DlteC do Brasil®
www.dltec.com.br
info@dltec.com.br | 41 3045.7810

DLTEC DO BRASIL

SERVIÇOS DE REDE

Serviços de Rede

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

Para mais informação visite www.dltec.com.br

Seja muito bem-vindo(a) ao curso Serviços de Rede!

Nesse curso iremos estudar com mais detalhe os principais Serviços de Rede e Aplicações TCP/IP.

Nesse curso você vai aprender o princípio de funcionamento e características dos seguintes protocolos de camada de aplicação: DNS, DHCP, DHCPv6, NTP, HTTP, HTTPS, SMTP, POP3, IMAP, FTP, SFTP, TFTP, RDP, Telnet, SSH, VNC, SNMP, SYSLOG, RTP/RTCP, SIP, H.323, LDAP, LDAPS e SMB.

Além disso, vai estudar o funcionamento e características dos serviços de NAT e PAT, assim como os Proxy Servers.

No final desse curso você aprenderá as opções de disponibilização dos serviços e exemplos práticos.

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

Bons estudos!

Introdução

Olá!

Existem diversos serviços de Rede, porém muitos não são bem compreendidos.

Serviços como DNS e DHCP são o coração de uma rede TCP/IP, porém existem outros serviços que devem ser conhecidos ou até mesmo dominados por quem deseja ser um profissional da área de Redes ou Infraestrutura de TI com destaque no mercado.

Não somente para área de Infra e administração de Redes esse assunto é importante, pois a área de segurança também depende do conhecimento das aplicações e suas características.

Esperamos que você aproveite ao máximo este material, que foi idealizado com o intuito verdadeiro de fazê-lo(a) obter êxito na sua vida profissional.

Estamos torcendo pelo seu sucesso!

Bons estudos!

Serviços de Rede

Objetivos

Ao final desse curso você deverá ter conhecimentos sobre:

- Conhecer os principais serviços e aplicações em Redes TCP/IP.
- Descrever o funcionamento dos serviços da camada de Aplicação:
  - Serviços de e-mail
  - Serviços de terminal e acesso remoto
  - Serviços de web
  - Gerenciamento de redes
  - Troca de arquivos em rede
  - Fornecimento de endereços IPs dinâmicos
  - Voz e Vídeo sobre IP
  - Serviços de diretórios
  - Compartilhamento de arquivos
  - Sincronização dos relógios dos dispositivos de Rede
- Descrever o funcionamento dos serviços da camada de Rede
  - NAT, PAT e Proxy
  - Encaminhamento de portas
- Descrever as possíveis opções de disponibilização dos serviços de Rede: Servidor, VM e Cloud

Sumário

1 Introdução ao Curso

Bem-vindo ao **Curso Serviços de Rede**, o qual também faz parte do conteúdo da formação de Redes da DlteC do Brasil.

O curso **Serviços de Rede** possui como objetivo fornecer ao aluno uma visão abrangente sobre serviços e aplicações das camadas 7 e 3 do modelo OSI.

Ao final do curso, você deverá ser capaz de:

- Conhecer os principais serviços e aplicações em Redes TCP/IP.
- Descrever o funcionamento dos serviços da camada de Aplicação:
  - Serviços de e-mail
  - Serviços de terminal e acesso remoto
  - Serviços de web
  - Gerenciamento de redes
  - Troca de arquivos em rede
  - Fornecimento de endereços IPs dinâmicos
  - Voz e Vídeo sobre IP
  - Serviços de diretórios
  - Compartilhamento de arquivos
  - Sincronização dos relógios dos dispositivos de Rede
- Descrever o funcionamento dos serviços da camada de Rede
  - NAT, PAT e Proxy
  - Encaminhamento de portas
- Descrever as possíveis opções de disponibilização dos serviços de Rede: Servidor, VM e Cloud

Esse curso possui E-Book e não esqueça que ao final do curso você poderá emitir o seu certificado!

1.1 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**.

Assim você terá um aproveitamento muito melhor do curso.

2 Introdução aos Serviços de Rede

Maioria dos serviços de Rede são conhecidos como "Aplicações de Rede" e, por isso mesmo, ficam na camada 7 do modelo OSI.

Nessa camada temos diversos serviços de rede, tais como:

- **Serviço de tradução de nomes de Internet**: DNS (TCP/UDP 53)
- **Fornecimento de endereços IPs dinâmicos**: DHCP (UDP 67/68) e DHCPv6 (UDP 546 e 547)
- **Sincronização dos relógios dos dispositivos de Rede**: NTP (UDP 123)
- **Serviços de web**: HTTP (TCP 80) e HTTPS (TCP 443)
- **Serviços de e-mail**: SMTP (TCP 25), POP3 (TCP 110) e IMAP (TCP 143)
- **Troca de arquivos em rede**: FTP (TCP 20/21), SFTP (TCP 22) e TFTP (UDP 69)
- **Serviços de terminal e acesso remoto**: RDP (TCP 3389) Telnet (TCP 23), SSH (TCP 22) e VNC (TCP 5800/5900)
- **Gerenciamento de redes**: SNMP (UDP 161) e SYSLOG (TCP/UDP 514)
- **Voz e Vídeo sobre IP**: RTP/**RTCP** (UDP 16384-32767), SIP (TCP/UDP 5060/5061) e H.323 (TCP 1720)
- **Serviços de diretórios**: LDAP (TCP/UDP 389) e LDAPS (TCP 636)
- **Compartilhamento de arquivos**: SMB (TCP 445)

Vamos fazer apenas uma observação sobre o protocolo RTCP, pois ele é considerado em muitas bibliografias como um exemplo da camada de sessão, porém como ele trabalha em conjunto com o RTP deixamos na lista para consolidar essa ideia.

Porém, existem outros serviços de Rede que você normalmente precisa implementar para que tudo funcione corretamente que não estão situados na camada 7 do modelo OSI.

Esses serviços de "Tradução de Endereços" são utilizados para acesso à Internet principalmente em redes IPv4, pois normalmente as empresas implementam faixas de endereços privativos (não roteáveis na Internet) em suas redes internas ou Intranet.

Por isso mesmo vamos também estudar a função do Network Address Translation ou NAT e o serviço de Proxy.

Vamos começar estudando os serviços da camada de aplicação pelo DHCP.

Bons estudos!

3 Fornecimento Dinâmico de Endereços IP: DHCP e DHCPv6

Protocolos: DHCP (UDP 67 – Server | 68 - Client) e DHCPv6 (UDP 546 - Client | 547 - Server)

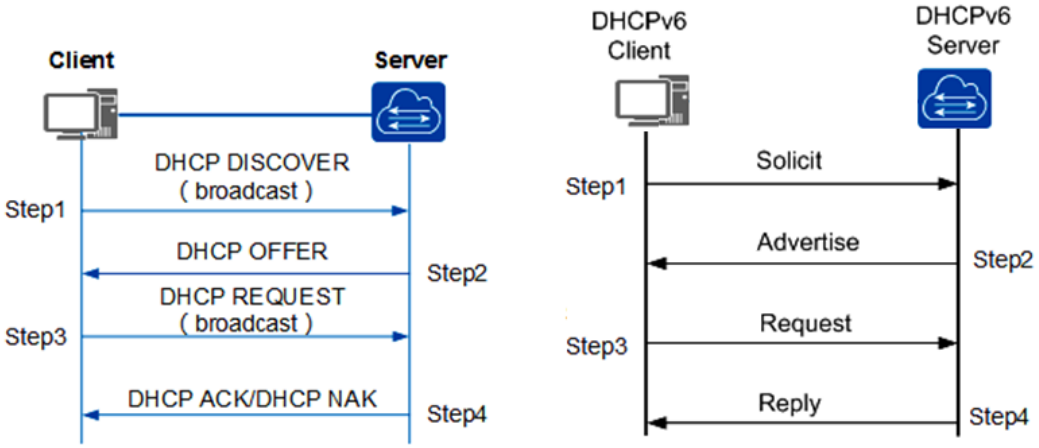
O protocolo DHCP está definido nas RFCs 2131 e 2132 como um padrão IETF (Internet Engineering Task Force) baseado no protocolo BOOTP, no qual o DHCP compartilha muitos detalhes de implementação.

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

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

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

Abaixo seguem as mensagens trocadas entre Cliente e Servidor DHCP e DHCPv6 respectivamente.



Existe uma diferença do funcionamento do IPv4 em relação ao IPv6, pois no IPv6 não temos mais mensagens em broadcast, por isso mesmo as mensagens do IPv6 são trocadas em Multicast.

As mensagens do DHCP são trocadas da seguinte maneira:

- DHCP Discover (1): O cliente de DHCP pede um endereço IP.
- DHCP Offer (2): Um endereço IP é oferecido ao cliente.
- DHCP Request (3): O cliente aceita a oferta e pedidos do endereço.
- DHCP Acknowledge (4): O endereço é nomeado oficialmente.

No DHCPv6 as mensagens trocadas são:

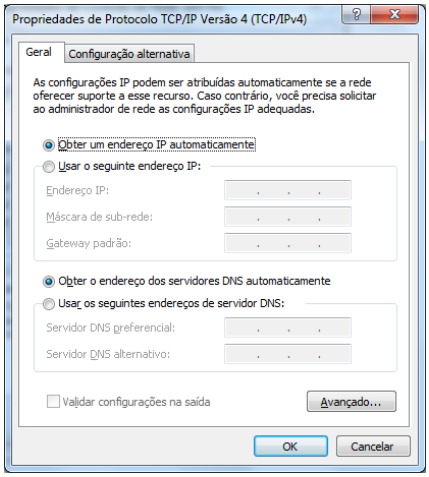
- Solicit (1): mensagem utilizada pelos clientes para localizarem os servidores DHCPv6.
- Advertise (2): mensagem enviada pelos servidores DHCPv6 para indicar que seus serviços DHCPv6 estão ativos para operar. Ela é enviada em resposta à mensagem Solicit.
- Request (3): mensagem enviada diretamente a um servidor DHCPv6 para requisitar parâmetros de configuração, incluindo o endereço IPv6.
- Confirm (4): mensagem enviada pelo cliente para qualquer servidor DHCPv6 disponível para confirmar se o endereço adquirido ainda é válido no enlace conectado.

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

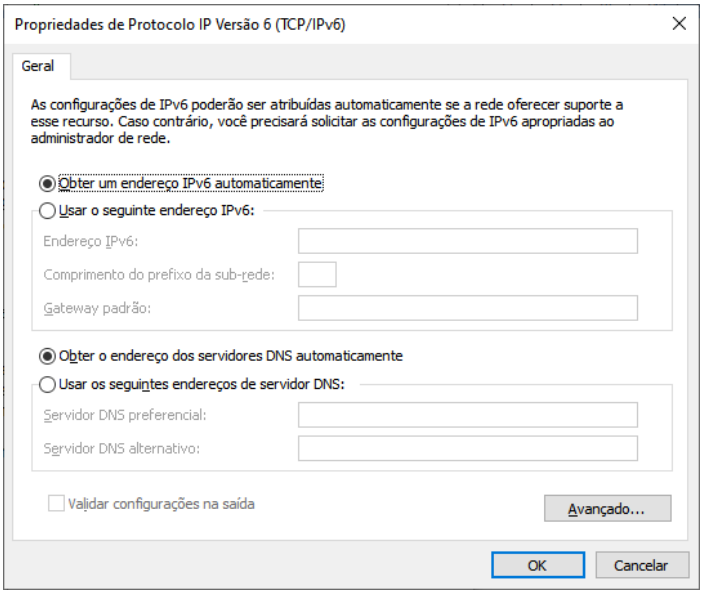
O padrão da maioria dos sistemas operacionais atualmente é deixar a placa de rede com o cliente DHCP habilitado, pois a maioria dos equipamentos de acesso à Internet, como os roteadores ADSL ou os Cable Modems, já fornecem os dados para os clientes via DHCP, não sendo necessária a configuração manual do IP nos computadores clientes.

Na placa de rede dos computadores a configuração do DHCP ou IP estático (manual) é realizada no mesmo local em ambiente Windows, o qual já vimos anteriormente.

Veja na figura a seguir a configuração de uma placa de rede com DHCP, onde as opções de obter um endereço IP e DNS automaticamente estão habilitadas.



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

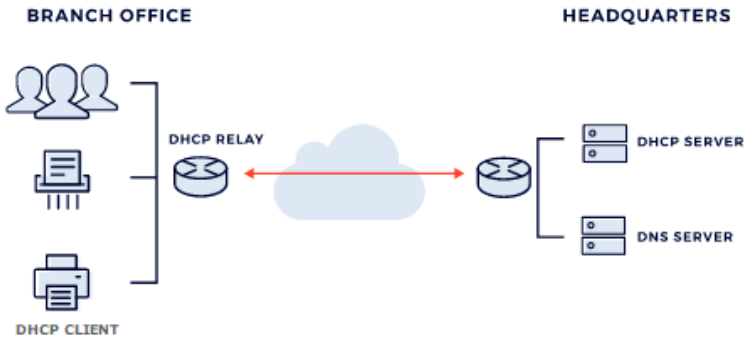


Existem três tipos de funções no DHCP:

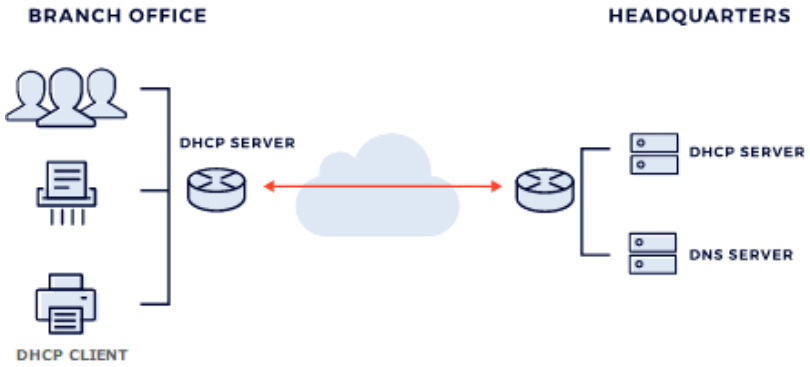
- **Cliente ou Client**: dispositivos que tem um aplicativo cliente que vai solicitar os dados da interface de rede ao servidor DHCP.
- **Server ou Servidor**: dispositivo que responde aos clientes ou aos agentes Relay com uma determinada configuração de rede.
- **Agente Relay**: dispositivo que encaminha a solicitação de um cliente DHCP para um servidor remoto que não está na mesma rede local do cliente, ou seja, uma arquitetura centralizada.

Existem dois tipos de arquitetura do DHCP:

- **Centralizada**: onde o servidor DHCP está centralizado e TODOS os clientes têm suas informações negociadas via agentes Relay (DHCP Relay).



- **Distribuída ou Descentralizada**: Cada segmento de rede possui o serviço de DHCP independente, por exemplo, o serviço de DHCP pode ser ativado em roteadores de unidades remotas (Branch Offices) ou então por VLAN em switches L3.



Existe a possibilidade de existir arquiteturas mistas, ou seja, algumas unidades possuírem seus próprios servidores DHCP e a maioria da rede obter as informações via um servidor centralizado.

3.1 Estudo de Caso 1: DHCP e Alocação de Endereços em Redes IPv4

A seguir seguem os passos necessários para um bom planejamento e operação do serviço de DHCP em redes TCP/IP.

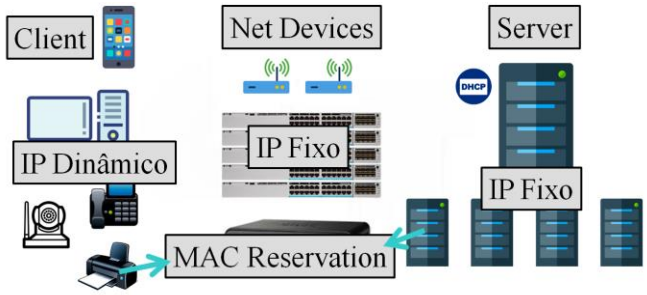
Lembramos que todas as opções foram abordadas na vídeo aula desse tópico do curso, em caso de dúvidas na leitura recorra a ela.

Passo 1: Definir a arquitetura

- Centralizada (DHCP Server + DHCP Relay ou IP Helper Address) ou
- Distribuída

Passo 2: Tipos de dispositivos e alocação de endereços

- **Endereço IP Fixo** (estático ou static IP Address): definido pelo administrador e configurado manualmente. Normalmente utilizado em dispositivos de rede e servidores.
- **Endereços IP dinâmicos**: distribuídos via serviço DHCP. São os clientes de rede como computadores, laptops, smartphones, ect.
- **MACs Reservados**: endereços distribuídos exclusivamente para determinados clientes pelo servidor DHCP. Existe um vínculo entre o MAC Address do cliente e o endereço IP que o servidor irá fornecer, portanto é como se fosse um IP fixo, porém sem necessidade de configuração manual no cliente.
- Tipos de clientes no Servidor DHCP:
  - **Clientes Dinâmicos**: PCs, tablets, smart phone, lap-top, telefone IP...
  - **Clientes com MAC Reservado**: impressoras, dispositivos de rede e servidores...



Passo 3: Definição do projeto de alocação de endereços

- Definir Endereços fixos ou estáticos
- Definir MACs Reservados e seus respectivos IPs
- Definir Escopo do DHCP (DHCP Scope): Faixas de endereços dinâmicos (pools) e MACs Reservados (vínculo MAC – IP)
- Definir Lista de Exclusão: Endereços fixos + Reservados (IP Address Exclusion) + Reserva técnica

Lembre-se que os endereços fixos e reservados devem ser excluídos com uma "lista de exclusão" do "pool" de endereços que o servidor DHCP vai fornecer para evitar "conflitos de IP".

Passo 4: Definir as Opções do DHCP: definir os parâmetros que serão passados para os clientes. Os quatro primeiros parâmetros da lista abaixo são os requisitos mínimos.

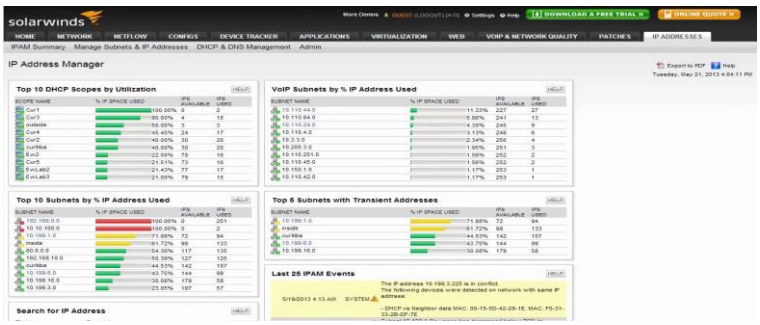
- **DHCP option 1**: subnet mask
- **DHCP option 3**: default router ou last resort gateway
- **DHCP option 6**: servidor (es) DNS (Domain Name Server)
- **DHCP option 51**: lease time
- DHCP option 2: time offset referência UTC
- DHCP option 12: Hostname (útil com dispositivos IOT)
- DHCP option 15: Nome de domínio
- DHCP option 42: lista de NTP Servers
- DHCP option 58 e 59: Renewal Time Value (T1) e Rebinding Time Value (T2)
- DHCP options 69 and 70: SMTP e POP3 respectivamente
- DHCP option 150: servidor TFTP

Passo 5: Aplicar as Configurações Conforme Planejamento

- As configurações dependem do tipo de servidor DHCP a ser utilizado.
- Os mais comuns são Windows Server, Linux e nos próprios dispositivos de rede, por exemplo, switches L3 e roteador (exemplo: Cisco IOS).

Passo 6: Monitoração e Controle do Endereçamento

- IPAM (IP Address Management ou Gerenciamento de Endereços IP)
  - Procedimento ou metodologia para gerenciamento, planejamento e rastreio de endereços IP
  - Normalmente integra os serviços de DHCP e DNS
- Ferramentas de mercado
  - Windows Server IPAM
  - SolarWinds IPAM



  - Infoblox DNS, DHCP and IP Address Management (DDI)
  - Free: IP Plan e NiPaP (Neat Address Planner)

3.2 Estudo de Caso 2: DHCPv6 e Alocação de Endereços em Redes IPv6

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:

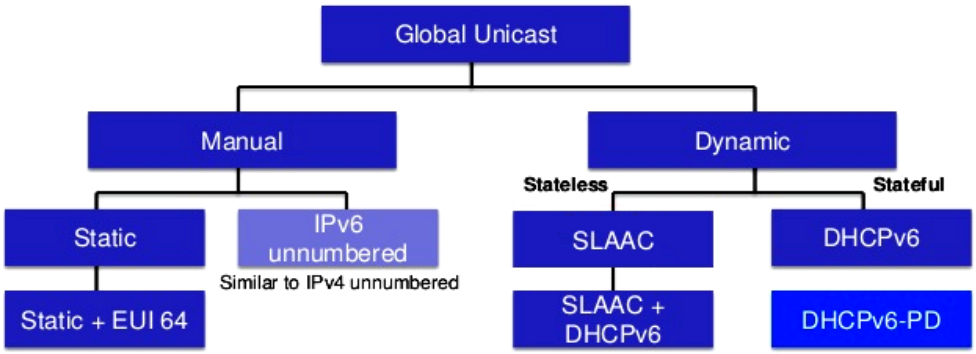
- **ff02::1:2** - todos os agentes DHCPv6 relay e servidores.
- **ff05::1:3** - todos os servidores DHCPv6.

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.

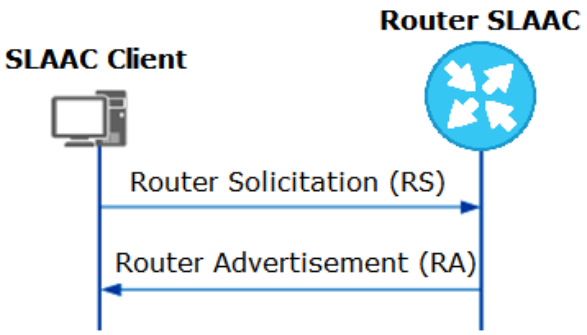
Apesar disso, o Link Local suporta a configuração manual ou static (estática).

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

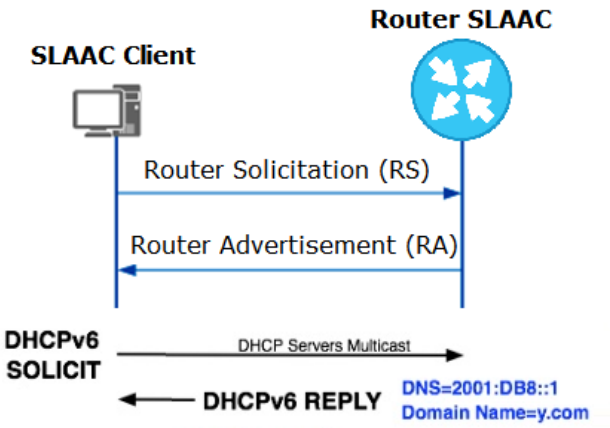


Resumindo as opções de configuração de IPv6:

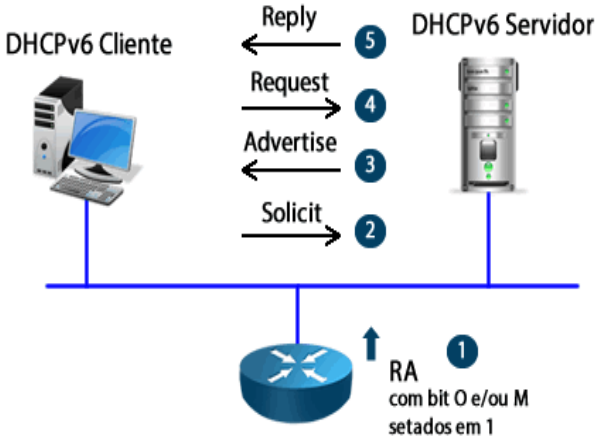
- **Estático (static)**: configuração manual onde o próprio adm. de redes define o IPv6.
- **SLAAC**: autoconfiguração stateless utilizando o EUI-64 ou extensão de privacidade, conforme característica de cada sistema operacional. Com essa opção o usuário recebe apenas um prefixo e seu gateway, bastante útil nos laboratórios.



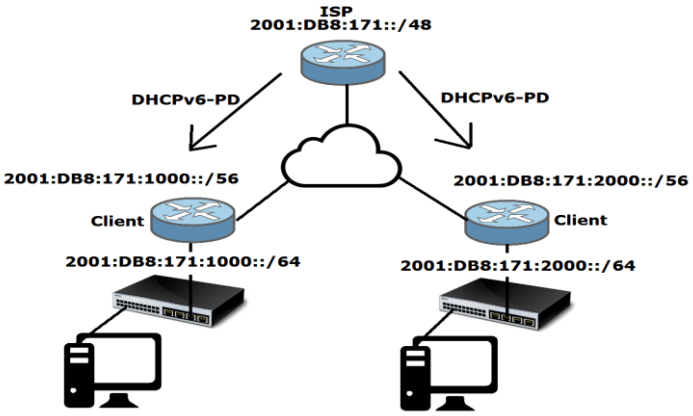
- **SLAAC + DHCPv6 Stateless**: o SLAAC não passa para o usuário informações como DNS e outras opções, para isso a combinação com um servidor DHCPv6 sem estado ajuda a fornecer essas informações.



- **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.

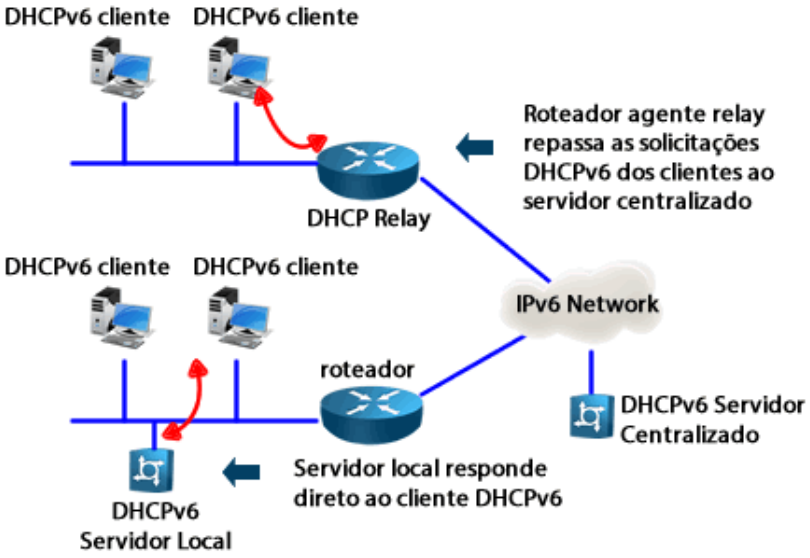


- **DHCPv6-PD (Prefix Delegation)**: mais utilizada em ambiente de Provedores de Serviço, pois fornece um prefixo para o cliente que pode utilizar para autoconfigurar seus próprios redes IPv6.



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.



4 Serviço de Tradução de Nomes na Internet: DNS

Protocolo: DNS (TCP/UDP 53)

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.

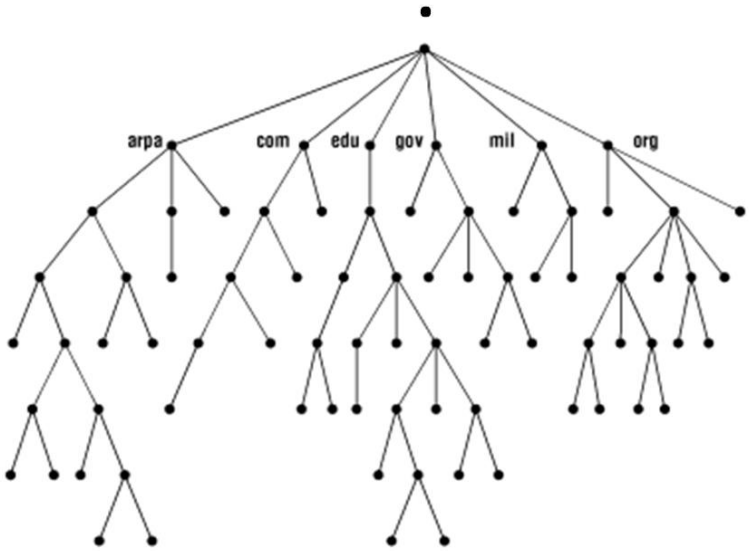
Ele é um sistema constituído por uma robusta, hierárquica e distribuída base de dados, cujo propósito é criar mapeamentos entre nomes de hosts com endereços IP (e vice versa).

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:



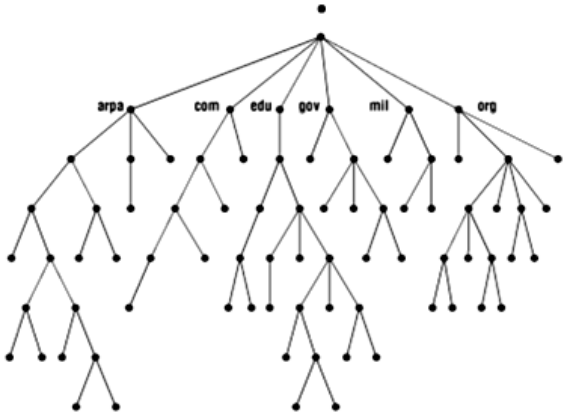
No **root domain** são encontrados diversos **root servers**, localizados em diferentes localizações do globo e classificados em 13 grandes autoridades, além disso, essa divisão é feita por questões de segurança e redundância.

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.

4.1 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:

- **SOA**: abreviação de "Start Of Authority" e indica o responsável por respostas autoritárias a um domínio, ou seja, o responsável pelo domínio. Também contém outras informações úteis como número serial da zona, replicação, etc.
- **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 do registro do tipo A, porém, para um endereço IPv6, ou seja, ele relaciona um nome de host a um endereço IPv6.
- **NS**: conhecido como Name Server (Servidor de Domínio), especifica servidores DNS para o domínio ou subdomínio. Correlaciona um domínio com seus servidores de nome autoritativos (vamos estudar em tópico posterior).
- **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.
- **PTR**: dá suporte à consulta reversa de nomes (reverse name lookup). Fornece o que é conhecido como "DNS reverso", ou seja, os registros PTR atribuem endereços IP a um nome de servidor, em vez de associar um nome de servidor a um endereço IP.
- **TXT (SPF, DKIM)**: Os registros TXT são um tipo de registro DNS que contém informações de texto de fontes fora do seu domínio, os quais podem ser utilizados para várias finalidades, por exemplo, utilização de ferramentas de E-Mail Marketing. Utilizado em conjunto com o SPF e DKIM.
- **SPF (Sender Policy Framework)**: é uma configuração feita no seu servidor DNS, e consiste na inserção de uma linha de texto nos registros DNS do seu domínio. Por exemplo, os registros SPF impedem que seu domínio seja usado para o envio de spam no caso de uso de uma ferramenta de Mail Marketing.
- **DKIM (Domain Keys Identified Mail)**: garante a segurança e autenticidade, por exemplo, no caso de envio de e-mails ele adiciona uma identificação no cabeçalho (header) do e-mail avisando aos servidores que a mensagem realmente partiu do seu domínio, e não de alguém querendo se passar por você.
- **SRV**: permite fornecer a localização de serviços disponíveis em um domínio, como protocolos e portas. Ao utilizar a entrada tipo SRV, ela deve ser apontada para do nome de domínio para um nome de host com um registro A ou AAAA. Não é possível apontar o registro SRV para um registro CNAME.

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).

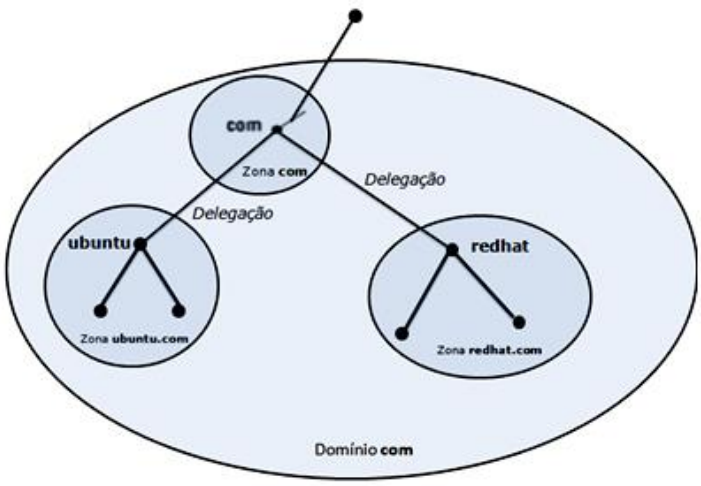
Uma consulta normal ao DNS (Forward DNS lookup) é utilizada para a tradução de um nome de domínio (domain name) para o endereço de rede onde o serviço está disponibilizado (IP address), porém se você notou nos tipos de entradas do DNS existe uma chamada PTR, a qual traduz um IP para um nome.

Isso é chamado de tradução reversa (Reverse DNS lookup) e é utilizada para resolução de problemas e para garantir em alguns casos que o "dono" daquele domínio é quem realmente diz ser.

Por exemplo, alguns servidores de correio de saída podem fazer um reverse DNS lookup antes de aceitar e-mails recebidos para garantir que o que eles estão recebendo não é SPAM ou um e-mail falsificado.

4.2 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.

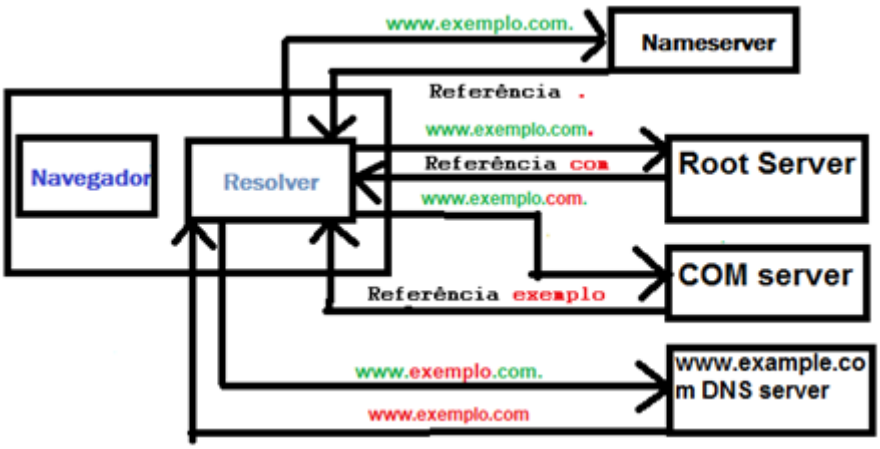
Os **nameservers autoritativos** também poderão assumir comportamentos diferentes em uma zona.

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 se trata 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.

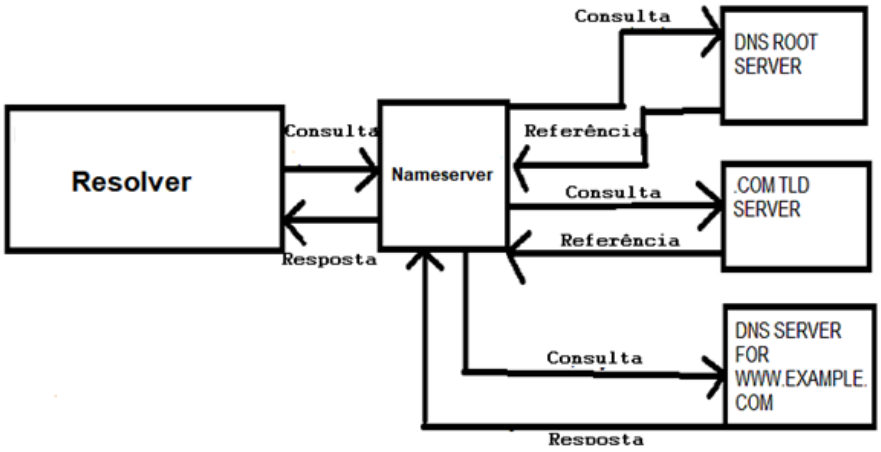
Existem variações que podem ser assumidas por um **nameserver**. Aliás, esses também se diferenciam pela forma em que manipulam as requisições de consultas que lhes são enviadas pelos resolvedores (**resolvers**) do sistema operacional.

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.

4.3 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 Serviço de Sincronização dos Relógios: NTP

Serviço: NTP (UDP 123)

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

Portanto, utilizando o protocolo NTP teremos uma informação de data/hora mais precisa e também teremos a garantia que todos os dispositivos fiquem sincronizados, ou seja, com a mesma informação de data/hora.

Isso é muito importante em uma rede, pois em caso de problemas teremos nos logs (registros) dos equipamentos a data e hora correta que eles ocorreram, possibilitando uma melhor auditoria e correlação de eventos.

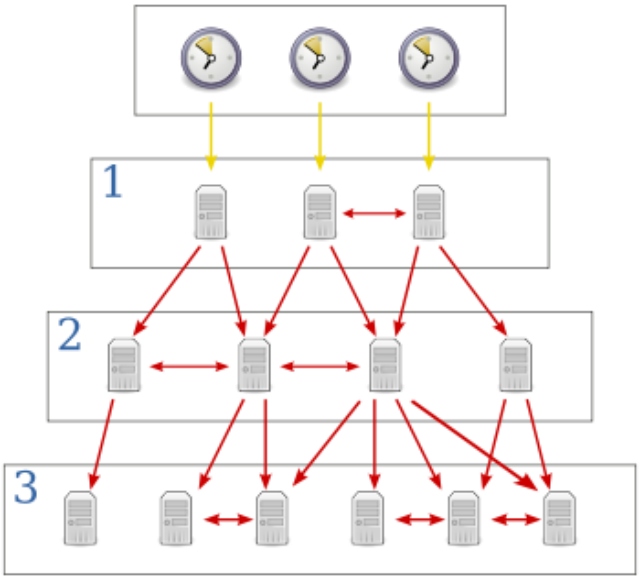
Os servidores NTP formam uma topologia hierárquica, dividida em camadas ou estratos (em inglês: strata) numerados de 0 (zero) a 16 (dezesseis).

O estrato 0 (stratum 0) na verdade não faz parte da rede de servidores NTP, mas representa a referência primária de tempo, que é geralmente um receptor do Sistema de Posicionamento Global (GPS) ou um relógio atômico.

O estrato 16 indica que um determinado servidor está inoperante.

O estrato 0, ou relógio de referência, fornece o tempo correto para o estrato 1, que por sua vez fornece o tempo para o estrato 2 e assim por diante.

O NTP é então, simultaneamente, servidor (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.

Uma lista dos servidores NTP disponíveis na Internet pode ser encontrada no endereço http://support.ntp.org/bin/view/Servers/WebHome.

6 Serviços de Web: HTTP e HTTPS

Protocolos: HTTP (TCP 80) e HTTPS (TCP 443)

O HTTP (Hypertext Transfer Protocol - Protocolo de Transferência de Hipertexto) é um protocolo da camada de aplicação que utiliza como transporte o TCP e fica disponível na porta 80 nos servidores.

Trata-se do serviço básico utilizado pelos navegadores de Internet ou browsers para acessar o conteúdo das páginas web normalmente escritos na linguagem HTML (HyperText Markup Language - Linguagem de Marcação de Hipertexto).

Contudo, para haver comunicação com o servidor onde o site da web está hospedado é necessário utilizar comandos adequados, que não estão em linguagem HTML.

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

Sua versão segura (com criptografia) é o HTTPS (HyperText Transfer Protocol Secure) que também utiliza o protocolo TCP como transporte, porém nos servidores é disponibilizado na porta 443.

O HTTPS é uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS.

Essa camada adicional permite que os dados sejam transmitidos através de uma **conexão criptografada** e que se verifique a autenticidade do servidor e do cliente através de **certificados digitais**.

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

Já os servidores web (HTTP Servers ou Web Servers) mais utilizados são o Apache e IIS (Internet Information Services).

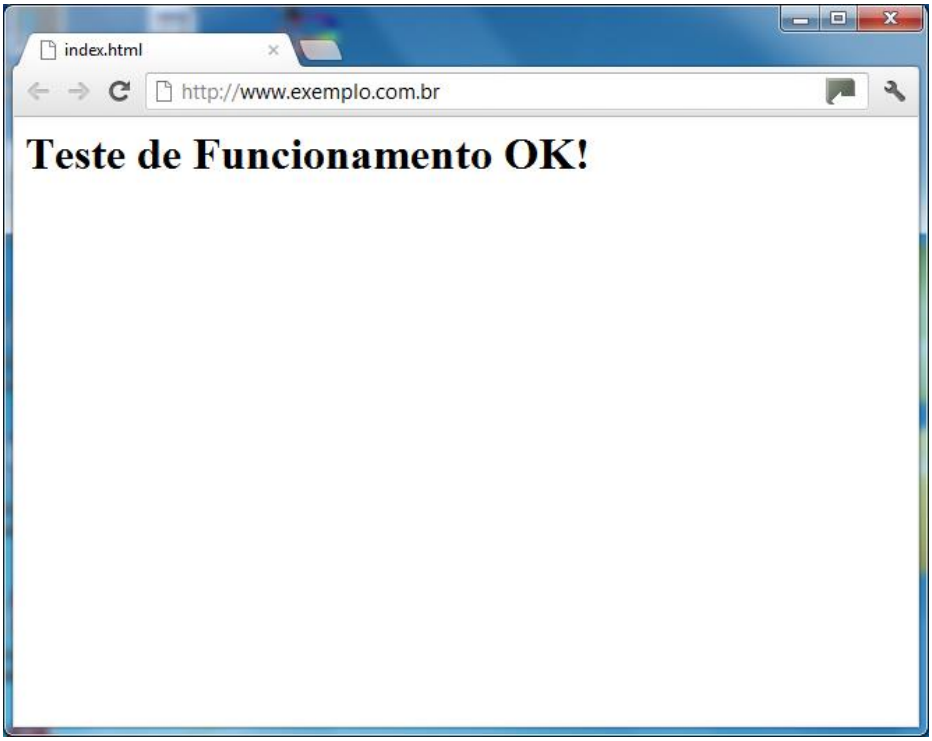
Ao digitar no seu browser http://www.exemplo.com.br na realidade ele está enviando ao servidor um comando GET para o endereço IP que o servidor DNS enviou da página e direcionado para a porta 80 do protocolo TCP, como o exemplo abaixo:

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

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

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

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



7 Serviços de E-mail: SMTP, POP3 e IMAP4

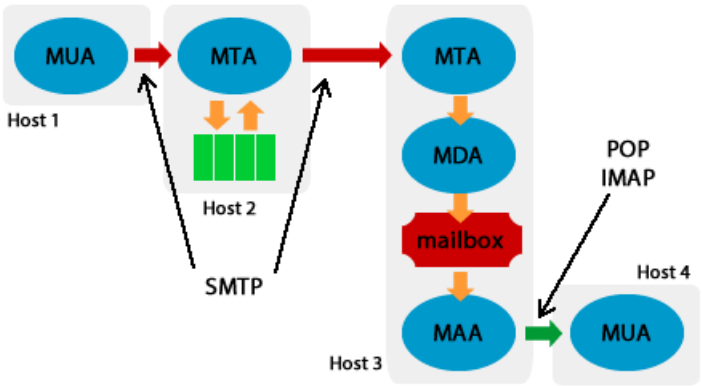
Protocolos: SMTP (TCP 25), POP3 (TCP 110) e IMAP (TCP 143)

O serviço de e-mail usa vários protocolos para o transporte das mensagens entre remetentes e destinatários.

O protocolo SMTP - Simple Mail Transfer Protocol é o protocolo responsável pelo envio do e-mail do cliente (MUA) ao servidor (MTA) e deste para outros servidores, até chegar ao servidor de destino.

O protocolo SMTP utiliza o TCP como transporte na porta 25 por padrão.

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



Normalmente o uso de POP3 é mais indicado quando os usuários são estáticos, ou seja, cada um possui seu computador e só acessa seu e-mail a partir dele.

POP3 é um protocolo leve e que não mantém conexão constante com o servidor, ou seja, você ao enviar e receber e-mails ele estabelece a conexão, baixa os e-mails para seu computador ou envia os e-mails que estão em sua caixa de saída e fecha a conexão.

O POP3 utiliza o TCP como transporte na porta 110 por padrão. Existe também a versão segura chamada POP3S que utiliza a porta 995 do TCP.

O uso de IMAP é indicado quando os usuários são "nômades", ou seja, quando usam vários computadores diferentes.

O IMAP exige mais recursos de CPU, disco e memória do servidor que o POP3.

A conexão IMAP normalmente é mantida enquanto durar a sessão de trabalho do usuário, pois seu cliente de e-mail fica sincronizado com o servidor e uma cópia dos e-mails é mantida nele, assim você pode ler seus e-mails de qualquer host.

Este protocolo é muito usado em ambientes de WebMail, para os acessos do servidor Web ao servidor de e-mail, normalmente sendo realizada através de seu browser, e por isso é o mais utilizado em ambientes corporativos, pois assim os funcionários podem acessar suas caixas de e-mail em qualquer computador, mesmo estando fora de sua rede local ou longe de seu computador.

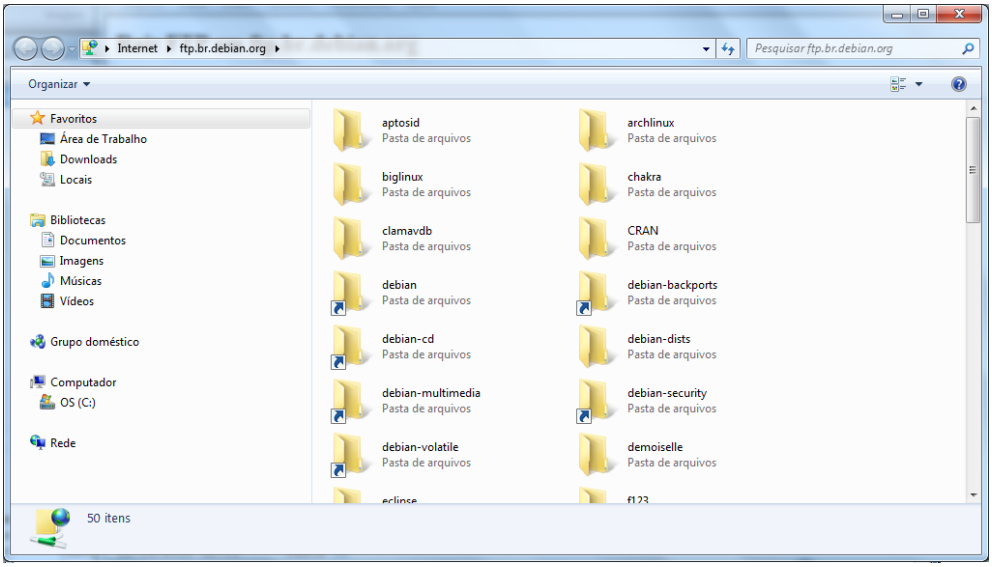
O IMAP utiliza também o TCP como protocolo de transporte na porta 143 por padrão. Existe também a versão segura chamada IMAPS que utiliza a porta 993 do TCP.

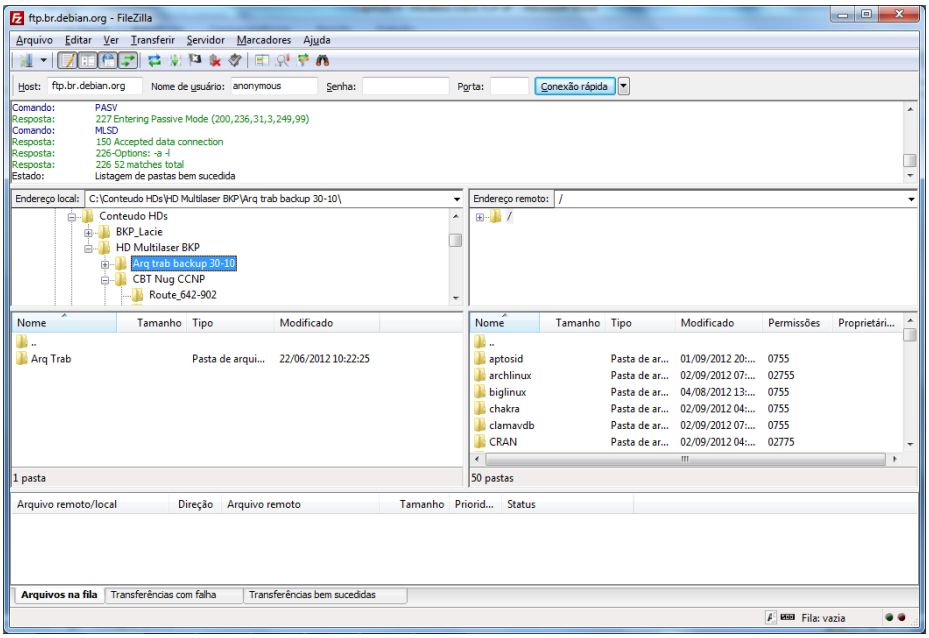
8 Serviço de Troca de Arquivos: FTP, SFTP, SCP e TFTP

Protocolos: FTP (TCP 20/21), SFTP (TCP 22) e TFTP (UDP 69)

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

Suporta transferências bidirecionais de arquivos binários e ASCII.





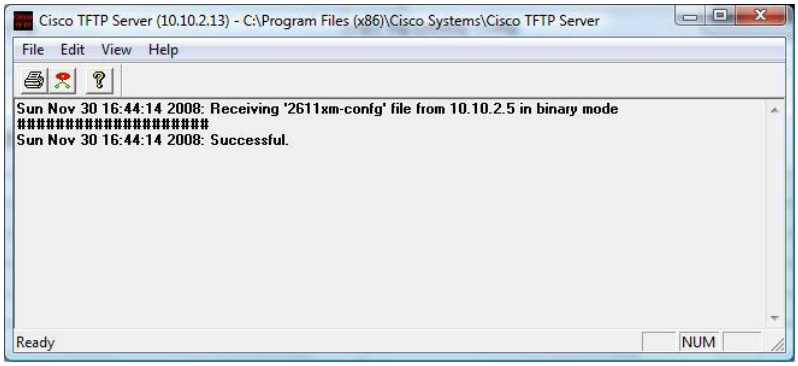
O serviço de FTP faz uso de duas portas TCP, ou seja, nas portas 20/TCP temos o fluxo de dados e na 21/TCP são passados os comandos de controle da conexão, mas também ele pode utilizar outras portas acima de 1024, tudo depende da configuração dos servidores.

Na prática isso quer dizer que quando você deseja, por exemplo, baixar um arquivo FTP o comando (get) para baixar o arquivo é passado pela porta 21 e assim que o servidor aceita ele envia os dados do arquivo pela porta 20.

Já o TFTP (Trivial File Transfer Protocol – Protocolo de Transferência de Arquivos Simples) é também utilizado para transferência de arquivos, porém é um serviço sem conexão e usa o UDP (User Datagram Protocol – Protocolo de Datagrama de Usuário) como protocolo de transporte na porta 69.

É usado por dispositivos de rede, tais como roteadores switches e telefones IP para transferir arquivos de configuração, imagens IOS e firmwares.

É útil em algumas redes locais porque opera mais rápido do que o FTP em um ambiente estável, porém não recomendado para utilizar em redes públicas, como a Internet, pois ele não suporta autenticação.



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

O SFTP roda como o SSH utilizando a porta 22 TCP por padrão.

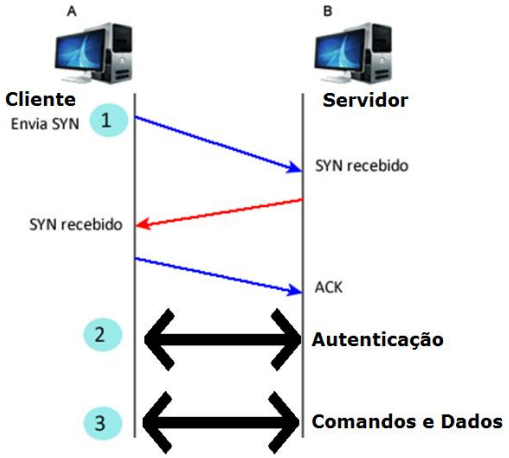
8.1 Protocolo FTP

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.

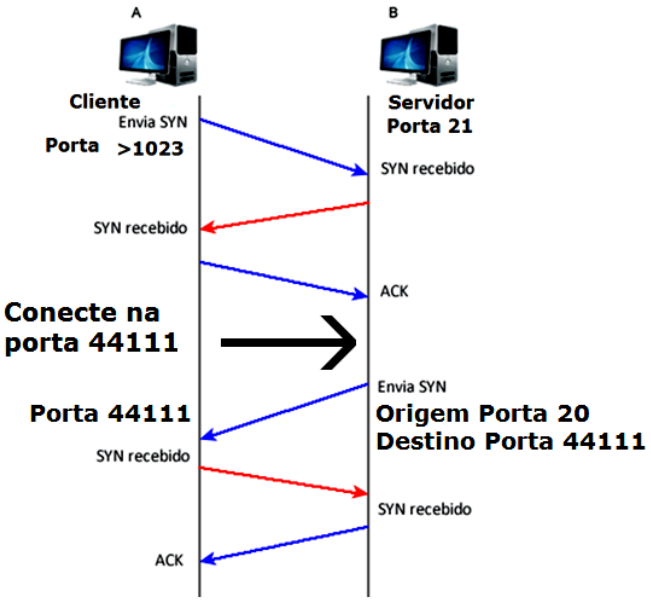
Além disso, o FTP também permite o acesso em modo "anônimo", ou seja, sem necessidade de utilizar usuário e senha.

8.1.1 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.



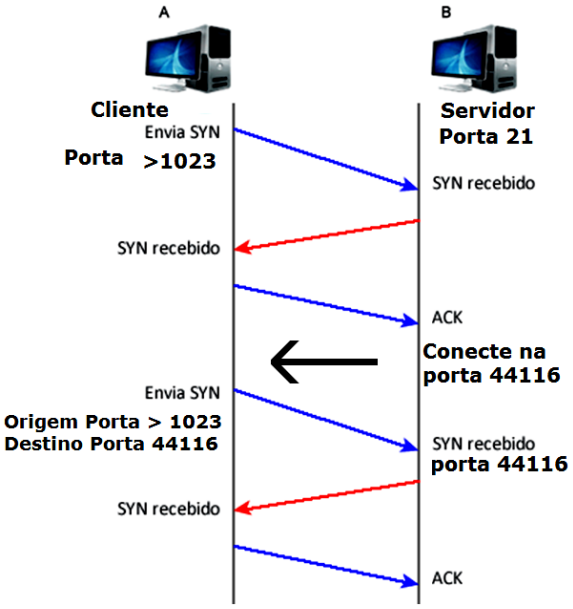
No modo ativo o cliente informa a porta que o servidor deve enviar o SYN e abrir a conexão com o comando PORT via canal de controle.

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

8.1.2 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

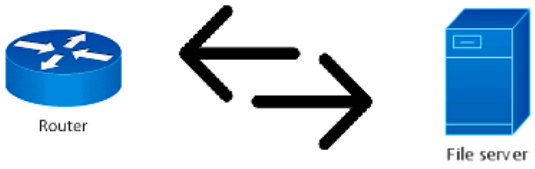
O FTP Secure ou FTPS é uma adaptação do FTP que pode utilizar certificados digitais para autenticação e TLS (Transport Layer Security) para criptografar tanto o canal de dados como o controle. Ele utiliza as portas 990 para controle e 989 para os dados.

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.

8.2 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.

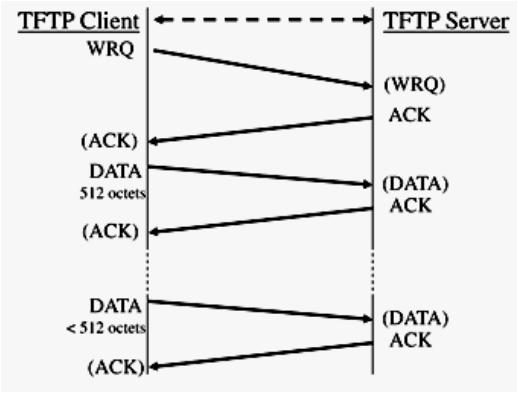
No servidor você pode configurar os arquivos como apenas escrita ou escrita/leitura.

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.

9 Serviços de Gerenciamento e Acesso Remoto: SNMP, Syslog, Telnet, SSH, RDP e VNC

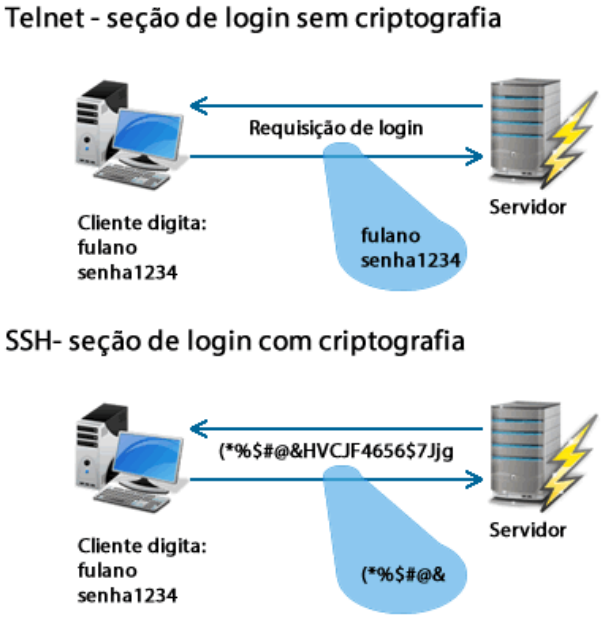
9.1 Serviços de Terminal e Acesso Remoto

Protocolos: Telnet (TCP 23), SSH (TCP 22), RDP (TCP 3389) e VNC (TCP 5900+N e 5800+N)

Tanto o Telnet como o SSH permitem o acesso remoto à linha de comando de outro computador, servidor ou dispositivo de rede, permitindo que um usuário efetue logon em um dispositivo da rede e execute comandos.

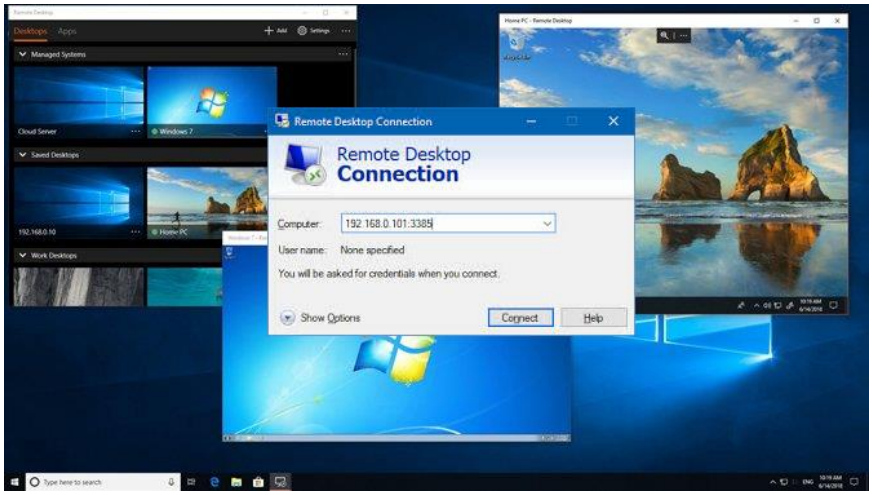
Eles são utilizados para a administração remota de servidores, roteadores e switches.

A diferença básica entre os dois serviços é a questão da segurança, pois o Telnet é enviado em modo texto claro através da rede, enquanto o SSH troca as informações entre os dispositivos de maneira segura e criptografada.



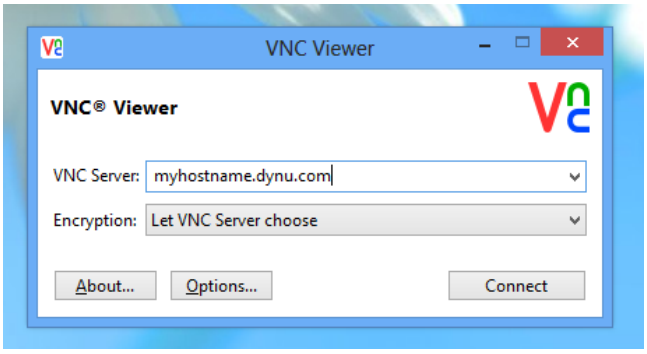
A sigla RDP vem do inglês Remote Desktop Protocol, ou seja, Protocolo de Área de Trabalho Remota. Ele permite que que usuários consigam ter acesso às suas respectivas áreas de trabalho sem que seja necessário estar fisicamente próximo a seus computadores.

A forma mais comum de conexão a esse serviço é através de um cliente disponível por padrão no Windows.



Outra alternativa para acesso remoto é o VNC (Virtual Network Computing), o qual permite a visualização de interfaces gráficas remotas através de uma conexão segura (criptografada).

Geralmente é bastante utilizado por profissionais que prestam suporte remoto a outros usuários, pois o VNC permite a captura completa do computador remoto conectado (conhecido como VNC Server) pelo computador cliente (chamado de VNC Viewer).



Os programas mais utilizados para acesso remoto via VNC são:

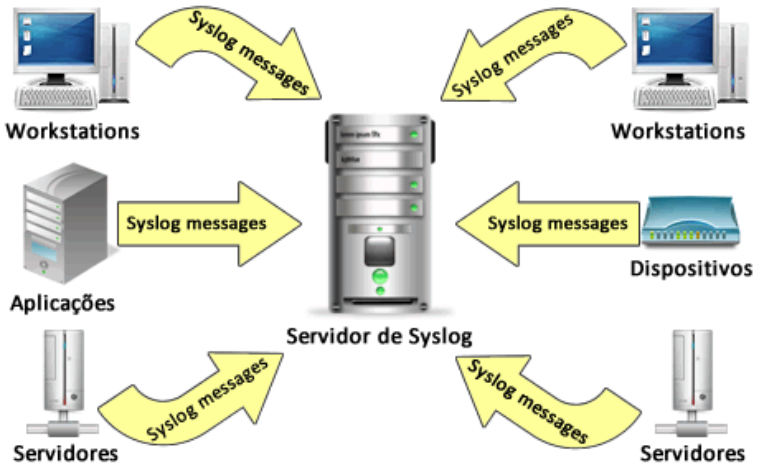
- VNC (desenvolvido pela RealVNC)
- TightVNC
- UltraVNC
- TeamViewer

9.2 Serviço de Envio de Mensagens de Log

Protocolo: SYSLOG (TCP/UDP 514)

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.

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 dispositivo 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** → 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.

O syslog é um serviço fundamental para as áreas de gerenciamento e segurança de redes, pois normalmente as mensagens de log gravadas em dispositivos de rede podem ser apagadas devido a uma reinicialização ou até mesmo para apagar rastros de um possível ataque cibernético.

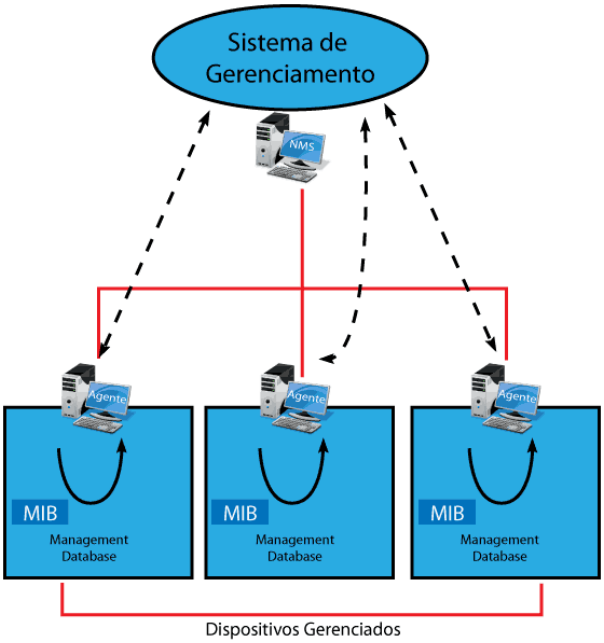
9.3 Serviço de Gerenciamento de Dispositivos de Rede

Protocolo: SNMP (UDP 161)

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.

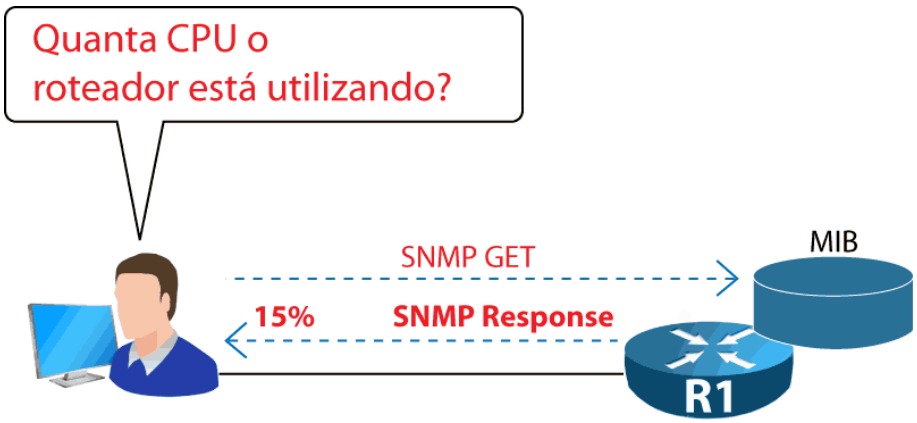
Um **Agente** é um módulo de software de gestão de rede que fica armazenado num Dispositivo Gerenciado. Um agente tem o conhecimento das informações de gestão locais e traduz estas informações para um formato compatível com o protocolo SNMP e padronizados em bancos de dados chamados **MIB** (**Management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

9.3.1 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.

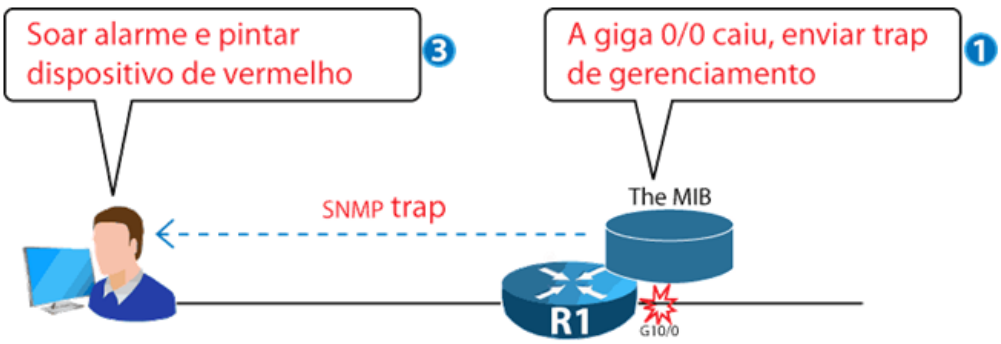


Esse tipo de operação pode ser automatizado em sistemas de gerência para geração de avisos, por exemplo, o gerenciador pode de 5 em 5 minutos checar o uso de CPU pelo roteador e se chegar a 50% gerar um aviso na tela de gerenciamento que a CPU passou desse limite configurado (threshold ou limiar).

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.

9.3.2 MIB ou Management Information Base

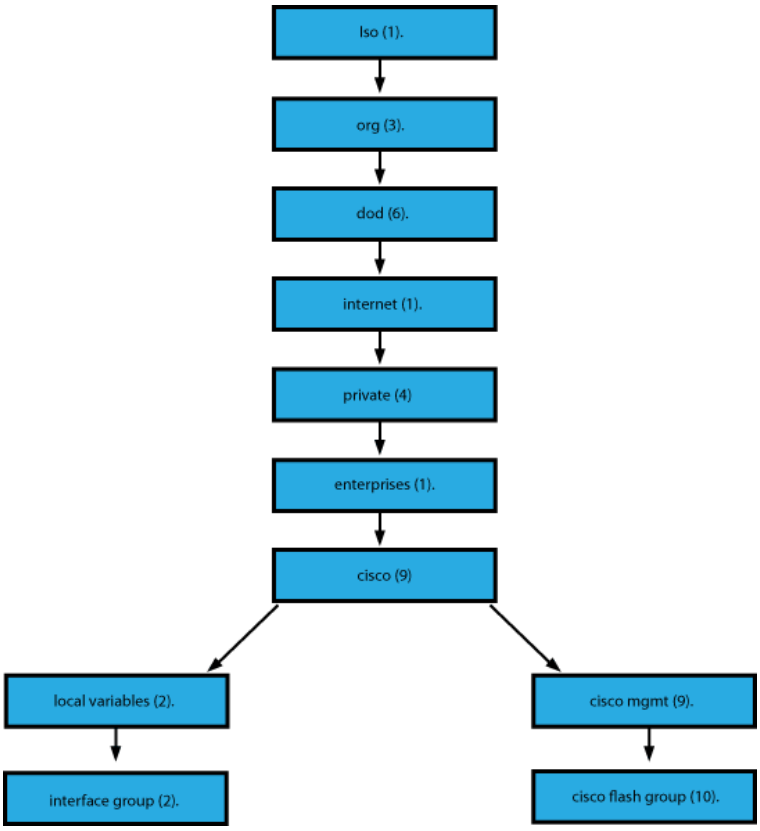
Um **Management Information Base** ou simplesmente **MIB** define variáveis de um dispositivo de rede que podem ser monitoradas e/ou controladas por um software de gerenciamento.

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 a seguir.



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.

9.3.3 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 (Lista de Controle de Acesso) apenas a esses IPs bem definidos.

Em servidores essas filtragens podem ser feitas via Firewall ou Iptables (Linux).

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.

10 Serviços de Voz e Vídeo Sobre IP: RTP, SIP e H.323

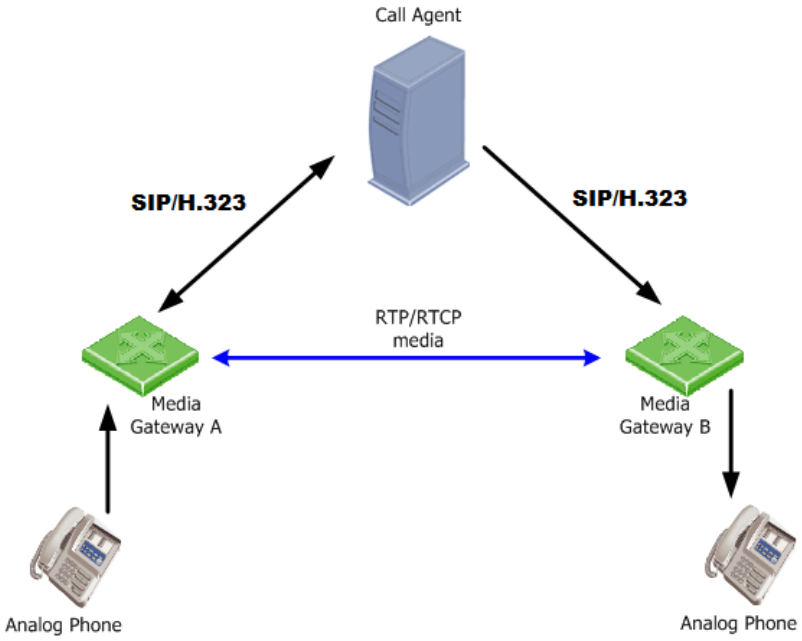
Protocolos: RTP/RTCP (UDP 16384-32767), SIP (TCP/UDP 5060/5061) e H.323 (TCP 1720)

Para ficar mais fácil a compreensão dos protocolos utilizados em chamadas de voz e vídeo sobre IP tenha em mente que existe a sinalização, a qual é utilizada para iniciar e finalizar uma chamada, e os dados enviados durante a chamada, ou seja, a voz ou vídeo trocado durante uma conexão.

O RTP e RTCP são utilizados para o envio da voz ou vídeo durante uma chamada, já o SIP e o H.323 são protocolos que cuidam do estabelecimento e finalização das chamadas, ou seja, fazem a sinalização.

Veja imagem a seguir onde o Call Agent é a central telefônica IP, a qual troca informações com dois gateways de voz que desejam iniciar uma chamada entre si.

Veja que primeiro existe uma troca de sinalizações para o estabelecimento da chamada, seja via SIP ou H.323, e depois a voz é trocada via RTP/RTCP.



O Real-Time Transport Protocol (RTP) é o principal protocolo utilizado pelos terminais, em conjunto com o RTCP, para o transporte fim-a-fim em tempo real de pacotes de mídia (Voz) através de redes de pacotes.

O RTP não reserva recursos de rede e nem garante qualidade de serviço para tempo real. O transporte dos dados é incrementado através do RTCP (Real-Time Transport Control Protocol - protocolo de controle) que monitora a entrega dos dados e provê funções mínimas de controle e identificação. No caso das redes IP este protocolo faz uso dos pacotes UDP, que estabelecem comunicações sem conexão.

Já o Session Initiation Protocol (SIP) estabelece o padrão de sinalização e controle para chamadas entre terminais que não utilizam o padrão H.323, e possui os seus próprios mecanismos de segurança e confiabilidade.

Estabelece recomendações para serviços adicionais tais como transferência e redirecionamento de chamadas, identificação de chamadas (chamado e chamador), autenticação de chamadas (chamado e chamador), conferência, entre outros.

O padrão H.323 é um conjunto de protocolos verticalizados para sinalização e controle da comunicação entre terminais que suportam aplicações de áudio (Voz), vídeo ou comunicação de dados multimídia.

Os pacotes de dados H.323 acrescentam cabeçalho com marcação do tempo e informações de transmissão permitindo a reordenação dos pacotes e eliminação de pacotes duplicados, sincronize áudio e vídeo, tornado possível uma comunicação contínua com atrasos aceitáveis.

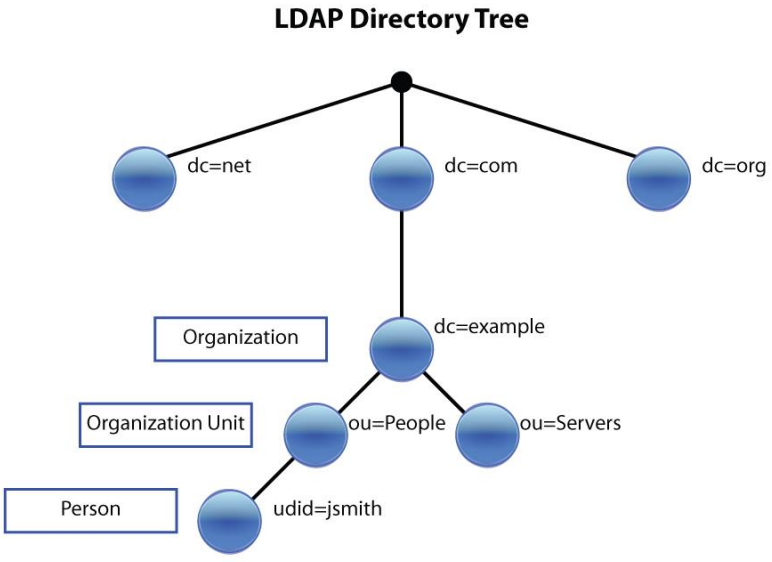
11 Serviços de Diretórios: LDAP e LDAPS

Protocolos: LDAP (TCP/UDP 389) e LDAPS (TCP 636)

O LDAP (Lightweight Directory Access Protocol) é um serviço de diretório que guarda as informações dos diversos clientes de rede, grupos de utilizadores, informações das máquinas entre outras informações.

Essas informações podem ser, por exemplo, o nome, username, password, informações sobre a conta, etc. Em uma rede bem estruturada normalmente é o serviço LDAP que mantém toda essa informação e ainda permite a autenticação de utilizadores.

A informação encontra-se organizada de forma hierárquica e centralizada, tal como uma agenda telefônica, facilitando a gestão dessas informações por parte de qualquer Administrador e o acesso por parte de outros serviços.



No modelo de informação do LDAP os dados são armazenados em Entradas, as quais são organizadas de forma hierárquica compondo assim uma árvore de informações conhecida como DIT (Directory Information Tree).

Cada entrada na DIT é identifica de forma única a partir do seu Distinguished Name – indicando a sua posição concreta na árvore.

A entrada de "udid" igual a "jsmith", por exemplo, é identificada pelo seguinte DN:

```
dn: udid=jsmith, ou=People, dc=example, dc=com
```

Cada entrada é constituída por **atributos**: conjunto de pares contendo uma chave e valor utilizados para registrar as suas diversas características.

Os atributos que poderão ser utilizados em uma dada entrada são determinados pela **Classe** correspondente. As classes são organizadas de forma hierárquica, onde as inferiores herdam atributos e características gerais das superiores. A classe "top" é aquela que se encontra na mais alta patente de classes.

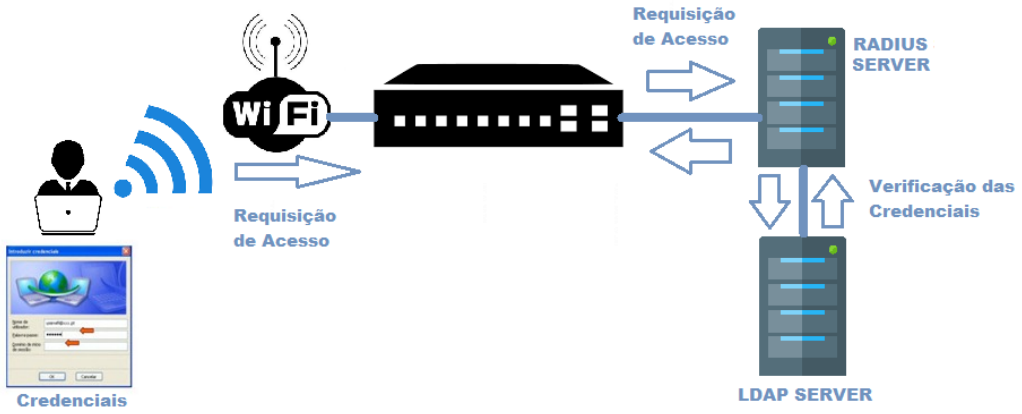
Para a implementação de um serviço de LDAP existem algumas alternativas sendo que as mais conhecidas são o Active Directory do Windows e o OpenLDAP para sistemas Linux.

O protocolo LDAP seguro (LDAPS) criptografa a comunicação entre o requisitante e o servidor de diretório LDAP. Isso evita que informações confidenciais no servidor de diretório e que credenciais LDAP sejam enviadas como texto não criptografado.

Um exemplo do uso do LDAP ou do LADPS é o serviço de autenticação, o qual permite autenticar usuários e dispositivos de rede.

Numa rede comum existirem servidores de autenticação de forma a que os usuários apenas tenham acesso aos recursos através da verificação de credenciais (usuário + password).

Na imagem abaixo está representado um usuário de rede tentando conectar-se à rede sem fio, porém antes de ser conectado o sistema faz uma autenticação via um servidor de autenticação RADIUS, o qual certifica que as credenciais estão corretas através de um serviço de diretórios LDAP.



O usuário terá o devido acesso à rede somente se os dados passados (login e senha) estiverem cadastrados no serviço de LDAP e tiverem sido corretamente digitados.

12 Serviço de Compartilhamento de Arquivos: SMB

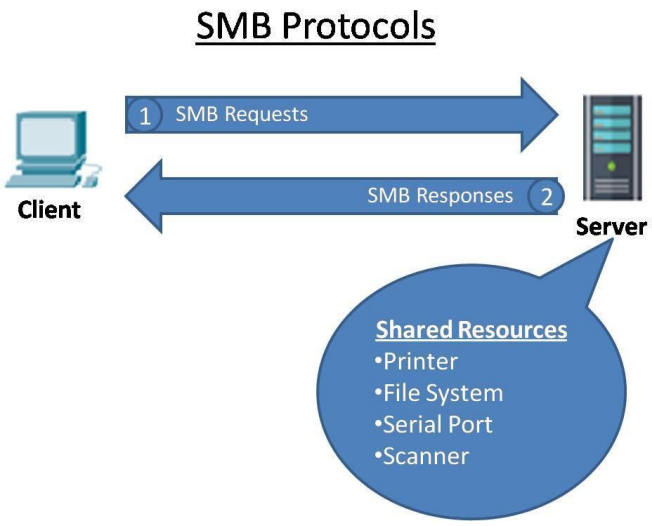
Protocolo: SMB (TCP 445)

O SMB (Server Message Block) é um protocolo de redes cujo uso mais comum é o compartilhamento de arquivos em uma LAN.

Este protocolo permite que o cliente manipule arquivos como se estes estivessem em sua máquina local e realize operações como leitura, escrita, criação, apagamento e renomeação são suportadas, sendo a única diferença de que os arquivos manipulados não estão no computador local e sim em um servidor remoto.

O protocolo SMB funciona enviando pacotes do cliente para o servidor (SMB Request). Cada pacote é tipicamente baseado em uma requisição de algum tipo, como a abertura ou leitura de um arquivo.

O servidor então recebe este pacote checa-o para ver se a requisição é válida, ou seja, verifica se o cliente possui as permissões apropriadas para efetuar a requisição e finalmente executa a requisição e retorna um pacote de resposta ao cliente (SMB Response).



O protocolo SMB é extremamente utilizado pelos sistemas operacionais Microsoft Windows para compartilhamento de arquivos em rede e compartilhar outros recursos como impressora (printer), portas seriais e scanners.

13 Serviços para a Camada de Rede: NAT, PAT e Proxy Server

Nesse capítulo temos três serviços ou recursos que são muito utilizados para acesso à Internet em Redes IP.

Você pode estranhar o fato de colocarmos aqui também o Proxy, pois ele pode utilizar informações da camada 7 para tomar decisões sobre o tráfego, porém resolvemos deixar junto com o NAT e PAT por suas funções serem semelhantes.

Pois, no final o maior uso desses três serviços é o de fornecer um gateway entre usuários de rede e a Internet.

13.1 Funcionamento do NAT e PAT

O NAT (Network Address Translation) e o PAT (Port and Address Translation) são mecanismos normalmente utilizados para conectar redes privadas (RFC 1918) à Internet, pois eles servem como pontos de tradução de IPs privados (não roteáveis na Internet) para IPs públicos (roteáveis na Internet).

Porém, tanto o NAT como o PAT fazem a tradução de endereços em camada-3, podendo ser utilizados em outras necessidades, por exemplo, fazer traduções de endereços para integração de redes de empresas que estão sendo unificadas.

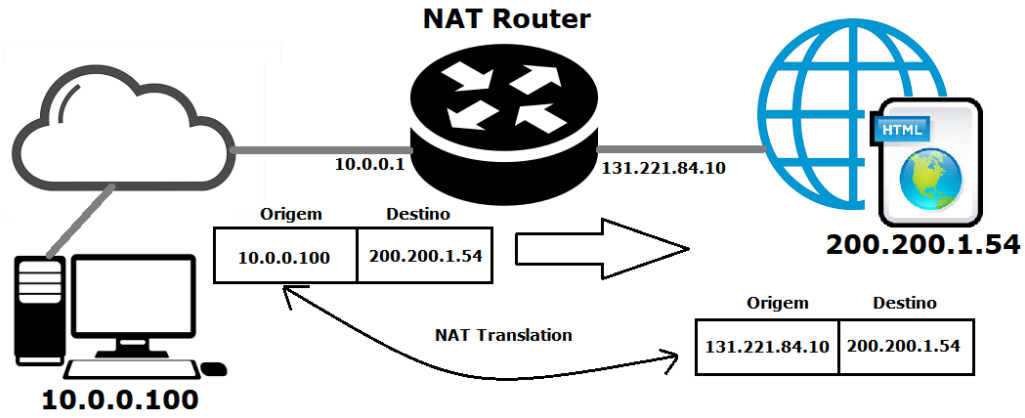
Mas o que é "tradução de endereços de camada-3" na prática?

Simplesmente você tem duas regiões, uma que será traduzida e outra que vai realizar a tradução.

Quando um endereço vindo da região a ser traduzida passa pela outra que fará a tradução seu endereço é trocado e o dispositivo que traduz guarda em uma tabela (que já pode até ter sido criada anteriormente) essa tradução realizada.

Assim, quando houver o retorno da resposta remota o dispositivo tradutor conseguirá devolver o pacote para quem enviou a mensagem original que foi traduzida.

Veja imagem a seguir mostrando o processo básico do NAT.



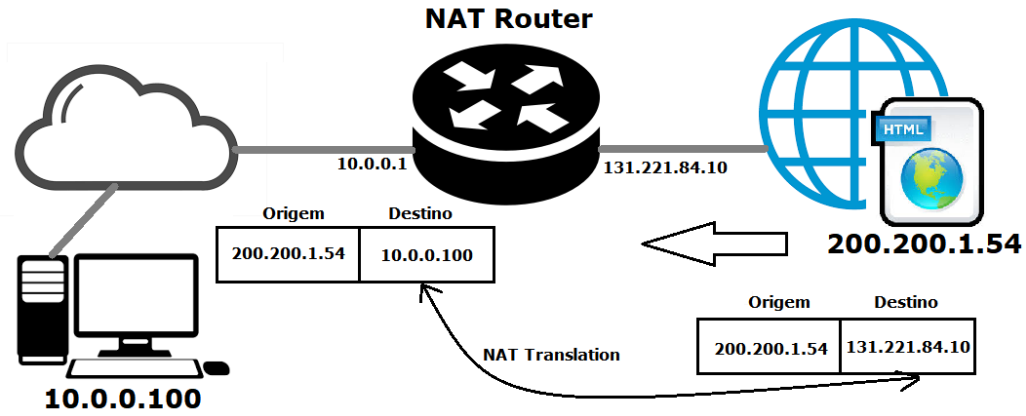
Note no exemplo da imagem temos o computador interno de uma rede privativa (10.0.0.0/24) querendo acessar o servidor de Web na Internet que possui o endereço IP público 200.200.1.54.

Normalmente isso não poderia acontecer, uma vez que a faixa de endereços privativos não são roteáveis na Internet.

Porém o serviço de NAT permite esse acesso, pois o dispositivo chamado NAT Router (roteador com o serviço ativado) faz a tradução do endereço interno para um endereço válido de Internet (131.221.84.10).

Essa tradução é gravada em uma tabela interna do roteador, pois quando o servidor 200.200.1.54 responder à mensagem o roteador deve "saber quem é o dono" daquele pacote de retorno.
Essa tabela é conhecida como tabela de traduções do NAT ou "NAT Translations".

Portanto, quando o NAT Router receber um pacote com o endereço origem 200.200.1.54 e o endereço de destino 131.221.84.10, o pacote será traduzido e enviado ao computador com endereço 10.0.0.100.



13.2 Tipos de NAT e PAT

O NAT o geralmente é implementado 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.

Já o PAT pode ser implementado das seguintes formas:

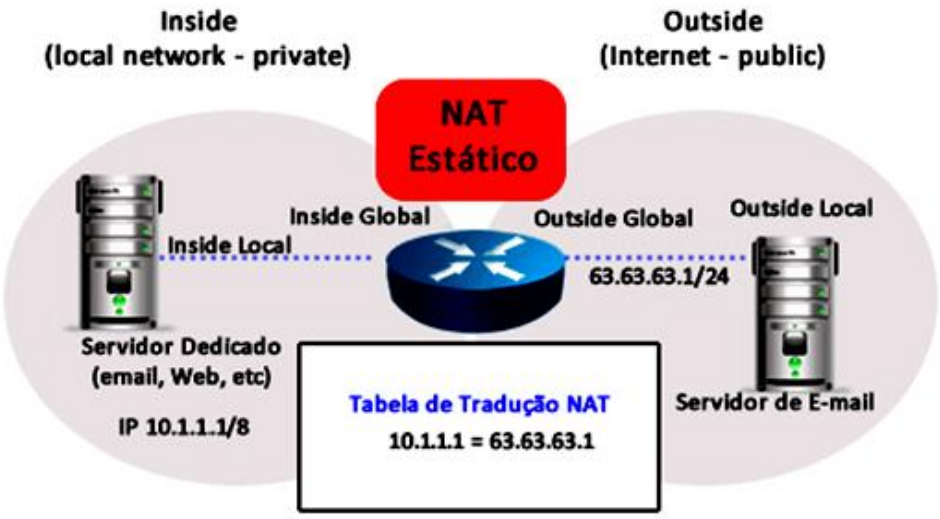
- **Um para muitos** (One to Many): onde existe apenas um endereço de saída na Interface de Internet que será utilizado para traduzir diversos endereços internos (da Intranet).
- **Dinâmico**: da mesma forma que para o NAT pode haver diversos endereços de saída e o PAT ser implementado de forma dinâmica.
- **Port Forwarding (Reverso)**: o PAT reverso pode traduzir uma conexão destinada a uma determinada porta TCP ou UDP para um dispositivo interno. Por exemplo, para um servidor Web interno que possui endereço IP privativo.

Nas duas primeiras opções o PAT utiliza tanto o endereço IP como as portas TCP ou UDP para realizar a tradução dos pacotes de entrada.

As traduções estáticas e port forwarding 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.

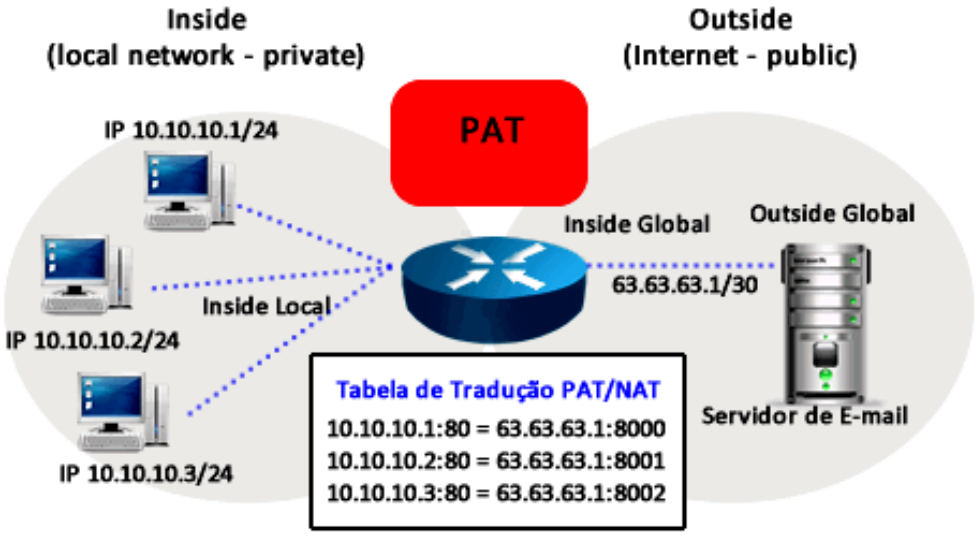
Qualquer endereço IP de um pool de endereços IP públicos pode ser atribuído a um host da rede.

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.

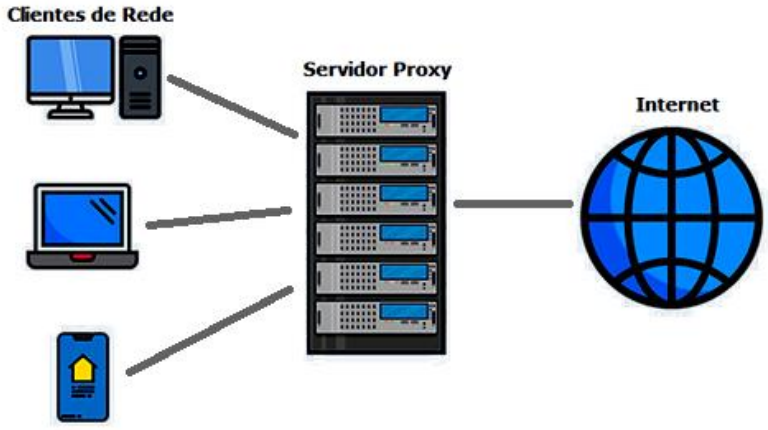
Quando não há mais portas disponíveis e há mais de um endereço IP externo configurado, o PAT passa para o próximo endereço IP, para tentar alocar novamente a porta de origem.

Esse processo continua até que não haja mais portas disponíveis nem endereços IP externos.

13.3 Funcionamento dos Servidores Proxy

Como já foi citado no início do capítulo, um servidor Proxy fornece um gateway entre usuários e a Internet, por isso mesmo é tratado como um "intermediário", pois um servidor Proxy vai entre os usuários e as páginas da Internet que eles desejam visitar.

Portanto, o servidor proxy é essencialmente um computador que tem pelo menos uma interface na rede interna (Intranet) e outra interface na Internet.



O funcionamento básico é semelhante ao que estudamos para o NAT, pois como um servidor proxy tem seu próprio endereço IP, quando um computador interno envia uma solicitação para a Internet, ele encaminha o pacote para o proxy, o qual encaminha essa solicitação para o servidor web.

Quando o proxy recebe a resposta do servidor web, ele encaminha os dados da página para o navegador do computador do cliente, por exemplo, para o Chrome, Safari, Firefox ou Microsoft Edge.

Porém, o proxy pode ir além do NAT e PAT!

Além de traduzir endereços, um servidor Proxy pode ser configurado como filtro da Web ou firewall, protegendo os computadores contra ameaças da Internet como malwares, pois ele tem a capacidade de analisar até protocolos da camada 7 (aplicação).

O proxy tem a capacidade de examinar os dados que entram e saem do seu computador ou rede, aplicando regras para evitar que os endereços internos sejam expostos na Internet ou tráfego não autorizado seja passado.

Dessa forma, o administrador de redes ou de segurança pode filtrar o tráfego de acordo com seu nível de segurança ou quanto tráfego sua rede ou até mesmo em nível de computadores individuais.

Algumas pessoas usam proxies para fins pessoais, como esconder sua localização enquanto assistem filmes online ou realizam "outras atividades".

Para uma empresa os proxies são utilizados principalmente para:

- Melhorar a segurança;
- Proteger a atividade dos funcionários na internet;
- Equilibrar o tráfego de internet para evitar indisponibilidade de acesso;
- Controle os sites que os funcionários acessam;
- Economizar a largura de banda salvando (caching) arquivos ou comprimindo o tráfego recebido.

Os servidores Proxy existem em versões de hardware e software.

As soluções de hardware ficam entre sua rede e a internet, onde obtêm, enviam e encaminham dados da web.

Os proxies de software são normalmente hospedados por um provedor ou residem na nuvem.

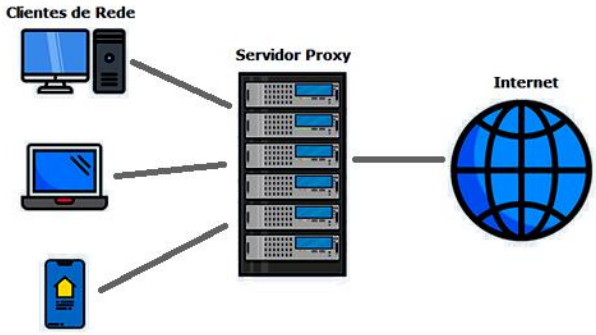
Você instala um aplicativo em seu computador que facilita a interação com o proxy.

Muitas vezes, um proxy de software pode ser obtido em versões gratuitas ou através do pagamento de uma taxa mensal.

13.4 Tipos de Servidores Proxy

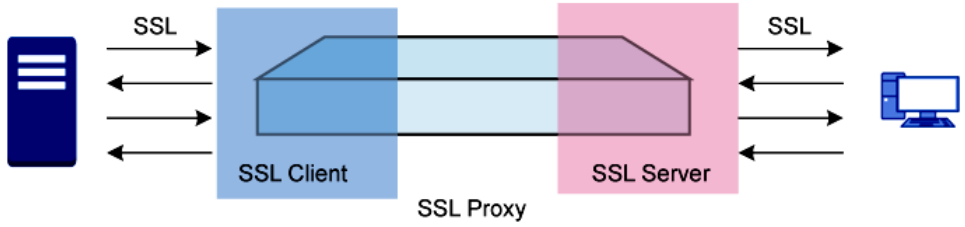
Nesse tópico vamos citar os principais tipos de servidores proxy e suas características.

- **Forward Proxy**: é o tipo mais comum de proxy, situado entre a rede Interna e a Internet. Quando uma solicitação de um cliente é enviada, o servidor proxy examina-a e decide se deve realizar ou não a conexão solicitada. Nesse modo de operação os navegadores de Internet dos clientes precisam de uma configuração específica relacionada ao servidor Proxy.

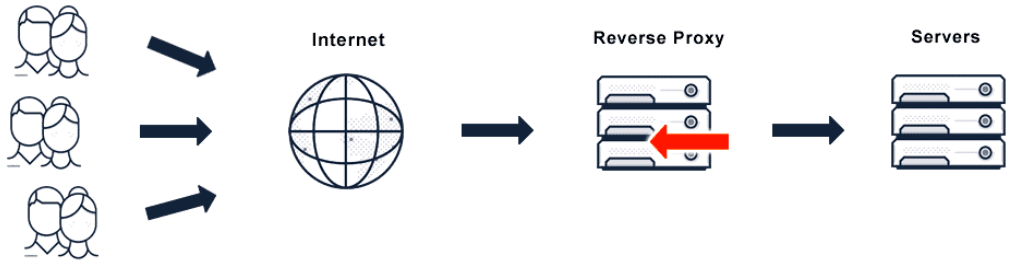


- **Proxy Transparente (Transparent Proxy)**: nesse modo de operação o proxy é "transparente" ao usuário, pois nada precisa ser configurado nos clientes. Esse proxy pode ser conhecido como "intercepting proxy" ou "forced proxy".

- **Proxy SSL**: Um proxy de camada de soquetes seguros (SSL) que fornece decriptografia entre o cliente e o servidor. À medida que os dados são criptografados em ambas as direções, o proxy oculta sua existência tanto do cliente quanto do servidor. Esses proxies são mais adequados para organizações que precisam de proteção reforçada contra ameaças ao protocolo SSL.



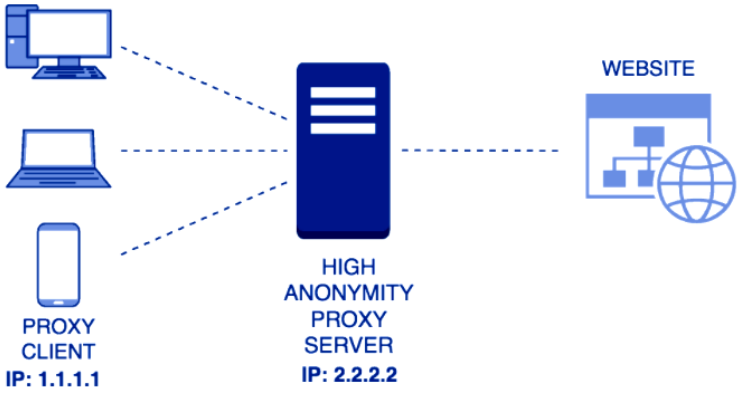
- **Proxy Reverso (Reverse Proxy)**: funciona como o NAT reverso e fica na frente de servidores de Internet, interceptando as mensagens dos clientes que são enviadas em direção a esses servidores. Pode ser utilizado também para o balanceamento de cargas entre servidores de Internet.



- **Data Center Proxy**: normalmente é um servidor proxy que existe em um data center físico, sendo que as solicitações de usuários são roteadas através desse servidor.

- **Proxy Residencial**: esse tipo de proxy fornece um endereço IP que pertence a um dispositivo físico específico. Todas as solicitações são então canalizadas através desse dispositivo e permitem um nível a mais de segurança para usuários residenciais.

- **Proxy Anônimo (Anonymous Proxy)**: Um proxy anônimo tem a função de tornar a atividade da Internet sem possibilidade de rastreamento. Ele funciona acessando a internet em nome do usuário enquanto esconde sua identidade e informações do computador. Normalmente utilizado para fins "obscuros".



- **Proxy de Alto Anonimato (High Anonymity Proxy)**: é um tipo proxy anônimo que leva o anonimato um passo adiante. Ele funciona apagando suas informações antes que o proxy tente se conectar ao site de destino. Tanto o proxy anônimo como o de alto anonimato são normalmente utilizados para fins "obscuros", sendo que suas versões gratuitas podem representar um risco de segurança a que deseja utilizar esse recurso, pois são muito utilizados como "iscas" para coletar dados e informações de seus usuários.

- **Distorting Proxy**: podemos chamar de "proxy distorcido", pois ele se identifica como um proxy para um site, mas esconde sua própria identidade. Ele faz isso alterando seu endereço IP para um incorreto. Normalmente esse tipo de proxy é utilizado para ocultar sua localização ao acessar a internet. Outro exemplo de proxy utilizado normalmente para operações "obscuras" na Internet.

- **Proxy Público**: Um proxy público é acessível por qualquer pessoa gratuitamente. Ele funciona dando aos usuários acesso ao seu endereço IP, escondendo sua identidade enquanto visitam sites. Embora sejam gratuitos e de fácil acesso, muitas vezes são lentos porque ficam lotados com usuários gratuitos, além disso, quando se utiliza um proxy público, o usuário corre um risco de ter suas informações acessadas por outros na Internet.

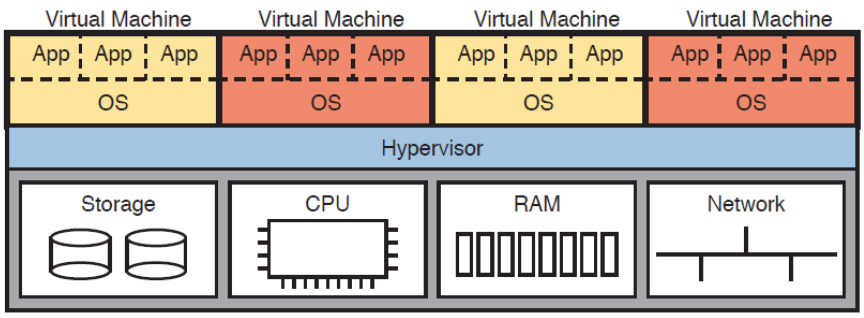
- **Proxy Compartilhado**: proxies compartilhados são usados por mais de um usuário ao mesmo tempo. Eles lhe dão acesso a um endereço IP que pode ser compartilhado por outras pessoas, e então você pode navegar na internet enquanto aparece para navegar a partir de um local de sua escolha. Como eles são compartilhados por outros, você pode acabar levando a culpa por eventuais usos indevidos de outra pessoa, o que pode levá-lo ao banimento de um site ou até coisa pior.

- **Proxy Rotativo (Rotating Proxy)**: Um proxy rotativo atribui um endereço IP diferente a cada usuário que se conecta a ele. À medida que os usuários se conectam, eles recebem um endereço único do dispositivo que se conectou antes dele.

14 Opções para Disponibilização dos Serviços de Rede

Tradicionalmente os serviços de rede estão atrelados a um "Servidor", o qual normalmente é uma máquina física com mais capacidade de processamento (CPU) e memória RAM que computadores normais.

Com a evolução das redes e sistemas computacionais surgiram as opções de virtualização de servidores, onde um servidor poderia ter seus recursos físicos compartilhados entre diversas máquinas virtuais ou "Virtual Machines" (VMs).



Dessa maneira os administradores de redes e de servidores puderam utilizar o "espaço ocioso" de memória e processamento de um servidor físico, criando diversas máquinas virtuais para centralizar vários serviços em apenas um dispositivo físico.

Por exemplo, na imagem anterior apenas um servidor está sendo utilizado com quatro sistemas operacionais diferentes, ou seja, com os recursos físicos de um servidor temos quatro VMs, possibilitando que os mesmos serviços ocupem menos espaço físico em rack e, por consequência, reduza o consumo de energia e custos operacionais de manutenção de hardware.

Atualmente maioria das empresas está migrando muitos desses serviços para a "Nuvem" ou "Cloud Computing".

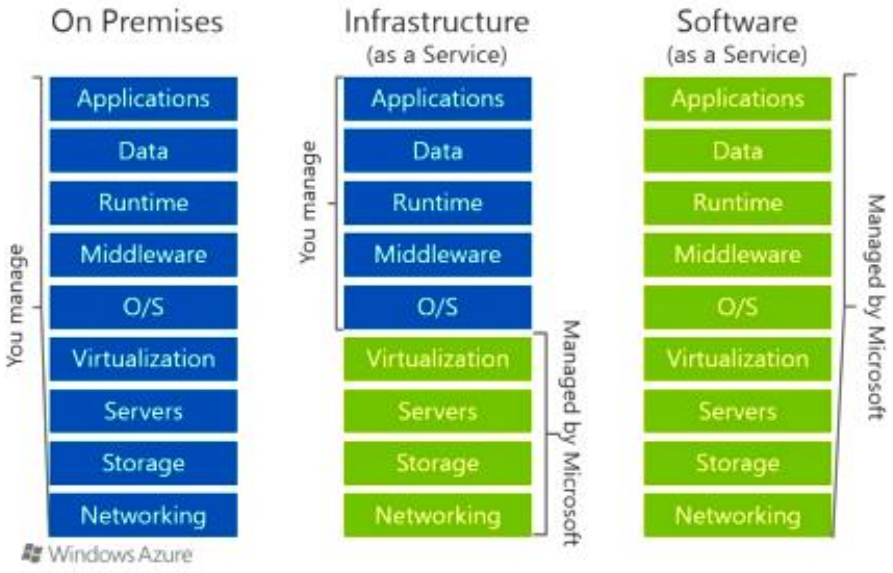
Uma nuvem pode ser **On-Premise** (dentro da empresa: nuvem privada ou private cloud) ou **pública** (public cloud ou apenas **Cloud**).

Existe também as nuvens **híbridas** ou **Hybrid Cloud**, uma mistura dos dois tipos de nuvens anteriores.

Você provavelmente já utiliza serviços em nuvem nas suas atividades pessoais ou até na empresa que trabalha.

Quando falamos em serviços em Nuvem temos algumas opções que são importantes conhecer:

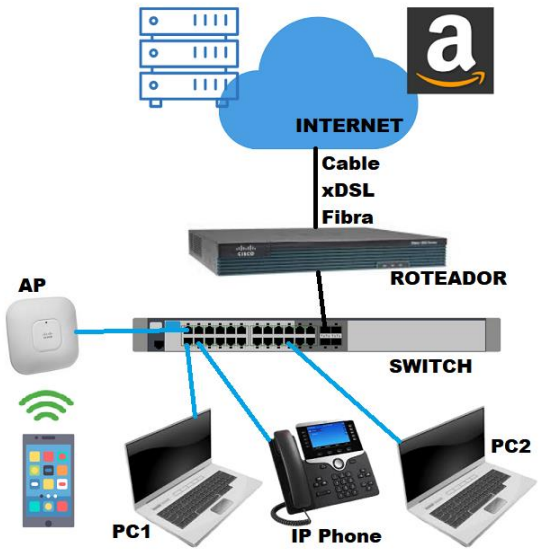
- **IaaS** - **Infrastructure as a Service:** na Infraestrutura como Serviço o cliente se utiliza uma percentagem de um servidor, geralmente com uma configuração que se adeque à sua necessidade, por exemplo, Winows Azure e Amazon Web Services (AWS). Esse serviço o mais simples de ser entendido, pois ele se assemelha a comprar um computador, onde você especifica as capacidades de CPU, memória RAM, armazenamento, sistema operacional e tem seu servidor em nuvem preparado para instalação dos seus aplicativos. Um dos serviços mais comuns é o Amazon Web Services (AWS), um provedor de nuvem pública onde você cria sua VM com parte do serviço de IaaS.



- **SaaS - Software as a Service:** o Software como Serviço é o uso de um software via web, por exemplo, Gmail, Office 360, Google Docs, Drop Box, Apple iCloud e Microsoft SharePoint Online. Além disso, maioria dos serviços de e-mail são considerados SaaS atualmente, até a Microsoft já está oferecendo a opção de utilização do Exchange como serviço, ou seja, você pode ter seus e-mails via Exchange sem precisar da licença instalada em seus servidores, pois o serviço está em nuvem. É importante lembrar que nessa modalidade de serviços o cliente não escolhe a máquina virtual que rodará o serviço de software ou suas características, ele apenas escolhe as opções da aplicação que deseja utilizar.

Além disso, serviços básicos de Rede como DHCP e TFTP podem ser administrados pelos próprios dispositivos de Rede como Roteadores e Switches L3.

É muito comum em unidades remotas (Branch Offices) ou pequenos escritórios (SOHO: Small Office | Home Office) os roteadores locais agregarem funções como a de servidor DHCP, Gateway de Internet, NAT ou Proxy Router, Firewall e concentrador VPN para a rede local.



Existem até dispositivos de Rede que suportam instalação de módulos de Servidor e Storage para a disponibilização localizada de aplicações.

14.1 Exemplo Prático dos Serviços de Rede

Conteúdo disponível apenas em vídeo aula.

15 Conclusão do Curso Serviços de Rede e Certificado

Parabéns por ter chegado ao final do curso Serviços de Rede!

Tenha certeza de que compreendeu todos os conceitos aqui mostrados:

- Conhecer os principais serviços e aplicações em Redes TCP/IP.
- Descrever o funcionamento dos serviços da camada de Aplicação:
  - Serviços de e-mail
  - Serviços de terminal e acesso remoto
  - Serviços de web
  - Gerenciamento de redes
  - Troca de arquivos em rede
  - Fornecimento de endereços IPs dinâmicos
  - Voz e Vídeo sobre IP
  - Serviços de diretórios
  - Compartilhamento de arquivos
  - Sincronização dos relógios dos dispositivos de Rede
- Descrever o funcionamento dos serviços da camada de Rede:
  - NAT, PAT e Proxy
  - Encaminhamento de portas
- Descrever as possíveis opções de disponibilização dos serviços de Rede: Servidor, VM e Cloud

Não esqueça que você deve ler e assistir tudo para obter o seu certificado de conclusão do curso.

Ficamos por aqui e nos encontramos nos próximos cursos!!!!!