Mestrado Integrado em Engenharia Informática

Redes de Computadores

Ano Letivo 2019/2020 • Exame de Recurso • 31 Janeiro 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 duma 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	Os endereços MAC deste nível protocolar são de maior comprimento (ocupam mais espaço em bits) do que os endereços de rede IPv4.
B2	As metodologias de partilha do meio de transmissão com deteção de portadora (CSMA – *Carrier-Sense Multiple Access*) 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 tecnologias físicas de interligação.
D4	Os PDUs a este nível protocolar costumam designar-se de tramas ou *frames*.

Verdadeiras:	A1	B2	C3	D4		
Falsas:						

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, só pode enviar uma trama de dados depois de esperar, no mínimo, um pequeno período de tempo denominado de SIFS (*Short Inter-Frame Sequence*).
B2	O controlo de acesso ao meio é baseado na combinação do mecanismo de deteção de portadora (CSMA – *Carrier-Sense Multiple Access*) com o mecanismo que não deteta as colisões mas que as tenta evitar (CA – *Collision Avoidance*).
C3	A variante 802.11b permite um alcance máximo e um débito de informação máximo que são superiores aos conseguidos com a variante 802.11a.
D4	Todas as tramas contêm quatro endereços MAC, cada um ocupando seis bytes, mas, no modo *ad-hoc*, apenas o valor dos primeiros três são relevantes.

Verdadeiras:		B2		D4		
Falsas:	A1		C3			

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

A1	Um interface de rede que está a enviar dados, assim que deteta uma colisão, cancela o envio do resto da trama de dados.
B2	Tal como os 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 (nível dois da pilha OSI) porque as colisões são detetadas.
D4	É possível dois interfaces comunicarem entre si a débitos de informação diferentes. Por exemplo, é possível um interface enviar dados a 1Gbps para um recetor que apenas suporta débitos de 10Mpbs.

Verdadeiras:	A1					
Falsas:		B2	C3	D4		

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

A1	Não é obrigatória a implementação de mecanismos de controlo de fluxo e de erros na troca de pacotes de dados.
B2	A troca de dados é possível entre interfaces na mesma rede física bem como entre interfaces em redes físicas distintas desde que utilizem a mesma tecnologia de nível de ligação.
C3	São necessários vários comutadores (*switches*) para interligar duas ou mais sub-redes IPv4.
D4	São necessários encaminhadores (*routers*) para interligar duas ou mais redes IPv6.

Verdadeiras:	A1			D4		
Falsas:		B2	C3			

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

A1	O protocolo IPv4 obriga ao estabelecimento de uma conexão entre o interface de origem e o interface de destino antes que sejam enviados datagramas, ainda que seja um protocolo não fiável.
B2	O protocolo *Internet Control Message Protocol* (ICMP) opera no nível protocolar de rede ainda que as mensagens ICMP sejam encapsuladas em pacotes IP.
C3	Um endereço IPv6 tem um espaço de endereçamento aproximadamente 2^{32} maior do que o espaço de endereçamento do IPv4.
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 rede por onde o pacote passar tendo em consideração o conjunto de endereços de rede ou sub-rede de destino.

Verdadeiras:		B2		D4		
Falsas:	A1		C3			

6. Numa rede local IPv4:

A1	Um equipamento com um único interface físico de rede é sempre considerado um sistema final ou *host*.
B2	O sub-endereçamento IPv4 aumenta o espaço de endereçamento, i.e., incrementa o número total de interfaces que é possível endereçar numa rede.
C3	A notação CIDR (*Classless Inter-Domain Routing*) tanto pode ser utilizada para agregar redes e sub-redes (*supernetting*) como para representar endereços completos de interfaces/*hosts* incluindo logo a informação da máscara de rede/sub-rede.
D4	Todas as classes de endereços IPv4 permitem endereçar o mesmo número máximo de interfaces ainda que o número máximo de redes endereçáveis seja diferente.

Verdadeiras:			C3			
Falsas:	A1	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 *Fragment Offset*=0.
B2	Um pacote IPv4, depois de ser fragmentado, só deve ser reconstruído no sistema final (ou *host*) de destino, ainda que fosse tecnicamente possível o pacote ser reconstruído num encaminhador (*router*) intermédio sem que o sistema final se aperceba.
C3	O processo de fragmentação dum pacote IPv4 garante que todos os fragmentos desse pacote tenham o mesmo tamanho.
D4	O processo de fragmentação torna a transmissão de dados através do protocolo IPv4 mais rápida e mais compatível com vários tipos de tecnologias de nível de ligação com diferentes MTUs.

Verdadeiras:	A1	B2				
Falsas:			C3	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 pelo que a informação contida numa tabela ARP num determinado encaminhador (*router*) só diz respeito a endereços IP numa só rede IPv4.
B2	Em redes IPv4, os encaminhadores (*routers*) e os *hosts* assumem papéis diferentes neste protocolo, uma vez que são os encaminhadores a 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 *unicast* (i.e., envio para apenas um interface/*host*) é usado nas respostas aos pedidos ARP.

Verdadeiras:				D4		
Falsas:	A1	B2	C3			

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

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

Verdadeiras:	A1			D4		
Falsas:		B2	C3			

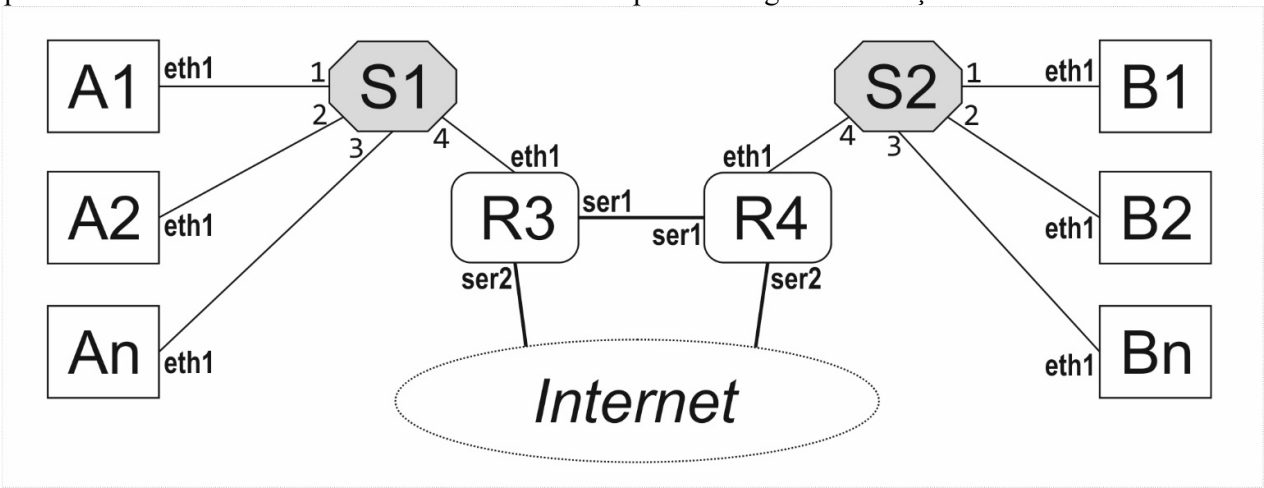
10. No contexto genérico das redes-sem-fios:

A1	Nas redes Wi-Fi (IEEE 802.11), o problema dos nós expostos ocorre porque um ou mais nós podem estar ocultos por algum obstáculo e não pela atenuação do sinal do meio de transmissão.
B2	Quando nas redes Wi-Fi (IEEE 802.11) são usadas tramas RTS (*Request to Send*) e CTS (*Clear to Send*), o débito máximo de informação diminui substancialmente, ainda que diminuam eventuais colisões.
C3	Se dois APs (*Access Points*) estiverem a operar em canais diferentes então não interferem um com o outro, mesmo que estejam ao alcance um do outro.
D4	A mobilidade nas redes celulares de dados pode ser suportada por encaminhamento indireto através de um *home agent* mas este modo é pouco escalável (computacionalmente pesado) para esse *home agent*.

Verdadeiras:		B2	C3	D4		
Falsas:	A1					

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 **An** são *hosts* do departamento A e os equipamentos referidos como **Bn** são *hosts* do departamento B. Os equipamentos referidos como **S1** e **S2** são comutadores (*switches ethernet*) e os referidos por **R3** e **R4** são encaminhadores (*routers*) IPv4. Os routers **R3** e **R4** servem para interligar os departamentos através duma linha dedicada e também para interligar a instituição Y à Internet.



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 o valor de **n**, i.e., que permita o maior número possível de *hosts* em cada sub-rede departamental (escolha um endereço IPv4 classe B a seu gosto):

End. Rede:	128.1.0.0	**Valor de n:**	**1 ≤ n ≤ 8189**
Máscara *Subnetting* (em binário):	255.255.224.0 *ou* /19		

Host/Router	**End. Sub-rede**	**Endereço Interface**		**Endereço Completo (formato CIDR)**
A1	001	eth1	0000000000001	128.1.32.1/19
An	001	eth1	n	$128.1.32+(n*2^{-8}).n-(n*2^{-8})*2^{8}$ /19
B1	010	eth1	0000000000001	128.1.64.1/19
Bn	010	eth1	n	$128.1.64+(n*2^{-8}).n-(n*2^{-8})*2^{8}$ /19
R3	001	eth1	1111111111110	128.1.63.254/19
R3	100	ser1	0000000000001	128.1.128.1/19
R4	010	eth1	1111111111110	128.1.95.254/19
R4	100	ser1	0000000000010	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 **B1**, **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 B1

Rede/Sub-rede Destino	Próximo *Hop*	Interface de saída
128.1.64.0/19	128.1.64.1/19	eth1
0.0.0.0	128.1.95.254/19	eth1

3. Suponha que **S1** e **S2** são reinicializados (tabelas de comutação ficam vazias) e em seguida o host **B1** envia um pacote IPv4 para o host **A1** que responde de imediato com um pacote IP para **B1**. 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 **A1** é "**A1:eth1"**, o de **B1** é "**B1:eth1"** e assim por diante.

Comutador	Evento	Porta Entrada	Portas Saída	MAC Origem
S2	Rec	1	-	B1:eth1
S2	Save	1	-	B1:eth1
S2	Send	-	2,3,4	B1:eth1
S1	Rec	4	-	R3:eth1
S1	Save	4	-	R3:eth1
S1	Send	-	1,2,3	R3:eth1
S1	Rec	1	-	A1:eth1
S1	Save	1	-	A1:eth1
S1	Send	-	4	A1:eth1
S2	Rec	4	-	R4:eth1
S2	Save	4	-	R4:eth1
S2	Send	-	1	R4:eth1

4. Sabendo que o MTU (*Maximum Transmission Unit*) da rede implementada sobre S2 é de 1520 bytes, **R3** tem que fragmentar um pacote IPv4 que recebeu de **A1**, com um total de 1586 bytes, por forma a enviar os fragmentos para **B1**. O pacote IPv4 original recebido de **A1** tem o seguinte cabeçalho (o símbolo "**?**" indica que o valor destes campos é irrelevante nesse pacote):

Ver = 4	HL = 5	Type of Service = ?	Total Length = 1586	
Identification = 33333			Flags=?00	Fragment Offset = 0
Time To Live = 10		Protocol = ?	Header Checksum = ?	
Source IP Address = ?				
Destination IP Address = ?				

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

Ver = 4	HL = [5]	Type of Service = ?	Total Length = [1516]		
Identification = [33333]			Flags=[X01]	Fragment Offset = [0]	
Time To Live = [9]		Protocol = ?	Header Checksum = ?		
Source IP Address = ?					
Destination IP Address = ?					

Ver = 4	HL = [5]	Type of Service = ?	Total Length = [90]		
Identification = [33333]			Flags=[X00]	Fragment Offset = [187]	
Time To Live = [9]		Protocol = ?	Header Checksum = ?		
Source IP Address = ?					
Destination IP Address = ?					

Ver = 4	HL = [ ]	Type of Service = ?	Total Length = [ ]		
Identification = [ ]			Flags=[X0]	Fragment Offset = [ ]	
Time To Live = [ ]		Protocol = ?	Header Checksum = ?		
Source IP Address = ?					
Destination IP Address = ?					

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