# Table of Contents

## Chapter 1: About This Help Text
- Alarm Forwarding Overview ................................................................. 5
- Alarm Forwarding Scope and Audience .................................................. 6
- About the Diameter Intelligence Hub (DIH) ......................................... 6
- Setting User Preferences ..................................................................... 7
- Customer Care Center ....................................................................... 14
- DIH Documentation Library ................................................................. 16
- Locate Product Documentation on the Customer Support Site ............ 17
- Diameter Intelligent Hub (DIH) - Copyright, Notice, Trademarks, and Patents ................................................................. 17

## Chapter 2: Introduction to NSP Alarm Forwarding
- Alarm Forwarding Key Features .......................................................... 20
- Alarm Forwarding Architecture .......................................................... 20

## Chapter 3: Working in Alarm Forwarding
- Accessing Alarm Forwarding .............................................................. 23
- Understanding Alarm Forwarding Components ............................... 23
- Alarm Forwarding Toolbar ................................................................ 23
- Using Alarm Forwarding ................................................................. 24
  - Creating a Filter ........................................................................... 24
  - Editing a Filter ............................................................................ 25
- Alarm Forwarding Test Connection ................................................... 26
  - Test Connection for SMTP ............................................................ 26
  - Test Connection for SNMP .......................................................... 26

## Chapter 4: SNMP Agent
- SNMP Overview .............................................................................. 28
- NSP Forwarding MIB ....................................................................... 28
List of Figures

Figure 1: Time Formatting Page.................................................................8
Figure 2: Directory Page..................................................................................9
Figure 3: Mapping Page.................................................................................10
Figure 4: Point Code Tab..............................................................................11
Figure 5: CIC Page........................................................................................12
Figure 6: Alarms Page..................................................................................13
Figure 7: Privacy Page..................................................................................14
Figure 8: Alarm Forwarding Page.................................................................23
Figure 9: Create New Filter Dialog...............................................................24
Figure 10: Filter Configuration Display.........................................................25
Figure 11: Summary Dialog Display..............................................................25
List of Tables

Table 1: Alarm Forwarding Toolbar Icons.................................................................23
Chapter 1

About This Help Text

Topics:

- Alarm Forwarding Overview.....6
- Alarm Forwarding Scope and Audience.....6
- About the Diameter Intelligence Hub (DIH).....6
- Customer Care Center.....14
- DIH Documentation Library.....16
- Locate Product Documentation on the Customer Support Site.....17
- Diameter Intelligent Hub (DIH) - Copyright, Notice, Trademarks, and Patents.....17
Alarm Forwarding Overview

NSP Alarm Forwarding (Alarm Forwarding) enables the user to forward alarms to specified destinations. The user can create alarm forwarding rules using Filters.

This application handles several types of alarms, including those pertaining to

- Traffic supervision
- Quality of service
- SS7 network (nodes, linksets, links)
- System errors

Alarm Forwarding Scope and Audience

This user’s guide provides information about the Network Software Platform (NSP) Alarm Forwarding application. This guide provides definitions and instructions to help the user efficiently and effectively define conditions and destinations for forwarding Alarms. The audience for this manual is the NSP ConfigManager and NSPConfigPowerUser.

About the Diameter Intelligence Hub (DIH)

The Diameter Intelligent Hub (DIH) is used to monitor a LTE network. DIH also creates a small hardware "footprint" for customers who administer 3G and 4G diameter networks. The DIH:

- Is a single blade server and storage blade collocated within a single or dual Diameter Signaling Router (DSR) enclosure(s).
- Provides filtering, data feed, tracing, decoding, and SNMP functions.
- Enables the selective collection and storage of diameter traffic within one or more instances of PMF and IXP.
- Provides nodal diameter troubleshooting.
- Provides data export for diameter messages.
- Supports both IPv4 and IPv6 traffic simultaneously.
- Provides KPI tracking using ProTrace application as well as viewing KPIs in graphic format using ProPerf dashboard configured at installation.
- Provides filtering for alarms using ProTraq Cell filter (see system alarms online help).
- Uses diameter protocol exclusively.

Note: The DIH system can use other protocols if the Diameter mode has not been selected and system is in Standard mode. (Default setting is Standard mode. For more information on selecting Diameter mode, see Centralized Configuration Manager Administration online help, "Setting System to Diameter Mode."

The Diameter Protocol
The diameter protocol has evolved from the Radius protocol and enables diameter applications to extend the base protocol by adding new commands and/or attributes, such as those for use of the Extensible Authentication Protocol (EAP).

The diameter protocol provides for an Authentication, Authorization, and Accounting (AAA) framework that overcomes the limitations of RADIUS, (a protocol that handles AAA and EAP), which cannot effectively deal well with remote access, IP mobility and policy control. The Diameter protocol defines a policy protocol used by clients to perform Policy, AAA and Resource Control. This allows a single server to handle policies for many services.

As mentioned above, Diameter protocol provides AAA functionality, but in addition it is made more reliable by using TCP and SCTP instead of UDP. The Diameter protocol is further enhanced by the development of the 3rd Generation Partnership Project (3GPP) IP Multimedia Subsystem (IMS). Through the use of extensions, the protocol was designed to be extensible to support Proxies, Brokers, Strong Security, Mobile-IP, Network Access Servers (NASREQ), Accounting and Resource Management.

**Setting User Preferences**

Users can set User Preferences that apply across all the NSP applications. These include

- Time specifications (date format, time zone, etc.)
- Directory names (for exporting, uploading, and downloading)
- Enumeration values (numerals vs. text)
- Point code specifications
- CIC specifications
- Default alarm colors
- Default object privacy privileges

**Setting Time Format**

Follow these steps to set the time format:

1. Click **User Preferences** on the Application board.
   The User Preferences page is displayed.
2. Click the **Time** tab.
   The Time page is displayed. The red asterisk denotes a required field.

   **Note:** Use the tips on the page to help you configure the time format.
3. Enter the format for these time-related displays.
   - Date format
   - Time format
   - Date and time fields

4. Select the formats for these time-related displays by using the drop-down arrow.
   - Duration fields
   - Time zone

   Note: You must choose your time zone to get local time.

5. If you want to reset the time-related displays to default settings, click **Reset for Time**. (The bottom **Reset** button resets all the tabbed pages to default settings.)

6. Click **Apply** to save settings.

**Setting Directory Preferences**

Use the User Preferences feature to set the Export, Upload and Download directory paths for your system. These paths define where xDR’s, dictionary files and other elements are stored.

Follow these steps to set the directory preferences.
1. Click **User Preferences** on the Application board. The User Preferences page is displayed.

2. Click the **Directory** tab. The Directory page is displayed. The red asterisk denotes a required field.

   ![Figure 2: Directory Page](image)

   - Type in the following:
     - Export directory
     - Upload directory
     - Download directory

   4. If you want to reset the directories to default settings, click **Reset for Directory**. (The bottom **Reset** button resets all the tabbed pages to default settings.)

   5. Click **Apply** to save your settings.

### Setting Mapping Preferences

You can set the Mapping settings using the User Preferences feature. Follow these steps to set Mapping preferences.

1. Click **User Preferences** in the Application board. The User Preferences page is displayed.

2. Click the **Mapping** tab. The Mapping page is displayed.
3. Check **Translate ENUM values** to display text instead of numerals. Enumeration is used by xDRs to display text values instead of numeric. (For example, rather than showing the numeral for Alarm Severity, the user interface will show the actual word, such as “Major” or “Critical.”)

4. Check **Point Code to Node Name** to display the custom (user-defined) name of the node. Otherwise, the Point Code value is displayed.

5. Check **Link Short Name to Long Name** to display the custom (user-defined) link name or the Eagle link name. Otherwise, the short name is displayed, which is the name that begins with an asterisk (*).

6. To reset the Mapping values to the default, click **Reset for Enumeration**. (The bottom **Reset** button resets all the tabbed pages to default settings.)

7. Click **Apply** to save the changes.

**Setting Point Code Preferences**

The User Preferences feature enables you to set the Point Code preferences for your system. A Point Code is a unique address for a node (Signaling Point), used to identify the destination of a message signal unit (MSU).

Follow these steps to set the Point Code preferences.

1. Click **User Preferences** in the Application board. The User Preferences page is displayed.

2. Click the **Point Code** tab. The Point Code page is displayed. The red asterisk denotes a required field.
3. Select either **Hexadecimal display** or **Decimal display**.

4. Select or de-select **Split format**.
   If **Split format** is checked, the Bit groups settings in the box below are active. If **Split format** is not checked, Bit groups settings are not applicable.

5. If you selected Split format above, go to the next step. If you did not select Split format, go to step **Step 8**.

6. In the Bit groups panel, use the drop-down box to select the **Separation** type.

7. Type in values for **Groups 0-3**.

8. To reset the point code preferences to default settings, click **Reset for Point code**. (The bottom **Reset** button resets all the tabbed pages to default settings.)

9. Click **Apply** to save your settings.

### Setting CIC Preferences

The Circuit Identification Code (CIC) provides a way to identify which circuit is used by the Message Signaling Unit (MSU). This is important in ProTrace applications. Use the User Preferences feature to set the CIC settings for your system.

Complete these steps to set the CIC preferences:

1. Click **User Preferences** in the Application board.
   The User preferences page is displayed.

2. Click the CIC tab.
   The CIC page is displayed. The red asterisk denotes a required field.
3. Select either **Hexadecimal display** or **Decimal display**.
4. Select or de-select **Split format**.
   If **Split format** is checked, the Bit groups settings in the box below are active. If **Split format** is not checked, Bit groups settings are not applicable.
5. If you selected Split format above, go to the next step. If you did not select Split format, go to step **Step 8**.
6. In the Bit groups panel, use the drop-down box to select **Separation** type.
7. Type in values for **Group 0** and **Group 1**.
8. If you want to reset CIC preferences to the default, click **Reset for CIC**. (The bottom Reset button resets all the tabbed pages to default settings.)
9. Click **Apply** to save your settings.

### Setting Alarms Preferences

Use the Alarms tab in User Preferences to define the default colors that indicate alarm severity. The colors are displayed in the Perceived Severity column of alarms tables and on object icons in maps.

Follow these steps to modify alarm status colors.

1. Click **User Preferences** in the Application board.
   The User preferences page is displayed.
2. Click the **Alarms** tab.
   The Alarms page is displayed. The red asterisk denotes a required field.
3. Click the color palette (icon on the right side of the screen) associated with the alarm status color(s) you want to modify.
   A pop-up palette window is displayed.
4. Click the color you want for the type of alarm.
   The color palette pop-up is closed and the color box for the alarm displays the selected color. The number for the color is also displayed.
5. If you want to reset the Alarm preferences to the default, click Reset for Alarmlist. (The bottom Reset button resets all the tabbed pages to default settings.)
6. Click Apply.
   The changes do not take effect until you log out of and in again to NSP.

Setting Default Object Privacy

All NSP users can set default access privileges for Objects (data) they create in NSP applications. An owner has full rights to modify or delete the object. Other users are assigned to a Profile and have access to these Objects through that Profile’s associated Privacy Roles.

To enter the default Object Privacy (data) settings, follow these steps:

1. Click User preferences in the Application board menu.
   The User Preferences window is displayed. The Time tab is active by default.
2. Click the Privacy tab.
   The Privacy page is displayed.
3. Click the appropriate box to select Read, Write, or eXecute. If you want the role to have no access to the selected object(s), ensure that no box is checked.

4. Click Save as default.

5. To reset all the tabbed pages to default settings, click Reset.

6. Click Apply.
   The settings are saved.

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- USA and Canada

  Phone:
  1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)
1-919-460-2150 (outside continental USA and Canada)

TAC Regional Support Office Hours:
8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

• Caribbean and Latin America (CALA)
  Phone:
  USA access code +1-800-658-5454, then 1-888-FOR-TKLC or 1-888-367-8552 (toll-free)

TAC Regional Support Office Hours (except Brazil):
10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

• Argentina
  Phone:
  0-800-555-5246 (toll-free)

• Brazil
  Phone:
  0-800-891-4341 (toll-free)

TAC Regional Support Office Hours:
8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

• Chile
  Phone:
  1230-020-555-5468

• Colombia
  Phone:
  01-800-912-0537

• Dominican Republic
  Phone:
  1-888-367-8552

• Mexico
  Phone:
  001-888-367-8552

• Peru
  Phone:
  0800-53-087

• Puerto Rico
  Phone:
  1-888-367-8552 (1-888-FOR-TKLC)

• Venezuela
Phone:
0800-176-6497

- **Europe, Middle East, and Africa**
  
  **Regional Office Hours:**
  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

- **Signaling**
  **Phone:**
  +44 1784 467 804 (within UK)

- **Software Solutions**
  **Phone:**
  +33 3 89 33 54 00

- **Asia**

  - **India**
    **Phone:**
    +91 124 436 8552 or +91 124 436 8553

    **TAC Regional Support Office Hours:**
    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

  - **Singapore**
    **Phone:**
    +65 6796 2288

    **TAC Regional Support Office Hours:**
    9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

---

**DIH Documentation Library**

DIH customer documentation and online help are created whenever significant changes are made that affect system operation or configuration. Revised editions of the documentation and online help are distributed and installed on the customer system. Consult your NSP Installation Manual for details on how to update user documentation. Additionally, a Release Notice is distributed on the Tekelec Customer Support site along with each new release of software. A Release Notice lists the PRs that have been resolved in the current release and the PRs that are known to exist in the current release.

Listed is the entire DIH documentation library of online help.

- Centralized Configuration Manager Administration Online Help
- Alarm Forwarding Administration Online Help
Locate Product Documentation on the Customer Support Site

Access to Tekelec’s Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the Tekelec Customer Support site.
   
   Note: If you have not registered for this new site, click the Register Here link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the Product Support tab.

3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.

4. Click a subject folder to browse through a list of related files.

5. To download a file to your location, right-click the file name and select Save Target As.

Diameter Intelligent Hub (DIH) - Copyright, Notice, Trademarks, and Patents

© 2012 Tekelec
All Rights Reserved
Printed in U.S.A.

Notice

Information in this documentation is subject to change without notice. Unauthorized use, copying, or translation of this documentation can result in civil or criminal penalties.

Any export of Tekelec products is subject to the export controls of the United States and the other countries where Tekelec has operations.

No part of this documentation may be reproduced, translated, or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of an authorized representative of Tekelec.

Other product names used herein are for identification purposes only, and may be trademarks of their respective companies.
RoHS 5/6 - As of July 1, 2006, all products that comprise new installations shipped to European Union member countries will comply with the EU Directive 2002/95/EC "RoHS" (Restriction of Hazardous Substances). The exemption for lead-based solder described in the Annex will be exercised. RoHS 5/6 compliant components will have unique part numbers as reflected in the associated hardware and installation manuals.

WEEE - All products shipped to European Union member countries comply with the EU Directive 2002/96/EC, Waste Electronic and Electrical Equipment. All components that are WEEE compliant will be appropriately marked. For more information regarding Tekelec’s WEEE program, contact your sales representative.

Trademarks

TEKELEC, EAGLE, G-Flex, G-Port, and CAMIANT are registered trademarks of Tekelec. The Tekelec logo, A-Port, EAGLE 5, EAGLE 5 ISS, IP7, IP7 Secure Gateway, V-Flex, ngHLR, BLUESLICE, and Subscriber Data Server (SDS) are trademarks of Tekelec. All other trademarks are the property of their respective owners.

Patents

This product may be covered by one or more of the following U.S. and foreign patents:

U.S. Patent Numbers:
6,456,845; 6,765,990; 6,968,048; 7,043,001; 7,155,512; 7,206,394; 7,215,748; 7,231,024; 7,286,516; 7,286,647; 7,401,360; 7,706,343; 7,844,033; 7,860,799;

Foreign Patent Numbers:
None.
Chapter 2

Introduction to NSP Alarm Forwarding

Topics:
- *Alarm Forwarding Key Features*.....20
- *Alarm Forwarding Architecture*.....20
Alarm Forwarding Key Features

Alarm Forwarding is part of Tekelec’s Network Software Platform (NSP) toolkit. Key features include:

- A Simple Network Management Protocol (SNMP) agent compliant with ITU x721, X733
- A Dedicated Access Module for HP TeMIP
- Trap sent reliability
  - Sequence number is added to trap sent.
  - Telecommunications Management Network (TMN) can check that none were lost.
  - Re-synchronization is available.
- Acknowledge / Terminate capability from SNMP
  - Two alarm attributes are writable:
    - Perceived Severity: Setting the value to 5 (clear) terminates the alarm in the NSP database.
    - Acknowledged: Setting the value to 1 acknowledges the alarm in the NSP database.
  - Terminate or Acknowledge action is associated with a user ID in the NSP database.
- For an alarm event, only one email is sent to a selective list of email addresses. Alarm Forwarding allows a list of email addresses to be attached to a filter. It is possible to send a particular type of alarm to a list of email addresses and another type of alarm to a different list of email addresses. These multiple email addresses are set when Creating a Filter and Editing a Filter.

Each alarm is evaluated against each filter. The same alarm can pass different filter conditions and be sent to different destinations. If the same alarm passes different filters and is forwarded using SNMP in each of those filters, the alarm is sent only once since Alarm Forwarding detects this condition and SNMP has only one destination.

Also see NSP Forwarding MIB.

Alarm Forwarding Architecture

Alarm Forwarding supports the forwarding of alarms to applications in an external system. It supports the following two protocols for alarm forwarding:

- Traps (SNMP)
- Mails (SMTP)

Alarm Forwarding supports the use of Filters. You can create, edit, and delete a Filter and select a forwarding destination. A Filter List provides the following information for a Filter:

- Rec No - record number; a number given for indexing alarms in the Filter alarm list
- Filter ID - unique system-generated number that identifies the Filter
- Filter Name - name of the Filter
- Destination Name - destination of the filtered alarm. It can be SNMP or SMTP or both.

You can set the forwarding criteria based on the Filters defined for the following fields:
• Ack State
• Alarm Cleared User
• Alarm ID
• Alarm Type
• Managed Object Class
• Managed Object ID
• Perceived Severity ID
• Probable Cause
• Specific Problem
• User Name

Note: Destination configuration is part of platform configuration. These steps (SMTP server, SNMP version, and target IP) are described in NSP installation.
Chapter 3

Working in Alarm Forwarding

Topics:

- Accessing Alarm Forwarding.....23
- Understanding Alarm Forwarding Components.....23
- Using Alarm Forwarding.....24
- Alarm Forwarding Test Connection.....26
Accessing Alarm Forwarding

To open Alarm Forwarding, follow these steps:

**Note:** NSP only supports versions of IE 7.0 or later and Firefox 3.6 or later. Before using NSP, turn off the browser pop up blocker for the NSP site.

1. Log in to NSP.
   The NSP Application board is displayed.
2. Click **Alarm Forwarding**.
   The Alarm Forwarding home page is displayed.

Understanding Alarm Forwarding Components

The figure below shows the Alarm Forwarding page with the toolbar and Filters list. Toolbar icons are explained in the table below the figure.

![Alarm Forwarding Page](image)

**Figure 8: Alarm Forwarding Page**

**Alarm Forwarding Toolbar**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Navigation arrow -- moves back and forth among the records. This example is the arrow to move to next page.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Filter -- adds a Filter, defining the types of alarms to be forwarded and their destination</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Column Select Record -- sets the order of the columns</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Edit Filter -- edits an existing filter’s definition</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Delete Filter -- deletes a selected filter</td>
</tr>
</tbody>
</table>
Using Alarm Forwarding

This section explains how to set conditions and destinations for forwarding alarms.

Creating a Filter

Filters define the types of alarms to be forwarded and their destination. Filters return True or False results depending upon whether the alarm should be forwarded or not. Each Filter that returns True is forwarded to its specified destination.

To create a Filter,

1. Click the Add Filter icon on the toolbar.
   The Create new Filter dialog is displayed.

2. Type in a Filter Name and Description.
3. Type in Description.
4. Select Filter and (Add).
5. Select a Field, Operator, and Value from the drop-down menus.

Note: Do not use the Function Keys (F1 through F12) when using NSP. Function keys work in unexpected ways. For example, the F1 key does not open NSP help but opens the help for the browser in use. The F5 key does not refresh a specific screen, but refreshes the entire session and results in a loss of any entered information.
Figure 10: Filter Configuration Display

6. Enter an Expression.
7. Select to advance to the Destination display.
8. Select SNMP and/or SMTP.
9. Enter Email list (addresses) information.
10. To advance to the Filter Creation Dialog Summary display, select Next.

Figure 11: Summary Dialog Display

11. If this information on the Summary display is correct, select finish create this filter. If there are errors in this summary information, select the previous to return to the display to correct the errors.
12. To add another filter, repeat from Step 1.

Editing a Filter

To edit an existing Filter:

1. Select a Filter from the Filter table.
2. Click the Edit Filter icon on the toolbar.
   The Filter Creation Dialog is displayed.
3. Modify the appropriate field(s) as needed.
For specific information on fields and options, see *Creating a Filter*.

4. Click **Next**. The Select Forwarding Destination dialog is displayed.

5. Update Destination information as necessary.

   **Note:** For SNMP, only one trap destination can be defined. For SMTP, multiple email destinations are permitted.

6. Click **Finish** to save the record changes.

**Alarm Forwarding Test Connection**

This section provides additional information referenced from the

*Connection Test Dialog*

screen when using the **Test Connection** GUI icon.

**Test Connection for SMTP**

The configurator should verify the SMTP address, SMTP availability thru firewalls, and SMTP access mode. Secured destinations require additional parameters be defined and are described in the Installation Document.

1. If the message was received in the targeted mail box, the test was successful. This procedure is complete.
   
   If the message is not in the targeted mail box, continue with this procedure.

2. Use the **Audit Viewer** application to verify if a mail sending error is logged.

3. Contact the Tekelec **Customer Care Center** to investigate and help determine the correct SMTP configuration.

**Test Connection for SNMP**

The configurator should check the JMX agent log on the NSP primary to identify any SNMP agent configuration errors, verify the SNMP address, and the SNMP availability thru firewalls. Secured destinations require additional parameters be defined and are described in the Installation Document.

1. Verify the test trap was received by the management system. If the test trap was received by the management system, the test was successful. This procedure is complete.
   
   If the test trap was not received by the management system, continue with this procedure.

2. Contact the Tekelec **Customer Care Center** to investigate and help determine the correct SNMP configuration.
Chapter 4

SNMP Agent

Topics:

- SNMP Overview......28
- NSP Forwarding MIB.....28
SNMP Overview

The main features of the Simple Network Management Protocol (SNMP) agent of Network Software Platform (NSP) Forwarding are explained below.

Overview of NSP Database

- The Management Information Base (MIB) contains Managed Object types, Managed Objects, and opened alarms in specific tables.
- The MIB is loaded at SNMP agent startup with metadata and opened alarms already forwarded.

Validation of Traps Sent

- Traps contain a sequence number (since agent startup) that permits Telecommunications Management Network (TMN) to check that none were lost.
- In case of a gap (lost trap) or if the number is lower, the process is restarted and TNM can re-synchronize its database by querying the opened alarms table.

Acknowledgement or Termination from SNMP

- Change in an alarm’s writable attributes is reflected in ProAlarm Viewer and System Alarms.
  - Setting the NspAlarmAcknowledged attribute of an alarm table entry to True (1) acknowledges that alarm.
  - Setting the NspAlarmPerceivedSeverity attribute of an alarm table entry to Cleared (5) terminates an alarm.

A dedicated Access Module for HP TeMIP is available to integrate easily with the NSP Forwarding SNMP agent.

NSP Forwarding MIB

Shown here is the NSP-Forwarding-MIB, which is located on the NSP server at

```
usr/TKLC/nsp/nsp-package/forwarding/target/misc/NSP-FORWARDING-MIB
```

| -- File Name     | NSP-FORWARDING-MIB          |
| -- Date          | Mon Nov 21 10:18:28 CET 2006 |
| -- Author        | AdventNet Agent Toolkit Java Edition - MIB Editor 6 |

```
NSP-FORWARDING-MIB DEFINITIONS ::= BEGIN
  IMPORTS
    RowStatus, DisplayString
    FROM SNMPv2-TC
    NOTIFICATION-GROUP, OBJECT-GROUP
    FROM SNMPv2-CONF
    enterprises, MODULE-IDENTITY, OBJECT-TYPE, Integer32,
    NOTIFICATION-TYPE
    FROM SNMPv2-SMI;
```

A dedicated Access Module for HP TeMIP is available to integrate easily with the NSP Forwarding SNMP agent.
steleus MODULE-IDENTITY
LAST-UPDATED "200602131148Z"
ORGANIZATION "Tekelec"
CONTACT-INFO "ttprocessing@tekelec.com"
DESCRIPTION "Description"
REVISION "200602131148Z"
DESCRIPTION "NSP module"
::= { enterprises 4404 }

nsp OBJECT IDENTIFIER
::= { steleus 8 }

forwarding OBJECT IDENTIFIER
::= { nsp 6 }

nspManagedObjectClassTable OBJECT-TYPE
SYNTAX SEQUENCE OF NspManagedObjectClassEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "NSP managed object class table"
::= { forwarding 1 }

NspManagedObjectClassEntry OBJECT-TYPE
SYNTAX NspManagedObjectClassEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "NSP managed object class entry"
INDEX { nsManagedDeobjectClassId }
::= { nspManagedObjectClassTable 1 }

nsManagedObjectClassId OBJECT-TYPE
SYNTAX Integer32 ( -2147483648 .. 2147483647 )
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Value that defines an instance of managed
object class in the table"
::= { nspManagedObjectClassEntry 1 }

nsManagedObjectClassName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION "NSP managed object class instance name"
::= { nspManagedObjectClassEntry 2 }

nsManagedObjectClassDescription OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION "NSP managed object class instance
description"
::= { nspManagedObjectClassEntry 3 }
nspManagedObjectClassRowStatus  OBJECT-TYPE
SYNTAX                  RowStatus { active ( 1 ), notInService ( 2 ), notReady ( 3 ), createAndGo ( 4 ), createAndWait ( 5 ), destroy ( 6 ) }  
MAX-ACCESS              read-create  
STATUS                  current  
DESCRIPTION             "SMI v2 required attribute"  
::=  {  nspManagedObjectClassEntry  50  }  

nspManagedObjectTable   OBJECT-TYPE
SYNTAX          SEQUENCE  OF  NspManagedObjectEntry  
MAX-ACCESS      not-accessible  
STATUS          current  
DESCRIPTION     "Description"  
::=  { forwarding  2 }  

nspManagedObjectEntry   OBJECT-TYPE
SYNTAX          NspManagedObjectEntry  
MAX-ACCESS      not-accessible  
STATUS          current  
DESCRIPTION     "Row Description"  
INDEX           {  nspManagedObjectId}  
::=  { nspManagedObjectTable 1 }  

NspManagedObjectEntry  ::=  SEQUENCE {  
  nspManagedObjectId  Integer32,  
  nspManagedObjectName  DisplayString,  
  nspManagedObjectClassIdRef  Integer32,  
  nspManagedObjectParent  Integer32,  
  nspManagedObjectRowStatus  RowStatus  
}  

nspManagedObjectId      OBJECT-TYPE
SYNTAX                  Integer32  ( -2147483648 .. 2147483647  )  
MAX-ACCESS              read-only  
STATUS                  current  
DESCRIPTION             "Value that defines an instance of managed object in the table"  
::=  { nspManagedObjectEntry  1 }  

nspManagedObjectName    OBJECT-TYPE
SYNTAX                  DisplayString  
MAX-ACCESS              read-only  
STATUS                  current  
DESCRIPTION             "Column Description"  
::=  { nspManagedObjectEntry  2 }  

nspManagedObjectClassIdRef      OBJECT-TYPE
SYNTAX                  Integer32  ( -2147483648 .. 2147483647  )  
MAX-ACCESS              read-only  
STATUS                  current  
DESCRIPTION             "Value that defines an instance of managed object class"  
::=  { nspManagedObjectEntry  10 }
nspManagedObjectParent OBJECT-TYPE
SYNTAX           Integer32
MAX-ACCESS       read-only
STATUS           current
DESCRIPTION      "Value that defines an instance of parent managed object"
::=  { nspManagedObjectEntry 20 }

nspManagedObjectRowStatus OBJECT-TYPE
SYNTAX           RowStatus
MAX-ACCESS       read-create
STATUS           current
DESCRIPTION      "SMI v2 required attribute"
::=  { nspManagedObjectEntry 50 }

nspAlarmsTable OBJECT-TYPE
SYNTAX         SEQUENCE OF NspAlarmsEntry
MAX-ACCESS     not-accessible
STATUS         current
DESCRIPTION    "NSP forwarded opened alarms table"
::=  { forwarding 3 }

NspAlarmsEntry OBJECT-TYPE
SYNTAX         NspAlarmsEntry
MAX-ACCESS     not-accessible
STATUS         current
DESCRIPTION    "NSP forwarded opened alarms entry"
INDEX          { nspAlarmId }
::=  { nspAlarmsTable 1 }

NspAlarmsEntry ::= SEQUENCE {
  nspManagedObjectIdRef       Integer32,
  nspAlarmId                  Integer32,
  nspManagedObjectDN          DisplayString,
  nspAlarmRowStatus           RowStatus,
  nspAlarmEventType           INTEGER,
  nspAlarmProbableCause       INTEGER,
  nspAlarmPerceivedSeverity   INTEGER,
  nspAlarmTrendIndication     INTEGER,
  nspAlarmThresholdLevel      DisplayString,
  nspAlarmObservedValue       DisplayString,
  nspAlarmAdditionalText      DisplayString,
  nspAlarmSpecificProblem     DisplayString,
  nspAlarmFirstDate           OCTET STRING,
  nspAlarmClearDate           OCTET STRING,
  nspAlarmCriticalCount       Integer32,
  nspAlarmMajorCount          Integer32,
  nspAlarmMinorCount          Integer32,
  nspAlarmWarningCount        Integer32,
  nspAlarmAcknowledged        INTEGER
}

nspManagedObjectIdRef OBJECT-TYPE
SYNTAX           Integer32  (-2147483648 .. 2147483647 )
MAX-ACCESS       read-only
STATUS           current
DESCRIPTION      "Value that refers to managed object involved in the forwarded alarm"
::=  { nspAlarmsEntry 1 }
nspAlarmId  OBJECT-TYPE
SYNTAX      Integer32  (-2147483648 .. 2147483647 )
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "Value that defines an instance of forwarded alarm"
::=  { nspAlarmsEntry  2  }

nspAlarmRowStatus OBJECT-TYPE
SYNTAX      RowStatus  { active ( 1 ) , notInService ( 2 ) , notReady ( 3 ) , createAndGo ( 4 ) , createAndWait ( 5 ) , destroy ( 6 ) }
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION "SMI v2 required attribute"
::=  { nspAlarmsEntry  50  }

nspManagedObjectDN OBJECT-TYPE
SYNTAX      DisplayString
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "Distinguished name that refers to managed object involved in the forwarded alarm"
::=  { nspAlarmsEntry  100  }

nspAlarmLastEventTime OBJECT-TYPE
SYNTAX      DisplayString
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "Last event time in ASN.1 format for the last event of the NSP forwarded alarm on the managed object"
::=  { nspAlarmsEntry  1000  }

nspAlarmProbableCause OBJECT-TYPE
SYNTAX      INTEGER  { adapterError ( 1 ) , applicationSubsystemFailure ( 2 ) , bandwidthReduced ( 3 ) , callEstablishmentError ( 4 ) , communicationsProtocolError ( 5 ) , communicationsSubsystemFailure ( 6 ) , configurationOrCustomizationError ( 7 ) , congestion ( 8 ) , corruptData ( 9 ) , cpuCyclesLimitExceeded ( 10 ) , dataSetOrModemError ( 11 ) , degradedSignal ( 12 ) , dteDceInterfaceError ( 13 ) , enclosureDoorOpen ( 14 ) , equipmentMalfunction ( 15 ) , excessiveVibration ( 16 ) , fileError ( 17 ) , fireDetected ( 18 ) , floodDetected ( 19 ) , framingError ( 20 ) , heatingVentCoolingSystemProblem ( 21 ) , humidityUnacceptable ( 22 ) , inputOutputDeviceError ( 23 ) , inputDeviceError ( 24 ) , lanError ( 25 ) , leakDetected ( 26 ) , localNodeTransmissionError ( 27 ) , lossOfFrame ( 28 ) , lossOfSignal ( 29 ) , materialSupplyExhausted ( 30 ) , multiplexerProblem ( 31 ) , outOfMemory ( 32 ) , outputDeviceError ( 33 ) , performanceDegraded ( 34 ) , powerProblem ( 35 ) , pressureUnacceptable ( 36 ) , processorProblem ( 37 ) , pumpFailure ( 38 ) , queueSizeExceeded ( 39 ) , receiveFailure ( 40 ) , receiverFailure ( 41 ) , remoteNodeTransmissionError ( 42 ) , resourceAtOrNearingCapacity ( 43 ) , responseTimeExcessive ( 44 ) , retransmissionRateExcessive ( 45 ) , softwareError ( 46 ) , softwareProgramAbnormallyTerminated ( 47 ) , softwareProgramError ( 48 ) , storageCapacityProblem ( 49 ) , temperatureUnacceptable ( 50 ) , thresholdCrossed ( 51 ) , timingProblem ( 52 ) , toxicLeakDetected ( 53 ) , transmitFailure ( 54 ) ,...
transmitterFailure (55), underlyingResourceUnavailable (56), versionMismatch (57), authenticationFailure (58), breachOfConfidentiality (59), cableTamper (60), delayedInformation (61), denialOfService (62), duplicateInformation (63), informationMissing (64), informationModificationDetected (65), informationOutOfSequence (66), intrusionDetection (67), keyExpired (68), nonRepudiationFailure (69), outOfHoursActivity (70), outOfService (71), proceduralError (72), unauthorizedAccessAttempt (73), unexpectedInformation (74)

MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the probable cause values for the alarms as per [X.721], [X.733] and [X.736] for the NSP forwarded alarm on the managed object"

::= { nspAlarmsEntry 1001 }

nspAlarmPerceivedSeverity OBJECT-TYPE SYNNTAX INTEGER { indeterminate (0), critical (1), major (2), minor (3), warning (4), cleared (5) }
MAX-ACCESS read-write
STATUS current
DESCRIPTION "Represents the perceived severity values for the alarms as per [X.733] and [X.721] for the NSP forwarded alarm on the managed object"

::= { nspAlarmsEntry 1002 }

nspAlarmTrendIndication OBJECT-TYPE SYNNTAX INTEGER { lessSevere (0), noChange (1), moreSevere (2) }
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the trend indication values for the alarms as per [X.733] for the NSP forwarded alarm on the managed object"

::= { nspAlarmsEntry 1003 }

nspAlarmThresholdLevel OBJECT-TYPE SYNNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the threshold level indication values (real) for the alarms as per [X.733] for the last event of the NSP forwarded alarm on the managed object"

::= { nspAlarmsEntry 1004 }

nspAlarmObservedValue OBJECT-TYPE SYNrax DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the threshold observed values (real) for the alarms as per [X.733] for the last event of the NSP forwarded alarm on the managed object"
 ::= { nspAlarmsEntry 1005 }

nspAlarmAdditionalText OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the additional text field for the alarm as per [X.733] for the last event of the NSP forwarded alarm on the managed object"
 ::= { nspAlarmsEntry 1006 }

nspAlarmEventType OBJECT-TYPE
SYNTAX INTEGER { otherAlarm (1), communicationAlarm (2), environmentalAlarm (3), equipmentAlarm (4), integrityViolation (5), processingErrorAlarm (10), qualityOfServiceAlarm (11) }
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the ITU event type value for the alarms as per [X.721], [X.733] and [X.736] for the NSP forwarded alarm on the managed object"
 ::= { nspAlarmsEntry 1007 }

nspAlarmSpecificProblem OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the specific problem name for the NSP forwarded alarm on the managed object"
 ::= { nspAlarmsEntry 1008 }

nspAlarmFirstDate OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the raised date in ASN.1 format for the NSP forwarded alarm on the managed object"
 ::= { nspAlarmsEntry 1010 }

nspAlarmClearDate OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the clear date in ASN.1 format for the NSP forwarded alarm on the managed object"
 ::= { nspAlarmsEntry 1011 }
nsAlarmCriticalCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the number of critical events for the NSP forwarded alarm on the managed object"
::= { nspAlarmsEntry 1012 }

nsAlarmMajorCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the number of major events for the NSP forwarded alarm on the managed object"
::= { nspAlarmsEntry 1013 }

nsAlarmMinorCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the number of minor events for the NSP forwarded alarm on the managed object"
::= { nspAlarmsEntry 1014 }

nsAlarmWarningCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Represents the number of warning events for the NSP forwarded alarm on the managed object"
::= { nspAlarmsEntry 1015 }

nsAlarmAcknowledged OBJECT-TYPE
SYNTAX INTEGER { false ( 0 ), true ( 1 ) }
MAX-ACCESS read-write
STATUS current
DESCRIPTION "Represents the acknowledged status for the NSP forwarded alarm of the managed object"
::= { nspAlarmsEntry 1016 }

fwdVersion OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Current version of the NSP Forwarding SNMP sub-agent"
::= { forwarding 10 }

fwdStatus OBJECT-TYPE
SYNTAX INTEGER { allGood (0), failure (1) }
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Global state of the NSP Forwarding SNMP sub-agent"
::= { forwarding 11 }

ituAlarmEvent OBJECT IDENTIFIER ::= { forwarding 733 }
otherAlarm NOTIFICATION-TYPE
OBJECTS { nspAlarmId, nspManagedObjectId, nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity, nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue, nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate, nspAlarmClearDate, nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmWarningCount, nspAlarmAcknowledged, nspManagedObjectName, nspManagedObjectDN }
STATUS current
DESCRIPTION "Represents the event type for other alarms as per [X.721],[X.733] and [X.736]"
::= { ituAlarmEvent 1 }

communicationAlarm NOTIFICATION-TYPE
OBJECTS { nspAlarmId, nspManagedObjectId, nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity, nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue, nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate, nspAlarmClearDate, nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmWarningCount, nspAlarmAcknowledged, nspManagedObjectName, nspManagedObjectDN }
STATUS current
DESCRIPTION "Represents the event type for the communication alarms as per [X.721],[X.733] and [X.736]"
::= { ituAlarmEvent 2 }

environmentalAlarm NOTIFICATION-TYPE
OBJECTS { nspAlarmId, nspManagedObjectId, nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity, nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue, nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate, nspAlarmClearDate, nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmWarningCount, nspAlarmAcknowledged, nspManagedObjectName, nspManagedObjectDN }
STATUS current
DESCRIPTION "Represents the event type for the environment alarms as per [X.721],[X.733] and [X.736]"
::= { ituAlarmEvent 3 }
equipmentAlarm NOTIFICATION-TYPE
OBJECTS { nspAlarmId, nspManagedObjectId, nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity, nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue, nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate, nspAlarmClearDate, nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmWarningCount, nspAlarmAcknowledged, nspManagedObjectName, nspManagedObjectDN }
STATUS current
DESCRIPTION "Represents the event type for the equipment alarms as per [X.721],[X.733] and [X.736]"
::= { ituAlarmEvent 4 }
integrityViolation NOTIFICATION-TYPE
OBJECTS
  { nspAlarmId, nspManagedObjectId,
nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity,
nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue,
nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate,
nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmWarningCount,
nspAlarmAcknowledged, nspManagedObjectName, nspManagedObjectDN } 

STATUS current
DESCRIPTION "Represents the event type for the integrity
violation as per [X.721],[X.733] and [X.736]"
  ::= { ituAlarmEvent 5 } 

processingErrorAlarm NOTIFICATION-TYPE
OBJECTS
  { nspAlarmId, nspManagedObjectId,
nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity,
nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue,
nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate,
nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmWarningCount,
nspAlarmAcknowledged, nspManagedObjectName, nspManagedObjectDN } 

STATUS current
DESCRIPTION "Represents the event type for the processing
error alarms as per [X.721],[X.733] and [X.736]"
  ::= { ituAlarmEvent 10 } 

qualityOfServiceAlarm NOTIFICATION-TYPE
OBJECTS
  { nspAlarmId, nspManagedObjectId,
nspAlarmLastEventTime, nspAlarmProbableCause, nspAlarmPerceivedSeverity,
nspAlarmTrendIndication, nspAlarmThresholdLevel, nspAlarmObservedValue,
nspAlarmAdditionalText, nspAlarmSpecificProblem, nspAlarmFirstDate,
nspAlarmCriticalCount, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmWarningCount,
nspAlarmAcknowledged, nspManagedObjectName, nspManagedObjectDN } 

STATUS current
DESCRIPTION "Represents the event type for the quality
of service alarms as per [X.721],[X.733] and [X.736]"
  ::= { ituAlarmEvent 11 } 

ituAlarmEventGroup NOTIFICATION-GROUP
NOTIFICATIONS { communicationAlarm, environmentalAlarm,
equipmentAlarm, integrityViolation, otherAlarm, processingErrorAlarm,
qualityOfServiceAlarm } 

STATUS current
DESCRIPTION "ITU alarm Event notifications"
  ::= { forwarding 500 } 

managedObject OBJECT-GROUP
OBJECTS
  { nspManagedObjectClassDescription, nspManagedObjectId,
nspManagedObjectClassId, nspManagedObjectClassIdRef, nspManagedObjectClassName,
nspManagedObjectClassRowStatus, nspManagedObjectParent, nspManagedObjectIdRef,
nspManagedObjectName, nspManagedObjectRowStatus, nspManagedObject DN } 

STATUS current
DESCRIPTION "Data related to NSP managed objects"
  ::= { forwarding 200 } 

alarm OBJECT-GROUP
OBJECTS
  { nspAlarmAcknowledged, ...
nspAlarmAdditionalText, nspAlarmClearDate, nspAlarmCriticalCount, nspAlarmFirstDate, nspAlarmId, nspAlarmLastEventTime, nspAlarmMajorCount, nspAlarmMinorCount, nspAlarmObservedValue, nspAlarmPerceivedSeverity, nspAlarmProbableCause, nspAlarmEventType, nspAlarmRowStatus, nspAlarmSpecificProblem, nspAlarmThresholdLevel, nspAlarmTrendIndication, nspAlarmWarningCount

STATUS current
DESCRIPTION "Data related to NSP alarms"
::= { forwarding 300 }

forward OBJECT-GROUP
OBJECTS { fwdVersion, fwdStatus }
STATUS current
DESCRIPTION "Data related to NSP forwarding module"
::= { forwarding 100 }

END