COM00147M

Department of Computer Science

Computer and Mobile Networks

SUMMATIVE ASSESSMENT BRIEF

|  |  |
| --- | --- |
| **Author** | Oluwaseyi Oginni and 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 for this module are as follows:

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.
2. Apply network concepts and design principles, design, communicate and implement a networked application.
3. Critically evaluate and apply tools for computer network performance analysis.
4. Critically evaluate network security techniques.
5. Critically evaluate the legal and ethical impact of computer networks and internet

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

# Assessment Background/Scenario

You are working as a network engineer for an IT company called YorkInc and you have been assigned to design and implement a new enterprise network infrastructure based on traditional technologies and IPv4 addressing for the company.

The company consists of four departments – Finance/HR, Engineering, Sales, and Administration – and provides wired LAN access and PC desktop workstations for office-based users.

The network requires five servers – Web, Email, DNS, Authorisation, and a File/Print server – and access to all servers must be provided for all office-based users. External users can access the company’s external website only.

It is company policy to allow staff to use a wireless network with their own devices, such as smartphones, to access the internet, although these devices should be able to access the servers but not be permitted to access the departmental networks. In addition, the company would like to trial the use of IoT devices to monitor the server room.

The distribution of workstations is shown in Table 1, which describes the high-level network requirements for each department.

|  |  |  |
| --- | --- | --- |
| **Department** | **Workstations** | **Network Requirements** |
| **Finance /HR** | 120 computers | Each department has a dedicated wired LAN network that cannot access workstations in any other department. |
| **Engineering** | 50 computers |
| **Sales** | 200 computers |
| **Administration** | 25 computers |
| **Wireless devices** | Staff-owned devices | Cannot access any internal departmental networks and requires a separate logical network to access the company servers. |
| **Authorisation server** | 1 server machine | Authorises users to logon to the internal company resources (servers and workstations) |
| **Email, DNS & file/ print server** | 3 server machines | Accessible by all company computers and authorised wireless devices, providing shared services to authorised users. |
| **Web server** | 1 server machine | Server hosting an externally facing website accessible to any users. |
| **IoT devices** | IoT devices | A new requirement for IoT devices to monitor the server room temperature and door. |

Table 1: workstation and server distribution and requirements

# Assessment Tasks

This assessment is broken down into the following tasks:

### Task 1

Analyse the requirements given in the scenario and design a suitable network model, IP address design and network components that meet the requirements of the stakeholders. Based on your analysis and evaluation apply the chosen design to the scenario.

### Task 2

The IT Director has highlighted the importance of the scalability and availability of the network. Evaluate how your chosen network architecture could be adapted to meet these requirements.

### Task 3

The Chief Information Security Officer (CISO) has requested an assessment of the potential wireless security vulnerabilities and any legal and ethical implications of the design.

# Deliverables

The deliverable is a single report, **no more than 3000 words** in length. Your report should consist of the following elements:

### Task 1

* 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 separated from other departments.
  + Indicate on your diagram where interfaces between the components should utilise internal or external network addresses.
* Justify the approach taken and how you selected your network design model, IP addressing, and network component choices, explaining how these are used to fulfil the requirements.

### Task 2

* Outline additional network components that could be added to meet the scalability and availability requirements and which will allow the network to grow in future.
* Explain any supporting technologies/protocols used, for instance: Routing and Addressing protocols.

### Task 3

* Research and evaluate three different potential wireless network attacks and their implications, with brief descriptions on how to mitigate such attacks, justifying your choice of approach. Also comment on the proposed location of the wireless access point.
* Evaluate the potential legal and ethical implications of adopting a Bring Your Own Device (BYOD) policy towards accessing the corporate network.

## 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 (like websites) used in your assignment.

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

## Other Formatting Requirements

The submission is a single document. It must be provided in a format which Canvas can display (i.e. PDF or MS-Word native format). Your report should be **no more than 3000 words** in length and adhere to the following formatting guidelines:

* You may use pen and paper or any network diagram tool to design the network, but the images and diagrams must be clear and viewable on the page without scaling.
* You must include a reference list of all citations made using IEEE standard (see induction modules).
* Present your report on A4 pages, with a minimum 12pt font (14 point for headings), minimum 120% line spacing (what Word calls “Multiple 1.08”), and minimum 2cm margins either side.
* Paragraphs must not be excessively long. “Wall of text” answers which do not contain breaks at logical points are not acceptable.
* All assignments have a +/- 10% allowance on the word count.

**NOTE:** Failure to comply with the specified format will result in a mark of 0.

# Marking Criteria

|  |  |  |
| --- | --- | --- |
| Learning Outcome | Criteria | Available marks |
|  | Academic integrity and referencing | **10** |
| 1, 2 | A description and network diagram, summarising the network design, network isolation and IP addressing needs.  Accommodates the plan for all the necessary devices.  Accounts for the inclusion of scalability, availability, and security in the architecture. | **30** |
| 1, 2, 3 | Demonstrates effective assessment and judgment in selecting components. Demonstrates understanding of issues based on evaluating and comparing different network components supported by literature and relevant theories.  Evaluation of different technologies such as addressing and routing protocols, VLANs, Trunking, Access control, DHCP etc. | **30** |
| 4,5 | Evaluates different wireless attacks common in wireless networks with descriptions on how to mitigate such attacks. The attacks should include both hardware and software elements that can compromise the network. Assess the legal and ethical implications of adopting a BYOD policy. | **30** |
| Total | | **100** |

| Criteria | **Marks**  **70 - 100 % +** | **Marks**  **60 – 69%** | **Marks**  **50 – 59%** | **Marks**  **0 – 49%** |
| --- | --- | --- | --- | --- |
| **Network Design and Analysis**  **Mark: 30** | The learner has provided an excellent recommendation and explanation of IPv4 addressing scheme that accounts for scalability | The learner has provided a very good recommendation and explanation of IPv4 addressing scheme that accounts for scalability | The learner has provided a good recommendation and explanation of IPv4 addressing scheme that accounts for scalability | The learner has provided a basic recommendation and explanation of IPv4 addressing scheme that accounts for scalability |
| **Evaluation of different components**  **Mark: 30** | Excellent evaluation of different technologies and/or protocols such as VLANs, Trunking, Access control, DHCP, STP, VTP etc. | Very good evaluation of different technologies and/or protocols such as VLANs, Trunking, Access control, DHCP, STP, VTP etc. | Good evaluation of different technologies and/or protocols such as VLANs, Trunking, Access control, DHCP, STP, VTP etc. | Limited evaluation of different technologies and/or protocols such as VLANs, Trunking, Access control, DHCP, STP, VTP etc. |
| **Critically evaluate network security and mitigation techniques**  **Mark: 30** | An excellent evaluation of network threats and a very thorough range of mitigations considered. | A very good evaluation of network threats and a very thorough range of mitigations considered. | A good evaluation of network threats and a very thorough range of mitigations considered. | A limited evaluation of network threats and a very thorough range of mitigations considered. |
| **Structure of report, quality of critical evaluation and referencing, appropriate and accurate technical language**  **Mark:10** | The report has an excellent structure, well-presented with appropriate referencing and citation details. Excellent spelling and grammar. All references and citations add to the argument style. | The report has a very good structure Well-presented with appropriate referencing and citation details. Competent spelling and grammar. | The report has a good structure, well-presented with appropriate referencing and citation details. Competent spelling and grammar are consistent. Some inconsistencies with respect to paraphrasing and quality of references. | The report is poorly organised and difficult to follow. Chaotic writing style. Little or no use of structured headings. Poor attention to spelling and grammar.  Poor quality of references and knowledge of their application. |

# 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.

This assessment requires you to anonymously upload your submission to Canvas. If you are submitting multiple files, you must upload all files simultaneously to ensure that they are marked as a single submission. If you want to resubmit one component of your work, you need to re-upload all other files at the same time: every submission must include **all** files required by the assessment brief.

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

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