PERFORMANCE EVALUATION OF ASYNCHRONOUS TRANSFER MODE (ATM) AS A VEHICLE FOR WIDE BANDWIDTH INTERNET CARRIAGE

D. E. Bassey., B. E. Okon., E. E. Eyime

Department of Physics,

University of Calabar, Calabar,

Cross River State, Nigeria.

benokon16@yahoo.com, **basseyde1@yahoo.com**

Abstract- The convergence of telecommunications and computer communication technologies heralded by innovations in Internet services requires the development of interworking units to convert different data formats and control procedures into a single unique protocol. Therefore, creating an information transfer protocol such as Asynchronous Transfer Mode (ATM), as a transport and switching model will enhance quality of service delivery. ATM is a standard for carriage of a complete range of user traffic through a single network. It is designed to unify telecommunications and computer networks. The study embarked on a simulation project where different LANs were modeled and configured to convey cells or packets under high speed, with the aid of ATM switching and transport nodes. Through "pinging", the network was examined in terms of carriage of converged signal with respect to time. In addition, wire-shark packet analyzer was activated to access the transferred time of each packet and converts these packets for assessment using window protocol. The study noted that like other Internet transport protocols, ATM also suffered different forms of threats. Recommendations were made from the study.

Keywords: ATM, ISDN, Ethernet, LAN, Interworking unit.

1. INTRODUCTION

Digital communication environment is generally characterized by two main support technologies: on one hand is computer oriented communications and Local Area Networks (LAN), supported by Ethernet or Token ring specifications [2,9]. This technique is based on data packets, using locally or remotely interconnected computers and terminals. On the other hand is the Public Switched Networks (PSN), based on data circuits such as the Integrated Services Digital Networks (ISDN) with capabilities to interconnect a large variety of terminal equipment and also interconnect several LANs remotely through switch or constant rate links [5,12].

In recognition of the main objective of ATM, Interworking units (IWU) were built in for the purpose of converting ISDN and Ethernet traffic to the ATM formats. These conversion procedures located on the lower layers of the OSI protocol reference model (the Physical Layer and the Medium Access Control Layer) [1,6], were briefly discussed.

2. LITERATURE REVIEW

The proposed Interworking device has two data buses: the Utopia Bus, which sustains the cell transfer between line interface modules and the processor bus, which allows ATM cells, ISDN channels and Ethernet packets, to be transferred between line interfaces, the processor, and the memory [3,18].

The Interworking unit has two ISDN interfaces for the basic and the primary access, respectively. The Basic Access Interface is specified at the reference point by several ITU recommendations. With a transmission rate of 144 Kbit/s, S bus is able to inter-connect at least 8 terminals, by sharing one or two 64 Kbit/s time slots for data information transfer (B channel), while the signaling information is transported out of band on a 16 Kbit/s D Channel [7,16].The Basic Access Interface can be used to interconnect ISDN terminals to Local Area Networks (LANs) over a Public Switched Network (PSN), through one or more of the other interfaces of the IWU [13].

Since many computer terminals communicate through an Ethernet interface, according to IEEE 802.3 standards, namely: 10 Base T and 100 Base T specifications, the proposed IWU have to handle these interfaces at physical and logical levels in order to convert the Ethernet environment to ATM specifications [14].

The Interworking unit has two ATM physical interfaces operating at 156 Mbit/s. On the ATM interface, the cells were mapped according to ITU-T recommendation (G. 804) [17], on the frame described by G. 703 [15]. This interface is appropriate for the interconnection of ATM environments over the interconnect LANs [4].

The introduction of the Asynchronous Transfer Mode(ATM), which is neither circuit nor packet oriented transmission protocol, but a conjunction of the best of both techniques, permits the convergence of routing and switching technologies and the specification of new communication platforms, supported by different interfaces and transfer protocols. The integration of this technology, within telecommunications and computer networks, requires the development of special adaptation units with interworking functionalities [10]. Also, the compatibility between different types of services requires the development of adaptable protocols for data presentation, at the application level. On the other end, the compatibility between distinct systems forces the specification of common physical and logical interfaces and the development of Interworking units (IWU), to adapt different transmission, switch and flow control protocols [8,11].This paper, therefore, presents a simple model that interrogates Asynchronous Transfer Mode (ATM), as a vehicle for high speed bandwidth applications and discusses the integration of such device into different network scenarios.

3. METHODOLOGY

3.1 Modeling

A model is a demonstration of a system in a very simple way with the intention of advancing the idea of the real system. A simulator on the other hand is the process of manipulating a model in a way that its function with respect to space and time the proto-type of the model. Modeling as a means of representation has a long history. Man has tried all possible means of modeling creation, with a view to improving his living condition. Motivated by this fact, ATM transmission protocol was simulated and configured as a high speed carrier for a unified, converged network. This configuration served as a model to the real practice of ATM protocol.

3.2 ATM Networks Configuration

The ATM network was configured by using a set of ATM switches interconnected by point-to-point ATM links. Two types of interfaces were configured within the simulated network to support the switches. They were the user to network interface (UNI) and the network to network interface (NNI).The UNI was used to connect ATM end devices like routers and host to an ATM switch. While the network-to-network interfaces (NNI) was used to connect two ATM switches within the network. Table 1 is a comparative review of different protocols and network speed.

Table 1: Comparison between protocols and network speed

Protocol	Cable	Speed	Topology
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
LocalTalk	Twisted Pair	.23 Mbps	Linear Bus or Star
Token Ring	Twisted Pair	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fiber	100 Mbps	Dual ring
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree

SOURCE: http/www.atmforum.com

3.3 Materials

From Table 1, different network protocols were analyzed with a view to selecting the most effective transport protocol that can converge telecommunications signal and computer networking. From these analyses, ATM was selected as the choice protocol for the needed convergence. The following materials used for the study are hereby briefly explained:

i. ATM switch: ATM switches are electronic devices with high speed networking capacity used to transfer data from one end to the other. ATM switches support voice, video and data services and are designed to switch fixed-size data units called cells. Cells are used in ATM communications. The simulated ATM switch received the input cells or information from another ATM device, read and updated the cell header information in order to switch the information cell towards its end-points.
ii. GNS3: Graphical Network Simulation tool was used to design the ATM network.
iii. ATM end points: The end points used for the study were personal computers, IP phones, printers, work-stations and routers.
iv. Networking Cables: The cables employed here were straight-through cables, cross over cables and serial DCE cables.

3.4 System Configuration

The configuration of the unifying network carriage was carried out through a set of wireless switches configured on user network to network interface (UNI). Through the UNI, routers were configured as host to an ATM-configured switch. Another interface was configured through NNI to connect two ATM switches into the simulated network.

The simulator used was a software package called the GNS3 (Graphical Network Simulator).This is an open source graphical network simulation tool used to design flexible network. This package was selected after examining several other packages. They were flexible with ATM, Ethernet and frame relays. GNS3 guarantees a true network setting to carry out the configurations. It can run in all popular window versions. Its graphical user-interface was made in a way that no further customization was needed. GNS3 main program window enabled the researcher to drag network devices like routers, switches, firewalls, work stations, IP phones, etc., into the working interface. Through this medium, different connections were created and the focal features of the study were achieved: design of high quality complex network topology, simulation of simple Ethernet, ATM and frame relay switches, connection of the simulated network to the real wall and packet-capture using wire shark.

Further to the above, the following end points were aiding tools:

1) Personal Computers: personal computers were linked to the Local Area Network (LAN) via cables connection. The personal computer used was a laptop. It was used to send data and video services to the ATM network.
2) IP phone: IP phones were used to deliver voice communication through the ATM network. The model used was a software based phone.
3) Routers: routers were employed to make decisions on the directions of IP packets and route them correctly. A router can be set-up between the Internet service providers (ISP) and the customer network to direct information to either way. The function of a router was to forward packets to other networks until the packet reaches its destination. The router interfaced the two Local Area Network (LANs) used for the study. The routers used were CISCO IOS 7200 routers.
4) Networking cables: Networking cables were used to connect one network device to another network to form a LAN. Further to this accessories, were other shared components such as printers and scanners. The project was wired using the following networking cables.
5) Straight-through cables: Straight-through cables were used to link dissimilar networking devices like switch to pc, switch to router, router to switch, etc. Straight-through cables were used when each end of the communication linkages transmitted and received packets from different pairs. Similarly cross over cables were used to connect similar network devices like pc to pc, router to router, switch to switch, hub to hub, etc. Serial DCE cables were also used to provide the clock signals in order to communicate through bus topology and to connect one router to the other in the network.

3.5 Configuration-commands used to activate the ATM switch

The simulator used to model the ATM network was the GNS3.The above highlighted components of the network was configured using the following man-machine language commands:

Set the VCI to VPI ratio. The switching process of the ATM network was based entirely on the VCI to CPI ratio. The VCI to VPI values control the memory distribution in the network. It specifies the maximum value of the VCIs to support the VPI. Fig. 1 is a plate showing ATM switch port numbers configured during the project.

To set the VCI to VPI ratio, the under listed procedures present samples of man-machine language commands initiated.

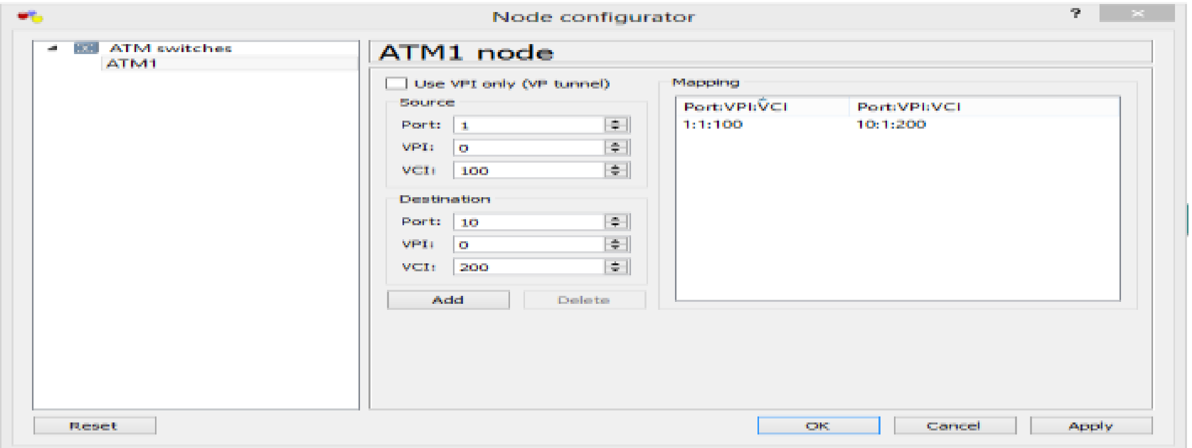
The numbers used were as follows:

1:1:100=10:1:200

Where

Port = 1
VCI = 100 } Source network
VPI = 0

Port = 2
VCI = 200 } Destination network
VPI= 0



ATM1

ATM1 node

□ Use VPI only (VP tunnel)

Source
Port: 1
VPI: 0
VCI: 100

Destination
Port: 10
VPI: 0
VCI: 200

Mapping

Port:VPI:VCI	Port:VPI:VCI
1:1:100	10:1:200

FIG. 1: ATM switch port numbers

3.6 Configuration of the routers

The routers used for this work were the CISCO IOS 7200 model. The router was chosen because of the in-built ATM configuration in it. The following procedures present summarized system configuration used.

Router 1

R1> enable

```
R1# configured terminal
R1 (config) # interface ATM1/0
R1 (config-if)# IP address 192.162.1.1 255.255.255.252
R1 (config-if)# map-group atm-cir-123
R1 (config-if)# no shut down
R1 (config-if)#atmpvc 1 1 100 aa/5 snap
R1 (config-if)# no atmilmi-keepalive
R1 (config-if)# exit
R1 (config)# map-list atm-cir-123
R1 (config)# IP 192.168.1.2 atm-VCI broadcast
R1 (config)# interface Ethernet 2/0
R1 (config-if)# IP address 192.168.2.1 255.255.255.0
R1 (config-if)# no shut down.
```

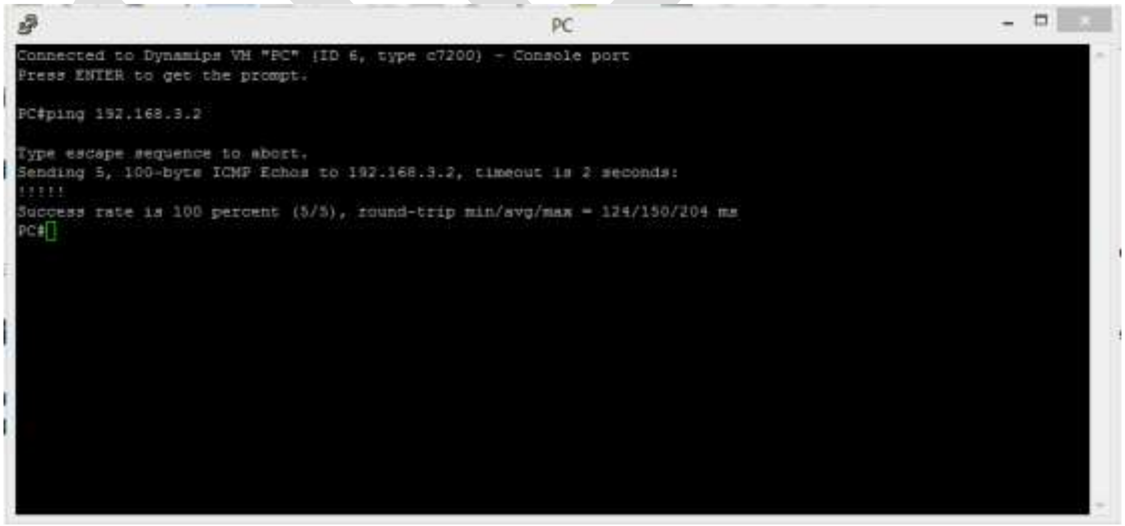
Configuration for router II

```
R2> enable
R2# configured terminal
R2 (config) # interface ATM1/0
R2 (config-if)# no shut down
R2 (config-if)# IP address 192.168.1.2 255.255.255.252
R2 (config-if)# map-group atm-cir-123
R2 (config-if)#atmpvc 1 1 200 aa/5snap
R2 (config-if)# no atmilmi-keepalive
R2 (config-if)# exit
R2 (config)# map-list atm-cir-123
R2 (config)# IP 192.168.1.1 atm-VCI broadcast
R2 (config)# interface Ethernet 2/0
R2 (config-if)# IP address 192.168.3.1 255.255.255.0
R2 (config-if)# no shut down.
```

Switch 1 (sw-1) and switch 2 (sw-2): (sw-1) and (sw-2) in the ATM Network were activated to function as manageable switches. They do not have special configuration in the GNS3 simulator. They simply acted as plug and play switches.

Pinging is a computer-based administrative utility used to test the connectivity of end devices in the network. It can also be used to calculate the transmission time used by a message sent from the source-end device to the destination-end devices.

At the end of the ATM network configuration processes, pinging commands were used to test the ability of the device to terminate the packets in real-time. The pinging commands used for the personal computer, the IP phone and the work-station are presented below: The Pinging commands activated during the transceiver processes are respectively presented as follows: Personal computer (Fig, 2), IP phone (Fig.3) and Work-station (Fig.4).

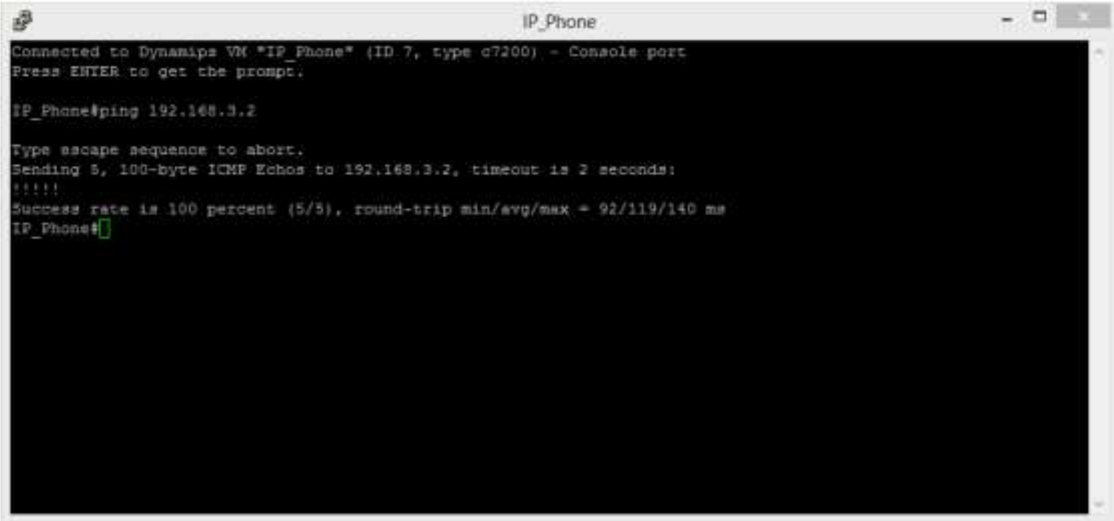


```
Connected to Dynamips VM "PC" (ID 6, type c7200) - Console port
Press ENTER to get the prompt.

PC#ping 192.168.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 124/150/204 ms
PC#
```

FIG. 2: Pinging command for the personal computer

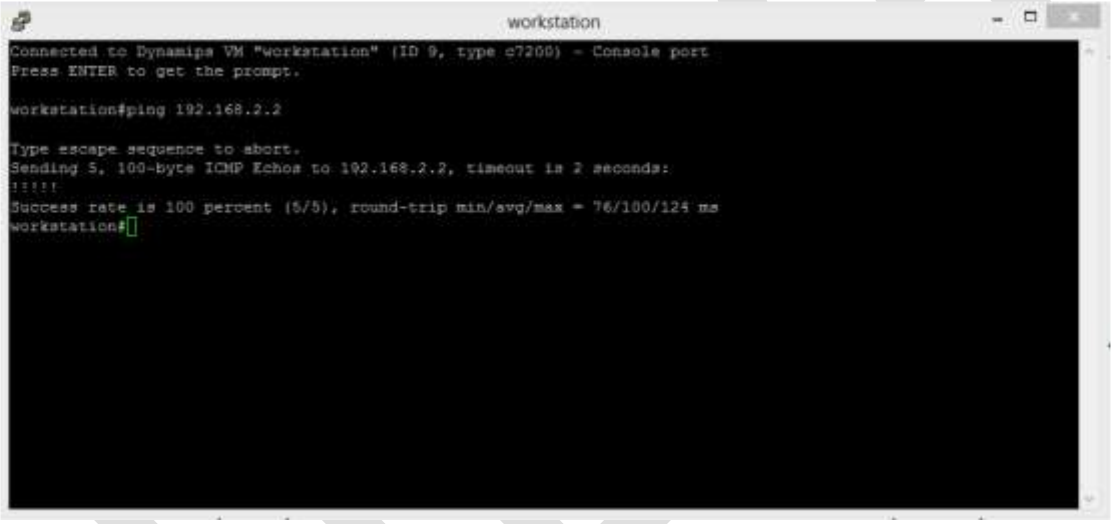


```
Connected to Dynamips VM "IP_Phone" (ID 7, type c7200) - Console port
Press ENTER to get the prompt.

IP_Phone#ping 192.168.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/119/140 ms
IP_Phone#
```

FIG. 3: Pinging command for the IP phone



```
Connected to Dynamips VM "workstation" (ID 9, type c7200) - Console port
Press ENTER to get the prompt.

workstation#ping 192.168.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/100/124 ms
workstation#
```

FIG. 4: Pinging command for the work-station

4. RESULTS AND DISCUSSIONS

4.1 Interpretation of Results

Fig. 5 below shows results obtained after the simulation process. Here, an ATM network was simulated and configured to send information at a speed of 155Mbps.The figure shows two LAN networks: the remote network and the headquarters' network. All the network devices and their IP addresses are also shown. The ATM switch with an IP address 192.168.1.0 connects the two LANs; thereby making the ATM network a WAN. End devices such as personal computers, IP phones, servers and workstations with their various IP addresses were also connected. The switches serve as a link between the end devices and the routers. The routers job is to forward packets from the remote network to the headquarters' network. At the end of the configuration, pinging commands were used to test the connectivity of the devices in the network. Packets were sent successfully from the remote network to the headquarters' network. Table 2 is the presentation made on samples of IP addresses used in configuring the ATM network.

TABLE 2

Samples of IP addresses used in configuring the ATM network

S/N	IP Address	Sample	Remark
1	network address	192.168.1.0	WAN
		192.168.2.0	Remote Network (LAN)
		192.168.3.0	headquarter Network (LAN)
2	Host Address	192.168.1.1	Router 1
		192.168.2.2	Router 2
		192.168.2.1	PC
		192.168.2.2	IP Phone
		192.168.3.1	Server
		192.168.3.2	Work Station
		192.168.3.3	
3	Subnet Mask	255.255.255.0	- LAN
		255.255.255.252	- WAN

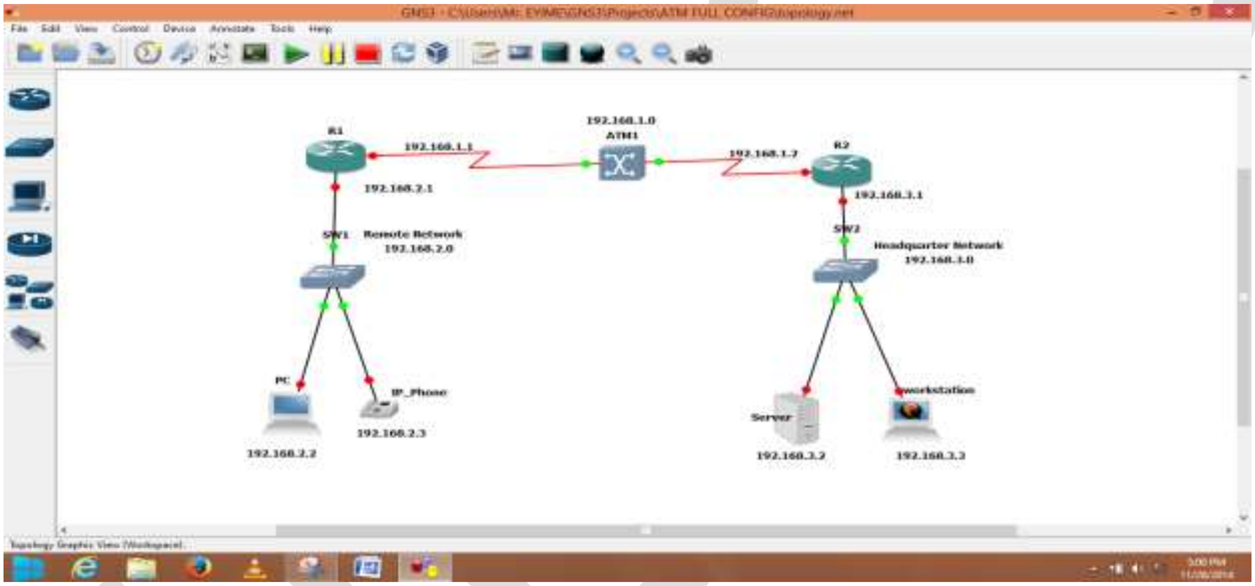
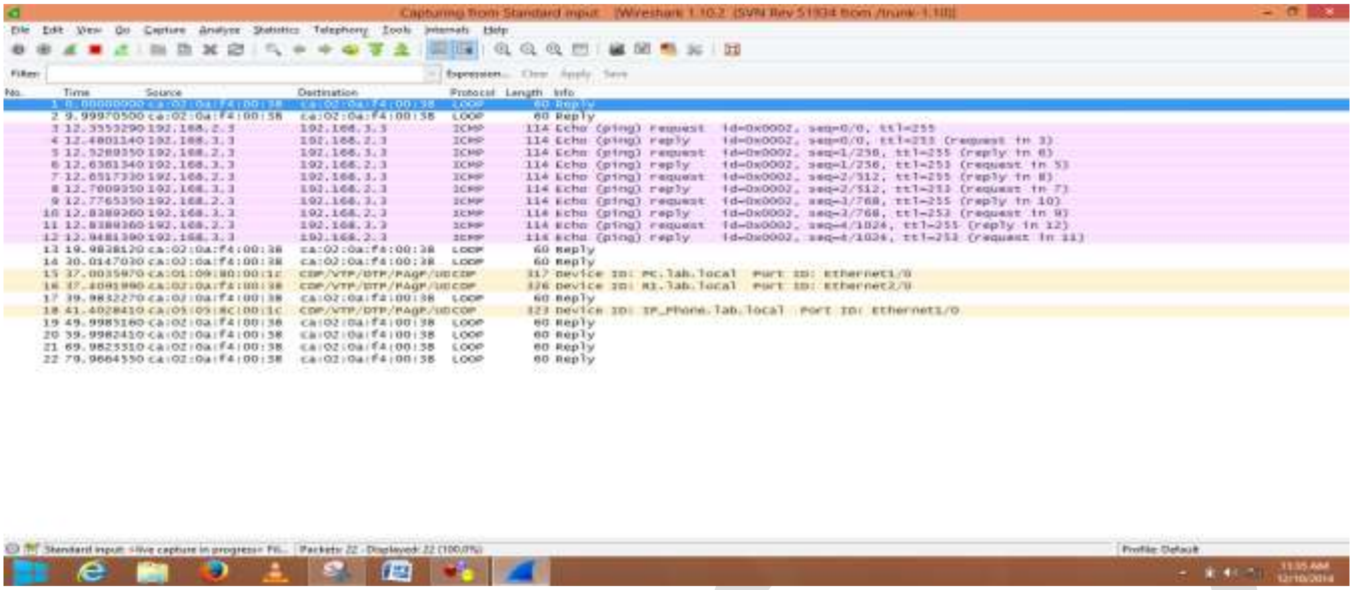


FIG. 5: The ATM network model

4.2 Analysis of Results using Wire Shark

Wire shark is a network packet analyzer. A network packet analyzer is capable of capturing network packets and showing its details as much as possible. Wire shark application helps users to know exactly what is happening inside the network. Wire shark is the best open source packet analyzer used today.

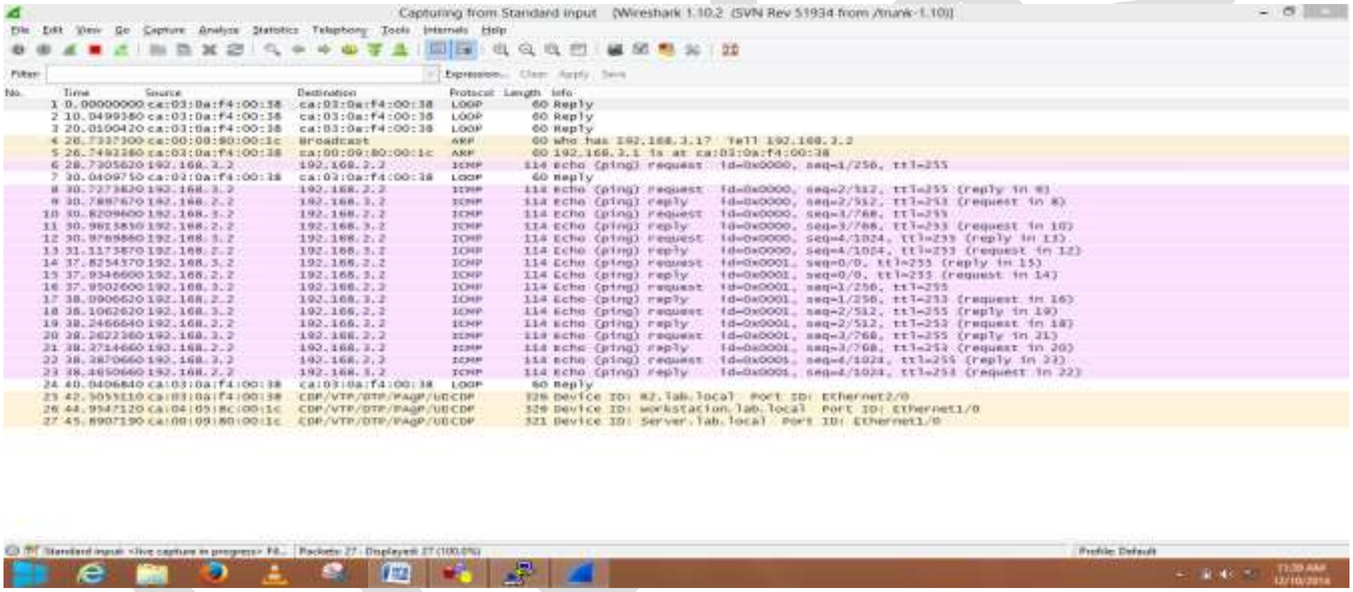
After configuring the simulated network, the packet analyzer (wire shark) was activated to examine the functionality of the network. Key issues were examined through wire-shark application (network administrator) to troubleshoot issues arising from the simulated network, check security issues, debug protocol performance and access the networking protocols. Through activating the wire-shark, the simulated network progressively accessed all the captured line packets, examined and displayed details of these packets, save the captured packets and converted these packets to be accessible through windows. Fig. 6 shows Wire-shark configuration captured at the remote network and Fig. 7 is the configuration of Wire-shark captured at the headquarters' network


Capturing from Standard input [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default

```
No.  Time       Source             Destination         Protocol Length Info
   1 0.00000000 ca:02:0a:f4:00:38  ca:02:0a:f4:00:38   LOOP       60 Reply
   2 9.99970500 ca:02:0a:f4:00:38  ca:02:0a:f4:00:38   LOOP       60 Reply
   3 12.3553290 192.168.2.3        192.168.3.3         ICMP      114 Echo (ping) request  id=0x0002, seq=0/0, ttl=255
   4 12.4801140 192.168.3.3        192.168.2.3         ICMP      114 Echo (ping) reply    id=0x0002, seq=0/0, ttl=253 (request in 3)
   5 12.5289350 192.168.2.3        192.168.3.3         ICMP      114 Echo (ping) request  id=0x0002, seq=1/256, ttl=255 (reply in 6)
   6 12.6361340 192.168.3.3        192.168.2.3         ICMP      114 Echo (ping) reply    id=0x0002, seq=1/256, ttl=253 (request in 5)
   7 12.6517330 192.168.2.3        192.168.3.3         ICMP      114 Echo (ping) request  id=0x0002, seq=2/512, ttl=255 (reply in 8)
   8 12.7009350 192.168.3.3        192.168.2.3         ICMP      114 Echo (ping) reply    id=0x0002, seq=2/512, ttl=253 (request in 7)
   9 12.7765350 192.168.2.3        192.168.3.3         ICMP      114 Echo (ping) request  id=0x0002, seq=3/768, ttl=255 (reply in 10)
  10 12.8289260 192.168.3.3        192.168.2.3         ICMP      114 Echo (ping) reply    id=0x0002, seq=3/768, ttl=253 (request in 9)
  11 12.8389360 192.168.2.3        192.168.3.3         ICMP      114 Echo (ping) request  id=0x0002, seq=4/1024, ttl=255 (reply in 12)
  12 12.9481390 192.168.3.3        192.168.2.3         ICMP      114 Echo (ping) reply    id=0x0002, seq=4/1024, ttl=253 (request in 11)
  13 19.9838120 ca:02:0a:f4:00:38  ca:02:0a:f4:00:38   LOOP       60 Reply
  14 30.0147030 ca:02:0a:f4:00:38  ca:02:0a:f4:00:38   LOOP       60 Reply
  15 37.0035970 ca:01:09:80:00:1c  CDP/VTP/DTP/PAgP/UDCDP        317 Device ID: PC.lab.local  Port ID: Ethernet1/0
  16 37.4091990 ca:02:0a:f4:00:38  CDP/VTP/DTP/PAgP/UDCDP        326 Device ID: R1.lab.local  Port ID: Ethernet2/0
  17 39.9832270 ca:02:0a:f4:00:38  ca:02:0a:f4:00:38   LOOP       60 Reply
  18 41.4028410 ca:05:05:8c:00:1c  CDP/VTP/DTP/PAgP/UDCDP        323 Device ID: IP_Phone.lab.local  Port ID: Ethernet1/0
  19 49.9985160 ca:02:0a:f4:00:38  ca:02:0a:f4:00:38   LOOP       60 Reply
  20 59.9982410 ca:02:0a:f4:00:38  ca:02:0a:f4:00:38   LOOP       60 Reply
  21 69.9823310 ca:02:0a:f4:00:38  ca:02:0a:f4:00:38   LOOP       60 Reply
  22 79.9884350 ca:02:0a:f4:00:38  ca:02:0a:f4:00:38   LOOP       60 Reply

Standard input: <live capture in progress> Fi...   Packets: 22 · Displayed: 22 (100.0%)
```

FIG. 6: Wire shark captured at the remote network


Capturing from Standard input [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default

```
No.  Time       Source             Destination         Protocol Length Info
   1 0.00000000 ca:03:0a:f4:00:38  ca:03:0a:f4:00:38   LOOP       60 Reply
   2 10.0499380 ca:03:0a:f4:00:38  ca:03:0a:f4:00:38   LOOP       60 Reply
   3 20.0100420 ca:03:0a:f4:00:38  ca:03:0a:f4:00:38   LOOP       60 Reply
   4 26.7337300 ca:00:09:80:00:1c  Broadcast           ARP        60 Who has 192.168.3.1?  Tell 192.168.3.2
   5 26.7493380 ca:03:0a:f4:00:38  ca:00:09:80:00:1c   ARP        60 192.168.3.1 is at ca:03:0a:f4:00:38
   6 28.7305620 192.168.3.2        192.168.2.2         ICMP      114 Echo (ping) request  id=0x0000, seq=1/256, ttl=255
   7 30.0409750 ca:03:0a:f4:00:38  ca:03:0a:f4:00:38   LOOP       60 Reply
   8 30.7273820 192.168.3.2        192.168.2.2         ICMP      114 Echo (ping) request  id=0x0000, seq=2/512, ttl=255 (reply in 9)
   9 30.7887670 192.168.2.2        192.168.3.2         ICMP      114 Echo (ping) reply    id=0x0000, seq=2/512, ttl=253 (request in 8)
  10 30.8209600 192.168.3.2        192.168.2.2         ICMP      114 Echo (ping) request  id=0x0000, seq=3/768, ttl=255
  11 30.9813850 192.168.2.2        192.168.3.2         ICMP      114 Echo (ping) reply    id=0x0000, seq=3/768, ttl=253 (request in 10)
  12 30.9789860 192.168.3.2        192.168.2.2         ICMP      114 Echo (ping) request  id=0x0000, seq=4/1024, ttl=255 (reply in 13)
  13 31.1173870 192.168.2.2        192.168.3.2         ICMP      114 Echo (ping) reply    id=0x0000, seq=4/1024, ttl=253 (request in 12)
  14 37.8254370 192.168.3.2        192.168.2.2         ICMP      114 Echo (ping) request  id=0x0001, seq=0/0, ttl=255 (reply in 15)
  15 37.9346600 192.168.2.2        192.168.3.2         ICMP      114 Echo (ping) reply    id=0x0001, seq=0/0, ttl=253 (request in 14)
  16 37.9502600 192.168.3.2        192.168.2.2         ICMP      114 Echo (ping) request  id=0x0001, seq=1/256, ttl=255
  17 38.0906620 192.168.2.2        192.168.3.2         ICMP      114 Echo (ping) reply    id=0x0001, seq=1/256, ttl=253 (request in 16)
  18 38.1062620 192.168.3.2        192.168.2.2         ICMP      114 Echo (ping) request  id=0x0001, seq=2/512, ttl=255 (reply in 19)
  19 38.2466640 192.168.2.2        192.168.3.2         ICMP      114 Echo (ping) reply    id=0x0001, seq=2/512, ttl=253 (request in 18)
  20 38.2622360 192.168.3.2        192.168.2.2         ICMP      114 Echo (ping) request  id=0x0001, seq=3/768, ttl=255 (reply in 21)
  21 38.3714660 192.168.2.2        192.168.3.2         ICMP      114 Echo (ping) reply    id=0x0001, seq=3/768, ttl=253 (request in 20)
  22 38.3870660 192.168.3.2        192.168.2.2         ICMP      114 Echo (ping) request  id=0x0001, seq=4/1024, ttl=255 (reply in 23)
  23 38.4650660 192.168.2.2        192.168.3.2         ICMP      114 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=253 (request in 22)
  24 40.0406840 ca:03:0a:f4:00:38  ca:03:0a:f4:00:38   LOOP       60 Reply
  25 42.5055110 ca:03:0a:f4:00:38  CDP/VTP/DTP/PAgP/UDCDP        326 Device ID: R2.lab.local  Port ID: Ethernet2/0
  26 44.9547120 ca:04:05:8c:00:1c  CDP/VTP/DTP/PAgP/UDCDP        329 Device ID: workstation.lab.local  Port ID: Ethernet1/0
  27 45.8907190 ca:00:09:80:00:1c  CDP/VTP/DTP/PAgP/UDCDP        321 Device ID: Server.lab.local  Port ID: Ethernet1/0

Standard input: <live capture in progress> Fi...   Packets: 27 · Displayed: 27 (100.0%)
```

FIG. 7: Wire-shark captured at the headquarters' network

4.3 Analysis of transfer time using Wire-shark

Many analyses were carried out from the results obtained. However, an example of the analyses carried out is hereby described:

Let the remote network be IP address = 192.168.2.0. Let the headquarter network be IP address = 192.168.3.0. To analyze the time the packet left the remote network, IP address = 192.168.2.0 (click enter)

Press CTRL + ALT + 0 to show the time the packet left the remote network (2014-12-22 12:30:00).

To analyze the time the packet reached the headquarters network, IP address = 192.168.3.0 (click enter)

Press CTRL + ALT + 0 to show the time the packet reached the headquarter network (2014-12-22 12:30:01).

4.4 Threats in ATM network

From the study, it was noted that the ATM networks suffered many threats. Examples of some of these threats and their brief descriptions are as follows:

(a) Eavesdropping threat: Here, the attacker linked up to the transmission medium and gained illegal contact to the information. Eavesdropping is a common threat in networks and has been discovered by this study to also occur under ATM network configuration, in spite of the speed of the network.

(b) Spoofing threat: in this case, the attacker pretended to be another user (third party) in order to access the information of the victim with the intention to destroy them. Spoofing attack has some special ways of manipulating information. It might be that the attacker needed special permission to access the unique environment. The study confirmed that ATM operating under a public network environment is subject to spoofing threat. This was observed when a third network was introduced to serve as the intruding network. In the same vein, since a network is often connected to another network using the Internet, it was not possible to stop the attackers from having access. However, this theory was further put to test by configuring the attacker with a special code not recognized by the network. In the light of this, the attacker, which can be viewed as a virus, was blocked and prevented from having access to other legitimate packages. By so doing, the destructive effect of the virus was reduced, if not eliminated.

(c) Service denial: Since ATM network employs connection-oriented services, a connection, called Virtual circuit (VC) was established and controlled by a set of signals. Virtual circuit was connected by set-up signals and disconnected by drop-party signals. It was observed that the virtual circuit and the network were disconnected when an attacker sent drop party signals to any transitional switch between the Virtual circuit and the network. By regularly sending these signals, the attacker was able to destabilize the links between the users, thereby reducing the Quality of Service (QOS) rendered by the ATM network.

(d) Virtual circuits stealing: When two ATM switches in a network are manipulated, the virtual circuit may be stolen by another customer. For instance, if Virtual circuit-1 and Virtual circuit-2 are two channels activated to pass through switch A and switch B, when user-1 and user-2 were configured to use Virtual circuit-1 and Virtual circuit-2 respectively; if switch A and switch B are synchronized, switch A can switch Virtual circuit-1's cells from switch A to switch B along Virtual circuit-2, while switch B shall switch back this cells to Virtual circuits-1. However, if switch-A and switch-B failed to recognize these changes, then, the status-quo remains and stealing occurs.

(e) Threat to traffic analysis: under this scenario, the illegal user accessed the message, analyzed and interpreted the message of the communicating parties of the Virtual circuits. This was accomplished through illegal entry into the volume and timing of information processed. This threat was possible because the source and destination points were taken from the cell- header and the routing table.

4.5 Security framework for ATM network

Security is one of the major hurdles of network administrators. In system designing, the services' security is usually considered after the network has been designed. This method has consequently proven unsatisfactory. The study made conscious efforts to avoid such traps by making security one major part in the process of designing the ATM network. This was done in order to ensure confidentiality, data integrity, accountability and network availability.

Maintaining confidentiality and data integrity are very important in ATM network security. Under accountability, all the ATM network management activities are accounted for. Each network administrator is expected to be liable for any action taken. Being accountable means validation and non-repudiation. It is also necessary for network operators to manage the network and also account for the services rendered. Availability means that all valid users should be able to get access to the ATM services. No service denial should occur. This is necessary so that the quality of service operation can be guaranteed. In view of the above reasons, the following functions were activated to test the ATM security services:

i. Verifying identities: ATM security services were able to create and authenticate the identity of any performer in the ATM network.
ii. Controlling access and permission: The performers in the ATM network were not able to have access to resources they were not permitted to access.
iii. Protecting the confidentiality: Reserved information was transmitted confidentially.
iv. Protecting the information integrity: The integrity of the reserved packets was guaranteed by the security services introduced.
v. Accountability: The ATM security services were observed to be accountable for every action executed.
vi. Functionalities logging: The ATM security services were able to retrieve data configured for security activities in the network facility with the ability to trace this data to their entry points.
vii. Reporting of alarm: The ATM security service was able to produce alarm information relating to threatening variables and selective security situations. This is a relevant tool to aid maintenance officers.
viii. Auditing: In a situation where there was a bridge in security, the ATM security service was able to evaluate the logged information appropriately.
ix. Recovering Security: When there was a breach in data security, the ATM security service was able to identify the threat and recover the network.

5. CONCLUSION

This study confirmed that ATM is a blend of hardware and software packages that offer high speed networking backbone to end-to-end users with improved quality of service delivery, when compared to other network protocols. It further established Asynchronous Transfer Mode to be more than the basic structure of the Broadband Integrated Services Digital Network (B-ISDN). Rather, it is a shared platform for the transmission and switching of circuit or packet oriented networks. ATM, as Interworking unit presented in this study, has a flexible architecture based on a central processor unit that controls the information flux between the modular interfaces, broads through two independent data buses, and is able to process in real time, the protocol conversion between the involved data formats. This electronic device can be integrated on a wide variety of communication infrastructures and traffic environments: such as interconnection of ATM, ISDN or LAN terminals, locally or remotely, over a public telecommunications network.

REFERENCES:

[1]. Bassey, D. E., Okon, B. E. & FaithPraise, F. O. (2016). Design and Construction of a GSM-Based Multipurpose Measuring Device for UHF Signal Strength Levels. International Journal of Science, Engineering and Technology Research, Vol. 5, Issue 3, pp. 841-846.

[2] Coppo,P., D'Ambrosio,M. & Melen,R (2003):Optimal cost/performance design of ATM switches. IEEE/ACM Transactions on Networking Vol: 1 Iss: 5 p. 566-575,

[3] Bassey, D. E., R. C. Okoro., J. C. Ogbulezie. (2016). Design Considerations of Different Segments of UHF Wireless Network in Cross River State, Nigeria. International Journal of Science, Engineering and Technology Research, Vol. 5, Issue 3, pp. 835-840.

[4] Bassey, D. E., Okon, B. E. & Effiom, E. O. (2016). Pilot Case Study of GSM - Network Load Measurement in Ikeja - Nigeria. International Journal of Science, Engineering and Technology Research, Vol. 5, Issue 3, pp. 824-829.

[5] Bassey, D. E., Ogbulezie, J. C. & Okon, B. E. (2016). Modeling a Low Latency IP Network in Nigeria. International Journal of Science, Engineering and Technology Research, Vol. 5, Issue 3, pp. 830-834.

[6] Bassey, D. E., Okoro, R. C., Okon, B. E. (2016). Modeling of Radio Waves Transmission of Building Located around Niger Delta Urban Microcell Environment Using "Ray Tracing Techniques". International Journal of Science and Research, *Vol.5, Issue 2,* pp. 337-346.

[7] Bassey, D. E., Okoro, R. C., Okon, B. E. (2016). Issues of Variance of Extreme Values in a Heterogenous Teletraffic Environment. International Journal of Science and Research, Vol. 5, Issue 2, pp. 164-169.

[8] Bassey, D. E., Okoro, R. C. & Okon, B. E. (2016). Issues Associated with Decimeter Waves Propagation at 0.6, 1.0 and 2.0 Peak Fresnel Zone Levels. International Journal of Science and Research, Vol. 5, Issue 2, pp. 159-163.

[9] Bassey, D. E., Okoro, R. C., Okon, B. E., & Eyime, E. E. (2016). Broadband – Infrastructural Deficit and ICT Growth Potentials in Cross River State, Nigeria. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol. 4, Issue 5, pages 8465-8476.

[10] Bassey, D. E & Okon, B. E (2015). Comparative Studies between Reduction of Discrete Frequency Ranges and Radiated Sound Levels (A Case Study of 50 kVA Diesel Engine Cooling Fan). International Journal of Technology and Research (IJTNR), Vol. 3, Issue 4, pages 85-92.

[11] Bassey, D. E., Okon, B. E., Faith-Praise, F. O., & Eyime, E. E. (2016). Characterization of Traffic Flow Consumption Pattern and Subscribers' Behaviour. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol. 4, Issue 5, pages 8484-8493.

[12] Bassey, D. E., Okon, B. E. & Effiom, E. O. (2016). 'Broadband Network Penetration and Growth Pattern in North Eastern Part of Nigeria'. International Journal of Scientific & Engineering Research (IJSER), Volume 7, Issue 3, pages 1156-1170.

[13] Bassey, D. E., Okon, B. E. & Umunnah, R. (2016). 'The Security Implications of Virtual Local Area Network (VLAN), Niger Mills, Calabar, Nigeria'. International Journal of Scientific & Engineering Research (IJSER), Volume 7, Issue 3, pages 1187-1194.

[14] Bassey, D. E., Ogbulezie, J. C. & R. Umunnah (2016). Empirical Review of Basic Concepts of Teletraffic Postulates. International Journal of Scientific & Engineering Research, Volume 7, Issue 3, pages 1171-1186.

[15] Bassey, D. E., Akpan, Aniefiok. O. & Udoeno, E. (2016). UHF Wave Propagation Losses Beyond 40 Percent Fresnel Zone Radius in South-South Nigeria. International Journal of Science and Research, Volume 5, Issue 2, pp. 740-745.

[16] Bassey, D. E., Ogbulezie, J. C. & Effiom, E. O. (2016). Local Area Network (LAN) Mock-up and Prevention of Cybernetics Related Crimes in Nigermills Company Using Firewall Security Device. International Journal of Scientific & Engineering Research, Volume 7, Issue 3, pages 1124-1130.

[17] Okon, B. E & Bassey, D. E. (2016). Discrete Frequency Noise Reduction of 100 kVA Diesel Engine Cooling Fan International Journal of Engineering Research and General Science, Volume 4, Issue 4, pages 414-422.

[18] Sexton, M. and Reid, A. (1997): Broadband Networking: ATM, SDH and SONET, Artech HouseInc., Boston, London, ISBN 0-89006-578-0.