Migrating to Pure IP with NetWare 5

Articles and Tips: article

COREY PLETT
Technical Writer
Documentation Development Group

01 Sep 1998

Support Home
Download
Help yourself
Let us help
Contribute

Customer Center

For those who are standardizing on TCP/IP for their network protocol, this AppNote discusses the issues and processes involved in migrating to Pure IP with NetWare 5.

Introduction

NetWare 5 provides the ability to access NetWare services through the use of the IP networking protocol. As an open standard, Pure IP offers flexibility and interoperability previously unavailable to users of NetWare. Although many network administrators may use both IP and IPX on their networks, a Pure IP network is easier to administer, and more easily integrated with other systems such as UNIX and Windows NT. New IP migration components and services in NetWare 5 make migrating to a Pure IP network manageable, even for the largest networks. Whether you choose to migrate from IPX to IP will largely depend upon the goals of your organization.

Because of the complexity of migrating a NetWare IPX network to Pure IP, there is no single migration utility or patch. Most PC-based networks have evolved over the last 10-15 years. Some networks were designed specifically, while others grew as system administrators addressed the immediate needs of their organization. Any administrator attempting to migrate from one network protocol to another is faced with the challenge of implementing the new technology while providing continued access to all existing network services.

The challenges of migrating can be offset by their benefits. Migrating a NetWare network from IPX to IP reduces administrative costs, especially if you are already supporting both protocols, or if you are expending a significant portion of your Information Services' (IS) budget managing IPX.

Migration Components

Because of the complexity of migrating an IPX-based network to an IP-based network, the migration components have been integrated into NetWare 5 rather than placed in a separate migration tool. The migration components, and more specifically, the IPX Compatibility Mode Drivers, are used by the server only when an IPX application requires them. And because an IPX stack is loaded on the server, some IPX symbols may persist. This does not mean, though, that the system is using IPX on the wire, only that the system is compatible with IPX if it is needed by an IPX application. If there are no requests for IPX, IPX is not used.

Besides IPX Compatibility Mode Drivers, there are a number of other components that facilitate IPX to IP migration in NetWare 5. They include:

- Migration Agent
- Protocol Independent NetWare Client and Server
- Protocol Independent Novell Directory Services
- Service Location Protocol
- Domain Name Service
- Dynamic Host Control Protocol

IPX Compatibility Mode Drivers

The IPX Compatibility Mode Drivers are the core of the IPX Compatibility feature. These drivers are automatically loaded in both the NetWare Clients and Servers when installed as IP only systems. The IPX Compatibility Driver provides IPX connectivity over the IP network allows applications using the IPX stack to function in a Pure IP network. The IPX Compatibility driver also allows IP systems to communicate with IPX systems by utilizing the services of Migration Agents.

The IPX Compatibility driver treats the IP Network as a virtual IPX Network Segment (CMD Network Segment), by encapsulating IPX datagrams inside of UDP datagrams, and by resolving RIP and SAP requests through the use of the Service Location Protocol (SLP).

The services of the IPX Compatibility drivers are only utilized when the system uses an IPX application or tries to establish connections between IP and IPX systems. When not in use, the IPX Compatibility drivers are dormant and do not effect network communications.

To run IPX applications in your IP network or to connect IP systems with IPX systems, Service Location Protocol (SLP) must be enabled across the network since the IPX Compatibility Drivers are dependent upon the capabilities of SLP. Additionally, at least one Migration Agent must be used on the network if you interconnect IPX and IP systems.

The default IPX network number (CMD Network Number) assigned to the Virtual IPX Network created by the IPX Compatibility Drivers is 0xFFFFFFFD. Migration Agents that interconnect IP Systems with IPX systems must have a CMD Network Number that does not conflict with the internal IPX network number of any server or the IPX network number of any network segment. Also, IPX routers should not filter this address.

If a system or a segment conflicts with the CMD Network Number you can either override the default CMD Network Number by modifying the configuration of the IP only clients and servers, or change the network number of the conflicting system or segment.

Migration Agent

The Migration Agent is a migration component that enables communication between IPX and IP systems and/or creates an IP backbone that interconnects IPX segments. The Migration Agent is utilized to migrate systems from IPX to IP in a phased manner without losing connectivity.

The Migration Agent serves as a router between the IPX network and the virtual IPX Network Segment created by the IPX Compatibility Drivers (see Figure 1).

More than one Migration Agent is needed to enable Migration Agent resiliency and load-sharing or when you want to interconnect IPX segments with an IP backbone (see Figure 2).

Figure 1: Illustration of a Migration Agent interconnecting IP and IPX nodes.

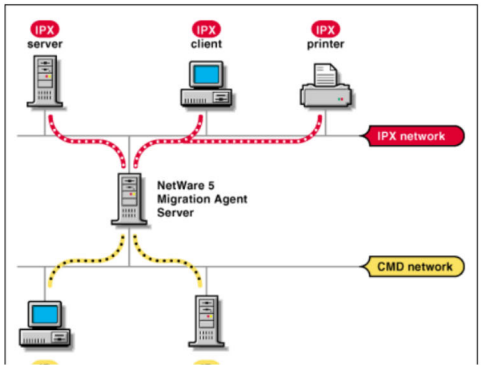
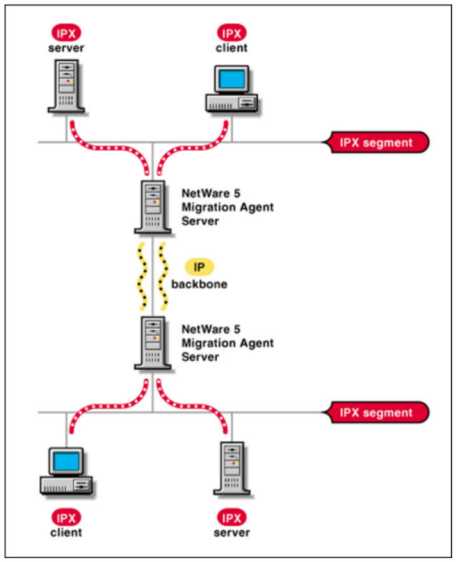


Figure 2: Illustration of two Migration Agents interconnecting two IPX segments.



The Migration Agent is only supported at the NetWare 5 Server. The Migration Agent is enabled by loading the IPX Compatibility Driver (SCMD.NLM) with the Migration Agent option(/g). The Migration Agents are then utilized by the IP systems on the network.

If more than one Migration Agent is needed, Migration Agents must be able to access the same IPX networks or be able to exchange IPX network information. Migration Agents exchange IPX network information by invoking the IP Backbone Support feature. This is accomplished by loading the (SCMD.NLM) with the backbone support options (/bs).

To set up Migration Agents, SLP must be enabled across the networks since the Migration Agents are dependent upon the capabilities of SLP.

The IPX Compatibility drivers are capable of dynamically discovering Migration Agents through SLP but you are also given the choice to statically configure the address of the Migration Agents, if more control is desired. The IPX Compatibility drivers will discover Migration Agents if they are in the same IP network and will give preference to those Migration Agents within the local IP subnet. The address of the Migration Agents must be specified in IP systems that reside in different IP networks.

Note: Migration Agent addresses can be configured by either manipulating the local configuration files or by disseminating the information through DHCP, or to ZENworks clients via ZENworks. The server and clients have different abilities: for example, servers don't get Migration Agent addresses from DHCP.

Protocol Independent NetWare Client and Server

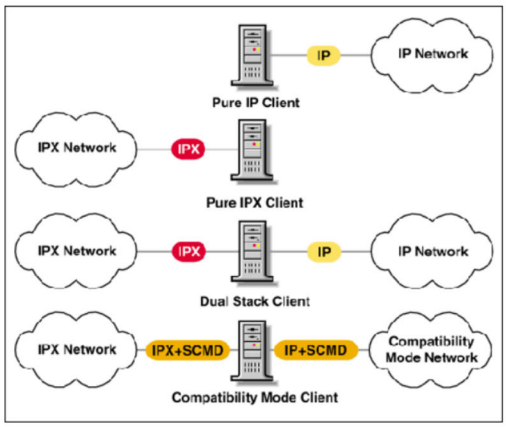
The foundation of NetWare 5 Pure IP lies in the protocol independent client for Microsoft Windows 95, NT, and 3.1 and the protocol independent NetWare 5 Operating System. The IP port for the NetWare Core Protocol (NCP) was registered by IANA as port 524. The NetWare system implements the IP connection as a TCP connection.

Multi-protocol NCP and Dual Protocol Stacks

NetWare 5 provides an NCP that can run on either IPX or IP. In a dual stack environment, the NCP engine will select an IP connection before an IPX connection. If an IP connection is made, then all of the NCP packets will use the TCP transport for communication. One of the advantages of a protocol independent system is that the system can support IP, IPX, or both concurrently. The same applies for the NetWare Client. Thus, there is significant opportunity for mixing and matching the multiple protocols to achieve migration goals.

Dual Stacks. Both NetWare 5 Client and NetWare 5 Server allow the user to implement dual protocol stacks. The system has been designed to prefer IP if an IP connection can be made. IPX is available for communication with the remaining IPX network. Such an approach minimizes the risk of discontinuity; most network clients already use both IP and IPX stacks.

Figure 3: Possible client stack configurations.



With the dual stack approach, the wire carries packets from both protocols. Clients and servers with both stacks loaded will prefer an IP connection for all NCP-based communications. As the remaining IPX communications are reduced by relocating or replacing applications, the system just evolves into a Pure IP system. The IPX traffic is reduced, contained, and then removed via removal of legacy applications or through limited use of the IPX Compatibility Mode migration tool.

Protocol Independent NDS

Novell Directory Services (NDS) has been modified in NetWare 5 to support the IP protocol suite in addition to the IPX protocol suite. The Novell Directory Access Protocol (NDAP) is able to provide NDS communications via UDP or TCP. This support extends to the partition level where an NDS tree can support some partitions that are located on IPX-based machines, other partitions that are located on IP-based machines, and yet other partitions that are based on machines that support both IP and IPX stacks concurrently.

Note: It is important to remember that all servers in a tree must be able to talk to all the other servers in a tree to handle NDS backlink obituaries and external references.

Service Location Protocol (SLP)

SLP is an Internet Standard protocol (RFC2165) used for the discovery of network services. It is not a name resolution service like DNS or NDS. The function of SLP is discovery and is implemented in NetWare 5 to accomplish two goals: first, to discover infrastructure services such as NDS servers, DNS servers, DHCP servers, NDPS registration servers, and various protocol gateways; and second, to encapsulate SAP broadcasts in an IPX Compatibility Mode network.

Discovery of Infrastructure Service Providers

When NetWare 5 ships, developers will have had many years to integrate NDS system calls into their software. Consequently, many applications will already be prepared to register themselves directly into the NDS name base. IPX-based applications that use SAP are already registered into the Bindery Container of NDS and are made accessible through the existing Bindery calls. Finally, any service may be manually registered into the NDS name base. So, where does SLP fit in?

SLP works with NDS to help bring together the IP infrastructure services (NDS trees, DNS servers, NCP servers, NDPS service registries, and some protocol gateways). This allows NetWare clients to discover services by querying one database

rather than the whole network. The NetWare Client uses this information to gain access to infrastructure services. The SLP system does not create end user accessible NDS objects from these infrastructure services. Instead, it uses NDS to collect and replicate knowledge of these services for the benefit of the client.

In previous IPX-based versions of NetWare, this kind of global distribution of infrastructure knowledge was accomplished through the SAP/Bindery architecture. SAP was global, and each machine had a bindery. Consequently, any service that could place a SAP packet on the wire could be globally known. Unfortunately, there was a price to be paid for this global distribution. Bandwidth was consumed and network administrators had to engage in significant filtering to regulate line congestion and service visibility. With the advent of NDS, this began to change. Newer applications were able to forego SAP, register themselves directly with NDS, and take advantage of the NDS replication to attain global visibility.

Many administrators, however, wanted not one, but many, NDS trees to service their companies. So how was the network client to find these many trees? Each tree generated a SAP advertisement that was saved in the router tables of each NetWare Server. The client had only to make it to an initial server to find this global infrastructure information.

SAP was created in the early days of networking with a worst case scenario in mind. The system refreshed itself every 60 seconds whether anything had changed or not. This was advantageous for plug-&-play in the LAN, but impractical across WAN links. Services are registered in SLP with a lifetime that defines the amount of time the service will be available. If the service goes away or deregisters before the lifetime has elapsed, a request to that service fails. If a server goes down, it deregisters.

NDPS makes significant use of SLP in the IP environment. The presence of SLP allows a degree of automated management in the IP environment that is equivalent to that found in the IPX environment. NDPS will function without SLP, but the automated management is reduced.

SAP Redirector in Compatibility Mode

SLP also functions as a compatibility facilitator in NetWare 5. In the Compatibility Mode architecture, a way is provided for IPX-based (and SAP/Bindery-based) applications to continue to work in an IP network. SLP helps make this happen by allowing the Compatibility Mode drivers to translate SAP packets into SLP packets that can be delivered to other Compatibility Mode servers. Additionally, the SLP packets are placed back in the router tables where they can populate the Bindery.

A small network will not need SLP configuration. The User and Service Agents on both client and server are automatically loaded and require no configuration. In a small network (up to 25-30 servers) there is probably no need to implement a Directory Agent. For larger networks, a Directory Agent will be needed to provide scaling and enterprise visibility of services. Placement and frequency of Directory Agents in the network will depend upon several factors, discussed in greater detail below:

- Is the company centralized, distributed, or does it support many small branch offices?
- Should IP-Multicast be routed outside of the local segment?
- What does the existing NDS replication infrastructure look like?
- Will there be a need to use SLP Scoping for congestion control?
- What degree of fault tolerance is desired in the system?
- Will every network segment need to work with every other network segment?
- How many services will be represented on the network?
- What is an acceptable response time for service discovery?

Organizational Concentration. There is no "average" network infrastructure. A network can exist in a single building, in several buildings on a single campus, or in many campuses located around the world. A common profile in the service industry is a few main campuses and thousands of sales or service offices located around the world. The network administrator must address such geographical concerns when implementing the SLP technology. Within buildings, high performance LAN segments make IP Multicast and NDS replication attractive technologies. When the WAN is based on leased line, NDS replication with WAN Management synchronization technology or on-demand location of services through DHCP and DNS might be appropriate technologies.

Figure 4: Possible network relationships within an organization.

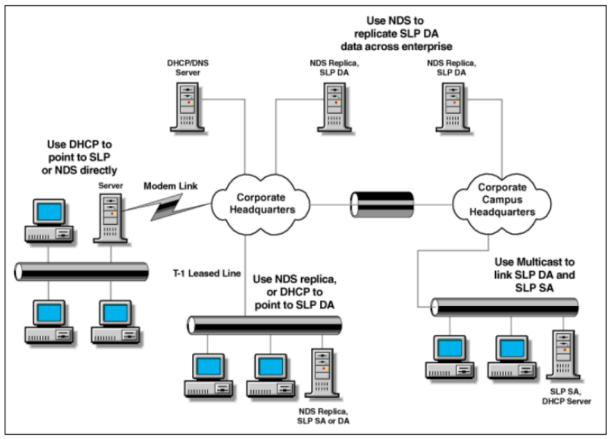


Figure 4 illustrates several of the possible network relationships in an organization. Each of these relationships may justify a different implementation of SLP. For example, a remote office that connects through a modem link would not implement IP Multicast, nor would it likely implement an NDS replica across the modem link. There are several possible solutions for this connection. First, the administrator could configure the local SLP User and Service Agents to use DHCP to locate one of the corporate SLP Directory Agents. The administrator could also use a static configuration to point the clients directly to a specific SLP Directory Agent or directly to a specific NDS tree.

Note: You could also use a Directory Agent on a server without a replica. This causes the Directory Agent to obtain updated SLP information at a specified time each day. The TTLs (Time to Lives) do not expire in this configuration either.

Unlike modems, with leased lines, the connection is often continuous, but the bandwidth is limited at times, or perhaps the office is billed for the amount of traffic on the wire. The administrator could configure this office network the same as the network that uses the modem connection, but there are additional options available that offer increased service levels. The administrator could elect to create an NDS replica of a corporate NDS partition and an SLP Directory Agent at this office. This would provide synchronization between the SLP Directory Agents with little NDS synchronization traffic. This traffic could then be regulated in NetWare 5 through the use of the NDS WAN Traffic Manager.

Finally, within the corporate LAN, the administrator could easily use any of the technologies presented, as well as IP Multicast for SLP Directory Agent synchronization. There could be a mixture of technologies working concurrently in the LAN environment.

IP Multicast. The advent of IP Multicast technology creates an additional factor that the system administrator must consider. On a local segment, Multicast is manageable, but when routers are configured to enable Multicast, the Multicast packet enters the router (which checks to determine whether any other local segments have registered) to listen to Multicast. Upon finding a registered listener, the router moves the Multicast packet into another segment. With the wrong configuration, Multicast takes on characteristics of broadcast consuming bandwidth. Properly configured, however, IP Multicast can provide a global distribution of critical information.

In its default mode in a local network segment environment, the SLP User Agent uses IP Multicast to access the several SLP Service Agents. Additionally, IP Multicast can be configured and made available across the networks. Then SLP will utilize the available bandwidth to continue seeking Service Agents. If you decide to restrict Multicast traffic, you can implement DHCP to help the User Agents find Service and Directory Agents that are not local and cannot be discovered through Multicast.

NDS Replication. NDS replication can be used to synchronize the data in numerous SLP Directory Agents across the enterprise. Synchronization traffic across a WAN link can be expensive though, and consume bandwidth. Within the LAN, however, this replication service is a viable alternative. System administrators should consult the existing literature on NDS deployment to understand the administrative requirements and network impacts of NDS replication.

Fault Tolerance. While a single SLP Directory Agent could provide service for a fairly large company, it would create a single point of failure. The presence of multiple Directory Agents provides a degree of fault tolerance so that the failure of a single DA will not impact the network. Once again, there exists the issue of synchronizing the multiple Directory Agents. Each of the alternatives previously presented carries both costs and benefits.

Service Visibility. Services do not necessarily have to be provided to the whole network. For many years, NetWare administrators have been regulating network congestion and service visibility through IPX packet filtering at the routers. Not every user of the network would see every service that SAP advertised in the network. A similar situation could also be achieved by disabling IP Multicast. A network could then be configured to use multiple SLP Directory Agents, each containing different data and servicing a different region of the network.

Administration. In a large network, the system administrator will likely have to use the SLP Directory Agent to achieve scalability across the network. The Directory Agent may be installed with system defaults that make it immediately usable. On installation, the Directory Agent will extend the NDS NCP object schema and create a SLP-DA record within the NCP server object. It will also create a default container in the NDS name base for SLP entries. This container may be replicated at the discretion of the system administrator.

In the largest networks, however, the use of a "flat" SLP implementation may prove inadequate for scalability and traffic management. SLP scopes subdivide services. For example, some services may be regularly registered on the machines in the engineering department and have no use to anyone outside of that department. Thus, the administrator could configure the system to attach a scope attribute of "ENG" to each service in that area. These services would then be seen only by requests that included the attribute of SCOPE=ENG. Such subdividing of the services provides a kind of filtering that administrators are used to in both IP and IPX environments. SLP implementations that don't utilize scopes are said to be "unscoped."

- **Small Network Implementation (less than 25 Servers in Multicast radius).** A small network with less than 25 servers gains no advantage from an SLP Directory Agent. All SLP communication can be handled by the SLP Service and User Agents with local segment IP Multicast. With this simple system, the network client is able to have dynamic discovery of NDS Trees, NCP servers, NDPS Service Registry, and other infrastructure services such a gateways. NDS aware services could register themselves with NDS.
- **Medium to Large Network Implementation.** In a medium to large-sized network, the SLP will require SLP Directory Agents to provide scaling and WAN support. If the network is architected to be a rather flat network, then a single Directory Agent might be sufficient. Unlike the smaller systems, there may be no IP Multicast in this network. In that case, the Directory Agent can be found by the User Agents through the use of DHCP. Also, with the Directory Agent, information can be stored in an NDS container that can be replicated through the corporate network and have information that can be made available to other Directory Agents. Classification of service information would not normally be necessary in this environment.
- **Enterprise Implementation.** Large scale implementation of SLP will most likely require a combination of SLP Directory Agents, NDS, DHCP, and local IP Multicast. The SLP Directory Agent would collect service information from the local Service Agents. That information would then be loaded to a container in NDS. That container would then be replicated as necessary with other SLP Directory Agents feeding in information from different parts of the network and retrieving information collected from yet other Directory Agents. Thus, the local service receives global distribution (at the administrator's discretion).
- **Using DHCP.** In the case where IP Multicast is not available or NDS container replication is not a desirable option, the SLP system can be configured to use DHCP. This is illustrated in Figure 6. This is an attractive option for remote office networks where a replicated NDS container might not be a desirable system design.

The Server SLP configuration options discussed above can be configured from the server console using the SET command with the parameters (included in the startup.ncf file) in the table below:

Parameter	Function
SLP DA Discovery Options = value	Use Multicast DA advertisements.Bit 0x01 = Use Multicast Directory Agent advertisementsBit 0x02 = Use DHCP discoveryBit 0x04 = Use static file SYS:ETC\SLP.CFG (you must first change the set parameter to something else, then back to static to reread SLP.CFG)Bit 0x08 = Scopes Required.These bits can be ordered together for Multiple values.*Supported values:*0 to 8*Default:* 3
SLP TCP = value	Use TCP packets instead of UDP packets when possible.*Supported values:* OFF, ON *Default:* OFF
SLP Debug = value	Enable SLP debug mode. Bit 0x01 = COMMBit 0x02 = TRANBit 0x04 = APIBit 0x08 = DABit 0x10 = ERRBit 0x20 = SA *Supported values:*0 to 4294967255*Default:* 0
SLP Multicast Radius = value	Specify an integer describing the Multicast radius.*Supported values:*0 to 32*Default:* 32
SLP DA Discovery Options = value	Use Multicast DA advertisements.Bit 0x01 = Use Multicast Directory Agent advertisementsBit 0x02 = Use DHCP discoveryBit 0x04 = Use static file SYS:ETC\SLP.CFGBit 0x08 = Scopes Required.These bits can be ordered together for multiple values.*Supported values:*0 to 8*Default:* 3
SLP TCP = value	Use TCP packets instead of UDP packets when possible.*Supported values:* OFF, ON *Default:* OFF
SLP Debug = value	Enable SLP debug mode.Bit 0x01 = COMM Bit 0x08 = DABit 0x02 = TRAN Bit 0x10 = ERRBit 0x04 = API Bit 0x20 = SA *Supported values:*0 to 4294967255*Default:* 0
SLP Multicast Radius = value	Specify an integer describing the Multicast radius.*Supported values:*0 to 32*Default:* 32
SLP Broadcast = value	Use broadcast packets instead of Multicast packets.*Supported values:* OFF, ON *Default:* OFF
SLP MTU Size = value	Specify an integer describing the maximum transfer unit size.*Supported values:*0 to 4294967255*Default:* 1450
SLP Rediscover Inactive Directory Agents = value	Specify the minimum time period in seconds that SLP will wait to issue service requests to rediscover inactive Directory Agents. *Supported values:*0 to 4294967255*Default:* 60
SLP Retry Count = value	Specify an integer value describing the maximum number of retries.*Supported values:*0 to 128*Default:* 3
SLP Scope List = value	Specify a comma-delimited scope policy list.*Max Length:*1023*Default:* 1023
SLP SA Default Lifetime = value	Specify an integer value describing the default lifetime in seconds of service registers.*Supported values:*0 to 4294967255*Default:* 900
SLP Event Timeout = value	Specify an integer value describing the number of seconds to wait before timing out Multicast packet requests.*Supported values:*0 to 4294967255*Default:* 53
SLP DA Heart Beat Time = value	Specify an integer value describing the number of seconds before sending the next Directory Agent heartbeat packet.*Supported values:*0 to 4294967255*Default:* 10800
SLP Close Idle TCP Connections Time = value	Specify an integer value describing the number of seconds before idle TCP connections should be terminated.*Supported values:*0 to 4294967255*Default:* 300
SLP DA Event Timeout = value	Specify an integer value describing the number of seconds to wait before timing out Directory Agent packet requests.*Supported values:*0 to 429*Default:* 5

SLP Query and Debugging commands will be covered in a future AppNote.

SLP Client Configuration Settings

In addition to Server SLP configuration, the NetWare Client SLP interaction can be configured from the Novell Client Configuration Property Page under Advanced Settings. The client settings are listed below:

Setting	Parameter Group	Function
SLP Active Discovery	SLP General	This parameter specifies that SLP is required to look up services from a Directory Agent and not to use IP Multicasting directly to SLP Service Agents for services. SLP's normal operation is to first check Directory Agents. If no Directory Agent is found, SLP Multicasts to Service Agents.*Default:* ON
SLP Cache Replies	SLP Times	When SLP receives a service request from a User Agent, the SLP reply is saved for the amount of time specified by the SLP Cache Replies parameter. If SLP receives a duplicate of this request, the cached reply is sent, so the same reply does not have to be generated again.The default value is one minute. Setting this value higher will consume more memory to retain replies longer. It is recommended that you do not change this default, because any duplicate requests should occur within the first minute.*Range:*1 to 60 (minutes)*Default:* 1
SLP Default Registration Lifetime	SLP Times	This parameter specifies the lifetime of a service registration which is registered by a service provider requesting the default lifetime value. If the service provider specifies a lifetime value when the service is registered, this value is not used.The Directory Agent deletes the service when the lifetime expires if it hasn't been specifically renewed or unregistered before then. This prevents the Directory Agent's information from becoming too stale if the Server Agent registering the service goes down. The Server Agent automatically renews the service so the application doesn't need to.The default value is 10800 seconds, which is 3 hours. Using a smaller value will make the Directory Agent's information less stale at the expense of more network traffic to renew services more frequently. This parameter does not effect how long the service is registered by the Server Agent.*Range:*60 to 60000 (seconds)*Default:* 10800
SLP Maximum Transmission Unit	SLP General	This parameter specifies the maximum transmission unit (UDP packet size) for the link layer used. Setting this parameter either too large or too small will adversely affect performance of SLP.*Range:*576 to 4096*Default:* 1400

Unit		SLP.*Range*:576 to 4096*Default*: 1400
SLP Multicast Radius	SLP General	SLP uses IP Multicasting to dynamically discover other SLP Service Agents and Directory Agents. This parameter is a number specifying the maximum number of subnets (number of routers plus 1) that SLP's Multicasting should traverse. A value of 1 confines Multicasting to the local segment (no routers).*Range*:1 to 32 (number of routers plus 1)*Default*: 32

Protocol Stack Configurations

The server and client connectivity capabilities are limited by the options selected when systems are installed. Systems can be installed with the following protocol options:

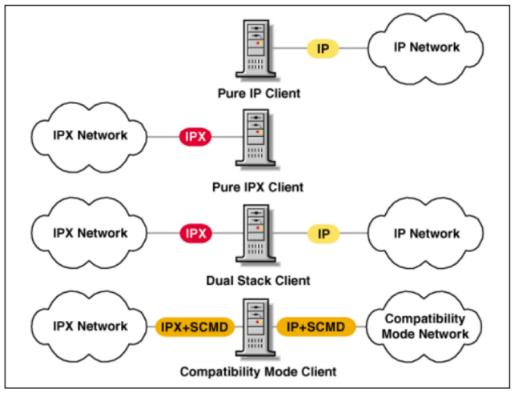
- IP Only Install Option
- IPX Only Install Option
- IP and IPX Install Option

The protocol install option determines the binding between protocol stacks and network adapters. It does not determine which protocol stacks are loaded in the system. For example, if the IP Only Install Option is selected, only the TCP/IP stack is attached to the network adapter. An exception to this rule is NetWare/IP which requires IPX only or IP and IPX.

Client

Using the install options described above, the client can be configured to work in the following network configurations, as shown in Figure 5.

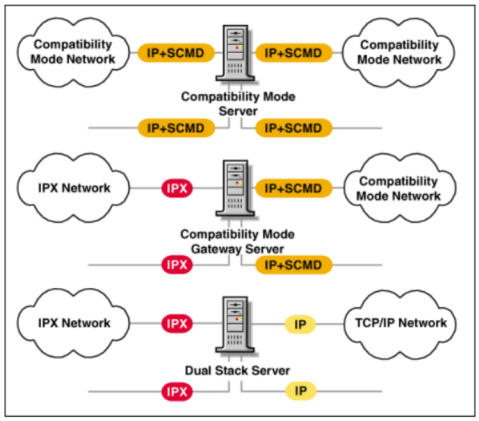
Figure 5: Client configuration options.



Server

The NetWare 5 server can be installed to support both IPX and IP using either dual IPX and IP stacks or by using Server Compatibility Mode, as illustrated in Figure 6. Additionally, to create a Pure IP implementation, the server can be installed with Compatibility Mode and then the administrator can unload the IPX stack by issuing the server console command *UNLOAD SCMD.NLM*.

Figure 6: Server configuration options.



Systems Installed Using the IP Only Install Option

These systems have both the TCP/IP and the IPX stacks loaded but only the TCP/IP stack is bound to the network adapter. Systems installed with the IP and IPX Option are configured to establish NCP connections over either the TCP/IP stack or over the IPX stack.

The IPX stack is loaded on systems installed with the IP Only Option to give those systems the ability to execute IPX applications and to connect with IPX systems through a Migration Agent.

NetWare clients and servers installed with the IP Only Option have the following capabilities:

- They can establish NCP connections with clients installed with one of the install options that include IP.
- They can establish NCP connections through a Migration Agent with pre-NetWare 5 clients (these clients only support NCP connections over IPX) or with NetWare 5 clients installed with the IPX Only option.
- They can execute IPX applications and communicate directly with NetWare 5 systems installed with the IP Only Option.
- They can execute IPX applications and communicate through a Migration Agent with IPX nodes.

Systems Installed Using the IPX Only Install Option

Systems installed using the IPX Only Install Option have the IPX stack loaded and may also have the TCP/IP stack loaded. Each stack is normally attached to the network adapter unless NetWare/IP is loaded. Systems installed with the IPX Only Option are configured to only establish NCP connections over the IPX stack.

NetWare clients and servers installed with the IPX Only Option have the following capabilities:

- They can establish NCP connections with pre-NetWare 5 clients or with NetWare 5 clients installed with one of the install options that include IPX.
- They can establish NCP connections through a Migration Agent with NetWare 5 clients installed with the IP Only option.
- They can execute IPX applications and communicate directly with other IPX nodes.
- They can execute IPX applications and communicate through a Migration Agent with NetWare 5 systems installed with the IP Only Option.

Systems Installed Using the IP and IPX Install Option

Systems installed using the IP and IPX Install Option have the TCP/IP and IPX stacks loaded. Each stack is normally attached to the network adapter unless NetWare/IP is loaded. Systems installed with the IP and IPX Option are configured to establish NCP connections over either the TCP/IP stack or over the IPX stack.

NetWare servers installed with the IP and IPX Option have the following capabilities:

- They can establish NCP connections with pre-NetWare 5 clients or with NetWare 5 clients without regard for the option used to install it.

- They can execute IPX applications and communicate directly with other IPX nodes.
- They can execute IPX applications and communicate through a Migration Agent with NetWare 5 systems installed with the IP Only Option.

NetWare clients installed with the IP and IPX Option have the following capabilities:

- They can establish NCP connections with pre-NetWare 5 servers or with NetWare 5 servers installed with one of the install options that include IPX.
- They can establish NCP connections with NetWare 5 servers installed with the IP Only Option if the clients are able to obtain IP addresses for those servers.
- They can establish NCP connections through a Migration Agent with NetWare 5 servers installed with the IP Only Option if the clients are only able to obtain IPX addresses for those servers.
- They can execute IPX applications and communicate directly with other IPX nodes.
- They can execute IPX applications and communicate through a Migration Agent with NetWare 5 systems installed with the IP Only Option.

Having a NetWare client installed with the IP and IPX Option does not guarantee that the client will be able to establish an NCP connection with a server installed with the IP Only Option without the use of a Migration Agent. The type of address obtained by the client when trying to connect to a server determines the protocol stack utilized to establish the connection.

Applications that obtain address information from the bindery will not be able to connect with servers installed with the IP Only Option if there is no Migration Agent installed and if the client is installed with the IP and IPX Option. Notice that this problem does not exist if the client and the server are installed with the IP Only Option.

The Migration Agent and Servers Installed Using the IP and IPX Install Option

The Migration Agent can only be enabled in a NetWare 5 server installed with the IP and IPX Option.

Notice that the Migration Agent makes use of the IPX Router present in the IPX stack to route packets between the CMD Network and the IPX Networks.

NetWare 5 servers installed with the Migration Agent enabled are capable of communicating directly with other systems without regard for the install option used during installation. They are also capable of routing network traffic between IP and IPX systems.

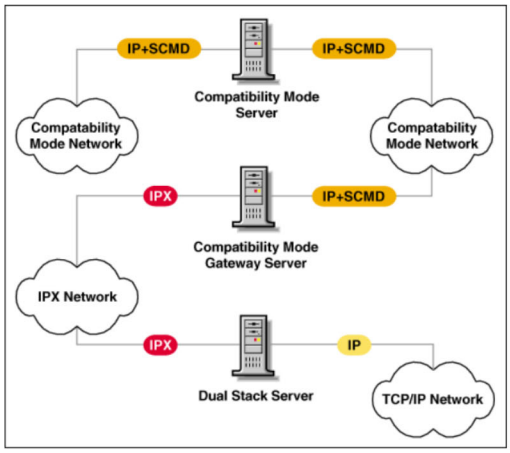
The IP-Only Network

There are two basic approaches to implementing the IP-Only network. Some administrators will choose to begin by replacing IPX on the network backbone with IP. This approach focuses on the cost savings that can be realized by a routing infrastructure that supports only one protocol. Another approach focuses on migrating selected network segments first, and the backbone later. The administrator might begin with the implementation of dual protocol stacks across the network, followed by the gradual removal of the IPX stack where there are no legacy IPX applications to support. This approach seeks to minimize risk and disruption to overall operations. However, IP and IPX can still be routed together by setting up two different routing infrastructures and still routing IPX.

Immediate or Phased Transition

Some smaller networks with minimal legacy considerations might well consider an immediate rollover to the IP protocol. This is possible with a little planning and a good understanding of how to build an IP infrastructure. Most larger installations, however, will require some time for the transition to an IP-Only network. NetWare 5 provides the tools whereby an administrator could first "clear the wire" and have only IP traffic on the wire, and then "clean the applications" by replacing some of the legacy IPX applications with newer versions that work in an IP environment. In removing IPX traffic from the wire, NetWare 5 was designed so that all NCP communications are IP-based and use the TCP protocol. Remaining IPX applications that write directly to the IPX stack and make use of SAP and the Bindery can be accommodated with the IPX Compatibility Mode.

Figure 7: Integrating various configuration options.

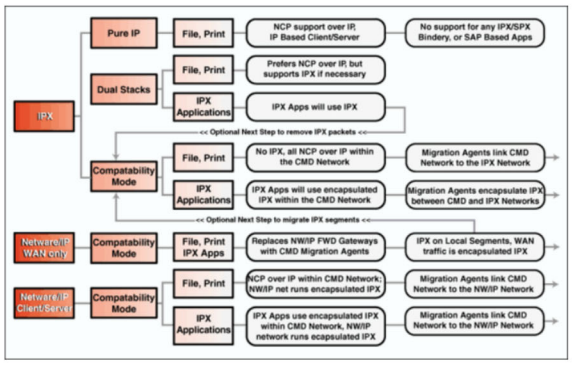


Migration Strategies

Figure 8 shows three migration paths. The first path moves from an IPX only network to Pure IP by installing the server in each of the modes that support IP. The Pure IP path assumes a small network that has no requirement to run IPX, Bindery, or SAP-based applications. Both the client and server are installed using the IP-Only install option. The second IPX path, dual stacks, supports IPX applications but the system uses IP whenever possible. The server is installed with the IP and IPX protocol option and the client can be installed with IP Only, IPX Only, or IP and IPX protocol options. The third IPX path, Compatibility Mode, also supports IPX applications with encapsulated IPX within the virtual CMD network using the Migration Agent. The system encapsulates IPX only when an IPX request is made to the server, and even then, since IPX is encapsulated in IP, there is no IPX on the wire. In both of the latter two paths, Pure IP is achieved when there are no more IPX requests.

The second and third migration paths move from NetWare/IP to Pure IP. Both paths use Compatibility Mode. The first NW/IP path replaces NW/IP forwarding gateways with CMD Migration Agents. This creates a Pure IP backbone connected by NetWare 5 Migration Agents which encapsulate IPX over the WAN. The IPX segments on each end of the WAN link can then be migrated using one of the IPX Compatibility Mode paths discussed earlier. The last path, NetWare/IP Client/Server uses Compatibility Mode to support IPX applications using encapsulated IPX within the virtual CMD network and uses Migration Agents to link the virtual CMD network to the NW/IP network.

Figure 8: Possible protocol migration senarios.



Migration Strategy Dependent upon Organizational Goals

The following sections describe migration strategies that are effective in meeting the following goals:

- Migrating to obtain Internet Connectivity
- Migrating to quickly cut administrative costs associated with IPX networking
- Migrating to eventually have an IP-Only network

- Migrating to eventually have an IP-Only network

Migration Strategy to Obtain Internet Connectivity

To add Internet connectivity to NetWare systems, simply upgrade to NetWare 5 using the IP and IPX Option. This upgrade path requires administration of both IP and IPX networking protocols.

Those who choose this migration path do not have to worry about setting up Migration Agents to maintain connectivity as they upgrade their systems.

Migrating Strategies to Cut IPX Administrative Costs

Administrators wanting to quickly migrate networks from IPX to IP to maximize their return on investment will want to take advantage of the functionality provided by the IPX Compatibility Drivers and the Migration Agents. The IPX Compatibility feature is critical in this scenario because it allows migration without losing connectivity and without having to upgrade existing applications.

Administrators wanting to migrate networks using the IPX Compatibility feature must understand that the IPX Compatibility Drivers are dependent upon the functions of SLP and that there are costs associated with setting up an SLP infrastructure. Additionally, setting up an SLP infrastructure is an investment in the future because SLP is an emerging Internet standard that will be leveraged by future applications and devices.

When utilizing the IPX Compatibility feature to migrate, start the migration with the leafs of the network and finish with the backbone of the network or vice-versa. Complex network environments are characterized by a backbone formed by a variety of systems interconnected with a combination of WAN and LAN links.

Migration Scenarios

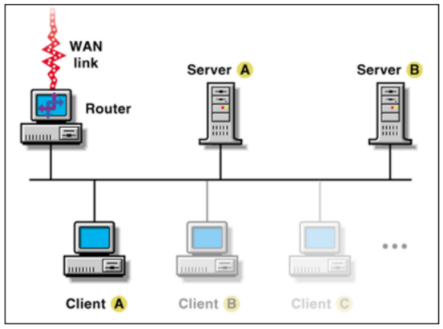
The following sections describe how to migrate a portion of the network, how to migrate networks starting with the leafs of the network, and how to migrate networks starting with the backbone.

Migrating a Section of the Network

The steps below describe how to migrate a section of the network. In order to complete this procedure successfully, the network section being migrated must not be used to interconnect other sections of the network using IPX. The following steps allow upgrading or installing clients and servers in a phased manner without losing connectivity.

1. Select and upgrade/install some servers in the network section to be migrated to serve as Migration Agents (on the IPX network).
2. Upgrade/Install all servers in the network section using the IP and IPX Option.
3. Upgrade/Install all clients in the network section using the IP Only Option.
4. Modify the configuration of the servers and services in the network section.
5. Turn off IPX networking between the selected section of the network and the rest of the network.

Figure 9: Example of migrating a section of the network.



Example of How to Migrate a Section of the Network. Refer to the illustration in Figure 9 as you read through the following steps:

1. Upgrade Server A to NetWare 5 as a Migration Agent.
2. Upgrade Server B to NetWare 5 using the IP and IPX Install Option.
3. Upgrade clients to NetWare 5 using the IP Only Install Option.
4. Unbind IPX from the network adapters in server B and load the SCMD.NLM. Unbind IPX from the network adapters in server A and re-load the SCMD.NLM without the Migration Agent option.
5. Turn off IPX routing at the router.

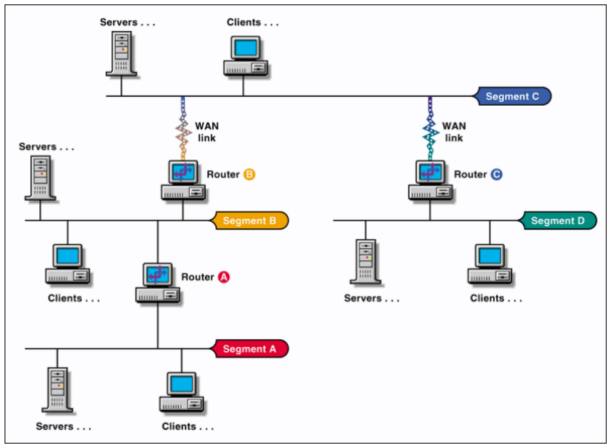
Migrating Leaf Networks First

Migrating leaf networks first reduces the impact of the migration on the IPX routing infrastructure of the network, and it allows the administrator to focus efforts on specific sites. However, since the backbone is the last portion of the network migrated, administrative costs may not be offset as quickly.

The steps below describe how to migrate a network from IPX to IP starting with the leaf networks first.

1. Identify the nodes and links that form the backbone of the network.
2. Select and Upgrade/Install some servers in the backbone to serve as Migration Agents.
3. Select the leaf portion of the network to be migrated. This may be a group of segments connected to the backbone via a WAN link. Migrate the selected portion of the network following the steps outlined above in "Migrating a Section of the Network".
4. Repeat step 3 until all networks connected to the backbone are migrated.
5. Migrate the backbone section using the steps outlined in "Migrating a Section of the Network".

Figure: 10 Example of migrating a Leaf of the network first.



Example of How to Migrate Leaf Networks First. Refer to the illustration in Figure 10 as you read through the following steps:

1. Identify Segment C as the backbone.
2. Upgrade/Install two servers in Segment C as NetWare 5 Migration Agents.
3. Select the portion of the network consisting of segments A and B as the first portion to migrate and do it following the steps outlined in "Migrating a Section of the Network". Make sure that you first upgrade/install servers in Segment A and Segment B as NetWare 5 Migration Agents to minimize performance degradation while the section is being migrated. Turn off IPX routing in routers A and B when all the nodes in the section have been migrated to IP Only.

migrated. Turn off IPX routing in routers A and B when all the nodes in the section have been migrated to IP-Only.

4. Migrate Segment D following the steps outlined in "Migrating a Section of the Network".
5. Migrate Segment C following the steps outlined in "Migrating a Section of the Network".

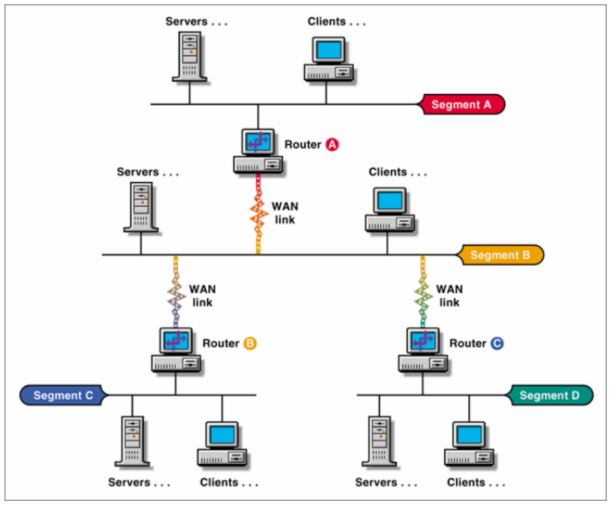
Migrating the Backbone First

Migrating the backbone first alleviates administrative costs associated with maintaining IPX over the backbone. This migration path requires Migration Agents at each of the segments connected to the backbone and the Backbone Support feature of the Migration Agents before IPX routing is disabled on the backbone. Migration Agents with the Backbone Support feature enabled are able to interconnect IPX segments by exchanging RIP and SAP information and by routing encapsulated IPX datagrams.

The steps below describe how to migrate a network from IPX to IP starting with the backbone first.

1. Identify the nodes and links that form the backbone of your network.
2. Select and Upgrade/Install some servers in each one of the segments connected to the backbone to serve as Migration Agents with the Backbone Support feature enabled.
3. Migrate the backbone section using the steps outlined in "Migrating a Section of the Network".
4. Select the leaf portion of the network to migrate. This may be a group of segments connected to the backbone via a WAN link. Migrate the selected portion of the network following the steps outlined in "Migrating a Section of the Network".
5. Repeat step 5 until all networks connected to the backbone are migrated.

Figure: 11 Example of migrating the Backbone first.



Example of How to Migrate the Backbone First. Refer to the illustration in Figure 11 as you read through the following steps:

1. Identify Segment B as the backbone.
2. Upgrade/Install one or two servers in segments A, C, and D as NetWare 5 Migration Agents with the Backbone Support option enabled.
3. Migrate the Segment B (the backbone segment) using the steps outlined in "Migrating a Section of the Network". Turn off IPX routing in routers A, B, and C to complete the migration of Segment B.
4. Migrate segments A, C, and D using the steps outlined in "Migrating a Section of the Network".

Avoiding Inefficient Routing

The following two examples show problems that you can avoid by carefully selecting the placement of Migration Agents in the network.

Example 1. Figure 12 shows a client installed as IP Only in Segment C trying to communicate with an IPX Server in Segment A. The IPX server knows that the client is part of the virtual CMD Network and that routers 1 and 2 present equally good paths to the CMD Network Server (the Migration Agent servers present the CMD Network route to the routers attached to their network segment). Under this scenario, Server A may choose to route packets to Client A through Router 1 resulting in the packets following the inefficient path shown by the broken line in the figure. The problem presented here could be solved by placing a Migration Agent in Segment A as shown in Figure 13, the Migration Server would then present to Server A the "best" route to the CMD Network and the packets from Server A to Client A would follow the path shown by the broken line.

Figure:12 Less efficient sample network setup for Example 1.

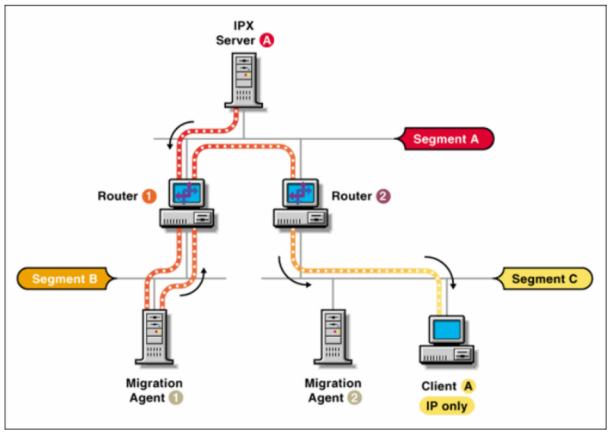
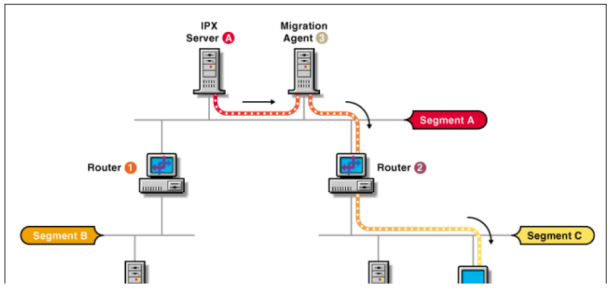


Figure:13 More efficient sample network for Example 1.



Example 2. Figure 14 shows segments A and B interconnected via a WAN link. Nodes A and B wish to communicate but can only do so through the Migration Agent present in Segment A. Under this scenario, packets sent between Node A and Node B are forced to traverse the WAN link twice as shown by the broken line in the figure resulting in poor performance. The problem presented here could be solved by placing a Migration Agent in Segment B as shown in Figure 15.

Figure: 14 Less efficient sample network setup for Example 2.

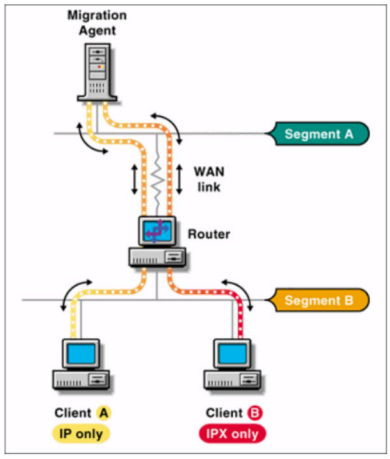
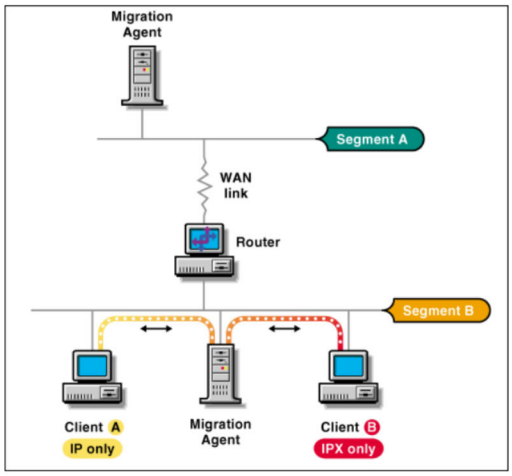


Figure: 15 More efficient sample network setup for Example 2.



SAP/RIP Filters and the Migration Agent Backbone Support Feature. If the Backbone Support feature of the Migration Agents is enabled, then the RIP/SAP information exchange between these agents may bypass the RIP/SAP filters that you may have set up in your routers. Refer to the Migration Agent documentation to learn how to set up RIP/SAP filters using the Migration Agents.

Placing of SLP Directory Agents. If the SLP infrastructure is set up using Directory Agents and while relying on the IPX Compatibility feature to accomplish the migration, Directory Agent placing must minimize the round trip distance between the IP Only nodes and their closest Directory Agent. This is necessary to avoid having IPX applications timing out when they perform RIP or SAP requests.

Turning Off Microsoft IPX Networking. Clients may be set up to do Microsoft Networking using IPX and/or IP. If clients are setup to do Microsoft Networking over IPX and you want to migrate them from IPX to IP, you may want to enable Microsoft Networking over TCP/IP and then disable Microsoft Networking over IPX. This may be necessary to reduce the demand on the services provided by the IPX Compatibility feature.

Gradual Migration to an IP-Only Network

Use this migration method when Pure IP is eventually desired but there is no immediate need to remove IPX from the network. This migration path requires migration of all applications from IPX to IP before IPX is disabled on the network.

Applications are considered IPX applications if they use the interfaces provided by the IPX stack or they specify IPX addresses when trying to establish NCP connections. The best way to screen out IPX applications is to run them on a test network on which IPX is absent (no IPX stacks loaded). Many applications let you specify the networking protocol to use when communicating.

NetWare clients must be configured twice during the course of this migration. The cost of modifying client configurations can be minimized by taking advantage of the Automatic Client Update features of NetWare and the Workstation Manager feature.

If it is later discovered that your applications require IPX, you must switch to one of the migration strategies outlined above.

The steps below describe how to migrate a network from IPX to IP without relying on the IPX Compatibility feature:

1. Identify IPX applications and make sure that they can be configured/upgraded/replaced to run over the TCP/IP stack.
2. Start upgrading/installing your servers and clients using the IP and IPX Option.
3. Start migrating applications from IPX to IP.
4. Turn off IPX networking at the routers when all the IPX applications have been migrated and all the NetWare clients and servers have been upgraded/installed using the IP and IPX Option.
5. Modify the configuration of the NetWare servers and clients to be IP-Only servers and clients.

Other Migration Considerations

Most networks have evolved slowly over the years and are generally a combination of old and new software and hardware. Legacy software and legacy network infrastructure remain necessary for many years after newer replacements have been made available. Sometimes these applications and infrastructure elements limit the ease of migration. The following items might present such limitations when migrating from an IPX to an IP network.

IPX, Bindery, and SAP-based Applications and Utilities

Many of the DOS utilities that were released in the intraNetWare (4.11) release were modified to work with both NDS and the older Bindery. These utilities will make their first attempt at discovery by going to the bindery context of NDS. If the discovery attempt fails, then these utilities will attempt to use SAP and Bindery Calls to use the older technology.

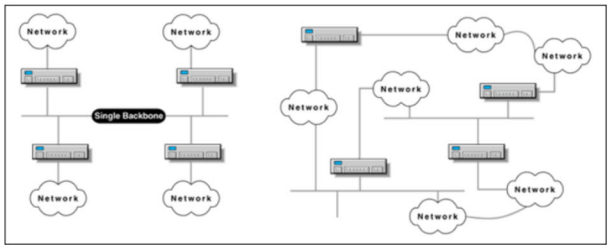
Many of the scripts that IS&T staffs use to run their daily operations are based on both NCP and DOS batch processing files. In both cases, the NetWare specific elements are generally command line versions of NetWare DOS Utilities or NetWare NLMs. The reasons for continuing to use these commands should be re-evaluated in light of the newer technology that will be shipped with NetWare 5.

The Backbone

In some companies, there is a single network that is the backbone for all other networks in the company. Other companies have a less elegant backbone. It is the composite of many networks slowly grown over time. Figure 16 shows an example of both single and fragmented backbones.

Note: Keep in mind that all servers in a given tree must be able to communicate with all other servers in the tree if you are migrating from an IPX to an IP tree.

Figure: 16



The composition of the corporate backbone will impact the migration decision.

The Filtered Network

The first question that needs to be addressed with regard to filtering is whether it remains necessary in the IP environment. Filtering in the IPX environment sought to address congestion control and service access. With an IP-based system, the SAP that created congestion no longer exists. Service visibility is a different issue. The real solution for this issue is the use of NDS rather than the SAP/Bindery infrastructure. There is still filtering capability within the IP routers that can be used to replace the IPX routing. But in the IPX environment, SAP was just a special packet type that could be easily managed at the routing level. SLP, DHCP, DNS, NCP, NDS and other protocols are just data within the IP packet and not so easily managed at the router.

Conclusion

This AppNote has provided an introduction to migrating from an IPX-based network to an IP-based network. It has described the various components and tools involved, and has given several migration strategies to follow.

** Originally published in Novell AppNotes*