Port Security

The *port security* feature restricts the number of MAC addresses used on a switch or restricts the use of a port to a specified group of users. The number of devices on a secured port can range from one to 132. The MAC addresses are assigned either automatically or by the administrator (assigned statically).

Address violations occur when a secured port receives a source address already assigned to another secured port or when a port exceeds its address table size limit. When a violation occurs, the action can be suspended, ignored, or disabled.

A suspended port is reenabled when a valid address is received. A disabled port must be reenabled manually. If the action is ignored, the switch port remains enabled.

Here is the procedure for configuring the IP address:

```
RouterA(config)#interface e0/1
RouterA(config-if)#port secure max-mac-count 1
RouterA(config-if)#exit
RouterAhost#show mac-address-table security
RouterA(config-if)#exit
RouterA(config)#address-violation ignore
```

The **no port secure** command disables addressing security and sets the maximum number of addresses on the interface to the default (132).

The **show** command yields a list of enabled ports and their security statuses.

The action for an address violation can be suspend, disable, or ignore.

Use the **no address-violation** command to set the switch to its default value (suspend).

Configuring the Catalyst 1900 Switch Summary

- To configure global switch parameters (switch, host name, or IP address), use the **config term** command. To configure a particular port, use the **interface** command while in global configuration mode.
- MAC address tables can be dynamic, permanent, or static.
- Switches are assigned IP addresses for network management purposes.
- A default gateway is used to reach a network that has a different IP address.
- Use the various **show** commands to verify switch configuration.

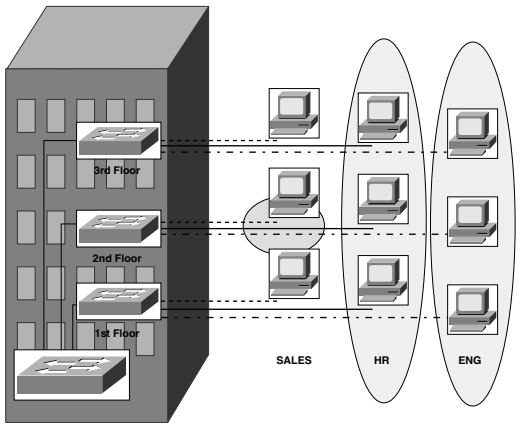
VLANs

VLAN Operation Overview

The *virtual LAN* (VLAN) allows you to group physically separate users into the same broadcast domain. The use of VLANs improves security, segmentation, and flexibility. The use of VLANs also decreases the cost of arranging users, because no extra cabling is required.

VLAN Characteristics

VLANs allow an administrator to define user groups logically rather than by their physical locations. For example, you can arrange user groups such as accounting, engineering, and finance rather than grouping everyone on the first floor, everyone on the second floor, and so on.



- VLANs define broadcast domains that can span multiple LAN segments.
- VLAN segmentation is not bound by the physical location of users.
- Each switch port can be assigned to only one VLAN.
- Ports not assigned to the same VLAN do not share broadcasts, improving network performance.
- A VLAN can exist on one switch or on multiple switches.
- VLANs can connect across wide-area networks (WANs).