Mestrado Integrado em Engenharia Informática

Redes de Computadores

Ano Letivo 2019/2020 • Teste Escrito • 13 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 PDUs a este nível protocolar costumam designar-se de tramas.
B2	As metodologias de partilha do meio de transmissão com deteção de portadora (CSMA – *Carrier-Sense Multiple Access*) só são utilizadas em redes-sem-fios.
C3	Neste nível protocolar tanto podemos ter tecnologias de partilha do meio de transmissão como tecnologias de ligações dedicadas.
D4	A associação entre endereços MAC deste nível protocolar e os endereços de rede IPv4 é feita por tabelas de associação, não existindo uma relação lógica/semântica entre os dois tipos de endereços.

Verdadeiras:	A1		C3	D4		
Falsas:		B2				

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

A1	O controlo de acesso ao meio é baseado na combinação do mecanismo de deteção de portadora (CSMA – *Carrier-Sense Multiple Access*) com o mecanismo de deteção de colisões (CD – *Collision Detection*).
B2	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 DIFS (*Distributed Coordination Function Inter-Frame Sequence*).
C3	No modo intra-estrutura são necessários pontos de acesso (APs – *Access Points*) que servem de elementos coordenadores da comunicação entre estações (STA) e como ponto de interligação para o resto da rede local cablada (para eventual acesso a redes externas e resto da Internet).
D4	Independente do modo, todas as tramas de dados utilizam efetivamente (i.e., o seu valor é relevante) os quatro endereços MAC, cada um ocupando seis bytes.

Verdadeiras:		B2	C3			
Falsas:	A1			D4		

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

A1	O paradigma de controlo de acesso e de utilização do meio não permite comunicações fiáveis ao nível de ligação de dados (nível dois da pilha OSI) porque as colisões não são evitadas.
B2	O tamanho do campo de dados em todas as tramas Ethernet é fixo e mais pequeno que o tamanho máximo do campo de dados dos pacotes IPv4.
C3	Um interface de rede pronta a enviar dados, assim que deteta o meio sem comunicações ativas inicia o envio duma trama de dados e só termina a transmissão depois do envio da trama completa.
D4	A atenuação do sinal é muito inferior do que em tecnologias de meio de transmissão sem fios Wi-Fi (IEEE 802.11), sendo por isso possível utilizar mecanismos de deteção de colisões.

Verdadeiras:	A1			D4		
Falsas:		B2	C3			

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

A1	É obrigatória a implementação de mecanismos de controlo de fluxo e de erros na troca de PDUs (*Protocol Data Units*).
B2	O uso do mecanismo de deteção de erros denominado de CRC (*Cyclic Redundancy Check*) é baseado no uso de polinómios geradores cíclicos normalizados.
C3	São necessários encaminhadores (*routers*) para interligar duas ou mais redes IPv4.
D4	São utilizados comutadores (*switches*) para interligar duas ou mais sub-redes IPv4.

Verdadeiras:		B2	C3			
Falsas:	A1			D4		

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

A1	Podemos ter duas versões do protocolo IP a funcionar (Pv4 e IPv6) e que, sendo diretamente compatíveis entre si (i.e. a origem e o destino dum pacote IP podem ser interfaces/*hosts* com versões diferentes do IP), utilizam pacotes com formatos diferentes.
B2	Os endereços de rede IPv4 podem ter tamanhos diferentes, dependendo da classe de endereço.
C3	O protocolo IP oferece um serviço de entrega de pacotes não fiável e não orientado à conexão.
D4	A processo de encaminhamento em redes locais IP pode utilizar tanto estratégias de encaminhamento estático como de encaminhamento dinâmico.

Verdadeiras:			C3	D4		
Falsas:	A1	B2				

6. Numa rede local IPv4:

A1	Em redes classe A, B ou C, a capacidade de endereçamento de sub-redes e a capacidade de endereçamento de interfaces/*hosts* dentro de cada sub-rede é sempre limitada e interdependente entre si.
B2	Um equipamento com um único interface físico de rede nunca pode ser considerado um encaminhador/*router*.
C3	Um equipamento com mais do que um interface físico de rede é sempre considerado um encaminhador/*router*.
D4	A notação CIDR (*Classless Inter-Domain Routing*) tanto pode ser utilizada para representar grupos de redes (*supernetting*) como para representar endereços de interfaces/*hosts* incluindo logo a informação da máscara de rede/sub-rede.

Verdadeiras:	A1			D4		
Falsas:		B2	C3			

Número:		Nome:	

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

A1	Os interfaces de origem e de destino dum pacote podem residir em redes IPv4 de classes diferentes e não precisam de estar na mesma rede local ou as redes serem suportadas sobre a mesma tecnologia de nível de ligação de dados ou de nível físico.
B2	Um pacote IPv4, depois de ser fragmentado, só é reconstruído no pacote de tamanho original no último encaminhador/*router* da rede local do interface/*host* destino.
C3	O processo de fragmentação dum pacote IPv4 não garante, nem é preciso, que os fragmentos desse pacote cheguem ordenados ao *host* destino.
D4	O processo de fragmentação não é recomendado no protocolo IPv6 e nem é possível utilizando somente o cabeçalho inicial do pacote IPv6.

Verdadeiras:	A1		C3	D4		
Falsas:		B2				

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 (nível dois da pilha OSI) e que serve para um *host* saber qual o endereço MAC correspondente ao endereço IP do interface/*host* da rede/sub-rede local para o qual quer enviar o pacote de dados.
B2	Todos os *hosts* duma rede/sub-rede local IP assumem o mesmo papel neste protocolo, não existindo um servidor ARP para fazer a gestão centralizada da associação entre endereços IP e endereços MAC.
C3	As entradas da tabela ARP num *host* têm uma validade limitada no tempo, ou seja, a informação mantida nestes tabelas é dinâmica e automaticamente atualizada (sem intervenção humana).
D4	O método de transmissão por *broacast* (i.e., envio para todos os interfaces/*hosts* que partilham o meio físico) é usado nos pedidos ARP.

Verdadeiras:	A1	B2	C3	D4		
Falsas:						

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

A1	Os comutadores (*switches*) aprendem quais os interfaces/*hosts* que interligam analisando os endereços MAC das tramas recebidas em todas as suas portas (*links*) mas não sabem exatamente a que portas específicas cada um dos interfaces/hosts estão ligados.
B2	Não é possível ligar um comutador (*switch*) a um *hub* ou vice-versa.
C3	Num comutador (*switch*) é possível interligar várias portas (*links*) numa topologia em estrela e garantir que na comunicação entre *hosts* ligados diretamente a essas portas não existem colisões.
D4	É possível ligar vários comutadores (*switches*) em árvore para assim poder interligar duas ou mais redes IP distintas sem precisar de usar um encaminhador/*router* IP.

Verdadeiras:			C3			
Falsas:	A1	B2		D4		

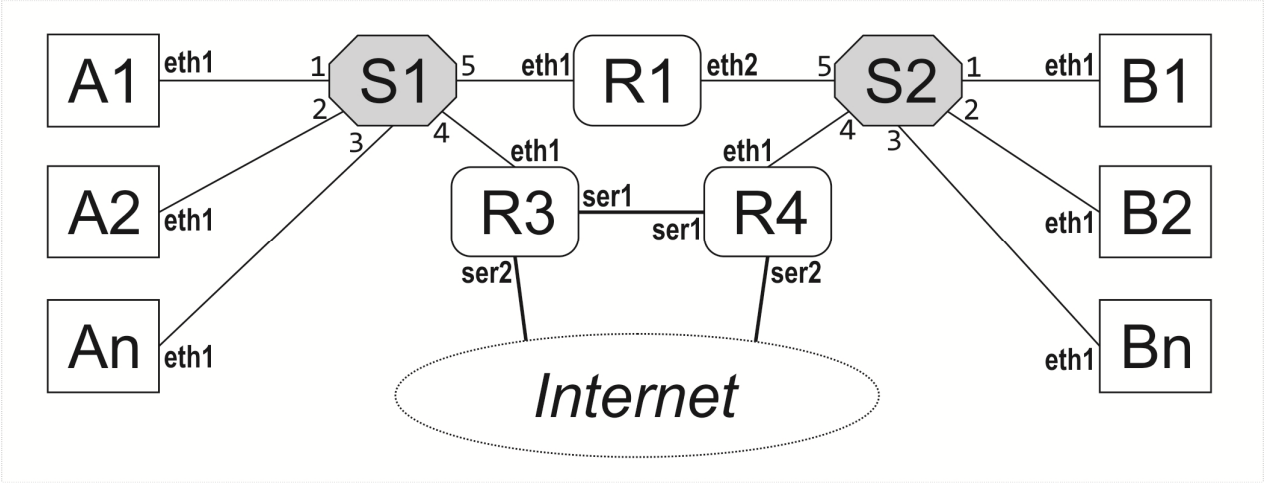
10. No contexto genérico das redes-sem-fios:

A1	Quando nas redes Wi-Fi (IEEE 802.11) são usadas tramas RTS (*Request to Send*) e CTS (*Clear to Send*), a probabilidade de haver colisões no meio de transmissão aumenta substancialmente.
B2	Nas redes Wi-Fi (IEEE 802.11), o problema dos nós escondidos ocorre porque um ou mais nós podem estar ocultos por algum obstáculo e não pela atenuação do sinal do meio de transmissão.
C3	Nas redes celulares de dados, a comunicação entre os utilizadores (nós/*nodes*) não é direta e precisa sempre duma ligação intermédia a uma célula duma estação base onde o meio de transmissão é partilhado por todos os utilizadores ligados a essa célula.
D4	A mobilidade nas redes celulares de dados pode ser suportada por encaminhamento direto através dos nós finais e é menos suscetível a problemas de escalabilidade do que encaminhamento indireto.

Verdadeiras:			C3	D4		
Falsas:	A1	B2				

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 **R1**, **R3** e **R4** são encaminhadores (*routers*) IPv4. O *router* **R1** serve para interligar as redes dos dois departamentos e 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 C 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 C a seu gosto diferente de 192.168.*.0):

End. Rede:	199.2.2.0/24	**Máscara *Subnetting*:**		255.255.255.224
Host/Router	**Endereço Sub-rede**	**Endereço Interface**		**Endereço Completo (formato CIDR)**
A1	001	eth1	00001	199.2.2.33/27
An	001	eth1	n	199.2.2.32+n/27, 0<n<30
B1	010	eth1	00001	199.2.2.65/27
Bn	010	eth1	n	199.2.2.64+n/27, 0<n<30
R1	001	eth1	11110	199.2.2.62/27
R1	010	eth2	11110	199.2.2.94/27
R3	001	eth1	11101	199.2.2.61/27
R3	011	ser1	00001	199.2.2.97/27
R4	010	eth1	11101	199.2.2.93/27
R4	011	ser1	00010	199.2.2.98/27

2. Sabendo que os dois departamentos têm que ter interligação entre si e à Internet, complete as tabelas de encaminhamento manual/estático IPv4 para **A1**, **R1** e **R4** (a ordem das entradas numa tabela é irrelevante; escreva os endereços no formato CIDR):

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	128.20.0.5/30	ser2
199.2.2.64/27	199.2.2.93/27	eth1
199.2.2.96/27	199.2.2.98/27	ser1
199.2.2.32/27	199.2.2.94/27	eth1

Número:		Nome:	

Tabela de encaminhamento de R1

Rede/Sub-rede Destino	Próximo *Hop*	Interface de saída
199.2.2.32/27	199.2.2.62/27	eth1
199.2.2.64/27	199.2.2.94/27	eth2
0.0.0.0	199.2.2.61/27	eth1

Tabela de encaminhamento de A1

Rede/Sub-rede Destino	Próximo *Hop*	Interface de saída
199.2.2.32/27	199.2.2.33/27	eth1
199.2.2.64/27	199.2.2.62/27	eth1
0.0.0.0	199.2.2.61/27	eth1

3. Suponha que **S1** e **S2** são reinicializados (tabelas de comutação ficam vazias) e em seguida o host **A1** envia um pacote IPv4 para o host **B1** que responde de imediato com um pacote IP para **A1**. 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 os de **R1** são "**R1:eth1"** e "**R1:eth2"**.

Comutador	Evento	Porta Entrada	Portas Saída	MAC Origem
S1	Rec	1	-	A1:eth1
S1	Save	1	-	A1:eth1
S1	Send	-	2,3,4,5	A1:eth1
S2	Rec	5	-	R1:eth2
S2	Save	5	-	R1:eth2
S2	Send	-	1,2,3,4	R1:eth2
S2	Rec	1	-	B1:eth1
S2	Save	1	-	B1:eth1
S2	Send	-	5	B1:eth1
S1	Rec	5	-	R1:eth1
S1	Save	5	-	R1:eth1
S1	Send	-	1	R1:eth1

4. Sabendo que o MTU (*Maximum Transmission Unit*) da rede dedicada entre **R3** e **R4** é de 420 bytes, **R3** tem que fragmentar um pacote IPv4 que recebeu de **A1**, com um total de 900 bytes, por forma a enviar os fragmentos para **R4**. O pacote IPv4 original recebido de **A1** tem o seguinte cabeçalho (o símbolo "**?**" indica que o valor destes campos é irrelevante neste exercício):

Ver = 4	IHL = 5	Type of Service = ?	Total Length = 900	
Identification = 33333			Flags=000	Fragment Offset = 0
Time To Live = 5		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 = [420]
Identification = [33333]		Flags=[X11]	Fragment Offset = [0]
Time To Live = [4]		Protocol = ?	Header Checksum = ?
Source IP Address = ?			
Destination IP Address = ?			

Ver = 4	HL = [5]	Type of Service = ?	Total Length = [420]
Identification = [33333]		Flags=[X11]	Fragment Offset = [50]
Time To Live = [4]		Protocol = ?	Header Checksum = ?
Source IP Address = ?			
Destination IP Address = ?			

Ver = 4	HL = [5]	Type of Service = ?	Total Length = [100]
Identification = [33333]		Flags=[X10]	Fragment Offset = [100]
Time To Live = [4]		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 **Header Length** (HL) é de 4 bits e indica o número de palavras de 4 bytes que o cabeçalho ocupa.

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