Network Working Group
Request for Comments: 1552
Category: Standards Track

W. Simpson
Daydreamer

December 1993

The PPP Internetwork Packet Exchange Control Protocol (IPXCP)

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

The Point-to-Point Protocol (PPP) [1] provides a method for transmitting multi-protocol datagrams over point-to-point links. PPP defines an extensible Link Control Protocol, and proposes a family of Network Control Protocols for establishing and configuring different network-layer protocols.

The IPX protocol was originally used in Novell’s NetWare products [3], and is now supported by numerous other vendors. This document defines the Network Control Protocol for establishing and configuring the IPX protocol over PPP.

This memo is the product of the Point-to-Point Protocol Working Group of the IETF. Comments should be submitted to the ietf-ppp@ucdavis.edu mailing list.

Table of Contents

1. Introduction

PPP has three main components:

1. A method for encapsulating multi-protocol datagrams.

2. A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.

3. A family of Network Control Protocols for establishing and configuring different network-layer protocols.

In order to establish communications over a point-to-point link, each end of the PPP link must first send LCP packets to configure and test the data link. After the link has been established and optional facilities have been negotiated as needed by the LCP, PPP must send IPXCP packets to choose and configure the IPX network-layer protocol. Once IPXCP has reached the Opened state, IPX datagrams can be sent over the link.

The link will remain configured for communications until explicit LCP or IPXCP packets close the link down, or until some external event occurs (an inactivity timer expires or network administrator intervention).

1.1 Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST

This word, or the adjective "required", means that the definition is an absolute requirement of the specification.

MUST NOT

This phrase means that the definition is an absolute prohibition of the specification.

SHOULD

This word, or the adjective "recommended", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and carefully weighed before choosing a different course.

MAY

This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option MUST be prepared to interoperate with another implementation which does include the option.

1.2 Terminology

This document frequently uses the following terms:

peer

The other end of the point-to-point link.

silently discard

This means the implementation discards the packet without further processing. The implementation SHOULD provide the capability of logging the error, including the contents of the silently discarded packet, and SHOULD record the event in a statistics counter.

end-system

A user's machine. It only sends packets to servers and other end-systems. It doesn't pass any packets through itself.

router

Allows packets to pass through, usually from one ethernet segment to another. Sometimes these are called "intermediate-systems".

half-router

Two normal routers, with an unnumbered link between them. Each looks like a router to the local users, but Netware doesn't understand unnumbered links, so each router is made to look like they both are a single machine.

2. A PPP Network Control Protocol for IPX

The IPX Control Protocol (IPXCP) is responsible for configuring, enabling, and disabling the IPX protocol modules on both ends of the point-to-point link. IPXCP uses the same packet exchange mechanism as the Link Control Protocol. IPXCP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase. IPXCP packets received before this phase is reached should be silently discarded.

The IPX Control Protocol is exactly the same as the Link Control Protocol [1] with the following exceptions:

Frame Modifications

The packet may utilize any modifications to the basic frame format which have been negotiated during the Link Establishment phase.

Data Link Layer Protocol Field

Exactly one IPXCP packet is encapsulated in the Information field of a PPP Data Link Layer frame where the Protocol field indicates type hex 802B (IPX Control Protocol).

Code field

Only Codes 1 through 7 (Configure-Request, Configure-Ack, Configure-Nak, Configure-Reject, Terminate-Request, Terminate-Ack and Code-Reject) are used. Other Codes should be treated as unrecognized and should result in Code-Rejects.

Timeouts

IPXCP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase. An implementation should be prepared to wait for Authentication and Link Quality Determination to finish before timing out waiting for a Configure-Ack or other response. It is suggested that an implementation give up only after user intervention or a configurable amount of time.

Configuration Option Types

IPXCP has a distinct set of Configuration Options.

2.1 Sending IPX Datagrams

Before any IPX packets may be communicated, PPP must reach the Network-Layer Protocol phase, and the IPX Control Protocol must reach the Opened state.

Exactly one IPX packet is encapsulated in the Information field of a PPP Data Link Layer frame where the Protocol field indicates type hex 002B (IPX datagram).

The maximum length of an IPX datagram transmitted over a PPP link is the same as the maximum length of the Information field of a PPP data link layer frame. Since there is no standard method for fragmenting and reassembling IPX datagrams, PPP links supporting IPX MUST allow at least 576 octets in the information field of a data link layer frame.

2.2 IPX-WAN protocol

A Novell specification called IPX-WAN [4] is intended to provide mechanisms similar to IPXCP negotiation over wide area links. As viewed by PPP, IPX-WAN is a part of IPX, and IPX-WAN packets are indistinguishable from other IPX packets.

Currently, Novell has implemented IPXCP without any Configuration Options, and requires successful IPX-WAN completion, even when all required parameters have been hand configured. This makes it impossible for the current Novell products to interoperate with other IPXCP implementations which do not already include support for IPX-WAN.

2.3 Desired Parameters

To resolve the possible conflict between the two configuration methods, this specification defines the concept of "Desired

Parameters". Where applicable, each Configuration Option indicates the environment where the parameter which is negotiated MAY be required by the implementation for proper operation.

This determination is highly implementation dependent. For example, a particular implementation might require that all links have addresses, while another implementation might not need such addresses. The configuration negotiation is intended to discover that this pair of implementations will never converge.

2.4 Co-existence with IPX-WAN

An IPXCP implementation which includes support for IPX-WAN SHOULD always reach Opened state, even when unable to negotiate some "Desired Parameter", and when no Configuration Options are successfully negotiated. This allows IPX-WAN the opportunity to finish the negotiation.

If an implementation does not include support for IPX-WAN, it SHOULD NOT reach Opened state when unable to negotiate some "Desired Parameter".

IPX-WAN uses a "Timer Request" packet to set up the link. These MUST NOT be sent until IPXCP has Opened the link.

An implementation which provides both IPX-WAN and IPXCP Configuration Options capability SHOULD only send a Timer Request packet when a Timer Request packet is received, or upon failure to successfully negotiate a "Desired Parameter".

If unable to complete IPX-WAN setup when a "Desired Parameter" is unknown, by default IPXCP SHOULD terminate the link.

However, some implementations might be capable of operating without all indicated "Desired Parameters", in which case the termination MUST be configurable.

3. IPXCP Configuration Options

IPXCP Configuration Options allow modifications to the standard characteristics of the network-layer protocol to be negotiated. If a Configuration Option is not included in a Configure-Request packet, the default value for that Configuration Option is assumed.

IPXCP uses the same Configuration Option format defined for LCP [1], with a separate set of Options.

Up-to-date values of the IPXCP Option Type field are specified in the

most recent "Assigned Numbers" RFC [2]. Current values are assigned as follows:

```
1       IPX-Network-Number
2       IPX-Node-Number
3       IPX-Compression-Protocol
4       IPX-Routing-Protocol
5       IPX-Router-Name
6       IPX-Configuration-Complete
```

3.1 IPX-Network-Number

Description

This Configuration Option provides a way to negotiate the IPX network number to be used for the link. This allows an implementation to learn the network number, or to ensure agreement on the network number.

The network number MUST be unique within the routing domain, or zero to indicate that it is not used for routing.

The sender of the Configure-Request states which network number is desired. A network number specified as zero in a Configure-Request shall be interpreted as requesting the peer to specify another value in a Configure-Nak. A network number specified as zero in a Configure-Ack shall be interpreted as agreement that no value exists.

Both ends of the link MUST have the same network number. When a Configure-Request is received which has a lower network number than locally configured, a Configure-Nak MUST be returned with the highest network number.

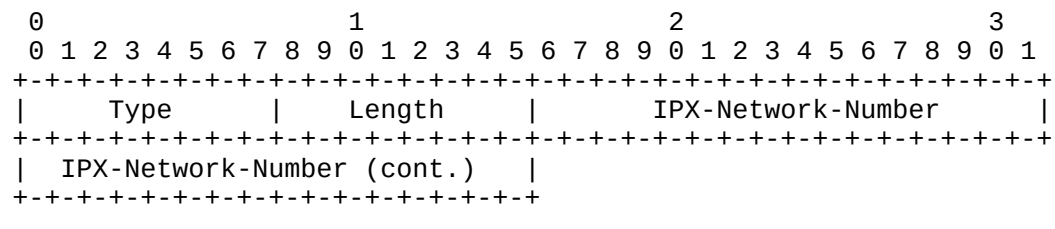
When the peer did not provide the option in its Configure-Request, the option SHOULD NOT be appended to a Configure-Nak.

By default, no network number is assigned to the link (the network number is zero). There is no need for a network number if the interface is not used by a routing protocol.

This is a Desired Parameter when the implementation is operating as a router. It MUST be negotiated if the network number is non-zero, and has been derived from another interface.

Any IPX-WAN packets received MUST supercede information negotiated in this option.

A summary of the IPX-Network-Number Configuration Option format is shown below. The fields are transmitted from left to right.



Type

1

Length

6

IPX-Network-Number

The four octet IPX-Network-Number is the desired local IPX network number of the sender of the Configure-Request. This number may be zero, which is interpreted as being a local network of unknown number that is not used by the routing protocol.

3.2 IPX-Node-Number

Description

This Configuration Option provides a way to negotiate the IPX node number to be used for the local end of the link. This allows an implementation to learn its node number, or to inform the peer of its node number.

The node number MUST be unique for the network number.

The sender of the Configure-Request states which node number is desired. A node number specified as zero in a Configure-Request shall be interpreted as requesting the peer to specify another value in a Configure-Nak. A node number specified as zero in a Configure-Ack shall be interpreted as agreement that no value exists.

If negotiation about the peer node number is required, and the peer did not provide the option in its Configure-Request, the option can be appended to a Configure-Nak. The value of the node number given MUST be acceptable as the peer IPX-Node-Number, or

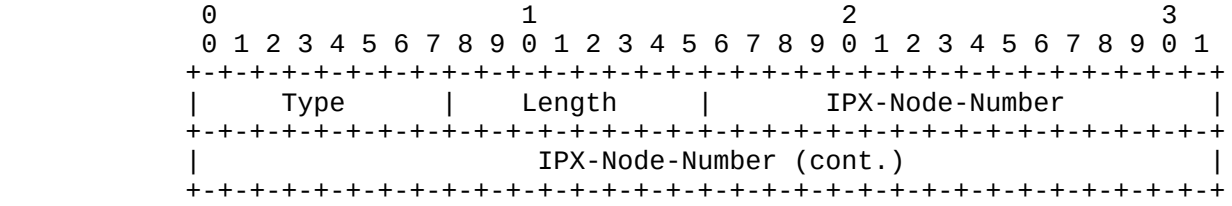
indicate with a zero value that the peer provide the information.

By default, no node number is assigned to the link (the node number is zero). There is no need for a node number if the interface is not used by a routing protocol.

This is a Desired Parameter when the implementation is operating as an end-system. However, when the node number has been statically configured, this option SHOULD NOT be negotiated unless requested by the peer.

Any IPX-WAN packets received MUST supercede information negotiated in this option.

A summary of the IPX-Node-Number Configuration Option format is shown below. The fields are transmitted from left to right.



Type

2

Length

8

IPX-Node-Number

The six octet IPX-Node-Number is the desired local IPX node number of the sender of the Configure-Request.

3.3 IPX-Compression-Protocol

Description

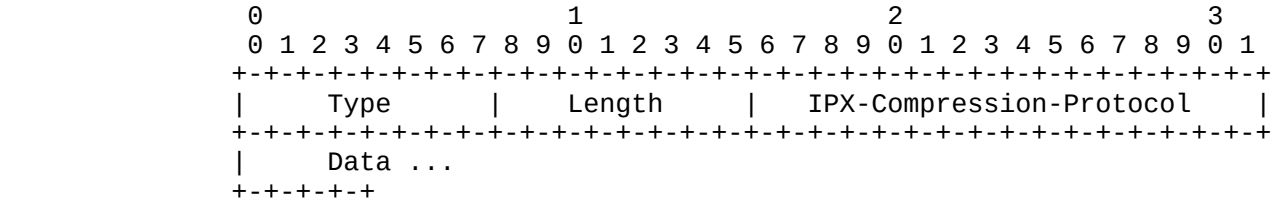
This Configuration Option provides a way to negotiate the use of a specific compression protocol. By default, compression is not enabled.

The sender of this Configuration Option indicates that it can receive packets with the specified compression technique. A

Configure-Ack MAY obligate the peer to send such packets, depending on the protocol negotiated.

Information negotiated in this option MUST supercede any IPX-WAN packets received, since IPX-WAN packets could be affected by the compression technique.

A summary of the IPX-Compression-Protocol Configuration Option format is shown below. The fields are transmitted from left to right.



Type

3

Length

>= 4

IPX-Compression-Protocol

The IPX-Compression-Protocol field is two octets and indicates the compression protocol desired. Odd values for this field are always the same as the PPP Data Link Layer Protocol field values for that same compression protocol. Even values are used when the compression protocol is interleaved with IPX packets.

Up-to-date values of the IPX-Compression-Protocol field are specified in the most recent "Assigned Numbers" RFC [2]. Current values are assigned as follows:

Value (in hex)	Protocol
0002	Telebit Compressed IPX
0235	Shiva Compressed NCP/IPX

Data

The Data field is zero or more octets and contains additional data as determined by the particular compression protocol.

3.4 IPX-Routing-Protocol

Description

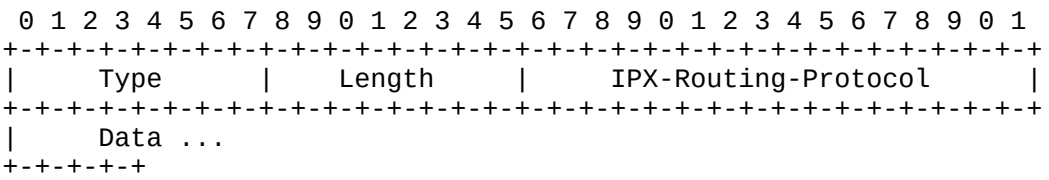
This Configuration Option provides a way to negotiate the use of a specific routing protocol (or no routing protocol, if desired). The sender of this option is specifying that it wishes to receive information of the specified routing protocol. Multiple protocols MAY be requested by sending multiple IPX-Routing-Protocol Configuration Options. The "no routing protocol required" value is mutually exclusive with other values.

By default, Novell's combination of Routing Information Protocol (RIP) and Server Advertising Protocol (SAP) is expected.

This is a Desired Parameter when the implementation is operating as an end-system, to indicate that no routing protocol is necessary.

Any IPX-WAN packets received MAY add to information negotiated in this option.

A summary of the IPX-Routing-Protocol Configuration Option format is shown below. The fields are transmitted from left to right.



Type

4

Length

>= 4

IPX-Routing-Protocol

The IPX-Routing-Protocol field is two octets and indicates the type of Routing-Protocol desired. This two octet quantity is sent most significant octet first.

Up-to-date values of the IPX-Routing-Protocol field are specified

in the most recent "Assigned Numbers" RFC [2]. Current values are assigned as follows:

Value	Protocol
0	No routing protocol required
1	RESERVED
2	Novell RIP/SAP required
4	Novell NLSP required

Data

The Data field is zero or more octets and contains additional data as determined by the routing protocol indicated in the Routing-Protocol field.

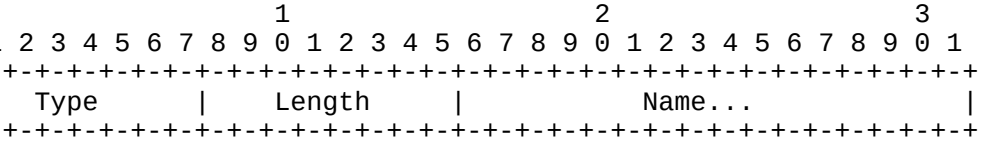
3.5 IPX-Router-Name

Description

This Configuration Option provides a way to convey information about the IPX server name.

The nature of this option is advisory only. It is provided as a means of improving the end system's ability to provide a simple user interface. This option MUST NOT be included in a Configure-Nak.

A summary of the IPX-Router-Name Option format is shown below. The fields are transmitted from left to right.



Type

5

Length

>= 3

Name

This field contains the name of the IPX entity on this end of the link. The symbolic name should be between 1 and 47 ASCII characters in length, containing the characters 'A' through 'Z', underscore (_), hyphen (-) and "at" sign (@). The length of the name is bounded by the option length.

On reception, the name SHOULD be padded to 48 characters using the NUL character. Those readers familiar with NetWare 3.x servers will realize that this is equivalent to the file server name.

3.6 IPX-Configuration-Complete

Description

This Configuration Option provides a way to indicate that all implementation-dependent Desired Parameters are satisfied. It is provided as a means of detecting when convergence will occur in a heterogeneous environment.

This option SHOULD be included in a Configure-Request when the combination of statically configured parameters and offered Configuration Options will result in successful configuration.

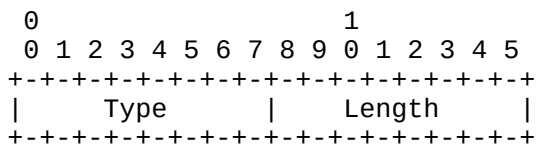
The nature of this option is advisory only. This option MUST NOT be included in a Configure-Nak.

Implementation Note: An implementation which does not support IPX-WAN can immediately detect that link setup will not be successful when a Desired Parameter is unknown, if this option is not present in the peer's Configure-Request or is Rejected by the peer. This avoids timeout delays.

An implementation which supports IPX-WAN may improve link setup time by skipping IPX-WAN entirely when this option has been Ack'd in both directions.

However, it is perfectly acceptable to complete configuration without including this option. An implementation which includes the entire panoply of configuration options and IPX- WAN SHOULD interoperate with an implementation which does not support IPX-WAN nor any configuration options (including this one), as long as the Desired Parameters are satisfied by default or hand configuration.

A summary of the IPX-Configuration-Complete Option format is shown below. The fields are transmitted from left to right.



Type

6

Length

2

APPENDIX A. Link Delay and Throughput

There has been some concern over correctly estimating the link delay (in 55 millisecond ticks) used by Novell routing protocols.

IPX-WAN uses its Timer Request and Reply for this purpose. The measured delay is multiplied by a factor of 6, because the measurement is done during initialization of the link, and does not reflect actual loading.

The delay is better measured using the PPP LCP Echo facility, by inserting a timestamp in the data part of the Request, and comparing it with the same timer when the reply returns. This method could be used to periodically re-evaluate the actual round trip delay as link and system loads change. The echo packet size SHOULD be 576, to match the default IPX packet size.

In the absence of such dynamic measurements, empirical evidence has shown the following to be sufficient:

2,400 bps	134 ticks
14,400 bps	21 ticks
57,600 bps	5 ticks
> 1 Mbps	1 tick

Security Considerations

Security issues are not discussed in this memo.

References

[1] Simpson, W., "The Point-to-Point Protocol (PPP)", RFC 1548, Daydreamer, December 1993.

[2] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1340, USC/Information Sciences Institute, July 1992.

[3] Novell Inc., "NetWare System Interface Technical Overview", Novell Part Number 883-001143-001.

[4] Allen, M., "Novell IPX Over Various WAN Media", RFC 1551, Novell Inc., December 1993.

[5] Mathu, S., and M. Lewis, "Compressing IPX Headers Over WAN Media (CIPX)", RFC 1553, Telebit Corporation, December 1993.

Acknowledgments

Some of the text in this document is taken from previous documents produced by the Point-to-Point Protocol Working Group of the Internet Engineering Task Force (IETF).

This document is derivative of drafts written by the following people. Many thanks for their work, and for taking an initial stab at the protocol:

Michael Allen (mallen@novell.com)
Dave McCool (dave@shiva.com)
Robert D Vincent (bert@shiva.com)
Marty Del Vecchio (marty@shiva.com)

Chair’s Address

The working group can be contacted via the current chair:

Fred Baker
Advanced Computer Communications
315 Bollay Drive
Santa Barbara, California, 93111

EMail: fbaker@acc.com

Author's Address

Questions about this memo can also be directed to:

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
P O Box 6205
East Lansing, MI 48826-6205

EMail: Bill.Simpson@um.cc.umich.edu