

Mestrado Integrado em Engenharia Informática
Redes de Computadores

Ano Letivo 2019/2020 • Exame de Recurso • 3 Fevereiro 2020

Duração Total: 120 Minutos

INSTRUÇÕES

- Salvo indicações alternativas expressas pelo docente na sala, o único material permitido é material de escrita, cartão de identificação com fotografia, uma garrafa de água e um pacote de lenços de papel.
- Os alunos responderão às questões do enunciado na própria folha do enunciado.
- Depois de terminarem, os alunos devem sair ordeiramente e em silêncio da sala após permissão do docente, deixando o teste em cima da mesa. Os testes serão recolhidos pelo docente.
- Nenhum aluno poderá abandonar a sala sem que tenham passado pelo menos 30 minutos depois do início do teste e sem que o docente na sala não tenha procedido à confirmação da sua identidade e rubricado o teste.
- Nenhum aluno poderá abandonar a sala nos últimos 15 minutos do tempo disponível para realização do teste por forma a causar a menor disrupção possível. Os alunos que ficarem para os últimos 15 minutos deverão abandonar a sala apenas no final do tempo total e após indicação do docente, deixando o teste em cima da mesa.

Número:		Nome:	
----------------	--	--------------	--

GRUPO I (10x5%, 60 minutos)

Classifique cada uma das quatro afirmações (A1, B2, C3 e D4) em cada questão como verdadeira ou falsa. Em cada questão, cada afirmação mal classificada anulará a pontuação numa afirmação bem classificada, não havendo transporte de pontuações negativas entre questões ou grupos.

1. Uma tarefa básica do nível da ligação de dados (segundo nível da pilha OSI) é transferir PDUs (*Protocol Data Units*) entre nós adjacentes, sendo que:

A1	Quando os PDUs transmitidos entre nós deste nível da pilha não são tratados nos encaminhadores a uma velocidade adequada podem ficar retidos em filas de espera antes de serem reenviados para o próximo nó.					
B2	As metodologias de partilha do meio de transmissão com deteção de colisões são utilizadas tanto em tecnologias de redes-com-fios (cabladas) como em tecnologias de redes-sem-fios (Wi-Fi).					
C3	Este nível protocolar define mecanismos e funcionalidades em processos de comunicação direta entre interfaces por forma a serem suportados vários tipos de protocolos de comunicação de nível de rede.					
D4	É costume utilizarem-se mecanismos de controlo de fluxo e recuperação de erros no nível de ligação de dados quando suportados sobre tecnologias de nível físico sem partilha do meio de transmissão.					
Verdadeiras:		B2	C3	D4		
Falsas:	A1					

2. Em tecnologias de partilha de meio de transmissão sem fios Wi-Fi (IEEE 802.11):

A1	Uma estação pronta a enviar dados, assim que deteta o meio sem comunicações ativas, pode enviar dados durante um tempo máximo específico que lhe é reservado para o efeito, independentemente de haver colisões ou não durante o processo.					
B2	Nas tramas de dados, os bits <i>toDS</i> e <i>fromDS</i> definem a utilização que os quatro campos de endereçamento têm.					
C3	A variante 802.11n permite um alcance máximo e um débito de informação máximo superiores aos conseguidos com a variante 802.11b, mesmo sem a utilização de múltiplas antenas.					
D4	Todas as tramas contêm quatro endereços MAC, cada um ocupando 48 bits e, no modo infra-estrutura, o valor dos quatro endereços são sempre relevantes.					
Verdadeiras:	A1	B2	C3			
Falsas:				D4		

3. Em tecnologias de partilha de meio de transmissão com fios Ethernet (IEEE 802.3):

A1	O comprimento máximo dos cabos de ligação depende do valor temporal máximo que é usado para detetar colisões no meio de transmissão.				
B2	Ao contrário dos endereços de rede IPv4, os endereços MAC IEEE 302.3 são de natureza lógica, i.e., dependem do endereçamento da rede a que o interface está ligado.				
C3	O paradigma de controlo de acesso e de utilização do meio permite comunicações fiáveis ao nível de ligação de dados porque as colisões são detetadas e evitadas.				
D4	Só é possível dois interfaces comunicarem entre si se funcionarem ambos a débitos de informação exatamente iguais.				
Verdadeiras:	A1			D4	
Falsas:		B2	C3		

4. No nível protocolar de rede (terceiro nível da pilha OSI):

A1	O paradigma de comunicação por comutação de circuitos (ou circuitos virtuais) é mais fiável (menos sujeita a disrupção por falhas de nós intermédios) que a comunicação no paradigma de comutação de pacotes (ou redes de datagramas) porque mais facilmente permite controlo de fluxo e de congestão.				
B2	A troca de dados é possível entre interfaces na mesma rede física bem como entre interfaces em redes físicas distintas desde que utilizam a mesma tecnologia de nível de ligação.				
C3	Os endereços de rede são sempre endereços lógicos sem qualquer ligação semântica aos endereços dos níveis protocolares inferiores.				
D4	O paradigma de comunicação por comutação de pacotes (ou redes de datagramas) é mais escalável em termos do número de sistemas finais (<i>hosts</i>) do que o paradigma por comutação de circuitos (ou circuitos virtuais).				
Verdadeiras:			C3	D4	
Falsas:	A1	B2			

5. No nível de rede da pilha protocolar TCP/IP:

A1	Nas redes IPv4 nunca é possível um pacote de dados passar no mesmo sistema intermédio mais do que uma vez devido à utilização do campo de <i>Time to Live</i> (TTL) no cabeçalho de todos os pacotes.				
B2	As mensagens do <i>Internet Control Message Protocol</i> (ICMP) são encapsuladas em pacotes IPv4 pelo que estes pacotes IPv4, em especial, nunca podem ser fragmentados.				
C3	O processo de encaminhamento em redes IP utiliza tabelas de encaminhamento em todos os sistemas finais (<i>hosts</i>) ou intermédios (<i>routers</i>) e podem conter, simultaneamente, entradas resultantes de mecanismos dinâmicos e entradas resultantes de definições estáticas.				
D4	O processo de encaminhamento em redes IP permite que um pacote de dados se aproxime, a cada iteração, do interface de destino, sendo que a decisão de encaminhamento é tomada em todos os equipamentos de nível rede por onde o pacote passar tendo em consideração o endereço de rede, ou sub-rede, de origem.				
Verdadeiras:		B2	C3		
Falsas:	A1			D4	

6. No endereçamento de redes IP:

A1	Um endereço IPv4 tem um espaço de endereçamento aproximadamente 8^{32} menor do que o espaço de endereçamento do IPv6.				
B2	A existir, o sub-endereçamento, numa determinada rede classe C, tem, para todas as sub-redes, a mesma máscara de sub-endereçamento.				
C3	O endereço 100.0.0.1/30 é um endereço que não pode ser utilizado por nenhum interface IPv4.				
D4	O uso dum endereço IPv4 com os bits todos a zero na parte de endereçamento de sub-redes e tudo a um na parte de endereçamento de interfaces/ <i>hosts</i> indica o envio do pacote para todos os interfaces/ <i>hosts</i> de todas as sub-redes (<i>broadcast</i>).				
Verdadeiras:	A1		C3		
Falsas:		B2		D4	

Número:		Nome:	
----------------	--	--------------	--

7. No serviço de entrega de pacotes em redes IPv4:

A1	Todos os pacotes IPv4 podem ser vistos como fragmentos. Um pacote IPv4 que não tenha sofrido fragmentação pode ser visto, na realidade, como um único fragmento final com <i>Fragment Offset</i> =0.				
B2	Um pacote IPv4, depois de ser fragmentado, só deve ser reconstruído no sistema final com o interface com o endereço de destino, ainda que fosse tecnicamente possível o pacote ser reconstruído num <i>router</i> intermédio sem que o sistema final se apercebesse.				
C3	O processo de fragmentação dum pacote IPv4 pode acontecer no próprio sistema inicial com o interface com o endereço de origem.				
D4	Só é possível entregar um pacote IPv4 para um sistema que tenha um interface com o mesmo endereço de rede que o endereço de destino contido no pacote. No caso do endereço de destino no pacote ser o endereço de <i>broadcast</i> da rede ou sub-rede, então o pacote é entregue a todos os interfaces nessa rede ou sub-rede.				

Verdadeiras:	A1	B2	C3			
Falsas:				D4		

8. Considere o protocolo ARP (*Address Resolution Protocol*) da pilha protocolar TCP/IP:

A1	É um protocolo que opera no nível de ligação de dados mas a informação contida numa tabela ARP num <i>router</i> diz respeito a endereços de todas as redes IPv4 a que está ligado.				
B2	Em redes IPv4, os <i>routers</i> e os <i>hosts</i> assumem papéis iguais neste protocolo, ainda que alguns <i>hosts</i> possam fornecer os endereços de rede de forma dinâmica.				
C3	Este protocolo permite que numa rede local IPv4 se descubra o endereço MAC de destino a partir do endereço IP de origem do pacote.				
D4	O método de transmissão por <i>broadcast</i> em IPv4 (i.e., envio para todos os interfaces/ <i>hosts</i> da rede ou sub-rede) é usado nos pedidos ARP.				

Verdadeiras:	A1	B2				
Falsas:			C3	D4		

9. Considere os equipamentos mais comuns de interligação no nível de ligação de dados:

A1	Se num comutador (<i>switch</i>) estão definidas múltiplas redes virtuais (VLANs) o tráfego é isolado entre VLANs, i.e., funcionalmente é equivalente a ter <i>routers</i> físicos distintos, um por cada VLAN.				
B2	Os comutadores (<i>switches</i>) aprendem quais os interfaces/ <i>hosts</i> que interligam analisando os endereços MAC de origem e de destino nas tramas recebidas em todas as suas portas (<i>links</i>).				
C3	É possível ligar vários comutadores (<i>switches</i>) e vários <i>hubs</i> em árvore para assim poder interligar duas ou mais redes IP distintas sem precisar de usar um encaminhador/ <i>router</i> IP.				
D4	Um comutador (<i>switch</i>) interliga várias portas (<i>links</i>) numa topologia em estrela que emula o comportamento duma topologia clássica com mecanismo de <i>token</i> partilhado.				

Verdadeiras:	A1					
Falsas:		B2	C3	D4		

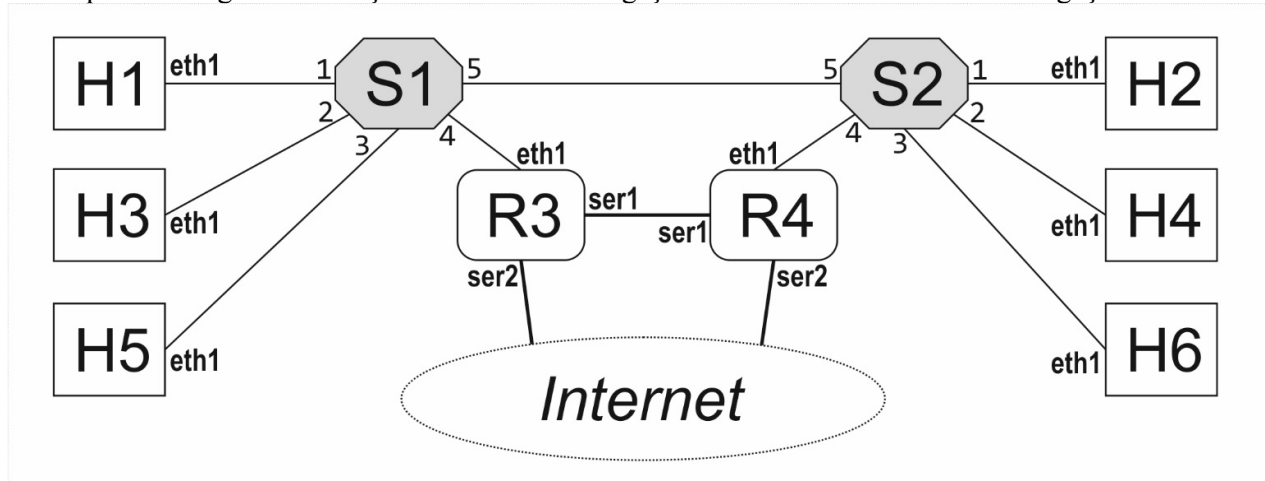
10. No contexto genérico das redes-sem-fios:

A1	Nas redes Wi-Fi (IEEE 802.11), o problema dos nós expostos ocorre porque um ou mais nós podem estar ao alcance de vários AP (<i>Access Point</i>) em simultâneo.				
B2	A adaptação do débito de informação entre dois nós específicos é feita dinamicamente tendo em consideração a proporção entre a potência do sinal e a potência do ruído.				
C3	Se dois APs (<i>Access Points</i>) estiverem ao alcance livre (sem obstáculos) um do outro existe sempre interferência mútua, mesmo que operem em canais diferentes.				
D4	A mobilidade nas redes celulares de dados pode ser suportada por encaminhamento indireto através de um <i>home agent</i> mas este modo é pouco escalável para esse <i>home agent</i> .				

Verdadeiras:		B2		D4		
Falsas:	A1		C3			

GRUPO II (15%+15%+10%+10%, 60 minutos)

Tenha em consideração a figura 1 que ilustra o equipamento duma instituição Y que é necessário interligar através de IPv4 à Internet. A instituição possui dos departamentos diferentes, A e B. Os equipamentos referidos como **H1**, **H2** e **H3** são *hosts* no departamento A e os equipamentos referidos como **H4**, **H5** e **H6** são *hosts* do departamento B. Os *switches* **S1** e **S2** implementam duas redes virtuais de nível dois, uma para cada departamento. Os *routers* **R3** e **R4** servem para interligar as duas sub-redes dos departamentos e também para interligar a instituição Y à Internet. A ligação série entre os *routers* é uma ligação dedicada.



1. Tendo em consideração que a instituição Y tem apenas disponível uma rede classe B para o endereçamento de todos os equipamentos, defina um esquema de endereçamento que maximize, no futuro, o número possível de *hosts* em cada sub-rede departamental (escolha um endereço IPv4 classe B a seu gosto):

End. Rede:	128.1.0.0	Máscara Subnetting:		255.255.224.0 ou /19
Host/Router	End. Sub-rede	Endereço Interface		Endereço Completo (formato CIDR)
H1	001	eth1	00000000000001	128.1.32.1/19
H2	001	eth1	00000000000010	128.1.32.2/19
H3	001	eth1	00000000000011	128.1.32.3/19
H4	010	eth1	00000000000001	128.1.64.1/19
H5	010	eth1	00000000000010	128.1.64.2/19
H6	010	eth1	00000000000011	128.1.64.3/19
R3	001	eth1	11111111111110	128.1.63.254/19
R3	100	ser1	00000000000001	128.1.128.1/19
R4	010	eth1	11111111111110	128.1.95.254/19
R4	100	ser1	00000000000010	128.1.128.2/19

2. Sabendo que os dois departamentos têm que ter interligação entre si e à Internet, complete as tabelas de encaminhamento manual/estático IPv4 para **H1**, **R3** e **R4** (a ordem das entradas numa tabela é irrelevante; escreva os endereços no formato CIDR):

Tabela de encaminhamento de R3

Rede/Sub-rede Destino	Próximo Hop	Interface de saída
0.0.0.0	128.20.0.6/30	ser2
128.20.0.4/30	128.20.0.5/30	ser2
128.1.32.0/19	128.1.63.254/19	eth1
128.1.128.0/19	128.1.128.1/19	ser1
128.1.64.0/19	128.1.128.2/19	ser1

Número:		Nome:	
---------	--	-------	--

Tabela de encaminhamento de R4

Rede/Sub-rede Destino	Próximo Hop	Interface de saída
0.0.0.0	128.20.0.6/30	ser2
128.20.0.4/30	128.20.0.4/30	ser2
128.1.64.0/19	128.1.95.254/19	eth1
128.1.128.0/19	128.1.128.2/19	ser1
128.1.32.0/19	128.1.128.1/19	ser1

Tabela de encaminhamento de H1

Rede/Sub-rede Destino	Próximo Hop	Interface de saída
128.1.32.0/19	128.1.32.1/19	eth1
0.0.0.0	128.1.63.254/19	eth1

3. Suponha que **S1** e **S2** são reinicializados (tabelas de comutação ficam vazias) e em seguida o host **H6** envia um pacote IPv4 para o host **H1** que responde de imediato com um pacote IP para **H6**. Complete a tabela seguinte com os eventos que acontecem em **S1** e **S2** (as entradas devem estar por ordem temporal). Considere que os eventos possíveis são: receber trama na porta X (**Rec**), gravar informação na tabela de comutação (**Save**) ou enviar trama nas portas X, Y, etc. (**Send**). Parta do princípio que o endereço MAC de **H1** é "**H1:eth1**", o de **H6** é "**H6:eth1**" e assim por diante.

Comutador	Evento	Porta Entrada	Portas Saída	MAC Origem
S2	Rec	3	-	H6:eth1
S2	Save	3	-	H6:eth1
S2	Send	-	2,4,5	H6:eth1
S1	Rec	4	-	R3:eth1
S1	Save	4	-	R3:eth1
S1	Send	-	1,2,5	R3:eth1
S1	Rec	1	-	H1:eth1
S1	Save	1	-	H1:eth1
S1	Send	-	4	H1:eth1
S2	Rec	4	-	R4:eth1
S2	Save	4	-	R4:eth1
S2	Send	-	3	R4:eth1

4. Sabendo que o MTU (*Maximum Transmission Unit*) da rede entre **R3** e **R4** é de 1210 bytes, **R3** tem que fragmentar um pacote IPv4 que recebeu de **H1**, com um total de 2392 bytes, por forma a enviar os fragmentos para **H6**, via **R4**. Sabendo que pacote IPv4 original recebido de **H1** tem o seguinte cabeçalho (o símbolo "?" indica que o valor destes campos é irrelevante) preencha os campos incompletos:

Ver = 4	HL = [5]	Type of Service = ?	Total Length = 2392	
Identification = [12345]		Flags=[?00]	Fragment Offset = [0]	
Time To Live = 10		Protocol = ?	Header Checksum = ?	
Source IP Address = [128.1.32.1]				
Destination IP Address = [128.1.64.3]				

Preencha também os campos incompletos dos cabeçalhos necessários dos pacotes IP que sejam resultantes do processo de fragmentação do pacote original e que serão enviados a **R4**:

Ver = 4	HL = [5]	Type of Service = ?	Total Length = [1204]	
Identification = [12345]			Flags=[?01]	Fragment Offset = [0]
Time To Live = [9]		Protocol = ?	Header Checksum = ?	
Source IP Address = [128.1.32.1]				
Destination IP Address = [128.1.64.3]				

Ver = 4	HL = [5]	Type of Service = ?	Total Length = [1204]	
Identification = [12345]		Flags=[?01]	Fragment Offset = [148]	
Time To Live = [9]		Protocol = ?	Header Checksum = ?	
Source IP Address = [128.1.32.1]				
Destination IP Address = [128.1.64.3]				

Ver = 4	HL = [5]	Type of Service = ?	Total Length = [24]	
Identification = [12345]			Flags=[?00]	Fragment Offset = [296]
Time To Live = [9]		Protocol = ?	Header Checksum = ?	
Source IP Address = [128.1.32.1]				
Destination IP Address = [128.1.64.3]				

Campo **Flags** do cabeçalho do pacote IPv4 (3 bits):

- Primeiro bit é reservado (valor irrelevante);
- Segundo bit é o DF (*Don't Fragment*) bit e se for 1 indica que o pacote não pode ser fragmentado;
- Terceiro bit é o MF (*More Fragment*) bit e se for 1 indica que o fragmento não é o último.

Campo **Fragment Offset** é de 13 bits e indica o *offset*, em palavras de 8 bytes, do fragmento em relação aos dados do pacote original.

4 bits		4 bits		8 bits		16 bits	
Version	HL	Type of Service			Total Length		
Identification					Flags	Fragment Offset	
Time To Live		Protocol			Header Checksum		
Source IP Address							
Destination IP Address							
Options + Padding (if any)							
DATA							
...							

Formato do pacote IPv4

Octets: 2	2	6	6	6	2	6	2	4	0-7951	4
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

Formato da trama MAC IEEE 802.11