NÃO PODE FALTAR

ETHERNET E IPV6

Renato Cividini Matthiesen

O QUE É IPV6?

O IPv6 é a versão mais atual do Protocolo de Internet, que veio suprir o IPv4, principalmente em relação na excassez de endereços IPs na internet.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

PRATICAR PARA APRENDER

Caro aluno, seja bem-vindo a esta segunda seção da unidade, na qual serão tratadas informações a respeito do padrão Ethernet, utilizado nas redes locais com grande intensidade, e sobre o protocolo IPv6, o qual, em conjunto com o IPv4, suportam o endereçamento e o roteamento das redes atuais. Considerando o padrão Ethernet, abordaremos também questões de cabeamento de redes.

As tecnologias de comunicação da camada de host de rede do conjunto de protocolos TCP/IP (*Transmission Control Protocol/Internet Protocol*) utilizam o padrão Ethernet para redes cabeadas na maioria dos sistemas de redes locais. Este padrão acompanha o cenário das redes locais desde a década de 1970 e vem sendo modificado, considerando novas tecnologias de materiais para cabeamento, porém ainda mantém a sua essência para transmissão e controle da onda portadora no canal de comunicação.

Já o protocolo IPv6 deverá se tornar o padrão de endereçamento para redes na internet, considerando que o IPv4 possui limitações de volume de endereços disponíveis, mesmo considerando as técnicas de NAT (*Network Address Translator*) e o CDIR (*Classless Inter-Domain Routing*), que levam ao endereçamento alternativo e suportam a imensidão de dispositivos parametrizados dentro de redes locais de computadores.

Após finalizarmos os estudos do projeto de topologia, protocolos de rede, segmentação para a divisão da rede em sub-redes e definição de endereçamento IP mediante uma política estabelecida com endereços e máscaras de sub-rede no projeto de redes para o espaço de coworking, daremos sequência ao estudo de redes.

Convidamos você a estudar estes dois conceitos e dar seguimento ao projeto de redes na empresa de coworking através de uma nova etapa do projeto para implantação de estrutura de cabeamento e dispositivos na rede local com a utilização do protocolo IEEE 802, ou seja, o padrão Ethernet, o que reflete a instalação física de dispositivos e a definição de domínios de colisão e *broadcast*.

Para que a empresa de coworking, para a qual sua consultoria de rede está desempenhando uma consultoria de projeto de redes, tenha documentado toda a estrutura física implantada, é necessário um relatório apresentando os equipamentos, cabos e domínios de colisão e *broadcast* que serão utilizados para operacionalizar a rede implantada.

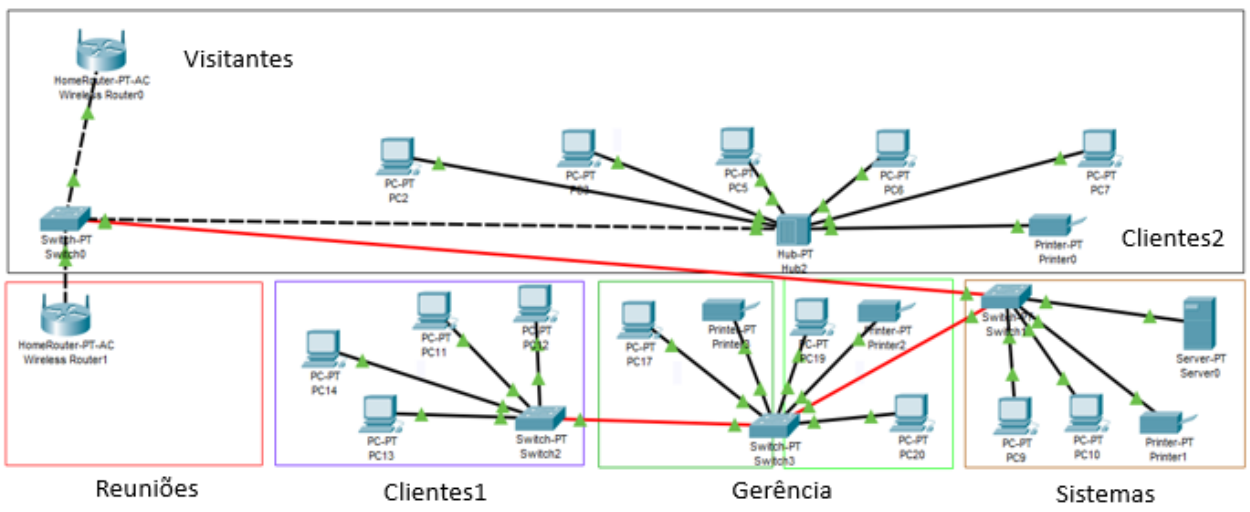
A compreensão sobre domínios de colisão e *broadcast* em uma rede Ethernet, a definição de equipamentos físicos e a definição de um novo padrão de endereçamento IPv6 devem melhorar ainda mais o projeto de rede que está em planejamento e seu desempenho.

Ver anotações

Em uma nova fase da consultoria para implantação de um sistema de redes de computadores em uma empresa de espaços compartilhados para trabalho (coworking), houve uma nova solicitação para que a equipe de desenvolvimento do projeto pudesse apresentar informações mais detalhadas sobre os dispositivos que fazem parte da rede, a fim de identificar os equipamentos disponíveis em cada um dos setores do ambiente (Sistemas, Gerência, Clientes1, Reuniões, Clientes2, Visitantes), conforme relatado na Figura 2.24, e também possam ser descritos os domínios de colisão e de *broadcast* da rede. Esta análise fará com que a rede tenha uma documentação mais completa e deverá definir os domínios da topologia implementada via padrão Ethernet, ou seja, para a parte da rede cabeada.

A análise a ser realizada deverá levar em consideração a segmentação da rede com os dispositivos comutadores, que tem a capacidade de definir domínios de colisão e *broadcast*. O relatório deve apresentar os equipamentos da rede, o número de domínios de colisão e o número de domínios de *broadcast*, de acordo com a topologia proposta a seguir:

Figura 2.24 | Topologia de rede para análise dos domínios de colisão e *broadcast*



Fonte: elaborada pelo autor.

Deverá ser gerado o **Relatório do projeto de redes: equipamentos de rede e análise de domínios de colisão e *broadcast*.**

Reconhecer como são realizadas as operações de acesso ao meio (cabos) e dispositivos de rede no padrão Ethernet é importante para que se possa desenvolver uma rede de computadores com os dispositivos de repetição e

gerenciamento de rede dentro de domínios de colisão e broadcast adequados. O endereçamento dentro do padrão IPv6 também contribui para o adequado controle de endereçamento e performance da rede.

As redes locais formam as estruturas chamadas de *Local Area Network* (LAN), que configuram os ambientes operacionais onde se localizam a maioria dos dispositivos conectados indiretamente à internet.

Em sua essência, a internet é descrita por Kurose e Ross (2013) como uma infraestrutura de redes que fornece serviços para aplicações distribuídas, interconectando centenas de milhões de dispositivos de computação ao redor do mundo. Estas aplicações distribuídas são operacionalizadas dentro de dispositivos dentro de redes local.

A seguir, conheceremos o padrão Ethernet como tecnologia utilizada na interconexão de redes locais, relacionada aos padrões e protocolos definidos na camada de host de rede da arquitetura TCP/IP. Se olharmos para o modelo OSI, estes protocolos atuam na camada de enlace de dados, que define e controla os dados transmitidos via dispositivos da camada física da rede.

CONCEITOS DE ETHERNET, DOMÍNIOS DE *BROADCAST* E DE COLISÃO

Muitos padrões de rede foram desenvolvidos nestes últimos anos, dentre eles, projetos para redes pessoais, redes locais e redes metropolitanas, padronizados como IEEE 802 (*Institute of Electrical and Electronic Engineers*, e 802 define um padrão de redes). Segundo Forouzan (2010), o IEEE subdividiu a camada de enlace do modelo OSI em duas subcamadas: **LLC (Logical Link Control) e MAC (Media Access Control)** e criou vários padrões de camada física para diversos protocolos LAN. As normas definidas pelo IEEE 802 trazem diversas tecnologias para implementação de redes locais, algumas com ampla utilização na atualidade, outras ainda em desuso. O Quadro 2.4 apresentado a seguir mostra os subgrupos que perfazem as normas IEEE 802.

Quadro 2.4 | Padrões de redes definidos pelo IEEE 802

Padrão	Definação/Padrão

Ver anotações 0

Padrão	Definação/Padrão
IEEE 802.1	Primitivas de interface e gerência
IEEE 802.2	LLC (*Logical Link Control*)
IEEE 802.3	CSMA/CD Ethernet
IEEE 802.4	Token Bus
IEEE 802.5	Token Ring
IEEE 802.6	Redes Metropolitanas
IEEE 802.7	Redes Metropolitanas
IEEE 802.8	Redes de Fibra Óptica
IEEE 802.10	Segurança em LAN
IEEE 802.11	CSMA/CA *Wireless*
IEEE 802.12	AnyLAN
IEEE 802.15	Rede PAN *Bluetooth*
IEEE 802.16	Rede Metropolitana *Wi-Max*

Fonte: adaptado de Tanenbaum (1997, p. 254).

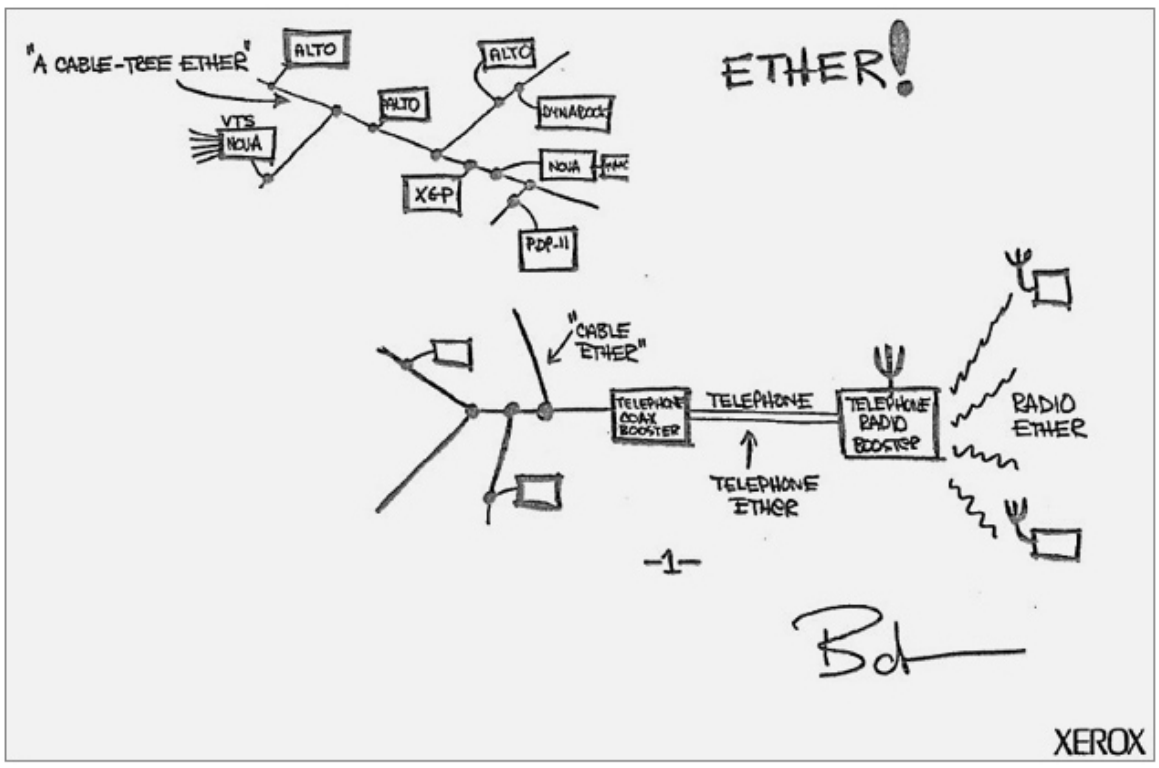
Conforme relata Comer (2016), a Ethernet é uma tecnologia LAN desenvolvida pela Xerox PARC e padronizada pela *Digital Equipment Corporation*, pela Intel e pela Xerox. O responsável pela tecnologia foi Robert Metcalfe, que trabalhava na Xerox na década de 1970 e que mais tarde fundou a 3Com. A tecnologia Ethernet foi padronizada pelo IEEE em 1985 e vem sendo utilizada por 35 anos como a principal tecnologia de rede local. Embora os dispositivos de hardware, cabeamento e meios usados com ela tenham mudado, o seu funcionamento continua praticamente o mesmo.

ASSIMILE

> Os padrões de rede que se mantiveram ativos e são atualmente utilizados nas redes locais e pessoais são o IEEE 802.3, padrão para redes locais cabeadas, definido como Ethernet; o IEEE 802.11, mais recente e padrão para redes locais sem fio (*wireless*), conhecido como Wi-Fi; e o IEEE 802.15, usado em redes pessoais sem fio e conhecido como *bluetooth*.

A seguir, faremos um estudo mais aprofundado sobre o padrão IEEE 802.3. O conceito de Ethernet é considerado por Tanenbaum (2011) como o padrão de redes locais mais utilizado no mundo. Este tipo de rede é classificado pelo autor como Ethernet clássica, que resolve problemas de acesso múltiplo ao meio compartilhado, e a Ethernet comutada, utilizada em dispositivos, como switches, para conectar os dispositivos da rede. A Ethernet comutada oferece velocidades e tecnologias físicas de conexão diferentes, mas utiliza o mesmo padrão de controle de colisões de onda portadora ao utilizar um meio compartilhado, ou seja, o cabo de rede. A Figura 2.25 apresenta um estudo original de uma rede Ethernet, em que um mesmo meio de comunicação é compartilhado por diversos dispositivos conectados na rede.

Figura 2.25 | Desenho do padrão Ethernet de Robert Metcalfe



Fonte: Computer History.

Em uma rede com padrão Ethernet, há dois assuntos importantes. O primeiro diz respeito ao meio de conexão, ou seja, ao cabo de rede. A segunda se refere à operação na utilização de um mesmo canal de comunicação e controle da

transmissão.

CABEAMENTO

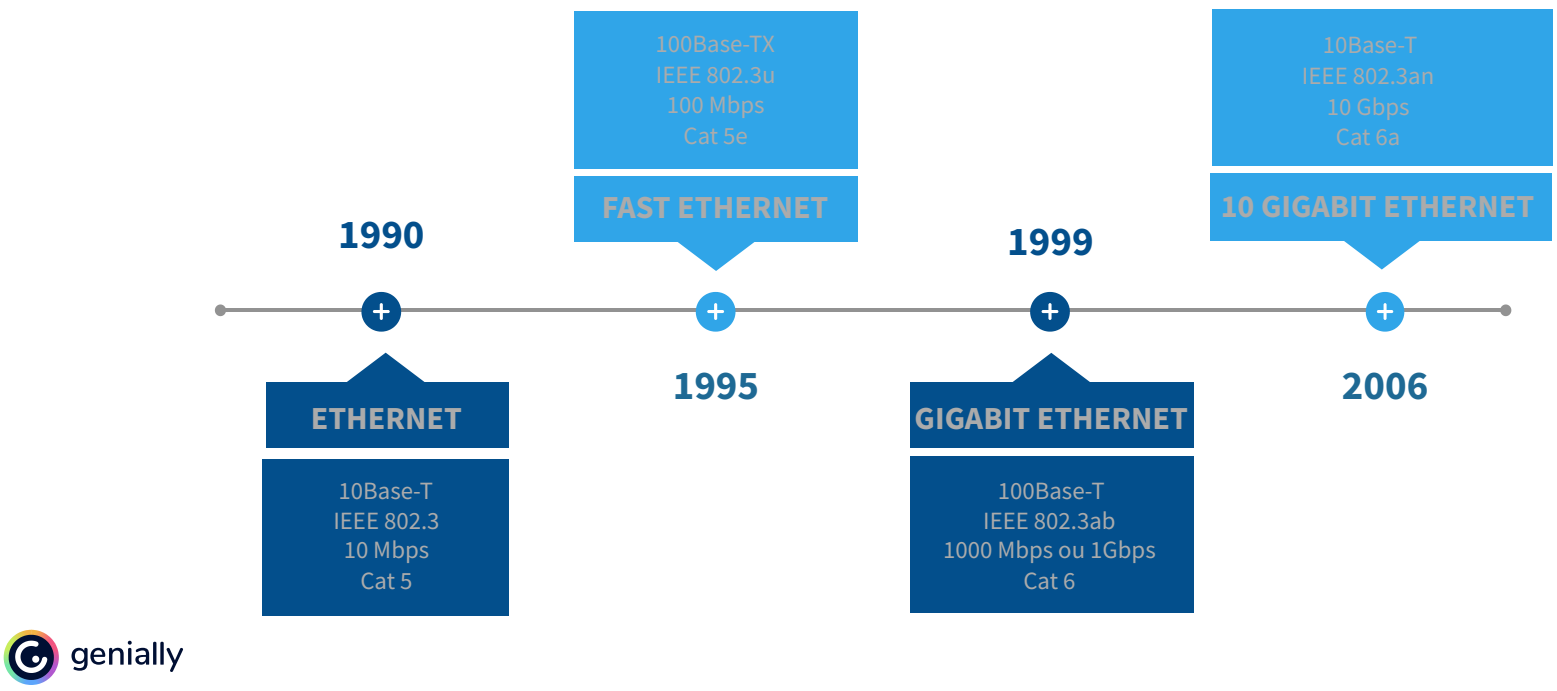
Os cabos e os conectores utilizados nesta tecnologia compõem o meio físico da comunicação. No passado, foram utilizados cabos coaxiais; depois, cabos metálicos de par trançado, úteis nos dias atuais junto aos cabos de fibra óptica.

Veja a seguir uma linha do tempo da evolução do padrão Ethernet.

Para visualizar o objeto, acesse seu material digital.

PADRÕES ETHERNET

Evolução do padrão Ethernet para cabos metálicos de par trançado



Comer (2016) resume que, da mesma forma que as versões anteriores das redes Ethernet, a primeira tecnologia de par trançado operava a 10 Mbit/s, denominada 10BaseT. Uma versão nomeada formalmente de 100BaseT que opera a 100 Mbit/s é conhecida comercialmente como Fast Ethernet. Uma terceira versão, chamada Gigabit Ethernet, ou Gig-E, opera a 1.000 Mbit/s, o que equivale a 1 Gbit/s. O hardware para as redes Ethernet de maior velocidade detecta automaticamente quando um dispositivo de baixa velocidade está conectado e reduz sua velocidade de acordo com ele para que a operação seja adequada ao dispositivo e à tecnologia conectada. O Quadro 2.5 mostra alguns padrões Ethernet.

Quadro 2.5 | Padrões Ethernet

Padrão	Cabo	Capacidade	Comprimento (m)
10base2	Coaxial fino	10 Mbps	185
10base5	Coaxial grosso	10 Mbps	500
10baseT	Par trançado CAT3	10 Mbps	100
100baseTX	Par trançado CAT5	100 Mbps	100
1000baseT	Par trançado CAT5/6	1000 Mbps	100
10GbaseT	Par trançado CAT 6	10 Gbps	55 ou 100
100BaseFX	Fibra óptica multimodo	100 Mbps	2000
1000BaseLX	Fibra óptica monomodo/multimodo	1000 Mbps	550
1000BaseSX	Fibra óptica multimodo	1000 Mbps	550
10GBaseSR	Fibra óptica multimodo	10 Gbps	550
10GBaseLX4	Fibra óptica multimodo	10 Gbps	550

Fonte: adaptado de Filippetti (2008, p. 55-57).

Ver anotações 0

ASSIMILE

As versões mais conhecidas do padrão IEEE 802.3 são:

- **IEEE 802.3u**: define os padrões da Fast Ethernet com velocidade de transmissão de 100 Mbps, representada pelos padrões 100BaseTX, 100BaseT e 100BaseFX.
- **IEEE 802.3z**: define os padrões da Gigabit Ethernet com utilização de cabo de fibra óptica e velocidade de 1000 Mbps, representada pelos padrões 1000BaseLX, 1000BaseSX e 1000BaseCX.
- **IEEE 802.3ab**: define os padrões da Gigabit Ethernet com utilização de cabo metálico e par trançado e velocidade de 1000 Mbps e padrão

1000Base-T.

- **IEEE 802.3ae**: define o padrão da 10 Gigabit Ethernet com velocidade de 10 Gbps com utilização de cabo de fibra óptica e utilizada para *backbones* e representada pelos padrões 10GBaseZR, 10GBaseSR, 10GBaseLRM e 10GBaseCX4.
- **IEEE 802.3an**: define o padrão da 10 Gigabit Ethernet com velocidade de 10 Gbps com utilização de cabo metálico de par trançado.

Mais recentemente, em 2012, houve a publicação do padrão IEEE 802.3-1012 com definições de eficiência energética, redes veiculares, data center e distribuição de conteúdo com velocidades de 40 a 100 Gbps.

O cabeamento metálico para redes Ethernet exige que se utilizem um padrão de pinagem, para que os pares de fios que compõem um cabo de par trançado realizem a transmissão de forma adequada. O Quadro 2.6 traz a sequência de pinagem (sequência de fios na ligação com o conector RJ 45) padronizada como TIA/EIA T568A. No quadro, o TX representa transmissão; RX, recepção; BI, comunicação bidirecional; D1-4, o caminho em que o fio está posicionado.

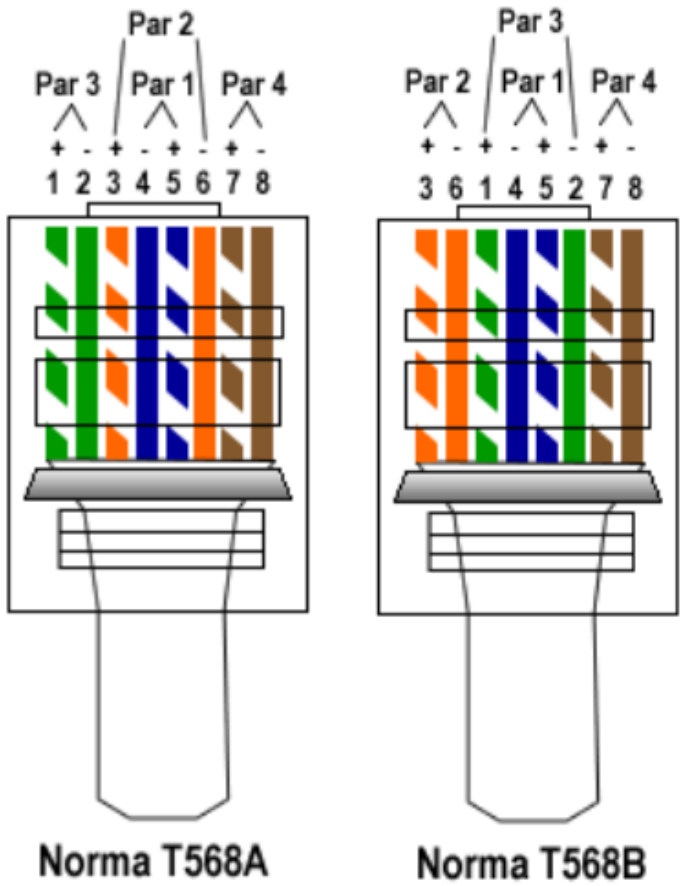
Quadro 2.6 | Padrão de operação de um cabo de par trançado

Pino	Cor do fio	Função
1	Branco-verde	TX D1+
2	Verde	TX D1-
3	Branco-laranja	RX D2+
4	Azul	BI D3+
5	Branco-azul	BI D3-
6	Laranja	RX DE-
7	Branco-marrom	BI D4+
8	Marrom	BI D4-

Fonte: adaptado de Comer (2016, p. 227).

De forma ilustrativa, a Figura 2.26 apresenta os padrões TIA/EIA T568A e T568B, que podem ser utilizados na montagem de um cabo de rede de par trançado junto ao seu conector RJ45.

Figura 2.26 | Padrões de conexão de cabos Ethernet TIA/EIA T568A (esquerda) e T568B (direita)



Par 1: + Azul-branco e – Azul

Par 2: + Laranja-branco e – Laranja

Par 3: + Verde-branco e – Verde

Par 4: + Marrom-branco e – Marrom

Fonte: Wikimedia Commons.

EXEMPLIFICANDO

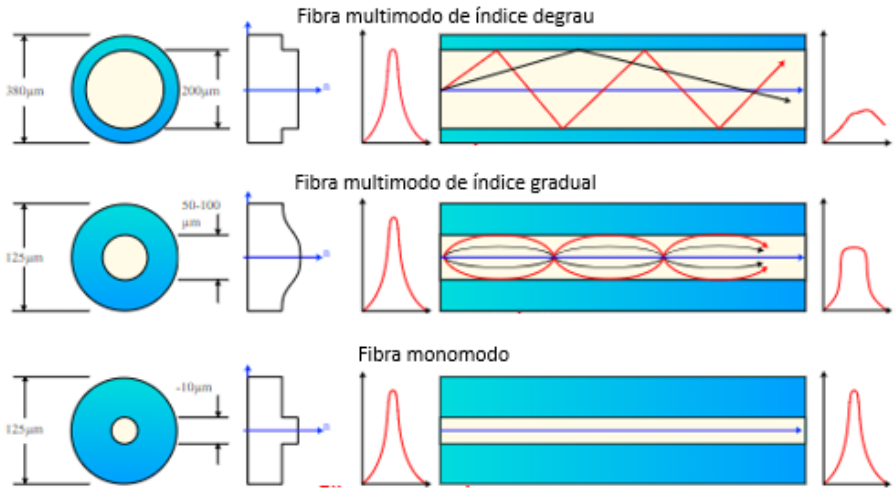
As redes Ethernet utilizam, aa maioria dos projetos, dois tipos de cabos para conexão física dos dispositivos de rede. Um deles é o cabo metálico de par trançado, e o outro é o cabo de fibra óptica. Ambos os tipos de cabos possuem especificações para cada categoria de rede Ethernet. Uma rede local normalmente utiliza um cabo de par trançado Cat6 que opera em velocidade de 1 Gbps, mas permite velocidades até 10 Gbps com comprimentos de enlace até 100 metros. Cabos Cat7 e Cat8 também são padrões utilizados em redes locais e oferecem velocidades maiores, porém com menores comprimentos de enlace. Os cabos de fibra óptica são

> utilizados normalmente para *backbones* (linhas principais de interligação de redes), que interligam *switches* e canais de comunicação com operadoras, mas também são utilizados para conexão local de dispositivos.

O cabeamento óptico nas redes Ethernet utiliza fibras ópticas em formato de cabos sempre em pares, sendo um fio utilizado para a transmissão de dados e outro para recepção.

Os cabos ópticos são classificados em cabos monomodo e multimodo. Os cabos monomodo, chamados de *Single Mode Fiber* (SMF), têm um maior desempenho e possuem espessura em torno de 10 mícron. Já os cabos multimodo, chamados de *Multiple Mode Fiber* (MMF), são mais grossos, com espessura de 50 a 62,5 mícron. Conforme apresenta Tanenbaum (2011), enquanto um cabo multimodo varia de 300 metros até 2.000 metros de comprimento, cabos monomodo podem chegar a 40.000 metros (ou 80.000, segundo alguns fabricantes) sem a utilização de repetidores. As redes locais utilizam as fibras multimodo em sua implementação. Importante salientar que estes padrões e tecnologias estão em constante evolução. A Figura 2.27 apresenta o comportamento do sinal luminoso dentro da fibra óptica em suas janelas de operação em fibras monomodo e multimodo.

Figura 2.27 | Cabos de fibra óptica monomodo e multimodo



Fonte: adaptada de Wikimedia Commons.

OPERAÇÃO, VELOCIDADES E COMUTAÇÃO

Caro aluno, conhecemos a tecnologia Ethernet e um pouco mais sobre o cabeamento metálico de par trançado. Agora, verificaremos sobre os meios de transmissão dentro desta tecnologia.

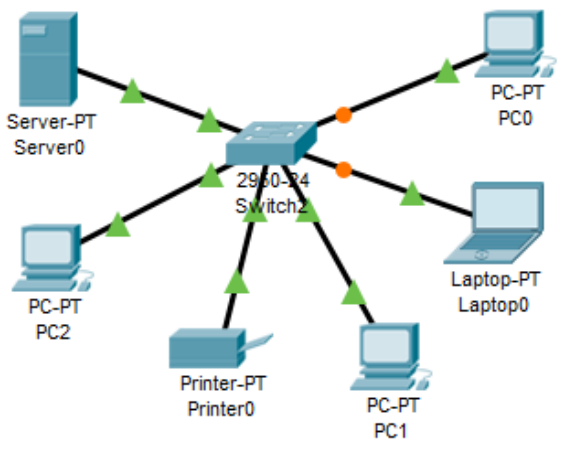
O protocolo Ethernet é um padrão de comunicação que compartilha um mesmo meio de comunicação (cabo) com todos os dispositivos de rede (*hosts*). Para transmissão, um dispositivo verifica a disponibilidade do canal e transmite. Caso haja outro dispositivo também transmitindo, ocorrerá uma colisão, a transmissão é interrompida e refeita em um tempo aleatório controlada pelo algoritmo do protocolo de acesso múltiplo ao meio compartilhado. Este protocolo é o CSMA (*Carrier Sense Multiple Access*), o qual, conforme Forouzan (2010), faz a transmissão em um meio compartilhado via três algoritmos:

1. CSMA não persistente: se o meio de transmissão estiver ocupado, o dispositivo aguarda um tempo para retransmitir.
2. CSMA 1 persistente: o dispositivo verifica a rede até que o meio fique livre para transmissão.
3. CSMA p-persistente: o algoritmo calcula a probabilidade de colisão e, quando livre e com baixa possibilidade de colisão, realiza a transmissão.

O CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) utilizado no padrão Ethernet tem um mecanismo de detecção de colisão, no qual os dispositivos da rede verificam colisões e controlam a retransmissão dos dados no canal compartilhado.

De acordo com Filippetti (2008), o padrão Ethernet com o CSMA/CD utiliza uma topologia em estrela e define uma rede comutada por um elemento central chamado de *switch* (antes eram utilizados apenas hubs) ou roteadores. A apresentação de uma topologia de rede comutada no padrão Ethernet é apresentada na Figura 2.28 a seguir.

Figura 2.29 | Rede em topologia estrela com um comutador (*switch*)



Fonte: elaborada pelo autor.

Em uma rede Ethernet, podem ocorrer colisões de duas formas, sendo uma pelo domínio de colisão e outra pelo domínio de *broadcast*.

No domínio de colisão, os pacotes da rede têm a possibilidade de efetuar colisão uns com os outros, o que leva à degradação da performance da rede, pois faz com que muitas retransmissões sejam necessárias. Esta situação se agrava ainda mais quando há equipamentos de comutação (*hubs*) em formato de cascata, ou seja, interligados, formando uma topologia híbrida de estrela e árvore para expansão do número de dispositivos na rede.

Já no domínio de broadcast é possível determinar o limite que o pacote pode chegar utilizando-se um dispositivo comutador de rede local que operacionalize a comunicação com outro dispositivo sem que seja utilizado um roteador.

Os dispositivos comutadores possuem, desta forma, um importante papel para a performance de uma rede de computadores em domínios de colisão e *broadcast*. Estes dispositivos podem ser:

- ***Hub***: são dispositivos concentradores que fazem comutação em uma rede com a repetição das mensagens para todas as suas portas de conexão, formando um único domínio de colisão e *broadcast*. Estes dispositivos foram muito importantes no cenário das redes, mas encontram-se praticamente em desuso na implantação de novas redes pois, conforme Stallings (2016), estes equipamentos foram substituídos pelos switches de camada 2 e têm seu nome também atribuído de *switching hub* ou ponte de rede multiporta.
- ***Switch***: dispositivo capaz de formar um domínio de colisão em cada porta de comunicação e formar um único domínio de *broadcast*. Dispositivo fundamental na operação das redes de computadores na atualidade, os switches estão divididos em *switches* de camada 2 e *switches* de camada 3. Como sustenta Stallings (2016), um *switch* de camada 2 tem maior desempenho e pode incorporar as funções de uma ponte, assim novas instalações tipicamente incluem *switches* de camada 2 com funcionalidades de ponte em vez de pontes. Estes *switches* de camada 2 são boas opções para utilização em redes, nas quais usuários utilizam 80% do tempo se comunicando com dispositivos no segmento local. Os *switches* de camada 3 são definidos por Stallings (2016) como um roteador baseado em hardware. Eles têm a função de

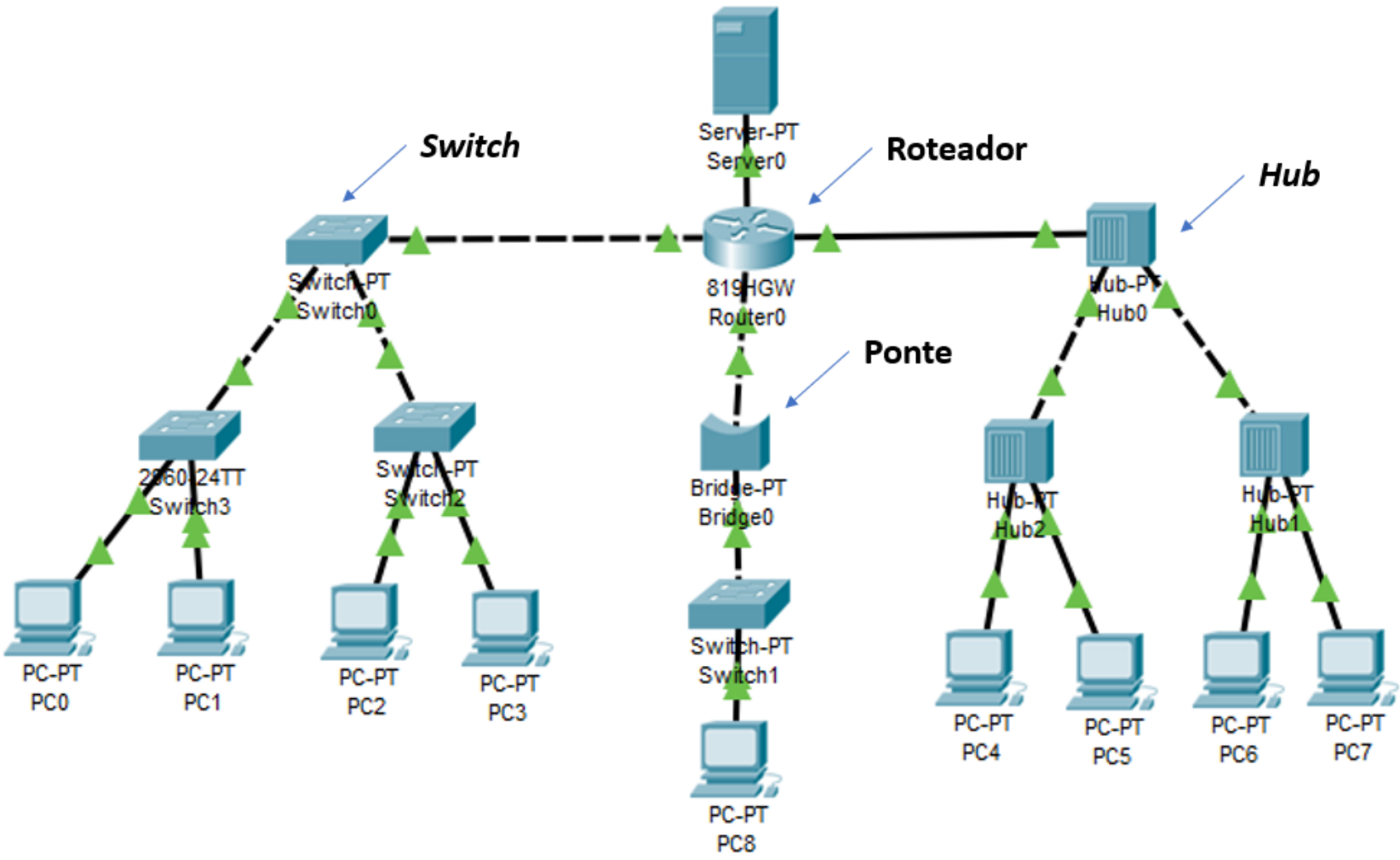
gerenciar melhor as redes, identificando os fluxos dos pacotes IP com a mesma origem e destino, segmentando em sub-redes e quebrando os domínios de *broadcast*. Importante salientar que apenas *switches* de camada 3 podem desempenhar a função de gerenciamento.

- ***Router***: ou roteador, é um dispositivo que opera na camada 3 (inter-rede) do conjunto de protocolos TCP/IP e quebram o domínio de *broadcast*, pois operacionalizam roteamento na rede. São dispositivos utilizados nas redes de computadores da atualidade.

- ***Bridge***: ou ponte, são dispositivos que podem separar domínios de colisão, porém não separam os domínios de *broadcast*. Estes dispositivos podem ainda ser sua implementação realizada por *switches*.

A Figura 2.29 traz um exemplo de uma rede um pouco mais complexa, na qual os dispositivos de rede são utilizados para implementar o modelo Ethernet para uma rede local com domínio de colisão. Verifique que o roteador separa os domínios de *broadcast* em três domínios. No domínio de colisão à direita do roteador, a topologia é conectada por hubs, formando um único domínio de colisão e *broadcast*. À esquerda do roteador, há dois domínios de colisão, formados pelos *switches*, e abaixo do roteador há um domínio de colisão formado por um único *switch*.

Figura 2.29 | Rede em topologia com domínio de colisão



Fonte: adaptada de Nunes (2017).

Assim finalizamos nosso estudo sobre operação de uma rede Ethernet, observando que esta tecnologia utiliza o método CSMA/CD para compartilhamento de um único canal de comunicação e dispositivos de rede, como *hubs*, *switches*, roteadores e pontes para definição de domínios de colisão e broadcast. Este planejamento faz com que uma rede tenha a performance adequada dentro das possibilidades de utilização de equipamentos de comutação.

SAIBA MAIS

O cabeamento utilizado dentro do padrão IEEE 802.3, ou seja, o padrão Ethernet, teve importantes evoluções tecnológicas nos últimos 50 anos. Comer (2016) relata que desde a versão original, na década de 1970, a Ethernet passou por várias alterações, sendo que a mais significativa foi no cabeamento. O cabo de rede utilizado no primeiro padrão Ethernet era chamado de *Thicknet*, ou cabo Ethernet grosso, passando pelos cabos *Thinnet*, chamados de cabo Ethernet, ou coaxial fino, pelos cabos de par trançado e hubs, utilizou diferentes tipos de conectores e chegou a padrões de cabos metálicos de par trançado mais atuais, que suportam redes Gigabit Ethernet.

> A leitura da Seção 15.7, Evolução da Ethernet e cabos *Thicknet*, do Capítulo 15, *Tecnologias de LAN com fio (Ethernet e 802.3)*, do livro *Redes de Computadores e internet*, de Comer (2016), é prazerosa e traz informações sobre a evolução histórica e aplicada na prática de cabos de rede no padrão Ethernet.

IPV6 (*INTERNET PROTOCOL VERSION 6*)

Conforme sustentam Kurose e Ross (2013), o projeto de endereçamento IPv6 teve início na década de 1990, mediante um aumento expressivo de número de computadores e dispositivos que se interconectavam às redes de computadores. Atualmente, o conceito de IoT (*Internet of Things*) corrobora com um aumento exponencial no número de sensores e dispositivos que estão sendo conectados à internet. Importante observar que o esgotamento do IPv4 ocorreu em 2014.

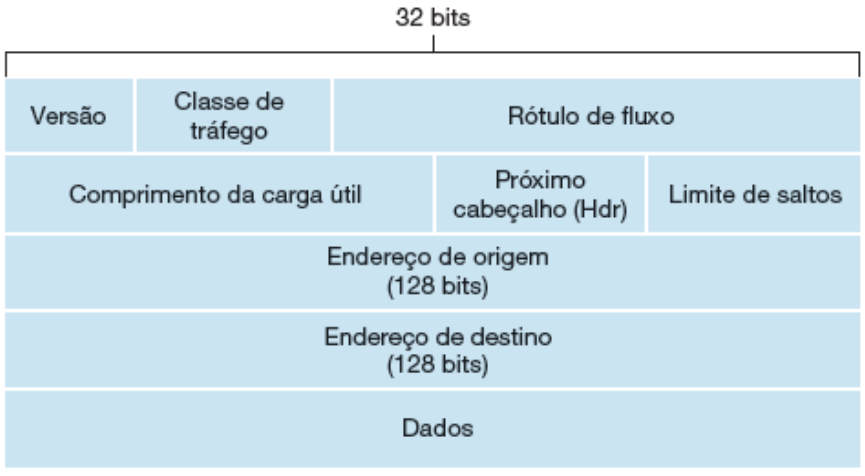
O projeto do IPv6 foi liderado pela IETF (*Internet Engineering Task Force*) e contou com a participação da LACNIC (*Latin American and Caribbean Internet Addresses Registry*), com um estudo e monitoramento a respeito do esgotamento de endereços IPv4 disponíveis no mundo.

Com a intenção de desenvolver um novo protocolo de endereçamento e roteamento de rede, o IPv6 veio para suprir algumas necessidades além das possibilidades do protocolo IPv4:

1. Resolver a escassez de endereços IPs na internet.
2. Simplificar o cabeçalho do endereço IP.
3. Deixar como opcional alguns campos de cabeçalho IP, para facilitar o roteamento de pacotes na rede.
4. Melhorar a segurança das transmissões, adicionando o IPSec (*Internet Protocol Secure*).

A Figura 2.30 apresenta o formato de um datagrama IPv6.

Figura 2.30 | Formato do datagrama IPv6



Fonte: Kurose e Ross (2013, p. 264).

É importante salientar que o datagrama IPv6 também pode ser composto por 64 bits, conforme sustenta IPv6.BR (2020).

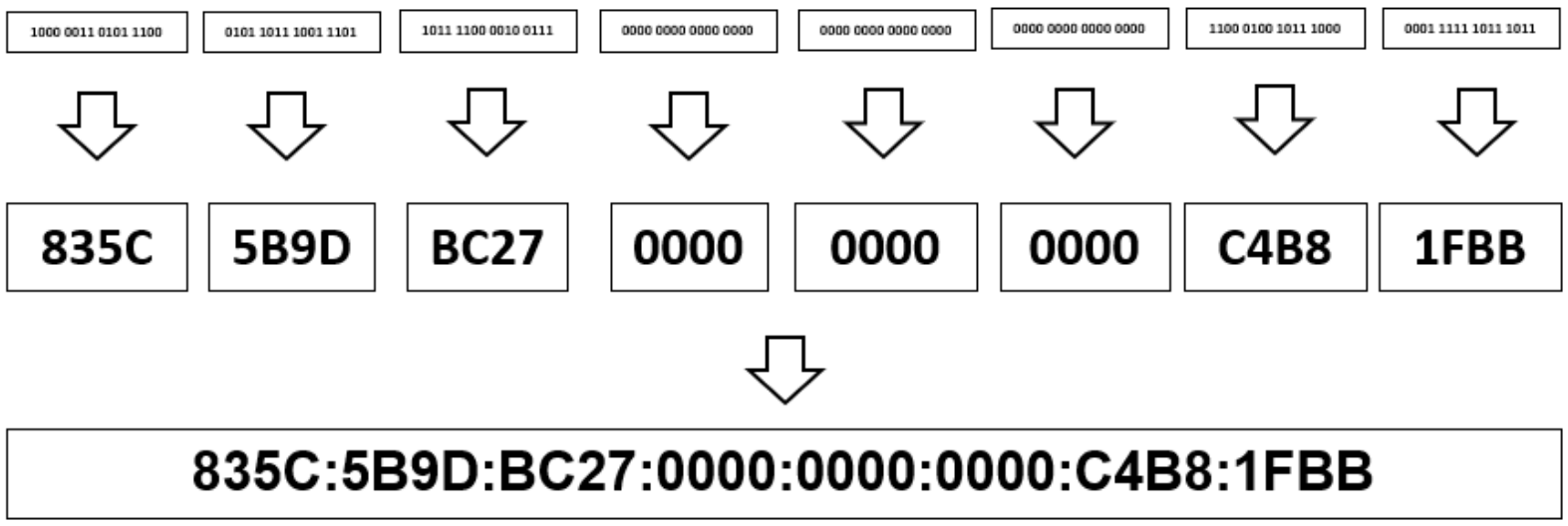
A seguir, é apresentada uma breve descrição dos campos do datagrama IPv6.

- **Versão**: (4 bits) versão do protocolo IP (4 ou 6).
- **Classe de tráfego**: (8 bits) campo para prioridade.
- **Rótulo de fluxo**: (20 bits) identifica o fluxo de datagramas.
- **Comprimento da carga útil**: (16 bits) tamanho total do pacote (datagrama).
- **Próximo cabeçalho**: (8 bits) identifica o protocolo ao qual o conteúdo será entregue (TCP ou UDP).
- **Limite de saltos**: (8 bits) limite de saltos em roteadores.
- **Endereço IP de origem**: (128 bits) endereço do remetente.
- **Endereço IP de destino**: (128 bits) endereço do receptor
- **Dados**: dados a serem transmitidos.

Comer (2015) sustenta que, da mesma forma que o IPv4, o IPv6 atribui um endereço exclusivo para cada conexão entre um computador e uma rede física. Um endereço IPv6 possui 128 bits, o que permite um total de 340 undecilhões de endereços (2^{128}), em um formato de oito grupos de quatro dígitos hexadecimais. Conforme apresenta Stallings (2016), a combinação de endereços longos e diversos por interface permite melhor eficiência de roteamento pelo IPv4. Ainda de acordo o mesmo autor, a notação para um endereço IPv6 usa oito números hexadecimais para representar os oito blocos de 16 bits no endereço de 128 bits, com os números separados por dois pontos (:). Exemplo:

835C:5B9D:BC27:0000:0000:0000:C4B8:1FBB. Este número realmente é muito grande e suficiente para que possamos endereçar os dispositivos das redes pessoais, locais, metropolitanas, globais e os dispositivos de IoT na internet. A Figura 2.31 apresenta a composição de um endereço IP de 128 bits.

Figura 2.31 | Formato do endereço IPv6

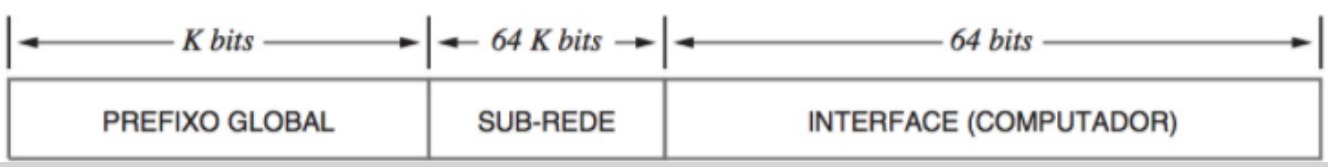


Fonte: elaborada pelo autor.

Um endereço IPv6 tem sua composição diferenciada de um endereço IPv4, apesar de ter uma mesma abordagem na atribuição aos *hosts*. Como nos endereços em notação CDIR (*Classless Inter-domain Routing*), a divisão entre parte da rede (prefixo) e parte do *host* (sulfixo) no endereço ocorre em limites flexíveis na utilização de seus bits. O endereço IPv6 possui três níveis de hierarquia, conforme sustenta Comer (2015). Um prefixo inicial é um valor único e global usado para roteamento na internet, atribuído a uma organização. A segunda parte do endereço identifica a sub-rede (ou seja, a própria rede) da organização. A terceira parte especifica o host de rede.

Um endereço IPv4 tem tamanho variável e definido por um ISP (*Internet Service Provider*), ou servidor de serviços de internet, em conformidade com a necessidades de volume de hosts de uma empresa cliente. A terceira parte do endereço tem tamanho fixo de 64 bits, formando um prefixo global de /64. A Figura 2.32 apresenta a estrutura de um endereço IPv6.

Figura 2.32 | Formato do endereço IPv6



Fonte: Comer (2015, p. 316).

Segundo Stallings (2016), o protocolo IPv6 permite a definição de três tipos de endereços: *unicast, anycast e multicast.*

- ***Unicast***: possui um identificador para uma única interface de rede, ou seja, para um único host, sendo que um pacote enviado para um endereço *unicast* é entregue para a interface identificada pelo endereço.
- ***Anycast***: possui um identificador para um conjunto de interfaces (em diferentes nós de rede), sendo que um pacote enviado para um endereço *anycast* é entregue para uma das interfaces identificadas por esse endereço (o mais próximo na distância de roteamento).
- ***Multicast***: possui um identificador para um conjunto de interfaces (em diferentes nós de rede), sendo que um pacote enviado para um endereço *multicast* é entregue para todas as interfaces identificadas pelo endereço.

> **ASSIMILE**
>
> Os blocos de um endereço IPv4 são chamados de **octetos**, pois possuem oito símbolos binários (bits), que variam de 00000000 a 11111111. Os blocos de um endereço IPv6 são chamados de **decahexateto** ou **duocteto**, pois possuem quatro símbolos hexadecimais, os quais variam de 0000 até FFFF. Veja a composição do endereço IPv6 exemplificado no texto: **835C:5B9D:BC27:0000:0000:0000:C4B8:1FBB.**

Com o objetivo de manter os dois protocolos coexistentes e interoperáveis, ou seja, que possam ser utilizados e se prover de endereçamento e roteamento nas redes de computadores que podem ser configuradas apenas com endereços IPv4, apenas com endereços IPv6 ou com os dois protocolos, o que se chamou de Pilha Dupla (*Dual Stack*). Dispositivos de rede que suportam o conceito de **Pilha Dupla** defendido por Kurose e Ross (2013) os hosts configurados com IPv6 também devem possuir uma implementação IPv4 completa, o que os determinará como IPv6/IPv4. Na operação de um dispositivo configurado como Pilha Dupla, as mensagens oriundas da camada de Aplicação serão encapsuladas na Pilha Dupla, para que a mensagem enviada à camada de enlace e física (*host* de rede no TCP/IP)

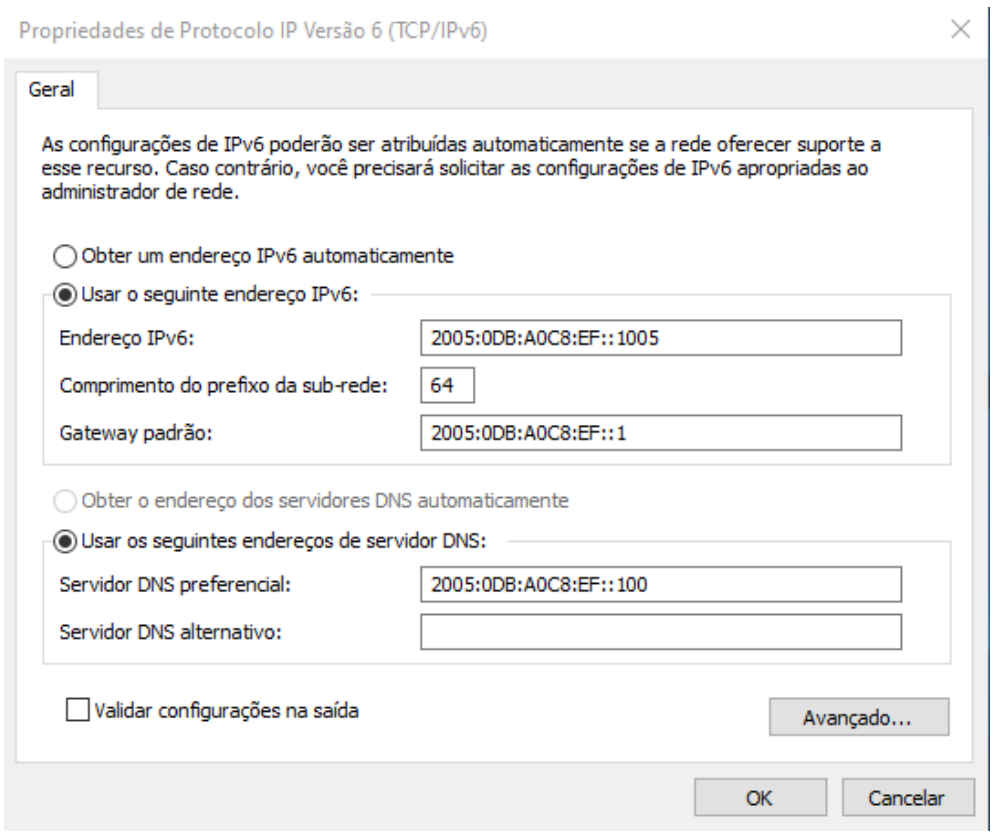
seja enviada ao meio disponível, onde podem ocorrer duas situações: 1. Mensagem com formato IPv4 é encapsulada com Ipv6; 2. Mensagem com formato IPv6 é encapsulada com IPv4.

EXEMPLIFICANDO

Dispositivos de rede, ou seja, *hosts* que estiverem configurados com o protocolo IPv6, deverão também ter uma implementação IPv4. Ao interagir um host IPv4, um *host* IPv6/IPv4 poderá usar datagramas IPv4; ao interagir com um *host* IPv6, poderá utilizar o IPv6. *Hosts* IPv6/IPv4 possuem endereços IPv6 e IPv4. Dispositivos de rede, como computadores, câmeras IP, impressoras, smartphones e dispositivos de IoT, devem estar configurados com a opção de Pilha Dupla.

Os endereços IPv6s e as máscaras (e sub-rede, se desejado) precisam ser informados em cada host da rede. Segue, na Figura 2.33, um exemplo de configuração de endereço IPV6 e máscara de rede (e/ou sub-rede) em um sistema Windows. Os servidores DHCP também podem ser configurados para configuração automática de endereços em *hosts* em uma rede.

Figura 2.33 | Exemplo de configuração de endereço IPv6



Fonte: captura de tela elaborada pelo autor.

TRADUÇÃO DE ENDEREÇOS E COEXISTÊNCIA

A comunicação entre *hosts* que operam em um ambiente onde as duas versões do protocolo IP são utilizadas também pode contar com um protocolo de tradução de endereços, como o ***Network Address Translation*** **(NAT)**. Este protocolo implementa um mecanismo de tradução de endereços IPv4 em endereços IPv6 com equivalência de valor.

Como exemplo de tradução de endereço IP, tomaremos o número IPv4 192.168.0.1. Para fazer a conversão do endereço, faça as seguintes etapas:

- Converta o endereço IPv4 para notação binária:

192.168.0.1 = 11000000.10101000.00000000.00000001

- Separe os números binários em grupos de quatro dígitos:

1100 0000 . 1010 1000 . 0000 0000 . 0000 0001

- Utilize as bases 8, 4, 2 e 1 para converter os grupos dos números binários:

1100 = 12 e 0000 = 0

1010 = 10 e 1000 = 8

0000 = 0 e 0000 = 0

0000 = 0 e 0001 = 1

- Converta os números encontrados em cada um dos oito grupos para a notação hexadecimal:

1100 = 12 = C e 0000 = 0 ➔ O primeiro duocteto fica C0.

1010 = 10 = A e 1000 = 8 ➔ O segundo duocteto fica A8.

0000 = 0 e 0000 = 0 ➔ O terceiro duocteto fica 00.

0000 = 0 e 0001 = 1 ➔ O quarto duocteto fica 01.

- Desta forma, o endereço IPv4 192.168.0.1 é representado em IPv6:

C0A8:0001.

- Adicione o 0 nos cinco primeiros grupos de 16 bits, seguido de FFFF:

0:0:0:0:0:FFFF:COA8:0001.

Ver anotações

- O IPv6 ainda permite a representação de seu endereço de forma reduzida, abstendo-se de apresentar os endereços com 0:

::FFFF:C0A8:0001.

Com os dispositivos configurados nas redes, os hosts devem ter também um mecanismo para que o roteamento das mensagens ocorra. Os hosts configurados com IPv4/IPv6 possuem suporte aos dois protocolos, não necessitando de técnicas de transição. Já um dispositivo configurado apenas com IPv4 ou IPv6 suportará operações de roteamento somente conforme o protocolo configurado.

Outra técnica adotada para a coexistência e interoperabilidade entre as diferentes versões do IP é o mecanismo de **6to4**, o qual permite que redes IPv6 tenham a comunicação entre os roteadores de forma automática. Roteadores 6to4 encaminham os dois endereços (Ipv4 e Ipv6) dos *hosts*, e os dispositivos clientes (*hosts*) devem estar configurados com os endereços IPv4. A Figura 2.34 apresenta uma topologia com exemplo de implementação de mecanismo 6to4.

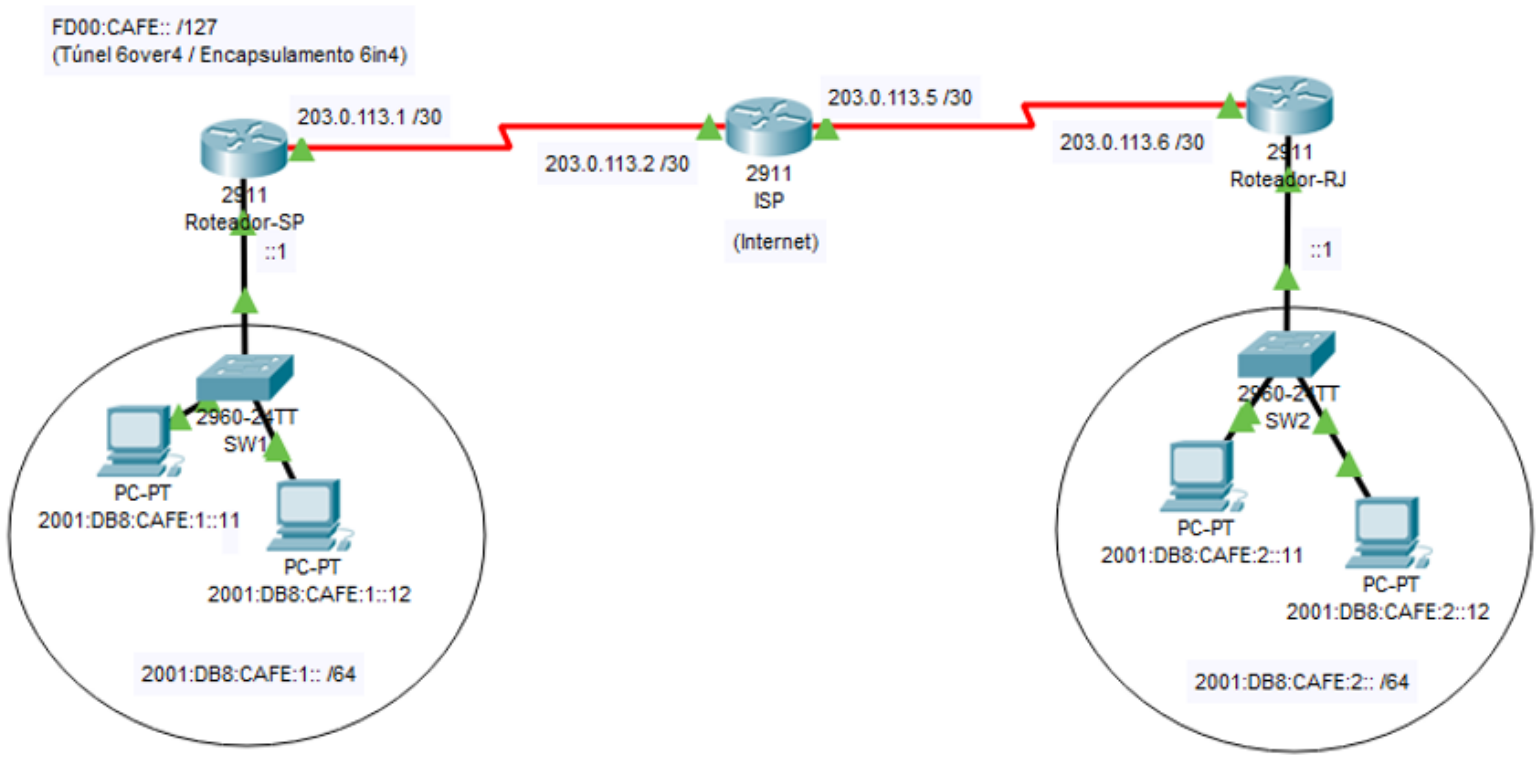
O **tunelamento** na rede permite que o IPv4 possa encaminhar pacotes ao IPv6 através de algumas possibilidades:

1. Roteador a roteador: o IPv6 é encapsulado dentro de um pacote IPv4 no início da transmissão.
2. Roteador a *host*: um host com IPv4 envia pacotes a um host IPv6, e o pacote utiliza-se da configuração de Pilha Dupla do roteador para alcançar o *host* de destino através de um túnel entre o roteador e o *host* destino.
3. *Host* a *host*: um host configurado com Pilha Dupla se comunica com outro *host* em uma rede configurada com o protocolo IPv4 via tunelamento entre os *hosts*.

Outro mecanismo, chamado de ***Tunel Broker***, encapsula o pacote IPv6 dentro do pacote IPv4 e permite que seja realizado o roteamento do pacote na rede através de um túnel em redes configuradas como IPv4 e necessidade de interoperabilidade com sites IPv4/IPv6.

A última técnica utilizada para interoperabilidade entre o IPv4 e IPv6 é a ***Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)***. Ela possibilita utilizar endereços atribuídos pelo servidor DHCP (*Dynamic Host Configuration Protocol*) com IPv4 para dispositivos com tunelamento de IPv6. Interessante observar que o ISATAP é default para sistemas operacionais Windows. Você pode reconhecer o endereço ISATAP com a utilização do comando *ipconfig* no *prompt* de comando. A Figura 2.34 apresenta um exemplo com topologia de túnel 6to4.

Figura 2.34 | Exemplo de topologia para implementação de técnica de túnel 6to4



Fonte: adaptada de LabCisco.

DIFERENÇAS ENTRE IPV4 E IPV6

As principais diferenças entre os protocolos IPv4 e IPv6 referem-se ao tamanho do endereço, à quantidade de endereços disponíveis para utilização, à representação do endereço, ao roteamento, à segurança e às questões de qualidade de serviço (*Quality of Services – QoS*). O Quadro 2.7 apresenta um comparativo de algumas características entre o endereço IPv4 e IPv6.

Quadro 2.7 | Comparação entre os protocolos IPv4 e IPv6

Área	**IPv4**	**IPv6**
Endereços	2^{32}	2^{128}
Campos	14	8
MTU mínimo	576 bytes	1280 bytes

Área	IPv4	IPv6
Representação	4 grupos de 8 bits	8 grupos de 16 bits
Roteamento	Tabela grande	Cabeçalho
Segurança	Não há	IPSeg
QoS	Não há	Com garantia

Fonte: adaptado de Forouzan (2010).

Segundo Tanenbaum (2011), os administradores de redes e os provedores de internet deverão suportar a interoperabilidade entre os dois protocolos, o IPv4 e o IPv6, por algum tempo ainda, porém esta coexistência deverá trazer alguns problemas de gerenciamento. Alguns deles são:

- **Falhas**: as redes deverão operar com o IPv4 e com o IPv6.
- **Contabilização**: recalcular limites de utilização de recursos.
- **Configuração**: pela necessidade de coexistência entre os protocolos.
- **Desempenho**: necessidade de adaptações para garantia de performance em serviços.
- **Segurança**: buscar técnica para garantia da interoperabilidade (coexistência) sem riscos à segurança de sistemas.

As informações técnicas apresentadas suportam a configuração de ambientes de rede de computadores com protocolos IPv4, IPv6 e, principalmente, com a coexistência e interoperabilidade dos dois protocolos no mesmo ambiente.

REFLITA

Um endereço IPv4 é composto por quatro blocos de oito bits cada, totalizando 32 bits, o que resulta em uma quantidade de endereços para hosts diretamente interligados à internet de aproximadamente 4.3 bilhões, ou seja, 2^{32} endereços. A sua utilização em redes locais privadas, porém,

pode incrementar este número de endereços, por serem redes isoladas da internet, através de seus servidores e controles de atribuição de endereços pelos provedores de serviços de conexão à internet.

Já um endereço IPv6 é composto por oito blocos de 16 bits cada, totalizando 128 bits, o que representa uma quantidade de endereços para *hosts* diretamente interligados à internet de 340 undecilhões. O número é grande, mesmo considerando previsões de termos mais de 10 trilhões de dispositivos de IoT (*Internet of Things*) interconectados até o ano de 2030, conforme previsto por Diamandis e Kotler (2018).

Qual deverá ser a versão de IP para endereçamento de dispositivos de IoT adequado?

Caro aluno, esta seção trouxe para você importantes conceitos a respeito do padrão Ethernet (IEEE 802.3) e suas diferentes versões utilizadas para implementação de sistemas de redes de computadores locais através de cabos, com uma tecnologia amplamente utilizada nos últimos 30 anos. De forma complementar, e com grande importância, trouxe também informações sobre o IPv6 como uma versão atualizada do protocolo IP para endereçamento e roteamento de redes, que deverá ser utilizado como padrão de endereçamento de redes junto à versão IPv4. Estas informações são fundamentais para que um profissional de tecnologia da informação possa projetar e implementar uma rede de computadores com performance adequada.

FAÇA VALER A PENA

Questão 1

O padrão Ethernet para redes de computadores pode utilizar cabos metálicos e cabos ópticos na implementação física do meio de transmissão em camada de *host* de rede do conjunto de protocolos TCP/IP (ou camada física no modelo de referência OSI). A comunicação de dados em nível de enlace ocorre utilizando um protocolo de acesso múltiplo ao meio compartilhado nestas redes, de forma que um único cabo é utilizado para a comunicação entre *hosts*.

Assinale a alternativa que apresenta o nome do protocolo de acesso ao meio compartilhado utilizado no padrão Ethernet:

a. CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*).

b. CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*).

c. PPP (*Point to Point Protocol*).

d. UDP (*User Datagram Protocol*).

e. TCP (*Transmission Control Protocol*).

Questão 2

Conforme sustentam Kurose e Ross (2013), a partir da década de 1990, a comunidade responsável pelas tecnologias de rede de computadores, especificamente pelo protocolo IP, passou a buscar uma alternativa para substituição do protocolo utilizado no final do século XIX, que já vinha sendo utilizado desde o surgimento da ARPAnet (*Advanced Research Project Agency Network*).

Com a intenção de desenvolver um novo protocolo de endereçamento e roteamento de rede, o _____ veio para suprir algumas necessidades além das possibilidades do protocolo _____, que eram: 1. Resolver a _____ de endereços IPs na internet; 2. Simplificar o cabeçalho do endereço IP; 3. Deixar como opcionais alguns campos de cabeçalho IP para facilitar o roteamento de pacotes na rede; 4. Melhorar a segurança das transmissões, adicionando o _____ para prover segurança ao protocolo.

Assinale a alternativa que preenche corretamente as lacunas:

a. IPv4; IPv6; escassez; IPsec.

b. IPv4; IPv6; padronização; UDP.

c. IPv6; IPv4; escassez; IPsec.

d. IPv6; IPv4; escassez; TCP.

e. IPv6; IPv4; padronização; TCP.

Questão 3

O planejamento de topologia de uma rede padrão Ethernet precisa levar em consideração o volume de dispositivos conectados e endereçados na rede mediante a utilização de dispositivos chamados de comutadores, os quais buscam comutar a transmissão com os hosts na rede. Os dispositivos estão dentro de um ambiente de acesso múltiplo ao meio compartilhado e têm um importante papel referente à performance da rede.

Considerando as características de uma rede Ethernet e os dispositivos comutadores que pertencem a este padrão de rede, analise as afirmativas a seguir:

- Em uma rede Ethernet, podem ocorrer colisões de duas formas, sendo uma pelo domínio de colisão e outra pelo domínio de *broadcast*.
- No domínio de colisão, os pacotes da rede têm a possibilidade de efetuar colisão uns com os outros, o que leva à degradação da performance da rede, pois faz com que muitas retransmissões sejam necessárias.
- Um *hub* é um dispositivo que faz comutação em uma rede com a repetição das mensagens para todas as suas portas de conexão, formando um único domínio de colisão e *broadcast*.
- Um *switch* é um dispositivo capaz de formar um domínio de colisão em cada porta de comunicação e formar um único domínio de *broadcast*. Dispositivo fundamental na operação das redes de computadores na atualidade.

Considerando o contexto apresentado, é correto o que se afirma em:

a. I e II, apenas.

b. I, II e III, apenas.

c. I e IV, apenas.

d. I, III e IV, apenas.

e. I, II, III e IV.

Ver anotações 0

REFERÊNCIAS

COMER, D. E. **Redes de Computadores e Internet**. 6. ed. Porto Alegre, RS: Bookman, 2016.

DIAMANDIS, P. H.; KOTLER, S. **Oportunidades Exponenciais**: um manual prático para transformar os maiores problemas do mundo nas maiores oportunidades de negócio. Rio de Janeiro: Alta Books, 2018.

FILIPPETTI, M. A. **CCNA 4.1**: Guia completo de estudos. Florianópolis, SC: Visual Books, 2008.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. Porto Alegre, RS: AMGH, 2010.

GOMES, A. IPv6: entenda por que este padrão é indispensável. **Olhar Digital**, 2020. Disponível em: https://olhardigital.com.br/video/ipv6-entenda-por-que-o-padrao-e-indispensavel/109920. Acesso em: 1º out. 2020.

IPV6.BR. **Cabeçalho**. 2020. Disponível em: http://ipv6.br/post/cabecalho/. Acesso em: 14 nov. 2020.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**: uma abordagem top-down. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

NUNES, S. E. **Redes de Computadores**. Londrina, PR: Editora e Distribuidora Educacional S. A., 2017.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados**. Rio de Janeiro: Elsevier, 2016. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595156708/. Acesso em: 21 out. 2020.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 1997.

TANENBAUM, A. S. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011.