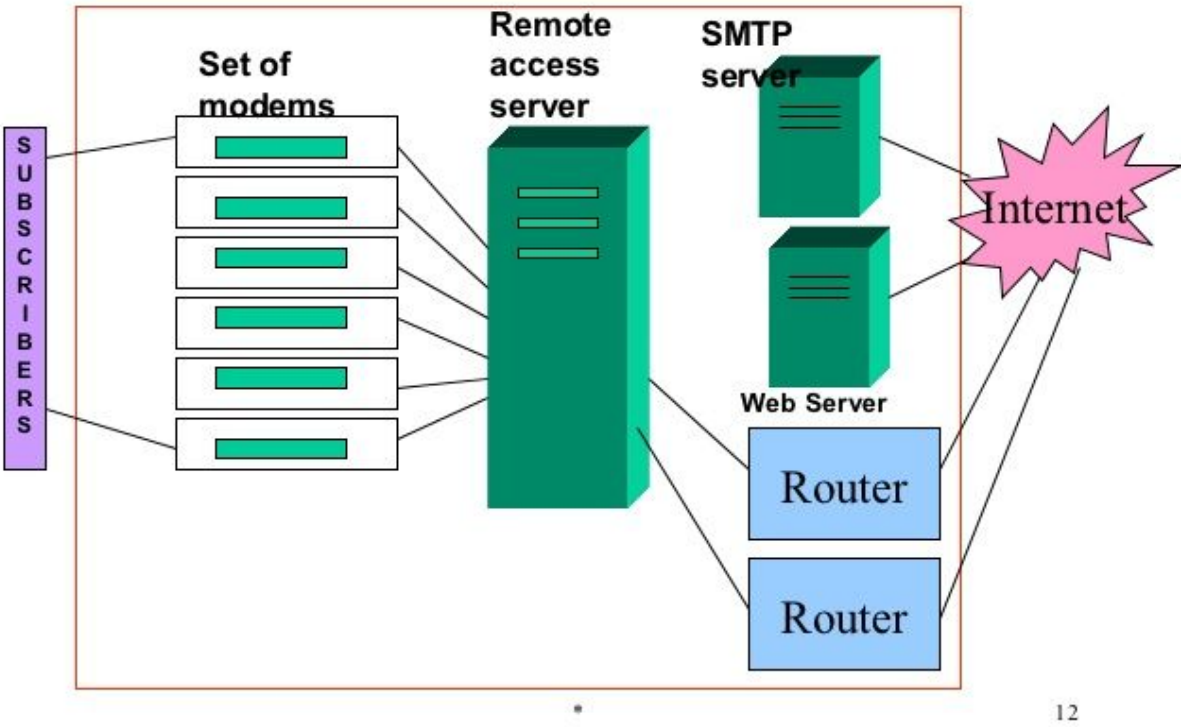
Fig.3.Internal Architecture of ISP



An ISP provides Internet services to business and residential subscribers, also referred to as users. ISPs provide basic services such as email, web hosting, and news. Also, ISPs offer value-added services such as calendars, address books, search engines, chat rooms, instant messages, etc.

An ISP architect defines the overall structure, called the architecture, that sets forth structuring principles and patterns for an ISP's infrastructure, services, network, customer care system, and so on.

The architecture sets system-wide constraints that must be adhered to by each portion of the subsequent design. Within the architecture, the architect identifies major components and their interrelationships. An ISP architect defines how:

Overall processing should be decomposed into components

Major components should be organized and well integrated

Developing an ISP architecture is important because it becomes the fundamental organization of a system embodied in its components, their relationships to each other and to the environment, and the principles guiding an architecture's design and evolution.

CONTENT MIRRORING

A mirror site is a website or set of files on a computer server that has been copied to another computer server so that the site or files are available from more than one place. A mirror site has its own URL, but is otherwise identical to the principal site. Load-balancing devices allow high-volume sites to scale easily, dividing the work between multiple mirror sites.

A mirror site is usually updated frequently to ensure it reflects the contents of the original site. In some cases, the original site may arrange for a mirror site at a larger location with a higher speed connection and, perhaps, a closer proximity to a large audience.

If the original site generates too much traffic, a mirror site can ensure better availability of the website or files. For websites that offer copies or updates of widely used software, a mirror site allows the site to handle larger demands and enables the downloaded files to arrive more quickly. Microsoft, Sun Microsystems and other companies have mirror sites from which their browser software can be downloaded.

Mirror sites are used to make site access faster when the original site may be geographically distant from those accessing it. A mirrored web server is often located on a different continent from the principal site, allowing users close to the mirror site to get faster and more reliable access.

DNS

The Domain Name System (DNS) associates various sorts of information with domain names; most importantly, it serves as the “phone book” for the Internet by translating human-readable computer hostnames, e.g. http://www.example.com, into the IP addresses, e.g. 208.77.188.166, that networking equipment needs to deliver information. It also stores other information such as the list of mail exchange servers that accept email for a given domain. In providing a worldwide keyword-based redirection service, the Domain Name System is an essential component of contemporary Internet use.

The most basic task of DNS is to translate hostnames to IP addresses. In very simple terms, it can be compared to a phone book. DNS also has other important uses.

Above all, DNS makes it possible to assign Internet names to organizations (or concerns they represent), independently of the physical routing hierarchy represented by the numerical IP address. Because of this, hyperlinks and Internet contact information can remain the same, whatever the current IP routing arrangements may be, and can take a human-readable form (such as “example.com”), which is easier to remember than the IP address 208.77.188.166.

How Resolve Mode Works:

- Steps in the DNS resolution process.
- Webtrends makes call to DNS server to resolve IP addresses.

- DNS server makes attempt to translate IP address to DNS entry.
- DNS server returns domain name to Webtrends.
- Webtrends takes domain name and checks it against the company database (company.big) or GeoTrends database.
- Company database or GeoTrends database returns geographical information.

WEB

Web is the common name for the World Wide Web, a subset of the Internet consisting of the pages that can be accessed by a Web browser. Many people assume that the Web is the same as the Internet, and use these terms interchangeably. However, the term Internet actually refers to the global network of servers that makes the information sharing that happens over the Web possible.

Web pages are formatted in a language called Hypertext Markup Language (HTML). It this language that allows users to click through pages on the Web via links. The Web uses HTTP protocol to transmit data and share information. Browsers such as Internet Explorer, Google Chrome or Mozilla Firefox are used to access Web documents, or Web pages, which are connected via links.

MAIL

Electronic mail (email) is a digital mechanism for exchanging messages through Internet or intranet communication platforms.

Email messages are relayed through email servers, which are provided by all Internet service providers (ISP).

Emails are transmitted between two dedicated server folders: sender and recipient. A sender saves, sends or forwards email messages, whereas a recipient reads or downloads emails by accessing an email server.

Email messages are comprised of three components, as follows:

- Message envelope: Describes the email's electronic format
- Message header: Includes sender/recipient information and email subject line
- Message body: Includes text, image and file attachments

PROXY

A proxy server, also known as a "proxy" or "application-level gateway", is a computer that acts as a gateway between a local network (e.g., all the computers at one company or in one building) and a larger-scale network such as the Internet. Proxy servers provide increased performance and security.

A proxy server works by intercepting connections between sender and receiver. All incoming data enters through one port and is forwarded to the rest of the network via another port. By blocking direct access between two networks, proxy servers make it much more difficult for hackers to get internal addresses and details of a private network.Proxies may also cache web pages. Each time an internal user requests a URL from outside, a temporary copy is stored locally. The next time an internal user requests the same URL, the proxy can serve the local copy instead of retrieving the original across the network, improving performance.

NTP

Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network. It belongs to and is one of the oldest parts of the TCP/IP protocol suite. The term NTP applies to both the protocol and the client-server programs that run on computers.

NTP, which was developed by David Mills at the University of Delaware in 1981, is designed to be highly fault-tolerant and scalable.

How does NTP work?

The NTP client initiates a time-request exchange with the NTP server. As a result of this exchange, the client is able to calculate the link delay and its local offset, and adjust its local clock to match the clock at the server's computer. As a rule, six exchanges over a period of about five to 10 minutes are required to initially set the clock.

Once synchronized, the client updates the clock about once every 10 minutes, usually requiring only a single message exchange. In addition to client-server synchronization. This transaction occurs via the User Datagram Protocol on port 123. NTP also supports broadcast synchronization of peer computer clocks.

FIREWALL

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

A firewall acts as a barrier between a trusted network and and an untrusted network. A firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network is defined in the firewall policy; all other traffic is denied.

TYPES OF FIREWALL

1.Packet firewalls

The earliest firewalls functioned as packet filters, inspecting the packets that are transferred between computers on the Internet. When a packet passes through a packet-filter firewall, its source and destination address, protocol, and destination port number are checked against the firewall's rule set. Any packets that aren't specifically allowed onto the network are dropped (i.e., not forwarded to their destination). For example, if a firewall is configured with a rule to block Telnet access, then the firewall will drop packets destined for TCP port number 23, the port where a Telnet server application would be listening.

Packet-filter firewalls work mainly on the first three layers of the OSI reference model (physical, data-link and network), although the transport layer is used to obtain the source and destination port numbers. While generally fast and efficient, they have no ability to tell whether a packet is part of an existing stream of traffic. Because they treat each packet in isolation, this makes them vulnerable to spoofing attacks and also limits their ability to make more complex decisions based on what stage communications between hosts are at.

2.Stateful firewalls

In order to recognize a packet's connection state, a firewall needs to record all connections passing through it to ensure it has enough information to assess whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection. This is what's called stateful packet inspection.
This additional information can be used to grant or reject access based on the packet's history in the state table, and to speed up packet processing; that way, packets that are part of an existing connection based on the firewall's state table can be allowed through without further analysis. If a packet does not match an existing connection, it's evaluated according to the rule set for new connections.

3.Application-layer firewalls

As attacks against Web servers became more common, so too did the need for a firewall that could protect servers and the applications running on them, not merely the network resources behind them. Application-layer firewall technology first emerged in 1999, enabling firewalls to inspect and filter packets on any OSI layer up to the application layer.

The key benefit of application-layer filtering is the ability to block specific content, such as known malware or certain websites, and recognize when certain applications and protocols -- such as HTTP, FTP and DNS -- are being misused.

Firewall technology is now incorporated into a variety of devices; many routers that pass data between networks contain firewall components and most home computer operating systems include software-based firewalls. Many hardware-based firewalls also provide additional functionality like basic routing to the internal network they protect.

4.Proxy firewalls

Firewall proxy servers also operate at the firewall's application layer, acting as an intermediary for requests from one network to another for a specific network application. A proxy firewall prevents direct connections between either sides of the firewall; both sides are forced to conduct the session through the proxy, which can block or allow traffic based on its rule set. A proxy service must be run for each type of Internet application the firewall will support, such as an HTTP proxy for Web services.

Firewall Uses:

1. It restricts and manages traffic according to the user specifications
2. Blocks the view of any unnecessary websites
3. Restricts access according to the needs of the organization
4. Keeps a check on the incoming and outgoing traffic
5. Gives you a proper report on the network traffic as and when required

UTM

UNIFIED THREAT MANAGEMENT

Unified threat management (UTM) is an approach to security management that allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console.

UTM is an information security term that refers to a single security solution, and usually a single security appliance, that provides multiple security functions at a single point on the network. A UTM appliance will usually include functions such as: antivirus, anti-spyware, anti-spam, network firewalling,

intrusion detection and prevention, content filtering and leak prevention. Some units also provide services such as remote routing, network address translation (NAT), and virtual private network (VPN) support. The allure of the solution is based on simplicity, so organizations that may have had individual vendors or appliances for each separate security task can now have them all under one vendor umbrella, supported by one IT team or segment, and run through one console.
The principal advantage of a UTM product is its ability to reduce complexity. The principal disadvantage is that a UTM appliance can become a single point of failure.

How UTM Appliances Block a Computer Virus ?

Unified threat management appliances have gained traction in the industry due to the emergence of blended threats, which are combinations of different types of malware and attacks that target separate parts of the network simultaneously. Preventing these types of attacks can be difficult when using separate appliances and vendors for each specific security task, as each aspect has to be managed and updated individually in order to remain current in the face of the latest forms of malware and cybercrime. By creating a single point of defense and providing a single console, UTM solutions make dealing with varied threats much easier.

While unified threat management solutions do solve some network security issues, they aren't without some drawbacks, with the biggest one being that the single point of defense that an UTM appliance provides also creates a single point of failure. Because of this, many organizations choose to supplement their UTM device with a second software-based perimeter to stop any malware that got through or around the UTM firewall.

Network Monitoring techniques

2.1 **Simple Network Management Protocol (SNMP)**
SNMP is a network management protocol that is used for exchanging information between hosts in a network that includes network monitoring software. This is the most widely used protocol for management and monitoring of the network and includes the below components:
Managed device: The node in the network that supports SNMP and access to specific information.
Managed device: The node in the network that supports SNMP and access to specific information.

Agent: software that is part of the monitored device. An agent has access to the MIB (management information database) of the device and allows NMS systems to read

and write to the MIB.

Network Management System (NMS): An application on a system that monitors and controls the managed devices through the agent using SNMP commands. SNMP data is collected or sent to a managed device, either by polling or using traps. Traps allow an agent to send information to an NMS about events on the device.

The MIB holds information about the structure of the data on a device for management. The MIBs contain OID (object identifiers) which is the actual identifier for the variable to be read from the device or set on the device.

WLAN SECURITY ISSUES

Wireless local are network security (WLAN security) is a security system designed to protect networks from the security breaches to which wireless transmissions are susceptible. This type of security is necessary because WLAN signals have no physical boundary limitations, and are prone to illegitimate access over network resources, resulting in the vulnerability of private and confidential data. Network operations and availability can also be compromised in case of a WLAN security breech. To address these issues, various authentication, encryption, invisibility and other administrative controlling techniques are used in WLANs. Business and corporate WLANs in particular require adequate security measures to detect, prevent and block piggybackers, eavesdroppers and other intruders.

Security has remained a major concern in WLANs around the globe. While wireless networks provide convenience and flexibility, they also increase network vulnerability. Security threats such as unauthorized access, denial of service attacks, IP and MAC spoofing, session hijacking and eavesdropping can all be problems for WLANs. To counter these threats, various standard authentication and encryption techniques are combined with other access control mechanisms.

IP SPOOFING

IP spoofing is the crafting of Internet Protocol (IP) packets with a source IP address that has been modified to impersonate another computer system, or to hide the identity of the sender, or both. In IP spoofing, the header field for the source IP address contains an address that is different from the actual source IP address.

IP spoofing is a technique often used by hackers to launch distributed denial-of-service (DDoS) attacks and man-in-the-middle (MITM) attacks against targeted devices or the surrounding infrastructures. The goal of the DDoS attack is to overwhelm a target with traffic while hiding the identity of the malicious source, preventing mitigation efforts.

Using spoofed IP addresses can give attackers the ability to:

- avoid being discovered and implicated by the authorities as well as forensic cyberinvestigators;
- prevent targeted devices from alerting about attacks in which they are unwitting and unwilling participants; and
- bypass security scripts, devices and services that attempt to mitigate DDoS attacks by blacklisting IP addresses known to be sources of malicious traffic.

NETWORK MONITORING

1. Overview:
A network is a collection of devices that are connected and can communicate with one another over a common transport or communication protocol. Here communication can refer to the transfer of data among users or instructions between nodes in the network, such as computers, mobile devices, output devices, management elements, servers, routing and switching devices, etc.

Networks can be categorized based on the geo area they span as LAN, WAN, or Internet. Further, the design or topology of a network too can differ based on user and organizational requirements, such as star, ring, bus, mesh, etc. Whatever be the design or the topology, every network follows a reference design as described in the OSI model for data transmission and communication. Open System Interconnection (OSI) is a reference model for a network and describes how information from an application installed on a device or system moves through various nodes in the network to another device within the same network or to an external network. There are many components that make a network and enables communication between various nodes, such as network addresses, data transport & communication protocols, and methods used for transfer of packets between nodes within the same network or different networks. Below are some of the basic components that are part of every computer network and these also are the vectors that form the essentials of network monitoring.

a. IP address and subnetting

An IP address is the reference label assigned to each node in a network and is used by other nodes for location and communication. Further, IP addresses are binary numbers, but are stored in human readable format, either as an IPv4 address or IPv6 address. The elements with an IP address that make up a network can be divided into different sub networks based on the device type, location, access, etc. The devices in the same subnet all have a common network prefix defined in its IP address.

b. Switching and Routing
Switching refers to the process in which data is divided into smaller packets before they are sent and transported over the network. Routing is the act of finding a path for the packets that form data to traverse from a source node in one network to a destination node in a different network.

c. Domain Name System (DNS)
Each element in a network, in addition to an IP address, can also have a reference name. This allows a user to communicate with a resource using an easy to remember alphabetical name rather than a difficult to remember IP address. DNS maps the name of a resource to its physical IP address or translates a physical IP address to a name.

d. Dynamic Host Configuration Protocol (DHCP)
DHCP is a network protocol that allows a management server (DHCP server) to dynamically assign an IP address to the resources in its network. Without DHCP, network admins would have to assign IP addresses for each host in their network manually, making management of IP addresses difficult.

PING
Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network. It measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source.

TRACEROUTE

Traceroute is one of the most common utilities built into most operating systems. It is useful for diagnosing network connections. It shows the path of a packet going from your host/computer through each of the individual routes that handle the packet and time required for it to go from one router to another up to the final host/destination.

DIG
dig (domain information groper) is a Unix-like network administration command-line tool for querying Domain Name System (DNS) servers.

dig is useful for network troubleshooting and for educational purposes. dig can operate in interactive command line mode or in batch mode by reading requests from an operating system file. When a specific name server is not specified in the command invocation, it will use the operating system's default resolver, usually configured via the resolv.conf file. Without any arguments it queries the DNS root zone.

Nslookup

The Nslookup command is a DNS lookup utility. You can use the following commands to look up the information for a selected hostname: nslookup hostname - provides an A record for the hostname:

TCPDUMP

tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.