UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
COLEGIADO DE CIÊNCIA DA COMPUTAÇÃO

Relatório de Aula Prática – Redes de Computadores

Título: WLAN
Aluno: Vitor Mayorca Camargo Data: 30/01/2025

---

1. INTRODUÇÃO

A internet surgiu na década de 1960 como ARPANET, inicialmente usada para comunicação militar e acadêmica nos EUA (LEINER, *et al*. 2009). Em 1989, a criação da World Wide Web democratizou o acesso e compartilhamento de informações por meio de navegadores web, permitindo que pessoas comuns usassem a internet de forma fácil e rápida (MONTEIRO, 2001).

As informações transmitidas na internet seguem protocolos rigorosos, como o TCP e o IP, que surgiram da necessidade de estabelecer regras e padrões para unificar as diferentes redes e máquinas que formam a internet (CORONA, 2004). O protocolo TCP (Transmission Control Protocol) foi projetado para fornecer uma comunicação confiável entre dois computadores, reduzindo ou aumentando a taxa de transmissão de dados de forma dinâmica, com o fim de evitar perda de dados. (CAMPISTA, *et al*. 2010).

Já o protocolo IPv4 (Internet Protocol) define a base para a transação, tráfego e reconhecimento de dados em uma rede. Ele é responsável por definir o "Endereço IP", que é um número único dado a cada máquina ou "host" na rede. Esse endereço é composto por quatro números (de 0 a 255) separados por pontos (de 000.000.000.000 a 255.255.255.255), e permite que uma máquina seja identificada e se comunique com outras na rede (CORONA, *et al*. 2004). Os autores também explicam que o protocolo TCP/IP divide os dados em pequenas porções para transferência na Internet. O protocolo IP organiza o envio e recebimento desses pacotes, enquanto o protocolo TCP se encarrega de dividir, ordenar e garantir que o fluxo de dados ocorra corretamente.

Duas versões do protocolo IP são usadas como padrão na internet. O IPv4 especifica as capacidades e protocolos básicos que toda máquina deve seguir, e usa um endereço de 32 bits (TANENBAUM, 2003). Já o IPv6, mais avançado, possui uma maior segurança e melhor comunicação entre as redes, fornecendo um endereço de 128 bits (CHANDRA, KATHING, KUMAR. 2013).

Segundo Ross (2008), redes LAN (Local Area Network) são redes locais que conectam dispositivos em uma área limitada, como uma residência, escritório ou campus. Elas são projetadas para alta velocidade e baixa latência, utilizando tecnologias como Ethernet e Wi-Fi para permitir a comunicação eficiente entre dispositivos próximos. Quando uma rede LAN é projetada por Wi-Fi, chamamos ela de “WLAN”.

Tanenbaum (2003) explica que uma WLAN (Wireless Local Area Network), é uma tecnologia que permite a conexão de diferentes dispositivos à Internet e/ou a outras redes sem a necessidade de uma conexão física direta. A WLAN é baseada no padrão IEEE 802.11 (IEEE, 1997), e também é conhecida como Wi-Fi. Ela opera por meio de transmissores e receptores de rádio que utilizam ondas curtas para estabelecer a comunicação entre dispositivos.

O padrão 802.11 funciona em dois modos principais: com uma estação base (ponto de acesso), onde toda a comunicação passa por esse ponto, e no modo ad hoc, onde os dispositivos se comunicam diretamente entre si. Desde sua criação, a tecnologia evoluiu para oferecer velocidades

mais altas, como as dos padrões 802.11a, 802.11b e 802.11g, tornando-se uma solução essencial para a conectividade móvel e o acesso à Internet em diversos cenários (TANENBAUM, 2003).

O padrão 802.11 também define o conceito de Frames Beacon. Eles são um quadro de sinalização e sincronismo que transmite informações essenciais sobre o funcionamento de uma rede sem fio. Os Access Points (APs) são configurados para enviar esses quadros no canal em que operam, bem como nos canais adjacentes (subsequente e antecessor). A presença de Beacon Frames pode indicar a existência de Rogue Access Points, dispositivos instalados sem autorização que representam um grande risco à segurança da rede institucional, pois podem facilitar acesso não autorizado ou ataques (IEEE, 1997).

O Beacon Interval define a frequência de envio dos frames beacon pelo AP em uma WLAN. Geralmente, é 100 ms, mas pode ser ajustado. Intervalos curtos melhoram a descoberta da rede, mas consomem mais energia e largura de banda, enquanto intervalos longos economizam recursos, mas podem atrasar a conexão.

Normalmente, os frames beacon são invisíveis ao usuário. Porém, eles podem ser visualizados usando ferramentas conhecidas como sniffers de rede. Essas ferramentas capturam e analisam o tráfego de rede, permitindo a visualização dos pacotes em tempo real. As duas ferramentas de sniffing de redes mais populares são o Wireshark e o Tcpdump (GOYAL, GOYAL. 2017).

Por fim, segundo Javid (2014), muitos desses conceitos básicos do funcionamento de redes de computadores são muito difíceis de aprender de forma totalmente teórica. Nesse sentido, o software Cisco Packet Tracer é amplamente utilizado, pois facilita o aprendizado por meio da simulação de redes em ambientes acadêmicos e profissionais. Por exemplo, essa ferramenta permite criar ambientes virtuais que simulam em tempo real o funcionamento de protocolos como o IPv4, IPv6, TCP, e UDP. Com isso, o Packet Tracer oferece uma plataforma de experimentação e visualização que contribui para a compreensão dos detalhes operacionais das redes e dos pacotes de dados.

2. OBJETIVOS

A atividade prática realizada no dia 30/01/2025 teve como objetivo simular o funcionamento de uma WLAN (Wireless Local Area Network) com a ajuda do software *Cisco Packet Tracer*, e analisar um trace WireShark, com o objetivo de analisar os frames beacon, os pacotes SYN TCP, SYN SAC, e verificar a associação e dissociação do AP.

3. MATERIAL UTILIZADO

Os testes foram realizados num notebook da marca DELL, modelo Vostro 3520, com um CPU Intel Core i7-1255U 1.70 GHz, 16Gb de memória RAM DDR4, placa de vídeo integrada Intel Iris Xe Graphics, placa de vídeo dedicada NVIDIA GeForce MX550, adaptador de rede modelo Intel(R) Wi-Fi 6 AX201 160MHz, unidade de disco SSD NVMe ADATA 512Gb.

Dentro dele, foi executado o sistema operacional Windows 11 Home, versão 10.0.26100. Mais especificações da máquina estão explícitas na figura 1. Na máquina foi instalado o software *Cisco Packet Tracer*, diretamente do website oficial da Cisco, e o *WireShark*, diretamente do site oficial da ferramenta. Os testes foram feitos durante a aula prática do dia 30 de janeiro de 2025.

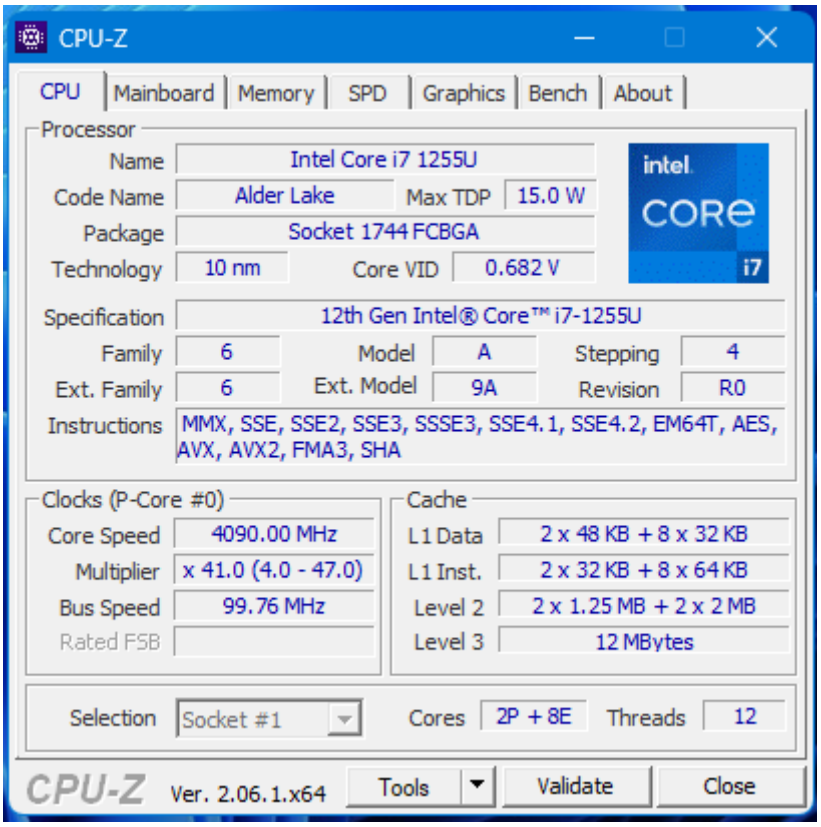

Figura 1: Especificações do sistema segundo o software *CPU-Z*.

4. METODOLOGIA

4.1 Simulação:

Usando as ferramentas do Cisco Packet Tracer, foi implementada a rede representada inicialmente na atividade. A interface Ethernet do Laptop foi então substituída por uma interface Wireless, e o IP do Laptop foi configurado por DHCP. Depois, foi incluído um roteador Wireless e um segundo laptop, conforme a figura 3.

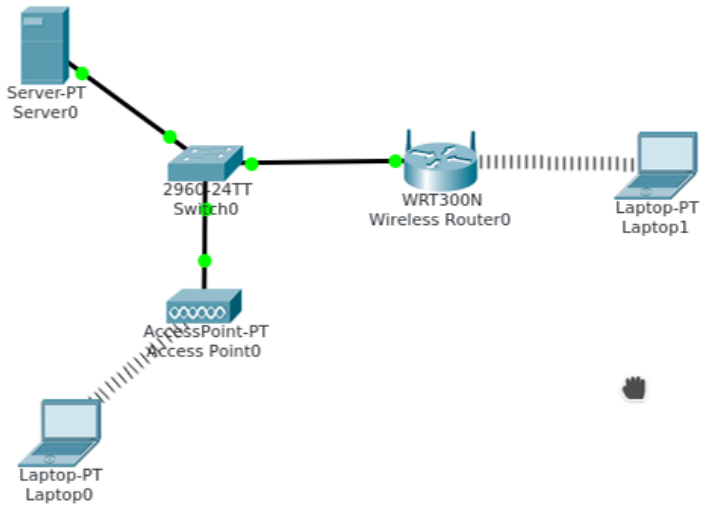

Figura 3: Rede a ser implementada na etapa.

4.2 Traces Reais:

Com o wireshark, foi aberto o trace Wireshark_802_11.pcap. Depois, o trace foi analisado, e algumas informações foram anotadas, como: O intervalo de envio dos frames beacon; O endereço MAC de origem do quadro beacon de 30 Munroe St, junto com o seu destino; os pacotes SYN TCP e SYN SACK da solicitação HTTP feita no tempo t = 24.82, junto com os endereços MAC presentes e a quem pertencem; os dois pacotes enviados pelo host quando se dissocia do AP após t = 49.0, quantos frames AUTHENTICATION são enviados após t = 49.0, e qual a taxa de dados sendo utilizada.

5. RESULTADOS E DISCUSSÃO

5.1 Simulação:

Os dispositivos foram criados, editados, ligados, e conectados com sucesso por meio de uma rede Wireless. O resultado pode ser visualizado na figura 4.

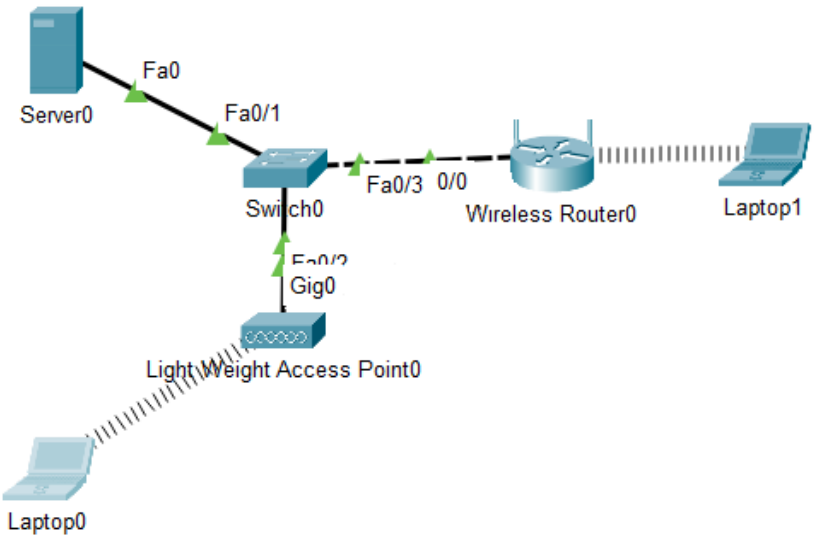

Figura 4: Rede implementada na etapa.

5.2 Traces Reais:

Após a análise do trace, obteve-se todos os valores desejados. Inicialmente, percebe-se que o beacon interval se manteve numa moda de 0,102400 segundos (Figura 5). A figura 6 também mostra os endereços de recebimento, destinação, transmissão, e origem dos frames beacon. De forma similar, também obteve-se os endereços MAC dos envolvidos na comutação do pacote SYN TCP e SYN SACK feitos em t = 24.82. Eles podem ser visualizados nas figuras 7 e 8, respectivamente.

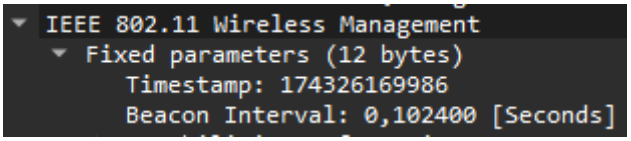

Figura 5: Beacon interval.

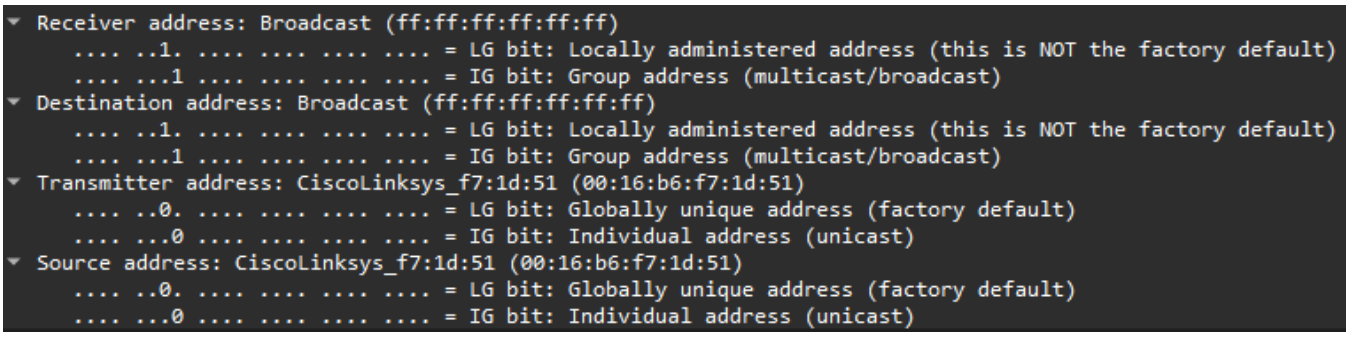

Figura 6: Endereços MAC relacionados aos frames beacon.

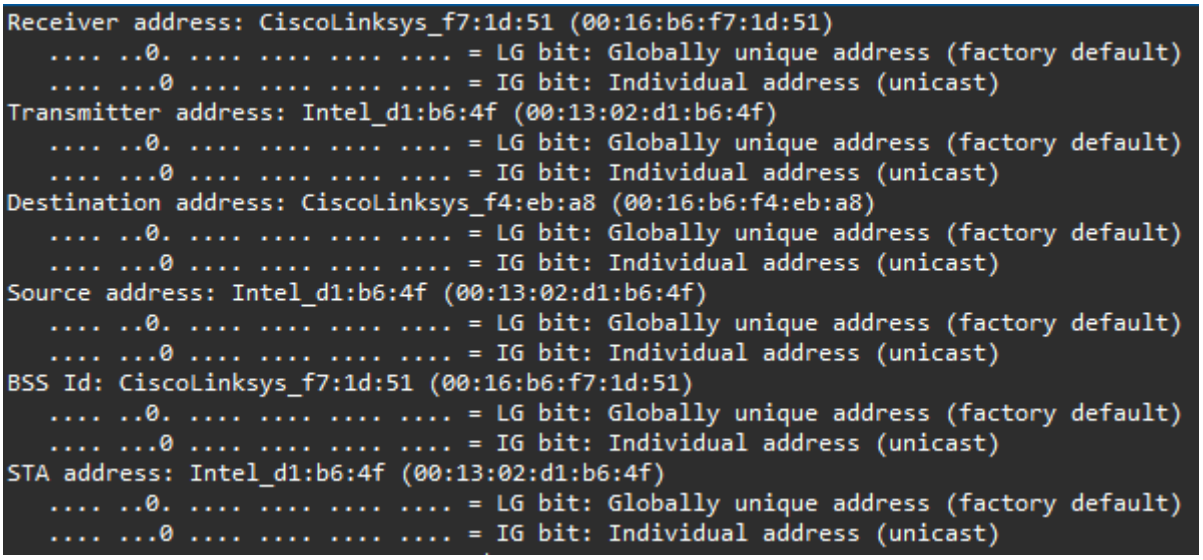

Figura 7: Endereços MAC relacionados ao pacote SYN TCP.

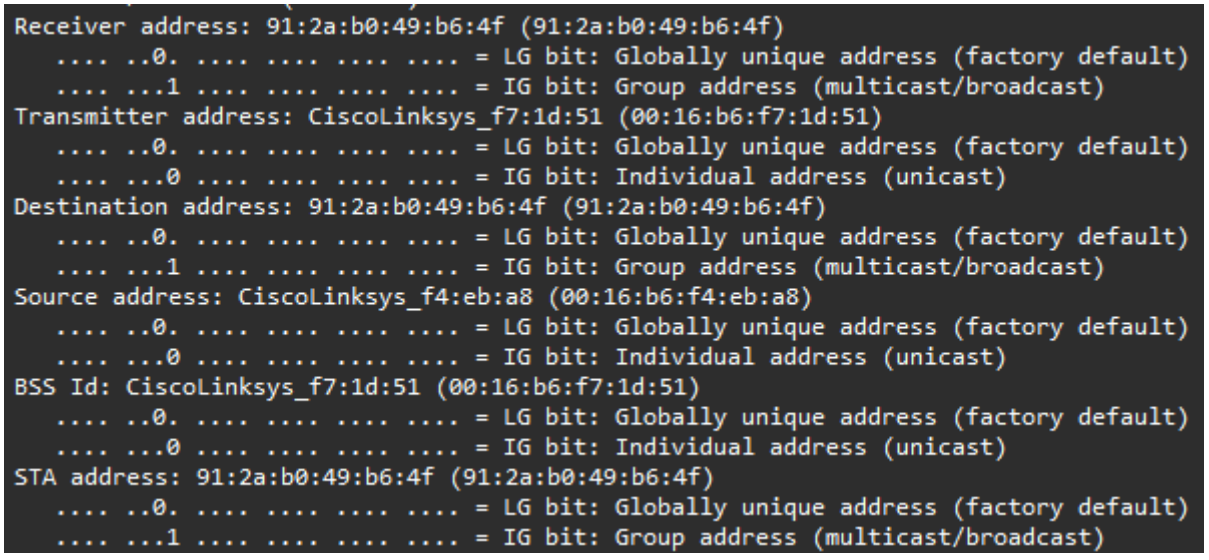

Figura 8: Endereços MAC relacionados ao pacote SYN SACK.

Após se dissociar do AP em t = 49.0, o host envia dois pacotes TCP, mostrados na figura 9. Após este instante, são enviados 19 frames AUTHENTICATION (Figura 10). Também constata-se que, logo após o instante t = 49.0, a taxa de dados utilizada foi de 24,0 Mb/s (Figura 11).

1714	49.020356	128.119.101.5	192.168.1.109	TCP	108 80 → 2543 [SYN, PSH, ECE, AE] Seq=0 Win=7504[Malformed Packet]
1715	49.020948	192.168.1.109	128.119.101.5	TCP	102 2543 → 80 [ACK] Seq=1 Ack=1 Win=16132 Len=0

Figura 9: Pacotes enviados pelo host quando se desassocia do AP após o tempo t = 49.0.

1740	49.638857	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1606, FN=0, Flags=........C
1741	49.639700	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1612, FN=0, Flags=........C
1822	53.787070	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1619, FN=0, Flags=........C
1922	57.890325	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1644, FN=0, Flags=........C
2123	62.172946	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	Intel_d1:b6:…	CiscoLinksys_f5:ba:…	802.11	58 Authentication, SN=1644, FN=0, Flags=....R...C
2156	63.168087	Intel_d1:b6:…	CiscoLinksys_f7:1d:…	802.11	58 Authentication, SN=1647, FN=0, Flags=........C
2158	63.169071	CiscoLinksys…	Intel_d1:b6:4f	802.11	58 Authentication, SN=3726, FN=0, Flags=........C
2160	63.169707	Intel_d1:b6:…	CiscoLinksys_f7:1d:…	802.11	58 Authentication, SN=1647, FN=0, Flags=....R...C
2164	63.170692	CiscoLinksys…	Intel_d1:b6:4f	802.11	58 Authentication, SN=3727, FN=0, Flags=........C

Figura 10: Frames AUTHENTICATION enviados após o tempo t = 49.0.

Figura 11: Taxa de dados logo após o instante t = 49.0.

6. CONCLUSÕES

A aula prática proporcionou uma boa compreensão sobre a parte prática da implementação e funcionamento de WLANs, e ajudou na visualização dos protocolos envolvidos no processo. O uso do Packet Tracer se mostrou útil para ajudar no entendimento da parte física do processo, enquanto a análise dos traces com o Wireshark foi essencial para entender mais a troca e estruturação dos pacotes comutados.

Conclui-se, portanto, que a prática foi bem-sucedida em atingir seus objetivos, consolidando o entendimento sobre WLAN, e mostrando que o *Cisco Packet Tracer* e o *Wireshark* de fato são duas ótimas ferramentas para ajudar na visualização do funcionamento de diferentes aspectos do funcionamento das redes de computadores.

BIBLIOGRAFIA

CAMPISTA, Miguel Elias M. et al. Interconexão de Redes na Internet do Futuro: Desafios e Soluções. **Minicursos do Simpósio Brasileiro de Redes de Computadores-SBRC**, v. 2010, p. 47-101, 2010.

CHANDRA, Deka Ganesh; KATHING, Margaret; KUMAR, Das Prashanta. A comparative study on IPv4 and IPv6. In: **2013 International Conference on Communication Systems and Network Technologies**. IEEE, 2013. p. 286-289.

CORONA, Adrián Estrada. *et al*. **Protocolos TCP/IP de internet**. 2004.

GOYAL, Piyush; GOYAL, Anurag. Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark. In: **2017 9th International Conference on Computational Intelligence and Communication Networks (CICN)**. IEEE, 2017. p. 77-81.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE 802.11:** Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. New York: IEEE, 1997.

LEINER, Barry M. et al. **A brief history of the Internet**. ACM SIGCOMM computer communication review, v. 39, n. 5, p. 22-31, 2009.

MONTEIRO, Luís. **A internet como meio de comunicação: possibilidades e limitações**. In: Congresso Brasileiro de Comunicação. sn, 2001.

ROSS, Julio. **Redes de computadores**. Julio Ross, 2008.

TANENBAUM, Andrew S. **Redes de Computadores**, 7ª Edição, Editora Campus, Rio de Janeiro – RJ, 2003.