

# BLG609E - Special Topics: 4G Wideband Wireless Network Architectures (Spring 2012)

## Homework - 10: Network Availability

1. Given the following information compute the overall system availability in percentage over a 24 hour period. There are four eNBs in the network. eNB-1 has 50% of the load, and the other three eNBs carry the remaining 50% of the load. eNB-1 has a downtime of 6 hours during the 24 hour period. The other three eNBs do not suffer any downtime. (5 POINTS)

Overall System Availability is then =

$$\frac{50 * Availability_{ENB-1} + (50/3) * Availability_{ENB-2} + (50/3) * Availability_{ENB-3} + (50/3) * Availability_{ENB-4}}{100}$$

NOTE: We need to take weighted average of the availabilities of all eNBs with respect to their traffic loads to calculate overall system availability.

$$Availability_{ENB-1} = \frac{\overline{T_{ON-ENB-1}}}{\overline{T_{ON-ENB-1}} + \overline{T_{OFF-ENB-1}}} = \frac{24 - 6 = 18 \text{ hours}}{18 + 6 = 24 \text{ hours}} = 75 \%$$

$$Availability_{ENB-2} = \frac{\overline{T_{ON-ENB-2}}}{\overline{T_{ON-ENB-2}} + \overline{T_{OFF-ENB-2}}} = \frac{24 - 0 = 24 \text{ hours}}{24 \text{ hours}} = 100 \%$$

Similarly  $Availability_{ENB-3} = Availability_{ENB-4} = 100\%$

Overall System Availability =

$$\frac{50 * 75 + \left(\frac{50}{3}\right) * 100 + \left(\frac{50}{3}\right) * 100 + \left(\frac{50}{3}\right) * 100}{100} = 87.5 \%$$

2. Download and open the following SCTP trace:

<http://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=view&target=sctp- test.cap>

(5 POINTS). Answer the following questions

- a. The SCTP association has how many streams in each direction?

SCTP INIT message (msg # 1) can be checked for *how many streams the client has wanted* in each direction (outband is wanted, inband is maximum inband streams it supports):

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.170.8	192.168.170.56	SCTP	78	INIT
2	0.000296	192.168.170.56	192.168.170.8	SCTP	174	INIT_ACK
3	0.000783	192.168.170.8	192.168.170.56	SCTP	150	COOKIE_ECHO
4	0.001000	192.168.170.56	192.168.170.8	SCTP	150	COOKIE_ACK

[Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)  
 [Ethernet II, Src: AsustekC\_b1:0c:ad (00:e0:18:b1:0c:ad), Dst: 3com\_45:e4:55 (00:60:08:45:e4)  
 [Internet Protocol Version 4, Src: 192.168.170.8 (192.168.170.8), Dst: 192.168.170.56 (192.168.170.56)  
 [Stream Control Transmission Protocol, Src Port: 7 (?), Dst Port: 7 (?)  
   Source port: 7  
   Destination port: 7  
   Verification tag: 0x00000000  
   Checksum: 0x3761a746 (not verified)  
   [INIT chunk (Outbound streams: 17, inbound streams: 17)  
     [Chunk type: INIT (1)  
       Chunk flags: 0x00  
       Chunk length: 32  
       Initiate tag: 0x43232544  
       Advertised receiver window credit (a\_rwnd): 65535  
       Number of outbound streams: 17  
       Number of inbound streams: 17  
       Initial TSN: 1560161255  
       [Forward TSN supported parameter  
       [Supported address types parameter (Supported types: IPv4)

Did the server acknowledged? Check INIT\_ACK (msg #2) (same numbers of streams acknowledged)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.170.8	192.168.170.56	SCTP	176	INIT
2	0.000783	192.168.170.8	192.168.170.56	SCTP	176	INIT_ACK
3	0.000800	192.168.170.56	192.168.170.8	SCTP	176	COOKIE_ECHO

Frame 2: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0, Src: 3com\_45:e4:55 (00:60:08:45:e4:55), Dst: AsustekC\_b1:0c:ad (00:e0:18:b1:0c:ad)

Internet Protocol Version 4, Src: 192.168.170.56 (192.168.170.56), Dst: 192.168.170.8 (192.168.170.8)

Stream Control Transmission Protocol, Src Port: 7 (?), Dst Port: 7 (?)

Source port: 7  
Destination port: 7  
Verification tag: 0x43232544  
Checksum: 0xc9018524 (not verified)

INIT\_ACK chunk (Outbound streams: 17, inbound streams: 17)

Chunk type: INIT\_ACK (2)

Chunk flags: 0x00  
Chunk length: 128  
Initiate tag: 0x000000b0  
Advertised receiver window credit (a\_rwnd): 4096  
Number of outbound streams: 17  
Number of inbound streams: 17  
Initial TSN: 13844  
State cookie parameter (Cookie length: 100 bytes)  
Forward TSN supported parameter

Therefore, after this connection is set up (after cookie ack) there are 17 streams in both directions.

b. The two data chunks in message 5 belong to which two stream identifiers?

Data Chunk 1: Stream Identifier: 0

Data Chunk 2: Stream Identifier: 1

5	0.002712	192.168.170.8	192.168.170.56	SCTP	1102	DATA DATA
---	----------	---------------	----------------	------	------	-----------

Frame 5: 1100 bytes on wire (8800 bits), 1100 bytes captured (8800 bits) on interface 0, Src: AsustekC\_b1:0c:ad (00:e0:18:b1:0c:ad), Dst: 3com\_45:e4:55 (00:60:08:45:e4:55)

Internet Protocol version 4, Src: 192.168.170.8 (192.168.170.8), Dst: 192.168.170.56 (192.168.170.56)

Stream Control Transmission Protocol, Src Port: 7 (?), Dst Port: 7 (?)

Source port: 7  
Destination port: 7  
Verification tag: 0x000000b0  
Checksum: 0xc7b04068 (not verified)

DATA chunk (ordered, complete segment, TSN: 1560164255, SEQ: 0, SSN: 0, PPID: 0, payload length: 512 bytes)

Chunk type: DATA (0)  
Chunk flags: 0x07  
Chunk length: 528  
TSN: 1560164255  
Stream identifier: 0x0000  
Stream sequence number: 0  
Payload protocol identifier: not specified (0)

Stream Control Transmission Protocol

DATA chunk (ordered, complete segment, TSN: 1560164255, SEQ: 1, SSN: 0, PPID: 0, payload length: 512 bytes)

Chunk type: DATA (0)  
Chunk flags: 0x07  
Chunk length: 528  
TSN: 1560164256  
Stream identifier: 0x0001  
Stream sequence number: 0  
Payload protocol identifier: not specified (0)

Data (512 bytes)

c. Is the cookie value in Cookie-echo the same as that in INIT-ACK and what is its value?

Cookie-Echo (msg #3) is checked and cookie value is: 00 00 0e b0 .... 00 04

INIT-ACK (msg #2) is checked and cookie value is: 00 00 0e b0 .... 00 04

YES, they are same, controlled from cookie content details below.

2	0.000783	192.168.170.8	192.168.170.56	SCTP	174	INIT_ACK
---	----------	---------------	----------------	------	-----	----------

Frame 2: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0, Src: 3com\_45:e4:55 (00:60:08:45:e4:55), Dst: AsustekC\_b1:0c:ad (00:e0:18:b1:0c:ad)

Internet Protocol version 4, Src: 192.168.170.56 (192.168.170.56), Dst: 192.168.170.8 (192.168.170.8)

Stream Control Transmission Protocol, Src Port: 7 (?), Dst Port: 7 (?)

Source port: 7  
Destination port: 7  
Verification tag: 0x43232544  
Checksum: 0xc9018524 (not verified)

INIT\_ACK chunk (Outbound streams: 17, inbound streams: 17)

Chunk type: INIT\_ACK (2)

Chunk flags: 0x00  
Chunk length: 128  
Initiate tag: 0x000000b0  
Advertised receiver window credit (a\_rwnd): 4096  
Number of outbound streams: 17  
Number of inbound streams: 17  
Initial TSN: 13844  
State cookie parameter (Cookie length: 100 bytes)  
Parameter type: State cookie (0x0007)  
Parameter length: 104  
State cookie: 000000b0000010000011001100003614432325440000ffff...  
Forward TSN supported parameter

0000	00 e0 18 b1 0c ad 00 60 08 45 e4 55 00 00 45 00	.....E.U.E.
0010	00 a0 b0 e0 00 00 80 84 b3 5a c0 a8 aa 38 c0 a8	.....Z.S.S.
0020	00 80 00 00 00 00 00 00 10 00 00 11 00 11 00 00	.....C#X.D.S.
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....C.H
0040	36 14 00 07 00 68 00 00 00 00 00 00 10 03 00 13	.....C.T#X
0050	00 11 00 00 30 14 43 23 23 44 00 00 ff ff 00 13	.....U...X
0060	00 11 76 18 2f 10 00 00 00 00 00 00 00 00 00 00	.....U...X
0070	00 00 00 42 85 b3 2f 10 00 00 00 00 00 00 00 00	.....U...X
0080	00 00 00 15 40 00 00 00 00 00 00 00 00 00 00 00	.....U...X
0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....U...X
00a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....U...X

3	0.000800	192.168.170.56	192.168.170.8	SCTP	150	COOKIE_ECHO
---	----------	----------------	---------------	------	-----	-------------

Frame 3: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0, Src: AsustekC\_b1:0c:ad (00:e0:18:b1:0c:ad), Dst: 3com\_45:e4:55 (00:60:08:45:e4:55)

Internet Protocol version 4, Src: 192.168.170.8 (192.168.170.8), Dst: 192.168.170.56 (192.168.170.56)

Stream Control Transmission Protocol, Src Port: 7 (?), Dst Port: 7 (?)

Source port: 7  
Destination port: 7  
Verification tag: 0x000000b0  
Checksum: 0xb85148ea (not verified)

COOKIE\_ECHO chunk (Cookie length: 100 bytes)

Chunk type: COOKIE\_ECHO (10)

0... = Bit: Stop processing of the packet  
0... = Bit: Do not report  
Chunk flags: 0x00  
Chunk length: 104  
Cookie: 000000b0000010000011001100003614432325440000ffff...

0000	00 60 08 45 e4 55 00 e0 18 b1 0c ad 08 00 45 10	.....E.U... ..
0010	00 80 00 00 00 00 40 84 64 50 c0 a8 aa 38 c0 a8	.....S.S. dp.
0020	aa 28 00 07 00 00 00 00 00 00 00 00 51 48 ea 0a 00	.....S.S. dp.
0030	00 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....S.S. dp.
0040	36 14 00 07 00 68 00 00 00 00 00 00 10 03 00 13	.....S.S. dp.
0050	00 11 00 00 30 14 43 23 23 44 00 00 ff ff 00 13	.....S.S. dp.
0060	00 11 76 18 2f 10 00 00 00 00 00 00 00 00 00 00	.....S.S. dp.
0070	00 00 00 42 85 b3 2f 10 00 00 00 00 00 00 00 00	.....S.S. dp.
0080	00 00 00 15 40 00 00 00 00 00 00 00 00 00 00 00	.....S.S. dp.
0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....S.S. dp.
00a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....S.S. dp.

3. Virtual IP Address and Gratuitous ARP (TOTAL 10 POINTS)

Background:

My PC has ARP cache like:

Administrator: Command Prompt		
Interface: 192.168.1.101 --- 0xc		
Internet Address	Physical Address	Type
192.168.1.1	28-fc-11-28-b8-5e	dynamic
192.168.1.100	00-16-ea-cf-bf-5c	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static



May 7, 2012

After I've started the capture on Wireshark, I've deleted the ARP entry for 192.168.1.1 and checked it has been removed from the ARP cache:

```
C:\Windows\system32>arp -d 192.168.1.1
C:\Windows\system32>arp -a

Interface: 192.168.1.101 --- 0xc
Internet Address      Physical Address      Type
192.168.1.100         00-16-ea-cf-0f-5c     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Windows\system32>
```

Then, this address is pinged and after a minute Wireshark capture is stopped.

```
C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

- A. What is the destination MAC address of the "ARP Request"? (2 POINT)

When captured packets are filtered with arp, ARP packets can be seen in Wireshark. ARP Request message for the deleted ARP cache entry is message 58 and 181. They both have the target MAC address of 98:fc:11:98:b8:5e (MAC address of my router)

*destination MAC should be ff:ff:ff:ff:ff:ff*

- B. What is the "Sender IP address" and "Sender MAC address" in the ARP Response? Type "arp -a" on your PC. Is the sender MAC address in your ARP cache entry? (1 POINT).

Sender's IP and MAC address information is retrieved via ARP Response (message # 347)

IP : 192.168.1.101

MAC : 74:2f:68:cd:91:0b

Sender MAC address is not in the ARP cache because the MAC address is my PC's MAC address and need not to be discovered and attached with my IP address.

- C. What is the destination Ethernet address used in the Gratuitous ARP packet? (2 POINT)

Background: I've started Wireshark. Switched off the wireless card and after one minute switched it on again. Thereafter one minute, stopped the Wireshark capture. It is expected and observed that after my PC has gotten IP address via DHCP, it sends out a "Gratuitous ARP".



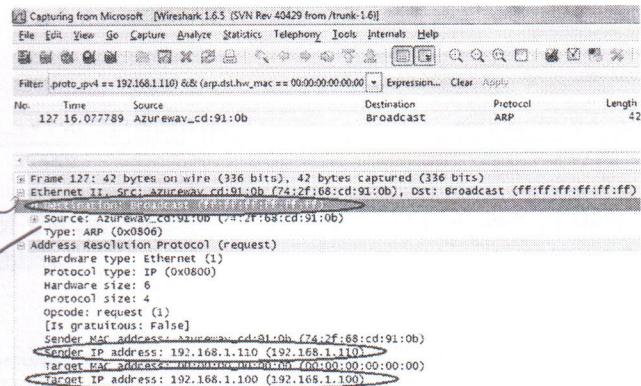
I have applied a filter like: (arp.src.proto\_ipv4 == 192.168.1.110) && (arp.dst.hw\_mac == 00:00:00:00:00:00) for capturing Gratuitous ARP packet. Because "ARP request contains the sender's protocol address (SPA) in the target field (TPA=SPA), with the target hardware address (THA) set to zero".

Note: My IP was changed to 192.168.1.111 after rebooting wireless adapter.

The destination Ethernet address used in the Gratuitous ARP packet: ff:ff:ff:ff:ff:ff (Broadcast)

(Why the is gratuitous field is false? I have tried many captures with many IP changes but could not find any packet with True field.)

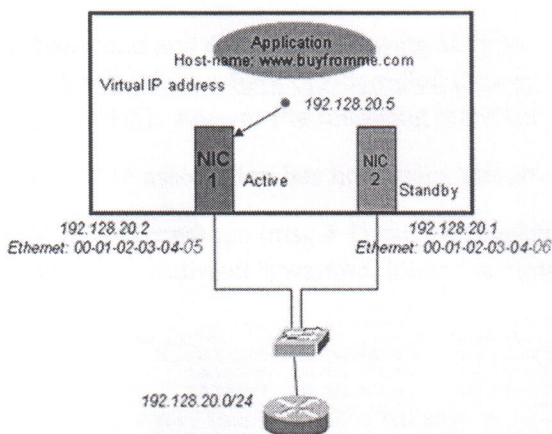
*Yes this is a bug in Wireshark software*



- D. What is the "Target IP address" value in the ARP packet? Does it correspond to your the IP address of your computer? ( 1 POINT)

The target IP address: 192.168.1.100 (was my IP address)

- E. Initially when the virtual IP address is bound to NIC-1, the computer will send out a Gratuitous ARP to inform all the other nodes in the network that the Ethernet address of NIC-1 corresponds to the virtual IP address. What is the "Sender MAC address" value and the "Target IP address" value in the Gratuitous ARP message? (2 POINTS)



In the Gratuitous ARP message:

Sender MAC address value: 00-01-02-03-04-05

Target IP address value: 192.128.20.5

- F. When NIC-1 fails, the Virtual IP address should now be bound to NIC-2, i.e all the other nodes in the network need to be informed that the Ethernet address of NIC-2 corresponds to the virtual IP address. What is the "sender MAC address" value and the "Target IP address" value in the Gratuitous ARP message that the computer now sends? (2 POINTS)

In the Gratuitous ARP message:

Sender MAC address value: 00-01-02-03-04-06

Target IP address value: 192.128.20.5