COM00147M

Department of Computer Science

Computer and Mobile Networks

SUMMATIVE ASSESSMENT BRIEF



|  |  |
| --- | --- |
| **Author** | Duncan Greaves |
| **Assessment type** | Summative assignment |
| **Weighting** | 100% |
| **Release** | Week 3 |
| **Deadline** | Monday following Week 8, 13:00 (UK time) \* |

\* If this date falls on a UK public holiday or a University of York closure day, the submission date will change. Please check the submission point in the ‘Assignments’ area of the module in Canvas for the exact submission deadline.

# Module Learning Outcomes

The module learning outcomes (MLO’s) for this module are as follows:

**MLO 1.** Critically analyse the core concepts in modern computer networks such as LANs and WANs, network architecture, communication protocols and their design principles, the layered organisation of computer networks, and mobile networks.

**MLO 2.** Apply network concepts and design principles, design, communicate and implement a networked application.

**MLO 3.** Critically evaluate and apply tools for computer network performance analysis.

**MLO 4.** Critically evaluate network security techniques.

**MLO 5.** Critically evaluate the legal and ethical impact of computer networks and the internet.

This assessment addresses **all** the module learning outcomes listed above.

# Assessment Background/Scenario

## Background

You have been appointed as the Network Consultant for a fictional company called York-Environmental Water Treatment (YEWAT). The company is run separately from the local water supply company but maintains strong reporting links.

The company is tasked with managing the wastewater treatment for the catchment area on behalf of the local water utility. Water treatment removes contaminants and undesirable components or reduces their concentration so that the water becomes fit for its desired end use. This treatment is crucial to human health and allows people to benefit from both drinking and irrigation use.

Wastewater treatment offers returns through reuse. Treated water is analysed and, when treated, is returned to the local water distribution system for use in homes and businesses.

In times of heavy flooding, the company has a permit to discharge a certain amount of untreated wastewater into the local rivers as a last resort. If this happens, these must be reported to the regulatory authority.

The company uses technology to dynamically monitor inflows of wastewater, analyse treated water quality, and monitor the quality and volume of outflows of clean water to the water supply system using SCADA sensors. A SCADA system is a combination of hardware and software that enables industrial process automation by capturing Operational Technology (OT) real-time data. SCADA connects the sensors that monitor equipment like motors, pumps, and valves to an onsite or remote server.

The network infrastructure could be described as hybrid, with the laboratory and operations centre utilising existing wired networks onsite but trialling the use of IoT devices and drones to complement their data collection and analysis.

For the purposes of this assessment, you will be analysing the network requirements for the wastewater site. The site contains the following buildings and facilities:

* An Operational Control Room (HQ).
* A Water Quality Laboratory.
* The IT Department (Data Centre).
* Several water treatment ponds with wired TCP/IP SCADA sensors that can operate the gates and pumps, which are distributed across the whole area of the site.
* Remote wireless IoT devices and drones.

## Network Requirements

The network should give access to the correct department networks by job role. This includes access to their own departmental records and those that they interact with. You do not need to consider the low-level details of how wastewater treatment works, but you should design the network to meet the following business needs:

* The Operational Control Room staff monitor and control all inflows to, and outflows from, the water treatment works and are in control of the pumping and water treatment sensors. These include the SCADA sensors used to operate sluice gates and pumps, which are part of a permanent wired network.
  + HQ 🡨🡪 SCADA
* The Water Quality Laboratory staff are responsible for sampling and testing water quality. They generate data which is stored on a server in the IT Department building.
  + Lab 🡨🡪 IT Dept
* The IT Department (Data Centre) consists of work-stations and servers that store and analyse data collected from the treatment ponds and laboratories and provide services to all other buildings.
  + IT WSs 🡨🡪 IT Servers
* The company is trialling several IoT devices that monitor weather conditions and water levels across the wider area. Many are fixed but include some mobile drones. These devices connect to 4G networks and transmit their data to the cloud.
  + IoT devices 🡪 4G 🡪 IT Servers

Due to cost issues, the business stakeholders have chosen not to run physical cables between the buildings. However, the offices are spaced out so that any wireless communication from one building to another is subject to environmental factors such as rain and cold, resulting in a weak signal being emitted.

4G here as well then – Overcoming rain and cold with adaptive modulation and coding (AMC) techniques. Can’t really do much about the cold though. Higher transmission power can counteract the effects also.

The distribution of work-stations and departments are shown in Table 1, which describes the high-level network requirements for each department.

Table 1: Department and Sensor distribution and requirements.

|  |  |  |
| --- | --- | --- |
| **Physical Work-stations and Devices** | | |
| **Department** | **Work-stations** | **Network Requirements** |
| **Operational Control**  **Room** | 50 computers | These wired LAN networks are physically separate from each other and are located in the department buildings. Access to the relevant network and work-stations is restricted by user job role. |
| **Laboratories** | 25 computers |
| **IT Department**  **(Data Centre)** | 25 computers |
| **Treatment Pond Sensors**  **(On site, wired)** | 200 sensors /devices  (pumps and gates) | Sensors are wired to the IT Department Data Centre but are operated from the control room. |
| **IoT Devices (Remote, wireless)** | Variable number of devices | Data collection devices that store data to a cloud data centre. |

The servers are in the IT Department Data Centre on the main site (Table 2):

Table 2: Network Server Details.

|  |  |  |  |
| --- | --- | --- | --- |
| **Network Servers** | | | |
| **Server** | **Device type** | **Location** | **Purpose** |
| **Authorisation Server** | 1 server machine | Physical, on site  [Data Centre] | Centralised authorisation for users to log on to the internal company resources. |
| **Web Server**  **(Cloud-based)** | 1 server machine | Cloud-based | Server hosting the external company website and an analytics dashboard showing the output of all IoT and remote sensor devices. |
| **Email, DNS & file Server** | 3 server machines | Physical, on site  [Data Centre] | Accessible by all authorised company computers, providing shared services to users. |
| **Laboratory Server** | 1 server machine | Physical, on site  [Laboratory] | Hosts the programs and stores data needed and produced by the water quality laboratory. |
| **SCADA**  **Sensor Data Server** | 1 server machine | Physical, on site  [Operational Control Room] | Stores data from the onsite SCADA sensors and hosts applications that operate the pumps and gates. |
| **IoT Device Server** | 1 server machine | Cloud-based | Used to collect data from the IoT devices and hosts applications that can process and display visual data to the Operational Control Room. |

# Assessment Tasks

This assessment is broken down into three tasks to address the following stakeholder concerns:

**Concern 1:** Analyse the requirements given in the scenario and design the physical layout of the proposed system, IP address design and the network components to meet the requirements of the scenario.

**Concern 2:** The IT Director has highlighted the importance of connectivity between the site buildings and the importance of a strong signal between them. She also has concerns about the resilience and availability of remote devices and sensors.

**Concern 3:** The Chief Information Security Officer (CISO) is concerned about the impact and feasibility of the proposed transition from SCADA sensor technology to IP-based wireless cyber-physical devices that control the flow of water into and out of the treatment ponds.

# Deliverables

Your assignment should be laid out following the formatting guidelines that are specified in the ‘Submission Formatting’ page in Canvas. This includes restrictions on the length of the appendices, expectations on how your work should be presented and any penalties when these expectations are not met.

Your report should not exceed 3,000 words in total and consist of three clear sections – one for each task. Your response to one section/task will not contribute to grades in another. Further formatting details and essential points are given below.

## Task 1 – Network Design

Design a network diagram for the given scenario, including labelling the types of network components used:

* Include appropriate design in your network to ensure each department’s network will be logically separated from other departments. The diagram should include the locations of the network components, including routers, hubs, switches, wireless access points and any other devices suggested by the scenario.
* Produce a high-level IP address design for the company and identify any subnets used in the design.
* Name the major network protocols used in your design, including the routing and addressing protocols that should be in place, with examples.
* Justify your design and network component choices, explaining how these are used to fulfil the requirements.

## Task 2 – IT Director Concerns

To address the concerns of the IT Director, the following must be part of your submission:

* The problem of signal strength at the operations centre and between the different departments needs to be addressed. Analyse the potential devices and methods to boost this signal.
* The growth in IoT devices is likely to increase the amount of investment required in the network to cope with network traffic and data and highlights the need to build resilience into the system. Propose and justify any technical remedies or considerations to increase network resilience and availability.

## Task 3 – CISO Concerns

The CISO is concerned about the impact of new technology on corporate stewardship. Assess the options for the following actions:

* Analyse potential security, business, and environmental concerns surrounding the security applied to the IoT sensors and drone devices and their implications.
* Evaluate the legal and ethical impacts of a security breach on the SCADA based pump and gate control systems. Assess the potential information security impacts of the proposed transition from wired SCADA sensor technology to IP-based wireless cyber-physical devices.

## Referencing

You are required to use the [IEEE referencing style](https://subjectguides.york.ac.uk/referencing-style-guides/ieee) for citing books, articles, and all other sources (such as websites) used in your assignment.

Good referencing is essential in order to meet the standards of academic integrity set by the University. All your sources must be acknowledged, regardless of whether you’ve included direct quotes or not. Visit your **Academic Integrity Tutorial module** in Canvas for additional guidance on effective referencing.

# Marking Criteria

|  |  |  |  |
| --- | --- | --- | --- |
| **Learning Outcome** | **Section/ Task** | **Criteria** | **Available marks** |
|  | All | Written communication and referencing | **10** |
| **1, 2** | Task 1 | A description and network diagram, summarising the network design, network isolation and IP addressing needs.  Accommodates the plan for all the necessary devices.  Justification of architecture and design choices. | **40** |
| **1, 2, 3** | Task 1, 2 | Demonstrates effective assessment and judgement in selecting components and techniques to improve signal strength.  Evaluation of different technologies that can improve network capacity and resilience.  Demonstrates understanding of issues based on evaluating and comparing different network components supported by literature and relevant theories. | **25** |
| **4, 5** | Task 3 | Evaluates different physical and information security attacks common in IP devices with descriptions of how to prevent or mitigate such attacks. Assessing the legal and ethical implications of implementing the proposed design changes. | **25** |
|  |  | TOTAL: | **100** |

# 

# Marking Criteria: Grade breakdown

## **Written Communication and Referencing: 10%**

| **Mark band** | **Grade** | **Criteria** |
| --- | --- | --- |
| 0-39% | Fail | The report is not organised and is difficult to follow. Chaotic writing style. No use of structured headings. Little or no attention given to spelling and grammar. No use of references or any knowledge of their application. |
| 40-49% | Marginal fail | The report is poorly organised and difficult to follow. No consistent writing style. Little or no use of structured headings. Poor attention to spelling and grammar. Poor quality of references and knowledge of their application. |
| 50-59% | Pass | The report has a good structure and is well presented, with appropriate referencing and citation details. Competent spelling and grammar but some inconsistencies with respect to paraphrasing and quality of references. |
| 60-69% | Merit | The report has a very good structure and is well presented, with appropriate referencing and citation details. Competent spelling and grammar. |
| 70-100% | Distinction | The report has an excellent structure and is well presented, with appropriate referencing and citation details. Excellent spelling and grammar. All references and citations add to the argument style. |

## **Network Design and Analysis: 40%**

| **Mark band** | **Grade** | **Criteria** |
| --- | --- | --- |
| 0-39% | Fail | The learner has provided little to no recommendation and explanation of a network and addressing scheme that fails to address any of the scenario requirements. |
| 40-49% | Marginal fail | The learner has provided a basic recommendation and explanation of a network and addressing scheme that fails to address many of the scenario requirements. |
| 50-59% | Pass | The learner has provided a good recommendation and explanation of a network and addressing scheme that accounts for many of the scenario requirements. |
| 60-69% | Merit | The learner has provided a very good recommendation and explanation of a network and addressing scheme that accounts for most of the scenario requirements. |
| 70-100% | Distinction | The learner has provided an excellent recommendation and explanation of a network and addressing scheme that fulfils all the requirements of the scenario. |

## **Addressing the IT Director’s Concerns: 25%**

| **Mark band** | **Grade** | **Criteria** |
| --- | --- | --- |
| 0-39% | Fail | Little to no evaluation of different technologies and/ protocols and a failure to fulfil any of the signal strength and scalability requirements. |
| 40-49% | Marginal fail | Limited evaluation of different technologies and/ protocols and a failure to fulfil many of the signal strength and scalability requirements. |
| 50-59% | Pass | Good evaluation of different technologies and/or protocols that support fulfilment of many of the signal strength and scalability requirements. |
| 60-69% | Merit | Very good evaluation of different technologies and/or protocols that fulfil most of the signal strength and scalability requirements. |
| 70-100% | Distinction | Excellent evaluation of different technologies and/or protocols that support fulfilment of all the signal strength and scalability requirements. |

## **Addressing the CISO Concerns: 25%**

| **Mark band** | **Grade** | **Criteria** |
| --- | --- | --- |
| 0-39% | Fail | Little to no evaluation of physical and infosec threats and a poorly analysed and proposed range of mitigations considered. |
| 40-49% | Marginal fail | A limited evaluation of physical and infosec threats and a poorly analysed and proposed range of mitigations considered. |
| 50-59% | Pass | A good evaluation of physical and infosec threats and an adequate range of mitigations considered. |
| 60-69% | Merit | A very good evaluation of physical and infosec threats and a thorough range of mitigations considered. |
| 70-100% | Distinction | An excellent evaluation of physical and infosec threats and a very thorough range of mitigations considered. |

# Assessment Submission

You will submit your assessment in the ‘Assignments’ area of the module in Canvas. Please check your Canvas module for the specific submission date for this assignment.

We recommend that you allow at least 30 minutes before the deadline to upload your submission, as failure to upload your assessment file within the allotted time is not admissible as an exceptional circumstance.

The webpage [How do I submit an online assignment?](https://community.canvaslms.com/t5/Student-Guide/How-do-I-submit-an-online-assignment/ta-p/503) provides further technical information on how to upload an assessment. The advice given here comes directly from Canvas. We do not recommend uploading assignments by mobile. We recommend you view the submission after uploading your work to ensure the correct file has been submitted and no technical errors have occurred.

If you face any technical difficulties whilst trying to submit this assessment, then contact Canvas support on [support@instructure.com](mailto:support@instructure.com) or +44 80 0060 8442 (available 24 hours) in advance of the deadline. You should also email [cs-online-admin@york.ac.uk](mailto:cs-online-admin@york.ac.uk) as a matter of urgency to report the issue and receive further instruction.

# Assessment Policies

This assessment is subject to the policies stated on the ‘Summative Assessment Policies’ page in Canvas. These policies include (but are not limited to):

* Academic Integrity and submission of student work to Turnitin
* Advice on anonymising your assessment
* Penalties for late submission
* Marking policy for multiple submissions
* The Fit to Sit / Submit policy
* Passing mark and module reassessment

Please ensure that you have read and understood these policies before starting the assessment.