AP CYBERSECURITY • EXERCISE SHEET

# 3.2 Protecting Networks: Managerial Controls and Wireless Security

Name: _____ Class: _____ Date: _____ **Total: 44 marks**

**KEY WORDS** beacon frames 信标帧 • wireless security 无线安全 • network security policies 网络安全策略 • switch 交换机 • mac addresses 物理地址

## Objective

Build the skills to answer exam questions on **network security policies** 网络安全策略 and configuring **wireless security** 无线安全 features.

**You must be able to:**

- state what a router, switch, VPN and wireless security policy each specify
- explain why disabling **beacon frames** 信标帧 makes a network harder to find
- explain how controlling signal direction and strength reduces exposure
- explain what strong wireless encryption protects, and what **MAC filtering** MAC 过滤 adds
- say why device and user **authentication** is the requirement none of the others replaces

## 1 Worked examples

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

### ■ The four network policies

Each sets a **minimum configuration standard** for a class of equipment - which is why they are managerial controls, not technical ones.

| Policy | Typical requirements |
|---|---|
| **Router security** | ban local user accounts (all logins through an approved authentication server); disable unnecessary services such as Telnet; require a firewall |
| **Switch security** | ban local user accounts; require **port security** enabled; use MAC filtering |
| **VPN** | minimum security requirements for employees reaching the internal network remotely |
| **Wireless security** | require users to authenticate through **EAP**; require **AES** encryption with a minimum key length; disable beacon frames |

Two threads run through all of them. **Banning local accounts** means no device carries its own separate password to be forgotten, shared or left at the default - authentication is centralised and revocable. **Disabling unnecessary services** removes ports an adversary could connect to, and Telnet is named because it transmits credentials unencrypted.

### ■ The four wireless configurations

| Configuration | What it does | What it does not do |
|---|---|---|
| **Disable beacon frame broadcasting** | the network no longer announces itself, so it is harder to find and to attack | a determined adversary can still detect it from other traffic |
| **Control broadcast direction and signal strength** | the signal does not extend beyond the physical space it serves | nothing, if the building is already the boundary |
| **Strong encryption (AES, minimum key length)** | intercepted wireless frames are not readable | does not stop a device joining |
| **MAC filtering, plus user authentication** | unauthorised devices cannot access the network | MAC addresses can be spoofed, so filtering alone is weak |

The ranking matters when a question asks which to do first. **Encryption and authentication are the load-bearing pair**; disabling beacons and shaping the signal make the network harder to find, which raises the effort required but protects nothing on its own. An answer that offers only "hide the SSID" has proposed obscurity rather than security.

*Example.* A café's guest network broadcasts to the street, uses an old encryption protocol, and filters by MAC. Reduce the signal so it covers the seating area only; move to AES with an adequate key length so intercepted frames are unreadable; and add user authentication, because MAC addresses can be copied from any frame the adversary captures.

## 2 Practice

**2.1** State **two** requirements a router security policy may include, and explain why each helps. [4]

**2.2** State **two** requirements a switch security policy may include. [2]

**2.3** Explain why banning local user accounts on routers and switches improves security. [2]

**2.4** Explain why a router security policy would require Telnet to be disabled. [2]

**2.5** State **three** requirements a wireless security policy may include. [3]

**2.6** Explain what disabling **beacon frame broadcasting** achieves, and one thing it does not achieve. [3]

**2.7** Explain how controlling the broadcast direction and signal strength of a wireless access point reduces risk. [2]

**2.8** Explain why **MAC filtering** alone is not sufficient to keep unauthorised devices off a wireless network. [2]



**2.9** State what strong wireless encryption protects against, and name the encryption a wireless policy would typically require. [2]

## 3 Exam-style questions

**3.1** A switch security policy would typically require [1]

- **A** disabling AES encryption
- **B** port security to be enabled
- **C** beacon frames to be broadcast
- **D** local user accounts on every switch

**3.2** Disabling beacon frames makes a wireless network [1]

- **A** impossible for an adversary to detect
- **B** harder for an adversary to find
- **C** encrypted without a key
- **D** immune to MAC spoofing

**3.3** MAC filtering is a weak control on its own because [1]

- **A** it slows the network noticeably
- **B** MAC addresses can be spoofed
- **C** it prevents authorised devices connecting
- **D** it requires beacon frames to be enabled

**3.4** A wireless security policy would typically require users to authenticate through [1]

- **A** Telnet
- **B** EAP
- **C** ARP
- **D** ICMP

**3.5** A secondary school's wireless network covers the whole site and reaches the pavement outside. It broadcasts its SSID, uses an encryption protocol chosen in 2011, and admits

any device whose MAC address is on a list the network manager maintains by hand. Router and switch logins each use a local account whose password is shared among three technicians, and Telnet is enabled on the routers "for convenience". A student is found to have been reading staff traffic from a bench outside the gates.

(a) Explain how the student was most likely able to read staff traffic, naming the **two** configuration weaknesses that allowed it. [4]

(b) Explain why the MAC address list did not stop the student. [2]

(c) Identify the weaknesses in the router and switch configuration and state which policy each would be covered by. [4]

(d) Explain the specific risk created by enabling Telnet and by sharing one local account. [4]

(e) Recommend the changes you would make, in priority order, and justify the order. [4]



## Solutions

**2.1** any two, each with a reason: **ban local user accounts** - all logins go through an approved authentication server, so access can be revoked centrally and no device carries its own forgotten or default password; **disable unnecessary services such as Telnet** - fewer open ports for an adversary to connect to; **require a firewall** - traffic in and out of the network is filtered against a rule set.

**2.2** any two of: ban local user accounts; require port security to be enabled; use MAC filtering.

**2.3** a local account exists only on that device, so its password is easily left at a default, shared between staff, or forgotten when someone leaves; routing every login through an approved authentication server means access is granted and revoked in one place and every login is attributable.

**2.4** Telnet is an unnecessary service on a secured router, and it transmits credentials and commands **unencrypted**, so anyone intercepting the traffic obtains the router's login.

**2.5** any three of: require users to authenticate through EAP; require all wireless traffic encrypted with AES at a minimum key length; disable beacon frames on wireless access points.

**2.6** the access point no longer announces the network's presence, so an adversary scanning for networks does not see it and it is harder to find and attack. It does not make the network undetectable - a determined adversary can still find it from other traffic, and it provides no protection at all once the network is found.

**2.7** the signal is confined to the physical space the access point is meant to serve, so an adversary standing outside that space cannot pick up the signals and beacon frames, and must gain physical access before they can attack the wireless network at all.

**2.8** MAC addresses can be **spoofed** - an adversary who captures any frame from the network can read an authorised MAC address and set their own device to use it, after which the filter admits them.

**2.9** it ensures wireless frames are not readable by an adversary who intercepts them; a policy would typically require **AES** with a minimum key length.

**3.1 B**. A policy bans local accounts rather than requiring them.

**3.2 B**. Harder to find, not impossible - and it is obscurity, not protection.

**3.3 B**.

**3.4 B**. EAP is the authentication protocol named; the others are unrelated.

**3.5** (a) the **signal extends beyond the school site** to the pavement, so the student could receive the traffic without entering the premises; and the **encryption protocol dates from 2011**, so it is weak enough to break, after which intercepted frames are readable.

(b) MAC addresses can be spoofed: the student could read an authorised MAC address from any captured frame and configure their own device to present it, after which the hand-maintained list admits them.

(c) **local accounts on routers and switches** - covered by the router and switch security policies, both of which ban them; **Telnet enabled** - covered by the router security policy's requirement to disable unnecessary services. Accept "no port security mentioned on switches" as a further weakness under the switch security policy.

(d) **Telnet** transmits credentials and commands unencrypted, so an adversary intercepting the traffic - which this student demonstrably can - obtains the router login directly. A **single shared local account** means no login is attributable to a person, so a misconfiguration or a compromise cannot be traced, and the password cannot be revoked for one technician without disrupting the other two, so it tends never to be changed at all.

(e) A defensible order with justification. Strongest: **1.** replace the 2011 encryption with AES at an adequate key length and require EAP authentication - this is the pair that actually protects the traffic and is what the breach exploited. **2.** disable Telnet and move router and switch logins to an authentication server - the shared account and cleartext protocol together put the whole network's configuration at risk. **3.** reduce the signal so it no longer reaches the pavement - a real reduction in exposure, but it only raises the effort. **4.** disable beacon frames - worth doing, and last, because it is obscurity rather than protection. The justification is the ranking itself: encryption and authentication protect the data, while hiding and shaping the signal only make the network harder to find.