One of the limiting factors in the operation of large Novell Internetwork Packet Exchange (IPX) internetworks is the amount of bandwidth consumed by the large, periodic Service Advertisement Protocol (SAP) updates. Novell servers periodically send clients information about the services they provide by broadcasting this information onto their connected local-area network (LAN) or wide-area network (WAN) interfaces. Routers are required to propagate SAP updates through an IPX network so that all clients can see the service messages. It is possible to reduce SAP traffic on Novell IPX networks by the following means:

- Filtering SAP updates through access lists. SAP updates can be filtered by prohibiting routers from advertising services from specified Novell servers.
- Configuring Cisco routers on Novell IPX networks to run Enhanced IGRP. Although filters provide a means of eliminating the advertisements of specified services, Enhanced IGRP provides incremental SAP updates for a finer granularity of control. Complete SAP updates are sent periodically on each interface only until an IPX Enhanced IGRP neighbor is found. Thereafter, SAP updates are sent only when there are changes to the SAP table. In this way, bandwidth is conserved, and the advertisement of services is reduced without being eliminated.
- Incremental SAP updates are automatic on serial interfaces and can be configured on LAN media. Enhanced IGRP also provides partial routing updates and fast convergence for IPX networks. Administrators may choose to run only the partial SAP updates or to run both the reliable SAP protocol and the partial routing update portion of Enhanced IGRP.
- Configuring Cisco routers on Novell IPX networks to send incremental SAP updates. With Software Release 10.0, the incremental SAP updates just described can be configured for Cisco routers on Novell IPX networks, without the requirement of running the routing update feature of Enhanced IGRP (only the partial SAP updates are enabled). This feature is supported on all interface types. Again, SAP updates are sent only when changes occur on a network. Only the changes to SAP tables are sent as updates.

To illustrate how to reduce SAP traffic, this case study is organized into two parts:

- Configuring Access Lists to Filter SAP Updates
- Configuring Incremental SAP Updates

Note: For a detailed case study on configuring Novell IPX Enhanced IGRP, see the Novell IPX Network section in Integrating Enhanced IGRP into Existing Networks.

The internet work for this case study is illustrated in Figure: Large-scale Novell IPX internetwork. The following portions of a large-scale Novell IPX network spanning across a Frame Relay WAN are examined:

- Router A connects from the Frame Relay internetwork to the central site with three Novell servers.
- Router B connects from the Frame Relay internetwork to a remote site with one Novell client and one Novell server.
- Router C connects from the Frame Relay internetwork to a remote site with two Novell clients.

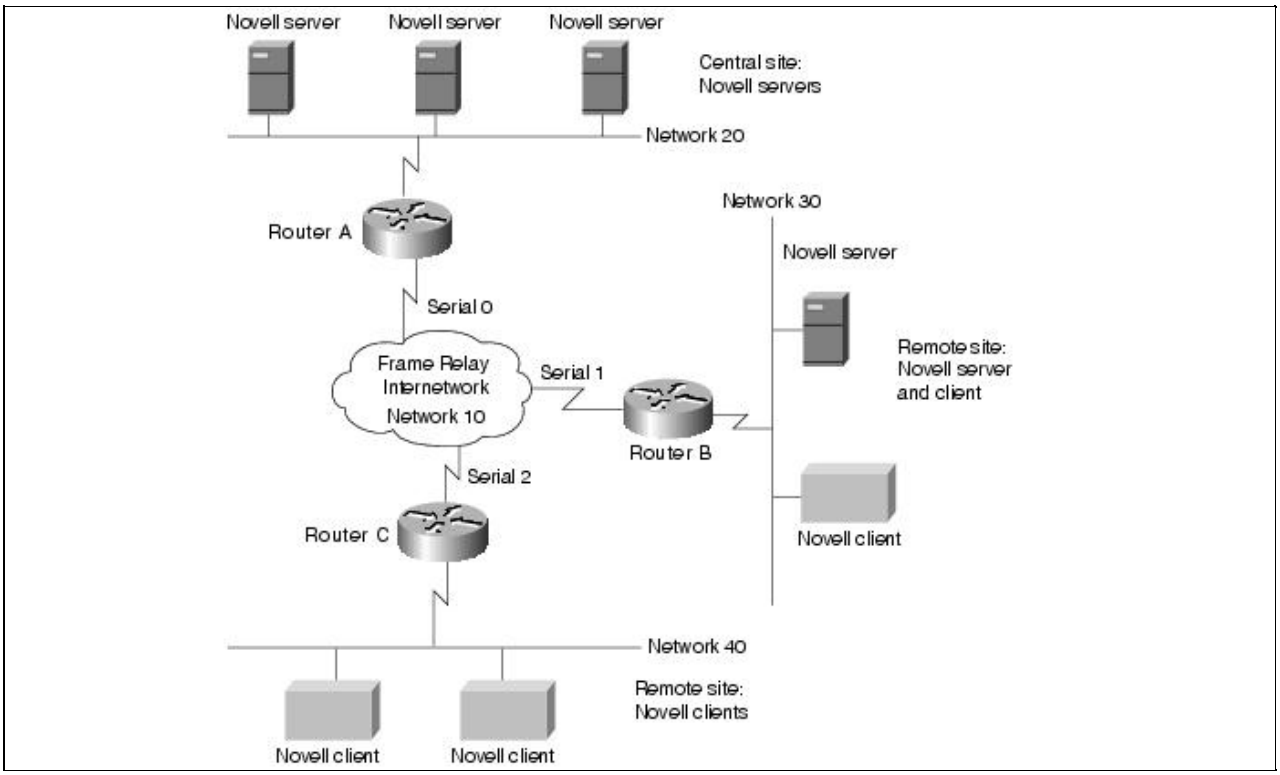
Guide Contents
Internetworking Design Basics
Designing various internetworks
Network Enhancements
IP Routing Concepts
UDP Broadcast Flooding
Large-Scale H.323 Network Design for Service Providers

LAN Switching
Subnetting an IP Address Space
IBM Serial Link Implementation Notes
References and Recommended Reading

Contents

- 1 Figure: Large-scale Novell IPX internetwork
- 2 Configuring Access Lists to Filter SAP Updates
  - 2.1 Central Site
  - 2.2 Remote Sites
    - 2.2.1 IPX Server and Client
    - 2.2.2 IPX Clients
- 3 Configuring Incremental SAP Updates
  - 3.1 Central Site
  - 3.2 Remote Sites
    - 3.2.1 IPX Server and Client
    - 3.2.2 IPX Clients
- 4 Summary

Figure: Large-scale Novell IPX internetwork



Configuring Access Lists to Filter SAP Updates

Access lists can control which routers send or receive SAP updates and which routers do not send or receive SAP updates. SAP access lists can be defined to filter SAP updates based on the source network address of a SAP entry, the type of SAP entry (file server, print server, and so forth), and the name of the SAP server. A

SAP access list is made up of entries in the following format:

```
access-list n [deny|permit] network[.node] [service-type[server-name]]
```

where n is between 1000-1099. A network number of -1 indicates any network, and a service type of 0 indicates any service. For example, the following access list accepts print server SAP entries from server PRINTER_1, all file servers, and any other SAP entries from network 123 except those from a server called UNTRUSTED; all other SAP entries are to be ignored:

```
access-list 1000 permit -1 47 PRINTER_1
access-list 1000 permit -1 4
access-list 1000 deny 123 0 UNTRUSTED
access-list 1000 permit 123
```

When checking the entries in a SAP update, each statement in the access list is processed in order, and if there is no match for a SAP entry, it is not accepted. Thus, to block server UNTRUSTED, the **deny** statement must be placed before the **permit** for all other devices on network 123.

Two techniques can be used with filtering. Either the SAP entries that are required can be permitted and the rest denied, or the unwanted SAP entries can be denied and the rest permitted. In general, the first method is preferred because it avoids new and unexpected services being propagated throughout the network.

The most common form of SAP filtering is to limit which services are available across a WAN. For example, it does not, in general, make sense for clients in one location to be able to access print servers in another location because printing is a local operation. In this case study, only file servers are permitted to be visible across the WAN.

Central Site

Router A connects to the central site. The following access lists configured on Router A permit everything except print servers from being announced out the serial interface:

```
access-list 1000 deny -1 47
access-list 1000 permit -1
!
interface serial 0
ipx network 10
ipx output-sap-filter 1000
```

To permit only IPX file servers and to deny all other IPX servers, use the following configuration:

```
access-list 1000 permit -1 4
!
interface serial 0
ipx network 10
ipx out-sap-filter 1000
```

Remote Sites

This section provides information on the configuration of the routers at the remote sites:

- Router B connected to an IPX server and client
- Router C connected to two IPX clients

IPX Server and Client

For Router B, the following access lists permit everything except print servers from being announced out the serial interface.

```
access-list 1000 deny -1 47
access-list 1000 permit -1
!
interface serial 1
ipx network 10
ipx output-sap-filter 1000
```

To permit only IPX file servers and to deny all other IPX servers, use the following configuration:

```
access-list 1000 permit -1 4
!
interface serial 1
ipx network 10
ipx out-sap-filter 1000
```

IPX Clients

Router C does not require an access list configuration because the remote site does not have any servers. Only Novell servers generate SAP updates.

Configuring Incremental SAP Updates

Incremental SAP updates allow any-to-any connectivity with reduced network SAP overhead. Instead of eliminating the receipt of SAP updates entirely, all necessary IPX services can be broadcast to remote sites only as changes to the SAP tables occur.

Central Site

To configure Enhanced IGRP encapsulated SAP updates to be sent only on a incremental basis, use the following configuration. Although the defined Enhanced IGRP autonomous system number is 999, Enhanced IGRP routing (and routing updates) are not performed because of the **rsup-only** keyword used with the **ipx sap-incremental** command. The **rsup-only** keyword indicates a reliable SAP update.

```
interface ethernet 0
ipx network 20
!
interface serial 0
ipx network 10
ipx sap-incremental eigrp 999 rsup-only
!
ipx router eigrp 999
network 10
```

To configure both incremental SAP and Enhanced IGRP routing, simply configure Enhanced IGRP with the following commands:

```
interface ethernet 0
ipx network 20
!
interface serial 0
ipx network 10
!
```

```
ipx router eigrp 999
network 10
```

Remote Sites

This section provides information on the configuration of the routers at the remote sites:

- Router B connected to an IPX server and client
- Router C connected to two IPX clients

IPX Server and Client

To configure Enhanced IGRP encapsulated SAP updates to be sent only on a incremental basis, use the following configuration for Router B. Although the defined Enhanced IGRP autonomous system number is 999, Enhanced IGRP routing is not performed because of the **rsup-only** keyword used with the **ipx sap-incremental** command.

```
interface ethernet 1
ipx network 30
!
interface serial 1
ipx network 10
ipx sap-incremental eigrp 999 rsup-only
!
ipx router eigrp 999
network 10
```

To configure both incremental SAP and Enhanced IGRP routing, simply configure Enhanced IGRP with the following commands:

```
interface ethernet 1
ipx network 30
!
interface serial 1
ipx network 10
!
ipx router eigrp 999
network 10
```

IPX Clients

To configure Enhanced IGRP encapsulated SAP updates to be sent only on a incremental basis, use the following configuration for Router C:

```
interface ethernet 2
ipx network 40
!
interface serial 2
ipx network 10
ipx sap-incremental eigrp 999 rsup-only
!
ipx router eigrp 999
network 10
```

Even though there are no servers, these configuration commands are required to support the incremental SAP updates being advertised from the central site and other remote sites to Router C.

Summary

This case study illustrates two methods of reducing SAP traffic on Novell IPX networks: the use of access lists to eliminate the advertisements of specified services, and the use of the incremental SAP feature to exchange SAP changes as they occur. This technique eliminates periodic SAP updates.