The University of Western Australia

1st SEMESTER EXAMINATIONS
JUNE 2017

**SCHOOL OF COMPUTER SCIENCE & SOFTWARE ENGINEERING**

# NETWORKS AND SECURITY (CITS3002)

This Paper Contains 5 Pages and 4 Questions
You are required to attempt THREE (3) of the FOUR (4) questions.

Time Allowed: 2 Hours (including reading time)

Do not write verbose answers to any question.
As a guide, a question worth EIGHT (8) marks should be answered on at most a single page of your answer booklet.

*PLEASE NOTE*

*Examination candidates may only bring authorised materials into the examination room. If a supervisor finds, during the examination, that you have unauthorised material, in whatever form, in the vicinity of your desk or on your person, whether in the examination room or the toilets or en route to/from the toilets, the matter will be reported to the head of school and disciplinary action will normally be taken against you. This action may result in your being deprived of any credit for this examination or even, in some cases, for the whole unit. This will apply regardless of whether the material has been used at the time it is found.*

*Therefore, any candidate who has brought any unauthorised material whatsoever into the examination room should declare it to the supervisor immediately. Candidates who are uncertain whether any material is authorised should ask the supervisor for clarification.*

THIS PAGE INTENTIONALLY LEFT BLANK

1a) Consider sliding window protocols which must deal with transmission errors in the presence of pipelining.

With the use of diagrams, explain the differences between a protocol incorporating *go-back-n* and a protocol incorporating *selective-repeat*.

(10)

1b) Develop some pseudo-code, with a syntax similar to either Java or C, that simulates the behaviour of the 1-persistent CSMA/CD protocol over 10Mbps Ethernet.

The simulation should support *N* identical nodes, each wishing to transmit a frame to other nodes at random intervals. Assume that the Ethernet's slot-time is 52 microseconds, and that collision detection and resolution takes exactly one slot-time.

With reference to your simulation's implementation, explain how the maximum channel utilization may be easily obtained.

(Do not be overwhelmed by this problem. You are not being asked to develop a protocol using the *cnet* framework. A correct solution requires only about 30 lines of pseudo-code).

(10)

---

2a) IPv4 addresses were originally split up into separate classes to partition them into different size blocks for use by different organisations. This system was then replaced with a more flexible mechanism to partition the addresses of IPv4.

Describe the original class based addresses that were, used detailing what they were, and what problems were caused by adopting that approach.

Describe the new system that was put in place to replace that mechanism.

How did the partitioning work?

What are the advantages of the new approach?

(10)

2b) Describe how ICMP messages can be used to trace the route IP packets will take from a source address to a destination.

Start by describing what ICMP is, its relationship to IP, the actual ICMP messages involved in implementing the route tracing and how it actually would work.

(10)

---

3a) Consider the case of two Ethernet LAN segments, connected by a single gateway device.

A host on one of the LAN segments wishes to send a UDP/IP datagram to a host on the other LAN segment. Both hosts know the IP address of the gateway device.

Assuming that none of the three devices knows the Ethernet addresses used by the other two devices, describe the complete sequence of Ethernet frames necessary to deliver the datagram.

(10)

3b) Draw a diagram showing the packet structure of a single Ethernet packet carrying an HTTP request using TCP/IP.

Highlight all fields that identify any forms of source/destination connectivity.

(10)

---

4a) Describe what problems the Transport Layer Security (TLS) protocol framework is trying to solve.

What are the problems that it can't get around and specifically discuss two ways in which a hacker could subvert TLS to be able to get at the contents of the traffic it is protecting.

(10)

4b) The Internet of Things (IoT) introduces a fundamental challenge to the integrity and security of the Internet.

Describe the types of threats that IoT bring and what could be done to safeguard the Internet and end users from this threat.

(10)

---

**END OF PAPER**