11.1 Routine status parameters include traffic statistics, current software used in the switch, and the switch configuration. Parameters or events that would trigger an alarm if they change significantly include traffic loads (overload conditions), number of broadcast messages sent out, errors caused by intermittent operation, and an interface card failure.

11.2 As an example of a device for troubleshooting Ethernet LAN connections consider the functions provided by the Enterprise LANMeter™ from Fluke Networks (http://www.flukenetworks.com). The capabilities and use of this device include the following:

- Ability to generate and edit test packets: ability to send out Discovery packets
- Ability to capture and display real-time data: a Control Option allows access to the Enterprise LANMeter regardless of where the test technician is located. Web access capability allows the technician to view troubleshooting and analysis information using a web browser.
- Protocols supported: troubleshooting and management capabilities for 10/100-Mbps Ethernet and Token Ring networks, plus the capability to examine frame relay, ISDN and T1/E1 configurations to check utilization and connectivity problems.
11.3 Points within an enterprise network where proprietary information might be compromised:

- Wiretaps could be put on a line to a telephone or a computer to monitor conversations or data traffic.
- Passwords that are easily guessed or that are posted for the convenience of the user near the computer (which should be against security policies) may be used by an intruder.
- A non-secure unattended terminal may be used by an intruder to steal information.
- Programs or databases could be corrupted by a virus so that the integrity of the information is not reliable.
- Physical access to restricted areas where proprietary information is kept can be compromised if there are lax access rules and procedures.

11.4 As an example of the capabilities of a commercially available LAN protocol analyzer, consider the Agilent LAN Analyzer (http://www.agilent.com). This is a software-based network analysis package which can be used on most PCs that are enabled with network interface cards (NIC). This low-cost solution can be used for 10/100/1000-Mbps Ethernet and 4/16-Mbps Token Ring networks. It offers real-time network statistics, 7-layer packet decodes and analysis, advanced alarm setting and actions, detection and examination of MAC-level error conditions, powerful multi-layer filtering, packet slicing, and automatic name table updating. The collected statistics can be collated, analyzed, and formatted for archiving and distribution.
11.5 As an example, Merlin™ from Computer Access Technology Corporation (http://www.catc.com) is a Bluetooth wireless protocol analyzer. Merlin is a non-intrusive design verification system that provides network traffic capture, display, and analysis of Bluetooth piconet data. It uses hardware triggering to capture real-time events and hardware filtering to preserve memory and assist in pinpointing data of interest. Recorded data is displayed as color-coded packets that can be searched for specific data, errors or other desired conditions. As a stand-alone unit, Merlin can be configured and controlled by a host portable computer or a desktop PC connected via its USB port.


Need: A directory service is useful for the following reasons: (a) It simplifies network management by providing a single, consistent management point for users, applications, and devices. (b) It strengthens security by having a single sign-on to network resources and provides network administrators powerful tools to manage security for internal desktop users, remote dial-up users, and external e-commerce customers. (c) It supplies standards-based access to all directory service features.

Functions: Active Directory lets organizations share and manage information about network resources and users. It acts as a central authority for network
security and serves as an integration point for bringing systems together and consolidating management tasks.

11.7 The goal of configuration management is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

Examples of some policies and standards that an enterprise might specify, implement, and monitor through software-based configuration management tools:

- A large manufacturing corporation: maintaining up-to-date software for raw-goods warehouse database management, product inventory control, manufacturing processes, and quality control procedures; remote control management; various status and alarm reporting capabilities.

- A medical research facility: security policies for maintaining confidentiality of clinical trials; help desk support; policies for usage of wireless devices; virus checking; server access procedures for uploading and downloading information.

- A financial organization: database for serial numbers of hardware or software; database for physical locations of network devices; directory of names, addresses, and telephone numbers of contacts; server monitoring and threshold setting for unusual CPU activity; security policies for personnel access to various departments and servers in the facility.

- A government agency: security policies for external information requests, physical access by personnel, and internal server access; help desk support; policies for usage of wireless devices; virus checking.
The management tool ZENworks for Desktops from Novell includes an extensive capability for inventory management (see http://www.novell.com). As another example, consider the inventory software tool LANauditor from iInventory Ltd. (http://www.lanauditor.com). LANauditor software automatically inventories standalone, networked, or remote PCs, Macs, and fileserver hardware and software. LANauditor performs tasks such as checking for software license compliance, creating and maintaining an accurate hardware inventory, running OS/hardware/software analysis prior to installation, identifying user file abuse, and providing system data to an IT helpdesk. In addition, it translates complex audit data into simple to understand reports, tracks and captures specific files (e.g. documents or spreadsheets) across a network, and detects and audits files in hidden directories or folders. LANauditor supports Windows 95/98/2000/ME/NT, NetWare, MacOS, and DOS.

ZENworks for Desktops from Novell (see http://www.novell.com for descriptions of the latest software version). ZENworks for Desktops is a directory-enabled, policy-based desktop management application. This tool can be used for automatically installing software and efficiently managing Windows-based workstations in a network. Imaging features are included to automatically install operating systems and rebuild workstations from the management console, thereby eliminating time-consuming installation trips to every company desktop. All applications delivered through ZENworks for Desktops are linked to the login ID of a user. This enables users to access their applications from any workstation on the network, thus allowing them to quickly reach the tools they need. A
network manager can gather information on the amount of RAM a workstation has, the devices and services it is running, and the interrupts and I/O ports in use as well as which applications are installed.

11.10 ZENworks for Servers from Novell (see http://www.novell.com for descriptions of the latest software version). ZENworks for Servers is a directory-integrated application that provides automatic distribution, configuration, and management of files and software to multiple servers. It also encompasses sophisticated network traffic monitoring and analysis software. ZENworks for Servers can be implemented from a single point of administration through centrally administered policies. Policies can be scheduled to run daily, weekly, monthly, yearly, at a specific time, at intervals of time, when certain events occur, or at a time relative to when the policy was last refreshed. The policies can be associated with individual servers, server groups, or organizational units, according to the needs of the enterprise. This enables a network to have one set of policies for database servers, another set for Web servers, one for file and print servers, and so on. ZENworks for Servers allows the network administrator to use a Web browser to manage and configure all server policies and software distribution services over the Internet. The tool also allows the network manager to monitor and analyze any traffic, whether it is generated by network segments, nodes, switches, or protocols. In addition, it enables the collection of current and historical statistics on the network components and can display that data in tables, graphs, charts, or reports.
ThresholdManager from Cisco (see http://www.cisco.com for details). *Thresholds* define the range in which one expects a network to perform. If these thresholds exceed or go below the expected bounds, these areas can be examined for potential problems. A network manager can create thresholds for a specific device. Threshold Manager is a CiscoView-launched threshold management application that allows a network manager to set thresholds and retrieve event information. Threshold Manager relies on RMON (Remote Network Monitoring) alarm and event groups supported in Cisco routers and switches. A working knowledge of RMON is required for using this application. Threshold Manager provides an easy-to-use interface to access device-specific threshold settings. Using Threshold Manager, a network manager can set thresholds for network devices using Cisco-provided, predefined default policies. These policies can be applied automatically to target devices. Threshold Manager also supports detailed customization of threshold settings.

The ManageWise software tool from Novell (see http://www.novell.com for details). (a) When NetExplorer on the ManageWise server discovers a network, it gathers information about the network objects and places this information in the ManageWise database. This database is then used to create ManageWise maps that can be used to display the network topology. The time needed to build the baseline data depends on the size of the network. For very small networks it might take one or two hours, whereas networks consisting of thousands of nodes might require a day or two. (b) In the course of handling alarms that it receives from various systems and devices on the network, ManageWise software provides
alerts concerning network conditions that are relevant or that require some type of action. When a software-based alarm manager receives an alarm, ManageWise might perform actions such as saving the alarm to a database, sounding an audible beep, executing a program, or displaying a message.

11.13 Enhancements offered by RFC 2021 (version 2 of the RMON MIB):

- Protocol directory - lists the inventory of protocols that the probe is capable of monitoring
- Protocol distribution - counts traffic for detected protocols
- Address map - discovers mappings between second-layer and third-layer addresses
- Network layer host - counts traffic for discovered third-layer addresses
- Network layer matrix - counts traffic in conversations between third-layer addresses
- Application layer host - counts traffic in different protocols for discovered third-layer addresses
- Application layer matrix - counts traffic in different protocols in conversations between third-layer addresses
- User history - periodically does statistical sampling of arbitrary counters
- Probe configuration - controls the configuration of various operating parameters of the probe
11.14 LAN monitoring capabilities:

- **HP OpenView:** [see "http://www.openview.hp.com"] (a) Has a user interface based on Java™ so that OpenView provides easy access to network maps and enables management of data from anywhere on the web. (b) Discovers TCP/IP, IPX, and level-2 devices on both LANs and WANs. (c) Presents discovery information in a graphical format. (d) Provides fault tolerance capabilities that allow users to schedule back-ups of business-critical network management information to occur while they continue to manage the network. Management stations can be configured to take over the functions of the collection stations if one or more collection stations fail.

- **LAN Management Solution (Cisco):** [see "http://www.cisco.com"] (a) This is a Web-based graphical device-management technology that enables management of data from anywhere on the Web. (b) Provides intelligent discovery and display of large layer-2 networks on browser-accessible topology maps. (c) Displays link and device status based on Simple Network Management Protocol (SNMP) polling. (d) Provides real-time fault analysis for Cisco devices.

- **NetView:** [see "http://www.tivoli.com"] (a) Allows a user to log in to remote TCP/IP-connected systems either from the NetView command line or from the NetView Management Console (NMC). (b) Enables discovery of TCP/IP stack resources plus servers and clients, and manages them from views in the NMC. Sets filters to collect only the information that is needed. (c) Enables
schedule-sensitive status reporting. Using object groupings of the user's choice, the user can build customized views and aggregates dynamically and easily with the Collection Manager's wizard or drag-and-drop capabilities. View contents are updated dynamically as resources are added to or removed from the network.

11.15 [Note that effective July 27, 2001, Cisco Systems discontinued the sale of its Switch Probe product line. Alternatively, Cisco offers its Catalyst® 6000 Network Analysis Module (NAM) for LAN traffic monitoring instrumentation. The NAM is a card that occupies a single slot in the Catalyst switch chassis and extends the network analysis capability already embedded in the Cisco Catalyst Supervisor Module.] (Using the key search words "RMON probe" check web resources concerning other vendors of RMON probes.) A switch probe for LAN traffic monitoring typically has three ports: (1) An Ethernet 10BASE-T port which is used for communicating between the switch probe and a traffic director application, (2) an interface for a dial-up modem, (3) a port for collecting data about the network traffic.

11.16 See the VPIsystems website for the most updated offerings: