Exp no: 2 ANLAYSIS OF VOIP SERVICE IN LINUX ENVIRONMENT   
  
  
  
AIM:  
 To setup a VOIP service in a LAN environment and to observe the protocols used while providing the service using wireshark in LINUX environment.  
  
SOFTWARE REQUIRED:  
 LINUX OS, Wireshark, Linphone application in mobile phone.  
  
PROCEDURE:  
   
1.Open ubuntu linux and the terminal.  
  
2. Enter “sudo apt update” to update the OS.  
  
3. To install Asterisk in the system enter the cmd “sudo apt install asterisk -y”.  
  
4. Now go to the location /etc/asterisk using the command “cd /etc/asterisk”  
  
5. Upto this the asterisk server installation is completed.  
  
6.Now we need to configure the server.  
  
7.Enter the command “sudo mv sip.conf sip.conf.backup” whick creates a backup file.  
  
8.Now we need to code to sip file. To create a file “sudo gedit sip.conf” for coding.  
  
code for sip :  
general]

context=default

allowoverlap=no

udpbindaddr=0.0.0.0

tcpenable=no

tcpbindaddr=0.0.0.0

transport=udp

srvlookup=yes

[7001]

type=friend

host=dynamic

secret=7001

username= 7001

[7002]

type=friend

host=dynamic

secret=7002

username= 7002

[7003]

type=friend

host=dynamic

secret=7003

username= 7003

[7004]

type=friend

host=dynamic

secret=7004

username= 7004  
  
  
9. Now we need to configure the extension file. Use the command “sudo mv extensions.conf extensions.conf.backup”  
  
10.For the coding inside extension file cmd “sudo gedit extensions.conf”  
  
code for extension file:  
[general]

static=yes

writeprotect=no

priorityjumpings=no

autofallthrough=yes

clearglobalvars=no

[default]

exten => 7001,1,Answer()

exten => 7001,2,Dial(SIP/7001,60)

exten => 7001,3,Playback(vm.nobodyavail)

exten => 7001,4,VoiceMail(7001@main)

exten => 7001,5,Hangup()

exten => 7002,1,Answer()

exten => 7002,2,Dial(SIP/7002,60)

exten => 7002,3,Playback(vm.nobodyavail)

exten => 7002,4,VoiceMail(7001@main)

exten => 7002,5,Hangup()

exten => 7003,1,Answer()

exten => 7003,2,Dial(SIP/7003,60)

exten => 7003,3,Playback(vm.nobodyavail)

exten => 7003,4,VoiceMail(7001@main)

exten => 7003,5,Hangup()

exten => 7004,1,Answer()

exten => 7004,2,Dial(SIP/7004,60)

exten => 7004,3,Playback(vm.nobodyavail)

exten => 7004,4,VoiceMail(7001@main)

exten => 7004,5,Hangup()

exten => 8001,1,VoicemailMain(7001@main)

exten => 8001,2,Hangup()

exten => 8002,1,VoicemailMain(7002@main)

exten => 8002,2,Hangup()

exten => 8003,1,VoicemailMain(7003@main)

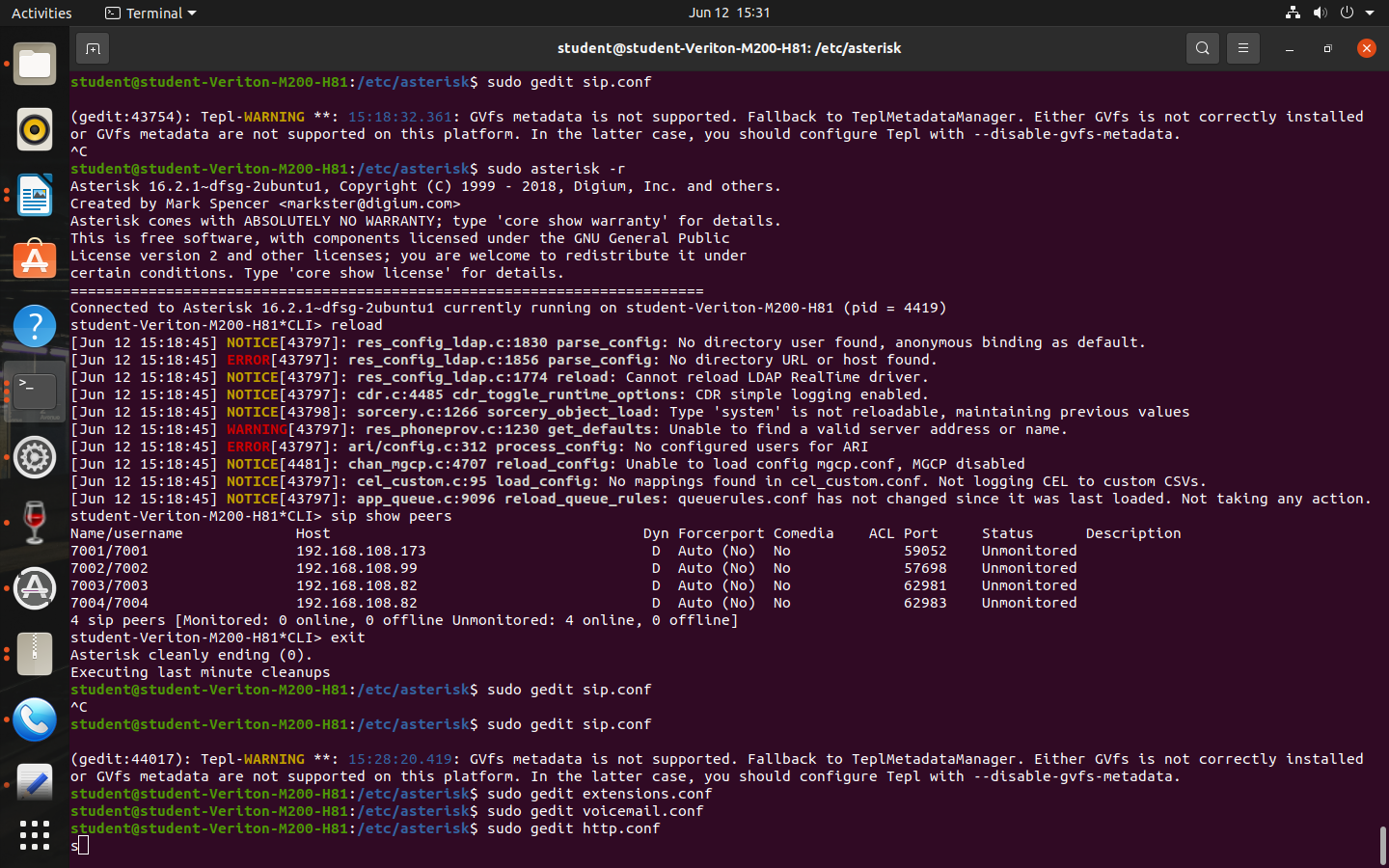
exten => 8003,2,Hangup()

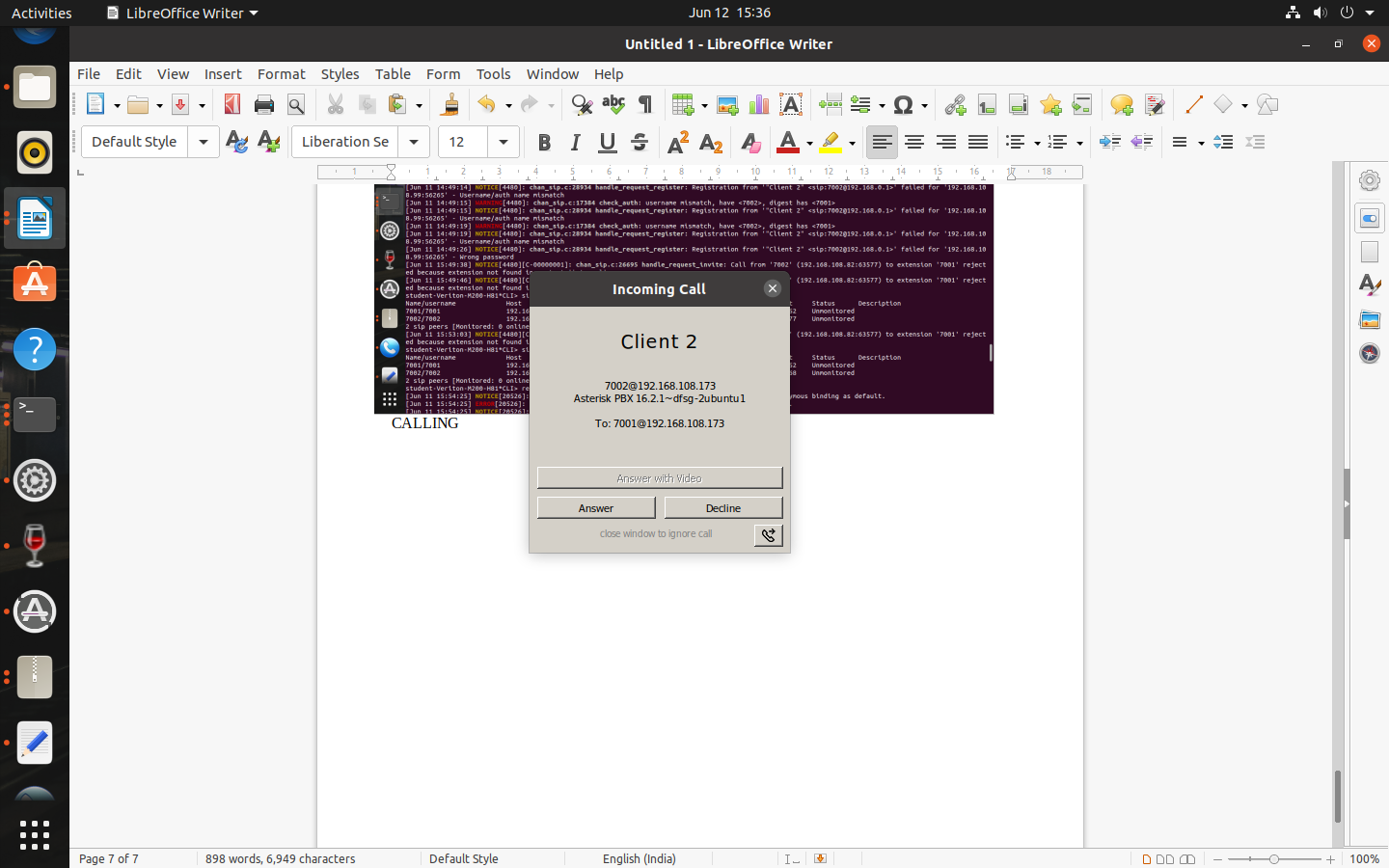
exten => 8004,1,VoicemailMain(7004@main)

exten => 8004,2,Hangup()  
  
11. The voicemail file have to be configured, so cmd “sudo mv voicemail.conf voicemail.conf.backup” and to code for voicemail “sudo gedit voicemail.com”  
  
code for voicemail:  
  
7001 >= 7001

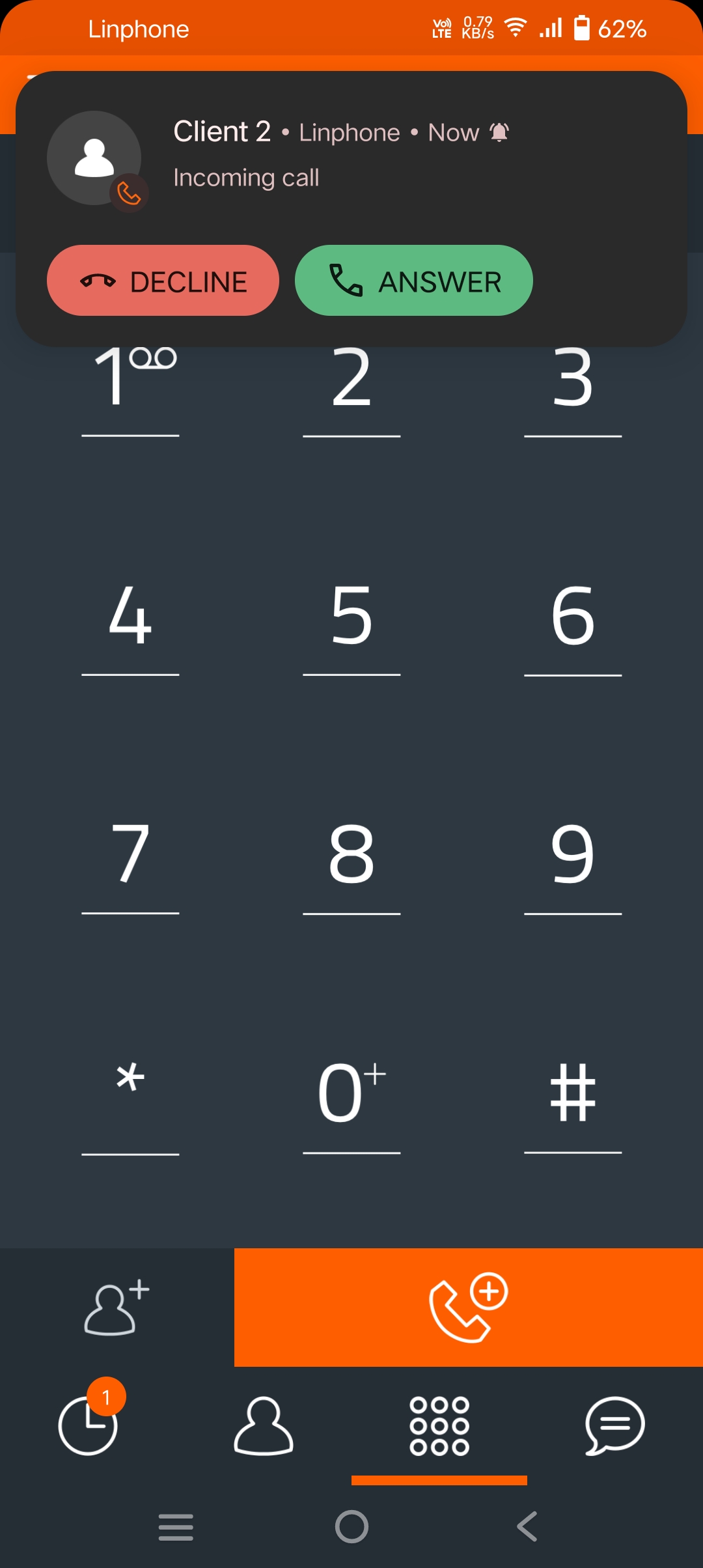
7002 >= 7002

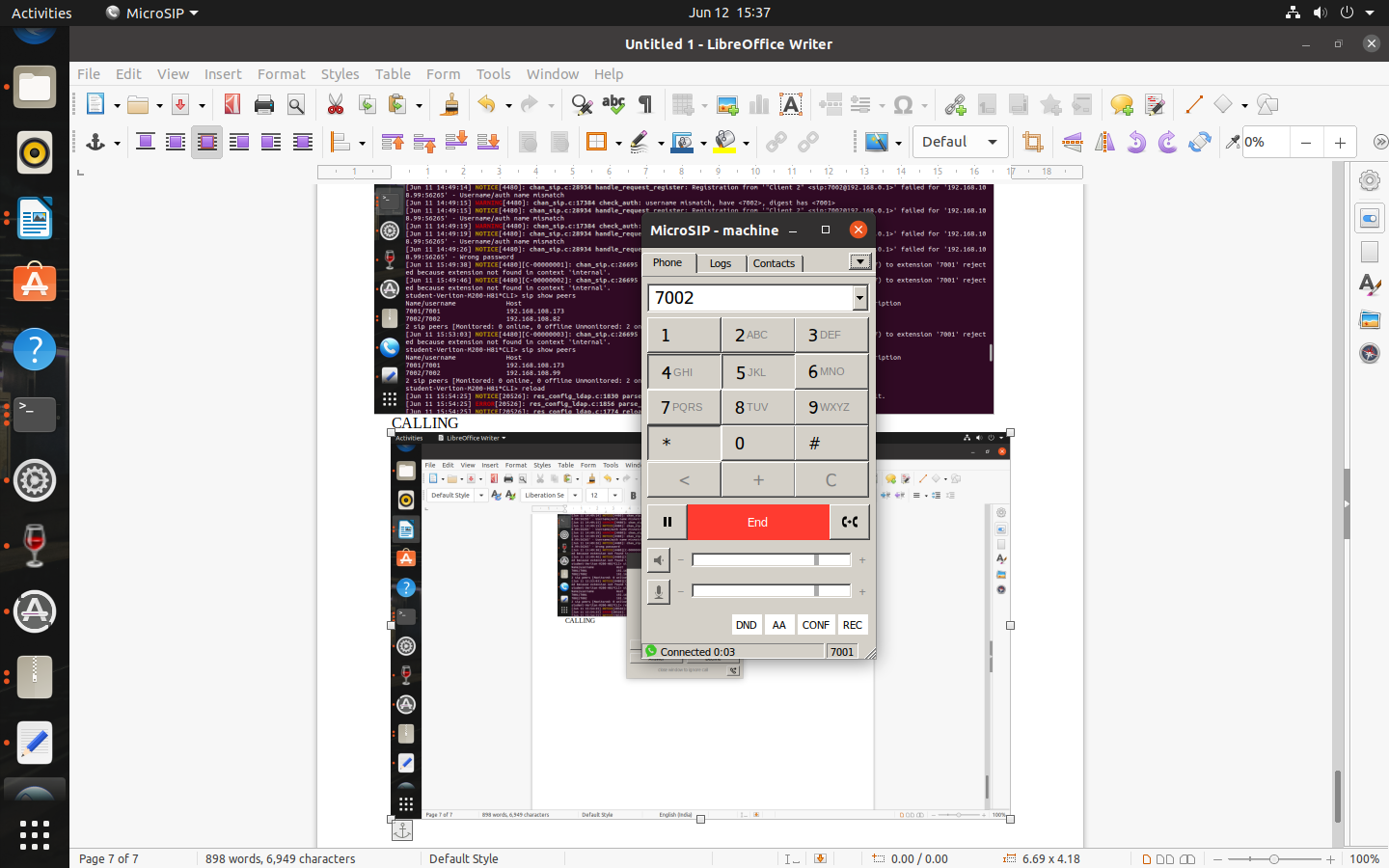
7003 >= 7003

7004 >= 7004  
  
12. To open the asterisk server use the cmd “ sudo asterisk -r” and type “reload” to update the code in the server.  
  
13. Type “sip show peers” to show the list of devices and their status in the server.  
  
14. After this we need to configure the clients. Download the linphone application in the devices of the LAN connenction.  
  
15.Open the application and enter ther sip account settings with the IP address of the server. Then enter the username and password as specified in the sip code file.  
  
16. Wait until the connected status is shown. We can verify the connection by reloading the server and seeing the status of the devices. Now we can call to the other devices.  
  
 (Display of status of the devices in the server)



(call received from client 2)



 (calling through linphone application)  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
 (call attended in the receiver side)  
  
ANALYSIS OF THE WIRESHARK FILE IN SERVER :  
1. On the analysis the wireshark captured packets in the server the major sources are listed below.  
  
  
 (sources and the packets sent)

|  |  |
| --- | --- |
| sources | number of packets sent |
| 104.21.3.209 | 2 |
| 104.21.3.209 | 2 |
| 142.250.182.46 | 2 |
| 142.250.183.234 | 2 |
| 192.168.108.1 | 7 |
| 192.168.108.109 | 12 |
| 192.168.108.158 | 9 |
| 192.168.108.173 | 723 |

2.The above are the major sources in the server side communication aspect.  
  
3. Now we have to analyse the protocols used in these sources and we can concentrate on 192.168.108.1, 192.168.108.109, 192.168.108.158 and 192.168.108.173.  
  
4, For 192.168.108.108  
  
 This shows that here OSPF protocol (Open Shortest Path First) is majorly used. The OSPF is a routing protocol used in IP networks to find the shortest path for the data packets by maintaining a map of the network topology. So we can conclude that this device is mainly involved in routing and attack on this system delays the packet transfer by changing the path.  
  
  
  
  
  
7. In 192.168.108.109  
  
  
SSDP – Simple Service Discovery Protocol , as it is used to advertisement and discovery of network services, attack on this ip could prevent the awareness of network topology for each device.  
  
NBNS- NetBIOS Name Service is a protocol used to locate the other devices in the network using the names similar to DNS. If this directory is disrupted then false routing could cause delay in the communication.  
  
LLMNR- Link -Local Multicast Name Resolution, it is based on DNS packet format that allows bot IPv4 and IPv6 hosts to perform name resolution in same local link.   
  
8. In 192.168.108.158  
  
  
9. In 192.168.108.173,  
  
  
RTP- Realtime Transport protocol, handles the realtime trafiic like audio/cvdeo used like udp. As this protocol is responsible for transfer of audio while using voicecall, if we attack over this packet the communication between sender and receiver can be disrupted.  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
RESULT:  
 From this analysis we can understand the server operation in a LAN and the protocol analysis of voicecall in the network