Solutions

Each answer shows the steps, then the **result**.

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