**Chapter 1**

**Device Configuration**

**Configuration Wizard**

A software **wizard** or **setup assistant** is a [user interface](https://en.wikipedia.org/wiki/User_interface) type that presents a [user](https://en.wikipedia.org/wiki/End-user_%28computer_science%29) with a sequence of [dialog boxes](https://en.wikipedia.org/wiki/Dialog_box) that lead the user through a series of well-defined steps. Tasks that are complex, infrequently performed, or unfamiliar may be easier to perform using a wizard.

A configuration is the arrangement - or the process of making the arrangement - of the parts that make up a whole. In computers and computer networks, a configuration often refers to the specific hardware and software details in terms of devices attached, capacity or capability, and exactly what the system is made up of.

**Automatic Discovery and Configuration Manager**

The discovery process immediately provides details such as name, device type, Operating System, services running and other important device configuration details. A Discovery Wizard allows one to set discovery credentials, select services to be discovered and choose the devices to be discovered and imported for monitoring.

Device discovery tools simplify the process using a variety of discovery protocols to discover and collect information about:

* Physical assets such as routers, switches, servers, hosts and firewalls
* Software assets such as applications, operating systems, and services
* Virtual devices and networks
* How everything is connected.

**Device Schedules**

Schedules can be used to set recurring times when you’d like a user’s connected devices to lose their connection to the Internet. When a schedule is activated, the devices associated with that user’s profile will automatically go into a paused state.

**Element Manager**

With Element Manager, you can manage individual server switches from an easy-to-use GUI. An element manager routinely audits the operational condition of core elements, including CPUs, power supplies and disk drives. In the event of hardware or software malfunctions, crashes, runtime errors and system boot failure, the element manager phones home and automatically generates a maintenance request. The use of standards-based mechanisms such as [SNMP](https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol) and [Syslog](https://en.wikipedia.org/wiki/Syslog) ensures full integration with today's network management systems and provides a unified view of system-wide functionality.

An element manager also includes update services that automate the process and management of delivering updates, patches and other upgrades to server appliances deployed in field, including the operating system and all related applications.

**What Is the Command Line Interface?**

The command line interface is the main, text-based interface for configuring, managing, and monitoring network devices such as a router or a data switch. CLI allows you to type in configuration commands to get the output from the router or a switch. The network software recognizes the command when you enter enough characters of the command to uniquely identify it, which in turn helps you monitor the status of your network device.

**Networking and internetworking devices**

There are different network devices some of these are listed below

**Network Interface Card (NIC)**

* NIC provides the physical interface between computer and cabling.
* It prepares data, sends data, and controls the flow of data. It can also receive and translate data into bytes for the CPU to understand.
* The following factors should be taken into consideration when choosing a NIC:
  + - Preparing data
  + - Sending and controlling data
  + - Configuration
  + - Drivers
  + - Compatibility
  + - Performance
* In the computer, data moves along buses in parallel, as on a four-lane interstate highway. But on a network cable, data travels in a single stream, as on a one lane highway. This difference can cause problems transmitting and receiving data, because the paths traveled are not the same.
* It is the NIC’s job to translate the data from the computer into signals that can flow easily along the cable.
* It does this by translating digital signals into electrical signals (and in the case of fiber-optic NICs, to optical signals).
* For two computers to send and receive data, the cards must agree on several things. These include the following:

- The maximum size of the data frames

- The amount of data sent before giving confirmation

- The time needed between transmissions

- The amount of time needed to wait before sending confirmation

- The amount of data a card can hold

- The speed at which data transmits

* In order to successfully send data on the network, you need to make sure the network cards are of the same type and they are connected to the same piece of cable.
* The NIC’s configuration includes things like a manufacturer’s hardware address, IRQ address, Base I/O port address, and base memory address. Some may also use DMA channels to offer better performance.
* Each card must have a unique hardware address. If two cards have the same hardware addresses, neither one of them will be able to communicate.
* For the computer to use the network interface card, it is very important to install the proper device drivers.

**Repeater**

* Repeaters are very simple devices. They allow a cabling system to extend beyond its maximum allowed length by amplifying the network voltages so they travel farther.
* Repeaters are nothing more than amplifiers and, as such, are very inexpensive.
* Repeaters can only be used to regenerate signals between similar network segments.
* For example, we can extend an Ethernet 10Base2 network to 400 meters with a repeater. But can’t connect an Ethernet and Token Ring network together with one.
* The main disadvantage to repeaters is that they just amplify signals. These signals not only include the network signals, but any noise on the wire as well.
* Eventually, if you use enough repeaters, you could possibly drown out the signal with the amplified noise. For this reason, repeaters are used only as a temporary fix.

**Hub**

* Hubs are devices used to link several computers together.
* They repeat any signal that comes in on one port and copy it to the other ports (a process that is also called *broadcasting*).
* There are two types of hubs: active and passive.
* *Passive hubs* simply connect all ports together electrically and are usually not powered.
* *Active hubs* use electronics to amplify and clean up the signal before it is broadcast to the other ports.
* In the category of active hubs, there is also a class called “intelligent” hubs, which are hubs that can be remotely managed on the network.

**Bridge**

* They join similar topologies and are used to divide network segments.
* For example, with 200 people on one Ethernet segment, the performance will be mediocre, because of the design of Ethernet and the number of workstations that are fighting to transmit. If you divide the segment into two segments of 100 workstations each, the traffic will be much lower on either side and performance will increase.
* If it is aware of the destination address, it is able to forward packets; otherwise a bridge will forward the packets to all segments. They are more intelligent than repeaters but are unable to move data across multiple networks simultaneously.
* Unlike repeaters, bridges *can* filter out noise.
* The main disadvantage to bridges is that they can’t connect dissimilar network types or perform intelligent path selection. For that function, you would need a router.

**Routers**

* Routers are highly intelligent devices that connect multiple network types and determine the best path for sending data.
* The advantage of using a router over a bridge is that routers can determine the best path that data can take to get to its destination.
* Like bridges, they can segment large networks and can filter out noise.
* However, they are slower than bridges because they are more intelligent devices; as such, they analyze every packet, causing packet-forwarding delays. Because of this intelligence, they are also more expensive.
* Routers are normally used to connect one LAN to another.
* Typically, when a WAN is set up, there will be at least two routers used.

**Switch**

* A network switch is a computer networking device that connects network segments.
* Low-end network switches appear nearly identical to network hubs, but a switch contains more "intelligence" (and a slightly higher price tag) than a network hub.
* Network switches are capable of inspecting data packets as they are received, determining the source and destination device of that packet, and forwarding it appropriately.
* By delivering each message only to the connected device it was intended for, a network switch conserves network bandwidth and offers generally better performance than a hub.
* A vital difference between a hub and a switch is that all the nodes connected to a hub share the bandwidth among themselves, while a device connected to a switch port has the full bandwidth all to itself.
* For example, if 10 nodes are communicating using a hub on a 10-Mbps network, then each node may only get a portion of the 10 Mbps if other nodes on the hub want to communicate as well.
* But with a switch, each node could possibly communicate at the full 10 Mbps.