A camada de aplicação é constituída pelos serviços e aplicações de rede, é a camada mais próxima do usuário final, sendo responsável por fornecer a interface entre os aplicativos usados para se comunicar e a rede pela qual as mensagens são transmitidas. A camada de aplicação do modelo TCP/IP é responsável por cumprir as funções descritas nas camadas de Aplicação, Apresentação e Sessão do modelo OSI.

Os protocolos da camada de aplicação são utilizados para troca de dados, através de mensagens entre programas executados nos hosts de origem e destino, estes protocolos são confundidos com os próprios serviços, pois em muitos casos, seus nomes são os mesmos. Há muitos protocolos e serviços da camada de aplicação e outros novos estão em constante desenvolvimento.

Dentre os protocolos da camada de aplicação mais conhecidos podemos citar o HTTP (Hypertext Transfer Protocol), utilizado na navegação WEB, o FTP (File Transfer Protocol) e o TFTP (Trivial File Transfer Protocol) para transferência de arquivos, o IMAP (Internet Message Access Protocol) e o POP3 utilizados para troca de e-mails, além do DNS (Domain Name System) utilizado para resolução de nomes na Internet.

Objetivo de Aprendizagem do Capítulo:
(Insira os objetivos de aprendizagem do capítulo conforme o documento de Briefing).

- Entender as funções das camadas de aplicação, apresentação e sessão do modelo OSI a partir da camada de aplicação do modelo TCP/IP.
- Entender o funcionamento dos serviços de FTP, e-Mail e WEB.
- Entender os serviços de resolução de nomes DNS e configuração automática DHCPv4 e DHCPv6.

1. Título do Subtema

(Texto)

Funções da camada de aplicação

No modelo OSI, a camada de aplicação é a camada mais próxima do usuário final, é a camada que fornece a interface com os aplicativos usados para se utilizar os serviços de rede. No modelo TCP/IP a camada de aplicação incorpora funções descritas nas camadas de apresentação e sessão do modelo OSI, além é claro, das próprias funções da camada de aplicação. A figura 1 apresenta a relação entre a

camada de aplicação do modelo TCP/IP e as camadas de aplicação, apresentação e sessão do modelo OSI.

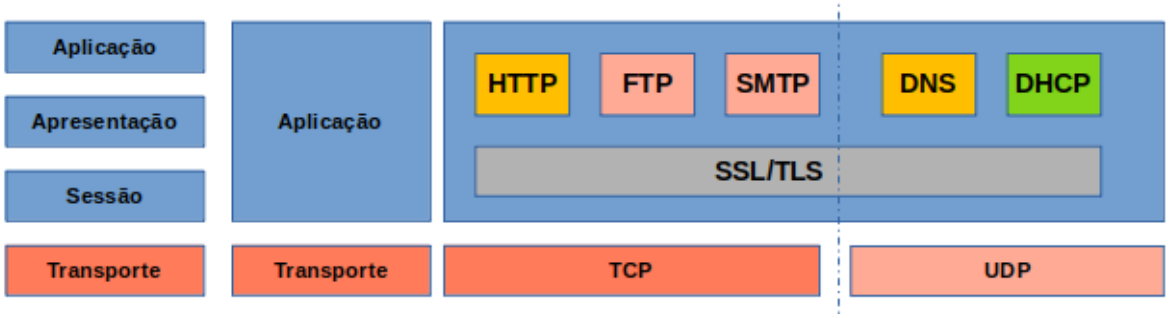


Fig. 1 - Relação entre a camada de aplicação do modelo TCP/IP e as camadas de aplicação, apresentação e sessão do modelo OSI. Fonte: o autor

1.1.Camada de apresentação

A camada de apresentação do modelo OSI as seguintes funções principais:

- Formatar os dados fornecidos pela camada de aplicação do dispositivo de origem em um formato compatível para recebimento pelo dispositivo de destino.
- Comprimir dados e descomprimir os dados a serem transmitidos.
- Criptografar dados para transmissão e descriptografar dados após o recebimento.

1.1.1. Criptografia dos dados

No modelo TCP/IP a criptografia de dados é feita através dos protocolos SSL/TLS. O SSL - Secure Socket Layer, desenvolvido inicialmente pela Netscape em 1995 e já descontinuado, foi substituído atualmente pelo TLS - Transport Layer Security, atualmente na versão 3.0 definido pela RFC 8446. A figura 2 apresenta o protocolo SSL em relação ao modelo TCP/IP.

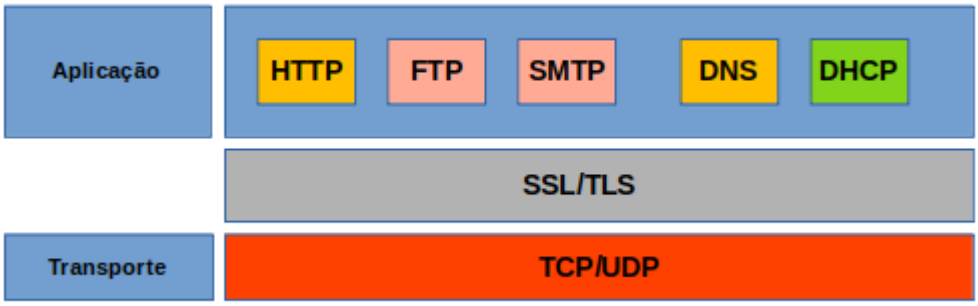


Fig.2. Protocolo TLS no modelo TCP/IP

Este protocolo é capaz de estabelecer uma conexão segura entre duas entidades e de garantir que dois aplicativos consigam se comunicar, garantindo a confidencialidade e autenticidade dos dados no canal de comunicação.

1.2. Camada de sessão

Como o nome sugere, as funções na camada de sessão criam e mantêm os diálogos entre as aplicações origem e destino. A camada de sessão processa a troca de informações para iniciar diálogos, mantê-los ativos e reiniciar sessões interrompidas ou ociosas por um longo período. No modelo TCP/IP geralmente essa função está embutida dentro dos serviços de rede da camada de aplicação.

2. Serviço DNS, e-Mail e WEB

Dos serviços de rede e Internet DNS, e-Mail e WEB são os mais utilizados, baseados neles uma gama de aplicações que vai desde redes sociais, aplicações bancárias e e-commerce foram construídas mudando a forma como trabalhamos, nos entretemos e nos relacionamos atualmente. Conhecer a base desses serviços é fundamental para um profissional de TI.

2.1. Domain Name Service - DNS

Os serviços de Rede (Internet) que usamos diariamente encontram-se instalados nos mais variados locais e cada um deles um endereço IP exclusivo que o identifica univocamente na rede. Seria impossível para nós humanos lembrar todos os endereços IP de todos os servidores que hospedam serviços na Internet, pois não somos muito bons em guardar números. O DNS (Domain Name System) permite utilizar nomes ao invés do IP para solicitar um serviço de rede. Os nomes DNS são

registrados e organizados na Internet, em um banco de dados hierárquico e distribuído, em grupos de alto nível específicos, chamados domínios. Alguns domínios de alto nível mais comuns na Internet são .com, .edu e .net, assim como um domínio para cada país como, .br. A figura 3 apresenta esta hierarquia de domínios.

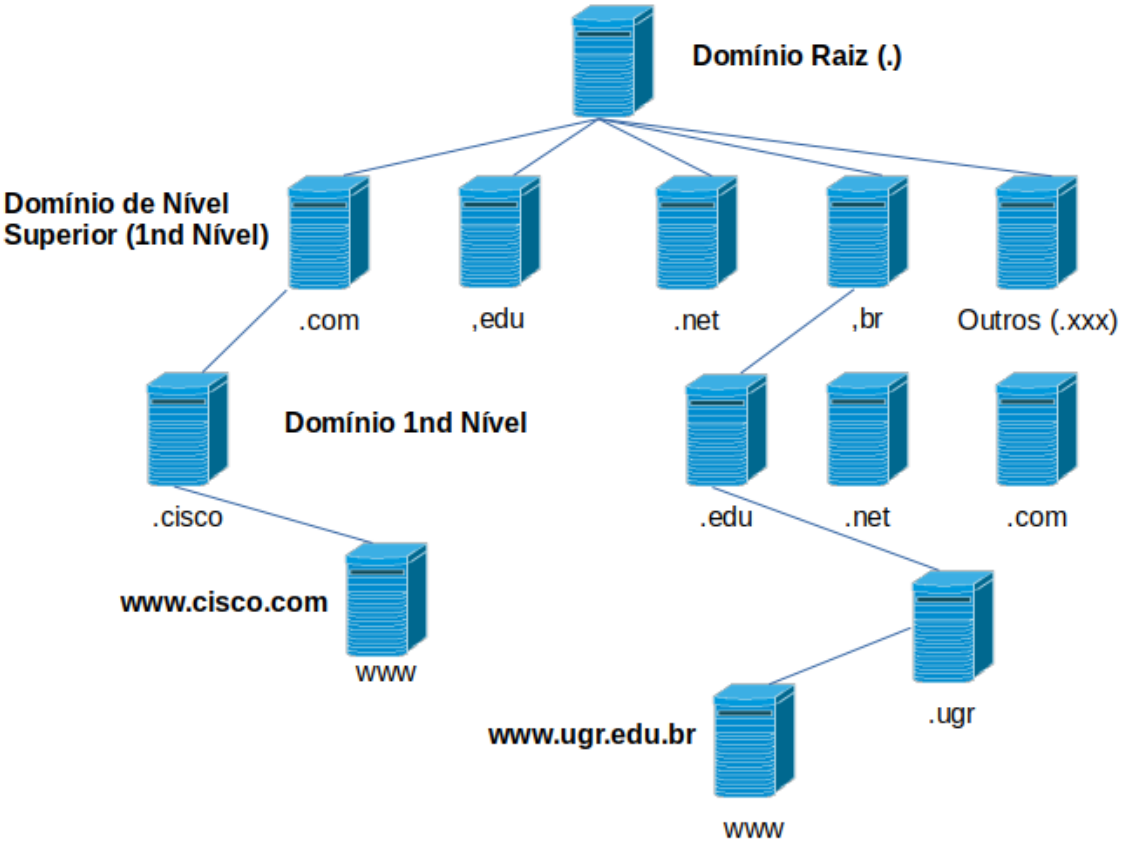


Fig. 3 - Hierarquia de Domínios DNS

Assim um determinado host tem seu nome definido desde a sua posição na hierarquia (na forma de uma árvore invertida) da base de dados até a raiz formando o seu FQDN - Full Qualified Domain Name, nome exclusivo, como por exemplo www.ugr,edu.br (o ponto que representa a raiz é omitido) ou www.cisco.com. Para utilizarmos o serviço de DNS, quando configuramos o endereçamento IP de um host além do seu endereço IP e do gateway padrão também precisamos definir o endereço dos servidores DNS primário e, opcionalmente, o secundário A figura 4 apresenta a configuração endereçamento IPv4 de um host Windows.

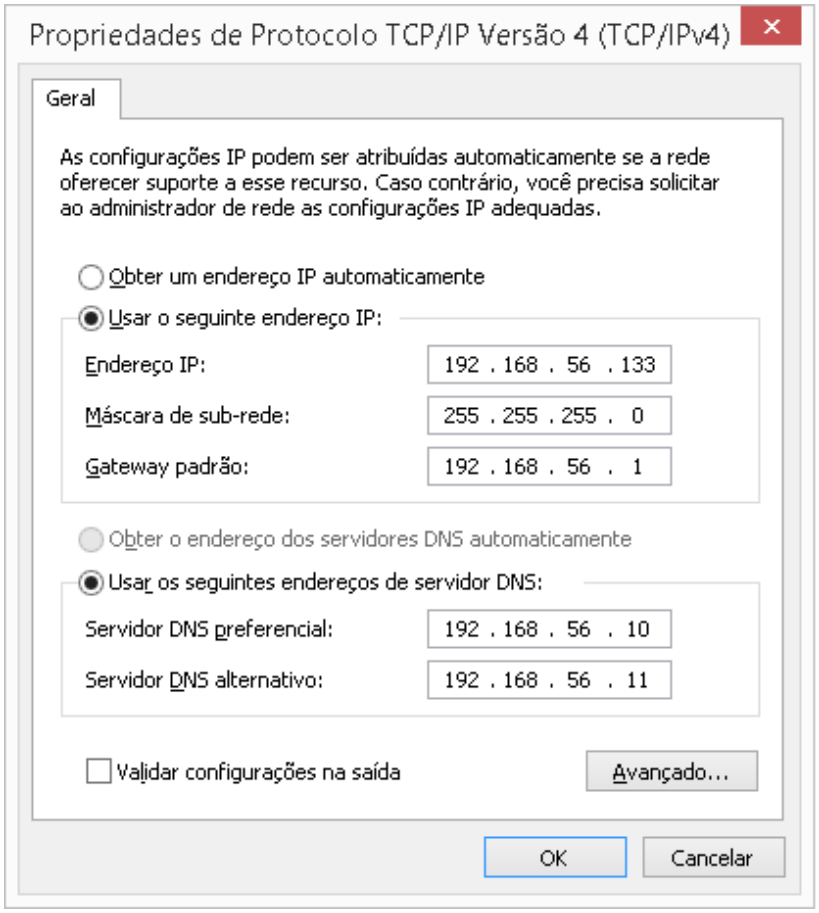


Fig. 4 - Configuração IPv4 de um host Windows com DNS

Nela podemos ver os servidores DNS preferencial (Primário) e DNS alternativo (secundário) configurados com os IPv4 192.168.56.10 e 92.168.56.10 respectivamente.

Consulta DNS

Entender mesmo que de forma simplificada como uma consulta DNS é executada é muito importante para entender o mecanismo de navegação WEB. Quando um usuário digita um nome de domínio, por exemplo, www.urg.edu.br, o resolver, que é o cliente DNS embutido como uma rotina do Sistema Operacional do cliente, executa a seguinte sequência de consulta:

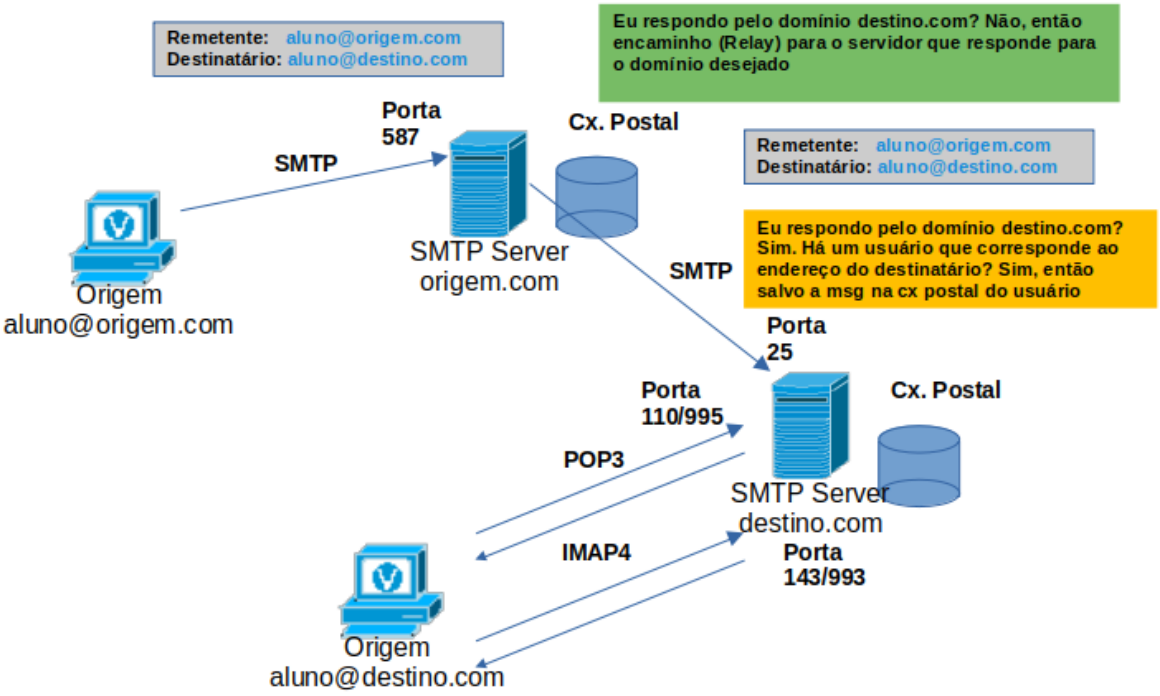
1. O resolver consulta as entradas do arquivo /etc/hosts no Linux/Unix ou C:\Windows\System32\drivers\etc no caso do Windows.
2. Caso não encontre o nome consultado, envia a consulta para o servidor DNS que está especificado nas configurações do protocolo IP da interface de rede. (Normalmente o roteador DSL da sua residência)

3. O Roteador faz um encaminhamento da consulta (forward) e envia a requisição para o servidor DNS do seu provedor (ISP).
4. Caso esse servidor não, tenha a informação no seu cache, e não seja a autoridade sobre o domínio, e também não conheça o servidor DNS responsável pelo domínio urg.edu.br, a requisição é enviada para um servidor DNS raiz, o qual é responsável por conhecer os domínios Top-Level Domain (TLD), devolvendo essa informação ao servidor.
5. Este por sua vez, consulta o servidor Top-Level Domain (TLD) para receber a informação do servidor de nível secundário, recebendo essa informação, no caso, .edu.br. Este processo se repete até o servidor de DNS receber a informação de servidor responsável (autoridade) sobre o domínio.
6. A requisição então é encaminha para o servidor autoritativo responsável pelo domínio ibmec.edu.br
7. O servidor autoritativo do domínio ugr.edu.br responde o endereço IP do host www.urg.edu.br
8. O servidor DNS do seu ISP então retorna a consulta para o seu roteador, que retorna para resolver.

Importante: O serviço de DNS utiliza o protocolo UDP 53 para consultas dos clientes e a porta TCP 53 para atualização e sincronismo entre os servidores.

2.2. Serviço de e-mail - Protocolos SMTP, POP3 e IMAP4

O e-mail (correio eletrônico) é um dos mais antigos e populares serviços de Internet. Com ele podemos trocar correspondências (mensagens de e-mail) como fazemos utilizando o serviço postal (Correio), só que muito mais rápido. Os clientes de e-mail se comunicam com os servidores de e-mail para enviar, através do protocolo SMTP ou receber e-mails, através dos protocolos POP3 ou IMAP, estes por sua vez se comunicam com outros servidores de e-mail, utilizando o protocolo SMTP, para transportar mensagens de um domínio para outro. Um cliente de e-mail não se comunica diretamente com outro para enviar e-mails. Em vez disso, os clientes utilizam os servidores para transportar mensagens. Cada servidor recebe e armazena os e-mails de usuários em caixas de correio configuradas no servidor, cada usuário deve usar um cliente de e-mail para acessar sua caixa postal e ler essas mensagens. Para utilizar o serviço de e-Mail um usuário precisa possuir um endereço no formato “usuario@Donínio“ como por exemplo aluno@alunos.ibmec.edu.br. A figura 5 ilustra o processo de envio de mensagens de um remetente até o destinatário.



Protocolo SMTP

O protocolo SMTP é definido pela RFC 6531, é responsável pelo envio de mensagens do destinatário (cliente), até o servidor SMTP, num processo chamado submissão, utilizando inicialmente a porta TCP 25, mas atualmente utilizando a porta TCP 587, via TLS. Caso o destinatário exista no mesmo servidor, isto é, o usuário é do mesmo domínio do remetente ou o servidor responde por ambos os domínios, a mensagem será salva no diretório do sistema de arquivos correspondente à caixa postal do usuário. Caso contrário o servidor localizará (via DNS) o servidor responsável pelo domínio do remetente e encaminhará a mensagem (fará um relay), normalmente utilizando a porta TCP 25, para este servidor, que salvará a mensagem no diretório do sistema de arquivos correspondente à caixa postal do usuário.

Protocolo POP3

Quando um cliente deseja recuperar as mensagens a ele enviadas, utilizando o protocolo POP3 (RFC 1939), ele envia uma solicitação para estabelecer uma conexão TCP 110 ou 995, via TLS com o servidor. Quando a conexão é estabelecida as mensagens de e-mail são baixadas para o cliente e removidas do servidor, portanto não há um local centralizado onde as mensagens de e-mail sejam mantidas.

Protocolo IMAP4

O IMAP4 (RFC 9051) é outro protocolo que descreve um método para recuperar mensagens de e-mail. Ao contrário do POP, quando o usuário se conecta a um servidor compatível com IMAP, as cópias das mensagens são baixadas para o aplicativo cliente e as mensagens originais são mantidas no servidor até que sejam excluídas manualmente. Os usuários podem criar uma estrutura de pastas no servidor para organizar e armazenar os e-mails que também é duplicada e sincronizada no cliente de e-mail.
Importante: Muitos sistemas de mensagens de Internet (webmail) usam um cliente baseado na Web para acessar e-mails, utilizando o protocolo IMAP4. Alguns exemplos desse tipo de cliente são Hotmail, Yahoo e Gmail.

2.3. Serviço WWW (World Wide Web)- Protocolo HTTP

Um projeto criado no CERN (Organização Europeia para a Pesquisa Nuclear) por Tim Berners-Lee nos anos 80 e apresentado em 1991, tornou-se a principal ferramenta o o responsaúel pela pela Internet que temos hoje.

Este serviço se baseia no compartilhamento de documentos de hipertexto e atualmente multimídia com base em uma linguagem de formatação HTML (Hypertext Markup Language), e do protocolo HTTP (Hypertext Transfer Protocol) definido na RFC 9112 recentemente publicada, que estabelece um protocolo aplicação sem estado, do tipo pedido e resposta, para sistemas de informação de hipertexto distribuídos e colaborativos que responde por padrão na porta TCP 80 e TCP 443 para HTTPS (HTTP sobre SSL/TLS), isto é, para conexões seguras. A figura 5 ilustra uma conexão padrão de um cliente a um servidor WEB.

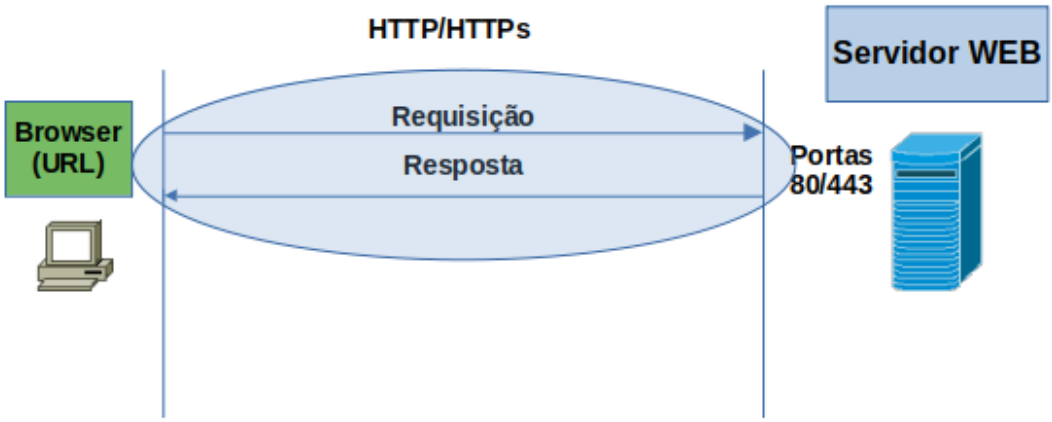


Fig. 5 - Conexão padrão - HTTP/HTTPs

Quando um cliente da Web (navegador) recebe a URI (endereço) de um servidor da Web, ele usa esse endereço IP e a porta TCP 80 ou 443 para solicitar serviços da Web, utilizando o protocolo HTTP. Quando o servidor recebe uma requisição, responde enviando a página da Web, solicitada na URL, para o cliente. O conteúdo de informações de uma página da Web é codificado por meio de linguagens de marcação especializadas, a linguagem HTML (HyperText Markup Language) informa ao navegador o modo de formatação da página da Web, além de gráficos e fontes a serem usados, outros formatos como XML e XHTML também podem ser utilizados

2.3.1 - URI - Uniform Resource Identificator

A URL, e um identificador universal de recursos, proposto pela RFC 8820, define um formato padrão para requisições na Internet. A figura 6 apresenta um URI e seus elementos construtivos.

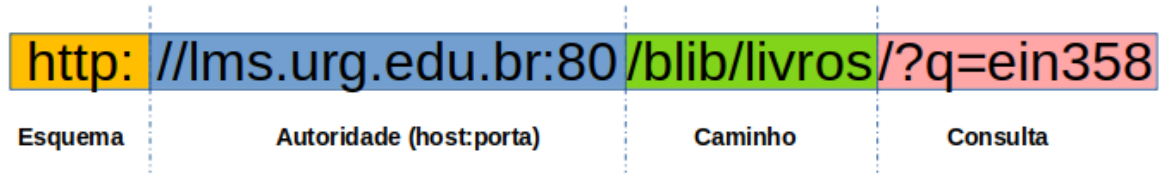


Fig. 6 - URL fonte: o autor

Esquema (Schema) - Especifica qual o protocolo usado na requisição HTTP, HTTPs, FTP, etc.

Autoridade (Authority) - Definir o servidor de destino, é composto de duas parte o nome ou endereço IP do servidor e a porta para a qual o serviço responde (normalmente 80 ou 443)

Caminho (Path) - Representa o caminho do recurso, a localização do recurso, os dados ou objeto, a ser manipulado no servidor. O caminho é precedido por uma barra (/) e pode consistir em vários segmentos separados por uma barra (/).

Consulta (Query) - A consulta, incluindo os parâmetros de consulta, é opcional, fornece detalhes adicionais para escopo, filtragem ou para especificar uma solicitação. Se estiver presente, ela será precedida por um ponto de interrogação (?). Não há uma sintaxe específica para parâmetros de consulta, mas geralmente é definida como um conjunto de pares chave-valor separados por um e comercial (&). Por exemplo, ?origem=RJ&destino=SP

2.3.2 - Mensagens HTTP

As mensagens HTTP são compostas de informação textual codificada em ASCII, e se espalham por múltiplas linhas, porém com uma estrutura básica dividida entre um cabeçalho (header) e um corpo (Body). O formato específico da mensagem vai depender do tipo de mensagem, se de requisição ou resposta.

2.3.2.1. Requisição HTTP

Uma requisição HTTP é apresentada na figura 7 e é composta dos seguintes elementos:

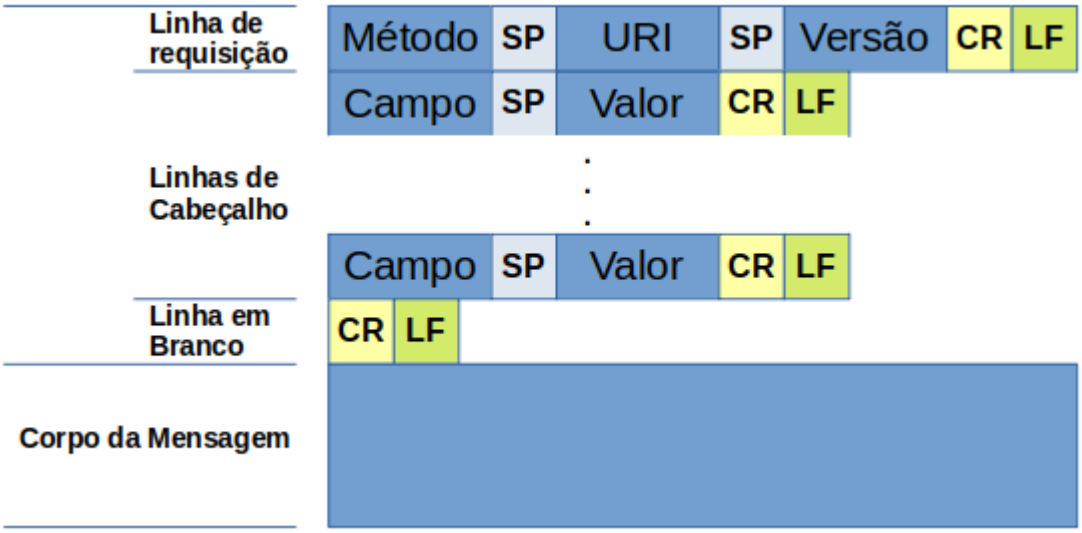


Fig. 7 - Requisição HTTP

Linha de requisição (1nd linha da mensagem) - Indica os parâmetros da requisição, método HTTP a ser utilizado na requisição, a URL e a versão do protocolo separados por um espaço, seguidos de um fim de linha e uma marca de parágrafo (CR+LF)

Linhas de cabeçalho - São linhas opcionais que tem o objetivo de passar informações adicionais entre o cliente e o servidor. São formatadas como pares nome-valor separados por dois pontos (:), [nome]:[valor], e podem representar informações relacionadas à requisição ou a entidade (corpo da mensagem).

Linha em Braco - Indica o Fim do cabeçalho e o início do corpo da mensagem, representada por fim de linha e uma marca de parágrafo (CR+LF)

Corpo do documento - O corpo de uma requisição HTTP contém os dados referentes ao recurso que o cliente deseja manipular. As requisições usam os métodos HTTP, POST, PUT e PATCH geralmente incluem um corpo. Dependendo do método HTTP, o corpo é opcional, mas quando são incluídos na mensagem, o tipo de dados deverá ser especificado no cabeçalho usando a chave Content-Type.

2.3.2.1.1. Métodos HTTP

Os métodos HTTP padrão, definem as ações que serão executadas no servidor, por isso também são conhecidos como verbos HTTP. Os principais métodos são definidos na tabela 1.

Tabela 1 – Principais métodos HTTP	
GET	O método GET solicita a representação de um recurso específico. Requisições utilizando o método GET devem retornar apenas dados. Neste método os dados enviados pelo cliente são enviados na URI no campo Consulta. Estes dados não podem ser criptografados pelo protocolo SSL/TLS.
HEAD	O método HEAD solicita uma resposta de forma idêntica ao método GET, porém sem conter o corpo da resposta.
POST	O método POST é utilizado para submeter uma entidade a um recurso específico, frequentemente causando uma mudança no estado do recurso ou efeitos colaterais no servidor. Os dados enviados são anexados no corpo do documento. Os dados enviados são anexados no corpo do documento possibilitando que os mesmos sejam criptografados pelo protocolo SSL/TLS
PUT	O método PUT substitui todas as atuais representações do recurso de destino pela carga de dados da requisição.
DELETE	O método DELETE remove um recurso específico.

Tabela 1 - Principais métodos HTTP Fonte: Adaptado de https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Methods

2.3.2.2. Resposta HTTP

Uma resposta HTTP retorna o resultado da requisição HTTP efetuado pelo cliente, e pode conter os dados que foram solicitados, a informação de que o servidor recebeu sua solicitação ou até mesmo informar um problema com a requisição. O formato de uma requisição HTTP é apresentado na figura 8.

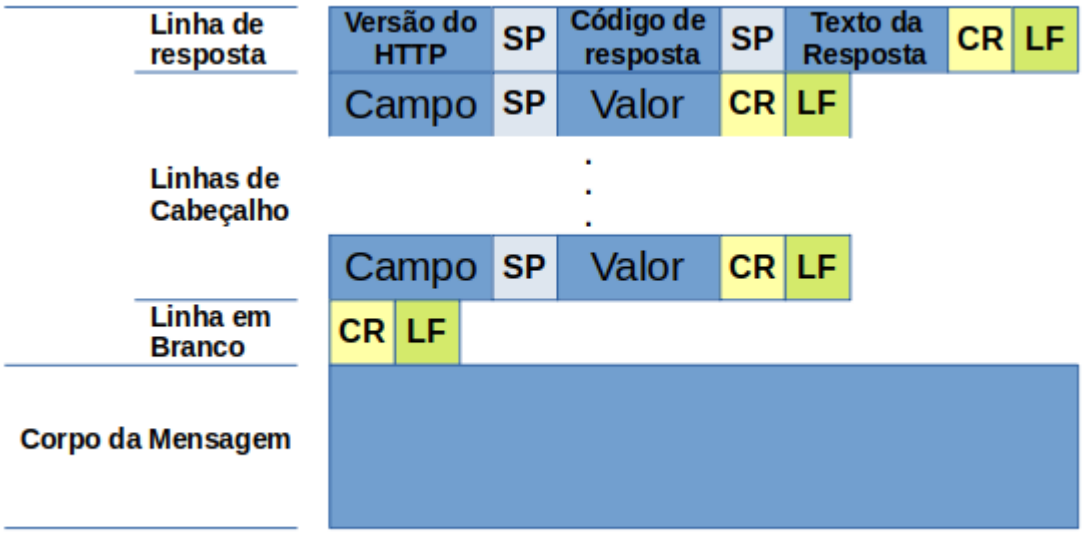


Fig. 8 - Mensagem de resposta HTTP fonte: o autor

Linha de resposta (1nd linha da mensagem) - Indica os parâmetros da resposta, a versão do protocolo HTTP, o código de status da resposta e um texto descrevendo o status, separados por um espaço, seguidos de um fim de linha e uma marca de parágrafo (CR+LF)

Linhas de cabeçalho - Assim como na requisição as linhas de cabeçalho são opcionais que tem o objetivo de passar informações adicionais entre o servidor e o cliente, também são formatadas como pares nome-valor separados por dois pontos (:), [nome]:[valor], e podem representar informações relacionadas à resposta ou a entidade (corpo da mensagem) que está sendo transmitida.

Linha em Braco - Indica o Fim do cabeçalho e o início do corpo da mensagem, representada por fim de linha e uma marca de parágrafo (CR+LF)

Corpo do documento - O corpo de uma resposta HTTP contém os dados referentes ao recurso solicitado pelo cliente. As respostas HTTP podem não conter corpo, mas quando são incluídos na mensagem, o tipo de dados deverá ser especificado no cabeçalho usando a chave Content-Type.

Códigos de resposta HTTP

Os códigos de resposta de status HTTP são utilizados para informar ao cliente se a solicitação foi bem-sucedida ou mal sucedida, além disso podem ajudar o cliente a determinar o motivo do erro e, às vezes, fornecer sugestões para corrigir o problema. Os códigos de status HTTP são sempre de três dígitos, o primeiro indica a categoria da resposta, um status específico dentre de cada categoria. A tabela 5 apresenta alguns dos códigos de status mais comuns para cada classe.

Tabela 5 - Códigos de status HTTP mais comuns

Código de status HTTP	Categoria	Mensagem de status	Descrição
200	2xx - sucesso	OK	A solicitação foi bem-sucedida e normalmente contém uma carga útil (corpo)
201		Criada	A solicitação foi atendida e o recurso solicitado foi criado
202		Aceitaram	A solicitação foi aceita para processamento e está em andamento
301	3xx - redirecionamento	Movido permanentemente	Esse código de resposta significa que a URI do recurso requerido mudou. Provavelmente, a nova URI será especificada na resposta.
400	4xx - erro do cliente	Pedido ruim	A solicitação não será processada devido a um erro com a solicitação
401		Não autorizado	A solicitação não possui credenciais de autenticação válidas para realizar a solicitação
403		Proibido	A solicitação foi compreendida, mas foi rejeitada pelo servidor
404		Não encontrado	A solicitação não pode ser atendida porque o caminho do recurso da solicitação não foi encontrado no servidor
500	5xx - erro do servidor	Erro do Servidor Interno	A solicitação não pode ser atendida devido a um erro do servidor
503		Serviço não disponível	A solicitação não pode ser atendida porque atualmente o servidor não pode lidar com a solicitação

3. Serviço DHCP IPv4 e IPv6

O DHCPv4 (Dynamic Host Configuration Protocol - IPv4) , especificado pela RFC 2131, é um serviço da camada de aplicação do modelo TCP/IP que atribui endereços IPv4 e outras informações de configuração de rede dinamicamente para os dispositivos de rede, utiliza a porta UDP 67 no servidor e UDP 68 no cliente. Um servidor DHCP pode ser baseado em Linux, MS Windows Server ou pode ser configurado em um roteador ou switch de camada 3 da rede. Os principais conceitos associados ao DHCPv4 são descritos a seguir:

- **Escopo:** É o intervalo consecutivo completo de endereços IP possíveis para uma rede por exemplo para a rede 192.168.1.0/24 o escopo será a faixa de endereços de 1 a 254.
- **Intervalo de exclusão:** É uma sequência limitada de endereços IP dentro de um escopo, que não são fornecidos pelo DHCP.
- **Pool de endereços:** Após definir um escopo DHCP e aplicar intervalos de exclusão, os endereços remanescentes formam o pool de endereços disponíveis dentro do escopo. Endereços em pool são qualificados para atribuição dinâmica pelo servidor para clientes DHCP na sua rede.
- **Concessão (Lease):** É a atribuição ao cliente de um endereço IP por um determinado período de tempo feita pelo servidor DHCP. Existem três formas dessa reserva ser feita:

- **Manual:** Neste caso, é possível atrelar um endereço IP a uma determinada máquina na rede. Para isso, é necessária a associação de um endereço existente no banco do servidor DHCP ao endereço MAC do adaptador de rede da máquina.
- **Automática:** Nesta forma, o servidor DHCP é configurado para atribuir um endereço IP a um equipamento por tempo indeterminado. Quando este conecta-se pela primeira vez na rede, lhe é atribuído um endereço por tempo indeterminado..
- **Dinâmica:** Neste tipo de configuração, é que reside a característica principal do DHCP.. Desta forma o endereço IP é alocado temporariamente a um equipamento e periodicamente, é necessária a atualização periódica dessa locação pelo cliente.

O DHCPv4 conforme o modelo cliente/servidor, onde o cliente solicita e o servidor DHCPv4 atribui, ou aluga (leasing), dinamicamente, um endereço IPv4 de um pool de endereços por um tempo determinado, configurado pelo administrador no servidor ou até que o cliente libere (release) esse endereço. O cliente deve renovar o leasing periodicamente caso deseje se manter conectado à rede.

O processo de obtenção de um endereço IP através do serviço de DHCPv4 é feito em quatro etapas ilustradas na figura 9:

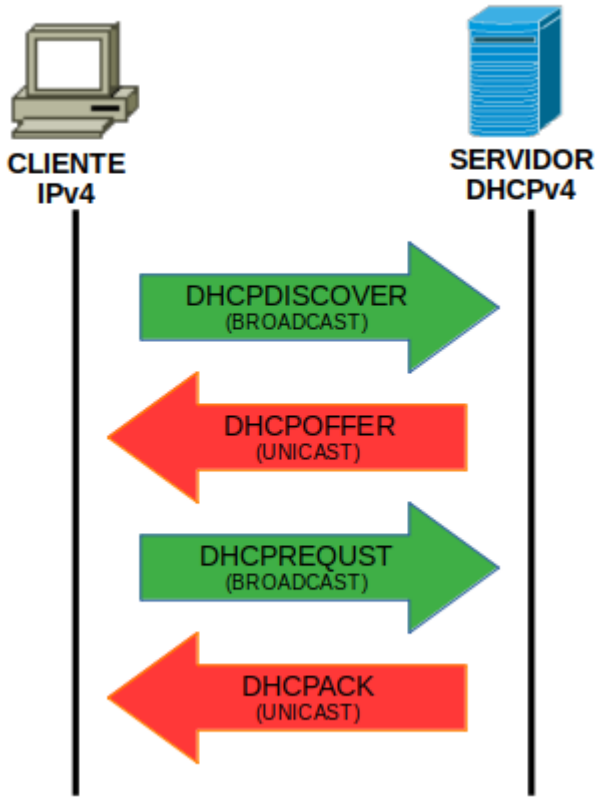


Fig. 12 processo de obtenção de um endereço IP através do serviço de DHCPv4 Fonte: o autor

9. **Descoberta do servidor DHCPv4 (DHCPDISCOVER)** - O cliente envia uma mensagem de broadcast com seu próprio endereço MAC - DHCPDISCOVER - para descobrir os servidores DHCPv4 disponíveis.

10. **Oferta DHCPv4 (DHCPOFFER) -** Quando o servidor DHCPv4 recebe a mensagem de descoberta DHCPDISCOVER, reserva o endereço IPv4 disponível para alugar para o cliente e envia a mensagem DHCPOFFER para o cliente solicitante com o endereço IPv4 reservado e outras informações de configuração.

11. **Solicitação de DHCPv4 (DHCPREQUEST) -** Uma vez que o cliente recebe o DHCPOFFER do servidor, ele envia uma mensagem de broadcast DHCPREQUEST como um aviso de aceitação de vinculação para o servidor selecionado e uma recusa implícita para os outros servidores que também enviaram uma oferta de vinculação. Essa mensagem também é utilizada quando o cliente solicita a renovação do aluguel (leasing) do seu endereço IPv4.

12. **Confirmação de DHCPv4 (DHCPACK) -** Após receber o DHCPREQUEST, o servidor verifica a concessão com um ping ICMP no endereço IPv4 concedido e em seguida envia uma mensagem DHCPACK. Quando o cliente recebe o DHCPACK, ele grava os dados recebidos e executa uma pesquisa ARP para o endereço que lhe foi atribuído. Se não receber uma resposta ao ARP, saberá que nenhum outro dispositivo da rede possui um endereço igual e pode usá-lo sem problemas.

3.2. Obtenção de endereço IPv6 dinamicamente

No IPv6 um dispositivo de rede pode ter dois tipos de endereço, um endereço unicast global (GUA) e um endereço de link local (LLA). O endereço de link local IPv6 é criado automaticamente pelo host quando ele é inicializado e a interface Ethernet está ativa. Para obter um endereço IPv6 endereço unicast global (GUA) um host não usa os mesmos mecanismos utilizados no DHCPv4, ele usará os métodos definidos pela flags da mensagem ICMPv6 - Router Advertisement (RA) recebida na interface vinda de um roteador IPv6 que está no mesmo link que o host sugerindo a este como obter suas informações de endereçamento IPv6. A tabela 6 resume como o endereço IPv6 pode ser obtido.

Tabela 6 - Obtenção dinâmica de endereços IPv6

Tipo	Descrição	Flag		
		Flag A	Flag O	Flag M

SLAAC	O roteador envia mensagens de anúncio RA (Router Advertisement) com o prefixo da rede, o tamanho do prefixo e o endereço do gateway padrão. O host então cria seu endereço a partir desses parâmetros.	1 (Default)	0 (Default)	0 (Default)
SLAAC + DHCPv6 Stateless (sem estado)	O roteador envia mensagens de anúncio RA (Router Advertisement) com o prefixo da rede, o tamanho do prefixo, o endereço do gateway padrão e informações do DHCPv6 stateless (não há um servidor que guarde as informações sobre que hosts possuem que endereço) para o host obter dados adicionais. O host então cria seu endereço a partir desses parâmetros, contacta o servidor DHCPv6 para obter dados adicionais.	1	1	0
DHCPv6 Stateful (com estado)	O roteador envia mensagens de anúncio RA (Router Advertisement) instruindo o host a obter os dados do servidor DHCPv6 stateful (o servidor DHCPv6 guarda as informações sobre que hosts possuem um determinado endereço). O host contacta o servidor DHCPv6 para obter todos os dados exceto o endereço do gateway padrão que ele obtém das mensagens RA do roteador.	0	0	1

3.2.1. - SLAAC

O SLAAC (Stateless Address Autoconfiguration) é um método para que dispositivos possam obter um endereço IPv6 Unicast Global (GUA) de forma automática mesmo sem haver um servidor DHCPv6 instalado na rede. Ele utiliza as mensagens ICMPv6 RS (Router Solicitation) e RA (Router Advertisement). A figura 9 ilustra este processo.

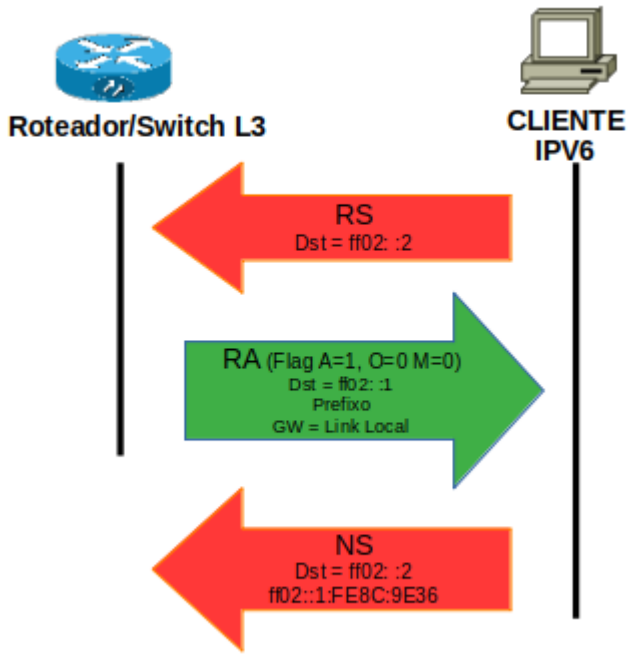


Fig. 9 Esquema de atribuição de endereços IPv6 pelo SLAAC Fonte: o autor

13. O Host configurado para obter o endereço IPv6 dinamicamente, ao iniciar, envia uma mensagem RS (Router Solicitation) para o endereço de multicast FF02::02.

14. O Roteador/Switch L3 responde com uma mensagem RA (Router Advertisement) para o endereço de multicast FF02::02 contendo o prefixo da rede a qual pertence e o seu endereço de link local LLA para ser utilizado como default gateway pelo host e o flag corresponde ao estado configurado (SLAAC)

15. Ao receber a mensagem RA (Router Advertisement) o host deve criar seu endereço GUA a partir das informações de sub-rede IPv6 de 64 bits que adquire do RA do roteador e, gerar o identificador de interface (ID) de 64 bits restante usando um dos dois métodos:

- De forma aleatória - O ID de interface de 64-bit é gerado randomicamente pelo Sistema Operacional do Host. Este é o método agora usado pelos hosts do Windows 10.

- EUI-64 - O host cria um ID de interface usando seu endereço MAC de 48 bits e insere o valor hexadecimal de FFFE no meio do endereço. este processo tem sido evita uma vez que ele já é utilizado para gerar o LLA da interface

Como SLAAC é um processo sem estado, não há garantia de que o endereço gerado seja único, portanto, um host pode verificar se um endereço IPv6 recém-criado é exclusivo antes de ser usado. este processo se chama DAD (Duplicate Address Detection) e, implementado usando ICMPv6 pelo envio de uma mensagem de Solicitação de Vizinhança (NS) ICMPv6 com um endereço multicast especialmente construído, chamado endereço multicast do nó solicitado. Esse endereço duplica os últimos 24 bits do endereço IPv6 do host. Se o host não receber uma mensagem NA de algum outro dispositivo, pode considerar seu endereço como único e utilizá-lo normalmente. Caso contrário, o sistema operacional precisará determinar um novo ID de interface.

3.2.2. DHCPv6

Apesar do DHCPv6 (RFC 8415) e do DHCPv4 serem funcionalmente equivalentes, são independentes um do outro. A troca de mensagens DHCPv6 entre o cliente e servidor só ocorre após o cliente receber a mensagem RA (Router Advertisement) de um roteador ou switch L3, e utiliza a porta UDP 547 no servidor e UDP 547 no cliente. O funcionamento esquemático do DHCPv6 é apresentado na figura 10.

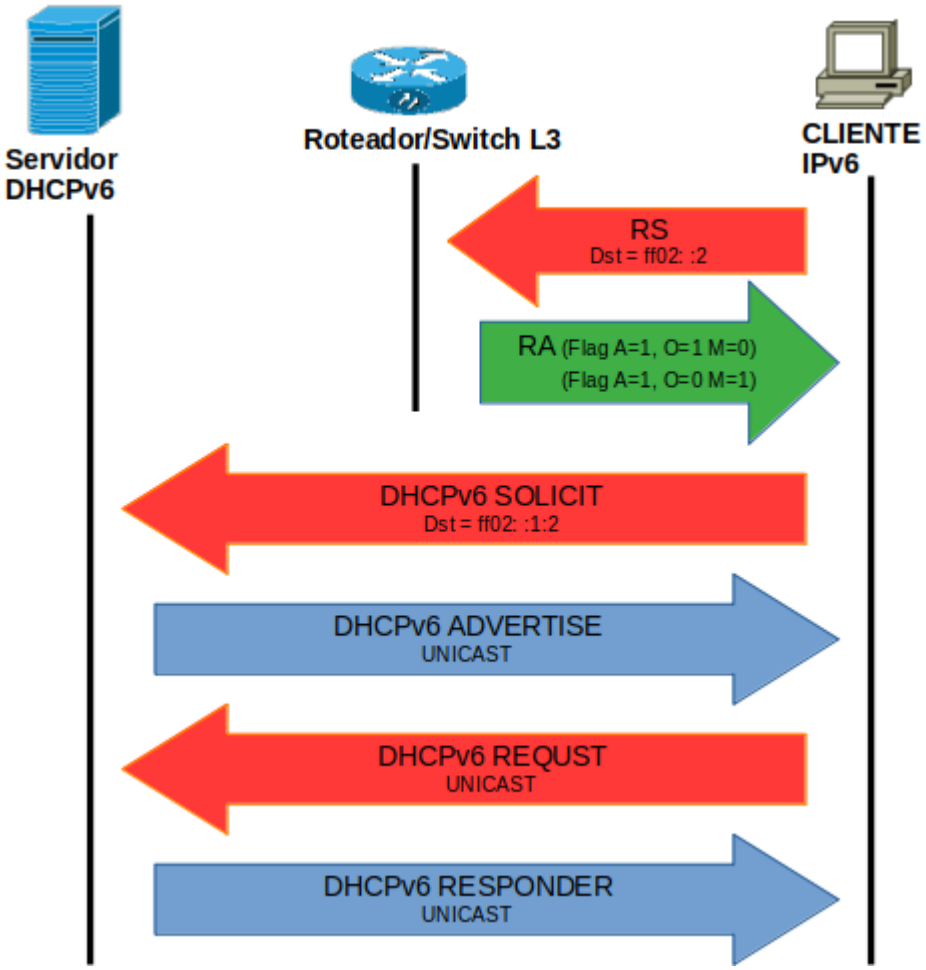


Fig. 9 funcionamento esquemático do DHCPv6 Fonte: o autor

16. O Host configurado para obter o endereço IPv6 dinamicamente ao iniciar envia uma mensagem RS (Router Solicitation) para o endereço de multicast FF02::02.

17. O Roteador/Switch responde com uma mensagem RA (Router Advertisement) para o endereço de multicast FF02::02 contendo o prefixo da rede a qual pertence e o seu endereços de link local LLA para ser utilizado como default gateway pelo host e o Flag (A=1, O=1, M=0 - Stateless ou A=1, O=0, M=1 - Stateful).

18. O host então envia uma mensagem DHCPv6 SOLICIT para o endereço de multicast ff02 :: 1: 2 que possui escopo definido na LAN local e não será difundido para outras redes.

19. Os servidores DHCPv6 respondem com uma mensagem unicast DHCPv6 ADVERTISE, informando ao host que o servidor está disponível para o serviço DHCPv6.

20. Se o Flag da RA (Router Advertisement) for A=1, O=1, M=0 - Stateless o host cria seu endereço GUA a partir das informações de sub-rede IPv6 de 64 bits que adquire do RA do roteador e, gera o identificador de interface (ID) de 64 bits restante usando um dos dois métodos já apresentados e envia uma mensagem DHCPv6 REQUEST um servidor DHCPv6 stateless para obter outras informações

21. Se o Flag da RA (Router Advertisement) for A=1, O=0, M=1 - Stateful o host envia uma mensagem DHCPv6 REQUEST a um servidor DHCPv6 stateful para obter todos os parâmetros necessários para configuração do endereço IPv6.

22. Por fim o servidor envia uma mensagem unicast DHCPv6 RESPONDER ao host. O conteúdo da mensagem depende da solicitação efetuado pelo host REQUEST or INFORMATION-REQUEST.

Importante: O endereço de gateway padrão do host será o endereço de Link-local RA (Router Advertisement) recebido do roteador ou switch L3

Considerações Finais:

A camada de é a camada mais próxima do usuário final, é nela que encontramos os serviços de rede propriamente ditos, sua função é possibilitar a comunicação entre duas ou mais aplicações na rede, através dos protocolos da camada de aplicação que são utilizados para troca de mensagens entre estes programas.

Cada aplicação tem uma característica específica e por isso demanda um protocolo da camada de transporte específico, umas utilizam que necessitam de confiabilidade o TCP enquanto outras, que são mais sensíveis ao atraso, vão fazer uso do UDP

Alguns protocolos estão diretamente ligados aos serviços de rede e as aplicações, como os protocolos da camada de aplicação mais conhecidos podemos citar o HTTP (Hypertext Transfer Protocol), utilizado na navegação WEB, o FTP (File Transfer Protocol) e o SMTP (Simple Mail Transfer protocol), o IMAP (Internet Message Access Protocol) e o POP3 utilizados para troca de e-mails, além do DNS (Domain Name System) utilizado para resolução de nomes na Internet. Já outros estão mais ligados às configurações de rede como o DHCP (Dynamic Host Configuration Protocol) nas versões IPv4 e IPv6 e o SNMP (Simple Network Management Protocol).