

## Olá! Tudo bem?

Seja bem-vindo(a) à Webaula 5 de Redes de Computadores.

| INTRODUÇÃO                                |  |  |  |
|---|--|--|--|
| Introdução à Webaula 5                    |  |  |  |
| ÓPICO 1                                   |  |  |  |
| Transmissão de Quadros em Enlaces de Rede |  |  |  |
| ÓPICO 2                                   |  |  |  |
| Padrões IEEE 802                          |  |  |  |
| Atividade de Passagem                     |  |  |  |
| TÓPICO 3                                  |  |  |  |
| Ligação Inter-Redes                       |  |  |  |
| Atividade de Passagem                     |  |  |  |
| ESUMO                                     |  |  |  |

| =     | Resumo da Webaula 5 |
|-------|---------------------|
| REFER | ÊNCIAS              |
| =     | Referências         |
| =     | Créditos            |

# Introdução à Webaula 5

Conforme vimos na introdução do nosso estudo de redes de computadores, a camada de enlace do modelo TCP/IP é responsável por criar um canal de comunicação livre de erros entre dois nós adjacentes de uma rede. A camada de enlace tem por objetivo transmitir os **quadros** com os dados enviados pela camada de rede. O protocolo de camada de enlace define o formato dos quadros trocados entre nós adjacentes bem como as ações realizadas por esses nós ao enviar e receber os pacotes da camada de rede (KUROSE; ROSS, 2013).

As funcionalidades que o protocolo da camada de enlace pode executar ao enviar e receber quadros entre nós de uma rede são:

- entrega confiável: garante a entrega dos quadros sem erros, através de confirmações de recebimento e pedidos de retransmissão, principalmente em enlaces baseados em tecnologias suscetíveis a erros de transmissão, como por exemplo em redes sem fio;
- detecção de erros: inclui bits redundantes de verificação de erros no quadro para que o nó de recepção verifique a sua integridade;
- retransmissão de quadros: requisita ao nó de envio a retransmissão de um quadro recebido com erros;
- controle de fluxo: previne que o nó de envio sobrecarregue a memória do nó de recepção, limitando a taxa de transmissão à capacidade do nó receptor de tratar os quadros recebidos;

- enquadramento de dados: especifica os campos da estrutura do quadro da camada de enlace utilizado para encapsular o pacote de dados da camada de rede;
- acesso ao meio físico: especifica a estrutura do quadro e as regras do protocolo de acesso ao meio físico utilizado na transmissão.

A implementação do protocolo das camadas física e de enlace em um nó está presente nas **placas de rede**, cujo objetivo é prover funcionalidades entre as listadas acima.

Observe que o processamento dos quadros é feito de forma independente do processamento do equipamento que contém a placa de rede, a qual somente encaminha o pacote extraído do quadro para o sistema operacional quando este for dirigido para o próprio equipamento e tiver sido recebido sem erros através do enlace.

Esta aula tem como objetivo que você reconheça como funcionam os principais padrões das placas de rede utilizadas nas LANs assim como quais são os principais equipamentos de interconexão de redes presentes nas infraestruturas LAN.

E então, vamos começar?

CONTINUE

# Transmissão de Quadros em Enlaces de Rede

Primeiramente você precisa saber que erros de transmissão em enlaces de rede são relativamente comuns, principalmente em alguns meios, como na transmissão sem fio e de fios de par trançado. Como resultado dos processos físicos que os geram, os erros tendem a acontecer mais frequentemente em grandes volumes (rajadas) do que separadamente.

Mas você já pensou como é que uma interface de rede é capaz de saber se um bit recebido está certo ou errado? Pois a estratégia básica para tratar erros utiliza códigos de **detecção de erros**, onde se inclui redundância de dados suficiente para permitir que o receptor deduza que houve um erro, sem identificar qual, e descarte os dados recebidos, podendo eventualmente solicitar uma retransmissão.

A forma mais simples de detecção de erro é através do uso de um bit de paridade. O bit de paridade acrescentado a um dado é escolhido de forma que o número de bits 1 do dado seja par ou ímpar. Por exemplo, quando o byte 10101100 é enviado com paridade par através da inclusão de um bit no final, a sequência transmitida passa a ser 101011000, ao passo que, com paridade ímpar, passa a ser 101011001. Observe que este método é capaz de detectar apenas um número ímpar de erros por dado.

Outra técnica de detecção de erro é denominada soma de verificação. Este método simplesmente soma os bytes (ou conjunto deles formando inteiros de 16 ou 32 bits) e o resultado complemento de 1 é enviado junto com o dado. Desta forma, o receptor precisa somar todos estes bytes (ou conjunto deles) com a soma de verificação e, se o seu resultado for nulo, pode concluir que não houve erro na sua transmissão.

Outro método muito difundido é o **método polinomial** ou **CRC** (*Cyclic Redundancy Check*). Quando o método do CRC é empregado, o transmissor e o receptor devem concordar em relação ao **polinômio** 

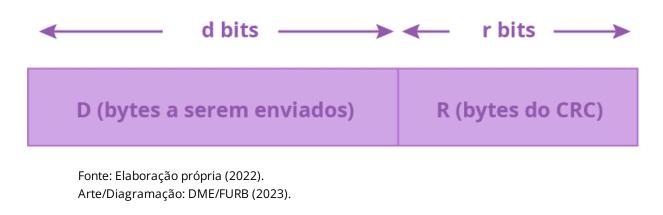
 ${\bf gerador}\,(G_{CRC})\, antecipa damente.\,\, Na\,\, internet,\, os\, dois\, principais\, polinômios\, geradores\, são:$ 

 $G_{CRC-16} = 1100000000000101$ 

 $G_{CRC-32} = 100000100110000010001110110110111$ 

A ideia fundamental por trás dos códigos de CRC (Figura 1) baseia-se em escolher r bits adicionais, R, e os anexar a um dado D de comprimento d de modo que o padrão de d bits concatenados com os r bits resultantes seja divisível exatamente por  $G_{CRC}$ . Portanto, para o cálculo do CRC é preciso calcular o resto da divisão R tal que ( $D.2^r$ ) xor R seja divisível por  $G_{CRC}$  (KUROSE; ROSS, 2013).

Figura 1 - CRC a ser enviado com um pacote



Apesar de o cálculo necessário para computar o CRC parecer complicado, um simples circuito de registro de deslocamento permite calcular e verificar CRCs no nível de hardware.

Os padrões de CRC identificam rajadas de erro de até r+1 bits e qualquer número ímpar de bits errados. Dos métodos de detecção de erros apresentados, o CRC é a técnica mais confiável.

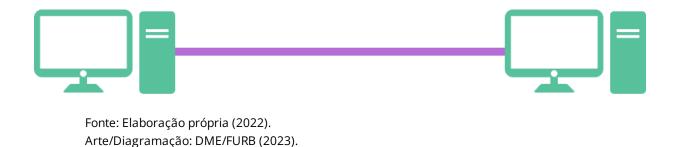
(i)

#### Reflita

Por que detectar erros através do CRC é mais confiável que através da soma de verificação ou do bit de paridade?

Quanto aos enlaces de rede, há dois tipos básicos: o **enlace ponto** a **ponto** e o **enlace de difusão**. O enlace ponto a ponto, representado esquematicamente na Figura 2, consiste em uma terminação de um enlace (um equipamento emissor) enviando bits à outra terminação de enlace (um equipamento receptor). Há vários protocolos que se destinam a este tipo de enlace, entre os quais se destaca o **PPP** (*Point-to-Point Protocol*).

Figura 2 - Enlace Ponto a Ponto



Por outro lado, o enlace de difusão permite que vários emissores e receptores estejam conectados a um mesmo, único e compartilhado canal de comunicação, como pode ser observado em diferentes tecnologias de rede representadas na Figura 3. As redes sem fio são exemplos de enlaces de difusão.

Como nesse tipo de protocolo mais de uma estação pode transmitir quadros ao mesmo tempo, é sua a responsabilidade de gerir o acesso ao meio de transmissão, pois nesse caso todos os nós receberão vários quadros ao mesmo tempo, ocorrendo uma colisão dos quadros nos receptores. Os quadros envolvidos na colisão são perdidos e o canal de difusão é desperdiçado durante o intervalo da colisão.

Figura 3 - Enlaces de Difusão



Fonte: Elaboração própria (2022). Arte/Diagramação: DME/FURB (2023).

Os equipamentos de uma LAN enviam quadros entre si normalmente através de um enlace de difusão. Isto significa que, quando um equipamento da LAN transmite um quadro, todos os outros equipamentos conectados o recebem.

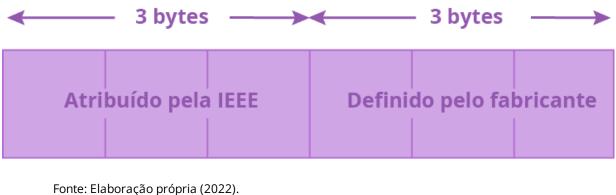
Mas como é que uma interface de rede de um equipamento pode saber se o quadro é ou não destinado a ele? Para permitir que um quadro seja enviado somente a um equipamento em particular, é preciso que este tenha um endereço específico que o identifique univocamente. Desta forma, quando a placa de rede dos equipamentos conectados à rede receberem um quadro, se o endereço de destino do quadro é igual ao endereço da placa de rede que o recebeu ou é um endereço de difusão, o pacote é extraído e passado para o protocolo da camada de rede; caso contrário, a placa de rede do equipamento simplesmente descarta o quadro.

Este endereço da placa de rede do equipamento é denominado **endereço físico** ou **endereço MAC** (*Media Access Control*), e é dado por 6 bytes expressos através da notação hexadecimal. Estes endereços são permanentes para cada placa de rede e programados durante a sua manufatura de

forma que não haja duas placas no mundo com o mesmo endereço MAC. Quem é responsável por gerenciar e distribuir estes endereços é a IEEE (KUROSE; ROSS, 2013).

Para garantir a unicidade dos endereços MAC, a empresa fabricante de placas de rede adquire da IEEE os 3 primeiros bytes do endereço e faz a combinação que quiser dos 3 últimos bytes (Figura 4).

Figura 4 - Alocação do Espaço de Endereços MAC



Fonte: Elaboração própria (2022). Arte/Diagramação: DME/FURB (2023).

### CONTINUE

## Padrões IEEE 802

O IEEE é uma organização profissional sem fins lucrativos, composta por engenheiros de todas as áreas da tecnologia, que se dedica ao avanço da tecnologia. Um de seus papéis mais difundidos é o estabelecimento de padrões para formatos e protocolos de comunicação entre computadores e dispositivos eletrônicos.

O conjunto de padrões IEEE 802 tem como objetivo definir uma padronização das camadas física e de enlace para LANs. Os padrões IEEE 802 oferecem um serviço de transporte de datagramas.

Os padrões IEEE 802 de LAN diferem na camada física e na subcamada MAC (*Media Access Control*) da camada de enlace, mas são compatíveis a partir da camada de enlace em função do LLC (*Logical Link Control* – IEEE 802.2). O MAC tem por objetivo gerir o acesso múltiplo a uma rede de difusão, determinando quem será o próximo a usar o canal (MENDES, 2010).

O IEEE 802.3, também denominado Ethernet, apesar de haver uma diferença em um campo do quadro destes dois protocolos, fornece um serviço sem conexão e não confiável à camada de rede.

A Ethernet é uma LAN CSMA/CD (Carrier Sense Multiple Access/Collision Detection). Isso significa que quando uma estação estiver ligada a um barramento de difusão e quiser transmitir, ela deve escutar o meio. Se o meio de transmissão estiver ocupado, a estação aguarda até que ele fique livre; caso contrário, ela começa imediatamente a transmitir.

Se duas ou mais estações começarem a transmitir simultaneamente em um meio desocupado, haverá uma colisão. Neste caso, todas as estações que colidirem terminam a transmissão, aguardam durante um tempo aleatório e então repetem o processo novamente.

| O padrão IEEE 802.3 está definido para as seguintes taxas de transmissão: |   |  |
|---|---|--|
| (Clique nos cartões para acessar os conteúdo                              | os)   |  |
| 10 Mbps ( <b>Ethernet</b> )   | Padrão IEEE 802.3i para par<br>trançado e IEEE 802.3j para<br>fibra óptica; |  |
| 100 Mbps ( <b>Fast Ethernet</b> )   | Padrão IEEE 802.3u para par<br>trançado e para fibra óptica;                |  |
|   |   |  |



Padrão IEEE 802.3an para par trançado e IEEE 802.3ae para fibra óptica.

O formato do quadro IEEE 802.3/Ethernet está representado na Figura 5.

Figura 5 - Formato do Quadro IEEE 802.3/Ethernet

| 6       | 6      | 2              | 461500 | 4   |
|---------|--------|----------------|--------|-----|
| Destino | Origem | Tipo ou Compr. | Dados  | CRC |
|         |        |                |        |     |

Fonte: Elaboração própria (2022). Arte/Diagramação: DME/FURB (2023).

Cada um dos seus campos tem a seguinte função:

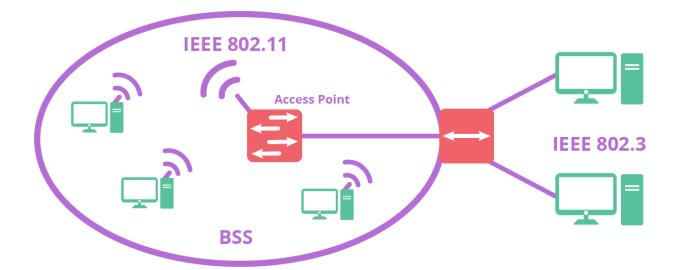
- destino: contém o endereço MAC da placa de rede do equipamento de destino;
- origem: contém o endereço MAC da placa de rede do equipamento de origem;

- tipo (Ethernet): indica a que tipo de protocolo de rede pertencem os dados enviados pelo quadro;
- **comprimento** (IEEE 802.3): indica quantos bytes existem no campo de dados, que neste caso inclui o cabeçalho LLC (IEEE 802.2);
- dados: contém o pacote da camada de rede. O tamanho máximo é de 1500 bytes e o tamanho mínimo é de 46 bytes – requisito necessário para garantir a indicação de colisão ao longo da rede;
- CRC: contém o valor do CRC de todos os campos do quadro

O WiFi (*Wireless Fidelity*), nome dado ao padrão **IEEE 802.11**, é uma família de especificações de uma arquitetura de rede local sem fio (**WLAN** – *Wireless LAN*) que se baseia em uma divisão da área de cobertura em células, denominadas **BSSs** (*Basic Service Set*), as quais contêm uma estação base denominada **AP** (*Access Point*), cuja topologia de infraestrutura está representada na Figura 6.

O tamanho das BSSs, tipicamente de 500 m2, depende das características do ambiente e dos receptores utilizados. As BSSs são identificadas por um SSID (Service Set Identifier) (MENDES, 2010). Esse SSID é aquele "apelido" que você dá para sua rede ou que você procura quando busca uma rede sem fio para acessar.

## Figura 6 - Rede IEEE 802.11



Fonte: Elaboração própria (2022). Arte/Diagramação: DME/FURB (2023).

Há atualmente cinco especificações na família 802.11:

(Clique no + para acessar os conteúdos)

#### IEEE 802.11a \_

A taxa máxima de transmissão é de 54 Mbps, operando na faixa de frequência de 5 GHz (OFDM – *Orthogonal Frequency Division Multiplexing*);

#### IEEE 802.11b \_\_

A taxa máxima de transmissão é de 11 Mbps, operando na faixa de frequência de 2,4 GHz (HR-DSSS – High Rate Direct Sequence Spread Spectrum);

#### IEEE 802.11g \_

A taxa máxima de transmissão é de 54 Mbps, operando na faixa de frequência de 2,4 GHz (OFDM);

#### IEEE 802.11n \_\_

A taxa máxima de transmissão é de 450 Mbps, operando na faixa de frequência de 2,4 ou 5 GHz (OFDM com MIMO – Multiple Input Multiple Output);

#### IEEE 802.11ac \_\_

A taxa máxima de transmissão é de 1,3 Gbps, operando na faixa de frequência de 5 GHz (OFDM com MIMO).

Uma rede sem fio é uma rede de difusão que usa uma mesma frequência em um mesmo meio de transmissão e, portanto, somente um equipamento pode transmitir por vez. Você já pensou como é que se decide quem é o próximo equipamento que irá transmitir? Quem faz isso é um protocolo de acesso ao meio do padrão IEEE 802.11 do tipo de coordenação distribuída, onde a decisão de transmitir é tomada individualmente pelas estações, conhecido por CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance).

Esse método de controle de acesso ao meio gera uma perda expressiva da taxa de transmissão, fazendo com que a taxa de transmissão efetiva de dados (*throughput*) seja em torno de 40% da taxa de

transmissão nominal dos padrões IEEE 802.11.

No CSMA/CA, quando uma estação ou um AP deseja transmitir um quadro, sente o meio para determinar se alguma outra estação está transmitindo. Se o meio permanecer livre por um período conhecido por DIFS (Distributed Inter-Frame Space), a estação ou AP transmite um pedido de transmissão. Caso contrário, a estação ou o AP espera o final de alguma transmissão, aguarda um DIFS e mais um tempo aleatório e reinicia o processo.

Quando o AP (no caso em que o quadro tiver sido transmitido por uma estação) ou a estação de destino (no caso em que o quadro tiver sido transmitido por um AP) tiver recebido a autorização para transmitir, ele/ela envia o quadro completo, e então ela/ele, após um curto período conhecido por SIFS (Short Inter-Frame Space), devolve um quadro de confirmação.

Ao receber o quadro de confirmação, a estação ou o AP saberá que o quadro foi enviado com sucesso. Caso contrário, a estação ou o AP aguarda um DIFS e mais um tempo aleatório e retransmite o quadro, reiniciando o processo.



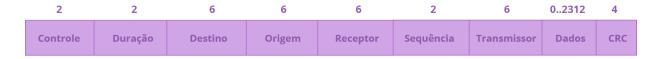
#### (i) Leitura Complementar

Para reforçar o entendimento da diferença dos tipos de controle de acesso ao meio CSMA/CD e CSMA/CA, veja a comparação aqui.

Quando as estações se comunicam através de um AP, a topologia da rede chama-se infraestrutura. O padrão IEEE 802.11 permite também que duas estações se comuniquem diretamente através uma rede sem fio utilizando um enlace ponto a ponto: neste caso a topologia da rede chama-se ad hoc. A implantação de um enlace ponto a ponto de uma rede sem fio IEEE 802.11, utilizando antenas direcionais, é um meio barato de disponibilizar conexões sem fio por vários quilômetros.

O formato do quadro IEEE 802.11 está representado na Figura 7.

## Figura 7 - Formato do Quadro IEEE 802.11



Fonte: Elaboração própria (2022). Arte/Diagramação: DME/FURB (2023).

Cada um dos seus campos tem a seguinte função:

- controle: contém bits para a identificação do tipo de quadro, topologia da rede utilizada e identificação do mecanismo de segurança ativo;
- duração: indica o tempo necessário para transmitir o quadro completo;
- endereço de destino: contém o endereço MAC da placa de rede do equipamento de destino;
- endereço de origem: contém o endereço MAC da placa de rede do equipamento de origem;
- endereço do receptor: contém o endereço MAC do próximo equipamento a receber o quadro (pode ser uma placa de rede de equipamento ou de AP);
- sequência: contém um número sequencial para permitir ao receptor distinguir entre um quadro novo recém-transmitido e a retransmissão de um quadro anterior;
- endereço do transmissor: contém o endereço MAC do último equipamento que transmitiu o quadro (pode ser uma placa de rede de equipamento ou de AP);
- dados: contém o pacote da camada de rede;

CRC: contém o valor do CRC dos campos do quadro.

Como a transmissão por uma rede sem fio ocorre pelo ar, você percebe que qualquer um pode "ouvir" o que está sendo transmitido? Por isso a segurança é uma preocupação particularmente importante em redes sem fio, nas quais ondas de rádio portando quadros podem se propagar para muito além do local onde estão as estações da rede. Neste contexto, a IEEE especificou um protocolo de segurança do nível de enlace chamado WEP (Wired Equivalent Privacy), projetado para tornar a segurança de uma WLAN tão boa quanto à de uma LAN fisicamente conectada (FOROUZAN, 2008).

O WEP fornece autenticação e criptografia de dados entre uma estação e um AP, utilizando uma abordagem de chaves simétricas compartilhadas, cuja forma de distribuição não é especificada. A criptografia do WEP utiliza o algoritmo RC4 sobre os dados do quadro com seu CRC-32.

Com o passar dos anos, a segurança das redes WiFi baseada no protocolo WEP utilizando RC4 mostrou-se bastante fraca. Em função disto, iniciou-se um processo de criação de um novo padrão de segurança robusto para redes sem fio. Enquanto o padrão não era homologado, um subconjunto da sua proposta foi publicado e solucionava vários problemas do WEP, mas não teve grande aceitação da indústria, pois se tratava de uma proposta intermediária de segurança do WiFi. Esta solução temporária chamou-se WPA (*WiFi Protected Access*).

O padrão definitivo de segurança para redes WiFi, chamado IEEE 802.11i ou WPA2 (WiFi Protected Access version 2), fornece, além de um conjunto extensível de mecanismos de autenticação e um mecanismo de distribuição de chaves, várias formas de criptografia, incluindo um esquema criptográfico baseado no algoritmo AES e integrado a uma versão reforçada do protocolo WEP.

## i

#### Leitura Complementar

Para reforçar o entendimento da diferença dos padrões de segurança das redes WiFi, veja a comparação e as dicas <u>aqui</u>.

## CONTINUE

# Atividade de Passagem

(ENADE) Em redes locais de computadores, o protocolo de controle de acesso ao meio define um conjunto de regras que devem ser adotadas pelos múltiplos dispositivos para compartilhar o meio físico de transmissão. No caso de uma rede Ethernet IEEE 802.3 conectada fisicamente a um *hub*, em que abordagem se baseia o protocolo de controle de acesso ao meio?

- na passagem de permissão em anel
- na ordenação com contenção
- na ordenação sem contenção
- na contenção com detecção de colisão
- na arbitragem centralizada

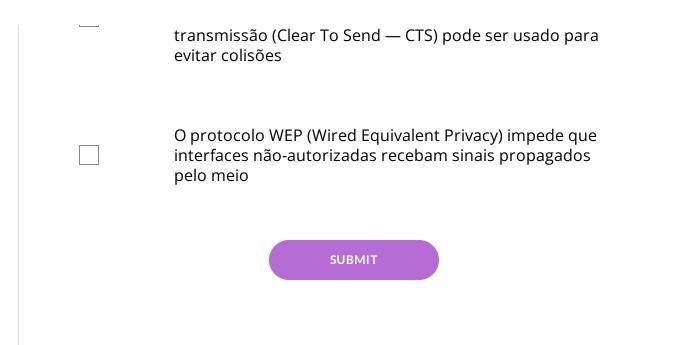
(ENADE) Redes locais sem fio que utilizam tecnologia IEEE 802.11, comumente referenciada como WiFi, estão se tornando cada vez mais populares. Julgue quais dos itens abaixo são VERDADEIROS, relativos a essa tecnologia.

Computadores em redes IEEE 802.11 podem-se comunicar por dois modos básicos: usando uma infraestrutura coordenada por pontos de acesso à rede (Access Points — AP), ou no modo *ad hoc*, em que cada computador troca informações diretamente com os demais

Para poder transmitir por meio de um ponto de acesso, uma interface de rede deve realizar um procedimento de associação, que inclui o conhecimento de um campo identificador (Service Set Identifier — SSI)

Um mecanismo de detecção de colisão durante a transmissão indica a necessidade de retransmissão e evita o envio de mensagens de confirmação

Um mecanismo de requisição para transmissão (request to send — RTS) e de liberação para



(ENADE) A arquitetura do padrão IEEE 802.11 (WiFi) é constituída fundamentalmente pelo conjunto básico de serviço (Basic Service Set – BSS). Um BSS contém uma ou mais estações sem fio e uma estação base, conhecida como Access Point (AP). Ao instalar um AP, um administrador de rede designa ao AP um Identificador de Conjunto de Serviços (Service Set Identifier – SSID). Cada estação sem fio precisa se associar com um AP antes de poder enviar e receber quadros IEEE 802.11. Suponha que um determinado restaurante no centro de uma cidade é atendido por dois provedores de acesso à Internet (Internet Service Provider - ISP) que trabalham no padrão 802.11b. Cada ISP opera seu próprio AP em sub-redes com endereços de Internet (Internet Protocol – IP) diferentes. Por desconhecimento, cada ISP considerou que a área do restaurante pertence a um de seus BSS e configurou seu respectivo AP para operar no mesmo canal (canal 3) na área do restaurante. Para que uma estação sem fio na área do

|            | associar-se aos dois SSID simultaneamente   |
|------------|---|
|            | associar-se a mais de um AP na mesma BSS  |
| $\bigcirc$ | comunicar-se simultaneamente com outra estação<br>sem a necessidade de associação   |
|            | associar-se a um SSID qualquer, desde que não haja<br>outra estação sem fio transmitindo simultaneamente<br>no canal 3      |
|            | comunicar-se simultaneamente com outra estação,<br>desde que cada estação se associe a um AP, ou seja, a<br>SSID diferentes |
|            | SUBMIT  |

(ENADE) "Historicamente, uma Ethernet foi inicialmente concebida como um segmento de um cabo coaxial em que um único canal de transmissão era

compartilhado por todas as estações de trabalho da rede local. A tecnologia Ethernet passou por uma série de evoluções ao longo dos anos e, na maioria das instalações atuais, as estações de trabalho são conectadas a um comutador (switch) utilizando uma topologia física estrela." Considerando a utilização do protocolo CSMA/CD em comutadores Ethernet, analise as seguintes asserções.

A utilização do protocolo CSMA/CD não é necessária em comutadores Ethernet transmitindo em modo full-duplex.

## **PORQUE**

Os comutadores, operando em modo full-duplex, mantêm canais de comunicação distintos para envio (TX) e recebimento (RX) de dados, além de não encaminhar mais do que um quadro por vez para a mesma interface (porta).

Acerca dessas asserções, assinale a opção correta:

- As duas asserções são proposições verdadeiras, e a segunda é uma justificativa correta da primeira
- As duas asserções são proposições verdadeiras, mas a segunda não é uma justificativa correta da primeira
- A primeira asserção é uma proposição verdadeira e a segunda, uma proposição falsa

- A primeira asserção é uma proposição falsa, e a segunda, uma proposição verdadeira
- Tanto a primeira quanto a segunda asserções são proposições falsas

SUBMIT

(ENADE) Um ponto de acesso é um dispositivo de camada 2 que funciona como um *hub* 802.3 Ethernet. A rádio frequência é um meio compartilhado, e pontos de acesso escutam todo o tráfego de rádio. Assim como no padrão IEEE 802.3 Ethernet, dispositivos que operam no padrão IEEE 802.11 WLAN também disputam o meio para transmitir. Apesar disso, diferentemente das placas de rede Ethernet, dispositivos de rádio em vez de detectarem colisões são criados para evitá-las. Sobre a operação dos padrões IEEE 802.3 e 802.11, avalie as afirmações a seguir.

- I. O padrão IEEE 802.3 permite detecção de colisão.
- II. O método de acesso para o padrão 802.3 é o CSMA/CD, enquanto o padrão 802.11 faz uso de CSMA/CA.
- III. O padrão IEEE 802.11 usa o CSMA/CD como protocolo de acesso múltiplo ao meio.

IV. O quadro 802.11, assim como o quadro 802.3, inclui uma verificação de redundância cíclica (CRC). V. A transmissão no padrão IEEE 802.11 inicia-se assim que a estação percebe que o canal está ocioso. É correto apenas o que se afirma em: l e II. ll e III. III e IV. I, II e IV. I, III e IV. SUBMIT

(ENADE) Uma empresa multinacional fornecedora de peças e acessórios automotivos planeja a realização de um evento em um resort para os seus

parceiros de negócio. O objetivo principal do evento é realizar o treinamento da equipe de vendas, por meio de acesso aos sistemas da empresa e de forma secundária disponibilizar acesso a sites da web e correio eletrônico para uso particular dos parceiros. Conforme recomendação de padronização da área de TI, contratou-se um link de internet e configurou-se uma rede sem fio denominada "parceiros". Considerando os mecanismos de segurança em redes sem fio e para alcançar o objetivo desejado, avalie as afirmações a seguir.

- I. Para garantir a confidencialidade dos dados trafegados, recomenda-se a utilização de um protocolo de algoritmo simétrico, denominado WEP.
- II. Os usuários devem solicitar autenticação através de um portal web (HTTPS) e posteriormente o seu acesso será limitado à navegação web, correio eletrônico e acesso aos sistemas da empresa.
- III. Recomenda-se a utilização do padrão de segurança WPS (Wi-Fi Protected Setup) para garantir todos os requisitos citados.
- IV. Para aumentar a segurança da informação trafegada deve-se optar pela utilização do WPA2, pois este usa o algoritmo AES. É correto apenas o que se afirma em:

| $\bigcirc$ | l e III  |  |  |
|------------|----------|--|--|
| $\bigcirc$ | II e IV  |  |  |
|            | III e IV |  |  |

| I, II e III |        |  |
|-------------|--------|--|
| I, II e IV  |        |  |
|             | SUBMIT |  |
|             |        |  |
|             |        |  |

(ENADE) O IEEE padronizou as redes locais e metropolitanas com o nome IEEE 802. Entre os mais conhecidos padrões de redes locais, citam-se o Ethernet 802.3, que padroniza propriedades físicas para as redes cabeadas, e o padrão 802.11, que define redes sem fio. Considerando-se a diferença entre padrões de rede, assinale a opção correta.

- Redes sem fio oferecem um caminho com menor probabilidade de interferência ou perda de dados quando comparadas às redes cabeadas
- O método de acesso para o padrão 802.3 é o CSMA/CD, ao passo que, para o padrão 802.11, o método de acesso é o CSMA/CA
  - Os padrões 802.11a, 802.11b e 802.11g operam na mesma faixa de frequência e, assim, podem comunicar-

Em redes sem fio, a qualidade de serviço não é comprometida pela associação ou desassociação de estações móveis

Os padrões 802.3 e 802.11 não podem coexistir na mesma rede local

## CONTINUE

# Ligação Inter-Redes

Diversos protocolos são amplamente usados em cada camada de rede. Para viabilizar a interconexão de redes é preciso examinar as questões que surgem quando duas ou mais redes se juntam para formar uma única, e estas questões são completamente dependentes da camada em que os equipamentos de rede utilizados na interconexão operam (KUROSE; ROSS, 2013).

O nome utilizado para identificar o equipamento de rede que interconecta dois segmentos de rede depende da camada em que opera, conforme apresentado na Tabela 1, e é representado graficamente por um símbolo padrão genérico utilizado para referenciar cada um destes tipos de equipamento de rede.

Tabela 1 - Equipamentos de Interconexão de Redes

| Camada    | Equipamento   | Símbolo  |  |
|-----------|---|----------|--|
| Física    | <b>Hub</b> : dispositivo que amplifica<br>e regenera sinais fracos, para<br>recuperar o nível de sinal  |          |  |
| Enlace    | <b>Switch e AP (Access Point)</b> : dispositivos que armazenam e encaminham quadros entre segmentos de LANs   |          |  |
| Rede      | <i>Router</i> : dispositivo que encaminha<br>pacotes entre diferentes redes, as quais<br>podem utilizar protocolos distintos                                    | <b>+</b> |  |
| Aplicação | <b>Gateway e Firewall</b> : dispositivo que<br>conecta duas partes de uma aplicação<br>através da inspeção do conteúdo<br>transportado pela camada de aplicação |          |  |

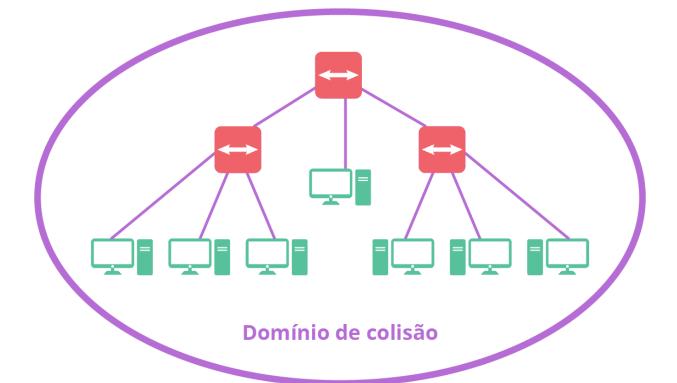
Fonte: Elaboração própria (2022). Arte/Diagramação: DME/FURB (2023).



## Hubs

Os hubs são dispositivos que operam na camada física: tratam essencialmente da amplificação e retransmissão de bits. Um exemplo de sua utilização está apresentado na Figura 8.

Figura 8 - Exemplo de Utilização de *Hubs* 



Fonte: Elaboração própria (2022). Arte/Diagramação: DME/FURB (2023). Quando um bit chega por uma de suas portas, o hub simplesmente o copia em todas as demais portas.

Através da utilização de *hubs* permite-se obter uma LAN hierarquizada, o que leva a um isolamento imediato de defeitos sem afetar os seus demais componentes, facilitando assim a sua manutenção. Por outro lado, é importante observar que a presença de *hubs* não isola a mídia de transmissão, fazendo com que todos os equipamentos estejam disputando a mesma mídia de transmissão como se os *hubs* não existissem, ou seja, todos os equipamentos participam de um mesmo **domínio de colisão**.

Atualmente os *hubs* têm sido utilizados basicamente apenas como repetidores em função do barateamento de outros equipamentos mais elaborados e eficientes, como os *switches*.

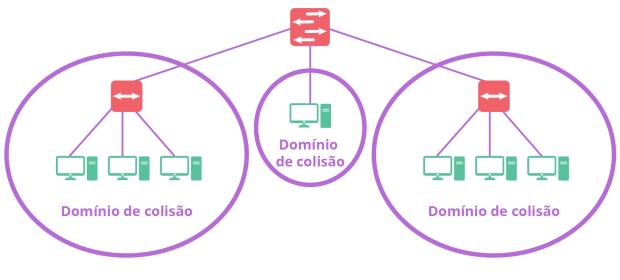
2

## Switches

Os **switches** são dispositivos que operam na camada de enlace: filtram e encaminham os quadros recebidos de acordo com o endereço MAC de seu destino.

Através da utilização de **switches** (Figura 9), que possuem várias portas de conexão, permite-se obter LANs separadas, ou seja, obtém-se um isolamento da mídia de transmissão entre cada uma das LANs interligadas por ela em domínios de colisão isolados.

## Figura 9 - Exemplo de Utilização de Switch



Fonte: Elaboração própria (2022). Arte/Diagramação: DME/FURB (2023).

Para que o processo de encaminhamento seja efetuado, cada *switch* gerencia uma tabela interna de endereços MAC, chamada **tabela de comutação**, identificando em qual das suas portas se encontra o segmento de rede que contém o equipamento a que cada quadro que chega se destina. Esta tabela é atualizada apenas pela observação do endereço de origem dos quadros que passam por suas portas, identificando a que porta os endereços MAC de origem pertencem.

Quando um quadro chega ao *switch* por uma de suas portas, se o endereço MAC de destino não estiver presente em sua tabela de comutação, ele transmite o quadro em todas as demais portas de saída.

Por outro lado, se o endereço MAC de destino estiver presente em sua tabela de comutação e a porta de saída for a mesma em que o quadro chegou, este é descartado e, portanto, o quadro não é repassado para nenhuma porta, pois os equipamentos de origem e de destino encontram-se sob a mesma porta do *switch*. Mas se a porta de saída for diferente da porta em que o quadro chegou, o quadro é transmitido somente na porta de saída especificada na sua tabela de comutação.

Essas regras simples permitem que um *switch* preserve domínios de colisão separados para cada um dos diferentes segmentos de LAN conectados a suas portas. Elas também permitem que dois

conjuntos de nós de diferentes segmentos de LAN se comuniquem simultaneamente sem interferência mútua.

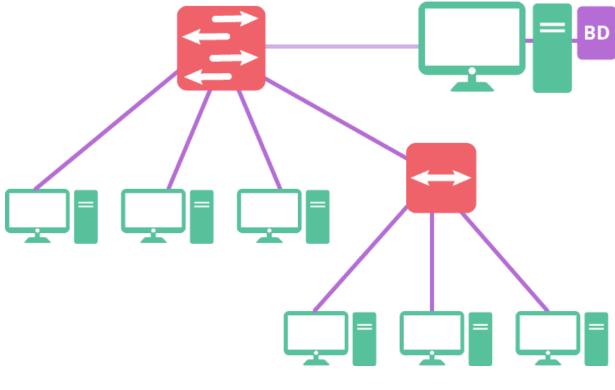


#### (i) Reflita

Você percebe que com esse mecanismo de encaminhamento de quadros um switch preserva a taxa de transmissão de pares de interfaces que estiverem transmitindo paralelamente?

Os switches costumam disponibilizar portas específicas de alto desempenho para a conexão de equipamentos específicos (servidores críticos de banco de dados ou de aplicações, por exemplo) através de acesso dedicado (ligação direta do equipamento com o switch), como está representado na Figura 10, operando num enlace ponto a ponto.

# Figura 10 - Exemplo de Utilização de Switches



Fonte: Elaboração própria (2022). Arte/Diagramação: DME/FURB (2023).

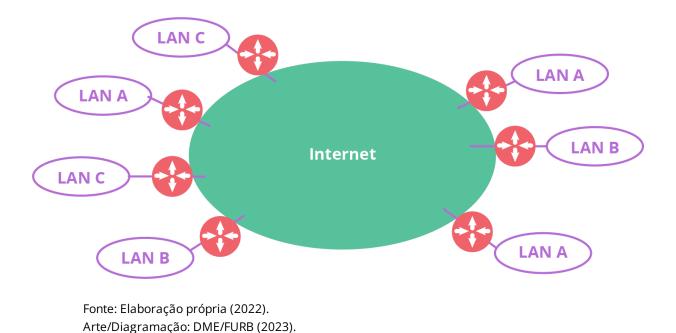
# 3 Redes VPN

Uma rede VPN (Virtual Private Network) é uma rede privada de equipamentos construída com a utilização da infraestrutura de rede pública e acessada somente por usuários ou grupos devidamente registrados na VPN.

O principal motivo para se utilizar uma VPN é o econômico, pois um conjunto de redes virtuais compartilhando uma única infraestrutura física de transmissão de dados é mais barato que implantar uma série de redes físicas de transmissão, cada qual servindo exclusivamente a um único cliente.

A Figura 11 apresenta um exemplo de três LANs, A, B e C, interconectadas através da internet, constituindo três VPNs.

Figura 11 - VPNs para LANs Através da Internet



A segurança é, em geral, a primeira preocupação de uma empresa interessada em utilizar uma VPN baseada na internet. A maior preocupação é que as informações privadas (confidenciais) poderiam ser acessadas (interceptadas) enquanto em trânsito ou diretamente de servidores ou nós da rede (TANENBAUM; WETHERALL, 2011).

Em função do receio de que informações privadas sejam acessadas, inúmeras medidas robustas de segurança estão disponíveis para manter os dados transmitidos estritamente confidenciais e evitar que usuários não autorizados consigam acessar as informações privadas e eventualmente os recursos internos das redes privadas.

# Atividade de Passagem

(ENADE) Ethernet e suas evoluções de 100 Mbps e 1 Gbps são tecnologias padronizadas para comunicações em redes locais com infraestrutura de transmissão compartilhada. Acerca das transmissões que usam essas tecnologias, assinale a opção incorreta.

- Embora diversos segmentos de uma rede possam ser definidos com o uso de *switches*, transmissões de pacotes com endereço de *broadcast* (difusão) atingem todos os computadores na mesma rede
- O mecanismo de controle de acesso ao meio utilizado é distribuído e, nas redes com *hubs*, cada interface de rede deve determinar quando é possível realizar uma transmissão
- Switches realizam o encaminhamento seletivo de quadros com base nos endereços IP de cada estação

A escuta do meio durante as transmissões permite detectar colisões em segmentos compartilhados e a

| necessidade de retransmissões, mas não há envio de quadros de confirmação de recebimento                 |
|--|
| Um mecanismo de controle de consistência é usado para verificar a integridade de cada quadro transmitido |
| SUBMIT   |
|  |

## CONTINUE

# Resumo da Webaula 5

Como você viu nessa aula, as camadas física e de enlace estão implementadas nas placas de rede dos equipamentos de rede. Além da identificação de erros na transmissão de quadros, a camada de enlace é responsável por controlar o acesso ao meio definindo quem será o próximo equipamento que irá transmitir.

Vimos também as duas principais tecnologias de transmissão para as redes locais: o IEEE 802.3 e o IEEE 802.11, conhecido como WiFi. Nessa aula você viu que cada uma dessas tecnologias possui vários padrões que foram evoluindo com o tempo aumentando a sua capacidade de transmissão.

Por fim, você conheceu os equipamentos de interconexão de redes utilizados nas redes locais de computadores, equipamentos esses que são classificados em função da camada de rede em que operam, ou seja, em função de como atuam sobre o fluxo de dados que passa por cada um deles.

#### CONTINUE

## Referências

O estudo das camadas do modelo de referência TCP/IP abordadas nesta parte do livro pode ser encontrado em:

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: Bookman, 2008.

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

MENDES, Douglas R. **Redes de computadores**: teoria e prática. São Paulo: Novatec, 2010.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011.

As normas referenciadas nessa unidade podem ser obtidas diretamente da página da internet dos respectivos organismos de padronização:

- IANA: <u>www.iana.org</u>
- ICANN: www.icann.org
- IEEE: <u>ieeexplore.ieee.org/Xplore/guesthome.jsp</u>

- IETF: <u>www.rfc-editor.org/rfc-index.html</u>
- ISO: <u>www.iso.org/standards-catalogue/browse-by-ics.html</u>
- ITU-T: <u>www.itu.int/pub/T-REC</u>

## CONTINUE

# **Créditos**

Reitora

Prof<sup>a</sup>. Ma. Marcia Cristina Sardá Espindola

**Vice-Reitor** 

Prof. Dr. Marcus Vinicius Marques de Moraes

Pró-Reitor de Ensino de Graduação, Ensino Médio e Profissionalizante

Prof. Dr. Romeu Hausmann

Pró-Reitor de Administração

Prof. Me. Jamis Antônio Piazza

Pró-Reitora de Pesquisa, Pós-Graduação, Extensão e Cultura

Prof<sup>a</sup>. Dr<sup>a</sup>. Michele Debiasi Alberton

Divisão de Modalidades de Ensino Chefia da Divisão

Profa. Dra. Clarissa Josgrilberg Pereira

**Professores Autores** 

Prof. Me. Francisco Adell Péricas

**Design Instrucional** 

Profa. Dra. Clarissa Josgrilberg Pereira

Prof. Dr. Maiko Rafael Spiess

Prof. Me. Francisco Adell Péricas

Marcia Luci da Costa

Me. Wilson Guilherme Lobe Junior

Revisão Textual

Me. Wilson Guilherme Lobe Junior

Laura Cristina Zorzo

Roteirização

Laura Cristina Zorzo

Produção de Mídia

Gerson Luís de Souza

Gustavo Bruch Féo

**Equipe de Design Gráfico** 

Amanda Kannenberg

Camylle Sophia Teske

Laura Cristina Zorzo

Nicolle Sassella

Renan Diogo Depiné Fiamoncini

Diagramado por Amanda Kannenberg em 10 de Fevereiro de 2023

## CONTINUE