HINDUSTHAN COLLEGE OF ENGINEERING AND TECHNOLOGY
Coimbatore 641 032, Tamilnadu, India

Phone: 0422 4242424, website: www.hicet.ac.in

HINDUSTHAN
EDUCATIONAL AND CHARITABLE TRUST
HICET

IT POLICY

TABLE OF CONTENTS

1. Need for IT Policy

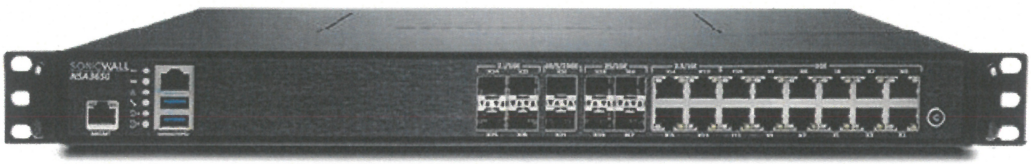
Essentially, the college IT policy exists to maintain, safeguards, and assure the legal and appropriate usage of the institution's information technology infrastructure on campus.

For the usage of various IT resources on campus by students, faculty, staff, management, and visiting guests and Research Fellowship Members an IT Policy is being developed for fair and transparent academic purposes.

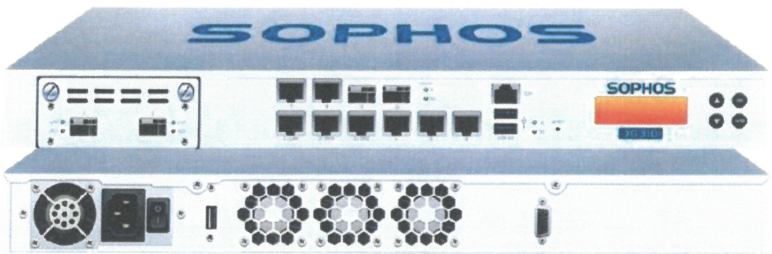
The use of IT resources on campus has increased dramatically over the last decade as a result of regulatory initiatives and academic initiatives.

Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

The Computer Management Department is responsible for the institutes two layer firewall protection, DHCP, VPN, web application servers, and network management.



SONICWALL NSA 4650 FIREWALL



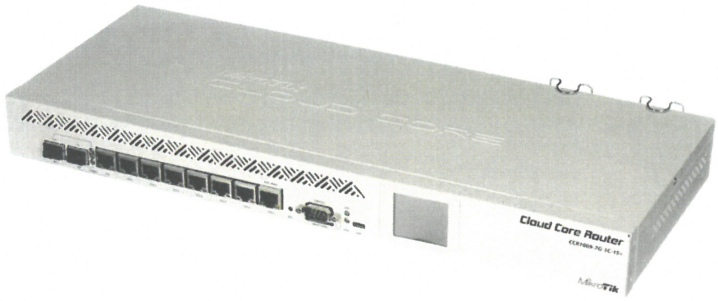
SOPHOS XG 310 FIREWALL

College is getting its Internet bandwidth from Wireline Solutions. Total bandwidth availability from primary in Airtel + fail over in Reliance source with 1 GBPS (leased line 1:1 Ratio) in Fiber/ Wireless AP and Backup of ACT & Cherri net Broadband of 500+175 Mbps.

Now, the College has about 1500 network connections for teaching

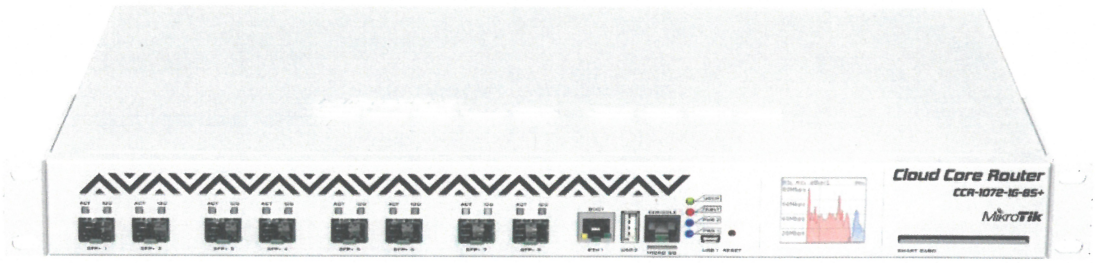
and non– teaching members covering more than eleven buildings across the campus and expected to reach 2000 connections very soon.

Apart from this we have excellent cloud router for backup to handle static IP's, Hotspot and DHCP servers' separately with syslog maintained in separate server.



MIKROTIK CLOUD ROUTER CCR1009-7G-1C-1S+

(7x Gigabit Ethernet, 1x Combo port (SFP or Gigabit Ethernet), 1xSFP+ cage, 9 cores x 1.2GHz CPU, 2GB RAM, LCD panel, Dual Power supplies, Smart Card slot, Router OS L6)



CCR1072-1G-8S+ (1x Gigabit Ethernet, 8xSFP+ cages, LCD, 72 cores x 1GHz CPU, 16GB RAM, up to 120 million packets per second, 80Gbps throughput, Router OS L6)

With the extensive use of the Internet, network performance affected in three ways:

- When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) is a potential bottleneck.
- When users are given free access to the Internet, non-critical downloads may log the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications.
- When computer systems are networked, viruses that get into the LAN,

through Intranet/Internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.

Too many concurrent users, who are on the high speed LANs trying to access Internet resources through a limited bandwidth, definitely create stress on the Internet bandwidth available.

Every download adds to the traffic on the Internet. This adds to costs and after a point, brings down the Quality of Service and Quality of Experience. Hence reducing Internet traffic is the solution.

Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. Others simply attach themselves to files and replicate themselves, taking the network space and slowing down the network.

Containing a virus once it spreads through the network is not an easy job. Plenty of man-hours and possibly data are lost in making the network safe once more. So preventing it at the earliest is crucial. Hence, in order to secure the network, Computer Management Department has been taking appropriate steps by installing firewalls, access **controlling and installing virus software's checking** and content filtering software at the gateway.

All the educational institutions worldwide have IT policies implemented in their respective institutions. Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires. Furthermore, the Guidelines must be followed by all faculty, students, employees, departments, approved visitors/visiting faculty, and those who may be granted authorization to utilize the Institute's information technology infrastructure. Certain infractions of the institute's IT policy by any institute member may result in the institute's administration taking disciplinary action against the offender. Law enforcement officials may become involved if the case concerns unlawful activity.

Applies to

Stake holders on campus or off campus Students

- UG, PG, Research
- Employees (Permanent/ Temporary/ Contractual)
- Faculty
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests

Resources Available in campus

- Network Devices wired/ wireless
- Internet Access (Wired and Wireless)
- Official Websites, web applications
- Official Email services
- Data Storage Server, FTP Server
- Mobile/ Desktop / server computing facility
- Documentation facility (Printers/Scanners/Projectors/smart classes)

2. Vision, Mission and Objectives

IT Vision - To be a globally competitive institution that will endeavor to give all students with the most up-to-date information technological resources as a means of providing high-quality education combined with practical experience.

IT Mission

- To make our institution as an IT enabled Institution.
- To become globally competitive and strategically efficient.
- To make the institution as a sustainable IT resource campus.

Policy Objectives

The objectives of the IT policy are as follows:

- To provide all required IT resources as per the academic programs laid down by UGC, AICTE and affiliated University. Also, introduce new IT technologies which will benefit the students and research staff.
- Create provision for priority up-gradation of the products.
- Create Provision for Annual Maintenance expenses to ensure maximum uptime of the products.
- To ensure that the products are updated and catered 24x7 in the campus or as per the policies lay down by the College Management.

3. IT Hardware/Software Installation Policy

When getting their computers or peripherals installed, the institute network user community should take special steps so that service disruptions due to hardware difficulties cause them the least amount of inconvenience.

Primary User

An individual in whose room the computer is installed and is primarily used by him/her is considered to be "primary" user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

End User Computer Systems

Apart from the user's client PCs, the institute will regard servers that are not directly operated by Computer Management Department to be end-user computers. If no primary user can be identified, the department must take on the end-user obligations. Even if they are registered with the Computer Management Department, computer systems that act as servers and provide services to other users on the Intranet/Internet are still considered "end-user" computers under this policy.

Warranty & Annual Maintenance Contract

Any Department/Cell should obtain computers that come with a 3-year

to 5-years onsite complete warranty. After the warranty period has expired, computers will be maintained on a call basis by the Computer Management Department or by external Service centers. This maintenance should also entail replacing the faulty hardware and checking for major issues.

Network Cable Connection

The connected network cable should be kept away from any electrical or electronic equipment when connecting the computer to the network, since they can interfere with network transmission. Furthermore, the power source from which the computer and its peripherals are connected should not be shared with any other electrical/electronic equipment.

File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

Maintenance of Computer Systems provided by the Institute

For all the computers that were purchased by the institute centrally and distributed by the Computer Management Department will attend the complaints related to any problems of maintenance.

4. Software Installation and Licensing Policy

Individual departments/cells should ensure that all licensed software (operating system, antivirus software, Language **Software's,** and appropriate application software) is installed on required computer systems they acquire.

Operating System and its updating

Individual users should ensure that their operating systems are up to date with the latest service packs/patches available over the Internet. This is very crucial for any machines that run Microsoft Windows (both PCs and Servers). Users who update their operating systems help their computers repair flaws and vulnerabilities in the operating system that Microsoft detects on a regular basis and fixes with patches/service packs.

Antivirus Software and its updating

Anti-virus software should be installed on all computers in the institute, and it should be running at all times. The principal user of a computer system is responsible for ensuring that it adheres to this virus prevention strategy and intrusion prevention. Individual users should ensure that current virus protection software is installed and updated on their computers.

Backups of Data

Individual users should back up their critical data on a regular basis. Virus infections frequently wipe up data on a computer. It may be hard to restore deleted files without appropriate backups. Ideally, the computer's hard disc should be partitioned into many volumes during the OS installation process, such as C, D, and so on.

The operating system and other software should be on the C drive, while the user's data files should be on the other drives (e.g. D, E and G Drive). In the event of a virus, just the C volume is usually corrupted. Only formatting one partition in such a situation will prevent data loss. It is not, however, a fail-safe solution. Apart from that, users should back up their important data on USB Drives, G Drive, FTP Server, File Server, CDs or DVDs.

5. **Network (Intranet & Internet) Use Policy**

The Institute IT Policy governs network connections supplied via an authorized network access link or Controller based Wi-Fi. The Computer Management Department is in charge of the Network's continuing maintenance and support, with the exception of local applications. Problems in the **institute's** network should be bought to the notice of the Computer Management Department.

IP Address Allocation

The Computer Management Department shall assign an IP address to every computer (PC/Server) that will be linked to the institute network. Departments should take a methodical approach in determining the range of IP addresses that will be assigned to each building / VLAN. As a result, every computer connecting to the network from that building will only be assigned an IP address from that pool. Furthermore, each network port in the room where that machine will be attached will have an internal binding with that IP address,

ensuring that no one else uses that IP address without permission from any other place.

DHCP Configuration by Individual Departments / Users

Any computer used as a DHCP server at the end user site (faculty laptops and mobiles) to connect to more nodes through an individual switch/hub and distribute IP addresses (public or private) should be provided at any costs, as it is a clear breach of the institute's IP address allocation policy.

Wireless Local Area Networks

This policy covers all wireless local area networks in a department or hostel. Departments or hostels must also register each wireless access point with the Computer Management Department, providing Point of Contact information, in addition to the policy's requirements.

Wireless local area networks with unfettered access are not permitted in departments or hostels. Authentication or MAC/IP address limitations must be used to limit network access. Encryption is required for both passwords and data.

Wi-Fi registration forms will give to the Staffs to get access to the campus Wi-Fi. Function days the campus Wi-Fi will be open access to all the students and faculty members.

Email Account Use Policy

It is encouraged that all faculty, staff, and students, as well as the Institute's administrators, use the institute's e-mail services for formal Institute contact and for academic and other official reasons, in order to enhance the efficient delivery of essential information with unlimited data storage.

It is critical to keep the e-mail address active by utilizing it on a frequent basis in order to get these alerts. Staff and teachers can access email by going to https://gmail.com and entering their institute domain User ID and password. The institute's email account can be obtained by submitting an application in the specified Performa to the Computer Management Department for email account and default password.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

- The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- Using the facility for illegal/commercial purposes is a direct violation of **the institute's IT policy** and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e- mail messages, generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
- User should not share his/her email account and password with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- Impersonating email account of others will be taken as a serious offence under the institute IT security policy.
- It is ultimately each individual's responsibility to keep their e-mail account free from violations of institute's email usage policy.

6. **Network Maintenance**

Responsibilities of Computer Management Department Campus Network Backbone Operations

- The campus network backbone and its active components are administered, maintained and controlled by Computer Management Department.
- Computer Management Department operates the campus network backbone such that service levels are maintained as required by the Institute Departments, and hostels served by the campus network backbone within the constraints of operational best practices.

Receiving Complaints

- Computer Management Department may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them is having any problems.
- The designated person in Computer Management Department receives complaints from the users of these computer systems and coordinates with the service engineers of the respective brands of the computer systems

(which are in warranty) to resolve the problem within a reasonable time limit. For out of warranty computer systems, problems resolved at Computer Management Department.

- Computer Management Department may receive complaints from the users if any of the users is not able to access network due to a network related problem at the user end. Such complaints may be received generally through phone call.
- The designated person in Computer Management Department receives complaints from the users and coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

Installation of Unauthorized Software

Computer Management Department or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

Campus Network Services Use Agreement

The "Campus Network Services Use Agreement" should be read by all members of the institute who seek network access through the institute campus network backbone. This can be found on the institute web site. All provisions of this policy are considered to be a part of the Agreement. Any Department or individual, who is using the campus network facility, is considered to be accepting the institute IT policy. It is user's responsibility to be aware of the Institute IT policy. Ignorance of existence of institute IT policy is not an excuse for any user's infractions.

Use of IT facilities by the visitors / guests

Use of the computing facilities at Hindusthan College by visitors / guests is subject to the following regulations.

- Computers are primarily intended for academic use. Computer games are not permitted.
- Software maintained on personal computers may not be modified, deleted, moved or copied. Default settings should not be changed.
- User supplied data files should not be stored on the hard drives. You must use your own network drive space, USB flash drive, or CDs for storage of any files you create.
- Making copies of software in violation of U.S. copyright law is forbidden.
- Making copies ofcopyrighted software and/or music CDs is not allowed.
- Use of computers is on a first come/first served basis.
- If no computer is available, you should give your name and computer preference (Windows or Mac) to the Supervisor on duty. You must be present when your turn comes or you will lose it.
- Computers left unattended for more than twenty minutes are considered available for use, even if someone has left work in progress. However, you should contact the technical team on duty before taking an unattended machine that appears to be in use so that applications can be shut down and data saved.
- Food and alcoholic drinks are not permitted in the computing facilities.
- Smoking and use of tobacco products are not permitted

Responsibilities of the Administrative Department

Computer Management Department needs latest information from the different Administrative Department for providing network and other IT facilities to the new members of the institute and for withdrawal of these facilities from those who are leaving the institute, and also for keeping the Hindusthan web site up-to-date in respect of its contents.

The information that is required could be broadly of the following nature:

- Information about New Appointments.
- Information about Termination of Services.
- Information of New Enrolment.

- Information on Important Events/ Achievements.
- Information on different Rules, Procedures, and Facilities.

Guidelines for Those Running Application or Information Servers

Departments may run an application server. They are responsible for maintaining their own servers.

- Obtain an IP address from Computer Management Department to be used on the server
- Get the host name of the server entered in the IP Address resolution.
- Make sure that only the services that are essential for running the server for the purpose it is intended for should be enabled on the server.
- Make sure that the server is protected adequately against virus attacks and intrusions, by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall, anti-spam etc.
- Operating System and the other security software should be periodically updated.

Guidelines for Desktop Users

- Due to the increase in hacker activity on campus, Institute IT Policy has put together recommendations to strengthen desktop security.
- The password should be difficult to break.
- The guest account should be disabled.
- In addition to the above suggestions, Computer Management Department recommends a regular backup strategy. It should be noted that even with all the procedures listed above; there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

The Cyber security concerns are addressed by the institution as below.

Video Surveillance Policy

Fixed position cameras, monitors, digital video recorders, storage, and public information signs are all part of the system.

Cameras will be placed in strategic locations around campus, primarily at site and building entrances and exits. There will be no cameras hidden from view,

and none will be able to focus on the frontages or back regions of private residences.

Signs will be clearly displayed at strategic locations across the campus, as well as at the entrance and departure points, to alert staff, students, visitors, and members of the public to the presence of a **CCTV (NVR) camera's installation.** Although every effort has been taken to ensure that the system is as successful as possible, it is impossible to guarantee that the system will identify every occurrence that occurs within the coverage area.

Web Application's content Filtered by Firewall's

Application	**Management**	**Staff**	**Student**	**Guest**
Captive portal Session	2 concurrent sessions /user			
Application Update	Allow	Allow	Time Based	Time Based
Sites Blocked	Porn, torrents, Proxy & Hacking, Gambling, Marijuana, Criminal Activity			
YouTube	Allow	Allow	Time based	Allow
What's App	Allow	Allow	Time based	Allow
Face book	Allow	Allow	Time based	Allow
Skype or Video calling	Allow	Allow	Time based	Allow
Entertainment	Deny	Deny	Function time	Allow
TV news Channel	Allow	Allow	Time based	Allow
Online Games	Deny	Deny	Deny	Deny
Windows Update	Allow	Allow	Allow	Allow

Default Block Category in Firewall

Online Games, Weapon, Phishing and fraud, Militancy and Extremist, Gambling, Pro-Suicide and self- Harm, Criminal Activity, Marijuana, Intellectual Piracy, Hunting and Fishing, Legal highs, Controlled substances, Anonymizers, Sexually Explicit, Nudity, Advertisement and Social Networks.

APPENDIX I

Campus Network Services Use Agreement

Before applying for a user account/email account, please read the following relevant policies. You agree to follow Hindusthan's IT policies and standards by signing the application form for a Net Access ID (user account)/email account. If you do not follow these policies, your account and IP address may be terminated. It is merely a synopsis of the institute's key IT policies. The detailed paper can be downloaded from the website and numerous intranet servers by the user. A Net Access ID is a login and password combination that allows you to access Institute computer systems, services, campus networks, and the internet.

Accounts and Passwords

If a student, staff member, or faculty member leaves the Institute, their Net Access ID, email address, and associated files will be erased.

No User will be authorized to have more than one Net Access ID at a time, with the exception of faculty or heads who have several portfolios and are entitled to a Net Access ID for each portfolio's functions.

Limitations on the use of resources

Computer Management Department retains the right, on behalf of the Institute, to terminate the Net Access ID of any user who is judged to be consuming excessive quantities of storage space or whose activities otherwise restrict the use of computer resources by other users.

Data Backup, Security, and Disclaimer

Computer Management Department will not be liable for any data loss or corruption on an individual user's computer as a result of the user's use and/or misuse of his or her computing resources (hardware or software), or for any damage that may result from the advice or actions of a Computer Management Department staff member while assisting the user in resolving their network/computer related problems. Despite Computer Management Department's best efforts to ensure data integrity, security, and privacy, the User

is solely responsible for backing up files in the allocated Net Access ID, storage space, or email account. Furthermore, Computer Management Department provides no assurances about a user's security or privacy.

APPENDIX II

HINDUSTHAN COLLEGE OF ENGINEERING AND TECHNOLOGY

Computer Management Department

Requisition Form for Staff E-Mail Account

1. Full Name: _____

(First Name) (Middle Name) (Last Name)

2. Designation: _____

3. Department: _____

4. Mobile No: _____

5. Existing Mail Id: _____

6. Purpose:_____

Date: Signature of Applicant:

.....

Computer Management Department Use only

The following email ID is created for Prof. /Dr. /Mr. /Ms. _____

_____on@*hindusthan.net / hicet.ac.in*

Signature on Behalf of In Charge,
Computer Management Department

APPENDIX III

HINDUSTHAN COLLEGE OF ENGINEERING AND TECHNOLOGY

Computer Management Department

Requisition Form for Staff Wi-Fi Registration form

1. Full Name: _____

   (First Name) (Middle Name) (Last Name)

2. Designation: _____

3. Department: _____

4. Mobile No: _____

5. Mail Id: _____

6. Hotspot User Name and Password:_____/_____

7. MAC Address : _____

8. Laptop Brand / Model : _____

Date: Signature of Applicant:

.....

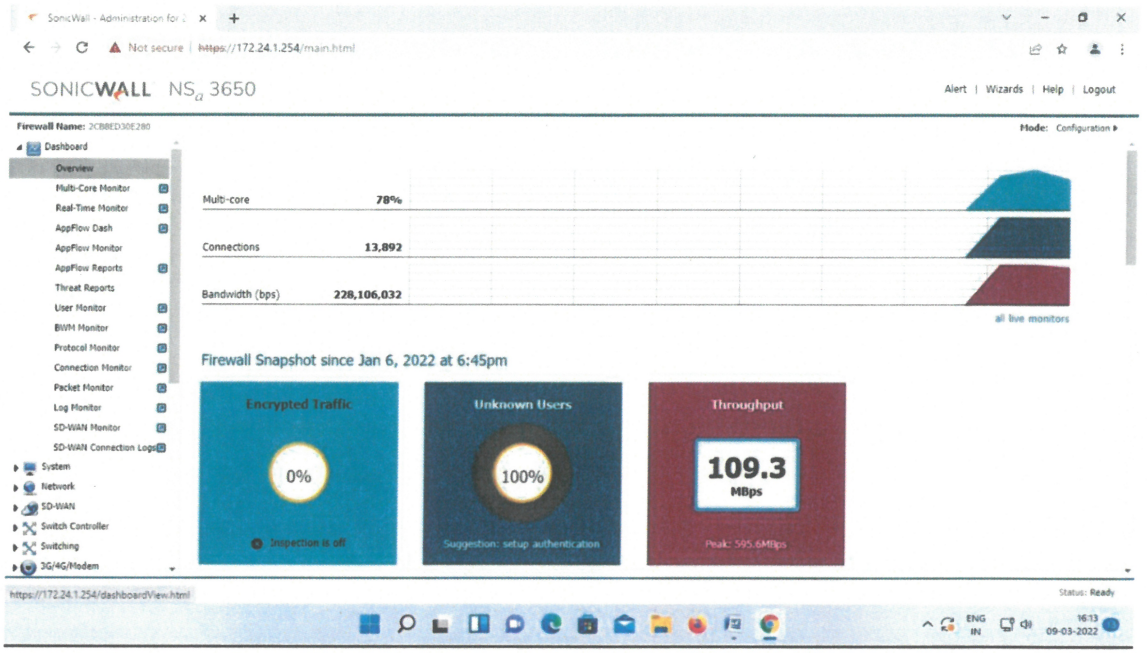
Computer Management Department Use only

The following Hot spot ID is created for Prof. /Dr. /Mr. /Ms. _____

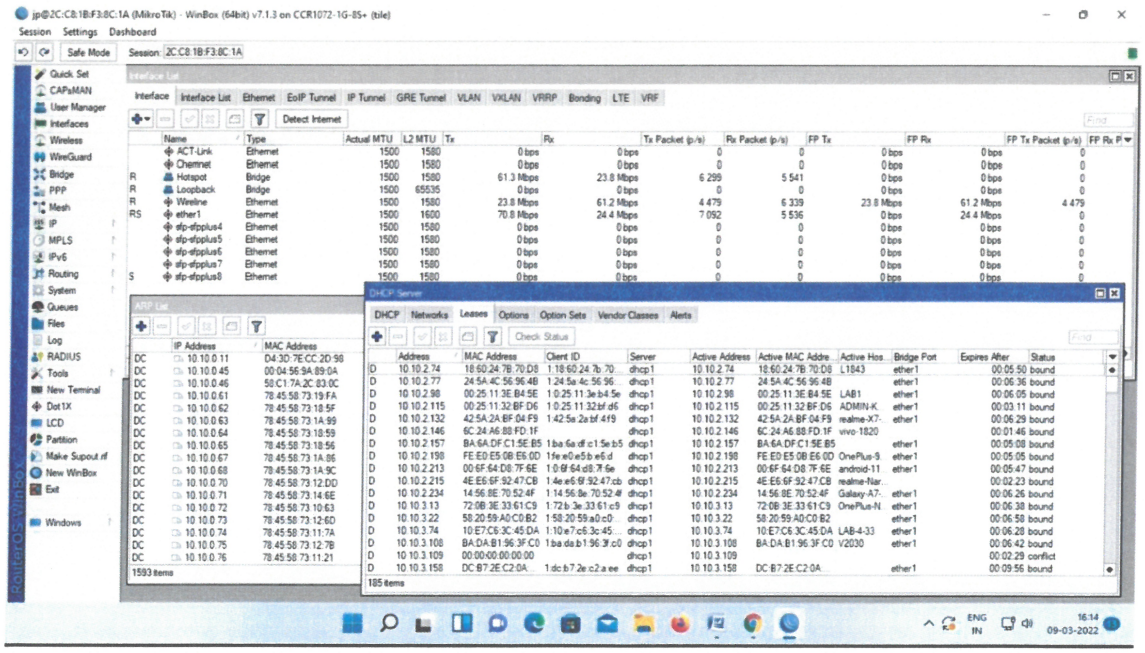
Signature on Behalf of In Charge,
Computer Management Department

SCREENSHOTS

FIREWALL



MIKROTIK CCR1071 CLOUD ROUTER



BANDWIDTH GRAPH

Traffic Analysis for Hindusthan College of Engineering and Technology

System: Wireline Solution India Pvt Ltd-NOC

Maintainer: Wireline Solution India Pvt Ltd,

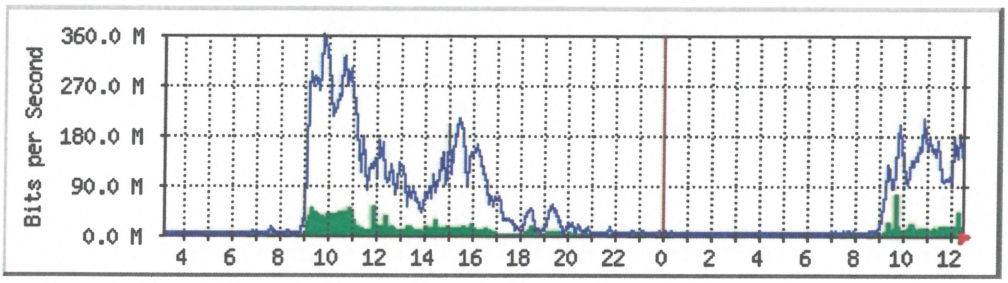
CoimbatoreDescription: Hindusthan-Engg

Port@Router: xe-2/0/0.59 Max Speed: 512 MBytes/s

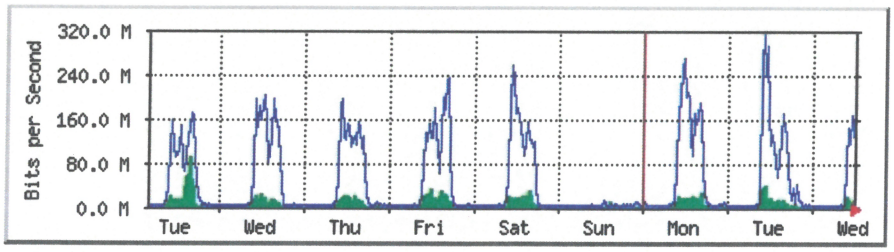
Ip: 121.200.53.160/28

The statistics were last updated **Wednesday, 27 July 2022 at 12:31**,at which time **'Wireline-CBE'** had been up for **361 days,11:42:34**.

`Daily' Graph (5 Minute Average)



	Max	Average	Current
In	75.0 Mb/s (0.7%)	6279.4 kb/s (0.1%)	12.2 Mb/s (0.1%)
Out	357.7 Mb/s (3.6%)	53.8 Mb/s (0.5%)	123.6 Mb/s (1.2%)



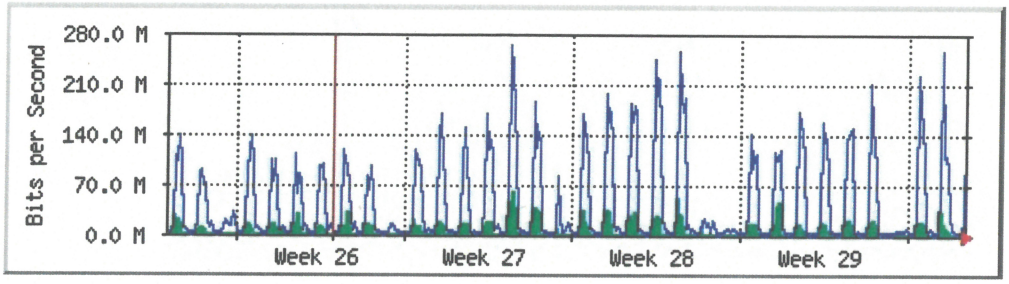
`Weekly' Graph (30 Minute Average)

	Max	Average	Current
In	91.4 Mb/s (0.9%)	5631.8 kb/s (0.1%)	14.9 Mb/s (0.1%)
Out	316.7 Mb/s	43.8 Mb/s (0.4%)	98.6 Mb/s

(3.2%) (1.0%)

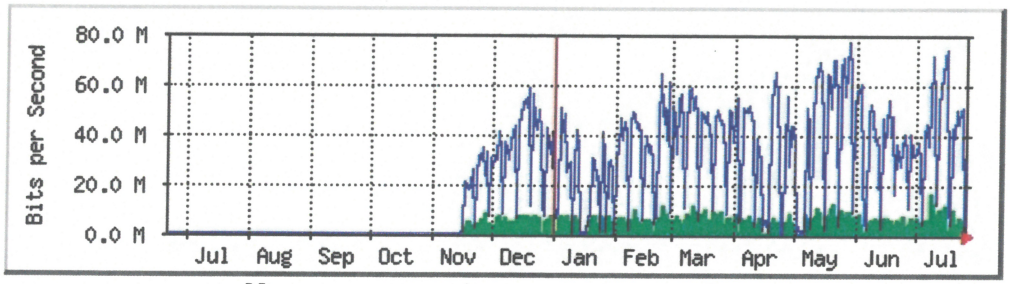
`Monthly' Graph (2 Hour Average)

usage.wls.net.in/HCET 1/2



	Max	Average	Current
In	61.0 Mb/s (0.6%)	6003.8 kb/s (0.1%)	13.8 Mb/s (0.1%)
Out	262.4 Mb/s (2.6%)	39.7 Mb/s (0.4%)	143.8 Mb/s (1.4%)

`Yearly' Graph (1 Day Average)



	Max	Average	Current
In	16.2 Mb/s (0.2%)	5169.7 kb/s (0.1%)	6366.2 kb/s (0.1%)
Out	76.2 Mb/s (0.8%)	34.6 Mb/s (0.3%)	58.2 Mb/s (0.6%)

GREEN ### Incoming Traffic in Bits per Second

BLUE ### Outgoing Traffic in Bits per Second

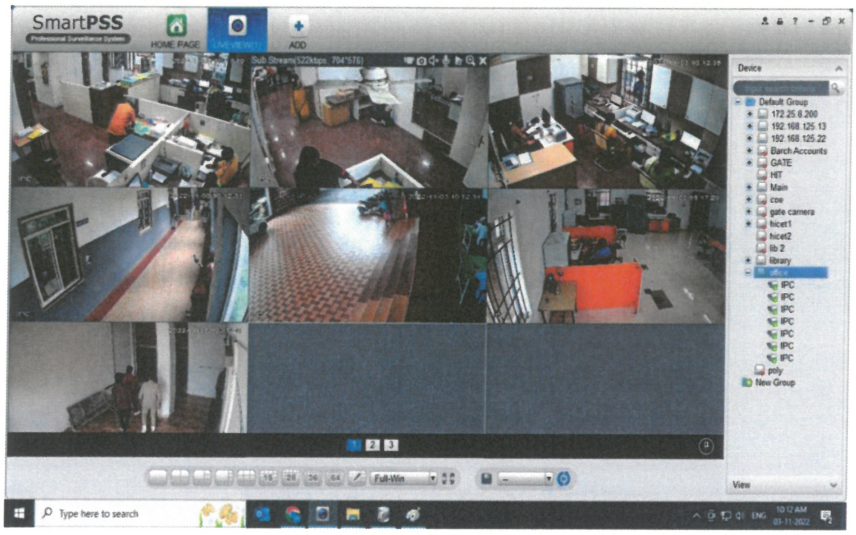
MRTG MULTI ROUTER TRAFFIC GRAPHER

2.17.4 Tobias Oetiker <tobi@oetiker.ch>and Dave Rand <dlr@bungi.com>

SURVEILLANCE FOOTAGE

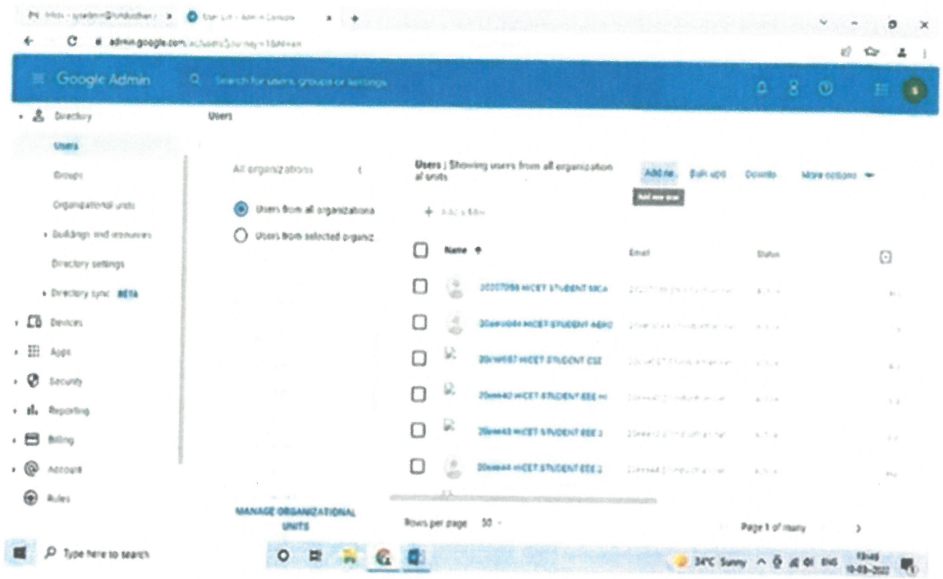
Mani Office 1

Mani Office 2

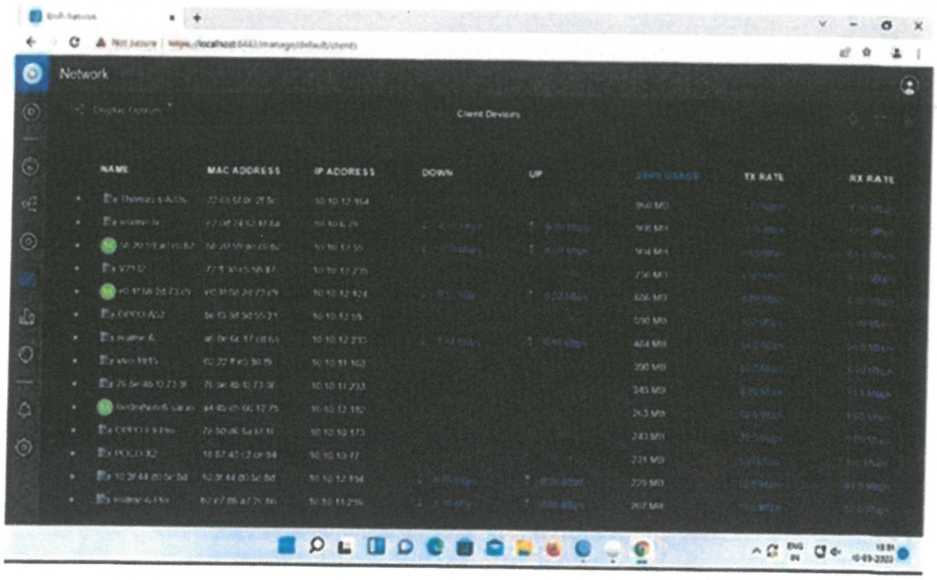


Library

EMAIL REGISTRATION:



WIFI USERS UBIQUTI CONTROLLER



PRINCIPAL
Hindusthan College of Engineering & Technology
COIMBATORE - 641 032

HINDUSTHAN COLLEGE OF ENGG & TECH ★ CBE-32 ★