IPX and IP Protocols

Phil Jensen
Y390 Internship

July 29, 1998

Table of Contents

* IPX
  - IPX Packet Structure
  - IPX Addressing
  - Network Number
  - Node Number
  - Socket Number
  - IPX Routing
IPX

Novell adapted IPX from the Xerox Network System (XNS) Internet Datagram Protocol (IDP). IPX is a connectionless datagram protocol. Connectionless means that when a process running on a particular node uses IPX to communicate with a process on another node, no connection between the two nodes is established. Thus, IPX packets containing data are addressed and sent to their destinations, but there is no guarantee or verification of successful delivery. Any packet acknowledgment, or connection control, is provided by protocols above IPX, such as SPX (Sequenced Packet Exchange). Datagram means that each packet is treated as an individual entity, having no logical or sequential relation to any other packet.

IPX operates at the Open Systems Interconnection (OSI) Network layer. As a Network-layer protocol, IPX addresses and
routes packets from one location to another on an IPX internetwork. IPX bases its routing decisions on the address fields in its header and on the information it receives from RIP (Routing Information Protocol) or NLSP (NetWare Link Services Protocol). IPX uses this information to forward packets to their destination node or to the next router, providing a path to the destination node.

(Novell 4.11 Online Documentation )

**IPX Packet Structure**

The IPX packet is similar to an XNS IDP packet and consists of two parts. First, there is a 30-byte IPX header. This includes the network, node, and socket addresses for both the destination and the source.

Second, there is a data section which often includes the header of a higher-level protocol, such as SPX.

The minimum IPX packet size, excluding the MAC (Media Access Control) header, is 30 bytes (IPX header only). Historically, the maximum size of routed IPX packets has been 576 bytes (IPX header and data). Until recently, all routed IPX packets were between 30 and 576 bytes. However, the IPX protocol has always allowed packet sizes up to 65,535 bytes. However, media constraints typically limit the actual maximum packet size allowed to something less than 65,535. Ethernet II packets, for example, are limited to a data size of 1500 bytes, not including the MAC header.

The IPX header is placed after the MAC header and before the data. The following figure shows the structure of an IPX packet.

![IPX Packet Structure Diagram](image-url)

The checksum is used by the NetWare SFT IIITM (System Fault Tolerant) software, NetWare 4, and newer versions of the NetWare shell (NETx.COM). Older versions of NetWare did not use the IPX checksum and required that this field be set to
The packet length is the length in bytes, of the complete packet, which is the length of the IPX header plus the length of the data. The packet length is at least 30 bytes (for the IPX header).

Transport Control is the number of routers a packet has traversed on the way to its destination. On a traditional, RIP-based IPX router, IPX packets whose Transport Control field reaches a value of 16 are discarded. With NLSP, an IPX packet can travel up to 127 hops to reach its destination. You make this possible by setting the Hop Count Limit parameter from the Internetworking Configuration utility (INETCFG). This enables you to limit the number of routers (hops) an IPX packet traverses before it is discarded. Sending nodes always set the Transport Control field to zero when building an IPX packet. When a router receives a packet that requires further routing, it increments this field by one and forwards the packet.

The packet type is the type of service offered or required by the packet.

The destination network is the number of the network to which the destination node is attached. When a sending node sets this field to zero, the destination node is assumed to be on the same network segment as the sending (or source) node. A special case exists when a workstation sends SAP (Service Advertising Protocol) Get Nearest Server and RIP Get Local Target (or Route Request) broadcast requests at initialization time. Because the workstation does not yet know which network it belongs to, it sets both the Source Network and Destination Network fields to 0 for these requests. When a router receives one of these requests, it sends a reply directly to the sending workstation, filling in the Source Network and Destination Network fields with the appropriate network numbers.

The Destination Node is a physical address of a device such as a file server, router, workstation or a printer. Not all LAN topologies use the same size address field. A node on an Ethernet network requires all six bytes to specify its address; a node on an Omninet network requires only one byte. A node address of 0xFFFFFFFFFFFF (that is, six bytes of 0xFF) broadcasts the packet to all nodes on the destination network.

The destination socket is the socket address of the packet destination process. Sockets route packets to different processes within a single node. Novell reserves several sockets for use in the NetWare environment. IPX does not have a broadcast socket number (such as 0xFFFF).

The source network is the number of the network to which the source node is attached. If a sending node sets this field to zero, the local network to which the source is connected is unknown. For routers, the rules that apply to the Destination Network field also apply to the Source Network field, except that routers can propagate packets that were received with this field set to zero.

The destination socket is the socket address of the process that transmits the packet. Processes communicating in a peer-to-peer fashion do not need to send and receive on the same socket number. In a workstation-server situation, the server usually "listens" on a specific socket for service requests. In such a case, the source socket is not necessarily the same or even significant. All that matters is that the server reply to the source socket. For example, all Netware file servers have the same socket address, but requests to them can originate from any socket number. Source socket numbers follow the same conventions as those for destination sockets.

The higher-level protocol headers are the headers of higher-level NetWare protocols, such as NCP (NetWare Core Protocol) or SPX. These headers occupy the data portion of the IPX packet.

**IPX Addressing**

IPX defines its own internetwork and intranode addressing. For intranetwork (node) addressing, IPX uses the physical address assigned to the network interface card (NIC).
The IPX network address uniquely identifies an IPX server on an IPX network and individual processes within the server. A complete IPX network address is a 12-byte hexadecimal number comprised of a four-byte network number (server), a six-byte node number (server) and a two-byte socket number (server process). A complete IPX network address looks something like this:

<table>
<thead>
<tr>
<th>Network #</th>
<th>Node #</th>
<th>Socket #</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEDCBA98</td>
<td>1A2B3C5D7E9F</td>
<td>0453</td>
</tr>
</tbody>
</table>

Each number is contained in a field in the IPX header and represents a source or destination network, node, or socket. The network number is used only for Network-layer operations, namely routing. The node number is used for local, or same-segment, packet transmission. The socket number directs a packet to a process operating within a node.

Each component of the IPX address is described in the following sections.

**Network Number**

The network number is the four-byte hexadecimal address that serves as the basis for IPX internetwork routing. Each network segment on an internetwork is assigned a unique network number. NetWare routers use this number to forward packets to their final destination segment.

The network number can contain up to eight digits, including zeros. (Leading zeros are usually not displayed.) For example, FEDCBA98, 1234567D, and C7 are all valid network numbers. The numbers 0 and FFFFFFFF are not available for network addressing; IPX reserves these for special purposes.

NetWare 3 and NetWare 4 servers have an additional identifier called an internal network number. This is a unique hexadecimal number between one and eight digits that is assigned to the server at installation. The internal network is a logical network that NetWare uses to advertise services and route IPX packets to the physical networks attached to the server.

The internal network number overcomes some routing and connectivity limitations inherent to NetWare 2. These are summarized in the following paragraphs.

A NetWare 2 server selects a primary interface and advertises its services as reachable through that interface. On a network with more than one server, packets might travel an extra hop to reach their destination.

A NetWare 2 server loses network connectivity if its primary network interface board fails, even if the server has Network-layer connectivity through another interface. Consider a NetWare 2 server with connections to two networks. The server advertises its services through the primary interface attached to one of the networks. If that interface fails, workstations attached to the server through the second network might not be able to log in to the server.

**Node Number**

The node number is the six-byte hexadecimal address that identifies a device on an IPX network. This device can be a file server, router, workstation, or printer. The node number is identical to the physical address assigned to the interface board that connects the device to the network.

The IPX header contains a Destination Node field and a Source Node field. These fields contain the same destination and source node addresses found in the MAC header. A NetWare workstation, for example, uses the destination node address to locate and forward packets to another workstation on the same network segment.

IPX requires the node number to be unique only within the same IPX network. For example, a node on network FEDCBA98
can use the number 1A2B3C5D7E9F, and a node on network 1234567D can also use the number 1A2B3C5D7E9F. Because each node has a different network number, IPX recognizes each node as having a legitimate, unique address.

**Socket Number**

The socket number is the two-byte hexadecimal number that identifies the ultimate destination of an IPX packet within the node. This destination is actually a process---such as routing (RIP) or advertising (SAP) that operates within the node. Because several processes are typically operating at any given time, socket numbers provide a type of "mail slot" by which each process can identify itself to IPX.

A process that must communicate on the network requests that a socket number be assigned to it. Any packets that IPX receives that are addressed to that socket are passed on to the process. Socket numbers provide a quick method of routing packets within a node.

**IPX Routing**

NetWare routers interconnect different IPX network segments and receive instructions for addressing and routing packets between these segments from the IPX protocol. IPX accomplishes these and other Network-layer tasks with the help of RIP, SAP, and NLSP.

---

**TCP/IP**

TCP/IP (Transmission Control Protocol/Internet Protocol) is a popular suite of standard networking protocols. These protocols are widely used, enabling dissimilar nodes in a heterogeneous environment to communicate with one another.

The general concept of connecting a network of dissimilar computers arose from research conducted by the Defense Advanced Research Projects Agency (DARPA). Within the framework of that research, DARPA developed the TCP/IP suite of protocols to communicate among networks and implemented an internetwork called the ARPAnet, which later evolved into the Internet. The TCP/IP suite of protocols defines formats and rules for the transmission and receipt of information independent of any given network organization or computer hardware. Although the protocols were developed for the Internet, TCP/IP is now the de facto standard as numerous private and public organizations use it for their networking.

The network, as conceived by DARPA and implemented with the TCP/IP suite of protocols, is a packet-switched network. A packet-switched network transmits information on the network in small segments, called packets. If one computer transmits a lengthy file to another computer, for example, the file is divided into many packets at the origin and then reassembled at the destination. The TCP/IP protocols define the format of these packets. This definition includes the origin of the packet, the destination of the packet, the length of the packet, and the type of packet, as well as the way computers on the networks are to receive and retransmit packets.

TCP/IP routing capabilities allow forwarding of IP traffic from one network to another. TCP/IP uses the Routing Information Protocol (RIP), Exterior Gateway Protocol (EGP), or Open Shortest Path First (OSPF) protocol to communicate with other routers. This lets all routers in the internetwork discover the internetwork configuration without human intervention.
IP Routing
TCP/IP's IP routing capabilities allow forwarding of IP traffic from one network to another. Routers on a TCP/IP internetwork exchange information about themselves. The TCP/IP software supports link state, distance vector, and static routing.

RIP
The Routing Information Protocol (RIP) uses the distance vector algorithm as the basis for routing operations and decisions. RIP is a standard protocol that is based on the distance vector algorithm. The majority of the TCP/IP sites use RIP.

(A Guide to Networking Essentials by Ed Tittel and David Johnson)

The Distance Vector Algorithm
The class of routing algorithms that periodically broadcast routing information rather than sending information only when a change occurs in a route. Routers using the distance vector algorithm periodically exchange information about accessible networks with their immediate neighbors. Each node on the network consolidates the information it receives and passes it on to other routers, servers, and end nodes.

The TCP/IP Suite of Protocols
The protocols in the TCP/IP suite roughly correspond to a network communications model defined by the International Organization for Standardization (ISO). This model is called the Open Systems Interconnection (OSI) reference model. The OSI model describes an ideal computer network system in which communication on the network occurs between processes at discrete and identifiable layers. Each layer on a given host provides services to layers above it and receives services from the layers below it.
Overview of TCP/IP Protocol Usage

Applications developed for TCP/IP generally use several of the protocols in the suite. The sum of the layers of the protocol suite is also known as the protocol stack. User applications communicate with the top layer of the protocol suite. The top-level protocol layer on the source computer passes information to the lower layers of the stack, which in turn pass it to the physical network. The physical network transfers the information to the destination computer. The lower layers of the protocol stack on the destination computer pass the information to higher layers, which in turn pass it to the destination application.

Each protocol layer within the TCP/IP suite has various functions; these functions are independent of the other layers. Each layer, however, expects to receive certain services from the layer beneath it, and each layer provides certain services to the layer above it.

Each layer of the protocol stack on the source computer communicates with that same layer on the destination computer. The layers at the same level on the source and destination computers are peers. The application on the source computer and the application on the destination computer are also peers. From the perspective of the software developer or user, the transfer takes place as if the peer layers sent their packets directly to one another.