Internet Protocols Midterm #2 Solutions

2016. 4. 25

Student ID _____ Name _____

1. Suppose a table in a SNMP agent has the following structure.

130	1	130
130	2	130
89	1	1600
92	1	1600
92	2	444
93	1	1600

A. Which should be the index column(s)? 1&2 (4pts)

B. If the OID of the table is .1.3.6.1.2.1.2.2 and the OID of the table entry is .1.3.6.1.2.1.2.2.1, what would be the OID of the value 444 in the table?

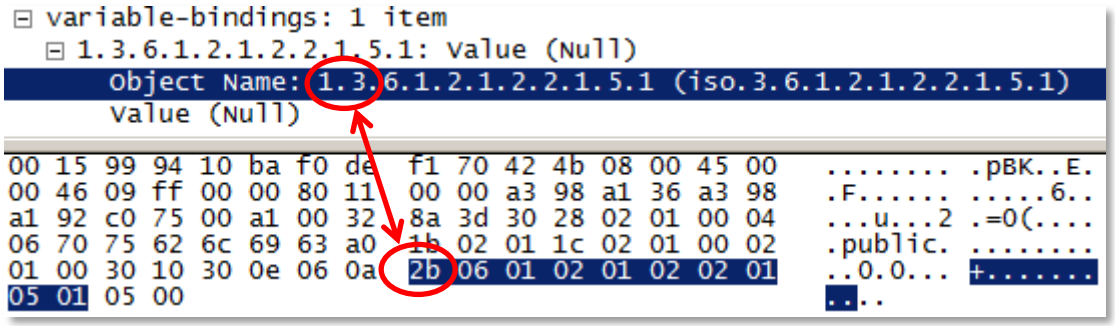
.1.3.6.1.2.1.2.2.1.3.92.2 (4pts)

C. What would you get if you issue GETNEXT on the OID of (B)? [Hint: the table is stored in memory in the lexicographic order of the OIDs, so the table traversal gets to follow the lexicographic order.]

1600 (5pts)

2. Explain the BER encoding rule behind the apparent discrepancy in the beginning part of the OID, between the decimal interpretation and its hexadecimal representation in the SNMP packet. (6pts)

First number * 40 + second number = 1*40+3 = 43 = 0x2b



3. The beginning part of a SNMP packet is given in the hexadecimal representation as follows. Using the BER encoding table for SMI data types and the SNMP PDU types table, answer the questions.

```
30 2c 02 01 00 04 06 70 75 62 6c 69 63 a2 1f 02 01 1c 02 01 00 02 01 00 30 14 30 …↵
```

<BER encoding of SMI data types>

Data Type	*Tag (Hex)*	*Data Type*	*Tag (Hex)*
INTEGER	**02**	IPAddress	**40**
OCTET STRING	**04**	Counter	**41**
OBJECT IDENTIFIER	**06**	Gauge	**42**
NULL	**05**	TimeTicks	**43**
SEQUENCE, SEQUENCE OF	**30**	Opaque	**44**

<SNMP PDU types>

Type	*Tag (Hex)*	*Type*	*Tag (Hex)*
GetRequest	**A0**	GetBulkRequest	**A5**
GetNextRequest	**A1**	InformRequest	**A6**
Response	**A2**	Trap (SNMPv2)	**A7**
SetRequest	**A3**	Report	**A8**

A. What is the total length of the SNMP packet? [Hint: You should take account of the type and length fields as well.] 0x2c + 1 + 1 = 46 bytes (4pts)

B. What is the version of the SNMP protocol here? 1 (= '00' + 1) (3pts)

C. What is the SNMP message type? A2 = Response (3pts)

4. What are the three components in Internet network management framework? [Hint: all are in acronyms.] SNMP , MIB , SMI (6pts)

5. What are the two uses of ICMP? (4pts)

- IP datagram delivery error report to source
- Network state query/response

6. Answer the questions about the following ICMP packet capture.

```
Internet Protocol Version 4, Src: 163.152.16.33 (163.152.16.33), Dst: 163.152.161.129 (163.152.161.129)
Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 1 (Host unreachable)
  Checksum: 0x2556 [correct]
⊞ Internet Protocol Version 4, Src: 163.152.161.129 (163.152.161.129), Dst: 163.152.255.255 (163.152.255.255)
⊟ User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
    Source port: 137 (137)
    Destination port: 137 (137)
    Length: 58
  ⊟ Checksum: 0xd65c [unchecked, not all data available]
```

```
00  d0 50 99 5e f7 b8 64 ae  0c 41 32 c0 08 00 45 00   .P.^..d. .A2...E.
10  00 38 3c f2 00 00 fe 01  86 ff a3 98 10 21 a3 98   .8<..... .....!..
20  a1 81 03 01 25 56 00 00  00 00 45 00 00 4e 44 a5   ....%V.. ..E..ND.
30  00 00 7e 11 0f 48 a3 98  a1 81 a3 98 ff ff 00 89   ..~..H.. ........
40  00 89 00 3a d6 5c                                  ...:.\
```

A. If the dead IP datagram does not have an option field, how many bytes does the ICMP at 163.152.16.33 copy beyond the IP header, from the dead IP datagram? 8 (i.e., UDP header) (4pts)

B. Why do we need the additional payload bytes in (A)?

To identify the process that sent the dropped IP datagram using IP addresses and port numbers

(4pts)

C. What do you think caused the destination unreachable error?

Directed broadcast to all hosts in all subnets in Korea University (i.e., destination address = 163.152.255.255)

(4pts)

7. In the following Wireshark trace,

A. What is going on in packet #39?

ACD (or DAD)

(3pts)

B. What is going on in packet #42?

10.16.25.1 trying to get the link layer address of the router

(3pts)

C. After which packet can the DHCP client use the assigned IP address first if it so wants? #34 (3pts)

D. Why is the assigned IP address shown in the destination IP address field, when the client insists on using 0.0.0.0 as the source IP address during DHCP transactions? [Hint: Consider what flag in the DHCP message would be involved.]

B flag = 0, hence responses delivered in unicast to the assigned address

(5pts)

E. Why do the DHCP messages carry Transaction ID?

To match responses with requests

(3pts)

F. What are the names of the field in SNMP and STUN, respectively, that are used for similar purpose as the DHCP Transaction ID?

Request ID , Transaction ID

(6pts)

2	0.034125	0.0.0.0	255.255.255.255	DHCP Discover - Transaction ID 0xacb6f52e
32	0.676999	10.16.6.10	10.16.25.12	DHCP Offer - Transaction ID 0xacb6f52e
33	0.678331	0.0.0.0	255.255.255.255	DHCP Request - Transaction ID 0xacb6f52e
34	0.684372	10.16.6.10	10.16.25.12	DHCP ACK - Transaction ID 0xacb6f52e
39	0.758735	IntelCor_99:cc:6	Broadcast	Who has 10.16.25.12? Tell 0.0.0.0
42	0.833010	IntelCor_99:cc:6	Broadcast	Who has 10.16.25.1? Tell 10.16.25.12

8. Why did we need network address translation in the first place?

(predicted) IP address shortage

(3pts)

9. A Basic NAT, which is one type of traditional NAT, maps one private IP address to a public address and vice versa at any one time. What property does it exploit to map m private addresses to n public addresses for m >> n?

Statistical multiplexing

(4pts)

10. Suppose you are using X:x as your transport address (private IP address=X, port=x). You want to talk to an outside peer with the transport address Y:y. Since you know that you are behind a NAT (by seeing your assigned IP address X through ipconfig, for example), you decide to consult a STUN service running at Z:z. The STUN server lets you know that your reflexive transport address towards the STUN server looks like X':x'.

A. If your NAT is a Symmetric NAT (a.k.a. "address- and port-dependent NAT"), you will end up having the following translation entries at the NAT. You informed Y:y of your STUN-provided address X':x'. Explain why you still cannot let your peer at Y:y send any packet to you using X':x' as the destination address.

Symmetric NAT filters incoming packets unless X':x' has sent a packet to Y:y.

(6pts)

<Symmetric NAT translation table>

Host address	Reflexive address	Peer address
X:x	X':x'	Z:z
X:x	X':x'' (x'' ≠ x')	Y:y

B. In case of (A), a different type of server is necessary for you to talk to Y:y. On this server, what transport address would be using?

Relayed address

(4pts)

C. If your NAT is a Full-Cone NAT (a.k.a. "endpoint-independent NAT"), what reflexive address would you use after talking to the STUN server?

X':x'

(6pts)

D. What attribute in the STUN packet would carry X':x' to X:x?

MAPPED-ADDRESS

(3pts)