

Teste 12/13.

1. O Modelo de referência OSI preconiza uma organização protocolar hierárquica em que as funções protocolares de cada camada são independentes entre si. Isso não impede que uma função genérica, como por exemplo o endereçamento, não exista em diferentes níveis protocolares e, portanto, em diferentes contextos. **Verdadeiro.**
2. Uma topologia de rede em estrela pode usar meios de transmissão com ou sem fios. **Falso. A ideia da rede em estrela é que todos os hosts tenham de passar por um hub/entidade central, e esta é que está encarregue de fazer o forwarding para outros elementos da rede (por isso nenhum dos dois hosts tem acesso direto um ao outro). Porém, por absurdo, se pudesse ser sem fios, qualquer dois hosts podiam ter acesso direto um ao outro. Logo topologia em estrela não funciona.**
3. As fibras óticas mono-nodo permitem cobrir maiores distâncias na transmissão do que as fibras multi-nodo por causarem menor dispersão. **Verdadeiro**

| Fiber Optic Cable Type | | Fiber Cable Distance | | | | | |
|------------------------|-----|-----------------------------|----------------------------|---|-------------------|-----------------|-------------------|
| | | Fast Ethernet 100BASE-FX | 1G Ethernet 1000BASE-SX | 1G Ethernet 1000BASE-LX | 10G Base SE-SR | 40G Base SR4 | 100G Base SR10 |
| Single mode fiber | OS2 | 200m | 5000m | 5000m | 10km | / | / |
| | OM1 | 200m | 275m | | / | / | / |
| Multimode fiber | OM2 | 200m | 550m | 550m (mode conditioning patch cable required) | / | / | / |
| | OM3 | 200m | 550m | | 300m | 100m | 100m |
| | OM4 | 200m | 550m | | 400m | 150m | 150m |
| | OM5 | 200m | 550m | | 300m | 400m | 400m |

4. O protocolo HDLC quando opera em modo estendido usa oito bits para sequenciar as tramas de informação portanto a contagem é modulo-8 e o tamanho máximo permitido de janela é **8.Falso, $8-1 = 7$.**

Nesta numeração existe um limite máximo de mensagens que podem ser enviadas sem aguardar reconhecimento. Este limite é denominada "largura da janela", sendo esta numeração organizada de forma circular. No caso do HDLC, esse valor corresponde ao tamanho do campo número de sequência (N(S)) da mensagem :

- modo normal - 3 bits - de 0 a 7 - máximo de 8 mensagens;
- modo estendido - 7 bits - de 0 a 127 - máximo de 128 mensagens;

Baseado nas características apresentadas, sempre que ocorrer um erro em uma das mensagens, podem ser implementados dois procedimentos:

- o destino solicita a retransmissão apenas da mensagem com erro;
- solicita a retransmissão de todas as mensagens a partir de um determinado número de sequência.

5. O tamanho de janela dum protocolo com controlo de fluxo define o número de pacotes de dados de informação que podem estar simultaneamente em trânsito numa ligação de dados entre o emissor e o recetor. **Verdadeiro**

6. O método de controlo Stop-And-Wait é equivalente ao da janela deslizante $W=1$. **Verdadeiro, Stop and Wait apenas circula uma mensagem de cada vez. W no sliding window para ser 1, n terá que ser 1, pelo que dessa forma apenas circula uma mensagem de cada vez.**

• **W é designado abertura da janela ($W_{\max}=2^n-1$)**

7. Numa rede local Ethernet, uma colisão não ocorre se a infraestrutura de comunicação for implementada por um Switch (Comutador) e cablagem com fios. **Verdadeiro, Função do switch.**
8. Numa rede Wide Area Network (WAN) o tempo de propagação é normalmente superior ao tempo de transmissão dum pacote de dados pelo que o parâmetro a tende a ter um valor inferior a 1. **Falso, superior a 1.**

$$\begin{aligned} a &= t_{\text{prop}} / t_{\text{trama}} \\ a &= (d/v) / (L/r) \\ a &= rd / vL \end{aligned}$$

d - distância (m); v - velocidade de propagação (m/s);

L - comprimento trama (bits); r - ritmo de transmissão (bps)

9. O protocolo RARP permite obter um endereço IP a partir de um endereço MAC correspondente. **Verdadeiro**
10. Um encaminhador IP, na presença de um pacote com Time To Live (TTL) igual a zero, descarta o pacote sem notificar o IP de origem através duma mensagem do Internet Control Message Protocol (ICMP). **Falso, a mensagem ICMP é emitida.**
11. O protocolo ICMP tem como objetivo prestar um serviço ao **nível aplicacional**, destinando-se a enviar, por exemplo, uma mensagem de diagnóstico a um cliente de email quando o servidor não responde. **Falso, o ICMP não opera ao nível aplicacional.**
12. O protocolo IPv6, contrariamente ao IPv4, não prevê fragmentação nativa, obrigando à utilização de um processo de descoberta do Maximum Transmission Unit (MTU) antes do envio do pacote na origem. **Verdadeiro. O IPv6 não prevê fragmentação logo devem ser os hosts que estão a enviar os encargos de fragmentar os pacotes (retirando o peso dos routers) daí que nos hosts que enviam deve haver algum tipo de processo de descoberta do MTU.**

IPv6 routers do not perform IP fragmentation. IPv6 hosts are required to either perform path MTU discovery, perform end-to-end fragmentation, or to send packets no larger than the default Maximum transmission unit (MTU), which is 1280 octets.

13. O endereço IP 139.128.131.255/22 é um endereço de Classe B com subendereçoamento, válido para poder ser atribuído a um interface de um encaminhador. **Falso. O endereço em binário fica: 10001011.10000000.10000011.11111111. 32-22 = 10 Bits, os últimos 10 bits estão a 1, logo é um endereço de broadcast.**
14. Um Switch (Comutador), ao contrário de um Hub, tem a capacidade de filtrar o tráfego por endereço de rede IP destino, direcionando os pacotes IP para a porta respectiva. **Falso, é por Mac Address.**

A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data

15. O cabeçalho normal de um datagrama IPv6 (sem cabeçalhos extra especiais), tem um comprimento fixo por questões de desempenho. **Verdadeiro.**

of size 40 bytes. Fixed length IPv6 header allows the routers to process the IPv6 datagram packets more efficiently. The following figure shows the structure of IPv6 datagram packet.

16. No protocolo IPv4, o processo de fragmentação envolve obrigatoriamente o uso dos campos identification, offset e flags do cabeçalho de um pacote. **Verdadeiro**

Campos manipulados na fragmentação IPv4:

- **identification** - identifica fragmentos pertencentes ao mesmo datagrama original
- **more fragments** - flag que determina se o fragmento é o último
- **may fragment** - identificação da possibilidade ou não do datagrama ser fragmentado pela rede
- **fragment offset** - offset dos dados do fragmento relativamente ao datagrama original

17. Numa comunicação half-duplex a utilização da ligação pode ser maximizada porque ambas as estações podem transmitir, ainda que em alturas diferentes. **Verdadeiro, Assumindo "ligação pode ser maximizada" como cada utilizador tem direito a transmitir a R bps, então half-duplex implica que apenas um pode transmitir no canal de cada vez (ou seja usando o máximo), full duplex ambos podem usar ao mesmo tempo, o que em média vai dar R/2 bps a cada.**
18. Não é útil efetuar super-endereçoamento/supernetting numa rede IP baseada em endereços privados. **Falso, subnetting/supernetting tem sempre o benefício de diminuir o tamanho das tabelas de encaminhamento.**

19. Uma rota explícita para uma rede IP tem maior prioridade do que qualquer rota por defeito existente na tabela de encaminhamento para garantir que se consegue encaminhar tráfego diretamente para essas redes. **Verdadeiro.**

Uma **rota padrão** (Default Route), também conhecida como "gateway de último recurso", é a rota de rede utilizada por um roteador quando não há nenhuma outra rota conhecida existente para o endereço de destino de um pacote IP.

20. Numa rede local sem fios, a designação de nó escondido/hidden node é utilizada quando um ponto de acesso à rede (Access Point) é inatingível por um número relevante de terminais de utilizadores. **Verdadeiro.**

In wireless networking, the **hidden node problem** or **hidden terminal problem** occurs when a node can communicate with a wireless access point (AP), but cannot directly communicate with other nodes that are communicating with that AP.^[1] This leads to difficulties in medium access

21. Numa rede local 100Base-FX(1000Base-Fx não "existe"), o débito e o alcance permitido são ambos superiores às redes 100Base-TX. **Falso, são iguais a nível de débito e diferentes em termos de distância máxima de transmissão.**

| Ethernet Type [↕] | Rate [↕] | Transmission Medium [↕] | Medium Type [↕] | Transmission Distance [↕] |
|--|--------------------|--------------------------------------|-------------------------------------|---|
| 10Base-T [↕] | 10M [↕] | UTP (two pairs) [↕] | Categories 3, 4, and 5 [↕] | 100 m [↕] |
| 100Base-TX [↕] | 100M [↕] | UTP/STP (two pairs) [↕] | Category 5 [↕] | 100 m [↕] |
| 100Base-FX [↕] | 100M [↕] | Multi-Mode Fiber (MMF) [↕] | 62.5 μm [↕] | 400 m (half duplex) [↕] 2 km (full duplex) [↕] |
| | | Single-Mode Fiber (SMF) [↕] | 9 μm [↕] | 10 km [↕] |
| 1000BASE-SX [↕] (850 nm laser) [↕] | 1000M [↕] | MMF [↕] | 62.5 μm [↕] | 275 m [↕] |
| | | [↕] | 50 μm [↕] | 550 m [↕] |
| 1000BASE-LX [↕] (1310 nm laser) [↕] | 1000M [↕] | MMF [↕] | 62.5/50 μm [↕] | 550 m [↕] |
| | | SMF [↕] | 9 μm [↕] | 10 km (5 km for the standard distance) [↕] |
| 1000BASE-ZX [↕] (1550 nm laser) [↕] | 1000M [↕] | SMF [↕] | 9 μm [↕] | 70 km [↕] |
| 1000BASE-T [↕] | 1000M [↕] | UTP (four pairs) [↕] | Category 5E [↕] | 100 m [↕] |

22. Uma bridge tem a capacidade de aprender qual as portas a que estão associadas as estações a ela interligadas através da análise dos endereços MAC de origem das tramas/frames em trânsito. **Verdadeiro.**

Redes Locais de Computadores

Equipamentos de Interligação: Bridge



Most wireless LAN networks use the carrier-sense multiple access with collision avoidance (CSMA/CA) method. In addition to the requirements of shared wire medium, wireless networks add the hidden node problem where two senders can't hear each other's transmissions, but they cause a collision at the receiver between them. Multiple Access with Collision Avoidance for Wireless is one such approach used and specifically in 802.11 RTS/CTS. Central coordination is another means of solving this problem for a collision domain. This technique is employed by Wireless Multimedia Extensions. For coordination function and distributed coordination function are specific implementations.

23. Quando várias estações estão ligadas numa rede Wi-Fi, no mínimo existe um domínio de colisão. **Verdadeiro.**
24. Tanto o controlo de acesso por Carrier Sense Multiple Access (CSMA) como o Time Division Multiple Access (TDMA) conduzem a processos de contenção no acesso ao meio. **Verdadeiro.**

Time-division multiple access (TDMA) is a channel access method for shared-medium networks. It allows several users to share the same frequency channel by dividing the signal into different time slots.^[1] The users transmit in rapid

Carrier-sense multiple access (CSMA) is a media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus or a band of the electromagnetic spectrum.

Ambos controlam o acesso aos respetivos meios.

25. A comunicação interativa entre duas interfaces IP implica a existência de rotas em ambos os sentidos da comunicação, mas que não necessitam de ser simétricas. **Verdadeiro.**

Path selection involves applying a routing metric to multiple routes to select (or predict) the best route. Most routing algorithms use only one network path at a time. Multipath routing techniques enable the use of multiple alternative paths.

Teste 11-12

1. Numa Ligação via satélite, a operação do protocolo HDLC em modo estendido é justificada pelo facto do tamanho de janela necessitar de ser elevado para melhorar a utilização da ligação. **Verdadeiro.**

Numa ligação por satélite, como a distancia entre os agentes da rede é alta, e como o protocolo HDLC usa um sliding window que, o numero de sequencia aumenta consoante o tamanho da sliding window.

2. A norma Ethernet pode operar a débitos diferentes consoante o tipo de meio físico utilizado, contudo, o débito máximo em par trançado é 100Mbps. **Falso**

| UTP Categories - Copper Cable | | | | |
|-------------------------------|---------------|-------------|--------------|--|
| UTP Category | Data Rate | Max. Length | Cable Type | Application |
| CAT1 | Up to 1Mbps | - | Twisted Pair | Old Telephone Cable |
| CAT2 | Up to 4Mbps | - | Twisted Pair | Token Ring Networks |
| CAT3 | Up to 10Mbps | 100m | Twisted Pair | Token Ring & 10BASE-T Ethernet |
| CAT4 | Up to 16Mbps | 100m | Twisted Pair | Token Ring Networks |
| CAT5 | Up to 100Mbps | 100m | Twisted Pair | Ethernet, FastEthernet, Token Ring |
| CAT5e | Up to 1 Gbps | 100m | Twisted Pair | Ethernet, FastEthernet, Gigabit Ethernet |
| CAT6 | Up to 10Gbps | 100m | Twisted Pair | GigabitEthernet, 10G Ethernet (55 meters) |
| CAT6a | Up to 10Gbps | 100m | Twisted Pair | GigabitEthernet, 10G Ethernet (55 meters) |
| CAT7 | Up to 10Gbps | 100m | Twisted Pair | GigabitEthernet, 10G Ethernet (100 meters) |



3. O protocolo ARP permite a partir de um endereço IP obter o endereço Ethernet correspondente independentemente do sistema destino estar ou não na mesma rede local. **Falso, endereço MAC.**

The **Address Resolution Protocol (ARP)** is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.

4. Se um router detecta um erro de header checksum num datagrama, solitica a sua retransmissão. **Verdadeiro. Um erro checksum indica corrupção nos pacotes IPv4, como o recetor não efetua correção de erros, tem que aguardar a retransmissão.**

5. Numa rede Ethernet, as estações envolvidas numa colisão têm maior probabilidade de transmitir que as que se encontram à espera do meio livre. **Verdadeiro**

In a half duplex [Ethernet](#) network, a collision is the result of two devices on the same Ethernet network attempt to transmit data at exactly the same time. The network detects the "collision" of the two transmitted packets and discards them both. Collisions are a natural occurrence on Ethernet. Ethernet uses Carrier Sense Multiple Access Collision Detect (CSMA/CD) as its method of allowing devices to "take turns" using the signal carrier line. When a device wants to transmit, it checks the signal level of the line to determine whether someone else is already using it. If it is already in use, the device waits and retries, perhaps in a few seconds. If it isn't in use, the device transmits. However, two devices can transmit at the same time in which case a collision occurs and both devices detect it. Each device then waits a random amount of time and retries until successful in getting the transmission sent.

6. O protocolo IPv6, ao contrário do IPv4, é orientado à conexão, garantindo assim comunicações mais fiáveis. **Verdadeiro**

IPv4 and IPv6 are internet protocol version 4 and internet protocol version 6, IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency.

7. O endereço IP 192.192.192.191/26 não é válido para identificar a interface de um host IP. **Verdadeiro.**
O endereço em binário é 1100 0000.11000000.11000000.10111111. 32-6 = 6. Como os últimos 6 bits estão todos a 1 esse endereço refere-se a um endereço de broadcast.

8. Um switch opera ao nível da ligação de dados, comutando o tráfego entre as suas portas com base em associações do tipo endereço MAC – Endereço IP. **Falso. Os switches encaminham os pacotes de acordo com o endereço mac de destino.**

9. O tamanho de janela do protocolo HDLC define o número de tramas de informação que podem ser cumulativamente confirmadas. **Verdadeiro.**

Esta técnica viabiliza o envio de diversas mensagens, por parte do transmissor, antes que este receba a confirmação se as mensagens enviadas foram recebidas satisfatoriamente. Neste método é necessário numerar as mensagens de forma a identificá-las quando for recebido o seu reconhecimento.

Nesta numeração existe um limite máximo de mensagens que podem ser enviadas sem aguardar reconhecimento. Este limite é denominado "largura da janela", sendo esta numeração organizada de forma circular. No caso do HDLC, esse valor corresponde ao tamanho do campo de número de sequência (N(S)) da mensagem :

10. Numa rede local o tempo de propagação é bastante inferior ao tempo de transmissão de uma trama (de tamanho comum) pelo que o parâmetro a tem um valor elevado ($a \gg 1$). **Falso, inferior a 1.**

11. O problema de esgotamento dos endereços IPv4 ficou resolvido com a criação de IPv4 privados. **Falso, a solução seria ipv6.**

12. Numa rede TCP/IP, o envio das primitivas ARP request ou ARP reply usa encapsulamento IP. **Verdadeiro.**

- Assim como o IP, o pacote ARP é encapsulado no campo de dados do *frame* Ethernet, logo após o cabeçalho.

13. Numa rede IP, a definição de rotas dinâmicas para encaminhamento envolve a utilização de protocolos de routing específicos(ex: RIP,OSPF). **Verdadeiro.**

There are several protocols that can be used for dynamic routing. Routing Information Protocol (RIP) is a distance-vector routing protocols that prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.^[6] Open Shortest Path First (OSPF) uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs).^[7] Intermediate System to Intermediate System (IS-IS) determines the best route for data through a packet-switched network.^[7] Interior Gateway Routing Protocol (IGRP) and its advanced form Enhanced Interior Gateway Routing Protocol (EIGRP) are used by routers to exchange routing data within an autonomous system.^[7]

14. O modo de operação NRM (Normal Response Mode) do protocolo HDLC adequa-se quando se pretende que as estações secundárias tomem a iniciativa na transmissão de dados, no estabelecimento e no termino da ligação. **Falso.**

- Normal Response Mode (NRM) is an unbalanced configuration in which only the primary terminal may initiate data transfer. The secondary terminals transmit data only in response to commands from the primary terminal. The primary terminal polls each secondary terminal to give it an opportunity to transmit any data it has.

15. No cabeçalho IPv6, o campo Hop Limit, equivalente ao TTL em IPv4, evita que um datagram circule indefinidamente na Rede. **Verdadeiro.**

16. Numa transmissão de dados em série assíncrona, o intervalo de tempo entre caracteres não é fixo, contudo o sincronismo na leitura dos bits de cada caractere tem de ser assegurado para que a recepção do mesmo se processe corretamente. **Verdadeiro, é uso o bit parity para tal.**

17. O método de controlo de fluxo stop-and-wait conduz sempre a uma boa utilização da ligação porque é bastante mais simples de implementar do que o mecanismo de janela deslizante. **Falso, o stop and wait é muito pouco eficiente quando comparado com sliding window.**

18. O protocolo ICMP (Internet Control Messsage Protocol) destina-se a reportar mensagens de diagnóstico da operação da rede IP (nível 3). **Verdadeiro.**

19. Numa rede Ethernet partilhada, o processo de deteção de colisões obriga a que as tramas Ethernet tenham um comprimento mínimo. **Verdadeiro.**

Frames must be at least 64 bytes long, not including the preamble, so, if the data field is shorter than 46 bytes, it must be compensated by the *Pad* field. The reason for specifying a minimum length lies with the collision-detect mechanism. In CSMA/CD a station must never be allowed to believe it has transmitted a frame successfully if that frame has, in fact, experienced a collision.

In the worst case it takes twice the maximum propagation delay across the network before a station can be sure that a transmission has been successful. If a station sends a really short frame, it may actually finish sending and release the Ether without realising that a collision has occurred.

Thats why it is/has a minimum of 64 Bytes.

20. Uma transmissão série assíncrona com 8 bits (ex interface RS-323c) para dados, no melhor dos casos tem uma eficiência na transmissão de 80%. ?

21. O conceito de internetworking tem como objetivo proporcionar um serviço de rede global sobre redes de comunicação baseadas em tecnologias de nível de ligação **heterogéneas. Falso**

Interligação de redes (internetworking) é uma referência aos princípios arquiteturais, **protocolos** e serviços de uma **internet** que tem como objectivo interligar múltiplas **redes físicas** de modo a formar um sistema coordenado e homogéneo. Define também a forma como os protocolos Internet (*protocol suite TCP/IP*) operam no sistema global e como as aplicações utilizam o sistema resultante.

22. A gama de endereços IP 192.168.1.0/24 pode ter conectividade IP global desde que os endereços atribuídos às estações seja únicos. **Falso, 192.168.1.0 é um endereço reservado.**

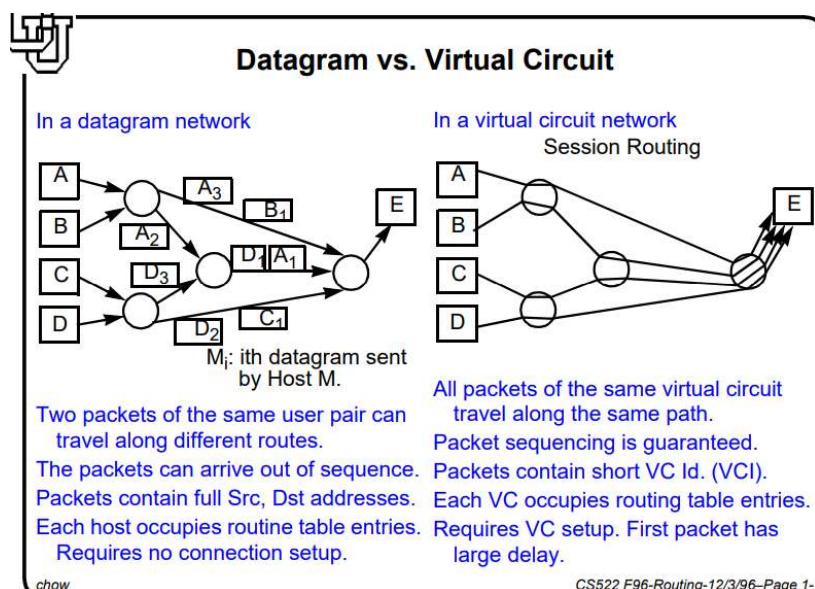
23. Numa rede IP, como as decisões de encaminhamento (unicast) são tomadas com base no endereço destino, o endereço IP de origem é redundante e desnecessário para a comunicação. **Falso.**

In **computer networking**, **unicast** refers to a one-to-one transmission from one point in the network to another point; that is, one sender and one receiver, each identified by a **network address**.^[1]

24. Os mecanismos volta-atrás-N e retransmissão seletiva permitem controlar o fluxo de uma ligação de dados.

Go-Back-N ARQ is a specific instance of the **automatic repeat request** (ARQ) protocol, in which the sending process continues to send a number of frames specified by a **window size** even without receiving an **acknowledgement** (ACK) packet from the receiver. It is a special case of the general sliding window protocol with the transmit window size of N and receive window size of 1. It can transmit N frames to the peer before requiring an ACK.

25. Numa rede IPv6, os dados são transportados em datagramas de tamanho fixo para que não haja fragmentação. **Falso, para que não haja colisões de endereços privados.**
26. Não é possível o uso de supernetting numa rede IP baseada em endereços privados. **Verdadeiro, pois não é possível fazer supernetting em endereços de**
27. O uso de uma rota por defeito tem menor prioridade do qualquer outra rota, estática ou dinâmica, existente na tabela de encaminhamento. **Verdadeiro, a rota por defeito é a última rota em termos de prioridade quando existem rotas especificadas.**
28. Se uma rede opera baseada em circuitos virtuais (orientada à conexão) apresenta uma latência inicial da comunicação superior a uma rede que opera baseada em datagramas (não orientada à conexão). **Verdadeiro.**



29. Um datagrama IPv4, após um processo de fragmentação, não pode ser novamente fragmentado pois isso impossibilitaria a reconstrução do datagrama original. **Falso.**

30. Um host IP conectado na rede eduroam fragmenta mais os pacotes do que quando conectado na rede com fios por forma a diminuir o risco de colisões. **Verdadeiro, como eduroam é uma rede Wi-Fi, irão haver mais colisões, logo mais fragmentação para prevenir.**

31. O esquema sem permite de causa uma largura de de rotas.

To fragment/segment a long internet packet, a router (R1 in the figure below) creates a new IP packet and copies the contents of the IP header fields from the long packet into the new IP header. The data of the long packet is then divided into two portions on a 8 byte (64 bit) boundary, so that the first packet is less than the MTU of the out-going interface. The more-fragments flag (MF) in the first packet is set to one (to indicate that more fragments of this packet follow). The More Flag may already be set in this packet if it has already been fragmented by another system. This packet is forwarded.

The second created new packet is then processed. The packet header field is identical to that of the original packet (including the same value of the packet ID, the total length field, the more-fragments flag (MF) and the fragment offset field in the original packet). The packet header field is updated with a new offset field, by adding the number of payload bytes sent in the first fragment. If this new packet is larger than the allowed link MTU, the packet is again fragmented.

de endereçamento classes (CIDR) uma melhor gestão endereços mas maior gasto de banda no anúncio **Verdadeiro, com**

CIDR, mais informação é transmitida(informação da sub-net mask), logo maior largura de banda.

32. Numa rede local sem fios, o problema do “nó exposto” (exposed node) traduz-se numa maior vulnerabilidade e ataques quando comparado com um “nó-escondido” (hidden-node). **Falso.**

In wireless networks, the **exposed node problem** occurs when a node is prevented from sending packets to other nodes because of **co-channel interference** with a neighboring transmitter.

In wireless networking, the **hidden node problem** or **hidden terminal problem** occurs when a node can communicate with a wireless access point (AP), but cannot directly communicate with other nodes that are communicating with that AP.^[1] This leads to difficulties in medium access control sublayer since multiple nodes can send data packets to the AP simultaneously, which creates interference at the AP resulting in neither packet getting through.

33. O uso da opção RTS/CTS (Request to Send/Clear To Send) numa rede local sem fios reduz a existência de colisões nos nós receptores causadas, por exemplo, por nós escondidos (hidden nodes). **Verdadeiro.**

RTS/CTS (Request to Send / Clear to Send) is the optional mechanism used by the **802.11** wireless networking protocol to reduce frame collisions introduced by the **hidden node problem**. Originally the protocol fixed the **exposed node problem** as well, but modern RTS/CTS includes ACKs and does not solve the exposed node problem.

34. O Internet Control Message Protocol (ICMP) permite tornar o protocolo IP fiável. **Verdadeiro, pois é essencial a deteção e gestão de erros.**

The **Internet Control Message Protocol (ICMP)** is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address, for example, an error is indicated when a requested service is not available or that a host or router could not be reached.^[1] ICMP differs from transport protocols such as TCP and UDP that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).

35. Numa rede local 1000baseT, o equipamento de interligação pode ser um hub comutado a 1Gbps. **Verdadeiro**

36. Uma bridge tem capacidade de aprender qual a localização das estações e ela interligadas através de análise dos endereços MAC de origem das tramas em trânsito. **Verdadeiro**

The forwarding information base stored in content-addressable memory (CAM) is initially empty. For each received ethernet frame the switch learns from the frame's source MAC address and adds this together with an ingress interface identifier to the forwarding information base. The switch then forwards the frame to the interface found in the CAM based on the frame's destination MAC address. If the destination address is unknown the switch sends the frame out on all interfaces (except the ingress interface). This behaviour is called unicast flooding.

37. Num endereço de rede IP, fazer supernetting de n para m bits ($n > m$), corresponde a agrupar $2^{(n-m)}$ prefixos de rede n distintos. **Verdadeiro**

38. Os repetidores são equipamentos transparentes ao nível de rede IP, contudo podem descartar pacotes IP se ocorrer erro no cabeçalho dos mesmos. **Falso, um repetidor não interpreta tramas.**

39. A tabela de encaminhamento de um router não pode ter mais de um caminho disponível para o mesmo destino (host ou rede) pois causa uma situação ambígua que o mesmo não consegue resolver. **Verdadeiro**

40. Se efetuar o download a imagem cisco-config-23011.img para um router através da porta série assíncrona RS-323c a 112kpbs, a transferência completa terá sempre uma duração superior a 9 segundos. ?