**Switch**

Besides filtering traffic by sending the data only to the port that the

destination system resides on, most network switches provide the

following benefits:

■ Filtering:

As mentioned, a switch filters traffic, which prevents others from capturing and

viewing potentially confidential information.

■ Port mirroring:

Port mirroring, also known as port monitoring, is a feature of some switches

that allows the administrator to copy traffic from other ports to a single

destination port (known as a monitoring port).

Because the switch filters traffic by default, the administrator cannot monitor

network traffic.

The switch vendors had to come up with a way to copy all the traffic to a

single port so the administrator could connect their monitoring system to that

port.

■ Port security:

Port security is a feature of a network switch that lets you configure a

port for a specific MAC address.

This allows you to control which systems can connect to that port on

the switch. When an unauthorized system connects to the port on the

switch, the switch can temporarily disable the port until the correct

system is plugged into the switch, or have the port disabled until an

administrator reenables the port.

Capability to disable ports:

If you have ports on the switch that are not being used, it is a security

best practice to disable them so that they cannot be used.

**Collision Domains:**

Another important feature of a switch is known as a collision domain, which

is a group of systems that share the same network segment and therefore

can have their data collide with one another.

All ports on a hub create a single collision domain, but each port on a switch

creates a separate collision domain.

For example, when using a network hub, if two systems were to send data at

the same time it would result in a data collision.

This is because the hub creates a “shared” network segment that all systems

have access to.

With a switch, each port on the switch creates a separate collision domain

that is its own network segment.

When connecting a system to a port on a switch, because no other system is

on the network segment, there won’t be data collisions.

**VLAN**

Most switches today support a feature known as virtual

LANs (VLANs).

The purpose of a VLAN is to create multiple networks

within the one network switch.

One way to do this is by placing ports on the switch

into VLAN groupings.

When a system is connected to a port on the switch, it

becomes a member of the VLAN that the port is

associated with.

The important point is that when a system is a

member of one VLAN, it cannot communicate with

systems in another VLAN. It’s as if each VLAN has

its own switch with no connection to another

switch.

Figure 1-4 displays a switch configured in two VLANs.

In this example, Computer A can communicate only

with Computer B because they are the only systems in

VLAN1.

Computer A and Computer B cannot communicate

with Computer C and Computer D because

communication across VLANs is not allowed without a router

**Router**

A router is a layer-3 device that is

responsible for routing, or sending,

data from one network to another

network.

The router uses a routing table

that resides in its memory to

determine the networks it knows

how to send data to.

Figure 1-5 displays a network

topology and the routing table on a

router.

Notice in the figure that in order for

router R1 to send data to the 25.0.0.0

network, it must send the data to the

24.0.0.2 address, as indicated by the

routing table