

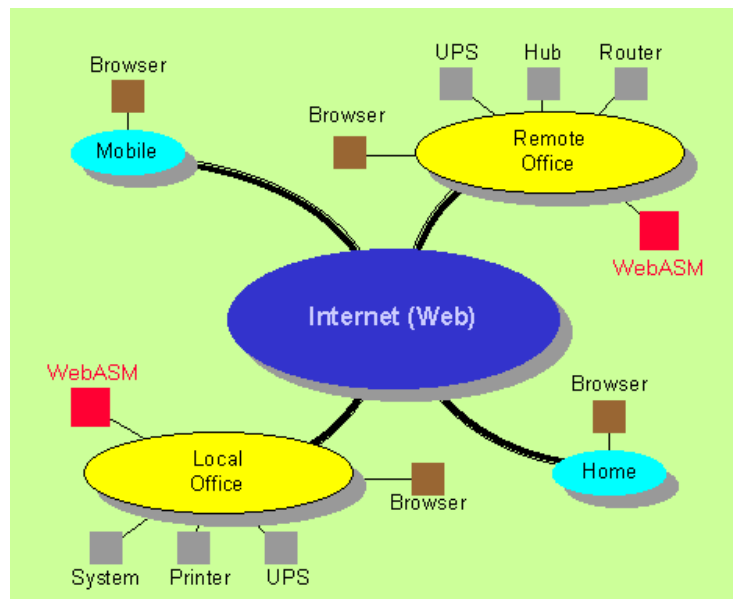
# **Chapter 1    Overview**

---

## **1.1.      Introduction**

Imagine a number of servers running in your company on different floors and that you have to go from floor to floor every day hour after hour to check on them. With the advent of server management software, you don't have to do that. Installing server management software like ASM Pro (Advanced Server Manager) helps server supervisors and management information system (MIS) personnel to spot errors or potential trouble spots in their network servers through a single management station. This way you won't exhaust yourself before the server you are managing does.

ASM Pro incorporates both software and server hardware implementations. This product aims to provide a tool for corporate end users to conveniently monitor servers on their networks without sacrificing efficiency. Now, the popularity of the Internet makes transferring and accessing the bits and bytes of data more mobile than ever. Integrated with ASM Pro, WebASM can monitor ASM Pro Agent for Windows NT Server, SCO OpenServer, SCO UnixWare, and Novell NetWare. It helps you manage your network system using a standard web browser. It runs on any workstation or PC supporting a Java run time environment. All you need to do is install WebASM in a machine connected to a LAN and you can access it from anywhere - at home, in your office, or even when you are on the road. Refer to the diagram below for a clear illustration of WebASM's connectivity. You can also monitor the health of networks, configure the parameters of the devices or view statistics in real time by browsing through the specially created HTML pages that come with WebASM.



WebASM is a comprehensive web-based SNMP server management tool that monitors Acer Server Systems with an ASM Pro Agent application installed. WebASM consists of three parts:

- Jigsaw, a Java-written HTTP server which provides a server-side Java environment
- Back-end information center, which collects data from SNMP agents and takes care of topology maintenance
- Front-end Java applets, which present dynamic information and give control to the back-end

---

## **1.2. Main Features of WebASM**

### **WebASM Management Console**

The WebASM management console is responsible for providing comprehensive server information, updated server management information, and an alert mechanism to an intuitive Web Browser through the Internet or an Intranet environment. This centralized monitoring of servers provides an easy way to monitor and maintain each server individually.

### **Preventive Maintenance and Fault Detection**

Integrated with ASM Pro, WebASM continuously checks on server components, highlighting components that are defective, checking power fluctuations and guarding against overheating.

### **System Performance Monitor**

Would you like to know how much work each network server handles? WebASM can look into network servers and check their resource utilization. Busy and idle times of servers can be monitored to enable you to determine a more efficient load distribution.

### **Comprehensive System Information Monitor & Event Notification Methods**

Providing a myriad of information about network server hardware and software components, this feature serves as a useful tool in replacing or upgrading components. Make your choice from a selection of notification methods on how WebASM should report faults or warnings.

---

### **Other Features**

WebASM maintains a log file of all trap events. In addition, you can open WebASM on-line help from anywhere in the program.

---

## 1.3 WebASM Technical Briefs

This section provides in-depth knowledge of WebASM and how it works. WebASM extends the manageability of SNMP manageable devices into the WEB environment. Users can launch a Java-enabled browser such as Microsoft Internet Explorer or Netscape Navigator, to manage the network wherever or whenever they are connected to the network, even through the Internet.

### WebASM System Architecture

Figure 1 illustrates the system architecture of WebASM. When users connect from a web browser to the WebASM HTTP server, topology viewer applet is downloaded and displays the network topology. Users then choose the nodes they want to manage. If the applet encounters any trouble connecting back to WebASM (e.g. when a firewall prevents a TCP connection), a snapshot of the topology can be generated and displayed I HTML by the HTML generator.

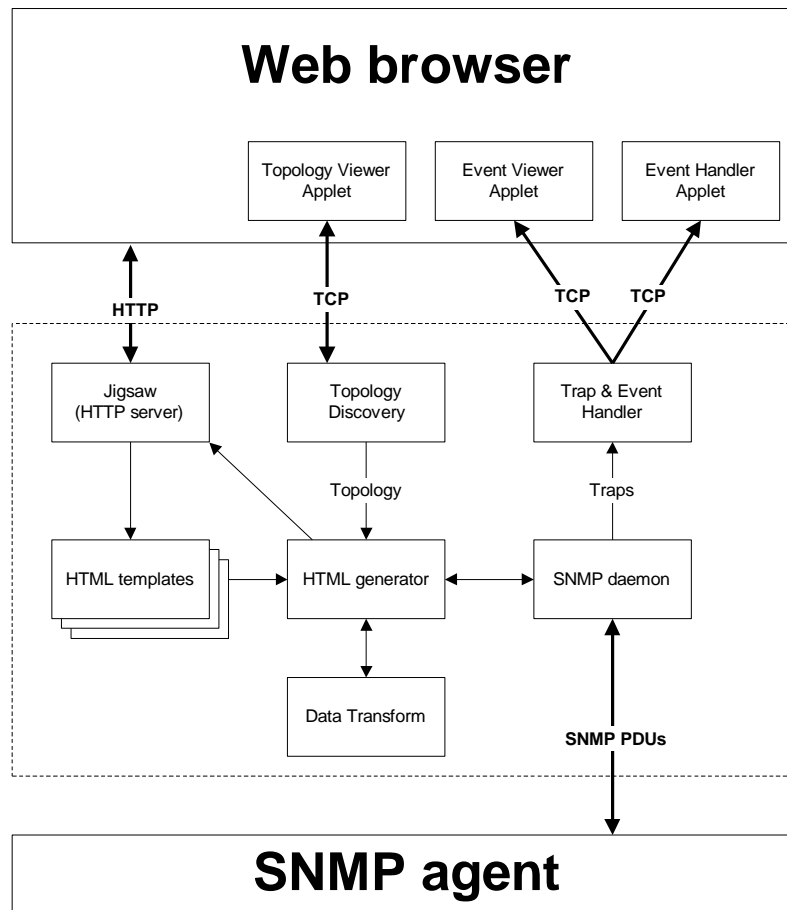


Figure 1 System Architecture Diagram

After users select a node to manage, another browser window will be opened, from which hyperlinks are provided to browse the management information. These hyperlinks link to HTML templates. When a template is loaded, the HTML generator is invoked to translate the template into the HTML document which replies to the browser.

---

The template includes tag extensions which instruct the HTML generator to form SNMP PDUs and send them through the SNMP daemon to manage the agent. Data Transform will then translate the replied value in each SNMP PDU into comprehensive information, if the HTML template instructs it to do so.

SNMP traps and system events are handled by the Trap & Event Handler, which will take the specified actions. The Event Viewer Applet is loaded into the browser if the user chooses to. The trap would then be displayed in event viewer applet. The Event Handler Applet is loaded when the user connects to the WebASM site, and it will be aware of the events which have occurred and take specified actions like popping-up a warning dialog box or involving alert mechanisms.

### **Topology Detection and Layout**

Topology Discovery will endeavour to find all SNMP manageable devices which reside in a subnet. The user can define different types of devices and give an SNMP OID which can be used to identify a device type. Topology Discovery will use this information to find correct type of manageable devices. WebASM is capable of distinguishing various types of devices, including the following:

- ASM for Windows NT
- ASM for NetWare
- ASM for SCO Unix
- Windows NT

Topology Discovery also discovers routers or gateways and connected subnets. Users can discover any subnet that they wish.

---

WebASM automatically detects all manageable SNMP (Simple Network Management Protocol) devices in a network. It recognizes a variety of different device types such as routers, printers, gateways, etc. Detected devices are displayed in a graphical manner. Multiple submaps or views of the network allow users to monitor distinct areas of the topology. Users can also create custom layouts for their viewing convenience. For more information, please refer to chapter 3, Network Views.

### **Real Time Event Logging**

WebASM logs any network event, such as an SNMP trap reported by a device, and displays it in a window in real-time. This means that you get the report as soon as it happens. Events also change the state of the associated devices and the color of their icons in the display. Users can then query WebASM for the event, view the event log, or click on the device icon to manage it.

### **MIB-II Compliant Devices**

The HTML pages of MIB-II (Management Information Base) allow you to view and modify the OID (Object ID) values of any MIB-II compliant devices you are managing on your network. As a result, even if customized management applications (HTML pages) do not exist for these devices, they can still be managed. Supported standard MIBs are MIB-II and Host Resources.

### **Trap & Event Handler**

WebASM is notified about events by managed agents. When a fault or error occurs or when a threshold has been exceeded, the agent will send a trap to WebASM. When a trap is received by WebASM, it will log it into the alarm log forward a notification message to the connected browser, and take the action previously selected by the user.



---

An alarm log will be updated in the agent once a trap occurs. This records the server that generated the event, the event type, time of occurrence, and event description in a file. The Alarm log is a useful tool to trace events that occur frequently. It can also be used as a database to analyze the causes of system faults.

Five types of alarm reporting methods are provided by WebASM. These are:

- Flash event log entry
- Audio alarm
- Dialog box with warning message pop-up
- Dial-up pager
- E-Mail

The flash event log entry, audio alarm and dialog box warning message provide on-screen notification at the connected browser, while E-Mail notification provides notification when the manager is not connected to WebASM. Pager notification is useful in providing prompt notification when the manager is out of the office.