BVCP

RFC 1763 http://www.cis.ohio-state.edu/htbin/rfc/rfc1763.html

The PPP Banyan VINES Control Protocol (BVCP) is responsible for configuring, enabling, and disabling the VINES protocol modules on both ends of the point-to-point link. BVCP uses the same packet exchange mechanism as the Link Control Protocol (LCP).

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

Code	Identifier	Length	Data
1 byte	1 byte	2 byte	variable

BVCP packet structure

Code

Decimal value which indicates the type of BVCP packet.

- 1 Configure-Request.
- 2 Configure-Ack.
- 3 Configure-Nak.
- 4 Configure-Reject.
- 5 Terminate-Request.
- 6 Terminate-Ack.
- 7 Code-Reject.

Identifier

Decimal value which aids in matching requests and replies.

Length

Length of the BVCP packet, including the Code, Identifier, Length and Data fields.

Data

Variable length field which may contain one or more configuration options. The format of the BVCP configuration options is as follows:

Type Lengt	n Data
------------	--------

BVCP configuration options

One-byte indication of the type of the configuration option.

- BV-NS-RTP-Link-Type.
- 2 BV-FRP (fragmentation protocol).
- 3 BV-RTP.
- 4 BV-Suppress-Broadcast.

Length

Length of the configuration option including the type, length and data fields.

Data

CCP

RFC 1962 http://www.cis.ohio-state.edu/htbin/rfc/rfc1962.html

The Compression Control Protocol (CCP) is responsible for configuring the data compression algorithms on both ends of the point-to-point link. It is also used to signal a failure of the compression/decompression mechanism in a reliable manner. CCP uses the same packet exchange mechanism as the Link Control Protocol. CCP packets cannot be exchanged until PPP has reached the Network-Layer Protocol phase. CCP packets received before this phase is reached are discarded.

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

Code	Identifier	Length	Data
1 byte	1 byte	2 bytes	variable

CCP packet structure

Code

Decimal value which indicates the type of CCP packet.

- 1 Configure-Request.
- 2 Configure-Ack.
- 3 Configure-Nak.
- 4 Configure-Reject.
- 5 Terminate-Request.
- 6 Terminate-Ack.
- 7 Code-Reject.
- 14 Reset Request.
- 15 Reset-Ack.

Identifier

Decimal value which aids in matching requests and replies.

Length

Length of the CCP packet, including the Code, Identifier, Length and Data fields.

Data

Variable length field which may contain one or more configuration options. The format of the CCP configuration options is as follows:

Туре	Length	Data

CCP configuration options

Type

One-byte indication of the type of the configuration option.

- 0 OUI.
- 1 Predictor Type 1.
- 2 Predictor Type 2.
- 3 Puddle Jumper.
- 16 Hewlett-Packard-PPC.
- 17 Stac Electronics LZS.
- 18 MicroSoft PPC.
- 19 Gandalf FZA.
- 20 V.42 bis Compression.
- 21 BSD LZW Compress.
- 23 LZS-DCP.

Length

Length of the configuration option including the Type, Length and Data fields.

Data

DNCP

RFC 1376 http://www.cis.ohio-state.edu/htbin/rfc/rfc1376.html

The PPP DECnet Phase IV Control Protocol is responsible for establishing and configuring Digital's DNA Phase IV routing protocol (DECnet Phase IV) over PPP. The protocol applies only to DNA Phase IV routing messages (both data and control), and not to other DNA Phase IV protocols (MOP, LAT, etc).

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

Code	Identifier	Length	Data
1 byte	1 byte	2 bytes	variable

DNCP packet structure

Code

Decimal value which indicates the type of DNCP packet.

- 1 Configure-Request.
- 2 Configure-Ack.
- 3 Configure-Nak.
- 4 Configure-Reject.
- 5 Terminate-Request.
- 6 Terminate-Ack.
- 7 Code-Reject.

Identifier

Decimal value which aids in matching requests and replies.

Length

Length of the DNCP packet, including the Code, Identifier, Length and Data fields.

Data

A variable length field which in similar protocols contains options, DNCP packets, however, have no options.



RFC 1968 http://www.cis.ohio-state.edu/htbin/rfc/rfc1968.html

The Encryption Control Protocol (ECP) is responsible for configuring and enabling data encryption algorithms on both ends of the point-to-point link. ECP uses the same packet exchange mechanism as the Link Control Protocol (LCP). ECP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase. ECP packets received before this phase is reached are silently discarded.

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

Code	Identifier	Length	Data
1 byte	1 byte	2 bytes	variable

ECP header structure

Code

A one octet field identifying the type of ECP packet. When a packet is received with an unknown Code field, a Code Reject packet is transmitted.

- 1 Configure-Request.
- 2 Configure-Ack.
- 3 Configure-Nak.
- 4 Configure-Reject.
- 5 Terminate-Request.
- 6 Terminate-Ack.
- 7 Code-Reject.
- 14 Reset-Request.
- 15 Reset-Ack.

Identifier

Decimal value which aids in matching requests and replies.

Length

Length of the ECP packet, including the Code, Identifier, Length and Data fields.

IPv6CP

RFC 2023 http://www.cis.ohio-state.edu/htbin/rfc/rfc2023.html

The IPv6 PPP Control Protocol is responsible for configuring, enabling and disabling the IPv6 protocol modules on both ends of the point-to-point link.

The format of the IPv6CP packet is shown in the following illustration:

Code	Identifier	Length	Data
1 byte	1 byte	2 bytes	variable

IPv6CP packet structure

Code

Decimal value which indicates the type of IPv6CP packet.

- 1 Configure-Request.
- 2 Configure-Ack.
- 3 Configure-Nak.
- 4 Configure-Reject.
- 5 Terminate-Request.
- 6 Terminate-Ack.
- Code-Reject.

Identifier

Decimal value which aids in matching requests and replies.

Length

Length of the IPv6CP packet, including the Code, Identifier, Length and Data fields.

Variable length field which may contain one or more configuration options. The format of the IPv6CP configuration options is as follows:

Туре	Length	Data
------	--------	------

IPv6CP configuration options

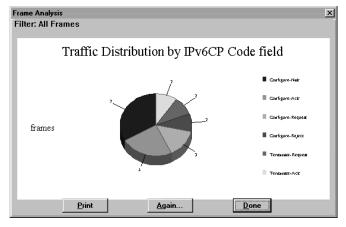
One-byte indication of the type of the configuration option.

- 1 Interface-Token.
- 2 IPv6-Compression-Protocol.

Length

Length of the configuration option including the type, length and data fields.

Data



Graph of traffic distribution by IPv6CP code field

IPCP

RFC 1332 http://www.cis.ohio-state.edu/htbin/rfc/rfc1332.html

The IP Control Protocol (IPCP) is responsible for configuring the IP protocol parameters on both ends of the point-to-point link. IPCP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPCP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase. Any IPCP packets received before this phase is reached are discarded.

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

Code	Identifier	Length	Data
1 byte	1 byte	2 bytes	variable

IPCP packet structure

Code

Decimal value which indicates the type of IPCP packet.

- 1 Configure-Request.
- 2 Configure-Ack.
- 3 Configure-Nak.
- 4 Configure-Reject.
- 5 Terminate-Request.
- 6 Terminate-Ack.
- 7 Code-Reject.

Identifier

Decimal value which aids in matching requests and replies.

Length

Length of the IPCP packet, including the Code, Identifier, Length and Data fields.

Data

Variable length field which may contain one or more configuration options. The format of the IPCP configuration options is as follows:

Type	Length	Data
------	--------	------

IPCP configuration options

One-byte indication of the type of the configuration option.

- IP Addresses use of which is deprecated. Use of 3 is preferred.
- 2 IP Compression Protocol.
- 3 IP Address - way to negotiate the IP address to be used on the local end of the link.

Length

Length of the configuration option including the Type, Length and Data fields.

Data

IPXCP

RFC 1552 http://www.cis.ohio-state.edu/htbin/rfc/rfc1552.html

In order to establish communication 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 may 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 format of the IPXCP packet is shown in the following illustration:

Code	Identifier	Length	Data
1 byte	1 byte	2 bytes	variable

IPXCP packet structure

Code

Decimal value which indicates the type of IPXCP packet.

- 1 Configure-Request.
- 2 Configure-Ack.
- 3 Configure-Nak.
- 4 Configure-Reject.
- 5 Terminate-Request.
- 6 Terminate-Ack.
- 7 Code-Reject.

Identifier

Decimal value which aids in matching requests and replies.

Length

Length of the IPXCP packet, including the Code, Identifier, Length and Data fields.

Data

Variable length field which may contain one or more configuration options. The format of the IPXCP configuration options is as follows:

Type Length	Data
-------------	------

IPXCP configuration options

One-byte indication of the type of the configuration option.

- IPX Network number.
- 2 IPX Node number.
- 3 IPX Compression protocol.
- 4 IPX Routing protocol.
- 5 IPX Router name.
- 6 IPX Configuration complete.

Length

Length of the configuration option including the Type, Length and Data

Data

LEXCP

RFC 1841 http://www.cis.ohio-state.edu/htbin/rfc/rfc1841.html

A LAN extension interface unit is a hardware device installed at remote sites (such as a home office or small branch office) that connects a LAN across a WAN link to a router at a central site. To accommodate this LAN extension interface architecture, a PPP Network Control Protocol was developed: the LAN extension interface protocol, PPP-LEX. The basic functionality of LEX is to encapsulate LAN extension interface control and data packets. Consequently packets can be control packets or data packets. Data packets are described under LEX.

There are two types of LEXCP packets:

- Startup options packet.
- Remote command options packets.

The startup options packet is the first LEX NCP packet that the LAN extension interface unit sends to the host router after the LCP has reached an open state. This required startup options packet configures the LAN extension interface protocol and puts the LEX NCP in an open state.

Remote command options are the LEX NCP packets that control the functioning and statistics gathering of the LAN extension interface protocol.

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

	Address	Control	Protocol type
	Code	Identifier	Length
Options		ions	
	1 byte	1 byte	2 bytes

PPP + LEX protocol header

Option-type	Option-length	Option-data
1 byte	1 byte	2 bytes

LEX startup options

Option-type	Option-flags	Option-length	Data
1 byte	1 byte	2 bytes	

LEX remote command options

Address

All-stations address: one-octet PPP-specified field which contains the binary sequence 11111111 (hexadecimal 0xFF). PPP does not assign individual station addresses. The all-stations address must be recognized and received by all devices.

Control

Unnumbered Information (UI) command with the P/F bit set to zero. Oneoctet PPP-specified field which contains the binary sequence 00000011 (hexadecimal 0x03).

Protocol type

IETF-assigned protocol type value. For control packets this field with take the value 0x8041.

Code

Identifies the type of LCP packet that the LAN extension interface packet is sending. Valid values are as follows:

Startup options:

0x01 Configure-Request.

0x02 Configure-Ack.

0x03 Configure-Nak.

0x04 Configure-Rej.

Remote command options:

0x40 LEX_RCMD_REQUEST packet.

0x41 LEX RCMD ACK packet.

0x42 LEX RCMD NAK packet.

0x43 LEX_RCMD_REJ packet.

Identifier

Randomly generated value which aids matching requests and replies. It is recommended that a non-zero value be used for the identifier. That is, zero could be used in the future for unsolicited messages from the LAN extension interface unit. Valid values are 0x01-0xFF.

Length

Length of the entire packet in octets, including the Code, Identifier, Length, and Option fields.

Option-type

Identifies the startup option or remote command option being negotiated.

Valid values for startup options are as follows:

- 0x01 MAC Type.
- 0x03 MAC Address.
- 0x05 LAN Extension.

Valid values for remote command options are as follows:

- 0x01 Filter Protocol Type.
- 0x02 Filter MAC Address.
- 0x03 Set Priority.
- 0x04 Disable LAN Extension Ethernet Interface.
- 0x05 Enable LAN Extension Ethernet Interface.
- 0x06 Reboot LAN Extension Interface Unit.
- 0x07 Request Statistics.
- 0x08 Download Request.
- 0x09 Download Data.
- 0x0A Download Status.
- 0x0B Inventory Request.

Option-length

Specifies the length of the option fields, including the option-type, optiondata, option-length and option-flags (for remote command) fields.

Option-data

Data relating to the value specified in the option-type field. The data for startup options is as specified here:

Option-data
The most up-to-date value of the MAC type,
currently 0x01 for IEEE 802.3/Ethernet with
canonical addresses.
Actual MAC address in IEEE 802.3 canonical
format.
LAN extension interface software information.
0x01 is the current protocol version supported.

Option-flags

Specifies the remote command option, containing specific actions that must be followed. This field is only present in remote command option packets.

NBFCP

RFC 2097 http://www.cis.ohio-state.edu/htbin/rfc/rfc2097.html

The PPP NetBIOS Frames Control Protocol (NBFCP) is a network control protocol responsible for establishing and configuring the NBF protocol over PPP. The NBFCP protocol is only applicable to an end system connecting to a peer system, or the LAN to which the peer system is connected.

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

Code	Identifier	Length	Data
1 byte	1 byte	2 bytes	variable

NBFCP packet structure

Code

Decimal value which indicates the type of NBFCP packet.

- Configure-Request.
- 2 Configure-Ack.
- 3 Configure-Nak.
- 4 Configure-Reject.
- 5 Terminate-Request.
- 6 Terminate-Ack.
- Code-Reject.

Identifier

Decimal value which aids in matching requests and replies.

Length

Length of the NBFCP packet, including the Code, Identifier, Length and Data fields.

Data

Variable length field which may contain one or more configuration options. The format of the NBFCP configuration options is as follows:

Туре	Length	Data
------	--------	------

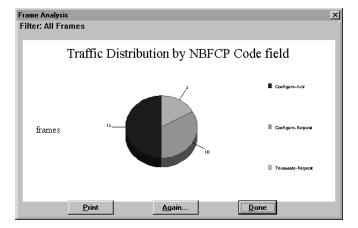
One-byte indication of the type of the configuration option.

- 1 Name-Projection.
- 2 Peer-Information.
- 3 Multicast-Filtering.
- 4 IEEE-MAC-Address-Required.

Length

Length of the configuration option including the Type, Length and Data fields.

Data



Graph of traffic distribution by NBFCP code field

OSINLCP

RFC 1377 http://www.cis.ohio-state.edu/htbin/rfc/rfc1377.html

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

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

Code	Identifier	Length	Data
1 byte	1 byte	2 bytes	variable

OSINLCP header structure

Code

A one-octet field identifying the type of OSINLCP packet. When a packet is received with an unknown Code field, a Code Reject packet is transmitted.

- 1 Configure-Request.
- 2 Configure-Ack.
- 3 Configure-Nak.
- 4 Configure-Reject.
- 5 Terminate-Request.
- 6 Terminate-Ack.
- 7 Code-Reject.

Identifier

Decimal value which aids in matching requests and replies.

Length

Length of the OSINLCP packet, including the Code, Identifier, Length and Data fields.

Data

Variable length field which may contain one or more configuration options.

SDCP

RFC 1963 http://www.cis.ohio-state.edu/htbin/rfc/rfc1963.html

The PPP Serial Data Control Protocol (SDCP) is responsible for configuring, enabling and disabling the SDTP (Serial Data Transport Protocol) modules on both ends of the point-to-point link. SDCP uses the same packet exchange mechanism and state machine as the Link Control Protocol. SDCP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase.

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

	Code	Identifier	Length	Data
_	1 byte	1 byte	2 bytes	variable

SDCP header structure

Code

A one octet field identifying the type of SDCP packet. When a packet is received with an unknown Code field, a Code Reject packet is transmitted.

- 1 Configure-Request.
- 2 Configure-Ack.
- 3 Configure-Nak.
- 4 Configure-Reject.
- 5 Terminate-Request.
- 6 Terminate-Ack.
- 7 Code-Reject.

Identifier

Decimal value which aids in matching requests and replies.

Length

Length of the SDCP packet, including the Code, Identifier, Length and Data fields.

Data

Variable length field which may contain one or more configuration options. The format of the SDCP configuration options is as follows:

Туре	Length	Data

SDCP configuration options

Type

One-byte indication of the type of the configuration option.

- Packet-Format.
- 2 Header-Type.
- 3 Length-Field-Present.
- 4 Multi-Port.
- 5 Transport-Mode.
- Maximum-Frame-Size. 6
- 7 Allow-Odd-Frames.
- 8 FCS-Type.
- 9 Flow-Expiration-Time.

Length of the configuration option including the Type, Length and Data fields.

Data

SNACP

RFC 2043 http://www.cis.ohio-state.edu/htbin/rfc/rfc2043.html

The SNA PPP Control Protocol (SNACP) is responsible for configuring, enabling, and disabling SNA on both ends of the point-to-point link. Note that there are actually two SNA Network Control Protocols; one for SNA over LLC 802.2 and another for SNA without LLC 802.2. These SNA NCPs are negotiated separately and independently of each other. 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 SNACP packets to choose and configure the SNA network-layer protocol. Once SNACP has reached the opened state, SNA datagrams can be sent over the link.

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

Code	Identifier	Length	Data
1 byte	1 byte	2 bytes	variable

SNACP packet structure

Code

Decimal value which indicates the type of SNACP packet.

- 1 Configure-Request.
- 2 Configure-Ack.
- 3 Configure-Nak.
- 4 Configure-Reject.
- 5 Terminate-Request.
- 6 Terminate-Ack.
- 7 Code-Reject.

Identifier

Decimal value which aids in matching requests and replies.

Length

Length of the SNACP packet, including the Code, Identifier, Length and Data fields.

Data

Variable length field.