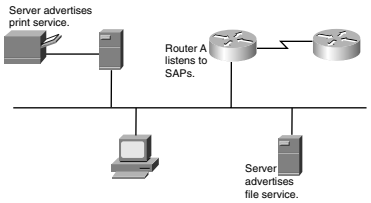
### Router SAP Tables




Rather than forward SAP broadcasts (which would add significant traffic to the network), routers build and send SAP tables. The tables are sent every 60 seconds by default.

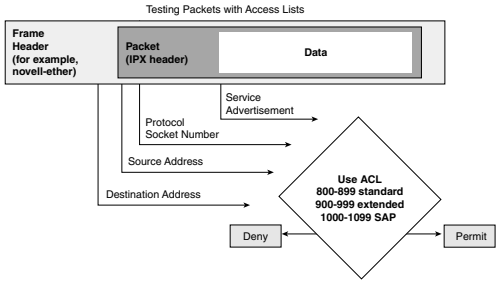
### Initiating a Connection to a NetWare Server

When a client powers up, it broadcasts a GNS SAP query. All local NetWare file servers respond with a SAP reply. The client can then log into the target server. If a Cisco router receives a GNS query, it does not respond unless no NetWare servers are on the network.

## IPX Routing Summary

- Novell NetWare supports access lists and filters, scalable routing protocols, serverless LAN, dial-on demand routing, and rich management control.
- RIP, SAP, IPX, SPX, and NLSP are included in the NetWare protocol stack.
- A Novell IPX address is made up of an administrator-assigned network number and a node number (usually derived from an interface MAC address).
- NetWare servers broadcast information tables every 60 seconds. Routers use this information to build SAP tables, which they share with other routers.
- Novell IPX RIP is a distance vector routing protocol. It uses hop count and ticks for a metric.
- Network devices advertise their services using SAP broadcasts.
- NetWare clients use GNS and SAP queries to locate network services.

## IPX Filtering




Novell IPX uses access lists to filter packets. Packets can be filtered using standard, extended, or SAP access lists. Standard access lists (numbered from 800 to 899) use destination and source IPX addresses to filter packets. Extended access lists (numbered from 900 to 999) use them to filter packets. SAP filter access lists use service advertisement numbers to filter packets and are numbered from 1000 to 1099. Packets are permitted or denied based on the criteria specified in the access list statements. Wildcard masks are used to specify individual addresses or blocks of addresses.

### IPX Standard Access Lists

The syntax for standard IPX access lists is as follows:

```
access-list access-list-number {deny | permit} source-network
  [.source-node [source-node-mask]] destination-network
  [.dest-node [dest-node-mask]]
```

*source-network.network-node* and *destination-network.network-node* denote the IPX source and destination addresses, respectively. (–1 equals any network.)

After entering the statements, you apply the access list to the interface using the following command:

```
ipx access-group access-list-number [in | out]
```

*Note:* IPX access lists default to outbound filters.