Named Access Lists

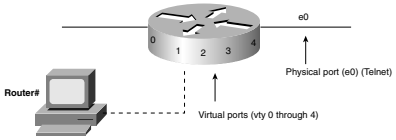
Named IP access addresses (Cisco IOS Release 11.2 and later) allow alphanumeric strings as identifiers rather than numbers. Named access lists can be standard or extended. Named IP access lists also allow you to delete individual statements from an access list.

You should use named access lists when more than 99 standard or extended access lists are configured on any router. Duplicate names are not allowed on any one router. (You can use the same name on two different routers.)

Guidelines for Placing Access Lists

Extended access lists can block traffic from leaving the source. They should be as close as possible to the source of the traffic to be denied. Standard access lists block traffic at the destination. They should be as close as possible to the destination of the traffic to be denied.

Virtual Terminal Access Lists



In addition to physical ports, devices also have virtual ports (called virtual terminal lines). There are five such virtual terminal lines, numbered vty 0 through vty 4. Standard and extended access lists do not prevent router-initiated Telnet sessions.

Virtual terminal access lists can block vty access to the router or block access to other routers on allowed vty sessions. Restrictions on vty access should include all virtual ports, because users can connect through any vty port. The syntax for a vty access list is **line vty {vty# | vty-range}**.

After you add the vty statements, you assign them to the router with the following command:

```
access-class access-list-number {in | out}
```

Specifying **in** prevents incoming Telnet connections, and **out** prevents Telnet connections to other routers from the vty ports.

Access List Configuration Summary

- Here are some general guidelines for configuring access lists:
  - All access lists end with an implicit **deny**.
  - More-specific tests should precede more-general tests.
  - Frequently used tests should precede infrequent tests.
- Standard access lists filter based on source addresses only.
- Extended access lists filter based on source and destination addresses, protocols, and ports.
- The **access-list** command assigns statements to a list. The **access-group** command assigns an access list to an interface.
- Named access lists allow you to identify access lists with alphanumeric strings rather than numbers. You can delete entries from a named access list.
- Extended access lists should be close to the source of the traffic to be denied.
- Standard access lists should be close to the destination.
- Access lists can be used to control virtual terminal (vty) access to or from a router.
- The **line vty** and **access-class** commands are used to configure and set vty access lists.

IPX Routing Overview

Cisco routers are compatible with NetWare (Novell) networks. They have the following features:

- Interface support, including native ISDN and ATM
- IPX access filters for several protocols (IPX, RIP, SAP, NCP, and NetBIOS)
- Support for EIGRP and NLSP
- Serverless LAN support
- Dial-on-demand routing (DDR)

Key Novell NetWare Features

- Novell IPX addresses use 32 bits for the network number and 48 bits for the node number, expressed as a hexadecimal number.
- The MAC address of an interface is used as the node number.
- Multiple logical networks can be configured on a single interface, but each network must use a different encapsulation type.