As we explained in the October 1999 issue of NetWare Connection, Novell has provided several technologies and migration strategies to help you migrate your company's network from IPX to pure IP. (See “Switching From IPX to IP,” p. 6–14. You can download this article from http://www.nwconnection.com/past.) However, choosing a migration strategy is not strictly a technical decision. This decision is heavily influenced by a company's network infrastructure, its functional requirements, its workflow habits, and its organizational structure.

To help you understand the process of choosing and implementing a migration strategy, this article presents a case study of a fictional company, Migration Enterprises Inc. To remove IPX traffic from WAN links and use WAN link bandwidth more efficiently, Migration Enterprises will complete the following steps:

1. Identify an appropriate migration strategy and determine how the company's functional requirements and the physical network impact this strategy.
2. Plan and set up the Service Location Protocol (SLP) infrastructure required to facilitate the removal of IPX from the WAN segments, given the company's functional requirements.
3. Place Migration Agents (MAs) on the network.

Note: If you, like Migration Enterprises, are planning a migration from IPX to pure IP with NetWare 5, you should be familiar with SLP as defined in Request for Comments (RFC) 2165. (For more information about RFC 2165, visit http://www.ietf.org/rfc/rfc2165.txt.) You should also be familiar with Novell's Compatibility Mode Driver (CMD). (For more information about CMD, see “Understanding SCMD Mechanics and Processes,” Novell AppNotes, Aug. 1999. You can download this article from http://developer.novell.com/research/appnotes.htm.)

UNDERSTANDING THE COMPANY

Migration Enterprises has 300 offices located throughout the United States. Each office maintains its own hardware infrastructure and IT services, which include at least one NetWare server per location. Each remote office site is connected to the main corporate network through a WAN link. As a result, Migration Enterprises uses a distributed administration model: Departmental administrators in each remote office have control over their portion of the network.

Migration Enterprises has established several central IT groups who are responsible for setting standards and proposing technology direction for the entire company. For example, one group handles systems administration and is responsible for network resources such as the company's Novell Directory Services (NDS) tree. Another group is responsible for the data communications of the enterprise network and for the physical connectivity including routers and switches.

The main problem plaguing Migration Enterprises is that the WAN links between remote sites and the corporate network are being cluttered with Routing Information Protocol (RIP)/Service Advertising Protocol (SAP) information. (IPX traffic is not filtered across the WAN links.) NetWare 5 appears to be a good solution to this problem. The big question is this: Given the unique characteristics of Migration Enterprises' organization and network, what is the best strategy for performing this migration?

DETERMINING THE MIGRATION STRATEGY

The distributed nature of Migration Enterprises’ network administration does not lend itself well to the dictation of and strict adherence to standards. The central IT groups can propose standards, but they cannot necessarily enforce these standards.

Although the central IT groups do not have the authority to dictate desktop standards or LAN protocol standards, they do control which protocols traverse WAN links, and they do control the key NetWare servers that make up the overall network infrastructure. As a result, the central IT groups can choose a migration strategy that will eliminate RIP/SAP traffic from WAN links, and they can implement this strategy without impacting departmental administrators. To meet these requirements, the central IT groups will use NetWare Migration Agents (MAs) to remove IPX from WAN links.
Removing IPX from WAN links is only the first step in the process of implementing a pure IP network. After IPX has been removed from WAN links, Migration Enterprises’ regional offices can begin converting local LANs to pure IP. After the local LANs are migrated to pure IP, MASs will no longer be required to provide the connections across the WAN links.

IDENTIFYING THE FUNCTIONAL REQUIREMENTS

After Migration Enterprises selects an overall migration strategy, the central IT groups can then identify the functional requirements of the migration. These functional requirements, which are listed below, will impact the actual design and implementation of the migration strategy.

- After IPX is removed from the WAN segments, all NetWare servers must remain visible from all locations.
- The central IT groups must minimize the amount of manual configuration required on servers. These groups do not want to be responsible for maintaining individual settings on hundreds of servers across the enterprise network.
- Multicast will not be enabled end-to-end on the enterprise network. Multicast may be enabled for portions of the network, but end-to-end use of multicast is not an option.

The Physical Network

Using these functional requirements, the central IT groups can evaluate the physical layout of the network. The network layout dictates the placement of the infrastructure servers and helps the central IT groups understand the new traffic flow on the network. Fortunately, Migration Enterprises already has a current map of its network infrastructure. (See Figure 1.)

The speed of the WAN links between regional offices varies, depending on the size of the regional office and the traffic patterns associated with that office. No link is slower than 56 kbps, and some links are T-1 lines.

The WAN links are managed through a Switched Multimegabit Data Service (SMDS) cloud. Each SMDS cloud services 25 regional offices. These links return from the regional sites through the SMDS clouds at three main sites, which are called POP sites. These POP sites are redundantly connected to each other.

Figure 1. The Migration Enterprises network

No POP site has more than four SMDS clouds connected to it. The backbone connections between these POP sites are T-3 links.

Figure 1 shows how network traffic flows between regional office sites. At this point, it is not important to know specifically which offices are connected to which SMDS clouds; however, the groupings of the clouds themselves are important. Network traffic will be isolated based upon the POP site to which the SMDS cloud is connected.

Figure 1 also shows the WAN links that are targeted for IP only. All SMDS clouds will be routing only IP traffic, and

Please visit our advertiser:

Biscom Inc.

http://www.biscom.com/cd_offer

For more information, visit http://www.nwconnection.com/advertise.html.
only IP traffic will be passing between POP sites.

CREATING THE DESIGN PLAN

After the central IT groups have evaluated the physical network, they can begin to formulate a design plan. For Migration Enterprises, the design plan will use SLP for dynamic service discovery. The design plan will also use Novell’s CMD.

Figure 2 shows how MAs, which are used for SLP, will be placed on the network. To facilitate the removal of IPX from the WAN links, each regional office will have an MA acting in Backbone Support mode (not shown in Figure 2). In addition, each POP site will have a number of MAs in Backbone Support mode.

Multicast will also be enabled on a per-POP basis. That is, multicast will be supported between the regional offices through the SMDS cloud up to the POP site itself. However, multicast packets will not be forwarded from POP site to POP site. In effect, each POP site and its associated SMDS clouds will become a multicast “island.”

This migration strategy addresses the needs defined in the functional requirements as follows:

• The use of MAs in Backbone Support mode will make all IPX-based services visible on the network. Users in one regional office will be able to see the servers in all other regional offices.
• Using multicast will minimize the manual configuration required on servers. Within the multicast islands, devices will use multicast to dynamically discover MAs.
• Multicast will not be enabled end-to-end on the network. No multicast packet generated on the network can pass beyond its local POP site.

BUILDING THE SLP INFRASTRUCTURE

SLP is one of the primary methods for providing service discovery and resolution in a NetWare 5 environment. For most NetWare 5 implementations, using SLP is requisite. Certain modules—such as CMD—have inherent dependencies upon SLP. SLP is also required to allow the MAs to dynamically discover each other on the network.

SLP uses user and service agents to discover services on the network. In a NetWare 5 environment, NetWare 5 servers contain SLP service agents, and the latest versions of the NetWare are client contain SLP user agents.

SLP is a passive protocol driven by user agent requests and service agent registrations. When a user agent sends a query to the network, all service agents holding pertinent information must respond.

To communicate, both user and service agents must use multicast end-to-end on the network. Because Migration Enterprises is not going to support multicast end-to-end on the network, it needs DAs to facilitate the communication between user agents and service agents. The DA’s exchange information to make the SLP services from one multicast island available to other multicast islands on the network.

Note: SLP makes use of TCP and UDP packets addressed to port 427. SLP requests can be identified in a packet trace through this unique characteristic.

Because the primary purpose of the migration strategy is to remove IPX from the WAN links, only servers contributing to that end goal need to participate in the SLP infrastructure. Initially, only the DAs and MAs will use the SLP infrastructure. Of course, as more NetWare 5 servers are added to the Migration Enterprises network, they can use the SLP infrastructure.

Creating an SLP Scope

The central IT group responsible for the NDS tree will create a separate Organizational Unit (OU) just below the Organization object to hold all SLP-related information. This OU will hold the NDS objects representing the DA and Scope Unit objects that will contain the SLP service objects.

The use of SLP scopes is required if the network includes more than 1,000 SLP services. For the initial migration strategy, one scope will be sufficient; however, as the presence of NetWare 5 grows on the Migration Enterprises network, the central IT group will need to create new SLP scopes to handle the new SLP services.

For the purposes of this case study, the name of the SLP scope is ME_SCOPE. Although creating a custom SLP scope will require the central IT groups to manually configure all servers that participate in the SLP infrastructure, the custom SLP scope is being created for future compatibility. When SLP v2 is eventually implemented, the custom SLP scope will provide easier compatibility between SLP v1 and the future version defined in RFC 2608. (You can view this RFC at http://www.ietf.org/rfc/rfc2608.txt.)

Discovering DAs

The DA acts as a central repository of SLP service information. All service agents on the network register their list of available services with the DA. All user agents that use DAs direct their requests to the DA instead of sending the request as a multicast packet. Because user agents...
and service agents are using unicast packets instead of multicast packets, network bandwidth is used more efficiently. Also, traffic can be isolated based upon the physical network topology instead of having to enable multicast packets end-to-end on the network.

User and service agents can discover DAs in one of three ways:

• Through multicast packets
• Through Dynamic Host Configuration Protocol (DHCP) information
• Through manual configuration

Multicast Discovery. If multicast is enabled on a network, using multicast to discover DAs is a good option. User and service agents send one multicast packet when they are loaded. DAs also send one multicast packet when they are loaded.

When a DA is loaded on a NetWare 5 server, the DA sends out an Internet Group Message Protocol (IGMP) multicast request to join the DA multicast group. The address for this multicast group is 224.0.1.35. Routers can then forward DA discovery packets to the DAs on the network.

When service agents are loaded on servers that are configured to discover DAs through multicast, these service agents send a multicast request to the DA multicast address (224.0.1.35). All DAs on the network respond to the request using a unicast packet.

A DA has been “activated” by a user or service agent, that DA is used for all SLP service requests. The user or service agent no longer sends multicast to discover services on the network. Figure 3 shows the traffic pattern on the Migration Enterprises network when service agents are configured to discover DAs through multicast. (See Figure 3 on p. 32.)

From the MA perspective, the DA that first responds to the multicast request for a given SLP scope will be the primary DA for that scope. The MA will send all future SLP queries to that DA through a unicast SLP packet. If the primary DA for a user agent is unavailable, the user agent tries the next DA in the list for that scope.

For example, Figure 3 shows one multicast island on the Migration Enterprises network. This island has two DAs. Because the multicast packet from the MA reaches both DAs, both DAs respond to the MA. The first response the MA receives is the primary DA. If that DA is ever unavailable, the MA will try the other DA in the DA list.

DHCP Discovery. The central IT groups can use two DHCP options to dynamically deliver DA configuration information: Option 78 allows a DHCP client to obtain DA address information; option 79 allows a DHCP client to obtain SLP scope information.

If DHCP is configured to deliver DA configuration information, user and service agents should not use multicast to discover DAs on the network. Both NetWare client and NetWare servers can use DHCP to obtain DA and SLP scope information.

When a NetWare client obtains an IP address from a DHCP server, this client can also receive DA and SLP scope information. A NetWare server sends a request to a DHCP server to retrieve option information—including DA and SLP scope information. However, a NetWare server does not receive an IP address from a DHCP server. NetWare servers must have statically configured IP addresses.

Static Discovery. The final method of DA discovery is through manual configuration. With manual configuration, the addresses of the DAs on the network are manually entered by user and service agents using a unicast packet.

Manually configuring service agents is fairly simple in the NetWare environment. The SYS:ETC directory on each NetWare 5 server contains the SLP.CFG file, which is used to hard-code DA information. To specify a DA in this file, use the following format:

DA IPv4, <ip_address_of_DA>

The SLP.CFG file can contain any number of addresses. The service agent running on the server registers with each DA listed.

User agents, on the other hand, use only the first activated DA from the list to retrieve SLP service information. If this primary DA is not available, the user agent contacts the next DA configured in the list.

Currently, you can use fully qualified Domain Naming System (DNS) names in the SLP.CFG file to specify DAs; however, only the first DA specified in the list can be identified in such a manner.
NetWare Connection February 2000

Figure 3. Dynamic discovery of DAs on the Migration Enterprises network

Multicast Island

1. Multicast SLP packet addressed to 224.0.1.35
2. DA responds with unicast SLP packet addressed to original host
3. DA responds with unicast SLP packet addressed to original host
4. MA builds a list of known DAs

The SET SLP DA DISCOVERY OPTIONS parameter setting is based on a bit comparison test. If the least significant bit of the parameter is set to 1, the server attempts to discover DAs through multicast. If the second least significant bit of the parameter is set to 1, the server attempts to discover DAs through DHCP.

You can configure a server to use multiple methods of discovery by performing a bit-wise Boolean OR of the desired value. Thus, if you want a NetWare 5 server to use both multicast discovery and static discovery, the calculation of the value would be as follows:

```
00000001  Discovery through multicast
00000100  Discovery through static configuration
```

The value for this parameter can be between 129 and 65,535 seconds. You should be careful how you set this value. Too small a TTL setting can lead to increased network traffic since service agents will need to re-register services more frequently. Too large a TTL setting can lead to the advertisement of services that are no longer available because a server may be down or a service may be disrupted.

Service agents register services with all known DAs. Thus, if a service agent knows five DAs, it sends five separate registration requests—one to each DA.

When DAs are enabled and service agents are configured to use the DAs, a service agent registers all SLP-enabled services on the server with the DA. It is important to understand this service registration process and how it impacts network traffic.

When a service agent registers a service, it attaches an associated time-to-live (TTL) to the service. The DA looks at the service’s TTL and begins a countdown based on the time since the service was registered. When the TTL reaches zero, the service is presumed to be no longer valid, and the DA no longer advertises the service.

The service agent must re-register the service with the DA before the TTL of the service expires. If the service agent fails to do so, an interruption in service may occur because the service will no longer be advertised by the DA.

The default TTL for Novell service agents is 3600 seconds (or one hour). Entering the following command at the server console sets the TTL for all services registered by that service agent:

```
SET SLP SA DEFAULT LIFETIME = <value>
```

The value for this parameter can be between 129 and 65,535 seconds. You should be careful how you set this value. Too small a TTL setting can lead to increased network traffic since service agents must contact DAs more frequently to re-register services. Too large a TTL can lead to the advertisement of services that are no longer available because a server may be down or a service may be disrupted.

Service agents register services with all known DAs. Thus, if a service agent knows five DAs, it sends five separate registration requests—one to each DA. Although registering with multiple DAs ensures fault tolerance, this SLP overhead can increase network traffic.

When a DA receives a registration request, it creates an entry for the service in its database. This entry contains the name of the service, the type of service, the attributes of the service, and the TTL. The DA then sends an acknowledgment to the service agent, indicating the service has been registered.

Figure 4 shows the entire registration process. (See p. 34.) There are some important points to note about this registration process. First, without a method for...
DA-to-DA synchronization, the list of services an MA retrieves depends upon which DA the MA contacts. For example, if the MA in Figure 4 requests a list of SLP services from DA2, DA2 only knows about MA1. Second, after the DA discovery process, all SLP transactions are accomplished via unicast SLP packets. Service agents are supposed to deregister a DA if a service is no longer available. The DA will then no longer advertise the service to user agents. Servers that are brought down gracefully notify the DA to remove their services.

Migration Enterprises will use the default TTL value of one hour in the implementation of the migration strategy. The central IT groups think that this value is a fair compromise after they weighed the cost of re-registration traffic versus the bandwidth on the WAN links between the regional offices and the POP sites. Users will never know about SLP services because they will be using IPX-dependent clients. Only the MAs will use the SLP infrastructure to discover other MAs for exchanging IPX information.

UNDERSTANDING NOVELL’S IMPLEMENTATION OF THE DA
Although RFC 2165 clearly defines SLP user agents and service agents, some areas of interpretation are left open with regard to DAs. For example, the RFC indicates the methods by which DAs can communicate with service and user agents. However, the RFC does not address the issue of DA-to-DA synchronization or the structure of the database that the DA uses to store SLP information.

NDS is one of the best object-oriented, distributed databases on the market, and it already takes care of such critical issues as synchronization. Not surprisingly, Novell used NDS as the back end for an SLP object data store and as a method of DA-to-DA synchronization.

In Novell’s implementation of the DA, user agents, service agents, and DAs communicate as described in this article. When a DA receives a service registration from a service agent, however, the DA creates an object in its local SLP cache. In addition, the DA creates or modifies an object in NDS to update the service.

When a DA is loaded, configuration information is stored in NDS for that DA. This information includes the server on which the DA is running and the SLP scope the DA is servicing.

For each scope defined in the SLP infrastructure, an SLP Scope Unit object is defined within NDS. Also in NDS, each DA object is configured to service a particular set of scopes. When the Novell DA receives an SLP service registration, it checks its local SLP cache. From there, one of two things can happen:

- If the service doesn’t exist in the local SLP cache, the DA creates an entry for the service with the attributes defined in the SLP registration packet. The DA then creates an NDS SLP Service object in each scope for which the DA is responsible.
- If the service exists in the local SLP cache, the DA modifies the entry. The DA also modifies the associated NDS SLP Service object in all of the scopes the DA services.

Does e-mail outsourcing make sense?

Yes.

According to Gartner Group, 40 percent of companies will decide to outsource all or part of their e-mail systems by 2001. Here’s why.

The evolution of e-mail from novelty item to business-critical status has been dramatic in recent years.

With that shift, companies of all sizes have begun outsourcing maintenance and day-to-day operation of their e-mail systems.

Fueling this trend is the challenge of offering the latest features – fax and paging service and access for remote and distributed users – while retaining skilled IT personnel in a competitive job market and controlling costs.

If you’re evaluating whether to outsource your e-mail system, Allegro – an industry leader in managed messaging – recommends you consider the vendor’s technical expertise, reputation, business understanding and communication access.

Call Allegro or visit us online to see how we can cut your e-mail expenses by up to 50 percent.
When a DA modifies the NDS SLP Service object, an NDS synchronization event is triggered, and all replicas of the partition that contain the NDS SLP Service object exchange information to make the partition consistent. The other DA’s on the network see the NDS synchronization event and reread the SLP service information from NDS to update their local SLP caches.

The NDS SLP Service objects contained in each scope reflect the SLP information for the entire network. Service agents that belong to the same scope do not have to register with all DAs servicing their scope. A service agent needs to register with only one DA. Assuming that all the DAs are in the same scope and that all DA’s hold a replica of the partition that contains the NDS SLP Service objects, the other DAs on the network will learn of the service without the service agent having to directly register via SLP.

You can use NDS to isolate SLP registration traffic. Service agents need to register only with their local DA, and NDS synchronization will propagate the registered SLP service to other DA’s servicing the SLP scope. A s a result, any user agent on the network can retrieve the same list of SLP services regardless of which DA is queried.

When a service agent de-registers with a Novell DA, this DA does not remove the service from NDS or from its local SLP cache. The DA simply sets the TTL of the object to zero, thereby preventing the DA from advertising the service to user agents. When the service re-registers, the object does not have to be re-created in cache and NDS; the TTL of the object is simply renewed.

To enable DAs to discover each other, the Migration Enterprises network requires the NDS method of SLP service propagation. All of the service agents (MAs) in a local multicast island will register with the dynamically discovered local DAs. The DAs at each POP site register known services to a common Scope object in NDS. As a result, the DA’s learn about all of the SLP services on the network through the NDS synchronization process.

**Figure 4. The SLP service registration process**

The NDS SLP Service objects contained in each scope reflect the SLP information for the entire network. Service agents that belong to the same scope do not have to register with all DAs servicing their scope. A service agent needs to register with only one DA. Assuming that all the DAs are in the same scope and that all DA’s hold a replica of the partition that contains the NDS SLP Service objects, the other DAs on the network will learn of the service without the service agent having to directly register via SLP.

You can use NDS to isolate SLP registration traffic. Service agents need to register only with their local DA, and NDS synchronization will propagate the registered SLP service to other DA’s servicing the SLP scope. A s a result, any user agent on the network can retrieve the same list of SLP services regardless of which DA is queried.

When a service agent de-registers with a Novell DA, this DA does not remove the service from NDS or from its local SLP cache. The DA simply sets the TTL of the object to zero, thereby preventing the DA from advertising the service to user agents. When the service re-registers, the object does not have to be re-created in cache and NDS; the TTL of the object is simply renewed.

To enable DAs to discover each other, the Migration Enterprises network requires the NDS method of SLP service propagation. All of the service agents (MAs) in a local multicast island will register with the dynamically discovered local DAs. The DAs at each POP site register known services to a common Scope object in NDS. As a result, the DA’s learn about all of the SLP services on the network through the NDS synchronization process.

**IMPACT OF THE MIGRATION STRATEGY ON THE NDS TREE**

Because the DAs and the NDS tree are closely intertwined, the registration of SLP services will affect both the design of the Migration Enterprises NDS tree and the network performance. From a design strategy, each NDS Scope U nit object should be made its own NDS partition because the Scope Unit object is an active area of the NDS tree. Each time a DA registers an SLP service in NDS, a partition synchronization event is triggered. Compound this synchronization event over the 300 registrations that will occur per hour on the Migration Enterprises network, and it will produce a significant amount of NDS traffic.

In addition, each DA that services the scope should hold a replica of that partition. This is the only way the DA can efficiently update the SLP object information in NDS. If a DA is running on a server that does not hold a replica of the partition that contains the SLP scope the DA services, this DA updates its local cache once only per day.

For the Migration Enterprises network, the central IT groups will make the ME_SCOPE container object a partition. This partition will be replicated only to the DAs that service the scope at the POP sites. This design will minimize the size of the active NDS partition and make the synchronization process more efficient.

The NDS synchronization traffic on the network between the POP sites may seem like a lot of overhead. From a W A N link perspective, however, the only overhead traffic associated with SLP on the slow W A N links in the SMDS clouds is the initial discovery of the DA’s, the periodic registrations of SLP services, and the occasional SLP lookup by the MAs. This traffic will be unicast packets.

Compared to the once-per-minute broadcast of RIP/SAP information required for IPX communications, the benefit of the SLP implementation is clear. The amount of traffic traversing the W A N links will be greatly reduced (although there will be some overhead associated with the MAs, as is explained in the next section). The spike in traffic will be between the POP sites, which are linked by T-3 lines. These connections can certainly handle this increased traffic.

**SETTING UP THE MAS**

Now that the central IT groups have designed the SLP structure, they will deploy MAs, which will enable the central IT groups to remove IPX from the W A N links. A fter IPX is removed, the Migration Enterprises network will really be a set of IPX-based LANs that communicate with each other over IP-only links. The best way to facilitate that communication is to use MAs in Backbone Support Mode.

To the IPX-based devices on the network, the IP-only W A N links will look like a virtual IPX network (also known as a C M D network). The MAs will encapsulate the IPX packets destined for a non-contiguous IPX segment in an IP packet and forward this IP packet to the MA that serves the remote IPX segment. The destination MA will un-encapsulate the IP packet and send the undisturbed IPX packet on the IPX segment where it will
Configuring Backbone Support

You can easily configure a server to function as a Backbone Support MA. You simply load SCMD.NLM on the server with the /G, /MA, or /BS option. The server must also be enabled to use NetWare Link Services Protocol (NLSP) routing. To configure NLSP routing, you use INETCFG.NLM.

If the server has been configured as a Backbone Support MA, the server will use one of the following methods to find other servers that are configured as Backbone Support MAs:

- The server will query SLP for services of type mgw.novell. These services indicate other Backbone Support MAs available on the network.
- The server will use a statically configured list of other Backbone Support servers available on the network.

Note: If one Backbone Support MA is statically configured to look for other Backbone Support MAs, all Backbone Support MAs on the same CMD network must be statically configured.

Backbone Support MAs must be part of the same CMD network in order to communicate and exchange bindery information with one another. Backbone Support MAs that belong to separate CMD networks will not communicate with each other to exchange bindery information or encapsulated data packets.

A server Backbone Support MA discovers one another, they exchange RIP/SAP information. They will continue to exchange this information to keep the services advertised on their respective IPX networks current.

To meet the functional requirements of Migration Enterprises, the Backbone Support MAs will rely on the SLP infrastructure, which was created for this purpose. Remember, manually configuring 300 MAs is not an option for the central IT groups at Migration Enterprises.

Enabling MA-to-MA Communication

When Backbone Support MAs exchange bindery information, they use MA-to-MA communication protocol. There are some special considerations you must make when enabling a large number of servers as Backbone Support MAs because NLSP has some overhead.

After Backbone Support MAs on the same CMD network discover each other, they become NLSP neighbors in the virtual IPX network that has been created for CMD. Because these servers are NLSP neighbors, they must exchange the normal overhead packets required for NLSP routing. These administrative packets (or Hello packets) are required to maintain the NLSP routing tables. If the Hello packets are not received within a specific time, the NLSP router marks its neighbor as being unavailable.

For example, suppose server NLSP1 sends a Hello packet to its neighbors via broadcast (because it is an IPX environment). The neighbor NLSP routers receive this packet and update their tables to reflect the refresh of NLSP1 as active. The neighbor NLSP routers update the TTL of NLSP1 in their NLSP table. If the TTL of NLSP1 reaches zero, it will be marked as unavailable and will not be used as a route to reach destination services.

By default, NLSP routers send Hello packets every 20 seconds. NLSP routers use a multiplier of three to determine the TTL for the NLSP router in the NLSP neighbor table. For example, the default TTL for the neighbor router is 60 seconds. To control NLSP overhead traffic, you can modify the multiplier and Hello packet interval.
protocol and IPX encapsulation is not broadcast-based, SCMD has to do a lot of work to mimic the NLSP environment. SCMD must send the IPX broadcast information to all required destinations. (See Figure 5 on p. 35.)

When the NLSP Hello packet is passed from the IPXRT module of the NetWare server to the virtual IPX network, SCMD takes over. SCMD encapsulates the Hello packet and individually addresses the packet to each known Backbone Support MA on the same CMD network. For example, when one NLSP Hello packet is sent on the network shown in Figure 5, SCMD must send three encapsulated packets across the IPX-only network to update the NLSP neighbor tables.

As the number of Backbone Support MAs on the same CMD network increases, the number of packets required for NLSP overhead also increases. As Backbone Support MAs on the same CMD network must communicate with all other Backbone Support MAs in this manner, this communication must be factored into any Backbone Support design.

In addition to the overhead NLSP traffic, the normal bindery information will flow between the MAs. However, this is where the benefit of NLSP is seen: Because NLSP is a link-state routing protocol, it communicates only changes in its routing tables to its neighbors. Instead of broadcasting the entire RIP/SAP table of a server every minute, an NLSP router sends only the changes it receives. The bindery information sent across the CMD network from MA to MA is drastically reduced because these MAs are NLSP neighbors. Therefore, the encapsulated NLSP traffic on the CMD network is significantly smaller than the amount of RIP/SAP traffic that would have to be sent in a normal IPX environment.

**Filtering Considerations With Backbone Support**

Before implementing the MA-to-MA protocol on a network, you should consider the implications this protocol may have. Because this protocol is a virtual routing environment that sits on top of an existing physical routing environment, you can route information across this virtual network that would not normally be permitted across the physical network.

For example, Figure 6 shows a physical IPX network with two IPX segments. Between these IPX segments is a router that filters SAP information. IPX services on network segment 1 are not visible on network segment 2, and vice versa. A Backbone Support MA is then installed on both IPX segments, and the two MAs discover one another through SLP.

Through the MA-to-MA protocol, IPX network segment 1 can see service information about IPX network segment 2. The RIP/SAP information is sent across the virtual IPX network, and the filters on the router are bypassed.

If the MA-to-MA protocol is used in such an environment, the filtering used on the physical network must be applied to the virtual network. To enable and enforce such filters on a NetWare server, you load and configure the latest version of the SCMD.NLM as an LND driver. To load and configure the SCMD.NLM as an LND driver, you use INETCFG.NLM. You can then use FILTCFG.NLM to configure filters.

**The MA Infrastructure**

After the central IT groups review MAs and understand how Backbone Support mode works, the groups can plan an MA infrastructure that will fit the needs of their corporate network. The critical pieces are properly deploying the MAs to control the amount of NLSP overhead, while still maintaining the end-to-end visibility of IPX services.

As far as the migration strategy is concerned, it is best to think of the Migration Enterprises network as 300 noncontiguous IPX segments that have to be connected across an IP-only backbone. With the MAs able to function in Backbone Support mode, this connectivity can be achieved, but it is going to take careful planning to make sure the network is not saturated with overhead traffic.

Effectively, Migration Enterprises will need to use at least 300 MAs to achieve the first step in the migration strategy. Fortunately, each regional office already has a server that can function as an MA.

Unfortunately, loading SCMD.NLM on each server won't be easy. Think about the NLSP overhead traffic of having 300 Backbone Support MAs all belonging to the same CMD network. Each MA will send an encapsulated NLSP Hello packet to the other 299 servers at least once per minute. This amounts to almost 90,000 packets of overhead traffic per minute, not including the bindery information transfer between networks or normal data traffic.

The central IT groups must come up with another solution that will allow for the end-to-end advertisement of IPX services on the network and also minimize the amount of overhead traffic required to keep the noncontiguous IPX networks connected. The solution is implementing multiple CMD networks on the network.

**Implementing Multiple CMD Networks**

As has been mentioned previously, only MAs belonging to the same CMD network will need to exchange NLSP Hello packets. MAs belonging to separate CMD networks will not exchange this information because they are not considered to be NLSP neighbors.

Given this fact, the central IT groups can review the network infrastructure and determine how to implement the CMD networks. As Figure 1 shows, the logical subdivision in the network is the SMDS cloud. (See p. 29.) The SMDS is a manageable unit to which 25 sites are connected, and 25 MAs in each CMD network is certainly an acceptable configuration. The overhead traffic required for 25 servers is significantly less than the traffic required for 300 servers in the same CMD network.

You may wonder how separate CMD networks will be able to propagate their bindery information to other CMD networks. The trick is to have a shared IPX segment where MAs belonging to different CMD networks can exchange their RIP/SAP information. The sole function of this common IPX segment is to facilitate a per-minute broadcast of RIP/SAP information between MAs. This RIP/SAP
broadcast will force each MA to become aware of the services available through the other CMD network. In turn, that information will be propagated to the remote IPX segments at each end.

The logical common point for the exchange of RIP/SAP information between the CMD networks (SMDS clouds) is the POP sites. For each CMD network that needs to exchange RIP/SAP information, the central IT groups will create a separate MA at the POP site. Each POP site will have 5 MAs to handle the 4 CMD networks corresponding to the SMDS clouds and the one CMD network corresponding to the links between the POP sites themselves.

Only one SCMD.NLM can be loaded one each NetWare server. A ISO, each SCMD.NLM driver can only accommodate one CMD network. A new version of SCMD.NLM supports multiple CMD networks. This updated SCMD.NLM is available in NetWare 5 Support Pack 4. By installing this support pack, Migration Enterprises will need only one MA per POP site to handle the exchange of RIP/SAP information between CMD networks.

Figure 7 shows the CMD network structure required for Migration Enterprises. Note the CMD network corresponding to each SMDS cloud and the CMD network required between the POP sites to exchange RIP/SAP information between the multicast islands. Each CMD network looks like just another IPX segment. Thus, all CMD network numbers must be unique to the entire network just like IPX network numbers must be unique.

Although having multiple CMD networks is the most elegant solution for Migration Enterprises, it will require some manual configuration of servers. Each server on which the MA is loaded will have to be configured to belong to a specific CMD network. The CMD network specification is just another SET parameter on the NetWare 5 server (SET CMD NETWORK NUMBER), which can be set at the server console or through MONITOR.NLM.

Note: DHCP can be used to dynamically distribute CMD network information to NetWare servers, which will reduce the manual configuration required. The CMD network option for DHCP is option tag 63, suboption 12. Migration Enterprises will need to implement this technology to achieve its functional requirements.

CONCLUSION

Now that the migration strategy has been planned, the central IT groups are confident they have a well-planned infrastructure to begin the migration of their corporate network to a pure IP environment. In planning any strategy to migrate from an IPX to a pure IP environment, you should gather the organization's functional requirements and the physical layout of the network. You can then set specific goals for that particular organization. After you set the initial goals, it is just a matter of understanding the technology required and the impact it will have on the network. This understanding is key to fleshing out the details of the migration strategy. Without this understanding, you can conceivably create a migration environment that is much less efficient than the current environment, which usually has IPX flowing freely from end-to-end.

Editor's Note: This article is taken from the Novell AppNotes article, "Removing IPX from WAN Segments During an Upgrade to NetWare 5: A Case Study." You can download this article from http://developer.novell.com/research/appnotes/1999/september/a4frame.htm.

Heath C. Ramsey is a Novell consultant who specializes in IPX to TCP/IP protocol migration strategies in enterprise networking environments. Heath is also interested in large-scale messaging infrastructures and metadirectory technology.