Ch7: **Configuration and maintenance**

Network Maintenance

- A simplified version of the tasks involved in network maintenance:

- Fixing network problems: When there are issues with the network, you need to find and fix them so that everything runs smoothly.

- Setting up and configuring hardware and software: Installing and setting up the necessary equipment and programs to make the network function properly.

- Monitoring and improving network performance: Keeping an eye on the network to make sure it's running efficiently, and making adjustments or improvements as needed.

- Planning for future growth: Anticipating the network's needs and making plans to accommodate future expansion or changes.

- Documenting the network: Creating and updating records and information about the network, like diagrams and configurations, so that everyone understands how it's set up.

- Following company policies: Making sure the network complies with the rules and guidelines set by the company or organization.

- Following legal regulations: Ensuring that the network meets any legal requirements or regulations that apply to its operation.

- Securing the network: Implementing measures to protect the network from various types of threats, such as unauthorized access or data breaches.

Structured tasks and Interrupt-driven tasks (1)

▶ **Structured network maintenance** refers to having a pre-defined plan in place to proactively address potential issues before they occur. By following this plan, network engineers can prevent problems from happening and make their work easier. It involves taking a proactive approach to maintenance and implementing preventive measures.

▶ **Interrupt-driven network maintenance** is more reactive. It means waiting for issues or problems to occur and then fixing them as quickly as possible. This approach is similar to a "fireman" who responds to emergencies. However, relying solely on an interrupt-driven approach can result in increased downtime and higher costs.

Structured tasks and Interrupt-driven tasks (2)

▶ Advantages

▶ Adopting a structured network maintenance approach with a clear strategy and plan in place helps minimize downtime.

▶ A structured approach enables maintenance activities to be performed in a more cost-effective manner.

▶ Proactive troubleshooting and preventive measures are possible with a structured maintenance approach.

▶ Implementing a structured approach leads to a more stable and reliable network.

▶ Disadvantages? ????

Network maintenance models

▶

There are several network maintenance models that are commonly used in the industry. Here are three of the most well-known models:

▶ Break-Fix Model: This model is a reactive approach to network maintenance where technicians are called upon to fix issues as they arise. It does not involve proactive monitoring or preventive measures.

▶ Preventive Maintenance Model: This model focuses on regular maintenance tasks and proactive measures to prevent potential issues. It includes activities such as routine equipment checks, firmware updates, security patches, and system backups.

▶ Predictive Maintenance Model: This model utilizes advanced monitoring and analytics tools to predict and prevent network failures. It involves collecting and analyzing data to identify potential issues before they occur, allowing for proactive maintenance and minimizing downtime.

FCAPS Models

- Network maintenance is closely related to the FCAPS model as it encompasses the activities and tasks performed in each of these functional areas to ensure the smooth operation, reliability, and security of the network.

- **Fault Management**

  - detection, isolation, and correction of abnormal operations

- **Configuration Management**

  - identify managed resources and their connectivity, discovery

- **Accounting Management**

  - keep track of usage for charging

- **Performance Management**

  - monitor and evaluate the behavior of managed resources

- **Security Management**

  - allow only authorized access and control

Fault Management

- Manages network problems to keep the network running reliably and efficiently.
- Fault management process involves the following steps
  - Detecting the problem symptoms.
  - Isolating the problem.
  - Fixing the problem automatically (if possible) or manually.
  - Logging the detection and resolution of the problem.

Configuration Management

▶ Configuration Management monitors network and system configuration information and stores it in a configuration management database.

▶ The maintenance of this database allows network administrators to <u>track</u> hardware, software, and other network resources

Configuration Management (2)

- Each network device has a variety of information associated with it:
  - Software version information for the operating system, protocol software, or management software.
  - Hardware version information for the interfaces or hardware controllers.
  - Contact information indicating who to contact if problems with the device arise.
  - Location information indicating the physical location of the device.

Configuration Management (3)

- Configuration management in the context of network maintenance
- Device Configuration: Involves setting up and managing network devices, configuring parameters, interfaces, and security settings.
- Configuration Documentation: Creating and maintaining documentation for network device configurations as a reference for troubleshooting and changes.
- Change Control: Implementing processes to control and track changes to network device configurations.
- Version Control: Maintaining a system to track and manage different versions of configurations and revert if needed.
- Configuration Auditing: Conducting regular audits to ensure compliance and identify discrepancies or vulnerabilities.
- Configuration Backup and Restoration: Implementing regular backups to protect against configuration loss and enable quick restoration.
- Configuration Automation: Leveraging automation tools to streamline configuration tasks, ensure consistency, and enhance efficiency.

Accounting Management

- Measures network utilization parameters in order to regulate individual and group use of the network.

- Minimizes network problems and maximizes fairness of user access to the network because network resources can be portioned based on network capacity and user needs.

Performance Management

▶ Maintains internetwork performance at acceptable levels by measuring and managing various network performance variables.

▶ Performance variables include network throughput, user response times, line utilization, and others.

▶ Performance management involves three basic steps:

▶ Gathering data relating to key performance variables.

▶ Analyzing data to determine the normal (baseline) performance levels.

▶ Determining appropriate performance thresholds for each variable so that exceeding these thresholds indicates a network problem worthy of attention.

Performance Management (2)
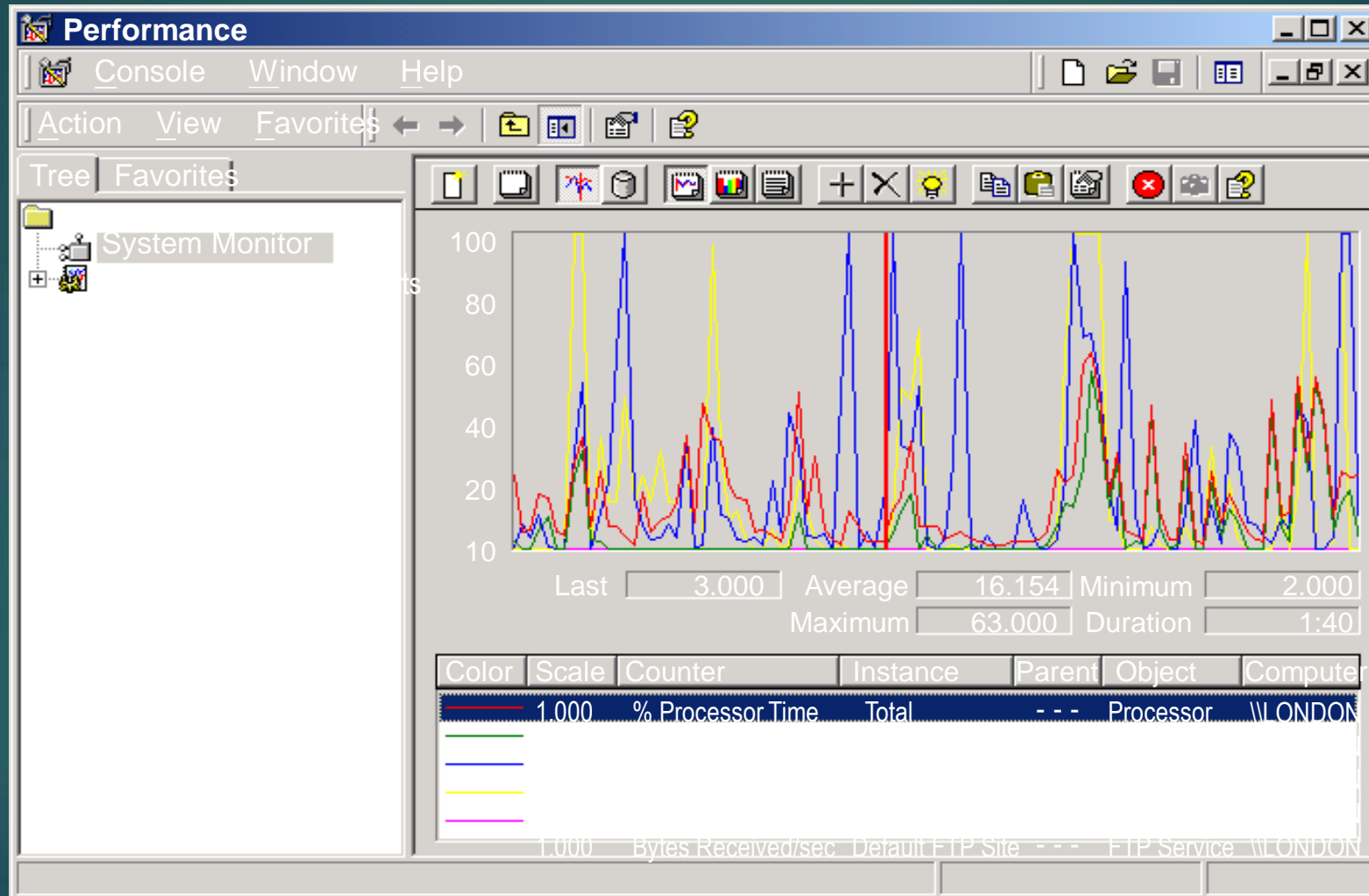
Performance Management (3)

▶ Reactive
  - ▶ when performance becomes unacceptable (that is, a user-defined threshold is exceeded), the managed device reacts by sending an alert to the network management system (NMS).

▶ Proactive
  - ▶ simulation is used to project how network growth will affect performance metrics. These simulations alert administrators to impending problems before they affect network users.

Performance Management (4)

- Reactive PM Components
  - The management entity continually monitors performance variables in managed devices.
  - When a particular performance threshold is exceeded, the NMS or the managed device detects the problem.
  - If the managed device detects the problem, it generates an alert and sends it to the NMS.
  - The NMS takes an appropriate action, such as alerting the network administrator.

Windows Task Manager

Security Management

- Access control
  - Controls access to network resources, and prevents network sabotage (intentional or unintentional) and unauthorized access to sensitive information.
  - Aids administrators in creating a secure network environment. This includes:
    - partitioning network resources into authorized and unauthorized areas,
    - mapping groups of users to those areas, and
    - monitoring, policing, and logging user access to resources in those areas.
- Security monitoring
  - Security event collection
  - Event analysis, correlation and alert generation
  - Alert handling