BINL Protocol Specifications

```
Client packet starts with: 0x81
Server packet starts with: 0x82
```

Note: int32, short16 and unicode strings are Little Endian

NCQ - Network Card Query (issued by the client)

```
00000000  81 4e 43 51 30 00 00 00  02 00 00 00 00 00 00 00  |.NCQ0...........|
00000010  00 0c 29 15 c4 17 00 00  00 00 00 00 00 00 00 00  |..).............|
00000020  02 00 00 00 22 10 00 20  02 00 00 10 88 00 00 00  |...."..  ........|
00000030  22 10 00 20 16 00 5c 5c  41 74 74 69 6c 61 5c 52  |".. ..\\Attila\R|
00000040  65 6d 49 6e 73 74 5c 77  69 6e 70 65 00 00        |emInst\winpe..  |
```

NCQ Structure

Name	Offset	Bytes	CType	Sample	Description
tag	0x00	4	char[4]	\x81NCQ	
len	0x04	4	int32	0x30	Size of the packet excluding tag and len
u1	0x08	4	int32	0x2	
u2	0x0c	4	int32	0x0	
mac	0x10	6	byte[6]	00:0c:29:15:c4:17	Mac Address
pad	0x16	2	byte[2]	00:00	Padding
u3	0x18	4	int32	0x0	
u4	0x1c	4	int32	0x0	
u5	0x20	4	int32	0x2	
vid	0x24	2	short16	0x1022	Vendor id 0x1022 is AMD
pid	0x26	2	short16	0x2000	Product id 0x2000 is AMD pcnet vmware card
rev_u1	0x28	1	byte	0x2	
rev_u2	0x29	1	byte	0x0	
rev_u3	0x2a	1	byte	0x0	
rev	0x2b	1	byte	0x10	
rev2	0x2c	4	int32	0x88	
subsys	0x30	4	int32	0x20001022	Device Subsystem
lenp	0x34	2	short16	0x16	Installation path len including trailing \x00
path	0x36	(23)	char	\\Attila\RemInst\winpe	Installation path
eop	0x4d	1	byte	0x0	End of packet - always 0x0

NCR - Network Card Reply (reply from server)

```
00000000  82 4e 43 52 c4 00 00 00  00 00 00 00 02 00 00 00  |.NCR............|
00000010  24 00 00 00 50 00 00 00  6a 00 00 00 56 00 00 00  |$...P...j...V...|
00000020  76 00 00 00 50 00 43 00  49 00 5c 00 56 00 45 00  |v...P.C.I.\.V.E.|
00000030  4e 00 5f 00 31 00 30 00  32 00 32 00 26 00 44 00  |N._.1.0.2.2.&.D.|
00000040  45 00 56 00 5f 00 32 00  30 00 30 00 30 00 00 00  |E.V._.2.0.0.0...|
00000050  70 00 63 00 6e 00 74 00  70 00 63 00 69 00 35 00  |p.c.n.t.p.c.i.5.|
00000060  2e 00 73 00 79 00 73 00  00 00 50 00 43 00 6e 00  |..s.y.s...P.C.n.|
00000070  65 00 74 00 00 00 44 65  73 63 72 69 70 74 69 6f  |e.t...Descriptio|
00000080  6e 00 32 00 53 63 68 65  64 61 20 45 74 68 65 72  |n.2.Scheda Ether|
00000090  6e 65 74 20 50 43 49 20  41 4d 44 20 50 43 4e 45  |net PCI AMD PCNE|
000000a0  54 20 46 61 6d 69 6c 79  00 43 68 61 72 61 63 74  |T Family.Charact|
000000b0  65 72 69 73 74 69 63 73  00 31 00 31 33 32 00 42  |eristics.1.132.B|
000000c0  75 73 54 79 70 65 00 31  00 35 00 00 00 00        |usType.1.5....  |
```

NCR Structure

Name	Offset	Bytes	CType	Sample	Description
tag	0x00	4	char[4]	\x82NCR	
len	0x04	4	int32	0xc4	Size of the packet excluding tag and len
res	0x08	4	int32	0x0	Result code 0x0: Ok - 0xc000000d: Not Found
type	0x0c	4	int32	0x2	Type
boff	0x10	4	int32	0x24	Base offset
doff	0x14	4	int32	0x50	Driver name offset
soff	0x18	4	int32	0x6a	Service name offset
plen	0x1c	4	int32	0x56	Parameters list length in chars
poff	0x20	4	int32	0x76	Parameters list offset
dev	0x24	(1)			
sep1	0x25	1	byte	0x0	Separator
drv	0x26	(25)	char	pcntpci5.sys	Unicode Driver name
sep2	0x3f	1	byte	0x0	Separator
srv	0x40	(11)	char	PCnet	Unicode Service Name
sep3	0x4b	1	byte	0x0	Separator
params	0x4c	(2)	char	-	Parameters: variable structure

RQU - File request

```
00000000  81 52 51 55 22 00 00 00  02 00 00 00 01 00 01 00  |.RQU"...........|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000020  00 00 00 00 4c 4f 47 49  4e 0a                    |....LOGIN.      |
```

RQU Structure

Name	Offset	Bytes	CType	Sample	Description
tag	0x00	4	char[4]	\x81RQU	
len	0x04	4	int32	0x22	Size of the packet excluding tag and len
u1	0x08	28	char[28]	Binary Data	Unknown binary data sent back in reply
file	0x24	(8)	char	LOGIN\n	Requested filename without .osc ext

RSU - File reply

```
00000000  82 52 53 55 a5 03 00 00  02 00 00 00 01 00 01 00  |.RSU............|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000020  00 00 00 00 3c 4f 53 43  4d 4c 3e 0a 3c 54 49 54  |....<OSCML>.<TIT|
00000030  4c 45 3e 20 20 43 6c 69  65 6e 74 20 49 6e 73 74  |LE>  Client Inst|
00000040  61 6c 6c 61 74 69 6f 6e  20 57 69 7a 61 72 64 20  |allation Wizard |
00000050  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20  |                |
...
00000380  42 4f 44 59 3e 0a 3c 2f  4f 53 43 4d 4c 3e 0a 00  |BODY>.</OSCML>..|
```

RSU Structure

Name	Offset	Bytes	CType	Sample	Description
tag	0x00	4	char[4]	\x82RSU	
len	0x04	4	int32	0x3a5	Size of the packet excluding tag and len
u1	0x08	28	char[28]	Binary Data	Unknown binary data sent back in reply
data	0x24	(6)	char	.....	File data
eop	0x2a	1	byte	0x0	End of packet - always 0x0