

**NEaD**  
Núcleo de Educação a Distância

# CYBER SECURITY

F a c u l d a d e  
**IMPACTA**

# 3

## Funcionamento dos protocolos Ethernet e IP

Alex Sandro da Silva Feitosa

### *Resumo*

*Nessa aula, falaremos sobre como o protocolo Ethernet, juntamente com o IPv4 e o IPv6, oferece suporte à comunicação de rede. Discutiremos de forma introdutória como estes protocolos permitem a troca de informações entre computadores e outros dispositivos, garantindo que os dados sejam transmitidos de forma eficiente e organizada em diferentes tipos de redes.*

### **Introdução**

Vamos explorar de forma introdutória como os protocolos Ethernet, IPv4 e IPv6 viabilizam a comunicação entre dispositivos em redes, assegurando a transmissão eficiente e estruturada de dados. Esses protocolos são fundamentais para o funcionamento da internet e das redes locais, permitindo a interoperabilidade entre diferentes sistemas e tecnologias.

#### **1.1. Ethernet**

##### **1.1.1 Encapsulamento Ethernet**

Os hackers podem configurar hotspots sem fio “invasores” abertos, fingindo ser uma rede sem fio genuína.

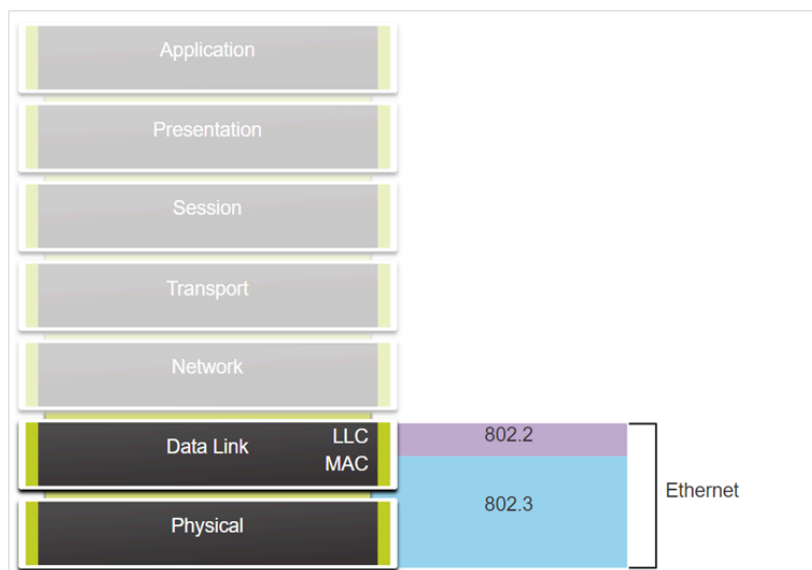
Ethernet opera na camada de enlace de dados e na camada física.

É uma família de tecnologias de rede definidas nos padrões IEEE 802.2 e 802.3.

Ethernet suporta larguras de banda de dados de 10 Mbps a 100.000 Mbps (100 Gbps).

Conforme mostrado na figura, os padrões Ethernet definem os protocolos da camada 2 e as tecnologias da camada 1.

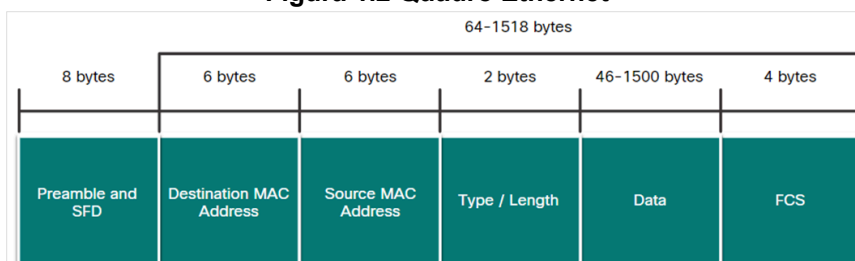
**Figura 1.1 Encapsulamento**



**Fonte: CCNA Cyber OPS Associate v1, 2020.**

- O tamanho mínimo de quadro Ethernet é 64 bytes e o máximo é 1518 bytes. Isso inclui todos os bytes do campo de endereço MAC de destino através do campo FCS (Frame Check Sequence).
- Qualquer quadro com comprimento menor que 64 bytes é considerado um "fragmento de colisão" ou um "quadro desprezível" e é automaticamente descartado pelas estações receptoras. Quadros com mais de 1.500 bytes de dados são considerados "jumbo" ou "baby giant".

**Figura 1.2 Quadro Ethernet**



**Fonte: CCNA Cyber OPS Associate v1, 2020.**

**Preâmbulo** – Utilizado para sincronização, também contém um delimitador para marcar o final da informação cronometrada.

**Endereço MAC de Destino**

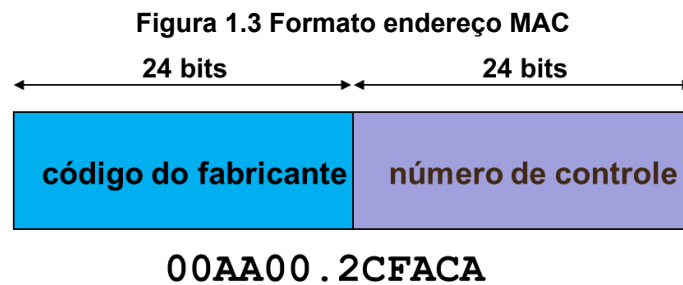
**Endereço MAC de Origem**

**Tipo** – Valor para indicar que protocolo de camada superior receberá os dados depois que o processo Ethernet for concluído.

**Dados de 46 a 1500 bytes** – informação do usuário.

**Sequência de Verificação do Quadro(FCS)** – valor utilizado para verificar quadros danificados/sequência.

Endereçamento físico MAC - Media Access Control



Fonte: CCNA Cyber OPS Associate v1, 2020.

O Endereço MAC pode ser representado por:

48 bits

12 dígitos hexadecimais

6 bytes hexadecimais

Exemplos de códigos de fabricantes:

00-00-0C Cisco

00-00-1B Novell

00-AA-00 Intel

02-60-8C 3Com

## 1.2. IPv4

### 1.2.1 Encapsulamento IP

Os hackers podem configurar hotspots sem fio “invasores” abertos, fingindo ser uma rede sem fio genuína.

O IP encapsula o segmento da camada de transporte.

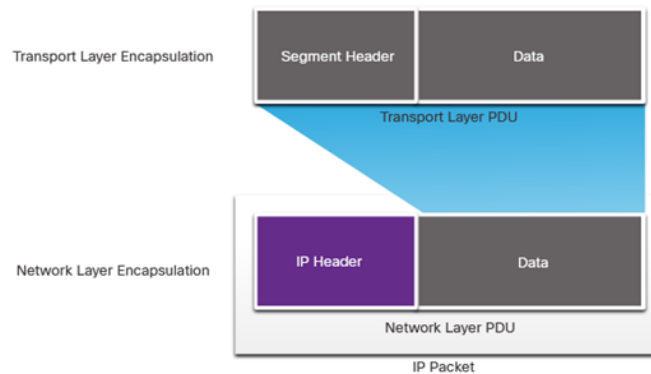
O IP pode usar um pacote IPv4 ou IPv6 e não afetar o segmento da camada 4.

O pacote IP será examinado por todos os dispositivos de camada 3 à medida que atravessa a rede.

O endereçamento IP não muda de origem para destino.

Observação: o NAT mudará o endereçamento, mas será discutido em um módulo posterior.

**Figura 1.4 encapsulamento IP**



**Fonte: CCNA Cyber OPS Associate v1, 2020.**

O IP deve ter baixa sobrecarga e pode ser descrito como:

- Sem Conexão
- Melhor Esforço
- Independente de Mídia

O endereço IP não tem conexão

1. Nenhuma conexão é estabelecida com o destino antes do envio dos pacotes de dados.
2. Não há informações de controle necessárias (sincronizações, confirmações, etc.).
3. O destino receberá o pacote quando ele chegar, mas nenhuma pré-notificação é enviada por IP.
4. Se houver necessidade de tráfego orientado para conexão, outro protocolo irá lidar com isso (normalmente TCP na camada

IP é melhor esforço

- IP não garantirá a entrega do pacote.
- O IP reduziu a sobrecarga, uma vez que não há mecanismo para reenviar dados que não são recebidos.
- IP não espera confirmações.
- IP não sabe se o outro dispositivo está operacional ou se recebeu o pacote.

IP não é confiável

- Ele não pode gerenciar ou corrigir pacotes não entregues ou corrompidos.
- IP não pode retransmitir após um erro.
- O IP não pode realinhar pacotes fora de sequência.
- IP deve depender de outros protocolos para essas funções.

O protocolo IP independe de meio físico.

- O IP não se preocupa com o tipo de quadro exigido na camada de link de dados ou com o tipo de mídia na camada física.
- IP pode ser enviado por qualquer tipo de mídia: cobre, fibra ou sem fio.

A camada de rede estabelecerá a Unidade Máxima de Transmissão (MTU).

- A camada de rede recebe isso a partir de informações de controle enviadas pela camada de link de dados.
- Em seguida, a rede estabelece o tamanho da MTU.

Fragmentação ocorre quando a Camada 3 divide o pacote IPv4 em unidades menores.

- Fragmentação causa latência.
- O IPv6 não fragmenta pacotes.
- Exemplo: Roteador vai de Ethernet para uma WAN lenta com um MTU menor

### 1.2.2 Cabeçalho do pacote IPv4

IPv4 é o principal protocolo de comunicação para a camada de rede.

O cabeçalho de rede tem muitas finalidades:

Ele garante que o pacote seja enviado na direção correta (para o destino).

Ele contém informações para o processamento da camada de rede em vários campos.

As informações no cabeçalho são usadas por todos os dispositivos de camada 3 que manipulam o pacote

As características do cabeçalho de rede IPv4:

É em binário.

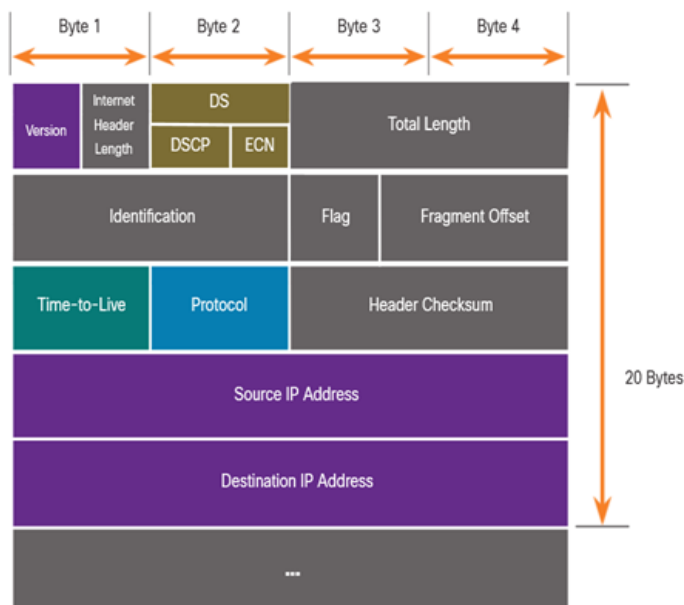
Contém vários campos de informação

O diagrama é lido da esquerda para a direita, 4 bytes por linha

Os dois campos mais importantes são a origem e o destino.

Protocolos podem ter uma ou mais funções.

**Figura 1.5 Pacote IPv4**



Fonte: CCNA Cyber OPS Associate v1, 2020.

Estes são os campos mais importantes no cabeçalho IPv4:

| Função                                  | Descrição  |
|---|--|
| <b>Versão</b>                           | Isso será para v4, ao contrário de v6, um campo de 4 bits = 0100                       |
| <b>Serviços Diferenciados</b>           | Usado para QoS: campo DiffServ — DS ou o IntServ mais antigo — ToS ou Tipo de Serviço  |
| <b>Soma de verificação do cabeçalho</b> | Detectar corrupção no cabeçalho IPv4   |
| <b>Tempo de vida (TTL)</b>              | Contagem de saltos de camada 3. Quando se tornar zero, o roteador descartará o pacote. |
| <b>Protocolos</b>                       | I.D.s protocolo de próximo nível: ICMP, TCP, UDP, etc.                                 |
| <b>Endereço IPv4 Origem</b>             | Endereço de origem de 32 bits  |
| <b>Endereço IPV4 de destino</b>         | Endereço de destino de 32 bits   |

**Figura 1.6 Wireshark**



| No. | Time       | Source                     | Destination     | Protocol | Length | Info                             |
|-----|------------|----------------------------|-----------------|----------|--------|----------------------------------|
| 16  | 3.64050300 | 192.168.1.109              | 192.168.1.1     | ICMP     | 74     | Echo (ping) request id=0x0001,   |
| 17  | 3.64506800 | 192.168.1.1                | 192.168.1.109   | ICMP     | 74     | Echo (ping) reply id=0x0001,     |
| 18  | 3.68215500 | 192.168.1.109              | 38.112.107.53   | TCP      | 54     | 55502 > https [ACK] Seq=1 Ack=13 |
| 19  | 4.19945400 | fe80::15ff:98d8:d28ff02::c |                 | SSDP     | 208    | M-SEARCH * HTTP/1.1              |
| 20  | 4.60748800 | fe80::15ff:98d8:d28ff02::c |                 | SSDP     | 453    | HTTP/1.1 200 OK                  |
| 21  | 4.64229900 | 192.168.1.109              | 192.168.1.1     | ICMP     | 74     | Echo (ping) request id=0x0001,   |
| 22  | 4.64509200 | 192.168.1.1                | 192.168.1.109   | ICMP     | 74     | Echo (ping) reply id=0x0001,     |
| 23  | 4.73605200 | 192.168.1.109              | 255.255.255.255 | DB-LSP   | 154    | Droobox LAN svnc Discoverv Proto |

|   |
|---|
| Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0                  |
| Ethernet II, Src: IntelCor_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li_a0:d1:be (00:18:39:a0:d1:be) |
| Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1)     |
| Version: 4  |
| Header length: 20 bytes   |
| Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Tran   |
| Total Length: 60  |
| Identification: 0x3704 (14084)  |
| Flags: 0x00   |
| Fragment offset: 0  |
| Time to live: 128   |
| Protocol: ICMP (1)  |
| Header checksum: 0x7ffe [correct]   |
| Source: 192.168.1.109 (192.168.1.109)   |
| Destination: 192.168.1.1 (192.168.1.1)  |
| [Source GeoIP: Unknown]   |
| [Destination GeoIP: Unknown]  |
| Internet Control Message Protocol   |

Fonte: CCNA Cyber OPS Associate v1, 2020.

A RFC 790 (1981) define a alocação dos endereços IPv4 em classes

Classe A (0.0.0/8 a 127.0.0/8)

Classe B (128.0.0.0 /16 — 191.255.0.0 /16)

Classe C (192.0.0.0 /24 — 223.255.255.0 /24)

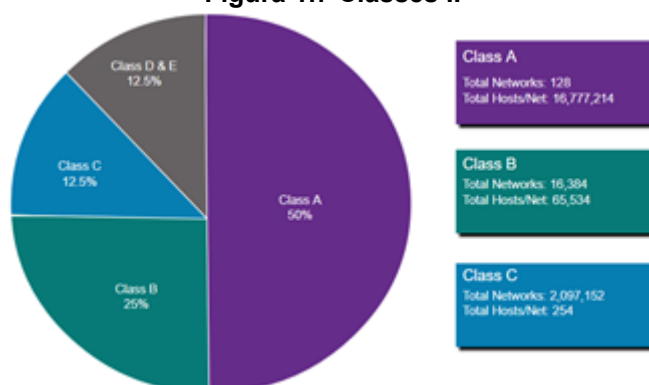
Classe D (224.0.0.0 a 239.0.0.0)

Classe E (240.0.0.0 — 255.0.0.0)

Endereços de classe desperdiçaram muitos endereços IPv4.

A alocação de endereços de classe foi substituída por endereçamento sem classe que ignora as regras das classes (A, B, C).

Figura 1.7 Classes IP



Fonte: CCNA Cyber OPS Associate v1, 2020.

Tabela das classes de endereços



### Endereços IPv4 públicos e privados

Conforme definido na RFC 1918, os endereços IPv4 públicos são roteados globalmente entre os roteadores do provedor de serviços de Internet (ISP).

| Classes | Range dos Endereços           | Nº de Endereços por Rede   |
|---------|-------------------------------|----------------------------|
| A       | 0.0.0.0 até 127.0.0.0         | 16.777.216                 |
| B       | 128.0.0.0 até 191.255.0.0     | 65.536                     |
| C       | 192.0.0.0 até 223.255.255.0   | 256                        |
| D       | 224.0.0.0 até 239.255.255.255 | Multicast                  |
| E       | 240.0.0.0 até 255.255.255.254 | Reservado para uso futuro. |

| Classes | RFC 1918 - Intervalos de endereços Privados |
|---------|---|
| A       | 10.0.0.0 até 10.255.255.255                 |
| B       | 172.16.0.0 até 172.31.255.255               |
| C       | 192.168.0.0 até 192.168.255.255             |

| Classes | Formato             | Máscara Padrão |
|---------|---------------------|----------------|
| A       | Rede.Host.Host.Host | 255.0.0.0      |
| B       | Rede.Red.Host.Host  | 255.255.0.0    |
| C       | Rede.Red.Red.Host   | 255.255.255.0  |

Endereços privados são blocos comuns de endereços usados pela maioria das organizações para atribuir endereços IPv4 a hosts internos.

Os endereços IPv4 privados não são exclusivos e podem ser usados internamente em qualquer rede.

No entanto, os endereços privados não são globalmente roteáveis.

**Loopback** - Apenas o único endereço 127.0.0.1 é usado, os endereços de 127.0.0.0 à 127.255.255.255 são reservados. Qualquer endereço dentro deste bloco fará um loop de volta para o host local. Comumente identificado como apenas 127.0.0.1. Usado em um host para testar se o TCP / IP está operacional.

**Link-Local** - Endereços IPv4 o bloco de endereço 169.254.0.0 a 169.254.255.255 (169.254.0.0/16) são designados como endereços link-local. Comumente conhecido como endereços APIPA (Automatic Private IP Addressing) ou

endereços auto-atribuídos. Usado pelos clientes DHCP do Windows para se autoconfigurar quando nenhum servidor DHCP está disponível.

**TEST-NET** - o bloco de endereço 192.0.2.0 a 192.0.2.255 (192.0.2.0/24) é usado para fins de ensino e aprendizagem.

**Endereços experimentais** - Os endereços no bloco 240.0.0.0 a 255.255.255.254 são listados como reservado para uso futuro (RFC 3330).

**Endereço de rede** - O endereço pelo qual nos referimos à rede

**Endereços de host** - Os endereços designados aos dispositivos finais da rede

**Endereço de broadcast** - Endereço especial usado para enviar dados a todos os hosts da rede

**Unicast** - o processo de envio de um pacote de um host para um host individual

**Broadcast** - o processo de envio de um pacote de um host para todos os hosts numa rede

**Multicast** - o processo de envio de um pacote de um host para um grupo de hosts selecionados

## 1.5. Vamos praticar:

Complete a Tabela

| Endereço IP do Host | Classe do Endereço | Endereço da Rede | Endereço do Host | Endereço de Broadcast | Máscara de sub-rede padrão |
|---------------------|--------------------|------------------|------------------|-----------------------|----------------------------|
| 194.125.35.199      | C                  |                  |                  |                       |                            |
|                     |                    | 175.12.0.0       | 239.244          |                       | 255.255.0.0                |
|                     |                    |                  | 221.224          | 150.127.255.255       |                            |
|                     |                    | 123.0.0.0        | 1.1.15           |                       |                            |
| 216.14.55.137       |                    |                  |                  |                       |                            |
| 210.23.67.102       |                    |                  |                  |                       |                            |
| 77.123.28.167       |                    |                  |                  |                       |                            |

## 1.3. IPv6

### 1.3.1 Pacote IPv6

Os hackers podem configurar hotspots sem fio “invasores” abertos, fingindo ser uma rede sem fio genuína.

O que impulsionou o IPv6?

O crescimento das redes e um possível esgotamento dos endereços IP;

- O aumento da tabela de roteamento;
- Problemas relacionados a segurança dos dados transmitidos;
- Prioridade na entrega de determinados tipos de pacotes;
- Consecutivamente o esgotamento do IPv4.

O IPv4 tem três limitações principais:

Esgotamento de endereços IPv4 — Nós basicamente ficamos sem endereçamento IPv4.

Falta de conectividade de ponta a ponta — Para que o IPv4 sobreviva a esse tempo, o endereçamento privado e o NAT foram criados. Isso terminou com as comunicações diretas com endereçamento público.

Maior complexidade da rede — o NAT foi concebido como solução temporária e cria problemas na rede como um efeito colateral da manipulação do endereçamento de cabeçalhos de rede. O NAT causa latência e solução de problemas.

O IPv6 foi desenvolvido pela Internet Engineering Task Force (IETF).

O IPv6 supera as limitações do IPv4.

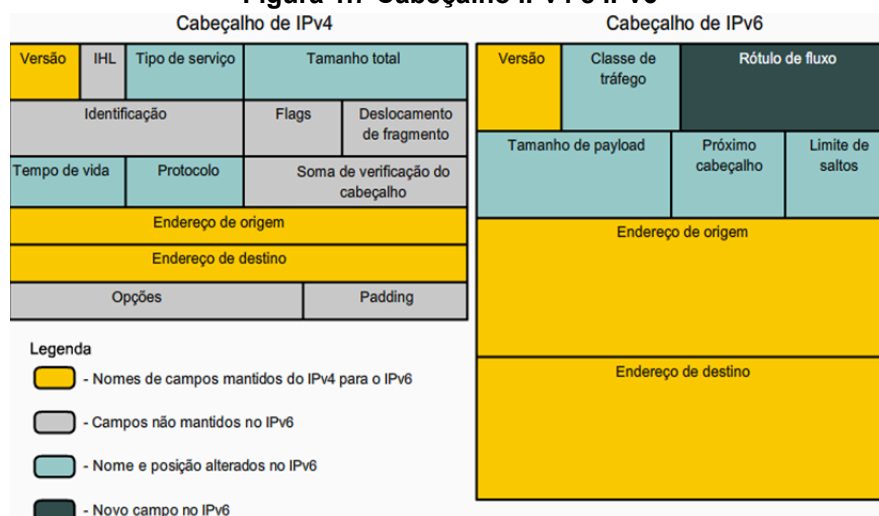
Melhorias que o IPv6 fornece:

Aumento do espaço de endereço — baseado no endereço de 128 bits, não em 32 bits.

Manipulação aprimorada de pacotes - O cabeçalho IPv6 foi simplificado com menos campos.

Elimina a necessidade de NAT — uma vez que há uma grande quantidade de endereçamento, não há necessidade de usar o endereçamento privado internamente e ser mapeado para um endereço público compartilhado.

**Figura 1.7 Cabeçalho IPv4 e IPv6**



Fonte: CCNA Cyber OPS Associate v1, 2020.

Figura 1.7 Cabeçalho IPv6 no Wireshark

| No. | Time       | Source                            | Destination                       | Protocol | Length | Info   |
|-----|------------|-----------------------------------|-----------------------------------|----------|--------|--|
| 47  | 325.030878 | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | TCP      | 82     | http > 59201 [SYN, ACK] Seq=0 Ack=1 win=...  |
| 48  | 325.031166 | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | TCP      | 74     | 59201 > http [ACK] Seq=1 Ack=1 win=5760 L... |
| 49  | 325.040411 | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | HTTP     | 314    | GET / HTTP/1.0                               |
| 50  | 325.045496 | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | TCP      | 1506   | [TCP segment of a reassembled PDU]           |
| 51  | 325.045525 | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | HTTP     | 901    | HTTP/1.1 200 OK (text/html)                  |
| 52  | 325.045627 | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | 2001:6f8:102d:0:2d0:9ff:fee3:e8de | TCP      | 74     | http > 59201 [FIN, ACK] Seq=2260 Ack=241...  |

Frame 49: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interface 0

Ethernet II, Src: HsingTec\_e3:e8:de (00:d0:09:e3:e8:de), Dst: Ibm\_82:95:b5 (00:11:25:82:95:b5)

Internet Protocol Version 6, Src: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de), Dst: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de)

0110 .... = Version: 6

.... 0000 0000 .... = Traffic class: 0x00000000

.... 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000

Payload length: 260

Next header: TCP (6)

Hop limit: 64

Source: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de)

[Source SA MAC: HsingTec\_e3:e8:de (00:d0:09:e3:e8:de)]

Destination: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de)

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 59201 (59201), Dst Port: http (80), Seq: 1, Ack: 1, Len: 240

Hypertext Transfer Protocol

(CCNA Cyber OPS Associate v1)

O pacote IPv6 também pode conter cabeçalhos de extensão (EH).

Características dos cabeçalhos EH:

Fornecer informações opcionais sobre a camada de rede são opcionais, são colocados entre o cabeçalho IPv6 e a carga útil e podem ser usados para fragmentação, segurança, suporte à mobilidade etc.

Nota: Ao contrário do IPv4, os roteadores não fragmentam pacotes IPv6.

### 1.3.2 Representação de endereços IPv6

Os endereços IPv6 têm 128 bits e são gravados em hexadecimal.

Os endereços IPv6 não diferenciam maiúsculas e minúsculas e podem ser escritos tanto em minúsculas como em maiúsculas.

Como mostrado na Figura 1, o formato preferencial para escrever um endereço IPv6 é x: x: x: x: x: x: x: x, com cada “x” consistindo de quatro valores hexadecimais.

No IPv6, um hexteto é o termo não oficial usado para se referir a um segmento de 16 bits ou quatro valores hexadecimais.

Exemplos de endereços IPv6 no formato preferido:

2001:0db8:0000:1111:0000:0000:0000:0200

2001:0db8:0000:00 a3:abcd:0000:0000:1234

Um endereço IPv4 é formado por 32 bits.

$$2^{32} = 4.294.967.296$$

Um endereço IPv6 é formado por 128 bits.

$$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$$

~ 56 octilhões (5,6x10<sup>28</sup>) de endereços IP por ser humano.

~ 79 octilhões (7,9x10<sup>28</sup>) de vezes a quantidade de endereços IPv4.

A representação dos endereços IPv6, divide o endereço em oito grupos de 16 bits, separando-os por “:”, escritos com dígitos hexadecimais.

**2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1**

  
**2 Bytes**

Na representação de um endereço IPv6 é permitido:

- Utilizar caracteres maiúsculos ou minúsculos;
- Omitir os zeros à esquerda; e
- Representar os zeros contínuos por “::”.

Exemplo:

**2001:0DB8:0000:0000:130F:0000:0000:140B**

**2001:db8:0:0:130f::140b**

Formato inválido: **2001:db8::130f::140b** (gera ambiguidade)

Representação dos Prefixos

Como o CIDR (IPv4)

“endereço-IPv6/tamanho do prefixo”

Exemplo:

Prefixo 2001:db8:3003:2::/64

Prefixo global 2001:db8::/32


ID da sub-rede 3003:2

URL

[http://\[2001:12ff:0:4::22\]/index.html](http://[2001:12ff:0:4::22]/index.html)

[http://\[2001:12ff:0:4::22\]:8080](http://[2001:12ff:0:4::22]:8080)

**2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F/64**



Prefixo de roteamento global    ID da sub-rede    ID da interface


O **prefixo do site** ou o **prefixo de roteamento global** constitui-se dos primeiros 3 sextetos ou 48 bits do endereço. Ele é determinado pelo provedor de serviços.

A **topologia do site** ou o **ID da sub-rede** é o quarto sexteto do endereço.

O **ID da interface** é composto pelos 4 últimos sextetos ou os últimos 64 bits do endereço. Ele pode ser determinado manualmente ou dinamicamente por meio do comando EUI-64 (identificador estendido exclusivo)

Os primeiros 3 bits são fixados em 001 ou 200::/12 (número de roteamento global IANA)

**2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64**



**IANA**

Os bits 16-24 identificam o registro regional:

- AfriNIC, APNIC, LACNIC, RIPE NCC and ARIN

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

  
Registro

2001:0000::/23 – IANA

2001:0200::/23 – APNIC (Região Ásia/Pacífico)

2001:0400::/23 – ARIN (Região da América do Norte)

2001:0600::/23 – RIPE (Europa, Oriente Médio e Ásia Central)

Os 8 bits restantes até o 32 identificam o ISP

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

  
ISP

O terceiro sexteto representa o identificador do site ou cliente.

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

  
Site

O quarto sexteto representa a topologia do site ou o ID da sub-rede.

- Permite 65.536 sub-redes com 18,446,744,073,709,551,616  
(18 quintilhões) para cada sub-rede.

- Não faz parte do endereço de host.

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F /64

  
Sub-rede

O IPv6 usa o mesmo método que o IPv4 para a criação de sub-redes em seus endereços.

/127 fornece 2 endereços.

/124 fornece 16 endereços

/120 fornece 256 endereços

O primeiro endereço em uma rede é formado somente por zeros, enquanto o último é formado somente por efes (F).

Por razões de simplicidade e de design, recomenda-se a utilização de /64 em todos os locais. Usar qualquer coisa menor que /64 poderia possivelmente romper recursos de IPv6 e aumentar a complexidade do projeto.

**Regra 1** de representação de endereço IPv6 — Omitir zero à esquerda

A primeira regra para ajudar a reduzir a notação de endereços IPv6 é omitir quaisquer 0s (zeros) iniciais.

Exemplos:

01AB pode ser representado como 1AB

09f0 pode ser representado como 9f0

0a00 pode ser representado como a00

00ab pode ser representado como ab

**Observação:** Essa regra se aplica somente aos 0s à esquerda, e NÃO aos 0s à direita. Caso contrário, o endereço ficaria ambíguo.

| Tipo                 | Formato                                       |
|----------------------|---|
| Preferencial         | 2001: 0db8: 0000:1111: 0000: 0000: 0000: 0200 |
| Sem zeros à esquerda | 2001: db8:0: 1111:0: 0:0: 200                 |

### Regra 2 de Representação de Endereço IPv6 — Dois-pontos duplos

Dois pontos-e-vírgula (: :) podem substituir qualquer sequência única e contígua de um ou mais hexadecimais de 16 bits que consistem em todos os zeros.

Exemplo:

2001:db8:cafe: 1:0:0:0:1 (0s principais omitidos) poderia ser representado como 2001:db8:cafe:1: :1

**Observação:** Os dois-pontos em dobro (::) só podem ser usados uma vez em um endereço; caso contrário, haveria mais de um endereço resultante possível.

| Tipo         | Formato                                       |
|--------------|---|
| Preferencial | 2001: 0db8: 0000:1111: 0000: 0000: 0000: 0200 |
| Compactado   | 2001:db8:0:1111::200                          |

### Conclusão

Concluimos que os protocolos Ethernet, IPv4 e IPv6 desempenham um papel essencial na comunicação em redes, ao possibilitarem a troca organizada e eficiente de dados entre dispositivos. Compreender o funcionamento desses protocolos é fundamental para entender as bases da conectividade em ambientes digitais, tanto em redes locais quanto na internet.



## Referências

Cisco Systems. **Cisco Networking Academy Program CCNA CyberOps Associate** v1, 2020. Disponível em: <<https://www.netacad.com>>.

SÊMOLA, Marcos. **Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

THOMAS, Tom. **Segurança de redes: primeiros passos**. Tradução de Flávio MORGADO. Rio de Janeiro: Ciência Moderna, 2007.

BEAL, A. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

STALLINGS, W. **Network security: applications and standards**. 3.nd. New Jersey: Prentice Hall, 2006.

ASSOCIAÇÃO Brasileira de Normas Técnicas. **NBR ISO/IEC 27001 E 27002** Tecnologia da informação.

WADLOW, Thomas A. **Segurança de redes: projeto e gerenciamento de redes seguras**. Rio de Janeiro: Campus, 2000.