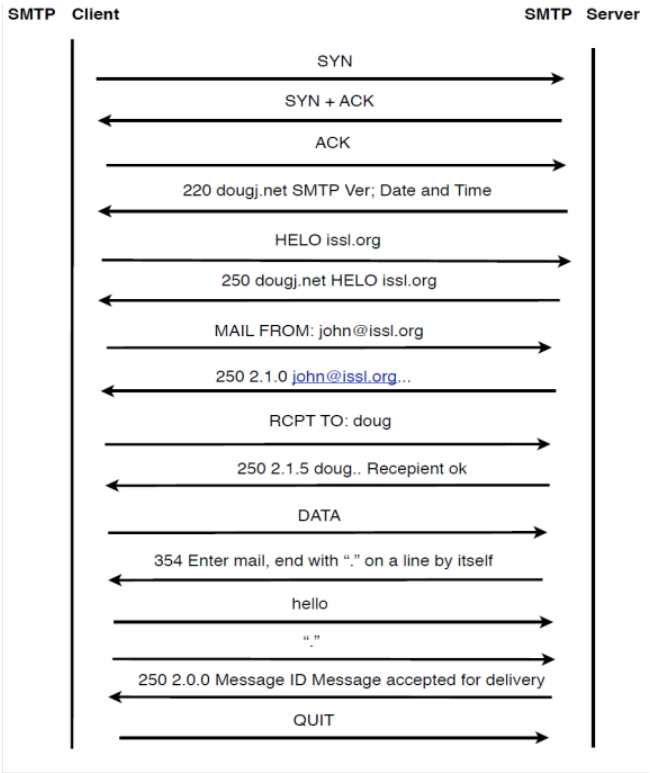
Cpre 530 – Homework 3

Fall 2011

Suganya Baskaran

Problem 1:
Part a)



Part b) Assuming each message is sent as one TCP packet, the total number of bytes (TCP payload) required to send this message is 55 bytes.

Part c) 936 is the total number of bytes transmitted on the network including all packets – 30 bytes for IP header and 25 bytes of Ethernet header per TCP packet

Part d) The total overhead (total number of bytes sent on the wire versus the total size of the payload) is 936 bytes vs 55 bytes.

Part e) The total overhead (total number of bytes sent on the wire versus the total size of the user message) is – 936 bytes vs 5 bytes.

Problem 12

Every MTA that passes the email attaches its own header to it. The header has details such as IP and machine name of every MTA through its path. A public IP can be traced. The geographical location of the IP of sender can be obtained by tracing back to MTA along with IP and help of network registration authorities. No such tracing is possible if the IP is private. Traceback might not be very helpful in finding someone that is using email for illegal

purposes as the person might use a public computer in which case tracing is not at all possible though tracing back to IP owner is possible if the IP is public.

Problem 13
13 spam emails headers were received and by tracing, it was found that all of them originated in USA.

Lab Experiment 1
1) Sending an email to suganya@spock.ee.iastate.edu
> telnet spock.ee.iastate.edu 25
Trying 129.186.215.48...
Connected to spock.ee.iastate.edu.
Escape character is '^]'.
220 spock.ee.iastate.edu ESMTP Sendmail 8.13.4/8.13.4; Wed,30 Nov 2011 15:46:54 -0600 (CST)
Welcome bones.ee.iastate.edu
250 spock.ee.iastate.edu Hello bones.ee.iastate.edu [129.186.215.41], Nice to meet you
MAIL FROM: suganya@bones.ee.iastate.edu
250 2.1.0 suganya@bones.ee.iastate.edu... Sender ok
rcply to: suganya
250 2.1.5 suganya... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Hello Welcome
.
250 2.0.0 mA7LksIL096730 Message accepted for delivery

2) Commands to Retrieve Mail from spock.ee.iastate.edu
> telnet spock.ee.iastate.edu 110
Trying 129.186.215.48...
Connected to spock.ee.iastate.edu.
Escape character is '^]'.
+ O K Q P O P (v e r s i o n 2 . 5 3) a t s p o c k . e e . i a s t a t e . e d u s t a r t i n g .
<76848.1226096425@spock.ee.iastate.edu>
user suganya
+OK Password required for suganya.
pass cpre530
+OK suganya has 1 message (520 octets).
list
+OK 1 messages (520 octets)
1 520
.
retr 1
+OK 520 octets
Return-Path: suganya@bones.ee.iastate.edu
Received: from bones.ee.iastate.edu (bones.ee.iastate.edu [129.186.215.41])
by spock.ee.iastate.edu (8.13.4/8.13.4) with SMTP id mA7LksIL096730
for suganya; Wed, 30 Nov 2011 15:47:34 -0600 (CST)
(envelope-from suganya@bones.ee.iastate.edu)
Date: Wed,30 Nov 2011 15:46:54 -0600 (CST)
From: suganya@bones.ee.iastate.edu
Message-Id: <201111302147.mA7LksIL096730@spock.ee.iastate.edu>
To: undisclosed-recipients:;

X-UIDL: 66bdfd8413c8100bd537c5ba22b05a26
Hello Welcome
.

3) Tracing back emails-
Email Message From Source Traced To
suganyab@gmail.com 72.33 .87.233 – Dallas, Texas
sunil@gmail.com 214.233.20.59 – Hyderabad, India
santhosh86@hotmail.com 81.32.65.43 – Seattle, Washington
hajamaideen@intel.com 202.138.127.106 - Bangalore, India

Reference:

1. http://www.dougj.net/modules/index.html