

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	B
C	D

- 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	B
C	D

- 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	B
C	D

- 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	B
C	D

- 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]

