23

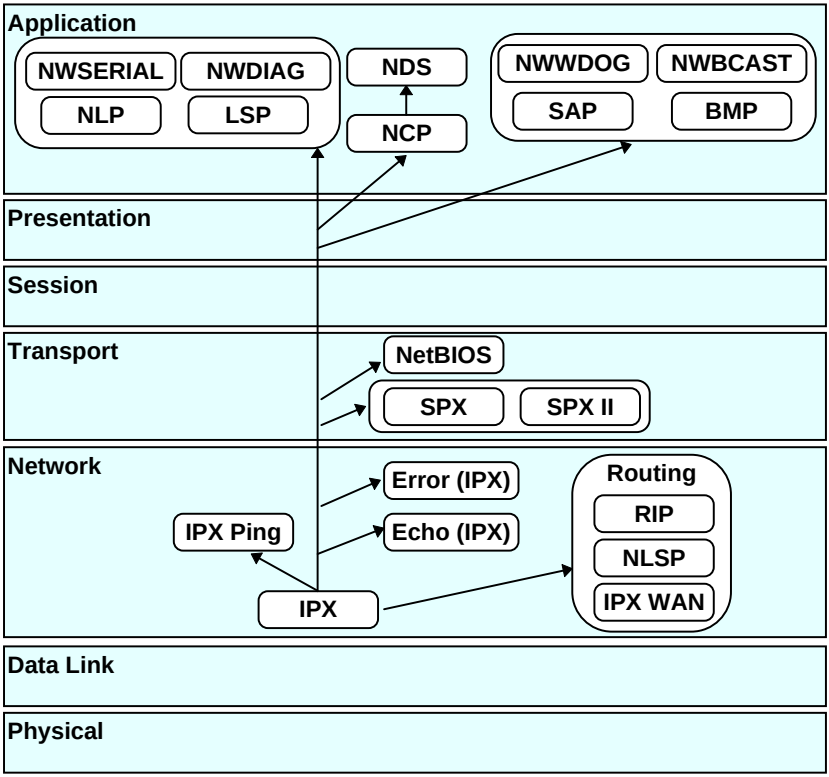
Novell Protocols

The Novell NetWare protocol suite was greatly influenced by the design and implementation of the Xerox Network System (XNS) protocol architecture. It provides comprehensive support for every major desktop operating system, including DOS, Windows, Macintosh, OS/2, and UNIX. In addition, Novell provides extensive support for local area networks and asynchronous wide area communications. The Novell suite includes the following protocols:

- IPX: Internetwork Packet Exchange.
- BCAST: Broadcast.
- BMP: Burst Mode Protocol.
- DIAG: Diagnostic Responder.
- NCP: NetWare Core Protocol.
- NDS: NetWare Directory Services.
- NLSP: NetWare Link Services Protocol.
- NovelNetBIOS.
- RIPX: Routing Information Protocol.
- SAP: Service Advertising Protocol.

- SER: Serialization.
- SPX: Sequenced Packet Exchange.
- WDOG: Watchdog.

The following diagram represents the Novell protocol suite in relation to the OSI model :



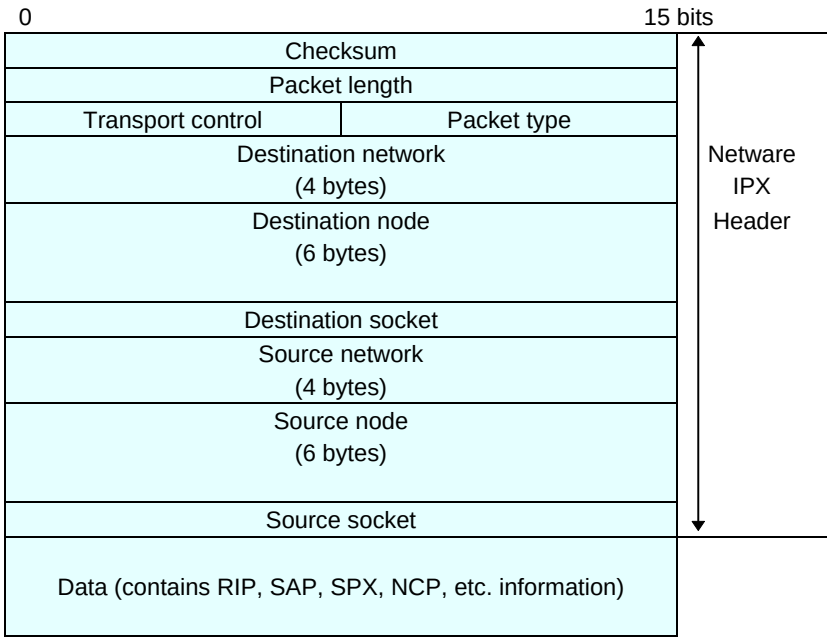
Novell protocol suite in relation to the OSI model

IPX

"Novell's Guide to NetWare LAN Analysis" by Laura A. Chappell and Dan E. Hakes, Novell Press, 1994

Internet Protocol Exchange (IPX) is Novell's implementation of the Xerox Internet Datagram Protocol (IDP). IPX is a connectionless datagram protocol that delivers packets across the Internet and provides NetWare workstations and file servers with addressing and internetworking routing services.

The structure of the IPX packet is shown in the following illustration:



IPX packet structure

Checksum
Set to FFFFH.

Packet length
Length of the IPX datagram in octets.

Transport control
Used by NetWare routers. Set to zero by IPX before packet transmission.

Packet type
Specifies the packet information:

0	Hello or SAP.
1	Routing Information Protocol.
2	Echo Packet.
3	Error Packet.
4	NetWare 386 or SAP.
5	Sequenced Packet Protocol.
16-31	Experimental protocols.
17	NetWare 286.

Network number
A 32-bit number assigned by the network administrator; set to 0 on the local network.

Node number
A 48-bit number that identifies the LAN hardware address. If the node number is FFFF FFFF FFFF, it means broadcast, and if the node number is 0000 0000 0001, it means it is the server (on NetWare 3.x and 4.x only).

Socket number
A 16-bit number that identifies the higher-layer packet:

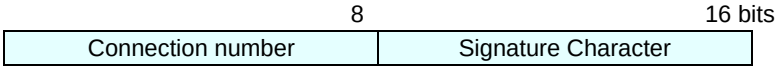
0451H	NCP.
0452H	SAP.
0453H	RIP.
0455H	NetBIOS.
0456H	Diagnostics.
0x457	Serialization packet (SER).
4000-6000H	Ephemeral sockets, used for file server and network communication.

BCAST

"Novell's Guide to NetWare LAN Analysis" by Laura A. Chappell and Dan E. Hakes, Novell Press, 1994

The Broadcast (BCAST) protocol deals with announcements from the network informing the user that he has received a message.

The format of the BCAST packet is shown in the following illustration:



BCAST packet structure

Connection number

Given to the station during the login process.

Signature character

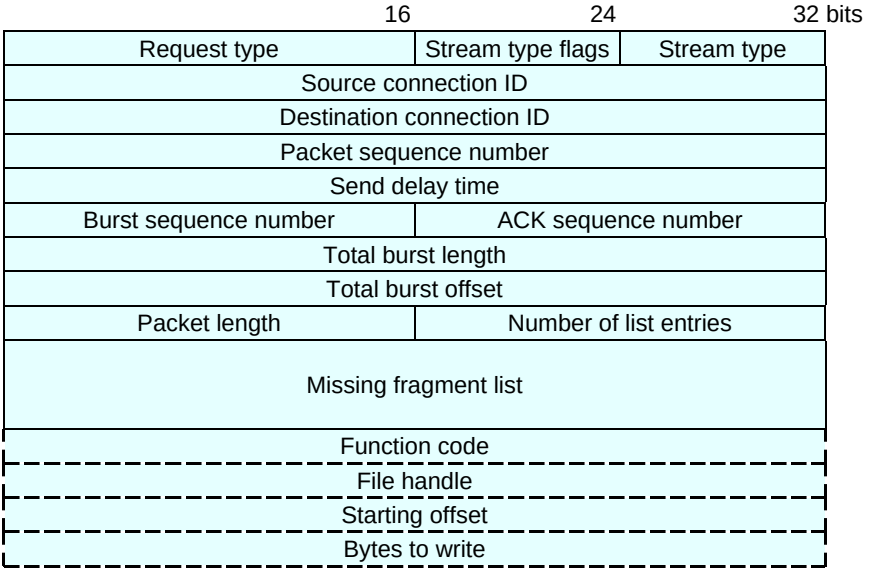
The value is 0x21 (ASCII character!) which means *Broadcast Message Waiting*.

BMP (Burst)

"Novell's Guide to NetWare LAN Analysis" by Laura A. Chappell and Dan E. Hakes, Novell Press, 1994

The Burst Mode Protocol (BMP) is actually a type of NCP packet (Request type = 7777H). BMP was designed to allow multiple responses to a single request for file reads and writes. Burst Mode increases the efficiency of client/server communications by allowing workstations to submit a single file read or write request and receive up to 64 kilobytes of data without submitting another request.

The format of the BMP packet is shown in the following illustration:



BMP packet structure

Request type

Identical to Request Type in NCP and always will be set to 7777H (Burst mode packet).

Stream type flags

Available flags.

Stream type
Burst mode control bits.

Source connection ID
Connection ID number assigned to source workstation.

Destination connection ID
Connection ID number assigned to destination workstation.

Packet sequence number
Used by workstation and file server to identify packets sent and received.

Send delay time
Time delay between packets.

Burst sequence number
Burst number being transmitted.

ACK sequence number
Next accepted burst sequence number.

Total burst length
Length of transmitted burst (in octets).

Burst offset
Location of packet data within the burst.

Packet length
Length of packet burst data (in octets).

Number of list entries
Number of elements in the missing fragment list.

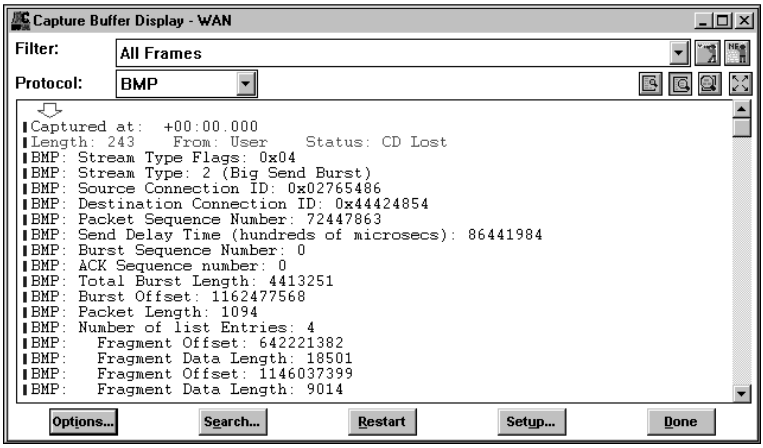
Missing fragment list
Data fragments not yet received.

If "Burst Offset = 0", four additional fields follow.

Function code
Write/read function.

Starting offset
Offset to start writing(/reading).

Bytes to write
No. of bytes to write(/read).



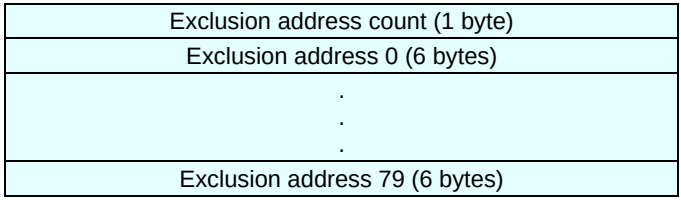
BMP decode

DIAG

"Novell's Guide to NetWare LAN Analysis" by Laura A. Chappell and Dan E. Hakes, Novell Press, 1994

The Diagnostic Responder (DIAG) protocol is useful in analyzing NetWare LANs. DIAG can be used for connectivity testing, configuration and information gathering.

The DIAG request packet structure is shown in the following illustration:

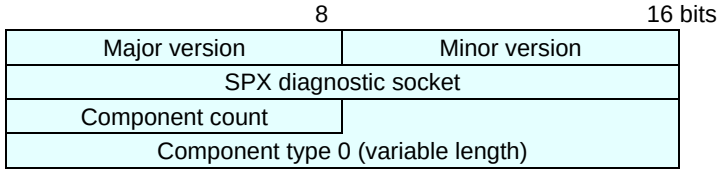


DIAG request packet structure

Exclusion address count

The number of stations that will be requested not to respond. A value of 0 in this field indicates that all stations should respond. The maximum value for this field is 80 (exclusion address 0-79).

The DIAG response packet structure is shown in the following illustration:



DIAG response packet structure

Major/minor version

Version of the diagnostic responder that is installed in the responding station.

SPX diagnostic socket

The socket No. to which all SPX diagnostic responses can be addressed.

Component count
Number of components found within this response packet.

Component type
Contains information about one of the components or active process at the responding node.

Simple:
0 = IPX/SPX.
1 = Router drivers.
2 = LAN drivers.
3 = Shells.
4 = VAPs.

Extended:
5 = Router.
6 = File Server/Router.
7 = Nondedicated IPX/SPX.

Each extended type will be followed by additional fields.

Number of local networks (1 byte)

DIAG additional field

Number of local networks
Number of local networks with which this component can communicate.

For each local network, there will be:

Local network type (1 byte)
Network address (4 bytes)
Node address (6 bytes)

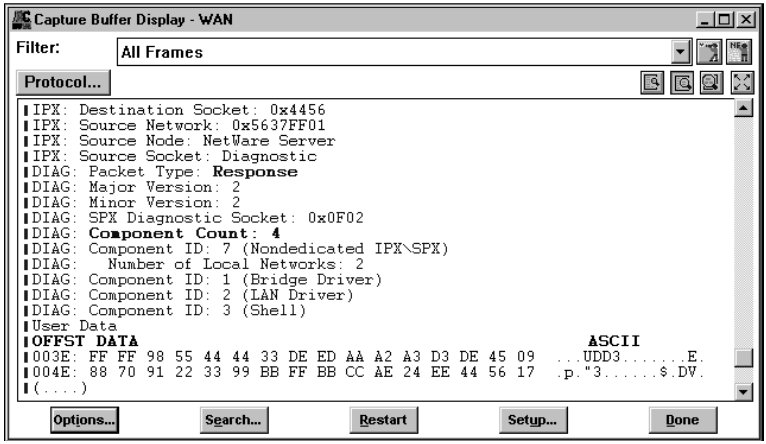
Format for local networks

Local network type
Contains a number indicating the type of network with which the component communicates.

Network address
Contains the 4-byte network address assigned to the network listed in the Local Network Type field.

Node address

Contains the 6-byte node address that accompanies the network address listed above. These will depend on the number of local networks.



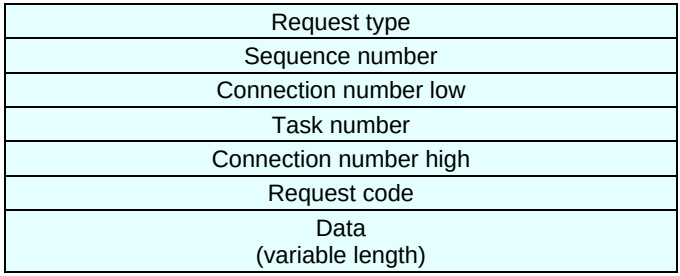
DIAG decode

NCP

"Novell's Guide to NetWare LAN Analysis" by Laura A. Chappell and Dan E. Hakes, Novell Press, 1994

The Novell NetWare Core Protocol (NCP) manages access to the primary NetWare server resources. It makes procedure calls to the NetWare File Sharing Protocol (NFSP) that services requests for NetWare file and print resources.

The format of the NCP Request header is shown in the following illustration. The request type is 2 bytes; all other fields are 1 byte.



NCP request header

Request type

Identifies the packet type:

1111H Allocate slot request.
2222H File server request.
3333H File server reply.
5555H Deallocate slot request.
7777H Burst mode packet (BMP).
9999H Positive acknowledge.
H signifies hexadecimal notation.

Sequence number

Number used by the workstation and file server to identify packets which are sent and received.

Connection number low

Low connection ID number assigned to the workstation.

Task number
Identifies the operating system e.g., DOS, task.

Connection number high
High Connection ID number assigned to the workstation. Used only on the 1000-user version of NetWare, on all other versions will be set to 0.

Request code
Identifies the specific request function code.

The structure of the NCP Reply header is the same as the Request header, but the last 2 bytes differ after Connection Number High. This is shown in the following illustration:

Completion code
Connection status

NCP reply header: last 2 bytes

Completion code
The completion code indicates whether or not the Client's request was successful. A value of 0 in the Completion Code field indicates that the request was successful. Any other value indicates an error.

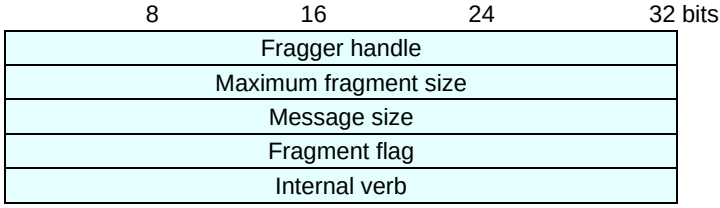
Connection status
The fourth bit in this byte will be set to 1 if DOWN is typed at the console prompt, to bring the server down.

NDS

"Novell's Guide to NetWare LAN Analysis" by Laura A. Chappell and Dan E. Hakes, Novell Press, 1994

NetWare Directory Services (NDS) is a globally distributed network database that replaces the bindery used in previous versions of NetWare. In an NDS-based network, one logs into the entire network providing access to all network services.

The format of the NDS packet is shown in the following illustration:



NDS packet structure

Fragger handle
Fragmented request/reply handle.

Maximum fragment size
Maximum number of data bytes that can be sent as a reply.

Message size
Actual size of the message being sent.

Fragment flag
Flag field, always set to 0.

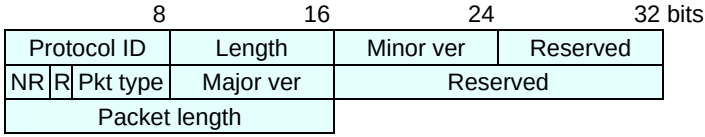
Internal verb
Number of the NDS verb that should be executed.

NLSP

Novell publication NetWare Link Services Protocol Specification rev 1.0

The NetWare Link Services Protocol (NLSP™) provides link state routing for Internetwork Packet Exchange networks. It is a protocol for information exchange among routers geared to the needs of large IPX networks. IPX is the network layer protocol used by the Novell NetWare operating system.

The general format of the header is shown in the following illustration:



NLSP header structure

Protocol ID
Identifies the NLSP routing layer.

Length indicator
The number of bytes in the fixed portion of the header.

Minor version
The value of this field is one.

NR
Multi-homed non-routing server, a 1-bit field. When the value of this field is one, the system has more than one network interface, but does not forward traffic from one network segment to another.

R
Reserved, 2-bit field.

Packet type
The packet type.

Major version
The value of this field is one.

Packet length

The entire length of the packet in bytes, including the fixed portion of the NLSP header.

NovelNetBIOS

This is a proprietary protocol developed by Novell based on NetBIOS.

The data stream type field is a 1-byte fixed field. All of the other fields are variable. Possible values for the data stream type field are:

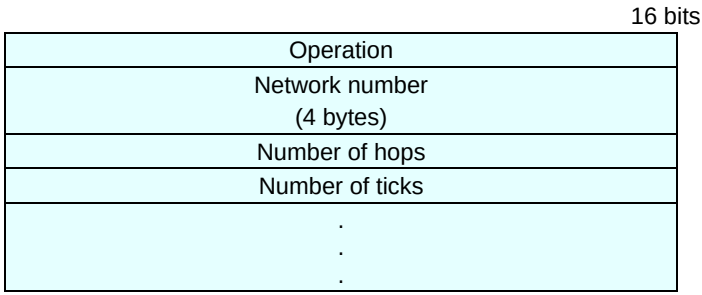
1 Find Name.
2 Name Recognized.
3 Check Name.
4 Name in Use.
5 De-Register Name.
6 Session Data.
7 Session End.
8 Session End Ack.
9 Status Query.
10 Status Response.
11 Directed Datagram.

RIPX

"Novell's Guide to NetWare LAN Analysis" by Laura A. Chappell and Dan E. Hakes, Novell Press, 1994

The Routing Information Protocol (RIP), is used to collect, maintain and exchange correct routing information among gateways within the Internet. This protocol should not be confused with RIP of the TCP/IP suite of protocols.

The format of the RIPX packet is shown in the following illustration.



Operation

Specifies the packet operation:

1 RIP Request.
2 RIP Response.

Network number

The 32-bit address of the specified network.

Number of hops

The number of routers that must be passed to reach the specified network. Routers broadcast "going down", containing the value 16 in this field, which means the route is no longer available.

Number of ticks

A measure of time needed to reach the specified network (18.21 ticks/second).

SER

"Novell's Guide to NetWare LAN Analysis" by Laura A. Chappell and Dan E. Hakes, Novell Press, 1994

To ensure that a single version of NetWare is not being loaded on multiple servers, the operating system broadcasts copy-protection packets, called Serialization packets, to determine whether there are multiple copies of the same operating system on the network.

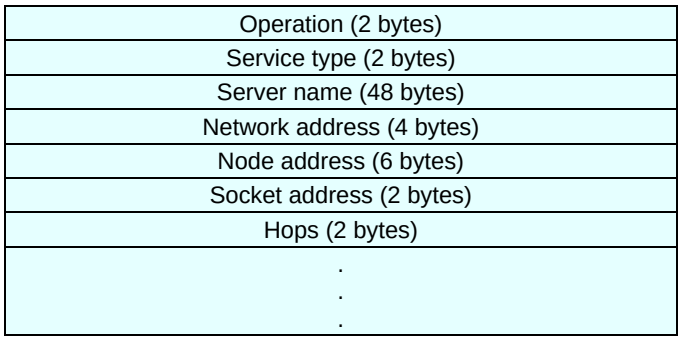
Serialization packets contain only one field, the 6-byte Serialization Data field.

SAP

"Novell's Guide to NetWare LAN Analysis" by Laura A. Chappell and Dan E. Hakes, Novell Press, 1994

Before a client can communicate with a server it must know what servers are available on the network. This information is made available through Novell's Service Advertising Protocol (SAP). SAP services provide information on all the known servers throughout the entire internetwork. These servers can include file servers, print servers, NetWare access servers, remote console servers and so on.

The format of the SAP response packet is shown in the following illustration:



SAP response packet structure

The SAP packet may have up to 7 sets of server information.

Operation

Specifies the operation that the packet will perform:

1 General service request.
2 General service response.
3 Nearest service request.
4 Nearest service response.

Service type

Specifies the service performed. Examples include:

01H User.
04H File service.
07H Print server.

21H NAS SNA gateway.
23H NACS.
27H TCP/IP gateway.
98H NetWare access server.
107H NetWare 386 STOREXP Spec.
137H NetWare 386 print queue.
H signifies hexadecimal notation.

Server name
48-byte field containing the server's name in quotation marks.

Network address
32-bit network number of server.

Node address
48-bit node number of server.

Socket address
16-bit socket number of server.

Hops
Number of routers that must be passed through to reach the specified network. If the value in this field is 16 the service in not available.

The structure of the Request header is shown in the following illustration:

Operation (2 bytes)
Service type (2 bytes)

SAP request header

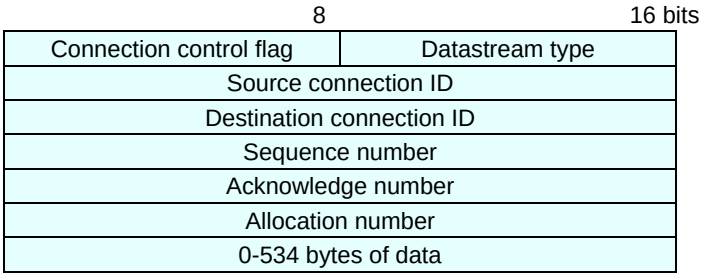
SPX

"Novell's Guide to NetWare LAN Analysis" by Laura A. Chappell and Dan E. Hakes, Novell Press, 1994

The Sequential Packet Exchange (SPX), is Novell's version of the Xerox Sequenced Packet Protocol (SPP). It is a transport layer protocol providing a packet delivery service for third party applications.

In July 1991, Novell established an SPX development team to create an improved version of SPX called SPX II. The primary improvements provided by SPX II include utilization of larger packets sizes and implementation of a windowing protocol.

The structure of the SPX packet is shown in the following illustration:



SPX packet structure

Connection control flag

Four flags which control the bi-directional flow of data across an SPX connection. These flags have a value of 1 when set and 0 if not set.

Bit 4 Eom: End of message.
Bit 5 Att: Attention bit, not used by SPX.
Bit 6 Ack: Acknowledge required.
Bit 7 Sys: Transport control.

Datastream type

Specifies the data within the packet:

0-253 Ignored by SPX.
254 End of connection.
255 End of connection acknowledgment.

Source connection ID
A 16-bit number assigned by SPX to identify the connection.

Destination connection ID
The reference number used to identify the target end of the transport connection.

Sequence number
A 16-bit number, managed by SPX, which indicates the number of packets transmitted.

Acknowledge number
A 16-bit number, indicating the next expected packet.

Allocation number
A 16-bit number, indicating the number of packets sent but not yet acknowledged.

The SPX II header is the same as the SPX header described above, except for the following differences:

Connection control flag
Bit 2 - Size negotiation.
Bit 3 - SPX II type.

Datastream type
252 - Orderly release request.
253 - Orderly release acknowledgment.

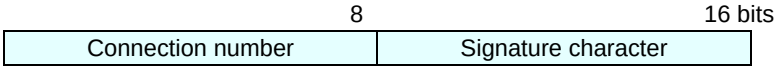
There is also an additional 2-byte Extended Acknowledgement field at the end.

WDOG

"Novell's Guide to NetWare LAN Analysis" by Laura A. Chappell and Dan E. Hakes, Novell Press, 1994

The Watchdog (WDOG) protocol provides constant validation of active workstation connections and notifies the NetWare operating system when a connection may be terminated as a result of lengthy periods without communication.

The format of the WDOG packet is shown in the following illustration:



WDOG packet structure

Connection number
Given to the station during the login process.

Signature character
Contains 0x3F (ASCII character ?) or 0x59 (ASCII character Y).