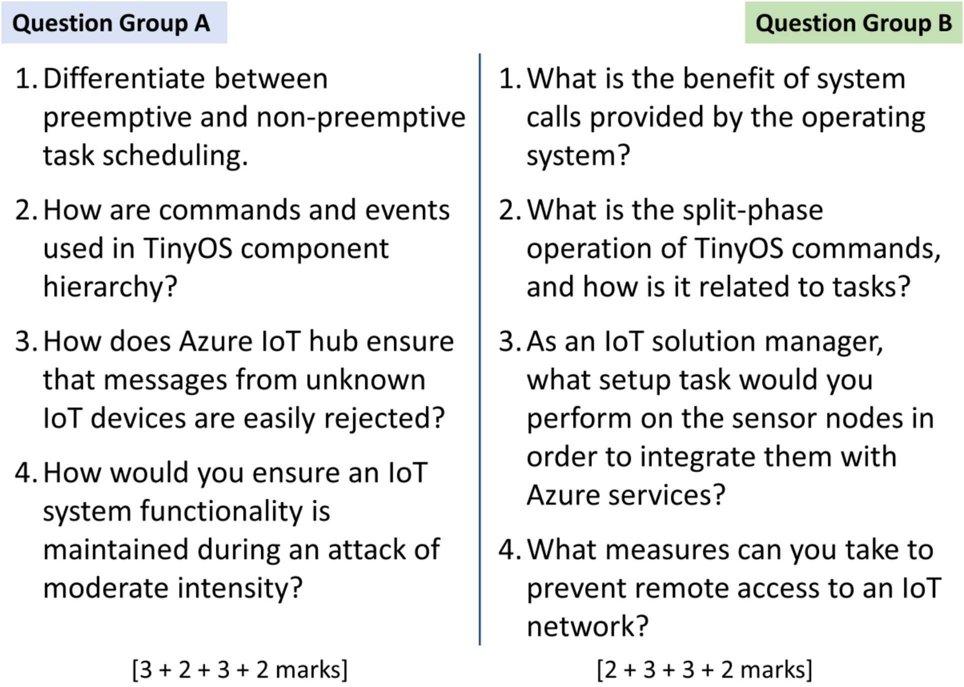

Question Group A

1. Differentiate between preemptive and non-preemptive task scheduling.
2. How are commands and events used in TinyOS component hierarchy?
3. How does Azure IoT hub ensure that messages from unknown IoT devices are easily rejected?
4. How would you ensure an IoT system functionality is maintained during an attack of moderate intensity?

[3 + 2 + 3 + 2 marks]

Question Group B

1. What is the benefit of system calls provided by the operating system?
2. What is the split-phase operation of TinyOS commands, and how is it related to tasks?
3. As an IoT solution manager, what setup task would you perform on the sensor nodes in order to integrate them with Azure services?
4. What measures can you take to prevent remote access to an IoT network?

[2 + 3 + 3 + 2 marks]

A

1

In non-preemptive scheduling, a task is executed to the end, it can't be interrupted by another task. Preemptive scheduler means a task of higher priority may interrupt a task of low priority.

2

higher-level components issue commands to lower-level components

lower-level components signal events to higher-level components

3

Firstly, all valid devices need to be provisioned. Then when a device connects to hub, it goes through the stages of authentication and attestation to prove its identity. If any of these steps fail, hub treats the device as unknown and rejects its data.

4

By keeping a redundant version of each critical component.

By allowing graceful degradation such that under an attack, system can continue to work with manual control instead of automatic operation.

B

1

Syscalls hide the complexity of hardware and provide a uniform method for user apps to perform hardware i/o.

2

When a command function call is made, the callee creates a task (that will be scheduled by OS sometime later) and returns immediately.

Later when the task is complete, the callee signals an event for the caller.

3

First, the nodes need to have Azure SDK installed. Secondly, they need to be configured with the correct authentication & attestation keys which were provided by Azure during device provisioning.

4

using unidirectional gateways, firewalls, dedicated authentication mechanisms, and multiple layers of protection.