Doc. No. 78-3942-01

CiscoWorks Blue Native Service Point for NetView Release Notes

This release note provides information about changes to CiscoWorks Blue Native Service Point 1.0 that are not documented in the *CiscoWorks Blue Native Service Point for NetView User Guide*. Use this release note as a supplement to the *CiscoWorks Blue Native Service Point for NetView User Guide*.

This release note contains information on the following:

SNA Alerts

The following sections list each of the Network Management Vector Transports (NMVTs) SNA alerts, by type, that are generated by Cisco devices and forwarded to NetView.

This section contains information on the following:

- SDLC Alerts
- Token Ring MAC (802.5) Alerts
- 802.2 Alerts
- CSMA/CD Alerts
- LAP-B Alerts
- (Q)LLC Alerts
- X.25 Packet Layer Alerts

In the tables of alerts, the following terms are used:

Alert ID The number that identifies the alert.

Failure Cause Vertical list of 2-byte codes in hexadecimal number.

Alert Description A brief description of the alert.

Note Information displayed in braces {} indicates the Communications Manager (CM) description. IDs displayed in braces {} indicate the CM version of the alert ID.

SDLC Alerts

Table 1 SDLC Alerts

Alert ID	Failure Cause	Alert Description
32A37F1B	F017	Poll retry exhausted
BD84C4C9	F01A	DM received
D635CA1E	F015	SNRM received while in NRM
B776CA94	F010	FRMR received—invalid cmd/rsp
B3B7D723	F011	FRMR received—I-field not allowed
BEF4F1FA	F012	FRMR received—invalid Nr
BA35EC4D	F013	FRMR received—max I-field exceeded
15C2CCE5	F020	Protocol error by remote—invalid cmd/rsp
1103D152	F021	Protocol error by remote—I-field not allowed
1C40F78B	F022	Protocol error by remote—invalid Nr
EABB6A14	F01B	Protocol error by remote—MAXIN exceeded
0E2DDF11	F019	Inactivity timer expired (not being polled)
0AECC2A6	F018	XID retry exhausted
A472BC48	F014	FRMR received—no reason given

Token Ring MAC (802.5) Alerts

Table 2 Token Ring MAC Alerts

Alert ID	Alert Description
55BF3E1C	Open failure; 3434—Lobe fault
CAF3C58A	Open failure; 3703—TR Fault Domain {Beaconing}
D615A61E	Open failure; Install Cause 3704—Duplicate TR address
44D1AD86	Open failure; User Cause 7101—Removed from Token Ring
016E5F4E	Adapter Open failed
A676B230	Wire fault; 3434—Lobe fault
EB61E14F	Auto-removal (adapter removed itself from ring)
59F32622	Remove cmd rcvd; User Cause 7101—removed from Token Ring

802.2 Alerts

Table 3 802.2 LLC Alerts

Alert ID	Failure Cause	Alert Description
5B8F5BA7	F017	Poll retry exhausted
B1D9A4C5	F01A	DM received
E65B0B7F	F016	SABME received while in ABME
8A5B2D2C	F010	FRMR received—invalid cmd/rsp
8E9A309B	F011	FRMR received—I-field not allowed
83D91642	F012	FRMR received—invalid Nr
87180BF5	F013	FRMR received—max I-field exceeded
23EF2B5D	F020	Protocol error by remote (FRMR sent)—invalid cmd/rsp
2C2E36EA	F021	Protocol error by remote (FRMR sent)—I-field not allowed
216D1033	F022	Protocol error by remote (FRMR sent)—invalid Nr
25AC0D84	F023	Protocol error by remote (FRMR sent)—max I-field exceeded

CSMA/CD Alerts

Table 4 CSMA/CD Alerts

Alert ID	Alert Description
8B1836C5	Open failure
EB1D6ABB	Remove cmd rcvd; User Cause 7107—removed from CSMA/CD ring
668E036D	Lost carrier
A48865FD	Congestion
91FDE97B	Bus inoperative failure

X.25 Packet Layer Alerts

Table 5 X.25 PLC Alerts

Alert ID	Failure Cause	Alert Description
B5B412E5 {D484ED27}	20C1	(DTE) Cleanup Indication Received {Clear/Reset}
CDA515B8	20C1	(DTE) Cleanup Indication Received {Restart}
D3A1B295 {6A837F72}	20C2	(DTE) Cleanup Request Sent {Reset}
056A9521	20C2	(DTE) Cleanup Request Sent {Clear/Restart}
F50A02F0	20D1	(DTE) Response timer expired
BA5D4659	20B2	(DTE) Protocol violation by remote
4C323FE5	20C3	Diagnostic Packet Received from Network
EFF5FAAD	20C4	(DCE) Cleanup Indication Sent {Restart/Reset/Clear}
FEC0F827	20C5	(DCE) Cleanup Request Received {Restart/Reset/Clear}

LAP-B Alerts

Table 6 LAP-B Alerts

Alert ID	Failure Cause	Alert Description
07B1E788	F023	Protocol error by remote (FRMR sent)—max I-field exceeded
C0E4E919	F022	Protocol error by remote (FRMR sent)—invalid Nr
A596712C {CEA222A9}		LAP-B Comms error {Poll retry exhausted}
985806E2		LAP-B Comms error {Unexpected DISC received}
00891F75	F010	FRMR received—invalid cmd/rsp
CF6F806D	F011	FRMR received—I-field not allowed
F5E40347	F013	FRMR received—max I-field exceeded

Alert ID	Failure Cause	Alert Description
C22CA6B4	F012	FRMR received—invalid Nr
1F9CF04A	F020	Protocol error by remote (FRMR sent)—invalid cmd/rsp
3FAE0180	F021	Protocol error by remote (FRMR sent)—I-field not allowed

(Q)LLC Alerts

Table 7 (Q)LLC Alerts

Alert ID	Failure Cause	Alert Description
6460D9A9	F023	- -
3DA4F8CD	F010	QFRMR received—invalid cmd/rsp
C15B15E8 {9C064C98}	F011	QFRMR received—I-field not allowed
C8C9E4FF {D82E7FD3}	F013	QFRMR received—max I-field exceeded
11A865CF {21F2236D}	F020	Protocol error by remote (QFRMR sent)—invalid cmd/rsp
0283E638 {5DBB5F97}	F021	Protocol error by remote (QFRMR sent)—I-field not allowed

Documentation Corrections

The following items are corrections to the existing *CiscoWorks Blue Native Service Point for NetView User Guide*.

- Steps 5 and 7 in the "Uploading the NSP Files" section located in the "Installing and Configuring Native Service Point" chapter of the *CiscoWorks Blue Native Service Point for NetView User Guide* states that the value for the *prefix* argument is:

  "*prefix* is the file prefix, if your system requires a prefix (the NSP default prefix is your TSO ID). If the TSO User ID option is on, do *not* specify a value for this argument."

  Please note that the correct statement does not include the TSO User ID option, but instead should read:

  "*prefix* is the file prefix, if your system requires a prefix (the NSP default prefix is your TSO ID). If the TSO Profile Command Prefix option is on, do *not* specify a value for this argument."

- The top line of Table E-5 refers to the NETV.NSP.CFCGA data set. The correct data set name is NETV.NSP.CFGA.

Calculating VSAM Storage Requirements

NSP provides a utility to calculate the virtual storage access method (VSAM) storage required by NSP for your network environment. The utility is started by issuing the **nspvsamc** command. Using the answers that you provide for questions about your network, the utility calculates how much VSAM storage is required for the following NSP VSAM data sets:

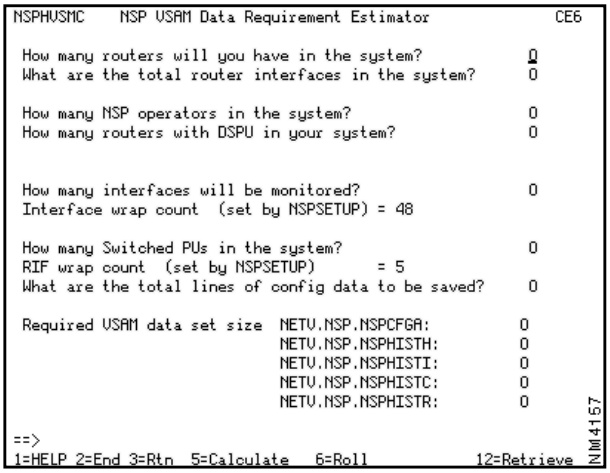
- NSPCFGA
- NSPHISTH
- NSPHISTI
- NSPHISTC
- NSPHISTP
- NSPHISTR

Note For more information on the direct access storage device (DASD) requirements for these data sets, refer to the "NSP DASD Storage Requirements" section in the "General Reference" appendix of the *CiscoWorks Blue Native Service Point for NetView User Guide*.

To calculate the VSAM data required by NSP for your network:

Step 1 From a NetView command line, type **nspvsamc** and press **Enter**. The VSAM Data Requirement Estimator panel is displayed.

Figure 1 NSP VSAM Data Requirement Estimator Panel

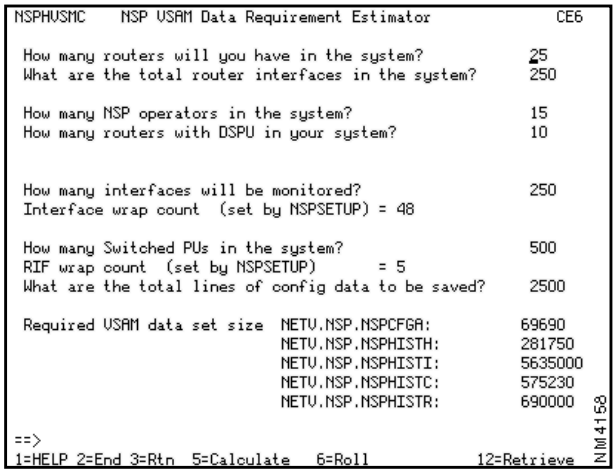


Step 2 In the fields located on the right side of the panel, type an answer for the following questions:

- How many routers will you have in the system?
- What are the total router interfaces in the system?
- How many NSP operators in the system?
- How many routers with DSPU in the system?
- How many interfaces will be monitored?
- How many switched PUs in the system?
- What are the total lines of configuration data to be saved?

Step 3 To calculate the VSAM data required, press **PF5**. In the Required VSAM data set size section, the calculated VSAM storage requirements for each data set are displayed to the right of the data set name.

Figure 2 NSP VSAM Data Requirement Estimator with Calculations



Additional Documentation Information

The following sections contain information that is currently not available in the *CiscoWorks Blue Native Service Point for NetView User Guide*.

Printing NSP VSAM Data Sets

To print an NSP VSAM data set:

Step 1 Open the NSPV1R2.SAMPLIB data set and locate and then open and change the *prefix* argument to the alias in the following members as appropriate:

Select and modify:	To print the:
NSPPCFGA	NSPCFGA member
NSPPHSTC	NSPHISTC member
NSPPHSTH	NSPHISTH member
NSPPHSTI	NSPHISTI member
NSPPHSTR	NSPHISTR member

Step 2 Save and submit the member.

Backing Up and Restoring NSP Data Sets

The NSPREPVS and NSPREPSV members are utilities to backup and restore existing NSP data sets. Use the members to backup NSP VSAM data sets to sequential data sets and restore the sequential data sets to NSP VSAM data sets.

To backup an NSP VSAM data set to a sequential data set:

Step 1 Open the NSPREPVS member (located in the NSPV1R2.SAMPLIB data set) and replace the *prefix* argument and the *member* argument to the appropriate alias and member name.

Step 2 Save and submit the member.

To restore the sequential data set to an NSP VSAM data set:

Step 1 Open the NSPREPSV member (located in the NSPV1R2.SAMPLIB data set) and replace the *prefix* argument and the *member* argument to the appropriate alias and member name.

Step 2 Save and submit the member.

This document is to be used in conjunction with the *CiscoWorks Blue Native Service Point for NetView User Guide* publication.

CiscoWorks Blue Native Service Point for NetView