AP CYBERSECURITY • EXERCISE SHEET

3.2 Protecting Networks: Managerial Controls and Wireless Security

Name: _____ Class: _____ Date: _____ **Total: 10 marks**

KEY WORDS wpa3 无线加密协议 • split tunneling 分离隧道 • switch 交换机

Objective

Build the skills to answer exam questions on network policies and wireless hardening with **WPA3** 无线加密协议.

You must be able to:

- give managerial controls: router, switch, VPN, and wireless security policies
- harden wireless: disable beacon frames, control signal, enable WPA3, MAC filtering
- explain why WEP and the original WPA are insecure

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Wireless hardening

Disable beacon frames so the network is harder to find, control signal strength so it does not leak outside, enable WPA3 (WEP and original WPA are broken), and use MAC filtering plus authentication.

■ Choosing encryption

WPA3 is today's strongest wireless encryption. WEP and the original WPA have known, unfixable weaknesses and must not be used for a secure network.

2 Practice

2.1 State the strongest current wireless encryption protocol. [1]

2.2 Give two ways to harden a wireless network. [2]

2.3 Explain why controlling a WAP's signal strength improves security. [2]

3 Exam-style questions

3.1 Which wireless encryption is insecure and should be avoided? [1]

- **A** WPA3
- **B** WEP
- **C** WPA3-Enterprise
- **D** AES-256

3.2 A VPN policy typically forbids [1]

- **A** strong encryption
- **B** split tunneling
- **C** MAC filtering
- **D** authentication

3.3 A company writes a wireless security policy.

(a) State one requirement the policy should include. [1]

(b) Explain how MAC filtering helps. [2]

Solutions

2.1 WPA3.

2.2 any two of: enable WPA3; disable beacon frames; control signal strength; MAC filtering.

2.3 it stops the signal leaking outside the building, so attackers outside cannot detect or probe it.

3.1 B. WEP is broken; WPA3 is the strong choice.

3.2 B. split tunneling can bypass the corporate VPN protections.

3.3 (a) e.g. require WPA3 / require authentication. (b) MAC filtering allows only known hardware addresses, so unknown devices cannot join the network.