A	A comutação de pacotes sem circuitos virtuais não garante que os pacotes sejam recebidos na mesma ordem em que são emitidos.	V
	A técnica ADSL (Asymmetric Digital Subscriber Line) utiliza sinais digitais sobre linhas telefónicas tradicionais.	F
	A linha de cabeçalho “Connection: close" pode ser usada tanto em pedidos como em respostas HTTP.	V
	A linha de cabeçalho Content-Type do HTTP nunca é usada nas mensagens de pedido, apenas nas respostas	F
	A deteção de erros de transmissão obriga à colocação de informação de controlo adicional no pacote.	V
	A maior vantagem de utilizar encaminhamento dinâmico e poupar o trabalho de definir tabelas estáticas.	F
	A técnica PSK (“Phase Shift Keying”) produz um sinal analógico em que a amplitude representa os dados a transmitir.	F
	A arquitetura TCP/IP implementa todas as camadas prevista no modelo OSI.	F
	A deteção de erros de transmissão garante que todos os erros ocorridos são detetados, mas podem existir falsas deteções	F
	A técnica ASK (Amplitude Shift Keying) gera sinais analógicos, a técnica PSK (Phase Shift Keying) produz sinais digitais.	F
	A utilização de etiquetas IEEE 802.1q reduz para metade o MTU (“Maximum Transmission Unit") das redes “ethernet".	F
	A comutação de pacotes com circuitos virtuais garante que os pacotes chegam ao destino na ordem em que foram emitidos.	V
	A tecnologia WLL (“Wireless Local Loop") utiliza a norma 802.11 para proporcionar uma ligação dos subscritores ao operador.	F
	A escolha entre a utilização de sinais analógicos ou sinais digitais depende do meio de transmissão que vai ser usado.	V
	A resolução de nomes NetBIOS não exige nenhum tipo de servidor, pode ser implementada apenas pelos postos de trabalho.	V
	A mensagem TRAP do SNMP (“Simple Network Management Protocol") é emitida pelo agente.	V
	A linha de cabeçalho “Content—Type” do HTTP pode ser usada nas mensagens de resposta, mas nunca nas mensagens de pedido.	F
	A missão de um encaminhador IPv4 é analisar o endereço de destino do pacote e determinar o “next-hop" mais apropriado.	V
	A meio de um cabeçalho HTTP nunca pode surgir uma dupla sequência CR/ LF.	V
	A arquitetura IEEE 802 (ISO 8802) define várias camadas que correspondem aos níveis 3 e 4 do modelo OSI.	F
	A resolução de noma via WINS (“Windows Internet Name Service") exige que os postos de trabalho estejam todos na mesma rede.	F
	A “system—call" “select" (linguagem C) nunca pode devolver o valor zero.	F
	A única vantagem do encaminhamento dinâmico é evitar a construção manual das tabelas de encaminhamento.	F
	A maioria dos protocolos de encaminhamento recorre a diferenta endereços “multicast" IPv4 para transmissão da informação.	V
	A mesma versão do protocolo ICMP é usada com IPv4 e IPv6.	F
	A comutação de células das redes ATM (“Asynchronous Transfer Mode") garante que a ordem de receção é a mesma da emissão.	V
	A mensagem TRAP do SNMP é enviada pelo agente ao sistema gestor em raposta a um pedido Getbulk Request.	F
	A mensagem de erro ICMP do tipo “Redirect” é produzida pelos “routers" quando não está a ser utilizado o caminho correto.	V
	A utilização de uma chave pública para cifar a informação não dá qualquer garantia de autenticidade.	V
	A camada de rede é a primeira camada do modelo de referência OSI (MR-OSI), todas as restantes utilizam a camada de rede.	F
	A linha de cabeçalho “Content-Transfer-Encoding: binary" não é suportada pelo SMTP “normal".	V
	A técnica RTS/ CTS apenas é usada para emitir pacots com dimensão superior a um valor predeterminado.	V
	A arquitetura TCP/IP não define nenhuma implementação concreta que corresponda aos níveis 1 e 2 do MR—OSI.	V
	A utilização de VLAN (Virtual Local Area Network) implica sempre a colocação de etiquetas nas tramas (IEEE802.1Q).	F
	A utilização de uma chave secreta pré partilhada (PSK) permite garantir a confidencialidade, mas não a autenticidade.	F
	A maioria dos vários tipos de tecnologias “Ethernet” mantém em comum o formato de pacote e o formato dos endereços de nó.	V
	A modulação FSK (“Frequency Shift Keying") produz um sinal analógico em que a respetiva frequência varia.	V
	A tecnologia ATM (“Asynchronous Transfer Mode")tem como principal objetivo garantir que não ocorrem erros na transmissão.	F
	A mensagem de resposta a um pedido do método HEAD é uma mensagem que está totalmente em formato de texto.	V
	A RSTP (“Rapid Spanning Tree Protocol") converge mais rapidamente do que o STP, mas define mais estados para as portas.	F
	A camada AAL 5 (“ATM Adaptation Layer 5") permite às redes ATM o transportar pacotes de dados do protocolo IP.	V
	A mensagem TRAP do SNMP é enviada pelo agente ao sistema gestor em resposta a um pedido “Getbulk Request".	F
	A utilização de etiquetas IEEE 802.1q é obrigatória quando várias VLAN passam através de uma mesma ligação física.	V
	A mensagem de resposta a um pedido do método HEAD é uma mensagem que nunca contém corpo (“content").	V
	A fragmentação de “datagramas” IPv4 é uma funcionalidade imprescindível que nunca pode ser evitada.	F
	A mensagem ICMP do tipo “Destination Unreachable" significa necasariamente que os dados não chegaram ao nó de destino.	F
	A linha de cabeçalho “Content-Length" é usada em muitas repostas, mas nunca pode existir num pedido.	F
	A técnica FSK (“Frequency Shift Keying") produz um sinal analógico cuja frequência se altera de acordo com os dados a transmitir.	V
	A principal característica das redes ATM é que qualquer erro de transmissão nos dados é automaticamente detetado e corrigido.	F
	A tecnologia ADSL (Asymmetric Digital Subscriber Line) produz sinais digitais.	V
	A fibra ótica é um meio de transmissão adequado para sinais elétricos.	F
	A gestão de grupos de multicast no IPv6 (“Internet Protocol" versão 6) é assegurada pelo protocoloICMPv6.	V
	A sessão SMTP (“Simple Mail Transfer Protocol")é iniciada pela aplicação que pretende enviar a mensagem de correio.	V
	A tecnologia DSL (“Digital Subscriber Line") baseia—se no aproveitamento de cabos telefónicos das redes telefónicas tradicionais.	V
	As redes “Ethernet" exigem um tamanho mínimo para os pacotes, ata restrição deriva da utilização da técnica CSMA/ CD	V
	As redes sem fios locais são um exemplo de rede de meio de transmissão partilhado(broadcast).	V
	As técnicas ASK, FSK e PSK produzem sinais digitais em que o nível de sinal é uma representação direta dos dados a transmitir.	F
	As camadas MAC (“Medium Access Control") da arquitetura IEEE 802 (ISO 8802) implementam mecanismos de deteção de erros.	V
	As redes Ethernet a 10 Mbps utilizam endereços de 48 bits, as redes Ethernet a 1 Gbps utilizam endereços de 128 bits.	F

	As vantagens do controlo de fluxo com janela deslizante são mais evidentes quando os atrasos de propagação são elevados.	V
	As ligações ADSL (“Asymmetric Digital Subscriber Line") utilizam como meio de transmissão um par de condutores de cobre.	V
	As células ATM (Asynchronous Transfer Mode) possuem um mecanismo de deteção de erros nos dados transportados.	F
	As mensagens de resposta HTTP a pedidos com o método GEI' terminam sempre com uma linha vazia.	F
	As mensagens SMTP são constituídas por um cabeçalho de texto terminado por uma linha vazia seguida do conteúdo.	V
	As redes locais sem fios 802.11 utilizam sinais analógicos.	v
	As mensagens SNMP “GetRequest” e “SetRequest” são emitidas pelo agente após solicitação do sistema gestor.	F
	As técnicas ASK, FSK e PSK produzem sinais digitais em que o nível de sinal é uma representação direta dos dados a transmitir.	F
	As mensagens ICMP dos tipos “echo request" e “echo reply" são usadas na implementação do comando “traceroute”.	F
	As mensagens de correio enviadas através do SMTP utilizam um formato semelhante ao das mensagens HTTP.	V
	As redes ATM (“Asynchronous Transfer Mode") utilizam a técnica comutação de pacotes (células) com circuitos virtuais.	V
	As redes ATM (“Asynchronous Transfer Mode") sãocapazes de suportar de forma eficiente transmissões em tempo real.	V
	Atualmente, na maioria das redes locais “Ethernet” (802.3) não ocorrem colisões porque são usados comutadores (“switches").	V
	Atualmente os endereços de correio eletrônico identificam registos DNS do tipo MX e não A ou AAAA.	V
	Atualmente a implementação de SPF (Sender Policy Framework) utiliza apenas registos do tipo DCI”.	V
	Ao contrário do IPv4, o protocolo UDP (User Datagram Protocol) permite identificar aplicações e não apenas nós.	V
	Ao contrário do IPv4, no IPv6 os cabeçalhos dos datagramas têm tamanho fixo.	V
	Ao contrário do IPv4, o protocolo UDP (User Datagram Protocol) permite detetar erros nos dados transportados.	V
	Ao contrário do que acontece em UDP, em TCP não é possível usar endereços de broadcast.	V
	Antes de receber o pedido, o servidor tem de conhecer o endereço do cliente para lhe poder responder.	F
	Ambos os protocolos ICMPvG e ICMPv4 implementam as mensagens de pedido de “echo" e resposta de “echo".	V
	Através de uma ligação TCP as operações de leitura e escrita são realizadas byte a byte, o número de bytes lido numa extremidade tem de corresponder sempre ao número de bytes escrito na outra.	V
	Após o estabelecimento da ligação com o servidor SMTP o cliente pode responder à mensagem inicial com “HELO” ou “EHLO”.	V
	Associado a um mesmo nome de domínio DNS podem ser definidos vários registos do tipo MX.	V
C	Cada domínio DNS tem de conhecer os registos NS(“Name Server") dos domínios imediatamente acima e imediatamente abaixo.	F
	Cada domínio DNS tem obrigatoriamente um registo NS (“Name Server") e não pode ter mais do que um registo NS.	F
	Com a técnica CSMA/ CD (Ethernet) o comprimento máximo da rede diminui quando se aumenta a taxa de transmissão.	V
	Com “Content—Transfer—Encoding: base64" cada conjunto de 3 bytes é representado por um conjunto de 4 símbolos.	V
D	De um PDU (”Protocol Data Unit") criado na camada de sessão vai resultar num PDU de maior dimensão na camada de rede.	V
	Duplicar a taxa de transmissão numa rede não garante que as transferências de dados passem a demorar metade do tempo.	V
	Designam-se “Backward Error Correction” (BEC) as técnicas de controlo de erros em que se procede à retransmissão.	V
	Duplicando a taxa de transmissão, 0 tempo que demora a transferir um pacotes entre dois nós passa sempre para metade.	F
E	Entre outros dados, o registo SOA ("Start Of Authority") contém informação que permite a sincronização dos servidores.	V
	Entre outras funcionalidades, o ICMPv6 assegura a gestão de grupos multicast.	V
	Em IPv6 os endereços UNICAST link-local são obtidos recorrendo a um servidor DHCPv6.	F
	Em qualquer codificação bifásica existe sempre uma transição de nível a meio de cada bit, independentemente do valor do bit.	F
	Em caso de sucesso, a system-call recvfrom devolve o número de bytes recebidos.	V
	Em IPv6, o endereço de nó “2:10C5:1B::7A” pertence à rede “2:10C5:1B::/48".	V
	Em JAVA, para implementar um servidor UDP deve ser usado um objeto da classe “ServerSocket”.	F
	Em TCP, quando o valor do RTT (Round Trip Time) aumenta, o RTO (Retransmission TimeOut) também vai aumentar.	V
	Em PSK (“Phase Shift Keying") a fase do sinal é sempre alterada, seja qual for o símbolo a transmitir.	V
	Embora de formas diferentes, ambos os métodos GET e POST podem ser usados para submeter formulários.	V
	E necessário utilizar sinais analógicos quando o meio de transmissão não suporta a frequência zero.	V
	E possível usar o protocolo UDP para enviar um conjunto de 1024 bytes de dados entre duas aplicações.	V
	Existirem duas respostas diferentes a um pedido ARP indica que se encontram na rede dois nós a utilizar o mesmo endereço IPv4.	V
F	FSK (Frequency Shift Keying), ASK e PSK podem ser combinadas para definir mais valores possíveis para o sinal.	V
N	Numa rede de meio partilhado (rede de broadcast) dois nós podem ter o mesmo endereço.	F
	Numa tabela de encaminhamento, se existem dois caminhos diferentes para o mesmo destino será usado o de menor métrica.	V
	Numa ligação ADSL o número de canais disponíveis tende a diminuir com a aumento da distância da ligação.	V
	Numa rede 802.11, 0 “roaming” apenas é possívelentre células que pertençam ao msmo ESS (“Extended Service Set").	V
	Numa ligação DSL (“Digital Subscriber Line") é utilizado um par de fibras óticas para transmitir sinais digitais em “full-duplex"	F
	Numa rede de “broadcast” (meio partilhado), a rede ignora os endereços de destino e entrega os pacotes em todos os nós.	V
	Numa rede IPv6 com o endereço “22:AA10:1::/16", o endereço “22:AA10:1::FFFF” corresponde a um nó válido dessa rede.	V
	Numa base de dados DNS nunca pode existir mais do que um registo Mx para o mesmo nome de domínio.	F
	Numa rede “Ethernet” constituída por 2 HUBs repetidores interligados por uma ponte (“bridge") existem 2 domínios de colisão	V
	Numa rede para enviar 1000 bytes de dados são suficientes dois pacotes com comprimento total de 500 bytes cada.	F
	Numa mensagem SMTP nunca pode existir nenhuma linha vazia.	F
	Nunca é possível aplicar simultaneamente ASK (“Amplitude Shift Keying") e PSK porque o sinal seria ilegível.	F
	Numa rede de comutação quando um pacote é emitido propaga—se sempre a todos os nós da rede.	F
	Numa rede “ethernet", o facto de se usar uma topologia em atrela (Ex.: 10baseT) garante desde logo a ausência de colisões.	F

	Numa ligação TCP nunca se pode enviar mais do que 512 bytes, após o envio de 512 bytes tem de ser criada nova ligação.	F
	Numa rede 802.11, para enviar um pacote de dados usando a técnica RTS] CTS são transferidas pela rede 4 tramas no total.	V
	Numa ligação DSL (Digital Subscriber Line) é utilizado um par de fibras óticas para transmitir sinais digitais em full—duplex.	F
	Numa codificação do tipo NRZ, seja qual for a sequência de símbolos transmitida, existem sempre mudanças de nível no sinal.	F
	Numa tabela de encaminhamento (“routing table")o “next-hop" pode ser um endereço pertencente a uma rede remota.	F
	Numa tabela de encaminhamento nunca podem existir duas regras que especifiquem uma mama rede de destino.	F
	Numa rede 802.11, a utilização da técnica RTS/ CTS é mais vantajosa para pacata de grande dimensão.	V
	Numa ligação TCP o número de bytes lido num lado deve ser sempre inferior ao número de bytes escrito no outro lado.	F
	Numa VPN de utilizador com o protocolo CHAP (“Challenge-Handshake Authentication Protocol”) o servidor não é autenticado.	F
	Numa rede de comutação de pacotes, não é possível emitir um pacote de tal forma que seja recebido em todos os nós da rede.	F
	Numa rede “ethernet", o protocolo ARP (“AddressResolution Protocol") é utilizado com o objetivo de obter endereços IPv4.	F
	Numa tabela de encaminhamento (“routing table”)nunca podem existir dois destinos diferentes com o mesmo “next—hop".	F
	Numa mensagem HTTP o cabeçalho está sempre em formato de texto, o corpo pode ou não estar em formato de texto.	V
	Num pacote UDP (“User Datagram Protocol") o número de porto de destino nunca pode ser igual ao número de porto de origem.	F
	Num servidor TCP multi processo típico, a system—call fork é invocada antes da system—call accept.	F
	Num domínio DNS, a cada registo PTR no domínio “in-addr.arpa." deve corresponder um registo do tipo AAAA.	F
	Num segmento TCP o valor zero no campo WINDOW (tamanho da janela de receção) impede o envio de dados.	V
	Num datagrama IPv6 que transporta um datagrama UDP, onde termina o cabeçalho IPv6 começa sempre o cabeçalho UDP.	F
	Num “router de fronteira" e possível transferir regras entre um sistema autónomo RIPv2 e um sistema autónomo OSPF.	V
	Num pedido HTTP com o método POST deve existir uma linha de cabeçalho “Content—Length", mas não com o método GET	V
	Num “router" CISCO, o comando “encapsulation doth 90" é vándo no contexto de configuração de umasub interface.	V
	Num pedido com o método GET, a linha de cabeçalho “Content-Length" não existe ou indica um valor nulo.	V
	Num cabeçalho SMTP “Content—Transfer—Encoding: base64" apenas é válido se não estiver presente “MIME—Version: 1.0".	F
	Num cabeçalho SMTP Content—Transfer—Encoding: base 64 apenas é válido se estiver presente MIME—Version: 1.0.	V
	Num cabeçalho SMTP a linha de cabeçalho “MIME-Version: 1.0" não é obrigatória.	V
	Num domínio DNS é possível definir vários registos CNAME diferentes associados ao mesmo registo A ou AAAA.	V
	Num cabeçalho IPv6, em conjunto os endereços de origem e destino ocupam mais de metade do espaço existente.	V
	Num local loop através de CATV são necessários mecanismos de controlo de acaso ao meio e garantia de privacidade.	V
	Num nó IPv4, se um número de porto atá a ser usado pelo UDP, ase mamo número de porto não pode ser usado pelo TCP.	F
	Num router CISCO, o comando “ip dhcp pool REDE1" serve para criar/ editar uma configuração do servidor DHCP.	V
	Num segmento TCP (“Transmission Control Protocol") o valor do parâmetro WINDOW nunca pode ser zero.	F
	No protocolo IPv6 o PMTUD (“Path MTU Discovery”) foi abandonado, sendo usada sempre a fragmentação dos pacotes	F
	No SNMP quando é usada a mensagem TRAP o emissor nunca sabe se ela chegou ao destino.	V
	No sistema DNS (Domain Name System) qualquer Name Server tem a capacidade de resolver qualquer nome da Internet.	V
	No HTTP (“Hyper Text Transfer Protocol") a linha de cabeçalho “WWW—Authenticate" é acompanhada de uma “password".	F
	No sistema de resolução de nomes DNS, os “root name servers" conhecem os registos NS de todos os domínios de topo	V
	No SNMP (Simple Network Management Protocol) as mensagens são sempre transportadas através de ligações TCP.	F
	No TCP o valor do RTO (“Retransmission TimeOut") deve ser sempre superior ao valor do RTT (“Round-Trip Time") medido.	V
	No interior de um domínio de colisão há garantias de que os pacotes são recebidos na mama ordem em que são emitidos.	V
	No recetor, a relação entre a potência de sinal e de ruído (S/ N) é tanto menor quanto maior for a distância ao emissor.	V
	No cabeçalho de um pacote IPv4, o campo IHL (“Internet Header Length") nunca pode ter o valor zero.	V
	No HTTP, linha de cabeçalho “User Agent” acompanha normalmente os pedidos, não as respostas.	V
	No SNMP um pedido só é aceite pelo agente se o nome de comunidade constante do pedido for o correto.	V
	No SNMP versão 1 o nome de comunidade pode funcionar como chave de acesso ao agente, mas será legível na rede.	V
	No SMTP (“Simple Mail Transfer Protocol”) é o cliente quem envia a mensagem e servidor quem a recebe.	V
	No DNS os registos do tipo A, AAAA e CNAME são todos registos que associam um nome a um endereço IPv4.	F
	No protocolo HTTP o recetor da mensagem só sabe o tamanho do cabeçalho depois de terminar a sua leitura	V
	No protocolo IPv6 um endereço ANYCAST começa sempre por “FF" (byte mais significativo) e identifica um conjunto de nós	F
	No protocolo HTTP (“Hyper Text Transfer Protocol") a primeira linha de qualquer mensagem está sempre em formato de texto	V
	No sistema DNS os registos do tipo NS (“Name Server") são também vulgarmente daignados “glue records".	F
	No protocolo HTTP os métodos GET e POST podem ser usados para enviar dados ao servidor.	V
	No protocolo TCP o MSS (Maximum Segment Size) nunca pode ser superior ao MTU (Maximum Transmission Unit).	V
	No SNMPvl o agente é um pequeno servidor UDP que também funciona como cliente quando envia a mensagem TRAP.	V
	No protocolo RIP (“Routing Information Protocol") cada “router" divulga aos “routers" vizinhos a sua tabela de encaminhamento.	V
	No SNMP versão 1, quando um agente envia uma mensagem TRAP não tem nenhuma forma de saber se ela foi recebida.	V

No modelo OSI o PDU (“Protocol Data Unit") de uma camada é o SDU (“Service Data Unit") da camada imediatamente abaixo.	V
No HTTP a autenticação de utilizadores e possível, mas não é obrigatória.	V
No sistema DNS o domínio “in—addr.arpa" é usado para implementar a raolução inversa de endereços IPv4.	V
No protocolo RIP (“Routing Information Protocol") cada “router" elabora uma lista de “routers" vizinhos que divulga aos restantes.	F
No MR—OSI, 0 PCI (“Protocol Control Information") é uma parte do PDU ("Protocol Data Unit").	V
No HTTP (“Hyper Text Transfer Protocol") a primeira linha de uma mensagem nunca pode começar por “HTTP:"	F
No SNMP a ausência de resposta a um pedido GET indica necessariamente uma falha grave no agente / sistema gerido.	F
Numa rede de “broadcast" (meio partilhado) se dois nós emitem simultaneamente, os dados vão perder-se.	V
No SNMP (“Simple Network Management Protocol") as mensagens contêm nomes dos objetos em formato de texto.	F
No HTTP a diferença principal entre os métodos GE!" e POST está no local da mensagem onde os dados a enviar são colocados.	V
No sistema de resolução de noma DNS, conhecendo os “root name servers" torna—se possível resolver qualquer nome da árvore.	V
No DNS os registos do tipo CNAME não envolvem diretamente endereços IP.	V
No cabeçalho de um pacote IPv4 (“Internet Protocol” versão 4) todos os campos têm dimensões de quatro, oito ou dezasseis bits.	F
No TCP (“Transmission Control Protocol") o valor do RTO (“Retransmission Timeºut”) nunca pode ser de 10 segundos.	F
No sistema DNS cada NS (Name Server) tem de conhecer os NS dos seus subdomínios.	V
No HTTP a linha de cabeçalho “Content—length:” indica quantas unha existem no cabeçalho.	F
No modelo OSI (“Open Systems Interconnection”) cada camada tem de conhecer o funcionamento de todas as camadas abaixo.	F
No TCP (Transmission Control Protocol) o valor do RTO (Retransmission Time Out) nunca pode ser de 10 segundos.	F
No DNS os registos do tipo PTR podem ser deduzidos diretamente dos registos do tipo A.	V
No DNS os registos do tipo CNAME definem diretamente endereços IPv4.	F
No IPv4 o emissor de um pacote tem a possibilidade de indicar se deseja que seja aplicada a fragmentação ao pacote ou não.	V
No TCP (“Transmission Control Protocol") o valor do RTO (“Retransmission Timeºut”) nunca pode ser nulo.	V
No DNS, para resolver um nome de um domínio é necessário determinar o endereço de um servidor de nomes desse domínio.	V
No sistema DNS cada servidor de noma deve conhecer os endereços IP dos servidores de noma dos seus subdomínios.	V
No modelo OSI (Open Systems Interconnection) podemos afirmar que PDUn = PCIn + PDUn+1.	V
No IPv6 todos os endereços “multicast" começam (bits mais significativos) com a sequência “FF02”.	F
No protocolo RIP (“Routing Information Protocol") os sistemas autónomos são identificados por um número de 1 a 65535.	F
No protocolo PPTP a autenticação dos utilizadores é assegurada pelo protocolo PPP.	V
No protocolo IPv4 (“Internet Protocol” versão 4) não são detetados erros na transmissão dos dados transportados.	V
No DNS cada registo (RR - “Resource Record”) contém um campo que especifica o tempo de validade do mesmo.	V
No PPP, para cada protocolo transportado existe um protocolo de controlo designado NCP (Network Control Protocol).	V
No protocolo L2TP as caraterísticas de segurança são asseguradas pelo IPSEC e eventualmente o PPP.	V
No sistema DNS o registo PTR “50.67.130.194.in-addr.arpa" permite a resolução inversa do endereço IPv4 “194.130.67.50".	V
No protocolo HTTP (“Hyper Text Transfer Protocol") qualquer mensagem começa sempre por uma sequência de linhas de texto.	V
No MR—OSI, de um PDU (Protocol Data Unit) criado no nível 5 vai resultar num PDU de maior dimensão no nível 3.	V
Nos protocolos do tipo distance-vector cada router divulga aos vizinhos a sua tabela de encaminhamento.	V
Nos cabeçalhos IPv4 (“Internet Protocol" versão4) o campo TTL deve ter sempre o valor zero quando o pacote é emitido.	F
Nem todos os servidores SMTP reconhecem o comando “EHLO”, nesse caso terá de ser usado o comando “HELO”.	V
Na emissão de uma trama (pacote) “Ethernet" os dados são emitidos em primeiro lugar, seguindo—se o endereço de destino.	F
Na API Sockets de Berkeley a System—call accept é bloqueante, quando desbloqueia devolve um novo socket.	V
Na arquitetura IEEE 802 a camada MAC implementa um mecanismo de deteção de erros.	V
Na técnica CSMA/ CA usada nas redes 802.11, as cofrsõa são detetadas pelo facto de não haver um ACK do recetor.	V
Na rede IPv6 fd1e:cafe:fd:4:: / 64 o endereço de broadcast é fd1e:cafe:fd:4:ffff:ffff:ffff:ffff.	V
Na deteção de erros, se o código calculado pelo recetor é diferente do enviado pelo emissor, então ocorreu um erro.	V
Na API “Berkeley Sockets" em linguagem C, a “system—call" “connect" apenas pode ser usada sobre “sockets" do tipo TCP.	F
Na deteção de erros de transmissão é necessário que o recetor conheça o algoritmo usado pelo emissor no cálculo do código.	V
Na técnica CSMA/ CA usada nas redes 802.11, quando um nó está a emitir e deteta uma colisão cessa de imediato a emissão.	F
Na arquitectura TCP/IP a camada IP (“Internet Protocol") corresponde à camada de rede do modelo OSI.	V
Na utilização de redes de televisão por cabo (CATV) para efeitos de “local loop" é necessário recorrer a algoritmos criptográficos.	V
Na arquitetura IEEE 802 (ISO 8802) a camada MAC(“Medium Access Control") não é usada nas implementações atuais.	F
Na comutação de pacotes com circuitos virtuais todos os pacotes com o mesmo identificador de circuito seguem o mesmo caminho.	V
Na comutação de pacotes sem circuitos virtuais cada pacote contém um endereço de nó de origem e um endereço de nó de destino.	V
Nas redes ATM os PDU são designados células, uma das suas caraterísticas é terem um tamanho fixo e reduzido.	V
Nas mensagens SNMP os objetos da MIB são identificados através do respetivo OID (Object Identifier).	V
Nas VPN que operam sobre TLS, a autenticação tem de ser sempre assegurada por certificados de chave pública.	F
Nas VPN do tipo LAN-LAN, cada utilizador tem sempre de se autenticar no servidor VPN para poder aceder à rede remota.	F
Nas codificações bifásicas, não existe nenhuma sequência de bits para a qual o sinal resultante permaneça no mesmo nível.	V
Nas células ATM não existe deteção de erros de transmissão que possam ocorrer nos dados transportados.	V
Nas redes locais sem fios 802.11 assim que ocorre uma colisão os nós deixam imediatamente de emitir.	F
Nas redes de comutação com caminhos virtuais todos os pacotes contêm o endereço do nó de destino.	F
Nas redes 802.11, quer seja utilizado CSMA/ CA ou RTS/ CTS, após a receção de dados bem-sucedida é sempre enviado um “ACK”.	V

	Nas redes 802.11 a utilização de uma chave pré—partilhada assegura a autenticação, mas não a confidencialidade.	F
	Nas redes ATM numa sequencia de células associadas ao mesmo canal virtual a ordem é garantida.	V
	Não é possível ligar um router de fronteira a dois sistemas autónomos RIP diferentes.	V
M	Mesmo que o cabeçalho TCP não inclua opções, tem sempre uma dimensão superior à de um cabeçalho UDP.	V
O	O ICMPv6 pode ser usado no contexto do IPv6 para implementar funcionalidades equivalentes às do ARP no IPv4.	V
	O protocolo PPP ("Point to Point Protocol") tema desvantagem de apenas transportar pacotes IPv4, não suportando IPv6 .	F
	O PMTUD (“Path Maximum Transmission Unit Discovery”) tem como objetivo evitar a necessidade de fragmentar os pacotes IP.	V
	Os sinais eletromagnéticos de baixa frequência (1 KHz) são sinais analógicos também conhecidos como “micro-ondas".	F
	O SMTP (“Simple Mail Transfer Protocol") é o protocolo usado nas comunicaçõs entre os MTA (“Mail Transport Agent")	V
	O Wireless Local Loop (WLL) permite alcances de vários quilômetros usando a tecnologia 802.11.	F
	O protocolo POP3 ("Post Office Protocol version3") é uma alternativa ao SMTP para o envio de mensagens de correio eletrónico.	F
	O ICMP (“Internet Control Message Protocol") é usado na implementação do mecanismo PMTUD	V
	O protocolo L2TP (“Layer 2 Tunnenng Protocol")não implementa mecan'smos que garantam a autenticação ou a privacidade.	V
	O número de endereços IPv6 (128 bits) possíveisé o quádruplo do número de endereços IPv4 (32 bits) possíveis.	F
	O controlo de fluxo com janela deslizante serve para garantir que os pacotes são recebidos na mesma ordem em que são emitidos.	F
	O controlo de fluxo “stop & wait" é mais adequado para comunicações de longa distância em que existem grandes atrasos	F
	O único registo DNS que associa diretamente um nome a um endereço IPv4 é o registo do tipo A.	V
	O SNMP versão 1 suporta autenticação baseada numa chave pré partilhada protegida com os algoritmos MDS ou SHA.	F
	O controlo de erros ARQ (Automatic Repeat reQuat) contínuo e do tipo BEC (Backward Error Correction).	V
	O “Content-Transfer—Encoding: base64” permite representar qualquer conjunto de bytes sob a forma de carateres legíveis.	V
	O SNMP (“Simple Network Management Protocol") versão 1 define um conjunto de mensagens que são transportadas por UDP.	V
	O SMTP (“Simple Mail Transfer Protocol") permite aos utilizadores receberem mensagens armazenadas em servidores remotos.	F
	O SNMP versão 3 entre outras melhorias inclui mecanismos de autenticação e confidencialidade nas transações.	V
	O ICMP (“Internet Control Message Protocol”) usa números de porto que possibilitam a utilização simultânea por várias aplicações.	V
	O cabeçalho IPv6 possui menor número de campos do que o cabeçalho IPv4 (sem opções), mas apesar disso ocupa mais espaço.	V
	O protocolo UDP não garante o envio de pacata com mais do que 512 bytes de dados.	V
	O registo TXT com o valor “v=spf1 +mx —a|\" associado ao nome do domínio serve para controlar o envio de correio eletrônico.	V
	O ARQ (“Automatic Repeat reQuest") é um mecanismo de correção de erros de transmissão que obriga o emissor a repetir o envio.	V
	O DOCSIS (“Data Over Cable Service Interface Specification”) inclui mecanismos de controlo de acesso ao meio partilhado.	V
	O protocolo IPv6 não utiliza o protocolo ARP (Address Resolution Protocol).	V
	O tempo que um sinal demora a percorrer um dado meio de transmissão depende da taxa de transmissão usada.	F
	O protocolo ICMP (Internet Control Message Protocol) é transportado pelo protocolo TCP (Transmission Control Protocol).	F
	O OSPF (Open Shortest Path First) é um protocolo da categoria distance—vector.	F
	O protocolo IGMP (Internet Group Management Protocol) é usado no IPv4 para gerir grupos de multicast.	V
	O endereço IPv6 “FECO::20A5" tanto pode ser usado como endereço UNICAST como endereço ANYCAST.	V
	O WINS (“Windows Internet Name Service”) elimina alguns dos problemas da resolução de nomes NetBIOS por “broadcast".	V
	O parâmetro “WINDOW” dos cabeçalhos TCP é usado para controlo de fluxo, nunca pode ter o valor zero.	F
	O protocolo ARP (“Address Resolution Protocol") opera sobre o UDP e tem como principal objetivo a construção da tabela MAC.	F
	O controlo de fluxo com janela dalizante nuncapode ser usado em rlgaçõa que não suportam “full-duplex”.	F
	O MR-OSI define apenas três camadas: IP; UDP e TCP.	F
	O ARQ (“Automatic Repeat reQust") contínuo usao protocolo de janela deslizante para controlo de erros por retransmissão.	V
	O controlo de erros ARQ (“Automatic Repeat reQuest") contínuo é do tipo BEC (“Backward Error Correction").	V
	Observando o registo SOA (“Start Of Authority")podemos determinar em que dia foi realizada a última alteração à base de dados.	V
	O PMTUD (Path Maximum Transmission Unit Discovery) faz uso de mensagens ICMP (Internet Control Message Protocol).	V
	O “local loop" é uma ligação de nível 2, mas a ligação entre subscritores tem de recorrer a um protocolo de nível 3.	V
	O pedido HTTP começado pela linha “OPTIONS * HTTP/1.1" permite saber quais são os métodos suportados pelo servidor.	V
	O SMTP (Simple Mail Transfer Protocol) permite aos utilizadores receberem mensagens armazenadas em servidores remotos.	F
	O nome DNS “200.30.89.120.in—addr.arpa" corresponde a um registo do tipo PTR para o endereço IPv4 “120.89.30.200".	V
	O protocolo DHCP (“Dynamic Host Configuration Protocol”) usa ligações TCP (“Transmission Control Protocol").	F
	O controlo de erros do tipo BEC (Backward Error Correction) baseia—se em pedidos de retransmissão em caso de erro.	V
	O objetivo do Local Loop é assegurar o transporte de pacata IP entre o subscritor e o operador de telecomunicações.	V
	O protocolo UDP (“User Datagram Protocol") deteta erros de transmissão e corrige—os através da retransmissão.	F
	O ICMP (“Internet Control Message Protocol") é normalmente usado para transportar dados entre aplicações de rede.	F
	O tempo que um pacote demora a ser transferido entre dois nós intermédios não depende da distância entre ela.	F
	O cabeçalho de uma trama “Ethernet II" (Dlx) contém dois endereços com 48 bits (6 bytes) cada.	V
	O endereço de nó IPv6 “0034:BC1F:1384::0510", pertence à rede IPv6 “0034:BC1F::/48".	F
	O endereço IPv6 “FF05::1” é um endereço multicast, vai corresponder ao endereço multicast ethernet “33:33:00:00:00:01”.	V

	O endereço de nó IPv6 “0034:BC1F:1384::0510", pertence à rede IPv6 “0034:BC1F::/48".	F
	O protocolo UDP (“User Datagram Protocol") é usado como meio de transporte pelo DHCP (“Dynamic Host Configuration Protocol").	V
	O encaminhamento dinâmico é fundamental quando existem vários caminhos diferentes para chegar ao mesmo destino.	V
	O mecanismo PMTUD (“Path Maximum Transmission Unit Discovery") evita a fragmentação de “datagramas” IPv4.	V
	O protocolo SNMP permite não apenas a consulta da MIB, mas também a sua alteração.	V
	O registo TXT com o valor “v=spf1 +mx —all” associado ao nome do domínio serve para controlar o envio de correio eletrônico.	V
	O ARP (“Addras Raolution Protocol") pode ser usado entre nós que se encontram em redes diferentes ligadas por um “router".	F
	O endereço IPv6 FF02::2 é um endereço multicast, quando um pacote é enviado para ele todos os membros recebem.	V
	O PCI ("Protocol Control Information”) adicionado pela camada de rede é recebido e interpretado pela camada de transporte.	F
	O diálogo com os servidores de nomes do sistema DNS recorre apenas ao UDP, nunca ao TCP.	F
	O SMTP é usado para enviar mensagens de correio, o endereço de correio do destinatário indica qual o MTA a contactar.	V
	O campo E—TYPE ex'stente nos cabeçalhos dos pacata “Ethernet" contém números de porto UDP/TCP.	F
	O parâmetro “WINDOW" dos cabeçalhos TCP é usado para controlo de fluxo, o seu valor é definido pelo nó recetor dos dados.	V
	O DNS (“Domain Name System") permite resolver qualquer nome da “Internet" desde que se conheça os “root name servers".	V
	O protocolo IPv6 (“Internet Protocol version 6") não suporta nenhum tipo de fragmentação de pacotes.	F
	O protocolo de acesso ao meio usado nas redes locais sem fios 802.11 é exatamente igual ao que é usado nas redes “Ethernet".	F
	O PCI (”Protocol Control Information") da camada de rede vai ser parte integrante do SDU da camada de ligação lógica.	V
	O tempo que um pacote demora a atravessar uma rede de comutação depende apenas da taxa de transmissão e da distância.	F
	Os valores que identificam os tipos de mensagens ICMPv6 são iguais aos do ICMPv4, mas os formatos são totalmente diferentes.	F
	Os registos MX do DNS são usados para associar ao nome de um domínio um endereço IP e número de porto.	F
	Os protocolos de VPN usados numa VPN do tipo “LAN—LAN" são semelhantes aos usados numa VPN “HOST-LAN".	V
	Os pacotes mais pequenos sofrem menos atraso ao atravessar os nós intermédios que estão a operar em modo “store & forward".	V
	Os registos Mx do DNS (“Domain Name System") não contêm qualquer referência direta a endereços IPv4 ou IPv6.	V
	Os endereços “multicast” do IPv6 começam sempre(bits mais significativos) com a sequência “FF".	V
	Os vários pontos de acesso 802.11 de uma infraestrutura devem ser sempre interligados por rede cablada.	V
	Os servidores WINS (“Windows Internet Name Service") são implementações do serviço DNS (“Domain Name System")	F
	Os pacotes criados na camada AAL 5 (“ATM Adaptation Layer 5”) podem ter um comprimento total com qualquer valor de 0 a 64k.	F
	Os problemas de eficiência da técnica “stop & wait” podem ser resolvidos se for usada uma taxa de transmissão muito elevada.	F
	Os sinas digitais caraterizam-se por apresentarem variações bruscas entre patamares bem definidos.	V
	Os sinais eletromagnéticos de baixa frequência (1 KHz) são sinais analógicos, os sinais de frequência superior são digitais.	F
	Os nós intermédios a operar em modo “cut-through" têm como principal vantagem uma redução do tempo de atraso na rede.	V
	Os registos DNS do tipo CNAME são úteis para atribuir vários nomes diferentes & um mesmo nó de rede.	V
	Os comutadores “Ethernet" em modo “store & forward” necessitam de ter a capacidade de armazenar dados internamente.	V
	Os endereços ANYCAST do IPv6 são equivalentes aos endereços MULTICAST do IPv4.	F
	Os mecanismos de deteção de erros de transmissão nunca são totalmente fiáveis, podem ocorrer erros que não são detetados.	V
	Os registos do tipo SRV do DNS servem para definir um serviço de rede incluindo o protocolo de transporte e o número de porto.	V
	Os “glue record" são registos do tipo A ou AAAAcorrespondentes a nomes associados a registos do tipo NS (“Name Server").	V
	Os servidores DNS atendem os pedidos dos clientes e outros servidores (“DNS QUERY") via UDP ou TCP num mesmo porto fixo.	V
	Os nós intermédios a operar em modo cut—through têm como principal vantagem uma redução do tempo de atraso na rede.	V
P	Para enviar dados para uma aplicação TCP residente num dado nó, e suficiente conhecer o endereço desse nó.	F
	Para o envio de uma mensagem de correio entre dois utilizadores locais é necessário criar uma sessão entre dois MTA.	F
	Para cada endereço IPv4 “multicast" de 32 bits existe um endereço Ethernet “multicast" de 48 bits correspondente.	V
	Para o DHCP (“Dynamic Host Configuration Protocol") funcionar é necessário que cliente e servidor estejam na mesma rede local.	V
	Para ligar por um cabo Ethernet a 1 Gbps dois pontos distantes entre si de 700 metros é necessário recorrera fibra ótica.	V
	Para a mesma taxa de transmissão, as codificações bifásicas produzem sinais de frequência mais elevada do que as NRZ.	V
	Para o DHCP (Dynamic Host Configuration Protocol) funcionar é necessário que cliente e servidor estejam na mama rede local.	V
	Para cada endereço IPv4 multicast existe um único endereço Ethernet multicast correspondente.	V
	Para um dado pacote de dados, o tempo necessário para o emitir a 100 Mbps e metade do tempo que seria necessário a 50 Mbps.	V
	Para transferir entre duas aplicações um volume de dados de 2048 bytes nunca poderá ser usado UDP (“User Datagram Protocol").	F
	Para os mamos dados, a codificação do tipo NRZ-l., produz um sinal de menor frequência do que a codificação “Bifásica—L".	V
	Para acesso remoto à respetiva mailbox um utilizador pode usar em alternativa ao SMTP, os protocolos POP3 ou IMAP4.	F

	Para que o protocolo de janela deslizante consiga operar sem pausas é necessário que a transmissão seja “full-duplex".	V
Q	Quando se solicita a receção de um datagrama através de um socket UDP é necessário indicar o tamanho exato do datagrama e tem de coincidir exatamente com o tamanho do datagrama que foi enviado.	V
	Quando se solicita a receção de um datagrama através de um socket UDP é necessário indicar o tamanho exato do datagrama e tem de coincidir exatamente com o tamanho do datagrama que foi enviado.	F
	Quando se usa o protocolo UDP para enviar um datagrama, ficamos de imediato a saber se ele chegou ao destino.	F
	Quando um nó envia um pedido de eco ICMP, pode receber uma mensagem ICMP que não é “Echo Reply".	V
	Quando um agente SNMP envia uma mensagem TRAP recebe uma confirmação (ACK) de que a mama chegou ao destino.	F
	Quando um cliente SMTP responde à mensagem inicial com “EHLO” todos os servidores SMTP devem indicar sucesso.	F
	Quando se utiliza a system—call connect para associar um socket UDP a um endereço remoto obtém—se um socket TCP.	F
	Quando uma trama Ethernet transporta um pacote IPv4, o endereço MAC de destino contém um endereço IPv4.	F
	Quando um nó de uma rede 802.11 escuta um RTS ou CTS de terceiros, isso significa que pode emitir imediatamente.	F
	Quando se utiliza o método GET para enviar dados a uma aplicação no servidor, os dados são colocados na primeira linha.	V
	Quando uma infraestrutura de rede utiliza VLANs, todos os nós ligados têm obrigatoriamente de utilizar etiquetas IEEE 802.1q.	F
	Quando uma aplicação recebe um “datagrama” UDP fica a saber o número de porto de origem e endereço IP de origem.	V
	Quando um subscritor emite uma trama ethernet no local loop, essa trama nunca pode chegar a outro subscritor.	V
	Quando uma aplicação pretende receber um “datagrama" UDP necasita de saber previamente a quantidade de byts a ler.	F
	Quando num domínio são definidos vários registos do tipo Mx nunca podem ter todos o mesmo nível de preferência.	F
	Quando uma trama 802.3 chega a um ponto de acesso (Access Point) pode ser fragmentada em várias tramas 802.11.	V
	Quando um servidor TCP aceita uma ligação TCP de um chente, é gerado um novo sockets ligado ao cliente.	V
	Quando o campo TTL do cabeçalho IPv4 chega a zero e emitida uma mensagem ICMP do tipo “Time Exceeded".	V
	Quando numa ligação TCP se utiliza a leitura baseada em marcador de fim de bloco, os bytes têm de ser lidos um a um.	V
	Quando se utilizam threads ou procasos para implementar a receção assíncrona o objetivo é que nenhum thread ou processo fique bloqueado á espera de dados.	F
	Quando se coloca um sinal num meio de transmissão, seja qual for a frequência do sinal, a atenuação é sempre a mesma.	F
	Quando em resposta ao comando EHLO se obtém um erro, isso pode significar que o servidor não suporta ESMTP.	V
	Quando um pacote IPv4 é recebido, observando o cabeçalho pode determinar—se que dados contém (TCP, UDP, ...).	V
	Quando um servidor SMTP responde com erro à mensagem EHLO deve ser usada a mensagem HELO.	V
	Quando um cliente estabelece uma ligação TCP com um servidor, do lado do servidor TCP é criado um novo “socket".	V
	Quando um comutador “Ethernet" está a receber uma trama numa porta fica impossibilitado de receber tramas noutras portas	F
	Qualquer tipo de rede Ethernet com topologia em atrela atá livre da ocorrência de colisões.	F
S	Se um comutador "ethernet" recebe simultaneamente dois pacotes com o mesmo endereço de destino ocorre uma colisão.	F
	Se um “router" está ligado apenas a duas redes IP, então na tabela de encaminhamento só podem existir dois “next-hop" diferentes.	F
	Se um pacote IPv6 é usado para transportar um pacote UDP, este pode não estar imediatamente a seguir ao cabeçalho IPv6.	V
	Se uma VPN opera sobre uma infraestrutura de rede IPv4, o único protocolo que pode transportar e IPv4.	F
	Se o código de deteção de erro for recebido antes dos dados, depois de recebido pode logo determinar—se se ocorreu um erro.	F
	Se o administrador de um domínio DNS (“Domain Name System”) quer definir um novo nome tem de contactar o “root name server".	F
	Se um nó possui o endereço Ethernet “01:2B:17:7A:BB:1A", através do valor “01:2B:17"é possível determinar qual é o fabricante.	V
	Se o endereço de destino se encontrasse no final do pacote (cauda) os nós não poderiam operar em modo “cut-through".	V
	Se uma trama Ethernet transporta um pacote IPv4, o endereço MAC de destino corresponde sempre ao endereço IPv4 de destino.	F
	Se duplicar—mos a distância entre dois nós, o tempo total para transferir um pacote entre ela também duplica.	F
	Se numa infraestrutura é necessário atravessar20 “routers" para chegar à rede de destino, o protocolo RIP não pode ser usado.	V
	Se um router está ligado a cinco redes IPv4 diferentes, o número máximo de diferentes next-hop que pode usar é cinco.	F
	Se o endereço de destino de um pacote IPv4 não corresponde a nenhuma linha da tabela de encaminhamento, o pacote não é encaminhado.	V
	Se uma mensagem SMTP não contém a linha de cabeçalho “Content—Transfer—Encoding:" então é assumido o valor “7bit”.	V
	Se o endereço de destino fosse o último elemento do pacote a ser emitido, não poderia ser usado o modo “cut-through “	V
	Segundo o modelo OSI os PCI (“Protocol Control Information”) das várias camadas são transferidos através do nível 1.	V
	Se o código de deteção de erros calculado pelo recetor não é igual ao enviado pelo emissor, então ocorreu um erro na transmissão.	V
	Se o meio de transmissão não suporta a frequência zero, em lugar de sinais digitais é necessário usar sinais analógicos.	V
	Se o campo “NEXT-HEADER" do cabeçalho IPv6 indicar o protocolo TCP, então não existem cabeçalhos de extensão.	V
	Se um “socket” UDP for associado a um endereço remoto através da “system—call” “connect” ele passa a ser um “socket” TCP.	F
	Se um meio de transmissão suporta um sinal com uma frequência de 100 MHz, então com NRZ é possível transmitir a 200 Mbps.	V
	Se recebemos um segmento TCP com o valor zero no parâmetro “window" ficamos impedidos de enviar dados para o nó de origem.	V
	Se o campo NEXT-HEADER do cabeçalho IPv6 indicar o protocolo TCP, então não existem cabeçalhos de extensão.	V
	Só é possível determinar se ocorreu um erro na transmissão de um pacote depois de se receber integralmente esse pacote.	V

	Segundo o modelo OSI o SDU ("Service Data Unit") do nível 3 é o conjunto de dados transacionado com o nível 4.	V
	Segundo o modelo “Agente-Gestor" a MIB (“Management Information Base”) encontra—se no agente que reside no sistema gerido.	V
	Seja qual for a técnica de codificação, observando o nível de um sinal digital pode determinar—se o símbolo (0, 1, ...).	F
T	Todas as mensagens de correio SMTP têm obrigatoriamente de conter a linha de cabeçalho “MIME—Version: 1.0".	F
	Tal como os registos MX, os registos CNAME associam um nome a um endereço IPv4	F
	Todas as mensagens SNMPvl contêm um string de controlo de acesso cifrado designado “Community".	F
	Tanto nos pedidos como nas resposta HTTP, a versão do protocolo é indicada na primeira linha da mensagem.	V
U	Uma das melhorias do RIPv2 relativamente ao RIPv1 é a utilização de multicast em lugar de broadcast.	V
	Uma mensagem HTTP começada por “HTTP/ 1.1 403“indica que não houve sucesso no tratamento do pedido correspondente	V
	Uma camada de ligação lógica (nível 2) identifica a camada superior a que os dados pertencem atravªs do número de porto.	F
	Uma resposta HTTP “500 Internal Server Error” significa que o pedido foi mal formulado.	F
	Uma mensagem SMTP que não contenha a linha de cabeçalho “MIME—Version: 1.0” não pode conter ficheiros anexos.	V
	Uma ligação de VPN tanto pode ser usada para simular uma ligação entre switchs como uma ligação entre routers.	V
	Uma caixa de correio (mailbox) pode ser um ficheiro ao qual apenas um utilizador e o sistema têm acesso.	V
	Uma VPN pode ser usada para interligar diretamente duas redes “ethernet" remotas que passam a funcionar como uma única rede.	V
	Uma vantagem da resolução de nomes NetBIOS por “broadcast" é o facto de permitir o registo de nomes iguais.	F
	Uma mesma ligação PPP pode ser usada para transportar simultaneamente pacotes de diversos protocolos.	V
	Uma trama “Ethernet II” (DIx) pode transportar um máximo de 1500 bytes de dados.	V
	Uma vantagem dos protocolos do tipo link-state é que apenas propagam informação quando existem alterações.	V
	Uma célula ATM consegue transportar aproximadamente a mesma quantidade de dados que uma trama “Ethernet".	F
	Um sistema autónomo (Autonomous System) delimita a zona de propagação de um protocolo de encaminhamento.	V
	Um endereço de nó IPv6 tem capacidade para conter um endereço de nível 2 com 48 bits, por isso o ARP não é necessário.	V
	Um efeito de associar um “socket” UDP a um endereço remoto através da “system—call” “connect" é a filtragem segundo a origem.	V
	Um sinal elétrico propaga-se mais rapidamente numa fibra ótica do que num cabo de cobre.	F
	Um pedido HTTP com o método GET pode ter corpo (body/content/entity).	F
	Um único pacote IPv6 pode ser usado para transportar vários cabeçalhos de extensão e um pacote UDP.	V
	Um datagrama IPv4 pode ter um comprimento total (cabeçalho e dados) superior a 1500 bytes.	V
	Um pedido HTTP com o método POST nunca contém a linha de cabeçalho “Content-type:".	F
	Um “socket" TCP pode ser usado para emitir em “broadcast” desde que não esteja associado a nenhum endereço remoto.	F
	Um servidor TCP nunca pode ser implementado sem recorrer a programação multi—processo.	F
	Um PDU AAL5 (ATM Adaptation Layer 5) é capaz de transportar muito mais dados do que uma trama ethernet.	V
	Um nó intermédio que opera em modo “cut-through" não consegue detetar erros antes de começar a retransmissão do pacote.	V
	Um agente SNMP (“Simple Network Management Protocol") é uma aplicação servidora residente no sistema gerido.	V
	Um valor possível para o campo “NEXT-HEADER" do cabeçalho IPv6 é o que representa o protocolo TCP.	V
	Um nó intermédio que opera em modo “cut—through"não pode emitir um pacote a uma taxa de transmissão superior à de receção.	V
	Usando ligações do tipo “local—loop” não é possível transmitir diretamente uma “trama" (pacote) “ethernet" entre dois subscritores.	V