Network Working Group
Request for Comments: 1356
Obsoletes: RFC 877

A. Malis
BBN Communications
D. Robinson
Computervision Systems Integration
R. Ullmann
Process Software Corporation
August 1992

Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode

Status of this Memo

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

Abstract

This document specifies the encapsulation of IP and other network layer protocols over X.25 networks, in accordance and alignment with ISO/IEC and CCITT standards. It is a replacement for RFC 877, "A Standard for the Transmission of IP Datagrams Over Public Data Networks" [1].

It was written to correct several ambiguities in the Internet Standard for IP/X.25 (RFC 877), to align it with ISO/IEC standards that have been written following RFC 877, to allow interoperable multiprotocol operation between routers and bridges over X.25, and to add some additional remarks based upon practical experience with the specification over the 8 years since that RFC.

The substantive change to the IP encapsulation is an increase in the allowed IP datagram Maximum Transmission Unit from 576 to 1600, to reflect existing practice.

This document also specifies the Internet encapsulation for protocols, including IP, on the packet mode of the ISDN. It applies to the use of Internet protocols on the ISDN in the circuit mode only when the circuit is established as an end-to-end X.25 connection.

Acknowledgements

RFC 877 was written by J. T. Korb of Purdue University, and this document follows that RFC's format and builds upon its text as appropriate. This document was produced under the auspices of the IP over Large Public Data Networks Working Group of the IETF.

1. Conventions

The following language conventions are used in the items of specification in this document:

- MUST -- the item is an absolute requirement of the specification. MUST is only used where it is actually required for interoperation, not to try to impose a particular method on implementors where not required for interoperability.

- SHOULD -- the item should be followed for all but exceptional circumstances.

- MAY or optional -- the item is truly optional and may be followed or ignored according to the needs of the implementor.

The words "should" and "may" are also used, in lower case, in their more ordinary senses.

2. Introduction

RFC 877 was written to document the method CSNET and the VAN Gateway had adopted to transmit IP datagrams over X.25 networks. Its success is evident in its current wide use and the inclusion of its IP protocol identifier in ISO/IEC TR 9577, "Protocol Identification in the Network Layer" [2], which is administered by ISO/IEC and CCITT.

However, due to changes in the scope of X.25 and the protocols that it can carry, several inadequacies have become evident in the RFC, especially in the areas of IP datagram Maximum Transmission Unit (MTU) size, X.25 maximum data packet size, virtual circuit management, and the interoperable encapsulation, over X.25, of protocols other than IP between multiprotocol routers and bridges.

As with RFC 877, one or more X.25 virtual circuits are opened on demand when datagrams arrive at the network interface for transmission. A virtual circuit is closed after some period of inactivity (the length of the period depends on the cost associated with an open virtual circuit). A virtual circuit may also be closed if the interface runs out of virtual circuits.

3. Standards

3.1 Protocol Data Units (PDUs) are sent as X.25 "complete packet sequences". That is, PDUs begin on X.25 data packet boundaries and the M bit ("more data") is used to fragment PDUs that are larger than one X.25 data packet in length.

In the IP encapsulation the PDU is the IP datagram.

3.2 The first octet in the Call User Data (CUD) Field (the first data octet in the Call Request packet) is used for protocol demultiplexing, in accordance with the Subsequent Protocol Identifier (SPI) in ISO/IEC TR 9577. This field contains a one-octet Network Layer Protocol Identifier (NLPID), which identifies the network layer protocol encapsulated over the X.25 virtual circuit. The CUD field MAY contain more than one octet of information, and receivers MUST ignore all extraneous octets in the field.

In the following discussion, the most significant digit of the binary numbers is left-most.

For the Internet community, the NLPID has four relevant values:

The value hex CC (binary 11001100, decimal 204) is IP [6]. Conformance with this specification requires that IP be supported. See section 5.1 for a diagram of the packet formats.

The value hex 81 (binary 10000001, decimal 129) identifies ISO/IEC 8473 (CLNP) [4]. ISO/IEC TR 9577 specifically allows other ISO/IEC connectionless-protocol packets, such as ES-IS and IS-IS, to also be carried on the same virtual circuit as CLNP. Conformance with this specification does not require that CLNP be supported. See section 5.2 for a diagram of the packet formats.

The value hex 82 (binary 10000010, decimal 130) is used specifically for ISO/IEC 9542 (ES-IS) [5]. If there is already a circuit open to carry CLNP, then it is not necessary to open a second circuit to carry ES-IS. Conformance with this specification does not require that ES-IS be supported.

The value hex 80 (binary 10000000, decimal 128) identifies the use of IEEE Subnetwork Access Protocol (SNAP) [3] to further encapsulate and identify a single network-layer protocol. The SNAP-encapsulated protocol is identified by including a five-octet SNAP header in the Call Request CUD field immediately following the hex 80 octet. SNAP headers are not included in the subsequent X.25 data packets. Only one SNAP-encapsulated protocol may be carried over a virtual circuit

opened using this encoding. The receiver SHOULD accept the incoming call only if it can support the particular SNAP-identified protocol. Conformance with this specification does not require that this SNAP encoding be supported. See section 5.3 for a diagram of the packet formats.

The value hex 00 (binary 00000000, decimal 0) identifies the Null encapsulation, used to multiplex multiple network layer protocols over the same circuit. This encoding is further discussed in section 3.3 below.

The "Assigned Numbers" RFC [7] contains one other non-CCITT and non-ISO/IEC value that has been in active use for Internet X.25 encapsulation identification, namely hex C5 (binary 11000101, decimal 197) for Blacker X.25. This value MAY continue to be used, but only by prior preconfiguration of the sending and receiving X.25 interfaces to support this value. The value hex CD (binary 11001101, decimal 205), listed in "Assigned Numbers" for "ISO-IP", is also used by Blacker and also can only be used by prior preconfiguration of the sending and receiving X.25 interfaces.

Each system MUST only accept calls for protocols it can process; every Internet system MUST be able to accept the CC encapsulation for IP datagrams. A system MUST NOT accept calls, and then immediately clear them. Accepting the call indicates to the calling system that the protocol encapsulation is supported; on some networks, a call accepted and cleared is charged, while a call cleared in the request state is not charged.

Systems that support NLPIDs other than hex CC (for IP) SHOULD allow their use to be configured on a per-peer address basis. The use of hex CC (for IP) MUST always be allowed between peers and cannot be configured.

3.3 The NLPID encodings discussed in section 3.2 only allow a single network layer protocol to be sent over a circuit. The Null encapsulation, identified by a NLPID encoding of hex 00, is used in order to multiplex multiple network layer protocols over one circuit.

When the Null encapsulation is used, each X.25 complete packet sequence sent on the circuit begins with a one-octet NLPID, which identifies the network layer protocol data unit contained only in that particular complete packet sequence. Further, if the SNAP NLPID (hex 80) is used, then the NLPID octet is immediately followed by the five-octet SNAP header, which is then immediately followed by the encapsulated PDU. The encapsulated network layer protocol MAY differ from one complete packet sequence to the next over the same

circuit.

When a receiver is presented with an Incoming Call identifying the Null encapsulation, the receiver MUST accept the call if it supports the Null encapsulation for any network layer protocol. The receiver MAY then silently discard a multiplexed PDU if it cannot support that particular encapsulated protocol. See section 5.4 for a diagram of the packet formats.

Use of the single network layer protocol circuits described in section 3.2 is more efficient in terms of bandwidth if only a limited number of protocols are supported by a system. It also allows each system to determine exactly which protocols are supported by its communicating partner. Other advantages include being able to use X.25 accounting to detail each protocol and different quality of service or flow control windows for different protocols.

The Null encapsulation, for multiplexing, is useful when a system, for any reason (such as implementation restrictions or network cost considerations), may only open a limited number of virtual circuits simultaneously. This is the method most likely to be used by a multiprotocol router, to avoid using an unreasonable number of virtual circuits.

If performing IEEE 802.1d bridging across X.25 is desired, then the Null encapsulation MUST be used. See section 4.2 for a further discussion.

Conformance with this specification does not require that the Null encapsulation be supported.

Systems that support the Null encapsulation SHOULD allow its use to be configured on a per-peer address basis.

3.4 For compatibility with existing practice, and RFC 877 systems, IP datagrams MUST, by default, be encapsulated on a virtual circuit opened with the CC CUD.

Implementations MAY also support up to three other possible encapsulations of IP:

- IP may be contained in multiplexed data packets on a circuit using the Null (multiplexed) encapsulation. Such data packets are identified by a NLPID of hex CC.

- IP may be encapsulated within the SNAP encapsulation on a circuit. This encapsulation is identified by containing, in the 5-octet SNAP

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.