NOKIA

Software Upgrade and Migration Application Procedures

Table of contents

List of figures

List of tables

List of procedures

1 Preface

This preface provides general information about the documentation set for the following products:

- 7302 Intelligent Services Access Manager (7302 ISAM)
- 7330 Intelligent Services Access Manager Fiber to the Node (7330 ISAM FTTN)
- 7356 Intelligent Services Access Manager Fiber to the Building (7356 ISAM FTTB)
- 7360 Intelligent Services Access Manager FX (7360 ISAM FX)
- 7362 Intelligent Services Access Manager DF/SF (7362 ISAM DF/SF)
- 7363 Intelligent Services Access Manager MX (7363 ISAM MX)
- 7367 Intelligent Services Access Manager SX/DX (7367 ISAM SX/DX)

1.1 Scope

This documentation set provides information about safety, features and functionality, ordering, hardware installation and maintenance, CLI and TL1 commands, and software upgrade and migration procedures.

1.2 Audience

This documentation set is intended for planners, administrators, operators, and maintenance personnel involved in installing, upgrading, or maintaining the 7302 ISAM, 7330 ISAM FTTN, 7356 ISAM FTTB, 7360 ISAM FX, 7362 ISAM DF/SF, 7363 ISAM MX, or 7367 ISAM SX/DX.

1.3 Required knowledge

The reader must be familiar with general telecommunications principles.

1.4 Acronyms and initialisms

See the *ISAM Glossary* in the customer documentation package for this release for the expansion and initialisms used in this documentation set.

1.5 Safety information

For safety information, see the *Safety Manual* for your product.

1.6   Documents

Refer to the *Product Information* document for your product to see a list of all the relevant customer documents and their part numbers for the current release.

1.7   Product Naming

When the term "ISAM" is used alone, the 7302 ISAM, the 7330 ISAM FTTN, the 7356 ISAM FTTB in stand-alone mode, 7360 ISAM FX, 7362 ISAM DF/SF, 7363 ISAM MX, and the 7367 ISAM SX/DX are meant. If a feature is valid for only one or two of the products, the applicability will be explicitly stated.

1.8   Special information

The following are examples of how special information is presented in this document.

Danger — Danger indicates that the described activity or situation may result in serious personal injury or death; for example, high voltage or electric shock hazards.

Warning — Warning indicates that the described activity or situation may, or will, cause equipment damage or serious performance problems.

Caution — Caution indicates that the described activity or situation may, or will, cause service interruption.

Note — A note provides information that is, or may be, of special interest.

1.8.1   Procedures with options or substeps

When there are options in a procedure, they are identified by letters. When there are required substeps in a procedure, they are identified by roman numerals.

Procedure 1   Example of options in a procedure

At step 1, you can choose option a or b. At step 2, you must do what the step indicates.

1   This step offers two options. You must choose one of the following:

   a   This is one option.

   b   This is another option.

2   You must perform this step.

Procedure 2   Example of required substeps in a procedure

At step 1, you must perform a series of substeps within a step. At step 2, you must do what the step indicates.

1   This step has a series of substeps that you must perform to complete the step. You must perform the following substeps:

   i   This is the first substep.

   ii   This is the second substep.

   iii   This is the third substep.

2   You must perform this step.

1.9   Release notes

Be sure to refer to the release notes (such as the Customer Release Notes or Emergency Fix Release Note) issued for software loads of your product before you install or use the product. The release notes provide important information about the software load.

2 Introduction

2.1 Introduction

This document contains the automated software upgrade and migration procedures using the Software Upgrade Automation Tool (also known as PBMT) for the ISAM system software. Table 1 lists the definitions for upgrade and migration.

Table 1 **Upgrade and migration definitions**

Term	Definition
Upgrade	A system software update during which the database is not modified and remains compatible with the original release. No new database is created.
Migration	A system software update during which the database is modified and must be converted to be compatible with the new software release.

Note — As mentioned above, this document focuses on the script-driven Software Upgrade and Migration actions. When planning Software Upgrade and Migration actions, it is important not to mix these script-driven actions with manual Software Upgrade settings such as, for example, the "automatic OSWP activation after DB restore" setting.

This document also contains procedures for the following tasks:

- reconfigure an NTIO unit using the Software Upgrade Automation Tool when replacing an existing unit with a new type of unit, for example, when replacing an NCNC-C card with an NCNC-E card; see "NTP 102 Reconfigure an NTIO unit" for more information.

  Note — This procedure applies only to the 7302 ISAM and the 7330 ISAM FTTN.

- replace an NPOT-A unit with and NPOT-C unit; see "NTP 103 Replace an NPOT-A LT unit with an NPOT-C LT unit" for more information.

- downgrade the software of an NT unit; see "DLP 109 Downgrade the software on an NT unit" for more information
- download and activate software on ONTs; see "NTP 100 Upgrade the software", "NTP 101 Migrate the software", and "NTP 104 Upgrade the ONT software" for more information

The Software Upgrade Automation Tool upgrades and migrates the software for all the components of the ISAM, including the ISAM Voice components.

> **Note —** The procedures in this document use the Software Upgrade Automation Tool components delivered with the software package; see the Customer Release Notes in the software package for the version number of the Software Upgrade Automation Tool needed to upgrade or migrate your system.

There must not be any unexplained system alarms or other problems in the system before you perform the procedures in this document. Nokia recommends that you back up your current database before you perform an upgrade or migration.

If problems are encountered while you perform the procedures in this document, suspend work and contact Nokia Technical Support immediately to investigate the situation.

2.1.1   The Software Upgrade Automation Tool

The Software Upgrade Automation Tool consists of Perl-based scripts that use CLI or TL1 commands to automatically perform the software upgrade and migration-related tasks for the ISAM, including verifying the status of the system before performing an upgrade or migration. The components tools of the Software Upgrade Automation Tool are installed on and run from the following EMS server: 5520 AMS server.

- See "TNG 100 Software Upgrade Automation Tool" for general information about the Software Upgrade Automation Tool and its component tools.
- See the other TNGs for detailed information about each component tool of the Software Upgrade Automation Tool, including the tasks performed by each tool, and detailed descriptions of the parameters for each tool.

You can use CLI, TL1, or the EMS to perform software-related tasks such as verifying and managing the installed software files at any time; see the following documents for your product:

- *CLI Commands*
- *TL1 Commands and Messages*
- *Operations and Maintenance using CLI*
- *Operations and Maintenance using TL1*
- *Operations and Maintenance using the 5520 AMS*

2.1.2   Applicable releases

This guide is applicable for the ISAM from release 6.0.01 on.

To upgrade an earlier release, see the documentation for that release.

2.1.3   Supported upgrade and migration paths

This section lists the supported upgrade and migration paths for this release of the ISAM.

2.1.3.1   Supported upgrade paths

The Software Upgrade Automation Tool supports upgrades within a release (example: from 5.0 to 5.0.01 or from 5.0.01 to 5.0.01a).

Check the Customer Release Notes for the new release. It may indicate that you need to perform a migration to go from the original release to the new release.

2.1.3.2   Supported migration paths

The migration paths supported by the Software Upgrade Automation Tool for a certain release are listed in the Customer Release Note of that release. See your Customer Release Notes for more information.

To migrate from any other release to this release, contact Nokia Technical Support. To migrate to an earlier release, see the documentation for that release.

2.2   How to use this document

This document follows the task-oriented practice (TOP). The TOP method is a documentation system that uses different types of layers, or documents, to describe the installation, operations, and maintenance of telecommunications equipment and software. Most layers in the TOP system provide step-by-step instructions for the completion of a specific task or procedure.

A TOP document is structured so that experienced and less experienced users can effectively use the material to perform work assignments. Less experienced users can refer to detailed procedures to complete a task. Experienced users can bypass detailed procedures and use only the level of information that they need.

2.2.1   TOP layers

TOP documentation is constructed in layers, which provide the user with easy access to any point within the task description. This guide and other guides referenced from this guide may contain any of the following layers:

- Index List (IXL)
- Non-Trouble Procedure (NTP)
- Detailed Level Procedure (DLP)
- Routine Task Procedure (RTP)
- Trouble Analysis Procedure (TAP)
- Training (TNG)

Figure 1 shows the major paths of TOP layers that may be used in this guide.

Figure 1   **TOP layers and major paths**

```
                          ┌──────────────┐
                          │  Index List  │
                          │    (IXL)     │
                          └──────────────┘
        ┌───────────────┬──────┼──────────┬──────────────┐
        ▼               ▼      ▼           ▼              ▼
 ┌──────────────┐ ┌──────────────┐ ┌──────────────┐ ┌──────────────┐
 │ Non-Trouble  │ │ Routine Task │ │Trouble Analysis│ │   Training   │
 │  Procedure   │ │  Procedure   │ │  Procedure   │ │    (TNG)     │
 │    (NTP)     │ │    (RTP)     │ │    (TAP)     │ │              │
 └──────────────┘ └──────────────┘ └──────────────┘ └──────────────┘
        │      ▲
        ▼      │
 ┌──────────────┐
 │Detailed Level│
 │  Procedure   │
 │    (DLP)     │
 └──────────────┘
```
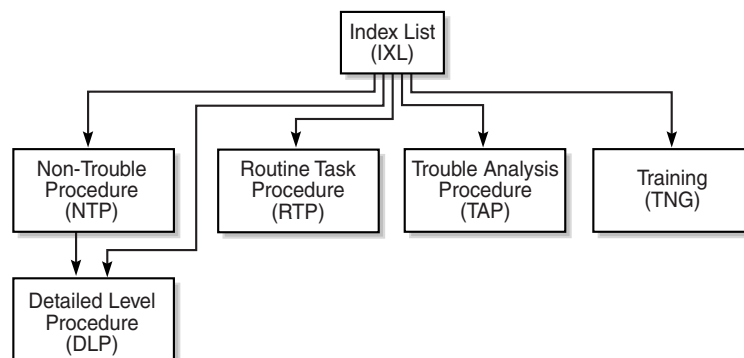
17664

2.2.1.1   Task index list (IXL)

An IXL lists the available tasks in the TOP document. An IXL is used to find a task category and the applicable procedures to perform a task.

2.2.1.2   Non-trouble procedure (NTP)

An NTP describes how to perform a task, such as how to save a system after it has been installed, turn up a system for service, or maintain a system according to a maintenance plan. NTPs are made up of steps that often refer to DLPs or TNGs. Less experienced users, or experienced users who need more information, can go to the DLPs for detailed procedural and safety information, and TNGs for supporting information. If users go to the referenced DLP or TNG, they must return to the NTP to continue the procedure.

2.2.1.3 Detailed level procedure (DLP)

A DLP contains detailed steps that describe how to perform a task. In addition to step-by-step information, a DLP contains any tables or illustrations that may be required to perform the task.

DLPs are typically referenced from an NTP, always referenced from the IXL, and sometimes referenced from other DLPs. When a DLP is referenced from another layer, users must return to the layer at which the DLP was referenced to continue the procedure.

2.2.1.4 Routine task procedure (RTP)

An RTP describes how to perform a routine maintenance task.

RTPs are typically referenced from the IXL.

2.2.1.5 Trouble analysis procedure (TAP)

A TAP describes how to identify and clear trouble in the system. TAPs are made up of step-by-step instructions. For less experienced users, or experienced users who need more information, some tasks provide a reference to a DLP or TNG. If users go to the referenced DLP or TNG, they must return to the TAP to continue the procedure.

2.2.1.6 Training (TNG)

A TNG contains supplementary information about a task or procedure. A TNG might refer to a DLP or other document. If users go to the referenced document, they need to return to the TNG to read the remaining information.

2.2.2 Step details

NTPs, DLPs, RTPs and TAPs use procedural steps and decision steps. Procedural steps provide instructions, and decision steps provide a go-to choice.

Procedural steps may contain notations that refer to additional information such as tables, figures, examples and other TOP layers. For example, a step in an NTP might refer to a DLP.

Key information required to complete a step is shown at the beginning of the step. More detailed information, which can be accessed according to experience level, is provided at the end of the step, as shown in the example below:

"Reconnect the power feeds; see DLP 106."

The completion of a specific task or procedure is indicated as follows:

"STOP. This procedure is complete."

2.2.3   Procedures with options or substeps

When there are options in a procedure, they are identified by letters. When there are required substeps in a procedure, they are identified by Roman numerals.

Procedure 3   Example of options in a procedure

At step 1, you can choose option a or b. At step 2, you must do what the step indicates.

---

1   This step offers two options. You must choose one of the following:

   a   This is one option.

   b   This is another option.

---

2   You must perform this step.

Procedure 4   Example of required substeps in a procedure

At step 1, you must perform a series of substeps within a step. At step 2, you must do what the step indicates.

---

1   This step has a series of substeps that you must perform to complete the step. You must perform the following substeps:

   i   This is the first substep.

   ii   This is the second substep.

   iii   This is the third substep.

---

2   You must perform this step.

2.3   Generic Notes

This chapter contains some general notes on the syntax in this manual.

2.3.1   Use of special characters

A customer can enter a username and password using CLI commands using the below format:

If a username or password contains any special character like #,$,& The username and password has to be given in single quotes and the entire --v3auth and --v3priv value has to be given in double quotes in the command line.

Example : if the SNMPV3 username is SUPER#USER and the authentication password is test?150 and the privacy password is alcatel#12345 then the syntax should be:

```
./precheck.pl --isam nt_ip_address --swp OSWPpath/OSWPnamexx.yyy --log
file.log --v3auth "'SUPER#USER':'test?150':md5" --v3priv
"DES:'alcatel#12345'"
```

If the username or password contains a special character and it is given into the PBMT script command line, then it should be preceded by a backslash (\) symbol As said above he can pass directly as it is configured in isam without addition of double quotes or single quotes or a backslash(\)

It is not needed to specify any double quotes or any backslash if the username or password is specified in the config.pl file.

Examples:

```
user1 --> user1
```

```
user:123 --> "'user1:123'"
```

```
'user:123' --> "\''user:123'\'"
```

Note: You need to escape a single quote since ' is reserved to handle a ':' or special characters

```
'user1' --> "\'user1\'"
```

2.3.2   Prerequisite for running PBMT

Syslog messages must be disabled before running any PBMT script as it may cause issues during parsing of the CLI response in the PBMT. This pre-condition applies to all the scripts of the PBMT.

Index List (IXL)

3 Index list

3 Index list

Tables 2 to 6 list the NTPs, DLPs, TAPs, and TNGs in this document.

Table 2   **Non-Trouble Procedures (NTPs)**

Title	NTP chapter
NTP 100 Upgrade the software	4
NTP 101 Migrate the software	5
NTP 102 Reconfigure an NTIO unit	6
NTP 103 Replace an NPOT-A LT unit with an NPOT-C LT unit	7
NTP 104 Upgrade the ONT software	8
NTP 105 Replace an NVPS-A LT unit with an NVPS-C LT unit	9

Table 3   **Detailed Level Procedures (DLPs)**

Title	DLP chapter
DLP 100 Prepare the software	10
DLP 102 Download the NE software	12
DLP 103 Upgrade the NE software	13
DLP 104 Migrate the NE software	14
DLP 105 Commit the NE software	15
DLP 106 Roll back the software	16
DLP 107 Reconfigure an NTIO unit	17
DLP 108 Replace an NPOT-A unit with an NPOT-C unit	18
DLP 109 Downgrade the software on an NT unit	19
DLP 110 Stage the ONT software	20
DLP 111 Download the ONT software	21
DLP 112 Replace an NVPS-A unit with an NVPS-C unit	22

Table 4   **Routine Task Procedures (RTPs)**

Title	NTP chapter
RTP 100 Replace an NT unit	23

Table 5   **Trouble and Analysis Procedures (TAPs)**

Title	NTP chapter
TAP 100 Verify the system status	24

Table 6   **Training (TNG)**

Title	TNG chapter
TNG 100 Software Upgrade Automation Tool	25
TNG 101 Automated software download tool	26
TNG 102 Automated software upgrade tool	27
TNG 103 Automated software migration tool	28
TNG 104 Automated software commitment tool	29
TNG 105 ONT automated tools	30
TNG 106 Additional automated tools	31
TNG 107 Network element management	32
TNG 108 Overall SoftWare Package concept	33
TNG 109 Software database processes	34
TNG 110 Descriptor files	35
TNG 111 Automated software rollback tool	36

Non-Trouble Procedures (NTP)

4 NTP 100 Upgrade the software

4.1 Purpose

Use this NTP to upgrade the software of ISAM NEs using the Software Upgrade Automation Tool.

4.2 General

An upgrade is a system software update during which the database is not modified and remains compatible with the original release. No new database is created.

Note 1 — Do not use this procedure when going from a major release to another major release (for example from Release 4.0 to Release 4.1) or if the Customer Release Notes for the new release indicates that you need to perform a migration to go from the original release to the new release. If you do, your current database will not be available to the new software package.

Note 2 — While using this procedure, ensure ONT Software files do not consume more than 800MB under /ONT in case of IHUB Boards

Table 7 lists the components of the Software Upgrade Automation Tool used to upgrade the software on one or more ISAM NEs and on the ONTs connected to these NEs; see "TNG 100 Software Upgrade Automation Tool" for more information about the Software Upgrade Automation Tool.

Table 7   **Automated tools used for software upgrade**

Name	Command	See chapter
Automated parameter configuration tool	Config.pl [3]	25
Automated system readiness verification tool [1]	preCheck.pl [3]	31
Automated system status verification tool [1]	statusCheck.pl [3]	31
Automated software minimization tool	MinimizeSWP.pl	31
Automated software download tool [1]	swdl.pl [3]	26
Automated ONT software staging tool [1]	stageont.pl	30
Automate ONT software download tool [1]	ontDownloadandActivate.pl	30
Automated software upgrade tool [1]	upgrade.pl [3]	27
Automated software commitment tool [1]	commit.pl [3]	29
Automated file clean-up tool [2]	cleanUp.pl	31
Automated system status comparison tool [1]	statusCheckCmp.pl	31
Automated software rollback tool [1]	rollback.pl	36

Notes

(1) This automated tool can be used on a single NE, or on multiple NEs using a single session or multiple parallel sessions; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information.

(2) The automated file clean-up tool can be used to clean up files for a single NE or for multiple NEs.

(3) A second password option is supported for this script, see "TNG 100 Software Upgrade Automation Tool" for more information.

These automated tools are Perl scripts installed and run from an EMS server. When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

4.2.1 Upgrading the software for NEs in a subtending configuration

In a subtending configuration, where subtended NEs are connected to the IP network via a subtending NE, Nokia recommends that you upgrade all the subtended NEs before upgrading the subtending NE. Because the subtended NEs use the subtending NE for connectivity to the network, upgrading the subtended NEs and the subtending NE at the same time can result in a communication disruption to the subtended NEs, and a failed upgrade.

4.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool", which contains very important information about the components of the Software Upgrade Automation Tool used in this procedure
- the system is operational
- all operator commands have finished running
- if you are using a customized operator profile, the defined prompt, if any, ends with a trailing space; see the following documents for your product for information about conifguring an operator profile:
  - *Operations and Maintenance Using CLI*
  - *Operations and Maintenance Using TL1*

4.4 Procedure

Use this procedure to upgrade the software using the Software Upgrade Automation Tool. See the references for detailed procedures.

---

1 Prepare the software for installation, see "DLP 100 Prepare the software".

---

2 If desired, verify the operational readiness and status of the system before the upgrade; see "TAP 100 Verify the system status".

3   If desired, verify and change the software replacement mode of the system before the upgrade. This is an optional step but it can minimize the service interruption during the upgrade; see "DLP 101 Configure software replacement mode".

> **Note —** This option is only supported on a limited set of supported system(s) and configuration(s).

4   Download the NE software; see "DLP 102 Download the NE software".

5   Download the ONT software (if applicable).

    i   Stage the ONT software; see "DLP 110 Stage the ONT software".

    ii   Download the ONT software to the ONTs without activating the ONT software; see "DLP 111 Download the ONT software".

6   Upgrade the NE software; see "DLP 103 Upgrade the NE software".

7   Activate the ONT software on the ONTs (if applicable); see "DLP 111 Download the ONT software".

8   If desired, verify the operational status of the system after the upgrade and compare the results with those of step 2; see "TAP 100 Verify the system status".

9   If needed, commit the NE software; see "DLP 105 Commit the NE software".

> **Caution —** Nokia does not recommend committing the software until you are ready to move to the next release of software. If you need to commit the software before the next release, ensure that the system is up and running, traffic has resumed, and you are satisfied with the performance of the new release before committing the software. You cannot roll back to a previous load after the software is committed. The previous load is deleted.

10   STOP. This procedure is complete.

5 NTP 101 Migrate the software

5.1 Purpose

Use this NTP to migrate the software of ISAM NEs using the Software Upgrade Automation Tool.

5.2 General

A migration is a system software update during which the database is modified and must be converted to be compatible with the new software release.

Warning — When migrating the ISAM, Nokia recommends that you use the procedures in this document. Do not use the upgrade and migration procedures documented in any other documentation, including the EMS documentation.

Failure to use the Software Upgrade Automation Tool to migrate can result in a failed upgrade or migration and can cause the system to become isolated.

Caution 1 — Before performing a migration using the automated software migration tool, ensure that each multicast source is a member of all membership packages or of no more than 20 membership packages.

- In CLI, the `packagemember` field of the `configure mcast` command must not have more then 20 entries associated with it and the `pkg-mem-bitmap` bitmap must be set so that the source belongs to no more than 20 packages.
- In TL1, the `MEMBERSHIP` field of the `ENT-MCSRC` command must not have more then 20 entries associated with it.

Caution 2 — In ISAM R5.7 and onwards, the hardcoded SSH key pair will be removed and replaced by a newly generated key-pair. When migrating from an older release where the operator is still the default, hard coded key pair, any connection with SSH clients will be refused because of discrepancy with the key in the known-hosts file at the SSH clients, for the existing ISAM IP addresses.

In order to prevent the post migration connection failure (man in the middle attack warning), the operator must renew the SSH key pair prior the start of the migration and update the known-hosts entries in the SSH client. In this case, the generated SSH key will be migrated when moving to R5.7 or higher and the connection with the SSH clients will be restored after the migration.

Note 1 — While using this procedure, ensure ONT Software files do not consume more than 800MB under /ONT in case of IHUB Boards

Note 2 — When migrating to R57 from a lower release with customer generated keys (for example. DSA-1024 bit key), migration will be successful. If required post migration, a new DSA-2048/RSA-2048 bit key can be generated through CLI/TL1/SNMP, setting it as the host key and adopting the known_hosts file in the SSH clients.

Table 8 lists the components of the Software Upgrade Automation Tool used to migrate the software on one or more ISAM NEs and upgrade the software on the ONTs connected to these NEs; see "TNG 100 Software Upgrade Automation Tool" for more information about the Software Upgrade Automation Tool.

Table 8   **Automated tools used for software migration**

Name	Command	See chapter
Automated parameter configuration tool	Config.pl [3]	25
Automated system readiness verification tool [1]	preCheck.pl [3]	31
Automated system status verification tool [1]	statusCheck.pl [3]	31
Automated software minimization tool	MinimizeSWP.pl	31
Automated software download tool [1]	swdl.pl [3]	26
Automated ONT software staging tool [1]	stageont.pl	30
Automate ONT software download tool [1]	ontDownloadandActivate.pl	30
Automated software migration tool [1]	migrate.pl [3]	28
Automated software commitment tool [1]	commit.pl [3]	29
Automated file clean-up tool [2]	cleanUp.pl	31
Automated system status comparison tool [1]	statusCheckCmp.pl	31
Automated software rollback tool [1]	rollback.pl	36

Notes

[1]   This automated tool can be used on a single NE, or on multiple NEs using a single session or multiple parallel sessions; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information.

[2]   The automated file clean-up tool can be used to clean up files for a single NE or for multiple NEs.

[3]   A second password option is supported for this script, see "TNG 100 Software Upgrade Automation Tool" for more information.

These automated tools are Perl scripts installed and run from an EMS server. When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

5.2.1 Migrating the software for NEs in a subtending configuration

In a subtending configuration, where subtended NEs are connected to the IP network via a subtending NE, Nokia recommends that you migrate all the subtended NEs before migrating the subtending NE. Because the subtended NEs use the subtending NE for connectivity to the network, migrating the subtended NEs and the subtending NE at the same time can result in a communication disruption to the subtended NEs, and a failed migration.

5.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool", which contains very important information about the components of the Software Upgrade Automation Tool used in this procedure
- the system is operational
- all operator commands have finished running
- if you are using a customized operator profile, the defined prompt, if any, ends with a trailing space; see the following documents for your product for information about configuring an operator profile:
    - *Operations and Maintenance Using CLI*
    - *Operations and Maintenance Using TL1*

5.4 Procedure

Use this procedure to migrate the software using the Software Upgrade Automation Tool. See the references for detailed procedures.

---

1 Prepare the software for installation, see "DLP 100 Prepare the software".

---

2 If desired, verify the operational readiness and status of the system before the migration; see "TAP 100 Verify the system status".

---

3 Download the NE software; see "DLP 102 Download the NE software".

---

4 Download the ONT software (if applicable).

    i Stage the ONT software; see "DLP 110 Stage the ONT software".

    ii Download the ONT software to the ONTs without activating the ONT software; see "DLP 111 Download the ONT software".

---

5 Migrate the NE software; see "DLP 104 Migrate the NE software".

6   Activate the ONT software on the ONTs (if applicable); see "DLP 111 Download the ONT software".

7   If desired, verify the operational status of the system after the migration and compare the results with those of step 2; see "TAP 100 Verify the system status".

8   If needed, commit the NE software; see "DLP 105 Commit the NE software".

> ⚠ **Caution —** Nokia does not recommend committing the software until you are ready to move to the next release of software. If you need to commit the software before the next release, ensure that the system is up and running, traffic has resumed, and you are satisfied with the performance of the new release before committing the software. You cannot roll back to a previous load after the software is committed. The previous load is deleted.

9   STOP. This procedure is complete.

6 NTP 102 Reconfigure an NTIO unit

6.1 Purpose

Use this NTP to reconfigure an ISAM NE, such as the 7302 ISAM or the 7330 ISAM FTTN, using the Software Upgrade Automation Tool when an NTIO unit is replaced by a new type of NTIO unit.

6.2 General

When replacing an NTIO unit with a new type of NTIO unit, you must reconfigure the system for the new type of NTIO unit. Table 9 lists the NTIO unit reconfigurations you can perform using the Software Upgrade Automation Tool.

Table 9   **NTIO unit reconfigurations**

From	To
NCNC-C	NCNC-E

Use this procedure only if the NTIO unit is replaced outside of a migration window, for example, when a card failure has occurred and the card is replaced by a new type.

Table 10 lists the components of the Software Upgrade Automation Tool used to reconfigure an NTIO unit; see "TNG 100 Software Upgrade Automation Tool" for more information about the Software Upgrade Automation Tool.

Table 10   **Automated tools used for NTIO unit reconfiguration**

Name	Command	See chapter
Automated system status verification tool	statusCheck.pl	31
NCNC-C to NCNC-E reconfiguration tool	cvtNcncC2E.pl	31
Automated system status comparison tool	statusCheckCmp.pl	31

These automated tools are Perl scripts installed and run from an EMS server. When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

6.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool", which contains very important information about the components of the Software Upgrade Automation Tool used in this procedure
- the system is operational

- all operator commands have finished running
- if you are using a customized operator profile, the defined prompt, if any, ends with a trailing space; see the following documents for your product for information about configuring an operator profile:
    - *Operations and Maintenance Using CLI*
    - *Operations and Maintenance Using TL1*

6.4   Procedure

Use this procedure to reconfigure a system for a new type of NTIO unit using the Software Upgrade Automation Tool. See the references for detailed procedures.

1	Prepare the software for installation, see "DLP 100 Prepare the software".

2	If desired, verify the operational status of the system before the database conversion; see "TAP 100 Verify the system status".

3	Reconfigure the system for the new type of NTIO unit; see "DLP 107 Reconfigure an NTIO unit".

4	Replace the NTIO unit by the new NTIO unit; see the documentation for your product for information about replacing a card.

5	If desired, verify the operational status of the system after the database conversion and compare the results with those of step 2; see "TAP 100 Verify the system status".

6	STOP. This procedure is complete.

7 NTP 103 Replace an NPOT-A LT unit with an NPOT-C LT unit

7.1 Purpose

Use this NTP to replace an existing NPOT-A LT unit with an NPOT-C LT unit in the ISAM system and enable a successful start-up of the NPOT-C LT unit.

7.2 General

A software upgrade or migration is required when replacing an existing NPOT-A LT unit with an NPOT-C LT unit. Depending on the LT units equipped in a shelf and the LT units being replaced, addtional steps may be required to allow the new LT unit to start-up successfully.

Table 11 lists the LT unit replacements you can perform using this NTP.

Table 11   **LT unit replacements**

From	To
NPOT-A	NPOT-C

7.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool", which contains very important information about the components of the Software Upgrade Automation Tool used in this procedure
- you have reviewed "TNG 103 Automated software migration tool", which contains very important information about the components of the Software Migration Automation Tool used in this procedure
- you have completed the steps to either upgrade software in "NTP 100 Upgrade the software" or to migrate software in "NTP 101 Migrate the software"
- the system is operational
- all operator commands have finished running
- if you are using a customized operator profile, the defined prompt, if any, ends with a trailing space; see the following documents for your product for information about configuring an operator profile:
    - *Operations and Maintenance Using CLI*
    - *Operations and Maintenance Using TL1*

7.4 Procedure

Use this procedure to replace an NPOT-A LT unit with an NPOT-C LT unit. See the references for detailed procedures.

---

1   If desired, verify the operational status of the system after the database upgrade or migration conversion; see "TAP 100 Verify the system status".

---

2   To replace an NPOT-A unit with an NPOT-C unit; see "DLP 108 Replace an NPOT-A unit with an NPOT-C unit".

---

3   STOP. This procedure is complete.

8 NTP 104 Upgrade the ONT software

8.1 Purpose

Use this NTP to upgrade the software of ISAM ONTs using the Software Upgrade Automation Tool.

8.2 General

Use this procedure to upgrade the software of the ISAM ONTs outside of an NE upgrade or migration window. If the ONT software upgrade is done at the same time as an NE software upgrade or migration, use the procedure in "NTP 100 Upgrade the software" or "NTP 101 Migrate the software".

Table 12 lists the components of the Software Upgrade Automation Tool used to upgrade the software on the ONTs connected to one or more ISAM NEs; see "TNG 100 Software Upgrade Automation Tool" for more information about the Software Upgrade Automation Tool.

Table 12   **Automated tools used for ONT software upgrade**

Name	Command	See chapter
Automated parameter configuration tool	Config.pl	25
Automated system readiness verification tool [1][3]	preCheck.pl	31
Automated system status verification tool [1]	statusCheck.pl	31
Automated ONT software staging tool [1]	stageont.pl	30
Automated ONT software download tool [1]	ontDownloadandActivate.pl	30
Automated file clean-up tool [2]	cleanUp.pl	31
Automated system status comparison tool [1]	statusCheckCmp.pl	31
Automated software rollback tool [1]	rollback.pl	36

Notes
[1] This automated tool can be used on a single NE, or on multiple NEs using a single session or multiple parallel sessions; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information.
[2] The automated file clean-up tool can be used to clean up files for a single NE or for multiple NEs.
[3] The precheck script does not perform any checks on the ONT. It checks the validity of the migrate/upgrade target path where migration/upgrade is attempted.Also other checks like presence of Migration tool SW are done.

These automated tools are Perl scripts installed and run from an EMS server. When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

8.3   Prerequisites

Before you start this procedure, ensure that:

* you have reviewed "TNG 100 Software Upgrade Automation Tool", which contains very important information about the components of the Software Upgrade Automation Tool used in this procedure
* the system is operational
* all operator commands have finished running
* if you are using a customized operator profile, the defined prompt, if any, ends with a trailing space; see the following documents for your product for information about configuring an operator profile
    * *Operations and Maintenance Using CLI*
    * *Operations and Maintenance Using TL1*

8.4   Procedure

Use this procedure to upgrade the ONT software using the Software Upgrade Automation Tool. See the references for detailed procedures.

---

1   Prepare the ONT software for installation, see "DLP 100 Prepare the software".

---

2   If desired, verify the operational readiness and status of the system before the ONT software upgrade; see "TAP 100 Verify the system status".

---

3   Stage the ONT software; see "DLP 110 Stage the ONT software".

---

4   Download and activate the ONT software; see "DLP 111 Download the ONT software".

---

5   If desired, verify the operational status of the system after the ONT software upgrade and compare the results with those of step 2; see "TAP 100 Verify the system status".

---

6   STOP. This procedure is complete.

9 NTP 105 Replace an NVPS-A LT unit with an NVPS-C LT unit

9.1 Purpose

Use this NTP to replace an existing NVPS-A LT unit with an NVPS-C LT unit in the ISAM system and enable a successful start-up of the NVPS-C LT unit.

9.2 General

A software upgrade or migration is required when replacing an existing NVPS-A LT unit with an NVPS-C LT unit. Depending on the LT units equipped in a shelf and the LT units being replaced, additional steps may be required to allow the new LT unit to start-up successfully.

Table 13 lists the LT unit replacements you can perform using this NTP.

Table 13   **LT unit replacements**

From	To
NVPS-A	NVPS-C

9.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool", which contains very important information about the components of the Software Upgrade Automation Tool used in this procedure
- you have reviewed "TNG 103 Automated software migration tool", which contains very important information about the components of the Software Migration Automation Tool used in this procedure
- you have completed the steps to either upgrade software in "NTP 100 Upgrade the software" or to migrate software in "NTP 101 Migrate the software"
- the system is operational
- all operator commands have finished running
- if you are using a customized operator profile, the defined prompt, if any, ends with a trailing space; see the following documents for your product for information about configuring an operator profile:
  - *Operations and Maintenance Using CLI*
  - *Operations and Maintenance Using TL1*

9.4 Procedure

Use this procedure to replace an NVPS-A LT unit with an NVPS-C LT unit. See the references for detailed procedures.

---

1 If desired, verify the operational status of the system after the database upgrade or migration conversion; see "TAP 100 Verify the system status".

---

2 To replace an NVPS-A unit with an NVPS-C unit; see "DLP 112 Replace an NVPS-A unit with an NVPS-C unit".

---

3 STOP. This procedure is complete.

Detailed Level Procedures (DLP)

10 DLP 100 Prepare the software

10.1 Purpose

Use this DLP to prepare the software for installation before upgrading or migrating the software on the ISAM.

10.2 General

To use the Software Upgrade Automation Tool, you must be logged in as one of the following:

- root
- member of a UNIX or LINUX group account with appropriate permissions; see step 1

10.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool", which contains very important information about the Software Upgrade Automation Tool
- you have access to an EMS TFTP server accessible by the ISAM NEs
- you have the software package containing the software for the release to which you are upgrading or migrating
- you are logged in as root to the EMS server

10.4 Procedure

Use this procedure to prepare the software for installation before using the Software Upgrade Automation Tool. You must be logged in as root to perform this procedure. All the steps are performed using UNIX or LINUX.

---

1 Create a UNIX or LINUX group account for the non-root users that will have authorization to run the Software Upgrade Automation Tool:

Note — Skip this step when the procedures in this document are done when logged in as root.

i   Create the Software Upgrade Automation Tool group account

```
groupadd autotoolgroup
```

where *autotoolgroup* is the name of the group of users authorized to use the Software Upgrade
Automation Tool; the length of the group account name cannot exceed 8 characters.

ii   For each user authorized to use the Software Upgrade Automation Tool, add the user
to the new group:

```
usermod -G autotoolgroup username
```

where
autotoolgroup is the name of the group of users authorized to use the Software Upgrade Automation
Tool
username is the name of the user being added to the group of users authorized to use the Software
Upgrade Automation Tool

2   Add the new OSWP to the EMS library; see your EMS documentation for the procedure to
add an OSWP to the EMS library.

3   If you will be using FTP or SFTP for file transfer, change the configured server location in the
OSWP; see the EMS documentation for the procedure to change the location of the server
in the OSWP.

> **Note —** SFTP is strongly recommended to be used for downloading
> Software to the ISAM since the SFTP protocol has built-in checks that
> check that the file is correctly transferred to the Network Element.

4   Copy the Software Upgrade Automation Tool package from the ISAM software package to
the directory of your choice on the EMS TFTP server and extract the components of the
Software Upgrade Automation Tool from the software package:

> **Note —** If you already have a version of the Software Upgrade
> Automation Tool installed on your EMS server, see "Installing and using
> the components of the Software Upgrade Automation Tool" in "TNG 100
> Software Upgrade Automation Tool" for information about adding a newer
> version of the tool.

i   Create a directory for the Software Upgrade Automation Tool package. This directory
can be any directory on the EMS TFTP server.

```
mkdir autotooldir
```

where *autotooldir* is the name of the directory for the Software Upgrade Automation Tool package

ii   Copy the Software Upgrade Automation Tool package from the ISAM software package
to the directory created in step 4 i:

```
cp migrateIsam.x.y.z.tgz /autotooldir/migrateIsam.x.y.z.tgz
```

where
x.y.z is the version number of the Software Upgrade Automation Tool package (for example, migrateIsam.2.1.23.tgz)
autotooldir is the name of the directory for the Software Upgrade Automation Tool package

iii   Unzip the software package that was copied in step 4 ii.

iv   Extract the Software Upgrade Automation Tool components from the Software Upgrade Automation Tool package:

```
tar -xvf migrateIsam.x.y.z.tar
```

where *x.y.z* is the version number of the Software Upgrade Automation Tool package (for example, migrateIsam.2.1.23.tgz)

---

5   Copy the NT offline migration tool software package to the EMS TFTP server:

i   Copy the NT offline migration tool software package from the ISAM software package to the directory created in step 4 i:

```
cp MLXAAAxx.yyy.tgz /autotooldir/tools/NT/MLXAAAxx.yyy.tgz
```

where
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, MLXAAA40.126.tgz)
autotooldir is the name of the directory for the Software Upgrade Automation Tool package

ii   Unzip the NT offline migration tool software package that was copied in step 5 i.

```
cd autotooldir/tools/NT

gunzip MLXAAAAxx.yyy.tgz
```

where
autotooldir is the name of the directory for the Software Upgrade Automation Tool package
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, MLXAAA40.126)

iii   Extract the NT offline migration tool from the software package:

```
tar -xvf MLXAAAxx.yyy.tar
```

where
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, MLXAAA40.126)

There will be a Solaris Sparc, Solaris X86, and LINUX executable as follows:

- MJSH for Solaris Sparc platform
- MJSH_i386 for Solaris X86 platform
- MJSH_l for LINUX platform

iv   Perform one of the following:

- If you are using PBMT on LINUX, rename the NT offline migration tool on the TFTP server:

  ```
  mv MJSH_l /autotooldir/tools/NT/MJSH_l.exe
  ```

  where *autotooldir* is the name of the directory for the Software Upgrade Automation Tool package
- If you are using PBMT on Solaris Sparc, rename the NT offline migration tool on the TFTP server:

  ```
  mv MJSH /autotooldir/tools/NT/MJSH.exe
  ```

  where *autotooldir* is the name of the directory for the Software Upgrade Automation Tool package
- If you are using PBMT on Solaris X86, go to step 6.

6   Copy the SHub offline migration tool software package to the EMS TFTP server:

Note — This step is not applicable to 7363 ISAM MX and 7367 ISAM SX/DX.

i   Copy the SHub offline migration tool software package from the ISAM software package to the TFTP server:

```
cp LanxMigTool.x.yy.tgz
/autotooldir/tools/Lanx/LanxMigTool.x.yy.tgz
```

where
x.yy is the version number of the SHub migration tool
autotooldir is the name of the directory for the Software Upgrade Automation Tool package

ii   Unzip the NT offline migration tool software package that was copied in step 6 i.

```
cd autotooldir/tools/Lanx
```

```
gunzip LanxMigTool.x.yy.tgz
```

where
autotooldir is the name of the directory for the Software Upgrade Automation Tool package
x.yy is the version number of the SHub migration tool

iii   Extract the SHub offline migration tool from the software package. The files are automatically placed in a new subdirectory.

```
tar -xvf LanxMigTool.x.yy.tar
```

where
autotooldir is the name of the directory for the Software Upgrade Automation Tool package
x.yy is the version number of the SHub migration tool

iv   Move the extracted files to the *autotooldir*/tools/Lanx directory, where *autotooldir* is the name of the directory for the Software Upgrade Automation Tool package:

```
mv subdirectory/* .
```

where *subdirectory* is the subdirectory automatically created when the files were extracted in step iii.

v   Delete the subdirectory automatically created when extracting the files in step iii:

```
rm -R subdirectory
```

where *subdirectory* is the subdirectory automatically created when the files were extracted in step iii.

---

7   If you will also be migrating an ISAM Voice system, copy the ISAM Voice offline migration tool software package to the EMS TFTP server:

> **Note —** This step is not applicable to 7363 ISAM MX and 7367 ISAM SX/DX.

i   Copy the ISAM Voice offline migration tool software package from the ISAM software package to the directory created in step 4 i:

```
cp NBTTAAxx.yyy.tgz /autotooldir/tools/IVPS/NBTTAAxx.yyy.tgz
```

where
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, NBTTAA40.126.tgz)
autotooldir is the name of the directory for the Software Upgrade Automation Tool package

ii   Unzip the ISAM Voice offline migration tool software package that was copied in step 7 i.

```
cd autotooldir/tools/IVPS
```

```
gunzip NBTTAAxx.yyy.tgz
```

where
autotooldir is the name of the directory for the Software Upgrade Automation Tool package
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, NBTTAA40.126)

iii   Extract the ISAM Voice offline migration tool from the software package:

```
tar -xvf NBTTAAxx.yyy.tar
```

where

xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, NBTTAA40.126)

There will be a Solaris Sparc, Solaris X86, and LINUX executable as follows:

- NBTW for Solaris Sparc platform
- NBTW_i386 for Solaris X86 platform
- NBTW_l for LINUX platform

iv Perform one of the following:

- If you are using PBMT on Linux, rename the ISAM Voice offline migration tool on the TFTP server:

  ```
  mv NBTW_l /autotooldir/tools/IVPS/NBTW_l.exe
  ```

  where *autotooldir* is the name of the directory for the Software Upgrade Automation Tool package
- If you are using PBMT on Solaris Sparc, rename the ISAM Voice offline migration tool on the TFTP server:

  ```
  mv NBTW /autotooldir/tools/IVPS/NBTW.exe
  ```

  where *autotooldir* is the name of the directory for the Software Upgrade Automation Tool package
- If you are using PBMT on Solaris X86, go to step 8.

v Rename the ISAM Voice database configuration tool on the TFTP server:

```
mv ivpsa_dbtool.cfg /autotooldir/tools/IVPS/dbtool.cfg
```

where*autotooldir* is the name of the directory for the Software Upgrade Automation Tool package

---

8 Copy the ONT software package to the EMS TFTP server:

Note — This step is not applicable to 7363 ISAM MX and 7367 ISAM SX/DX.

i Copy the ONT software package from the ONT software package to the directory created in step 4 i:

```
cp ONT_xx_yy_zz.tar /autotooldir/tools/ONT/ONT_xx_yy_zz.tar
```

where
xx.yy.zz is the 6-digit ONT software release number (for example, R04.00.10)
autotooldir is the name of the directory for the Software Upgrade Automation Tool package

ii Unzip the ONT software package that was copied in step 8 i.

```
cd autotooldir/tools/ONT
```

```
gunzip ONT_xx_yy_zz.tar
```

where
autotooldir is the name of the directory for the Software Upgrade Automation Tool package
xx.yy.zz is the 6-digit ONT software release number (for example, R04.00.10)

iii   Extract the ONT software files from the software package:

```
tar -xvf ONT_xx_yy_zz.tar
```

where
xx.yy.zz is the 6-digit ONT software release number (for example, R04.00.10)

---

9   Give the users of the Software Upgrade Automation Tool group account created in Step 1 access to the directories for the Software Upgrade Automation Tool.

> **Note —** Skip this step when the procedures in this document are done when logged in as root.

i   Create the temporary directory that will be used by the Software Upgrade Automation Tool:

```
mkdir /topdir/workdir
```

where
topdir is the name of the FTP, SFTP, or TFTP top directory used to store the transferred files; see "Transfer protocols and top directory" in "TNG 100 Software Upgrade Automation Tool" for more information.
workdir is the name of the working directory, as defined in the configuration file; see Table 18

ii   Create the directory that will be used for the log files of the Software Upgrade Automation Tool components:

```
mkdir logdir
```

where *logdir* is the name of the directory for the log files of the Software Upgrade Automation Tool components, relative to the TFTP root directory

iii   Change the ownership of the Software Upgrade Automation Tool directories to the Software Upgrade Automation Tool group account:

```
chown -R root:autotoolgroup /autotooldir
```

```
chown root:autotoolgroup /topdir/workdir
```

```
chown root:autotoolgroup /logdir
```

where
autotoolgroup is the name of the group of users authorized to use the Software Upgrade Automation Tool
autotooldir is the name of the directory for the Software Upgrade Automation Tool package
topdir is the name of the FTP, SFTP, or TFTP top directory used to store the transferred files; see "Transfer protocols and top directory" in "TNG 100 Software Upgrade Automation Tool" for more information.
workdir is the name of the working directory, as defined in the configuration file; see Table 18
logdir is the name of the directory for the log files of the Software Upgrade Automation Tool components

iv Give the Software Upgrade Automation Tool group account read, write, and execute access to the Software Upgrade Automation Tool directories:

```
chmod g=rwx /autotooldir
```

```
chmod g=rwx /autotooldir/tools
```

```
chmod g=rwx /autotooldir/tools/NT
```

```
chmod g=rwx /autotooldir/tools/Lanx
```

```
chmod g=rwx /autotooldir/tools/IVPS
```

```
chmod g=rwx /autotooldir/tools/ONT
```

```
chmod g=rwx /autotooldir/tools/octopus
```

```
chmod g=rwx /topdir/workdir
```

```
chmod g=rwx /logdir
```

where
autotooldir is the name of the directory for the Software Upgrade Automation Tool package
topdir is the name of the FTP, SFTP, or TFTP top directory used to store the transferred files; see
"Transfer protocols and top directory" in "TNG 100 Software Upgrade Automation Tool" for more
information.
workdir is the name of the working directory, as defined in the configuration file; see Table 18
logdir is the name of the directory for the log files of the Software Upgrade Automation Tool components

---

10 Run the automated parameter configuration tool to create the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool" for more information:

```
Config.pl
```

---

11 Verify that the OSWP is available in one of the 5520 AMS directory:

i Verify if the OSWP is present in any of the Ethernet interface directories in the following directory of the 5520 AMS TFTP server. The OSWP file is called L6GPAA*xx.yyy*.

```
tftpdir/OSWP
```

where
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, L6GPAA40.924)
tftpdir is the name of the TFTP top directory used to store the files transferred by TFTP, as defined in
the configuration file; see Table 18

ii If there is no Ethernet interface directory or if the OSWP is not present in any of the Ethernet interface directories, download the software from the EMS to an NE to create the OSWP; see the EMS documentation for information about downloading the software to an NE.

---

12 STOP. This procedure is complete.

11 DLP 101 Configure software replacement mode

11.1 Purpose

Use this DLP to review/change the software replacement mode before upgrading the software on the ISAM.

Note — This DLP is only applicable to the 7360 ISAM FX in this release.

11.2 General

For software upgrades, the system can perform a "per-LT upgrade" on supported LTs of a redundant system. For this, the "software replacement mode" concept was introduced to allow control of the upgrade behavior.

11.3 Prerequisites

Before you start this procedure, ensure that:

- you have CLI or EMS access.
- the system is a duplex system in hot-standby state.
  The software replacement mode "lt-by-lt" requires an operational duplex system. If the standby NT is not in hot-standby state, software activation will be rejected.

11.4 Procedure

Use this procedure to review/change the software replacement mode to determine the type of upgrade.

1   Run the following CLI command to show the current software replacement mode that will determine the type of software download:

```
info configure software-mngt
```

where
the software replacement mode in the output of this command can have the values as listed in the next step.

2   Run the following CLI command to specify the software replacement mode that will determine
the type of software download:

```
configure software-mngt sw-replacement-mode <mode>
```

where:

the software replacement mode can be set to the following values;

upgrade-via-active: software activation is completely handled by the active NT, all boards are reset at the
same moment,

upgrade-via standby: the standby NT is upgraded first, then the active NT and all boards are reset and
upgraded

lt-by-lt: the standby NT is upgraded first, then the boards having "lt-by-lt" upgrade capabilities are upgraded
one-by-one by the original standby NT. When all of these boards have completed their upgrade, then the
active NT and remaining boards are reset and upgraded.

Note 1 — The software replacement mode parameter is persistent. The
possible values that can be configured depend on the capabilities of the
NT board.

Setting a non-compatible replacement mode will be rejected by the
system.

Note 2 — For more details on the above listed commands, see other
documents in the documentation set of this release;

- *CLI commands guide*
- *Operations and Maintenance guide using CLI*

3   STOP. This procedure is complete.

12 DLP 102 Download the NE software

12.1 Purpose

Use this DLP to download the NE software before upgrading or migrating the software on the ISAM.

12.2 General

The NE software can be downloaded to the NEs ahead of performing the software upgrade or migration. By default, only the software for planned and detected cards in the system is downloaded. To allow the download of software for cards not yet planned or installed, use the automated software minimization tool before downloading the software.

> **Warning —** The automated software download tool will terminate if you have planned or detected cards in the system that are not supported by the software you are downloading. Always ensure that all the cards in your system are supported by the new software before upgrading or migrating the software on the ISAM.
>
> You can force the software to download even if there are unsupported planned or detected cards in the system by using the --force option of the automated software download tool; see "TNG 101 Automated software download tool" for more information.

> **Note 1 —** Starting in R04.03.02, the current active OSWP is minimized autonomously to make room for the new downloaded OSWP. The active OSWP is minimized up to the files for the NT and the planned and/or detected LT boards.
>
> **Note 2 —** The 7367 ISAM SX/DX does not have separate cards, therefore, the software content is not dependent on any planned or installed cards.

12.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool", "TNG 101 Automated software download tool", and "TNG 106 Additional automated tools", which contain very important information about the components of the Software Upgrade Automation Tool used in this procedure
- you have completed all the steps in "DLP 100 Prepare the software"
- you have access to an EMS TFTP server accessible by the ISAM NEs

- you are logged in to the EMS server as root or as an authorized user to run the Software Upgrade Automation Tool. If logging in as an authorized user, ensure that the proper user authorization permissions have been set; see "DLP 100 Prepare the software".
- when using SNMP version 1 or version 2C, community string is configured on the EMS
- the correct version of the Software Upgrade Automation Tool is installed on the EMS server; see the Customer Release Notes for your release to determine which version of the Software Upgrade Automation Tool you must use

12.4   Procedure

Use this procedure to download the NE software to one or more NEs. All the steps are performed using UNIX.

Caution — When downloading software on multiple NEs, all the NEs listed in *hosts_filename* must have:

- a common CLI username
- a common CLI password

Note 1 — The command, although spanning multiple lines, is a single command. To run the command, enter it in its entirety before pressing Enter. You can also enter the command in sections if needed; for example, if your terminal settings prevent you from entering a long command. To split the command over multiple lines, enter a backslash (\) then press Enter at the end of each command section, and press Enter at the end of the command.

Note 2 — Command parameters in square brackets indicate optional parameters.

Note 3 — From R4.5.02 onward, and where applicable, you can choose the option to use a second CLI password when using CLI over SSH configurations, in case the first CLI password should fail. See "TNG 101 Automated software download tool" for more information.

1   If required, run the automated software minimization tool on the new OSWP to include only the cards listed in a card configuration file.

Note 1 — Use the automated software minimization tool if you will be adding cards to the system before the next upgrade or migration to ensure that the software for the new cards is available when the cards are added to the system. You must use the --minset parameter to allow the download of the software for all cards in the minimized OSWP; see "TNG 106 Additional automated tools" for more information.

Note 2 — The automated software minimization tool renames the OSWP to indicate that the OSWP has been minimized (the suffix is replaced by ZA); see "TNG 108 Overall SoftWare Package concept" for more information.

```
./MinimizeSWP.pl --config config_filename --swp OSWPpath/OSWPnamexx.yyy
--minset --logfile swminlogpath/logname [--debug] [--target targetpath]
[--comm commstring] [--v2] [--v3auth
auth_username:auth_pwd:auth_protocol] [--v3priv
priv_protocol:priv_pwd][--btype <SNMP│YANG>]
```

where

config_filename is the location and filename of the card configuration file; see "TNG 106 Additional automated tools" for more information

OSWPpath/*OSWPname* is the path and filename of the new (full) OSWP package (suffix = AA); see "TNG 108 Overall SoftWare Package concept" for more information about the OSWP filename

xx is the 2-digit ISAM software release number

yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)

swminlogpath/logname is the path and filename of the software minimization log file

targetpath is the location where the minimized OSWP and OSWP Descriptor file will be saved, if different from the location of the full OSWP and OSWP Descriptor file

commstring is the SNMP community string used by the automated software download tool when communicating with an NT unit using SNMP version 1 or version 2C

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

btype is the type to select the use of SNMP or YANG build

Note — Minimization is not applicable to 7367 ISAM SX/DX as there are no separate cards.

2   Run the automated software download tool. This tool automatically commits the software on an NE if the active OSWP on that NE is not in Committed state.

> **Note 1 —** When you download a minimized OSWP, make sure that you use the correct name for the OSWP (the suffix in the OSWP name is replaced by ZA to indicate that the OSWP has been minimized); see "TNG 108 Overall SoftWare Package concept" for more information.
>
> **Note 2 —** If you are downloading software to an NT unit that contains a large OSWP, for example, an OSWP that has never been minimized, use the --reduce parameter to reduce the size of the active OSWP on the NT unit. This ensures that there is enough space to download the new OSWP on the NT unit. The active OSWP on the NT unit is renamed to indicate it has been reduced (the suffix is replaced by RA); see "TNG 108 Overall SoftWare Package concept" for more information.
>
> **Note 3 —** If the active OSWP on the ISAM is already minimized and a new LT (whose software is not present in the active OSWP package) is now inserted, the user may try one of the following methods to download the new OSWP package:
>
> • prepare a minimized package of the new OSWP which includes the newly added LT and then run the Software Download script without using –reduce option
> • perform a direct download of the new OSWP package without using –reduce option

a   To download software to a single NE, enter:

```
./swdl.pl --isam nt_ip_address --swp OSWPpath/OSWPnamexx.yyy
--logfile swdllogpath/logname [--cliusername CLIuser] [--clipassword
CLIpwd] [--clipassword2 SecondCLIpwd] [--reduce] [--force] [--seplog
| --noseplog] [--continue] [--debug] [--multi] [--comm commstring]
[--haip haipaddress]  [--noping] [--v2] [--v3auth
auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--btype <SNMP|YANG>]
```

where
nt_ip_address is the IP address of the NT
OSWPpath/*OSWPname* is the path and filename of the OSWP package (suffix = AA if not minimized and ZA if minimized); see "TNG 108 Overall SoftWare Package concept" for more information about the OSWP filename
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)
swdllogpath/logname is the path and filename of the software download log file
CLIuser is your CLI username if it differs from the CLI username specified in the configuration file
CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file
SecondCLIpwd is your second CLI password specifies an alternative password in the case when CLI over SSH is configured and when the first CLI password fails to connect to one or more NEs
commstring is the SNMP community string used by the automated software download tool when communicating with an NT unit using SNMP version 1 or version 2C
haipaddress is the IP address associated with the physical interface used to communicate with high-availability NEs via SNMP
auth_username is the SNMP version 3 authentication username
auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)
priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)
priv_pwd is the SNMP version 3 privacy password
btype is the type to select the use of SNMP or YANG build

b To download software to multiple NEs, enter:

```
./swdl.pl --hosts hosts_filename --sessions #sessions
--swp OSWPpath/OSWPnamexx.yyy --logfile swdllogpath/logname
[--cliusername CLIuser] [--clipassword CLIpwd] [--clipassword2
SecondCLIpwd] [--reduce] [--force] [--seplog | --noseplog]
[--continue] [--debug] [--multi] [--comm commstring] [--haip
haipaddress] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--btype <SNMP|YANG>]
```

where
hosts_filename is the file with the IP addresses of the NEs when you download software to multiple NEs; see "Hosts file" in TNG 25 for more information about the hosts file
#sessions is the number of parallel sessions to download software to multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information
OSWPpath/OSWPname is the path and filename of the OSWP package (suffix = AA if not minimized and ZA if minimized); see "TNG 108 Overall SoftWare Package concept" for more information
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)
swdllogpath/logname is the path and filename of the software download log file
CLIuser is your CLI username if it differs from the CLI username specified in the configuration file
CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file
SecondCLIpwd is your second CLI password specifies an alternative password in the case when CLI over SSH is configured and when the first CLI password fails to connect to one or more NEs
commstring is the SNMP community string used by the automated software download tool when communicating with an NT unit using SNMP version 1 or version 2C
haipaddress is the IP address associated with the physical interface used to communicate with high-availability NEs via SNMP
auth_username is the SNMP version 3 authentication username
auth_pwd is the SNMP version 3 authentication password (8 characters minimum)
auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)
priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)
priv_pwd is the SNMP version 3 privacy password
btype is the type to select the use of SNMP or YANG build

3 STOP. This procedure is complete.

13 DLP 103 Upgrade the NE software

13.1 Purpose

Use this DLP to upgrade the NE software of the ISAM.

13.2 General

An upgrade is a system software update during which the database is not modified and remains compatible with the original release. No new database is created.

> **Note —** Do not use this procedure when going from a major release to another major release (for example from Release 4.0 to Release 4.1) or if the Customer Release Notes for the new release indicates that you need to perform a migration to go from the original release to the new release. If you do, your current database will not be available to the new software package.

You can upgrade the NE software on one or more ISAM NEs.

These automated tools are Perl scripts installed and run from an EMS server. When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

13.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool" and "TNG 102 Automated software upgrade tool", which contain very important information about the components of the Software Upgrade Automation Tool used in this procedure
- you have completed all the steps in "DLP 102 Download the NE software"
- you have write access to the EMS TFTP server defined in the configuration file; see Table 18 for more information
- you are logged in to the EMS server as root or as an authorized user to run the Software Upgrade Automation Tool. If logging in as an authorized user, ensure that the proper user authorization permissions have been set; see "DLP 100 Prepare the software".
- when using SNMP version 1 or version 2C, community string is configured on your EMS
- the correct version of the Software Upgrade Automation Tool is installed on the EMS server; see the Customer Release Notes for your release to determine which version of the Software Upgrade Automation Tool you must use

13.4   Procedure

Use this procedure to upgrade the software on one or more NEs. All the steps are performed using UNIX.

Warning — In case of a duplex NT system with NANT-E, FANT-F or FANT-G boards, and when both the current running software release and the release to upgrade to support a software upgrade on the stand-by NT, the stand-by NT will be the active NT after the successful completion of the software upgrade. (in case the stand-by NT is in hot stand-by before a software upgrade)

Caution 1 — The NT units, LT units, and ONTs will reset as part of this procedure. For 7367 ISAM SX/DX, the complete system will be reset.

Caution 2 — When upgrading NEs in a subtending configuration, Nokia recommends that you upgrade all the subtended NEs before the subtending NE; see "NTP 100 Upgrade the software" for more information.

Caution 3 — When upgrading software on multiple NEs, all the NEs listed in *hosts_filename* must have:

- a common CLI username
- a common CLI password

Note 1 — When you upgrade software using a minimized OSWP, make sure that you use the correct name for the OSWP (the AA suffix in the OSWP name is replaced by ZA to indicate that the OSWP has been minimized); see "TNG 108 Overall SoftWare Package concept" for more information.

Note 2 — The command, although spanning multiple lines, is a single command. To run the command, enter it in its entirety before pressing Enter. You can also enter the command in sections if needed; for example, if your terminal settings prevent you from entering a long command. To split the command over multiple lines, enter a backslash (\) then press Enter at the end of each command section, and press Enter at the end of the command.

Note 3 — Command parameters in square brackets indicate optional parameters.

Note 4 — From R4.5.02 onward, where applicable, you can choose the option to use a second CLI password when using CLI over SSH configurations, in case the first CLI password should fail. See "TNG 102 Automated software upgrade tool" for more information.

1   Run the automated software upgrade tool:

a   To upgrade a single NE, enter:

```
./upgrade.pl --isam nt_ip_address --swp OSWPpath/OSWPnamexx.yyy
--logfile upgradelogpath/logname [--cliusername CLIuser]
[--clipassword CLIpwd] [--clipassword2 SecondCLIpwd] [--force]
[--seplog | --noseplog] [--continue] [--debug] [--multi] [--comm
commstring] [--haip haipaddress] [--oprid] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--btype <SNMP|YANG>]
```

where
nt_ip_address is the IP address of the NT unit
OSWPpath/*OSWPname* is the path and filename of the OSWP package (suffix = AA if not minimized and ZA if minimized); see "TNG 108 Overall SoftWare Package concept" for more information
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)
upgradelogpath/logname is the path and filename of the upgrade log file
CLIuser is your CLI username if it differs from the CLI username specified in the configuration file
CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file
SecondCLIpwd is your second CLI password specifies an alternative password in the case when CLI over SSH is configured and when the first CLI password fails to connect to one or more NEs
commstring is the SNMP community string used by the automated software upgrade tool when communicating with an NT unit using SNMP version 1 or version 2C
haipaddress is the IP address associated with the physical interface used to communicate with high-availability NEs via SNMP
auth_username is the SNMP version 3 authentication username
auth_pwd is the SNMP version 3 authentication password (8 characters minimum)
auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)
priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)
priv_pwd is the SNMP version 3 privacy password

btype is the type to select the use of SNMP or YANG build

b   To upgrade multiple NEs, enter:

```
./upgrade.pl --hosts hosts_filename --sessions #sessions --swp
OSWPpath/OSWPnamexx.yyy --logfile upgradelogpath/logname
[--cliusername CLIuser] [--clipassword CLIpwd] [--clipassword2
SecondCLIpwd] [--force] [--seplog | --noseplog] [--continue]
[--debug] [--multi] [--comm commstring] [--haip haipaddress]
[--oprid] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--btype <SNMP|YANG>]
```

where

hosts_filename is the file with the IP addresses of the NEs when you upgrade multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information about the hosts file

#sessions is the number of parallel sessions to upgrade multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information

OSWPpath/*OSWPname* is the path and filename of the OSWP package (suffix = AA if not minimized and ZA if minimized); see "TNG 108 Overall SoftWare Package concept" for more information

xx is the 2-digit ISAM software release number

yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)

upgradelogpath/logname is the location and filename of the upgrade log file

CLIuser is your CLI username if it differs from the CLI username specified in the configuration file

CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file

SecondCLIpwd is your second CLI password specifies an alternative password in the case when CLI over SSH is configured and when the first CLI password fails to connect to one or more NEs

commstring is the SNMP community string used by the automated software upgrade tool when communicating with an NT unit using SNMP version 1 or version 2C

haipaddress is the IP address associated with the physical interface used to communicate with high-availability NEs via SNMP

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

btype is the type to select the use of SNMP or YANG build

2   STOP. This procedure is complete.

14 DLP 104 Migrate the NE software

14.1 Purpose

Use this DLP to migrate the NE software of the ISAM.

14.2 General

A migration is a system software update during which the database is modified and must be converted to be compatible with the new software release.

You can migrate the NE software on one or more ISAM NEs.

These automated tools are Perl scripts installed and run from an EMS server. When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

> **Warning —** The SHub database is automatically saved 10 min after a successful migration. If a manual system reset is required within this 10 min time frame, you must manually save the SHub database before resetting the system, using the following CLI command:
>
> ```
> admin software-mngt shub database save
> ```

14.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool" and "TNG 103 Automated software migration tool", which contain very important information about the components of the Software Upgrade Automation Tool used in this procedure
- you have completed all the steps in "DLP 102 Download the NE software"
- you have write access to the EMS TFTP server defined in the configuration file; see Table 18 for more information
- you are logged in to the EMS server as root or as an authorized user to run the Software Upgrade Automation Tool. If logging in as an authorized user, ensure that the proper user authorization permissions have been set; see "DLP 100 Prepare the software".
- when using SNMP version 1 or version 2C, community string is configured on your EMS
- you have verified that the multicast source for each NE does not belong to more than 20 packages; see "NTP 101 Migrate the software" for more information
- the correct version of the Software Upgrade Automation Tool is installed on the EMS server; see the Customer Release Notes for your release to determine which version of the Software Upgrade Automation Tool you must use

- you have verified that there is only one CDE directory on the EMS when migrating a system with ISAM Voice components
- you have verified that there are no voice boards configured when there are no services configured (in case of CDE file requirement)

Note 1 — For SHub Boards, when you migrate to release ISR5301 or later, there should be at least 100 MB of space available in the /data directory to allocate enough memory for the /data/Sw (overlay) directory

Note 2 — For IHub Boards, when you migrate to release ISR5301 or later, there should be at least 200MB of space available in the /ONT directory to allocate enough memory for the /ONT/Sw (overlay) directory

Note 3 — For NANT-A, a maximum of 5 different LT types can be fitted in the SW partition

14.4 Procedure

Use this procedure to migrate the software on one or more NEs. All the steps are performed using UNIX or LINUX.

Warning 1 — When migrating to Release 5.1 or later, whenever the old object has a value greater than the proposed value, the PBMT will migrate the object with the proposed max value.

Warning 2 — When migrating to Release 4.1 a NANT-D system in which VLAN ID 4089 is already used, you must use the --intlnwvlan parameter to set the network VLAN ID; see "TNG 103 Automated software migration tool" for more information.

Warning 3 — When migrating to release 4.3 and a system already uses VLAN ID 4088, you must use the --ssmoutvlan parameter to set the SSM OUT VLAN ID; see "TNG 103 Automated software migration tool" for more information.

Warning 4 — In case of a duplex NT system with NANT-E, FANT-F or FANT-G boards, and when both the current running software release and the release to upgrade to support a software upgrade on the stand-by NT, the stand-by NT will be the active NT after the successful completion of the software upgrade. (in case the stand-by NT is in hot stand-by before a software upgrade)

Caution 1 — The NT units, LT units, and ONTs will reset as part of this procedure. For 7367 ISAM SX/DX, the complete system will be reset.

Caution 2 — When migrating NEs in a subtending configuration, Nokia recommends that you migrate all the subtended NEs before the subtending NE; see "NTP 101 Migrate the software" for more information.

Caution 3 — When migrating software on multiple NEs, all the NEs listed in *hosts_filename* must have:

- a common CLI username
- a common CLI password

Note 1 — When you migrate using a minimized OSWP, make sure that you use the correct name for the OSWP (the AA suffix in the OSWP name is replaced by ZA to indicate that the OSWP has been minimized); see "TNG 108 Overall SoftWare Package concept" for more information.

Note 2 — The command, although spanning multiple lines, is a single command. To run the command, enter it in its entirety before pressing Enter. You can also enter the command in sections if needed; for example, if your terminal settings prevent you from entering a long command. To split the command over multiple lines, enter a backslash (\) then press Enter at the end of each command section, and press Enter at the end of the command.

Note 3 — Command parameters in square brackets indicate optional parameters.

Note 4 — From R4.5.02 onward, where applicable, you can choose the option to use a second CLI password when using CLI over SSH configurations, in case the first CLI password should fail. See "TNG 103 Automated software migration tool" for more information.

1   Run the automated software migration tool:

   a   To migrate a single NE, enter:

```
./migrate.pl --isam nt_ip_address --swp OSWPpath/OSWPnamexx.yyy
--logfile migratelogpath/logname [--cliusername CLIuser]
[--clipassword CLIpwd] [--clipassword2 SecondCLIpwd]
[--ntdbtool NTDBpath] [--lanxtool SHubpath] [--ivpstool xVPSpath]
[--force] [--seplog │ --noseplog] [--continue] [--debug] [--multi]
[--comm commstring] [--oflonly] [--intlnwvlan nwvlanid]
[--ssmoutvlan ssmoutvlanid] [--bwreduce] [--noact] [--actonly]
[--confopt82][--confarberg][--confmcastgrp][--confgapsize][--ttl0fw
d vrfid] [--haip haipaddress] [--oprid] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--btype <SNMP│YANG>]
[--gpononurngmd]
```

where
nt_ip_address is the IP address of the NT unit
OSWPpath/*OSWPname* is the path and filename of the OSWP package (suffix = AA if not minimized and ZA if minimized); see "TNG 108 Overall SoftWare Package concept" for more information
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)
migratelogpath/logname is the path and filename of the migration log file
CLIuser is your CLI username if it differs from the CLI username specified in the configuration file
CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file
SecondCLIpwd is your second CLI password specifies an alternative password in the case when CLI over SSH is configured and when the first CLI password fails to connect to one or more NEs
NTDBpath is the path of the NT database offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename
SHubpath is the path of the SHub offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename
xVPSpath is the path and filename of the xVPS offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename

commstring is the SNMP community string used by the automated software migration tool when communicating with an NT unit using SNMP version 1 or version 2C

nwvlanid is the new network VLAN ID when VLAN ID 4089 is already used in the system; see "TNG 103 Automated software migration tool" for more information

ssmoutvlandid is the new SSM OUT VLAN ID when VLAN ID 4088 is already used in the system; see "TNG 103 Automated software migration tool" for more information

vrfid is the VRF ID of the SHub (only applicable for SHub-based systems)

haipaddress is the IP address associated with the physical interface used to communicate with a high-availability NE via SNMP

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

btype is the type to select the use of SNMP or YANG build

gpononurngmd sets the range-mode for GPON ports

b   To migrate multiple NEs, enter:

```
./migrate.pl --hosts hosts_filename --sessions #sessions --swp
OSWPpath/OSWPnamexx.yyy --logfile migratelogpath/logname
[--cliusername CLIuser] [--clipassword CLIpwd] [--clipassword2
SecondCLIpwd] [--ntdbtool NTDBpath] [--lanxtool SHubpath]
[--ivpstool xVPSpath] [--force] [--seplog │ --noseplog] [--continue]
[--debug] [--multi] [--comm commstring] [--oflonly] [--intlnwvlan
nwvlanid] [--ssmoutvlan ssmoutvlanid] [--bwreduce] [--noact]
[--actonly]
[--confopt82][--confarberg][--confmcastgrp][--confgapsize][--ttl0fw
d vrfid][--haip haipaddress] [--oprid] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--btype <SNMP│YANG>]
[--gpononurngmd]
```

where

hosts_filename is the file with the IP addresses of the NEs when you migrate multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information about the hosts file

#sessions is the number of parallel sessions to migrate multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information

OSWPpath/OSWPname is the path and filename of the OSWP package (suffix = AA if not minimized and ZA if minimized); see "TNG 108 Overall SoftWare Package concept" for more information

xx is the 2-digit ISAM software release number

yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)

migratelogpath/logname is the path and filename of the migration log file

CLIuser is your CLI username if it differs from the CLI username specified in the configuration file

CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file

SecondCLIpwd is your second CLI password specifies an alternative password in the case when CLI over SSH is configured and when the first CLI password fails to connect to one or more NEs

NTDBpath is the path of the NT database offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename

SHubpath is the path of the SHub offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename

xVPSpath is the path and filename of the xVPS offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename

commstring is the SNMP community string used by the automated software migration tool when communicating with an NT unit using SNMP version 1 or version 2C

nwvlanid is the new network VLAN ID when VLAN ID 4089 is already used in the system; see "TNG 103 Automated software migration tool" for more information

ssmoutvlandid is the new SSM OUT VLAN ID when VLAN ID 4088 is already used in the system; see "TNG 103 Automated software migration tool" for more information

vrfid is the VRF ID of the SHub (only applicable for SHub-based systems)

haipaddress is the IP address associated with the physical interface used to communicate with high-availability NEs via SNMP

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

btype is the type to select the use of SNMP or YANG build

gpononurngmd sets the range-mode for GPON ports

2   STOP. This procedure is complete.

15 DLP 105 Commit the NE software

15.1 Purpose

Use this DLP to commit the NE software of the ISAM.

15.2 General

The automated software commitment tool is used to commit the NE software on one or more ISAM NEs.

These automated tools are Perl scripts installed and run from an EMS server. When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

Caution — Nokia does not recommend committing the software until you are ready to move to the next release of software. If you need to commit the software before the next release, ensure that the system is up and running, traffic has resumed, and you are satisfied with the performance of the new release before committing the software. You cannot roll back to a previous load after the software is committed. The previous load is deleted.

You can verify the status of the active OSWP using CLI or TL1.

- Using CLI: `show software-mngt oswp` *OSWP#*
  where *OSWP#* is the number of the active OSWP
- Using TL1: `rept-opstat-oswp::oswp-`*OSWP#*`::;`
  where *OSWP#* is the number of the active OSWP

After running the automated software commitment tool, you can run the automated file clean-up tool to delete all the temporary files and folders created by the components of the Software Upgrade Automation Tool.

15.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool", "TNG 104 Automated software commitment tool", and "TNG 106 Additional automated tools", which contain very important information about the components of the Software Upgrade Automation Tool used in this procedure
- you have completed all the steps in
  - "DLP 103 Upgrade the NE software" if upgrading the software
  - "DLP 104 Migrate the NE software" if migrating the software
- you have write access to the EMS TFTP server defined in the configuration file; see Table 18 for more information

- you are logged in to the EMS server as root or as an authorized user to run the Software Upgrade Automation Tool. If logging in as an authorized user, ensure that the proper user authorization permissions have been set; see "DLP 100 Prepare the software".
- when using SNMP version 1 or version 2C, community string is configured on your EMS
- the correct version of the Software Upgrade Automation Tool is installed on the EMS server; see the Customer Release Notes for your release to determine which version of the Software Upgrade Automation Tool you must use

15.4 Procedure

Use this procedure to commit the software on one or more NEs. All the steps are performed using UNIX or LINUX.

Caution — When committing software on multiple NEs, all the NEs listed in *hosts_filename* must have:

- a common CLI username
- a common CLI password

Note 1 — When you commit a minimized OSWP, make sure that you use the correct name for the OSWP (the AA suffix in the OSWP name is replaced by ZA to indicate that the OSWP has been minimized); see "TNG 108 Overall SoftWare Package concept" for more information.

Note 2 — The command, although spanning multiple lines, is a single command. To run the command, enter it in its entirety before pressing Enter. You can also enter the command in sections if needed; for example, if your terminal settings prevent you from entering a long command. To split the command over multiple lines, enter a backslash (\) then press Enter at the end of each command section, and press Enter at the end of the command.

Note 3 — Command parameters in square brackets indicate optional parameters.

Note 4 — From R4.5.02 onward, where applicable, you can choose the option to use a second CLI password when using CLI over SSH configurations, in case the first CLI password should fail. See "TNG 104 Automated software commitment tool" for more information.

1 Run the automated software commitment tool:

> ⚠️ **Caution —** Commit the software only if the system is up and running and traffic has resumed. You cannot roll back to a previous load after the software is committed. The previous load is deleted.

a To commit software on a single NE, enter:

```
./commit.pl --isam nt_ip_address --swp  OSWPpath/OSWPnamexx.yyy
--logfile commitlogpath/logname [--cliusername CLIuser]
[--clipassword CLIpwd] [--clipassword2 SecondCLIpwd] [--force]
[--seplog │ --noseplog] [--debug] [--multi] [--comm commstring]
[--noping] [--v2] [--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd]
```

where
nt_ip_address is the IP address of the NT unit
OSWPpath/*OSWPname* is the path and filename of the OSWP package (suffix = AA if not minimized and ZA if minimized); see "TNG 108 Overall SoftWare Package concept" for more information
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)
commitlogpath/logname is the path and filename of the software commitment log file
CLIuser is your CLI username if it differs from the CLI username specified in the configuration file
CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file
SecondCLIpwd is your second CLI password specifies an alternative password in the case when CLI over SSH is configured and when the first CLI password fails to connect to one or more NEs
commstring is the SNMP community string used by the automated software commitment tool when communicating with an NT unit using SNMP version 1 or version 2C
auth_username is the SNMP version 3 authentication username
auth_pwd is the SNMP version 3 authentication password (8 characters minimum)
auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)
priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)
priv_pwd is the SNMP version 3 privacy password

b To commit software on multiple NEs, enter:

```
./commit.pl --hosts hosts_filename --sessions #sessions --swp
OSWPpath/OSWPnamexx.yyy --logfile commitlogpath/logname
[--cliusername CLIuser] [--clipassword CLIpwd] [--clipassword2
SecondCLIpwd] [--force] [--seplog │ --noseplog] [--debug] [--multi]
[--comm commstring] [--noping] [--v2] [--v3auth
auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd]
```

where
hosts_filename is the file with the IP addresses of the NEs when you commit software on multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information about the hosts file
#sessions is the number of parallel sessions to commit software on multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information
OSWPpath/*OSWPname* is the path and filename of the OSWP package (suffix = AA if not minimized and ZA if minimized); see "TNG 108 Overall SoftWare Package concept" for more information
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)
commitlogpath/logname is the path and filename of the software commitment log file
CLIuser is your CLI username if it differs from the CLI username specified in the configuration file

CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file

SecondCLIpwd is your second CLI password specifies an alternative password in the case when CLI over SSH is configured and when the first CLI password fails to connect to one or more NEs

commstring is the SNMP community string used by the automated software commitment tool when communicating with an NT unit using SNMP version 1 or version 2C

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

2   If desired, run the automated file clean-up tool to delete the temporary files created by the Software Upgrade Automation Tool during an upgrade or migration.

    a   To run the automated file clean-up tool on a single NE, enter:

```
./cleanUp.pl --isam nt_ip_address --logfile clnuplogpath/logname
[--debug] [--multi]
```

where
nt_ip_address is the IP address of the NT unit
clnuplogpath/logname is the path and filename of the file clean-up log file

    b   To run the automated file clean-up tool on multiple NEs, enter:

```
./cleanUp.pl --hosts hosts_filename --logfile clnuplogpath/logname
[--debug] [--multi]
```

where
hosts_filename is the file with the IP addresses of the NEs when you clean up files on multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information about the hosts file
clnuplogpath/logname is the path and filename of the file clean-up log file

3   STOP. This procedure is complete.

16 DLP 106 Roll back the software

16.1 Purpose

Use this DLP to use the automated software rollback tool to roll back the software of the ISAM if you want to go back to the previous software load.

Note — Automated Rollback is only supported on the 7360 ISAM FX platform.

16.2 General

The automated software rollback tool is used to roll back the active software to downgrade single or multiple NEs to the previous active software load.

Note 1 — You cannot roll back to the previous software release if you have committed the new software release.

Note 2 — If you add a new type of card to a NE which is introduced in the current software and then roll back the software on the NE, the new card will not be supported by the software after the rollback.

Note 3 — You can roll back to previous software release only when the passive OSWP is in committed state and active software is associated to its database.

Note 4 — Once you have rolled back to previous release, you will no longer have access to configuration done after the migration since the NE has been rolled back to the passive OSWP.

Note 5 — If the software on the ONTs was upgraded during the NE software upgrade or migration, rolling back the NE software also rolls back the software on the ONTs.

Please contact Nokia Technical Support if you encounter problems that require a rollback of the operational software to the previous release.

16.3 Prerequisites

Before you start this procedure, ensure that:

- you have run "TAP 100 Verify the system status" to verify the system status

Note 1 — If ISR5301 or later is installed and a software package less than ISR5301 is downloaded, all the NT and LT files will be downloaded in /Sw. The LT software files corresponding to software less than 5301 will not be downloaded in overlay directory (/data for SHub boards and /ONT for IHub boards)..

Note 2 — If software less than ISR5301 is activated and committed, LT software files related to ISR5301 present in /Sw will be deleted. LT files of ISR5301 which are present in the overlay directory will not be deleted.

16.4 Procedure

Use this procedure to roll back the software on one or more NEs. All the steps are performed using UNIX or LINUX.

1 Run the automated software rollback tool:

Caution — When a rollback of software is performed on multiple NEs, all the NEs listed in hosts_filename must have:

- a common CLI username
- a common CLI password

Note 1 — The command, although spanning multiple lines, is a single command. To run the command, enter it in its entirety before pressing Enter. You can also enter the command in sections if needed; for example, if your terminal settings prevent you from entering a long command. To split the command over multiple lines, enter a backslash (\) then press Enter at the end of each command section, and press Enter at the end of the command.

Note 2 — Command parameters in square brackets indicate optional parameters.

a   To roll back software on a single NE, enter:

```
./rollback.pl --isam nt_ip_address --swp OSWPpath/OSWPnamexx.yyy
--logfile rollbacklogpath/logname │ --id runid [--cliusername
CLIuser][--clipassword CLIpwd] [--clipassword2
SecondCLIpwd][--seplog │ --noseplog] [--continue] [--debug] [--comm
commstring][--noname] [--noping] [--v2] [--v3auth
auth_username:auth_pwd:auth_protocol] [--v3priv
priv_protocol:priv_pwd]
```

where
nt_ip_address is the IP address of the NT unit
OSWPpath/OSWPname is the path and filename of the OSWP package (suffix = AA if not minimized and ZA if minimized)
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)
rollbacklogpath/logname is the path and filename of the software rollback log file
runid is a session identifier used by the 5529 LRM. All log files are fixed named and contain this ID value.
CLIuser is your CLI username if it differs from the CLI username specified in the configuration file
CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file
SecondCLIpwd is your second CLI password (it is an alternative password in the case when CLI over SSH is configured and when the first CLI password fails to connect to one or more NEs)
commstring is the SNMP community string used by the automated software rollback tool when communicating with an NT unit using SNMP version 1 or version 2C
auth_username is the SNMP version 3 authentication username
auth_pwd is the SNMP version 3 authentication password (8 characters minimum)
auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)
priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)
priv_pwd is the SNMP version 3 privacy password

b   To roll back software on multiple NEs, enter:

```
./rollback.pl --hosts hosts_filename --sessions #sessions  --swp
OSWPpath/OSWPnamexx.yyy --logfile rollbacklogpath/logname
[--clipassword CLIpwd] [--clipassword2 SecondCLIpwd] [--seplog |
--noseplog] [--continue] [--debug] [--comm commstring] [--noping]
[--noname][--v2] [--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd]
```

where

hosts_filename is the file with the IP addresses of the NEs when you roll back software on multiple NEs; see the Hosts file description in "TNG 100 Software Upgrade Automation Tool" for more information about the hosts file.

#sessions is the number of parallel sessions to rollback software on multiple NEs; see the information about installing and using the components of the Software Upgrade Automation Tool in "TNG 100 Software Upgrade Automation Tool" for more information

OSWPpath/OSWPname is the path and filename of the OSWP package (suffix = AA if not minimized and ZA if minimized)

xx is the 2-digit ISAM software release number

yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)

rollbacklogpath/logname is the path and filename of the software rollback log file

CLIuser is your CLI username if it differs from the CLI username specified in the configuration file

CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file

SecondCLIpwd is your second CLI password (it is an alternative password in the case when CLI over SSH is configured and when the first CLI password fails to connect to one or more NEs)

commstring is the SNMP community string used by the automated software rollback tool when communicating with an NT unit using SNMP version 1 or version 2C

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

2   STOP. This procedure is complete.

17 DLP 107 Reconfigure an NTIO unit

17.1 Purpose

Use this DLP to reconfigure an ISAM NE, such as the 7302 ISAM or the 7330 ISAM FTTN, using the Software Upgrade Automation Tool when an NTIO unit is replaced by a new type of NTIO unit.

Note — This DLP does not apply to the 7356 ISAM FTTB in stand-alone mode, the 7360 ISAM FX or the 7367 ISAM SX/DX.

17.2 General

When replacing an NTIO unit with a new type of NTIO unit, you must reconfigure the system for the new type of NTIO unit.

Use this procedure only if the NTIO unit is replaced outside of a migration window, for example, when a card failure has occurred and the card is replaced by a new type.

Note — You can only replace an NTIO unit with a unit of the same family, for example, an NCNC-C card with an NCNC-E card; see "NTP 102 Reconfigure an NTIO unit" for more information.

17.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool" and "TNG 106 Additional automated tools", which contain very important information about the components of the Software Upgrade Automation Tool used in this procedure
- you have completed all the steps in "DLP 100 Prepare the software"
- you are logged in to the EMS server as root or as an authorized user to run the Software Upgrade Automation Tool. If logging in as an authorized user, ensure that the proper user authorization permissions have been set; see "DLP 100 Prepare the software".
- the correct version of the Software Upgrade Automation Tool is installed on the EMS server; see the Customer Release Notes for your release to determine which version of the Software Upgrade Automation Tool you must use

17.4   Procedure

Use this procedure to reconfigure an NTIO unit. This step is performed using UNIX or LINUX.

Note 1 — The command, although spanning multiple lines, is a single command. To run the command, enter it in its entirety before pressing Enter. You can also enter the command in sections if needed; for example, if your terminal settings prevent you from entering a long command. To split the command over multiple lines, enter a backslash (\) then press Enter at the end of each command section, and press Enter at the end of the command.

Note 2 — Command parameters in square brackets indicate optional parameters.

---

1   Reconfigure the system for the new type of NTIO unit using UNIX or LINUX.

```
./cvtNcncC2E.pl --isam nt_ip_address --logfile configlogpath/logname
[--username CLIuser] [--password CLIpwd] [--debug]
```

where

nt_ip_address is the IP address of the NT unit

configlogpath/*logname* is the path and filename of the conversion log file

CLIuser is your CLI username if it differs from the CLI username specified in the configuration file

CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file

---

2   STOP. This procedure is complete.

18 DLP 108 Replace an NPOT-A unit with an NPOT-C unit

18.1 Purpose

Use this DLP when replacing an NPOT-A LT unit with an NPOT-C LT unit in the ISAM system after software upgrade or migration has been completed.

Note — This DLP is not applicable to 7362 ISAM DF/SF, 7363 ISAM MX and 7367 ISAM SX/DX.

18.2 General

The NPOT-A LT and the NPOT-C LT units are defined as compatible board types meaning that operators can replace the NPOT-A LT unit with the compatible NPOT-C LT unit without re-planning the slot at both the voice service and the equipment service domain level.

When slot ID planning is desired, the operator can directly re-plan the NPOT-A LT as NPOT-C LT without doing an 'un-plan', as the boards are compatible. For incompatible LT units, the slot must be un-planned and then re-planned again. See DLP 2111 in *Operations and Maintenance Using CLI Guide.*

Note — For compatible LT units, a board-type mismatch alarm is not raised and the system brings the board in-service using the present configuration data.

Replacing an NPOT-A unit with an NPOT-C unit requires an additional step to bring the NPOT-C unit online successfully. A re-download of the active OSWP is required in order to bring the NPOT-C LT unit online.

Note — Re-download of the active OSWP is only required for the very first NPOT-A by NPOT-C LT unit replacement in the shelf.

Software migration for an NPOT-C unit is supported by the following releases:

- ISAM R4.2.05 and higher R4.2 maintenance releases
- ISAM R4.3.02 and higher R4.3 maintenance releases
- R4.4 and higher main releases

> **Note 1 —** NPOT-A and NPOT-C units can co-locate within the same shelf.
>
> **Note 2 —** NPOT-B and NPOT-C units can co-locate within the same shelf.
>
> **Note 3 —** An NPOT-C LT unit cannot be replaced by an NPOT-A LT unit.

18.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool" and "TNG 106 Additional automated tools", which contain very important information about the components of the Software Upgrade Automation Tool used in this procedure
- you have reviewed "TNG 108 Overall SoftWare Package concept", that contains information about OSWP.
- you have completed all the prerequisites and procedure steps in "NTP 103 Replace an NPOT-A LT unit with an NPOT-C LT unit".
- you are logged in to the EMS server as root or as an authorized user to run the Software Upgrade Automation Tool. If logging in as an authorized user, ensure that the proper user authorization permissions have been set; see "DLP 100 Prepare the software".
- the correct version of the Software Upgrade Automation Tool is installed on the EMS server; see the Customer Release Notes for your release to determine which version of the Software Upgrade Automation Tool you must use.

18.4 Procedure

Use this procedure to replace an NPOT-A unit with an NPOT-C unit in the ISAM system.

1   Replace the NPOT-A unit with the NPOT-C unit, using the same slot, according to the installation documentation for your product.

> **Note —** In case it is the very first NPOT-A to NPOT-C replacement in the shelf, the NPOT-C unit will not start-up immediately. An alarm will be generated that states "Failed to load or find requested software". The equipment status for this board will display an error message that states "waiting for software".

2   Re-download the active OSWP using the same version and index of the active OSWP; see
"TNG 109 Software database processes" for procedure.

Note — This step is only required for the very first NPOT-A to NPOT-C
LT unit replacement in the shelf. For all subsequent replacement of the
NPOT-C , the software files will already be present in the active OSWP.

After completion of the active OSWP re-download, the system will be in the same state as it
was, but with the NPOT-C software image files present in the active OSWP and the NPOT-C
unit will start-up successfully.

3   Verify the equipment using the following command:

```
show equipment slot [(slot)]
```

4   STOP. This procedure is complete.

3HH-10318-AAAA-TCZZA

19 DLP 109 Downgrade the software on an NT unit

19.1 Purpose

Use this DLP to downgrade the software of the ISAM.

Note — This DLP is not applicable to 7367 ISAM SX/DX.

19.2 General

When replacing an NT unit or installing a new NE, if the software on the new NT unit is higher than the software on the rest of the system, you need to downgrade the software on the new NT unit to match the software on the rest of the system.

Warning — In case of a duplex NT system with NANT-E, FANT-F or FANT-G boards, and when both the current running software release and the release to downgrade to support a software upgrade on the stand-by NT, the stand-by NT will be the active NT after the successful completion of the software downgrade. (in case the stand-by NT is in hot stand-by before a software downgrade)

Caution — For a nonredundant system, NT unit failure in a shelf will cause a service outage. Replacement of an NT unit and data restoration are required to restore service. If backups of the NE and SHub/IHub databases are not available to be restored from the EMS, the entire NE will have to be reprovisioned. Proceed according to established local procedures. Even if database backups are used, you will still need to re-enter any database changes made after the backups were taken.

Note — In a redundant system, you only need to downgrade the software of the active NT unit, the software on the standby NT unit will be downgraded when it is synchronized to the active NT unit (same as for an upgrade or migration).

19.3   Prerequisites

Before you start this procedure, ensure that:

- if you are downgrading software on a new NE, the new NE is installed and ready to be configured
- the system is operational
- all operator commands have finished running

19.4   Procedure

Use this procedure to downgrade the software to a previous software release. All the steps are performed using CLI, TL1, or UNIX or LINUX.

---

1   If you are downgrading the software on a new NT unit.

   i   Back up the database on the NT unit; see the *Operations and Maintenance Using CLI* or the *Operations and Maintenance Using TL1* for your product for information about backing up the database.

   Note — If it is not possible to back up the database, note all the parameter values so you can reconfigure the NE after the software has been downgraded.

   ii   Replace the NT unit; see "RTP 100 Replace an NT unit".

---

2   Set up the connectivity between the NE and the TFTP server on the EMS; see the *Operations and Maintenance Using CLI* or the *Operations and Maintenance Using TL1* for your product for information about configuring the system, including how to set up connectivity.

---

3   Minimize and download the correct NE software version to the new NT unit using the automated software download tool; see "DLP 102 Download the NE software".

   Note — You must use the automated software minimization tool before downloading the NE software; see "DLP 102 Download the NE software". Ensure that the new NT unit is listed in the card configuration file.

---

4   Stage the correct ONT software on the new NT unit using the automated ONT software staging tool; see "DLP 110 Stage the ONT software".

---

5   If you are downgrading the software on a new NT unit, restore the database on the NT unit; see the *Operations and Maintenance Using CLI* or the *Operations and Maintenance Using TL1* for your product for information about restoring the database.

---

6   Activate the software with the restored database:

> ⚠️ **Caution —** The NT and LT units will reset when the software is
> activated.

    a   Using CLI:

            `admin software-mngt oswp OSWP# activate with-linked-db`

            where *OSWP#* is the number of the active OSWP

    b   Using TL1:

            `ed-oswp::oswp-OSWP#::::activation= withlinkeddb;`

            where *OSWP#* is the number of the active OSWP

7   Wait until the new NT unit is operational.

8   Verify the connectivity between the NE and the network by verifying the following:

- IP address, default route, and other system-related settings
- uplink configuration
- configuration of the external management VLAN

See the *Operations and Maintenance Using CLI* or the *Operations and Maintenance Using TL1* for your product for information about verifying system configuration settings.

9   STOP. This procedure is complete.

3HH-10318-AAAA-TCZZA

20   DLP 110 Stage the ONT software

20.1   Purpose

Use this DLP to stage the ONT software on the ISAM.

i	**Note —** This DLP is not applicable to 7363 ISAM MX and 7367 ISAM SX/DX.

20.2   General

Before downloading the ONT software to the ONTs, you must download the ONT software to the NE or NEs to which the ONTs are connected. This is called staging the ONT software.

You can stage the ONT software on one or more ISAM NEs.

These automated tools are Perl scripts installed and run from an EMS server. When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

20.3   Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool" and "TNG 103 Automated software migration tool", which contain very important information about the components of the Software Upgrade Automation Tool used in this procedure
- you have completed all the steps in "DLP 100 Prepare the software"
- you have write access to the EMS TFTP server defined in the configuration file; see Table 18 for more information
- you are logged in to the EMS server as root or as an authorized user to run the Software Upgrade Automation Tool. If logging in as an authorized user, ensure that the proper user authorization permissions have been set; see "DLP 100 Prepare the software".
- when using SNMP version 1 or version 2C, community string is configured on your EMS
- the correct version of the Software Upgrade Automation Tool is installed on the EMS server; see the Customer Release Notes for your release to determine which version of the Software Upgrade Automation Tool you must use

20.4   Procedure

Use this procedure to stage the ONT software on one or more NEs. All the steps are performed using UNIX or LINUX.

Caution — When staging ONT software on multiple NEs, all the NEs listed in *hosts_filename* must have:

- a common CLI username
- a common CLI password
- a common TL1 username
- a common TL1 password

Note 1 — The command, although spanning multiple lines, is a single command. To run the command, enter it in its entirety before pressing Enter. You can also enter the command in sections if needed; for example, if your terminal settings prevent you from entering a long command. To split the command over multiple lines, enter a backslash (\) then press Enter at the end of each command section, and press Enter at the end of the command.

Note 2 — Command parameters in square brackets indicate optional parameters.

1   Run the automated ONT software staging tool:

a   To stage ONT software on a single NE, enter:

```
./stageont.pl --isam nt_ip_address --servdir ONTswpath --release
Rxx.yy.zz --onttypes Type1:Load1,Type2:Load2,..,Typen:Loadn
--logfile ONTstagelogpath/logname [--warn threshold]
[--ontreleasemap releasemappath] [--tl1username TL1user]
[--tl1password TL1pwd] [--cliusername CLIuser]
[--clipassword CLIpwd] [--multi] [--seplog | --noseplog] [--noping]
[--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol [:priv_protocol:
priv_pwd]]
```

where
nt_ip_address is the IP address of the NT unit
ONTswpath is the path of the server directory that contains the new ONT software
xx.yy.zz is the 6-digit ONT software release number (for example, R04.00.10)
Typen and *Loadn* are the specific ONT model types and load types for which you are staging software; see "TNG 105 ONT automated tools" for more information
ONTstagelogpath/logname is the path and filename of the software staging log file
threshold is the maximum number of operation failures that can occur before the script stops; see "TNG 105 ONT automated tools" for more information
releasemappath is the path of the server directory that contains the ONT release map
TL1user is your TL1 username if it differs from the TL1 username specified in the configuration file
TL1pwd is your TL1 password if it differs from the TL1 password specified in the configuration file
CLIuser is your CLI username if it differs from the CLI username specified in the configuration file
CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file
commstring is the SNMP community string used by the automated ONT software staging tool when communicating with an NT unit using SNMP version 1 or version 2C

auth_username is the SNMP version 3 authentication username
auth_pwd is the SNMP version 3 authentication password (8 characters minimum)
auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)
priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)
priv_pwd is the SNMP version 3 privacy password

b   To stage ONT software on multiple NEs, enter:

```
./stageont.pl --hosts hosts_filename [--sessions #sessions]
--servdir ONTswpath --release Rxx.yy.zz
--onttypes Type1:Load1,Type2:Load2,..,Typen:Loadn
--logfile ONTstagelogpath/logname [--warn threshold]
[--ontreleasemap releasemappath] [--tl1username TL1user]
[--tl1password TL1pwd] [--cliusername CLIuser]
[--clipassword CLIpwd] [--multi] [--seplog | --noseplog] [--noping]
[--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol [:priv_protocol:
priv_pwd]]
```

where
hosts_filename is the file with the IP addresses of the NEs when you stage ONT software on multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information about the hosts file

#sessions is the number of parallel sessions to stage ONT software on multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information

ONTswpath is the path of the server directory that contains the new ONT software

xx.yy.zz is the 6-digit ONT software release number (for example, R04.00.10)

Typen and *Loadn* are the specific ONT model types and load types for which you are staging software; see "TNG 105 ONT automated tools" for more information

ONTstagelogpath/logname is the path and filename of the software staging log file

threshold is the maximum number of operation failures that can occur before the script stops; see "TNG 105 ONT automated tools" for more information

releasemappath is the path of the server directory that contains the ONT release map

TL1user is your TL1 username if it differs from the TL1 username specified in the configuration file

TL1pwd is your TL1 password if it differs from the TL1 password specified in the configuration file

CLIuser is your CLI username if it differs from the CLI username specified in the configuration file

CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file

commstring is the SNMP community string used by the automated software migration tool when communicating with an NT unit using SNMP version 1 or version 2C

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

2   STOP. This procedure is complete.

21 DLP 111 Download the ONT software

21.1 Purpose

Use this DLP to download ONT software to the ISAM ONTs.

Note — This DLP is not applicable to 7363 ISAM MX and 7367 ISAM SX/DX.

21.2 General

The ONT software can be downloaded to the ONTs ahead of performing the ONT software upgrade, or the software can be activated at the same time the ONT software is download to the ONTs.

You can download ONT software to ONTs connected to one or more ISAM NEs.

These automated tools are Perl scripts installed and run from an EMS server. When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

21.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool" and "TNG 105 ONT automated tools", which contain very important information about the components of the Software Upgrade Automation Tool used in this procedure
- you have completed all the steps in "DLP 110 Stage the ONT software"
- you have write access to the EMS TFTP server defined in the configuration file; see Table 18 for more information
- you are logged in to the EMS server as root or as an authorized user to run the Software Upgrade Automation Tool. If logging in as an authorized user, ensure that the proper user authorization permissions have been set; see "DLP 100 Prepare the software".
- when using SNMP version 1 or version 2C, community string is configured on your EMS
- the correct version of the Software Upgrade Automation Tool is installed on the EMS server; see the Customer Release Notes for your release to determine which version of the Software Upgrade Automation Tool you must use

21.4 Procedure

Use this procedure to download the ONT software to ONTs connected to one or more NEs. All the steps are performed using UNIX or LINUX.

> **Caution 1 —** If the --operationmode parameter is set to either ACTONLY or DLANDACT, the ONTs will reset as part of this procedure.
>
> **Caution 2 —** When downloading software to ONTs connected to multiple NEs, all the NEs listed in *hosts_filename* must have:
>
> - a common TL1 username
> - a common TL1 password.

> **Note 1 —** The command, although spanning multiple lines, is a single command. To run the command, enter it in its entirety before pressing Enter. You can also enter the command in sections if needed; for example, if your terminal settings prevent you from entering a long command. To split the command over multiple lines, enter a backslash (\) then press Enter at the end of each command section, and press Enter at the end of the command.
>
> **Note 2 —** Command parameters in square brackets indicate optional parameters.

1 Run the automated ONT software download tool:

   a To download software to ONTs connected to a single NE, enter:

```
./ontDownloadandActivate.pl --isam nt_ip_address
--release Rxx.yy.zz
--onttypes Type1:Load1,Type2:Load2,..,Typen:Loadn
--ontdownloadandactivatemode Auto │ Manual
--operationmode DLONLY │ ACTONLY │ DLANDACT │ DELAYACT
--logfile ONTdllogpath/logname [--warn threshold]
[--ontreleasemap releasemappath] [--tl1username TL1user]
[--tl1password TL1pwd] [--cliusername CLIuser]
[--clipassword CLIpwd] [--multi] [--seplog │ --noseplog] [--noping]
[--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol [:priv_protocol:
priv_pwd]]
```

where
nt_ip_address is the IP address of the NT unit
xx.yy.zz is the 6-digit ONT software release number (for example, R04.00.10)
Typen and *Loadn* are the specific ONT model types and load types for which you are staging software; see "TNG 105 ONT automated tools" for more information
ONTdllogpath/logname is the path and filename of the software download log file
threshold is the maximum number of operation failures that can occur before the script stops; see "TNG 105 ONT automated tools" for more information
releasemappath is the path of the server directory that contains the ONT release map
TL1user is your TL1 username if it differs from the TL1 username specified in the configuration file
TL1pwd is your TL1 password if it differs from the TL1 password specified in the configuration file
CLIuser is your CLI username if it differs from the CLI username specified in the configuration file

CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file

commstring is the SNMP community string used by the automated ONT software download tool when communicating with an NT unit using SNMP version 1 or version 2C

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

b To migrate multiple NEs, enter:

```
./ontDownloadandActivate.pl --hosts hosts_filename
[--sessions #sessions] --release Rxx.yy.zz
--onttypes Type1:Load1,Type2:Load2,..,Typen:Loadn
--ontdownloadandactivatemode Auto │ Manual
--operationmode DLONLY │ ACTONLY │ DLANDACT │ DELAYACT
--logfile ONTdllogpath/logname [--warn threshold]
[--ontreleasemap releasemappath] [--tl1username TL1user]
[--tl1password TL1pwd] [--cliusername CLIuser]
[--clipassword CLIpwd] [--multi] [--seplog │ --noseplog] [--noping]
[--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol [:priv_protocol:
priv_pwd]]
```

where

hosts_filename is the file with the IP addresses of the NEs when you download ONT software to ONTs connected to multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information about the hosts file

#sessions is the number of parallel sessions to download ONT software to ONTs connected to multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information

xx.yy.zz is the 6-digit ONT software release number (for example, R04.00.10)

Typen and *Loadn* are the specific ONT model types and load types for which you are staging software; see "TNG 105 ONT automated tools" for more information

ONTdllogpath/logname is the path and filename of the software download log file

threshold is the maximum number of operation failures that can occur before the script stops; see "TNG 105 ONT automated tools" for more information

releasemappath is the path of the server directory that contains the ONT release map

TL1user is your TL1 username if it differs from the TL1 username specified in the configuration file

TL1pwd is your TL1 password if it differs from the TL1 password specified in the configuration file

CLIuser is your CLI username if it differs from the CLI username specified in the configuration file

CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file

commstring is the SNMP community string used by the automated ONT software download tool when communicating with an NT unit using SNMP version 1 or version 2C

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

2 STOP. This procedure is complete.

22 DLP 112 Replace an NVPS-A unit with an NVPS-C unit

22.1 Purpose

Use this DLP when replacing an NVPS-A LT unit with an NVPS-C LT unit in the ISAM system after software upgrade or migration has been completed.

> **Note —** This DLP is not applicable to 7362 ISAM DF/SF, 7363 ISAM MX and 7367 ISAM SX/DX.

22.2 General

The NVPS-A LT and the NVPS-C LT units are defined as compatible board types meaning that operators can replace the NVPS-A LT unit with the compatible NVPS-C LT unit without re-planning the slot at both the voice service and the equipment service domain level.

When slot ID planning is desired, the operator can directly re-plan the NVPS-A LT as NVPS-C LT without doing an 'un-plan', as the boards are compatible. For incompatible LT units, the slot must be un-planned and then re-planned again. See DLP 2111 in *Operations and Maintenance Using CLI Guide.*

> **Note —** For compatible LT units, a board-type mismatch alarm is not raised and the system brings the board in-service using the present configuration data.

Replacing an NVPS-A unit with an NVPS-C unit requires an additional step to bring the NVPS-C unit online successfully. A re-download of the active OSWP is required in order to bring the NVPS-C LT unit online.

> **Note —** Re-download of the active OSWP is only required for the very first NVPS-A by NVPS-C LT unit replacement in the shelf.

Software migration for an NVPS-C unit is supported by the following releases:

* ISAM R5.3 and higher R5.3 maintenance releases

> **Note 1 —** NVPS-A and NVPS-C pairs can co-locate within the same shelf.
>
> **Note 2 —** NVPS-A and NVPS-C cannot be mixed in an NVPS pair.

22.3   Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool" and "TNG 106 Additional automated tools", which contain very important information about the components of the Software Upgrade Automation Tool used in this procedure
- you have reviewed "TNG 108 Overall SoftWare Package concept", that contains information about OSWP.
- you have completed all the prerequisites and procedure steps in "NTP 103 Replace an NPOT-A LT unit with an NPOT-C LT unit".
- you are logged in to the EMS server as root or as an authorized user to run the Software Upgrade Automation Tool. If logging in as an authorized user, ensure that the proper user authorization permissions have been set; see "DLP 100 Prepare the software".
- the correct version of the Software Upgrade Automation Tool is installed on the EMS server; see the Customer Release Notes for your release to determine which version of the Software Upgrade Automation Tool you must use.

22.4   Procedure

Use this procedure to replace an NVPS-A unit with an NVPS-C unit in the ISAM system.

1   Replace the NVPS-A unit with the NVPS-C unit, using the same slot, according to the installation documentation for your product.

> **Note —** In case it is the very first NVPS-A to NVPS-C replacement in the shelf, the NVPS-C unit will not start-up immediately. An alarm will be generated that states "Failed to load or find requested software". The equipment status for this board will display an error message that states "waiting for software".

2   Re-download the active OSWP using the same version and index of the active OSWP; see "TNG 109 Software database processes" for procedure.

> **Note —** This step is only required for the very first NVPS-A to NVPS-C LT unit replacement in the shelf. For all subsequent replacement of the NVPS-C , the software files will already be present in the active OSWP.

After completion of the active OSWP re-download, the system will be in the same state as it was, but with the NVPS-C software image files present in the active OSWP and the NVPS-C unit will start-up successfully.

3   Verify the equipment using the following command:

```
show equipment slot [(slot)]
```

4   STOP. This procedure is complete.

Routine Task Procedures (RTP)

23 RTP 100 Replace an NT unit

23 RTP 100 Replace an NT unit

23.1 Purpose

Use this RTP to replace an NT unit in the ISAM.

Note — This RTP is not applicable to 7367 ISAM SX/DX as there are no removable cards.

23.2 General

Use this procedure to replace an NT unit in a redundant or non-redundant system. When you replace an NT unit, the replacement NT unit contains the correct, factory-loaded software version for the NT and SHub/IHub.

Note 1 — When you replace an NT unit in the ISAM you do not need to power down the shelf because NT units can be extracted and inserted while the system is powered up, even when replacing an NT unit in a non-redundant system. System down time will be minimized by not shutting down the power when replacing an NT unit.

Note 2 — When you replace an NT unit you can re-use the compact flash card from the old NT unit by replacing the compact flash card on the new NT unit with the compact flash card from the old NT unit.

23.3 Prerequisites

Before you start this procedure, ensure that:

- there is a backup on the EMS server of the database
- if the system is operational, all operator commands have finished running

23.3.1 Tools required

You need the following tools:

- an antistatic wrist strap
- cutters for cutting tie-wraps and tie downs

23.4   Procedure

Use this procedure to replace an NT unit. See the EMS documentation, the *Operations and Maintenance Using CLI,* or the *Operations and Maintenance Using TL1* for your product for information about using the EMS, CLI, or TL1.

> ⚠ **Warning 1 —** Possibility of equipment damage due to electrostatic discharge. Keep the NT unit in its original package until the unit is ready to be installed.
>
> **Warning 2 —** NT units contain ESD-sensitive devices. These devices are susceptible to ESD damage in unconnected circuit conditions. Appropriate ESD procedures should always be followed when installing or removing NT units.

---

1   If desired, verify the operational status of the system before replacing an NT unit; see "TAP 100 Verify the system status".

---

2   Back up the database on the NT unit; see the *Operations and Maintenance Using CLI* or the *Operations and Maintenance Using TL1* for your product for information about backing up the database.

---

3   If you are replacing an NT unit in a non-redundant system, prepare the system for the shut down that will happen when the NT is removed. This will save configuration data so that it can be easily restored after the NT is replaced.

   a   Using CLI:

```
admin equipment prepare-sys-shutdown
```

   b   Using TL1:

```
set-ne-all::com::::shutprep=ready;
```

---

4   Put on the antistatic wrist strap and connect it to the antistatic wrist strap connector on the shelf.

5   Remove the NT unit you are replacing.

> ⚠️ **Caution —** In a non-redundant system, service is interrupted until the replacement NT unit is installed and operational.

    i   If the shelf has a cover installed, remove the shelf cover.

    ii   Note where each cable is connected to the NT unit you are replacing.

> ⚠️ **Caution —** All cables must be attached to the same port on the replacement NT unit. Switching cables between ports requires reprogramming of each affected port.

    iii   Cut any tie down used to secure cables to the NT unit and remove the attached cables from the NT unit.

    iv   Pull the insertion and extraction tabs on the NT unit you are replacing to the unlocked position.

    v   Slide the NT unit out of the slot.

    vi   If you will be re-using the compact flash card from the old NT unit, remove the compact flash card from the NT unit and set it aside temporarily.

    vii   Place the NT unit in an ESD protective container.

6   Install the new NT unit.

    i   Remove the new NT unit to be installed from its ESD-protective package.

    ii   If you will be re-using the compact flash card from the old NT unit, replace the compact flash card with the one removed from the old NT unit in step 5.

    iii   Ensure that the insertion and extraction tabs on the NT unit are in the unlocked position.

    iv   Slide the new NT unit into the appropriate slot and ensure that the NT unit is firmly seated in the backplane.

    v   Push the insertion and extraction tabs to lock the NT unit in the shelf.

vi Connect the cables to the NT unit, ensuring that each cable connects to the same port it was connected to on the NT unit you removed in step 5.

> ⚠️ **Warning —** Proper fiber cable management is crucial. Improper fiber cable placement can cause the fiber cables to crimp and become damaged if a shelf cover is installed. Make sure the fiber cables are dressed properly as follows:
>
> - fiber cables are not twisted or kinked
> - fiber cables do not cross over the insertion and extraction tabs on top of the units; rather, they pass on the side of the tabs

vii If the shelf had a cover installed, install the shelf cover.

---

7 Wait until the new NT unit is operational.

---

8 If you replaced an NT unit in a non-redundant system:

i Set the IP address of the new NT unit using the EMS, CLI, or TL1. The IP address of the NT unit is the IP address of the NE.

ii Save the configuration using the EMS, CLI, or TL1.

---

9 Verify that the NT unit is active using the EMS, CLI, or TL1 and that the standby NT unit, if any, is synchronized to the active NT unit.

---

10 Restore the database on the NT unit; see the *Operations and Maintenance Using CLI* or the *Operations and Maintenance Using TL1* for your product for information about restoring the database.

---

11 If desired, verify the operational status of the system after replacing the NT unit and compare the results with those of step 1; see "TAP 100 Verify the system status".

---

12 STOP. This procedure is complete.

Trouble Analysis Procedures (TAP)

24 TAP 100 Verify the system status

24 TAP 100 Verify the system status

24.1 Purpose

Use this TAP to verify the operational and readiness status of the ISAM and to compare the operational status of the system before and after a software upgrade, software migration, or database conversion.

24.2 General

The following system verification tools are available:

- automated system readiness verification tool

  This tool is used before an upgrade or migration to verify if there are problems in one or more ISAM NEs that could prevent the procedure from running successfully.

- automated system status verification tool

  This tool is used to verify the operational status of one or more ISAM NEs before and after an upgrade, migration, or database conversion. Use the automated system status verification tool before and after a procedure and review the results to verify if the procedure was successful. For best results, use the automated system status verification tool while the system is in service.

- automated system status comparison tool

  This tool is used to compare the results of the automated system status verification tool. Use the automated system status comparison tool on two sets of results from the automated system status verification tool. One set must be obtained using the --pre parameter of the automated software status verification tool, and the other set using the --post parameter.

These automated tools are Perl scripts installed and run from an EMS server. When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

24.3 Prerequisites

Before you start this procedure, ensure that:

- you have reviewed "TNG 100 Software Upgrade Automation Tool" and "TNG 106 Additional automated tools", which contain very important information about the Software Upgrade Automation Tool and the automated system verification tools used in this procedure
- you have completed all the steps in "DLP 100 Prepare the software"
- you have write access to the EMS TFTP server defined in the configuration file; see Table 18 for more information
- you are logged in to the EMS server as root or as an authorized user to run the Software Upgrade Automation Tool. If logging in as an authorized user, ensure that the proper user authorization permissions have been set; see "DLP 100 Prepare the software".

- when using SNMP version 1 or version 2C, community string is configured on your EMS
- the correct version of the Software Upgrade Automation Tool is installed on the EMS server; see the Customer Release Notes for your release to determine which version of the Software Upgrade Automation Tool you must use

24.4   Procedure

Use this procedure to verify the operational and readiness status of the system on one or more nodes and to compare the operational status of the nodes before and after a software upgrade, software migration, or database migration. All the steps are performed using UNIX or LINUX.

Caution — When verifying the operational readiness and status of multiple NEs, all the NEs listed in *hosts_filename* must have:

- a common CLI username
- a common CLI password
- a common TL1 username
- a common TL1 password
- a common SFTP password

Note 1 — The command, although spanning multiple lines, is a single command. To run the command, enter it in its entirety before pressing Enter. You can also enter the command in sections if needed; for example, if your terminal settings prevent you from entering a long command. To split the command over multiple lines, enter a backslash (\) then press Enter at the end of each command section, and press Enter at the end of the command.

Note 2 — Command parameters in square brackets indicate optional parameters.

1   To run the automated system readiness verification tool:

a   To verify the system readiness for a single NE, enter:

```
./preCheck.pl --isam nt_ip_address --swp OSWPpath/OSWPnamexx.yyy
--logfile readinesslogpath/logname [--cliusername CLIuser]
[--clipassword CLIpwd] [--sftpusername SFTPuser]
[--ntdbtool NTDBpath] [--lanxtool SHubpath] [--ivpstool xVPSpath]
[--seplog │ --noseplog] [--debug] [--multi] [--comm commstring]
[--noping] [--v2] [--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--btype <SNMP│YANG>]
```

where
nt_ip_address is the IP address of the NT unit
OSWPpath/OSWPname is the path and filename of the new OSWP package (suffix = AA if not minimized and ZA if minimized); see "TNG 108 Overall SoftWare Package concept" for more information about the OSWP filename
xx is the 2-digit ISAM software release number
yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)
readinesslogpath/logname is the path and filename of the automated system readiness verification log file

CLIuser is your CLI username if it differs from the CLI username specified in the configuration file

CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file

SFTPuser is your SFTP username if it differs from the SFTP username specified in the configuration file

NTDBpath is the path of the NT database offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename

SHubpath is the path of the SHub offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename

xVPSpath is the path and filename of the xVPS offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename

commstring is the SNMP community string used by the automated system readiness verification tool when communicating with an NT unit using SNMP version 1 or version 2C

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

btype is the type to select the use of SNMP or YANG build

b To verify the system readiness on multiple NEs, enter:

```
./preCheck.pl --swp OSWPpath/OSWPnamexx.yyy --hosts hosts_filename
--sessions #sessions --logfile  readinesslogpath/logname
[--cliusername CLIuser] [--clipassword CLIpwd] [--sftpusername
SFTPuser] [--ntdbtool NTDBpath] [--lanxtool SHubpath]
[--ivpstool xVPSpath] [--seplog | --noseplog] [--debug] [--multi]
[--comm commstring][--noping] [--v2]
[--v3auth  auth_username:auth_pwd:auth_protocol]
[--v3priv  priv_protocol:priv_pwd] [--btype <SNMP|YANG>]
```

where

OSWPpath/OSWPname is the path and filename of the new OSWP package (suffix = AA if not minimized and ZA if minimized); see "TNG 107 Network element management" for more information about the OSWP filename

xx is the 2-digit ISAM software release number

yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046)

hosts_filename is the file with the IP addresses of the nodes when you verify the system readiness of multiple nodes; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information about the hosts file

#sessions is the number of parallel sessions to verify the system readiness of multiple nodes; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information

readinesslogpath/logname is the path and filename of the automated system readiness verification log file

CLIuser is your CLI username if it differs from the CLI username specified in the configuration file

CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file

SFTPuser is your SFTP username if it differs from the SFTP username specified in the configuration file

NTDBpath is the path of the NT database offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename

SHubpath is the path of the SHub offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename

xVPSpath is the path and filename of the xVPS offline migration tool if it differs from the default path and filename; see "DLP 100 Prepare the software" for the default path and filename

commstring is the SNMP community string used by the automated system readiness verification tool when communicating with an NT unit using SNMP version 1 or version 2C

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

btype is the type to select the use of SNMP or YANG build

2   To run the automated system status verification tool:

> **i**
>
> **Note —** Use the --pre parameter when running the automated system
> status verification tool before performing an upgrade, migration, or any
> other operation, and the --post parameter when running the tool after the
> operation.

a   To verify the system status of a single NE, enter:

```
./statusCheck.pl --isam nt_ip_address --logfile verlogpath/logname
--pre │ --post [--cliusername CLIuser] [--clipassword CLIpwd]
[--tl1username TL1user] [--tl1password TL1pwd]
[--release Rxx.yy.zz] [--ontreleasemap releasemappath] [--seplog │
--noseplog] [--debug] [--multi] [--comm commstring] [--bufsiz
buffersize] [--checks checks] [--telnetto tovalue] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd]
```

where
nt_ip_address is the IP address of the NT unit
verlogpath/logname is the path and filename of the automated system status verification log file
CLIuser is your CLI username if it differs from the CLI username specified in the configuration file
CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file
TL1user is your TL1 username if it differs from the TL1 username specified in the configuration file
TL1pwd is your TL1 password if it differs from the TL1 password specified in the configuration file
xx.yy.zz is the 6-digit ONT software release number (for example, R04.00.10)
releasemappath is the path of the server directory that contains the ONT release map
commstring is the SNMP community string used by the automated system status verification tool when communicating with an NT unit using SNMP version 1 or version 2C
buffersize is the internal buffer size in Mbytes for the CLI commands results
checks is the name of the checks to run; see "TNG 106 Additional automated tools" for more information
tovalue is the timeout value for the Telnet session, in seconds
auth_username is the SNMP version 3 authentication username
auth_pwd is the SNMP version 3 authentication password (8 characters minimum)
auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)
priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)
priv_pwd is the SNMP version 3 privacy password

b   To verify the system status on multiple NEs, enter:

```
./statusCheck.pl --hosts hosts_filename --sessions #sessions
--logfile verlogpath/logname --pre │ --post [--cliusername CLIuser]
[--clipassword CLIpwd] [--tl1username TL1user]
[--tl1password TL1pwd] [--release Rxx.yy.zz] [--ontreleasemap
releasemappath] [--seplog │ --noseplog] [--debug] [--multi]
[--comm commstring] [--bufsiz buffersize] [--checks checks]
[--telnetto tovalue] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd]
```

where
hosts_filename is the file with the IP addresses of the NEs when you verify the system status of multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information about the hosts file
#sessions is the number of parallel sessions to verify the system status of multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information

verlogpath/logname is the path and filename of the automated system status verification log file
CLIuser is your CLI username if it differs from the CLI username specified in the configuration file
CLIpwd is your CLI password if it differs from the CLI password specified in the configuration file
TL1user is your TL1 username if it differs from the TL1 username specified in the configuration file
TL1pwd is your TL1 password if it differs from the TL1 password specified in the configuration file
xx.yy.zz is the 6-digit ONT software release number (for example, R04.00.10)
releasemappath is the path of the server directory that contains the ONT release map
commstring is the SNMP community string used by the automated system status verification tool when communicating with an NT unit using SNMP version 1 or version 2C
buffersize is the internal buffer size in Mbytes for the CLI commands results
checks is the name of the checks to run; see "TNG 106 Additional automated tools" for more information
tovalue is the timeout value for the Telnet session, in seconds
auth_username is the SNMP version 3 authentication username
auth_pwd is the SNMP version 3 authentication password (8 characters minimum)
auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)
priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)
priv_pwd is the SNMP version 3 privacy password

3 To run the automated system status comparison tool:

Note — You must have two sets of results from the automated system status verification tool in order to run the automated system status comparison tool:

- one set obtained using the --pre parameter in the automated system status verification tool
- one set obtained using the --post parameter in the automated system status verification tool

a To compare the results of system status verifications done on a single NE, enter:

```
./statusCheckCmp.pl --isam nt_ip_address
--logfile cmplogpath/logname [--ontreleasemap releasemappath]
[--warn threshold] [--seplog | noseplog] [--debug] [--multi]
[--detail] [--incltoos] [--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd]
```

where
nt_ip_address is the IP address of the NT
cmplogpath/logname is the path and filename of the automated system status comparison log file
releasemappath is the path of the server directory that contains the ONT release map
threshold is the maximum number of operation failures that can occur before the script stops; see "TNG 105 ONT automated tools" for more information
commstring is the SNMP community string used by the automated system status verification tool when communicating with an NT unit using SNMP version 1 or version 2C
auth_username is the SNMP version 3 authentication username
auth_pwd is the SNMP version 3 authentication password (8 characters minimum)
auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)
priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)
priv_pwd is the SNMP version 3 privacy password

b   To verify the results of system status verification done on multiple NEs, enter:

```
./statusCheckCmp.pl --hosts hosts_filename --sessions #sessions
--logfile cmplogpath/logname [--ontreleasemap releasemappath]
[--warn threshold] [--seplog | noseplog] [--debug] [--multi]
[--detail] [--incltoos] [--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd]
```

where

hosts_filename is the file with the IP addresses of the NEs when you verify the system status of multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information about the hosts file

#sessions is the number of parallel sessions to verify the system status of multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information

cmplogpath/logname is the path and filename of the automated system status verification log file

releasemappath is the path of the server directory that contains the ONT release map

threshold is the maximum number of operation failures that can occur before the script stops; see "TNG 105 ONT automated tools" for more information

commstring is the SNMP community string used by the automated system status verification tool when communicating with an NT unit using SNMP version 1 or version 2C

auth_username is the SNMP version 3 authentication username

auth_pwd is the SNMP version 3 authentication password (8 characters minimum)

auth_protocol is the SNMP version 3 authentication protocol (SHA or MD5)

priv_protocol is the SNMP version 3 privacy protocol (DES, 3DES, or AES)

priv_pwd is the SNMP version 3 privacy password

4   STOP. This procedure is complete.

Training (TNG)

3HH-10318-AAAA-TCZZA

25 TNG 100 Software Upgrade Automation Tool

25.1 Introduction

This TNG provides general information about the Software Upgrade Automation Tool. This chapter contains the following information.

- Prerequisites
- Components of the Software Upgrade Automation Tool
- Installing and using the components of the Software Upgrade Automation Tool
    - Installing a new version of the Software Upgrade Automation Tool
    - Single and multiple sessions
    - Transfer protocols and top directory
    - Session protocols
    - Using SNMP
- Configuration file
- Callable scripts
- Hosts file
- Log files

Table 14 lists additional software management information provided in this document.

Table 14   **Additional software management information**

Title	See Chapter
TNG 107 Network element management	32
TNG 108 Overall SoftWare Package concept	33
TNG 109 Software database processes	34
TNG 110 Descriptor files	35

25.2 Prerequisites

Before you run any of the components of the Software Upgrade Automation Tool, ensure that:

- the EMS is connected to the applicable NEs
- you have write access to the EMS TFTP server used to store the files transferred by TFTP; see "Configuration file" for information about configuring this server for the Software Upgrade Automation Tool

- you have the proper permissions to run the Software Upgrade Automation Tool. You must be logged in as root or as an authorized user to run the Software Upgrade Automation Tool; see "DLP 100 Prepare the software" for information about authorizing users to run the Software Upgrade Automation Tool.
- you have Perl script version 5.0, 5.6, or 5.8 installed on the EMS TFTP server
- These automated tools are Perl scripts installed and run from an EMS server. When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.
- you have SNMP version 1, version 2C, or version 3. When using SNMP version 1 or version 2C, community string must be configured on the EMS; see "Using SNMP" for more information about SNMP.
- the components of the Software Upgrade Automation Tool are available on the EMS TFTP server
- the ports for the Octopus application, UDP 23 and 928 to 939, are open if there is a firewall between the network management stations and the ISAM network; see "Installing and using the components of the Software Upgrade Automation Tool" for more information
- for any customized login profiles, the prompt, if defined, has a trailing space
- it is recommended that terminal timeout and Idle timeout values are not to set less than 1 minute (or 60 seconds)

> **Note —** Nokia recommends that CLI and TL1 users using the Software Upgrade Automation Tool are assigned full read and write privileges to ensure all the CLI and TL1 commands used in the components of the Software Upgrade Automation Tool can be run without problems.

25.3   Components of the Software Upgrade Automation Tool

Table 15 lists the components of the Software Upgrade Automation Tool.

Table 15   **Components of the Software Upgrade Automation Tool**

Name	Command	Function	See chapter
Automated parameter configuration tool	Config.pl [2]	Creates and updates the configuration file	25
Automated ONT software download tool	ontDownloadandActivate.pl	Downloads ONT software from one or more NEs to the ONTs connected to these NEs	30
Automated ONT software staging tool	stageont.pl	Downloads the ONT software to one or more NEs for staging.	30
Automated software download tool	swdl.pl [2]	Downloads NE software to one or more NEs.	26
Automated software upgrade tool	upgrade.pl [2]	Upgrades software on one or more NEs.	27

(1 of 2)

Name	Command	Function	See chapter
Automated software migration tool	migrate.pl [2]	Migrates software on one or more NEs.	28
Automated software commitment tool	commit.pl [2]	Commits NE software on one or more NEs.	29
Automated software minimization tool	MinimizeSWP.pl	Reduces the size of an OSWP.	31
Automated software rollback tool	rollback.pl	Rolls back the software.	36
Automated system readiness verification tool	preCheck.pl [2]	Verifies the operational status of one or more NEs.	31
Automated system status verification tool	statusCheck.pl [2]	Verifies the operational readiness of one or more NEs for an upgrade or migration	31
Automated system status comparison tool	statusCheckCpm.pl	Compares the results of the automated system status verification tool.	31
Automated file clean-up tool	cleanUp.pl	Deletes the temporary files and folders created during an upgrade or migration	31
NCNC-C to NCNC-E reconfiguration tool [1]	cvtNcncC2E.pl	Reconfigures an NCNC-C NTIO unit when replacing it with an NCNC-E NTIO unit	31

(2 of 2)

Notes

[1]   This script does not apply to the 7360 ISAM FX and the 7356 ISAM FTTB in stand-alone mode.

[2]   A second password option is supported for this script.

25.3.1   Global parameters and log files for the automated tools

The global parameters used by the components of the Software Upgrade Automation Tool are contained in a common configuration file; see "Configuration file".

The results for each tool, session, and NE are saved in log files; see "Log files".

25.3.2   Finding the version number of the automated tools

You can find the version number for an automated tool by running the command with the --v parameter. For example:

```
migrate.pl --v
```

The output from this command shows the version of the automated tool as well as the versions of the applications used by the automated tool.

25.4   Using the second CLI password option

From R4.5.02 onward, where applicable, you can set the option to use a second CLI password for CLI over SSH configurations only. The second CLI password can be used when the first CLI password fails to connect to one or more NEs.

Table 15 specifies the command scripts that support the use of a second CLI password for CLI over SSH configurations.

When the Config.pl script is running, an additional configuration option appears on the screen to allow you to set a second CLI password. You will be prompted to enter 'Y' or 'N' to using a second CLI password applicable for CLI over SHH configurations only. This value is encrypted in the configuration file.

25.5   Installing and using the components of the Software Upgrade Automation Tool

The components of the Software Upgrade Automation Tool are installed on and run from the following EMS server: 5520 AMS.

Warning 1 — When there is a firewall between the network management stations and the ISAM network, the following UDP ports must be opened on the firewall to prevent failures when upgrading, migrating, or troubleshooting the system:

- UDP port 23 (destination port)
- UDP ports 928 to 939 (source and destination ports)

Warning 2 — Remote access for the debug port (UDP port 23) must be enabled to prevent failures when upgrading, migrating, or troubleshooting the system; see the *CLI Commands* or the *TL1 Commands and Messages* document for your product for information about enabling remote access on this port.

See the NTPs and DLPs in this document for the procedures to install and run the components of the Software Upgrade and Automation Tool.

This section contains the following information about installing and using components of the Software Upgrade Automation Tool:

- Installing a new version of the Software Upgrade Automation Tool
- Single and multiple sessions
- Transfer protocols and top directory
- Session protocols
- Using SNMP

25.5.1 Installing a new version of the Software Upgrade Automation Tool

If you already have a version of the Software Upgrade Automation Tool installed on your EMS server, you can replace the existing version by the new version, or install the new version in a separate directory.

Note — Ensure that the person installing the new version of the tool is logged in as root or is part of the Software Upgrade Automation Tool group account; see "DLP 100 Prepare the software".

When replacing an existing version of the Software Upgrade Automation Tool by a new version, use one of the following methods.

- If you don't need to keep any of the files created by the current version of the Software Upgrade Automation Tool, delete the contents of the directory in which the current version of the Software Upgrade Automation Tool is installed then install the new version in this directory using the steps in "DLP 100 Prepare the software".
- If you want to keep the files created by the current version of the Software Upgrade Automation Tool (for example, the configuration file param.cfg or the results from the automated system status verification tool), extract the new version of the Software Upgrade Automation Tool in the directory in which the current version is installed (see "DLP 100 Prepare the software"). All files common between the two versions of the Software Upgrade Automation Tool are replaced by the newer version of these files, and all other files are untouched.

Note — When using the second method, Nokia recommends that:

- the user updating of the Software Upgrade Automation Tool be the same user that installed the previous version of the tool
- you run the automated parameter configuration tool after updating the Software Upgrade Automation Tool, answering No to the first prompt. The version number stored in the configuration file is updated and any new prompts in the latest version of the tool are displayed

25.5.2 Single and multiple sessions

All components of the Software Upgrade Automation Tool can be used on a single NE.

Some components of the Software Upgrade Automation Tool can also be used on multiple NEs using a single session or multiple parallel sessions. When using multiple parallel sessions:

- Each session is assigned a number of NEs, and runs until all its assigned NEs have been processed, or an NE fails to restart properly after a reboot.
- The maximum number of parallel sessions for each component of the Software Upgrade Automation Tool is set in the configuration file; see Table 18.

Table 16 lists the components of the Software Upgrade Automation Tool that can be used on multiple NEs and the default maximum number of sessions in the configuration file for each tool.

Table 16   **Maximum number of parallel sessions**

Tool name	Command	Maximum number of parallel sessions [1]
Automated software download tool	swdl.pl	5
Automated software upgrade tool	upgrade.pl	3
Automated software migration tool	migrate.pl	3
Automated software commitment tool	commit.pl	5
Automated software rollback tool	rollback.pl	5
Automated ONT software staging tool	stageont.pl	5
Automated ONT software download tool	ontDownloadandActivate.pl	5
Automated system readiness verification tool	preCheck.pl	5
Automated system status verification tool	statusCheck.pl	5
Automated system status comparison tool	statusCheckCmp.pl	10

Note

[1]   Default value in the configuration file. This value can be changed using the automated parameter configuration tool; see "Configuration file".

25.5.3   Transfer protocols and top directory

The Automated Software Upgrade Tool uses the transfer protocol configured for the system. Files and folders are stored relative to a top directory and the working directory (defined using the automated parameter configuration tool). The top directory used by the Software Upgrade Automation Tool (referred to as *topdir* in the procedures of this document) depends on the transfer protocol.

When using TFTP/SFTP/FTP:

- The top directory is the TFTP top directory defined using the automated parameter configuration tool.
- All directory paths are relative to the TFTP top directory.

Note — SFTP is strongly recommended to be used for downloading Software to the ISAM since the SFTP protocol has built-in checks that check that the file is correctly transferred to the Network Element.

See the *Operations and Maintenance Using CLI* or the *Operations and Maintenance Using TL1* for your product for information about configuring general security settings, including how to configure the file transfer server for FTP or SFTP, and see "Configuration file" for more information about the working directory.

The components of the Automated Software Upgrade Tool verify where the OSWP is stored on the EMS library. If this location is not compatible with the transfer protocol configured for the system, the tools terminates and displays an error message.

Note — The OSWP provided in the software package is configured for TFTP. If you are using FTP or SFTP for file transfer, you must change the configured server location in the OSWP; see the EMS documentation for more information.

25.5.4   Session protocols

The Software Upgrade Automation Tool automatically determines which session protocol to use based on the SSH access configuration of the system for CLI and TL1. Table 17 lists the SSH access configuration options for CLI and TL1 and the session protocol used by the Software Upgrade Automation Tool for each option.

Table 17   **Session protocol options for Software Upgrade Automation Tool**

SSH access configuration options	Description	Session protocol used by Software Upgrade Automation Tool
Options for CLI		
ssh	CLI only allowed over SSH [1]	SSH for CLI sessions
telnet	CLI only allowed over Telnet	Telnet for CLI sessions
telnet-ssh	CLI allowed over Telnet and SSH	
Options for TL1		
none	TL1 not allowed	No TL1 data retrieval (alarm section empty)
ssh	TL1 only allowed over SSH	SSH for TL1 data retrieval
udp	TL1 only allowed over UDP	UDP for TL1 data retrieval (using port 13001)
udp-ssh	TL1 allowed over UDP and SSH	

Note
[1]   A second password option is supported for this configuration environment.

To ensure a secure connection, Nokia recommends that

- you configure all NEs as known NEs for the system (the NEs are listed in the /etc/ssh/ssh_known_hosts and username/.ssh/known_hosts files). This will prevent the connection to a NE from being refused.
- the system administrator generate the key pair and copy it to the environment of all users that need to access the ISAM using SSH
- SSH users using the Software Upgrade Automation Tool are assigned full read and write privileges to ensure all the CLI commands used in the components of the Software Upgrade Automation Tool can be run without problems.

> **Warning —** SSH Known Hosts file Automatic update:
>
> This feature can be enabled by adding the below feature flag to the PBMT configuration file, so that the PBMT scripts will dynamically add or modify the ISAM NE in the SSH known hosts file
>
> UPD_KNOWN_HOST_FILE="Y"
>
> By default the above setting will not be present in PBMT Configuration file
>
> The customer MAY use this feature at its OWN risk. Nokia strongly recommends against the use and will not be held responsible in case of security issues (Man In The Middle Attack) when this feature is being used.

See the *Operations and Maintenance Using CLI* or the *Operations and Maintenance Using TL1* for your product for information about configuring SSH.

25.5.5   Using SNMP

The Software Upgrade Automation Tool supports the following SNMP versions:

- version 1
- version 2C
- version 3

SNMP version 1 is enabled by default. You can enable SNMP version 2C or version 3 using the following methods:

- to enable SNMP version 2C or version 3 for all components of the Software Upgrade Automation Tool, use the automated parameter configuration tool; see "Configuration file" for more information
- to enable SNMP version 2C or version 3 for one only instance of a tool, use the appropriate parameter or parameters when running the tool; see the TNG for the tool for more information

When you enable SNMP version 2C or version 3, SNMP version 1 is automatically disabled.

> **Note —** When using SNMP version 3, Nokia recommends enabling full
> access to the NT MIB.

25.6   Configuration file

The configuration file (param.cfg) contains the global parameters used by the components of the Software Upgrade Automation Tool. The configuration file is created and updated using the automated parameter configuration tool. You must run the automated parameter configuration tool before you can use any of the components of the Software Upgrade Automation Tool. The configuration file parameters can be updated by re-running the automated parameter configuration tool.

> **Note 1 —** When updating the configuration file parameters, use "" to
> reset a parameter to an empty string.
>
> **Note 2 —** These automated tools are Perl scripts installed and run from
> an EMS server. When using the 5520 AMS, the perl script must be run as
> $AMS_PERL_DIR/perl <scriptname>.pl.

The syntax of the automated parameter configuration tool is:

Config.pl

or

perl Config.pl

For each parameter, the automated parameter configuration tool describes the parameter and prompts for a value. Table 18 lists the parameters that can be set using the automated parameter configuration tool and shows the related tool parameters, if any. The parameters are listed in the order they appear when running the automated parameter configuration tool.

Table 18   **Parameter prompts for the automated parameter configuration tool**

Parameter prompt	Description	Default value	Related tool parameter
Modify existing configuration?	Enter Y to change any of the configuration file settings, or N to exit the automated parameter configuration tool. This prompt is only displayed if there is an existing configuration file, that is, if you have run the automated parameter configuration tool at least once.	N	—

(1 of 10)

Parameter prompt	Description	Default value	Related tool parameter
Hosts filename	The name of the file listing the NEs when you use a component of the Software Upgrade Automation Tool using multiple sessions. See "Hosts file" for more information.	/etc/hosts	--hosts [1]
Directory for status result files	The absolute path and name of the directory used to store the results of the tools. The results for each NE are stored in a separate NE-specific subdirectory.	./	—
TFTP top directory name	The path and name of the TFTP top directory used to store the files transferred by TFTP. This is always the root directory on the EMS TFTP server. You need write access to this directory to perform a migration. For the 5520 AMS, use the directory specified in the 5523 AWS Administrator Guide or the 7302 ISAM | 7330 ISAM FTTN | 7356 ISAM FTTB | 7360 ISAM FX Operations and Maintenance Using the 5520 AMS guide. This parameter is ignored when the transfer protocol configured for the system is FTP or SFTP; see "Transfer protocols and top directory" for more information.	—	—
Working directory name	The path and name of the working directory for the files created by the components of the Software Upgrade Automation Tool, relative to the top directory used by the Software Upgrade Automation Tool; see "Transfer protocols and top directory" for more information. Nokia recommends that you do not keep important files in this directory. Some components of the Software Upgrade Automation Tool will delete the contents of this folder to ensure proper operation.	tmp	—
Maximum number of parallel software upgrades or migrations	The maximum number of parallel sessions you can have for the following components of the Software Upgrade Automation Tool: • automated software upgrade tool • automated software migration tool A high value may result in reduced network performance and increased software run time.	3	--sessions [2]
Maximum number of status check comparisons	The maximum number of parallel sessions you can have for the automated system status comparison tool. A high value may result in reduced network performance and increased software run time.	10	--sessions [2]

(2 of 10)

Parameter prompt	Description	Default value	Related tool parameter
Maximum number of parallel software downloads	The maximum number of parallel sessions you can have for the following components of the Software Upgrade Automation Tool: • automated software download tool • automated software commitment tool • automated ONT software staging tool • automated ONT software download tool • automated system readiness verification tool • automated system status verification tool A high value may result in reduced network performance and increased software run time.	5	--sessions [2]
CLI username	The CLI username used to connect to one or more NEs. This value is encrypted in the configuration file.	—	--cliusername [1]
CLI password	The CLI password used to connect to one or more NEs. This value is encrypted in the configuration file.	—	--clipassword [1]
Set Second CLI password (only applicable for CLI over SSH)	The second CLI password option is applicable only in the case when CLI over SSH is configured. Valid options are: • Y • N The second CLI password specifies an alternative password to be used to connect to the NE in the case of failure of the first password. This value is encrypted in the configuration file. When the 'Y' option is selected, the script will allow the second password to be set and will display a second prompt to enter the second password using the related tool parameter as follows: • parameter prompt: Second CLI password • related tool parameter: --clipassword2	N	— --clipassword2 [5]
TL1 username	The TL1 username used to connect to one or more NEs. This value is encrypted in the configuration file.	—	--tl1username [1]
TL1 password	The TL1 password used to connect to one or more NEs. This value is encrypted in the configuration file.	—	--tl1password [1]
SFTP username	The SFTP username used to connect to one or more NEs. This value is encrypted in the configuration file.	—	--sftpusername [1]
Configure SSH system-wide known hosts database	The path and name of the file on the system listing all known NEs; see "Session protocols" for more information.	/etc/ssh/ ssh_know n_hosts	—
Configure SSH user-specific known hosts database	The path and name of the file in the user directory listing all known NEs; see "Session protocols" for more information.	*username* /.ssh/ known_h osts	—

(3 of 10)

Parameter prompt	Description	Default value	Related tool parameter
Configure NT community string	When enabled, instructs the tool to configure the SNMP community string for SNMP version 1 or version 2C. Valid options are: • Yes - configure the SNMP community string; the NT community string prompt (see next row) is displayed • No - do not configure the SNMP community string; the NT community string prompt (see next row) is skipped	—	—
• NT community string	The SNMP version 1 or version 2C community string used by the Software Upgrade Automation Tool when communicating with an NT unit. This value is encrypted in the configuration file. This value must match the community string value configured on the NE. (3)	—	--comm (1)
Configure SNMPv2C?	When enabled, allows you to enable or disable SNMP version 2C. Valid options are: • Y - display the prompt to change the setting for SNMP version 2C (see next row) • N - skip the prompt to change the setting SNMP version 2C (see next row)	N	—
• Use SNMPv2C?	When enabled, instructs the tool to use SNMP version 2C for data transfers between the SNMP agent and the SNMP manager. Valid options are: • Yes - use SNMP version 2C • No - do not use SNMP version 2C This parameter prompt is only displayed if you entered Y at the Configure SNMPv2C? prompt.	N	--v2
Configure SNMPv3?	When enabled, instructs the tool to use SNMP version 3 for data transfers between the SNMP agent and the SNMP manager. Valid options are: • Yes - use SNMP version 3; the SNMP version 3 configuration prompts (see next rows) are displayed • No - do not use SNMP version 3; the SNMPV version 3 configuration prompts (see next rows) are skipped	N	--v3auth (1)
• Authentication protocol for SNMPv3	The authentication protocol used for SNMP version 3. Valid options are: • SHA • MD5 This parameter prompt is only displayed if you entered Y at the Configure SNMPv3? prompt.	MD5	--v3auth (1)
• Session authentication username	The authentication username for the SNMP version 3 session. This value is encrypted in the configuration file. This parameter prompt is only displayed if you entered Y at the Configure SNMPv3? prompt.	—	--v3auth (1)

(4 of 10)

Parameter prompt	Description	Default value	Related tool parameter
• Session authentication password	The authentication password for the SNMP version 3 session. The password must be at least 8 characters long. This value is encrypted in the configuration file. This parameter prompt is only displayed if you entered Y at the Configure SNMPv3? prompt.	—	--v3auth [1]
• Privacy protocol	The privacy protocol used for SNMP version 3. Valid options are: • DES • 3DES • AES This parameter prompt is only displayed if you entered Y at the Configure SNMPv3? prompt.	DES	--v3priv [1]
• Privacy password	The privacy password for the SNMP version 3 session. The password must be at least 8 characters long. This value is encrypted in the configuration file. This parameter prompt is only displayed if you entered Y at the Configure SNMPv3? prompt.	—	--v3priv [1]
Pre-upgrade script	The absolute path and filename of the pre-upgrade executable script; see "Callable scripts" for more information.	—	—
Telnet timeout	The timeout delay for the Telnet session to the NE, in seconds. Increase this value if you expect longer delays for your Telnet connection.	30	—
Post-upgrade script	The absolute path and filename of the post-upgrade executable script; see "Callable scripts" for more information.	—	—
Post-migration script	The absolute path and filename of the post-migration executable script; see "Callable scripts" for more information.	—	—
Pre-migration script	The absolute path and filename of the pre-migration executable script; see "Callable scripts" for more information.	—	—
Maximum time to wait	The maximum time that the Software Upgrade Automation Tool waits after an NE reset before declaring the NE unreachable, in seconds. Increase this value if you expect the NE restart time to be longer than the default value.	4000	—
Ping disabled in the network	Instructs the tool to use SNMP instead of ping to verify if the NE is reachable. Valid options are: • Y - disable ping • N - enable ping Enable this parameter when the use of ping is not allowed in the network.	N	--noping [1]

(5 of 10)

Parameter prompt	Description	Default value	Related tool parameter
Enable second OSWP activation if first one fails	Instructs the automated software migration tool to enable or disable the second OSWP activation. When this parameter is enabled, the automated software migration tool will attempt to activate the new OSWP a second time if the new OSWP has not been activated after a software migration. Valid options are: • Y - enable the second OSWP activation • N - disable the second OSWP activation Do not enable the second OSWP activation unless directed by Nokia personnel.	N	—
Enable hot reset remapping	Instructs the tool to enable or disable the NT hot reset before the OSWP activation during the procedure. Valid options are: • Y - enable NT hot reset • N - disable NT hot reset Do not enable the NT hot reset unless directed by Nokia personnel. If you enable the NT hot reset, ensure that all UDP ports are open before you run the tool. Note: this option will only work with Octopus and does not work with T&D via SSH	N	--remap [1]
Maximum time for ONT download	The maximum time the automated ONT software download tool waits for a response from an ONT before declaring the ONT unreachable, in seconds. Increase this value if you expect the ONT connection time to be longer than the default value.	1200	—
Maximum time for ONT activation	The maximum time the automated ONT software download tool waits after an ONT activation before declaring the ONT unreachable, in seconds. Increase this value if you expect the ONT activation time to be longer than the default value.	1200	—
ONT Download Progress Timer	The maximum time for software download on a single ONT in seconds. Increase this value if you expect the ONT software download time to be longer than the default value.	600	—
NT synchronization timeout	The maximum time the Software Upgrade Automation Tool waits after an NE reset in a redundant configuration (duplex NT) before declaring the NT unit synchronization a failure, in seconds. Increase this value if you expect the NT synchronization to take longer than the default value.	600	—
Bridge configuration mismatch percentage	The mismatch threshold of the bridge configuration data retrieved by the automated system status verification tool before and after a procedure, in percent. This parameter is used by the automated system status comparison tool; see "Automated system status verification and comparison tools" in "TNG 106 Additional automated tools".	0	--checks [4]

(6 of 10)

Parameter prompt	Description	Default value	Related tool parameter
LT out-of-service mismatch percentage	The mismatch threshold of the out-of-service LT unit data retrieved by the automated system status verification tool before and after a procedure, in percent. This parameter is used by the automated system status comparison tool; see "Automated system status verification and comparison tools" in "TNG 106 Additional automated tools".	0	--checks [4]
Line out-of-service configuration mismatch percentage	The mismatch threshold of the out-of-service lines data (not including the lines for out-of-service LT units) retrieved by the automated system status verification tool before and after a procedure, in percent. This parameter is used by the automated system status comparison tool; see "Automated system status verification and comparison tools" in "TNG 106 Additional automated tools".	5	--checks [4]
Authentication configuration mismatch percentage	The mismatch threshold of unauthenticated line data retrieved by the automated system status verification tool before and after a procedure, in percent. This parameter is used by the automated system status comparison tool; see "Automated system status verification and comparison tools" in "TNG 106 Additional automated tools".	5	--checks [4]
IP address of IP interface	The IP address associated with the physical interface used to communicate with high-availability NEs via SNMP. If not specified, the components of the Software Upgrade Automation Tool will use the IP address specified by the tool parameters. Only set this parameter when a high-availability system is used.	0.0.0.0	--haip [1]
Non-default ARBERGTAG setting?	When enabled, allows you to change the settings of ARBERGTAG for PPPoX relay. Valid options are: • Y - display the prompt to change the setting of ARBERGTAG for PPPoX relay (see next row) • N - skip the prompt to change the setting of ARBERGTAG for PPPoX relay (see next row)	N	—
• ARBERGTAG for PPPoX relay	The max-payload-tag parameter value for the CLI command `configure pppox-relay cross-connect` used by the automated software migration tool when the --confarberg option is enabled. Valid options are: 1 – insert ARBERGTAG for PPPoX relay 2 – do not insert ARBERGTAG for PPPoX relay This parameter prompt is only displayed if you entered Y at the Non-default ARBERGTAG setting? prompt.	2	--confarberg [4]
Non-default DHCP port identification?	When enabled, allows you to change the DHCP port identification settings. Valid options are: • Y - display the prompts to change the settings for DHCP port identification (see next rows) • N - skip the prompts to change the setting for DHCP port identification (see next rows)	N	—

(7 of 10)

Parameter prompt	Description	Default value	Related tool parameter
Customer-specific DHCP port numbering	The DHCP port numbering scheme for the CLI command `configure system port-num-in-proto` used by the automated software migration tool when the --confopt82 option is enabled. Valid options are: 1 – log-slot-num 2 – position-based 3 – type-based 4 – legacy-num This parameter prompt is only displayed if you entered Y at the Non-default DHCP port identification? prompt.	4	--confopt82 [4]
ATM-based port identification	The loop ID syntax for ATM-based lines for the CLI command `configure system loop-id-syntax` used by the automated software migration tool when the --confopt82 option is enabled. Must be a printable character string with a maximum of 64 characters. This parameter prompt is only displayed if you entered Y at the Non-default DHCP port identification? prompt.	Access_Node_ID atm Rack/Frame/Slot/Port:VPI.VCI	--confopt82 [4]
Ethernet-based port identification	The loop ID syntax for Ethernet-based lines for the CLI command `configure system loop-id-syntax` used by the automated software migration tool when the --confopt82 option is enabled. Must be a printable character string with a maximum of 64 characters. This parameter prompt is only displayed if you entered Y at the Non-default DHCP port identification? prompt.	Access_Node_ID eth Rack/Frame/Slot/Port:VPI.VCI	--confopt82 [4]
Ethernet-based-pon port identification	The loop ID syntax for Ethernet-based-pon lines for the CLI command *configure system loop-id-syntax* used by the automated software migration tool when the --confopt82 option is enabled. Must be a printable character string with a maximum of 80 characters. This parameter prompt is only displayed if you entered Y at the Non-default DHCP port identification? prompt.	Access_Node_ID eth Rack/Frame/Slot/Port	--confopt82 [4]
Ethernet-based-epon port identification	The loop ID syntax for Ethernet-based-epon lines for the CLI command *configure system loop-id-syntax* used by the automated software migration tool when the --confopt82 option is enabled. Must be a printable character string with a maximum of 80 characters. This parameter prompt is only displayed if you entered Y at the Non-default DHCP port identification? prompt.	BrasAccess_Node_ID/Rack/Frame/Slot/Subslot/Port/ONTOft	--confopt82 [4]

(8 of 10)

Parameter prompt	Description	Default value	Related tool parameter
Directory and name of the IVPS inventory script	The absolute path and name of the 5520 AMS script used to return to IP addresses allocated to voice server units in an ISAM Voice system. Use /opt/ams/ams-*swversion*/bin/getIVPSBoardsInNE.pl, where *swversion* is the software version number of the 5520 AMS; see the 5520 AMS Customer Release Note for the 5520 AMS software version number.	/opt/ams/ams-*swversion*/bin/getIVPSBoardsInNE.pl	—
CDE profile directory	The path and name of the CDE profile directory, relative to the TFTP top directory. The CDE directory contains the CDE packages for the ISAM Voice. There should only be one CDE directory per system. This parameter is required when migrating an ISAM Voice system from Release 3.3 or later to Release 3.5 or later.	cde_profiles	—
New CDE file to be included in database	The filename of the new ISAM Voice CDE file on the EMS, relative to the CDE profile directory in the TFTP top directory. This parameter is required when migrating an ISAM Voice system from Release 3.3 or later to Release 3.5 or later.	—	—
CDE file currently loaded	The filename of the active ISAM Voice CDE file currently loaded on the system and the EMS, relative to the CDE profile directory in the TFTP top directory. This parameter is required when migrating an ISAM Voice system from Release 3.3 or later to Release 3.5 or later.	—	—
Access operator ID	The access operator ID used when upgrading or migrating an ISAM to Release 3.6 or later. Supported values are 0 to 65535. The access operator ID is automatically configured when the automated software upgrade tool or the automated software migration tool is used with the --oprid parameter.	0	--oprid [4]
Force access operator ID	When enabled, verifies that the access operator ID configured matches the operator ID assigned by Nokia.	N	—
CLI command line buffer	The internal buffer size for the CLI commands results, in Mbytes. Increase this value if the default size of the buffer is insufficient. The maximum supported value is 100 Mbytes.	15	--bufsiz [1]
Allow grouping of IGMP multicast entries	The allowed grouping of IGMP multicast entries is enabled by default.	1	--confmcastgrp
Gap size between mutlicast group IP addresses while grouping	The allowed gap size between multicast group IP addresses while grouping. Default is to allow consecutive entries.	0	--confgapsize
Migration interrupt on emergency-call feature	Indicates whether the migration interrupt on emergency-call feature is enabled or disabled	N	—

(9 of 10)

Parameter prompt	Description	Default value	Related tool parameter
Polling time to fetch the emergency-call alarm (seconds)	Maximum time (in seconds) for emergency-call alarm polling. Possible values - 1 to 1200 (seconds)	120	—
Wait time before retrying TL1 communication after SARB/SSTP (seconds)	Time (in seconds) of the retry timer for the TL1 command to be re-issued by the script when the System All Resource Busy (SARB) state or Status Stop (SSTP) state is encountered. Possible values; 5 to 600 (seconds)	60	—

(10 of 10)

Notes

(1) Using the tool parameter overrides the value in the configuration file.

(2) If the value of the --sessions parameter is higher than the value in the configuration file, the value in configuration file is used.

(3) See the *Operations and Maintenance Using CLI* or the *Operations and Maintenance Using TL1* for your product for information about configuring SNMP, including how to configure the community string on the NE.

(4) Instructs the tool to automatically configure the parameter using the settings in the configuration file.

(5) A second CLI password option can be set when configuring CLI over SSH to allow an alternate password when the the first password fails to connect to one or more NEs.

25.7   Callable scripts

You can run UNIX or LINUX scripts automatically before and after the automated software upgrade tool and the automated software migration tool by specifying the script name in the configuration file; see Table 18 for more information.

The callable scripts must conform to the following rules:

- The script is called by the following parameters.
    - --ip *IPaddress*

        where *IPaddress* is the IP address of the NE.
    - --logdir *dirname*

        where *dirname* is the path and name of the directory that contains the working files for the Software Upgrade Automation Tool, relative to the TFTP top directory defined in the configuration file.
- The script uses UNIX-like exit codes, where zero indicates success, and non-zero indicates failure.

Note 1 — The automated tool calling the script will continue running even if the called script results in a failure exit code.

Note 2 — A script cannot be called if there is an active connection to CLI on the NE.

25.8   Hosts file

The hosts file is used to list the IP addresses and names of the NEs when using a component of the Software Upgrade Automation Tool on multiple NEs. The hosts file must list the NEs in the standard UNIX or LINUX /etc/hosts file format.

Caution — When upgrading or migrating NEs in a subtending configuration, Nokia recommends that you upgrade or migrate all the subtended NEs before the subtending NE; see "NTP 100 Upgrade the software" and "NTP 101 Migrate the software" for more information.

If subtended NEs are listed in a hosts file, the subtending NE or NEs for these subtended NEs should not be listed in the same host file.

All the NEs listed in the hosts file must conform to the following:

- one line per NE, using the format <IP address in dotted-decimal format> <space> <NE name>
- each NE name must start with AS-
- all the NEs listed in the hosts file must have:
    - a common CLI username
    - a common CLI password
    - a common TL1 username
    - a common TL1 password
    - a common SFTP username

Note — The NE names are only used for logging in and for temporary files, and do not need to resolve to the IP addresses listed.

25.8.1   Example

The following is an example of a hosts file.

- 192.168.1.112 AS-7330-1
- 192.168.1.114 AS-7330-2
- 192.168.1.116 AS-7330-3

25.9   Log files

A number of log files are generated by the components of the Software Upgrade Automation Tool.

25.9.1   Software Upgrade Automation Tool log files

Each component of the Software Upgrade Automation Tool creates a tool log file, which you can use for troubleshooting in case of errors. The filename for the tool log file is specified by the *--logfile* parameter.

For example, when you migrate a single NE:

```
./migrate.pl --logfile migr_40.041.log --swp OSWP/L6GPAA40.041 --isam
138.120.217.112
```

The automated software migration tool creates following log file:

- migr_40_041.log; the log file for the automated software migration tool listing general data and settings for the tool. This is the general execution logfile.

In addition, other logfiles will be generated based on the parameters passed:

- Use following parameter for node/NE based logging:

  ```
  --seplog
  ```

  By default (or by passing *--seplog* as parameter), Node/NE based logfiles will be generated. Each NE log file is created in an NE-specific directory that is created in the TFTP top directory defined in the configuration file. The NE log filename has the format *toolname_yyyy-mm-dd_hh_mm*.log, where *toolname* is the name of the component of the Software Upgrade Automation Tool as it appears in the command prompt.
  Use the *--seplog* parameter to specifically enforce the default log behavior (one log file per NE, as described above).
  Examples:
    - swdl_2006-12-06_10:03.log is created when the automated software download tool was run on December 6, 2006 at 10:03 in the morning.
    - migrate_2007-03-24_17:10.log is created when the automated software migration tool was run on March 24, 2007 at 5:10 in the afternoon.
- Use following parameter for session based logging:

  ```
  --noseplog
  ```

  A session log file is created for each session when you use a component of the Software Upgrade Automation Tool or verify and compare the system status on multiple NEs. The filename for a session log file is *--logname_#*, where *logname* is the log filename specified by the *--logfile* parameter, and # is the session number, starting from zero, where zero is the first session, one is the second session, and so on. When you migrate a single NE, the session number for the session log filename is zero.
  You can use the *--noseplog* parameter to have all NE log information included in the appropriate session log file when running a tool using parallel sessions.

When you migrate multiple NEs using two parallel sessions:

```
./migrate.pl --logfile migr_40.041.log --swp OSWP/L6GPAA40.041 --sessions 2
--hosts /etc/hosts --noseplog
```

The automated software migration tool creates three log files:

- migr_40_041.log; the log file for the automated software migration tool; it lists general data and settings for the tool (the execution logfile)
- migr_40_041.log_0; the log file for the first session
- migr_40_041.log_1; the log file for the second session

25.9.2   Migration log files (for SHub-based systems only)

When you migrate an NE, additional log files are created by the offline database migration tools invoked by the automated software migration tool:

- logfile.log: the log file for the NT offline database migration tool
- trc.log: the trace log file for the NT offline database migration tool
- logfile*mmddyyyy_hhmmss*.txt: the log file for the SHub offline migration tool

These log files are located in the *topdir*/*workdir*/*nodeid* directory, where *topdir* is the top directory used by the Software Upgrade Automation Tool, *workdir* is the working directory defined in the configuration file, and *nodeid* is the IP address or name of the NE that was migrated. The directory also contains the uploaded and migrated databases for the NE, as well as a directory containing the new migrated database. See "Transfer protocols and top directory" for information about the top directory used by the Software Upgrade Automation Tool.

26 TNG 101 Automated software download tool

26.1 Introduction

This TNG provides information about the syntax and parameters of the automated software download tool used to download the NE software to the ISAM. See "TNG 100 Software Upgrade Automation Tool" for general information about the Software Upgrade Automation Tool, the configuration file, the hosts file and the log files. See "NTP 100 Upgrade the software" and "NTP 101 Migrate the software" for the steps to use the automated software download tool.

26.2 Automated software download tool

The automated software download tool is the component of the Software Upgrade Automation Tool used to download a new OSWP to one or more NEs. By default, only the software for planned and detected cards in the system is downloaded. To allow the download of software for cards not yet planned or installed, use the automated software minimization tool before downloading the software. When using the automated software minimization tool, the suffix of the OSWP name is changed to indicate that it is a minimized OSWP; see "TNG 106 Additional automated tools" for more information about the automated software minimization tool.

For Sealed Remotes (7367 ISAM SX/DX family), no software minimization is needed since there is always a fixed HW board present. During download of a new OSWP, only the relevant software files are copied to the board and the software minimization has no effect.

Warning — The automated software download tool will terminate if you have planned or detected cards in the system that are not supported by the software you are downloading. Always ensure that all the cards in your system are supported by the new software before upgrading, migrating, or converting the database on the NE.

You can force the software to download even if there are unsupported planned or detected cards in the system by using the --force option of the automated software download tool.

Note — From R4.5.02 onward, you can choose the option to use a second CLI password when using CLI over SSH configurations, in case the first CLI password should fail. See "TNG 100 Software Upgrade Automation Tool" for more information.

The automated software download tool automatically performs the following steps for each NE specified:

1   Logs in to the NE using CLI.

2   Acquires a transaction.

3   Retrieves the status of the active OSWP.

4　Commits the active OSWP if the OSWP is not in Committed state; this deletes the inactive OSWP.

5　Terminates any active download.

6　Verifies the size of the software partition.

7　Verifies that all the planned and detected cards in each NE specified are supported by the new OSWP. If one or more cards are not supported by the new OSWP, the procedure is terminated and an error message is displayed.

If the --force parameter is used, this step is skipped.

8　If the --reduce parameter is used, reduces the size of the active OSWP on the NT unit by deleting the unneeded software files in the package. If the OSWP size is reduced, the suffix of the OSWP name is renamed to RA to indicate that it is a reduced OSWP; see "TNG 108 Overall SoftWare Package concept" for more information.

9　Configures the download parameters.

10　Downloads the new OSWP.

11　Releases the transaction.

12　Logs out of the NE.

You can download software to either a single NE or to multiple NEs using a single session or multiple parallel sessions; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 101 Automated software download tool" for more information.

26.3　Command syntax

The syntax of the automated software download tool is:

Note — When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

```
./swdl.pl --isam nt_ip_address │ --hosts hosts_filename --sessions #sessions
--swp OSWPpath/OSWPnamexx.yyy --logfile swdllogpath/logname │ --id runid
[--ont ONTswpath] [--cliusername CLIuser] [--clipassword CLIpwd]
[--clipassword2 SecondCLIpwd][--reduce] [--force] [--seplog │ --noseplog]
[--continue] [--debug] [--multi] [--noname] [--comm commstring] [--haip]
[--noping] [--v2] [--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--v] [--btype <SNMP│YANG>]
```

or

```
perl swdl.pl --isam nt_ip_address │ --hosts hosts_filename
--sessions #sessions --swp OSWPpath/OSWPnamexx.yyy
--logfile swdllogpath/logname │ --id runid [--ont ONTswpath]
[--cliusername CLIuser] [--clipassword CLIpwd] [--reduce] [--force]
[--seplog │ --noseplog] [--continue] [--debug] [--multi] [--noname] [--comm
commstring] [--haip] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--v] [--btype <SNMP│YANG>]
```

26.4 Command parameters

Table 19 describes the parameters of the automated software download tool.

Table 19 **Automated software download tool parameters**

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--isam *nt_ip_address*	The IP address or name of the NE when you download software to a single NE. When this parameter is used, the automated software download tool downloads the software to only the NE specified by the --isam parameter, and ignores the --sessions and --hosts parameters. [1]	Mandatory	—
--hosts *hosts_filename*	The file listing the IP addresses and names of the NEs when you download software to multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information This parameter is ignored if the --isam parameter is used. [1]	—	Mandatory
--sessions *#sessions*	The number of parallel sessions when you download software to multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in TNG 25 for more information. This parameter is ignored if the --isam parameter is used. This value cannot exceed the value set for the maximum number of parallel software downloads in the configuration file; see Table 18 for more information.	—	Mandatory
--swp *OSWPpath*/*OSWPnamexx.yyy*	The location and filename of the new OSWP. *OSWPpath*/*OSWPname* is the path and filename of the new OSWP package. When minimized, the OSWP suffix is ZA; see "TNG 108 Overall SoftWare Package concept" for more information. *xx* is the 2-digit ISAM software release number. *yyy* is the 3-digit ISAM software package number (for example, L6GPAA40.046).	Mandatory	Mandatory
--logfile *swdllogpath/logname*	The path and filename of the resulting log file. When this parameter is used, the --id parameter is ignored.	Mandatory	Mandatory

(1 of 4)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--id *runid*	This parameter is used by the 5529 LRM instead of the --logfile parameter to generate a log file and a result file when you download software to a single NE. This parameter cannot be used when you download software to multiple NEs. The filenames of the resulting files are *runid*_SWDL.log and *runid*_SWDL.result, where *runid* is the 5529 LRM run identification number. This parameter is ignored if the --logfile parameter is used.	—	—
--ont *ONTswpath*	The location the ONT software on the EMS server. *ONTswpath* is the path of the server directory that contains the ONT software.	—	—
--cliusername *CLIuser*	The CLI username if different from the one specified in the configuration file; see Table 18 for more information. When downloading software to multiple NEs, all the NEs must have a common CLI username.	Optional	Optional
--clipassword *CLIpwd* --clipassword2 *SecondCLIpwd*	The CLI password, if different from the one specified in the configuration file; see Table 18 for more information. When downloading software to multiple NEs, all the NEs must have the a common CLI password. The second CLI password will be used only in the case when CLI over SSH is configured. The second CLI password specifies an alternative password to be used when the first CLI password fails to connect to one or more NEs. This value is encrypted in the configuration file.	Optional	Optional
--reduce	Instructs the automated software download tool to reduce the size of the active OSWP on the NT unit [2].	Optional	Optional
--force	Overrides the download path and software compatibility checks and performs the download.	Optional	Optional
--seplog	--noseplog	Determines where the log information is stored for each NE listed in the hosts file. Use --seplog to create a separate log file for each NE listed in the hosts file, and --noseplog to create a single log file for all sessions. See "Log files" in "TNG 100 Software Upgrade Automation Tool" for more information about log files.	—	Optional

(2 of 4)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--continue	Instructs the automated software download tool to skip to the next NE if a fatal error is encountered instead of stopping the download session.	—	Optional
--debug	Instructs the automated software download tool to add additional troubleshooting information to the log file.	Optional	Optional
--multi	Allows multiple UNIX or LINUX users access to each NE. When this parameter is used, a working directory is created for each user that connects to the NE. The name of the working directory is the UNIX or LINUX username for the corresponding user. Nokia recommends that only one user connects to an NE at a time.	Optional	Optional
--noname	Instructs the automated software download tool to use the IP address of the NE when creating the output directory, instead of the NE name. This parameter is used by the 5529 LRM.	—	—
--comm *commstring*	The SNMP community string used by the automated software download tool when communicating with an NT unit using SNMP version 1 or version 2C. When this parameter is not specified, the tool uses the NT community string value defined in the configuration file; see Table 18 for more information.	Optional	Optional
--haip *haipaddress*	The IP address associated with the physical interface used to communicate with high-availability NEs via SNMP. If this parameter is not used, the automated software download tool uses the IP address of IP interface parameter in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool" for more information. [3]	Optional	Optional
--noping	Instructs the tool to use SNMP instead of ping to verify if the NE is reachable. Use this parameter when the use of ping is not allowed in the network.	Optional	Optional
--v2	Instructs the tool to use SNMP version 2C instead of version 1 for data transfers between the SNMP agent and the SNMP manager.	Optional	Optional

(3 of 4)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--v3auth *auth_username*: *auth_pwd*:*auth_protocol*	Instructs the tool to use SNMP version 3 instead of version 1 for data transfers between the SNMP agent and the SNMP manager. *auth_username* is the session authentication username, *auth_pwd* is the authentication password (at least 8 characters long), and *auth_protocol* is the authentication protocol (SHA or MD5).	Optional	Optional
--v3priv *priv_protocol*:*priv_pwd*	Sets the privacy protocol (DES, 3DES, or AES) and the privacy password (at least 8 characters long) for SNMP version 3.	Optional	Optional
--v	Instructs the automated software download tool to show the version number of the tool. The output shows the version of the automated tool as well as the versions of the applications used by the tool.	Optional	Optional
--btype	Instructs to use SNMP or YANG build type	Optional	Optional

(4 of 4)

Notes

(1)   If neither the --isam or --host parameter is used, the tool will download software to all the NEs listed in the hosts file specified in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool".

(2)   The name of the OSWP is changed to indicate that this is a reduced OSWP; see "TNG 108 Overall SoftWare Package concept" for more information.

(3)   If the IP address of IP interface parameter in the configuration file is 0.0.0.0, the tool uses the IP address specified by the --isam or --hosts parameter.

26.5   Examples

The following is an example of the automated software download tool command for a single NE download:

```
./swdl.pl --isam 138.120.217.112 --swp OSWP/L6GPAA40.041 --logfile
dl_40.041.log
```

The following is an example of the automated software download tool command for a multiple NE download:

```
./swdl.pl --swp OSWP/L6GPAA40.041 --sessions 2 --hosts /etc/hosts --logfile
dl_40.041.log
```

27 TNG 102 Automated software upgrade tool

27.1 Introduction

This TNG provides information about the syntax and parameters of the automated software upgrade tool used to upgrade the ISAM software. See "TNG 100 Software Upgrade Automation Tool" for general information about the Software Upgrade Automation Tool, the configuration file, the callable scripts, the hosts file and the log files. See "NTP 100 Upgrade the software" for the steps to use the automated software upgrade tool.

27.2 Automated software upgrade tool

The automated software upgrade tool is the component of the Software Upgrade Automation Tool used to upgrade one or more NEs after the new OSWP has been downloaded. The automated software upgrade tool automatically performs the following steps for each NE specified:

1 Runs the pre-upgrade script specified in the configuration file, if any; see "Callable scripts" in "TNG 100 Software Upgrade Automation Tool" for more information.

2 Verifies the connection to the NE.

3 Opens an SNMP session, disabling object identifier translation.

4 Logs in to the NE using CLI.

5 Retrieves the status of the active OSWP. Terminates the upgrade if:

- the NE is already running the release specified by the new OSWP name
- the new OSWP has not been downloaded

6 If the --oprid parameter is used, configures the access operator ID using the value defined in the configuration file.

7 Activates the new OSWP and resets the NT units, LT units, and ONTs.

8 When the NE is back up again, verifies that the active OSWP is the correct version.

9 Logs out of the NE.

10 Runs the post-upgrade script specified in the configuration file, if any; see "Callable scripts" in "TNG 100 Software Upgrade Automation Tool" for more information.

You can upgrade software on either a single NE or on multiple NEs using a single session or multiple parallel sessions; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information.

Note 1 — To perform an upgrade, you must have write access to the TFTP top directory defined in the configuration file; see "Transfer protocols and top directory" in "TNG 100 Software Upgrade Automation Tool" for more information.

Note 2 — From R4.5.02 onward, you can choose the option to use a second CLI password when using CLI over SSH configurations, in case the first CLI password should fail. See "TNG 100 Software Upgrade Automation Tool" for more information.

27.3   Command syntax

The syntax of the automated software upgrade tool is:

Note — When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

```
./upgrade.pl --isam nt_ip_address | --hosts hosts_filename
--sessions #sessions --swp OSWPpath/OSWPnamexx.yyy
--logfile upgradelogpath/logname | --id runid [--cliusername CLIuser]
[--clipassword CLIpwd] [--clipassword2 SecondCLIpwd][--force]
[--seplog | --noseplog] [--continue] [--debug] [--multi] [--noname] [--comm
commstring] [--haip haipaddress] [--oprid] [--remap] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--v] [--btype <SNMP|YANG>]
```

or

```
perl upgrade.pl --isam nt_ip_address | --hosts hosts_filename --sessions
#sessions --swp OSWPpath/OSWPnamexx.yyy
--logfile upgradelogpath/logname | --id runid [--cliusername CLIuser]
[--clipassword CLIpwd] [--force] [--seplog | --noseplog] [--continue]
[--debug] [--multi] [--noname] [--comm commstring] [--haip haipaddress]
[--oprid] [--remap] [--noping][--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--v] [--btype <SNMP|YANG>]
```

27.4   Command parameters

Table 20 describes the parameters of the automated software upgrade tool.

Table 20   **Automated software upgrade tool parameters**

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--isam *nt_ip_address*	The IP address or name of the NE when you upgrade software on a single NE only. When this parameter is used, the automated software upgrade tool upgrades only the software in the NE specified by the --isam parameter, and ignores the --sessions and --hosts parameters. [1]	Mandatory	—
--hosts *hosts_filename*	The file listing the IP addresses and names of the NEs when you upgrade software on multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information [1] This parameter is ignored if the --isam parameter is used. [1]	—	Mandatory
--sessions *#sessions*	The number of parallel sessions when you upgrade software on multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information. This parameter is ignored if the --isam parameter is used. This value cannot exceed the value set for the maximum number of parallel software upgrades or migrations in the configuration file; see Table 18.	—	Mandatory
--swp OSWP/*OSWPnamexx.yyy*	The location and filename of the new OSWP. *OSWPpath*/*OSWPname* is the path and filename of the new OSWP package. When minimized, the OSWP suffix is ZZ; see "TNG 108 Overall SoftWare Package concept" for more information. *xx* is the 2-digit ISAM software release number. *yyy* is the 3-digit ISAM software package number (for example, L6GPAA40.046).	Mandatory	Mandatory
--logfile *upgradelogpath/logname*	The path and filename of the resulting log file. When this parameter is used, the --id parameter is ignored.	Mandatory	Mandatory

(1 of 4)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--id *runid*	This parameter is used by the 5529 LRM instead of the --logfile parameter to generate a log file and a result file when you upgrade software on a single NE. This parameter cannot be used when you upgrade software on multiple NEs. The filenames of the resulting files are *runid*_UPGR.log and *runid*_UPGR.result, where *runid* is the 5529 LRM run identification number. This parameter is ignored if the --logfile parameter is used.	—	—
--cliusername *CLIuser*	The CLI username if different from the one specified in the configuration file; see Table 18 for more information. When upgrading software on multiple NEs, all the NEs must have a common CLI username.	Optional	Optional
--clipassword *CLIpwd* --clipassword2 *SecondCLIpwd*	The CLI password, if different from the one specified in the configuration file; see Table 18 for more information. When upgrading software on multiple NEs, all the NEs must have a common CLI password. The second CLI password will be used only in the case when CLI over SSH is configured. The second CLI password specifies an alternative password to be used when the first CLI password fails to connect to one or more NEs. This value is encrypted in the configuration file.	Optional	Optional
--force	Overrides the upgrade path checks and performs the upgrade.	Optional	Optional
--seplog | --noseplog	Determines where the log information is stored for each NE listed in the hosts file. Use --seplog to create a separate log file for each NE listed in the hosts file, and --noseplog to create a single log file for all sessions. See "Log files" in "TNG 100 Software Upgrade Automation Tool" for more information about log files.	—	Optional
--continue	Instructs the automated software upgrade tool to skip to the next NE if a fatal error is encountered instead of stopping the upgrade session.	—	Optional
--debug	Instructs the automated software tool to add additional troubleshooting information to the log file.	Optional	Optional

(2 of 4)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--multi	Allows multiple UNIX or LINUX users access to each NE. When this parameter is used, a working directory is created for each user that connects to the NE. The name of the working directory is the UNIX username for the corresponding user. Nokia recommends that only one user connects to an NE at a time.	Optional	Optional
--noname	Instructs the automated software upgrade tool to use the IP address of the NE when creating the output directory, instead of the NE name. This parameter is used by the 5529 LRM.	—	—
--comm *commstring*	The SNMP community string used by the automated software upgrade tool when communicating with an NT unit using SNMP version 1 or version 2C. When this parameter is not specified, the tool uses the NT community string value specified in the configuration file; see Table 18 for more information.	Optional	Optional
--haip *haipaddress*	The IP address associated with the physical interface used to communicate with high-availability NEs via SNMP. If this parameter is not used, the automated software migration tool uses the IP address of IP interface parameter in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool" for more information. [2]	Optional	Optional
--oprid	Instructs the tool to automatically configure the access operator ID using the value defined in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool" for more information.	Optional	Optional
--remap	Instructs the tool to disable the NT hot reset during the upgrade procedure. When using this parameter, ensure that all UDP ports are open. Do not use this parameter unless directed by Nokia personnel. Note: this option will only work with Octopus and does not work with T&D via SSH	Optional	Optional
--noping	Instructs the tool to use SNMP instead of ping to verify if the NE is reachable. Use this parameter when the use of ping is not allowed in the network.	Optional	Optional
--v2	Instructs the tool to use SNMP version 2C for data transfers between the SNMP agent and the SNMP manager.	Optional	Optional

(3 of 4)

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--v3auth *auth_username*:*auth_pwd*:*auth_protocol*	Instructs the tool to use SNMP version 3 for data transfers between the SNMP agent and the SNMP manager. *auth_username* is the session authentication username, *auth_pwd* is the authentication password (at least 8 characters long), and *auth_protocol* is the authentication protocol (SHA or MD5).	Optional	Optional
--v3priv *priv_protocol*:*priv_pwd*	Sets the privacy protocol (DES, 3DES, or AES) and the privacy password (at least 8 character long) for SNMP version 3.	Optional	Optional
--v	Instructs the automated software upgrade tool to show the version number of the tool. The output shows the version of the automated software upgrade tool as well as the versions of the applications used by the tool.	Optional	Optional
--btype	Instructs to use SNMP or YANG build type	Optional	Optional

(4 of 4)

Notes
[1]   If neither the --isam or --host parameter is used, the tool will upgrade software to all the NEs listed in the hosts file specified in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool".

[2]   If the IP address of IP interface parameter in the configuration file is 0.0.0.0, the tool uses the IP address specified by the --isam or --hosts parameter.

27.5   Examples

The following is an example of the automated software upgrade tool command for a single NE upgrade:

```
./upgrade.pl --swp OSWP/L6GPAA40.041 --isam 138.120.217.112 --logfile
upgr_40.041.log
```

The following is an example of the automated software upgrade tool command for a multiple NE upgrade:

```
./upgrade.pl --swp OSWP/L6GPAA40.041 --sessions 3 --hosts /etc/hosts
--logfile upgr_40.041.log
```

28 TNG 103 Automated software migration tool

28.1 Introduction

This TNG provides information about the syntax and parameters of the automated software migration tool used to migrate the ISAM software. See "TNG 100 Software Upgrade Automation Tool" for general information about the Software Upgrade Automation Tool, the configuration file, the callable scripts, the hosts file and the log files. See "NTP 101 Migrate the software" for the steps to use the automated software migration tool.

28.2 Automated software migration tool

The automated software migration tool is the component of the Software Upgrade Automation Tool used to migrate one or more NEs after the new OSWP has been downloaded. The automated software migration tool automatically performs the following steps for each NE specified:

Note — For 7363 ISAM MX and 7367 ISAM SX/DX, there is only a NT database.

1 Runs the pre-migration script specified in the configuration file, if any; see "Callable scripts" in "TNG 100 Software Upgrade Automation Tool" for more information.

2 Verifies if there are ISAM Voice components on the system.

3 Verifies the connection to the NE.

4 Opens an SNMP session, disabling object identifier translation.

5 Logs in to the NE using CLI.

6 Retrieves the status of the active OSWP. Terminates the migration if:

- the NE is already running the release specified by the new OSWP name
- the new OSWP has not been downloaded

7 Verifies the current software load version, and terminates the migration if the automated software migration tool does not support migration from that release.

8 Retrieves the SFP assignment information.

9 Saves the SHub database.

10 Creates the temporary directory for the migration files.

11 If the --oprid parameter is used, configures the access operator ID using the value defined in the configuration file.

12 Uploads the NT database.

13 Backs up the NT and SHub databases.

14 Migrates the NT database.

15 Migrates the SHub database.

16 If there are ISAM Voice components in the system, migrates the database for each ISAM Voice server unit.

17 Combines the migrated databases.

18 Downloads the new database to the NE.

19 Waits 120 s for the databases to synchronize (only performed for redundant systems).

20 Activates the new OSWP and resets the NT units, LT units, and ONTs.

21 When the NE is back up again, verifies that the active OSWP is the correct version.

22 Restores the SFP assignment retrieved in Step 8.

23 If the --ttl0fwd parameter is used, reconfigures the SHub VRF to allow forwarding of packets with TTL = 0.

24 Logs out of the NE.

25 Runs the post-migration script specified in the configuration file, if any; see "Callable scripts" in "TNG 100 Software Upgrade Automation Tool" for more information.

You can migrate software on either a single NE or on multiple NEs using a single session or multiple parallel sessions; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information.

Warning — The SHub database is automatically saved 10 min after a successful migration. If a manual system reset is required within this 10 min time frame, you must manually save the SHub database before resetting the system, using the following CLI command:

```
admin software-mngt shub database save
```

Note 1 — To perform a migration, you must have write access to the TFTP top directory defined in the configuration file; see "Transfer protocols and top directory" in "TNG 100 Software Upgrade Automation Tool" for more information.

Note 2 — From R4.5.02 onward, you can choose the option to use a second CLI password when using CLI over SSH configurations, in case the first CLI password should fail. See "TNG 100 Software Upgrade Automation Tool" for more information.

28.2.1   Migration of ISAM Voice

When migrating an ISAM Voice system, you must enter the following parameters in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool".

> **Note —** For 7367 ISAM SX/DX, this migration is not applicable as ISAM Voice is not supported.

- the filename of the CDE currently loaded in the system
- the filename of the new CDE file to be included in the database

If you do not specify these parameters, the migration will fail.

28.3   Command syntax

The syntax of the automated software migration tool is:

> **Note —** When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

```
./migrate.pl --isam nt_ip_address │ --hosts hosts_filename
--sessions #sessions --swp OSWPpath/OSWPnamexx.yyy
--logfile migratelogpath/logname │ --id runid [--cliusername CLIuser]
[--clipassword CLIpwd] [--clipassword2 SecondCLIpwd][--ntdbtool NTDBpath]
[--lanxtool SHubpath] [--ivpstool xVPSpath] [--force]
[--seplog │ --noseplog] [--continue] [--debug] [--multi] [--noname] [--comm
commstring] [--v] [--oflonly] [--intlnwvlan nwvlanid] [--ssmoutvlan
ssmoutvlanid] [--singleRestart] [--bwreduce] [--toecntc legacy │ native]
[--noact] [--actonly] [--secureDbSave waittime] [--confopt82] [--confarberg]
[--confmcastgrp] [--confgapsize] [--cap] [--ttl0fwd vrfid]
[--ofldb nttype│source-release│database] [--tonantb] [--haip haipaddress]
[--remap] [--oprid] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol][--v3priv priv_protocol:priv
_pwd] [--btype <SNMP│YANG>] [--gpononurngmd]
```

or

```
perl migrate.pl --isam nt_ip_address │ --hosts hosts_filename --sessions
#sessions --swp OSWPpath/OSWPnamexx.yyy
--logfile migratelogpath/logname │ --id runid [--cliusername CLIuser]
[--clipassword CLIpwd] [--ntdbtool NTDBpath] [--lanxtool SHubpath]
[--ivpstool xVPSpath] [--force] [--seplog │ --noseplog] [--continue]
[--debug] [--multi] [--noname] [--comm commstring] [--v] [--oflonly]
[--intlnwvlan nwvlanid] [--ssmoutvlan ssmoutvlanid] [--singleRestart]
[--bwreduce] [--toecntc legacy │ native] [--noact] [--actonly]
[--secureDbSave waittime] [--confopt82] [--confarberg] [--confmcastgrp]
[--confgapsize] [--cap] [--ttl0fwd vrfid]
[--ofldb nttype│source-release│database] [--tonantb] [--haip haipaddress]
[--remap] [--oprid] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--btype <SNMP│YANG>] [--gpononurngmd]
```

28.4 Command parameters

Table 21 describes the parameters of the automated software migration tool.

Table 21 **Automated software migration tool parameters**

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--isam *nt_ip_address*	The IP address or name of the NE when you migrate software on a single NE only. When this parameter is used, the automated software migration tool migrates only the software on the NE specified by the --isam parameter, and ignores the --sessions and --hosts parameters. [1]	Mandatory	—
--hosts *hosts_filename*	The file listing the IP addresses and names of the NEs when you migrate software on multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information This parameter is ignored if the --isam parameter is used. [1]	—	Mandatory
--sessions *#sessions*	The number of parallel sessions when you migrate software on multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information. This parameter is ignored if the --isam parameter is used. This value cannot exceed the value set for the maximum number of parallel software upgrade or migrations in the configuration file; see Table 18 for more information.	—	Mandatory
--swp OSWP/*OSWPnamexx.yyy*	The location and filename of the new OSWP. *OSWPpath*/*OSWPname* is the path and filename of the new OSWP package. When minimized, the OSWP suffix is ZA; see "TNG 108 Overall SoftWare Package concept" for more information. *xx* is the 2-digit ISAM software release number. *yyy* is the 3-digit ISAM software package number (for example, L6GPAA40.046).	Mandatory	Mandatory
--logfile *migratelogpath/logname*	The path and filename of the resulting log file. When this parameter is used, the --id parameter is ignored.	Mandatory	Mandatory

(1 of 7)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--id *runid*	This parameter is used by the 5529 LRM instead of the --logfile parameter to generate a log file and a result file when you migrate software on a single NE. This parameter cannot be used when you migrate software on multiple NEs. The filenames of the resulting files are *runid*_MIGR.log and *runid*_MIGR.result, where *runid* is the 5529 LRM run identification number. This parameter is ignored if the --logfile parameter is used.	—	—
--cliusername *CLIuser*	The CLI username if different from the one specified in the configuration file; see Table 18 for more information. When migrating software on multiple NEs, all the NEs must have a common CLI username.	Optional	Optional
--clipassword *CLIpwd* --clipassword2 *SecondCLIpwd*	The CLI password, if different from the one specified in the configuration file; see Table 18 for more information. When migrating software on multiple NEs, all the NEs must have a common CLI password. The second CLI password will be used only in the case when CLI over SSH is configured. The second CLI password specifies an alternative password to be used when the first CLI password fails to connect to one or more NEs. This value is encrypted in the configuration file.	Optional	Optional
--ntdbtool *NTDBpath*	The location of the NT database offline migration tool when different from the default location; see "DLP 100 Prepare the software" for the default location. *NTDBpath* is the directory path of the NT database migration tool.	Optional	Optional
--lanxtool *SHubpath*	The location of the SHub migration tool when different from the default location; see "DLP 100 Prepare the software" for the default location. *SHubpath* is the directory path of the LANX migration tool.	Optional	Optional
--ivpstool *xVPSpath*	The location of the xVPS migration tool when different from the default location and filename; see "DLP 100 Prepare the software" for the default location and filename. *xVPSpath* is the path and filename of the migration tool.	Optional	Optional
--force	Overrides the migration path checks and performs the migration.	Optional	Optional

(2 of 7)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--seplog | --noseplog	Determines where the log information is stored for each NE listed in the hosts file. Use --seplog to create a separate log file for each NE listed in the hosts file, and --noseplog to create a single log file for all sessions. See "Log files" in "TNG 100 Software Upgrade Automation Tool" for more information about log files.	—	Optional
--continue	Instructs the automated software migration tool to skip to the next NE if a fatal error is encountered instead of stopping the migration session.	—	Optional
--debug	Instructs the automated software migration tool to add additional troubleshooting information to the log file.	Optional	Optional
--multi	Allows multiple UNIX or LINUX users access to each NE. When this parameter is used, a working directory is created for each user that connects to the NE. The name of the working directory is the UNIX or LINUX username for the corresponding user. Nokia recommends that only one user connects to an NE at a time.	Optional	Optional
--noname	Instructs the automated software migration tool to use the IP address of the NE when creating the output directory, instead of the NE name. This parameter is used by the 5529 LRM.	—	—
--comm *commstring*	The SNMP community string used by the automated software migration tool when communicating with an NT unit using SNMP version 1 or version 2C. When this parameter is not specified, the tool uses the NT community string value specified in the configuration file; see Table 18 for more information.	Optional	Optional
--v	Instructs the automated software migration tool to show the version number of the tool. The output shows the version of the automated software migration tool as well as the versions of the applications used by the tool.	Optional	Optional
--oflonly	Instructs the automated software migration tool not to download the database. This is used when, for example, you need to replace a physical card on-site, then manually download and activate the database later. Note: this parameter is dependent on the parameter ofldb	Optional	Optional

(3 of 7)

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--intlnwvlan *nwvlanid*	Instructs the tool to change the network VLAN ID of a system with a NANT-D NT board from the default value of 4089 to the value specified by *nwvlanid*, where *nwvlanid* is a value from 1 to 4087 that is not already used for another VLAN ID in the system. This parameter is only used during migration to Release 4.1 a NANT-D system in which VLAN ID 4089 is already used, and is ignored for target releases other than Release 4.1 for NANT-D systems.	Optional	Optional
--ssmoutvlan *ssmoutvlanid*	Instructs the tool to change the SSM out VLAN ID of a system with a board from the default value of 4088 to the value specified by *ssmoutvlanid*, where *ssmoutvlanid* is a value from 1 to 4087 that is not already used for another VLAN ID in the system. This parameter is only used during migration to Release 4.3 on a system in which VLAN ID 4088 is already used, and is ignored for target releases other than Release 4.3.	Optional	Optional
--singleRestart	This parameter is obsolete.	—	—
--bwreduce	Instructs the automated software migration tool to reduce the bandwidth to the NE when migrating the software. This can prevent potential traffic problems.	Optional	Optional
--toecntc legacy|native	This parameter is not used in the ETSI market.	—	—
--toecnte legacy|native	This parameter is not used in the ETSI market.	—	—
--noact	Instructs the automated software migration tool to stop after the database has been downloaded to the NE. After a migration with the --noact parameter is done, another migration must be performed with the --actonly parameter enabled to active the new OSWP.	Optional	Optional
--actonly	Instructs the automated software migration tool to activate the database. This parameter is used to activate the new OSWP after a migration with the --noact parameter is performed.	Optional	Optional
--secureDbSave *waittime*	This parameter is obsolete.	—	—

(4 of 7)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--confopt82	Instructs the automated software migration tool to configure DHCP option 82 using the values defined by the following configuration file parameters; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool" for more information. • DHCP port identification • ATM-based port identification • Ethernet-based port identification If this parameter is not specified, the default DHCP option 82 settings for the system are used.	Optional	Optional
--confarberg	Instructs the automated software migration tool to use the max-payload-tag value for the PPPoX cross-connect engine that is defined by the ARGBERGTAG settings parameter in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool" for more information. If this parameter is not specified, the default max-payload-tag setting for the system is used.	Optional	Optional
--confmcastgrp	Allows grouping of IGMP multicast entries enabled by default. Default value is 1 (enabled).	Optional	Optional
--confgapsize	Allows gap size between multicast group IP addresses while grouping. Default value is 0 (allows consecutive entries).	Optional	Optional
--cap	Generates a list of the supported versions for the NT and SHub offline migration tools and of the supported releases for the NT units. Do not use this parameter unless directed by Nokia personnel.	Optional	Optional
--check	Verified that the NT and SHub offline migration tools were supported by the Software Upgrade Automation Tool. This parameter is obsolete.	—	—
--ttl0fwd *vrfid*	Instruct the automated software migration tool to reconfigure the SHub VRF to allow forwarding of packets with TTL = 0. Note: This parameter is only applicable for SHub-based systems.	Optional	Optional

(5 of 7)

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--ofldb *nttype|source-release|database*	Instructs the automated software migration tool to use the uploaded database when migrating the software to a single NE. The parameter value elements are: • *nttype*: the name of the NT unit, for example, nant-a • *source-release*: the source release, for example, L6GPAA40.213 • *database*: the absolute path and filename of the uploaded database Note: This parameter is typically used for testing purposes.	Optional	Optional
--tonantb	This parameter is obsolete.	—	—
--haip *haipaddress*	The IP address associated with the physical interface used to communicate with high-availability NEs via SNMP. If this parameter is not used, the automated software migration tool uses the IP address of IP interface parameter in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool" for more information. [2]	Optional	Optional
--oprid	Instructs the tool to automatically configure the access operator ID using the value defined in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool" for more information.	Optional	Optional
--remap	Instructs the tool to disable the NT hot reset during the migration procedure. When using this parameter, ensure that all UDP ports are open. Do not use this parameter unless directed by Nokia personnel. Note: this option will only work with Octopus and does not work with T&D via SSH	Optional	Optional
--noping	Instructs the tool to use SNMP instead of ping to verify if the NE is reachable. Use this parameter when the use of ping is not allowed in the network.	Optional	Optional
--v2	Instructs the tool to use SNMP version 2C for data transfers between the SNMP agent and the SNMP manager.	Optional	Optional
--v3auth *auth_username*: *auth_pwd*:*auth_protocol*	Instructs the tool to use SNMP version 3 for data transfers between the SNMP agent and the SNMP manager. *auth_username* is the session authentication username, *auth_pwd* is the authentication password (at least 8 characters long), and *auth_protocol* is the authentication protocol (SHA or MD5).	Optional	Optional

(6 of 7)

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--v3priv *priv_protocol*:*priv_pwd*	Sets the privacy protocol (DES, 3DES, or AES) and the privacy password (at least 8 characters long) for SNMP version 3.	Optional	Optional
--btype	Instructs to use SNMP or YANG build type	Optional	Optional
--gpononurngmd	The parameter "gpononurngmd 1" instructs the automated software migration tool to set the range-mode for GPON ports to "alientolerant". This parameter only applies when migrating from a release older than ISR53 to a release ISR53 or higher. It does not apply to other PON technologies (XGS-PON, TWDM-PON, EPON). In case the parameter is not used or the value is set to "0", the GPON range-mode will be set to the default value "normal".	Optional	Optional

(7 of 7)

Notes
[1]   If neither the --isam or --host parameter is used, the tool will migrate software to all the NEs listed in the hosts file specified in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool".

[2]   If the IP address of IP interface parameter in the configuration file is 0.0.0.0, the tool uses the IP address specified by the --isam or --hosts parameter.

28.5   Examples

The following is an example of the automated software migration tool command for a single NE migration:

```
./migrate.pl --swp OSWP/L6GPAA40.041 --isam 138.120.217.112 --logfile
migr_40.041.log
```

The following is an example of the automated software migration tool command for a multiple NE migration:

```
./migrate.pl --swp OSWP/L6GPAA40.041 --sessions 2 --hosts /etc/hosts
--logfile migr_40.041.log
```

29 TNG 104 Automated software commitment tool

29.1 Introduction

This TNG provides information about the syntax and parameters of the automated software commitment tool used to commit the ISAM software after a software upgrade or migration. See "TNG 100 Software Upgrade Automation Tool" for general information about the Software Upgrade Automation Tool, the configuration file, the hosts file and the log files. See "NTP 100 Upgrade the software" and "NTP 101 Migrate the software" for the steps to use the automated software migration tool.

29.2 Automated software commitment tool

The automated software commitment tool is the component of the Software Upgrade Automation Tool used to commit the software on one or more NEs after a software upgrade or migration.

> **Caution —** Nokia does not recommend committing the software until you are ready to move to the next release of software. If you need to commit the software before the next release, ensure that the system is up and running, traffic has resumed, and you are satisfied with the performance of the new release before committing the software. You cannot roll back to a previous load after the software is committed. The previous load is deleted.

The automated software commitment tool automatically performs the following steps for each NE specified:

1   Verifies the connection to the NE.

2   Opens an SNMP session, disabling object identifier translation.

3   Logs in to the NE using CLI.

4   Verifies if the active software load is the expected software load version.

5   Commits the active OSWP.

6   Logs out of the NE.

You can commit software on either a single NE or on multiple NEs using a single session or multiple parallel sessions; see "Installing and using the components of the Software Upgrade Automation Tool" in TNG 29 for more information.

> **Note 1 —** To commit software, you must have write access to the TFTP top directory defined in the configuration file; see Table 18 for more information.

> **Note 2 —** From R4.5.02 onward, you can choose the option to use a second CLI password when using CLI over SSH configurations, in case the first CLI password should fail. See "TNG 100 Software Upgrade Automation Tool" for more information.

29.3   Command syntax

The syntax of the automated software commitment tool is:

> **Note —** When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

```
./commit.pl --isam nt_ip_address │ --hosts hosts_filename
--sessions #sessions --swp OSWPpath/OSWPnamexx.yyy
--logfile commitlogpath/logname │ --id runid [--cliusername CLIuser]
[--clipassword CLIpwd] [--clipassword2 SecondCLIpwd][--force] [--seplog │
--noseplog] [--debug] [--multi] [--noname] [--comm commstring] [--noping]
[--v2] [--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--v]
```

or

```
perl commit.pl --isam nt_ip_address │ --hosts hosts_filename --sessions
#sessions --swp OSWPpath/OSWPnamexx.yyy
--logfile commitlogpath/logname │ --id runid [--cliusername CLIuser]
[--clipassword CLIpwd] [--clipassword2 SecondCLIpwd] [--force] [--seplog │
--noseplog] [--debug] [--multi] [--noname] [--comm commstring] [--noping]
[--v2] [--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--v]
```

29.4   Command parameters

Table 22 describes the parameters of the automated software commitment tool.

Table 22 **Automated software commitment tool parameters**

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--isam *nt_ip_address*	The IP address or name of the NE when you commit software on a single NE only. When this parameter is used, the automated software commitment tool commits only the software on the NE specified by the --isam parameter, and ignores the --sessions and --hosts parameters. [1]	Mandatory	—
--hosts *hosts_filename*	The file listing the IP addresses and names of the NEs when you commit software on multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information This parameter is ignored if the --isam parameter is used. [1]	—	Mandatory
--sessions *#sessions*	The number of parallel sessions when you commit software on multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information. This parameter is ignored if the --isam parameter is used. This value cannot exceed the value set for the maximum number of parallel software downloads parameter in the configuration file; see Table 18 for more information.	—	Mandatory
--swp OSWP/*OSWPnamexx.yyy*	The location and filename of the new OSWP. *OSWPpath*/*OSWPname* is the path and filename of the new OSWP package. When minimized, the OSWP suffix is ZA; see "TNG 108 Overall SoftWare Package concept" for more information. *xx* is the 2-digit ISAM software release number. *yyy* is the 3-digit ISAM software package number (for example, L6GPAA40.046).	Mandatory	Mandatory
--logfile *commitlogpath/logname*	The path and filename of the resulting log file. When this parameter is used, the --id parameter is ignored.	Mandatory	Mandatory

(1 of 3)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--id *runid*	This parameter is used by the 5529 LRM instead of the --logfile parameter to generate a log file and a result file when you commit software on a single NE. This parameter cannot be used when you commit software on multiple NEs. The filenames of the resulting files are *runid*_COMT.log and *runid*_COMT.result, where *runid* is the 5529 LRM run identification number. This parameter is ignored if the --logfile parameter is used.	—	—
--cliusername *CLIuser*	The CLI username if different from the one specified in the configuration file; see Table 18 for more information. When committing software on multiple NEs, all the NEs must have a common CLI username.	Optional	Optional
--clipassword *CLIpwd* --clipassword2 *SecondCLIpwd*	The CLI password, if different from the one specified in the configuration file; see Table 18 for more information. When committing software on multiple NEs, all the NEs must have a common CLI password. The second CLI password will be used only in the case when CLI over SSH is configured. The second CLI password specifies an alternative password to be used when the first CLI password fails to connect to one or more NEs. This value is encrypted in the configuration file.	Optional	Optional
--force	Overrides the software commitment path checks and commits the software.	Optional	Optional
--seplog | --noseplog	Determines where the log information is stored for each NE listed in the hosts file. Use --seplog to create a separate log file for each NE listed in the hosts file, and --noseplog to create a single log file for all sessions. See "Log files" in "TNG 100 Software Upgrade Automation Tool" for more information about log files.	—	Optional
--debug	Instructs the automated software commitment tool to add additional troubleshooting information to the log file.	Optional	Optional
--multi	Allows multiple UNIX or LINUX users access to each NE. When this parameter is used, a working directory is created for each user that connects to the NE. The name of the working directory is the UNIX or LINUX username for the corresponding user. Nokia recommends that only one user connects to an NE at a time.	Optional	Optional

(2 of 3)

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--noname	Instructs the automated software commitment tool to use the IP address of the NE when creating the output directory, instead of the NE name. This parameter is used by the 5529 LRM.	—	—
--comm *commstring*	The SNMP community string used by the automated software commitment tool when communicating with an NT unit using SNMP version 1 or version 2C. When this parameter is not specified, the tool uses the NT community string value specified in the configuration file; see Table 18 for more information.	Optional	Optional
--noping	Instructs the tool to use SNMP instead of ping to verify if the NE is reachable. Use this parameter when the use of ping is not allowed in the network.	Optional	Optional
--v2	Instructs the tool to use SNMP version 2C for data transfers between the SNMP agent and the SNMP manager.	Optional	Optional
--v3auth *auth_username*:*auth_pwd*:*auth_protocol*	Instructs the tool to use SNMP version 3 for data transfers between the SNMP agent and the SNMP manager. *auth_username* is the session authentication username, *auth_pwd* is the authentication password (at least 8 characters long), and *auth_protocol* is the authentication protocol (SHA or MD5).	Optional	Optional
--v3priv *priv_protocol*:*priv_pwd*	Sets the privacy protocol (DES, 3DES, or AES) and the privacy password (at least 8 characters long) for SNMP version 3.	Optional	Optional
--v	Instructs the automated software commitment tool to show the version number of the tool. The output shows the version of the automated tool as well as the versions of the applications used by the tool.	Optional	Optional

(3 of 3)

Note

(1)   If neither the --isam or --host parameter is used, the tool will commit software to all the NEs listed in the hosts file specified in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool".

29.5   Examples

The following is an example of the automated software commitment tool command for a single NE software commitment:

```
./commit.pl --swp OSWP/L6GPAA40.041 --isam 138.120.217.112 --logfile
commit_40.041.log
```

The following is an example of the automated software commitment tool command for a multiple NE software commitment:

```
./commit.pl --swp OSWP/L6GPAA40.041 --sessions 2 --hosts /etc/hosts
--logfile commit_40.041.log
```

30 TNG 105 ONT automated tools

30.1 Introduction

This TNG provides information about the syntax and parameters of the following components of the Software Upgrade Automation Tool:

- Automated ONT software staging tool
- Automated ONT software download tool

See "TNG 100 Software Upgrade Automation Tool" for general information about the Software Upgrade Automation Tool, the configuration file, the hosts file and the log files.

Note — This TNG is not applicable to 7363 ISAM MX and 7367 ISAM SX/DX.

30.2 Automated ONT software staging tool

The automated ONT software staging tool is the component of the Software Upgrade Automation Tool used to download the new ONT software to the NE, that is, to stage the ONT software. See "DLP 110 Stage the ONT software" for the steps to use the automated ONT software staging tool.

Note — The ONT software must be staged on the NE before it can be downloaded to the ONTs connected to that NE.

The automated ONT software staging tool automatically performs the following steps for the specified NE or NEs.

1   Verifies the connection to the NE.

2   Opens an SNMP session, disabling object identifier translation.

3   Logs in to the NE using TL1.

4   Retrieves the list of required ONT software files for the ONT types specified by the --onttypes parameter from the ONT release map.

5   Retrieves the list of ONT software available on the NE.

6   If a required ONT software file is available on the NE, compares the software file on the NE with the software file on the server specified by the --servdir parameter, and deletes the software file on the NE if it is not the latest one.

7   Logs out of the NE.

8   Opens an FTP, SFTP, or TFTP session with the NE.

9   Downloads the required ONT software files that are not already available on the NE from the
     server directory specified by the --servdir parameter to the NE.

10   Closes the FTP, SFTP, or TFTP session with the NE.

11   Logs in to the NE using TL1.

12   Verifies that the files downloaded in step 9 have been downloaded without errors by
     comparing each software file downloaded on the NE with the software file on the server
     specified by the --servdir parameter.

     If there is a problem with a software file on the NE, the software file is deleted from the NE and
     a warning flag is raised. The automated ONT software staging tool stops when the number of
     warning flags exceeds the value set for the --warn parameter.

13   Logs out of the NE.

30.2.1   Command syntax

The syntax of the automated ONT software staging tool is:

Note — When using the 5520 AMS, the perl script must be run as
$AMS_PERL_DIR/perl <scriptname>.pl.

```
./stageont.pl --isam nt_ip_address | --hosts hosts_filename
[--sessions #sessions] --servdir ONTswpath --release xx.yy.zz
--onttypes Type1:Load1,Type2:Load2,..,Typen:Loadn
--logfile ONTstagelogpath/logname [--warn threshold] [--ontreleasemap
releasemappath] [--tl1username TL1user] [--tl1password TL1pwd]
[--cliusername CLIuser] [--clipassword CLIpwd] [--multi] [--seplog |
--noseplog] [--v] [--debug] [--noname] [--noping] [--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol[:priv_protocol: priv_pwd]]
```

or

```
perl stageont.pl --isam nt_ip_address | --hosts hosts_filename
[--sessions #sessions] --servdir ONTswpath --release xx.yy.zz
--onttypes Type1:Load1,Type2:Load2,..,Typen:Loadn
--logfile ONTstagelogpath/logname [--warn threshold] [--ontreleasemap
releasemappath] [--tl1username TL1user] [--tl1password TL1pwd]
[--cliusername CLIuser] [--clipassword CLIpwd] [--multi] [--seplog |
--noseplog] [--v] [--debug] [--noname] [--noping] [--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol[:priv_protocol: priv_pwd]]
```

30.2.2   Command parameters

Table 23 describes the parameters of the automated ONT software staging tool.

Table 23   **Automated ONT software staging tool parameters**

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--isam *nt_ip_address*	The IP address or name of the NE when you stage ONT software on a single NE only. When this parameter is used, the automated ONT software staging tool downloads the ONT software to only the NE specified by the --isam parameter, and ignores the --sessions and --hosts parameters. [1]	Mandatory	—
--hosts *hosts_filename*	The file listing the IP addresses and names of the NEs when you stage ONT software on multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information This parameter is ignored if the --isam parameter is used. [1]	—	Mandatory
--sessions *#sessions*	The number of parallel sessions when you stage ONT software on multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information. This parameter is ignored if the --isam parameter is used. [1] This value cannot exceed the value set for the maximum number of parallel software downloads in the configuration file; see Table 18 for more information.	—	Mandatory
--servdir *ONTswpath*	The location the new ONT software on the EMS server. *ONTswpath* is the path of the server directory that contains the new ONT software.	Mandatory	Mandatory
--release *xx.yy.zz*	The ONT software release number. *xx.yy.zz* is the 6-digit ONT software release number (for example, R04.00.10)	Mandatory	Mandatory
--onttypes *Type1*:*Load1*,*Type2*: *Load2*,..,*Typen*:*Loadn*	The model and load types for the ONTs that require software staging. See the ONT Customer Release Notes for the list of supported ONT model types and their associated load type. *Typen* is the mnemonic for the ONT model type (for example, O-211M-H). *Loadn* is the load type for the ONT model type (for example, the load type for the O-211M-H ONT model type is SIP).	Mandatory	Mandatory
--logfile *ONTstagelogpath/logname*	The path and filename of the resulting log file.	Mandatory	Mandatory

(1 of 4)

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--warn *threshold*	The maximum number of operation failures that can occur before the script stops. Supported values are 0 to 100 (the default value is 0). All operation failures below the configured threshold is reached are reported as warnings.	Optional	Optional
--ontreleasemap *releasemappath*	The location of the ONT release map on the EMS server. The ONT release map lists the supported software for each ONT type for this release. *releasemappath* is the path of the server directory that contains the ONT release map.	Optional	Optional
--tl1username *TL1user*	The TL1 username if different from the one specified in the configuration file; see Table 18 for more information. When staging ONT software on multiple NEs, all the NEs must have the same TL1 username.	Optional	Optional
--tl1password *TL1pwd*	The TL1 password, if different from the one specified in the configuration file; see Table 18 for more information. When staging ONT software on multiple NEs, all the NEs must have the same TL1 password.	Optional	Optional
--cliusername *CLIuser*	The CLI username if different from the one specified in the configuration file; see Table 18 for more information. When staging ONT software on multiple NEs, all the NEs must have a common CLI username.	Optional	Optional
--clipassword *CLIpwd*	The CLI password, if different from the one specified in the configuration file; see Table 18 for more information. When staging ONT software on multiple NEs, all the NEs must have a common CLI password.	Optional	Optional
--multi	Allows multiple UNIX or LINUX users access to each NE. When this parameter is used, a working directory is created for each user that connects to the NE. The name of the working directory is the UNIX or LINUX username for the corresponding user. Nokia recommends that only one user connects to an NE at a time.	Optional	Optional

(2 of 4)

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--seplog | --noseplog	Determines where the log information is stored for each NE listed in the hosts file. Use --seplog to create a separate log file for each NE listed in the hosts file, and --noseplog to create a single log file for all sessions. See "Log files" in "TNG 100 Software Upgrade Automation Tool" for more information about log files.	—	Optional
--v	Instructs the automated ONT software staging tool to show the version number of the tool. The output shows the version of the automated ONT software staging tool as well as the versions of the applications used by the tool.	Optional	Optional
--debug	Instructs the automated ONT software staging tool to add additional troubleshooting information to the log file.	Optional	Optional
--noname	Instructs the automated ONT software staging tool to use the IP address of the NE when creating the output directory, instead of the NE name. This parameter is used by the 5529 LRM.	—	—
--noping	Instructs the tool to use SNMP instead of ping to verify if the NE is reachable. Use this parameter when the use of ping is not allowed in the network.	Optional	Optional
--comm *commstring*	The SNMP community string used by the automated ONT software staging tool when communicating with an NT unit using SNMP version 1 or version 2C. When this parameter is not specified, the tool uses the NT community string value specified in the configuration file; see Table 18 for more information.	Optional	Optional
--v2	Instructs the tool to use SNMP version 2C for data transfers between the SNMP agent and the SNMP manager.	Optional	Optional

(3 of 4)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--v3auth *auth_username*: *auth_pwd*:*auth_protocol* [:*priv_protocol*: *priv_pwd*]	Instructs the tool to use SNMP version 3 for data transfers between the SNMP agent and the SNMP manager. You can use this parameter to set the privacy protocol and the privacy password for SNMP version 3. • *auth_username* is the session authentication username • *auth_pwd* is the authentication password (at least 8 characters long) • *auth_protocol* is the authentication protocol (SHA or MD5) • *priv_protocol* is the privacy protocol (DES, 3DES, or AES) • *priv_pwd* is the privacy password (must have at least 8 characters)	Optional	Optional

(4 of 4)

Note

(1)   If neither the --isam or --host parameter is used, the tool will download ONT software to all the NEs listed in the hosts file specified in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool".

30.2.3   Examples

The following is an example of the automated ONT software staging tool command for a single NE migration:

```
./stageont.pl --isam 138.120.217.112 --servdir ONT_04_00_10/ONT --release
R04.00.10 --onttypes I-020E-H:DO,O-211M-H:SIP,I-241G-B:SIP,I-010G-A:DO
--logfile stageont_04.00.10.log
```

The following is an example of the automated ONT software staging tool command for a multiple NE migration:

```
./stageont.pl --hosts /etc/hosts --sessions 2 --servdir ONT_04_00_10/ONT
--release R04.00.10
--onttypes I-020E-H:DO,O-211M-H:SIP,I-241G-B:SIP,I-010G-A:DO --logfile
stageont_04.00.10.log
```

30.3   Automated ONT software download tool

The automated ONT software download tool is the component of the Software Upgrade Automation Tool used to download the new ONT OSWP from the NE to all ONTs of the specified type or types. See "DLP 111 Download the ONT software" for the steps to use the automated ONT software download tool.

The automated ONT software download tool automatically performs the following steps for the ONTs connected to the specified NE or NEs.

1 Verifies the connection to the NE.

2 Opens an SNMP session, disabling object identifier translation.

3 Logs in to the NE using TL1.

4 Retrieves the list of required ONT software files for the ONT types specified by the --onttypes parameter from the ONT release map.

5 Retrieves list of ONTs connected to the NE.

6 For each ONT connected to the NE, verifies if the software needs to be downloaded to the ONT by verifying the following information.

  • The ONT equipment version number and the active software version are defined on the ONT.
  • The ONT type is specified in the --onttypes parameter.
  • The ONT type is listed in the ONT release map.
  • All required information for the ONT type is available in the ONT release map.
  • The ONT is not is OOS-MA or OOS-AUMA mode.

7 For each ONT that needs software to be downloaded:

  • Gets the required ONT software version from the ONT release map.
  • Verifies if the planned load type for the ONT in the NE matches the information in the ONT release map, and updates the planned load type in the NE if needed.
  • Adds a new ONT software control entry in the NE if needed.
  • Verifies if the required software is already loaded on the ONT.

8 If the --operationmode parameter is set to DLONLY or DLANDACT, downloads the ONT software to the ONTs that require a software update.

   If there is a problem with the software download to an ONT, a warning flag is raised. The automated ONT software download tool stops when the number of warning flags exceeds the value set for the --warn parameter.

9 If the --operationmode parameter is set to ACTONLY or DLANDACT, activates the ONT software downloaded to the ONTs.

   If there is a problem with the software activation on an ONT, a warning flag is raised. The automated ONT software download tool stops when the number of warning flags exceeds the value set for the --warn parameter.

10 Verifies if the ONT software download and activation mode matches the mode set by the --ontdownloadandactivatemode parameter, and changes the mode if needed.

11 Logs out of the NE.

30.3.1   Command syntax

The syntax of the automated ONT software download tool is:

> **Note —** When using the 5520 AMS, the perl script must be run as
> $AMS_PERL_DIR/perl <scriptname>.pl.

```
./ontDownloadandActivate.pl --isam nt_ip_address | --hosts hosts_filename
[--sessions #sessions] --release xx.yy.zz
--onttypes Type1:Load1,Type2:Load2,..,Typen:Loadn
--ontdownloadandactivatemode Auto | Manual
--operationmode DLONLY | ACTONLY | DLANDACT | DELAYACT
--logfile ONTdllogpath/logname [--warn threshold]
[--ontreleasemap releasemappath] [--tl1username TL1user]
[--tl1password TL1pwd] [--cliusername CLIuser] [--clipassword CLIpwd]
[--multi] [--seplog | --noseplog] [--v] [--debug] [--noname] [--noping]
[--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol[:priv_protocol: priv_pwd]]
```

or

```
perl ontDownloadandActivate.pl --isam nt_ip_address | --hosts hosts_filename
[--sessions #sessions] --release xx.yy.zz
--onttypes Type1:Load1,Type2:Load2,..,Typen:Loadn
--ontdownloadandactivatemode Auto | Manual
--operationmode DLONLY | ACTONLY | DLANDACT | DELAYACT
--logfile ONTdllogpath/logname [--warn threshold]
[--ontreleasemap releasemappath] [--tl1username TL1user]
[--tl1password TL1pwd] [--cliusername CLIuser] [--clipassword CLIpwd]
[--multi] [--seplog | --noseplog] [--v] [--debug] [--noname] [--noping]
[--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol[:priv_protocol: priv_pwd]]
```

30.3.2   Command parameters

Table 23 describes the parameters of the automated ONT software download tool.

Table 24   **Automated ONT software download tool parameters**

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--isam *nt_ip_address*	The IP address or name of the NE when you download ONT software for a single NE only. When this parameter is used, the automated ONT software download tool downloads ONT software to the ONTs connected to the NE specified by the --isam parameter, and ignores the --sessions and --hosts parameters. [1]	Mandatory	—

(1 of 5)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--hosts *hosts_filename*	The file listing the IP addresses and names of the NEs when you download ONT software for multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information This parameter is ignored if the --isam parameter is used. [1]	—	Mandatory
--sessions *#sessions*	The number of parallel sessions when you download ONT software for multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information. This parameter is ignored if the --isam parameter is used. This value cannot exceed the value set for the maximum number of parallel software downloads in the configuration file; see Table 18 for more information.	—	Mandatory
--release *xx.yy.zz*	The ONT software release number. *xx.yy.zz* is the 6-digit ONT software release number (for example, R04.00.10)	Mandatory	Mandatory
--onttypes *Type1*:*Load1*,*Type2*:*Load2*,..,*Typen*:*Loadn*	The model and load types for the ONTs that require software download. See the ONT Customer Release Notes for the list of supported ONT model types and their associated load type. *Typen* is the mnemonic for the ONT model type (for example, O-211M-H). *Loadn* is the load type for the ONT model type (for example, the load type for the O-211M-H ONT model type is SIP).	Mandatory	Mandatory
--ontdownloadandactivatemode Auto | Manual	Sets the ONT software download and activation mode. • Auto: The ONT looks for new software on the NE and automatically downloads and activates any new version of the ONT software that is downloaded on the NE. • Manual: The ONT does not look for new software on the NE. Software updates are done manually.	Mandatory	Mandatory

(2 of 5)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--operationmode DLONLY | ACTONLY | DLANDACT | DELAYACT	Determines the actions performed by the automated ONT software download tool. The supported options are: • DLONLY: The tool downloads the new ONT software to the ONTs but does not activate the ONTs. • ACTONLY: The tool activates the new ONT software on the ONTs. • DLANDACT: The tool downloads and activates the new ONT software on the ONTs. • DELAYACT: The tool downloads and activates the new ONT software the next time the ONT services are interrupted, such as during power-off, reboot, or LT restart.	Mandatory	Mandatory
--logfile *ONTdllogpath/logname*	The path and filename of the resulting log file.	Mandatory	Mandatory
--warn *threshold*	The maximum number of operation failures that can occur before the script stops. Supported values are 0 to 100 (the default value is 0). All operation failures below the configured threshold is reached are reported as warnings.	Optional	Optional
--ontreleasemap *releasemappath*	The location of the ONT release map on the EMS server. The ONT release map lists the supported software for each ONT type for this release. *releasemappath* is the path of the server directory that contains the ONT release map.	Optional	Optional
--tl1username *TL1user*	The TL1 username if different from the one specified in the configuration file; see Table 18 for more information. When downloading ONT software for multiple NEs, all the NEs must have the same TL1 username.	Optional	Optional
--tl1password *TL1pwd*	The TL1 password, if different from the one specified in the configuration file; see Table 18 for more information. When downloading ONT software for multiple NEs, all the NEs must have the same TL1 password.	Optional	Optional
--cliusername *CLIuser*	The CLI username if different from the one specified in the configuration file; see Table 18 for more information. When downloading ONT software for multiple NEs, all the NEs must have the same CLI username.	Optional	Optional

(3 of 5)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--clipassword *CLIpwd*	The CLI password, if different from the one specified in the configuration file; see Table 18 for more information. When downloading ONT software for multiple NEs, all the NEs must have the same CLI password.	Optional	Optional
--multi	Allows multiple UNIX users access to each NE. When this parameter is used, a working directory is created for each user that connects to the NE. The name of the working directory is the UNIX username for the corresponding user. Nokia recommends that only one user connects to an NE at a time.	Optional	Optional
--seplog | --noseplog	Determines where the log information is stored for each NE listed in the hosts file. Use --seplog to create a separate log file for each NE listed in the hosts file, and --noseplog to create a single log file for all sessions. See "Log files" in "TNG 100 Software Upgrade Automation Tool" for more information about log files.	—	Optional
--v	Instructs the automated ONT software download tool to show the version number of the tool. The output shows the version of the automated ONT software download tool as well as the versions of the applications used by the tool.	Optional	Optional
--debug	Instructs the automated ONT software download tool to add additional troubleshooting information to the log file.	Optional	Optional
--noname	Instructs the automated ONT software download tool to use the IP address of the NE when creating the output directory, instead of the NE name. This parameter is used by the 5529 LRM.	—	—
--noping	Instructs the tool to use SNMP instead of ping to verify if the NE is reachable. Use this parameter when the use of ping is not allowed in the network.	Optional	Optional
--comm *commstring*	The SNMP community string used by the automated ONT software download tool when communicating with an NT unit using SNMP version 1 or version 2C. When this parameter is not specified, the tool uses the NT community string value specified in the configuration file; see Table 18 for more information.	Optional	Optional

(4 of 5)

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--v2	Instructs the tool to use SNMP version 2C for data transfers between the SNMP agent and the SNMP manager.	Optional	Optional
--v3auth *auth_username*: *auth_pwd*:*auth_protocol* [:*priv_protocol*: *priv_pwd*]	Instructs the tool to use SNMP version 3 for data transfers between the SNMP agent and the SNMP manager. You can use this parameter to set the privacy protocol and the privacy password for SNMP version 3. • *auth_username* is the session authentication username • *auth_pwd* is the authentication password (at least 8 characters long) • *auth_protocol* is the authentication protocol (SHA or MD5) • *priv_protocol* is the privacy protocol (DES, 3DES, or AES) • *priv_pwd* is the privacy password (must have at least 8 characters)	Optional	Optional

(5 of 5)

Note

(1)   If neither the --isam or --host parameter is used, the tool will download ONT software from all the NEs listed in the hosts file specified in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool".

30.3.3   Examples

The following is an example of the automated ONT software download tool command for a single NE migration:

```
./ontDownloadandActivate.pl --isam 138.120.217.112 --release R04.00.10
--onttypes I-020E-H:DO,O-211M-H:SIP,I-241G-B:SIP,I-010G-A:DO
--ontdownloadandactivatemode Auto --operationmode DLANDACT
--logfile ontdl_04.00.10.log
```

The following is an example of the automated ONT software download tool command for a multiple NE migration:

```
./ontDownloadandActivate.pl --hosts /etc/hosts --sessions 2
--onttypes I-020E-H:DO,O-211M-H:SIP,I-241G-B:SIP,I-010G-A:DO
--ontdownloadandactivatemode Auto --operationmode DLANDACT
--logfile ontdl_04.00.10.log
```

31 TNG 106 Additional automated tools

31.1 Introduction

This TNG provides information about the syntax and parameters of the following components of the Software Upgrade Automation Tool.

- Automated software minimization tool
- Automated file clean-up tool
- Automated system readiness verification tool
- Automated system status verification and comparison tools
- NTIO unit reconfiguration tools

See "TNG 100 Software Upgrade Automation Tool" for general information about the Software Upgrade Automation Tool, the configuration file, the hosts file and the log files.

31.2 Automated software minimization tool

The automated software minimization tool is the component of the Software Upgrade Automation Tool used to reduce the size of the new OSWP before downloading it to the ISAM, based on the detected and planned cards on an NE or on the content of a card configuration file. Minimizing the new OSWP reduces the size of the software package that will be downloaded to the NE or NEs. This reduces the time required to download the software and reduces the memory required to store the OSWP on the NT unit. See "DLP 102 Download the NE software" for the steps to use the automated software minimization tool.

Note 1 — By default, the automated software download tool downloads only the software for planned and detected cards in the system. Use the automated software minimization tool when you need to allow the automated software download tool to download the software for cards not yet planned or installed (for example, to download software for a new card type).

Note 2 — When using the automated software minimization tool, the suffix of the OSWP name is changed to indicate that it is a minimized OSWP.

Note 3 — The automated software minimization tool is not applicable to 7367 ISAM SX/DX.

The automated software minimization tool automatically performs the following steps for the specified NE or NEs.

1   Verifies that there is an OSWP in the specified server directory.

2   If the --isam parameter is specified:

- Verifies the connection to the NE.
- Opens an SNMP session, disabling object identifier translation.
- Logs in to the NE using CLI.
- Retrieves information about all detected and planned cards on the NE through an SNMP session.
- Logs out of the NE.

3   If the --config parameter is specified, retrieves the card configuration file. This step is always skipped if the --isam parameter is specified.

4   Creates the minimized SWP which contains only the software for the detected and planned cards or the cards listed in the card configuration file.

5   Saves the minimized SWP in the target location. The suffix of the minimized SWP is changed to ZA to indicate that this is a minimized SWP; see "TNG 108 Overall SoftWare Package concept" for more information.

6   Creates a customized SWP Descriptor file for the minimized OSWP and stores it in the same folder as the complete SWP Descriptor file.

- If the --target parameter is used, the customized SWP Descriptor file and the defined minimum set of software are stored instead in the location defined by the --target parameter; see Table 25.
- If the --minset parameter is used, the MINIMUMSET parameter in the SWP Descriptor file is set to Yes. When the OSWP is downloaded to an NE, the software for all the cards listed in the SWP Descriptor file is downloaded to that NE.
- If the --minset parameter is not used, the MINIMUMSET parameter in the SWP Descriptor file is set to No. When the OSWP is downloaded to an NE, only the software for the planned and detected cards on that NE that are listed in the SWP Descriptor file is downloaded to that NE.

31.2.1   Card configuration file

The card configuration file lists all the cards applicable to all the NEs where the software will be downloaded. Include any cards that will be added to the system before the next upgrade or migration to ensure that the software for the new cards is available when the cards are added to the system. This will reduce the time required to add a new card to the system.

Note — When adding unplanned cards to the card configuration file, you must use the --minset parameter when running the automated software minimization tool to ensure that the software for the unplanned cards is included in the downloaded OSWP; see Table 25.

The following is an example of the contents of a card configuration file.

```
NANT-A
NALT-B
NVLT-C
NVLT-G
```

From R5401 version onwards, PBMT's minimizeswp won't allow to configure two different platform(NT-TYPE) which fall under different SWP Descriptor files.

For Example:

```
AGNT-A L6GQAA55.059
FANT-F L6GQAB55.059
```

31.2.2   Command syntax

The syntax of the automated software minimization tool is:

Note — When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

```
./MinimizeSWP.pl --isam nt_ip_address | --config config_filename --swp
OSWPpath/OSWPnamexx.yyy --logfile swminlogpath/logname [--debug] [--v]
[--minset][--target targetpath] [--comm commstring] [--v2] [--v3auth
auth_username:auth_pwd:auth_protocol] [--v3priv priv_protocol:priv_pwd]
[--btype <SNMP|YANG>]
```

or

```
perl MinimizeSWP.pl --isam nt_ip_address | --config config_filename --swp
OSWPpath/OSWPnamexx.yyy --logfile swminlogpath/logname [--debug] [--v]
[--minset][--target targetpath] [--comm commstring] [--v2] [--v3auth
auth_username:auth_pwd:auth_protocol] [--v3priv priv_protocol:priv_pwd]
[--btype <SNMP|YANG>]
```

31.2.3   Command parameters

Table 25 describes the parameters of the automated software minimization tool.

Table 25   **Automated software minimization tool parameters**

Parameter	Description	Parameter type
--isam *nt_ip_address*	The IP address or name of the NE. When this parameter is used, only the software for the planned and detected cards on the NE is included in the minimized OSWP.	Mandatory if --config is not used [1]
--config *config_filename*	The location and filename of the card configuration file containing a list of the card types in the system. When this parameter is specified, only the software for the card types listed in the card configuration file is included in the minimized OSWP.	Mandatory if --isam is not used [1]

(1 of 2)

Parameter	Description	Parameter type
--swp *OSWPpath*/*OSWPnamexx.yyy*	The location and filename of the new OSWP. *OSWPpath*/*OSWPname* is the path and filename of the new (full) OSWP package (suffix = AA); see "TNG 108 Overall SoftWare Package concept" for more information. *xx* is the 2-digit ISAM software release number. *yyy* is the 3-digit ISAM software package number (for example, L6GPAA40.046).	Mandatory
--logfile *swminlogpath/logname*	The path and filename of the resulting log file.	Mandatory
--debug	Instructs the automated software minimization tool to add additional troubleshooting information to the log file.	Optional
--v	Instructs the automated software minimization tool to show the version number of the tool. The output shows the version of the automated software minimization tool as well as the versions of the applications used by the tool.	Optional
--minset	Instructs the automated software minimization tool to set the MINIMUMSET parameter of the SWP Descriptor file to Yes. When the OSWP is downloaded to an NE, the software for all the cards listed in the SWP Descriptor file is downloaded to that NE. If this parameter is not used, only the software for the planned and detected cards on the NE that are listed in the SWP Descriptor file is downloaded to the NE.	Optional
--target *targetpath*	The location where the minimized OSWP and SWP Descriptor file will be saved, if different from the location of the full OSWP and SWP Descriptor file. When the --isam option is used, the path is relative to the TFTP root directory setting.	Optional
--comm commstring	The SNMP community string used by the automated software download tool when communicating with an NT unit using SNMP version 1 or version 2C. When this parameter is not specified, the tool uses the NT community string value defined in the configuration file; see Table 18 for more information.	Optional
--v2	Instructs the tool to use SNMP version 2C instead of version 1 for data transfers between the SNMP agent and the SNMP manager.	Optional
--*v3auth auth_username:auth_pwd:auth _protocol*	Instructs the tool to use SNMP version 3 instead of version 1 for data transfers between the SNMP agent and the SNMP manager. auth_username is the session authentication username, auth_pwd is the authentication password (at least 8 characters long), and auth_protocol is the authentication protocol (SHA or MD5).	Optional
--v3priv priv_protocol:priv_pwd	Sets the privacy protocol (DES, 3DES, or AES) and the privacy password (at least 8 characters long) for SNMP version 3.	Optional
--btype	Intsructs to use SNMP or YANG build type	Optional

(2 of 2)

Note
(1)   The --isam and --config parameters are mutually exclusive. If both the --isam parameter and --config
       parameters are specified, the --config parameter is ignored.

31.2.4   Examples

The following is an example of the automated software minimization tool command:

```
MinimizeSWP.pl --isam 138.120.217.112 --SWP OSWP/L6GPAA40.059 --logfile
swminlog.txt
```

31.3   Automated file clean-up tool

The automated file clean-up tool is the component of the Software Upgrade Automation tool used
to delete the temporary files and folders created by the Software Upgrade and Automation Tool
during an upgrade or migration, including all files created by the automated system verification
tool.

Note — Nokia recommends that you only run the automated file
clean-up tool after committing the software.

You can run the automated file clean-up tool to delete the temporary files and folders created for
either a single NE or multiple NEs. See "DLP 105 Commit the NE software" for the steps to use
the automated file clean-up tool.

31.3.1   Command syntax for the automated file clean-up tool

The syntax for the automated file clean-up tool is:

Note — When using the 5520 AMS, the perl script must be run as
$AMS_PERL_DIR/perl <scriptname>.pl.

```
./cleanUp.pl --isam nt_ip_address │ --hosts hosts_filename
--logfile clnuplogpath/logname │ --id runid [--debug] [--multi] [--noname]
[--v]
```

or

```
perl cleanUp.pl --isam nt_ip_address │ --hosts hosts_filename --logfile
clnuplogpath/logname │ --id runid [--debug] [--multi] [--noname] [--v]
```

31.3.2   Command parameters

Table 26 describes the parameters of the automated file clean-up tool.

Table 26   **Automated file clean-up tool parameters**

Parameter	Description	Applies to	
		Single NE	**Multiple NEs**
--isam *nt_ip_address*	The IP address or name of the NE when cleaning up files for a single NE. When this parameter is used, the automated file clean-up tool deletes the temporary files and folders for only the NE specified by the --isam parameter, and ignores the --hosts parameter. [1]	Mandatory	—
--hosts *hosts_filename*	The file listing the IP addresses and names of the NEs when you cleaning up files for multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information This parameter is ignored if the --isam parameter is used. [1]	—	Mandatory
--logfile *clnuplogpath/logname*	The path and filename of the resulting log file for the automated file clean-up tool. When this parameter is used, the --id parameter is ignored.	Mandatory	Mandatory
--id *runid*	This parameter is used by the 5529 LRM instead of the --logfile parameter to generate a log file and a result file when you clean up files for a single NE. This parameter cannot be used when you clean up files for multiple NEs. The filenames of the resulting files are *runid*_CLUP.log and *runid*_CLUP.result, where *runid* is the 5529 LRM run identification number. This parameter is ignored if the --logfile parameter is used.	—	—
--debug	Instructs the automated file clean-up tool to add additional troubleshooting information to the log file.	Optional	Optional
--multi	Allows multiple UNIX or LINUX users access to each NE. When this parameter is used, a working directory is created for each user that connects to the NE. The name of the working directory is the UNIX or LINUX username for the corresponding user. Nokia recommends that only one user connects to an NE at a time.	Optional	Optional
--noname	Instructs the automated file clean-up tool to use the IP address of the NE when creating the output directory, instead of the NE name. This parameter is used by the 5529 LRM.	—	—

(1 of 2)

Parameter	Description	Applies to	
		Single NE	**Multiple NEs**
--v	Instructs the automated file clean-up tool to show the version number of the tool. The output shows the version of the automated file clean-up tool as well as the versions of the applications used by the tool.	Optional	Optional

(2 of 2)

Note

(1)   If neither the --isam or --host parameter is used, the tool will clean up the files for all the NEs listed in the hosts file specified in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool".

31.3.3   Examples

The following is an example of the automated file clean-up tool command for a single NE:

```
./cleanUp.pl --isam 138.120.217.112 --logfile clean_40.041.log
```

The following is an example of the automated file clean-up tool command for multiple NEs:

```
./cleanUp.pl --hosts /etc/hosts --logfile clean_40.041.log
```

31.4   Automated system readiness verification tool

The automated system readiness verification tool is the component of the Software Upgrade Automation tool used to verify if there are problems in one or more NEs that can prevent an upgrade or migration from running successfully.

You can verify the readiness of the system on either a single NE or on multiple NEs using a single session or multiple parallel sessions; see "Components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information. See "NTP 100 Upgrade the software", "NTP 101 Migrate the software", "NTP 102 Reconfigure an NTIO unit" for the steps to use the automated system readiness verification tool.

The following information is retrieved for each NE:

- the card type for the cards installed in the NTA and NTB slots
- any restrictions for upgrade or migration
- the SHub boot settings (for SHub-based systems only)
- the file size of the critical files
- the size of the software partition
- the ICS version of the NT unit or NT units
- the presence of software

31.4.1 Command syntax for the automated system readiness tool

The syntax of the automated system readiness tool is:

Note 1 — When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

Note 2 — From R4.5.02 onward, you can choose the option to use a second CLI password when using CLI over SSH configurations, in case the first CLI password should fail. See "TNG 100 Software Upgrade Automation Tool" for more information.

```
./preCheck.pl --isam nt_ip_address | --hosts hosts_filename --sessions
#sessions --swp OSWPpath/OSWPnamexx.yyy --logfile verlogpath/logname | --id
runid [--cliusername CLIuser] [--clipassword CLIpwd]
[--clipassword2 SecondCLIpwd] [--sftpusername SFTPuser]
[--ntdbtool NTDBpath] [--lanxtool SHubpath] [--ivpstool xVPSpath] [--seplog
| noseplog] [--debug] [--multi] [--noname] [--comm commstring]
[--noping][--v2] [--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--v] [--btype <SNMP|YANG>]
```

or

```
perl preCheck.pl --isam nt_ip_address | --hosts hosts_filename --sessions
#sessions --swp OSWPpath/OSWPnamexx.yyy --logfile verlogpath/logname | --id
runid [--cliusername CLIuser] [--clipassword CLIpwd] [--sftpusername
SFTPuser] [--ntdbtool NTDBpath] [--lanxtool SHubpath] [--ivpstool xVPSpath]
[--seplog | noseplog] [--debug] [--multi] [--noname] [--comm commstring]
[--noping][--v2] [--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd] [--v] [--btype <SNMP|YANG>]
```

31.4.2 Command parameters

Table 27 describes the parameters of the automated system readiness verification tools

Table 27   **Automated system readiness verification tool parameters**

Parameter	Description	Applies to	
		Single NE	**Multiple NEs**
--isam *nt_ip_address*	The IP address or name of the NE when you verify the system readiness of a single NE. When this parameter is used, the automated system readiness verification tool verifies the operational status of only the NE specified by the --isam parameter, and ignores the --sessions and --hosts parameters. [1]	Mandatory	—

(1 of 4)

Parameter	Description	Applies to	
		Single NE	Multiple NEs
--hosts *hosts_filename*	The file listing the IP addresses and names of the NEs when you verify the system readiness of multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information This parameter is ignored if the --isam parameter is used. [1]	—	Mandatory
--sessions *#sessions*	The number of parallel sessions when you verify the system readiness of multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information. This parameter is ignored if the --isam parameter is used. This value cannot exceed the value set for the maximum number of parallel software downloads in the configuration file; see Table 18 for more information.	—	Mandatory
--swp *OSWPpath/OSWPnamexx.yyy*	The location and filename of the new OSWP. OSWPpath/OSWPname is the path and filename of the new OSWP package. When minimized, the OSWP suffix is ZA; see "TNG 108 Overall SoftWare Package concept" for more information. xx is the 2-digit ISAM software release number yyy is the 3-digit ISAM software package number (for example, L6GPAA40.046).	Mandatory	Mandatory
--logfile *readinesslogpath/logname*	The path and filename of the resulting log file for the automated system readiness verification tool. When this parameter is used, the --id parameter is ignored.	Mandatory	Mandatory
--id *runid*	This parameter is used by the 5529 LRM instead of the --logfile parameter to generate a log file and a result file when you verify the system readiness of a single NE. This parameter cannot be used when you verify the system readiness of multiple NEs. The filenames of the resulting files are *runid*_PRCK.log and *runid*_PRCK.result, where *runid* is the 5529 LRM run identification number. This parameter is ignored if the --logfile parameter is used.	—	—
--cliusername *CLIuser*	The CLI username if different from the one specified in the configuration file; see Table 18 for more information. When verifying the system readiness of multiple NEs, all the NEs must have a common CLI username.	Optional	Optional

(2 of 4)

Parameter	Description	Applies to	
		Single NE	Multiple NEs
--clipassword *CLIpwd* --clipassword2 *SecondCLIpwd*	The CLI password, if different from the one specified in the configuration file; see Table 18 for more information. When verifying the system readiness of multiple NEs, all the NEs must have a common CLI password. The second CLI password will be used only in the case when CLI over SSH is configured. The second CLI password specifies an alternative password to be used when the first CLI password fails to connect to one or more NEs. This value is encrypted in the configuration file.	Optional	Optional
--sftpusername *SFTPuser*	The SFTP username, if different from the one specified in the configuration file; see Table 18 for more information. When verifying the system readiness of multiple NEs, all the NEs must have a common SFTP username.	Optional	Optional
--ntdbtool *NTDBpath*	The location of the NT database offline migration tool when different from the default location; see "DLP 100 Prepare the software" for the default location. *NTDBpath* is the directory path of the NT database migration tool.	Optional	Optional
--lanxtool *SHubpath*	The location of the SHub migration tool when different from the default location; see "DLP 100 Prepare the software" for the default location. *SHubpath* is the directory path of the LANX migration tool.	Optional	Optional
--ivpstool *xVPSpath*	The location of the xVPS migration tool when different from the default location and filename; see "DLP 100 Prepare the software" for the default location and filename. *xVPSpath* is the path and filename of the migration tool.	Optional	Optional
--seplog | --noseplog	Determines where the log information is stored for each NE listed in the hosts file. Use --seplog to create a separate log file for each NE listed in the hosts file, and --noseplog to create a single log file for all sessions. See "Log files" in "TNG 100 Software Upgrade Automation Tool" for more information about log files.	—	Optional
--debug	Instructs the automated system readiness verification tool to add additional troubleshooting information to the log file.	Optional	Optional

(3 of 4)

3HH-10318-AAAA-TCZZA

Parameter	Description	Applies to	
		Single NE	Multiple NEs
--multi	Allows multiple UNIX or LINUX users access to each NE. When this parameter is used, a working directory is created for each user that connects to the NE. The name of the working directory is the UNIX or LINUX username for the corresponding user. Nokia recommends that only one user connects to an NE at a time.	Optional	Optional
--noname	Instructs the automated system readiness verification tool to use the IP address of the NE when creating the output directory, instead of the NE name. This parameter is used by the 5529 LRM.	—	—
--comm *commstring*	The SNMP community string used by the automated system readiness verification tool when communicating with an NT unit using SNMP version 1 or version 2C. When this parameter is not specified, the tool uses the NT community string value specified in the configuration file; see Table 18 for more information.	Optional	Optional
--noping	Instructs the tool to use SNMP instead of ping to verify if the NE is reachable. Use this parameter when the use of ping is not allowed in the network.	Optional	Optional
--v2	Instructs the tool to use SNMP version 2C for data transfers between the SNMP agent and the SNMP manager.	Optional	Optional
--v3auth *auth_username*:*auth_pwd*:*auth_protocol*	Instructs the tool to use SNMP version 3 for data transfers between the SNMP agent and the SNMP manager. *auth_username* is the session authentication username, *auth_pwd* is the authentication password (at least 8 characters long), and *auth_protocol* is the authentication protocol (SHA or MD5).	Optional	Optional
--v3priv *priv_protocol*:*priv_pwd*	Sets the privacy protocol (DES, 3DES, or AES) and the privacy password (at least 8 characters long) for SNMP version 3.	Optional	Optional
--v	Instructs the automated system readiness verification tool to show the version number of the tool. The output shows the version of the automated system readiness verification tool as well as the versions of the applications used by the tool.	Optional	Optional
--btype	Instructs to use SNMP or YANG build type	Optional	Optional

(4 of 4)

Note
(1)   If neither the --isam or --host parameter is used, the tool will verify or compare the system status for all the NEs
       listed in the hosts file specified in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade
       Automation Tool".

31.4.3   Examples

The following is an example of the automated system readiness verification tool command for a single NE:

```
./preCheck.pl --isam 138.120.217.112 --swp OSWP/OSWPAN40.137 --logfile
readver_40.137.log
```

The following is an example of the automated system readiness verification tool command for multiple NEs:

```
./preCheck.pl --sessions 2 --hosts /etc/hosts --swp OSWP/OSWPAN40.137
--logfile readver_40.137.log
```

31.5   Automated system status verification and comparison tools

The automated system status verification tool is the component of the Software Upgrade Automation Tool used to verify the operational status of one or more NEs in the system before and after a procedure using the Software Upgrade Automation Tool. The result files can then be compared to verify that the procedure was successful.

The automated system status comparison tool is the component of the Software Upgrade Automation Tool used to compare the results of the automated system status verification tool before and after a procedure using the Software Upgrade Automation Tool.

Note — For best results, use the automated system status verification tool when the system is in service.

You can verify and compare the system status on either a single NE or on multiple NEs using a single session or multiple parallel sessions; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 106 Additional automated tools" for more information. See "NTP 100 Upgrade the software", "NTP 101 Migrate the software", "NTP 102 Reconfigure an NTIO unit" for the steps to use the automated system status verification tool and the automated system status comparison tool.

The following information is retrieved by the automated system status verification tool for each NE:

- LT unit configuration and status
- subscriber line configuration and status
- bridge configuration data

- authenticated users information
- outstanding alarms

The automated system status comparison tool compares the results of the automated system status verification tool run before and after a software upgrade or migration procedure and flags any difference in results greater than the predefined mismatch thresholds. The mismatch thresholds are defined in the configuration file; see "TNG 100 Software Upgrade Automation Tool" for more information.

Note — From R4.5.02 onward, you can choose the option to use a second CLI password when using CLI over SSH configurations, in case the first CLI password should fail. See "TNG 100 Software Upgrade Automation Tool" for more information.

31.5.1 Command syntax for automated system status verification tool

The syntax of the automated system status verification tool is:

Note — When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

```
./statusCheck.pl --isam nt_ip_address │ --hosts hosts_filename --sessions
#sessions --logfile verlogpath/logname │ --id runid --pre │ --post
[--release xx.yy.zz] [--ontreleasemap releasemappath]
[--cliusername CLIuser] [--clipassword CLIpwd] [--clipassword2 SecondCLIpwd]
[--tl1username TL1user] [--tl1password TL1pwd] [--seplog │ --noseplog]
[--debug] [--multi] [--noname] [--comm commstring] [--v] [--bufsiz
buffersize] [--checks checks] [--telnetto tovalue] [--noping] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd]
```

or

```
perl statusCheck.pl --isam nt_ip_address │ --hosts hosts_filename --sessions
#sessions --logfile verlogpath/logname │ --id runid --pre │ --post
[--release xx.yy.zz] [--ontreleasemap releasemappath]
[--cliusername CLIuser] [--clipassword CLIpwd] [--tl1username TL1user]
[--tl1password TL1pwd] [--seplog │ --noseplog] [--debug] [--multi]
[--noname] [--comm commstring] [--v] [--bufsiz buffersize] [--checks checks]
[--telnetto tovalue] [--noping] [--v2] [--v3auth
auth_username:auth_pwd:auth_protocol] [--v3priv priv_protocol:priv_pwd]
```

31.5.2 Command syntax for the automated system status comparison tool

The syntax of the automated system status comparison tool is:

Note — When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

```
./statusCheckCmp.pl --isam nt_ip_address | --hosts hosts_filename --sessions
#sessions --logfile verlogpath/logname [--warn threshold] [--ontreleasemap
releasemappath] [--seplog | noseplog] [--debug] [--multi] [--noname] [--v]
[--detail] [--incltoos] [--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd]
```

or

```
perl statusCheckCmp.pl --isam nt_ip_address | --hosts hosts_filename
--sessions #sessions --logfile verlogpath/logname [--warn threshold]
[--ontreleasemap releasemappath] [--seplog | noseplog] [--debug] [--multi]
[--noname] [--v] [--detail] [--incltoos] [--comm commstring] [--v2]
[--v3auth auth_username:auth_pwd:auth_protocol]
[--v3priv priv_protocol:priv_pwd]
```

31.5.3 Command parameters

Table 28 describes the parameters of the automated system status verification and comparison tools.

Table 28   **Automated system status verification and comparison
tool parameters**

Parameter	Description	Applies to	
		Single NE	**Multiple NEs**
--isam *nt_ip_address*	The IP address or name of the NE when you verify or compare the system status of a single NE. When this parameter is used: [1] • The automated system status verification tool verifies the operational status of only the NE specified by the --isam parameter, and ignores the --sessions and --hosts parameters. • The automated system status comparison tool compares the results for the NE specified by the --isam parameter, and ignores the --sessions and --hosts parameters.	Mandatory	—
--hosts *hosts_filename*	The file listing the IP addresses and names of the NEs when you verify or compare the operational status of multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information This parameter is ignored if the --isam parameter is used. [1]	—	Mandatory
--sessions *#sessions*	The number of parallel sessions when you verify or compare the operational status of multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information. This parameter is ignored if the --isam parameter is used. For the automated system status verification tool, this value cannot exceed the value set for the maximum number of parallel software downloads in the configuration file; see Table 18 for more information. For the automated system status comparison tool, this value cannot exceed the value set for the maximum number of status check comparisons in the configuration file; see Table 18 for more information.	—	Mandatory
--logfile *verlogpath/logname* --logfile *cmplogpath/logname*	The path and filename of the resulting log file for the automated system status verification tool and the automated system status comparison tool. When this parameter is used, the --id parameter is ignored.	Mandatory	Mandatory

(1 of 5)

Parameter	Description	Applies to	
		Single NE	Multiple NEs
--id *runid*	This parameter is used by the 5529 LRM instead of the --logfile parameter to generate a log file and a result file when you verify or compare the system status of a single NE. This parameter cannot be used when you verify or compare the system status of multiple NEs. The filenames of the resulting files are *runid*_SCHK.log and *runid*_SCHK.result for the automated system status verification tool, and *runid*_CHKC.log and *runid*_CHKC.result for the automated system status comparison tool, where *runid* is the 5529 LRM run identification number. This parameter is ignored if the --logfile parameter is used.	—	—
--pre --post	Indicates whether this instance of the automated system status verification tool is run before or after a procedure and instructs the tool to name the results file accordingly. This parameter is only used with the automated system status verification tool.	Mandatory	Mandatory
--release *xx.yy.zz*	The ONT software release number. *xx.yy.zz* is the 6-digit ONT software release number (for example, R04.00.10) This parameter is only used with the automated system status verification tool.	Optional	Optional
--warn *threshold*	The maximum number of operation failures that can occur before the script stops. Supported values are 0 to 100 (the default value is 0). All operation failures below the configured threshold is reached are reported as warnings. This parameter is only used with the automated system status comparison tool.	Optional	Optional
--ontreleasemap *releasemappath*	The location of the ONT release map on the EMS server. The ONT release map lists the supported software for each ONT type for this release. *releasemappath* is the path of the server directory that contains the ONT release map.	Optional	Optional
--cliusername *CLIuser*	The CLI username if different from the one specified in the configuration file; see Table 18 for more information. When verifying the system status of multiple NEs, all the NEs must have a common CLI username. This parameter is only used with the automated system status verification tool.	Optional	Optional

(2 of 5)

Parameter	Description	Applies to	
		Single NE	**Multiple NEs**
--clipassword *CLIpwd* --clipassword2 *SecondCLIpwd*	The CLI password, if different from the one specified in the configuration file; see Table 18 for more information. When verifying the system status of multiple NEs, all the NEs must have a common CLI password. This parameter is only used with the automated system status verification tool. The second CLI password will be used only in the case when CLI over SSH is configured. The second CLI password specifies an alternative password to be used when the first CLI password fails to connect to one or more NEs. This value is encrypted in the configuration file.	Optional	Optional
--tl1username *TL1user*	The TL1 username if different from the one specified in the configuration file; see Table 18 for more information. When verifying the system status of multiple NEs, all the NEs must have a common TL1 username. This parameter is only used with the automated system status verification tool.	Optional	Optional
--tl1password *TL1pwd*	The TL1 password, if different from the one specified in the configuration file; see Table 18 for more information. When verifying the system status of multiple NEs, all the NEs must have a common TL1 password. This parameter is only used with the automated system status verification tool.	Optional	Optional
--seplog	--noseplog	Determines where the log information is stored for each NE listed in the hosts file. Use --seplog to create a separate log file for each NE listed in the hosts file, and --noseplog to create a single log file for all sessions. See "Log files" in "TNG 100 Software Upgrade Automation Tool" for more information about log files.	—	Optional
--debug	Instructs the automated system status verification or comparison tool to add additional troubleshooting information to the log file.	Optional	Optional
--multi	Allows multiple UNIX or LINUX users access to each NE. When this parameter is used, a working directory is created for each user that connects to the NE. The name of the working directory is the UNIX or LINUX username for the corresponding user. Nokia recommends that only one user connects to an NE at a time.	Optional	Optional

(3 of 5)

Parameter	Description	Applies to	
		Single NE	Multiple NEs
--noname	Instructs the automated system status verification or comparison tool to use the IP address of the NE when creating the output directory, instead of the NE name. This parameter is used by the 5529 LRM.	—	—
--comm *commstring*	The SNMP community string used by the automated system status verification tool when communicating with an NT unit using SNMP version 1 or version 2C. When this parameter is not specified, the tool uses the NT community string value specified in the configuration file; see Table 18 for more information.	Optional	Optional
--v	Instructs the automated system status verification or comparison tool to show the version number of the tool. The output shows the version of the automated system status verification or comparison tool as well as the versions of the applications used by the tool.	Optional	Optional
--bufsiz *buffersize*	Defines the internal buffer size in Mb for the results of the CLI commands used by the automated system status verification tool. The maximum valid value is 100 Mbytes. If not specified, the tool uses the value specified in the configuration file; see Table 18 for more information. This parameter is only used with the automated system status verification tool.	Optional	Optional
--checks *checks*	Instructs the automated system status verification tool to only retrieve the specified information. Enter one or more of the following options, separated by a colon (:). • ltsts: LT unit configuration and status • xdsl: subscriber line configuration and status • bridge: bridge configuration • auth: authenticated users information • alarm: outstanding alarms • ont: read ont status If this parameter is not specified, all options except 'ont' status are retrieved. If ont status is to be retrieved, 'ont' option has to be explicitly mentioned in the --checks option. This parameter is only used with the automated system status verification tool.	Optional	Optional

(4 of 5)

Parameter	Description	Applies to	
		Single NE	Multiple NEs
--telnetto *tovalue*	The timeout value for the Telnet session, in seconds. This parameter is only used with the automated system status verification tool.	Optional	Optional
--detail	Displays the parameter mismatches. This parameter is only used with the automated system status comparison tool.	Optional	Optional
--incltoos	Includes the out-of-service lines for each LT unit in the resulting log file. This parameter is only used with the automated system status comparison tool.	Optional	Optional
--noping	Instructs the tool to use SNMP instead of ping to verify if the NE is reachable. Use this parameter when the use of ping is not allowed in the network. This parameter is only used with the automated system status verification tool.	Optional	Optional
--v2	Instructs the tool to use SNMP version 2C for data transfers between the SNMP agent and the SNMP manager.	Optional	Optional
--v3auth *auth_username*: *auth_pwd*:*auth_protocol*	Instructs the tool to use SNMP version 3 for data transfers between the SNMP agent and the SNMP manager. *auth_username* is the session authentication username, *auth_pwd* is the authentication password (at least 8 characters long), and *auth_protocol* is the authentication protocol (SHA or MD5).	Optional	Optional
--v3priv *priv_protocol*:*priv_pwd*	Sets the privacy protocol (DES, 3DES, or AES) and the privacy password (at least 8 characters long) for SNMP version 3.	Optional	Optional

(5 of 5)

Note

(1)   If neither the --isam or --host parameter is used, the tool will verify or compare the system status for all the NEs listed in the hosts file specified in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool".

31.5.4   Examples

The following is an example of the automated system status verification tool command for a single NE:

```
./statusCheck.pl --isam 138.120.217.112 --pre --logfile prever_40.041.log
```

The following is an example of the automated system status comparison tool command for multiple NEs:

```
./statusCheckCmp.pl --sessions 2 --hosts /etc/hosts --logfile cmp_40.041.log
```

31.6   NTIO unit reconfiguration tools

The NTIO unit reconfiguration tools are the components of the Software Upgrade Automation Tool used to reconfigure a system when replacing an NTIO unit with a new type of NTIO unit.

Note — The NTIO unit reconfiguration tools are not applicable to the 7356 ISAM FTTB in stand-alone mode, the 7360 ISAM FX or the 7367 ISAM SX/DX.

Use this procedure only if the NTIO unit is replaced outside of a migration window, for example, when a card failure has occurred and the card is replaced by a new type. See "NTP 102 Reconfigure an NTIO unit" for the steps to use the NTIO reconfiguration tool.

Note — You can only replace an NTIO unit with a unit of the same family, for example, an NCNC-C card with an NCNC-E card; see "NTP 102 Reconfigure an NTIO unit" for more information.

Table 29 lists the available NTIO unit reconfiguration tools.

Table 29   **NTIO unit reconfiguration tools**

Name	Command
NCNC-C to NCNC-E reconfiguration tool	cvtNcncC2E.pl

The NTIO unit reconfiguration tool automatically performs the following steps when invoked:

1   Retrieves the SFP configuration of the existing NTIO unit.

2   Unplans the existing NTIO unit.

3   Plans the new NTIO unit.

4   Reconfigures the new NTIO unit based on the information retrieved in step 1.

31.6.1   Command syntax

The syntax of the NCNC-C to NCNC-E reconfiguration tool is:

Note — When using the 5520 AMS, the perl script must be run as
$AMS_PERL_DIR/perl <scriptname>.pl.

```
./cvtNcncC2E.pl --isam nt_ip_address --logfile configlogpath/logname
[--username CLIuser] [--password CLIpwd] [--debug] [--v]
```

or

```
perl cvtNcncC2E.pl --isam nt_ip_address --logfile configlogpath/logname
[--username CLIuser] [--password CLIpwd] [--debug] [--v]
```

31.6.2   Command parameters

Table 30 describes the parameters of the NCNC-C to NCNC-E reconfiguration tools.

Table 30   **NCNC-C to NCNC-E reconfiguration tools parameters**

Parameter	Description	Parameter type
--isam *nt_ip_address*	The IP address or name of the NE.	Mandatory
--username *CLIuser*	The CLI username if different from the one specified in the configuration file; see Table 18 for more information.	Optional
--password *CLIpwd*	The CLI password, if different from the one specified in the configuration file; see Table 18 for more information.	Optional
--debug	Instructs the NCNC-C to NCNC-E reconfiguration tool to add additional troubleshooting information to the log file.	Optional
--v	Instructs the NCNC-C to NCNC-E reconfiguration tool to show the version number of the tool. The output shows the version of the NCNC-C to NCNC-E reconfiguration tool as well as the versions of the applications used by the tool.	Optional

31.6.3   Example

The following is an example of the NCNC-C to NCNC-E reconfiguration tool command:

```
./cvtNcncC2E.pl --isam 138.120.217.112 --logfile NCNCconfiglog.txt
```

3HH-10318-AAAA-TCZZA

32 TNG 107 Network element management

32.1 Introduction

The ISAM is a DSLAM. A DSLAM is a DSL access multiplexer that operates in an Ethernet packet aggregation network. Since the data in the ISAM is forwarded according to Ethernet bridging rules, the ISAM can also be referred to as an Ethernet DSLAM.

The ISAM is managed by the NT unit. The NT unit is composed of

- the NT subsystem, which manages the functionality of the system and the LT unit, and provides the interface to the IP network
- the SHub/IHub subsystem, which manages the Ethernet switching.

The ISAM software and database contains the software and database for the NT subsystem and for the SHub/IHub subsystem.

Note 1 — See the *7302 ISAM | 7330 ISAM FTTN System Description* for information about managing the ISAM Voice and the ONTs.

Note 2 — The SHub and IHub subsystems are not applicable to 7367 ISAM SX/DX.

This chapter provides the following information:

- Network management
- Software management
- Database management

32.2 Network management

Figure 2 shows how the ISAM NE can be managed in a network. The ISAM can be managed via the remote management system, the remote craft terminal, or the local craft terminal (via EIA/TIA-232). The NT and SHub/IHub subsystems share the same management interface.

Figure 2   **NE management in a network**
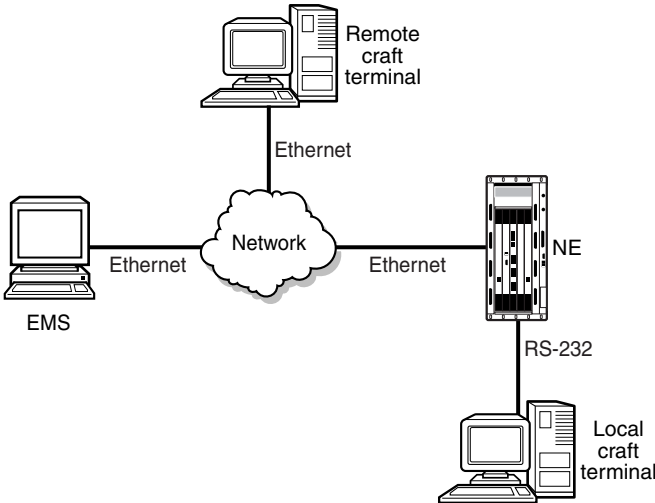
Table 31 shows an overview of the managers that are involved in the upgrade and migration procedures.

Table 31   **Manager overview**

Type	Description
EMS	Element Management System based on SNMP: • 5520 AMS for ETSI products
TL1	TL1 commands using craft terminal
CLI	CLI commands using craft terminal

32.3   Software management

This section describes the operational procedure to upgrade and migrate the ISAM. You can upgrade and migrate the ISAM using the Software Upgrade Automation Tool, your EMS, CLI, or TL1. The detailed procedures to upgrade and migrate the ISAM system using the Software Upgrade Automation Tool are contained in the NTPs and DLPs of this document.

Warning — When migrating the ISAM, Nokia recommends that you use the procedures in this document. Do not use the upgrade and migration procedures documented in any other documentation, including the EMS documentation.

Failure to use the Software Upgrade Automation Tool to migrate the ISAM can result in a failed upgrade or migration and can cause the system to become isolated.

Software management includes the following:

- OSWP
- general architecture
- software management procedure

32.3.1   OSWP

Software management is package based, that is, all the software files for the different components of the ISAM are grouped in an OSWP. Software management is related to the management of these OSWPs (download of a new OSWP, activation of an OSWP, and other activities). A maximum of two different OSWPs can be stored on the NT unit.

See "TNG 108 Overall SoftWare Package concept" for more information about OSWPs.

32.3.2   General architecture

The general architecture of the software management follows the manager-agent/ client-server model; see Figure 3.

Figure 3   **General software management architecture**
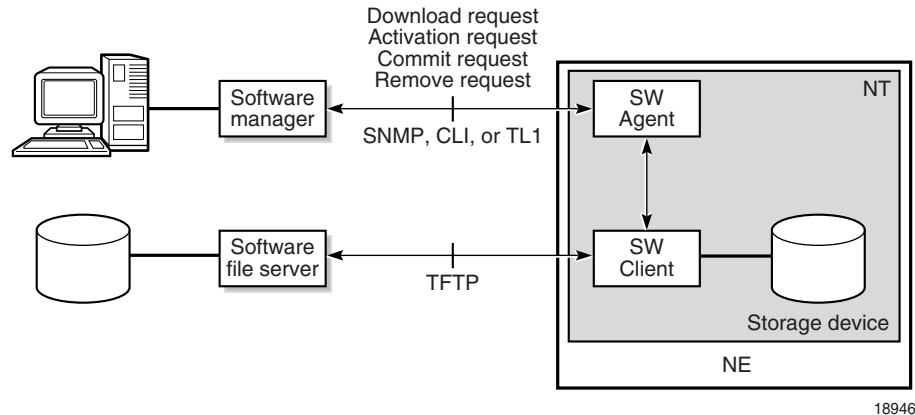
32.3.3   Software management procedure

Initially, the NE contains one OSWP. This OSWP is committed and its software is active in the system. New software for upgrade or migration is delivered on the software package.

The general procedure to install the software is as follows:

Note — See "NTP 100 Upgrade the software" and "NTP 101 Migrate the software" for the steps to upgrade and migrate software using the Software Upgrade Automation Tool.

1   If the active OSWP is not in Committed state, commit the software.

2   Install each OSWP in a specific directory on your server. To perform this task, repeat the following steps for each OSWP, in the order shown:

- Log in to the server.
- Create the directory where you want to store the software package (if the directory already exists, go to the directory).
- Load the software package.
- Copy the software from the package to the directory on the server.

3   Create an OSWP Descriptor file (see "TNG 110 Descriptor files" for the layout of this file). The OSWP Descriptor file must contain the following information about the different OSWPs:

- the path name of the OSWP
- the IP address of the TFTP server where the OSWP is stored

4   Download the OSWP. You can monitor the progress of the download. After the download process, two OSWPs are available on the NE: the currently active OSWP and the new downloaded OSWP. Make sure that the software file and SWP Descriptor file of a specific OSWP are stored in the same directory.

5   Activate the new OSWP.

The previously active OSWP remains available on the NE. Therefore, the NE can still roll back to the previously active OSWP in case you are not satisfied with the new OSWP.

6   If needed, commit the new OSWP. The previously active OSWP is then deleted from the NE software storage device (the NT unit).

Caution — Nokia does not recommend committing the software until you are ready to move to the next release of software. If you need to commit the software before the next release, ensure that the system is up and running, traffic has resumed, and you are satisfied with the performance of the new release before committing the software. You cannot roll back to a previous load after the software is committed. The previous load is deleted.

32.4   Database management

The ISAM can manage a maximum of three databases at the same time. Each stored database has a specific operational status with respect to each available OSWP (Active OSWP and NotActive OSWP). The different values of the operational status are listed in Table 32. Only one of the available databases is operational and each available OSWP is linked to a maximum of two available databases at the same time.

Table 32   **Operational status of a database corresponding to the available OSWPs**

Available OSWP	Value	Definition
Active: currently operational	Actual	The database is currently used by the Active OSWP.
	Preferable	The database has not been used yet, but will be used after a successful activation of the Active OSWP.
	Previous	The database has already been used by the Active OSWP. It corresponds to the previous Actual database of the Active OSWP.
	Failed	The database is compatible with the Active OSWP, but for some reason, for example, a corrupted database, the Active OSWP is not able to interpret the database.
	Not Useful	The database cannot, or may not, be used by the Active OSWP; for example, the database is not compatible.

(1 of 2)

Available OSWP	Value	Definition
NotActive: not operational	Actual	The database has not yet been used by the NotActive OSWP, and it is the first database for the NotActive OSWP. The database will be used after a successful activation of the NotActive OSWP.
		The database has already been used by the NotActive OSWP. The database will be used again after the successful activation of the NotActive OSWP, on the condition that there is no Preferable database available for the NotActive OSWP.
	Preferable	The database has not yet been used by the NotActive OSWP, and there is also an Actual database available for this OSWP. The Preferable database will be used after the successful activation of the NotActive OSWP.
	Previous	The database has already been used by the NotActive OSWP. It corresponds to the Previous database at the time the current NotActive OSWP was still active.
	Failed	The database is compatible with the NotActive OSWP, but for some reason, for example, a corrupted database, the NotActive OSWP was not able to interpret it.
	Not Useful	The database cannot, or may not, be used by the NotActive OSWP; for example, the database is not compatible.

(2 of 2)

The ISAM supports the following database management processes:

- the backup/restore process, which is always related to the database currently used by the Active OSWP
- the upload of one of the available databases from the system to a specified file server. You can request this at any time; see "TNG 109 Software database processes" for more information.
- the download of a new database from a specified file server to the system. You can request this at any time; see "TNG 109 Software database processes" for more information.

You can use these upload and download database processes to perform an offline database conversion when software is upgraded, but the new OSWP is not able to interpret the database currently used by the active OSWP:

1   Request the ISAM to transfer the currently used database to a specified file server.

2   Convert the database offline.

3   Request the ISAM to download this new, converted database from the specified file server.

33 TNG 108 Overall SoftWare Package concept

33.1 Introduction

This TNG provides information about the Overall SoftWare Package (OSWP).

Note — The OSWP and SWP files must be stored on the system where the components of the Software Upgrade Automation Tool are running in order for the OSWP to be read and the software directories to be accessed when minimizing the SWP.

33.2 OSWP composition

For a software upgrade of the ISAM, the operator must define the applicable ASAM-CORE software package (SWP).

An OSWP consists at least of:

- one Overall Descriptor file (also called the "OSWP Descriptor" file)
- one ASAM-CORE SWP

The composition of an OSWP is shown in Figure 4.

Figure 4   **Composition of an OSWP**
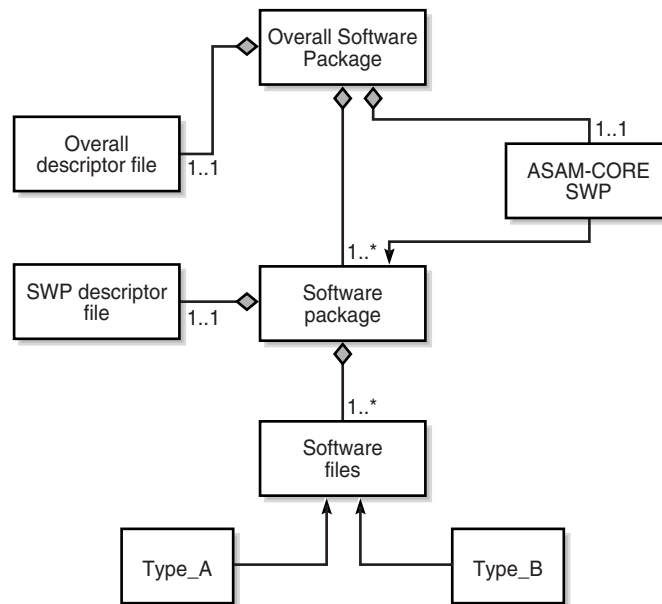
17669

The following sets of files exist for an OSWP:

- minimum set of files: the set of files that belong to the board types which the operator marked for inclusion during an OSWP download (even if the board type is not yet detected or planned in the NE)
- actual set of files: the complete set of files used by an OSWP in the active state (for example, files belonging to board types that are detected and/or planned at the moment of an OSWP download). This is the default set of files downloaded during an OSWP download action and is extendable by a set of files defined in the minimum set.
- complete set of files: all the files (used and unused) of an OSWP (not used due to CF size limitations)

33.2.1   Overall Descriptor file

The Overall Descriptor file (also called "OSWP Descriptor" file) contains information about the ASAM-CORE SWP that belongs to the OSWP. The following information is available:

- the path name of the ASAM-CORE SWP
- the IP address of the TFTP server(s) where the SWP can be found (primary file server and secondary file server).

The operator creates the OSWP Descriptor file. The OSWP Descriptor file is typically stored on a TFTP server managed by the operator.

The syntax and an example of an OSWP Descriptor file are shown in "TNG 110 Descriptor files".

33.2.2   ASAM-CORE SWP

The ASAM-CORE consists of the following:

- at least one SWP Descriptor file.
  The name of the SWP Descriptor file (L6GQAAxx.yyy) is equal to the name of the corresponding SWP.
- From R5401 onwards, an NT-SWP Descriptor mapping file (NT_SWP_Mapping.txt).This will indicate what SWP Descriptor file to use with what NT board type.
- at least one software (SW) file
  An SW file corresponds to an executable for a specific LT unit type.

33.2.3   SWP Descriptor File

An SWP Descriptor file contains the following information:

- the version number of the compatible database. This version number is also related to the database structure and the allowed database contents.
- for each supported card type, the SWP Descriptor file indicates whether:
  - the card expects the applicable SW files in a decompressed format
  - the related SW files belong to the minimum set of files of the considered OSWP
- for each applicable SW file of a specific card type, the SWP Descriptor file contains the file name, the file format, and the file size

The syntax and an example of an SWP Descriptor file are shown in "TNG 110 Descriptor files".

Note — Operators can use the minimum indication per board type to indicate that files of this board type should be included during an OSWP download although the board type is not detected or planned in the NE.

This is a helpful tool for long-term planning as the operator can avoid an OSWP re-download when introducing a new board type later within the same OSWP context or with plans to replace an existing board type with a new board type (for example, VDSL to vectoring - VDSL).

33.2.4   NT-SWP Descriptor mapping file

The NT-SWP Descriptor mapping file will indicate what SWP Descriptor file should be used for the NT board type used in a certain NE. The SWP Descriptor files all have the same cipher name (L6GQ) but use a different functional variant name (AA, AB, AC, etc…). The version of the file is the same as the ASAM-CORE SWP (xx.yyy).

Example of the NT-SWP Descriptor mapping file:

```
NANT-A L6GQAA54.364

NANT-D L6GQAA54.364

NANT-E L6GQAA54.364

NRNT-A L6GQAA54.364

AGNT-A L6GQAA54.364

FANT-F L6GQAB54.364

FANT-G L6GQAB54.364
```

In this example the FANT-F and FANT-G NT types, together with the supported LT board types, will be described in a different SWP Descriptor file.

It is important that the correct SWP Descriptor file is referred from the OSWP Descriptor file and that any "minimal set of files" requirement is updated in the correct SWP Descriptor file.

33.3   OSWP-database relationship

A maximum of two different OSWPs and three different ASAM-CORE databases can be stored persistently in the system at any time. Each ASAM-CORE database structure is identified by its version number, which is related to the database structure and to the allowed database contents.

Each ASAM-CORE SWP Descriptor file specifies the version number of the database that can be interpreted by the ASAM-CORE SWP. An OSWP will be linked to a specific ASAM-CORE SWP database when the version number reference inside the corresponding ASAM-CORE SWP Descriptor file is identical to the version number mentioned in the database.

The relationship between OSWPs and the ASAM-CORE database version number is a "one-to-one" relationship; see Figure 5. Each ASAM-CORE database (version number) can be interpreted by one OSWP, and a specific OSWP can only interpret one ASAM-CORE database (version number).

Figure 5   **One-to-one relationship between OSWPs and ASAM-CORE database**
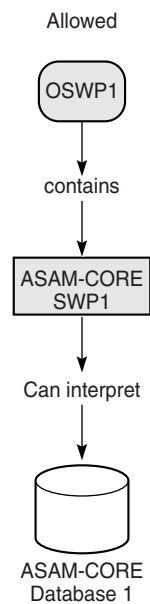
33.4   OSWP naming conventions

Table 33 lists the naming conventions of the OSWP for the ISAM. The OSWP name identifies the system (7302 ISAM, 7330 ISAM FTTN, 7360 ISAM FX, 7356 ISAM FTTB in stand-alone mode, or 7367 ISAM SX/DX), the type of OSWP (full, reduced, or minimized), the software release, and the software package number. These naming conventions apply to the OSWP on the EMS server and on the NT units.

Warning — To prevent problems when running the Software Upgrade Automation Tool, do not manually rename an OSWP.

Note — When specifying the path to the OSWP on the EMS server, always specify the path relative to the top directory defined in the configuration file; see "Transfer protocols and top directory" for more information.

Table 33   **OSWP naming conventions**

Type of OSWP	Suffix	OSWP name [1]
Full OSWP [4]	AA	L6GPAA*xx.yyy*

(1 of 2)

Type of OSWP	Suffix	OSWP name [1]
Minimized OSWP [2]	ZA	L6GPZA*xx.yyy*
Reduced OSWP [3][5]	RA	L6GPRA*xx.yyy*

(2 of 2)

Notes

[1] *xx* is the 2-digit ISAM software release number. *yyy* is the 3-digit ISAM software package number (for example, L6GPAA40.046).

[2] OSWP minimized using the automated software minimization tool; see "TNG 106 Additional automated tools" for more information. The OSWP name suffix is automatically changed to ZA by the automated software minimization tool.

[3] Active OSWP on NT unit reduced by the automated software download tool; see "TNG 101 Automated software download tool" for more information. The OSWP name suffix is automatically changed to RA by the automated software download tool.

[4] For 7367 ISAM SX/DX, only full OSWP is applicable.

[5] For 7363 ISAM MX reduced OSWP is not applicable and not supported

34 TNG 109 Software database processes

34.1 Introduction

This TNG describes the possible state transitions of an OSWP and the following SWDB processes:

- Downloading a new OSWP
- Redownloading an active OSWP
- Deleting an OSWP
- Activating an OSWP
- Committing a new OSWP
- Downloading an individual file
- Deleting an individual file
- Upgrading software on an individual card
- Uploading a database
- Downloading a database
- Clearing all databases

The following conditions must be established to complete one of these SWDB processes:

- the management channel must be established between the system and the manager
- the NE must not be involved in another SWDB process

34.2 Possible state transitions of an OSWP

The ISAM can handle two OSWPs simultaneously. Figure 6 shows the possible state transitions of these two OSWPs. The messages with the first word in uppercase correspond to requests from the management station. The other messages correspond to internal system events.

Figure 6 **Possible state transitions of an OSWP**
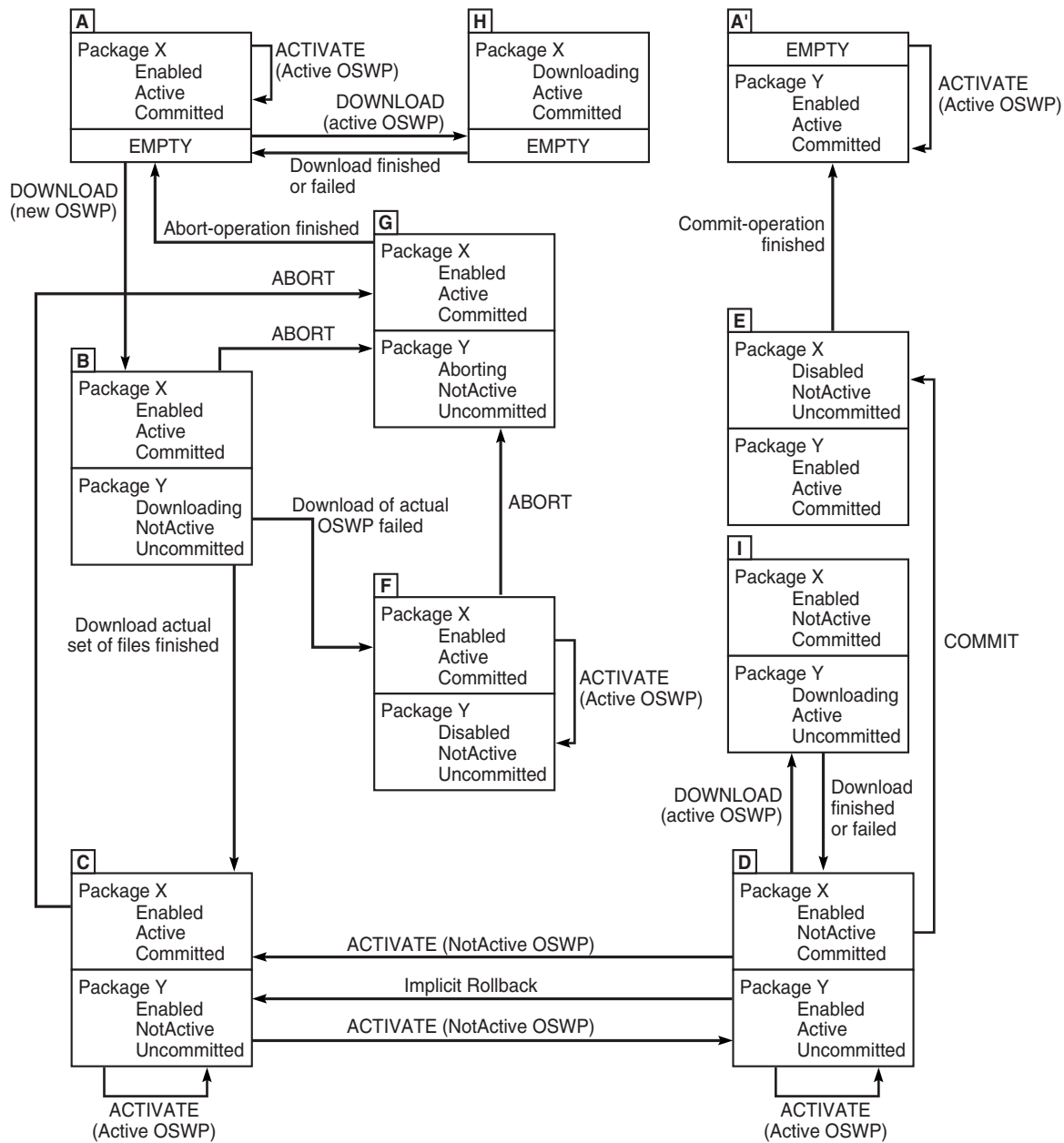
18869

Table 34 describes each of the possible OSWP state values.

Table 34   **OSWP state values**

State value	Description
Enabled	The OSWP is ready to become Active or is already Active. All files of the OSWP are available on the system.
Disabled	The OSWP cannot become Active since at least one of the files is not available on the system.
Downloading	The OSWP cannot become Active since the download of the requested set of files is still going on.
Aborting	The system is still busy removing the files that do not belong to the current Active OSWP from the disk file.
Active	The OSWP is currently operational.
NotActive	The OSWP is not operational.
Committed	The Active OSWP is committed and the NonActive OSWP is deleted from the system.
Uncommitted	The Active OSWP is not committed and can be replaced by the NonActive OSWP if needed.

34.3   Downloading a new OSWP

The following phases can occur during the download process of an OSWP:

Note — As of R04.03.02, the current active OSWP is minimized autonomously to make room for the new downloaded OSWP (to avoid the state transition B to F as shown in Figure 6). The active OSWP will be minimized up to the files for the NT and the planned and/or detected LT boards.

- Evaluation of the download request
- Download and interpretation of the files
- Interruption of the download by the system
- Interruption of the download by the manager
- Result of a successful download of the new OSWP

34.3.1   Evaluation of the download request

The manager initiates the download of an OSWP. The download request must contain the following information:

- the IP addresses of the each TFTP server where the OSWP Descriptor file can be found
- the path name of the corresponding OSWP Descriptor file
- the set of files the management station wants to have available on the system before activating the new OSWP

The download request is only accepted if the system is in state A in Figure 6:

- state of current OSWP: Enabled, Active, and Committed.
- state of new OSWP: Empty

After the download request is accepted, the download process starts.

34.3.2   Download and interpretation of the files

The manager can monitor the progress of the download process step-by-step. During the download, the system is in state B in Figure 6:

- status of current OSWP: Enabled, Active, and Committed
- status of new OSWP: Downloading, NotActive, and Uncommitted

Table 35 shows the different phases in a download process.

Table 35   **Download and interpretation of the files**

Phase	Description
1	After the download request is accepted, the system downloads the OSWP Descriptor file of the specified OSWP from the specified TFTP server. The location of this TFTP server is specified in the download request.
2	The OSWP Descriptor file specifies the different SWPs that belong to the considered OSWP. Based on the specified SWPs, the system downloads the different SWP Descriptor files (via TFTP). Mind that in the current use of the system, only one single SWP Descriptor will be in use, that is the one for the ASAM-CORE SWP.
3	Each SWP Descriptor file specifies the different applicable software file or files and whether they belong to the minimum set of the OSWP. The system downloads the software files that are specified in the downloaded SWP Descriptor files on the following conditions: • sufficient resources are available for their persistent storage • the software file is not yet available in the system • the software file belongs to the set requested by the management station The system downloads the selected software files in the following order: • software files that belong to the minimum set of the new OSWP • software files that belong to the actual set, but not to the minimum set of the OSWP (if requested by the manager) • software files that belong to the complete set, but not to the actual set of the OSWP (if requested by the manager)

34.3.3   Interruption of the download by the system

The download of a new OSWP can be interrupted by the system or by the manager. The following are possible cases when the system can interrupt the download process:

- the system does not have enough resources to store the selected software files
- the system cannot download the OSWP Descriptor file
- the system cannot interpret the OSWP Descriptor file because of a syntax error
- the system cannot download one of the selected SWP Descriptor files
- the system cannot interpret one of the selected SWP Descriptor files because of a syntax error
- the system cannot download one of the selected software files

The manager can query the system to find out the exact reason the download process was interrupted.

The previously downloaded files (software files, software Descriptor files) are not removed by the system. The following situations are possible, depending on the files already downloaded:

- State C in Figure 6: all the files that belong to the actual set of files (files that belong to the minimum set or to board types that are planned and/or detected in the system) of the new OSWP are available in the system:
    - status of current OSWP: Enabled, Active, and Committed
    - status of new OSWP: Enabled, NotActive, and Uncommitted
- State F in Figure 6: some files that belong to the actual set of files of the new OSWP are not available in the system:
    - status of first (current) OSWP: Enabled, Active, and Committed
    - status of second (new) OSWP: Disabled, NotActive, and Uncommitted

34.3.4   Interruption of the download by the manager

The download of a new OSWP can be interrupted by the system or by the manager. When the manager requests the system to abort the ongoing download process, the system starts to delete all the files that do not belong to the current OSWP from the file disk. The system is in state G in Figure 6:

- status of current OSWP: Enabled, Active, and Committed
- status of new OSWP: Aborting, NotActive, and Uncommitted

When the deletion of all the files is complete, the system is back in state A in Figure 6.

34.3.5   Result of a successful download of the new OSWP

The system is in state C of Figure 6:

- status of current OSWP: Enabled, Active, and Committed
- status of new OSWP: Enabled, NotActive, and Uncommitted

34.4   Redownloading an active OSWP

In cases when a new card or cards has been installed in the system and the software for the new card or cards is not available in the Active OSWP, the manager initiates a redownload of the Active OSWP to get the software for the new card or cards.

The following phases can occur during the redownload process of an OSWP:

- Evaluation of the redownload request
- Redownload and interpretation of the files
- Interruption of the redownload
- Result of a successful redownload of the new OSWP

34.4.1   Evaluation of the redownload request

The manager initiates the redownload of an OSWP. The redownload request must contain the following information:

- the IP addresses of the each TFTP server where the OSWP Descriptor file can be found
- the path name of the corresponding OSWP Descriptor file
- the set of files the management station wants to have available on the system before activating the new OSWP

The download request is only accepted if the system is in state A or D in Figure 6:

- State A:
  - status of current OSWP: Enabled, Active, and Committed
  - status of new OSWP: Empty
- State D:
  - status of current OSWP: Enabled, NotActive, and Committed
  - status of new OSWP: Enabled, Active, and Uncommitted

After the redownload request is accepted, the redownload process starts.

34.4.2   Redownload and interpretation of the files

The manager can monitor the progress of the download process step-by-step. During the download, the system is in state H or I in Figure 6:

- State H:
  - status of current OSWP: Downloading, Active, and Committed
  - status or new OSWP: Empty
- State I:
  - status of current OSWP: Enabled, NotActive, and Committed
  - status of new OSWP: Downloading, Active, and Uncommitted

Table 36 shows the different phases in a redownload process.

Table 36   **Redownload and interpretation of the files**

Phase	Description
1	After the redownload request is accepted, the system downloads the OSWP Descriptor file of the specified OSWP from the specified TFTP server. The location of this TFTP server is specified in the redownload request.
2	The OSWP Descriptor file specifies the different SWPs that belong to the considered OSWP. Based on the specified SWPs, the system downloads the different SWP Descriptor files (via TFTP).

(1 of 2)

Phase	Description
3	Each SWP Descriptor file specifies the different applicable software file or files and whether they belong to the minimum set of the OSWP.
	The system downloads the software files that are specified in the downloaded SWP Descriptor files on the following conditions:
	• sufficient resources are available for their persistent storage
	• the software file is not yet available in the system
	• the software file belongs to the set requested by the management station
	The system downloads the selected software files in the following order:
	• software files that belong to the minimum set of the new OSWP
	• software files that belong to the actual set, but not to the minimum set of the OSWP (if requested by the manager)
	• software files that belong to the complete set, but not to the actual set of the OSWP (if requested by the manager)

(2 of 2)

34.4.3   Interruption of the redownload

The download of a new OSWP can only be interrupted by the system. The following are possible cases when the system can interrupt the download process:

- the system does not have enough resources to store the selected software files
- the system cannot download the OSWP Descriptor file
- the system cannot interpret the OSWP Descriptor file because of a syntax error
- the system cannot download one of the selected SWP Descriptor files
- the system cannot interpret one of the selected SWP Descriptor files because of a syntax error
- the system cannot download one of the selected software files

The manager can query the system to find out the exact reason the download process was interrupted.

The previously downloaded files (software files, software Descriptor files) are not removed by the system. The following situations are possible, depending on the files already downloaded:

- State C in Figure 6: all the files that belong to the actual set of files (files that belong to the minimum set or to board types that are planned and/or detected in the system) of the new OSWP are available in the system:
    - status of current OSWP: Enabled, Active, and Committed
    - status of new OSWP: Enabled, NotActive, and Uncommitted
- State F in Figure 6: some files that belong to the actual set of files of the new OSWP are not available in the system:
    - status of first (current) OSWP: Enabled, Active, and Committed
    - status of second (new) OSWP: Disabled, NotActive, and Uncommitted

34.4.4   Result of a successful redownload of the new OSWP

After the redownload, the system remains in the same state as it was before the process, but with new software files in the Active OSWP.

34.5   Deleting an OSWP

The download of a new OSWP is only possible when only one OSWP is available in the system. Therefore, in some cases the manager must first request the system to delete one of the available OSWPs before it can initiate a new download process.

The following phases can occur during the deletion of an OSWP:

- Evaluation of the deletion request
- Deletion process
- Result of a successful deletion process

34.5.1   Evaluation of the deletion request

The deletion of an OSWP can only be initiated when the system is in state C or F in Figure 6:

- State C:
  - status of current OSWP: Enabled, Active, and Committed
  - status of new OSWP: Enabled, NotActive, and Uncommitted
- State F:
  - status of current OSWP: Enabled, Active, and Committed
  - status of new OSWP: Disabled, NotActive, and Uncommitted

34.5.2   Deletion process

The system starts to delete all the persistent stored files (Descriptor files and software files) and databases that are related to the NotActive OSWP. The system is in state G in Figure 6 during this process:

- status of current OSWP: Enabled, Active, and Committed
- status of new OSWP: Aborting, NotActive, and Uncommitted

34.5.3   Result of a successful deletion process

The system is in state A in Figure 6:

- status of current OSWP: Enabled, Active, and Committed
- status of new OSWP: Empty

The Active OSWP is the only OSWP in the system. Only Descriptor files, software files, and databases related to this OSWP are stored persistently in the system.

34.6   Activating an OSWP

The exact activation procedure depends on the status of the OSWP that must be activated. The following situations can occur:

- Activating a NotActive OSWP
- Activating an Active OSWP

34.7   Activating a NotActive OSWP

The following phases can occur during the activation process of a NotActive OSWP:

- Evaluation of the activation request
- Activation of the database
- Result of a successful activation

Note — On 7360 ISAM FX, the activation of a NotActive OSWP goes in two steps:

- SW download from NT to the LTs, while system remains operationally up, there is no service interruption yet the management interface is not accepting configuration commands.
- SW activation, with service interruption

34.7.1   Evaluation of the activation request

The activation can only start when the current and new OSWPs are in state C (for new OSWP) or D (for current OSWP) in Figure 6:

- State C:
    - status of current OSWP: Enabled, Active, and Committed
    - status of new OSWP: Enabled, NotActive, and Uncommitted
- State D:
    - status of current OSWP: Enabled, NotActive, and Committed
    - status of new OSWP: Enabled, Active, and Uncommitted

34.7.2   Activation of the database

The manager can request the system to activate the NotActive OSWP as follows:

- activate the NotActive OSWP with a compatible database

  The system starts the activation process as shown in Table 37. If the system does not find any compatible database linked to the NotActive OSWP, the activation request is refused.

- activate the NotActive OSWP with the default database

  The system starts the activation process as shown in Table 38.

Table 37   **Activation of a NonActive OSWP with a compatible database**

Phase	Description
1	The system selects from the available databases the database that is compatible with, and linked to, the NotActive OSWP.
2	For each detected and unplanned card that belongs to a card type supported by the NotActive OSWP, the software files of the NotActive OSWP become Active. (Not applicable to 7367 ISAM SX/DX.)
3	For each detected and planned card that belongs to a card type supported by the NotActive OSWP, the software files of the NotActive OSWP become Active on the condition that the card is not locked and no card-type mismatch alarm exists on this card. For 7367 ISAM SX/DX, the software files of the Not Active OSWP become unconditionally active.
4	For each detected card that belongs to a card type that is not supported by the NotActive OSWP, the card goes in Boot mode. The system reports this to the manager. (Not applicable to 7367 ISAM SX/DX.)
Implicit software rollback: If the system cannot activate the NotActive OSWP, it immediately interrupts the activation process and reactivates the current Active OSWP on all the cards. This also includes the cards for which an individual software upgrade was requested before the start of the activation procedure; see "Upgrading software on an individual card". The implicit software rollback is reported to the manager.	

Table 38   **Activation of a NonActive OSWP with the default database**

Phase	Description
1	The system creates a default database based on the detected cards.
2	For each detected and unplanned card that belongs to a card type supported by the NotActive OSWP, the software files of the NotActive OSWP become Active. (Not applicable to 7367 ISAM SX/DX.
3	For each detected and planned card that belongs to a card type supported by the NotActive OSWP, the software files of the NotActive OSWP become Active on the condition that the card is not locked and no card-type mismatch alarm exists on this card. For 7367 ISAM SX/DX, the software files of the Not Active OSWP become unconditionally active.
4	For each detected card that belongs to a card type that is not supported by the NotActive OSWP, the card goes in Boot mode. The system reports this to the manager. (Not applicable to 7367 ISAM SX/DX.)
Implicit software rollback: If the system cannot activate the NotActive OSWP, it immediately interrupts the activation process and reactivates the current Active OSWP on all the cards. This also includes the cards for which an individual software upgrade was requested before the start of the activation procedure; see "Upgrading software on an individual card". The implicit software rollback is reported to the manager.	

34.7.3 Result of a successful activation

The system goes from state C to D (new OSWP) or from state D to C (current OSWP) in Figure 6, together with the selected compatible database or the default database.

- State C:
  - status of current OSWP: Enabled, Active, and Committed
  - status of new OSWP: Enabled, NotActive, and Uncommitted
- State D:
  - status of current OSWP: Enabled, NotActive, and Committed
  - status of new OSWP: Enabled, Active, and Uncommitted

The system does not remove the Descriptor files, software files, and databases related to the NotActive OSWP. This makes it possible for the manager to return to the previous Active OSWP, in case the manager is not confident with the new activated OSWP.

34.8 Activating an Active OSWP

The activation of the Active OSWP is typically used during the backup and restore procedure of a database. After the restore operation, at least two different databases are available:

- the current (active) database
- the new downloaded (restored) database

Both databases have the same version number and are compatible with the Active OSWP. The restored database will be linked to the Active OSWP and selected during the activation of the Active OSWP.

The following phases can occur during the activation process of an Active OSWP:

- Evaluation of the activation request
- Activation of the database
- Result of a successful activation

34.8.1 Evaluation of the activation request

The activation can only start when the current and new OSWP have the conditions as defined in state A, A', C, F, or D in Figure 6:

- State A:
  - status of current OSWP: Enabled, Active, and Committed
  - status or new OSWP: Empty
- State A':
  - status of current OSWP: Empty
  - status of new OSWP: Enabled, Active, and Committed

- State C:
  - status of current OSWP: Enabled, Active, and Committed
  - status of new OSWP: Enabled, NotActive, and Uncommitted
- State D:
  - status of current OSWP: Enabled, NotActive, and Committed
  - status of new OSWP: Enabled, Active, and Uncommitted
- State F:
  - status of current OSWP: Enabled, Active, and Committed
  - status of new OSWP: Disabled, NotActive, and Uncommitted

34.8.2   Activation of the database

The activation process of an Active OSWP is less complex than the activation process of a NotActive OSWP because data checking is not needed. The system already contains a linked database that is compatible with the Active OSWP.

The manager can request the system to activate the Active OSWP as follows:

- the system selects from the available databases the database that is compatible with and linked the Active OSWP

  The system starts the activation process as shown in Table 39.
- the system activates the Active OSWP with the default database; the system creates a default database based on the detected cards

  The system starts the activation process as shown in Table 40.

Table 39   **Activation of an Active OSWP with a compatible database**

Phase	Description
1	The system selects from the available databases the database that is compatible with, and is linked to, the Active OSWP. The system will select the Preferable database if there is one; if there is no Preferable database, the system will select the Actual database. [1]
2	The software files of the Active OSWP are not reloaded on the different cards. The cards keep running.
Implicit software rollback: If the system cannot interpret the linked database, it reactivates the Active OSWP together with the previously used database. The implicit database rollback is reported to the manager.	

Note
[1]   See Table 32 for a description of the different values of the operational status of databases.

Table 40   **Activation of an Active OSWP with the default database**

Phase	Description
1	The system creates a default database based on the detected cards.

(1 of 2)

Phase	Description
2	The software files of the Active OSWP are not reloaded on the different cards. The cards keep running.

(2 of 2)

34.8.3   Result of a successful activation

After the activation, the system remains in the same state as it was before the process, but with the Active OSWP linked to another database (a compatible database or the default database).

34.9   Committing a new OSWP

The following phases can occur during the commitment process of an Active OSWP:

- Evaluation of the commitment request
- Commitment process
- Result of the commitment process

34.9.1   Evaluation of the commitment request

The commitment can only start when the system is in state D of Figure 6:

- status of current OSWP: Enabled, NotActive, and Committed
- status of new OSWP: Enabled, Active, and Uncommitted

34.9.2   Commitment process

After the commit request is accepted, the system removes all persistent stored Descriptor files, software files, and databases that are not related to the Active OSWP.

The system is in state E of Figure 6 during this process:

- status of current OSWP: Disabled, NotActive, and Uncommitted
- status of new OSWP: Enabled, Active, and Committed

The commitment process only implies a status change of the Active OSWP and can never fail.

34.9.3 Result of the commitment process

The system is in state A' of Figure 6:

- status of current OSWP: Empty
- status of new OSWP: Enabled, Active, and Committed

The Active OSWP is the only OSWP in the system.

34.10 Downloading an individual file

To make testing easier, the manager can download individual Descriptor files and software files on the system via TFTP.

The request from the manager to download an individual file is refused if:

- no resources are available for the storage of the file
- the file is already available in the system

34.11 Deleting an individual file

The manager can remove individual software files. All stored files can be removed individually, except the SWP/OSWP Descripter files or the files that belong to the NT file set.

34.12 Upgrading software on an individual card

The concept of an OSWP implies that the entire system is upgraded at the same time. The software cannot be upgraded on an individual card while the software on all the other cards of the same card type remains unchanged.

Note — Upgrading software on an individual card is not applicable to 7367 ISAM SX/DX.

However, it is possible to upgrade the software files on an individual card for the following type of cards:

- LT units
- NTIO units

The system only accepts a request to download software for an individual card if the system is in state C or D in Figure 6.

- State C:
    - status of first OSWP: Enabled, Active, and Committed
    - status of second OSWP: Enabled, NotActive, and Uncommitted

- State D:
  - status of first OSWP: Enabled, NotActive, and Committed
  - status of second OSWP: Enabled, Active, and Uncommitted

When the manager requests an upgrade to the software on individual cards, all these cards are reloaded with the applicable software files of the NotActive OSWP, even when these files do not differ from the current active files. The active software files on all other cards still belong to the Active OSWP. The status of the two available OSWPs in the system does not change.

The system refuses the upgrade request in the following cases:

- the system detects that the selected card belongs to a card type that is not supported by the NotActive OSWP
- the selected card belongs to a supported NT unit type
- the selected card belongs to a supported LT unit or NTIO type, but the card is blocked or there is a card type mismatch for the card
- the software files of the NotActive OSWP on the selected card are not compatible with the current active NT unit software files and the current active database

If the selected card for a software upgrade runs in Boot mode, the system reports this to the manager.

34.13   Uploading a database

The manager initiates the upload of a database. The database upload can be part of a binary backup and restore procedure, or a software upgrade or migration procedure.

The manager can request an upload of a database from the system to an FTP, SFTP, or TFTP server or to the management station of the manager.

34.13.1   Upload to an FTP, SFTP, or TFTP server

The manager requests that the system uploads one of its available databases from the system to a server via FTP SFTP, or TFTP. The database upload request must contain the following information:

- the identification of the database that needs to be uploaded
- the identification of the TFTP server where the database must be sent
- the directory path on the selected TFTP server to the directory where the uploaded database must be stored

The manager can monitor the progress of the upload process.

The upload of the database is aborted if:

- the system does not find the specified database
- the system finds the specified database, but is not able to transfer it successfully to the TFTP server

34.13.2   Upload to the manager

The manager requests that the system uploads one of its available databases from the system to its management station via FTP SFTP, or TFTP. This database upload request contains the identification of the database that needs to be uploaded.

Any other manager can monitor the progress of the upload process.

The upload of the database is aborted if:

- the system does not find the specified database
- the system finds the specified database, but is not able to transfer it successfully to the manager

34.14   Downloading a database

The manager initiates the download of a database. The database download can be part of a binary backup and restore procedure, or a software upgrade or migration procedure.

The manager can request a download of a database from an FTP SFTP, or TFTP server or the management station of the manager to the system.

34.14.1   Download from an FTP SFTP, or TFTP server

The manager requests that the system downloads a database from a server to the system via FTP SFTP, or TFTP. The database download request must contain the following information:

- the identification of the database that needs to be downloaded
- the identification of the server where the database is stored

The system stores the complete database persistently and links it to the compatible OSWPs.

The download of the database fails if:

- the system is not able to contact the server
- the TFTP server cannot download the requested database to the system

34.14.2   Download from the management station

The manager requests that the system downloads a database from its management station to the system via FTP SFTP, or TFTP. This database download request must contain the identification of the database that needs to be downloaded.

The system stores the complete database persistently and links it to the compatible OSWPs. Any other manager can monitor the progress of the download process.

The download of the database fails if the management station is not able to download the database successfully to the system.

34.15   Clearing all databases

The manager can send a request to the system to clear all databases. Table 41 shows the different phases of the process to clear all databases.

The system must have an Active OSWP linked to one of the available (and compatible) databases and cannot have a second OSWP present in the system.

Table 41   **Process to clear all databases**

Phase	Description
1	The system first removes all the persistent stored files that do not belong to the Active OSWP.
2	The system also makes sure that all the files that belong to the complete set of the Active OSWP are stored persistently.
3	The system removes the links between the OSWP and the available databases and replaces them with a link to the default database.
4	The system goes into shutdown mode. The management channel between the system and the manager is torn down.

35 TNG 110 Descriptor files

35.1 Introduction

This TNG describes the syntax and grammar of the OSWP Descriptor file and the SWP Descriptor file, and provides examples. These are both ASCII files.

Note — You create the OSWP Descriptor file before performing an upgrade or migration. The SWP Descriptor file is delivered by Nokia and you do not need to change this file.

35.2 Examples

The following are examples of an OSWP Descriptor file and an SWP Descriptor file.

35.2.1 Example of an OSWP Descriptor file

The following is an example of the required OSWP Descriptor file. You create the OSWP Descriptor file when performing an upgrade or migration.

```
OVERALL-DESCRIPTOR-FILE OSWPAA24.005 BEGIN

 SYNTAX-VERSION: 01.00 ;

 ASAM-CORE: /ASAM-CORE/L6GQAA24.005/L6GQAA24.005 123.65.1.2 123.65.1.4 ;

END
```

35.2.2   Example of an SWP Descriptor file

The following is an example of an SWP Descriptor file.

```
DESCRIPTOR-FILE L6GQAA24.005

BEGIN

   SYNTAX-VERSION : 01.00;

   TARGET         : ASAM-CORE;

   DBASE-VERSION  : A2.400;

   DESCRIPTION ECNT-A

   BEGIN

      COMPRESSION : YES;

      MINIMUMSET  : YES;

      TYPE-A       : L6GSAA24.005 22 ASCII;

      TYPE-A       : L6GTAA24.005 2 ASCII;

      TYPE-A       : L6GUAA24.005 16 ASCII;

      TYPE-A       : L6GVAA24.005 16 ASCII;

      TYPE-A       : MERYAA24.005 1393263 ASCII;

      TYPE-A       : L5YXAA20.518 51960 EXE;

      TYPE-B       : L5YYAA24.005 5909271 EXE;

      TYPE-G       : MJN5AA24.005 138752 TAR;

      TYPE-H       : MA6YAA24.062 3504814 EXE;

   END

   DESCRIPTION EVLT-E

   BEGIN

      COMPRESSION : NO;

      MINIMUMSET  : YES;

      TYPE-A       : MLQNAA22.001 537384 TAR;

      TYPE-B       : ME9TAA24.005 3041500 LZ77;

   END

END
```

36 TNG 111 Automated software rollback tool

36.1   Introduction

This TNG provides information about the syntax and parameters of the automated software rollback tool used to roll back the ISAM software after a software upgrade or migration. See "TNG 100 Software Upgrade Automation Tool" for general information about the Software Upgrade Automation Tool, the configuration file, the hosts file and the log files.

36.2   Automated software rollback tool

The automated software rollback tool is the component of the Software Upgrade Automation Tool used to roll back the software on one or more NEs after a software upgrade or migration.

If the software on the ONTs was upgraded during the NE software upgrade or migration, rolling back the NE software also rolls back the software on the ONTs.

The automated software rollback tool automatically performs the following steps for each NE specified:

1   Verifies the connection to the NE.

2   Opens an SNMP session, disabling object identifier translation.

3   Logs in to the NE using CLI.

4   Retrieves the status of the active OSWP. Terminates the rollback if the desired software load is already active.

5   Checks whether the passive OSWP is in enabled state and committed with the expected software load.

6   Performs the rollback by activating the passive OSWP with the respective database.

7   Waits for the NE to restart and become active.

8   Checks whether the NE is up with the desired software load.

9   Logs out of the NE.

You can roll back software on either a single NE or on multiple NEs using a single session or multiple parallel sessions; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 111 Automated software rollback tool" for more information.

Note — From R4.5.02 onward, you can choose the option to use a second CLI password when using CLI over SSH configurations, in case the first CLI password should fail. See "TNG 100 Software Upgrade Automation Tool" for more information.

36.3 Command syntax

The syntax of the automated software rollback tool is:

Note — When using the 5520 AMS, the perl script must be run as $AMS_PERL_DIR/perl <scriptname>.pl.

```
./rollback.pl --isam nt_ip_address | --hosts hosts_filename [--sessions
#sessions] --swp OSWPpath/OSWPnamexx.yyy --logfile rollbacklogpath/logname |
--id runid [--cliusername CLIuser][--clipassword CLIpwd] [--clipassword2
SecondCLIpwd][--seplog | --noseplog][--debug] [--noname] [--comm commstring]
[--noping] [--v2] [--v3auth auth_username:auth_pwd:auth_protocol] [--v3priv
priv_protocol:priv_pwd] [--v]
```

or

```
perl rollback.pl --isam nt_ip_address | --hosts hosts_filename [--sessions
#sessions] --swp OSWPpath/OSWPnamexx.yyy --logfile rollbacklogpath/logname |
--id runid [--cliusername CLIuser][--clipassword CLIpwd] [--clipassword2
SecondCLIpwd][--seplog | --noseplog] [--debug] [--noname] [--comm
commstring] [--noping] [--v2] [--v3auth
auth_username:auth_pwd:auth_protocol] [--v3priv priv_protocol:priv_pwd]
[--v]
```

36.4 Command parameters

Table 42 describes the parameters of the automated software rollback tool.

Table 42   **Automated software rollback tool parameters**

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--isam *nt_ip_address*	The IP address or name of the NE when you roll back software on a single NE only. When this parameter is used, the automated software rollback tool rolls back only the software on the NE specified by the --isam parameter, and ignores the --sessions and --hosts parameters. [1]	Mandatory	—
--hosts *hosts_filename*	The file listing the IP addresses and names of the NEs when you roll back software on multiple NEs; see "Hosts file" in "TNG 100 Software Upgrade Automation Tool" for more information. This parameter is ignored if the --isam parameter is used. [1]	—	Mandatory

(1 of 3)

Parameter	Description	Parameter type	
		Single NE	Multiple NEs
--sessions #*sessions*	The number of parallel sessions when you roll back software for multiple NEs; see "Installing and using the components of the Software Upgrade Automation Tool" in "TNG 100 Software Upgrade Automation Tool" for more information. This parameter is ignored if the --isam parameter is used. This value cannot exceed the value set for the maximum number of parallel software downloads parameter in the configuration file; see Table 18 for more information.	—	Mandatory
--swp *OSWPpath*/ *OSWPnamexx.yyy*	The location and filename of the new OSWP. *OSWPpath*/*OSWPname* is the path and filename of the new OSWP package. When minimized, the OSWP suffix is ZN; see see "TNG 108 Overall SoftWare Package concept" for more information. *xx* is the 2-digit software release number *yyy* is the 3-digit software package number (for example, L6GPAA40.046).	Mandatory	Mandatory
--logfile *rollbacklogpath/logname*	The path and filename of the resulting log file. When this parameter is used, the --id parameter is ignored.	Mandatory	Mandatory
--id *runid*	This parameter is used by the 5529 LRM instead of the --logfile parameter to generate a log file and a results file when you roll back software on a single NE. This parameter cannot be used when you roll back software on multiple NEs. The filenames of the resulting files are *runid*_COMT.log and *runid*_COMT.result, where *runid* is the 5529 LRM run identification number. This parameter is ignored if the --logfile parameter is used.	—	—
--cliusername *CLIuser*	The CLI username if different from the one specified in the configuration file; see Table 18 for more information. When rolling back software on multiple NEs, all the NEs must have a common CLI username.	Optional	Optional
--clipassword *CLIpwd* --clipassword2 *SecondCLIpwd*	The CLI password, if different from the one specified in the configuration file; see Table 18 for more information. When rolling back software on multiple NEs, all the NEs must have a common CLI password. The second CLI password will be used only in the case when CLI over SSH is configured. The second CLI password specifies an alternative password to be used when the first CLI password fails to connect to one or more NEs. This value is encrypted in the configuration file.	Optional	Optional

(2 of 3)

Parameter	Description	Parameter type	
		Single NE	**Multiple NEs**
--seplog | --noseplog	Determines where the log information is stored for each NE listed in the hosts file. Use --seplog to create a separate log file for each NE listed in the hosts file, and --noseplog to create a single log file for all sessions. See "Log files" in "TNG 100 Software Upgrade Automation Tool" for more information about log files.	—	Optional
--debug	Instructs the automated software rollback tool to add additional troubleshooting information to the log file.	Optional	Optional
--noname	Instructs the automated software rollback tool to use the IP address of the NE when creating the output directory, instead of the NE name. This parameter is used by the 5529 LRM.	—	—
--comm *commstring*	The SNMP community string used by the automated software rollback tool when communicating with an NT unit using SNMP version 1 or version 2C. When this parameter is not specified, the tool uses the NT community string value specified in the configuration file; see Table 18 for more information.	Optional	Optional
--noping	Instructs the tool to use SNMP instead of ping to verify if the NE is reachable. Use this parameter when the use of ping is not allowed in the network.	Optional	Optional
--v2	Instructs the tool to use SNMP version 2C for data transfers between the SNMP agent and the SNMP manager.	Optional	Optional
--v3auth *auth_username*:*auth_pwd*:*auth_protocol*	Instructs the tool to use SNMP version 3 for data transfers between the SNMP agent and the SNMP manager. *auth_username* is the session authentication username, *auth_pwd* is the authentication password (at least 8 characters long), and *auth_protocol* is the authentication protocol (SHA or MD5).	Optional	Optional
--v3priv *priv_protocol*:*priv_pwd*	Sets the privacy protocol (DES, 3DES, or AES) and the privacy password (at least 8 characters long) for SNMP version 3.	Optional	Optional
--v	Instructs the automated software tool to show the version number of the tool. The output shows the version of the automated tool as well as the versions of the applications used by the tool.	Optional	Optional

(3 of 3)

Note

(1)   If neither the --isam or --host parameter is used, the tool will roll back software for all the NEs listed in the hosts file specified in the configuration file; see "Configuration file" in "TNG 100 Software Upgrade Automation Tool".

36.5 Examples

The following is an example of the automated software rollback tool command for software rollback on a single NE:
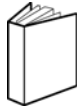
```
./rollback.pl --swp OSWP/L6GPAA40.046 --isam 138.120.217.112 --logfile
rollback_40.046.log
```

The following is an example of the automated software rollback tool command for software rollback on multiple NEs:

```
./rollback.pl --swp OSWP/L6GPAA40.046 --sessions 2 --hosts /etc/hosts
--logfile rollback_40.046.log
```

Customer document and product support

Customer documentation

[Customer Documentation Welcome Page](#)

Technical Support

[Product Support Portal](#)

Documentation feedback

[Customer Documentation Feedback](#)