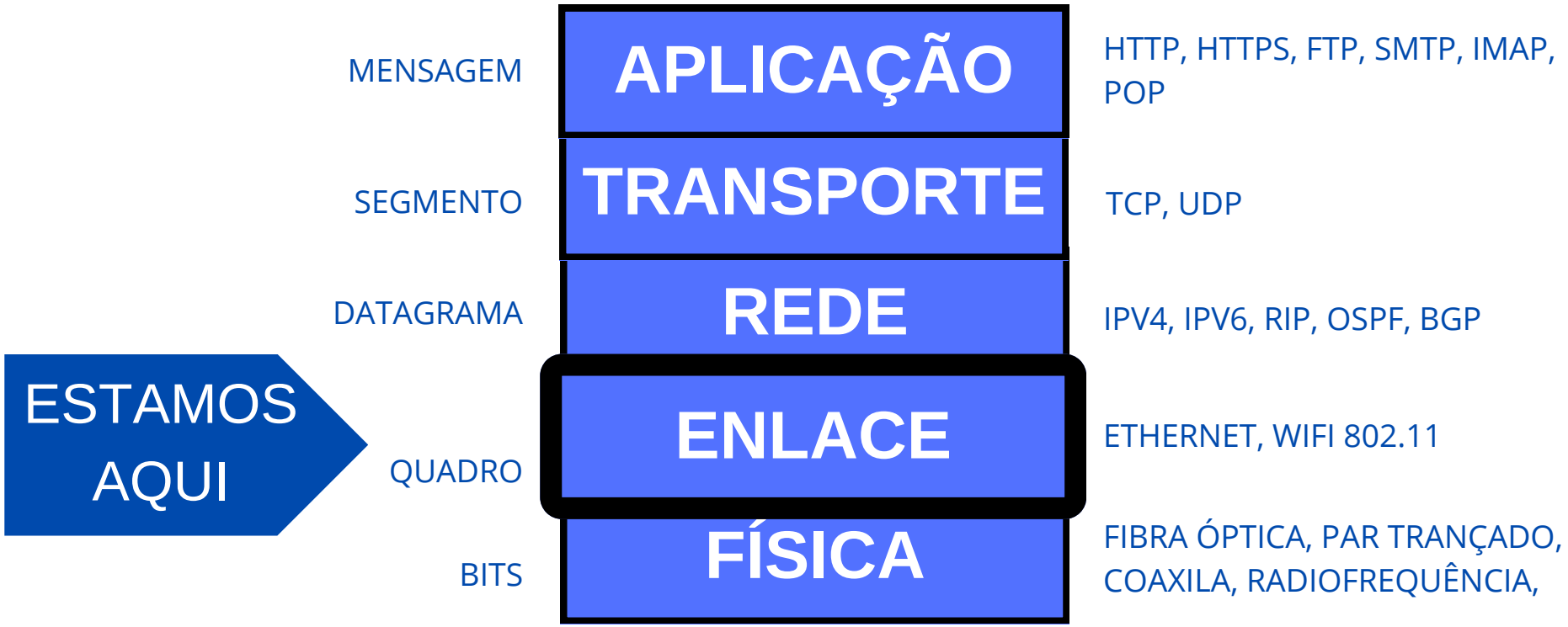
Redes de Computadores

Marisangila Alves, MSc

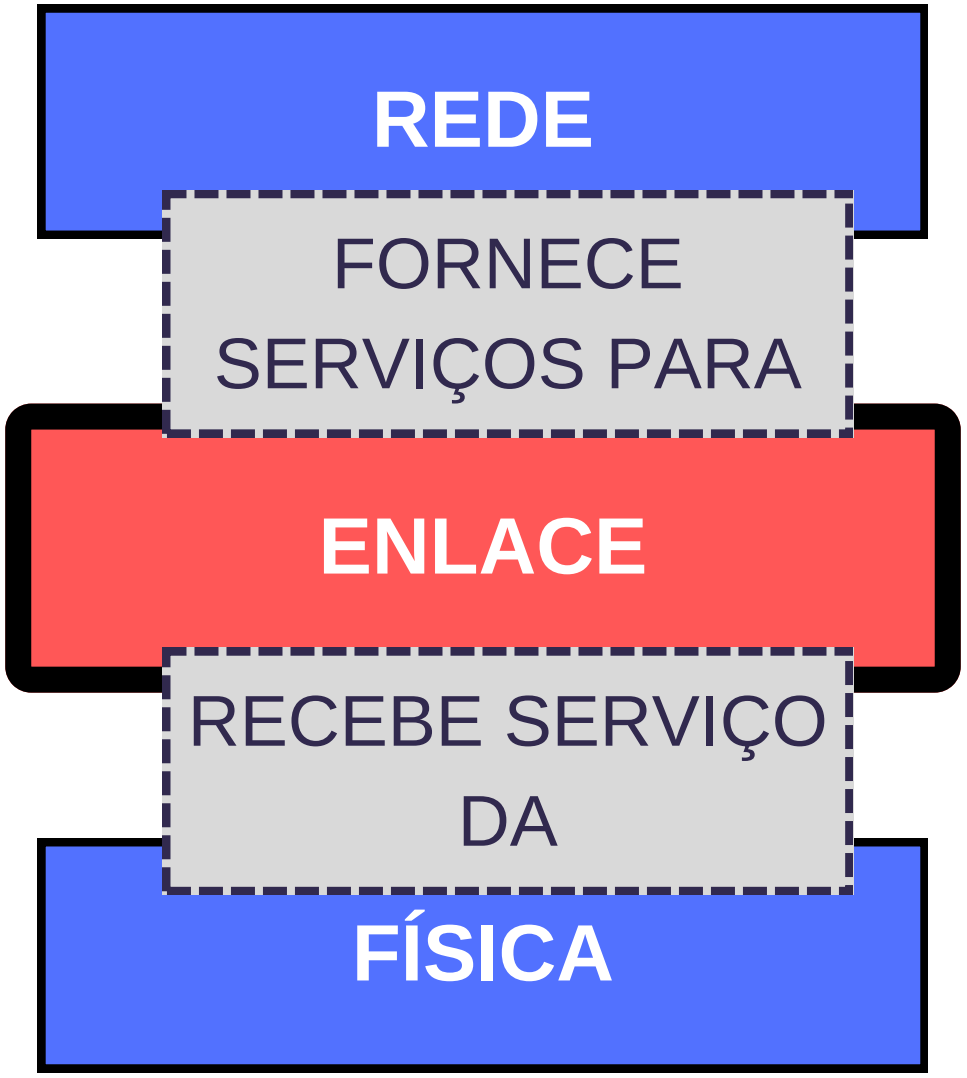
marisangila.alves@proton.me

Camada de Enlace

Camada de Enlace



Camada de Enlace



Camada de Enlace

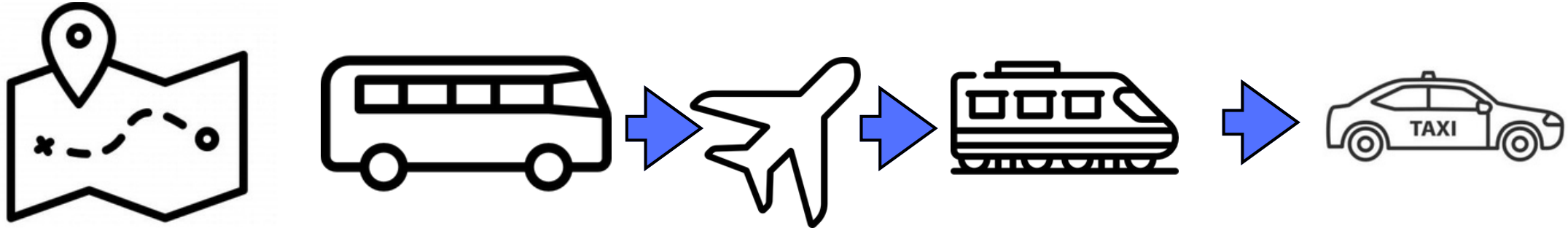
A camada de enlace é responsável pela entrega de quadros para hospedeiros em uma rede local.

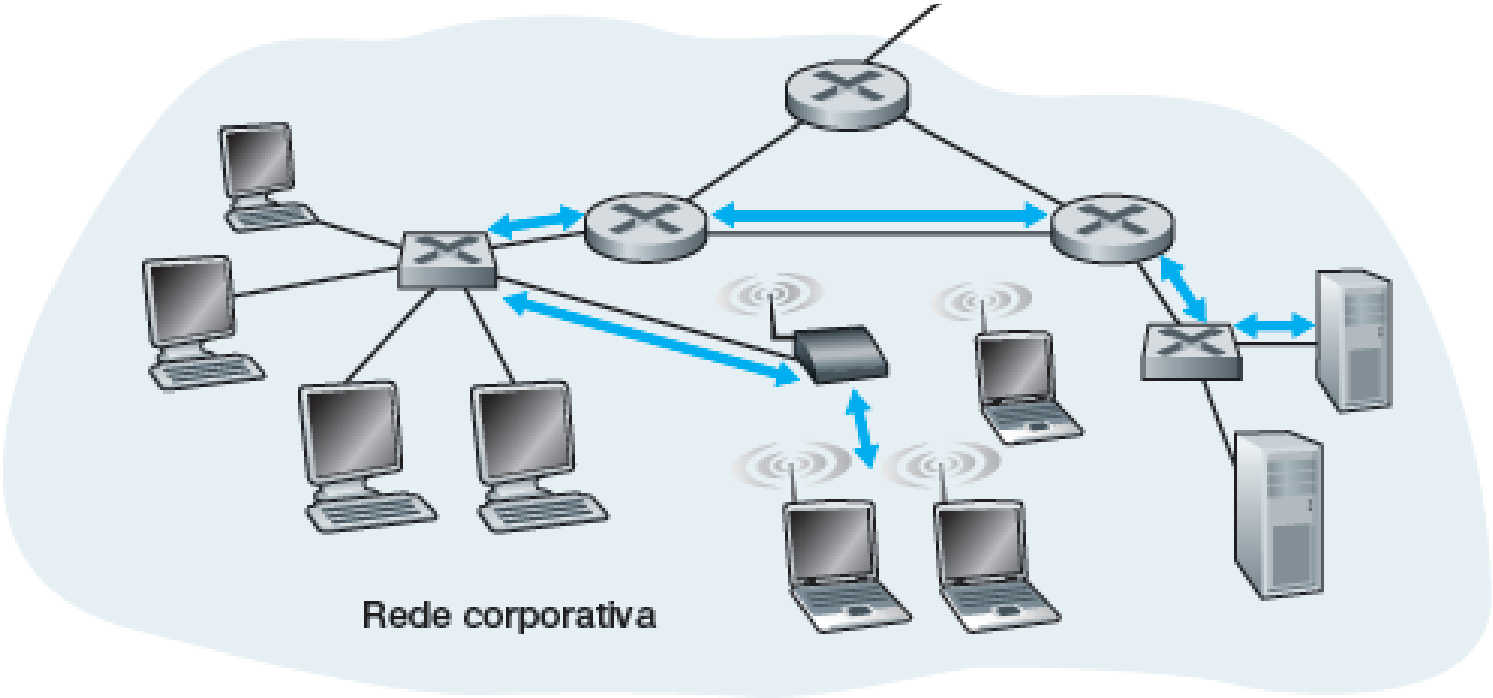
Camada de Enlace

O serviço básico de qualquer camada de enlace é mover um datagrama de um nó até um nó adjacente por um único enlace de comunicação.

Camada de Enlace

Analogia:

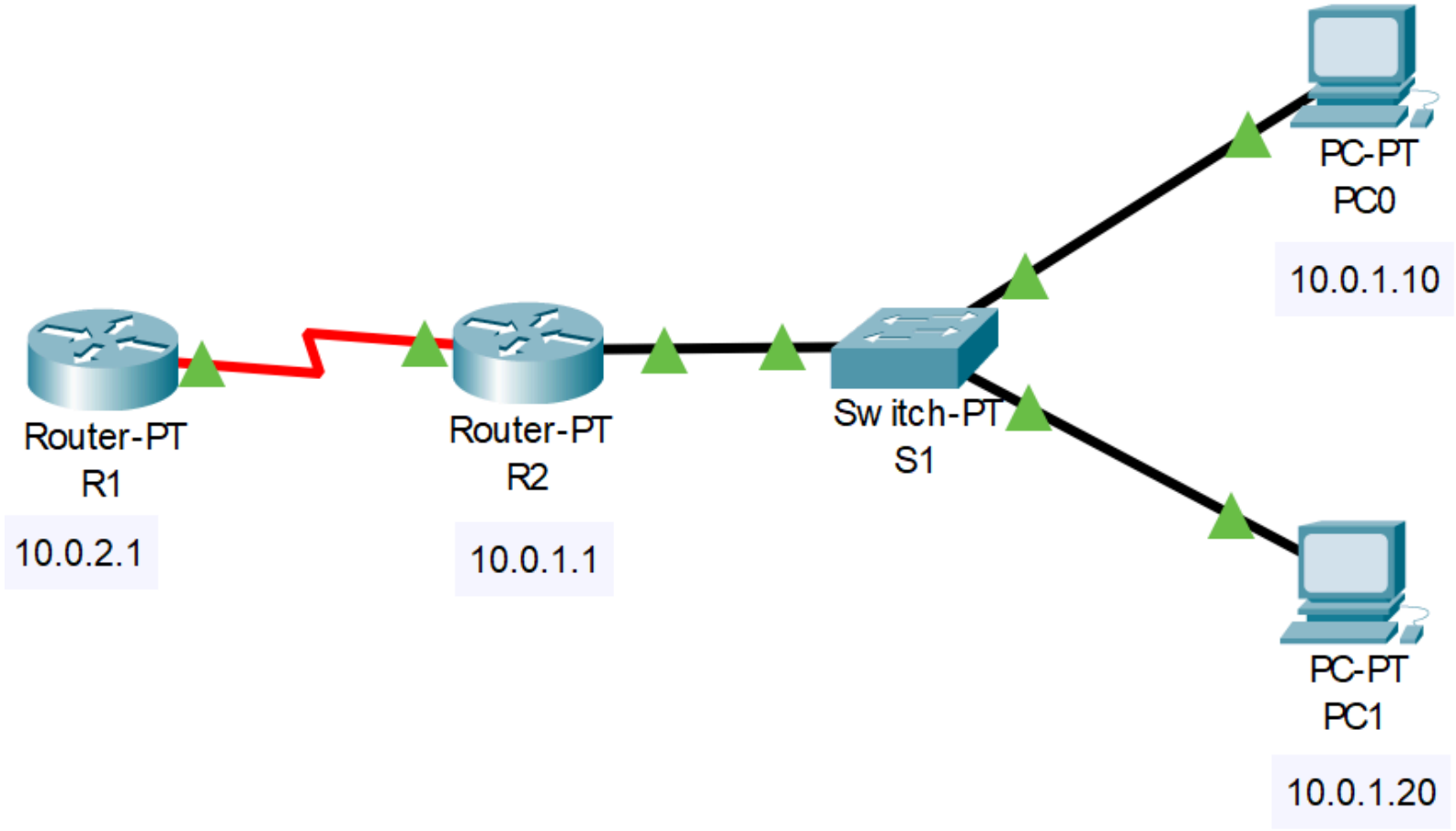




Fonte: Kurose, 2014.

Camada de Enlace

O roteador trabalha na camada de rede, portanto está interressado apenas no IP. Por outro lado, o switch precisa realizar o controle de acesso ao meio (enlace)



Camada de Enlace

Onde a camada de enlace é implementada?

NIC (Placa de interface de rede)

Camada de Enlace

Equipamentos de rede que atuam exclusivamente na camada de enlace:

Switches: Conectam vários dispositivos dentro de uma mesma rede local (LAN) e encaminham quadros com base em endereços MAC. *(Há switches de camada de rede)*

Pontes (Bridges): Conectam e filtram tráfego entre diferentes segmentos de uma rede local, ajudando a dividir grandes redes em segmentos menores.

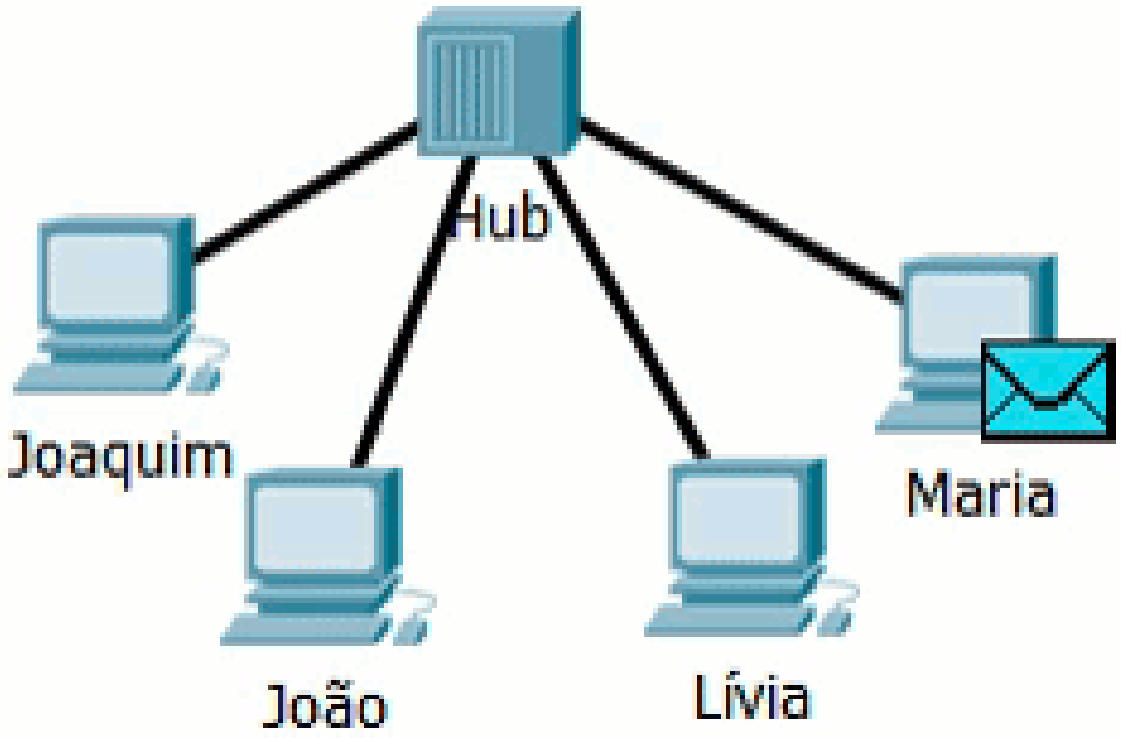
Adaptadores de Rede: Placas de interface que conectam um computador ou outro dispositivo à rede local e gerenciam a comunicação na camada de enlace.

Comutador vs Roteador

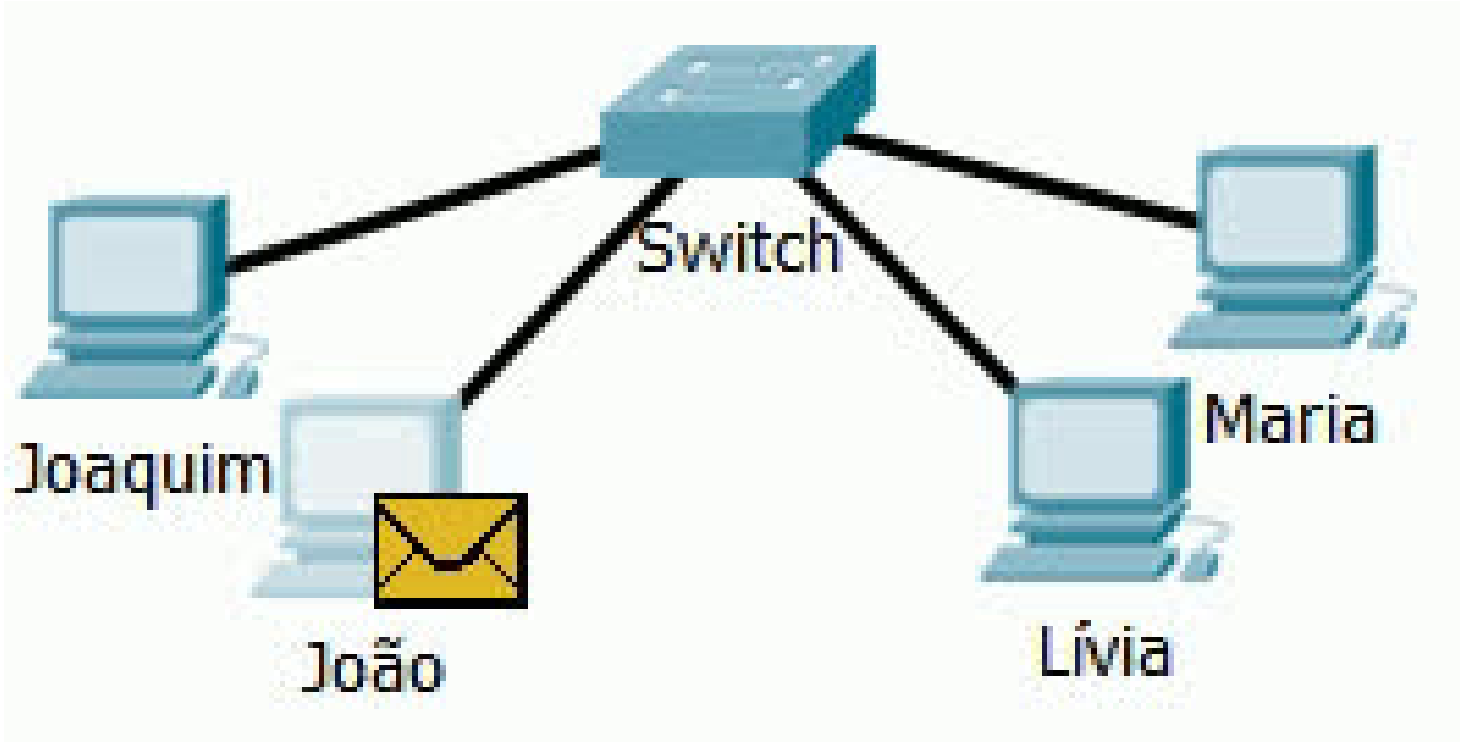
Roteadores são comutadores de pacotes do tipo armazena-e-repassa, que transmitem pacotes usando endereços da camada de rede (IP). Um comutador usa endereços da camada de enlace (MAC).

Enquanto um roteador é um comutador de pacotes da camada 3, um comutador opera com protocolos da camada 2.

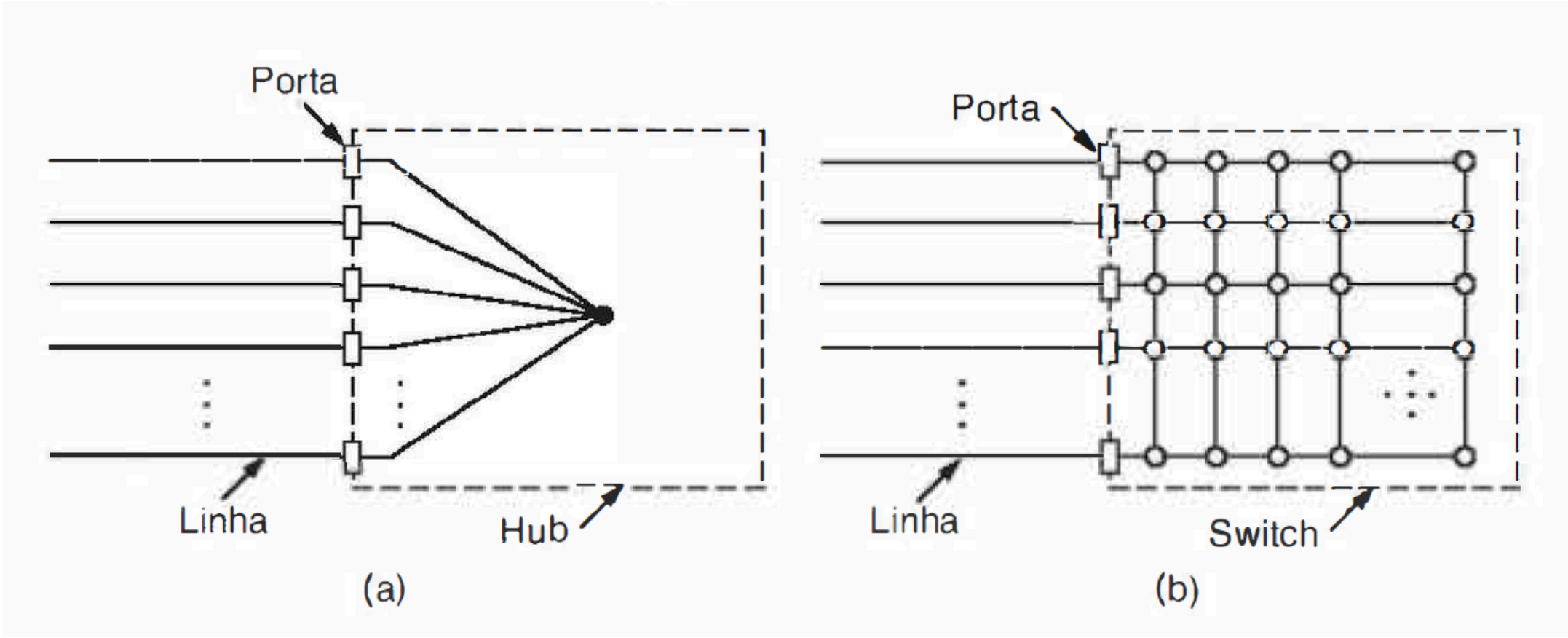
HUB *(Camada Física)*



Switch



Hub vs Switch



Fonte: Tanenbaum, 2011.

Switch

Bridges

- Um bridge conecta dois segmentos de rede, permitindo que dispositivos em diferentes segmentos se comportem como se estivessem na mesma LAN.
- Se você conectar dois switches usando um bridge, isso efetivamente cria uma única rede local estendida.
- Os dispositivos conectados aos dois switches poderão se comunicar entre si como se estivessem na mesma rede.

O que temos em nossas casas?

Modem (Transceptor) + Switch + Access Point + Roteador

Física - Enlace - Rede

O que temos em nossas casas?

Modem (Transceptor) + Switch + Access Point + Roteador

Física - Enlace - Rede

Hub vs Switch

Hub:

Desvantagens:

1. Um hub é um repetidor multiportas então não é interessante seu uso pois não trabalha na camada de enlace.
2. Domínio de colisão: aumenta as chances de colisão pois encaminha os bits a todas as portas, gerando um alto tráfego na rede.
3. Os hubs são vulneráveis a ataques de segurança, pois não têm recursos de segurança.

Vantagens:

1. Hubs são dispositivos simples e baratos;
2. Eles são fáceis de instalar e configurar;
3. Os hubs são capazes de conectar vários dispositivos em uma rede sem a necessidade de configuração.

Hub vs Switch

Switch:

Desvantagens:

1. Switches são mais caros e complexos do que hubs;
2. Eles podem exigir mais configuração e manutenção do que os hubs;
3. Em algumas situações, um switch pode ser excessivamente complexo para as necessidades da rede.

Vantagens:

1. Switches são mais eficientes do que hubs, pois enviam os dados apenas para os dispositivos que precisam deles, economizando largura de banda e melhorando o desempenho da rede;
2. A largura de banda total de uma rede com switch é dedicada a cada dispositivo conectado, o que melhora o desempenho da rede;
3. Os switches têm recursos de segurança, como VLANs, que permitem separar a rede em segmentos isolados para melhorar a segurança.
4. O switch por outro lado, atua na camada de enlace de dados segmentando domínios de broadcast.

Serviços fornecidos pela camada de enlace

REDE

FORNECE SERVIÇOS PARA

DETECÇÃO DE ERROS

CONTROLE DE ACESSO AO MEIO

ENLACE

ENQUADRAMENTO

ENDEREÇAMENTO

RECEBE SERVIÇO DA

FÍSICA

Camada de Enlace

- Funções:
  - Enquadramento de dados;
  - Acesso ao meio;
  - Entrega confiável;
  - Detecção de erros.

Enquadramento

REDE

FORNECE SERVIÇOS PARA

DETECÇÃO DE ERROS

ENQUADRAMENTO

ACE

CONTROLE DE ACESSO AO MEIO

ENDEREÇAMENTO

RECEBE SERVIÇO DA

FÍSICA

Camada de Enlace

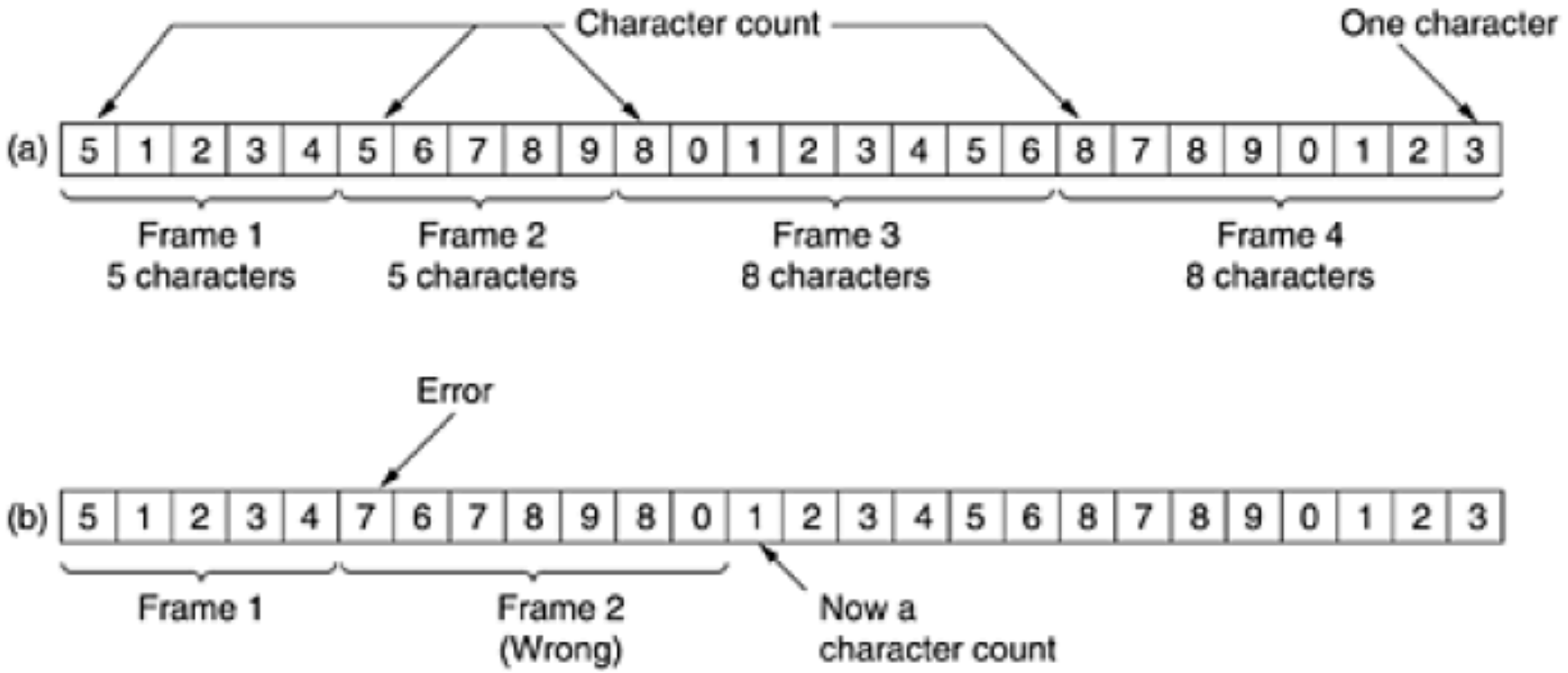
Camada de Enlace

O enquadramento na camada de enlace é o processo de organizar dados em pacotes ou quadros para garantir a transmissão eficiente e a detecção de erros na comunicação de rede.

- O enquadramento pode ser realizado das seguintes formas:
  - Intervalo de tempo;
  - Contagem de caracteres;
  - Bytes de flags, com inserção de bytes;
  - Flags iniciais e finais, com inserção de bits; ou
  - Violações de codificação da camada física.

Camada de Enlace

- Contagem de caracteres;



Fonte: Tanenbaum, 2011.

Detecção de Erros

REDE

FORNECE SERVIÇOS PARA

DETECÇÃO DE ERROS

CONTROLE DE ACESSO AO MEIO

ENDEREÇAMENTO

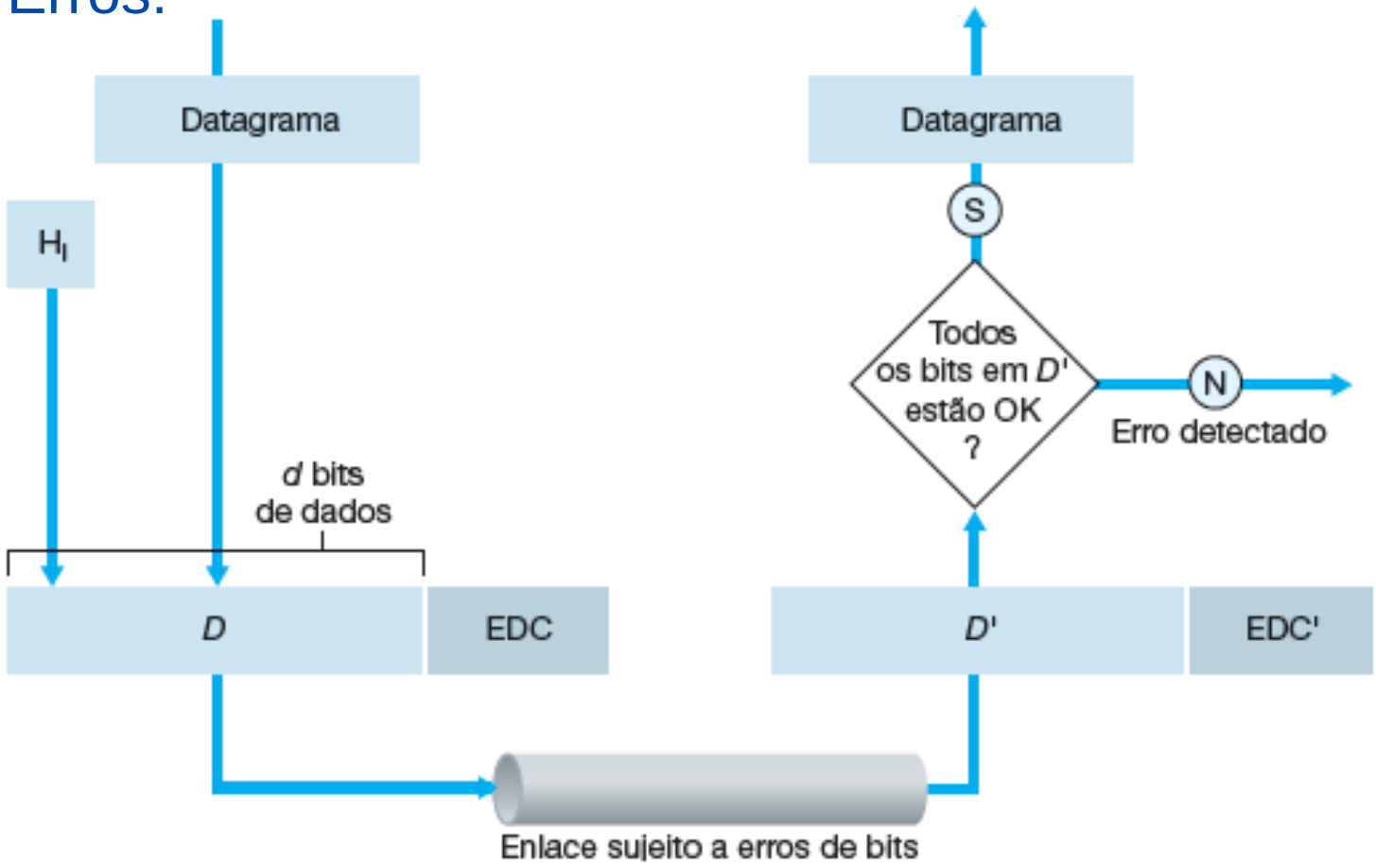
ENQUADRAMENTO

RECEBE SERVIÇO DA

FÍSICA

Camada de Enlace

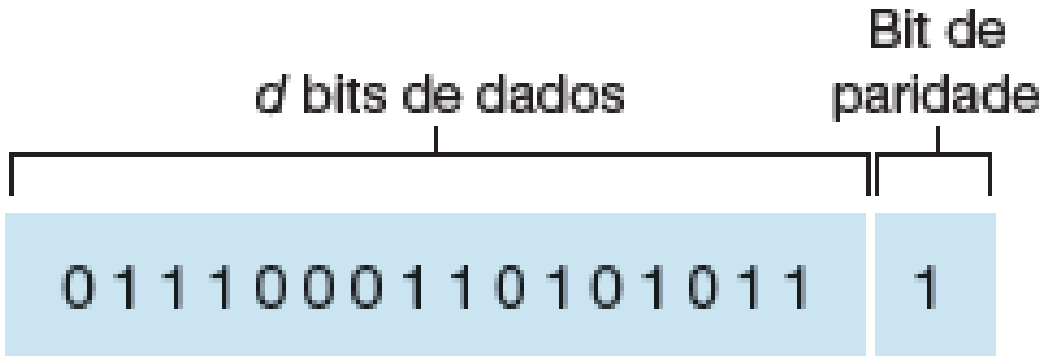
Detecção de Erros:



Fonte: Kurose, 2014.

Camada de Enlace

- Detecção de Erros:
  - Verificações de Paridade:
    - O sistema de detecção de erros de paridade de bits adiciona um bit extra a um conjunto de dados para verificar se o número total de bits "1" é par ou ímpar, ajudando a identificar erros simples de transmissão.



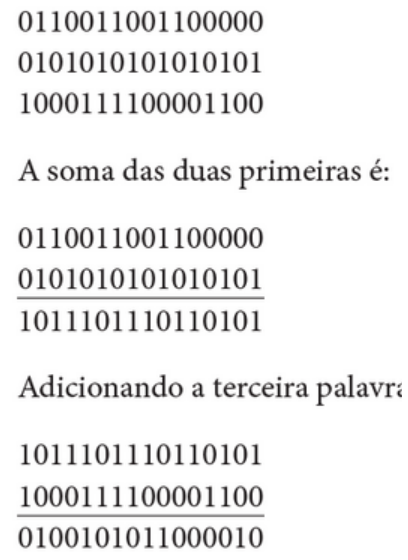
Fonte: Kurose, 2014.

Camada de Enlace

- Detecção de Erros:
  - **Verificações de Paridade:**
    - Problema:
      - Se ocorrer um número par de erros de bit, um sistema de paridade de bits pode não detectar esses erros;
      - Erros frequentemente se agrupam em “rajadas” de erros;
      - A probabilidade de falhas na detecção pode ser alta, chegando perto de 50% (Spragins, 1991).

Camada de Enlace

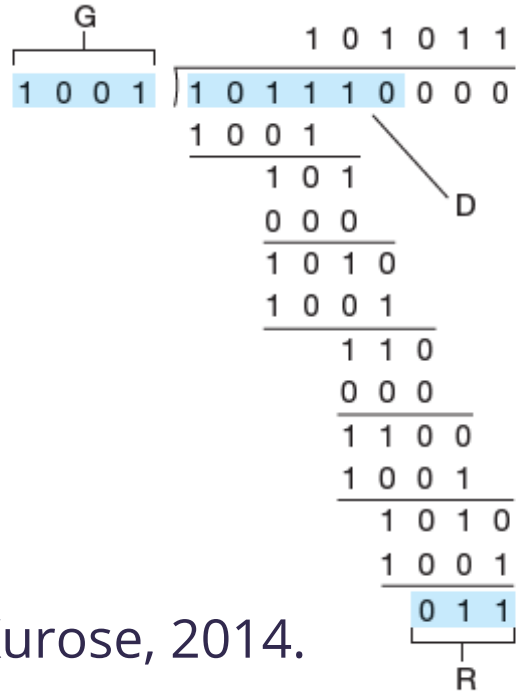
- Detecção de Erros:
  - **Soma de verificação:**
    - Calcula a soma dos dados em um pacote e adiciona esse valor ao pacote.
    - Quando os dados são recebidos, o mesmo cálculo é feito para verificar se o resultado corresponde ao valor original.



Fonte: Kurose, 2014.

Camada de Enlace

- Detecção de Erros:
  - **Verificação de redundância cíclica - CRC:**
    - O CRC verifica se o resto da divisão binária dos dados e do código gerador é zero, permitindo a detecção de erros de transmissão comuns.



Fonte: Kurose, 2014.

Camada de Enlace

- Detecção de Erros:
  - **Verificação de redundância cíclica - CRC:**
  - **Exemplo**:
    - **Dados Originais:** Imagine que você tem um dado simples, como o número binário 1011.
    - Cálculo do CRC:
      - Primeiro, você define um polinômio gerador (por exemplo, 1101).
      - Em seguida, você adiciona zeros ao final do dado para preparar para o cálculo (se o polinômio é de 4 bits, adicione 3 zeros ao final dos dados: 1011 000).
      - Você faz uma divisão binária (semântica) entre o dado estendido e o polinômio gerador, obtendo um resto. Suponha que o resto é 011.
    - Criação do Código CRC:
      - O código CRC (resto) é anexado ao final dos dados originais. Assim, o dado com o CRC seria 1011 011.

Camada de Enlace

- Detecção de Erros:
  - **Verificação de redundância cíclica - CRC:**
  - **Exemplo**:
    - Transmissão:
    - O dado 1011 011 é enviado para o destinatário.

Camada de Enlace

- Detecção de Erros:
  - **Verificação de redundância cíclica - CRC:**
  - **Exemplo**:
    - Verificação:
    - O destinatário realiza o mesmo cálculo usando o polinômio gerador e o dado recebido (1011 011).
    - Se o resto da divisão for zero, isso indica que os dados chegaram corretamente. Caso contrário, um erro foi detectado.

Protocolos de Acesso ao meio

REDE

FORNECE SERVIÇOS PARA

CONTROLE DE ACESSO AO MEIO

DETECÇÃO DE ERROS

ENLACE

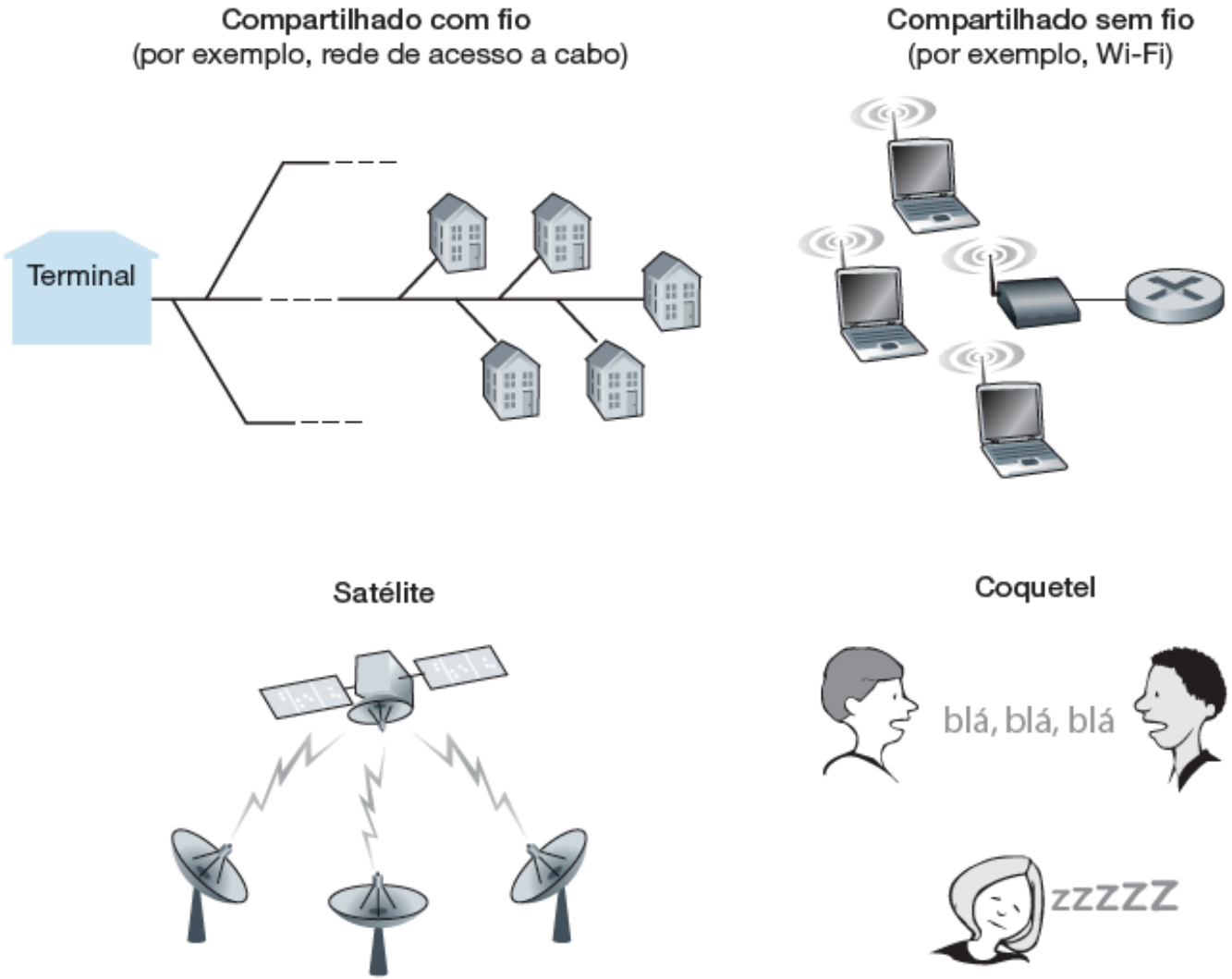
ENQUADRAMENTO

ENDEREÇAMENTO

RECEBE SERVIÇO DA

FÍSICA

Canais de Acesso múltiplo



Fonte: Kurose, 2014.

Enlaces e Protocolos de Acesso Múltiplo

Os protocolos de acesso ao meio são como semáforos!

Enlaces e Protocolos de Acesso Múltiplo

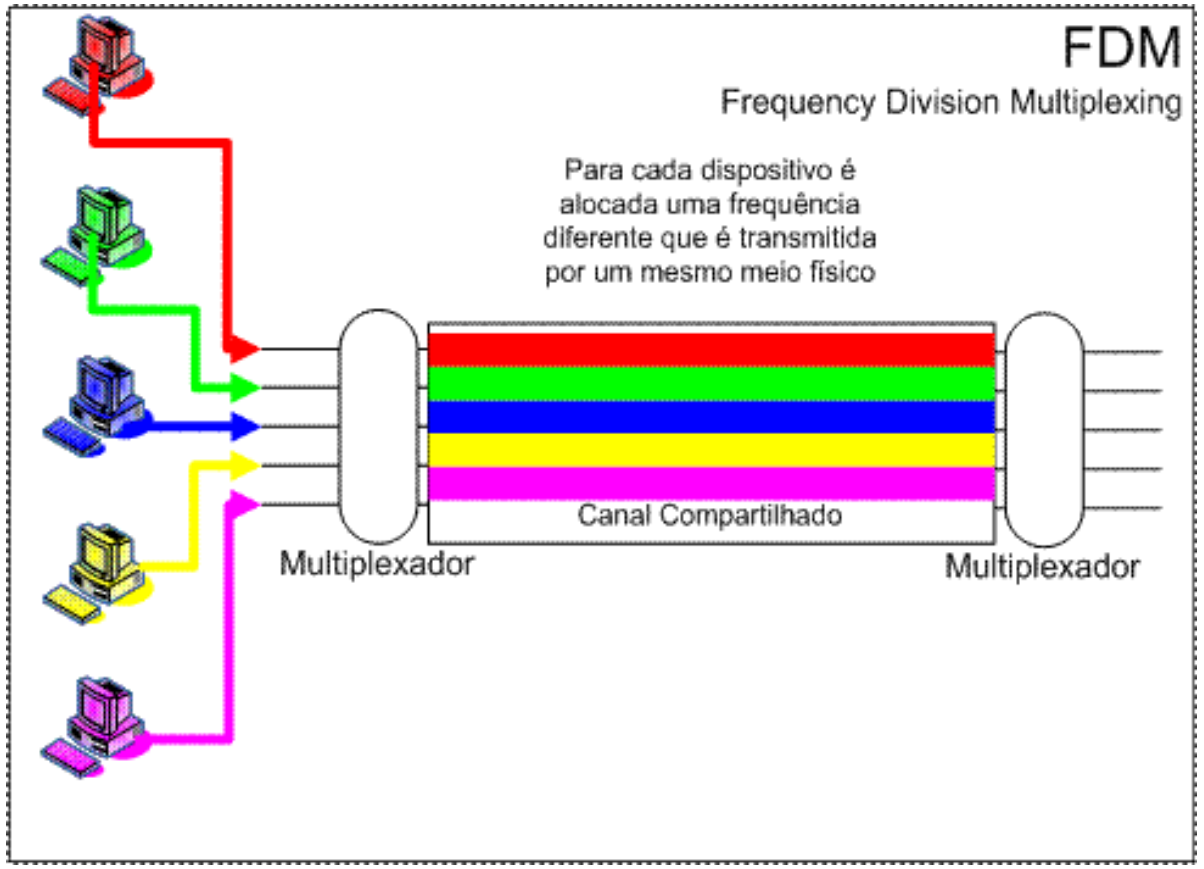
Os nós regulam sua transmissão pelos canais de difusão compartilhados.

Analogia:

- “De a todos uma oportunidade de falar.”
- “Não fale até que alguém fale com você.”
- “Não monopolize a conversa.””
- Levante a mão se tiver uma pergunta a fazer.”
- “Não interrompa uma pessoa quando ela estiver falando.”
- Não durma quando alguém estiver falando.”

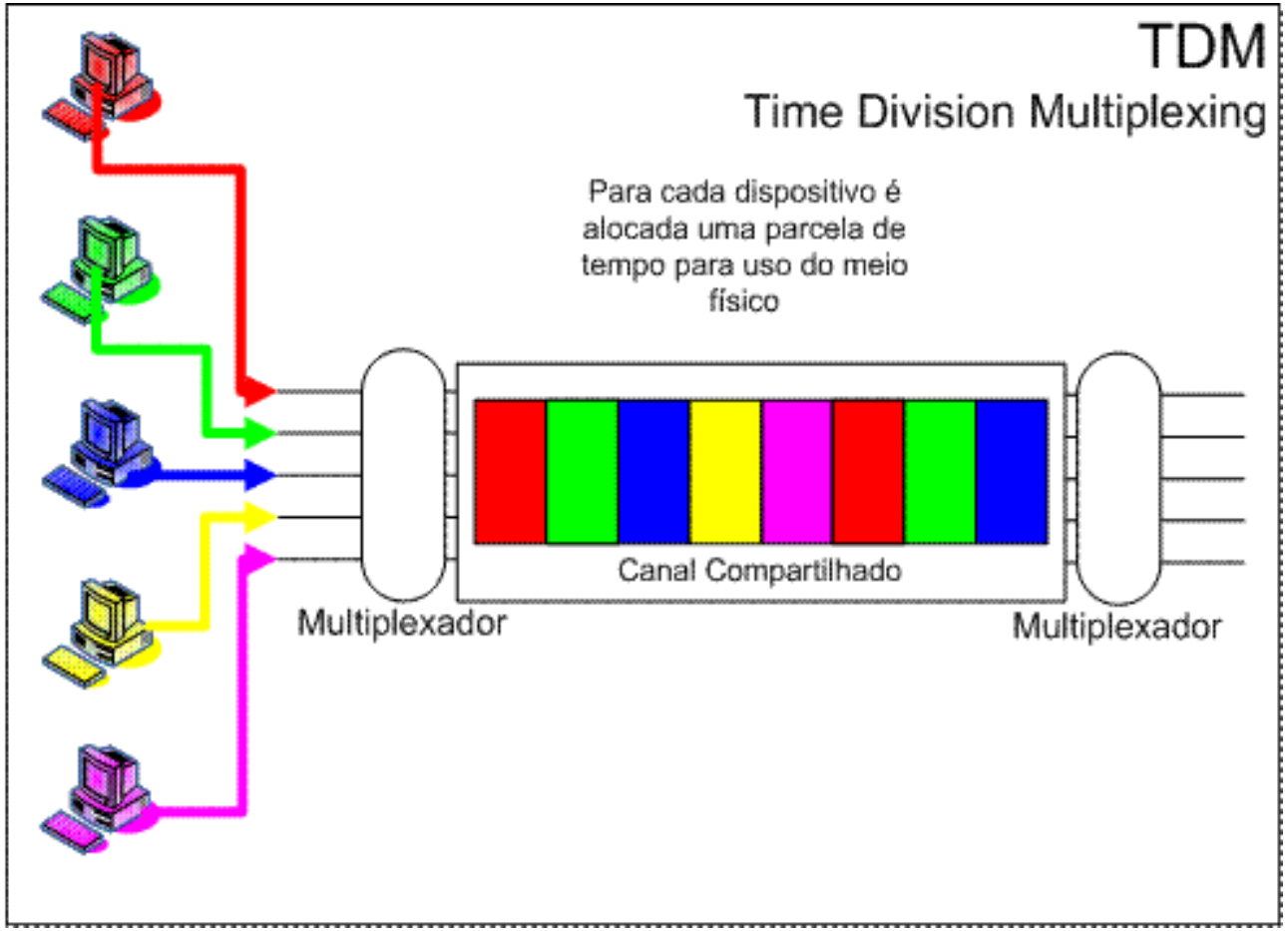
FDM (*Frequency-Division Multiple*)

Na divisão por frequência, o espectro de rádio é dividido em diferentes bandas de frequência, permitindo que várias transmissões ocorram simultaneamente em diferentes canais.



TDM (*Time Division Multiple Access)*

Na divisão por tempo, o tempo é dividido em intervalos ou *slots*, e cada usuário transmite apenas em seu intervalo designado, evitando sobreposição de sinais.



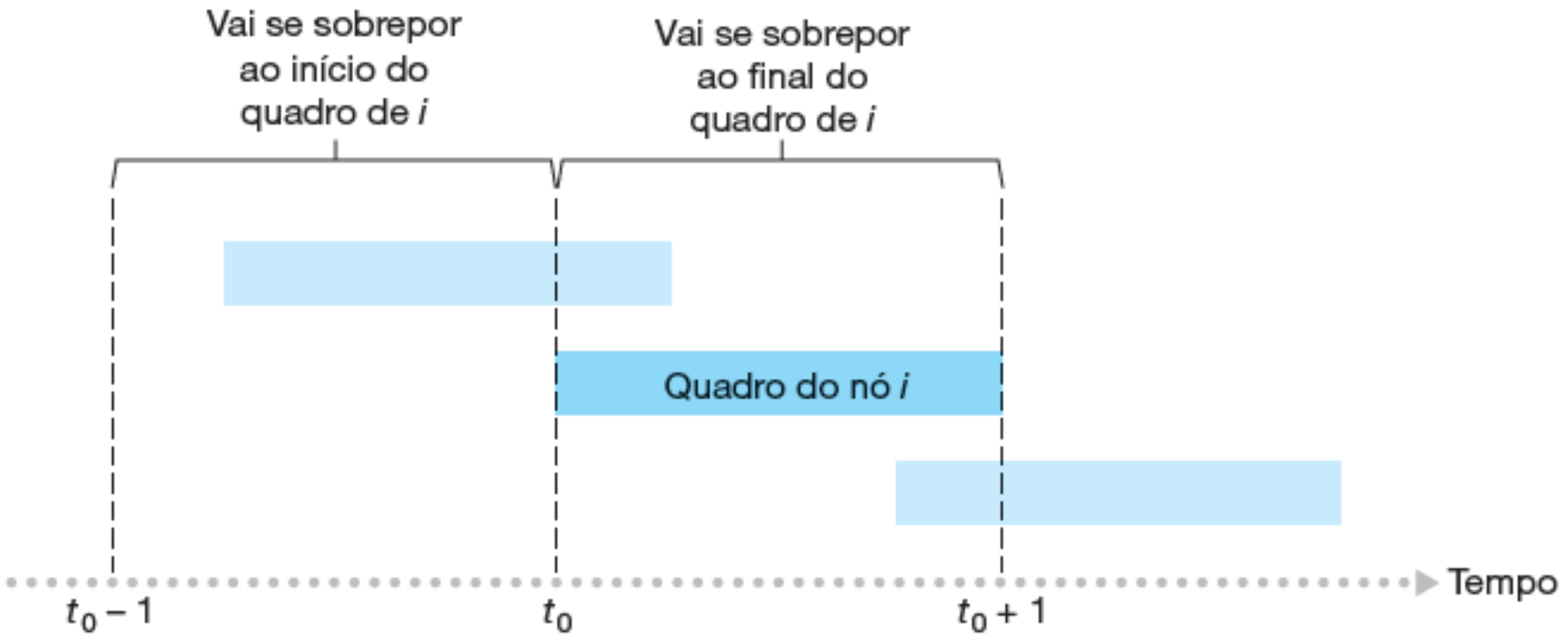
Aloha (Puro)

- É um método simples de controle de acesso ao meio em redes de comunicação, onde as estações transmitem dados sem coordenação prévia.

- Se uma colisão ocorre (ou seja, duas estações transmitem ao mesmo tempo), cada estação espera um intervalo de tempo aleatório antes de tentar retransmitir.

- Após o envio do frame o host deve aguardar 2xT, onde T é o tempo máximo de propagação.

Aloha (Puro)



Fonte: Kurose, 2014.

Aloha Puro

- **Analogia:**
  - O protocolo Aloha Puro é como um grupo de pessoas tentando falar ao mesmo tempo em uma sala sem se coordenar.

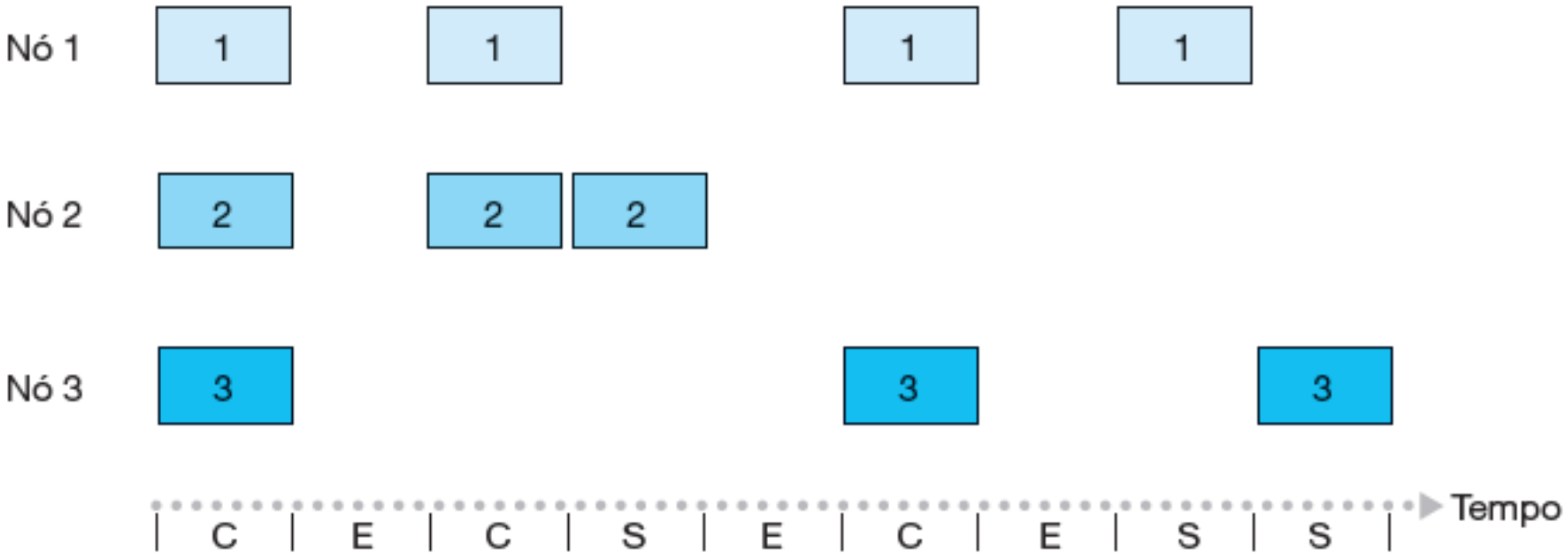
  - Se duas pessoas falam ao mesmo tempo, ninguém entende nada, então cada pessoa espera um tempo aleatório e tenta falar novamente.

  - É uma forma simples de evitar que todos falem de uma vez e causem confusão.

Aloha *Slotted*

- É uma versão mais organizada do Aloha Puro.
- O tempo é dividido em intervalos fixos, chamados de "slots".
- As estações só podem começar a transmitir no início de um *slot* de tempo, reduzindo a chance de colisões.
- Se duas estações tentarem transmitir no mesmo *slot*, elas ainda colidem, mas o sistema é mais eficiente porque o tempo de tentativa é mais previsível.

Aloha *Slotted*



Legenda:

C = Intervalo de colisão
E = Intervalo vazio
S = Intervalo bem-sucedido

Fonte: Kurose, 2014.

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

- Os dispositivos escutam o meio para detectar se outro dispositivo está transmitindo e, se não houver tráfego, eles transmitem seus próprios dados.

- Se ocorrer uma colisão (dois dispositivos transmitindo ao mesmo tempo), eles detectam a colisão e aguardam um período de tempo antes de tentar novamente.

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

O CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) é um protocolo que evita colisões em redes sem fio verificando se o meio está livre antes de transmitir e usando sinais de controle como **RTS/CTS** para coordenar o acesso ao canal.

Isso é essencial em redes sem fio onde a detecção direta de colisões é difícil devido à propagação e interferência do sinal.

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

- RTS/CTS (*Request to Send/Clear to Send*) é um mecanismo de controle usado em redes sem fio para minimizar colisões, onde um dispositivo solicita permissão para transmitir e o receptor responde, indicando que o canal está claro para a transmissão.

- O gerenciamento é feito pelo ponto de acesso (AP)

CSMA

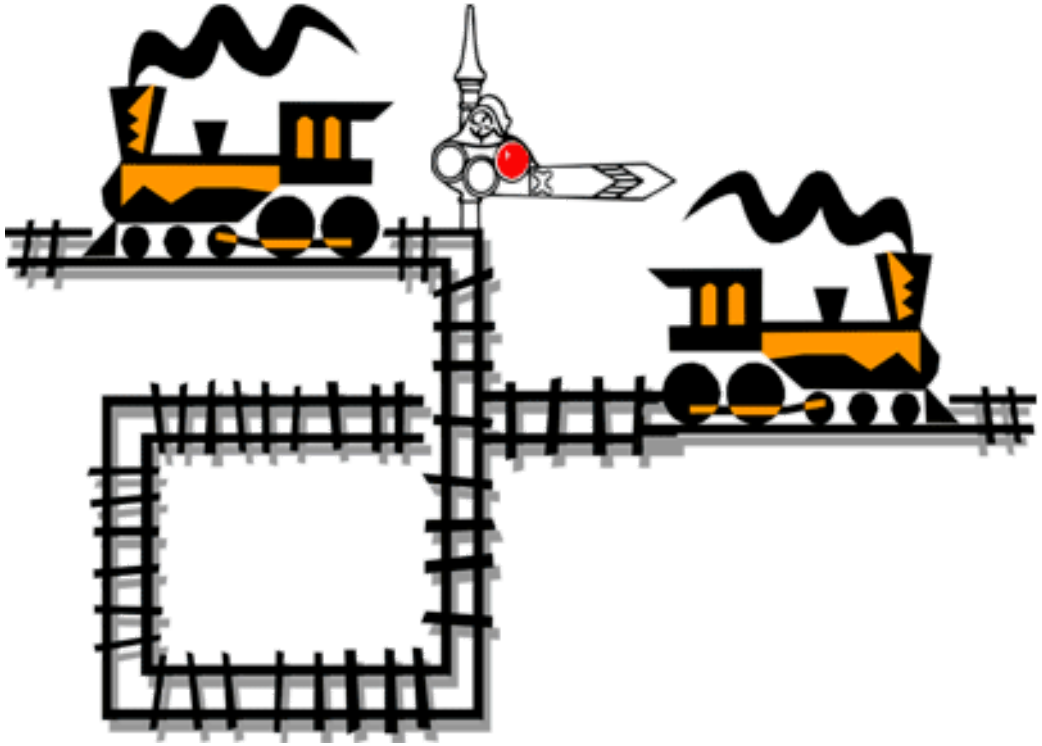
- **CSMA/CD (Ethernet).**
- **CSMA/CA (Wi-Fi):**
  - CSMA/CA é usado para Wi-Fi em vez de CSMA/CD porque o CSMA/CA evita colisões antes que ocorram, o que é crucial em redes sem fio onde a detecção direta de colisões é difícil e o meio é compartilhado de forma imprevisível.

Comunicação

- **Simplex**: Comunicação unidirecional onde os dados fluem em uma única direção.

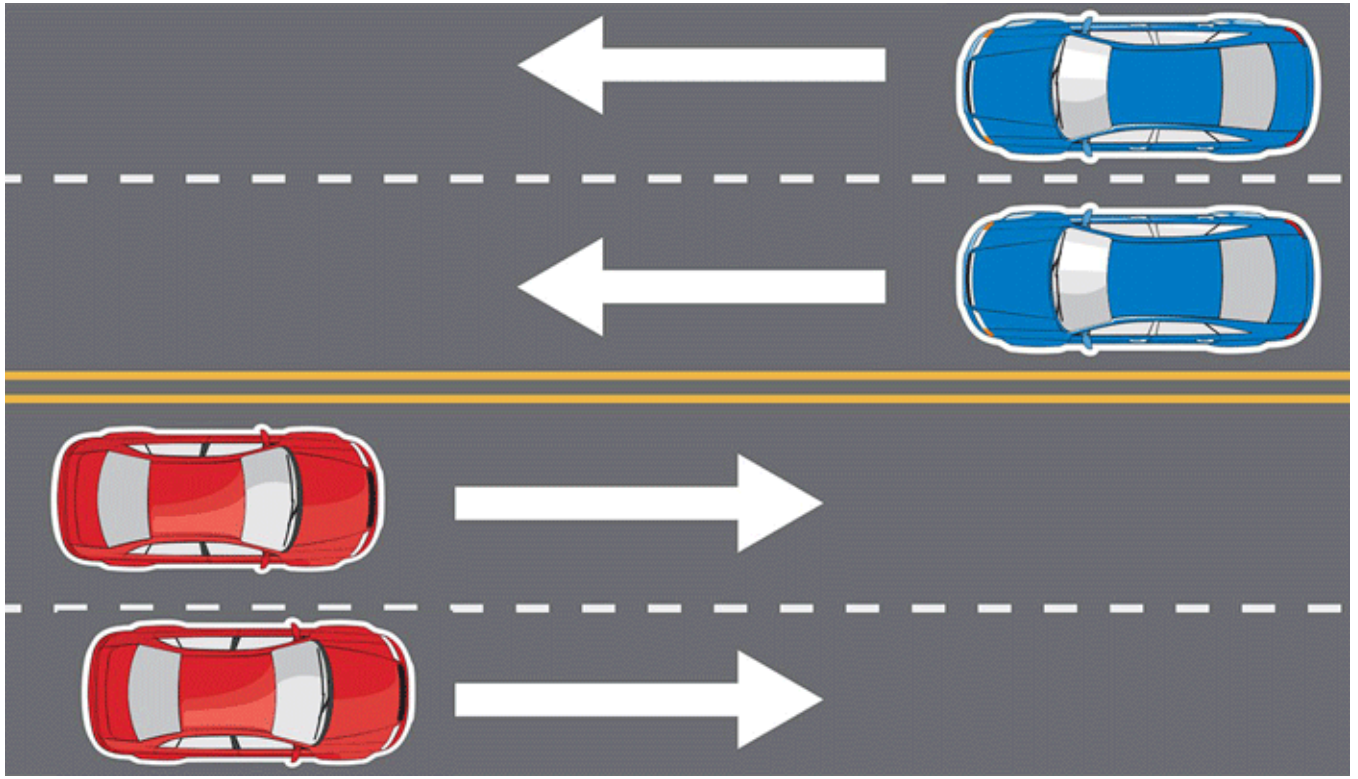
Comunicação

- **Half Duplex**: Comunicação bidirecional onde os dados podem fluir em ambas as direções, mas não ao mesmo tempo.

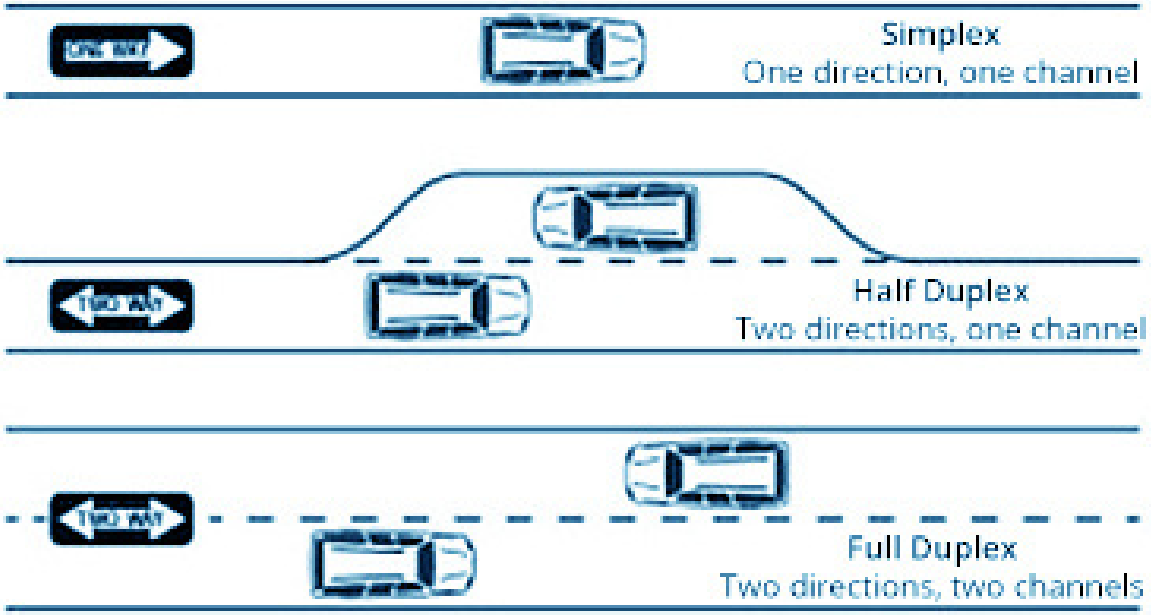


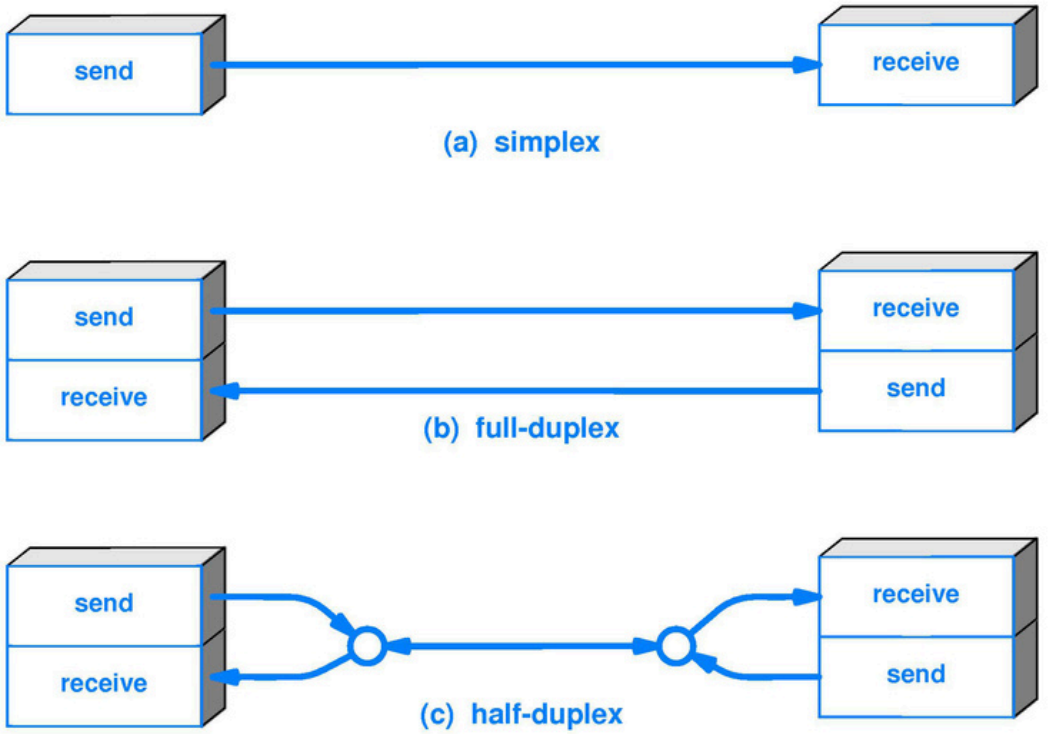
Comunicação

- **Full Duplex**: Comunicação bidirecional onde os dados podem fluir simultaneamente em ambas as direções.



Comunicação

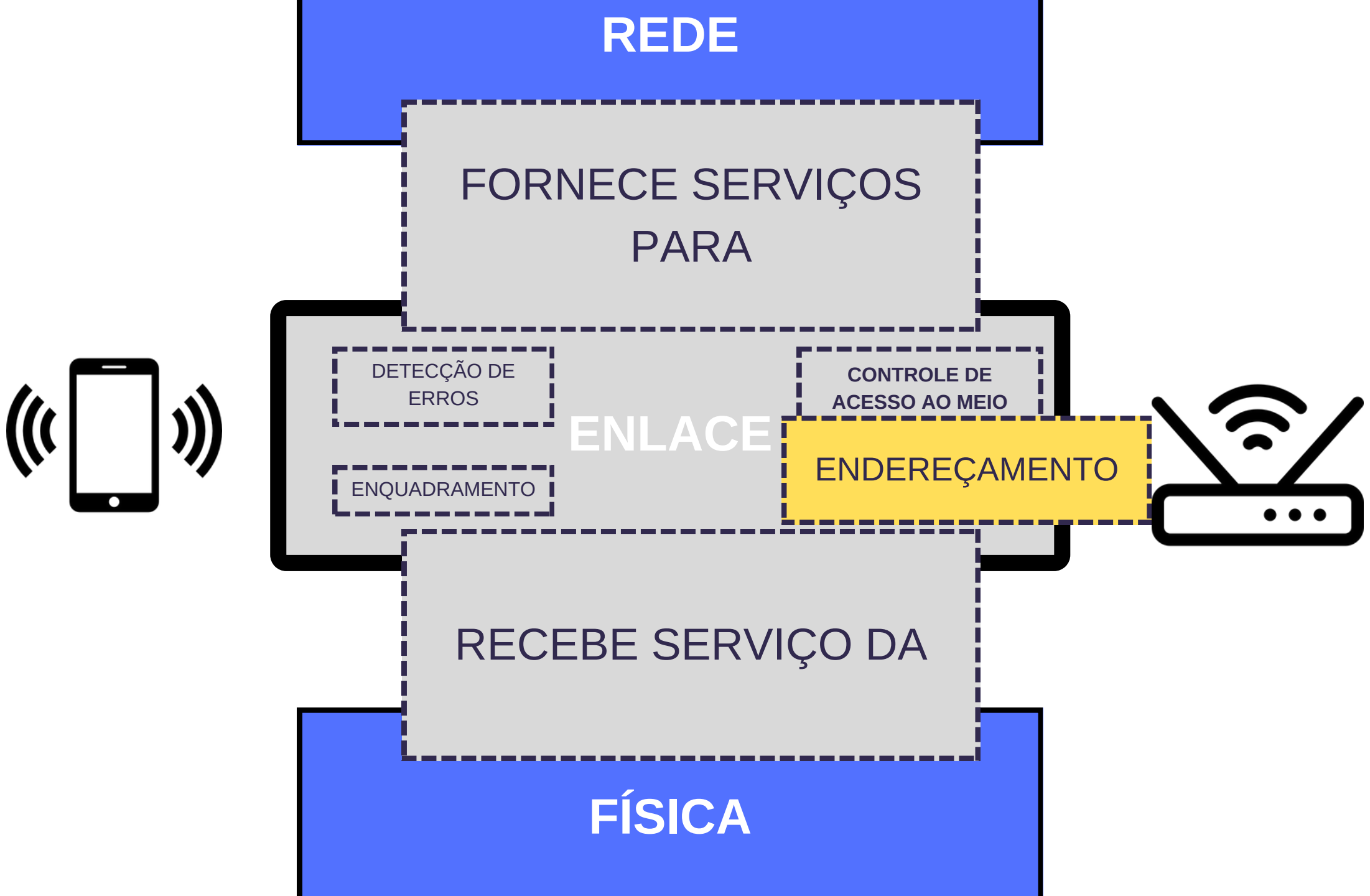




CSMA

- **Atenção**!
  - Antes, em redes half-duplex (Coaxial), técnicas como CSMA/CD eram necessárias para gerenciar colisões em redes Ethernet.
  - Mas com a maioria das redes modernas utilizando *switches* e comunicação full-duplex, essas técnicas de controle de colisão se tornaram **obsoletas**.

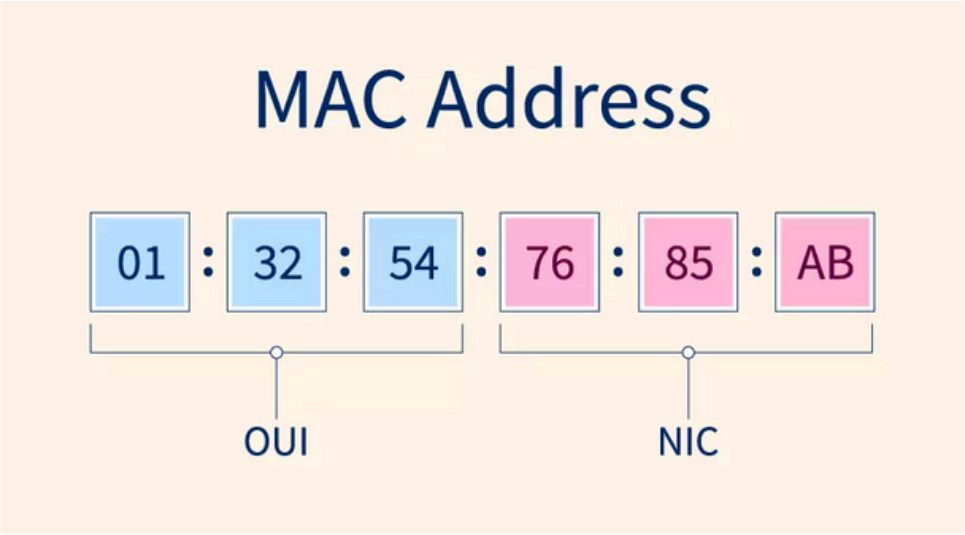
Endereçamento


REDE
FORNECE SERVIÇOS PARA
DETECÇÃO DE ERROS
ENQUADRAMENTO
ENLACE
CONTROLE DE ACESSO AO MEIO
ENDEREÇAMENTO
RECEBE SERVIÇO DA
FÍSICA

MAC *(Media Access Control)*

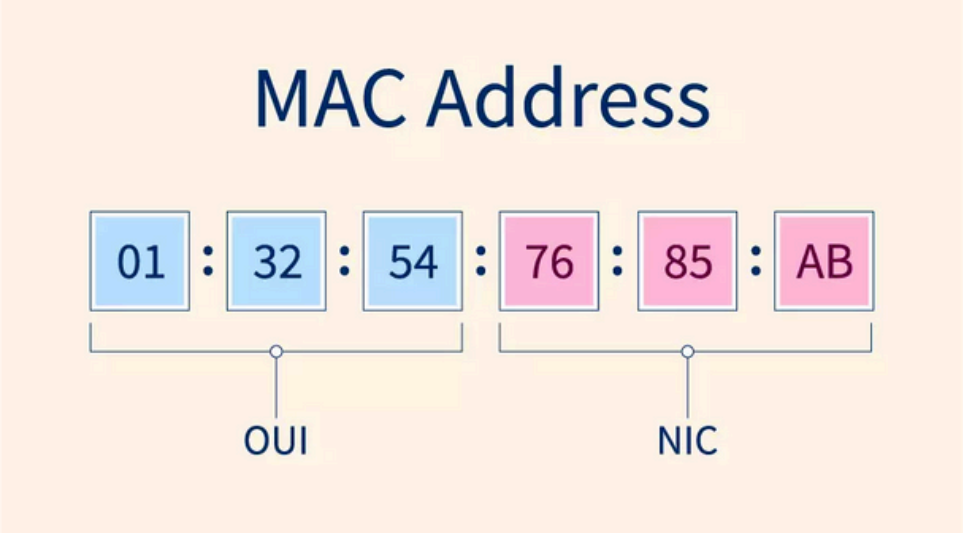
É um identificador único atribuído a uma placa de rede Ethernet por exemplo, em um dispositivo. Ele é um endereço físico gravado na memória da interface de rede durante sua fabricação.

O endereço MAC é usado para o roteamento e encaminhamento de dados em redes locais e é usado em conjunto com o Protocolo ARP para associar endereços IP a endereços MAC na resolução de endereços.



MAC *(Media Access Control)*

Decimal	Binario	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F



ARP (*Address Resolution Protocol*)

1. Um dispositivo na rede local deseja enviar dados para um dispositivo com um determinado endereço IP, mas precisa conhecer o endereço MAC correspondente.

1. O dispositivo emite uma solicitação ARP em broadcast para todos os dispositivos na rede local, perguntando: "Qual é o endereço MAC associado ao endereço IP X?"

1. Os dispositivos na rede local recebem a solicitação ARP e verificam se o endereço IP mencionado corresponde ao próprio endereço IP ou se é um endereço IP que eles conhecem.

1. O dispositivo com o endereço IP correspondente responde à solicitação ARP, enviando seu endereço MAC ao dispositivo solicitante.

1. O dispositivo solicitante recebe a resposta ARP e associa o endereço MAC recebido ao endereço IP alvo.

1. Agora, o dispositivo solicitante possui o endereço MAC necessário para enviar os dados diretamente ao dispositivo de destino na rede local.

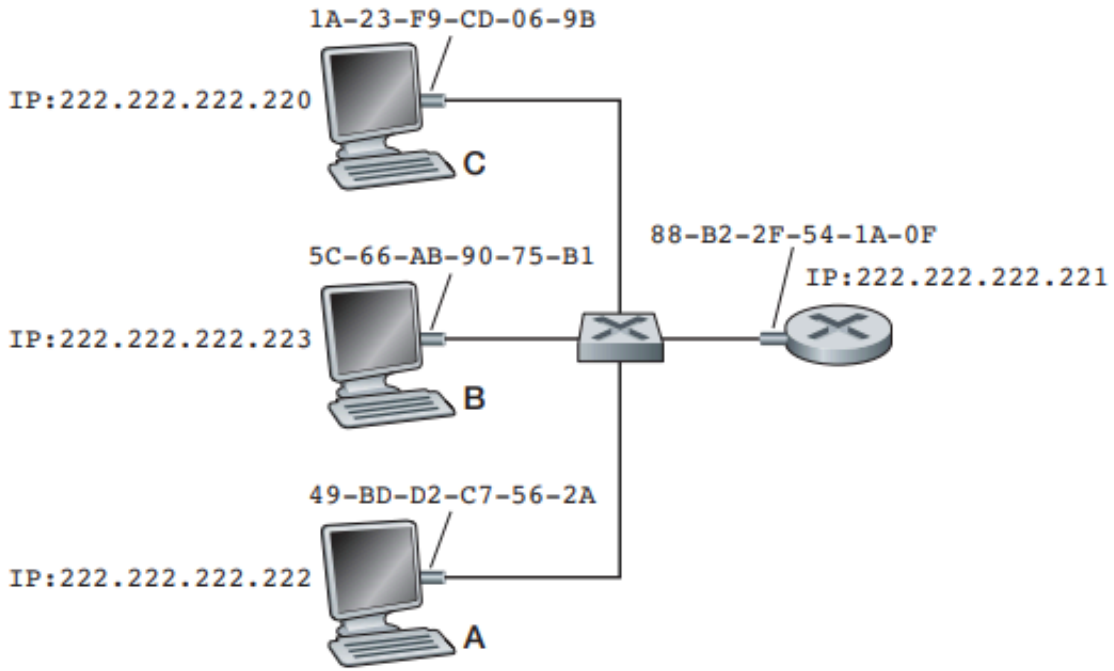
É importante destacar que o ARP é um protocolo local, usado apenas em redes locais. Para comunicação entre redes, é necessário o uso de outros protocolos, como o roteamento IP.

ARP (*Address Resolution Protocol*)

O ARP é um protocolo de rede usado para associar um endereço IP (*Internet Protocol*) para um endereço MAC em uma rede local (LAN).

ARP (*Address Resolution Protocol*)

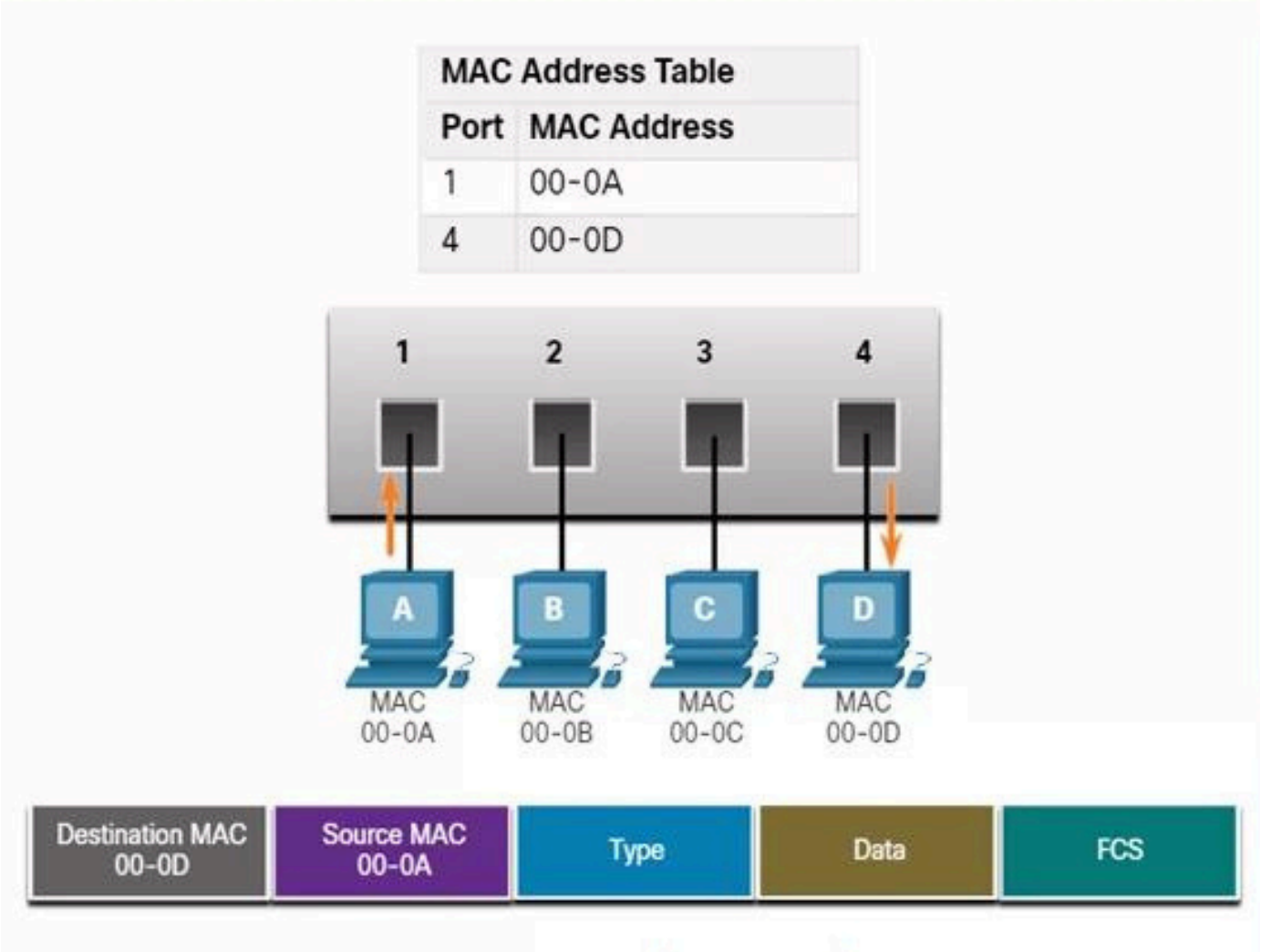
CADA INTERFACE EM UMA LAN TEM UM ENDEREÇO IP E UM ENDEREÇO MAC



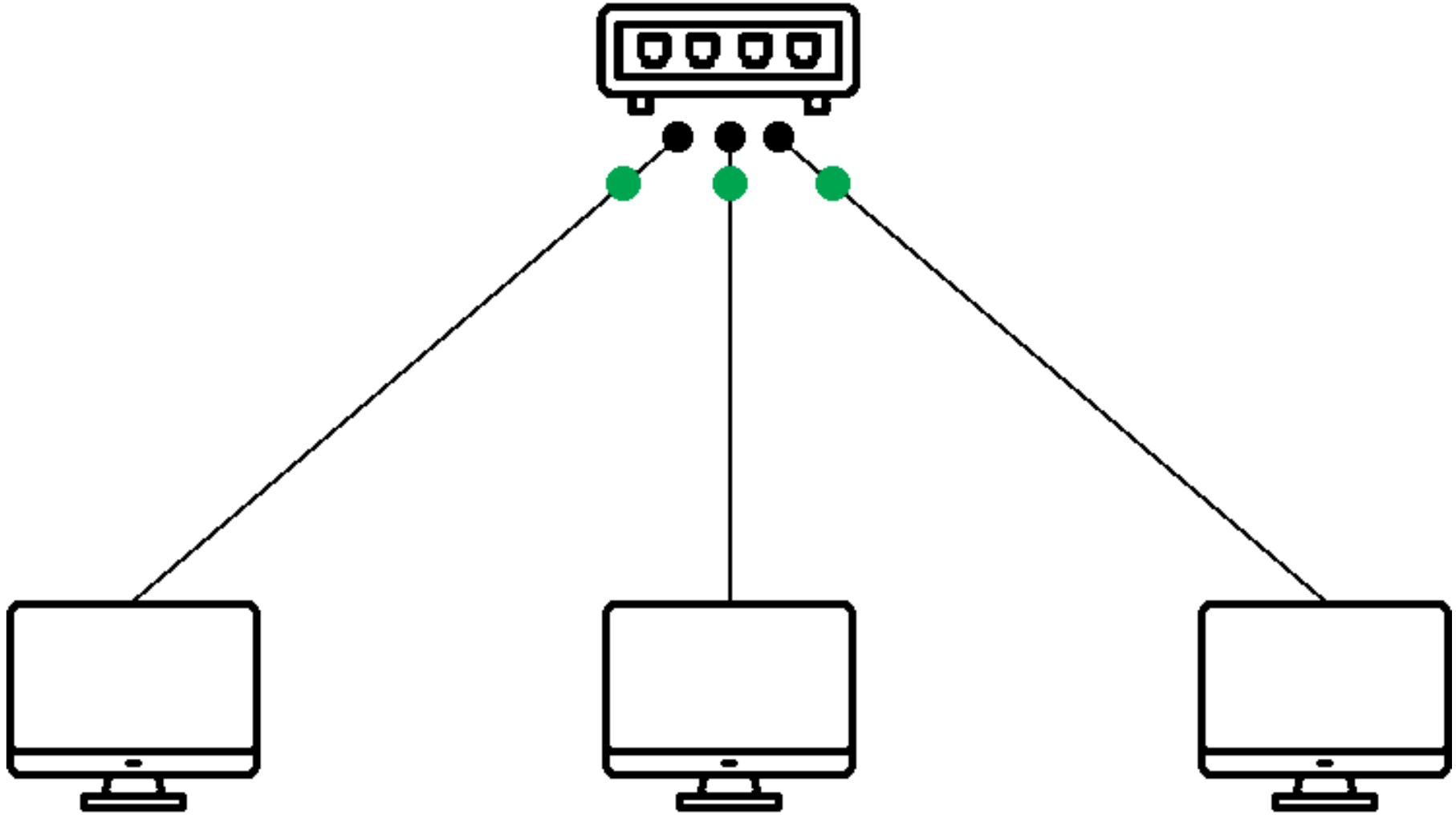
Endereço IP	Endereço MAC
222.222.222.221	88-B2-2F-54-1A-0F
222.222.222.223	5C-66-AB-90-75-B1

Fonte: Kurose, 2014.

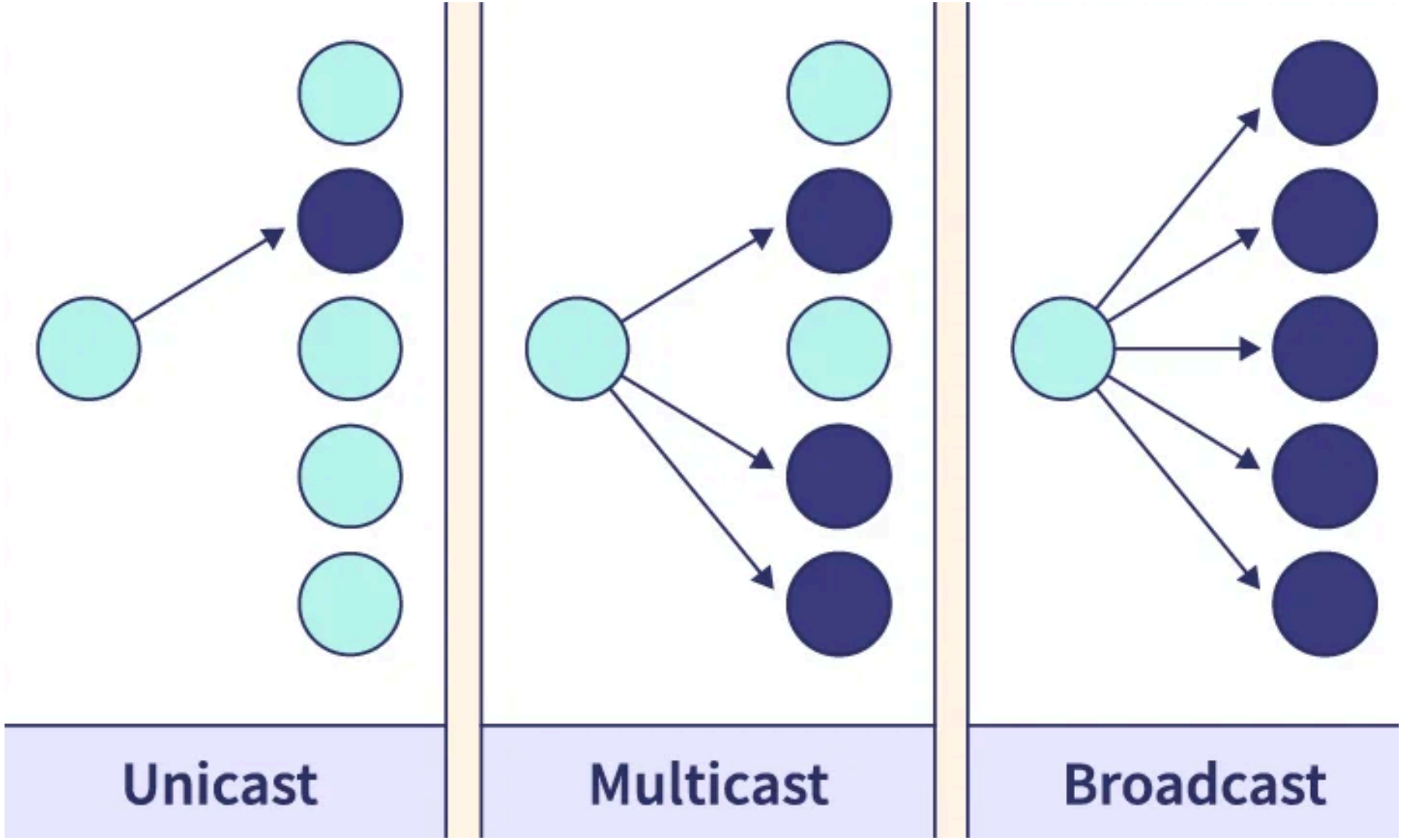
MAC *(Media Access Control)*



Broadcast



Métodos de Comunicação



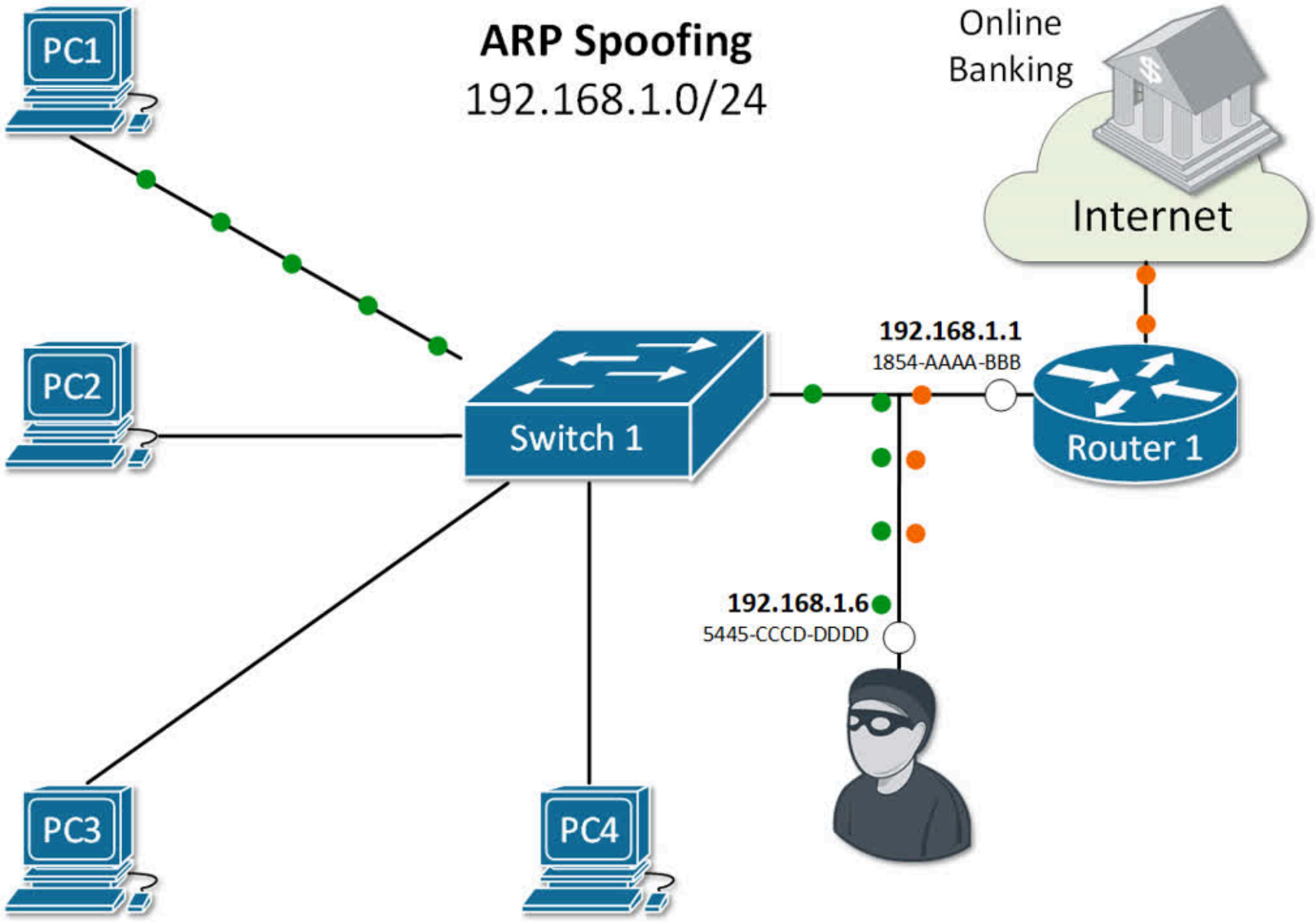
Curiosidade - Segurança do Protocolo ARP

O protocolo ARP pode ser explorado em ataque Ataque *man-in-the-middle*.

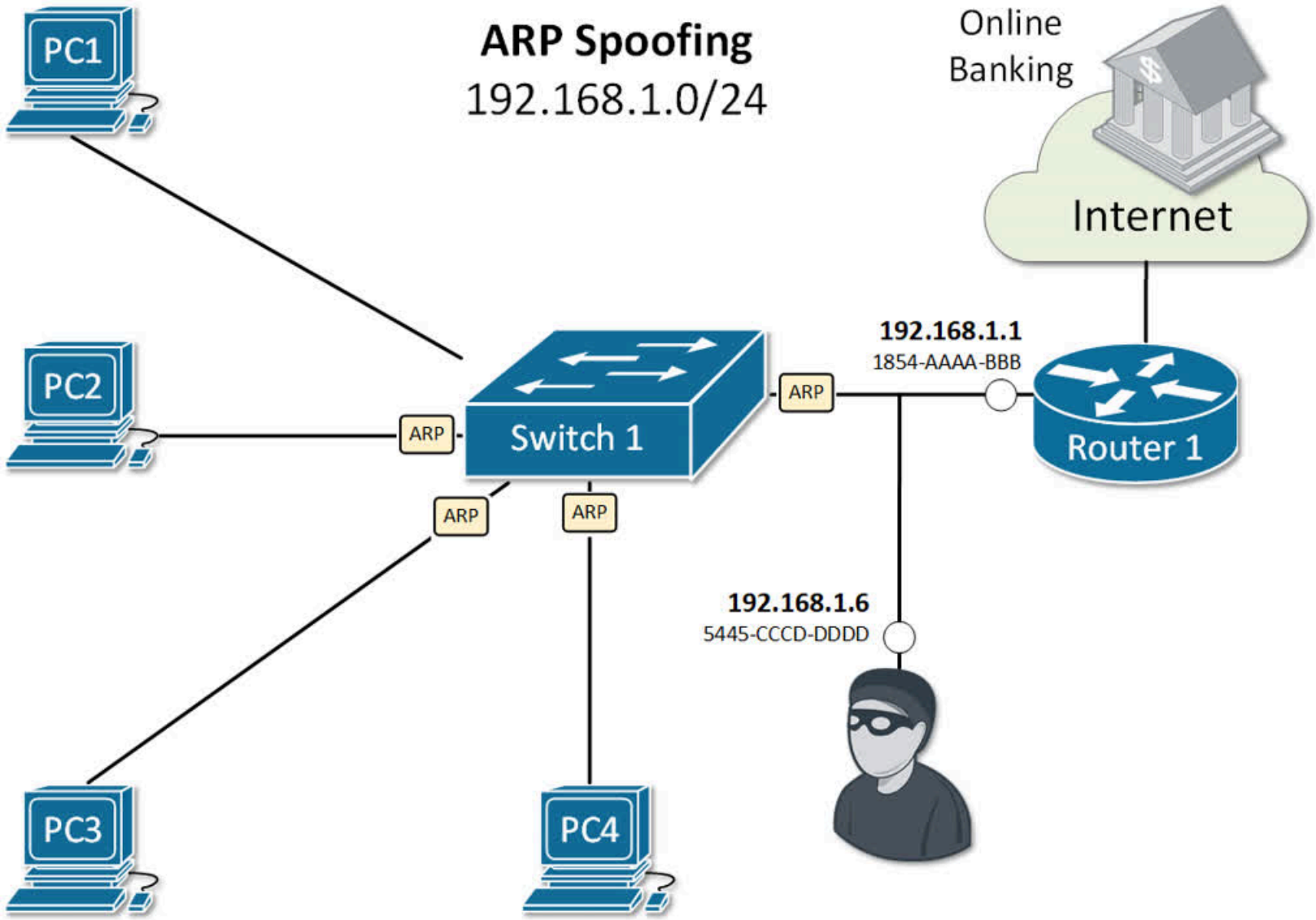
- Spoofing (Envenamento:):
  - ARP *poisoning:*
    - Inundação de pacotes ARP confundem o *host* sobre a informação de quem é o *gateway*.

`Comando CMD: arp -a`

Curiosidade - Segurança do Protocolo ARP



Curiosidade - Segurança do Protocolo ARP



Protocolo 802.3 - Ethernet

- O protocolo Ethernet é usado para conectar dispositivos em uma rede e permitir a comunicação através de pacotes de dados.

- Ele define como os dispositivos devem formatar e transmitir dados, como identificar e corrigir erros, e como acessar o meio de transmissão compartilhado.

- O Ethernet usa endereços MAC para identificar dispositivos e pode operar em diferentes velocidades e meios físicos, como cabos de par trançado e fibra ótica.

Protocolo 802.3 - Ethernet

- **Preâmbulo** (7 bytes): Sequência de bits que prepara o receptor para a chegada do quadro, ajudando a sincronizar a comunicação.
- **Delimitador de Início** de Quadro (SFD) (1 byte): Marca o início real dos dados do quadro, indicando onde começa o conteúdo real.
- **Endereço de Destino** (6 bytes): Endereço MAC do dispositivo para o qual o quadro está sendo enviado.
- **Endereço de Origem** (6 bytes): Endereço MAC do dispositivo que está enviando o quadro.

Fonte: Kurose, 2014.

Protocolo 802.3 - Ethernet

- **Tipo/Comprimento** (2 bytes): Indica o tipo de protocolo da camada superior (como IP) ou o comprimento dos dados no quadro (em Ethernet II).
- **Dados** (46 a 1500 bytes): Contém a carga útil, ou seja, os dados reais que estão sendo transmitidos.
- **Sequência de Verificação de Redundância Cíclica (CRC)** (4 bytes): Código usado para verificar a integridade dos dados transmitidos, detectando possíveis erros.

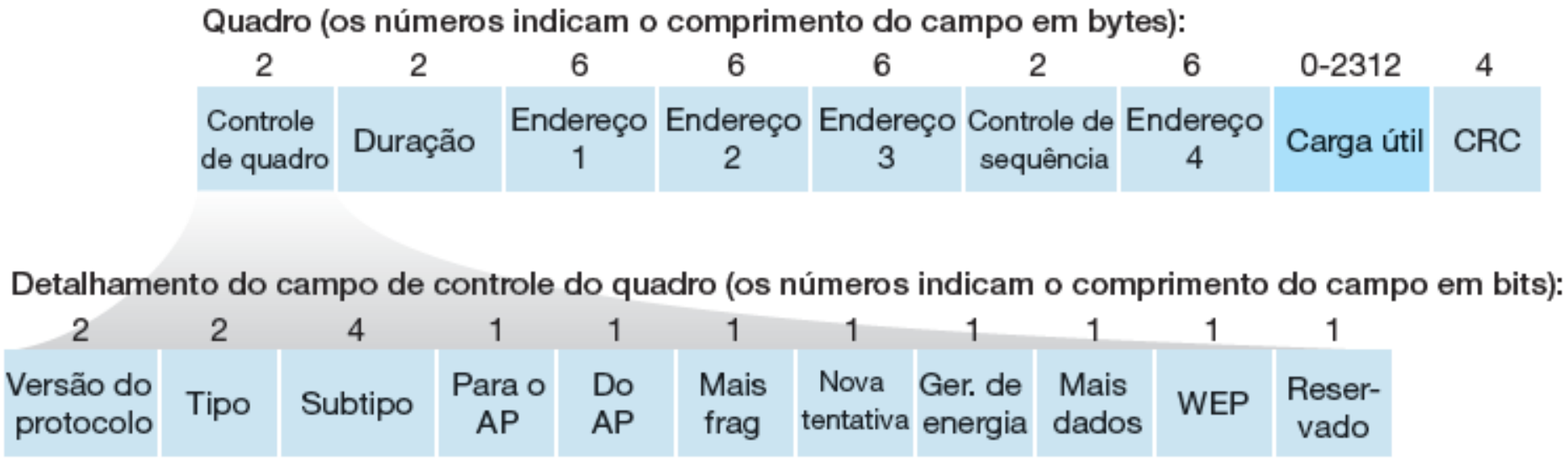
Fonte: Kurose, 2014.

Wi-Fi

O termo "Wi-Fi" refere-se a um conjunto de protocolos de comunicação sem fio baseados nas especificações do IEEE 802.11. O Wi-Fi permite a conexão sem fio de dispositivos em redes locais (LANs) e é comumente usado para acesso à Internet sem fio.

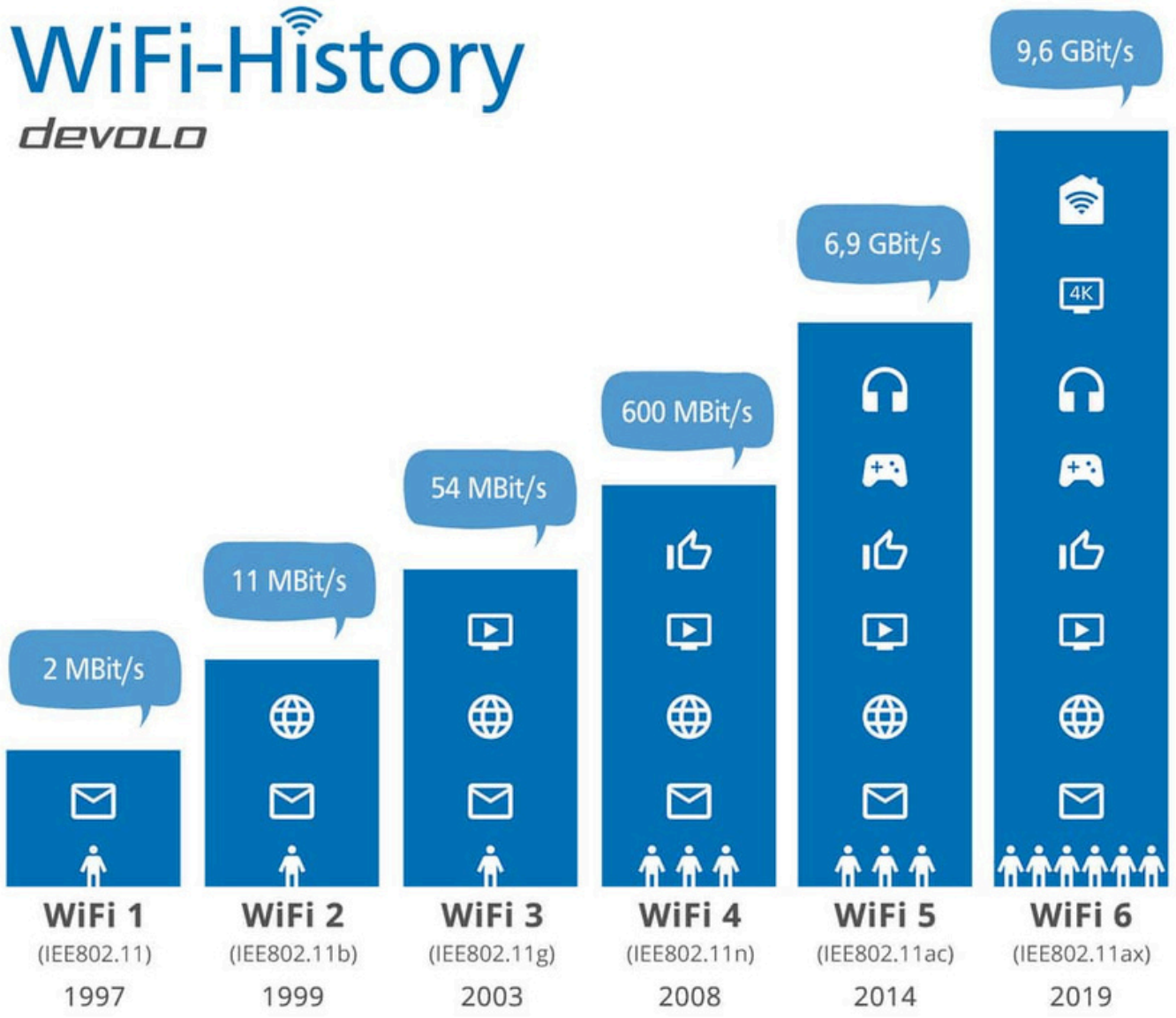
O protocolo Wi-Fi oferece comunicação sem fio em várias frequências de rádio, como 2,4 GHz e 5 GHz

Cabeçalho de um Quadro Wi-Fi (IEEE 802.11)



Fonte: Kurose, 2014.

Protocolos IEEE 802.11

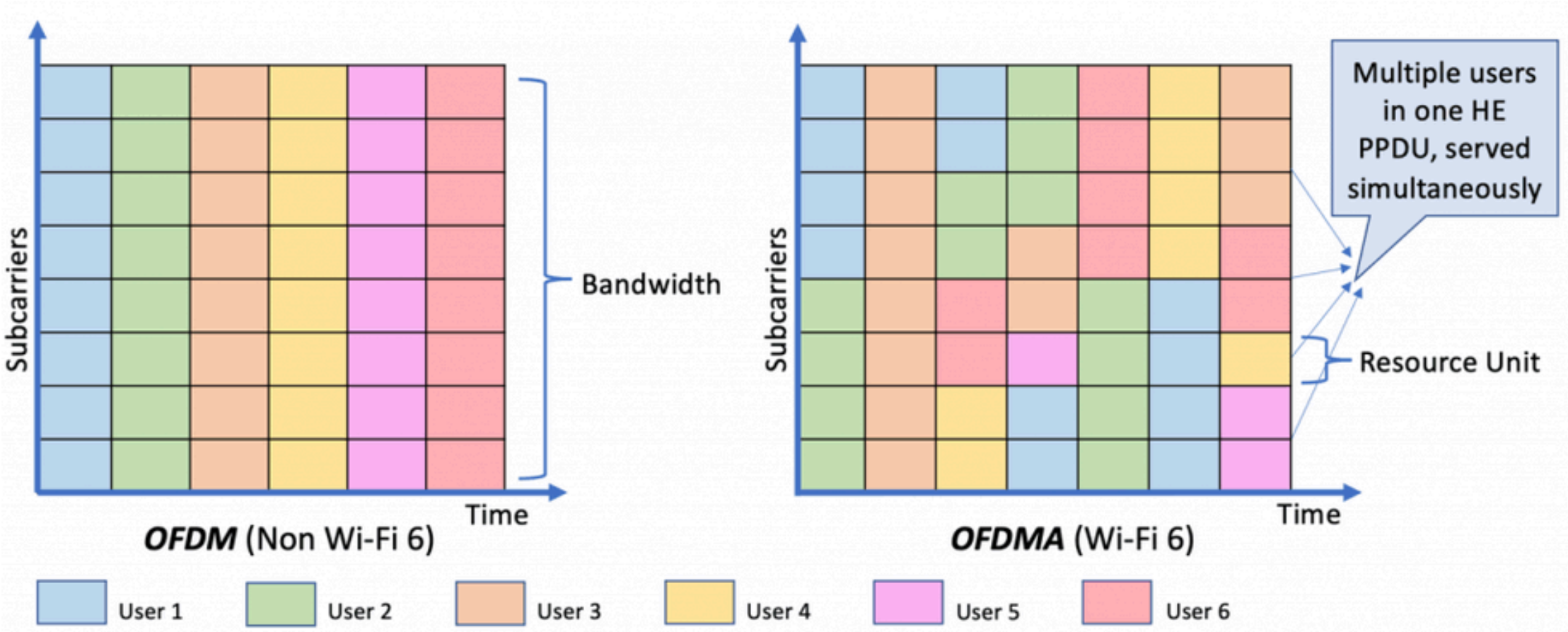


IEEE 802.11be - Wi-Fi 7

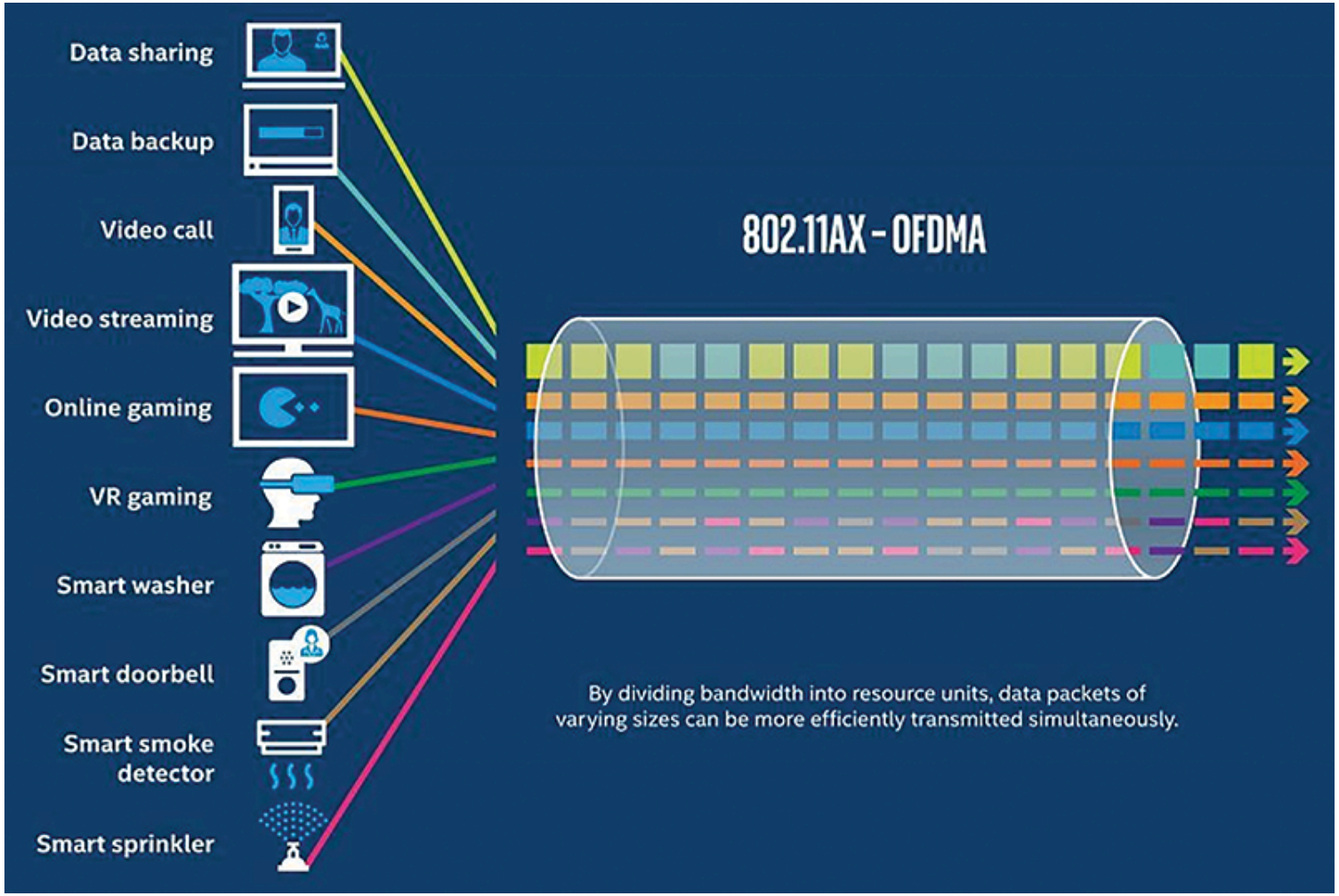
	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E	Wi-Fi 7 (expected)
Launch Date	2007	2013	2019	2021	2024
IEEE Standard	802.11n	802.11ac	802.11ax		802.11be
Max Data Rate	1.2 Gbps	3.5 Gbps	9.6 Gbps		46 Gbps
Bands	2.4 GHz, 5 GHz	5 GHz	2.4 GHz, 5 GHz	6 GHz	1-7.25 GHz (including 2.4 GHz, 5 GHz, 6 GHz bands)
Security	WPA 2	WPA 3	WPA 3		WPA 3
Channel Size	20, 40 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz		Up to 320 MHz
Modulation	64-QAM OFDM	256-QAM OFDM	1024-QAM OFDMA		4096-QAM OFDMA (with extensions)
MIMO	4x4 MIMO	4x4 MIMo, DL MU-MIMO	8x8 UL/DL MU-MIMO		16x16 MU-MIMO

Source : IEEE, Intel Corporation, Wi-Fi Alliance

OFDMA (*Orthogonal Frequency-Division Multiple Access*)



OFDMA (*Orthogonal Frequency-Division Multiple Access*)

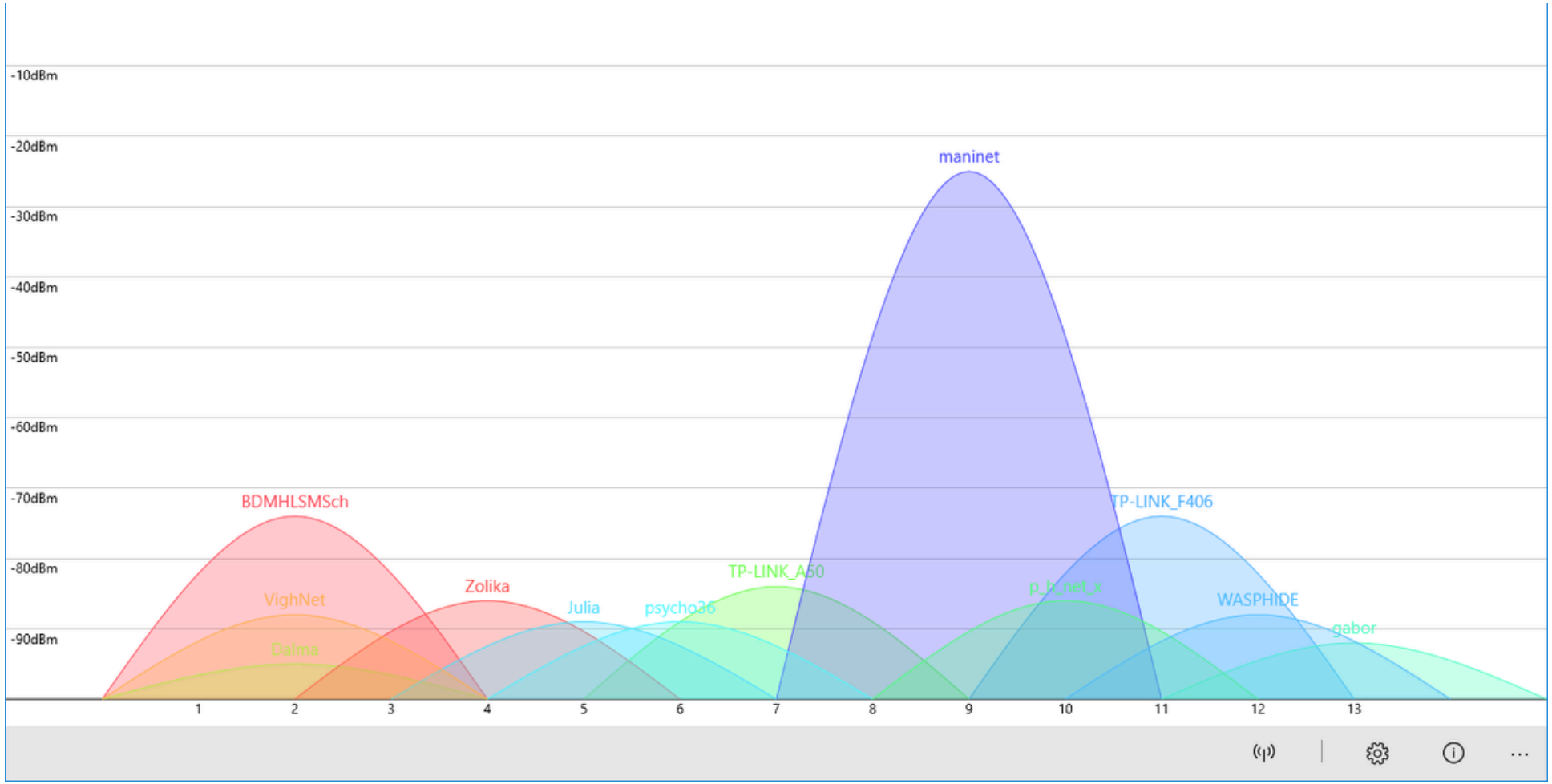


OFDMA (*Orthogonal Frequency-Division Multiple Access*)

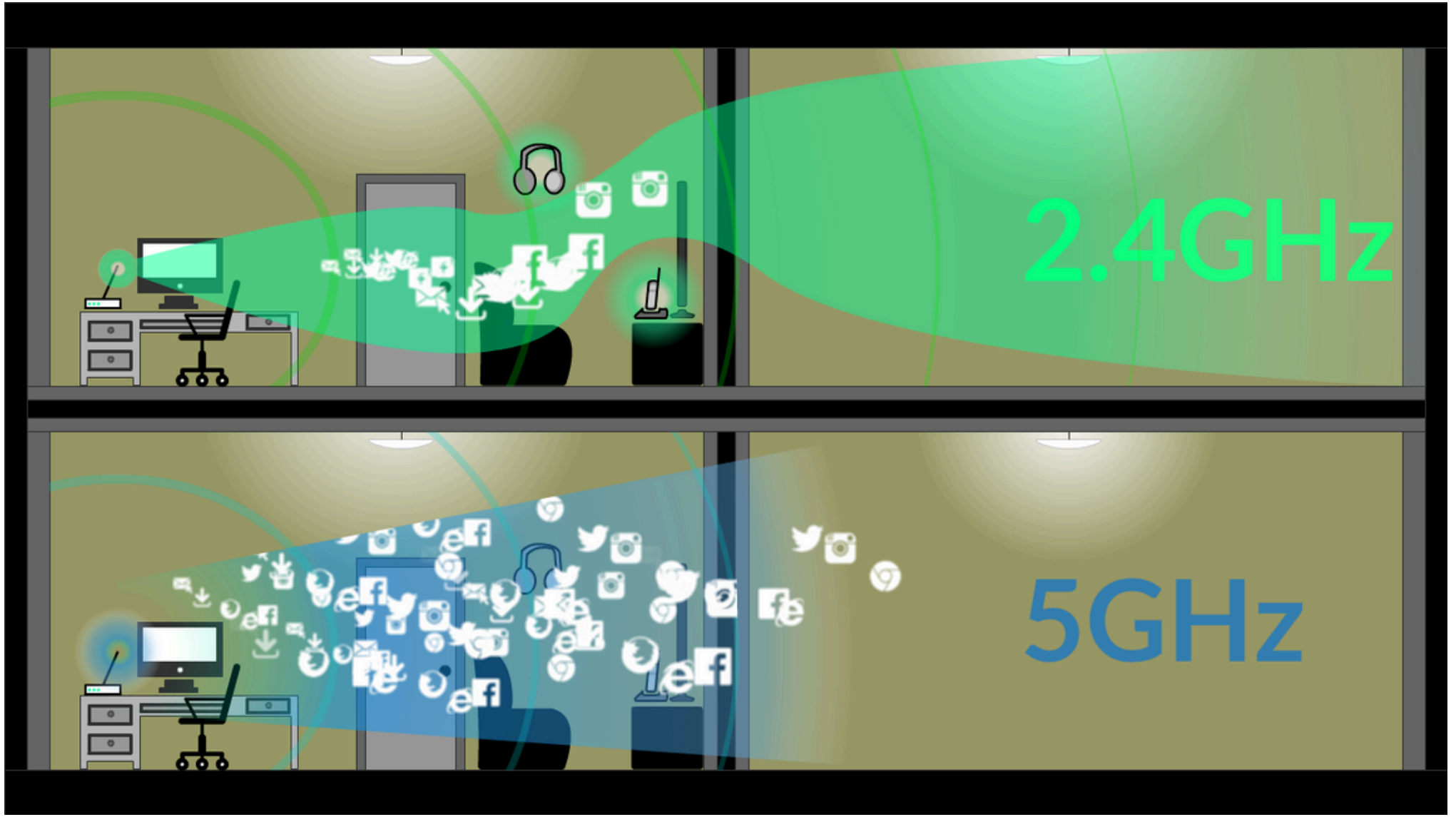
- No Wi-Fi 6, OFDMA é usado em conjunto com CSMA/CA.

- Enquanto o OFDMA permite a transmissão simultânea de múltiplos usuários, o CSMA/CA ainda é utilizado para gerenciar o acesso ao meio e evitar colisões entre transmissões.

Canais de uma rede Wifi

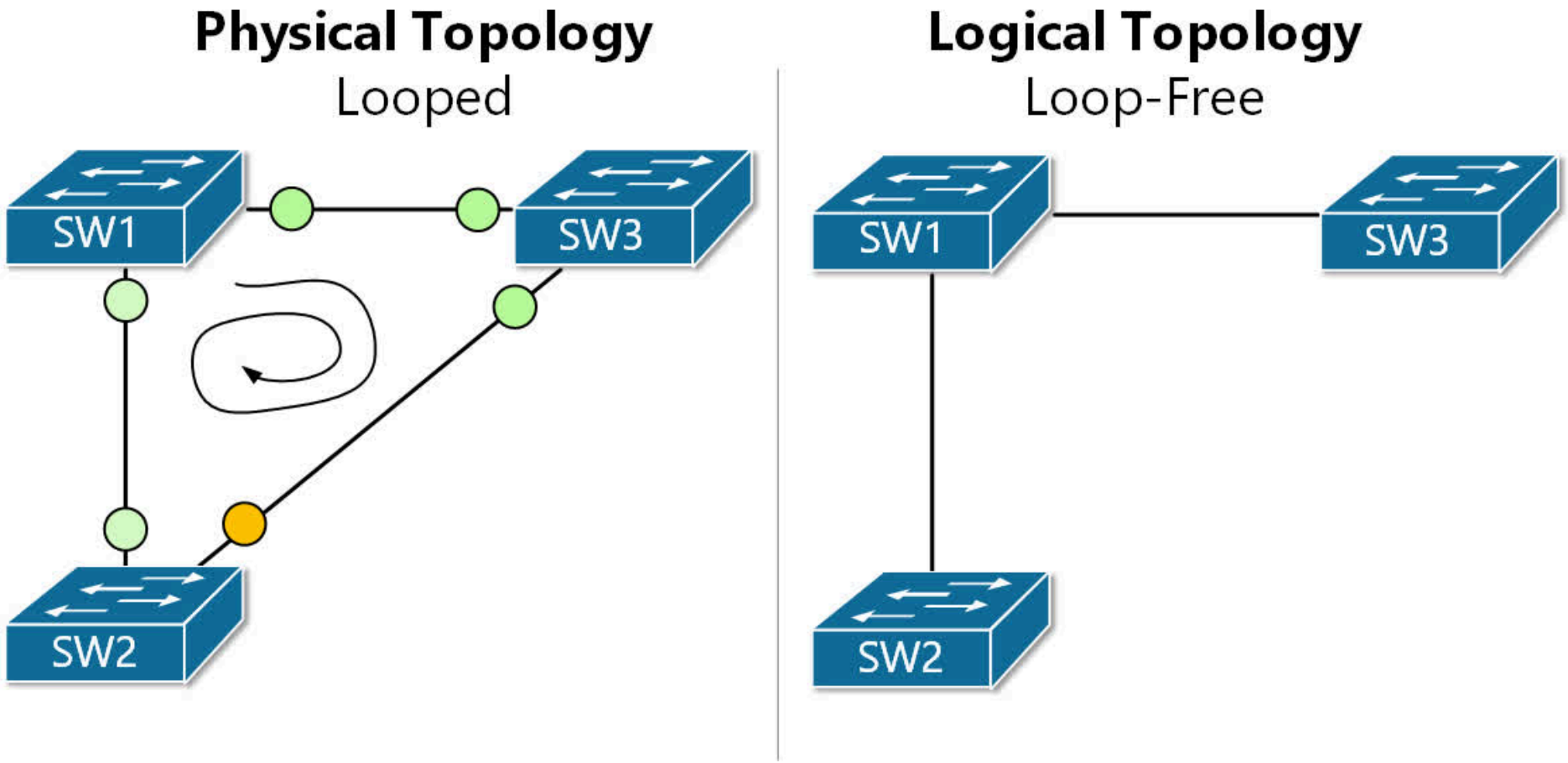


Largura de Banda

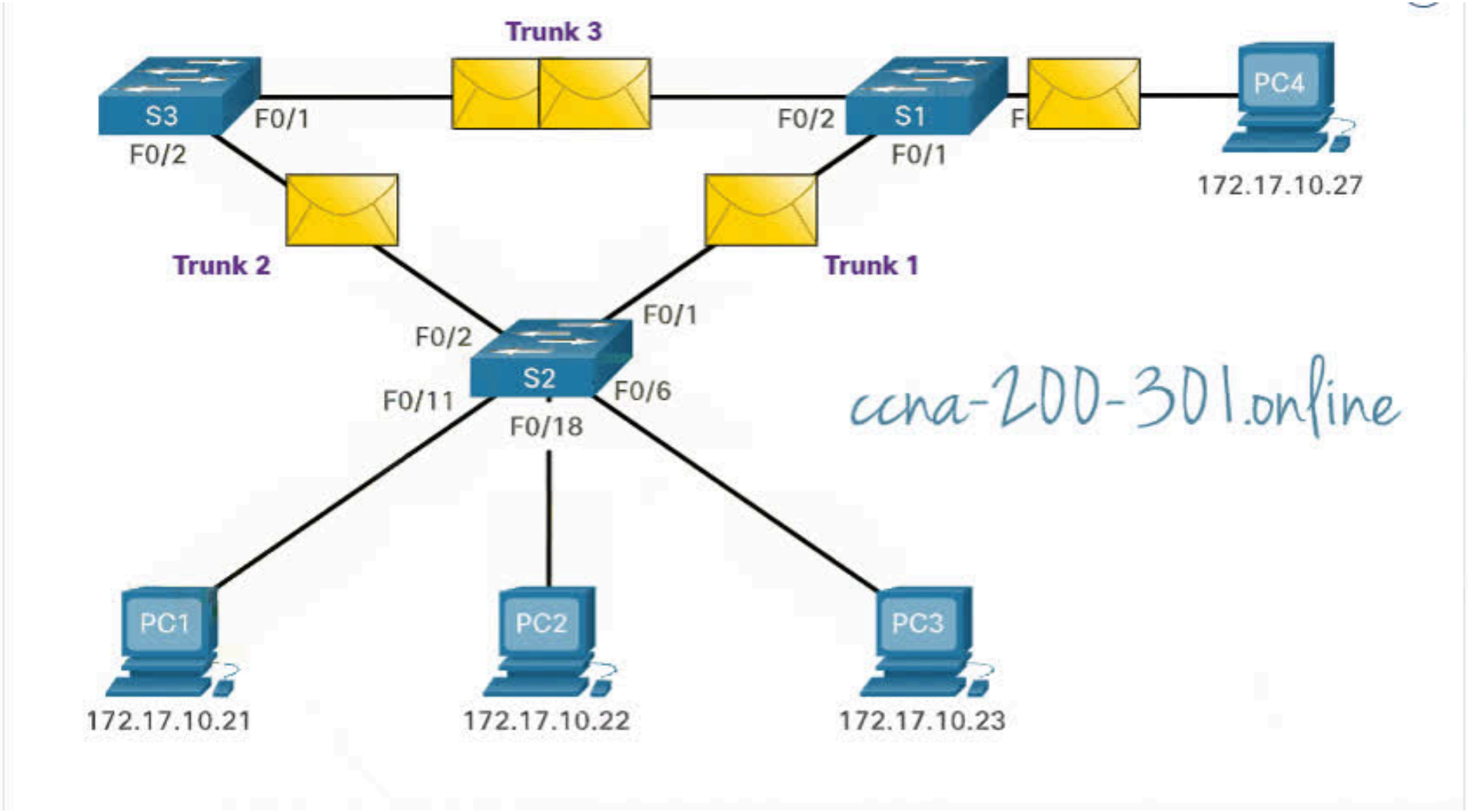


Access Point

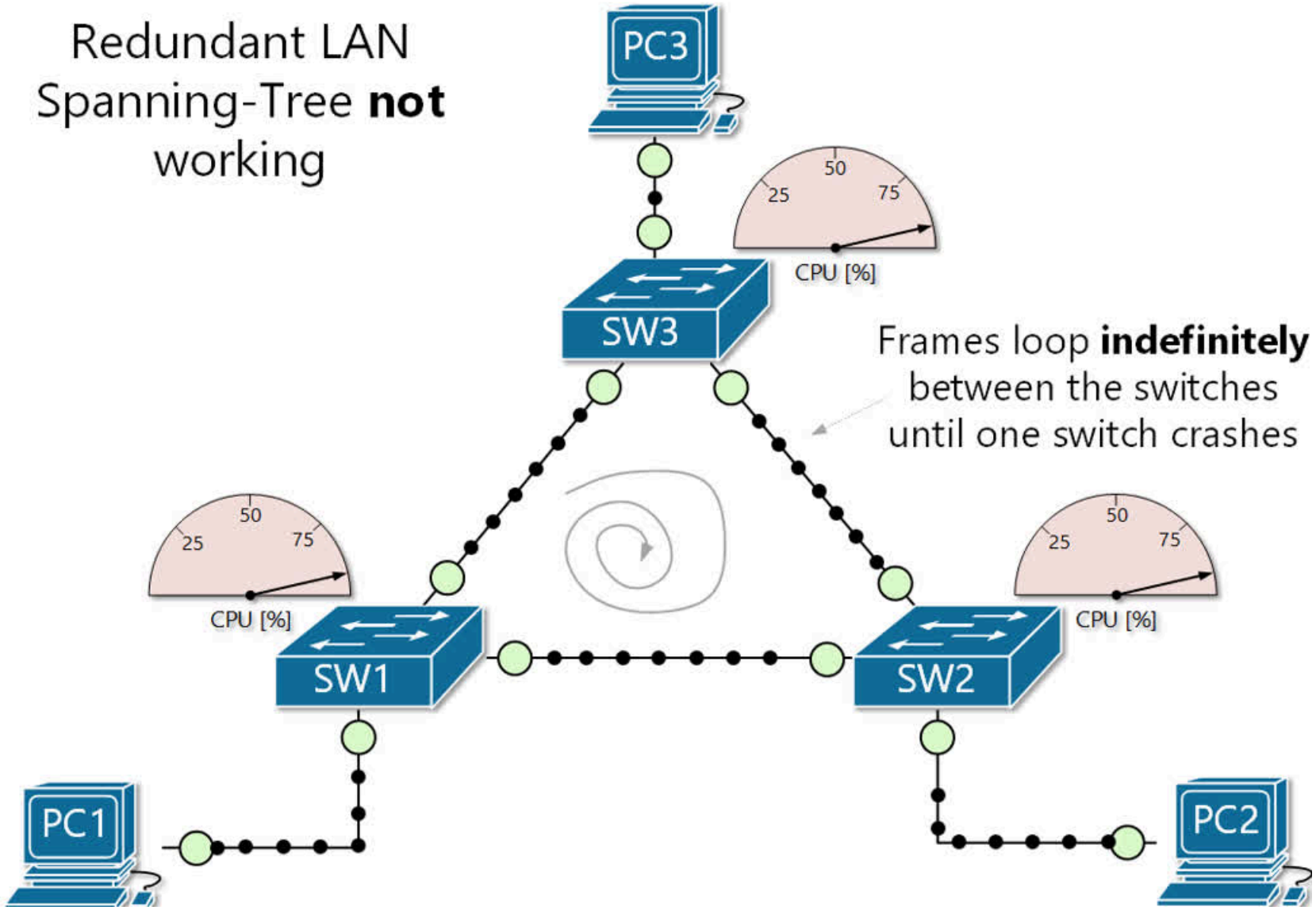
Broadcast


Physical Topology
Looped
SW1
SW3
SW2
Logical Topology
Loop-Free
SW1
SW3
SW2

Topologia Anel



LOOP

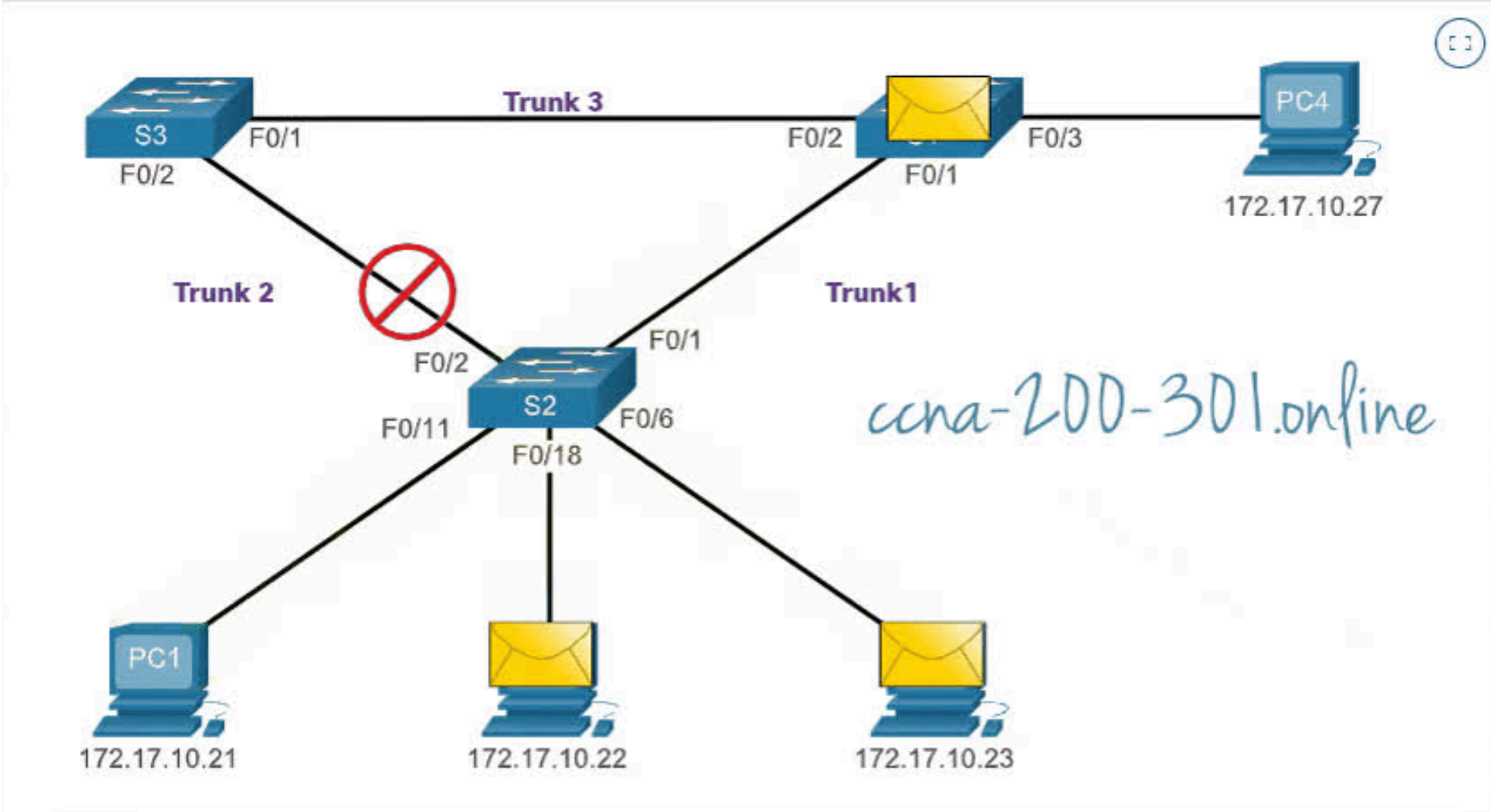

Redundant LAN
Spanning-Tree **not**
working
PC3
50
25
75
CPU [%]
SW3
Frames loop **indefinitely**
between the switches
until one switch crashes
50
25
75
CPU [%]
50
25
75
CPU [%]
SW1
SW2
PC1
PC2

Spanning Tree Protocol (STP)

O Spanning Tree Protocol (STP) é um protocolo que evita loops de rede em redes Ethernet, garantindo uma topologia livre de loops ao desativar caminhos redundantes e manter apenas um caminho ativo entre switches.

Spanning Tree Protocol (STP)

Como Funciona?

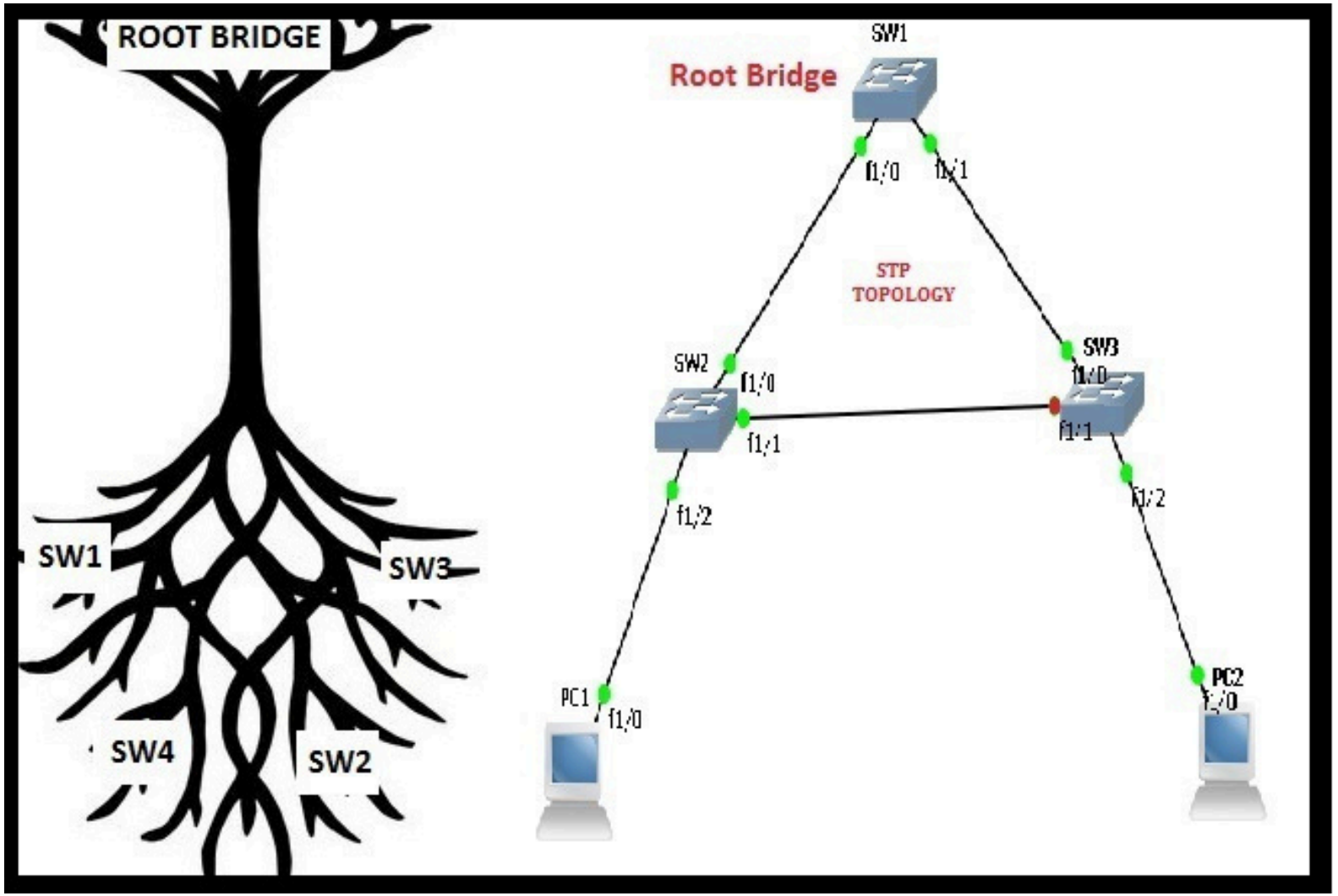


Spanning Tree Protocol (STP)

- **Como Funciona?**
  - O Spanning Tree Protocol (STP) evita loops em redes de switches criando uma **árvore** de cobertura que desativa portas redundantes, garantindo uma única rota ativa entre qualquer par de switches.

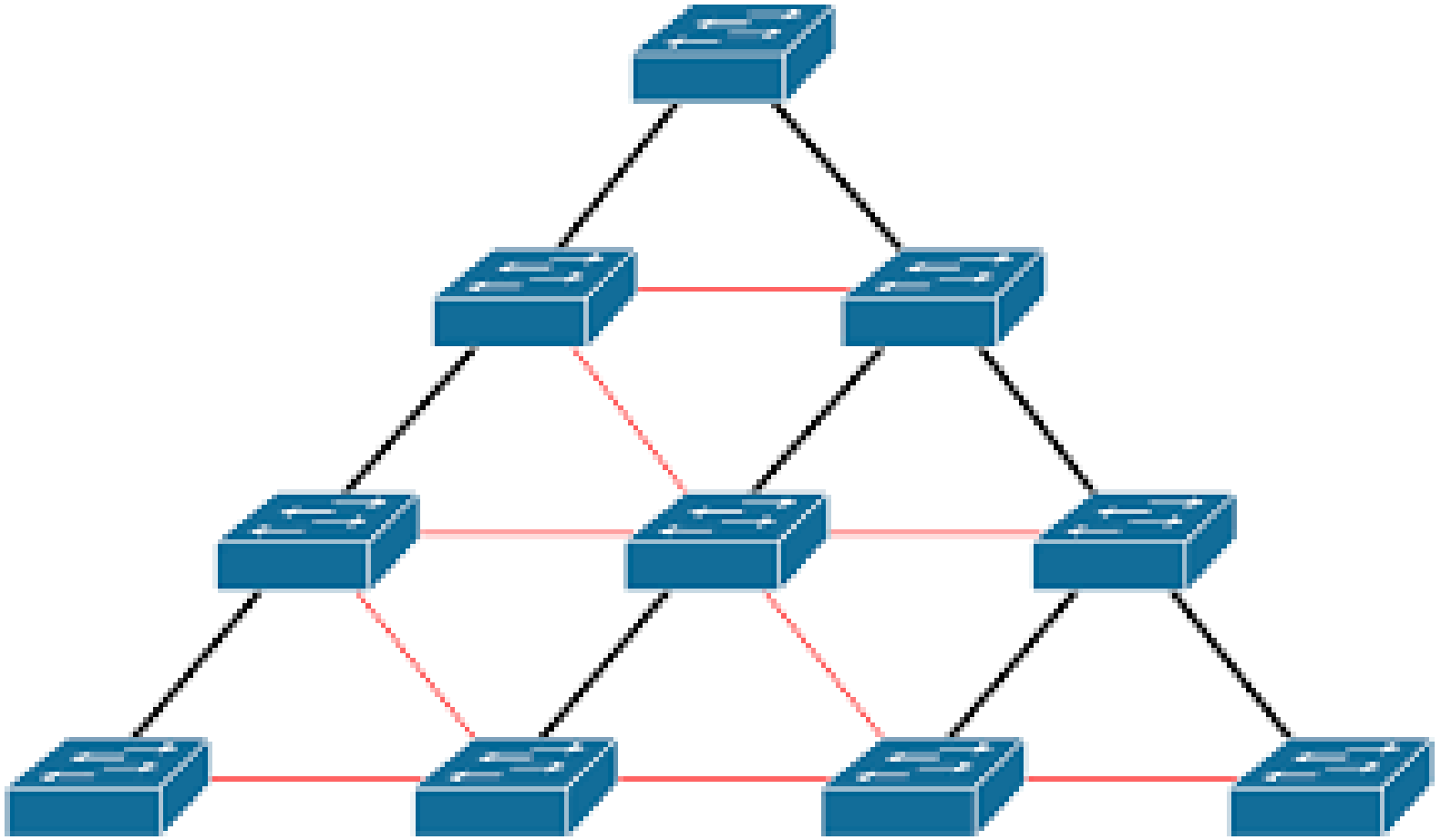
Spanning Tree Protocol (STP)

Como Funciona?



Spanning Tree Protocol (STP)

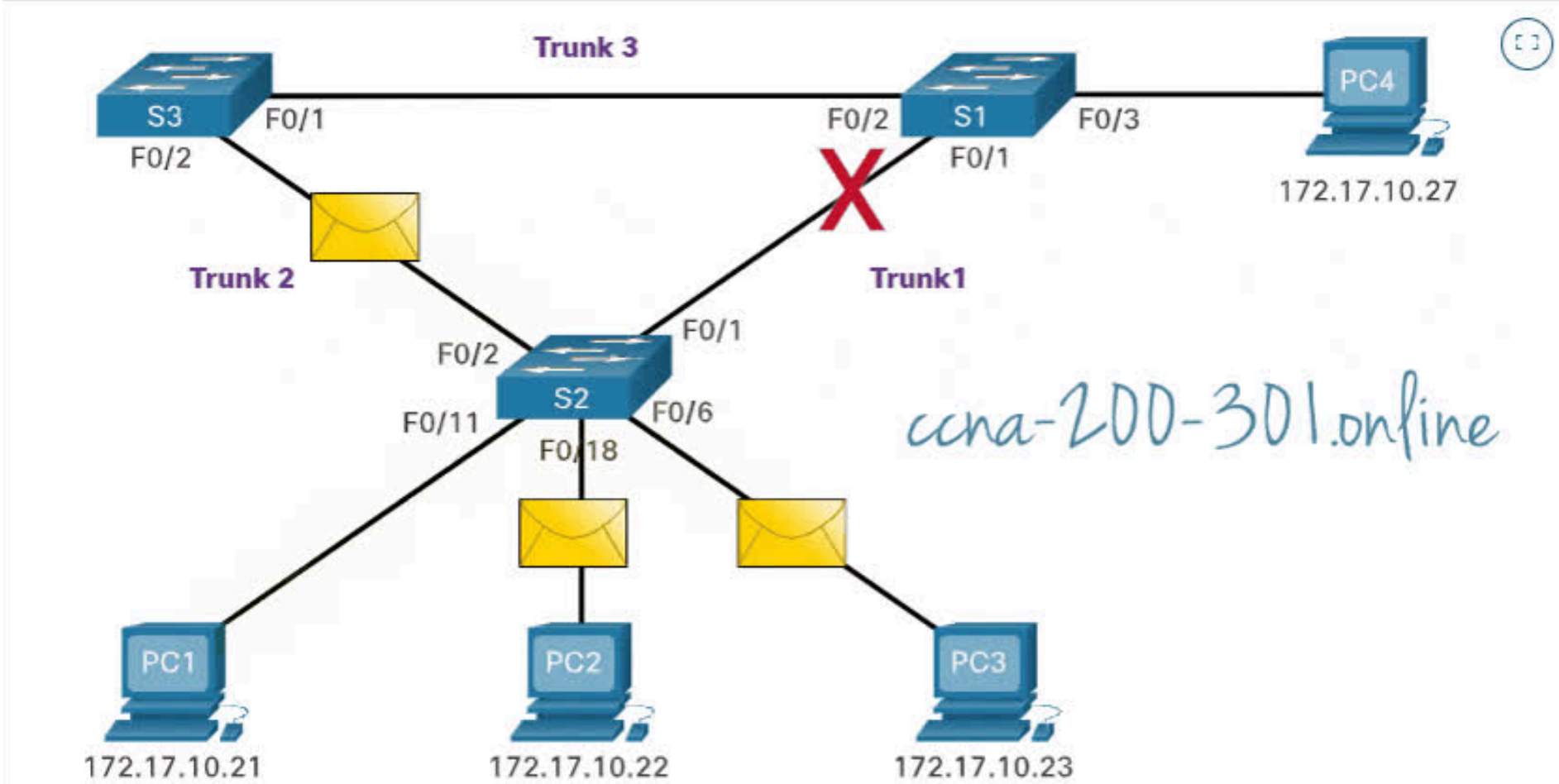
Como Funciona?



Spanning Tree Protocol (STP)

Como Funciona?

Adaptação se um a topologia da rede muda, isto é, um enlace fica offline.



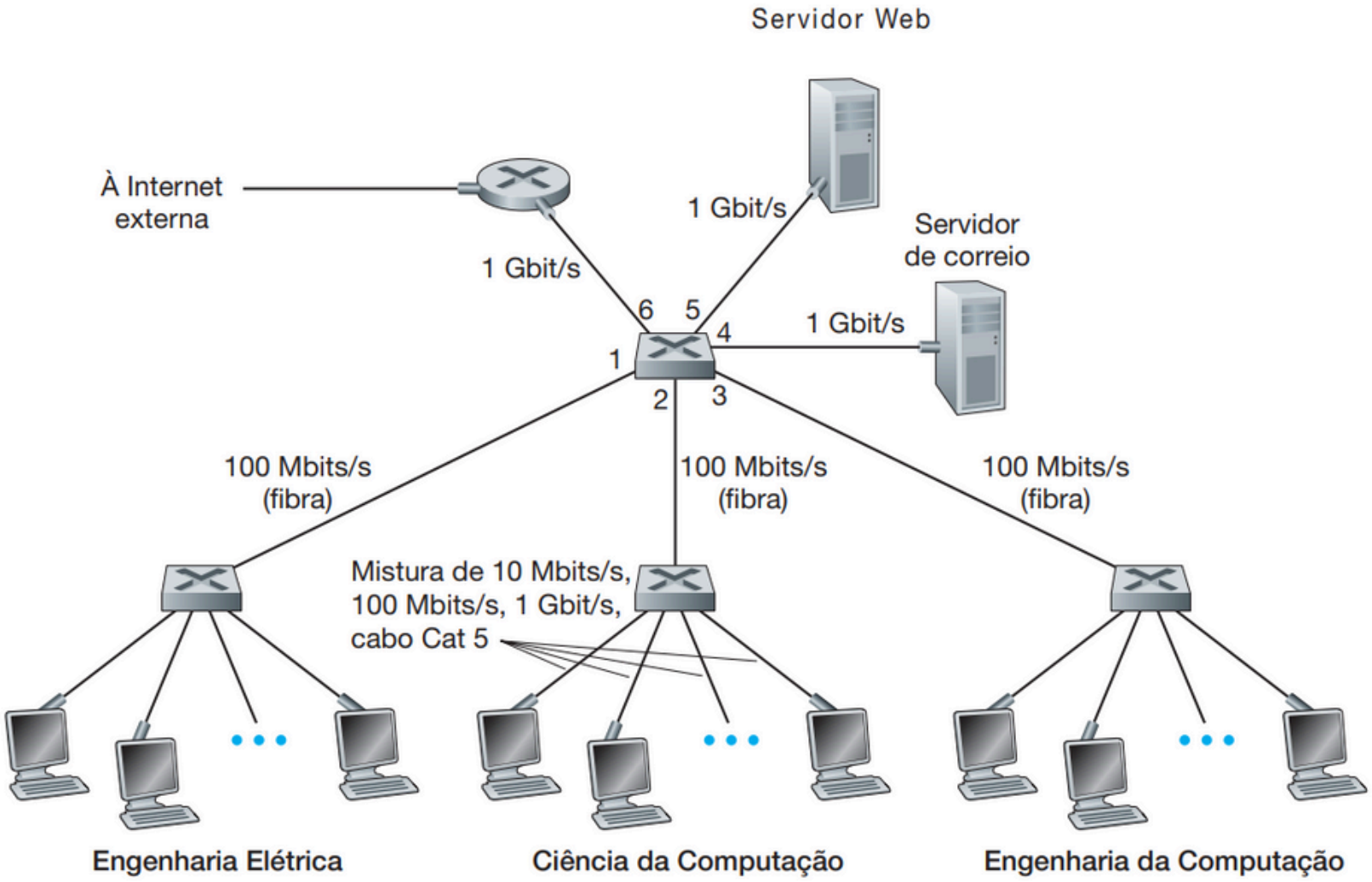
Spanning Tree Protocol (STP)

- **Spanning Tree Protocol (STP) - IEEE 802.1D:**
  - O padrão original e mais amplamente utilizado para evitar loops em redes Ethernet.
- **Rapid Spanning Tree Protocol (RSTP) - IEEE 802.1w:**
  - Uma evolução do STP que oferece tempos de convergência mais rápidos após mudanças na topologia da rede.
- **Multiple Spanning Tree Protocol (MSTP) - IEEE 802.1s:**
  - Permite a criação de múltiplas instâncias de STP, cada uma correspondendo a uma VLAN.

VLANs
Virtualização

Virtualização de Redes

FIGURA 5.15 UMA REDE INSTITUCIONAL CONECTADA POR QUATRO COMUTADORES



Fonte: Kurose, 2014.

Virtualização de Redes

- Redes Locais Virtuais:
  - Falta de isolamento.
  - Uso ineficiente de comutadores.
  - Gerencimento de usuários.
  - Redução de *broadcast*.

Virtualização de Redes

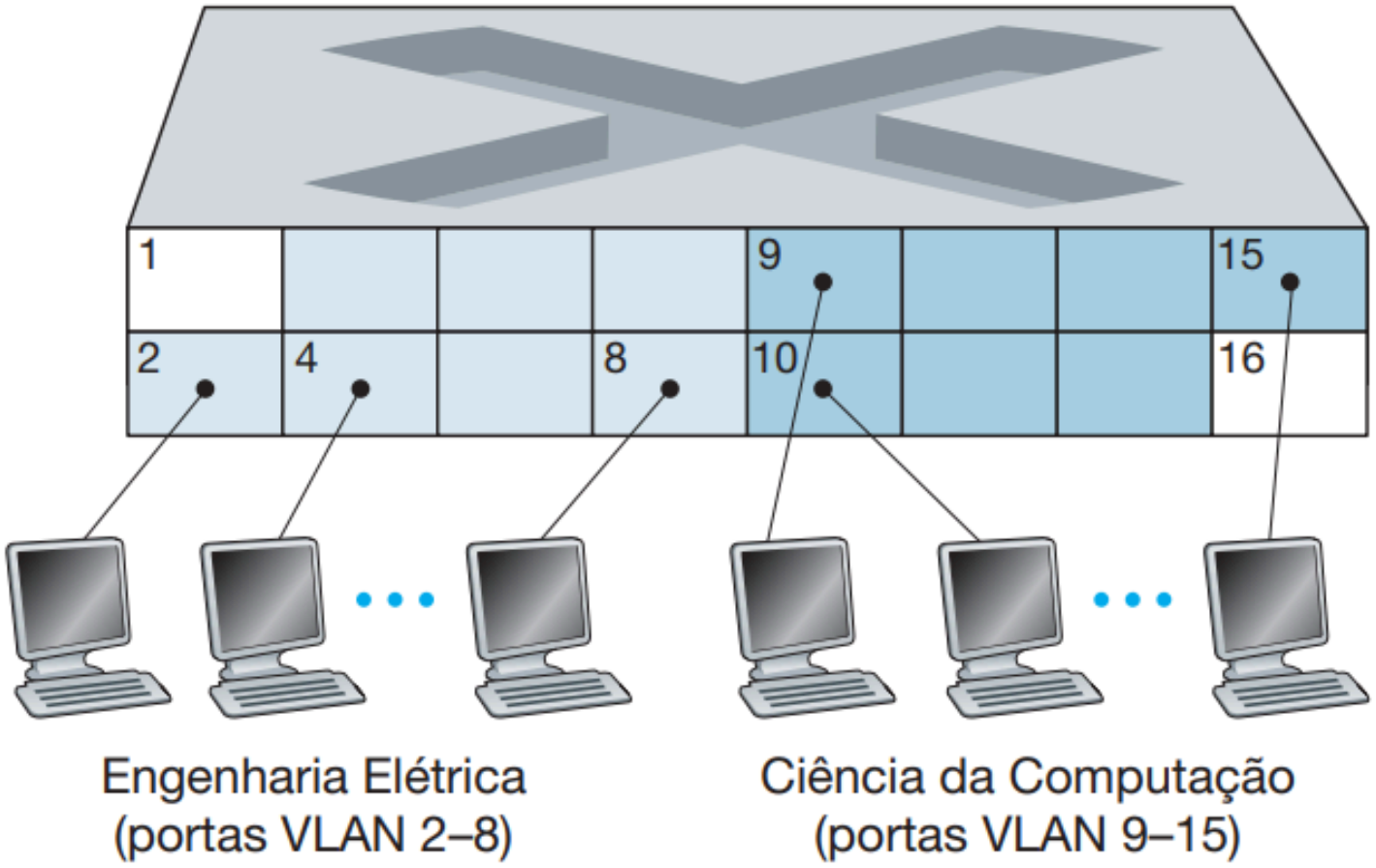
- As VLANs dividem uma rede em segmentos lógicos distintos, reduzindo o domínio de broadcast a cada VLAN individualmente.

- Isso significa que os pacotes de broadcast enviados em uma VLAN não são propagados para outras VLANs, o que melhora a eficiência da rede e reduz o tráfego desnecessário.

Virtualização de Redes

Um comutador que suporta VLANs (switch gerenciável) permite que diversas redes locais virtuais sejam executadas por meio de uma única infraestrutura física de uma rede local virtual.

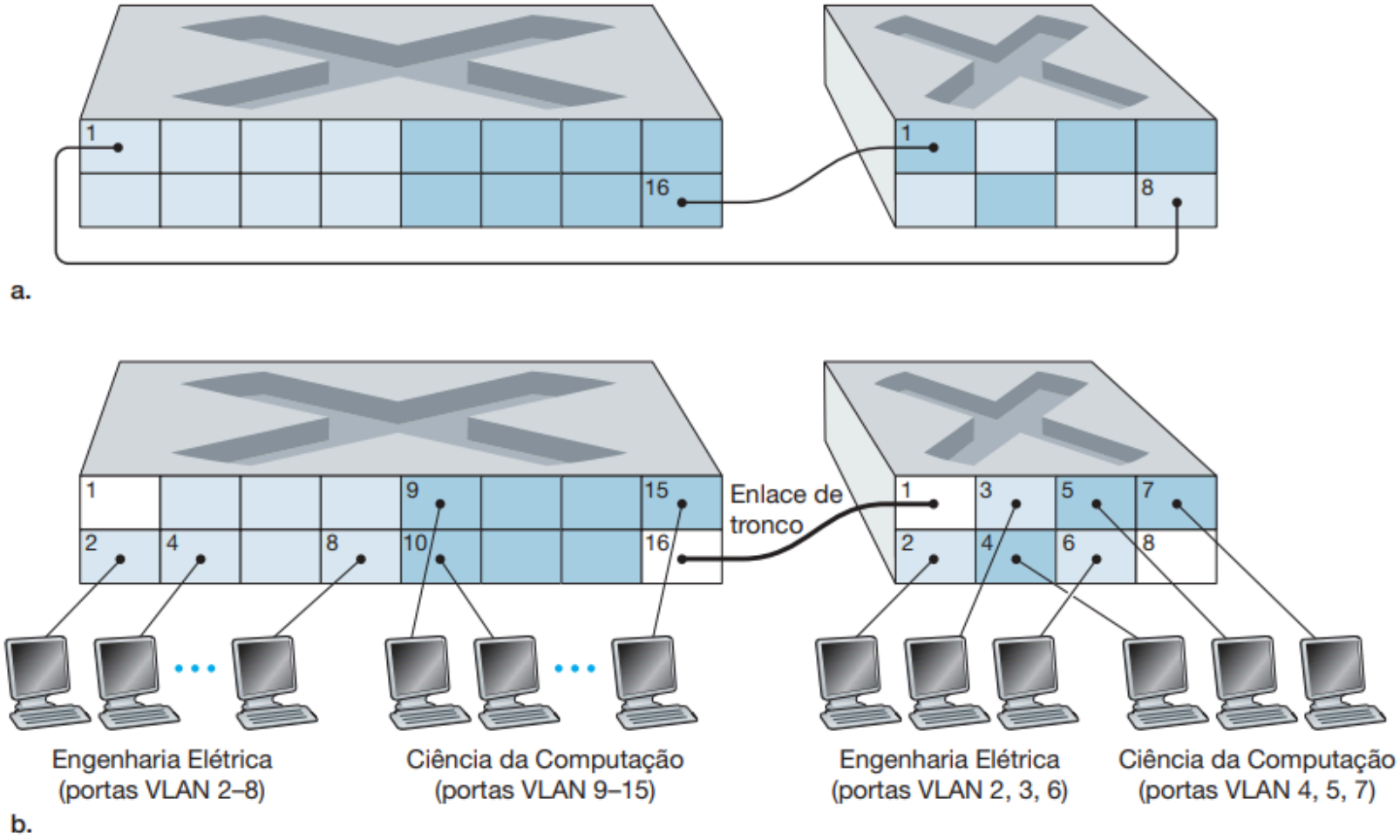
Virtualização de Redes



Fonte: Kurose, 2014.

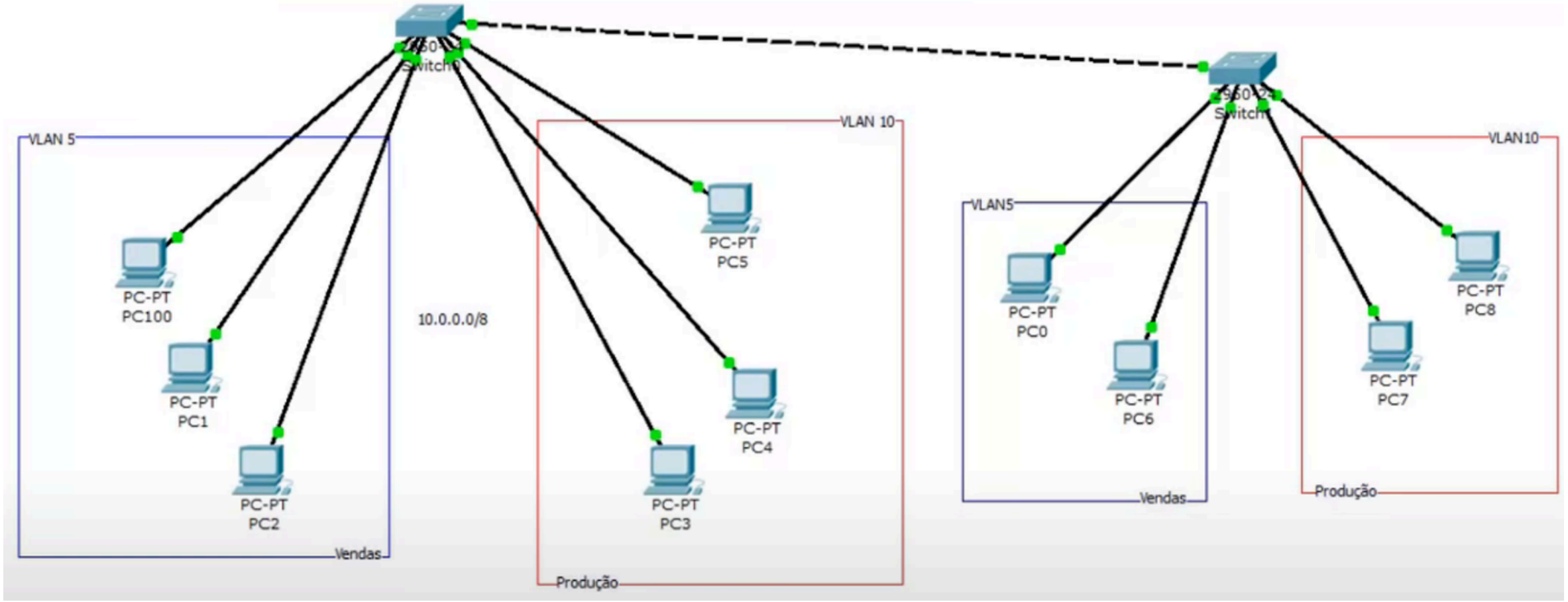
Virtualização de Redes

FIGURA 5.26 CONECTANDO 2 COMUTADORES DA VLAN A DUAS VLANS: (A) 2 CABOS (B) ENTRONCADOS



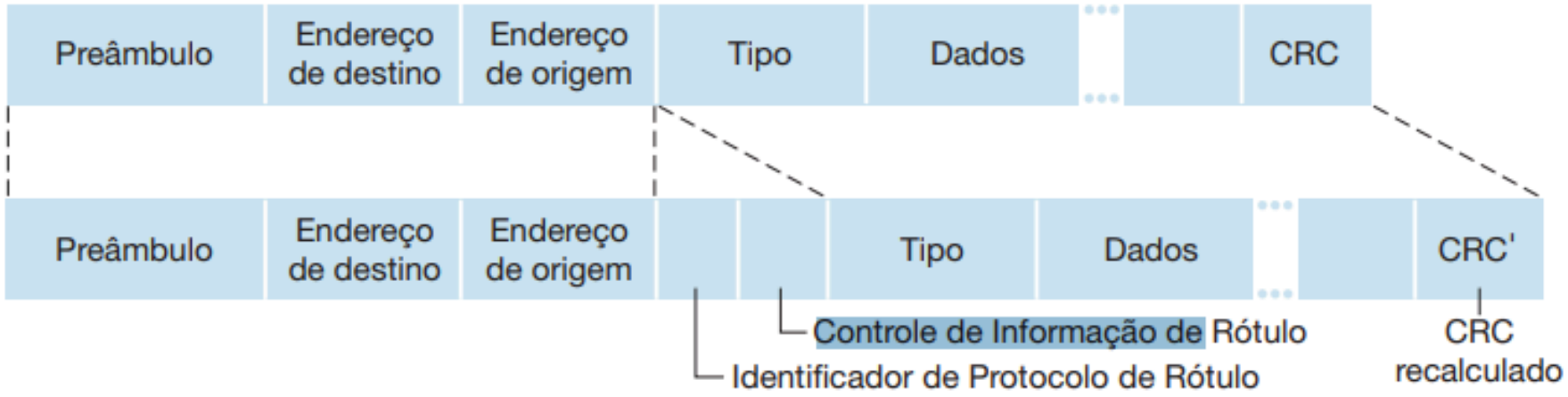
Fonte: Kurose, 2014.

Virtualização de Redes



Virtualização de Redes

FIGURA 5.27 QUADRO ETHERNET ORIGINAL (NO ALTO); QUADRO VLAN ETHERNET 802.1Q-TAGGED (EMBAIXO)



Fonte: Kurose, 2014.

Switch não gerenciável vs Switch gerenciável

Característica	Switch Não Gerenciável	Switch Gerenciável
Configuração e Controle	Não configurável; plug-and-play	Altamente configurável; ajustes detalhados possíveis
Funcionalidade	Função básica de comutação; sem suporte a VLANs	Funcionalidades avançadas; suporte a VLANs, QoS, etc.
Gerenciamento e Monitoramento	Sem opções de monitoramento ou diagnósticos	Monitoramento detalhado; geração de logs e alertas
Escalabilidade e Flexibilidade	Menos flexível; adequado para redes pequenas	Mais flexível; adequado para redes grandes e complexas
Custo	Mais barato	Mais caro
Uso Típico	Pequenas redes domésticas ou de escritório	Redes empresariais, data centers, ambientes complexos

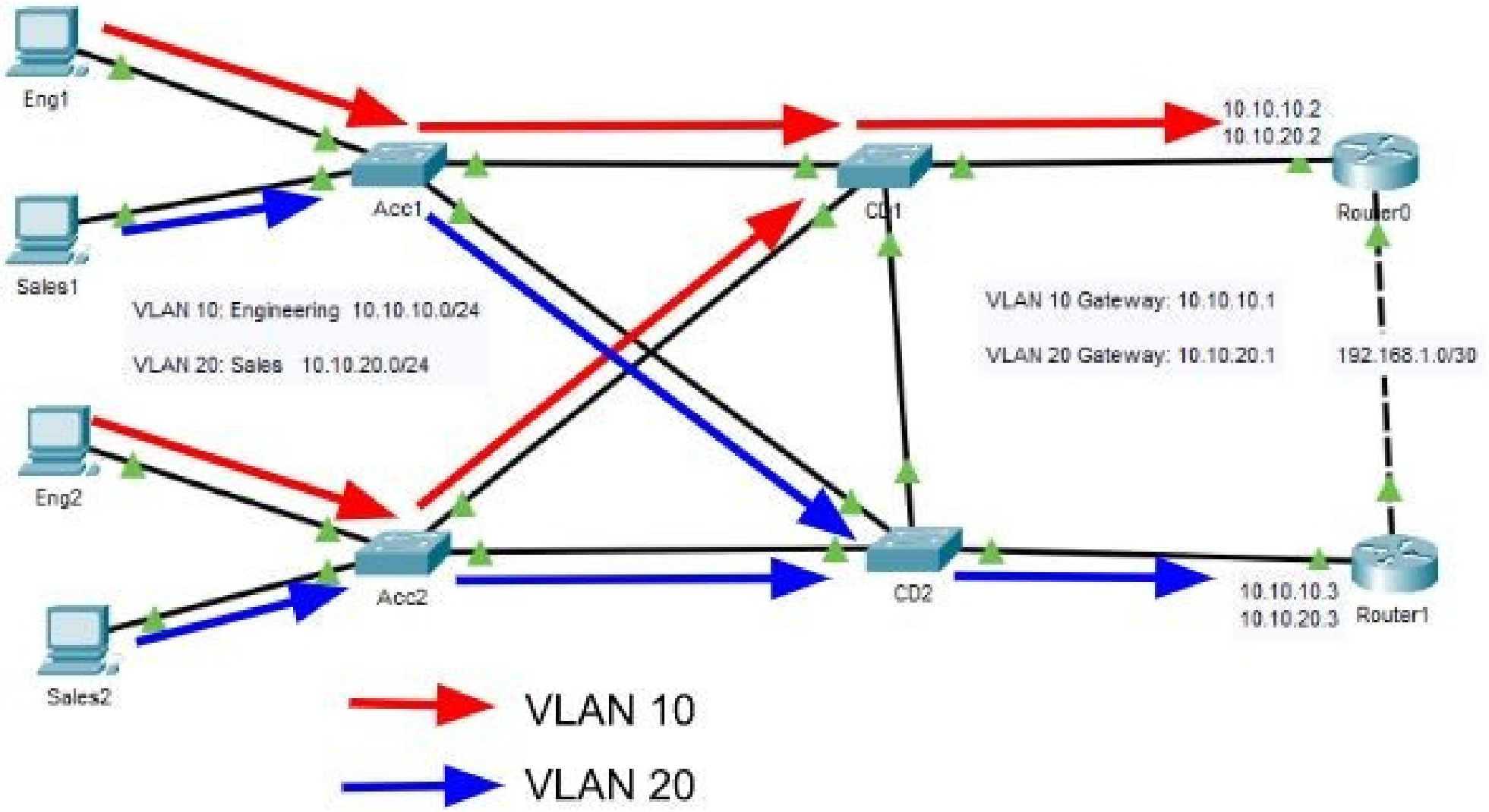
Virtualização de Redes

É possível definir VLANs não apenas através das portas, mas também por meio de endereços MAC ou endereços IP.

Switch Camada 3 vs Roteador

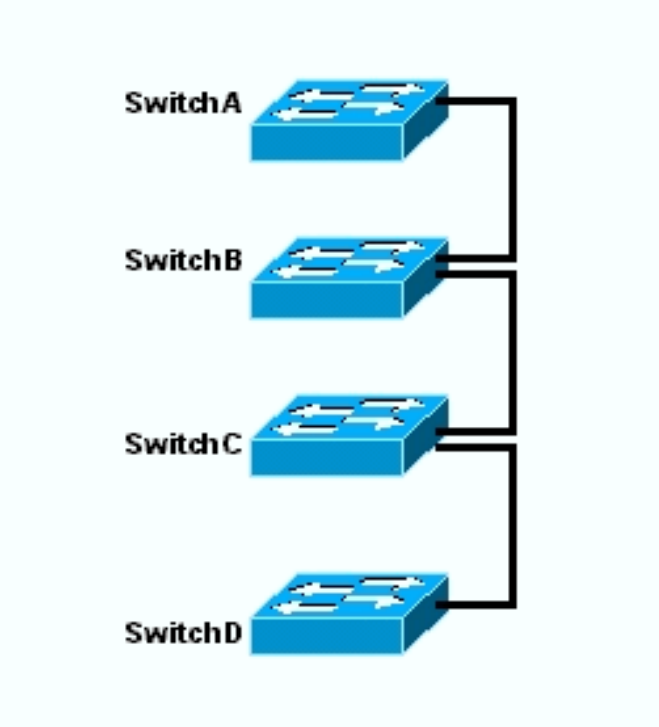
Característica	Switch de Camada 3	Roteador
Função Principal	Roteamento interno entre VLANs ou sub-redes dentro da mesma rede local	Roteamento entre diferentes redes, incluindo a Internet
Camada de Operação	Camada 3 (rede)	Camada 3 e superior
Capacidades	Roteamento Inter-VLAN, roteamento básico	Roteamento avançado, NAT, firewall, VPN, QoS
Desempenho	Alta performance em ambientes locais	Versatilidade em redes internas e externas
Uso Típico	Redes corporativas e locais onde é necessário roteamento interno	Conexão de redes internas com externas e à Internet

MSTP e VLAN's


Eng1
Sales1
Eng2
Sales2
Acc1
Acc2
CD1
CD2
Router0
Router1
10.10.10.2
10.10.20.2
10.10.10.3
10.10.20.3
192.168.1.0/30
VLAN 10: Engineering 10.10.10.0/24
VLAN 20: Sales 10.10.20.0/24
VLAN 10 Gateway: 10.10.10.1
VLAN 20 Gateway: 10.10.20.1
VLAN 10
VLAN 20

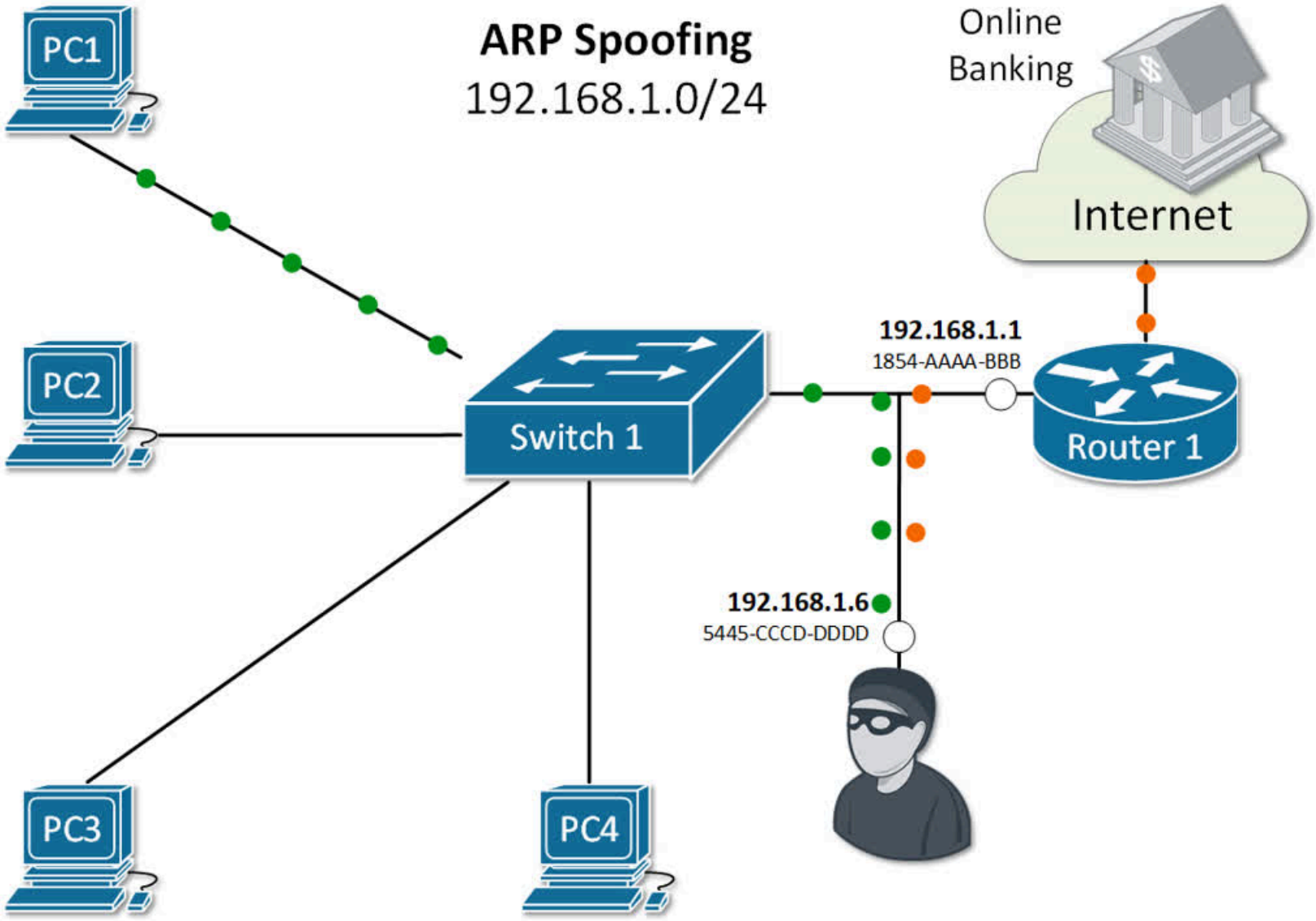
Empilhamento de switch

- **Empilhamento** cria uma unidade lógica única a partir de vários switches conectados fisicamente.
- **Cascateamento** conecta switches em série, formando uma cadeia.
- **Cluster** agrupa switches para gestão unificada e melhor desempenho.



Segurança na camada de enlace

Prevenção ARP Spoofing



Prevenção ARP Spoofing

- **Inspeção dinâmica de ARP:**
  - **DHCP Snooping:** Constrói um banco de dados confiável de associações IP-MAC ao monitorar mensagens DHCP.
  - A ideia principal é que, se você atribuir dinamicamente endereços IP para hosts com DHCP, o switch pode monitorar as mensagens DHCP e rastrear qual IP é dado a qual host na LAN.
- Limitação de Taxa de ARP.
- Registro de DAI.

Segurança de Porta

- Bloqueia o acesso à rede com base exclusivamente no endereço MAC.

- Permite que você defina quais endereços MAC são permitidos em uma porta específica, e pode tomar ações como proteger, restringir ou desativar a porta se houver uma violação da política de segurança.

Segurança de Porta

- Fácil de configurar e eficaz para proteger portas contra acessos não autorizados.

- Falsificação de MAC: Endereços MAC podem ser facilmente falsificados.

- Requer manutenção e configuração adequadas para garantir que endereços MAC autorizados sejam gerenciados corretamente.

Criptografia em Redes Padrão Wifi

- **WEP *(Wired Equivalent Privacy):***
  - Um dos primeiros métodos de segurança para redes Wi-Fi.
  - Usa uma chave de criptografia compartilhada para proteger os dados.
  - Seu uso não é recomendado.
- **WPA *(Wi-Fi Protected Access):***
  - Melhorou a segurança em comparação com o WEP.
  - Usa o TKIP (*Temporal Key Integrity Protocol*) para criptografar dados.

Criptografia em Redes Padrão Wifi

- **WPA2 (*Wi-Fi Protected Access II*)**
  - Usa o AES (Advanced Encryption Standard) para criptografia, mais seguro que o TKIP.
  - Padrão mais utilizado.
- **WPA3** (***Wi-Fi Protected Access III***)
  - Introduz o SAE (*Simultaneous Authentication of Equals*) para melhor proteção contra ataques de força bruta e melhor segurança em redes públicas.

Wi-Fi *Protected Setup* (WPS)

Padrão desenvolvido para facilitar a configuração de redes Wi-Fi seguras, permitindo que dispositivos se conectem à rede sem a necessidade de inserir manualmente uma senha.

Wi-Fi *Protected Setup* (WPS)

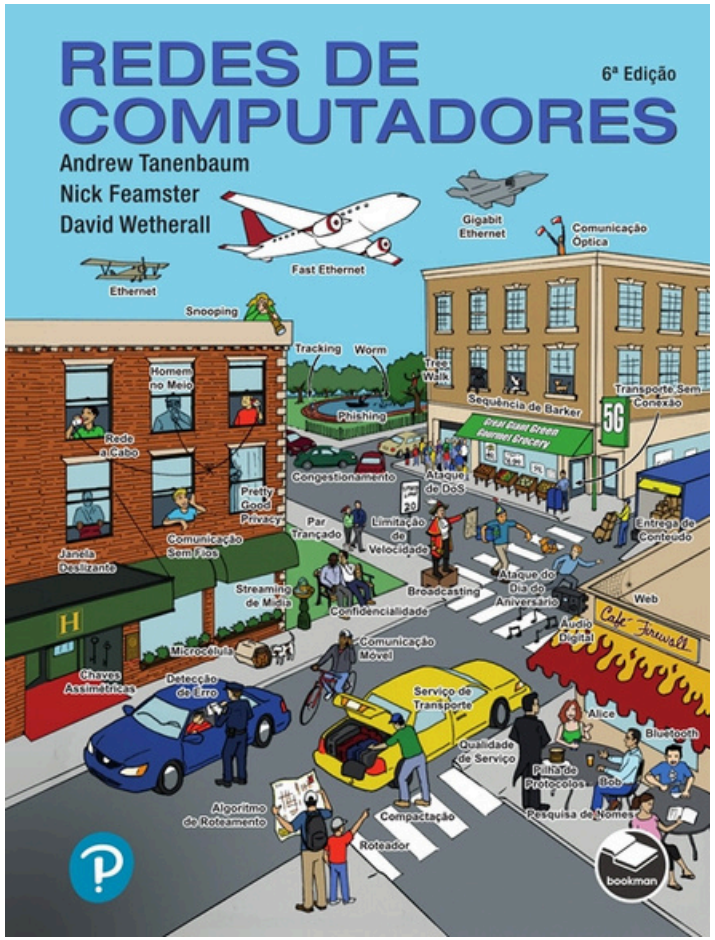
- Botão de Configuração (Push Button Connect): O usuário pressiona um botão físico no roteador e no dispositivo cliente para estabelecer uma conexão segura.
- PIN de 8 Dígitos: O roteador e o dispositivo cliente usam um PIN de 8 dígitos para autenticar a conexão. O PIN pode ser inserido manualmente no dispositivo cliente.
- Um atacante pode usar um ataque de força bruta para tentar todas as combinações possíveis do PIN, obtendo o PIN correto em poucas horas.

Simple Network Management Protocol (SNMP)

O *Simple Network Management Protocol* (SNMP) é um protocolo usado para gerenciar e monitorar dispositivos de rede, permitindo que administradores coletem informações de status, configurem dispositivos e recebam notificações de eventos em uma rede.

Leitura Recomendada

Capítulo 3 do livro:
Redes de Computadores



Capítulo 2 do livro:
Redes de Computadores e a Internet

Leitura Recomendada

Leitura Extra e Opcional:

Redes de Computadores
para quem está começando

Referências

KUROSE, J. & ROSS, K. Computer Networking: A Top-Down Approach Featuring the Internet. Addison-Wesley, 2014, sexta edição

TANENBAUM, Andrew. Redes de Computadores. 5a. Edição. Editora Campus, Ltda. 2011

FOROUZAN, Behrouz, MOSHARRAF, Firouz, Redes de Computadores. Uma abordaegm Top-Down, McGrtaw Hill, 2014

Redes de Computadores

Marisangila Alves, MSc

marisangila.alves@proton.me