IPX Extended Access Lists

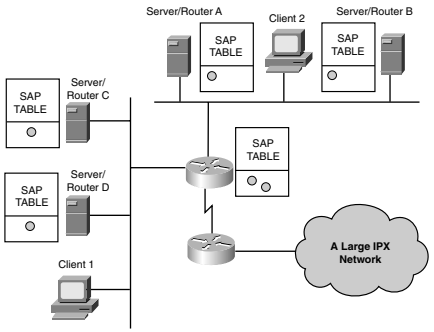
Use the following syntax for extended IPX access lists:

```
access-list access-list-number {deny | permit} protocol
  [source-network]
  [[.source-node] source-node-mask] |
  [.source-node source-network-mask. source-node-mask]]
  [source-socket] [dest.network] [[[.dest-node]dest-node-mask] |
  [.dest-nodedest-network-mask. destnodemask]] [des-socket] [log]
```

protocol can be a name or number (decimal) of an IPX protocol type. The **log** parameter logs IPX access control list violations to a syslog server whenever a packet matches a particular access list entry.

Procedure for Configuring Extended IP Access Lists

SAP Operation



To minimize overhead traffic, routers synchronize the list of available services by forwarding SAP tables rather than forwarding every SAP broadcast. The router advertises its SAP table every 60 seconds by default.

SAP Filter Types

IPX input SAP filters limit the number of services entered into the SAP table. The propagated SAP updates contain a subset of all services.

IPX output SAP filters limit the number of services propagated from the table. The propagated SAP updates contain a subset of all the known services.

Be sure that all clients will see all advertisements required for their application processing. Always place SAP filters as close as possible to the source of the SAP information. This is the most efficient use of bandwidth.

Examining SAP Filter Configuration

Use the following syntax for SAP filter definition statements:

```
access-list access-list-number {deny | permit} network [.node]
  [network-mask.node-mask] [service-type [server-name]]
```

SAP filters use the range 1000 to 1999. Each SAP service type is identified by a hexadecimal number (a 0 matches all services).

After entering the definition statements, you activate the SAP filter with the following command:

```
ipx [input | output]-sap-filter access-list-number
```

IPX Filtering Summary

- Novell addressing is used to create standard, extended, and SAP filter access lists.
- Standard access lists permit or deny information based on source and destination.
- Extended access lists filter on protocol type, source network/node, destination network/node, IPX protocol, and IPX socket number.
- Routers build SAP tables based on SAP server advertisements. Routers forward their tables every 60 seconds by default.
- SAP filters can be placed on a router for both incoming and outgoing traffic.
- SAP filters control the propagation of SAP messages.

Configuring IPX Routing

You must do the following to configure Novell IPX as a routing protocol:

- Start the IPX routing process.
- Enable load sharing to balance packets across multiple routes and links.
- Assign unique network numbers to each interface. (Multiple network numbers can be assigned to an interface for different encapsulation types.)
- Change the encapsulation type, if required.

IPX Configuration Commands

The following commands are used when configuring IPX routing:

- **ipx routing [node]**—Enables IPX routing and SAP services.
- **ipx maximum-paths [paths]**—Enables load sharing. The default is 1, and the maximum is 64.
- **ipx network network [encapsulation encapsulation type]**—Enables IPX routing on a particular interface.