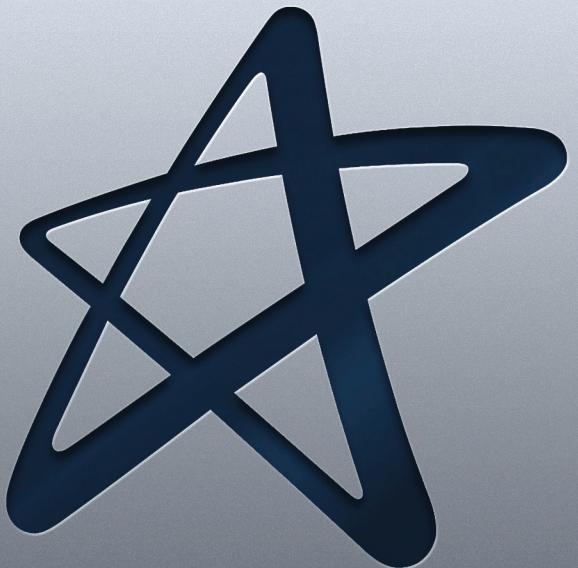


Tecnologias de Redes



Cruzeiro do Sul Virtual
Educação a distância

Material Teórico



Camada de Rede e Endereçamento IP

Responsável pelo Conteúdo:

Prof. Esp. Antonio Eduardo Marques da Silva

Revisão Textual:

Prof. Luciano Vieira Francisco

UNIDADE

Camada de Rede e Endereçamento IP



- Camada de Rede;
- Características do Protocolo IP;
- Encapsulamento IPv4;
- Introdução ao IPv6;
- Encapsulamento IPv6;
- Endereçamento IP;
- Representação e Formato de Preferência do IPv6.



OBJETIVO DE APRENDIZADO

- Compreender as principais características da camada de rede baseada no modelo OSI/ISO e TCP/IP;
- Conhecer o protocolo IP e seus endereços lógicos.



Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:



Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

Camada de Rede

A camada 3 do modelo OSI, ou camada de rede, pode fornecer serviços para que se possa permitir que dispositivos finais troquem dados através da rede. Para que possa fazer o transporte fim a fim, a camada de rede usa quatro processos básicos, que seriam:

1. **Endereçamento:** da mesma maneira que um telefone convencional, que possui um identificador numérico exclusivo, dispositivos finais de rede precisam ser configurados com um endereço IP único que o identifica em uma rede. Tal dispositivo final de rede identificado com um endereço IP é conhecido como host;
2. **Encapsulamento:** em um processo chamado de encapsulamento, a camada correspondente – ou e de rede no exemplo – adiciona as informações do cabeçalho IP, como os endereços IP dos dispositivos origem e destino da transmissão e outros qualificadores de controle. Depois que as informações de cabeçalho são adicionadas à Protocol Data Unit (PDU) correspondente, é apelidada de vários nomes como, por exemplo, bit para a camada física, quadro para a camada de enlace e pacote para a camada de rede;
3. **Roteamento:** a camada de rede tem como função fornecer serviços para direcionar os pacotes a um dispositivo destino para uma mesma ou outra rede de uma melhor forma possível. Para que esse pacote seja encaminhado ao transporte de outra rede, deve ser processado por um dispositivo que faz roteamento – roteador. A função do roteador é fazer a escolha dos melhores caminhos para que os pacotes sejam direcionados aos hosts de destino. Os pacotes enviados podem atravessar vários dispositivos intermediários de rede antes de alcançar o destino final. Cada rota que um pacote faz para chegar ao host destino é chamada de salto – hops;
4. **Desencapsulamento:** quando determinado pacote chega à camada de rede do equipamento destino, tal dispositivo examina o cabeçalho IP do pacote recebido. Se o endereço IP destino incluído no cabeçalho corresponder ao seu próprio endereço IP, o cabeçalho IP será removido do pacote com a finalidade de dar camadas mais internas desse invólucro. Tal processo de remover os cabeçalhos das camadas inferiores é conhecido como desencapsulamento de dados. Como exemplo, considere que depois que o pacote – camada 3 – for desencapsulado pela camada de rede, a PDU resultante da camada 4 – segmentos – é passada à camada de transporte em um serviço apropriado.

A camada de rede – camada 3 do modelo OSI – especifica uma estrutura para que os pacotes possam ser processados a fim de serem transmitidos corretamente na rede por meio de um determinado endereço de destino. Já a camada de transporte – camada 4 do modelo OSI – é encarregada de gerenciar como tal dado é transportado, verificando, assim, características como controle de fluxo e correção de erros de eventuais segmentos perdidos.

Outros Protocolos de Camada de Rede

Existe grande gama de protocolos de camada de rede como, por exemplo, o IPX da Novell etc. Como tratamos aqui de tecnologias relacionadas à internet, focaremos nos seguintes protocolos que são, comumente, assim implementados:

- Internet Protocol versão 4 (IPv4);
- Internet Protocol versão 6 (IPv6).



Figura 1 – Protocolos da camada de rede

Fonte: Cisco Netacad, 2017

Outros protocolos antigos da camada de rede herdados que não são amplamente utilizados hoje em dia incluem:

- AppleTalk, da Apple Computer;
- Internetwork Packet Exchange (IPX), da Novell;
- Connectionless Network Service (CLNS/DECNet).

Características do Protocolo IP

IP é o serviço da camada de rede implementado pelo conjunto de protocolos da família TCP/IP. Foi desenvolvido como um protocolo com baixa sobrecarga. Fornece somente as funções necessárias para enviar um pacote de uma origem a um destino por um sistema de redes interconectadas. O protocolo não foi elaborado para rastrear e gerenciar o fluxo dos pacotes. Essas funções, se necessárias, são realizadas por outros protocolos em outras camadas (CISCO NETACAD, 2017).

Ademais, as características básicas do IP são as seguintes:

- **Sem orientação a conexão:** nenhuma conexão com o destino é estabelecida antes de encaminhar os pacotes de dados;

- **Melhor esforço – não confiável:** a entrega do pacote não é garantida;
- **Independente de meio físico:** a operação é independente do meio físico que transporta os dados.

Sem Orientação a Conexão

A principal função da camada de rede é transportar os pacotes de dados entre os dispositivos de forma menos sobrecarregada possível. Nesse caso, a camada de rede não sabe o que é encapsulado em seu campo de dados – payload. O protocolo IP também é sem orientação a conexão, significando que nenhuma conexão fim a fim dedicada é criada antes que os dados sejam devidamente enviados. Um exemplo de comunicação sem orientação a conexão seria enviar uma carta a alguém sem a necessidade de notificação ao destinatário com antecedência, que é a forma clássica do envio de uma carta.

Como um protocolo sem orientação a conexão, o IP não exige nenhuma troca inicial de informações de controle para estabelecer uma conexão fim a fim antes que os pacotes sejam encaminhados para um destino. Não requer também campos adicionais no cabeçalho da Unidade de Dados do Protocolo (PDU) para que mantenha uma conexão estabelecida. No entanto, sem uma conexão fim a fim previamente estabelecida, os remetentes não sabem se os dispositivos destino estão presentes e funcionais ao encaminharem pacotes, não estão cientes se o destino recebe o pacote, ou se os dispositivos destino podem acessar e ler o pacote. (CISCO NETACAD, 2017)

Entrega de Melhor Esforço

O IP também é considerado um protocolo de melhor esforço de entrega, ou seja, não confiável. Isso não significa que o IP é um protocolo ruim e que as vezes funcione – e outras vezes não. O significado de não confiável é simplesmente devido ao IP não possuir capacidade de gerenciamento e recuperação de pacotes que não foram entregues ou foram corrompidos. Isso ocorre porque, embora os pacotes IP sejam enviados com informações sobre o local de entrega, não contêm nenhuma informação que pode ser processada para relatar ao remetente se a entrega foi bem-sucedida. Dito de outra forma, não há dados de sincronização incluídos no cabeçalho do pacote para controlar a ordem da entrega.

Não há também confirmações de entrega de pacotes com IP ou dados de controle de erros para rastrear os pacotes que foram entregues. Assim, os pacotes podem chegar ao destino corrompidos, fora de sequência, ou até mesmo não chegarem. Com base nas informações fornecidas no cabeçalho do IP, não há recursos de retransmissão de pacotes se erros como esses ocorrerem. (CISCO NETACAD, 2017)

Caso os pacotes em uma transmissão sejam perdidos ou cheguem fora de ordem, não será o protocolo IP que fará eventuais correções – e sim um protocolo de camada superior como, por exemplo, o protocolo de transporte TCP. Isso faz com

que o IP possa funcionar com grande eficiência, velocidade e baixa sobrecarga, por conseguir baixo consumo de largura de banda. No conjunto de protocolos da família TCP/IP, a camada de transporte pode utilizar os protocolos TCP ou UDP com base nas necessidades de confiabilidade e comunicação. Deixar o processo de decisão de confiabilidade para a camada de transporte faz com que o endereço IP seja mais adaptável e que possa ser utilizado em diferentes tipos de comunicação.

Já os protocolos orientados à conexão exigem que dados de controle sejam trocados para estabelecer a conexão antes que a mesma seja formada – como, por exemplo, TCP. Para que possa manter informações sobre a conectividade realizada, requer campos adicionais de controle no cabeçalho da respectiva PDU.

Independência de Meio Físico

O IP opera independentemente do meio físico que transporta os dados nas camadas inferiores e, por este motivo, não é sobrecarregado por tais características. Qualquer pacote IP pode ser carregado por meio de várias formas de conexão física como, por exemplo, pares metálicos, fibras ópticas e/ou redes sem fio através de radiofrequência e outros modos de transmissão.

Para que isso possa ocorrer sem problemas é necessário que a camada de enlace de dados prepare as informações para que possam ser enviadas para os meios físicos utilizados na rede.

Há, no entanto, uma característica de grande importância dos meios físicos que a camada de rede considera: o tamanho máximo da PDU que cada meio físico consegue transportar é chamada de Unidade Máxima de Transmissão (MTU). Parte das comunicações de controle entre a camada de enlace de dados e a camada de rede é o estabelecimento de um tamanho máximo ao pacote. A camada de enlace de dados passa o valor da MTU para a camada de rede, esta que determina quão grandes os pacotes devem ser.

Em alguns casos, um dispositivo intermediário, geralmente um roteador, deve dividir o pacote ao encaminhá-lo de um meio físico para um meio físico com uma MTU menor. Tal processo é chamado de fragmentação do pacote ou apenas fragmentação e, como dito, é realizado por cada dispositivo intermediário de rede até o destino final. (CISCO NETACAD, 2017)

Encapsulamento IPv4

A transmissão IP empacota ou encapsula o segmento da camada de transporte dentro do campo de dados da camada de rede, adicionando um cabeçalho IP, no qual são identificados os endereços origem e destino que são utilizados pelos dispositivos intermediários para que o dado seja entregue ao destinatário corretamente. O cabeçalho IP permanece íntegro, da mesma forma que o pacote deixa a camada de rede do dispositivo origem até a sua chegada à camada de rede do dispositivo destino.

O processo de encapsulamento de dados possibilita que os serviços nas diferentes camadas se desenvolvam e escalem sem que possam afetar outras camadas de rede. Significa que os segmentos da camada de transporte podem ser imediatamente empacotados pelo IPv4, IPv6 ou por qualquer outro novo protocolo que possa ser desenvolvido em um futuro próximo.

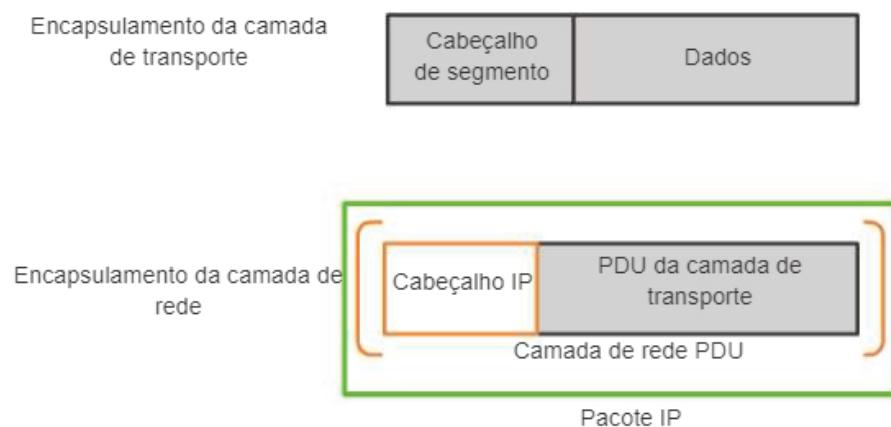


Figura 2 – Encapsulamento IP

Fonte: Cisco Netacad, 2017

Os dispositivos de roteamento podem implementar esses diferentes protocolos de camada de rede para que possam operar simultaneamente em uma rede entre os mesmos dispositivos ou entre dispositivos diferentes. O processo de roteamento realizado por esses dispositivos intermediários como, por exemplo, o roteador, considera somente o conteúdo do cabeçalho do pacote que encapsula o segmento e os dados por consequência.

Cabeçalho do IPv4

O IPv4 é utilizado desde 1983, quando foi implantado na *Advanced Research Projects Agency Network* (Apanet), que foi a precursora da internet, esta que é baseada, principalmente, no protocolo IPv4, que até hoje é o protocolo de camada de rede mais amplamente utilizado.

Ademais, um pacote IPv4 possui duas partes:

- *Cabeçalho IP*: identifica as características do pacote a ser transmitido;
- *Payload*: contém informações de segmento da camada 4 e os dados reais encapsulados em outras camadas.

Um cabeçalho de pacote IPv4 consiste nos campos que contêm informações muito importantes sobre o pacote e que serão utilizados para que o dado seja entregue corretamente em seu destino. Vejamos os campos do IPv4 e suas respectivas características:

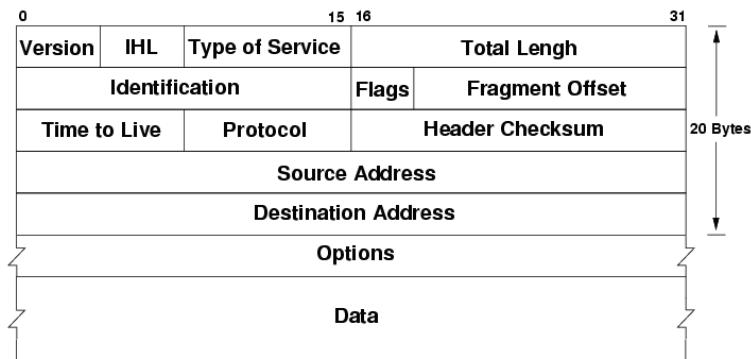


Figura 3 – Cabeçalho IPv4

Fonte: Wikimedia Commons

Note que os campos do cabeçalho IPv4 incluem:

- **Versão:** contém um valor binário de 4 bits que identifica a versão do pacote IP. Nos pacotes IPv4, esse campo é sempre definido como 0100;
- **Serviços Diferenciados (DS):** anteriormente chamado de campo Tipo de Serviço (ToS), o campo DS é de 8 bits e usado para determinar a prioridade de cada pacote. Os primeiros 6 bits identificam o valor do Ponto de Códigos de Serviços Diferenciados (DSCP), sendo utilizado por um mecanismo de Qualidade de Serviço (QoS) que tem como função priorizar o tráfego na rede. Os últimos 2 bits identificam o Valor de Notificação Explícito (ECN) que pode ser usado para evitar pacotes descartados durante períodos de congestionamento de rede;
- **Time-to-live (TTL):** contém um valor binário de 8 bits que é usado para limitar a vida de um pacote transmitido. É especificado em segundos, mas comumente conhecido como contagem de saltos, ou seja, por quantos dispositivos intermediários o pacote passou. O remetente do pacote define o valor inicial do TTL e diminui em um a cada vez que o pacote for processado – salto – por um roteador. Se o campo TTL diminuir ao número zero, o roteador descartará o pacote e enviará uma mensagem de Protocolo de Controle de Mensagens de Internet (ICMP) ao endereço IP origem, informando que o destino não foi devidamente alcançado;
- **Protocolo:** o valor binário de 8 bits indica o tipo de payload de dados que o pacote carrega, permitindo que a camada de rede passe os dados para o protocolo apropriado das camadas superiores. Os valores comuns incluem ICMP (1), TCP (6) e UDP (17);
- **Endereço IP origem:** contém um valor binário de 32 bits que representa o endereço IP origem do pacote;
- **Endereço IP destino:** contém um valor binário de 32 bits que representa o endereço IP destino do pacote.

Certamente, os dois campos que são consultados com mais frequência são os endereços IP de origem e destino. Esses campos identificam a origem do pacote e para onde será enviado. Normalmente, esses endereços não mudam ao serem transmitidos da origem ao destino. Os campos restantes são utilizados para identificar e validar o pacote ou para reordenar um pacote fragmentado pelos dispositivos intermediários.

Ademais, os campos usados para identificar e validar o pacote incluem:

- **Tamanho do Cabeçalho da Internet (IHL):** contém um valor binário de 4 bits que indica o número de palavras de 32 bits no cabeçalho. O valor do IHL varia devido aos campos *Opções* e *Padding*, de modo que o valor mínimo desse campo é 5 (isto é, $5 \times 32 = 160$ bits = 20 bytes) e o valor máximo é 15 (isto é, $15 \times 32 = 480$ bits = 60 bytes);
- **Comprimento total:** às vezes conhecido como comprimento do pacote, esse campo de 16 bits define o tamanho total do pacote – fragmento –, incluindo cabeçalho e dados, em bytes. O pacote de comprimento mínimo é 20 bytes (cabeçalho de 20 bytes + dados de 0 bytes) e o máximo é 65.535 bytes;
- **Checksum do cabeçalho:** o campo de 16 bits é usado para verificar erros do cabeçalho IP. O checksum do cabeçalho é recalculado e comparado ao valor no campo checksum. Se os valores não coincidem, o pacote é descartado.

Um roteador pode precisar fragmentar um pacote ao encaminhá-lo de um meio físico para outro que tenha uma MTU menor. Quando isso acontece, ocorre a fragmentação e o pacote IPv4 usa os seguintes campos para controlar os fragmentos:

- **Identificação:** este campo de 16 bits identifica exclusivamente o segmento de um pacote de IP original;
- **Flags:** este campo de 3 bits identifica como o pacote é fragmentado. É usado com os campos *Deslocamento de fragmento* e *Identificação* para ajudar a reconstruir o fragmento dentro do pacote original;
- **Deslocamento de fragmento:** este campo de 13 bits identifica a ordem na qual o fragmento do pacote deve ser colocado na reconstrução do pacote original desfragmentado.

Limitações do IPv4

Desde o nascimento da internet e ao longo dos anos, o IPv4 foi atualizado para enfrentar novos desafios na rede; porém, mesmo com as alterações realizadas, o IPv4 ainda apresenta três problemas principais, vejamos:

1. **Esgotamento dos endereços IP:** o IPv4 tem um número limitado de endereços IP públicos exclusivos disponíveis em aproximadamente 4 bilhões. Conforme o crescimento da internet e a evolução de novas aplicações, serviços e dispositivos, esse número praticamente se esgotou e, por esse motivo, foram criadas novas alternativas técnicas para evitar que a rede ficasse sem endereços disponíveis como, por exemplo, as técnicas de subnets, VLSM, utilização do NAT e muitas outras alternativas;

2. **Expansão da tabela de roteamento de internet:** com o crescimento das redes, ampliou-se também a quantidade de rotas possíveis para encontrar os seus destinos, de modo que os roteadores passaram a incluir tais rotas em uma matriz chamada de tabela de roteamento, utilizada por esses dispositivos para escolher o melhor caminho. O crescimento dessas tabelas de rotas fez com que o roteador passasse a consumir muitos recursos de memória e CPU, podendo acarretar perdas de performance ou até mesmo incapacidade de armazenamento das rotas aprendidas pela rede;
3. **Falta de conectividade fim a fim:** um Network Address Translation (NAT) é uma tecnologia geralmente implementada nas redes IPv4 com o intuito de fornecer uma forma de vários dispositivos compartilharem um único endereço de IP público. Para isso, torna-se necessário que o administrador de rede utilize em seu mapeamento de rede local endereços reservados e não roteados na internet. Tal processo faz com que se obtenha economia de endereços IP públicos; porém, tal solução de NAT traz problemas para aplicações que necessitam de conectividade fim a fim como, por exemplo, jogos na rede.

Introdução ao IPv6

O crescimento maciço da internet fez com que rapidamente o IPv4 se esgotasse; por esse motivo, no início da década de 1990, a *Internet Engineering Task Force* (IETF) teve preocupação com os problemas apresentados pelo IPv4 e procurou um eventual substituto. Isso levou ao desenvolvimento do IP versão 6 (IPv6), que supera as limitações do IPv4 e traz, em sua arquitetura, melhorias com recursos mais avançados e que atendem às demandas atuais e previsíveis da rede como um todo.

As melhorias que o IPv6 fornece incluem:

- **Aumento do espaço de endereçamento:** os endereços IPv6 são baseados em um endereçamento hierárquico de 128 bits – ao contrário do IPv4, que possui 32 bits. Isso aumenta significativamente o número de endereços IP disponíveis e que podem ser utilizados tanto como endereços de significado local, como global;
- **Melhor tratamento de pacotes:** o cabeçalho IPv6 foi simplificado com quantidade menor de campos se comparado ao IPv4. Isso melhora o gerenciamento do pacote enviado pelos roteadores intermediários e também oferece melhor suporte e opções de escalabilidade e longevidade avançadas;
- **Elimina a necessidade de utilização do Network Address Translation (NAT):** com um número tão grande de endereços públicos do IPv6, o NAT não é mais uma aplicação necessária na rede. Empresas de grande e médio porte a um único cliente domiciliar, podem agora obter um único endereço de rede IPv6 válido na internet – endereço público. Isso evita muitos problemas associados à utilização do NAT em relação a aplicativos que exijam conectividade fim a fim como, por exemplo, jogos e propagação de aplicações de vídeo;

- **Segurança integrada:** originalmente, o IPv6 suporta recursos de autenticação e privacidade embutidos no mesmo protocolo, ou seja, não tem a necessidade da utilização de protocolos de segurança externos ao protocolo, como ocorrido no IPv4.

No caso do IPv4, possui um espaço de 32 bits de um endereço que pode fornecer aproximadamente 4.294.967.296 endereços exclusivos, dos quais apenas cerca de 3,7 bilhões podem ser atribuídos ao cliente, pois o sistema de endereçamento IPv4 separa os endereços em classes e reserva aqueles para serviços multicast, aplicações de teste e para outras utilizações.

O espaço de endereços IPv6 fornece um valor de 340 undecilhões, que é equivalente a como se cada cidadão nascido no planeta Terra tivesse, para si, um endereço de classe A exclusivo.

Encapsulamento IPv6

Sem sombra de dúvida, a mais importante melhoria do IPv6, se comparado ao IPv4, é a estrutura de cabeçalho simplificado, afinal, o cabeçalho:

- *IPv4* possui o tamanho de 20 octetos (até 60 bytes se o campo opções for usado) e 12 campos básicos de cabeçalho, sem incluir os campos *Opções* e *Padding*;
- *IPv6* possui o tamanho de 40 octetos (em grande parte devido ao comprimento dos endereços IPv6 origem e destino) e 8 campos de cabeçalho (3 campos básicos de cabeçalho IPv4 e 5 adicionais).

Como dito, no IPv6 alguns campos permaneceram os mesmos que no IPv4, enquanto outros campos de cabeçalho IPv4 não são usados e alguns campos possuem posições e nomes alterados, conforme mostrado na próxima Figura:

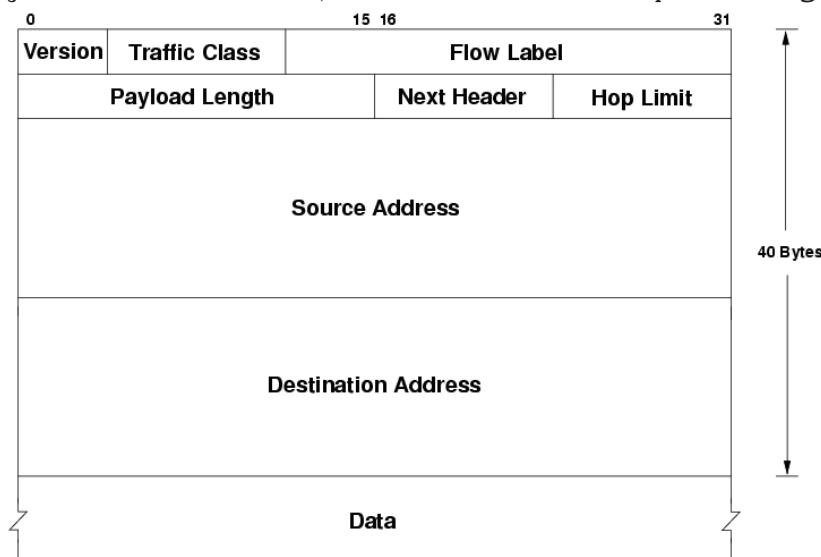


Figura 4 – Cabeçalho IPv6

Fonte: Wikimedia Commons

Um novo campo foi adicionado no IPv6 que não é utilizado no IPv4, chamado de *cabeçalho simplificado*, o qual oferece várias vantagens sobre o IPv4, vejamos:

- Maior eficiência de roteamento, melhorando o desempenho e a escalabilidade de encaminhamento de pacotes;
- Não é necessário o processamento de correção de erros – os conhecidos checksums;
- Mecanismos de cabeçalho simplificado e mais eficiente que as opções incluídas no cabeçalho do IPv4;
- Campo *Identificação de fluxo*, sem a necessidade de abrir o pacote interno de transporte para identificar os vários fluxos de tráfego.

Cabeçalho IPv6

Os campos no cabeçalho do pacote IPv6 incluem:

- **Versão:** contém um valor de 4 bits que identifica a versão do pacote IP. Em pacotes IPv6, tal campo é sempre definido como 0110;
- **Classe de tráfego:** este campo de 8 bits é equivalente ao campo *Serviços Diferenciados* (DS) do IPv4. Contém também um valor diferenciado de 6 bits do Differentiated Services Code Point (DSCP) usado para classificar pacotes e um Explicit Congestion Notification (ECN) de 2 bits empregado para o controle de congestionamento de tráfego;
- **Identificação de fluxo:** este campo de 20 bits fornece um serviço especial para aplicações em tempo real. Pode ser usado para informar roteadores e switches para manter o mesmo caminho ao fluxo de pacotes, de modo que estes não sejam reordenados;
- **Comprimento da payload:** este campo de 16 bits é equivalente ao campo *Comprimento Total no Cabeçalho IPv4*. Define o tamanho total do pacote – fragmento –, incluindo cabeçalho e extensões opcionais;
- **Próximo cabeçalho:** este campo de 8 bits é equivalente ao campo do protocolo IPv4. Exibe o tipo de payload de dados que o pacote está carregando, permitindo que a camada de rede passe os dados ao protocolo apropriado das camadas superiores. É usado também se houver cabeçalhos de extensão opcionais adicionados aos pacotes IPv6;
- **Limite de saltos:** este campo de 8 bits substitui o campo de TTL do IPv4. Tal valor é diminuído por 1 para cada roteador que encaminha o pacote. Quando o contador chega a 0, o pacote é descartado e uma mensagem ICMPv6 é encaminhada ao host de envio, indicando que o pacote não atingiu o seu destino;
- **Endereço origem:** este campo de 128 bits identifica o endereço IPv6 do host origem;
- **Endereço destino:** este campo de 128 bits identifica o endereço IPv6 do host destino.

Um pacote IPv6 pode conter também os novos Cabeçalhos de Extensão (EH), os quais têm por objetivo fornecer informações opcionais de camada de rede. Esses tipos de cabeçalhos são opcionais e, por este motivo, são incluídos entre o cabeçalho e payload do IPv6. Os EH são usados para várias funções como, por exemplo, a fragmentação, segurança, para dar suporte à mobilidade etc.

Endereçamento IP

Para que possamos entender a operação e o funcionamento dos dispositivos dentro de uma rede, precisamos conhecer os endereços e outros dados da forma como os dispositivos fazem, ou seja, utilizando a notação binária, esta que é uma representação das informações a serem transmitidas na rede usando apenas os valores 1 e 0. Logo, os dispositivos de rede se comunicam usando dados binários.

Os dados binários podem ser usados para representar muitas formas diferentes de dados. Por exemplo, quando você digita letras em um teclado, estas aparecem na tela da forma que se possa entender; no entanto, o computador converte cada letra em uma sequência de dígitos binários para armazenamento e transmissão. Assim, para converter tais letras, o computador usa a tabela de códigos Ascii ou EBCIDIC.

Cada host em uma rede deve ser identificado exclusivamente usando um endereço binário, no caso das redes IPv4, tal endereço é representado por uma sequência de 32 bits – entre repetições de 0 e 1. Na camada de rede do modelo OSI, os pacotes incluem a informação que identifica os endereços de origem e destino.

Para facilitar a compreensão, ao invés de o sistema apresentar a sequência de 32 bits, indica essa informação de endereçamento em um formato decimal separado por pontos – decimal pontuado. Essa separação é realizada em grupo de 8 bits (1 byte), que chamamos de octeto, sendo que um octeto possui um intervalo numérico entre 0 e 255.

Para que possamos melhor entender essa estrutura, torna-se necessário aprender as conversões de binário para decimal e vice-versa.

Máscaras de Rede

Além do endereço IP, a máscara de rede também é representada no formato decimal pontuado – razão da importância do conhecimento das conversões binárias e decimais.

Assim, é importante lembrar que o endereço IP é um endereço hierárquico composto por duas partes: uma que define a porção de rede e a outra parte, que define a porção de host; ou seja, o endereço IP tem a capacidade de identificar a rede que define um grupo de hosts e o host que define um componente específico dentro de uma rede.

Quando um dispositivo IP é devidamente configurado, uma máscara de rede ou sub-rede é atribuída em conjunto ao endereço IP. Da mesma forma que o endereço IP, a máscara de rede e sub-rede possui o formato decimal pontuado e o tamanho de 32 bits. A máscara de rede e sub-rede é comparada binariamente – bit a bit – ao endereço IP da esquerda à direita.

Os valores em números 1 na máscara de rede ou sub-rede representam a porção de rede; já os valores em números 0 representam a porção de host. Ou seja, se

tivermos uma máscara de rede no formato 255.255.255.0, então, representaremos o primeiro, segundo e terceiro octeto do endereço IP comparado à porção rede; já o último octeto será representado como a porção host desse endereço.

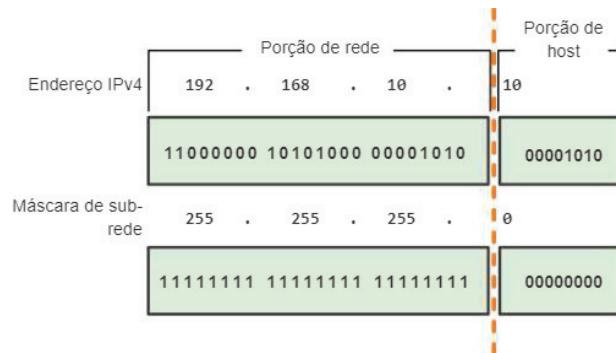


Figura 5 – Endereço IPv4 e máscara de rede

Fonte: Cisco Netacad, 2017

Tipos de Endereços IPv4

Existem três tipos de endereços quando utilizamos uma rede IPv4, tratam-se dos endereços de:

1. Rede;
2. Host; e
3. Broadcast.

Endereço de Rede

O endereço de rede tem como função identificar um conjunto de dispositivos – e não um dispositivo em comum. Para isso, a máscara de rede, sub-rede ou o comprimento do prefixo também pode ser utilizado para se referir ao endereço de rede – por exemplo, a rede 10.1.1.0 255.255.255.0 ou 10.1.1.0/24. Ademais, todos os dispositivos na rede 10.1.1.0 terão os mesmos bits de identificação da porção de rede.

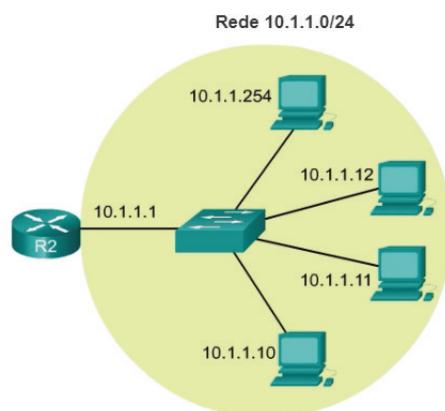


Figura 6 – Tipos de endereços IPv4

Fonte: Cisco Netacad, 2017

Endereço do Host

Todo host final de rede necessita de um endereço específico para se comunicar dentro da rede. Na rede IPv4, os valores entre os endereços de rede e de broadcast podem ser designados aos hosts finais, conhecidos também como endereços válidos em uma rede. Por exemplo, o endereço 10.1.1.200/24 identifica como rede 10.1.1.0/24 e o host 0.0.0.200 dentro dessa rede.

Endereço de Broadcast

O endereço IPv4 de broadcast é especial para cada rede, tendo como função permitir a comunicação para todos os dispositivos naquela rede. Para que os dados sejam enviados imediatamente a todos os dispositivos de uma única vez, um host pode disparar um único pacote, o qual é destinado ao endereço de broadcast da rede, de modo que cada host da rede deve receber esse pacote e processar o seu conteúdo utilizando recursos de memória e CPU dos dispositivos relacionados.

Ademais, utiliza o endereço mais alto dentro do intervalo de rede, ou seja, o endereço no qual os bits na porção host são todos de números 1. Todos os bits de números 1 em um octeto na forma binária são iguais ao número 255 na forma decimal, tal como é apresentado. Na rede 10.1.1.0/24, o quarto e último octeto é utilizado para uma porção de host, de modo que o endereço de broadcast seria 10.1.1.255.

Endereços Públicos e Privados do IPv4

Quando o endereçamento IPv4 foi devidamente implementado na internet, os endereços eram praticamente todos públicos, ou seja, endereços únicos na rede e entregues por meio dos provedores e órgãos de administração da internet. Com o aumento da utilização da rede e o eventual esgotamento desses endereços, surgiu a necessidade da criação de blocos de endereços privados, ou seja, que possuem apenas significado local em uma rede e não são roteados na internet, pois podem ser repetidos em outras redes locais.

Endereços Privados

Os endereços privativos são definidos pelo RFC 1918, conhecido como alocação de endereço de internet privada, e algumas vezes chamados de endereços RFC 1918, apenas. Os blocos de endereço que identificam o espaço privado são apresentados a seguir.

Foram extraídos e reservados com essa finalidade um bloco das classes A, B e C. Isso foi realizado porque, dependendo da classe que é utilizada, torna-se possível identificar uma quantidade limitada de hosts dentro de uma rede. Por exemplo, se usarmos uma rede de classe C usando uma máscara de rede padrão (/24), podemos ter, dentro dessa rede, cerca de 254 hosts ativos. Quando usamos endereços privados em um host dentro de uma rede local, estes não são conhecidos pela internet e, por esse motivo, necessitam da utilização de NAT para que possam “sair” do ambiente local e poderem ser identificados na rede mundial.

Os blocos de endereços particulares são:

- 10.0.0.0 a 10.255.255.255 (10.0.0.0/8);
- 172.16.0.0 a 172.31.255.255 (172.16.0.0/12);
- 192.168.0.0 a 192.168.255.255 (192.168.0.0/16).

No RFC 6598, o Iana também reservou outro grupo de endereços conhecidos como o espaço de endereço compartilhado. Semelhante ao espaço de endereço privado RFC 1918, os de espaço de endereço compartilhado não são roteáveis globalmente. Entretanto, esses endereços são destinados somente ao uso em redes de provedores de serviços. O bloco de endereços é compartilhado como 100.64.0.0/10 (CISCO NETACAD, 2017).

Endereços Públicos

A maioria dos endereços unicast do IPv4 é pública, desenvolvida para ser utilizada de forma que possa ser acessível por meio da rede, publicamente, ou seja, constituída por endereços válidos na internet. Além desses endereços, existem muitos outros que são atribuídos a outros fins especiais.

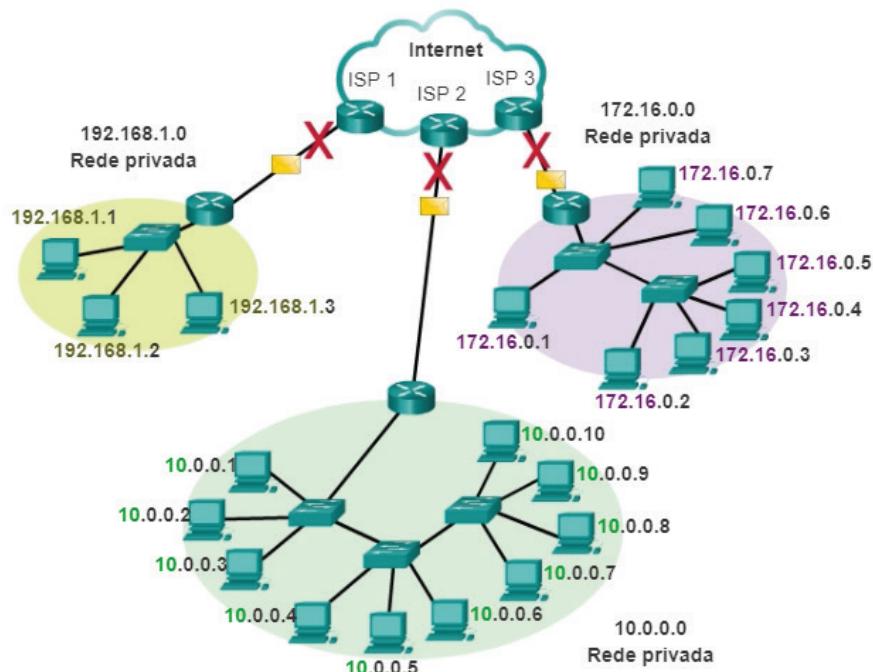


Figura 7 – Endereços públicos e privados do IPv4

Fonte: Cisco Netacad, 2017

Endereços ClassFull

No RFC1700, foram agrupados intervalos de endereços de unicast que definem tamanhos específicos da quantidade de hosts em uma rede através das classes A, B e C. Além dessas classes, possuem outras que definem endereços de multicast, definidos pelas classes D e E, consideradas classes experimentais.

Classe	Primeiro octeto	Parte da rede (N) e parte para hosts (H)	Máscara	Nº Redes / hosts por rede
A	1-127	N.H.H.H	255.0.0.0	126 redes 16,777,214 hosts por rede (2^{24-2})
B	128-191	N.N.H.H	255.255.0.0	16,384 redes (2^{14}) 65,534 hosts por rede (2^{16-2})
C	192-223	N.N.N.H	255.255.255.0	2,097,150 redes (2^{21}) 254 hosts por rede (2^{8-2})
D	224-239	Multicast	NA	NA
E	240-255	experimental	NA	NA

Figura 8 – Endereços ClassFull do IPv4

Fonte: Cisco Netacad, 2017

- **Blocos de classe A:** esta classe possui um bloco de endereços projetado para suportar redes grandiosas, com mais de 16 milhões de endereços reservados para dispositivos, que utilizavam um prefixo fixo /8 (ou 255.0.0.0), com o primeiro octeto para indicar os endereços na rede. Os três outros octetos à direita eram empregados para mapear dispositivos de rede. Ademais, todos os endereços de classe A possuem um bit mais significativo à esquerda do primeiro octeto reservado como zero. Ou seja, podemos afirmar que havia apenas 128 redes possíveis de classe A, 0.0.0.0/8 a 127.255.255.255/8, sendo que o 127.0.0.0, apesar de ser uma classe A, é também reservado à função de loopback;
- **Blocos de classe B:** esta classe possui um bloco de endereços projetado para suportar redes de tamanho moderado com, aproximadamente, 65.000 dispositivos. Tal endereço usava dois octetos da esquerda à direita para indicar o endereço de rede /16 (255.255.0.0), já os dois últimos octetos à direita especificavam os endereços de dispositivos. No caso de endereços de classe B, os dois bits mais significativos do octeto de alta ordem eram 10 (lê-se um e zero), restringindo o bloco de endereços de 128.0.0.0/16 para 191.255.255.255/16, podendo suportar, pelo menos, cerca de 16.000 redes;
- **Blocos de classe C:** esta classe possui um bloco de endereços projetado para suportar redes de tamanho pequeno com 254 dispositivos. Esses blocos de endereço usavam um prefixo /24 (255.255.255.0), ou seja, uma rede de classe C possuía apenas o último octeto para a criação de dispositivos e os três octetos de alta ordem eram usados para indicar o endereço da rede. Os blocos de endereço de classe C reservavam espaço de endereço usando um valor fixo de 110 (um, um, zero) para os três dígitos mais significativos do octeto de alta ordem, da esquerda à direita. Isso restringe tal bloco de endereçamento de classe C entre 192.0.0.0/24 para 223.255.255.255/24. Mesmo ocupando apenas 12,5% do total de espaço de endereços IPv4, podendo fornecer endereços para 2 milhões de redes, aproximadamente.

Endereçamento Classfull e Classless

Os endereços IPv4 nasceram com a alocação classfull – forma padrão –, porém, essa alocação possuía grande desperdício de endereços válidos. Tal sistema classfull foi abandonado no final da década de 1990, porém, até os dias atuais, quando vamos configurar um sistema operacional em um computador, o mesmo atribui baseando-se nos formatos default, assumindo, assim, os prefixes padronizados.

O sistema em utilização nos dias atuais é conhecido como o endereçamento sem classe, ou em inglês *Classless Inter-Domain Routing* (CIDR), fazendo com que os provedores pudessem definir os prefixos de rede em função da quantidade de dispositivos que uma rede pudesse suportar, economizando endereços de uma forma muito mais inteligente se comparado ao método classfull, que desperdiçava grande quantidade de endereços.

O IETF sabia, naquela época, que o CIDR era apenas uma solução temporária e que um novo protocolo de rede deveria ser desenvolvido para acomodar o crescimento escalável do número de usuários dentro da internet. Assim, em meados de 1994, a IETF iniciou os trabalhos para a criação de um sucessor ao IPv4, que acabou se tornando o IPv6.

Representação e Formato de Preferência do IPv6

Os endereços IPv6 possuem uma capacidade de endereçamento muito maior que o IPv4, ou seja, possuem 128 bits de comprimento e são escritos como uma sequência de valores hexadecimais ao invés de decimais, como o seu antecessor. O formato de apresentação é hexadecimal e cada 4 bits são representados por um único dígito hexadecimal. Os endereços IPv6 não diferenciam caracteres maiúsculos e minúsculos, ou seja, podem ser digitados das duas formas.

O formato de preferência para se armazenar um endereço IPv6 é x: x: x: x: x: x: x: x, com cada x representando quatro valores hexadecimais. No IPv4, esse conjunto de 8 bits é chamado de octeto – byte. Já no endereço IPv6, um hextet é o termo não oficial utilizado para referenciar um segmento de 16 bits ou de tamanho composto de quatro valores hexadecimais. O formato de preferência significa que o endereço IPv6 é armazenado usando todos os 32 dígitos hexadecimais do endereço, sendo que não constitui necessariamente que tal método seja o ideal para representar o endereço IPv6 – veremos adiante que existem outras formas de representar o IPv6 (algumas mais compactas).

Formas de Compactação e Representação do IPv6

Como já observamos em outros parágrafos, o endereço IPv6 é composto de 128 bits e representado no formato hexadecimal, por meio dos hextet. Essa forma padrão pode se tornar estressante ou dificultosa ao administrador de rede, pois o endereço se torna muito grande. Assim, foram criados modos de compactação para que os endereços IPv6 possam ser representados de uma forma mais fácil.

A primeira regra utilizada para reduzir a notação clássica dos endereços IPv6 é que os zeros à esquerda de um endereço possam ser omitidos, por exemplo:

- 01BA pode ser representado como 1BA;
- 08F0 pode ser representado como 8F0;

- $0C00$ pode ser representado como $C00$;
- $00CD$ pode ser representado como CD .

Como observado, essa regra omite apenas os zeros à esquerda, enquanto que os à direita não são ignorados. Para evitar ambiguidades em tais valores, o hextet ABC poderia ser $0ABC$ ou $ABC0$.

Preferência de	2001: 0DB8:0000:1111:0000:0000:0000:0200
Nenhum 0 à esquerda	2001: DB8: 0:1111: 0: 0: 0: 200

Figura 9 – Primeira regra

Fonte: Cisco Netacad, 2017

A segunda regra de redução para a notação dos endereços IPv6 é a utilização dos dois pontos, ou pontos em dobro :: que podem substituir uma única sequência contígua de um ou mais segmentos de 16 bits – *hextets* – que possuem zeros como valores.

Os dois pontos em dobro :: podem ser utilizados apenas uma vez dentro de um endereço, por exemplo: o endereço 2001:0000:0000:0000:0000:0000:0000:0001, ao utilizar as regras apresentadas, ficará da seguinte forma: 2001::1. Vejamos outro exemplo da utilização das regras de compactação:

Preferência de	2001: 0DB8:0000:1111:0000:0000:0000:0200
Nenhum 0 à esquerda	2001: DB8: 0:1111: 0: 0: 0: 200
Compactado	2001:DB8:0:1111::200

Figura 10 – Primeira e segunda regras

Fonte: Cisco Netacad, 2017

Tipos de Endereços IPv6

Há três tipos possíveis de mensagens no IPv6:

1. **Unicast:** pode identificar de uma forma exclusiva uma interface em um host rede habilitado com IPv6;
2. **Multicast:** é utilizado para enviar um único pacote IPv6 para vários hosts dentro de uma rede exclusiva;
3. **Anycast:** é utilizado quando um endereço é roteado ao host mais próximo que tem tal endereço.



Esses endereços não serão apresentados nesta Disciplina.



Importante!

Ao contrário do IPv4, o IPv6 não possui um endereço de broadcast. Nesse caso, o endereço de multicast fornece o mesmo resultado.

Endereços Unicast do IPv6

Certamente, os endereços unicast do IPv6 são os mais importantes e utilizados nesse tipo de rede, pois identificam, de forma exclusiva, a interface de um host habilitado com IPv6. Muito parecido com o IPv4, o endereço IPv6 origem deve ser unicast, enquanto os endereços destino podem ser unicast ou multicast.

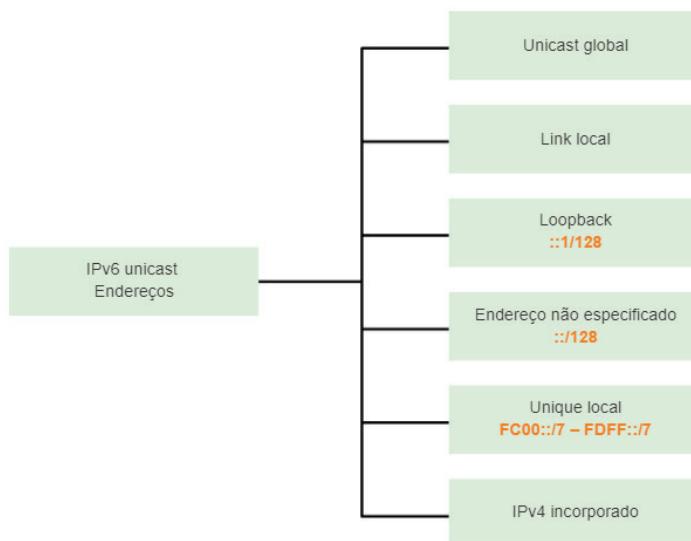


Figura 11 – Endereços unicast IPv6

Fonte: Cisco Netacad, 2017

Há seis tipos de endereços unicast no IPv6:

1. **Unicast global address:** é semelhante a um endereço IPv4 público, que são os endereços válidos na internet, ou seja, roteáveis da internet e globalmente únicos – não se pode ter dois endereços repetidos. Os endereços unicast globais do IPv6 podem ser configurados estaticamente – quando o operador manualmente registra o IPv6 em uma interface – ou também atribuídos de forma dinâmica – quando o operador configura um recurso automático para obter endereços. Em relação ao serviço DHCP do IPv6 – que é um recurso de obtenção dinâmica de endereços –, é um pouco diferente em comparação ao IPv4;
2. **Link local:** como o nome indica, tem significado local, sendo utilizado para a comunicação com outros dispositivos dentro de uma mesma rede. Com o IPv6, o termo link se refere a uma sub-rede, sendo exclusivo a uma única conexão, sendo que a exclusividade deve ser confirmada

apenas nessa conexão porque não são endereços roteáveis, ou seja, os roteadores não encaminham pacotes com um endereço origem ou destino de uma conexão local;

3. **Loopback:** é empregado por um dispositivo de rede para enviar um pacote para o mesmo com o intuito de testar a conectividade, de modo que não pode ser atribuído a uma interface física. Muito parecido com um endereço de loopback IPv4, é possível fazer ping em um endereço de loopback IPv6 para testar a conectividade do TCP/IP em um dispositivo local. O endereço de loopback IPv6 é all-0s, com exceção do último bit, razão pela qual podemos representá-lo como ::1/128 ou, de forma compactada, apenas como ::1;
4. **Endereço não especificado:** não se trata de um endereço de all-0s representado em formato compactado como :: /128 ou apenas :: no formato compactado; por esse motivo, não pode ser atribuído a uma interface e também pode ser utilizado somente como um endereço origem em um pacote IPv6. Assim, será empregado como endereço origem quando o dispositivo ainda não possuir um endereço IPv6 permanente ou quando a origem do pacote for irrelevante ao destino; (CISCO NETACAD, 2017)
5. **Unique local:** tais endereços do IPv6 possuem algumas similaridades aos reservados e privados do RFC 1918 do protocolo IPv4, afinal, são utilizados ao endereçamento local – dentro de um local ou entre um número limitado de dispositivos. Por esse motivo, tais endereços não devem ser roteáveis globalmente em redes IPv6, sendo reservados dentro do intervalo de FC00:: /7 a FDFF:: /7;
6. **IPv4 incorporado:** estes endereços de unicast são empregados em uma transição de redes IPv4 a IPv6, criando uma formatação e incorporação nessa nova rede. Ou seja, trata-se de uma técnica utilizada para traduzir um IPv4 que está no formato decimal ao IPv6, este no formato hexadecimal, por exemplo: o endereço IPv4 191.168.10.1 no IPv6 pode ser especificado como ::192:168:10:1, porém, a representação passa a ser hexadecimal.

Material Complementar

Indicações para saber mais sobre os assuntos abordados nesta Unidade:

Sites

Curso WEB: CISCO NETACAD

Curso WEB: CISCO NETACAD – Módulo de Introdução a Redes – Capítulo 6: Camada de Rede. [S.I.], 2017a.

<https://goo.gl/kSQz1K>

Curso WEB: CISCO NETACAD

Curso WEB: CISCO NETACAD – Módulo de Introdução a Redes – Capítulo 8: Endereçamento IP. [S.I.], 2017b.

<https://goo.gl/kSQz1K>

Livros

Redes de Computadores e a Internet

STALLINGS, W. e ROSS K. – Redes de Computadores e a Internet - 5^a Ed., Pearson, 2010.

Redes de Computadores

TANENBAUM, A. S. – Redes de Computadores – 5^a Ed., Pearson, 2011.

Referências

CISCO NETACAD – **Módulo de Introdução a Redes (CCNA1)** – 6^a Versão, Cisco Systems, 2017. (material on-line). Disponível em: <<https://www.netacad.com/pt-br>>

STALLINGS, W.; ROSS K. **Redes de computadores e a internet**. 5. ed. [S.l.]: Pearson, 2010.

TANENBAUM, A. S. **Redes de computadores**. 5. ed. [S.l.]: Pearson, 2011.



Cruzeiro do Sul
Educacional