ms, ou seja, uma diferença de 20 ms entre o primeiro e o segundo pacote de voz. Portando dizemos que há 20 ms de variação de delay (jitter) entre os pacotes.

- **Perda de pacotes (Packet loss):** a perda de pacotes pode ocorrer por dois motivos básicos, devido a um congestionamento na rede ou pela rede não ser confiável (problemas de infraestrutura ou dimensionamento).

8.2 Requisitos de Rede para Voz, Vídeo e Dados

Conforma já mencionamos anteriormente nesse capítulo, diferentes tipos de tráfego circulam pela rede e cada um pode exigir requisitos de QoS diferentes.

Alguns protocolos, tais como HTTP, são menos exigentes, podem funcionar com pouca largura de banda e suportam bem o delay.

Outros são mais são mais exigentes, precisam de largura de banda disponível com pouco delay, caso dos tráfegos de voz e vídeo.

Diferente do tráfego de dados, um **fluxo de voz é previsível**, ele se mantém constante **durante toda a ligação**. Essa largura de banda depende basicamente do tipo de codec escolhido.

O codec é o codificador que transforma o áudio em um código binário, ou seja, transforma a voz de analógico para digital na transmissão e digital para analógico na recepção.

Existem vários tipos de codecs, por exemplo, o mais utilizado em redes LAN é o G.711.

Uma ligação através de telefonia IP realizada com codec padrão G.711 precisa de aproximadamente 80Kbps de largura de banda por chamada realizada.

Já um codec como o G.729 precisa de aproximadamente 24Kbps por chamada. Ambos os exemplos ignoram cabeçalhos por tipo de link, são valores aproximados.

Isso já não ocorre com um fluxo de dados, o qual pode saltar repentinamente quando fazemos um download de grande porte através da Internet, podendo até ocupar toda a banda com esse download.

Porém, além dos **requisitos de largura de banda**, o qual é definido principalmente pelo **codec** utilizado para fazer a conversão da voz para digital, o **tráfego de voz** depende também dos requisitos citados a seguir.

- **Delay fim a fim (End-to-end delay):** 150 ms ou menor
- **Jitter:** 30 ms ou menor
- **Perda de pacotes:** 1% ou menor

Muitas bilbiografias citam que o **vídeo** tem **requisitos idênticos aos de voz**, porém **precisa de uma largura de banda maior**. Além disso, essa banda utilizada pode variar dependendo dos movimentos que o vídeo tem, pois quanto mais movimento mais largura de banda necessária.

Se você consultar, por exemplo, o "End-to-End QoS Network Design", Second Edition (Cisco Press, 2013), existem alguns requisitos extras para o QoS em Vídeo:

- Largura de banda: 384 Kbps a 20Mbps (ou mais)
- Delay (one-way): 200–400 ms
- Jitter: 30–50 ms
- Loss (perda de pacotes): 0.1%–1%

Já os requerimentos de dados são mais complexos e não podem ser tradados como um só serviço, por isso normalmente ele é dividido em quatro categorias macro.

Você pode na realidade vincular cada tipo de aplicação a um nível específico de QoS, mapeando as aplicações através de vários métodos, tais como interface de entrada ou saída, access lists, e assim por diante.

- **Aplicações de missão crítica (Mission-critical applications):** São aplicações críticas para a organização e necessitam de muita largura de banda dedicada.
- **Aplicações transacionais (Transactional applications):** São aplicações normalmente interativas e necessitam de resposta rápida aos usuários, como por exemplo uma consulta a base de dados de clientes para atendentes de call center.
- **Aplicações Best-effort (melhor esforço):** São aplicações menos críticas e não categorizadas, por exemplo, acesso web, e-mail e transferências FTP.
- **Scavenger applications:** Esses são aplicativos que consomem um alto valor de largura de banda e não são de interesse organizacional, tais como Kazaa, BitTorrent e LimeWire, aplicativos de transferência de arquivos peer-to-peer.

Características dos fluxos de Dados

- **Smooth or Bursty (Contínuo ou em rajadas):** um fluxo de dados pode ser contínuo (smooth) ou em rajadas (bursty), ou seja, pode ocupar a rede de qualquer maneira.
- **Drop insensitive (não sensível a perda de pacotes):** não é sensível a perda de pacotes em sua maioria podemos até dizer que é "drop insensitive", ou seja, não sensível a perda de pacotes devido aos mecanismos de retransmissão e confirmação do TCP.
- **Delay insensitive (não sensível a delay):** não tem problemas com relação ao delay (atraso) de rede.
- **Benign or greedy (benigno ou agressivo na alocação de banda):** pode ou não oferecer risco ao tráfego de redes, ou seja, pode ser benigno (benign) ou agressivo (greedy – ganancioso). Uma aplicação P2P como o Kazaa pode ocupar toda a banda de rede em segundos.
- **TCP retransmit (se utiliza de retransmissões TCP):** utiliza a retransmissão do TCP em caso de problemas de comunicação, pois maioria das aplicações de dados utilizam TCP.

Características dos fluxos de Voz

- **Smooth (contínuo ou suave):** fluxo contínuo durante a chamada estabelecida, pois os codecs utilizam uma taxa previsível.
- **Delay sensitive (sensível ao atraso):** tem sensibilidade ao atraso (padrão 150ms).
- **Drop sensitive (sensível à perda de pacotes):** tem sensibilidade à perda de pacotes (padrão menor que 1%).
- **Benign (benigno):** ocupa a rede de forma previsível e com uma banda fixa por chamada.
- **UDP priority (precisa de priorização UDP):** precisa de ter prioridade UDP, pois o RTP trabalha com o serviço de UDP para transmitir a voz pela rede.

Características dos fluxos de Vídeo

- **Bursty** (transmissão em rajadas): trabalha com o envio da diferença nas imagens em movimento e normalmente acaba enviando uma rajada de dados quando as alterações no quadro são grandes, por isso é considerado "Bursty".
- **Greedy**: agressivo na alocação de banda, normalmente requer muito mais banda que as chamadas de voz.
- **Delay sensitive** (sensível ao atraso): tem sensibilidade ao atraso.
- **Drop sensitive** (sensível à perda de pacotes): tem sensibilidade à perda de pacotes.
- **UDP priority** (precisa de priorização UDP): precisa de ter prioridade UDP, pois o RTP trabalha com o serviço de UDP para transmitir a voz pela rede.

8.3 Mecanismos de QoS

Para se adequar a diferentes requisitos de diferentes aplicações vários **mecanismos de QoS** surgiram ao longo do tempo, vamos analisar os principais disponíveis atualmente.

Best Effort ou Melhor Esforço: o melhor esforço é a maneira padrão que a rede opera, ou seja, sem nenhum mecanismo de QoS implementado nela. Sem mecanismos de QoS a rede trata todo tráfego de uma maneira "first come, first served" (first in, first out), ou seja, quem chega primeiro é o que utiliza o serviço. Este tipo de mecanismo **não atende as exigências de QoS das redes atuais**.

Integrated Services (IntServ): já o IntServ funciona em um modelo baseado em reservas. Por exemplo, uma chamada que utiliza 100kbps precisa ser realizada pela rede, se essa rede foi projetada para trabalhar apenas com o modelo IntServ ela reservaria 100Kbps em todo dispositivo de rede situado entre os telefones que irão se comunicar utilizando o protocolo RSVP (Resource Reservation Protocol – protocolo de reserva de recursos).

Durante toda chamada essa banda de 100Kbps fica disponível para a ligação. Apesar de ser o único modelo que fornece essa garantia de banda o IntServ tem um problema de escalabilidade, porque um número muito grande de reservas poderia consumir toda a banda disponível na rede.

Differentiated Services (DiffServ): o DiffServ é atualmente o **modelo mais flexível e popular** entre as implementações de QoS na atualidade. Nesse modelo você pode configurar cada dispositivo de rede de maneira que ele responda aos variados tipos de tráfego com uma variedade de métodos de QoS, possibilitando criar diversas classes de tráfego, cada uma com um tratamento específico.

Uma diferença entre o Diffserv e o IntServ é que com o primeiro o tráfego não pode ser garantido, uma vez que os dispositivos não trabalham com reserva de banda. Porém, segundo documentação oficial da Cisco, o DiffServ pode chegar muito próximo a garantia de banda, sendo um modelo que consegue tratar dos problemas de escalabilidade do IntServ, o que o tornou um **padrão de QoS utilizado na maioria das organizações ao redor do mundo**.

Os modelos de QoS podem utilizar várias estratégias para o projeto e implementação em toda a rede. Os mecanismos de QoS combinam uma série de **ferramentas** para fornecer diversos níveis de serviço para que o tráfego de rede possa atravessar a rede, sendo que essas ferramentas se enquadram nas categorias a seguir.

- **Classificação e Marcação (Classification and Marking):** são ferramentas que permitem a identificação e marcação dos pacotes para que os dispositivos possam identificar e dar o devido tratamento ao tráfego que cruza a rede. Normalmente o primeiro dispositivo que recebe os pacotes faz a identificação utilizando ferramentas como access-lists, interfaces de entrada ou "deep packet inspection" (inspeção da aplicação), ferramentas que podem utilizar o processamento de maneira intensiva e adicionar delay ao pacote. Depois de identificado, então o pacote é marcado, sendo que essa marcação pode ser feita no cabeçalho da camada-2 (enlace/data link – permitindo que os switches possam ler essa marcação) e/ou no cabeçalho da camada-3 (rede/network) para que os roteadores possam ler essa marcação. Com isso os pacotes podem atravessar a rede e serem "lidos" pelos equipamentos sem que uma análise mais profunda precise ser realizada a cada salto, permitindo que os pacotes sejam tradados de acordo com sua marcação.

- **Controle de Congestionamento (Congestion Management):** o controle de congestionamento é basicamente tratado pelas estratégias de QoS para enfileiramento (queuing), as quais são as ferramentas básicas de QoS que devem ser implementadas em

toda a rede. Essas ferramentas e estratégias de enfileiramento são aplicadas quando ocorre o congestionamento, ou seja, são ferramentas reativas. Basicamente o roteador terá que decidir quem vai ser liberado primeiro quando houver disponibilidade de banda durante um congestionamento, enfileirando o restante do tráfego em um "buffer" (espaço de memória RAM reservado para armazenamento temporário dos pacotes).

- **Congestion Avoidance:** em português poderíamos traduzir esse mecanismo para "Prevenção de Congestionamento". A maioria dos mecanismos de QoS entram em ação quando ocorre o congestionamento, são reativos, aqui a filosofia é diferente, tenta fazer um trabalho preventivo para evitar que o congestionamento ocorra. Esse mecanismo utiliza técnicas como excluir (drop) tráfego não interessante ou não essencial antes que um tráfego muito pesado cause um congestionamento.

- **Policing and Shaping:** aqui são criadas políticas (policy) de tráfego e o modelamento (shaping), onde a política normalmente é utilizada para filtrar o tráfego excessivo e o modelamento faz o enfileiramento do tráfego excessivo para depois enviá-lo na rede. Normalmente são utilizados quando a largura de banda pode ser maior que a velocidade física da rede ou interface, como no caso do Frame-relay.

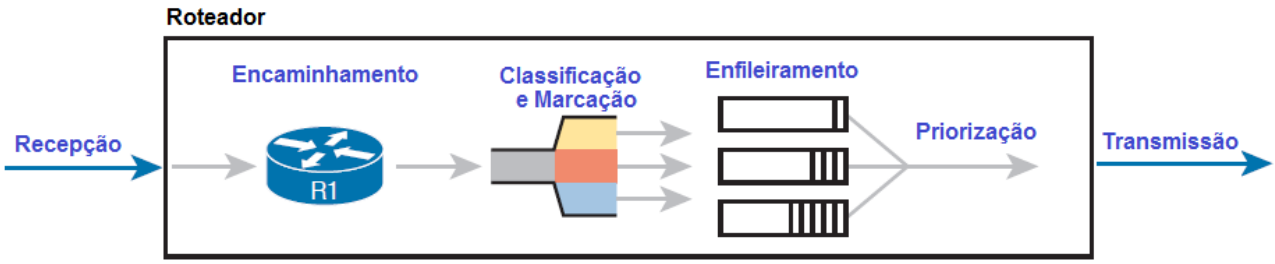
- **Link Efficiency:** em português "eficiência do link ou enlace", são técnicas utilizadas no estágio final da transmissão, ou seja, no momento de enviar os pacotes por uma interface (link). Podem ser utilizadas técnicas de compressão, por exemplo, para melhorar a performance de um link de baixa velocidade.

Abaixo segue algumas técnicas de QoS e onde são mais recomendadas aplicar.

QoS para Tráfego de Entrada (Input)	QoS para Tráfego de Saída (Output)
Classificação	Congestion Management
Marcação	Marcação
Policing	Congestion Avoidance
	Shaping
	Policing
	Compressão
	Fragmentation and Interleaving

8.4 Visão Geral do QoS em Roteadores

Em termos gerais a ideia do QoS nos roteadores é fazer a classificação, marcação e priorização do tráfego conforme as necessidades de cada tipo de aplicação.



Por padrão quando o roteador recebe um pacote ele é colocado em uma fila de recepção, depois é realizado o encaminhamento (roteamento). Uma vez decidida a interface de saída o pacote é colocado em uma fila de saída, ou seja, o roteador segura o pacote até que a interface escolhida esteja disponível para envio.

Podemos alterar esse comportamento com as configurações de QoS fazendo a classificação e marcação dos pacotes para que eles sejam colocados em filas com diferentes prioridades, tudo conforme as necessidades de cada tráfego, assim o roteador pode priorizar o tráfego mais sensível.

Por exemplo, os pacotes de voz são pequenos e precisam ser enviados em sequência, afinal trata-se de uma conversação e precisa ter "fluência". Agora imagine que chega ao mesmo tempo desse fluxo de conversação de voz pacotes de backup de uma determinada aplicação.

Normalmente esses pacotes são grandes e podem ocupar a fila de saída por um bom tempo.

O que ocorreria nesse caso? Simples, a conversação de voz iria ter atraso e até perdas, pois a interface gastaria muito tempo com os pacotes do backup.

Portanto, esses pacotes de voz devem ter uma marcação que faça com que eles sejam colocados em uma fila prioritária, a qual passe na frente dos pacotes de backup que são menos sensíveis ao atraso.

Os mecanismos de QoS visam fazer essa priorização, principalmente em momentos de "pico", onde as interfaces estão sobrecarregadas ou próximas do limite máximo de ocupação.

8.5 Classificação e Marcação

O termo classificação (classification) é o processo de verificar certos campos do quadro ou pacote para tomar uma ação de QoS. Normalmente a primeira ação a ser tomada será a marcação do tráfego (marking) para que ele possa receber o correto tratamento pelo QoS.

Portanto as ferramentas de QoS fazem a classificação do tráfego (por exemplo, verificando campos do cabeçalho IP) para decidir que ação de QoS deverá ser tomada com aquele pacote. Essas ações serão discutidas ao longo do capítulo, por exemplo, podemos enfileirar os pacotes, fazer o shaping, policing e assim por diante.

Atualmente a classificação pode ser realizada de diversas maneiras, porém para facilitar o trabalho dos administradores e economizar processamento nos dispositivos, normalmente os pacotes são classificados e marcados (marking) logo que entram na rede, possibilitando que os

demais dispositivos da rede não precisem realizar novamente esses processos complexos de classificação.

Isso porque os pacotes já foram classificados e agora basta utilizar uma lógica que leia essa marcação e tome uma decisão sem precisar realizar a mesma classificação inicial mais complexa que foi realizada lá no início quando a rede recebeu o pacote IP.

Podemos utilizar ACLs para classificar o tráfego para o QoS. Outra ferramenta bastante utilizada para classificar o tráfego é o NBAR (Network Based Application Recognition).

O NBAR está atualmente na sua versão 2 chamado NBAR2 ou next-generation NBAR. O NBAR2 consegue verificar os pacotes e classificá-los de várias formas diferentes que são muito úteis para o QoS.

Outra vantagem do NBAR2 é que ele pode analisar outros parâmetros do pacote em relação a uma ACL, resolvendo problemas quando uma aplicação não pode ser descoberta por sua porta padrão do UDP ou TCP.

Por exemplo, a aplicação Cisco WebEx fornece conferências de áudio e vídeo. No planejamento do QoS você pode classificar esse tráfego de voz e vídeo do Webex de forma diferente da voz e vídeo padrão da empresa, ou seja, pode utilizar um valor de DSCP (vamos estudar mais a seguir) exclusivo para marcar o tráfego do Webex.

Portanto, o planejamento de QoS deve definir classes para os diferentes tipos de tráfego para que eles recebam tratamento adequado conforme suas necessidades.

Cada pacote deve ser classificado e marcado com valores que os associem a classe correta de tráfego ou serviço. Por exemplo:

- Pacotes de voz devem utilizar DSCP com valor EF e CoS 5.
- Vídeo conferência e outros vídeos corporativos interativos devem utilizar DSCP com valor AF41 e CoS 4.
- Aplicações críticas para o negócio devem ser marcadas com DSCP AF21 e CoS 2.

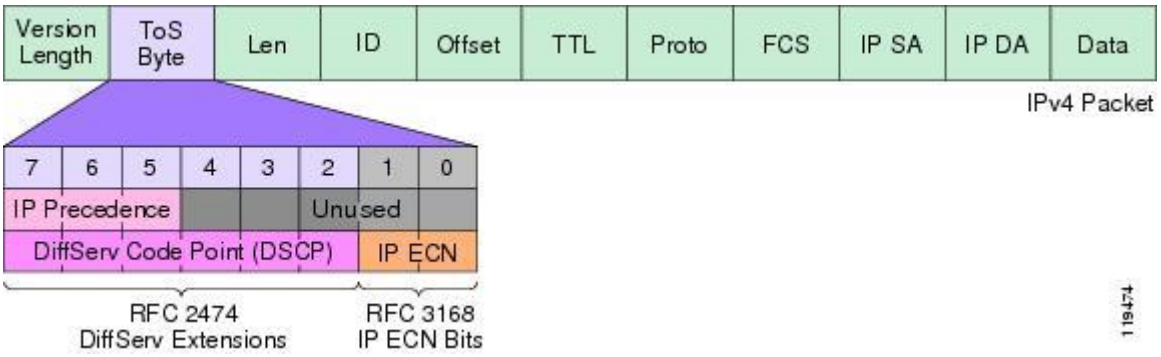
O valor de DSCP é definido no cabeçalho do pacote IP, já o CoS está no quadro do protocolo 802.1Q (trunks).

8.5.1 Entendendo as Marcações via DSCP e CoS

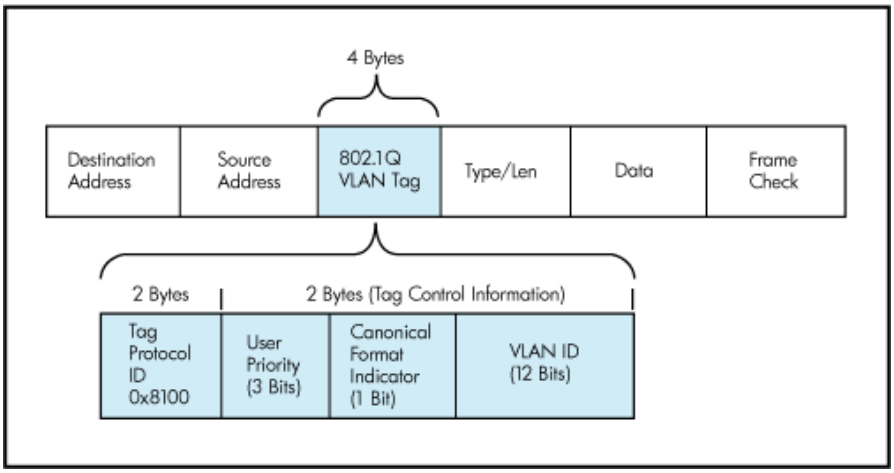
O DSCP (Differentiated Services Code Point - DiffServ) é um campo de 6 bits chamado de TOS (Type of service) dentro do cabeçalho IP. Com esse campo podem ser formadas quatro classes, as quase podem ser subdivididas em mais três classes de descarte (drop probability classes).

Em geral quanto maior o número melhor é o tratamento de QoS do pacote em momentos de congestionamento. Outro detalhe é que esse parâmetro permite uso fim a fim na rede, podendo ser utilizado por toda a rede desde que seja definido uma fronteira de confiança (trust boundary – será estudado a seguir).

Anteriormente esse campo TOS era conhecido como "IP Precedence" (IPP), porém essa forma não é mais utilizada para QoS atualmente. O IPP utiliza os três primeiros bits do TOS para definir prioridades que poderiam ir de 0 (000 em binário) a 7 (111 em binário). Note que o DSCP utiliza seis bits, três a mais que o antigo IPP.



O CoS ou Class of service é um campo de 3 bits definido dentro da especificação 802.1p, a qual faz parte do cabeçalho do protocolo 802.1q. Portanto, essa marcação é utilizada entre os trunks da rede. Na figura abaixo o CoS é chamado de "User Priority".



Quanto maior o CoS, mais prioritário será o quadro. Note também que o CoS é uma marcação de layer 2, já o DSCP e IP Precedence são marcações de layer 3.

Existem outras formas de marcação, por exemplo, o TID (3 bits) que é utilizado pelo 802.11 em redes sem fio (Wi-Fi) e o EXP (3 bits) utilizado para marcação em redes MPLS.

8.5.2 Trust Boundary

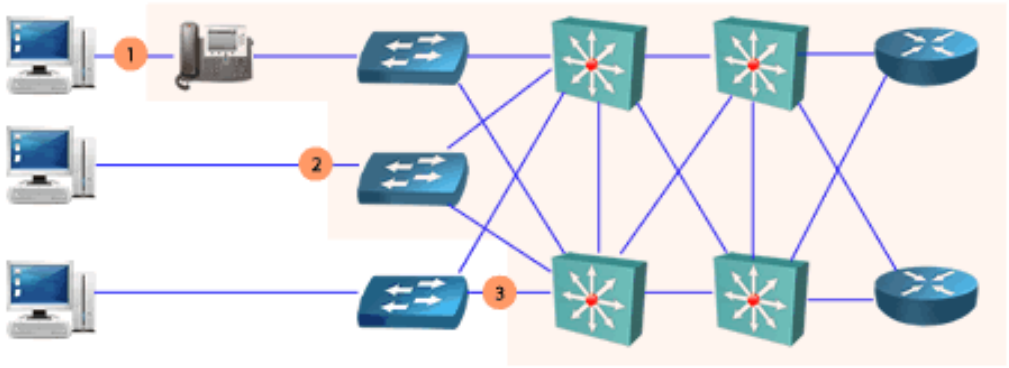
O **"trust boundary"** podemos traduzir como "limite ou fronteira de confiança".

Tudo inicia quando enviamos um determinado tráfego na rede e esse tráfego pode estar ou não com **marcações de QoS**, tais marcações são utilizadas para identificar e dar a devida prioridade para cada tipo de classe de tráfego. Porém, essas marcações podem ser ou não ser confiáveis, ou seja, será que o equipamento que fez a marcação tinha realmente autoridade para isso?

Um telefone IP da Cisco, por exemplo, já faz a marcação dos seus pacotes de voz como prioritários antes de enviá-los na rede e essa marcação é realmente confiável, pois o tráfego de voz deve ter prioridade sobre os demais. Agora imagine que um usuário instalou um programa que marca os quadros dessa aplicação não prioritária como se fossem quadros de voz, ou seja, com alta prioridade, com certeza não podemos confiar nessa marcação.

Portanto, o **limite de confiança** ou **"trust boundary"** é o ponto onde vamos confiar naquela marcação que está sendo recebida e utilizá-la para dar a devida prioridade aos pacotes, ou seja, é o ponto onde a partir dele a marcação de QoS está correta. Qual é esse limiar ou fronteira?

Tudo depende das características de cada equipamento, se o dispositivo do usuário tiver uma marcação confiável você pode utilizar a fronteira mais perto do usuário ou utilizar os equipamentos de rede para fazer a marcação correta, veja a **figura abaixo**.



Os telefones IP da Cisco tem capacidade de fazer a marcação dos seus pacotes de voz e também retirar a marcação de alta prioridade feita pelos computadores que estão ligados à sua porta de switch. Utilizando o telefone IP para fazer a marcação utilizamos o **ponto 1** como limite de confiança (trust boundary ou fronteira de confiança). Essa é a situação ideal, pois evita que os switches tratem de um volume muito alto de informações para realizar a marcação no ponto B.

Se você tem micros conectados diretamente aos switches de acesso e tem switches de acesso com capacidade de marcação de QoS, você pode fazer a marcação nesses equipamentos que estão no **ponto 2**. Caso os switches de acesso não tenham capacidade de marcação de QoS você pode aplicar no **ponto 3**, ou seja, nos switches de distribuição, o que também funciona bem, porém traz uma sobrecarga para esses equipamentos. Aplicando a marcação no ponto 3 você terá os pacotes trafegando pelos switches de acesso sem nenhum tratamento de QoS, porém como as velocidades na LAN são maiores isso acaba não afetando a voz. O QoS é fundamental onde pode haver gargalos (bottleneck), porém recomenda-se aplicá-lo em toda a rede (QoS fim a fim).

8.5.3 Sugestão de Valores de Marcação do DSCP

A arquitetura DiffServ foi originalmente descrita na RFC2475 e apesar de existirem várias recomendações vamos estudar aqui três conjuntos de marcações que podem ser realizadas através dos valores de DSCP definidos dentro do DiffServ:

1. Expedited Forwarding (EF)
2. Assured Forwarding (AF)
3. Class Selector (CS)

Criando uma marcação consistente via uso dos valores de DSCP em sua rede pode garantir a melhor entrega dos pacotes e até mesmo o provedor de serviços que você utiliza pode tratar melhor seu tráfego que cruza a rede dele, principalmente quando utilizamos redes de provedores de serviços via MPLS.

Mas vamos começar a estudar o primeiro conjunto de valores definido pelo DiffServ que é o Expedited Forwarding (DSCP - EF), o qual é um valor único sugerido para pacotes que precisam de baixa latência (low latency - delay), baixo jitter (low jitter) e baixa perda de pacotes (low loss). Essa descrição encaixa-se em que tipo de tráfego? Pense um pouco antes de continuar a leitura...

O Expedited Forwarding foi definido na RFC 3246 com o valor de DSCP decimal 46 ou o acrônimo EF, que é a inicial de "Expedited Forwarding".

Na configuração do QoS você pode utililizar tanto o EF ou o valor em decimal 46, porém costuma-se utilizar mais a opção de letras ao invés do decimal.

Maioria dos planos de QoS utilizam o EF para marcação de pacotes de voz.

Uma dica, a voz narealidade utiliza dois tipos de pacotes: voz e sinalização. O EF é utilizado para a voz apenas, a sinalização pode utilizar uma prioridade menor, pois ela não necessita dos mesmos requisitos da voz.

Os pacotes de voz trafegam a voz digitalizada e precisam de um QoS melhor que a sinalização, a qual é enviada normalmente no início ou final de uma chamada. Os telefones IP Cisco marcam os pacotes de voz como EF e a sinalização como CS3 (vamos estudar o CS ainda nesse tópico).

O segundo tipo de marcação que podemos utilizar é o Assured Forwarding ou AF, definido no DiffServ detro da RFC 2597. Diferente do EF que possui um valor apenas o AF define 12 valores de DSCP para marcação dos pacotes.

Isso porque ele é dividido em duas partes, a primeira define quatro tipos de prioridade de fila e a segunda parte do AF define três classes de descarte de pacotes (drop priority) que podem ser utilizadas pelos mecanismos de "congestion avoidance". Por isso, com essas quatro filas mais três classes de descarte temos 12 valores de marcação do DSCP.

Os valores de AF tem o formato "AFXY", onde X refere-se a fila (1 a 4) e Y refere-se a prioridade de descarte (1 a 3). Portanto temos as filas de 1 a 4 (AF1Y, AF2Y, AF3Y e AF4Y) e cada fila tem três prioridades de descarte, por exemplo, a fila 1 pode ter os valores AF11, AF12 e AF13.

Quanto maior o valor de X mais prioritária será a fila, por exemplo, a fila AF41 terá prioridade sobre a fila marcada com o valor AF 11. Já dentro de uma mesma fila quanto menor o valor de Y melhor será o tratamento do pacote marcado, por exemplo, um pacote com o valor AF21 tem tratamento preferencial em relação a outro pacote marcado como AF23.

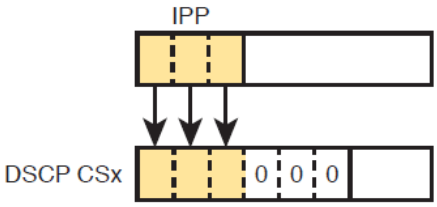
Podemos converter o valor de AF para DSCP em decimal utilizando uma fórmula simples para calcular esse valor: 8x + 2y = valor decimal. Por exemplo: AF41 seria o valor decimal DSCP 34, veja os valores em binário e decimal abaixo.

Drop	Classe 1	Classe 2	Classe 3	Classe 4
Baixo	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Médio	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
Alto	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

Nessa tabela podemos ver como será o comportamento dos pacotes, por exemplo, os pacotes podem entrar em quatro classes de fila, de 1 a 4, sendo que cada fila pode tratar os pacotes de três formas diferentes em relação ao descarte (drop). Esse descarte é importante quando utilizamos mecanismos de shaping e/ou congestion avoidance.

Veja que na tabela os valores de AF 1 (001) a 4 (100) estão definidos nos três primeiros bits para manter compatibilidade com a versão antiga do campo TOS chamada IP Precedence ou IPP.

Por último temos os valores de DSCP chamados de Class Selector (CS), o qual pode ser dividido em oito valores podendo ser representados como CS 0 a 7 (CS0, CS2 ... CS7) ou em decimal. Veja na figura abaixo.



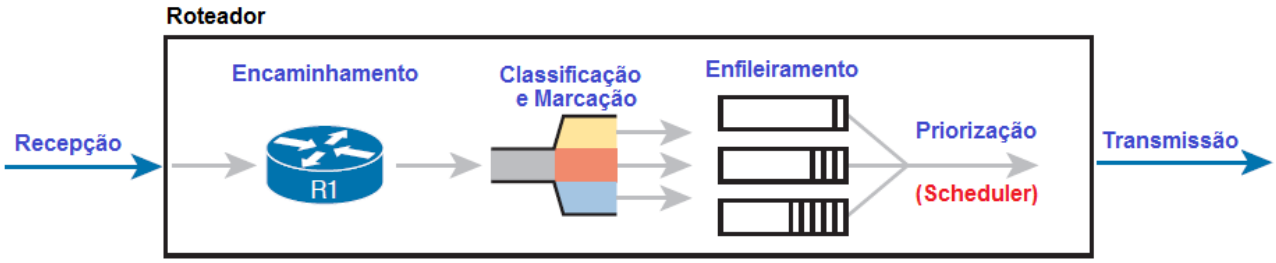
IPP	CS	Decimal DSCP
0	CS0	0
1	CS1	8
2	CS2	16
3	CS3	24
4	CS4	32
5	CS5	40
6	CS6	48
7	CS7	56

Note que os três primeiros bits do CSx acabam sendo os mesmos que do IPP value (0 through 7).

Com isso aprendemos como podemos marcar os pacotes e a seguir vamos estudar os mecanismos de QoS que podem ser utilizados após a marcação para priorizar o tráfego.

8.6 Controle de Congestionamento –Enfileiramento e Priorização

Como já estudamos maioria dos roteadores não enviam diretamente os pacotes através de suas interfaces de saída, ao invés disso esses pacotes são posicionados em "filas de saída" (output queues) e são enviados quando a interface está livre.

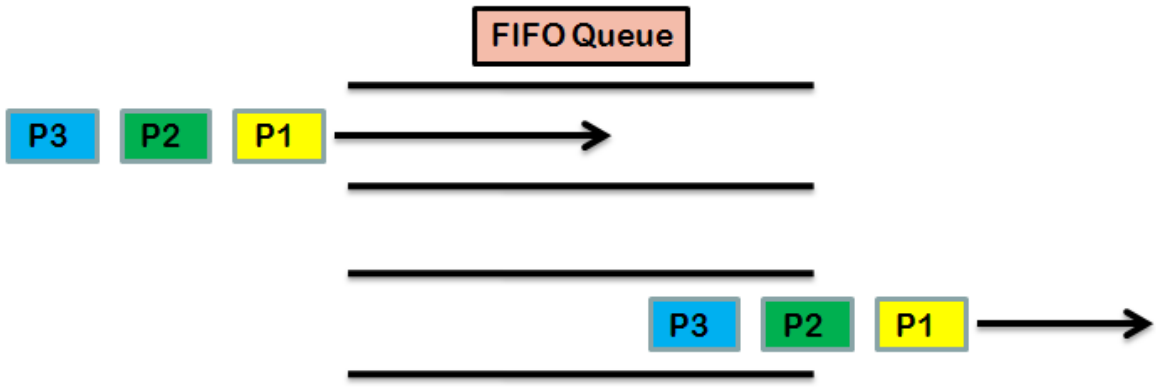


Dica: "queue" ou fila em inglês pronuncia-se "kiu".

As filas na prática são buffers ou espaços da memória RAM disponibilizados para armazenamento desses pacotes e diversos outros tipos de informações do roteador.

O processo de verificar se a interface está livre e mover o pacote da fila para a interface é realizada por um agendador ou scheduler, na figura representado pela "Priorização".

A maioria das interfaces de rede utilizam por padrão uma técnica de agendamento básica chamada **First-in, First-out** (FIFO – o primeiro que entra é o primeiro que sai), ou seja, o pacote que chega primeiro é enviado primeiro, simples assim. Veja na figura a seguir, P1 (pacote 1) chegou primeiro, por isso é o primeiro a ser enviado na interface de saída.

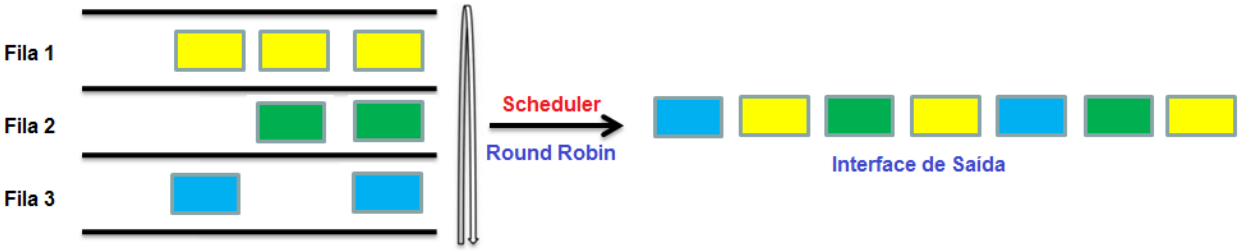


O problema desse tipo de agendamento de pacotes é que o tráfego de rede não é igual, os pacotes podem variar em tamanho dependendo da aplicação, por exemplo, como já vimos o VoIP (protocolo RTP) tem pacotes pequenos e em grande número, já um pacote enviado entre um storage e um sistema de backup são os maiores possíveis que a rede pode enviar (MTU máximo), agora imagine esses dois tráfegos sendo passados ao mesmo tempo na rede, com certeza utilizando um agendador FIFO a voz iria sofrer muito.

Portanto, o enfileiramento (queuing) tem um objetivo básico de seprar os tráfegos para que o agendador (scheduler) possa **dar prioridade ao tráfego mais crítico** da rede e que tem necessidade de baixo atraso (por exemplo, tráfego de tempo real como voz e vídeo).

Portanto, nesse processo de enfileiramento o agendador é o mais importante, pois ele pode "priorizar" o tráfego.

Outra forma de fazer o agendamento ou scheduling utilizado pelos roteadores Cisco é através da lógica do "Round Robin". O round Robin faz uma leitura cíclica das filas (queues) em ordem. A cada ciclo o scheduler pega uma mensagem ou um número de bytes da fila 1, depois vai para a fila 2, depois vai para a fila 3 e assim por diante, retornando no final para a fila 1 novamente e repetindo o ciclo.

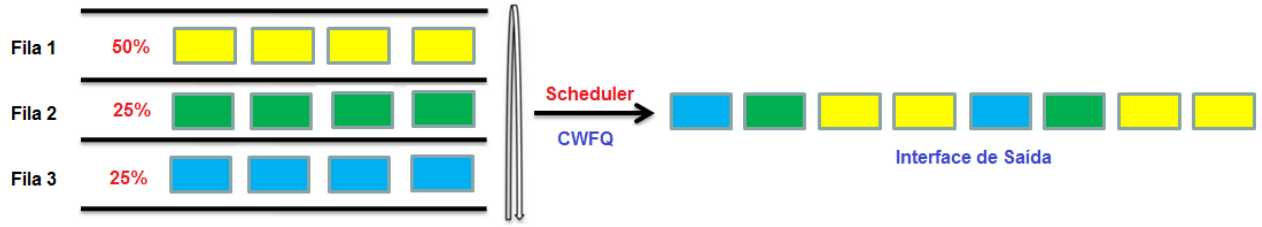


O Round Robin é utilizado no "Weighted Fair Queuing" ou WFQ. O WFQ tenta balancear a disponibilidade de largura de banda entre os fluxos que estão sendo enviados de maneira igual, por isso o nome "fair-queuing", em português "fila justa ou igualitária".

Utilizando esse método um usuário que está utilizando uma largura de banda para enviar seus dados tem uma menor prioridade que outro usuário de baixa velocidade. Muitas vezes o WFQ é o método padrão utilizado pelas interfaces serias nos roteadores Cisco.

Existe uma variação do método de agendamento anterior chamado "Class-Based Weighted Fair Queuing" ou CBWFQ. Apesar do nome complicado esse método de agendamento de filas nada

mais é que um WFQ "Class Based" quer dizer "baseado em classes", isso diz muito sobre esse método de enfileiramento. Por exemplo, temos três filas e a fila 1 terá 50% a mais de prioridade que as filas 2 e 3, as quais cada uma tem 25% de prioridade no tráfego, veja como fica na figura abaixo.

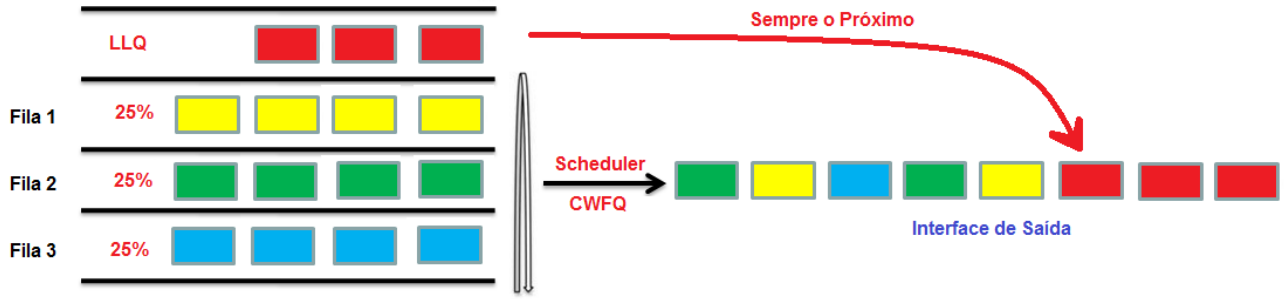


Com o CWFQ você pode definir uma largura de banda para determinados tipos ou classes de tráfego. Por exemplo, você pode dedicar 20% da largura de banda (bandwidth) para o VoIP (RTP) e 40% para um determinado aplicativo da empresa, como o SAP. Assim os 40% restantes da banda que não foram especificados na CWFQ são tratados pelo roteador utilizando uma fila WFQ.

O Round Robin, seja ele WFQ ou CWFQ, não é eficiente para voz e vídeo, pois ele pode trazer muito delay e variação de delay (jitter) para os pacotes, o que é prejudicial a esse tipo de tráfego.

Para pacotes RTP (Real time protocol) de voz ou vídeo o mais aconselhável é utilizar o "Low Latency Queuing" ou LLQ, também é conhecido como PQ-CWFQ (Priority Queue CWFQ). O LLQ é exatamente igual ao CBWFQ com a adição de uma priority queue (PQ – fila de alta prioridade) em seu funcionamento.

Note que se um pacote chegar na fila de alta prioridade (priority queue – PQ) ele sempre será o próximo a ser enviado, pois ele tem prioridade sobre os demais tráfegos das filas 1, 2 e 3, as quais utilizam o CWFQ como scheduler.



Por exemplo, o **VoIP** em uma fila **LLQ** terá largura de banda garantida e será enviado antes dos demais tráfegos. Se fosse no CBWFQ puro, esse mesmo tráfego de voz poderia ter uma garantia de 60% de largura de banda e mesmo assim não ter seu tráfego enviado antes do roteador garantir outros tráfegos que estão também priorizados.

Para fechar esse item vamos analisar algumas estratégias de QoS muitas empresas utilizam na prática:

- Utilizar um método round robin como o CBWFQ para dados e voz/vídeo não interativos.
- Em links de baixa velocidade procurar dar mais largura de banda para aplicativos de críticos para a empresa (business-critical) e menos prioridade aos menos críticos.
- Utilizar priority queue com LLQ para voz e vídeo interativos para garantir baixo delay, jitter e perda de pacotes.

- Separar voz e vídeo em filas diferentes, assim pode-se definir uma política separada para cada um dos tipos de tráfego.
- Calcular a largura de banda correta para cada fila prioritária para que pacotes dessas filas não sejam descartados pelos mecanismos internos de policiamento de tráfego.
- Utilizar mecanismos como Call Admission Control (CAC – controle de admissão de chamadas) para evitar que o excesso de chamadas de voz e vídeo não comprometam a rede como um todo.

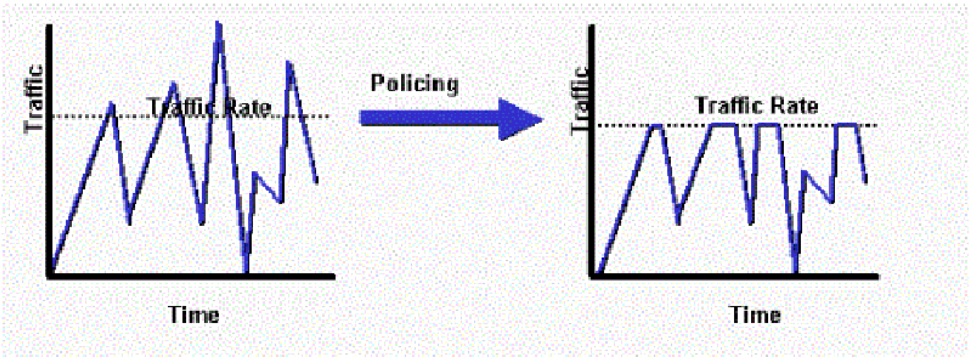
8.7 Policing

Ambos policing e shaping monitoram a taxa de bits das mensagens que são trocadas por um dispositivo. Ambos procuram manter essa taxa em um determinado valor ou abaixo dele utilizando diferentes recursos: policers descartam pacotes e shapers normalmente seguram os pacotes em uma fila e atrasam o envio para acertar a taxa de bits.

Portanto, a função do "Policing" é de medir o tráfego ao longo do tempo, comparar com uma política de tráfego previamente configurada e tomar uma ação para ajustar a taxa de bits até o nível esperado.

A ação do policer pode ser descartar o pacote o marcá-lo para uma ação em outro dispositivo ao longo da jornada do pacote até o destino.

Abaixo tem um gráfico de uma rede com policing, note que após o policing o tráfego (traffic rate) fica limitado a banda configurada como máxima via configuração.



Apesar de normalmente os pacotes serem descartados, o policing permite alguns picos de tráfego chamados de "burst" depois de um período de inatividade. Esses picos normalmente são de curta duração e servem para não descaracterizar tráfegos que tem essa característica.

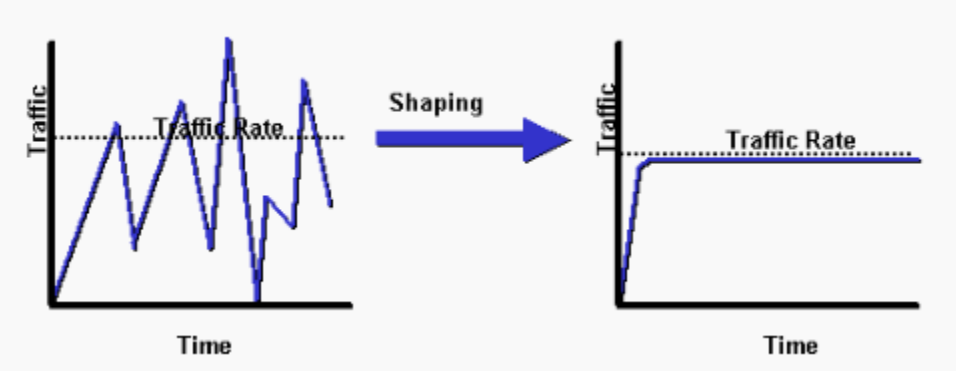
O policing é ativado por interface e normalmente na entrada dos pacotes (ingress), porém pode ser aplicado em ambas as direções.

Normalmente o policing é utilizado em provedores de serviço para garantir a banda contratada pelo cliente sem afetar o restante da rede, por exemplo, no Metro Ethernet pode-se fazer um policing na entrada das interfaces para garantir que o CIR mínimo seja cumprido e os pacotes que ficarem acima da CIR podem ser marcados para serem descartados em caso de congestionamento na rede.

Dessa maneira um cliente com um link de 100Mbps e CIR de 10Mbps pode chegar a utilizar os 100Mbps de banda, porém os pacotes que ultrapassam os 10Mbps são marcados para serem descartados pela rede em caso de congestionamento. Essa estratégia garante ao cliente um uso melhor da sua largura de banda sem prejudicar os demais usuários, os quais serão garantidos pelos descartes acima da CIR em caso de congestionamento.

8.8 Traffic Shaping

O shaping, ao contrário do policing, normalmente tem um gráfico estável em relação a velocidade máxima configurada. Veja a imagem a seguir.



No shaping ao invés de haver o descarte de pacotes, o tráfego excessivo é enfileirado e de tempos em tempos os pacotes são enviados.

Portanto se o provedor de serviços precisar garantir que a banda nunca ultrapasse a CIR do cliente o shaping é o método mais indicado, pois ele mantém o tráfego de saída constante.

Os shapers criam filas para segurar as mensagens durante o congestionamento, por exemplo, você pode utilizar o CBWFQ e LLQ para fazer o shaping das filas e garantir um fluxo mais constante na saída da interface.

Esse método traz duas desvantagens: aumento na latência (delay e jitter) devido a necessidade de enfileiramento (segurar o tráfego excessivo na saída) e do uso de memória e processamento para gerenciar a fila.

Para reduzir o efeito do atraso você terá que trabalhar o intervalo de tempo (Tc) que o shaper envia as informações, por exemplo, se você tem um link de 1Gbps e CIR de 200Mbps podemos dizer que 20% do tempo o link vai estar ocupado e os outros 80% do tempo nada deve ser enviado, pois 200Mbps são apenas 20% do total do link que é 1Gbps.

Por exemplo, com o Tc igual a um segundo (1000 ms) podemos mandar 1Gbps por 200ms e os outros 800ms restantes o link deve ficar desocupado. Isso vai gerar um atraso de 800ms entre os pacotes de voz, mesmo eles estando em uma fila prioritária.

Para voz e vídeo utilizando shaping recomenda-se utilizar um Tc de 10ms, assim os pacotes de voz e vídeo nunca irão esperar mais que 10ms para serem enviados considerando que eles estão em filas de alta prioridade.

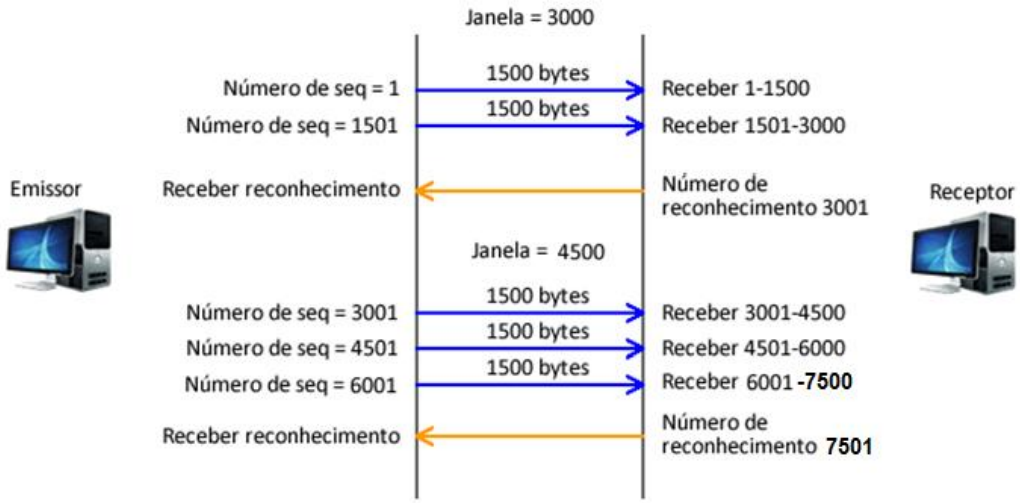
Os shapers são ativados na interface de saída (egress) dos dispositivos.

8.9 Congestion Avoidance

As técnicas para evitar congestionamento ou "Congestion Avoidance" visam monitorar o tráfego TCP e antecipar possíveis gargalos de rede que possam causar congestionamento. Isso é feito através de monitoração e descarte de pacotes, sendo que por padrão o roteador utilizará um recurso chamado "tail drop" para descartar os pacotes.

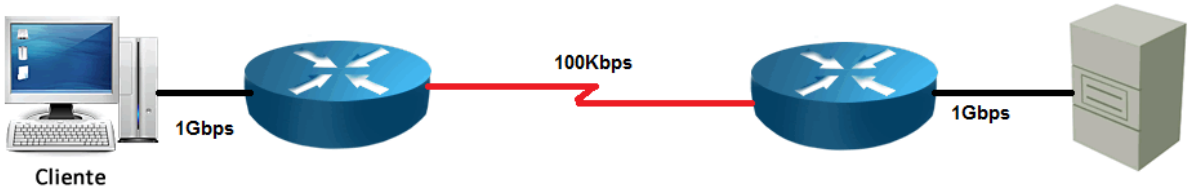
O tail drop não é a melhor opção, pois ele trata o tráfego de maneira igual e não diferencia classes por padrão, ou seja, no momento de descarte os pacotes são eliminados até que o congestionamento acabe, sem tratamento diferenciado entre as filas ou tipos de pacotes/tráfego.

O nome tail drop vem da maneira que ocorre o congestionamento no TCP devido ao janelamento (windowing). Se você lembrar do curso Fundamentos de Redes Cisco o protocolo TCP define um tamanho máximo de bytes que podem ser enviados, o qual aumenta gradativamente conforme o transmissor vai recebendo as confirmações (ACK) dos bytes enviados ao receptor. Veja abaixo onde a janela aumenta de 3000 para 4500 bytes.

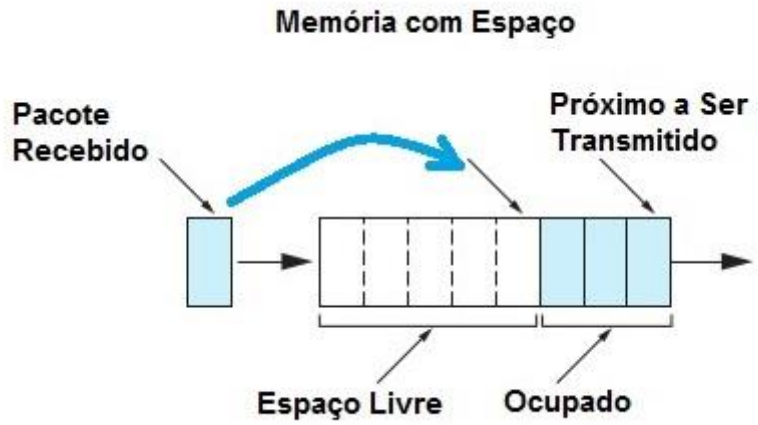


Essa janela aumenta até um momento que o receptor percebe que um segmento foi perdido e não envia o reconhecimento que o transmissor esperava (ACK), nesse momento o transmissor diminui pela metade o tamanho da janela de transmissão.

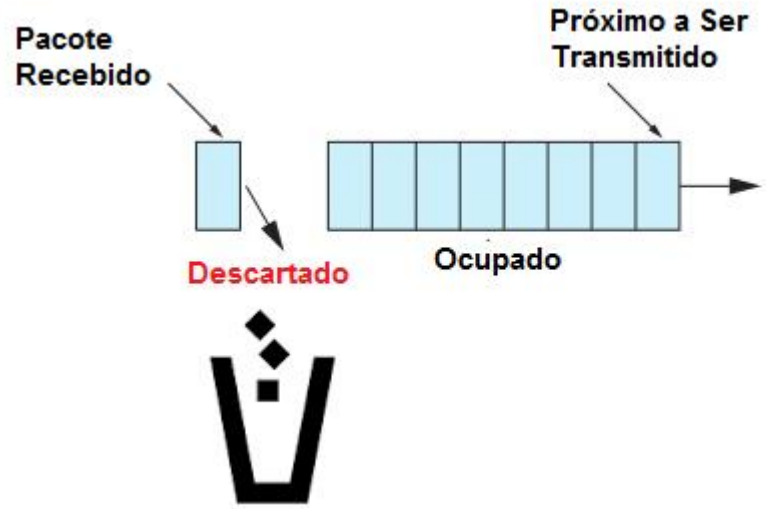
Mas quem está descartando pacotes? Por exemplo, um roteador no meio do caminho entre transmissor e receptor tem uma LAN de 1Gbps e um link WAN de baixa velocidade com 100kbps.



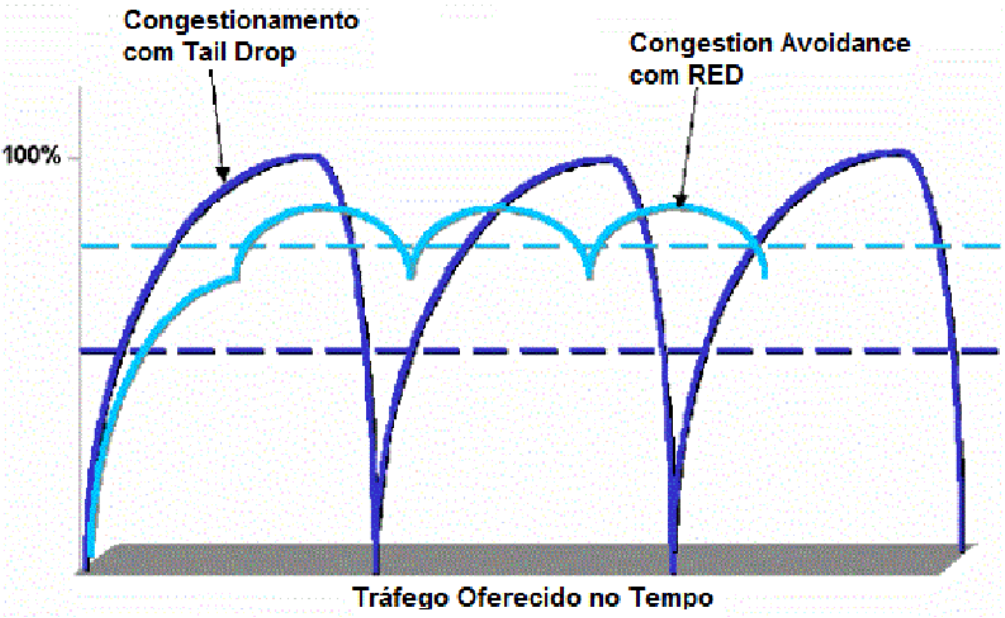
A medida que o TCP aumenta sua janela de transmissão essa interface de baixa velocidade vai chegando a sua capacidade máxima, ou seja, seus buffers (memória) de saída vão sendo ocupados mais que o normal.



Quando ela chega a sua capacidade máxima (buffer ou fila de saída 100% ocupada) esses segmentos TCP serão enfileirados no buffer de saída, o qual se for totalmente lotado haverá o tail drop, ou seja, os pacotes novos que chegarem serão descartados, por isso descarta o tail ou "final da fila" (o pacote que acabou de chegar).



Quando o roteador descarta pacotes o transmissor utiliza novamente o Slow Start (mecanismo de início suave do TCP) para iniciar a transmissão e você nota uma queda na curva dos bytes transmitidos nas interfaces para aquele fluxo conforme gráfico abaixo. Colocamos também a curva do tráfego com um recurso de congestion avoidance configurado para você ver a diferença da média da banda utilizada como aumenta sensivelmente.



Os mecanismos de congestion avoidance tratam esse problema antes que ele ocorra descartando pacotes conforme configurado e não após o congestionamento. A estratégia é simples: jogue algo fora pouco no curto prazo para ter menos descarte a longo prazo.

Além disso, essas técnicas de congestion avoidance mais avançadas que o tail drop, que é o padrão, podem utilizar os valores de DSCP para priorizar quem será descartado antes e tornar o processo muito mais eficiente.

Entre os mais comuns recursos de congestion avoidance temos o Random Early Detection (RED), que funciona muito bem para redes de alta velocidade, o Weighted Random Early Detection (WRED) e o distributed WRED (DWRED), os quais combinam as capacidades do RED com os valores de DSCP para priorização do tráfego a ser descartado primeiro.

Basicamente com essas técnicas você define limiares ou thresholds onde os descartes podem começar a ocorrer, por exemplo, com 20% da fila ocupada comece a descartar pacotes conforme sua prioridade. Também é possível configurar um limiar máximo, o qual se excedido todo o tráfego é descartado até o congestionamento parar.

9 Configurando o Acesso Remoto via SSH

9.1 Introdução

Já aprendemos no curso **Cisco IOS Essentials** 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, ou seja, é uma forma insegura de acesso remoto e administração de dispositivos, pois as informações podem ser "espionadas" e copiadas facilmente.

A configuração básica do Telnet é realizada na line vty definindo uma senha e o login:

```
Line vty 0 4
 password cisco
 login
```

Além da senha simples você pode configurar um usuário na base de dados local dos dispositivos ou então utilizar um servidor TACACS ou RADIUS para autenticação remota (vamos estudar o AAA e a autenticação remota em outro curso da trilha para o CCNA).

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, muito mais segura e recomendada que o Telnet.

O SSH utiliza o protocolo TCP na porta 22 e o Telnet a porta 23.

9.2 Passos para Ativação do SSH

Acompanhe abaixo os comandos necessários para ativar o SSH.

Passo 1. Configure a senha de enable, o hostname, usuário e senha para login na base de dados local do roteador:

```
enable secret dltec1234
hostname DlteC
username dltec [privilege 15] secret dltec1234
```

Passo 2. Configure o domínio do DNS:

```
ip domain-name dltec.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 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
```

Se o comando "login local" não entrar você precisa digitar o comando "**no aaa new-model**" em modo de configuração global e voltar para a line em seguida para finalizar essa configuração.

Passo 5. Opcionalmente configure a versão do SSH.

Configurando SSH v1:
```
Router(config)#ip ssh version 1
```

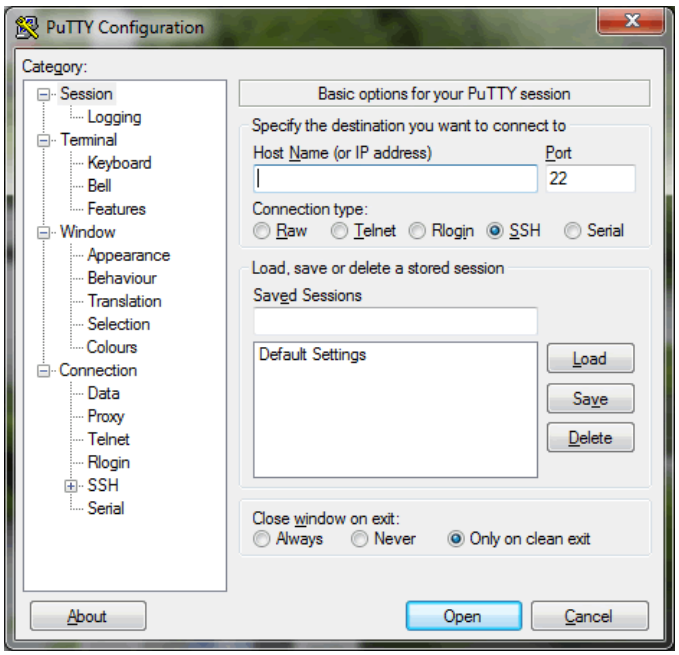
Configurando SSH v2:
```
Router(config)#ip ssh version 2
```

Configurando SSH v1 e v2:
```
Router(config)#no ip ssh version
```

A mesma configuração pode ser utilizada para acesso IPv4 ou IPv6.

9.3 Acessando um Dispositivo Cisco via SSH

Para acessar um roteador ou switch via SSH você deverá utilizar um programa SSH Client, por exemplo, o Putty ou Teraterm.



Você pode utilizar o comando "ssh" na linha de comando do Cisco IOS utilizando a opção "-l" para definir o usuário de acesso SSH e logo após digitando o IP remoto. Veja exemplo a seguir onde o usuário é "dltec" e o IP remoto 192.168.1.1.

```
SW-DlteC#ssh -l dltec 192.168.1.1
CC## DlteC do Brasil - Acesso Restrito ##
Password:
CC
####################################################

  DLTEC DO BRASIL - ROTEADOR DE ACESSO RESTRITO

####################################################

DlteC-GW#
```

9.4 Script de Configuração Básica do SSH

Abaixo seguem os comandos utilizados na vídeo aula em forma de script.

```
hostname R1
!
enable secret dltec
!
username dltec secret dltec123
!
ip domain-name dltec.com.br
!
crypto key generate rsa modulus 1024
!
line vty 0 4
transport input ssh
login local
end
```

10 Uso do TFTP e FTP nas Redes IP

10.1 Introdução

Os protocolos TFTP (Trivial File Transfer Protocol) e FTP (File Transfer Protocol) são utilizados para transferência de arquivos entre dispositivos, porém tem funcionamento e características diferentes um do outro.

Vamos iniciar estudando as características de cada um dos protocolos e a seguir o uso deles pelos dispositivos Cisco.

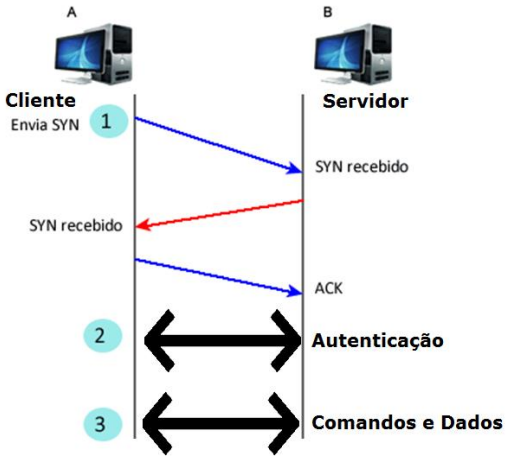
10.2 Protocolo FTP

O FTP ou File Transfer Protocol é um protocolo antigo (1985) e definido na RFC 959 que visa permitir a transferência de arquivos entre clientes e servidores utilizando o TCP como transporte.

Portanto, em uma rede que utiliza FTP os arquivos ficam armazenados em pastas em um dispositivo configurado como servidor, o qual "escuta" nas portas 20 e 21 (mais comum) do protocolo TCP por conexões de clientes.

A porta TCP 21 é utilizada para envio de mensagens de controle e a porta TCP 20 é normalmente utilizada para transferência dos dados.

Como qualquer serviço TCP o FTP inicia por uma fase de estabelecimento da sessão TCP através de um 3-way handshake (1), depois opcionalmente passa por uma fase de autenticação (2) e por último o envio de comandos/transferência de arquivos (3).



Com o serviço de FTP um cliente pode dar comandos para:

- Listar diretórios e arquivos
- Adicionar ou remover diretórios e arquivos
- Transferir arquivos do servidor para o cliente ou vice versa

No servidor FTP é possível definir que arquivos e diretórios são apenas de escrita ou leitura/escrita.

Dependendo da aplicação do servidor FTP essa definição pode ser feita por usuário criado, ou seja, dependendo do login/senha do usuário ele pode ter determinado perfil de acesso com diferentes pastas.

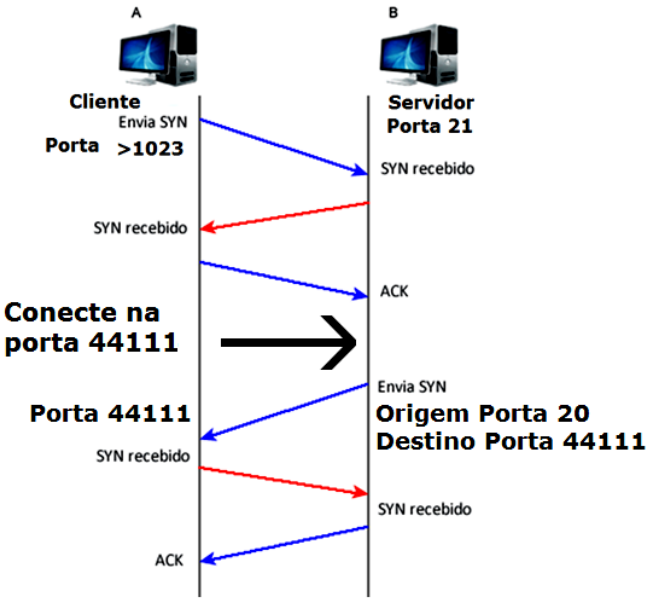
Além disso, o FTP também permite o acesso em modo "anônimo", ou seja, sem necessidade de utilizar usuário e senha.

10.2.1 FTP Modo Ativo versus Modo Passivo

O protocolo FTP pode ser configurado em dois modos de operação: **Ativo** (Active) ou **Passivo** (Passive).

O mais comum é o modo ativo, onde utilizamos as portas bem conhecidas TCP 20 e 21 no servidor e portas randômicas nos clientes (acima de 1023).

Portanto, no modo ativo o cliente inicia uma conexão TCP na porta 21 (canal de controle), enviando um SYN para dar início ao processo de 3-way handshake. Após finalizado esse processo de estabelecimento da conexão da porta 21, algumas ações são tomadas pelo servidor e em seguida ele abre uma conexão com o cliente enviando um SYN na porta TCP 20 (canal de dados) em direção ao cliente que usará uma porta randômica acima de 1023.

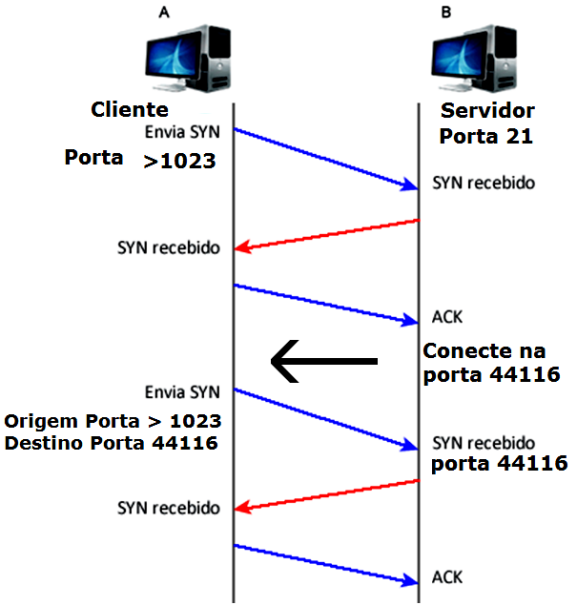


No modo ativo o cliente informa a porta que o servidor deve enviar o SYN e abrir a conexão com o comando PORT via canal de controle.

Resumindo a operação do FTP no Modo ativo:

1. O cliente solicita abertura do canal de controle através de uma porta local TCP randômica (acima de 1023) enviando um SYN para a porta TCP 21 do servidor
2. O 3-way handshake é finalizado e o canal de controle aberto
3. O cliente envia o comando PORT via canal de controle informando que vai utilizar a porta 44111 (uma porta randômica escolhida no cliente) como canal de dados
4. O servidor confirma através do canal de controle
5. O servidor abre o canal de dados enviando um SYN para o cliente utilizando a porta TCP de origem 20 e o destino a porta 44111 (informada no comando PORT)
6. O 3-way handshake é finalizado e o canal de dados está aberto
7. Os canais de controle e dados estão abertos e prontos para uso

Já no modo passivo o cliente abre ambas as sessões TCP, porém o servidor envia via canal de controle o comando PASV, informando que ele utiliza o modo passivo, assim como o número da porta de dados a ser utilizada sendo acima de 1023 também, ou seja, nesse modo o canal de controle continua sendo via porta TCP 21, porém os dados serão trocados por uma porta TCP acima de 1023.



Resumindo a operação do FTP no Modo passivo:

1. O cliente solicita abertura do canal de controle através de uma porta local TCP randômica (acima de 1023) enviando um SYN para a porta TCP 21 do servidor
2. O 3-way handshake é finalizado e o canal de controle aberto
3. O servidor envia o comando PASV via canal de controle informando que vai utilizar a porta 44116 (uma porta randômica escolhida no servidor) como canal de dados
4. O cliente confirma através do canal de controle
5. O cliente abre o canal de dados enviando um SYN para o servidor utilizando a porta TCP de origem randômica e o destino a porta 44116 (informada no comando PASV)
6. O 3-way handshake é finalizado e o canal de dados está aberto
7. Os canais de controle e dados estão abertos e prontos para uso

10.2.2 Secure FTP e Opções mais Seguras para Transferência de Arquivos

Como já citado, tanto o FTP como o TFTP não oferecem segurança no envio das informações através da rede, pois eles não possuem nenhum mecanismo de criptografia.

Apesar do FTP possuir o recurso de autenticação via usuário e senha, tanto os dados dos usuários como as informações de controle são passadas na rede em texto claro, ou seja, se os pacotes forem capturados existe a possibilidade de leitura.

Mesmo assim, ambos os protocolos são muito utilizados tanto em Intranets como na Internet!

Existem algumas opções mais seguras para transmissão de arquivos:

- FTPS ou FTP Secure
- SSH File Transfer Protocol ou SFTP
- Secure Copy Protocol ou SCP

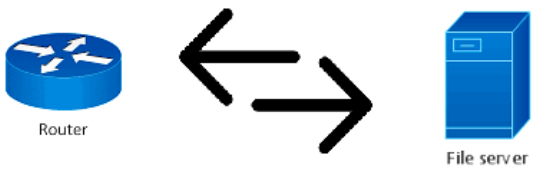
O FTP Secure ou FTPS é uma adaptação do FTP que pode utilizar certificados digitais para autenticação e TLS (Transport Layer Security) para criptografar tanto o canal de dados como o controle. Ele utiliza as portas 990 para controle e 989 para os dados.

Já o SFTP utiliza a mesma criptografia oferecida pelo SSH para proteger o acesso remoto aos dispositivos para proteger também a troca de arquivos entre um cliente e um servidor.

Já o Protocolo SCP apenas implementa a transferência de arquivos conectando-se ao servidor usando SSH e lá executando um serviço SCP (scp). O programa do servidor SCP geralmente é exatamente o mesmo programa que o cliente SCP utiliza.

10.3 Protocolo TFTP

O TFTP ou Trivial File Transfer Protocol (Protocolo de Transferência de Arquivos Simples) é um serviço sem conexão que usa o UDP (User Datagram Protocol – Protocolo de Datagrama de Usuário) como transporte de dados.



O TFTP está definido na RFC 1350 e utiliza a porta 69 no servidor e uma porta randômica no cliente, porém diferente do FTP não possui a opção de autenticação dos usuários antes da troca de arquivos.

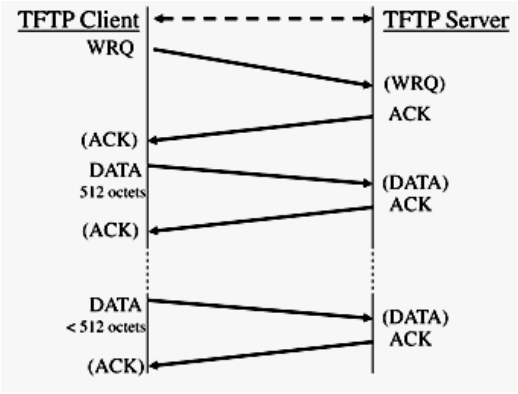
No servidor você pode configurar os arquivos como apenas escrita ou escrita/leitura.

É usado em roteadores, switches e outros dispositivos de infraestrutura de redes para transferir arquivos de configuração, imagens de sistema operacional, firmware e outros arquivos pequenos, sendo muito utilizada na administração dos dispositivos Cisco.

Ele possui apenas cinco mensagens:

- **RRQ**: É a solicitação feita pelo cliente TFTP para ler ou buscar um arquivo do servidor.
- **WRQ**: É a solicitação feita pelo cliente TFTP para transferir ou enviar um arquivo pelo servidor.
- **DATA**: São as mensagens que contêm blocos de um arquivo a ser enviado ao servidor.
- **ACK**: É a resposta do lado receptor confirmando a recepção de um bloco do arquivo para o remetente.
- **ERROR**: É uma mensagem enviada ao par referente a alguma operação inválida realizada.

Veja exemplo a seguir de uma escrita de arquivo a partir do cliente para o servidor TFTP.



Note que agora o transporte é via UDP, não existe 3-way handshake, simplesmente o Cliente envia a mensagem de WRQ informando que vai escrever um arquivo e o servidor confirma com ACK ou não.

Após a confirmação do servidor os blocos do arquivo são enviados até sua finalização. Note que os blocos são trocados com as mensagens de Data e confirmados com um ACK.

Toda essa troca de mensagem está no nível da aplicação, pois para o UDP são apenas envios de datagrama, NÃO É PAPEL DO UDP esse controle e sim da aplicação.

O TFTP é útil em algumas redes locais porque opera mais rápido do que o FTP em um ambiente estável.

10.4 Uso do FTP e TFTP pelos Dispositivos Cisco

Tanto o FTP como o TFTP podem ser utilizados para transferência de arquivos entre servidores e dispositivos Cisco como roteadores e switches.

Podemos utilizar um servidor FTP ou TFTP para armazenar backups dos arquivos de configuração inicial, imagens de sistema operacional ou Cisco IOS, assim como outros arquivos utilizados pelos roteadores, switches, telefones IP, access points e demais dispositivos de infraestrutura da rede.

Executamos essas tarefas dentro dos roteadores e switches Cisco com o comando "copy" e as opções "tftp" e "ftp".

10.4.1 Utilizando o TFTP para Backup da Configuração

Para fazer o backup do arquivo de configuração de um roteador ou switch Cisco em um servidor 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-confg]?
!!
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-confg** 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.

Para voltar a configuração que está em um servidor TFTP para um roteador é preciso ter cuidado, pois quando inserimos informações na "running-config", ou seja, na configuração que está rodando no dispositivo ele faz um "merge" de vários comandos ou até mesmo substitui outros, por isso é preciso ter cuidado.

O ideal é copiar a configuração para a NVRAM (copy tftp: startup-config) e reiniciar o dispositivo, porém lembre-se que a configuração atual e salva serão substituídas por esse novo arquivo.

10.4.2 Utilizando o TFTP para Administrar o Cisco IOS

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".

```
MatrizCTBA#delete 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#
Exemplo do comando "Erase flash"
MatrizCTBA#erase flash:
Erasing the flash filesystem will remove all files! Continue?
[confirm]
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeee ...eraseee
Erase of flash: complete
MatrizCTBA#
```

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 TFTPDNLD.

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 atualizá-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... eeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
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 reinicializar o equipamento. Isso pode ser feito com o comando "**verify /md5 flash:nomedoios.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 incialização.
8. Executar um reload para o roteador carregar a nova versão de IOS.

10.4.3 Utilizando FTP 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.

Podemos também fazer o mesmo que estudamos para o TFTP, ou seja, fazer backup de configurações, imagens de Cisco IOS, arquivos dos dispositivos, assim como fazer upload de informações do servidor para dentro dos roteadores e switches.

Veja os passos de configuração abaixo, pois primeiro temos que configurar a autenticação antes da utilização dos comandos copy para servidores FTP.

```
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 de acesso ao servidor FTP foram definidos nos comandos "ip ftp username/password". No exemplo o usuário (username) é cisco e a senha (password) é cisco123. Esses dados são passados pelo administrador de servidores ou configurados por você mesmo no programa do servidor FTP.

O comando "no ip ftp passive" é o padrão que aceita os dois tipos de servidores FTP, tanto no modo ativo como no modo passivo.

Com o comando "ip ftp source-interface" você pode definir o IP da interface que será coloca como origem nos pacotes IP. É importante que você antes de fazer o processo teste a conectividade entre esse endereço IP e o servidor FTP.

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:nome-do-arquivo ftp://IP-servidor/pasta".

Veja exemplo abaixo onde vamos fazer um backup do Cisco IOS (c2801-adventerprisek9-mz.124-24.T8.bin) 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#
```

10.4.4 Problemas Comuns com FTP e TFTP

Apesar de parecer um processo simples, o Upgrade ou Downgrade do Cisco IOS pode gerar 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.
- Usuário e senha do FTP.

Quando houver erros em ambiente prático em sua empresa ou cliente, procure verificar as mensagens do roteador e no programa do serviço FTP/TFTP, normalmente analisando os dois lados (servidor e roteador) fica mais fácil de resolver os problemas.

11 Conclusão do Curso

11.1 Conclusão

Bem pessoal, chegamos ao final de mais um curso!

É muito importante que nesse ponto do curso você tenha domínio dos seguintes itens:

- Configurar e verificar o NAT de maneira estática ou através de pools
- Configurar e verificar o NTP operando em modo cliente e servidor
- Explicar a função dos serviços de DHCP e DNS em uma Rede IP
- Explicar a função do protocolo SNMP na operação de uma rede IP
- Descrever o uso do syslog incluindo suas facilidades e níveis
- Configurar e verificar o DHCP cliente e relay
- Explicar o encaminhamento por salto ou "Per-hop Behavior" (PHB) para o QoS, tais como classificação, marcação, enfileiramento, congestionamento, policing e shaping
- Ativar o SSH em dispositivos Cisco
- Descrever o funcionamento e uso dos serviços de TFTP e FTP na Rede

Lembre-se que esse curso conta também com vídeo aulas, questionários e laboratórios extras que estão dentro da trilha do CCNA para quem está se preparando para a prova de certificação ou então quer ter os conhecimentos de um profissional nível associado exigido pela Cisco.